Upgradeprocessor en downgrade van Catalyst 9800 controllers: Tips en riskjes

Inhoud

Referenties

Inleiding

Dit document beschrijft dingen om uit te kijken wanneer het verbeteren of het verlagen van een Catalyst 9800 draadloze LAN controller (WLC) door verschillende Cisco IOS XE releases.

Voordat u verdergaat

Dit document heeft niet tot doel de introductieaantekeningen te vervangen, die bij de verbetering altijd het doorlopend document moeten zijn. Het doel is de upgrade te vergemakkelijken door middel van verscheidene releases door de meest impactvolle veranderingen tussen introducties onder de aandacht te brengen.

Dit document vervangt niet het lezen van de release opmerkingen van de doelsoftware-release. Maak een back-up van de configuratie en neem alle benodigde voorzorgsmaatregelen voordat u doorgaat met een upgrade.

Standaard wordt de http server van de 9800 niet stapsgewijs toegewezen aan een bepaald certificaat/betrouwbaar punt dat tot veranderingen na de upgrade kan leiden. Stel de HTTP server in op een statisch trustpunt (bij voorkeur op een certificaat dat u voor het doel hebt afgegeven, of op het MIC-certificaat anders) in de configuratie voordat u opwaarderen.

Het bijzondere geval van speciale technische versies

Speciale gebouwen in de technische bouw ondersteunen de ISSU-upgrade niet. Dit document richt zich alleen op openbare releases die naar cisco.com zijn gepubliceerd. Als u daarom op een technische speciale bouwstijl bent, raadpleeg de release notes die u samen met deze heeft ontvangen om ondersteuning te ontvangen voor al uw upgradevragen.

Upgraden

U kunt de opmerkingen rechtstreeks lezen onder de doelsoftwareversie die u beoogt. Tips die van toepassing zijn via meerdere releases worden telkens voor uw gemak herhaald. Geen upgrade uitvoeren door meer dan 3 releases tegelijkertijd. Bijvoorbeeld de opwaardering van 16.12.1 naar 17.3.2 valt onder dit document, maar geen opwaarderingen van 16.12 naar 17.4. In dat geval moet u 17.3 doornemen en de aantekeningen onder het punt 17.3 controleren, de upgrade uitvoeren en dan kijken naar het punt 17.4 en de tweede upgrade voorbereiden. Als conclusie worden de tips in de lijst niet meer herhaald na drie belangrijke releases, zelfs als ze nog geldig zijn volgens de methode in het document, waarbij u eerst belangrijke releases maakt.

Gibraltar

16.12.2

- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de

standaard beleidstag gebruikt, gaat deze dan omlaag vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.

16.12.3

- 16.12.3 is het eerste release om de ondersteuning van alleen de SFP's die in de documentatie worden ondersteund, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP's compatibel zijn om te voorkomen dat de gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden geüpload.
- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, gaat deze dan omlaag vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.

16.12.4

- 16.12.3 en 17.2.1 zijn de eerste releases om de ondersteuning van alleen de SFP's die in de documentatie worden genoemd, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP's compatibel zijn om te voorkomen dat de gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden geüpload.
- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, gaat deze dan omlaag vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.

16.12.5

- Hetzelfde als 16.12.4

Amsterdam

17.1.1

- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden geüpload.
- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, zal deze naar beneden gaan vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.
- Vanaf deze release wordt er een nieuwe gateway bereikbaarheidscontrole geïntroduceerd. APs verzenden periodieke de (pingelen) van de echo van ICMP naar de standaardgateway om connectiviteit te controleren. U moet ervoor zorgen dat het verkeer tussen de AP's en de standaardgateway (zoals ACL's) wordt gefilterd zodat ICMP-pings tussen de AP en de standaardgateway mogelijk is. Als deze pings geblokkeerd zijn, zelfs als de verbinding tussen de controller en de AP actief is, zullen de AP's met een tussenpoos van 4 uur opnieuw laden.

17.2.1

- 16.12.3 en 17.2.1 zijn de eerste releases om de ondersteuning van alleen de SFP's die in de documentatie worden genoemd, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP’s compatibel zijn om te voorkomen dat de gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden geüpload.
- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u van een release vroeger werkt dan Cisco IOS XE Gibraltar 16.12.2s en als uw draadloze netwerk de standaard beleidstag gebruikt, kan deze naar beneden gaan vanwege de standaard mapping verandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.
- Vanaf 17.1 wordt een nieuwe gateway bereikbaarheidscontrole geïntroduceerd. APs verzenden periodieke de (pingelen) van de echo van ICMP naar de standaardgateway om connectiviteit te controleren. U moet ervoor zorgen dat het verkeer tussen de AP's en de standaardgateway (zoals ACL's) wordt gefilterd zodat ICMP-pings tussen de AP en de standaardgateway mogelijk is. Als deze pings geblokkeerd zijn, zelfs als de connectiviteit tussen de controller en de AP actief is, herladen de APs met tussenpozen van 4 uur.

