Upgrade und Downgrade der Catalyst Controller 9800: Tipps und Tricks

Inhalt

Referenzen

Einleitung

Dieses Dokument beschreibt Aspekte, die beim Upgrade oder Downgrade eines Catalyst 9800 Wireless LAN Controller (WLC) über mehrere Cisco IOS XE-Versionen zu beachten sind.

Bevor Sie fortfahren

Dieses Dokument soll nicht die Versionshinweise ersetzen, die beim Upgrade immer das Einstiegsdokument sein müssen. Ziel ist es, das Upgrade durch mehrere Releases zu erleichtern, indem die wichtigsten Änderungen zwischen Releases hervorgehoben werden.

Dieses Dokument ersetzt nicht das Lesen der Versionshinweise Ihrer Zielsoftware-Version. Sichern Sie Ihre Konfiguration, und treffen Sie alle erforderlichen Vorsichtsmaßnahmen, bevor Sie mit einem Upgrade fortfahren.

Standardmäßig ist der HTTP-Server des 9800 nicht einem bestimmten Zertifikat/Trustpoint statisch zugeordnet, was nach einem Upgrade zu Änderungen führen kann. Legen Sie den HTTP-Server vor der Aktualisierung auf einen statischen Trustpoint (vorzugsweise auf ein Zertifikat, das Sie zu diesem Zweck ausgestellt haben, oder auf das MIC-Zertifikat, das ansonsten ausgegeben wird) in der Konfiguration fest.

Der Sonderfall von Engineering-Spezialversionen

Spezielle technische Builds unterstützen kein ISSU-Upgrade von ihnen. Dieses Dokument konzentriert sich nur auf öffentliche Veröffentlichungen, die unter cisco.com veröffentlicht werden. Wenn Sie sich in einer speziellen Engineering-Version befinden, lesen Sie die Versionshinweise, die Sie zusammen mit diesen erhalten haben, um Unterstützung für alle Ihre Upgrade-Fragen zu erhalten.

Upgrade

Sie können die Notizen direkt unter der Zielsoftware-Version lesen, die Sie anstreben. Tipps, die für mehrere Versionen gelten, werden jedes Mal wiederholt. Aktualisieren Sie nicht mehr als drei Versionen gleichzeitig. Beispielsweise wird ein Upgrade von 16.12.1 auf 17.3.2 von diesem Dokument abgedeckt, jedoch nicht Upgrades von 16.12 auf 17.4. In einem solchen Szenario gehen Sie bitte durch 17.3 und überprüfen Sie die Hinweise im Abschnitt 17.3, führen Sie das Upgrade durch, schauen Sie sich den Abschnitt 17.4 an und bereiten Sie das zweite Upgrade vor. Abschließend wird festgestellt, dass die aufgeführten Tipps nicht mehr nach 3 Hauptversionen wiederholt werden, auch wenn sie noch gültig sind, da das Dokument voraussetzt, dass Sie Zwischenveröffentlichungen durchlaufen.

Gibraltar

16.12.2

- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum

Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.

16.12.3

- 16.12.3 ist die erste Version, die nur die Unterstützung der in der Dokumentation aufgeführten SFPs durchsetzt. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.

16.12.4

- 16.12.3 und 17.2.1 sind die ersten Versionen, die die Unterstützung nur der SFPs durchsetzen, die in der Dokumentation als unterstützt aufgeführt sind. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.

16.12.5

- Identisch mit 16.12.4

Amsterdam

17.1.1

- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.
- Ab dieser Version wird eine neue Überprüfung der Gateway-Erreichbarkeit eingeführt. Die APs senden periodische ICMP-Echoanfragen (Ping) an das Standard-Gateway, um die Verbindung zu überprüfen. Sie müssen sicherstellen, dass die Datenverkehrsfilterung zwischen den APs und dem Standard-Gateway (wie ACLs) ICMP-Pings zwischen dem AP und dem Standard-Gateway zulässt. Wenn diese Pings blockiert werden, werden die APs auch dann neu geladen, wenn die Verbindung zwischen dem Controller und dem AP aktiv ist.

17.2.1

- 16.12.3 und 17.2.1 sind die ersten Versionen, die die Unterstützung nur der SFPs durchsetzen, die in der Dokumentation als unterstützt aufgeführt sind. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, kann es aufgrund der Standardzuordnungsänderung heruntergefahren werden. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.
- Ab 17.1 wird eine neue Prüfung der Gateway-Erreichbarkeit eingeführt. Die APs senden periodische ICMP-Echoanfragen (Ping) an das Standard-Gateway, um die Verbindung zu überprüfen. Sie müssen sicherstellen, dass die Datenverkehrsfilterung zwischen den APs und dem Standard-Gateway (wie ACLs) ICMP-Pings zwischen dem AP und dem Standard-Gateway zulässt. Wenn diese Pings blockiert werden, selbst wenn die Verbindung zwischen

dem Controller und dem AP aktiv ist, werden die APs im Abstand von 4 Stunden neu geladen.

