Actualización y downgrade de los controladores Catalyst 9800: consejos y trucos

Contenido

Introducción

Este documento describe las cosas que se deben tener en cuenta al actualizar o degradar un Controlador de LAN Inalámbrica (WLC) Catalyst 9800.

Antes de continuar

Este documento no tiene como objetivo reemplazar las notas de la versión, que siempre deben ser el documento de acceso al actualizar. El objetivo es facilitar la actualización a través de varias versiones destacando los cambios más impactantes entre las versiones.

Este documento no reemplaza la lectura de las notas de la versión de su versión de software de destino. Realice una copia de seguridad de la configuración y tome todas las precauciones necesarias antes de continuar con la actualización.

De forma predeterminada, el servidor http del 9800 no está asignado estadísticamente a un certificado/punto de confianza específico que puede generar cambios después de la actualización. Establezca el servidor HTTP en un punto de confianza estático (preferiblemente en un certificado que haya emitido para este fin, o en el certificado MIC en caso contrario) en la configuración antes de actualizar.

El caso especial de las versiones especiales de ingeniería

Las versiones especiales de ingeniería no admiten la actualización ISSU desde ellas. Este documento solo se centra en las versiones públicas publicadas en cisco.com, por lo tanto, si se encuentra en una compilación especial de ingeniería, consulte las notas de la versión que recibió junto con ellas para obtener asistencia para todas sus preguntas sobre actualizaciones.

Actualizar

Puede leer directamente las notas en la versión de software de destino que desea. Las sugerencias aplicables en varias versiones se repiten cada vez para su comodidad. No actualice más de 3 versiones a la vez. Por ejemplo, la actualización de 16.12.1 a 17.3.2 está cubierta por este documento, pero no las actualizaciones de 16.12 a 17.4. En tal escenario, pase por 17.3 y verifique las notas bajo la sección 17.3, realice la actualización y luego mire la sección 17.4 y prepare la segunda actualización. Como conclusión, las sugerencias enumeradas ya no se repiten después de 3 versiones principales, aunque sigan siendo válidas ya que el documento supone que se van a realizar versiones principales intermedias.

Gibraltar

16.12.2

- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, ésta se interrumpirá debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.

- No utilice más de 31 caracteres para los nombres de AP. Si el nombre del AP es de 32 caracteres o más, puede conducir a una caída del controlador.

- No implemente archivos OVA directamente en VMware ESXi 6.5. Se recomienda utilizar una herramienta OVF para implementar los archivos OVA.

16.12.3

- 16.12.3 es la primera versión que impone el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, ésta se interrumpirá debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.

- No utilice más de 31 caracteres para los nombres de AP. Si el nombre del AP es de 32 caracteres o más, puede conducir a una caída del controlador.

- No implemente archivos OVA directamente en VMware ESXi 6.5. Se recomienda utilizar una herramienta OVF para implementar los archivos OVA.

16.12.4

- 16.12.3 y 17.2.1 son las primeras versiones en hacer cumplir el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, ésta se interrumpirá debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.

- No utilice más de 31 caracteres para los nombres de AP. Si el nombre del AP es de 32 caracteres o más, puede conducir a una caída del controlador.

- No implemente archivos OVA directamente en VMware ESXi 6.5. Se recomienda utilizar una herramienta OVF para implementar los archivos OVA.

16.12.5

- Igual que 16.12.4

16.12.6a

- Igual que 16.12.4

16.12.7

- Igual que 16.12.4

Amsterdam

17.1.1

- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, se interrumpirá debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.
- A partir de esta versión, se introduce una nueva comprobación de disponibilidad del gateway. Los AP envían solicitudes de eco ICMP (ping) periódicas al gateway predeterminado para verificar la conectividad. Debe asegurarse de que el filtrado de tráfico entre los AP y la gateway predeterminada (como las ACL) permita los pings ICMP entre el AP y la gateway predeterminada. Si estos pings se bloquean, incluso si la conectividad entre el controlador y el AP está activa, los AP se recargan en el intervalo de 4 horas.

17.2.1

- 16.12.3 y 17.2.1 son las primeras versiones en hacer cumplir el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, puede caer debido al cambio de asignación predeterminada. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.
- A partir de la versión 17.1, se introduce una nueva comprobación de disponibilidad del gateway. Los AP envían solicitudes de eco ICMP (ping) periódicas al gateway predeterminado para verificar la conectividad. Debe asegurarse de que el filtrado de tráfico entre los AP y la gateway predeterminada (como las ACL) permita los pings ICMP entre el AP y la gateway predeterminada. Si estos pings se bloquean, incluso si la conectividad entre el controlador y el AP está activa, los AP se recargan en el intervalo de 4 horas.

17.3.1

- 16.12.3 y 17.2.1 son las primeras versiones en hacer cumplir el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, se interrumpirá debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.
- A partir de la versión 17.1, se introduce una nueva comprobación de disponibilidad del gateway. Los AP envían solicitudes de eco ICMP (ping) periódicas al gateway predeterminado para verificar la conectividad. Debe asegurarse de que el filtrado de tráfico entre los AP y la gateway predeterminada (como las ACL) permita los pings ICMP entre el AP y la gateway predeterminada. Si estos pings se bloquean, incluso si la conectividad entre el controlador y el AP está activa, los AP se recargan en el intervalo de 4 horas.
- Si ha configurado el modo FIPS, asegúrese de quitar la configuración **security wpa wpa1 cipher tkip** de cualquier WLAN antes de actualizar Cisco IOS XE Amsterdam 17.3.x desde una versión anterior. Si no lo hace, la seguridad WLAN se establece en TKIP, que no es compatible con el modo FIPS. Después de la actualización, debe volver a configurar la WLAN con AES.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el controlador inalámbrico Cisco Catalyst 9800-CL requiere 16 GB de espacio en disco para nuevas implementaciones. Solo es posible aumentar el tamaño del espacio en disco mediante una reinstalación con una imagen 17.3.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el nombre del AP solo puede tener hasta 32 caracteres.
- Para la autenticación de direcciones MAC locales (de clientes o AP), sólo se admite el formato aaaabbbcccc (sin separador) a partir de 17.3.1. Esto significa que la autenticación falla si agrega la dirección MAC con separadores en la interfaz de usuario web o CLI.
- A partir de esta versión en adelante, los AP se recargarán después de 4 horas si no pueden unirse a un WLC, no pueden hacer ping a su gateway Y ARP a su gateway (los 3 deben fallar para que el AP se reinicie). Esta es una mejora (Id. de error de Cisco CSCvt89970) a la anterior verificación de gateway solo icmp de versiones anteriores
- A partir de la versión 17.3.1, la nueva forma de configurar el código de país para los puntos de acceso es el comando "Wireless country <1 country code>" que puede repetir varias veces con diferentes códigos de país. Esto permite aumentar la cantidad máxima de código de país en más de 20. Los comandos "ap country" todavía están presentes y seguirán funcionando, sin embargo, considere cambiarlos a los comandos "Wireless country" ya que los comandos ap country quedarán obsoletos en una versión futura

17.3.2

- 16.12.3 y 17.2.1 son las primeras versiones en hacer cumplir el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice

otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.

- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, se desactivará debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.
- A partir de la versión 17.1, se introduce una nueva comprobación de disponibilidad del gateway. Los AP envían solicitudes de eco ICMP (ping) periódicas al gateway predeterminado para verificar la conectividad. Debe asegurarse de que el filtrado de tráfico entre los AP y la gateway predeterminada (como las ACL) permita los pings ICMP entre el AP y la gateway predeterminada. Si se bloquean estos pings, incluso si la conectividad entre el controlador y el AP está activa, los AP se recargarán en el intervalo de 4 horas.
- Si ha configurado el modo FIPS, asegúrese de quitar la configuración **security wpa wpa1 cipher tkip** de cualquier WLAN antes de actualizar Cisco IOS XE Amsterdam 17.3.x desde una versión anterior. Si no lo hace, la seguridad WLAN se establecerá en TKIP, lo que no se admite en el modo FIPS. Después de la actualización, debe volver a configurar la WLAN con AES.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el controlador inalámbrico Cisco Catalyst 9800-CL requiere 16 GB de espacio en disco para nuevas implementaciones. Solo es posible aumentar el tamaño del espacio en disco mediante una reinstalación con una imagen 17.3.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el nombre del AP solo puede tener hasta 32 caracteres.
- Para la autenticación de direcciones MAC locales (de clientes o AP), sólo se admite el formato aaaabbbcccc (sin separador) a partir de 17.3.1. Esto significa que la autenticación fallará si agrega la dirección MAC con separadores en la interfaz de usuario web o CLI.
- A partir de 17.3.1 en adelante, los AP se recargarán después de 4 horas si no pueden unirse a un WLC, no pueden hacer ping a su gateway Y ARP a su gateway (los 3 deben fallar para que el AP se reinicie). Esta es una mejora (Id. de error de Cisco CSCvt89970) a la anterior verificación de gateway solo icmp de versiones anteriores
- A partir de la versión 17.3.1, la nueva forma de configurar el código de país para los puntos de acceso es el comando "Wireless country <1 country code>" que puede repetir varias veces con diferentes códigos de país. Esto permite aumentar la cantidad máxima de código de país en más de 20. Los comandos "ap country" todavía están presentes y seguirán funcionando, sin embargo, considere cambiarlos a los comandos "Wireless country" ya que los comandos ap country quedarán obsoletos en una versión futura.

17.3.3

- 16.12.3 y 17.2.1 son las primeras versiones en hacer cumplir el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, se desactivará debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.

- A partir de la versión 17.1, se introduce una nueva comprobación de disponibilidad del gateway. Los AP envían solicitudes de eco ICMP (ping) periódicas al gateway predeterminado para verificar la conectividad. Debe asegurarse de que el filtrado de tráfico entre los AP y la gateway predeterminada (como las ACL) permita los pings ICMP entre el AP y la gateway predeterminada. Si se bloquean estos pings, incluso si la conectividad entre el controlador y el AP está activa, los AP se recargarán en el intervalo de 4 horas.
- Si ha configurado el modo FIPS, asegúrese de quitar la configuración **security wpa wpa1 cipher tkip** de cualquier WLAN antes de actualizar Cisco IOS XE Amsterdam 17.3.x desde una versión anterior. Si no lo hace, la seguridad WLAN se establecerá en TKIP, lo que no se admite en el modo FIPS. Después de la actualización, debe volver a configurar la WLAN con AES.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el controlador inalámbrico Cisco Catalyst 9800-CL requiere 16 GB de espacio en disco para nuevas implementaciones. Solo es posible aumentar el tamaño del espacio en disco mediante una reinstalación con una imagen 17.3.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el nombre del AP solo puede tener hasta 32 caracteres.
- Para la autenticación de direcciones MAC locales (de clientes o AP), sólo se admite el formato aaaabbbcccc (sin separador) a partir de 17.3.1. Esto significa que la autenticación fallará si agrega la dirección MAC con separadores en la interfaz de usuario web o CLI.
- A partir de 17.3.1 en adelante, los AP se recargarán después de 4 horas si no pueden unirse a un WLC, no pueden hacer ping a su gateway Y ARP a su gateway (los 3 deben fallar para que el AP se reinicie). Esta es una mejora (Id. de error de Cisco CSCvt89970) la verificación de la gateway solo icmp anterior de versiones anteriores
- A partir de la versión 17.3.1, la nueva forma de configurar el código de país para los puntos de acceso es el comando "Wireless country <1 country code>" que puede repetir varias veces con diferentes códigos de país. Esto permite aumentar la cantidad máxima de código de país en más de 20. Los comandos "ap country" todavía están presentes y seguirán funcionando, sin embargo, considere cambiarlos a los comandos "Wireless country" ya que los comandos ap country quedarán obsoletos en una versión futura.
- El WLC puede fallar si sus AP tienen hostnames de más de 32 caracteres (Id. de bug Cisco CSCvy11981)

17.3.4

- 16.12.3 y 17.2.1 son las primeras versiones en hacer cumplir el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de política predeterminada, se desactivará debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.
- A partir de la versión 17.1, se introduce una nueva comprobación de disponibilidad del gateway. Los AP envían solicitudes de eco ICMP (ping) periódicas al gateway predeterminado para verificar la conectividad. Debe asegurarse de que el filtrado de tráfico entre los AP y la gateway predeterminada (como las ACL) permita los pings ICMP entre el AP y la gateway predeterminada. Si se bloquean estos pings, incluso si la conectividad entre el controlador y el AP está activa, los AP se recargarán en el intervalo de 4 horas.

- Si ha configurado el modo FIPS, asegúrese de quitar la configuración **security wpa wpa1 cipher tkip** de cualquier WLAN antes de actualizar Cisco IOS XE Amsterdam 17.3.x desde una versión anterior. Si no lo hace, la seguridad WLAN se establecerá en TKIP, lo que no se admite en el modo FIPS. Después de la actualización, debe volver a configurar la WLAN con AES.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el controlador inalámbrico Cisco Catalyst 9800-CL requiere 16 GB de espacio en disco para nuevas implementaciones. Solo es posible aumentar el tamaño del espacio en disco mediante una reinstalación con una imagen 17.3.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el nombre del AP solo puede tener hasta 32 caracteres.
- Para la autenticación de direcciones MAC locales (de clientes o AP), sólo se admite el formato aaaabbbcccc (sin separador) a partir de 17.3.1. Esto significa que la autenticación fallará si agrega la dirección MAC con separadores en la interfaz de usuario web o CLI.
- A partir de la 17.3.1 en adelante, los APsl se recargan después de 4 horas si no pueden unirse a un WLC, no pueden hacer ping a su gateway Y ARP a su gateway (los 3 deben fallar para que el AP se reinicie). Esta es una mejora (Id. de error de Cisco CSCvt89970) a la anterior verificación de gateway solo icmp de versiones anteriores
- A partir de la versión 17.3.1, la nueva forma de configurar el código de país para los puntos de acceso es el comando "Wireless country <1 country code>" que puede repetir varias veces con diferentes códigos de país. Esto permite aumentar la cantidad máxima de código de país en más de 20. Los comandos "ap country" todavía están presentes y siguen funcionando, sin embargo, considere cambiarlos a los comandos "Wireless country" ya que los comandos ap country están planeados para ser desaprobados en una futura versión.
- Al actualizar a 17.3.4 y versiones posteriores, se recomienda tener el cargador de inicialización/rommon 16.12.5r instalado en los controladores donde sea aplicable (9800-80). El 9800-40 no tiene un rommon 16.12.5r en este momento y no necesita una actualización rommon).
- La actualización del controlador, desde Cisco IOS XE Bengaluru 17.3.x a cualquier versión que use ISSU, puede fallar si se configura el comando **snmp-server enable traps hsrp**. Asegúrese de quitar el comando **snmp-server enable traps hsrp** de la configuración antes de iniciar una actualización ISSU porque el comando **snmp-server enable traps hsrp** se quita de Cisco IOS XE Bengaluru 17.4.x.