17.3.1

- 16.12.3 en 17.2.1 zijn de eerste releases om de ondersteuning van alleen de SFP's die in de documentatie worden genoemd, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP’s compatibel zijn om te voorkomen dat de

gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden geüpload.
- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, zal deze naar beneden gaan vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.
- Vanaf 17.1 wordt een nieuwe gateway bereikbaarheidscontrole geïntroduceerd. APs verzenden periodieke de (pingelen) van de echo van ICMP naar de standaardgateway om connectiviteit te controleren. U moet ervoor zorgen dat het verkeer tussen de AP's en de standaardgateway (zoals ACL's) wordt gefilterd zodat ICMP-pings tussen de AP en de standaardgateway mogelijk is. Als deze pings geblokkeerd zijn, zelfs als de verbinding tussen de controller en de AP actief is, zullen de AP's met een tussenpoos van 4 uur opnieuw laden.
- Als u de FIPS-modus hebt ingesteld, zorg er dan voor dat u **het security wpa1-**algoritme uit een WLAN verwijdert voordat u Cisco IOS XE Amsterdam 17.3.x van een eerdere versie upgrades uitvoert. Wanneer u dit niet doet, stelt u de WLAN-beveiliging in op TKIP, wat niet in FIPS-modus wordt ondersteund. Na de upgrade moet u WLAN met AES aanpassen.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 vereist Cisco Catalyst 9800-CL draadloze controller 16 GB schijfruimte voor nieuwe implementaties. Het is alleen mogelijk de schijfruimte te vergroten door opnieuw te installeren met een 17.3-afbeelding.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 kan de AP naam alleen tot 32 tekens zijn.
- Voor lokale MAC-adresverificatie (van klanten of AP's) wordt alleen de format Abbcc (zonder scheidingsteken) ondersteund vanaf 17.3.1. Dit betekent dat verificatie mislukt als u MAC-adres met scheidingstekens in de web UI of CLI toevoegt.
- Vanaf deze release zullen AP's na 4 uur herladen als ze zich niet bij een WLC kunnen aansluiten, hun gateway en ARP hun gateway kunnen ping (alle 3 moet afbreken om de AP te herstarten). Dit is een verbetering (Cisco bug-ID CSCv8970) naar de vorige icmp-only gateway-verificatie uit eerdere releases
- Vanaf 17.3.1 is de nieuwe manier om landcode voor toegangspunten te configureren de opdracht "Draadloos land <1 landcode>" die u meerdere malen met verschillende landcodes kunt herhalen. Hierdoor kan de maximale hoeveelheid landcode van meer dan 20 worden verhoogd. De opdrachten "land van het begin" zijn nog aanwezig en werken nog steeds. U kunt ze echter overwegen om ze in de opdrachten "Draadloos land" te veranderen, omdat de opdrachten van het land in een toekomstige versie zullen worden afgekeurd

17.3.2

- 16.12.3 en 17.2.1 zijn de eerste releases om de ondersteuning van alleen de SFP's die in de documentatie worden genoemd, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP's compatibel zijn om te voorkomen dat de gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren

van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden geüpload.
- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, zal deze naar beneden gaan vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.
- Vanaf 17.1 wordt een nieuwe gateway bereikbaarheidscontrole geïntroduceerd. APs verzenden periodieke de (pingelen) van de echo van ICMP naar de standaardgateway om connectiviteit te controleren. U moet ervoor zorgen dat het verkeer tussen de AP's en de standaardgateway (zoals ACL's) wordt gefilterd zodat ICMP-pings tussen de AP en de standaardgateway mogelijk is. Als deze pings geblokkeerd zijn, zelfs als de verbinding tussen de controller en de AP actief is, zullen de AP's met een tussenpoos van 4 uur opnieuw laden.
- Als u de FIPS-modus hebt ingesteld, zorg er dan voor dat u **het security wpa1-**algoritme uit een WLAN verwijdert voordat u Cisco IOS XE Amsterdam 17.3.x van een eerdere versie upgrades uitvoert. Wanneer u dit niet doet, stelt u de WLAN-beveiliging in op TKIP, wat niet in FIPS-modus wordt ondersteund. Na de upgrade moet u WLAN met AES aanpassen.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 vereist Cisco Catalyst 9800-CL draadloze controller 16 GB schijfruimte voor nieuwe implementaties. Het is alleen mogelijk de schijfruimte te vergroten door opnieuw te installeren met een 17.3-afbeelding.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 kan de AP naam alleen tot 32 tekens zijn.
- Voor lokale MAC-adresverificatie (van klanten of AP's) wordt alleen de format Abbcc (zonder scheidingsteken) ondersteund vanaf 17.3.1. Dit betekent dat verificatie mislukt als u MAC-adres met scheidingstekens in de web UI of CLI toevoegt.
- Vanaf 17.3.1 zullen APs na 4 uur herladen als zij zich niet bij een WLC kunnen aansluiten, hun gateway EN ARP hun gateway kunnen pingelen (Alle 3 hoeven te falen om de AP te herstarten). Dit is een verbetering (Cisco bug-ID CSCv8970) naar de vorige icmp-only gateway-verificatie uit eerdere releases
- Vanaf 17.3.1 is de nieuwe manier om landcode voor toegangspunten te configureren de opdracht "Draadloos land <1 landcode>" die u meerdere malen met verschillende landcodes kunt herhalen. Hierdoor kan de maximale hoeveelheid landcode van meer dan 20 worden verhoogd. De opdrachten "land van koopsom" zijn nog aanwezig en werken nog. U kunt ze echter overwegen om ze in de opdrachten "Draadloos land" te veranderen, omdat de opdrachten van het toetredende land in een toekomstige versie zullen worden afgekeurd.