17.3.1

- 16.12.3 und 17.2.1 sind die ersten Versionen, die die Unterstützung nur der SFPs durchsetzen, die in der Dokumentation als unterstützt aufgeführt sind. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.
- Ab 17.1 wird eine neue Prüfung der Gateway-Erreichbarkeit eingeführt. Die APs senden periodische ICMP-Echoanfragen (Ping) an das Standard-Gateway, um die Verbindung zu überprüfen. Sie müssen sicherstellen, dass die Datenverkehrsfilterung zwischen den APs und dem Standard-Gateway (wie ACLs) ICMP-Pings zwischen dem AP und dem Standard-Gateway zulässt. Wenn diese Pings blockiert werden, werden die APs auch dann neu geladen, wenn die Verbindung zwischen dem Controller und dem AP aktiv ist.
- Wenn Sie den FIPS-Modus konfiguriert haben, stellen Sie sicher, dass Sie die **Sicherheits-**wpa wpa1 cipher tkip-Konfiguration aus einem WLAN entfernen, bevor Sie ein Upgrade von Cisco IOS XE Amsterdam 17.3.x von einer früheren Version durchführen. Andernfalls wird die WLAN-Sicherheit auf TKIP gesetzt, das im FIPS-Modus nicht unterstützt wird. Nach dem Upgrade müssen Sie das WLAN mit AES neu konfigurieren.
- Ab Cisco IOS XE Amsterdam ab 17.3.1 benötigt der Cisco Catalyst Wireless Controller 9800-CL 16 GB Festplattenspeicher für neue Bereitstellungen. Eine Neuinstallation mit einem Image von 17.3 ist nur möglich, um die Größe des Festplattenspeichers zu erhöhen.
- Ab Cisco IOS XE Amsterdam 17.3.1 darf der Name des Access Points nur bis zu 32 Zeichen enthalten.
- Für die lokale MAC-Adressenauthentifizierung (von Clients oder APs) wird ab 17.3.1 nur das Format aaaabbcc (ohne Trennzeichen) unterstützt. Dies bedeutet, dass die Authentifizierung fehlschlägt, wenn Sie in der Webbenutzeroberfläche oder CLI MAC-Adressen mit Trennzeichen hinzufügen.
- Ab dieser Version werden APs nach 4 Stunden neu geladen, wenn sie nicht einem WLC beitreten können, ihr Gateway nicht mehr anpingen können UND ihr Gateway nicht mehr anpingen können (Alle 3 müssen fehlschlagen, damit der Access Point neu gestartet werden kann). Dies ist eine Erweiterung (Cisco Bug ID CSCvt89970) zur vorherigen Überprüfung des nur-icmp-Gateways von früheren Versionen
- Ab 17.3.1 können Sie die Ländervorwahl für Access Points über den Befehl "Wireless country <1 country code>" konfigurieren. Dieser Befehl kann mit unterschiedlichen Ländercodes

mehrfach wiederholt werden. Dadurch kann die maximale Anzahl an Ländercode auf über 20 erhöht werden. Die Befehle "ap country" sind immer noch vorhanden und werden noch funktionieren. Erwägen Sie jedoch, sie in die Befehle "Wireless country" zu ändern, da die Befehle des ap country in einer zukünftigen Version veraltet werden.

17.3.2

- 16.12.3 und 17.2.1 sind die ersten Versionen, die die Unterstützung nur der SFPs durchsetzen, die in der Dokumentation als unterstützt aufgeführt sind. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.
- Ab 17.1 wird eine neue Prüfung der Gateway-Erreichbarkeit eingeführt. Die APs senden periodische ICMP-Echoanfragen (Ping) an das Standard-Gateway, um die Verbindung zu überprüfen. Sie müssen sicherstellen, dass die Datenverkehrsfilterung zwischen den APs und dem Standard-Gateway (wie ACLs) ICMP-Pings zwischen dem AP und dem Standard-Gateway zulässt. Wenn diese Pings blockiert werden, werden die APs auch dann neu geladen, wenn die Verbindung zwischen dem Controller und dem AP aktiv ist.
- Wenn Sie den FIPS-Modus konfiguriert haben, stellen Sie sicher, dass Sie die **Sicherheits-**wpa wpa1 cipher tkip-Konfiguration aus einem WLAN entfernen, bevor Sie ein Upgrade von Cisco IOS XE Amsterdam 17.3.x von einer früheren Version durchführen. Andernfalls wird die WLAN-Sicherheit auf TKIP gesetzt, das im FIPS-Modus nicht unterstützt wird. Nach dem Upgrade müssen Sie das WLAN mit AES neu konfigurieren.
- Ab Cisco IOS XE Amsterdam ab 17.3.1 benötigt der Cisco Catalyst Wireless Controller 9800-CL 16 GB Festplattenspeicher für neue Bereitstellungen. Eine Neuinstallation mit einem Image von 17.3 ist nur möglich, um die Größe des Festplattenspeichers zu erhöhen.
- Ab Cisco IOS XE Amsterdam 17.3.1 darf der Name des Access Points nur bis zu 32 Zeichen enthalten.
- Für die lokale MAC-Adressenauthentifizierung (von Clients oder APs) wird ab 17.3.1 nur das Format aaaabbcc (ohne Trennzeichen) unterstützt. Dies bedeutet, dass die Authentifizierung fehlschlägt, wenn Sie in der Webbenutzeroberfläche oder CLI MAC-Adressen mit Trennzeichen hinzufügen.
- Ab 17.3.1 werden APs nach 4 Stunden neu geladen, wenn sie nicht einem WLC beitreten können, ihr Gateway nicht mehr anpingen können UND ihr Gateway nicht mehr anpingen können (Alle 3 müssen fehlschlagen, damit der Access Point neu gestartet werden kann). Dies ist eine Erweiterung (Cisco Bug ID CSCvt89970) zur vorherigen Überprüfung des nur-

icmp-Gateways von früheren Versionen
- Ab 17.3.1 können Sie die Ländervorwahl für Access Points über den Befehl "Wireless country <1 country code>" konfigurieren. Dieser Befehl kann mit unterschiedlichen Ländercodes mehrfach wiederholt werden. Dadurch kann die maximale Anzahl an Ländercode auf über 20 erhöht werden. Die Befehle "ap country" sind immer noch vorhanden und werden noch funktionieren. Erwägen Sie jedoch, sie in die Befehle "Wireless country" zu ändern, da die Befehle des ap country in einer zukünftigen Version veraltet werden.

