Mise à niveau et rétrogradation des contrôleurs Catalyst 9800 : conseils et astuces

Table des matières

- Introduction
- Avant de continuer
  - Le cas particulier de l'ingénierie Versions spéciales
- Mise à niveau
  - GIBRALTAR
    - Commutateurs 16.12.2
    - Commutateurs 16.12.3
    - Commutateurs 16.12.4
    - 16.12.5, 16.12.6a et 16.12.7
  - Amsterdam
    - Commutateurs 17.1.1
    - Commutateurs 17.2.1
    - Commutateurs 17.3.1
    - Commutateurs 17.3.2
    - Commutateurs 17.3.3
    - Commutateurs 17.3.4
    - Commutateurs 17.3.5
  - Bengaluru
    - Commutateurs 17.4.1
    - Commutateurs 17.5.1
    - Commutateurs 17.6.1
    - Commutateurs 17.6.2
  - Cupertino
    - Commutateurs 17.7.1
    - Commutateurs 17.8.1
    - 17.9.x.
  - Dublin
    - Commutateurs 17.10.1
    - Commutateurs 17.11.1
    - Commutateurs 17.12.1
- Déclasser
  - GIBRALTAR
    - Commutateurs 16.12.2
    - Commutateurs 16.12.3
    - Commutateurs 16.12.4
  - Amsterdam
    - Commutateurs 17.1.1
    - Commutateurs 17.2.1
    - Commutateurs 17.3.1
    - Commutateurs 17.3.2
    - Commutateurs 17.3.3
    - Commutateurs 17.4.1

Commutateurs 17.5.1
17.9.x.
Commutateurs 17.10.1
Commutateurs 17.11.1
17.12.x
Informations connexes

Introduction

Ce document décrit les points à surveiller lors de la mise à niveau ou de la rétrogradation d'un contrôleur LAN sans fil (WLC) Catalyst 9800.

Avant de continuer

Ce document ne vise pas à remplacer les notes de version qui doivent toujours être le document de référence lors de la mise à niveau. L'objectif est de faciliter la mise à niveau à travers plusieurs versions en mettant en évidence les changements les plus significatifs entre les versions.

Ce document ne remplace pas la lecture des notes de version de votre version logicielle cible. Sauvegardez votre configuration et prenez toutes les précautions nécessaires avant de procéder à une mise à niveau.

Par défaut, le serveur HTTP du 9800 n'est pas mappé de manière statique à un certificat/point de confiance spécifique, ce qui peut entraîner des modifications après la mise à niveau. Définissez le serveur HTTP sur un point de confiance statique (de préférence sur un certificat que vous avez émis à cette fin, ou sur le certificat MIC dans le cas contraire) dans la configuration avant la mise à niveau.

Le cas particulier de l'ingénierie Versions spéciales

Les versions spéciales d'ingénierie ne prennent pas en charge les mises à niveau ISSU. Ce document se concentre uniquement sur les versions publiques publiées sur Cisco.com. Par conséquent, si vous travaillez sur une version spéciale d'ingénierie, reportez-vous aux notes de version que vous avez reçues avec elles afin de recevoir une assistance pour toutes vos questions sur la mise à niveau.

Mise à niveau

Vous pouvez lire directement les notes sous la version du logiciel de destination que vous visez. Les conseils applicables à plusieurs versions sont répétés à chaque fois pour votre commodité. Ne mettez pas à niveau plusieurs versions à la fois. Par exemple, la mise à niveau de 16.12.1 vers 17.3.2 est traitée dans ce document, mais elle ne couvre pas les mises à niveau de 16.12 vers 17.4. Dans un tel scénario, naviguez à travers 17.3 et vérifiez les notes sous la section 17.3, effectuez la mise à niveau, puis regardez la section 17.4 et préparez la deuxième mise à niveau. En conclusion, les conseils répertoriés ne sont plus répétés après trois versions principales, même si elles sont toujours valides, car le document suppose que vous passez par les versions principales intermédiaires.

GIBRALTAR

Commutateurs 16.12.2

- Depuis Cisco IOS® XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise la balise de stratégie par défaut, il se désactive en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- N'utilisez pas plus de 31 caractères pour les noms de points d'accès. Si le nom de l'AP est de 32 caractères ou plus, il peut conduire à une panne du contrôleur.
- Ne déployez pas les fichiers OVA directement sur VMware ESXi 6.5. Il est recommandé d'utiliser un outil OVF pour déployer les fichiers OVA.

Commutateurs 16.12.3

- La version 16.12.3 est la première à imposer la prise en charge des seuls modules SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient hors service après la mise à niveau.
- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise la balise de stratégie par défaut, il se désactive en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- N'utilisez pas plus de 31 caractères pour les noms de points d'accès. Si le nom de l'AP est de 32 caractères ou plus, il peut conduire à une panne du contrôleur.
- Ne déployez pas les fichiers OVA directement sur VMware ESXi 6.5. Il est recommandé d'utiliser un outil OVF afin de déployer les fichiers OVA.

Commutateurs 16.12.4

- Les versions 16.12.3 et 17.2.1 sont les premières à imposer la prise en charge des seuls modules SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient

hors service après la mise à niveau.
- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise une balise de stratégie par défaut, il s'arrête en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.

- N'utilisez pas plus de 31 caractères pour les noms de points d'accès. Si le nom de l'AP est de 32 caractères ou plus, il peut conduire à une panne du contrôleur.

- Ne déployez pas les fichiers OVA directement sur VMware ESXi 6.5. Il est recommandé d'utiliser un outil OVF afin de déployer les fichiers OVA.

16.12.5, 16.12.6a et 16.12.7

Identique à la version 16.12.4.

Amsterdam

Commutateurs 17.1.1

- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise une balise de stratégie par défaut, elle s'arrête en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- À partir de cette version, une nouvelle vérification de l'accessibilité de la passerelle est introduite. Les points d’accès envoient des requêtes d’écho ICMP périodiques (ping) à la passerelle par défaut afin de vérifier la connectivité. Vous devez assurer le filtrage du trafic entre les AP et la passerelle par défaut (comme les ACL) pour autoriser les requêtes ping ICMP entre l'AP et la passerelle par défaut. Si ces requêtes ping sont bloquées, même si la connectivité entre le contrôleur et le point d'accès est active, les points d'accès se rechargent à intervalles de 4 heures.

Commutateurs 17.2.1

- Les versions 16.12.3 et 17.2.1 sont les premières à imposer la prise en charge des seuls modules SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient hors service après la mise à niveau.
- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s et si votre réseau sans fil utilise une balise de stratégie par défaut, il peut s'arrêter en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- À partir de la version 17.1, un nouveau contrôle d'accessibilité de la passerelle est introduit. Les points d’accès envoient des requêtes d’écho ICMP périodiques (ping) à la passerelle par défaut afin de vérifier la connectivité. Vous devez assurer le filtrage du trafic entre les AP et la passerelle par défaut (comme les ACL) pour autoriser les requêtes ping ICMP entre l'AP et la passerelle par défaut. Si ces requêtes ping sont bloquées, même si la connectivité entre le contrôleur et le point d'accès est active, les points d'accès se rechargent à intervalles de 4 heures.