17.3.3

- 16.12.3 en 17.2.1 zijn de eerste releases om de ondersteuning van alleen de SFP's die in de documentatie worden genoemd, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP's compatibel zijn om te voorkomen dat de gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden

geüpload.

- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, zal deze naar beneden gaan vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.
- Vanaf 17.1 wordt een nieuwe gateway bereikbaarheidscontrole geïntroduceerd. APs verzenden periodieke de (pingelen) van de echo van ICMP naar de standaardgateway om connectiviteit te controleren. U moet ervoor zorgen dat het verkeer tussen de AP's en de standaardgateway (zoals ACL's) wordt gefilterd zodat ICMP-pings tussen de AP en de standaardgateway mogelijk is. Als deze pings geblokkeerd zijn, zelfs als de verbinding tussen de controller en de AP actief is, zullen de AP's met een tussenpoos van 4 uur opnieuw laden.
- Als u de FIPS-modus hebt ingesteld, zorg er dan voor dat u **het security wpa1-**algoritme uit een WLAN verwijdert voordat u Cisco IOS XE Amsterdam 17.3.x van een eerdere versie upgrades uitvoert. Wanneer u dit niet doet, stelt u de WLAN-beveiliging in op TKIP, wat niet in FIPS-modus wordt ondersteund. Na de upgrade moet u WLAN met AES aanpassen.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 vereist Cisco Catalyst 9800-CL draadloze controller 16 GB schijfruimte voor nieuwe implementaties. Het is alleen mogelijk de schijfruimte te vergroten door opnieuw te installeren met een 17.3-afbeelding.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 kan de AP naam alleen tot 32 tekens zijn.
- Voor lokale MAC-adresverificatie (van klanten of AP's) wordt alleen de format Abbcc (zonder scheidingsteken) ondersteund vanaf 17.3.1. Dit betekent dat verificatie mislukt als u MAC-adres met scheidingstekens in de web UI of CLI toevoegt.
- Vanaf 17.3.1 zullen APs na 4 uur herladen als zij zich niet bij een WLC kunnen aansluiten, hun gateway EN ARP hun gateway kunnen pingelen (Alle 3 hoeven te falen om de AP te herstarten). Dit is een verbetering (Cisco bug-ID CSCv8970) de vorige icmp-only gateway-verificatie uit eerdere releases
- Vanaf 17.3.1 is de nieuwe manier om landcode voor toegangspunten te configureren de opdracht "Draadloos land <1 landcode>" die u meerdere malen met verschillende landcodes kunt herhalen. Hierdoor kan de maximale hoeveelheid landcode van meer dan 20 worden verhoogd. De opdrachten "land van koopsom" zijn nog aanwezig en werken nog. U kunt ze echter overwegen om ze in de opdrachten "Draadloos land" te veranderen, omdat de opdrachten van het toetredende land in een toekomstige versie zullen worden afgekeurd.
- WLC kan crashen als uw APs hostnamen van meer dan 32 tekens hebben (Cisco bug-ID CSCvy1981)

17.3.4

- 16.12.3 en 17.2.1 zijn de eerste releases om de ondersteuning van alleen de SFP's die in de documentatie worden genoemd, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP's compatibel zijn om te voorkomen dat de gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden

geüpload.

- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, zal deze naar beneden gaan vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.
- Vanaf 17.1 wordt een nieuwe gateway bereikbaarheidscontrole geïntroduceerd. APs verzenden periodieke de (pingelen) van de echo van ICMP naar de standaardgateway om connectiviteit te controleren. U moet ervoor zorgen dat het verkeer tussen de AP's en de standaardgateway (zoals ACL's) wordt gefilterd zodat ICMP-pings tussen de AP en de standaardgateway mogelijk is. Als deze pings geblokkeerd zijn, zelfs als de verbinding tussen de controller en de AP actief is, zullen de AP's met een tussenpoos van 4 uur opnieuw laden.
- Als u de FIPS-modus hebt ingesteld, zorg er dan voor dat u **het security wpa1-**algoritme uit een WLAN verwijdert voordat u Cisco IOS XE Amsterdam 17.3.x van een eerdere versie upgrades uitvoert. Wanneer u dit niet doet, stelt u de WLAN-beveiliging in op TKIP, wat niet in FIPS-modus wordt ondersteund. Na de upgrade moet u WLAN met AES aanpassen.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 vereist Cisco Catalyst 9800-CL draadloze controller 16 GB schijfruimte voor nieuwe implementaties. Het is alleen mogelijk de schijfruimte te vergroten door opnieuw te installeren met een 17.3-afbeelding.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 kan de AP naam alleen tot 32 tekens zijn.
- Voor lokale MAC-adresverificatie (van klanten of AP's) wordt alleen de format Abbcc (zonder scheidingsteken) ondersteund vanaf 17.3.1. Dit betekent dat verificatie mislukt als u MAC-adres met scheidingstekens in de web UI of CLI toevoegt.
- Vanaf 17.3.1, herladen APsl na 4 uur als zij zich niet bij een WLC kunnen aansluiten, kan hun gateway EN ARP hun gateway niet pingelen (Alle 3 moeten voor de AP om opnieuw op te starten falen). Dit is een verbetering (Cisco bug-ID CSCv8970) naar de vorige icmp-only gateway-verificatie uit eerdere releases
- Vanaf 17.3.1 is de nieuwe manier om landcode voor toegangspunten te configureren de opdracht "Draadloos land <1 landcode>" die u meerdere malen met verschillende landcodes kunt herhalen. Hierdoor kan de maximale hoeveelheid landcode van meer dan 20% worden verhoogd. De opdrachten "land van koopsom" zijn nog aanwezig en werken nog steeds. Overweeg echter om ze in de opdrachten "Draadloos land" te veranderen, aangezien de opdrachten van het toetredende land in een toekomstige versie zullen worden afgekeurd.
- Aanbevolen wordt om de 16.12.5r bootloader/rommon te laten installeren op controllers waar deze van toepassing is (de 9800-80. De 9800-40 heeft op dit moment geen rommong 16.12.5r en heeft geen roommon-upgrade nodig).
- Een upgrade van de controller, van Cisco IOS XE Bengaluru 17.3.x naar elke release met ISSU, kan mislukken als de **snmp-server** de **snelle** opdracht **voor** het **maken van** vallen **mogelijk maakt**, is ingesteld. Zorg ervoor dat u de **snmp-server** verwijdert **en** de **hsrp**-opdracht van de configuratie **uitschakelt** voordat u een ISSU-upgrade start, omdat de **snmp-server de** opdracht **trap** Hsrp **mogelijk maakt**, wordt verwijderd uit Cisco IOS XE Bengaluru 17.4.x.
- Tijdens het verbeteren naar Cisco IOS XE 17.3.x en latere releases, als de ip http actieve-sessie-modules is geen opdracht ingeschakeld, hebt u geen toegang tot de controller-GUI met HTTPS. U hebt toegang tot de GUI met HTTPS. U voert deze opdrachten uit:ip-http-sessie-module-list-popoloog OPENRESTY_PKIip http actieve-sessiemodules

17.3.5

- Vanwege Cisco bug-id CSCwb1374 , als uw pad MTU lager is dan 1500 bytes, kunnen APs zich wellicht niet aansluiten. Download de SMU-pleister beschikbaar voor 17.3.5 om dit probleem op te lossen.
- 16.12.3 en 17.2.1 zijn de eerste releases om de ondersteuning van alleen de SFP's die in de documentatie worden genoemd, af te dwingen. SFP's die niet in de lijst zijn opgenomen, veroorzaken een situatie waarin de haven moet worden ingedrukt. Verifieer de lijst met ondersteunde SFP en zorg ervoor dat uw SFP's compatibel zijn om te voorkomen dat de gegevenspoorten na de upgrade worden ingedrukt
- Upgradebestand voor deze release kan te groot zijn voor HTTP-uploaden (bij het uitvoeren van web UI-upgrade) als u in 16.12.1 release bent. Gebruik een andere overdrachtmethode of ga door 16.12.2 die grotere bestanden ondersteunt die via de web UI moeten worden geüpload.
- Van Cisco IOS XE Gibraltar 16.12.2s, is automatische WLAN-mapping naar het standaardbeleidsprofiel onder de standaard beleidstag verwijderd. Als u vanuit een release eerder opwaarderen dan Cisco IOS XE Gibraltar 16.12.2s, en als uw draadloze netwerk de standaard beleidstag gebruikt, zal deze naar beneden gaan vanwege de standaardkaartverandering. Als u de netwerkwerking wilt herstellen, voegt u de gewenste WLAN toe aan de beleidskaarten onder de standaardbeleidstag.
- Vanaf 17.1 wordt een nieuwe gateway bereikbaarheidscontrole geïntroduceerd. APs verzenden periodieke de (pingelen) van de echo van ICMP naar de standaardgateway om connectiviteit te controleren. U moet ervoor zorgen dat het verkeer tussen de AP's en de standaardgateway (zoals ACL's) wordt gefilterd zodat ICMP-pings tussen de AP en de standaardgateway mogelijk is. Als deze pings geblokkeerd zijn, zelfs als de verbinding tussen de controller en de AP actief is, zullen de AP's met een tussenpoos van 4 uur opnieuw laden.
- Als u de FIPS-modus hebt ingesteld, zorg er dan voor dat u **het security wpa1-**algoritme uit een WLAN verwijdert voordat u Cisco IOS XE Amsterdam 17.3.x van een eerdere versie upgrades uitvoert. Wanneer u dit niet doet, stelt u de WLAN-beveiliging in op TKIP, wat niet in FIPS-modus wordt ondersteund. Na de upgrade moet u WLAN met AES aanpassen.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 vereist Cisco Catalyst 9800-CL draadloze controller 16 GB schijfruimte voor nieuwe implementaties. Het is alleen mogelijk de schijfruimte te vergroten door opnieuw te installeren met een 17.3-afbeelding.
- Vanaf Cisco IOS XE Amsterdam 17.3.1 kan de AP naam alleen tot 32 tekens zijn.
- Voor lokale MAC-adresverificatie (van klanten of AP's) wordt alleen de format Abbcc (zonder scheidingsteken) ondersteund vanaf 17.3.1. Dit betekent dat verificatie mislukt als u MAC-adres met scheidingstekens in de web UI of CLI toevoegt.
- Vanaf 17.3.1, herladen APsl na 4 uur als zij zich niet bij een WLC kunnen aansluiten, kan hun gateway EN ARP hun gateway niet pingelen (Alle 3 moeten voor de AP om opnieuw op te starten falen). Dit is een verbetering (Cisco bug-ID CSCv8970) naar de vorige icmp-only gateway-verificatie uit eerdere releases
- Vanaf 17.3.1 is de nieuwe manier om landcode voor toegangspunten te configureren de opdracht "Draadloos land <1 landcode>" die u meerdere malen met verschillende landcodes kunt herhalen. Hierdoor kan de maximale hoeveelheid landcode van meer dan 20% worden verhoogd. De opdrachten "land van koopsom" zijn nog aanwezig en werken nog steeds. Overweeg echter om ze in de opdrachten "Draadloos land" te veranderen, aangezien de opdrachten van het toetredende land in een toekomstige versie zullen worden afgekeurd.
- Aanbevolen wordt om de 16.12.5r bootloader/rommon te laten installeren op controllers waar deze van toepassing is (de 9800-80. De 9800-40 heeft op dit moment geen rommong 16.12.5r en heeft geen roommon-upgrade nodig).