- Al actualizar a Cisco IOS XE 17.3.x y versiones posteriores, si se habilita el comando ip http active-session-modules none, no podrá acceder a la GUI del controlador mediante HTTPS. Para acceder a la GUI mediante HTTPS, ejecute estos comandos:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

17.3.5

- Debido al ID de bug de Cisco CSCwb13784 , si su MTU de trayectoria es inferior a 1500 bytes, es posible que los AP no puedan unirse. Descargue el parche SMU disponible para 17.3.5 para solucionar este problema.
- 16.12.3 y 17.2.1 son las primeras versiones en hacer cumplir el soporte de solamente los SFP que se enumeran como soportados en la documentación. Los SFP que no aparecen en la lista provocan una situación de puerto inactivo. Verifique la lista de SFP admitidos y asegúrese de que los SFP sean compatibles para evitar que los puertos de datos se desactiven después de la actualización
- El archivo de actualización de esta versión puede ser demasiado grande para la carga HTTP (al realizar la actualización de la interfaz de usuario web) si se encuentra en la versión 16.12.1. Utilice otro método de transferencia o vaya a través de 16.12.2, que permite cargar archivos más grandes a través de la interfaz de usuario web.
- Desde Cisco IOS XE Gibraltar 16.12.2s, se ha eliminado la asignación automática de WLAN al perfil de política predeterminado bajo la etiqueta de política predeterminada. Si está actualizando desde una versión anterior a Cisco IOS XE Gibraltar 16.12.2s, y si su red inalámbrica utiliza la etiqueta de

política predeterminada, se desactivará debido al cambio de asignación predeterminado. Para restaurar el funcionamiento de la red, agregue la WLAN necesaria a las asignaciones de políticas en la etiqueta de política predeterminada.

- A partir de la versión 17.1, se introduce una nueva comprobación de disponibilidad del gateway. Los AP envían solicitudes de eco ICMP (ping) periódicas al gateway predeterminado para verificar la conectividad. Debe asegurarse de que el filtrado de tráfico entre los AP y la gateway predeterminada (como las ACL) permita los pings ICMP entre el AP y la gateway predeterminada. Si se bloquean estos pings, incluso si la conectividad entre el controlador y el AP está activa, los AP se recargarán en el intervalo de 4 horas.
- Si ha configurado el modo FIPS, asegúrese de quitar la configuración **security wpa wpa1 cipher tkip** de cualquier WLAN antes de actualizar Cisco IOS XE Amsterdam 17.3.x desde una versión anterior. Si no lo hace, la seguridad WLAN se establecerá en TKIP, lo que no se admite en el modo FIPS. Después de la actualización, debe volver a configurar la WLAN con AES.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el controlador inalámbrico Cisco Catalyst 9800-CL requiere 16 GB de espacio en disco para nuevas implementaciones. Solo es posible aumentar el tamaño del espacio en disco mediante una reinstalación con una imagen 17.3.
- A partir de Cisco IOS XE Amsterdam 17.3.1 en adelante, el nombre del AP solo puede tener hasta 32 caracteres.
- Para la autenticación de direcciones MAC locales (de clientes o AP), sólo se admite el formato aaaabbbcccc (sin separador) a partir de 17.3.1. Esto significa que la autenticación fallará si agrega la dirección MAC con separadores en la interfaz de usuario web o CLI.
- A partir de la 17.3.1 en adelante, los APsl se recargan después de 4 horas si no pueden unirse a un WLC, no pueden hacer ping a su gateway Y ARP a su gateway (los 3 deben fallar para que el AP se reinicie). Esta es una mejora (Id. de error de Cisco CSCvt89970) a la anterior verificación de gateway solo icmp de versiones anteriores
- A partir de la versión 17.3.1, la nueva forma de configurar el código de país para los puntos de acceso es el comando "Wireless country <1 country code>" que puede repetir varias veces con diferentes códigos de país. Esto permite aumentar la cantidad máxima de código de país en más de 20. Los comandos "ap country" todavía están presentes y siguen funcionando, sin embargo, considere cambiarlos a los comandos "Wireless country" ya que los comandos ap country están planeados para ser desaprobados en una futura versión.
- Al actualizar a 17.3.4 y versiones posteriores, se recomienda tener el cargador de inicialización/rommon 16.12.5r instalado en los controladores donde sea aplicable (9800-80). El 9800-40 no tiene un rommon 16.12.5r en este momento y no necesita una actualización rommon).
- La actualización del controlador, desde Cisco IOS XE Bengaluru 17.3.x a cualquier versión que use ISSU, puede fallar si se configura el comando **snmp-server enable traps hsrp**. Asegúrese de quitar el comando **snmp-server enable traps hsrp** de la configuración antes de iniciar una actualización ISSU porque el comando **snmp-server enable traps hsrp** se quita de Cisco IOS XE Bengaluru 17.4.x.

- Al actualizar a Cisco IOS XE 17.3.x y versiones posteriores, si se habilita el comando ip http active-session-modules none, no podrá acceder a la GUI del controlador mediante HTTPS. Para acceder a la GUI mediante HTTPS, ejecute estos comandos:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

Bengaluru

17.4.1

- A partir de la versión 17.4.1, los AP basados en Cisco IOS de la onda 1 ya no son compatibles (1700, 2700, 3700 y 1570) con la excepción de IW3700.
- Las WLAN se pueden apagar después de la actualización si no son WPA (SSID de invitado, abierto o

CWA) y tienen FT adaptable configurado. La solución es eliminar la configuración de FT adaptable antes de la actualización (Id. de error de Cisco CSCvx34349). La configuración FT adaptable no tiene sentido en SSID que no sea WPA, por lo que no se pierde nada al eliminarla.
- El WLC puede fallar si sus AP tienen hostnames más de 32 caracteres (Id. de bug Cisco CSCvy11981)