17.3.3

- 16.12.3 und 17.2.1 sind die ersten Versionen, die die Unterstützung nur der SFPs durchsetzen, die in der Dokumentation als unterstützt aufgeführt sind. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.
- Ab 17.1 wird eine neue Prüfung der Gateway-Erreichbarkeit eingeführt. Die APs senden periodische ICMP-Echoanfragen (Ping) an das Standard-Gateway, um die Verbindung zu überprüfen. Sie müssen sicherstellen, dass die Datenverkehrsfilterung zwischen den APs und dem Standard-Gateway (wie ACLs) ICMP-Pings zwischen dem AP und dem Standard-Gateway zulässt. Wenn diese Pings blockiert werden, werden die APs auch dann neu geladen, wenn die Verbindung zwischen dem Controller und dem AP aktiv ist.
- Wenn Sie den FIPS-Modus konfiguriert haben, stellen Sie sicher, dass Sie die **Sicherheits-**wpa wpa1 cipher tkip-Konfiguration aus einem WLAN entfernen, bevor Sie ein Upgrade von Cisco IOS XE Amsterdam 17.3.x von einer früheren Version durchführen. Andernfalls wird die WLAN-Sicherheit auf TKIP gesetzt, das im FIPS-Modus nicht unterstützt wird. Nach dem Upgrade müssen Sie das WLAN mit AES neu konfigurieren.
- Ab Cisco IOS XE Amsterdam ab 17.3.1 benötigt der Cisco Catalyst Wireless Controller 9800-CL 16 GB Festplattenspeicher für neue Bereitstellungen. Eine Neuinstallation mit einem Image von 17.3 ist nur möglich, um die Größe des Festplattenspeichers zu erhöhen.
- Ab Cisco IOS XE Amsterdam 17.3.1 darf der Name des Access Points nur bis zu 32 Zeichen enthalten.
- Für die lokale MAC-Adressenauthentifizierung (von Clients oder APs) wird ab 17.3.1 nur das Format aaaabbcc (ohne Trennzeichen) unterstützt. Dies bedeutet, dass die Authentifizierung fehlschlägt, wenn Sie in der Webbenutzeroberfläche oder CLI MAC-Adressen mit Trennzeichen hinzufügen.
- Ab 17.3.1 werden APs nach 4 Stunden neu geladen, wenn sie nicht einem WLC beitreten

können, ihr Gateway nicht mehr anpingen können UND ihr Gateway nicht mehr anpingen können (Alle 3 müssen fehlschlagen, damit der Access Point neu gestartet werden kann). Dies ist eine Erweiterung (Cisco Bug ID CSCvt89970) die vorherige Überprüfung des nur-icmp-Gateways von früheren Versionen
- Ab 17.3.1 können Sie die Ländervorwahl für Access Points über den Befehl "Wireless country <1 country code>" konfigurieren. Dieser Befehl kann mit unterschiedlichen Ländercodes mehrfach wiederholt werden. Dadurch kann die maximale Anzahl an Ländercode auf über 20 erhöht werden. Die Befehle "ap country" sind immer noch vorhanden und werden noch funktionieren. Erwägen Sie jedoch, sie in die Befehle "Wireless country" zu ändern, da die Befehle des ap country in einer zukünftigen Version veraltet werden.
- WLC kann abstürzen, wenn Ihre APs Hostnamen über mehr als 32 Zeichen haben (Cisco Bug ID CSCvy11981)

17.3.4

- 16.12.3 und 17.2.1 sind die ersten Versionen, die die Unterstützung nur der SFPs durchsetzen, die in der Dokumentation als unterstützt aufgeführt sind. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.
- Ab 17.1 wird eine neue Prüfung der Gateway-Erreichbarkeit eingeführt. Die APs senden periodische ICMP-Echoanfragen (Ping) an das Standard-Gateway, um die Verbindung zu überprüfen. Sie müssen sicherstellen, dass die Datenverkehrsfilterung zwischen den APs und dem Standard-Gateway (wie ACLs) ICMP-Pings zwischen dem AP und dem Standard-Gateway zulässt. Wenn diese Pings blockiert werden, werden die APs auch dann neu geladen, wenn die Verbindung zwischen dem Controller und dem AP aktiv ist.
- Wenn Sie den FIPS-Modus konfiguriert haben, stellen Sie sicher, dass Sie die **Sicherheits-**wpa wpa1 cipher tkip-Konfiguration aus einem WLAN entfernen, bevor Sie ein Upgrade von Cisco IOS XE Amsterdam 17.3.x von einer früheren Version durchführen. Andernfalls wird die WLAN-Sicherheit auf TKIP gesetzt, das im FIPS-Modus nicht unterstützt wird. Nach dem Upgrade müssen Sie das WLAN mit AES neu konfigurieren.
- Ab Cisco IOS XE Amsterdam ab 17.3.1 benötigt der Cisco Catalyst Wireless Controller 9800-CL 16 GB Festplattenspeicher für neue Bereitstellungen. Eine Neuinstallation mit einem Image von 17.3 ist nur möglich, um die Größe des Festplattenspeichers zu erhöhen.
- Ab Cisco IOS XE Amsterdam 17.3.1 darf der Name des Access Points nur bis zu 32 Zeichen enthalten.