- Een upgrade van de controller, van Cisco IOS XE Bengaluru 17.3.x naar elke release met ISSU, kan mislukken als de **snmp-server** de **snelle** opdracht **voor** het **maken van** vallen **mogelijk maakt**, is ingesteld. Zorg ervoor dat u de **snmp-server** verwijdert **en** de **hsrp**-opdracht van de configuratie **uitschakelt** voordat u een ISSU-upgrade start, omdat de **snmp-server de** opdracht **trap** Hsrp **mogelijk maakt**, wordt verwijderd uit Cisco IOS XE Bengaluru 17.4.x.
- Tijdens het verbeteren naar Cisco IOS XE 17.3.x en latere releases, als de ip http actieve-sessie-modules is geen opdracht ingeschakeld, hebt u geen toegang tot de controller-GUI met HTTPS. U hebt toegang tot de GUI met HTTPS. U voert deze opdrachten uit:ip-http-sessie-module-list-popoloog OPENRESTY_PKIip http actieve-sessiemodules

Bengaluru

17.4.1

- Vanaf 17.4.1 wordt Wave 1 Cisco IOS-gebaseerde AP's niet meer ondersteund (1700.2700.3700.1570) met uitzondering van IW3700.
- Uw WLAN's kunnen na de upgrade worden uitgeschakeld als zij niet-WAP (gast, open of CWA-sid's) zijn en aangepaste FT-instellingen hebben ingesteld. De oplossing is om de adaptieve FT-configuratie voor de upgrade te verwijderen (Cisco bug ID CSCvx34349). De adaptieve FT configuratie heeft geen zin op niet-WAP SSID, zodat er geen verlies van iets is door het te verwijderen.
- WLC kan crashen als uw APs hostnamen van meer dan 32 tekens hebben (Cisco bug-ID CSCvy1981)

17.5.1

- Vanaf 17.4.1 wordt Wave 1 Cisco IOS-gebaseerde AP's niet meer ondersteund (1700.2700.3700.1570) met uitzondering van IW3700.
- Vanaf Cisco IOS XE Bengaluru release 17.4.1 biedt de telemetrie-oplossing een naam voor ontvangeradres in plaats van het IP-adres voor telemetrie-gegevens. Dit is een extra optie. Tijdens de upgrade van de controller en de daaropvolgende upgrade is er waarschijnlijk een probleem-de upgrade-versie die de nieuwe ontvangers gebruikt, en deze worden niet in de upgrade herkend. De nieuwe configuratie wordt verworpen en mislukt in de volgende upgrade. Het verlies van de configuratie kan worden vermeden wanneer de upgrade of afwaardering wordt uitgevoerd via Cisco DNA Center.
- Uw WLAN's kunnen na de upgrade worden uitgeschakeld als ze niet-WAP (gast, open of CWA-sid's) zijn en aangepaste FT-instellingen hebben ingesteld. De oplossing is om de adaptieve FT-configuratie voor de upgrade te verwijderen (Cisco bug ID CSCvx34349). De adaptieve FT configuratie heeft geen zin op niet-WAP SSID, zodat er geen verlies van iets is door het te verwijderen.
- WLC kan crashen als uw APs hostnamen van meer dan 32 tekens hebben (Cisco bug-ID CSCvy1981)
- Wanneer u de GUI van de ene release naar de andere upgrades uitvoert, raden we u aan het geheugen van de browser voor alle GUI pagina's op de juiste manier te herladen.
- Tijdens het verbeteren naar Cisco IOS XE 17.3.x en later releases, als de ip http actieve-sessie-modules is geen opdracht ingeschakeld, kunt u geen toegang tot de GUI krijgen met HTTPS. U hebt toegang tot de GUI met HTTPS. U voert deze opdrachten uit:ip-http-sessie-

module-list-popoloog OPENRESTY_PKIip http actieve-sessiemodules
- Als u de ERR_SSL_VERSION_OR_CIPHER_MISMATCH fout van de GUI na een herstart of een systeemcrash tegenkomt, raden we u aan het trustpuntcertificaat te regenereren.De procedure voor het creëren van een nieuw zelfgetekend trustpunt is als volgt:
```
configure terminal no crypto pki trustpoint
```