Commutateurs 17.3.1

- 16.12.3 et 17.2.1 sont les premières versions afin d'appliquer la prise en charge des SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient hors service après la mise à niveau.
- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise une balise de stratégie par défaut, elle s'arrête en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- À partir de la version 17.1, un nouveau contrôle d'accessibilité de la passerelle est introduit. Les points d’accès envoient des requêtes d’écho ICMP périodiques (ping) à la passerelle par défaut afin de vérifier la connectivité. Vous devez assurer le filtrage du trafic entre les AP et la passerelle par défaut (comme les ACL) pour autoriser les requêtes ping ICMP entre l'AP et la passerelle par défaut. Si ces requêtes ping sont bloquées, même si la connectivité entre le contrôleur et le point d'accès est active, les points d'accès se rechargent à

intervalles de 4 heures.

- Si vous avez configuré le mode FIPS, veillez à supprimer le `security wpa wpa1 cipher tkip` configuration à partir d'un WLAN avant la mise à niveau de Cisco IOS XE Amsterdam 17.3.x à partir d'une version antérieure. Si vous ne le faites pas, la sécurité WLAN est définie sur TKIP, ce qui n'est pas pris en charge en mode FIPS. Après la mise à niveau, vous devez reconfigurer le WLAN avec AES.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le contrôleur sans fil Cisco Catalyst 9800-CL nécessite 16 Go d'espace disque pour les nouveaux déploiements. Il n'est possible d'augmenter la taille de l'espace disque que par une réinstallation avec une image 17.3.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le nom du point d'accès ne peut contenir que 32 caractères.
- Pour l'authentification des adresses MAC locales (des clients ou des points d'accès), seul le format `aaaabbbbcccc` (sans séparateur) est pris en charge depuis la version 17.3.1. Cela signifie que l'authentification échoue si vous ajoutez une adresse MAC avec des séparateurs dans l'interface utilisateur Web ou l'interface de ligne de commande.
- À partir de cette version, les AP se rechargent après 4 heures s'ils ne peuvent pas joindre un WLC, ne peuvent pas envoyer de requête ping à leur passerelle et ARP à leur passerelle (les trois doivent échouer pour que l'AP redémarre). Il s'agit d'une amélioration (ID de bogue Cisco CSCvt8970) par rapport à la vérification précédente de la passerelle ICMP uniquement à partir des versions précédentes.
- À partir de la version 17.3.1, la nouvelle méthode de configuration des codes de pays pour les points d'accès est la `Wireless country <1 country code>` que vous pouvez répéter plusieurs fois avec différents codes de pays. Cela permet d'augmenter le nombre maximum de codes de pays bien au-delà de 20. Les commandes `ap country` sont toujours présents et continuent à travailler, cependant, envisagez de les changer en `Wireless country` comme la commande `ap country` sont déconseillées dans une version ultérieure.

Commutateurs 17.3.2

- Les versions 16.12.3 et 17.2.1 sont les premières à imposer la prise en charge des seuls modules SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient hors service après la mise à niveau.
- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise une balise de stratégie par défaut, elle s'arrête en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- À partir de la version 17.1, un nouveau contrôle d'accessibilité de la passerelle est introduit.

Les points d'accès envoient des requêtes d'écho ICMP périodiques (ping) à la passerelle par défaut afin de vérifier la connectivité. Vous devez assurer le filtrage du trafic entre les AP et la passerelle par défaut (comme les ACL) pour autoriser les requêtes ping ICMP entre l'AP et la passerelle par défaut. Si ces requêtes ping sont bloquées, même si la connectivité entre le contrôleur et le point d'accès est active, les points d'accès se rechargent à intervalles de 4 heures.

- Si vous avez configuré le mode FIPS, veillez à supprimer le `security wpa wpa1 cipher tkip` configuration à partir d'un WLAN avant la mise à niveau de Cisco IOS XE Amsterdam 17.3.x à partir d'une version antérieure. Si vous ne le faites pas, la sécurité WLAN est définie sur TKIP, ce qui n'est pas pris en charge en mode FIPS. Après la mise à niveau, vous devez reconfigurer le WLAN avec AES.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le contrôleur sans fil Cisco Catalyst 9800-CL nécessite 16 Go d'espace disque pour les nouveaux déploiements. Il n'est possible d'augmenter la taille de l'espace disque que par une réinstallation avec une image 17.3.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le nom du point d'accès ne peut pas dépasser 32 caractères.
- Pour l'authentification des adresses MAC locales (des clients ou des points d'accès), seul le format `aaaabbbbcccc` (sans séparateur) est pris en charge depuis la version 17.3.1. Cela signifie que l'authentification échoue si vous ajoutez une adresse MAC avec des séparateurs dans l'interface utilisateur Web ou l'interface de ligne de commande.
- À partir de la version 17.3.1, les AP se rechargent après 4 heures s'ils ne peuvent pas joindre un WLC, ne peuvent pas envoyer de requête ping à leur passerelle et ARP à leur passerelle (les trois doivent échouer pour que l'AP redémarre). Il s'agit d'une amélioration (ID de bogue Cisco CSCvt8970) de la vérification de passerelle ICMP-only précédente à partir des versions précédentes.
- À partir de la version 17.3.1, la nouvelle méthode de configuration des codes de pays pour les points d'accès est la `Wireless country <1 country code>` que vous pouvez répéter plusieurs fois avec différents codes de pays. Cela permet d'augmenter le nombre maximum de codes de pays bien au-delà de 20. Les commandes `ap country` sont toujours présents et en cours d'exécution, mais pensez à les remplacer par `Wireless country` comme la commande `ap country` sont déconseillées dans une version ultérieure.

Commutateurs 17.3.3

- Les versions 16.12.3 et 17.2.1 sont les premières à imposer la prise en charge des seuls modules SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient hors service après la mise à niveau.
- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez

une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise la balise de stratégie par défaut, elle s'arrête en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.

- À partir de la version 17.1, un nouveau contrôle d'accessibilité de la passerelle est introduit. Les points d'accès envoient des requêtes d'écho ICMP périodiques (ping) à la passerelle par défaut afin de vérifier la connectivité. Vous devez assurer le filtrage du trafic entre les AP et la passerelle par défaut (comme les ACL) pour autoriser les requêtes ping ICMP entre l'AP et la passerelle par défaut. Si ces requêtes ping sont bloquées, même si la connectivité entre le contrôleur et le point d'accès est active, les points d'accès se rechargent à intervalles de 4 heures.
- Si vous avez configuré le mode FIPS, veillez à supprimer le `security wpa wpa1 cipher tkip` configuration à partir d'un WLAN avant la mise à niveau de Cisco IOS XE Amsterdam 17.3.x à partir d'une version antérieure. Si vous ne le faites pas, la sécurité WLAN est définie sur TKIP, ce qui n'est pas pris en charge en mode FIPS. Après la mise à niveau, vous devez reconfigurer le WLAN avec AES.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le contrôleur sans fil Cisco Catalyst 9800-CL nécessite 16 Go d'espace disque pour les nouveaux déploiements. Il n'est possible d'augmenter la taille de l'espace disque que par une réinstallation avec une image 17.3.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le nom du point d'accès ne peut contenir que 32 caractères.
- Pour l'authentification des adresses MAC locales (des clients ou des points d'accès), seul le format `aaaabbbbcccc` (sans séparateur) est pris en charge depuis la version 17.3.1. Cela signifie que l'authentification échoue si vous ajoutez une adresse MAC avec des séparateurs dans l'interface utilisateur Web ou l'interface de ligne de commande.
- À partir de la version 17.3.1, les AP se rechargent après 4 heures s'ils ne peuvent pas joindre un WLC, ne peuvent pas envoyer de requête ping à leur passerelle et ARP à leur passerelle (les trois doivent échouer pour que l'AP redémarre). Il s'agit d'une amélioration (ID de bogue Cisco CSCvt8970) de la vérification de la passerelle ICMP-only précédente à partir des versions précédentes.
- À partir de la version 17.3.1, la nouvelle méthode de configuration des codes de pays pour les points d'accès est la `Wireless country <1 country code>` que vous pouvez répéter plusieurs fois avec différents codes de pays. Cela permet d'augmenter le nombre maximum de codes de pays bien au-delà de 20. Les commandes `ap country` sont toujours présents et fonctionnent, mais envisagez de les remplacer par `Wireless country` comme la commande `ap country` sont déconseillées dans une version ultérieure.
- WLC peut planter si vos AP ont des noms d'hôte de plus de 32 caractères (ID de bogue Cisco CSCvy11981).