- Für die lokale MAC-Adressenauthentifizierung (von Clients oder APs) wird ab 17.3.1 nur das Format aaaabbcc (ohne Trennzeichen) unterstützt. Dies bedeutet, dass die Authentifizierung fehlschlägt, wenn Sie in der Webbenutzeroberfläche oder CLI MAC-Adressen mit Trennzeichen hinzufügen.
- Ab 17.3.1 wird APsl nach 4 Stunden neu geladen, wenn sie einem WLC nicht beitreten können. Wenn sie nicht beitreten können, können sie nicht mehr an das Gateway senden UND ihr Gateway ARP senden (alle 3 müssen fehlschlagen, damit der Access Point neu gestartet werden kann). Dies ist eine Erweiterung (Cisco Bug ID CSCvt89970) zur vorherigen Überprüfung des nur-icmp-Gateways von früheren Versionen
- Ab 17.3.1 können Sie die Ländervorwahl für Access Points über den Befehl "Wireless country <1 country code>" konfigurieren. Dieser Befehl kann mit unterschiedlichen Ländercodes mehrfach wiederholt werden. Dadurch kann die maximale Anzahl an Ländercode auf über 20 erhöht werden. Die Befehle "ap country" sind immer noch vorhanden und funktionieren noch, aber denken Sie daran, sie in die Befehle "Wireless country" zu ändern, da die Befehle des ap country in einer zukünftigen Version veraltet sein sollen.
- Bei einem Upgrade auf 17.3.4 und höher wird empfohlen, den 16.12.5r-Bootloader/-Rom auf den entsprechenden Controllern (9800-80) zu installieren. Der 9800-40 verfügt derzeit nicht über einen regulären 16.12.5r und benötigt kein reguläres Upgrade).
- Ein Controller-Upgrade von Cisco IOS XE Bengaluru 17.3.x auf eine beliebige Version mit ISSU kann fehlschlagen, wenn der Befehl **snmp-server enable traps hsrp** konfiguriert ist. Stellen Sie sicher, dass Sie den Befehl **snmp-server enable traps hsrp** aus der Konfiguration entfernen, bevor Sie ein ISSU-Upgrade starten, da der Befehl **snmp-server enable traps hsrp** aus dem Cisco IOS XE Bengaluru 17.4.x entfernt wird.
- Wenn beim Upgrade auf Cisco IOS XE 17.3.x und höher der Befehl ip http active-session-modules none aktiviert ist, können Sie nicht über HTTPS auf die Controller-GUI zugreifen. Führen Sie folgende Befehle aus, um über HTTPS auf die GUI zuzugreifen:ip http session-module-list pkilist OPENRESTY_PKIip http active-session-modules pkilist

17.3.5

- Aufgrund der Cisco Bug-ID CSCwb13784 Wenn die MTU-Größe des Pfades weniger als 1500 Byte beträgt, können die Access Points möglicherweise nicht beitreten. Laden Sie den SMU-Patch für 17.3.5 herunter, um dieses Problem zu beheben.
- 16.12.3 und 17.2.1 sind die ersten Versionen, die die Unterstützung nur der SFPs durchsetzen, die in der Dokumentation als unterstützt aufgeführt sind. SFPs, die nicht aufgeführt werden, verursachen einen Port-Ausfall. Überprüfen Sie die Liste der unterstützten SFPs, und stellen Sie sicher, dass Ihre SFPs kompatibel sind, um zu verhindern, dass die Datenports nach dem Upgrade nicht mehr verfügbar sind.
- Upgrade-Datei für diese Version kann zu groß für HTTP-Upload (wenn Sie Web-UI-Upgrade durchführen) sein, wenn Sie in Version 16.12.1 sind. Verwenden Sie eine andere Übertragungsmethode, oder gehen Sie durch 16.12.2, die größere Dateien unterstützt, die über die Webbenutzeroberfläche hochgeladen werden.
- Aus Cisco IOS XE Gibraltar 16.12.2s wurde die automatische WLAN-Zuordnung zum Standard-Richtlinienprofil unter dem Standard-Richtlinien-Tag entfernt. Wenn Sie ein Upgrade von einer früheren Version als Cisco IOS XE Gibraltar 16.12.2s durchführen und Ihr Wireless-Netzwerk die Standard-Richtlinien-Tag verwendet, wird es aufgrund der Standardzuordnungsänderung heruntergefahren. Um den Netzwerkbetrieb

wiederherzustellen, fügen Sie das erforderliche WLAN den Richtlinienzuordnungen unter dem Standard-Policy-Tag hinzu.