17.6.1

- Vanaf 17.4.1 wordt Wave 1 Cisco IOS-gebaseerde AP's niet meer ondersteund (1700.2700.3700.1570) met uitzondering van IW3700.
- Vanaf Cisco IOS XE Bengaluru release 17.4.1 biedt de telemetrie-oplossing een naam voor ontvangeradres in plaats van het IP-adres voor telemetrie-gegevens. Dit is een extra optie. Tijdens de upgrade van de controller en de daaropvolgende upgrade is er waarschijnlijk een probleem-de upgrade-versie die de nieuwe ontvangers gebruikt, en deze worden niet in de upgrade herkend. De nieuwe configuratie wordt verworpen en mislukt in de volgende upgrade. Het verlies van de configuratie kan worden vermeden wanneer de upgrade of afwaardering wordt uitgevoerd via Cisco DNA Center.
- Uw WLAN's kunnen na de upgrade worden uitgeschakeld als ze niet-WAP (gast, open of CWA-sid's) zijn en aangepaste FT-instellingen hebben ingesteld. De oplossing is om de adaptieve FT-configuratie voor de upgrade te verwijderen (Cisco bug ID CSCvx34349). De adaptieve FT configuratie heeft geen zin op niet-WAP SSID, zodat er geen verlies van iets is door het te verwijderen.
- Wanneer u de GUI van de ene release naar de andere upgrades uitvoert, raden we u aan het geheugen van de browser voor alle GUI pagina's op de juiste manier te herladen.
- AP die zich bij een 17.6.1 of later WLC aansloot kan zich niet meer bij een AireOS WLC aansluiten tenzij het 8.10.162 of later, of 8.5.176.2 of later 8.5 code in werking stelt.
- Aanbevolen wordt om de 16.12.5r bootloader/rommon te laten installeren op controllers waar deze van toepassing is (de 9800-80. De 9800-40 heeft op dit moment geen romong 16.12.5r en heeft geen roommon-upgrade nodig).
- Een upgrade van de controller, van Cisco IOS XE Bengaluru 17.3.x naar elke release met ISSU, kan mislukken als de **snmp-server** de **snelle** opdracht **voor** het **maken van** vallen **mogelijk maakt**, is ingesteld. Zorg ervoor dat u de **snmp-server** verwijdert **en** de **hsrp**-opdracht van de configuratie **uitschakelt** voordat u een ISSU-upgrade start, omdat de **snmp-server de** opdracht **trap** Hsrp **mogelijk maakt**, wordt verwijderd uit Cisco IOS XE Bengaluru 17.4.x.
- Terwijl het verbeteren naar Cisco IOS XE 17.3.x en latere releases, als de ip http active-sessie-modules geen opdracht is ingeschakeld, werkt HTTPS-toegang tot de controller GUI niet. U hebt toegang tot de GUI met HTTPS. U voert deze opdrachten uit:ip-http-sessie-module-list-popoloog OPENRESTY_PKIip http actieve-sessiemodules
- Als u de ERR_SSL_VERSION_OR_CIPHER_MISMATCH fout van de GUI na een herstart of een systeemcrash tegenkomt, raden we u aan het trustpuntcertificaat te regenereren.De procedure voor het creëren van een nieuw zelfgetekend trustpunt is als volgt:
```
configure terminal no crypto pki trustpoint
```

17.6.2

- Vanaf 17.4.1 wordt Wave 1 Cisco IOS-gebaseerde AP's niet meer ondersteund (1700.2700.3700.1570) met uitzondering van IW3700.
- Vanaf Cisco IOS XE Bengaluru release 17.4.1 biedt de telemetrie-oplossing een naam voor

ontvangeradres in plaats van het IP-adres voor telemetrie-gegevens. Dit is een extra optie. Tijdens de upgrade van de controller en de daaropvolgende upgrade is er waarschijnlijk een probleem-de upgrade-versie die de nieuwe ontvangers gebruikt, en deze worden niet in de upgrade herkend. De nieuwe configuratie wordt verworpen en mislukt in de volgende upgrade. Het verlies van de configuratie kan worden vermeden wanneer de upgrade of afwaardering wordt uitgevoerd via Cisco DNA Center.