Commutateurs 17.3.4

- 16.12.3 et 17.2.1 sont les premières versions afin d'appliquer la prise en charge des SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient hors service

après la mise à niveau.

- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise une balise de stratégie par défaut, elle s'arrête en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- À partir de la version 17.1, un nouveau contrôle d'accessibilité de la passerelle est introduit. Les points d'accès envoient régulièrement des requêtes d'écho ICMP (ping) à la passerelle par défaut pour vérifier la connectivité. Vous devez assurer le filtrage du trafic entre les AP et la passerelle par défaut (comme les ACL) pour autoriser les requêtes ping ICMP entre l'AP et la passerelle par défaut. Si ces requêtes ping sont bloquées, même si la connectivité entre le contrôleur et le point d'accès est active, les points d'accès se rechargent à intervalles de 4 heures.
- Si vous avez configuré le mode FIPS, veillez à supprimer le `security wpa wpa1 cipher tkip` configuration à partir d'un WLAN avant la mise à niveau de Cisco IOS XE Amsterdam 17.3.x à partir d'une version antérieure. Si vous ne le faites pas, la sécurité WLAN est définie sur TKIP, ce qui n'est pas pris en charge en mode FIPS. Après la mise à niveau, vous devez reconfigurer le WLAN avec AES.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le contrôleur sans fil Cisco Catalyst 9800-CL nécessite 16 Go d'espace disque pour les nouveaux déploiements. Il n'est possible d'augmenter la taille de l'espace disque que par une réinstallation avec une image 17.3.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le nom du point d'accès ne peut pas dépasser 32 caractères.
- Pour l'authentification des adresses MAC locales (des clients ou des points d'accès), seul le format `aaaabbbbcccc` (sans séparateur) est pris en charge depuis la version 17.3.1. Cela signifie que l'authentification échoue si vous ajoutez une adresse MAC avec des séparateurs dans l'interface utilisateur Web ou l'interface de ligne de commande.
- À partir de la version 17.3.1, APsl se recharge après 4 heures s'ils ne peuvent pas joindre un WLC, ne peuvent pas envoyer de requête ping à leur passerelle et ARP à leur passerelle (les trois doivent échouer pour que l'AP redémarre). Il s'agit d'une amélioration (ID de bogue Cisco CSCvt8970) par rapport à la vérification de passerelle ICMP-only précédente à partir des versions précédentes.
- À partir de la section 17.3.1, la nouvelle méthode de configuration des codes de pays pour les points d'accès est la `Wireless country <1 country code>` que vous pouvez répéter plusieurs fois avec différents codes de pays. Cela permet d'augmenter le nombre maximum de codes de pays bien au-delà de 20. Les commandes `ap country` sont toujours présents et fonctionnent, mais envisagez de les remplacer par `Wireless country` comme la commande `ap country` sont prévues pour être déconseillées dans une version ultérieure.
- Lors de la mise à niveau vers 17.3.4 et les versions ultérieures, il est conseillé d'avoir le chargeur de démarrage 16.12.5r/rommon installé sur les contrôleurs le cas échéant (le

9800-80). (Le 9800-40 ne dispose pas de rommon 16.12.5r pour le moment et n'a pas besoin d'une mise à niveau rommon.)

- La mise à niveau du contrôleur, de Cisco IOS XE Bengaluru 17.3.x vers n'importe quelle version utilisant ISSU, peut échouer si le `snmp-server enable traps hsrp`est configurée. Assurez-vous que vous retirez le `snmp-server enable traps hsrp` avant de démarrer une mise à niveau d'ISSU car la commande `snmp-server enable traps hsrp` est supprimée de Cisco IOS XE Bengaluru 17.4.x.
- Lors de la mise à niveau vers Cisco IOS XE 17.3.x et versions ultérieures, si le `ip http active-session-modules none` est activée, vous ne pouvez pas accéder à l'interface graphique utilisateur du contrôleur via HTTPS. Afin d'accéder à l'interface utilisateur graphique à l'aide de HTTPS, exécutez ces commandes :
  - ip http session-module-list pkilist OPENRESTY_PKI
  - ip http active-session-modules pkilist

Commutateurs 17.3.5

- En raison de l'ID de bogue Cisco CSCwb13784, si votre MTU de chemin est inférieure à 1500 octets, les AP ne peuvent peut-être pas se joindre. Téléchargez le correctif SMU disponible pour 17.3.5 afin de résoudre ce problème.
- 16.12.3 et 17.2.1 sont les premières versions afin d'appliquer la prise en charge des SFP répertoriés comme pris en charge dans la documentation. Les modules SFP non répertoriés provoquent une panne de port. Vérifiez la liste des SFP pris en charge et assurez-vous que vos SFP sont compatibles afin d'éviter que les ports de données ne soient hors service après la mise à niveau.
- Le fichier de mise à niveau de cette version peut être trop volumineux pour le téléchargement HTTP (lors d'une mise à niveau de l'interface utilisateur Web) si vous utilisez la version 16.12.1. Utilisez une autre méthode de transfert ou passez par 16.12.2 qui prend en charge les fichiers plus volumineux à télécharger via l'interface utilisateur Web.
- À partir de Cisco IOS XE Gibraltar 16.12.2s, le mappage WLAN automatique au profil de stratégie par défaut sous la balise de stratégie par défaut a été supprimé. Si vous effectuez une mise à niveau à partir d'une version antérieure à Cisco IOS XE Gibraltar 16.12.2s, et si votre réseau sans fil utilise une balise de stratégie par défaut, elle s'arrête en raison de la modification du mappage par défaut. Afin de restaurer le fonctionnement du réseau, ajoutez le WLAN requis aux mappages de stratégie sous la balise de stratégie par défaut.
- À partir de la version 17.1, un nouveau contrôle d'accessibilité de la passerelle est introduit. Les points d’accès envoient des requêtes d’écho ICMP périodiques (ping) à la passerelle par défaut afin de vérifier la connectivité. Vous devez assurer le filtrage du trafic entre les AP et la passerelle par défaut (comme les ACL) pour autoriser les requêtes ping ICMP entre l'AP et la passerelle par défaut. Si ces requêtes ping sont bloquées, même si la connectivité entre le contrôleur et le point d'accès est active, les points d'accès se rechargent à intervalles de 4 heures.
- Si vous avez configuré le mode FIPS, veillez à supprimer le `security wpa wpa1 cipher tkip` configuration à partir d'un WLAN avant la mise à niveau de Cisco IOS XE Amsterdam 17.3.x à partir d'une version antérieure. Si vous ne le faites pas, la sécurité WLAN est définie sur TKIP, ce qui n'est pas pris en charge en mode FIPS. Après la mise à niveau, vous devez

reconfigurer le WLAN avec AES.

- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le contrôleur sans fil Cisco Catalyst 9800-CL nécessite 16 Go d'espace disque pour les nouveaux déploiements. Il n'est possible d'augmenter la taille de l'espace disque que par une réinstallation avec une image 17.3.
- À partir de la version 17.3.1 de Cisco IOS XE Amsterdam, le nom du point d'accès ne peut contenir que 32 caractères.
- Pour l'authentification des adresses MAC locales (des clients ou des points d'accès), seul le format aaaabbbbcccc (sans séparateur) est pris en charge depuis la version 17.3.1. Cela signifie que l'authentification échoue si vous ajoutez une adresse MAC avec des séparateurs dans l'interface utilisateur Web ou l'interface de ligne de commande.
- À partir de la version 17.3.1, les APsl se rechargent après 4 heures s'ils ne peuvent pas joindre un WLC, ne peuvent pas envoyer de requête ping à leur passerelle et ARP à leur passerelle (les trois doivent échouer pour que l'AP redémarre). Il s'agit d'une amélioration (ID de bogue Cisco CSCvt8970) de la vérification de passerelle ICMP-only précédente à partir des versions précédentes.
- À partir de la section 17.3.1, la nouvelle méthode de configuration des codes de pays pour les points d'accès est la Wireless country <1 country code> que vous pouvez répéter plusieurs fois avec différents codes de pays. Cela permet d'augmenter le nombre maximum de codes de pays bien au-delà de 20. Les commandes ap country sont toujours présents et fonctionnent, mais envisagez de les remplacer par Wireless country comme la commande ap country sont prévues pour être déconseillées dans une version ultérieure.
- Lors de la mise à niveau vers 17.3.4 et les versions ultérieures, il est conseillé d'avoir le chargeur de démarrage 16.12.5r/rommon installé sur les contrôleurs le cas échéant (le 9800-80). (Le 9800-40 ne dispose pas de rommon 16.12.5r pour le moment et n'a pas besoin d'une mise à niveau rommon.)
- La mise à niveau du contrôleur, de Cisco IOS XE Bengaluru 17.3.x vers n'importe quelle version utilisant ISSU, peut échouer si le snmp-server enable traps hsrpest configurée. Assurez-vous que vous retirez le snmp-server enable traps hsrp avant de démarrer une mise à niveau d'ISSU car la commande snmp-server enable traps hsrp est supprimée de Cisco IOS XE Bengaluru 17.4.x.

- Lors de la mise à niveau vers Cisco IOS XE 17.3.x et versions ultérieures, si le ip http active-session-modules none est activée, vous ne pouvez pas accéder à l'interface graphique utilisateur du contrôleur via HTTPS. Afin d'accéder à l'interface utilisateur graphique à l'aide de HTTPS, exécutez ces commandes :

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

Bengaluru

Commutateurs 17.4.1

- À partir de la version 17.4.1, les points d'accès Cisco IOS de phase 1 ne sont plus pris en charge (1700, 2700, 3700, 1570), sauf IW3700.
- Vos réseaux locaux sans fil peuvent être arrêtés après la mise à niveau s'ils ne sont pas

WPA (SSID invité, ouvert ou CWA) et si le mode de transfert adaptatif est configuré. La solution consiste à supprimer la configuration FT adaptative avant la mise à niveau (ID de bogue Cisco CSCvx34349). La configuration FT adaptative n'a aucun sens sur un SSID non WPA, il n'y a donc aucune perte de quoi que ce soit en le supprimant.
- Le WLC peut planter si vos AP ont des noms d'hôte de plus de 32 caractères (ID de bogue Cisco CSCvy1981).

Commutateurs 17.5.1

- À partir de la version 17.4.1, les points d'accès Cisco IOS de phase 1 ne sont plus pris en charge (1700, 2700, 3700, 1570), sauf IW3700.
- À partir de la version 17.4.1 de Cisco IOS XE Benghaluru, la solution de télémétrie fournit un nom pour l'adresse du récepteur au lieu de l'adresse IP pour les données de télémétrie. Il s'agit d'une option supplémentaire. Lors de la rétrogradation du contrôleur et de la mise à niveau suivante, il est probable qu'il y ait un problème avec la version de la mise à niveau qui utilise les récepteurs nouvellement nommés, et ceux-ci ne sont pas reconnus dans la rétrogradation. La nouvelle configuration est rejetée et échoue lors de la mise à niveau suivante. La perte de configuration peut être évitée lorsque la mise à niveau ou la rétrogradation est effectuée à partir de Cisco DNA Center.
- Vos réseaux locaux sans fil peuvent être arrêtés après la mise à niveau s'ils ne sont pas WPA (SSID invité, ouvert ou CWA) et si le mode de transfert adaptatif est configuré. La solution consiste à supprimer la configuration FT adaptative avant la mise à niveau (ID de bogue Cisco CSCvx34349). La configuration FT adaptative n'a aucun sens sur un SSID non WPA, il n'y a donc aucune perte de quoi que ce soit en le supprimant.
- Le WLC peut planter si vos AP ont des noms d'hôte de plus de 32 caractères (ID de bogue Cisco CSCvy1981).
- Lorsque vous mettez à niveau l'interface graphique d'une version à une autre, il est recommandé d'effacer le cache du navigateur pour que toutes les pages de l'interface graphique se rechargent correctement.

- Lors de la mise à niveau vers Cisco IOS XE 17.3.x et versions ultérieures, si le ip http active-session-modules none est activée, vous ne pouvez pas accéder à l'interface utilisateur graphique à l'aide de HTTPS. Afin d'accéder à l'interface utilisateur graphique à l'aide de HTTPS, exécutez ces commandes :

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

- Si vous rencontrez l'erreur « ERR_SSL_VERSION_OR_CIPHER_MISMATCH » à partir de l'interface utilisateur graphique après un redémarrage ou une panne système, il est recommandé de régénérer le certificat trustpoint.
- La procédure de génération d'un nouveau point de confiance auto-signé est la suivante :