17.5.1

- A partir de la versión 17.4.1, los AP basados en Cisco IOS de la onda 1 ya no son compatibles (1700, 2700, 3700 y 1570) con la excepción de IW3700.
- A partir de Cisco IOS XE Bengaluru Release 17.4.1, la solución de telemetría proporciona un nombre para la dirección del receptor en lugar de la dirección IP para los datos de telemetría. Esta es una opción adicional. Durante la reversión del controlador y la subsiguiente actualización, es probable que haya un problema: la versión de actualización utiliza los receptores recién nombrados, y estos no se reconocen en la reversión. La nueva configuración se rechaza y falla en la actualización posterior. La pérdida de configuración se puede evitar cuando la actualización o la reversión se realiza desde Cisco DNA Center.
- Las WLAN se pueden apagar después de la actualización si no son WPA (SSID de invitado, abierto o CWA) y tienen FT adaptable configurado. La solución es eliminar la configuración de FT adaptable antes de la actualización (Id. de error de Cisco CSCvx34349). La configuración FT adaptable no tiene sentido en SSID que no sea WPA, por lo que no se pierde nada al eliminarla.
- El WLC puede fallar si sus AP tienen hostnames más de 32 caracteres (Id. de bug Cisco CSCvy11981)
- Al actualizar la GUI de una versión a otra, se recomienda borrar la caché del navegador para que todas las páginas de la GUI se vuelvan a cargar correctamente.

- Al actualizar a Cisco IOS XE 17.3.x y versiones posteriores, si se habilita el comando ip http active-session-modules none, no podrá acceder a la GUI mediante HTTPS. Para acceder a la GUI mediante HTTPS, ejecute estos comandos:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

- Si encuentra el error ERR_SSL_VERSION_OR_CIPHER_MISMATCH en la GUI después de un reinicio o un desperfecto del sistema, le recomendamos que regenere el certificado de punto de confianza.

  El procedimiento para generar un nuevo punto de confianza autofirmado es el siguiente:

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http au
```

```
! use local or aaa as applicable.
```

17.6.1

- A partir de la versión 17.4.1, los AP basados en Cisco IOS de la onda 1 ya no son compatibles (1700, 2700, 3700 y 1570) con la excepción de IW3700.
- A partir de Cisco IOS XE Bengaluru Release 17.4.1, la solución de telemetría proporciona un nombre para la dirección del receptor en lugar de la dirección IP para los datos de telemetría. Esta es una opción adicional. Durante la reversión del controlador y la subsiguiente actualización, es probable que haya un problema: la versión de actualización utiliza los receptores recién nombrados, y estos no se reconocen en la reversión. La nueva configuración se rechaza y falla en la actualización posterior. La pérdida de configuración se puede evitar cuando la actualización o la reversión se realiza desde Cisco DNA Center.
- Las WLAN se pueden apagar después de la actualización si no son WPA (SSID de invitado, abierto o CWA) y tienen FT adaptable configurado. La solución es eliminar la configuración de FT adaptable antes de la actualización (Id. de error de Cisco CSCvx34349). La configuración FT adaptable no tiene sentido en SSID que no sea WPA, por lo que no se pierde nada al eliminarla.
- Al actualizar la GUI de una versión a otra, se recomienda borrar la caché del navegador para que todas las páginas de la GUI se vuelvan a cargar correctamente.
- Un AP que se unió a un WLC 17.6.1 o posterior no puede unirse a un WLC de AireOS a menos que ejecute 8.10.162 o posterior, o 8.5.176.2 o posterior código 8.5.
- Actualizando a 17.6,1 y versiones posteriores, se recomienda tener el cargador de inicialización/rommon 16.12.5r instalado en los controladores donde sea aplicable (9800-80. El 9800-40 no tiene un rommon 16.12.5r en este momento y no necesita una actualización rommon).
- La actualización del controlador, desde Cisco IOS XE Bengaluru 17.3.x a cualquier versión que use ISSU, puede fallar si se configura el comando **snmp-server enable traps hsrp**. Asegúrese de quitar el comando **snmp-server enable traps hsrp** de la configuración antes de iniciar una actualización ISSU porque el comando **snmp-server enable traps hsrp** se quita de Cisco IOS XE Bengaluru 17.4.x.

- Al actualizar a Cisco IOS XE 17.3.x y versiones posteriores, si el comando ip http active-session-modules none está habilitado, el acceso HTTPS a la GUI del controlador no funciona. Para acceder a la GUI mediante HTTPS, ejecute estos comandos:

    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist
    -

- Si encuentra el error ERR_SSL_VERSION_OR_CIPHER_MISMATCH en la GUI después de un reinicio o un desperfecto del sistema, le recomendamos que regenere el certificado de punto de confianza.

  El procedimiento para generar un nuevo punto de confianza autofirmado es el siguiente:

```
configure terminal
```

```
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http au
```

```
! use local or aaa as applicable.
```

17.6.2

- A partir de la versión 17.4.1, los AP basados en Cisco IOS de la onda 1 ya no son compatibles (1700, 2700, 3700 y 1570) con la excepción de IW3700.
- A partir de Cisco IOS XE Bengaluru Release 17.4.1, la solución de telemetría proporciona un nombre para la dirección del receptor en lugar de la dirección IP para los datos de telemetría. Esta es una opción adicional. Durante la reversión del controlador y la subsiguiente actualización, es probable que haya un problema: la versión de actualización utiliza los receptores recién nombrados, y estos no se reconocen en la reversión. La nueva configuración se rechaza y falla en la actualización posterior. La pérdida de configuración se puede evitar cuando la actualización o la reversión se realiza desde Cisco DNA Center.
- Las WLAN se pueden apagar después de la actualización si no son WPA (SSID de invitado, abierto o CWA) y tienen FT adaptable configurado. La solución es eliminar la configuración de FT adaptable antes de la actualización (Id. de error de Cisco CSCvx34349) La configuración FT adaptativa no tiene sentido en SSID que no sea WPA, por lo que no se pierde nada al eliminarla.
- Al actualizar la GUI de una versión a otra, se recomienda borrar la caché del navegador para que todas las páginas de la GUI se vuelvan a cargar correctamente.
- Un AP que se unió a un WLC 17.6.1 o posterior no puede unirse a un WLC de AireOS a menos que ejecute 8.10.162 o posterior, o 8.5.176.2 o posterior código 8.5.
- Actualizando a 17.6,1 y versiones posteriores, se recomienda tener el cargador de inicialización/rommon 16.12.5r instalado en los controladores donde sea aplicable (el 9800-80). El 9800-40 no tiene un rommon 16.12.5r en este momento y no necesita una actualización rommon).
- La actualización del controlador, desde Cisco IOS XE Bengaluru 17.3.x a cualquier versión que use ISSU, puede fallar si se configura el comando **snmp-server enable traps hsrp**. Asegúrese de quitar el comando **snmp-server enable traps hsrp** de la configuración antes de iniciar una actualización ISSU porque el comando **snmp-server enable traps hsrp** se quita de Cisco IOS XE Bengaluru 17.4.x.
    -
- Al actualizar a Cisco IOS XE 17.3.x y versiones posteriores, si el comando ip http active-session-modules none está habilitado, el acceso a la GUI del controlador HTTPS no funciona. Para acceder a la GUI mediante HTTPS, ejecute estos comandos:
    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

- No utilice más de 31 caracteres para los nombres de AP. Si el nombre del AP es de 32 caracteres o más, puede ocurrir una caída del controlador.
- Si encuentra el error ERR_SSL_VERSION_OR_CIPHER_MISMATCH en la GUI después de un reinicio o un desperfecto del sistema, le recomendamos que regenere el certificado de punto de confianza.

  El procedimiento para generar un nuevo punto de confianza autofirmado es el siguiente:

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http au
```

```
! use local or aaa as applicable.
```

Cupertino

En esta sección se supone que está comenzando desde la versión 17.6.1 o posterior y actualizando a una versión de Cupertino. Si está actualizando directamente desde una versión anterior (que podría ser compatible, compruebe las notas de la versión para estar seguro), lea las advertencias de la sección 17.3 y 17.6.