- Uw WLAN's kunnen na de upgrade worden uitgeschakeld als zij niet-WAP (gast, open of CWA-sid's) zijn en aangepaste FT-instellingen hebben ingesteld. De oplossing is om de adaptieve FT-configuratie voor de upgrade te verwijderen (Cisco bug ID CSCvx34349) De adaptieve FT-configuratie heeft geen zin op niet-WAP-SSID, zodat er geen verlies van iets is door het te verwijderen.
- Wanneer u de GUI van de ene release naar de andere upgrades uitvoert, raden we u aan het geheugen van de browser voor alle GUI pagina's op de juiste manier te herladen.
- AP die zich bij een 17.6.1 of later WLC aansloot kan zich niet meer bij een AireOS WLC aansluiten tenzij het 8.10.162 of later, of 8.5.176.2 of later 8.5 code in werking stelt.
- Aanbevolen wordt om de 16.12.5r bootloader/rommon te laten installeren op controllers waar deze van toepassing is (de 9800-80. De 9800-40 heeft op dit moment geen romong 16.12.5r en heeft geen roommon-upgrade nodig).
- Een upgrade van de controller, van Cisco IOS XE Bengaluru 17.3.x naar elke release met ISSU, kan mislukken als de **snmp-server** de **snelle** opdracht **voor** het **maken van** vallen **mogelijk maakt**. Zorg ervoor dat u de **snmp-server** verwijdert **en** de **hsrp**-opdracht van de configuratie **uitschakelt** voordat u een ISSU-upgrade start, omdat de **snmp-server de** opdracht **trap** Hsrp **mogelijk maakt**, wordt verwijderd uit Cisco IOS XE Bengaluru 17.4.x.
- Terwijl het verbeteren naar Cisco IOS XE 17.3.x en latere releases, als de ip http active-sessie-modules geen opdracht is ingeschakeld, werkt HTTPS controller GUI-toegang niet. U hebt toegang tot de GUI met HTTPS. U voert deze opdrachten uit:ip-http-sessie-module-list-popoloog OPENRESTY_PKIip http actieve-sessiemodules
- Gebruik niet meer dan 31 tekens voor AP-namen. Als de AP-naam 32 tekens of meer is, kan een controlecrisis optreden.
- Als u de ERR_SSL_VERSION_OR_CIPHER_MISMATCH fout van de GUI na een herstart of een systeemcrash tegenkomt, raden we u aan het trustpuntcertificaat te regenereren.De procedure voor het creëren van een nieuw zelfgetekend trustpunt is als volgt:
  `configure terminal no crypto pki trustpoint`

Cupertino

Deze paragraaf veronderstelt dat u begint van 17.6.1 of later en opwaardeert tot een CUG release. Als u direct vanaf een eerdere release upgrades uitvoert (dit kan worden ondersteund, controleert u of de releaseopmerkingen zeker zijn), lees dan de uitzonderingen in de rubrieken 17.3 en 17.6.

17.7.1

- Gebruik niet meer dan 31 tekens voor AP-namen. Als de AP-naam 32 tekens of meer is, kan een controlecrisis optreden.
- 17.7.1 vereist dat de AP landcode in AP profiel wordt gevormd om samen te voegen.
- Vanwege Cisco bug-id CSCvu286 , als je 9130 of 9124 AP's hebt, moet je 17.3.5a doorlopen bij een verbetering naar 17.7.1 of later vanaf een release eerder dan 17.3.4

17.8.1

- Gebruik niet meer dan 31 tekens voor AP-namen. Als de AP-naam 32 tekens of meer is, kan een controlecrisis optreden.
- 17.7.1 vereist dat de AP landcode in AP profiel wordt gevormd om samen te voegen.
- Vanwege Cisco bug-id CSCvu286 , als je 9130 of 9124 AP's hebt, moet je 17.3.5a doorlopen bij een verbetering naar 17.7.1 of later vanaf een release eerder dan 17.3.4

afzwakken

Downgrade worden niet officieel ondersteund en het verlies van nieuwe functies kan plaatsvinden als gevolg van een configuratie. Aangezien in de echte wereld echter wel dalingen kunnen optreden, worden in dit document nog steeds de meest voorkomende vallen genoemd die voorkomen moeten worden wanneer de kwaliteit wordt verlaagd. Om de informatie te vinden die u nodig hebt, controleert u de versie waarvan u het cijfer wilt verlagen (de versie vóór de upgrade)

Gibraltar

16.12.2

- Niets om op te wijzen.

16.12.3

- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.

16.12.4

- Als u van deze release naar een lagere waarde bent gedegradeerd, kan de WLC in een laarslus eindigen als telemetrie is geconfigureerd vanwege Cisco bug-id CSCvt6990 / Cisco bug-id CSCv87417
- De Cisco Catalyst 9800 draadloze controller kan opnieuw laden als deze is gedeclasseerd van 17.x tot 16.12.4a. Om dit te voorkomen, raden we u aan om naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a te degraderen

Amsterdam

17.1.1

- Als u van deze release naar een lagere waarde bent gedegradeerd, kan de WLC in een laarslus eindigen als telemetrie is geconfigureerd vanwege Cisco bug-id CSCvt6990 / CSCv8741
- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.

17.2.1

- Als u van deze release naar een lagere waarde bent gedegradeerd, kan de WLC in een laarslus eindigen als telemetrie is geconfigureerd vanwege Cisco bug-id CSCvt6990 / Cisco bug-id CSCv87417
- Als u van Cisco IOS XE Amsterdam 17.3.1 naar een vroegere release wilt inkrimpen, verdwijnen de poortkanalen die met groter bereik dan 4 zijn geconfigureerd
- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.