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

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentic
```

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

Commutateurs 17.6.1

- À partir de la version 17.4.1, les points d'accès Cisco IOS de phase 1 ne sont plus pris en charge (1700, 2700, 3700, 1570), sauf IW3700.
- À partir de la version 17.4.1 de Cisco IOS XE Benghaluru, la solution de télémétrie fournit un nom pour l'adresse du récepteur au lieu de l'adresse IP pour les données de télémétrie. Il s'agit d'une option supplémentaire. Lors de la rétrogradation du contrôleur et de la mise à niveau suivante, il est probable qu'il y ait un problème avec la version de la mise à niveau qui utilise les récepteurs nouvellement nommés, et ceux-ci ne sont pas reconnus dans la rétrogradation. La nouvelle configuration est rejetée et échoue lors de la mise à niveau suivante. La perte de configuration peut être évitée lorsque la mise à niveau ou la rétrogradation est effectuée à partir de Cisco DNA Center.
- Vos réseaux locaux sans fil peuvent être arrêtés après la mise à niveau s'ils ne sont pas WPA (SSID invité, ouvert ou CWA) et si le mode de transfert adaptatif est configuré. La solution consiste à supprimer la configuration FT adaptative avant la mise à niveau (ID de bogue Cisco CSCvx34349). La configuration FT adaptative n'a aucun sens sur un SSID non WPA, il n'y a donc aucune perte de quoi que ce soit en le supprimant.
- Lorsque vous mettez à niveau l'interface graphique d'une version à une autre, il est recommandé d'effacer le cache du navigateur pour que toutes les pages de l'interface graphique se rechargent correctement.
- Un AP qui a rejoint un WLC 17.6.1 ou ultérieur ne peut plus rejoindre un WLC AireOS à moins qu'il exécute le code 8.10.162 et ultérieur, ou 8.5.176.2 et ultérieur 8.5.
- Lors d'une mise à niveau vers 17.6.1 et les versions ultérieures, il est conseillé d'installer le chargeur de démarrage 16.12.5r/rommon sur les contrôleurs, le cas échéant (le 9800-80). (Le 9800-40 ne dispose pas de rommon 16.12.5r pour le moment et n'a pas besoin d'une mise à niveau rommon.)
- La mise à niveau du contrôleur, de Cisco IOS XE Bengaluru 17.3.x vers n'importe quelle version utilisant ISSU, peut échouer si le snmp-server enable traps hsrpest configurée. Assurez-vous que vous retirez le snmp-server enable traps hsrp avant de démarrer une mise à niveau d'ISSU car la commande snmp-server enable traps hsrp est supprimée de Cisco IOS XE Bengaluru 17.4.x.

- Lors de la mise à niveau vers Cisco IOS XE 17.3.x et versions ultérieures, si le ip http active-session-modules none est activée, l'accès HTTPS à l'interface graphique du contrôleur ne fonctionne pas. Afin d'accéder à l'interface utilisateur graphique à l'aide de HTTPS, exécutez ces commandes :
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist
- Si vous rencontrez l'erreur « ERR_SSL_VERSION_OR_CIPHER_MISMATCH » à partir de l'interface utilisateur graphique après un redémarrage ou une panne système, il est recommandé de régénérer le certificat trustpoint.
- La procédure de génération d'un nouveau point de confiance auto-signé est la suivante :

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

```
no ip http server no ip http securffwe-server ip http server ip http secure-server ip http authen
```

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

Commutateurs 17.6.2

- À partir de la version 17.4.1, les points d'accès Cisco IOS de phase 1 ne sont plus pris en charge (1700, 2700, 3700, 1570), sauf IW3700.
- À partir de la version 17.4.1 de Cisco IOS XE Benghaluru, la solution de télémétrie fournit un nom pour l'adresse du récepteur au lieu de l'adresse IP pour les données de télémétrie. Il s'agit d'une option supplémentaire. Lors de la rétrogradation du contrôleur et de la mise à niveau suivante, il est probable qu'il y ait un problème avec la version de la mise à niveau qui utilise les récepteurs nouvellement nommés, et ceux-ci ne sont pas reconnus dans la rétrogradation. La nouvelle configuration est rejetée et échoue lors de la mise à niveau suivante. La perte de configuration peut être évitée lorsque la mise à niveau ou la rétrogradation est effectuée à partir de Cisco DNA Center.
- Vos réseaux locaux sans fil peuvent être arrêtés après la mise à niveau s'ils ne sont pas

WPA (SSID invité, ouvert ou CWA) et si le mode de transfert adaptatif est configuré. La solution consiste à supprimer la configuration FT adaptative avant la mise à niveau (ID de bogue Cisco CSCvx34349). La configuration FT adaptative n'a aucun sens sur un SSID non WPA, il n'y a donc aucune perte de quoi que ce soit en le supprimant.

- Lorsque vous mettez à niveau l'interface graphique d'une version à une autre, il est recommandé d'effacer le cache du navigateur pour que toutes les pages de l'interface graphique se rechargent correctement.
- Un AP qui a rejoint un WLC 17.6.1 ou ultérieur ne peut plus rejoindre un WLC AireOS à moins qu'il exécute le code 8.10.162 et ultérieur, ou 8.5.176.2 et ultérieur 8.5.
- Lors d'une mise à niveau vers 17.6.1 et les versions ultérieures, il est conseillé d'installer le chargeur de démarrage 16.12.5r/rommon sur les contrôleurs, le cas échéant (le 9800-80). (Le 9800-40 n'a pas de rommon 16.12.5r pour le moment et n'a pas besoin d'une mise à niveau rommon.)
- La mise à niveau du contrôleur, de Cisco IOS XE Bengaluru 17.3.x vers n'importe quelle version utilisant ISSU, peut échouer si le snmp-server enable traps hsrpest configurée. Assurez-vous que vous retirez le snmp-server enable traps hsrp avant de démarrer une mise à niveau d'ISSU car la commande snmp-server enable traps hsrp est supprimée de Cisco IOS XE Bengaluru 17.4.x.
- Lors de la mise à niveau vers Cisco IOS XE 17.3.x et versions ultérieures, si le ip http active-session-modules none est activée, l'accès à l'interface graphique du contrôleur HTTPS ne fonctionne pas. Afin d'accéder à l'interface utilisateur graphique à l'aide de HTTPS, exécutez ces commandes :
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist
- N'utilisez pas plus de 31 caractères pour les noms de points d'accès. Si le nom du point d'accès est de 32 caractères ou plus, une panne du contrôleur peut se produire.
- Si vous rencontrez l'erreur « ERR_SSL_VERSION_OR_CIPHER_MISMATCH » à partir de l'interface utilisateur graphique après un redémarrage ou une panne système, il est recommandé de régénérer le certificat trustpoint.
- La procédure de génération d'un nouveau point de confiance auto-signé est la suivante :

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

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentic
```

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

Cupertino

Cette section suppose que vous démarrez à partir de la version 17.6.1 ou ultérieure et que vous effectuez une mise à niveau vers une version de Cupertino. Si vous effectuez une mise à niveau directement à partir d'une version antérieure (qui peut être prise en charge, consultez les notes de version afin d'être certain), lisez les mises en garde des sections 17.3 et 17.6.

Commutateurs 17.7.1

- N'utilisez pas plus de 31 caractères pour les noms de points d'accès. Si le nom du point d'accès est de 32 caractères ou plus, une panne du contrôleur peut se produire.
- 17.7.1 nécessite la configuration des codes pays AP dans les profils de jointure AP.
- En raison de l'ID de bogue Cisco CSCvu2886, si vous avez 9130 ou 9124 AP, vous devez passer par 17.3.5a lors de la mise à niveau vers 17.7.1 ou une version ultérieure à partir d'une version antérieure à 17.3.4.
- À partir de la version 17.7.1 de Cisco IOS XE Cupertino, pour le contrôleur sans fil Cisco Catalyst 9800-CL, assurez-vous que vous avez terminé le reporting RUM (Resource Utilization Measurement) et que l'ACK est disponible sur l'instance du produit au moins une fois. Cela permet de s'assurer que les informations d'utilisation correctes et à jour sont reflétées dans Cisco Smart Software Manager (CSSM). Si vous n'y parvenez pas, un maximum de 50 points d'accès peuvent rejoindre un 9800-CL jusqu'à ce qu'un rapport de licence soit envoyé par accusé de réception.