- Ab 17.1 wird eine neue Prüfung der Gateway-Erreichbarkeit eingeführt. Die APs senden periodische ICMP-Echoanfragen (Ping) an das Standard-Gateway, um die Verbindung zu überprüfen. Sie müssen sicherstellen, dass die Datenverkehrsfilterung zwischen den APs und dem Standard-Gateway (wie ACLs) ICMP-Pings zwischen dem AP und dem Standard-Gateway zulässt. Wenn diese Pings blockiert werden, werden die APs auch dann neu geladen, wenn die Verbindung zwischen dem Controller und dem AP aktiv ist.
- Wenn Sie den FIPS-Modus konfiguriert haben, stellen Sie sicher, dass Sie die **Sicherheits-**wpa wpa1 cipher tkip-Konfiguration aus einem WLAN entfernen, bevor Sie ein Upgrade von Cisco IOS XE Amsterdam 17.3.x von einer früheren Version durchführen. Andernfalls wird die WLAN-Sicherheit auf TKIP gesetzt, das im FIPS-Modus nicht unterstützt wird. Nach dem Upgrade müssen Sie das WLAN mit AES neu konfigurieren.
- Ab Cisco IOS XE Amsterdam ab 17.3.1 benötigt der Cisco Catalyst Wireless Controller 9800-CL 16 GB Festplattenspeicher für neue Bereitstellungen. Eine Neuinstallation mit einem Image von 17.3 ist nur möglich, um die Größe des Festplattenspeichers zu erhöhen.
- Ab Cisco IOS XE Amsterdam 17.3.1 darf der Name des Access Points nur bis zu 32 Zeichen enthalten.
- Für die lokale MAC-Adressenauthentifizierung (von Clients oder APs) wird ab 17.3.1 nur das Format aaaabbcc (ohne Trennzeichen) unterstützt. Dies bedeutet, dass die Authentifizierung fehlschlägt, wenn Sie in der Webbenutzeroberfläche oder CLI MAC-Adressen mit Trennzeichen hinzufügen.
- Ab 17.3.1 wird APsl nach 4 Stunden neu geladen, wenn sie einem WLC nicht beitreten können. Wenn sie nicht beitreten können, können sie nicht mehr an das Gateway senden UND ihr Gateway ARP senden (alle 3 müssen fehlschlagen, damit der Access Point neu gestartet werden kann). Dies ist eine Erweiterung (Cisco Bug ID CSCvt89970) zur vorherigen Überprüfung des nur-icmp-Gateways von früheren Versionen
- Ab 17.3.1 können Sie die Ländervorwahl für Access Points über den Befehl "Wireless country <1 country code>" konfigurieren. Dieser Befehl kann mit unterschiedlichen Ländercodes mehrfach wiederholt werden. Dadurch kann die maximale Anzahl an Ländercode auf über 20 erhöht werden. Die Befehle "ap country" sind immer noch vorhanden und funktionieren noch, aber denken Sie daran, sie in die Befehle "Wireless country" zu ändern, da die Befehle des ap country in einer zukünftigen Version veraltet sein sollen.
- Bei einem Upgrade auf 17.3.4 und höher wird empfohlen, den 16.12.5r-Bootloader/-Rom auf den entsprechenden Controllern (9800-80) zu installieren. Der 9800-40 verfügt derzeit nicht über einen regulären 16.12.5r und benötigt kein reguläres Upgrade).
- Ein Controller-Upgrade von Cisco IOS XE Bengaluru 17.3.x auf eine beliebige Version mit ISSU kann fehlschlagen, wenn der Befehl **snmp-server enable traps hsrp** konfiguriert ist. Stellen Sie sicher, dass Sie den Befehl **snmp-server enable traps hsrp** aus der Konfiguration entfernen, bevor Sie ein ISSU-Upgrade starten, da der Befehl **snmp-server enable traps hsrp** aus dem Cisco IOS XE Bengaluru 17.4.x entfernt wird.
- Wenn beim Upgrade auf Cisco IOS XE 17.3.x und höher der Befehl ip http active-session-modules none aktiviert ist, können Sie nicht über HTTPS auf die Controller-GUI zugreifen. Führen Sie folgende Befehle aus, um über HTTPS auf die GUI zuzugreifen:ip http session-module-list pkilist OPENRESTY_PKIip http active-session-modules pkilist

Bengaluru

17.4.1

- Ab 17.4.1 werden Cisco IOS-basierte APs der ersten Welle (1700.2700.3700.1570) mit Ausnahme von IW3700 nicht mehr unterstützt.
- Ihre WLANs können nach dem Upgrade heruntergefahren werden, wenn sie nicht WPA-konform sind (Gast-, offene oder CWA-SSIDs) und eine adaptive FT konfiguriert wurde. Die Lösung besteht darin, vor dem Upgrade die adaptive FT-Konfiguration zu entfernen (Cisco Bug ID CSCvx34349).). Eine anpassungsfähige FT-Konfiguration ist für SSIDs ohne WPA nicht sinnvoll, sodass durch deren Entfernung keine Verluste entstehen.
- WLC kann abstürzen, wenn Ihre APs Hostnamen über mehr als 32 Zeichen haben (Cisco Bug ID CSCvy11981)

17.5.1

- Ab 17.4.1 werden Cisco IOS-basierte APs der ersten Welle (1700.2700.3700.1570) mit Ausnahme von IW3700 nicht mehr unterstützt.
- Ab der Cisco IOS XE Bengaluru Version 17.4.1 bietet die Telemetrielösung einen Namen für die Empfängeradresse anstelle der IP-Adresse für Telemetriedaten. Dies ist eine zusätzliche Option. Während des Downgrades des Controllers und des nachfolgenden Upgrades besteht wahrscheinlich ein Problem: Die Upgrade-Version verwendet die neu benannten Empfänger, die beim Downgrade nicht erkannt werden. Die neue Konfiguration wird abgelehnt und schlägt bei der nachfolgenden Aktualisierung fehl. Konfigurationsverluste können vermieden werden, wenn das Upgrade oder Downgrade vom Cisco DNA Center aus durchgeführt wird.
- Ihre WLANs können nach dem Upgrade heruntergefahren werden, wenn sie nicht WPA-konform sind (Gast-, offene oder CWA-SSIDs) und eine adaptive FT konfiguriert wurde. Die Lösung besteht darin, vor dem Upgrade die adaptive FT-Konfiguration zu entfernen (Cisco Bug ID CSCvx34349).). Eine anpassungsfähige FT-Konfiguration ist für SSIDs ohne WPA nicht sinnvoll, sodass durch deren Entfernung keine Verluste entstehen.
- WLC kann abstürzen, wenn Ihre APs Hostnamen über mehr als 32 Zeichen haben (Cisco Bug ID CSCvy11981)
- Wenn Sie die GUI von einer Version auf eine andere aktualisieren, empfehlen wir, den Browser-Cache zu löschen, damit alle GUI-Seiten ordnungsgemäß neu geladen werden.
- Wenn beim Upgrade auf Cisco IOS XE 17.3.x und höher der Befehl ip http active-session-modules none aktiviert ist, können Sie nicht über HTTPS auf die grafische Benutzeroberfläche zugreifen. Führen Sie folgende Befehle aus, um über HTTPS auf die GUI zuzugreifen:ip http session-module-list pkilist OPENRESTY_PKIip http active-session-modules pkilist
- Wenn der Fehler ERR_SSL_VERSION_OR_CIPHER_MISMATCH nach einem Neustart oder Systemabsturz in der GUI auftritt, empfehlen wir Ihnen, das Trustpoint-Zertifikat neu zu generieren.Das Verfahren zum Generieren eines neuen selbstsignierten Trustpoints ist wie folgt:

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

17.6.1

- Ab 17.4.1 werden Cisco IOS-basierte APs der ersten Welle (1700.2700.3700.1570) mit Ausnahme von IW3700 nicht mehr unterstützt.
- Ab der Cisco IOS XE Bengaluru Version 17.4.1 bietet die Telemetrielösung einen Namen für die Empfängeradresse anstelle der IP-Adresse für Telemetriedaten. Dies ist eine zusätzliche

Option. Während des Downgrades des Controllers und des nachfolgenden Upgrades besteht wahrscheinlich ein Problem: Die Upgrade-Version verwendet die neu benannten Empfänger, die beim Downgrade nicht erkannt werden. Die neue Konfiguration wird abgelehnt und schlägt bei der nachfolgenden Aktualisierung fehl. Konfigurationsverluste können vermieden werden, wenn das Upgrade oder Downgrade vom Cisco DNA Center aus durchgeführt wird.

- Ihre WLANs können nach dem Upgrade heruntergefahren werden, wenn sie nicht WPA-konform sind (Gast-, offene oder CWA-SSIDs) und eine adaptive FT konfiguriert wurde. Die Lösung besteht darin, vor dem Upgrade die adaptive FT-Konfiguration zu entfernen (Cisco Bug ID CSCvx34349).). Eine anpassungsfähige FT-Konfiguration ist für SSIDs ohne WPA nicht sinnvoll, sodass durch deren Entfernung keine Verluste entstehen.
- Wenn Sie die GUI von einer Version auf eine andere aktualisieren, empfehlen wir, den Browser-Cache zu löschen, damit alle GUI-Seiten ordnungsgemäß neu geladen werden.
- Ein AP, der einem WLC der Version 17.6.1 oder höher beigetreten ist, kann einem AireOS-WLC nicht mehr beitreten, es sei denn, er führt 8.10.162- oder 8.5.176.2- oder spätere 8.5-Codes aus.
- Bei einem Upgrade auf 17.6,1 und höher wird empfohlen, den 16.12.5r-Bootloader/-Rom auf den entsprechenden Controllern (9800-80) zu installieren. Der 9800-40 verfügt derzeit nicht über einen regulären 16.12.5r und benötigt kein reguläres Upgrade).
- Ein Controller-Upgrade von Cisco IOS XE Bengaluru 17.3.x auf eine beliebige Version mit ISSU kann fehlschlagen, wenn der Befehl **snmp-server enable traps hsrp** konfiguriert ist. Stellen Sie sicher, dass Sie den Befehl **snmp-server enable traps hsrp** aus der Konfiguration entfernen, bevor Sie ein ISSU-Upgrade starten, da der Befehl **snmp-server enable traps hsrp** aus dem Cisco IOS XE Bengaluru 17.4.x entfernt wird.
- Wenn beim Upgrade auf Cisco IOS XE 17.3.x und höher der Befehl ip http active-session-modules none aktiviert ist, funktioniert der HTTPS-Zugriff auf die Controller-GUI nicht. Führen Sie folgende Befehle aus, um über HTTPS auf die GUI zuzugreifen:ip http session-module-list pkilist OPENRESTY_PKIip http active-session-modules pkilist
- Wenn der Fehler ERR_SSL_VERSION_OR_CIPHER_MISMATCH nach einem Neustart oder Systemabsturz in der GUI auftritt, empfehlen wir Ihnen, das Trustpoint-Zertifikat neu zu generieren.Das Verfahren zum Generieren eines neuen selbstsignierten Trustpoints ist wie folgt:

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

17.6.2

- Ab 17.4.1 werden Cisco IOS-basierte APs der ersten Welle (1700.2700.3700.1570) mit Ausnahme von IW3700 nicht mehr unterstützt.
- Ab der Cisco IOS XE Bengaluru Version 17.4.1 bietet die Telemetrielösung einen Namen für die Empfängeradresse anstelle der IP-Adresse für Telemetriedaten. Dies ist eine zusätzliche Option. Während des Downgrades des Controllers und des nachfolgenden Upgrades besteht wahrscheinlich ein Problem: Die Upgrade-Version verwendet die neu benannten Empfänger, die beim Downgrade nicht erkannt werden. Die neue Konfiguration wird abgelehnt und schlägt bei der nachfolgenden Aktualisierung fehl. Konfigurationsverluste können vermieden werden, wenn das Upgrade oder Downgrade vom Cisco DNA Center aus durchgeführt wird.
- Ihre WLANs können nach dem Upgrade heruntergefahren werden, wenn sie nicht WPA-konform sind (Gast-, offene oder CWA-SSIDs) und eine adaptive FT konfiguriert wurde. Die Lösung besteht darin, vor dem Upgrade die adaptive FT-Konfiguration zu entfernen (Cisco Bug ID CSCvx34349).) Die adaptive FT-Konfiguration ist für SSIDs ohne WPA nicht sinnvoll,