17.3.1

- Als u van deze release naar een lagere waarde bent gedegradeerd, kan de WLC in een beginlus belanden als telemetrie is geconfigureerd vanwege Cisco bug-id CSCvt6990 / CSCv8741
- Als u van Cisco IOS XE Amsterdam 17.3.1 naar een vroegere release wilt reduceren, verdwijnen de poortkanalen die met hoger bereik zijn geconfigureerd
- Als u van Cisco IOS XE Amsterdam 17.3.1 naar een eerdere release bent gedowngraveerd, kunt u de day-0 wizard opnieuw bekijken als u de opdracht "Wireless country" hebt ingesteld omdat deze niet bestond voor 17.3
- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.
- Het is niet mogelijk om het WLAN-beleidsprofiel af te sluiten wanneer u uw software converteert van Cisco IOS XE Amsterdam 17.3.x (ter ondersteuning van lokale IPv6 AVC) naar Cisco IOS XE Gibraltar 16.12.x (waar lokale IPv6 AVC niet wordt ondersteund). In dergelijke gevallen raden we u aan het bestaande WLAN-beleidsprofiel te verwijderen en een nieuwe te maken.

17.3.2

- Als u van deze release naar een lager niveau wilt verlagen, wordt de WLC in een beginlus weergegeven als telemetrie is geconfigureerd vanwege Cisco bug-id CSCvt6990 / Cisco bug-id CSCv87417
- Als u van Cisco IOS XE Amsterdam 17.3.1 naar een vroegere release wilt reduceren, verdwijnen de poortkanalen die met hoger bereik zijn geconfigureerd
- Als u van Cisco IOS XE Amsterdam 17.3.1 naar een eerdere release bent gedegradeerd, kunt u de day-0 wizard opnieuw bekijken als u de opdracht "Wireless country" hebt geconfigureerd omdat deze niet bestond voor 17.3
- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.
- Het is niet mogelijk om het WLAN-beleidsprofiel af te sluiten wanneer u uw software converteert van Cisco IOS XE Amsterdam 17.3.x (ter ondersteuning van lokale IPv6 AVC) naar Cisco IOS XE Gibraltar 16.12.x (waar lokale IPv6 AVC niet wordt ondersteund). In dergelijke gevallen raden we u aan het bestaande WLAN-beleidsprofiel te verwijderen en een

nieuwe te maken.

17.3.3

- Als u van deze release naar een lagere waarde bent gedegradeerd, kan de WLC in een beginlus belanden als telemetrie is geconfigureerd vanwege Cisco bug-id CSCvt6990 / Cisco bug-id CSCv87417
- Als u van Cisco IOS XE Amsterdam 17.3.1 naar een vroegere release wilt reduceren, verdwijnen de poortkanalen die met hoger bereik zijn geconfigureerd
- Als u van Cisco IOS XE Amsterdam 17.3.1 naar een eerdere release bent gedegradeerd, kunt u de day-0 wizard opnieuw bekijken als u de opdracht "Wireless country" hebt geconfigureerd omdat deze niet bestond voor 17.3
- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.
- Het is niet mogelijk om het WLAN-beleidsprofiel af te sluiten wanneer u uw software converteert van Cisco IOS XE Amsterdam 17.3.x (ter ondersteuning van lokale IPv6 AVC) naar Cisco IOS XE Gibraltar 16.12.x (waar lokale IPv6 AVC niet wordt ondersteund). In dergelijke gevallen raden we u aan het bestaande WLAN-beleidsprofiel te verwijderen en een nieuwe te maken.

17.4.1

- Als u van Cisco IOS XE Amsterdam 17.4.1 naar een eerdere release vóór 17.3 bent gedowngradeerd, kunt u de day-0 wizard opnieuw bekijken als u de opdracht "Wireless country" hebt ingesteld omdat deze niet bestond voor 17.3
- Als u van Cisco IOS XE Amsterdam 17.4.1 naar een vroegere release bent gedegradeerd, verliest u de telemetrie-verbinding als 17.4 gebruikers die telemetrie-bestemming genoemd hebben en die geen opdrachten in eerdere versies kregen. Je moet de telemetrie verbinding opnieuw maken.
- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.

17.5.1

- Als u van Cisco IOS XE Amsterdam 17.4.1 naar een eerdere release vóór 17.3 bent gedowngradeerd, kunt u de day-0 wizard opnieuw bekijken als u de opdracht "Wireless country" hebt ingesteld omdat deze niet bestond voor 17.3
- Als u van Cisco IOS XE Amsterdam 17.4.1 naar een vroegere release bent gedegradeerd, verliest u de telemetrie-verbinding als 17.4 gebruikers die telemetrie-bestemming genoemd hebben en die geen opdrachten in eerdere versies kregen. Je moet de telemetrie verbinding opnieuw maken.
- Continu opnieuw laden wordt waargenomen wanneer Cisco Catalyst 9800 draadloze controller gedowngradeerd is van 17.x tot 16.12.4a. Wij raden u aan om te werken naar Cisco IOS XE Gibraltar 16.12.5 in plaats van 16.12.4a.

Referenties

17.1 hete patching en Rollend AP-upgradegeleider

17.3 hete patching en ISSU-upgradegids.