Commutateurs 17.8.1

- N'utilisez pas plus de 31 caractères pour les noms de points d'accès. Si le nom du point d'accès est de 32 caractères ou plus, une panne du contrôleur peut se produire.
- 17.7.1 nécessite la configuration des codes pays AP dans les profils de jointure AP.
- En raison de l'ID de bogue Cisco CSCvu2886, si vous avez 9130 ou 9124 AP, vous devez passer par 17.3.5a lors de la mise à niveau vers 17.7.1 ou une version ultérieure à partir d'une version antérieure à 17.3.4.
- À partir de la version 17.7.1 de Cisco IOS XE Cupertino, pour le contrôleur sans fil Cisco Catalyst 9800-CL, assurez-vous que vous avez terminé le reporting RUM et que l'ACK est disponible sur l'instance du produit au moins une fois. Cela permet de s'assurer que les informations d'utilisation correctes et à jour sont reflétées dans le CSSM. Si vous n'y parvenez pas, un maximum de 50 points d'accès peuvent rejoindre un 9800-CL jusqu'à ce qu'un rapport de licence soit envoyé par accusé de réception.

17.9.x.

- Les points d'accès exécutant Cisco IOS-XE 17.9.3 peuvent rencontrer des problèmes lors de la tentative de mise à niveau de leur logiciel en raison d'un espace insuffisant dans le /tmp répertoire. Quand le /tmp l'espace sur l'AP devient plein, il empêche le téléchargement de la nouvelle image AP. Dans de tels cas, il est recommandé de redémarrer l'AP.

- Les points d'accès 11AC de phase 2 peuvent entrer dans une boucle de démarrage lors de la mise à niveau du logiciel sur une liaison WAN. Pour plus d'informations, consultez 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.

- Les versions 17.9.3 et ultérieures réactivent la prise en charge des points d'accès Cisco IOS (séries x700 et 1570). Ils n'étaient pas pris en charge entre 17.4 et 17.9.2. La prise en charge de ces points d'accès ne s'étend pas au-delà du cycle de vie normal du produit. Reportez-vous aux bulletins de fin de support individuels sur Cisco.com.
- La mise à niveau du contrôleur de Cisco IOS XE Bengaluru 17.3.x vers Cisco IOS XE Bengaluru 17.6.x ou Cisco IOS XE Cupertino 17.9.x et versions ultérieures à l'aide d'ISSU peut échouer si la commande domain est configurée. Assurez-vous que vous exécutez la commande no domain avant de démarrer une mise à niveau ISSU parce que la commande domain a été supprimée de Cisco IOS XE Benghaluru 17.6.x.
- À partir de la version 17.7.1 de Cisco IOS XE Cupertino, pour le contrôleur sans fil Cisco Catalyst 9800-CL, assurez-vous que vous avez terminé le reporting RUM et que l'ACK est disponible sur l'instance du produit au moins une fois. Cela permet de s'assurer que les informations d'utilisation correctes et à jour sont reflétées dans le CSSM. Si vous n'y parvenez pas, un maximum de 50 points d'accès peuvent rejoindre un 9800-CL jusqu'à ce qu'un rapport de licence soit envoyé par accusé de réception.
- Une fragmentation inférieure à 1500 n'est pas prise en charge pour les paquets RADIUS générés par les clients sans fil dans l'interface Gi0 (OOB).
- À partir de la version 17.3, le 9800-CL nécessite 16 Go d'espace disque pour fonctionner correctement. Vous ne pouvez pas augmenter la taille dynamiquement si votre instance WLC a commencé avec un OVA de 8 Go (depuis avant 17.3). La seule façon est de créer un nouveau WLC à partir d'un OVA daté de plus de 17.3.
- Le contrôleur sans fil Cisco Catalyst 9800-L peut ne pas répondre aux signaux d'interruption reçus sur son port de console pendant le démarrage, empêchant ainsi les utilisateurs d'accéder au rommon. Ce problème est observé sur les contrôleurs fabriqués jusqu'en novembre 2019, avec le paramètre config-register par défaut de 0x2102. Ce problème peut être évité si vous définissez config-register sur 0x2002. Ce problème est résolu dans la rommon 16.12(3r) du contrôleur sans fil Cisco Catalyst 9800-L. Pour plus d'informations sur la mise à niveau de rommon, consultez la Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers du document Mise à niveau des périphériques matériels programmables sur site pour les contrôleurs sans fil de la gamme Cisco Catalyst 9800.

- Si ce message d'erreur s'affiche après un redémarrage ou une panne du système, il est recommandé de régénérer le certificat trustpoint :

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilisez ces commandes dans l'ordre spécifié afin de générer un nouveau certificat de point de confiance auto-signé :

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

- Vérifiez que votre adresse MAC de mobilité est définie avec la wireless mobility mac-address erasecat4000_flash:.
- Ces protocoles sont désormais pris en charge par le port de service de la version 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infrastructure Cisco Prime
  - Telnet
  - Interface graphique du contrôleur
  - DNS
  - Transfert de fichiers
  - RNB
  - HTTP
  - HTTPS
  - LDAP
  - Licence pour la fonction Smart Licensing pour communiquer avec CSSM
  - Netconf
  - NetFlow

    - NTP
    - RADIUS (y compris CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+

- L'image AP pour 17.9 est plus grande que la mémoire flash AP autorisée à l'origine. Si vous voyez l'AP se plaindre de ne pas avoir assez d'espace lors du téléchargement de l'image 17.9, c'est probablement parce que vous n'avez pas respecté le chemin de mise à niveau par 17.3.5 comme conseillé dans les notes de publication ou que votre AP exécute une image AireOS plus ancienne. Soit en passant par un WLC 17.3.5 ou ultérieur, soit en mettant à niveau l'image AireOS vers la dernière redimensionne la mémoire flash AP afin de permettre le téléchargement de l'image 17.9.

Dublin

Commutateurs 17.10.1

- La fonction CCKM (Cisco Centralized Key Management) est en cours de désapprobation par rapport à la version 17.10.x de Cisco IOS XE Dublin.
- Smart Call Home devient obsolète en faveur de Smart Transport pour les licences.

- Les points d'accès exécutant Cisco IOS-XE 17.9.3 ou version ultérieure peuvent rencontrer des problèmes lors de la tentative de mise à niveau de leur logiciel en raison d'un espace insuffisant dans le `/tmp` répertoire. Quand le `/tmp` l'espace sur l'AP devient plein, il empêche le téléchargement de la nouvelle image AP. Dans de tels cas, il est recommandé de redémarrer l'AP.

  Les points d'accès de phase 2 peuvent entrer dans une boucle de démarrage lors de la mise à niveau du logiciel sur une liaison WAN. Pour plus d'informations, consultez 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.

- À partir de la version 17.7.1 de Cisco IOS XE Cupertino, pour le contrôleur sans fil Cisco Catalyst 9800-CL, assurez-vous que vous avez terminé la création de rapports RUM et que l'accusé de réception est disponible sur l'instance du produit au moins une fois. Cela permet de s'assurer que les informations d'utilisation correctes et à jour sont reflétées dans le CSSM. Si vous n'y parvenez pas, un maximum de 50 points d'accès peuvent rejoindre un 9800-CL jusqu'à ce qu'un rapport de licence soit envoyé par accusé de réception.
- Une fragmentation inférieure à 1500 n'est pas prise en charge pour les paquets RADIUS

générés par les clients sans fil dans l'interface Gi0 (OOB).