17.7.1

- No utilice más de 31 caracteres para los nombres de AP. Si el nombre del AP es de 32 caracteres o más, puede ocurrir una caída del controlador.
- 17.7.1 requiere que el código de país de AP se configure en los perfiles de unión de AP.
- Debido al Id. de bug Cisco CSCvu22886 , si tiene AP 9130 o 9124, debe pasar por 17.3.5a al actualizar a 17.7.1 o posterior desde una versión anterior a 17.3.4
- A partir de Cisco IOS XE Cupertino 17.7.1 en adelante, para el controlador inalámbrico Cisco Catalyst 9800-CL, asegúrese de completar los informes de medición de utilización de recursos (RUM) y de que el ACK esté disponible en la instancia del producto al menos una vez. De este modo se garantiza que la información de uso correcta y actualizada se refleja en Cisco Smart Software Manager (CSSM). Si no lo hace, un máximo de 50 AP podrán unirse a un 9800-CL hasta que se ACK un informe de licencia.

17.8.1

- No utilice más de 31 caracteres para los nombres de AP. Si el nombre del AP es de 32 caracteres o más, puede ocurrir una caída del controlador.
- 17.7.1 requiere que el código de país de AP se configure en los perfiles de unión de AP.
- Debido al Id. de bug Cisco CSCvu22886, si tiene AP 9130 o 9124, debe pasar por 17.3.5a al actualizar a 17.7.1 o posterior desde una versión anterior a 17.3.4
- A partir de Cisco IOS XE Cupertino 17.7.1 en adelante, para el controlador inalámbrico Cisco Catalyst 9800-CL, asegúrese de completar los informes de medición de utilización de recursos (RUM) y de que el ACK esté disponible en la instancia del producto al menos una vez. De este modo se garantiza que la información de uso correcta y actualizada se refleja en Cisco Smart Software Manager (CSSM). Si no lo hace, un máximo de 50 AP podrán unirse a un 9800-CL hasta que se ACK un informe de licencia.

17.9.x

- Los AP que ejecutan Cisco IOS-XE 17.9.3 podrían encontrar problemas al intentar actualizar su software debido a espacio insuficiente en el directorio /tmp. Cuando el espacio /tmp en el AP se llena, evita la descarga de la nueva imagen del AP. En tales casos, recomendamos que reinicie el AP.

- 11AC Wave 2 AP puede entrar en un bucle de arranque al actualizar el software sobre un link WAN. Para obtener más información, visite: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- Las versiones 17.9.3 y posteriores ofrecen compatibilidad con los puntos de acceso basados en Cisco IOS (series x700 y 1570). No se admitieron entre 17.4 y 17.9.2. La compatibilidad con estos puntos de acceso no va más allá del ciclo de vida normal del producto. Consulte los boletines de fin de soporte técnico individuales en Cisco.com.
- La actualización del controlador de Cisco IOS XE Bengaluru 17.3.x a Cisco IOS XE Bengaluru 17.6.x o Cisco IOS XE Cupertino 17.9.x o posterior mediante ISSU puede fallar si se configura el comando domain. Asegúrese de ejecutar el comando no domain antes de iniciar una actualización ISSU porque el comando domain se ha eliminado de Cisco IOS XE Bengaluru 17.6.x.
- A partir de Cisco IOS XE Cupertino 17.7.1 en adelante, para el controlador inalámbrico Cisco Catalyst 9800-CL, asegúrese de completar los informes de medición de utilización de recursos (RUM) y de que el ACK esté disponible en la instancia del producto al menos una vez. De este modo se garantiza que la información de uso correcta y actualizada se refleja en Cisco Smart Software Manager (CSSM). Si no lo hace, un máximo de 50 AP podrán unirse a un 9800-CL hasta que se ACK un informe de licencia.
- No se admite la fragmentación inferior a 1500 para los paquetes RADIUS generados por clientes inalámbricos en la interfaz Gi0 (OOB).
- A partir de la versión 17.3, el 9800-CL requiere 16 gb de espacio en disco para funcionar correctamente. Usted no puede aumentar el tamaño dinámicamente si su instancia del WLC comenzó con un OVA de 8gb (de antes de 17.3). la única manera es crear un nuevo WLC a partir de un OVA fechado después de 17.3
- Es posible que el controlador inalámbrico Cisco Catalyst 9800-L no pueda responder a las señales BREAK recibidas en el puerto de la consola durante el arranque, lo que impide que los usuarios accedan a ROMMON. Este problema se observa en los controladores fabricados hasta noviembre de 2019, con la configuración predeterminada config-register de 0x2102. Este problema puede evitarse si configura config-register en 0x2002. Este problema se corrige en el ROMMON 16.12(3r) para el controlador inalámbrico Catalyst 9800-L de Cisco. Para obtener información sobre cómo actualizar ROMMON, vea la sección Actualización de ROMMON para los Controladores Inalámbricos Cisco Catalyst 9800-L del documento *Actualización de Dispositivos de Hardware Programables de Campo para los Controladores Inalámbricos Cisco Catalyst 9800 Series*.

- Si se muestra este mensaje de error después de un reinicio o un desperfecto del sistema, se recomienda que regenere el certificado de punto de confianza:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  Utilice estos comandos en el orden especificado para generar un nuevo certificado de punto de confianza autofirmado:

  1. **device#** configure terminal
  2. device(config)# no crypto pki trustpoint *trustpoint_name*
  3. device(config)# no ip http server
  4. **device(config)#** no ip http secure-server
  5. **device(config)#** ip http server
  6. **device(config)#** ip http secure-server
  7. device(config)# ip http authentication *local/aaa*

- Verifique que su dirección MAC de movilidad esté configurada con el comando **wireless mobility mac-address**
- Estos protocolos ahora se soportan a través del puerto de servicio en 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infraestructura Cisco Prime
  - TELNET
  - GUI del controlador
  - DNS
  - Transferencia de archivos
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - Licencias para que la función Smart Licensing se comunique con CSSM
  - Netconf
  - Netflow
  - NTP

    - RADIUS (incluida CoA)
    - Restconf
    - SNMP (Protocolo de administración de red simple)
    - SSH
    - SYSLOG
    - TACACS+

- La imagen AP para 17.9 es más grande que la flash AP permitida originalmente. Si ve que el AP se queja de no tener suficiente espacio al descargar la imagen 17.9, probablemente se deba a que no respetó la trayectoria de actualización a través de 17.3.5 como se indica en las notas de la versión o a que su AP está ejecutando una imagen AireOS más antigua. Ya sea transitando a través de ha 17.3.5 o WLC posterior o actualizando la imagen de AireOS a la última cambiará el tamaño de la flash AP para permitir descargar la imagen 17.9

Dublín

17.10.1

- La función Cisco Centralized Key Management (CCKM) está siendo obsoleta en Cisco IOS XE Dublin 17.10.x.
- Smart Call Home está quedando obsoleto en favor de Smart Transport para las licencias

- Los AP que ejecutan Cisco IOS-XE 17.9.3 o posterior pueden encontrar problemas al intentar actualizar su software debido a espacio insuficiente en el directorio /tmp. Cuando el espacio /tmp en el AP se llena, evita la descarga de la nueva imagen del AP. En tales casos, recomendamos que reinicie el AP.