sodass durch das Entfernen nichts verloren geht.
- Wenn Sie die GUI von einer Version auf eine andere aktualisieren, empfehlen wir, den Browser-Cache zu löschen, damit alle GUI-Seiten ordnungsgemäß neu geladen werden.
- Ein AP, der einem WLC der Version 17.6.1 oder höher beigetreten ist, kann einem AireOS-WLC nicht mehr beitreten, es sei denn, er führt 8.10.162- oder 8.5.176.2- oder spätere 8.5-Codes aus.
- Bei einem Upgrade auf 17.6.1 und höher wird empfohlen, den 16.12.5r-Bootloader/-Rom auf den entsprechenden Controllern (9800-80) zu installieren. Der 9800-40 verfügt derzeit nicht über einen regulären 16.12.5r und benötigt kein reguläres Upgrade).
- Ein Controller-Upgrade von Cisco IOS XE Bengaluru 17.3.x auf eine beliebige Version mit ISSU kann fehlschlagen, wenn der Befehl **snmp-server enable traps hsrp** konfiguriert ist. Stellen Sie sicher, dass Sie den Befehl **snmp-server enable traps hsrp** aus der Konfiguration entfernen, bevor Sie ein ISSU-Upgrade starten, da der Befehl **snmp-server enable traps hsrp** aus dem Cisco IOS XE Bengaluru 17.4.x entfernt wird.
- Wenn beim Upgrade auf Cisco IOS XE 17.3.x und höher der Befehl ip http active-session-modules none aktiviert ist, funktioniert der GUI-Zugriff für den HTTPS-Controller nicht. Führen Sie folgende Befehle aus, um über HTTPS auf die GUI zuzugreifen:ip http session-module-list pkilist OPENRESTY_PKIip http active-session-modules pkilist
- Verwenden Sie nicht mehr als 31 Zeichen für AP-Namen. Wenn der AP-Name mindestens 32 Zeichen umfasst, kann es zu einem Controller-Absturz kommen.
- Wenn der Fehler ERR_SSL_VERSION_OR_CIPHER_MISMATCH nach einem Neustart oder Systemabsturz in der GUI auftritt, empfehlen wir Ihnen, das Trustpoint-Zertifikat neu zu generieren.Das Verfahren zum Generieren eines neuen selbstsignierten Trustpoints ist wie folgt:
```
configure terminal no crypto pki trustpoint
```

Cupertino

In diesem Abschnitt wird davon ausgegangen, dass Sie ab 17.6.1 oder höher beginnen und auf eine Cupertino-Version aktualisieren. Wenn Sie ein Upgrade direkt von einer früheren Version durchführen (die möglicherweise unterstützt wird, lesen Sie die Versionshinweise, um sicher zu sein), lesen Sie die Abschnitte 17.3 und 17.6.

17.7.1

- Verwenden Sie nicht mehr als 31 Zeichen für AP-Namen. Wenn der AP-Name mindestens 32 Zeichen umfasst, kann es zu einem Controller-Absturz kommen.
- 17.7.1 erfordert, dass der Ländercode des Access Points in den AP-Verbindungsprofilen konfiguriert wird.
- Aufgrund der Cisco Bug-ID CSCvu22886 , wenn Sie 9130 oder 9124 APs haben, müssen Sie 17.3.5a durchlaufen, wenn Sie von einer Version vor 17.3.4 auf 17.7.1 oder höher aktualisieren.

17.8.1

- Verwenden Sie nicht mehr als 31 Zeichen für AP-Namen. Wenn der AP-Name mindestens 32 Zeichen umfasst, kann es zu einem Controller-Absturz kommen.
- 17.7.1 erfordert, dass der Ländercode des Access Points in den AP-Verbindungsprofilen

konfiguriert wird.
- Aufgrund der Cisco Bug-ID CSCvu22886 , wenn Sie 9130 oder 9124 APs haben, müssen Sie 17.3.5a durchlaufen, wenn Sie von einer Version vor 17.3.4 auf 17.7.1 oder höher aktualisieren.

Downgrade

Downgrades werden offiziell nicht unterstützt, und es kann zum Verlust neuer Funktionen kommen. Da Downgrades in der Praxis jedoch möglich sind, werden in diesem Dokument immer noch die häufigsten Traps aufgelistet, die bei Downgrades vermieden werden sollten. Um die benötigten Informationen zu erhalten, überprüfen Sie die Version, von der Sie ein Downgrade durchführen (die Version vor dem Downgrade).

Gibraltar

16.12.2

- Hier gibt es nichts zu vermerken.

16.12.3

- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.

16.12.4

- Wenn Sie von dieser Version auf eine niedrigere Version herabstufen, kann der WLC in einer Boot-Schleife enden, wenn die Telemetrie aufgrund der Cisco Bug-ID CSCvt69990 konfiguriert wurde. / Cisco Bug ID CSCvv87417
- Der Cisco Catalyst Wireless Controller der Serie 9800 kann neu geladen werden, wenn er von 17.x auf 16.12.4a herabgestuft wird. Um dies zu vermeiden, empfehlen wir ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.