- À partir de la version 17.3, le 9800-CL nécessite 16 Go d'espace disque pour fonctionner correctement. Vous ne pouvez pas augmenter la taille dynamiquement si votre instance WLC a commencé avec un OVA de 8 Go (depuis avant 17.3). La seule façon est de créer un nouveau WLC à partir d'un OVA daté de plus de 17.3.
- Le contrôleur sans fil Cisco Catalyst 9800-L peut ne pas répondre aux signaux BREAK reçus sur son port de console pendant le démarrage, empêchant ainsi les utilisateurs d'accéder au rommon. Ce problème est observé sur les contrôleurs fabriqués jusqu'en novembre 2019, avec le paramètre config-register par défaut de 0x2102. Ce problème peut être évité si vous définissez config-register sur 0x2002. Le problème est résolu dans le rommon 16.12(3r) du contrôleur sans fil Cisco Catalyst 9800-L. Pour plus d'informations sur la façon de mettre à niveau le rommon, consultez la section Mise à niveau du rommon pour les contrôleurs sans fil Cisco Catalyst 9800-L du document Mise à niveau des périphériques matériels programmables sur site pour les contrôleurs sans fil Cisco Catalyst 9800.

- Si ce message d'erreur s'affiche après un redémarrage ou une panne du système, il est recommandé de régénérer le certificat trustpoint :

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilisez ces commandes dans l'ordre spécifié afin de générer un nouveau certificat de point de confiance auto-signé :

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

- Vérifiez que votre adresse MAC de mobilité est définie avec la wireless mobility mac-address erasecat4000_flash:.
- Ces protocoles sont désormais pris en charge par le port de service de la version 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infrastructure Cisco Prime

    - Telnet
    - Interface graphique du contrôleur
    - DNS
    - Transfert de fichiers
    - RNB
    - HTTP
    - HTTPS
    - LDAP
    - Licence pour la fonction Smart Licensing pour communiquer avec CSSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (y compris CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- L'image AP pour 17.9 est plus grande que la mémoire flash AP autorisée à l'origine. Si vous voyez l'AP se plaindre de ne pas avoir assez d'espace lors du téléchargement de l'image 17.9, c'est probablement parce que vous n'avez pas respecté le chemin de mise à niveau par 17.3.5 comme indiqué dans les notes de publication, ou que votre AP exécute une image AireOS plus ancienne. Soit en passant par un WLC 17.3.5 et ultérieur ou en mettant à niveau l'image AireOS vers la dernière redimensionne la mémoire flash AP afin de permettre le téléchargement de l'image 17.9.

Commutateurs 17.11.1

- La fonctionnalité CCKM est désapprouvée de Cisco IOS XE Dublin 17.10.x.
- Smart Call Home devient obsolète en faveur de Smart Transport pour les licences

- Les points d'accès exécutant Cisco IOS-XE 17.9.3 ou version ultérieure peuvent rencontrer des problèmes lors de la tentative de mise à niveau de leur logiciel en raison d'un espace

insuffisant dans le /tmp répertoire. Quand le /tmp l'espace sur l'AP devient plein, il empêche le téléchargement de la nouvelle image AP. Dans de tels cas, il est recommandé de redémarrer l'AP.

Les points d'accès de phase 2 peuvent entrer dans une boucle de démarrage lors de la mise à niveau du logiciel sur une liaison WAN. Pour plus d'informations, consultez 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.

- À partir de la version 17.7.1 de Cisco IOS XE Cupertino, pour le contrôleur sans fil Cisco Catalyst 9800-CL, assurez-vous que vous avez terminé le reporting RUM et que l'ACK est disponible sur l'instance du produit au moins une fois. Cela permet de s'assurer que les informations d'utilisation correctes et à jour sont reflétées dans le CSSM. Si vous n'y parvenez pas, un maximum de 50 points d'accès peuvent rejoindre un 9800-CL jusqu'à ce qu'un rapport de licence soit envoyé par accusé de réception.
- Une fragmentation inférieure à 1500 n'est pas prise en charge pour les paquets RADIUS générés par les clients sans fil dans l'interface Gi0 (OOB).
- À partir de la version 17.3, le 9800-CL nécessite 16 Go d'espace disque pour fonctionner correctement. Vous ne pouvez pas augmenter la taille dynamiquement si votre instance WLC a commencé avec un OVA de 8 Go (depuis avant 17.3). La seule façon est de créer un nouveau WLC à partir d'un OVA daté de plus de 17.3.
- Le contrôleur sans fil Cisco Catalyst 9800-L peut ne pas répondre aux signaux d'interruption reçus sur son port de console pendant le démarrage, empêchant ainsi les utilisateurs d'accéder au rommon. Ce problème est observé sur les contrôleurs fabriqués jusqu'en novembre 2019, avec le paramètre config-register par défaut de 0x2102. Elle peut être évitée si vous définissez config-register sur 0x2002. Ce problème est résolu dans la rommon 16.12(3r) du contrôleur sans fil Cisco Catalyst 9800-L. Pour plus d'informations sur la façon de mettre à niveau le rommon, consultez la section Mise à niveau du rommon pour les contrôleurs sans fil Cisco Catalyst 9800-L du document Mise à niveau des périphériques matériels programmables sur site pour les contrôleurs sans fil Cisco Catalyst 9800.

- Si ce message d'erreur s'affiche après un redémarrage ou une panne du système, il est recommandé de régénérer le certificat trustpoint :

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilisez ces commandes dans l'ordre spécifié afin de générer un nouveau certificat de point de confiance auto-signé :

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

- Vérifiez que votre adresse MAC de mobilité est définie avec la wireless mobility mac-address erasecat4000_flash:.
- Ces protocoles sont désormais pris en charge par le port de service de la version 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infrastructure Cisco Prime
  - Telnet
  - Interface graphique du contrôleur
  - DNS
  - Transfert de fichiers
  - RNB
  - HTTP
  - HTTPS
  - LDAP
  - Licence pour la fonction Smart Licensing pour communiquer avec CSSM
  - Netconf
  - NetFlow
  - NTP
  - RADIUS (y compris CoA)
  - Restconf
  - SNMP
  - SSH

    - SYSLOG
    - TACACS+

- L'image AP pour 17.9 est plus grande que la mémoire flash AP autorisée à l'origine. Si vous voyez l'AP se plaindre de ne pas avoir assez d'espace lors du téléchargement de l'image 17.9, c'est probablement parce que vous n'avez pas respecté le chemin de mise à niveau par 17.3.5 comme indiqué dans les notes de publication, ou que votre AP exécute une image AireOS plus ancienne. Soit en passant par un WLC 17.3.5 et ultérieur ou en mettant à niveau l'image AireOS vers la dernière redimensionne la mémoire flash AP afin de permettre le téléchargement de l'image 17.9.

Commutateurs 17.12.1

- La fonctionnalité CCKM est désapprouvée de Cisco IOS XE Dublin 17.10.x.
- Smart Call Home devient obsolète en faveur de Smart Transport pour les licences.