  Los AP de la onda 2 pueden entrar en un loop de arranque cuando se actualiza el software sobre un link WAN. Para obtener más información, visite: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- A partir de Cisco IOS XE Cupertino 17.7.1 en adelante, para el controlador inalámbrico Cisco Catalyst 9800-CL, asegúrese de completar los informes de medición de utilización de recursos (RUM) y de que el ACK esté disponible en la instancia del producto al menos una vez. De este modo se garantiza que la información de uso correcta y actualizada se refleja en Cisco Smart Software Manager (CSSM). Si no lo hace, un máximo de 50 AP podrán unirse a un 9800-CL hasta que se ACK un informe de licencia.
- No se admite la fragmentación inferior a 1500 para los paquetes RADIUS generados por clientes inalámbricos en la interfaz Gi0 (OOB).
- A partir de la versión 17.3, el 9800-CL requiere 16 gb de espacio en disco para funcionar correctamente. Usted no puede aumentar el tamaño dinámicamente si su instancia del WLC comenzó con un OVA de 8gb (de antes de 17.3). la única manera es crear un nuevo WLC a partir de un OVA fechado después de 17.3
- Es posible que el controlador inalámbrico Cisco Catalyst 9800-L no pueda responder a las señales BREAK recibidas en el puerto de la consola durante el arranque, lo que impide que los usuarios accedan a ROMMON. Este problema se observa en los controladores fabricados hasta noviembre de 2019, con la configuración predeterminada config-register de 0x2102. Este problema puede evitarse si configura config-register en 0x2002. Este problema se corrige en el ROMMON 16.12(3r) para el

controlador inalámbrico Catalyst 9800-L de Cisco. Para obtener información sobre cómo actualizar ROMMON, vea la sección Actualización de ROMMON para los Controladores Inalámbricos Cisco Catalyst 9800-L del documento *Actualización de Dispositivos de Hardware Programables de Campo para los Controladores Inalámbricos Cisco Catalyst 9800 Series*.

- Si se muestra este mensaje de error después de un reinicio o un desperfecto del sistema, se recomienda que regenere el certificado de punto de confianza:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilice estos comandos en el orden especificado para generar un nuevo certificado de punto de confianza autofirmado:

1. **device#** configure terminal
2. device(config)# no crypto pki trustpoint *trustpoint_name*
3. device(config)# no ip http server
4. **device(config)#** no ip http secure-server
5. **device(config)#** ip http server
6. **device(config)#** ip http secure-server
7. device(config)# ip http authentication *local/aaa*

- Verifique que su dirección MAC de movilidad esté configurada con el comando **wireless mobility mac-address**
- Estos protocolos ahora se soportan a través del puerto de servicio en 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infraestructura Cisco Prime
  - TELNET
  - GUI del controlador
  - DNS
  - Transferencia de archivos
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - Licencias para que la función Smart Licensing se comunique con CSSM
  - Netconf

    - Netflow
    - NTP
    - RADIUS (incluida CoA)
    - Restconf
    - SNMP (Protocolo de administración de red simple)
    - SSH
    - SYSLOG
    - TACACS+
- La imagen AP para 17.9 es más grande que la flash AP permitida originalmente. Si ve que el AP se queja de no tener suficiente espacio al descargar la imagen 17.9, probablemente se deba a que no respetó la trayectoria de actualización a través de 17.3.5 como se indica en las notas de la versión o a que su AP está ejecutando una imagen AireOS más antigua. Ya sea transitando a través de ha 17.3.5 o WLC posterior o actualizando la imagen de AireOS a la última cambiará el tamaño de la flash AP para permitir descargar la imagen 17.9

17.11.1

- La función Cisco Centralized Key Management (CCKM) está siendo obsoleta en Cisco IOS XE Dublin 17.10.x.
- Smart Call Home está quedando obsoleto en favor de Smart Transport para las licencias

- Los AP que ejecutan Cisco IOS-XE 17.9.3 o posterior pueden encontrar problemas al intentar actualizar su software debido a espacio insuficiente en el directorio /tmp. Cuando el espacio /tmp en el AP se llena, evita la descarga de la nueva imagen del AP. En tales casos, recomendamos que reinicie el AP.

  Los AP de la onda 2 pueden entrar en un loop de arranque cuando se actualiza el software sobre un link WAN. Para obtener más información, visite: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- A partir de Cisco IOS XE Cupertino 17.7.1 en adelante, para el controlador inalámbrico Cisco Catalyst 9800-CL, asegúrese de completar los informes de medición de utilización de recursos (RUM) y de que el ACK esté disponible en la instancia del producto al menos una vez. De este modo se garantiza que la información de uso correcta y actualizada se refleja en Cisco Smart Software Manager (CSSM). Si no lo hace, un máximo de 50 AP podrán unirse a un 9800-CL hasta que se ACK un informe de licencia.
- No se admite la fragmentación inferior a 1500 para los paquetes RADIUS generados por clientes inalámbricos en la interfaz Gi0 (OOB).
- A partir de la versión 17.3, el 9800-CL requiere 16 gb de espacio en disco para funcionar correctamente. Usted no puede aumentar el tamaño dinámicamente si su instancia del WLC comenzó con un OVA de 8gb (de antes de 17.3). la única manera es crear un nuevo WLC a partir de un OVA fechado después de 17.3
- Es posible que el controlador inalámbrico Cisco Catalyst 9800-L no pueda responder a las señales BREAK recibidas en el puerto de la consola durante el arranque, lo que impide que los usuarios accedan a ROMMON. Este problema se observa en los controladores fabricados hasta noviembre de 2019, con la configuración predeterminada config-register de 0x2102. Este problema puede evitarse si

configura config-register en 0x2002. Este problema se corrige en el ROMMON 16.12(3r) para el controlador inalámbrico Catalyst 9800-L de Cisco. Para obtener información sobre cómo actualizar ROMMON, vea la sección Actualización de ROMMON para los Controladores Inalámbricos Cisco Catalyst 9800-L del documento *Actualización de Dispositivos de Hardware Programables de Campo para los Controladores Inalámbricos Cisco Catalyst 9800 Series*.