Amsterdam

17.1.1

- Wenn Sie von dieser Version auf eine niedrigere Version herabstufen, kann der WLC in einer Boot-Schleife enden, wenn die Telemetrie aufgrund der Cisco Bug-ID CSCvt69990 konfiguriert wurde. / CSCvv8741
- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.

17.2.1

- Wenn Sie von dieser Version auf eine niedrigere Version herabstufen, kann der WLC in einer Boot-Schleife enden, wenn die Telemetrie aufgrund der Cisco Bug-ID CSCvt69990 konfiguriert wurde. / Cisco Bug ID CSCvv87417
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version durchführen, werden die Port-Channels, die für einen höheren Bereich als 4 konfiguriert sind, ausgeblendet
- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.

17.3.1

- Wenn Sie von dieser Version auf eine niedrigere Version herabstufen, kann der WLC in einer Boot-Schleife enden, wenn die Telemetrie aufgrund der Cisco Bug-ID CSCvt69990 konfiguriert wurde / CSCvv8741
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version durchführen, werden die Port-Channels, die für einen höheren Bereich konfiguriert sind, ausgeblendet
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version durchführen, können Sie den Day-0-Assistenten erneut aufrufen, wenn der Befehl "wireless country" konfiguriert wurde, da er vor 17.3 nicht vorhanden war.
- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.
- Das WLAN-Richtlinienprofil kann nicht heruntergefahren werden, wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.x (unterstützt lokales Switching von IPv6 AVC) auf Cisco IOS XE Gibraltar 16.12.x durchführen (wobei IPv6 AVC für lokales Switching nicht unterstützt wird). In solchen Fällen empfehlen wir, das vorhandene WLAN-Richtlinienprofil zu löschen und ein neues Profil zu erstellen.

17.3.2

- Wenn Sie von dieser Version auf eine niedrigere Version herabstufen, endet der WLC in einer Bootschleife, wenn die Telemetrie aufgrund der Cisco Bug-ID CSCvt69990 konfiguriert wurde. / Cisco Bug ID CSCvv87417
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version durchführen, werden die Port-Channels, die für einen höheren Bereich konfiguriert sind, ausgeblendet
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version durchführen, wird möglicherweise der Day-0-Assistent erneut gestartet, wenn der Befehl "wireless country" konfiguriert wurde, da er vor 17.3 nicht vorhanden war.
- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.
- Das WLAN-Richtlinienprofil kann nicht heruntergefahren werden, wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.x (unterstützt lokales Switching von IPv6 AVC) auf Cisco IOS XE Gibraltar 16.12.x durchführen (wobei IPv6 AVC für lokales Switching nicht unterstützt

wird). In solchen Fällen empfehlen wir, das vorhandene WLAN-Richtlinienprofil zu löschen und ein neues Profil zu erstellen.

17.3.3

- Wenn Sie von dieser Version auf eine niedrigere Version herabstufen, kann der WLC in einer Boot-Schleife enden, wenn die Telemetrie aufgrund der Cisco Bug-ID CSCvt69990 konfiguriert wurde / Cisco Bug ID CSCvv87417
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version durchführen, werden die Port-Channels, die für einen höheren Bereich konfiguriert sind, ausgeblendet
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version durchführen, wird möglicherweise der Day-0-Assistent erneut gestartet, wenn der Befehl "wireless country" konfiguriert wurde, da er vor 17.3 nicht vorhanden war.
- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.
- Das WLAN-Richtlinienprofil kann nicht heruntergefahren werden, wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.3.x (unterstützt lokales Switching von IPv6 AVC) auf Cisco IOS XE Gibraltar 16.12.x durchführen (wobei IPv6 AVC für lokales Switching nicht unterstützt wird). In solchen Fällen empfehlen wir, das vorhandene WLAN-Richtlinienprofil zu löschen und ein neues Profil zu erstellen.

17.4.1

- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.4.1 auf eine frühere Version vor 17.3 durchführen, wird möglicherweise der Day-0-Assistent erneut gestartet, wenn der Befehl "wireless country" konfiguriert wurde, da er nicht vor 17.3 vorhanden war.
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.4.1 auf eine frühere Version durchführen, verlieren Sie die Telemetrie-Verbindung, da in Version 17.4 benannte Telemetrie-Ziele verwendet werden, die in früheren Versionen nicht unterstützt wurden. Sie müssen die Telemetrie-Verbindung neu erstellen.
- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.

17.5.1

- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.4.1 auf eine frühere Version vor 17.3 durchführen, wird möglicherweise der Day-0-Assistent erneut gestartet, wenn der Befehl "wireless country" konfiguriert wurde, da er nicht vor 17.3 vorhanden war.
- Wenn Sie ein Downgrade von Cisco IOS XE Amsterdam 17.4.1 auf eine frühere Version durchführen, verlieren Sie die Telemetrie-Verbindung, da in Version 17.4 benannte Telemetrie-Ziele verwendet werden, die in früheren Versionen nicht unterstützt wurden. Sie müssen die Telemetrie-Verbindung neu erstellen.
- Ein kontinuierliches erneutes Laden wird beobachtet, wenn der Cisco Catalyst Wireless Controller 9800 von 17.x auf 16.12.4a herabgestuft wird. Wir empfehlen ein Downgrade auf

Cisco IOS XE Gibraltar 16.12.5 anstelle von 16.12.4a.

Referenzen

17.1 Leitfaden für Hot-Patching und rollende AP-Upgrades

17.3 Hot-Patching und ISSU-Upgrade-Leitfaden.