- Si se muestra este mensaje de error después de un reinicio o un desperfecto del sistema, se recomienda que regenere el certificado de punto de confianza:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilice estos comandos en el orden especificado para generar un nuevo certificado de punto de confianza autofirmado:

1. **device#** configure terminal
2. device(config)# no crypto pki trustpoint *trustpoint_name*
3. device(config)# no ip http server
4. **device(config)#** no ip http secure-server
5. **device(config)#** ip http server
6. **device(config)#** ip http secure-server
7. device(config)# ip http authentication *local/aaa*

- Verifique que su dirección MAC de movilidad esté configurada con el comando **wireless mobility mac-address**
- Estos protocolos ahora se soportan a través del puerto de servicio en 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infraestructura Cisco Prime
  - TELNET
  - GUI del controlador
  - DNS
  - Transferencia de archivos
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - Licencias para que la función Smart Licensing se comunique con CSSM

    - Netconf
    - Netflow
    - NTP
    - RADIUS (incluida CoA)
    - Restconf
    - SNMP (Protocolo de administración de red simple)
    - SSH
    - SYSLOG
    - TACACS+

- La imagen AP para 17.9 es más grande que la flash AP permitida originalmente. Si ve que el AP se queja de no tener suficiente espacio al descargar la imagen 17.9, probablemente se deba a que no respetó la trayectoria de actualización a través de 17.3.5 como se indica en las notas de la versión o a que su AP está ejecutando una imagen AireOS más antigua. Ya sea transitando a través de ha 17.3.5 o WLC posterior o actualizando la imagen de AireOS a la última cambiará el tamaño de la flash AP para permitir descargar la imagen 17.9

17.12.1

- La función Cisco Centralized Key Management (CCKM) está siendo obsoleta en Cisco IOS XE Dublin 17.10.x.
- Smart Call Home está quedando obsoleto en favor de Smart Transport para las licencias

- Los AP que ejecutan Cisco IOS-XE 17.9.3 o posterior pueden encontrar problemas al intentar actualizar su software debido a espacio insuficiente en el directorio /tmp. Cuando el espacio /tmp en el AP se llena, evita la descarga de la nueva imagen del AP. En tales casos, recomendamos que reinicie el AP.

  Los AP de la onda 2 pueden entrar en un loop de arranque cuando se actualiza el software sobre un link WAN. Para obtener más información, visite: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- Las versiones 17.12.1 y posteriores ofrecen compatibilidad con los puntos de acceso basados en Cisco IOS (series x700 y 1570). No se admitieron entre 17.4 y 17.9.2. La compatibilidad con estos puntos de acceso no va más allá del ciclo de vida normal del producto. Consulte los boletines de fin de soporte técnico individuales en Cisco.com.
- A partir de Cisco IOS XE Cupertino 17.7.1 en adelante, para el controlador inalámbrico Cisco Catalyst 9800-CL, asegúrese de completar los informes de medición de utilización de recursos (RUM) y de que el ACK esté disponible en la instancia del producto al menos una vez. De este modo se garantiza que la información de uso correcta y actualizada se refleja en Cisco Smart Software Manager (CSSM). Si no lo hace, un máximo de 50 AP podrán unirse a un 9800-CL hasta que se ACK un informe de licencia.
- No se admite la fragmentación inferior a 1500 para los paquetes RADIUS generados por clientes inalámbricos en la interfaz Gi0 (OOB).
- A partir de la versión 17.3, el 9800-CL requiere 16 gb de espacio en disco para funcionar correctamente. Usted no puede aumentar el tamaño dinámicamente si su instancia del WLC comenzó

con un OVA de 8gb (de antes de 17.3). la única manera es crear un nuevo WLC a partir de un OVA fechado después de 17.3

- Es posible que el controlador inalámbrico Cisco Catalyst 9800-L no pueda responder a las señales BREAK recibidas en el puerto de la consola durante el arranque, lo que impide que los usuarios accedan a ROMMON. Este problema se observa en los controladores fabricados hasta noviembre de 2019, con la configuración predeterminada config-register de 0x2102. Este problema puede evitarse si configura config-register en 0x2002. Este problema se corrige en el ROMMON 16.12(3r) para el controlador inalámbrico Catalyst 9800-L de Cisco. Para obtener información sobre cómo actualizar ROMMON, vea la sección Actualización de ROMMON para los Controladores Inalámbricos Cisco Catalyst 9800-L del documento *Actualización de Dispositivos de Hardware Programables de Campo para los Controladores Inalámbricos Cisco Catalyst 9800 Series*.
- Si se muestra este mensaje de error después de un reinicio o un desperfecto del sistema, se recomienda que regenere el certificado de punto de confianza:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilice estos comandos en el orden especificado para generar un nuevo certificado de punto de confianza autofirmado:

1. **device#** configure terminal
2. device(config)# no crypto pki trustpoint *trustpoint_name*
3. device(config)# no ip http server
4. **device(config)#** no ip http secure-server
5. **device(config)#** ip http server
6. **device(config)#** ip http secure-server
7. device(config)# ip http authentication *local/aaa*

- Verifique que su dirección MAC de movilidad esté configurada con el comando **wireless mobility mac-address**
- Estos protocolos ahora se soportan a través del puerto de servicio en 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infraestructura Cisco Prime
  - TELNET
  - GUI del controlador
  - DNS
  - Transferencia de archivos
  - GNMI
  - HTTP

    - HTTPS
    - LDAP
    - Licencias para que la función Smart Licensing se comunique con CSSM
    - Netconf
    - Netflow
    - NTP
    - RADIUS (incluida CoA)
    - Restconf
    - SNMP (Protocolo de administración de red simple)
    - SSH
    - SYSLOG
    - TACACS+
- La imagen AP para 17.9 es más grande que la flash AP permitida originalmente. Si ve que el AP se queja de no tener suficiente espacio al descargar la imagen 17.9, probablemente se deba a que no respetó la trayectoria de actualización a través de 17.3.5 como se indica en las notas de la versión o a que su AP está ejecutando una imagen AireOS más antigua. Ya sea transitando a través de ha 17.3.5 o WLC posterior o actualizando la imagen de AireOS a la última cambiará el tamaño de la flash AP para permitir descargar la imagen 17.9

Reducir

Las reversiones no son oficialmente compatibles y la pérdida de configuración de nuevas funciones puede ocurrir. Sin embargo, como las reversiones pueden ocurrir en el mundo real, este documento todavía enumera las trampas más comunes para evitar cuando se rebaja. Para encontrar la información que necesita, compruebe la versión desde la que está realizando la descarga (la versión anterior a la descarga)

Gibraltar

16.12.2

- Nada que señalar aquí.

16.12.3

- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a.

16.12.4

- Si usted baja de esta versión a una inferior, el WLC puede terminar en un loop de arranque si la telemetría fue configurada debido al ID de bug de Cisco CSCvt69990 / ID de bug de Cisco

CSCvv87417
- El controlador inalámbrico Cisco Catalyst 9800 se puede volver a cargar si se cambia de 17.x a 16.12.4a. Para evitar esto, le recomendamos que actualice a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a

Amsterdam

17.1.1

- Si usted baja de esta versión a una inferior, el WLC puede terminar en un loop de arranque si la telemetría fue configurada debido al ID de bug de Cisco CSCvt69990 / CSCvv8741
- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a.

17.2.1

- Si usted baja de esta versión a una inferior, el WLC puede terminar en un loop de arranque si la telemetría fue configurada debido al ID de bug de Cisco CSCvt69990 / ID de bug de Cisco CSCvv87417
- Si realiza una actualización anterior desde Cisco IOS XE Amsterdam 17.3.1 a una versión anterior, los canales de puerto que están configurados con un rango superior a 4 desaparecen
- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a.

17.3.1

- Si usted baja de esta versión a una inferior, el WLC puede terminar en un loop de arranque si la telemetría fue configurada debido al ID de bug de Cisco CSCvt69990 / CSCvv8741
- Si realiza una actualización anterior desde Cisco IOS XE Amsterdam 17.3.1 a una versión anterior, los canales de puerto que están configurados con un rango más alto desaparecen
- Si cambia de Cisco IOS XE Amsterdam 17.3.1 a una versión anterior, puede enfrentarse nuevamente al asistente de día 0 si tenía el comando "wireless country" configurado ya que no existía antes de 17.3
- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a.
- No es posible apagar el perfil de política de WLAN cuando se realiza una downgrade de Cisco IOS XE Amsterdam 17.3.x (compatible con IPv6 AVC de switching local) a Cisco IOS XE Gibraltar 16.12.x (donde no se admite IPv6 AVC de switching local). En estos casos, se recomienda eliminar el perfil de política WLAN existente y crear uno nuevo.

17.3.2

- Si usted baja de esta versión a una inferior, el WLC termina en un loop de arranque si la telemetría fue configurada debido al ID de bug de Cisco CSCvt69990 / ID de bug de Cisco CSCvv87417
- Si realiza una actualización anterior desde Cisco IOS XE Amsterdam 17.3.1 a una versión anterior, los canales de puerto que están configurados con un rango más alto desaparecen
- Si realiza una reversión de Cisco IOS XE Amsterdam 17.3.1 a una versión anterior, puede enfrentarse nuevamente al asistente de día 0 si tenía el comando "wireless country" configurado ya que no existía antes de 17.3
- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en

lugar de 16.12.4a.
- No es posible apagar el perfil de política de WLAN cuando se realiza una downgrade de Cisco IOS XE Amsterdam 17.3.x (compatible con IPv6 AVC de switching local) a Cisco IOS XE Gibraltar 16.12.x (donde no se admite IPv6 AVC de switching local). En estos casos, se recomienda eliminar el perfil de política WLAN existente y crear uno nuevo.

17.3.3

- Si usted baja de esta versión a una inferior, el WLC puede terminar en un loop de arranque si la telemetría fue configurada debido al ID de bug de Cisco CSCvt69990 / ID de bug de Cisco CSCvv87417
- Si realiza una actualización anterior desde Cisco IOS XE Amsterdam 17.3.1 a una versión anterior, los canales de puerto que están configurados con un rango más alto desaparecen
- Si realiza una reversión de Cisco IOS XE Amsterdam 17.3.1 a una versión anterior, puede enfrentarse nuevamente al asistente de día 0 si tenía el comando "wireless country" configurado ya que no existía antes de 17.3
- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a.
- No es posible apagar el perfil de política de WLAN cuando se realiza una downgrade de Cisco IOS XE Amsterdam 17.3.x (compatible con IPv6 AVC de switching local) a Cisco IOS XE Gibraltar 16.12.x (donde no se admite IPv6 AVC de switching local). En estos casos, se recomienda eliminar el perfil de política WLAN existente y crear uno nuevo.

17.4.1

- Si realiza una reversión de Cisco IOS XE Amsterdam 17.4.1 a una versión anterior anterior a 17.3, puede enfrentarse nuevamente al asistente de día 0 si tenía el comando "wireless country" configurado ya que no existía antes de 17.3
- Si cambia de Cisco IOS XE Amsterdam 17.4.1 a una versión anterior, perderá la conexión de telemetría, ya que 17.4 utiliza un destino de telemetría con nombre que no era compatible con los comandos de versiones anteriores. Debe volver a crear la conexión de telemetría.
- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a.

17.5.1

- Si realiza una reversión de Cisco IOS XE Amsterdam 17.4.1 a una versión anterior anterior a 17.3, puede enfrentarse nuevamente al asistente de día 0 si tenía el comando "wireless country" configurado ya que no existía antes de 17.3
- Si cambia de Cisco IOS XE Amsterdam 17.4.1 a una versión anterior, perderá la conexión de telemetría, ya que 17.4 utiliza un destino de telemetría con nombre que no era compatible con los comandos de versiones anteriores. Debe volver a crear la conexión de telemetría.
- La recarga continua se observa cuando el controlador inalámbrico Cisco Catalyst 9800 se rebaja de 17.x a 16.12.4a. Le recomendamos que realice una actualización a Cisco IOS XE Gibraltar 16.12.5 en lugar de 16.12.4a.

17.9.x

- No puede ver contraseñas 802.1x en texto sin cifrar de esta versión porque están cifradas. Si usted desactualiza a una imagen anterior que no soporta una contraseña cifrada, los AP se atascarán y fallarán repetidamente la autenticación dot1x debido a credenciales incorrectas. Necesitará inhabilitar

802.1x en el puerto del switch AP para permitir que el AP se una al controlador antes de configurar la contraseña de texto sin cifrar.

17.10.1

- No puede ver contraseñas 802.1x en texto sin cifrar de esta versión porque están cifradas. Si usted desactualiza a una imagen anterior que no soporta una contraseña cifrada, los AP se atascarán y fallarán repetidamente la autenticación dot1x debido a credenciales incorrectas. Necesitará inhabilitar 802.1x en el puerto del switch AP para permitir que el AP se una al controlador antes de configurar la contraseña de texto sin cifrar.

17.11.1

- No puede ver contraseñas 802.1x en texto sin cifrar de esta versión porque están cifradas. Si usted desactualiza a una imagen anterior que no soporta una contraseña cifrada, los AP se atascarán y fallarán repetidamente la autenticación dot1x debido a credenciales incorrectas. Necesitará inhabilitar 802.1x en el puerto del switch AP para permitir que el AP se una al controlador antes de configurar la contraseña de texto sin cifrar.

17.12.x

- No puede ver contraseñas 802.1x en texto sin cifrar de esta versión porque están cifradas. Si usted desactualiza a una imagen anterior que no soporta una contraseña cifrada, los AP se atascarán y fallarán repetidamente la autenticación dot1x debido a credenciales incorrectas. Necesitará inhabilitar 802.1x en el puerto del switch AP para permitir que el AP se una al controlador antes de configurar la contraseña de texto sin cifrar.

Referencias

17.1 guía de actualización de puntos de acceso de revisión en funcionamiento y laminación

17.3 revisión en funcionamiento y guía de actualización de ISSU.

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).