- Les points d'accès exécutant Cisco IOS-XE 17.9.3 ou version ultérieure peuvent rencontrer des problèmes lors de la tentative de mise à niveau de leur logiciel en raison d'un espace insuffisant dans le /tmp répertoire. Quand le /tmp l'espace sur l'AP devient plein, il empêche le téléchargement de la nouvelle image AP. Dans de tels cas, il est recommandé de redémarrer l'AP.

  Les points d'accès de phase 2 peuvent entrer dans une boucle de démarrage lors de la mise à niveau du logiciel sur une liaison WAN. Pour plus d'informations, consultez 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.

- Les versions 17.12.1 et ultérieures réactivent la prise en charge des points d'accès Cisco IOS (séries x700 et 1570). Ils n'étaient pas pris en charge entre 17.4 et 17.9.2. La prise en charge de ces points d'accès ne s'étend pas au-delà du cycle de vie normal du produit. Reportez-vous aux bulletins de fin de support individuels sur Cisco.com.
- À partir de la version 17.7.1 de Cisco IOS XE Cupertino, pour le contrôleur sans fil Cisco Catalyst 9800-CL, assurez-vous que vous avez terminé le reporting RUM et que l'ACK est disponible sur l'instance du produit au moins une fois. Cela permet de s'assurer que les informations d'utilisation correctes et à jour sont reflétées dans le CSSM. Si vous n'y parvenez pas, un maximum de 50 points d'accès peuvent rejoindre un 9800-CL jusqu'à ce qu'un rapport de licence soit envoyé par accusé de réception.
- Une fragmentation inférieure à 1500 n'est pas prise en charge pour les paquets RADIUS générés par les clients sans fil dans l'interface Gi0 (OOB).
- À partir de la version 17.3, le 9800-CL nécessite 16 Go d'espace disque pour fonctionner correctement. Vous ne pouvez pas augmenter la taille dynamiquement si votre instance WLC a commencé avec un OVA de 8 Go (depuis avant 17.3). La seule façon est de créer un nouveau WLC à partir d'un OVA daté de plus de 17.3.
- Le contrôleur sans fil Cisco Catalyst 9800-L peut ne pas répondre aux signaux d'interruption reçus sur son port de console pendant le démarrage, empêchant ainsi les utilisateurs d'accéder au rommon. Ce problème est observé sur les contrôleurs fabriqués jusqu'en

novembre 2019, avec le paramètre config-register par défaut de 0x2102. Ce problème peut être évité si vous définissez config-register sur 0x2002. Ce problème est résolu dans la rommon 16.12(3r) du contrôleur sans fil Cisco Catalyst 9800-L. Pour plus d'informations sur la façon de mettre à niveau le rommon, consultez la section Mise à niveau du rommon pour les contrôleurs sans fil Cisco Catalyst 9800-L du document Mise à niveau des périphériques matériels programmables sur site pour les contrôleurs sans fil Cisco Catalyst 9800.

- Si ce message d'erreur s'affiche après un redémarrage ou une panne du système, il est recommandé de régénérer le certificat trustpoint :

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilisez ces commandes dans l'ordre spécifié afin de générer un nouveau certificat de point de confiance auto-signé :

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

- Vérifiez que votre adresse MAC de mobilité est définie avec la wireless mobility mac-address erasecat4000_flash:.
- Ces protocoles sont désormais pris en charge par le port de service de la version 17.9 :
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Infrastructure Cisco Prime
  - Telnet
  - Interface graphique du contrôleur
  - DNS
  - Transfert de fichiers

    - RNB
    - HTTP
    - HTTPS
    - LDAP
    - Licence pour la fonction Smart Licensing pour communiquer avec CSSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (y compris CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- L'image AP pour 17.9 est plus grande que la mémoire flash AP autorisée à l'origine. Si vous voyez l'AP se plaindre de ne pas avoir assez d'espace lors du téléchargement de l'image 17.9, c'est probablement parce que vous n'avez pas respecté le chemin de mise à niveau par 17.3.5 comme indiqué dans les notes de publication, ou que votre AP exécute une image AireOS plus ancienne. Soit en passant par un WLC 17.3.5 et ultérieur ou en mettant à niveau l'image AireOS vers la dernière redimensionne la mémoire flash AP afin de permettre de télécharger l'image 17.9.

Déclasser

Les rétrogradations ne sont pas officiellement prises en charge et la perte de configuration de nouvelles fonctionnalités peut se produire. Cependant, comme les rétrogradations peuvent se produire dans le monde réel, ce document répertorie toujours les pièges les plus courants afin d'éviter la rétrogradation. Afin de trouver les informations dont vous avez besoin, vérifiez la version à partir de laquelle vous effectuez la rétrogradation (la version avant la rétrogradation).

GIBRALTAR

Commutateurs 16.12.2

- Rien à signaler ici.

Commutateurs 16.12.3

- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.

Commutateurs 16.12.4

- Si vous rétrogradez de cette version à une version inférieure, le WLC peut se retrouver dans une boucle de démarrage si la télémétrie a été configurée en raison de l'ID de bogue Cisco CSCvt6990/ID de bogue Cisco CSCvv87417.
- Le contrôleur sans fil Cisco Catalyst 9800 peut être rechargé en cas de rétrogradation de 17.x à 16.12.4a. Afin d'éviter cela, il est recommandé de passer à Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.

Amsterdam

Commutateurs 17.1.1

- Si vous rétrogradez de cette version à une version inférieure, le WLC peut se retrouver dans une boucle de démarrage si la télémétrie a été configurée en raison de l'ID de bogue Cisco CSCvt6990/CSCv8741.
- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.

Commutateurs 17.2.1

- Si vous rétrogradez de cette version à une version inférieure, le WLC peut se retrouver dans une boucle de démarrage si la télémétrie a été configurée en raison de l'ID de bogue Cisco CSCvt6990/ID de bogue Cisco CSCvv87417.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.3.1 vers une version antérieure, les canaux de port configurés avec une plage supérieure à quatre disparaissent.
- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.

Commutateurs 17.3.1

- Si vous rétrogradez de cette version à une version inférieure, le WLC peut se retrouver dans une boucle de démarrage si la télémétrie a été configurée en raison de l'ID de bogue Cisco CSCvt69990

  /CSCvv8741.

- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.3.1 vers une version antérieure, les

canaux de port configurés avec une plage supérieure disparaissent.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.3.1 vers une version antérieure, vous pouvez à nouveau faire face à l'assistant du jour 0 si vous avez configuré la commande « wireless country » car elle n'existait pas avant 17.3.
- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.
- Il n'est pas possible d'arrêter le profil de stratégie WLAN lorsque vous effectuez une mise à niveau de Cisco IOS XE Amsterdam 17.3.x (prenant en charge la commutation locale IPv6 AVC) vers Cisco IOS XE Gibraltar 16.12.x (où la commutation locale IPv6 AVC n'est pas prise en charge). Dans ce cas, il est recommandé de supprimer le profil de stratégie WLAN existant et d'en créer un nouveau.

Commutateurs 17.3.2

- Si vous rétrogradez de cette version à une version inférieure, le WLC se retrouve dans une boucle de démarrage si la télémétrie a été configurée en raison de l'ID de bogue Cisco CSCvt6990/ID de bogue Cisco CSCvv87417.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.3.1 vers une version antérieure, les canaux de port configurés avec une plage supérieure disparaissent.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.3.1 vers une version antérieure, vous pouvez à nouveau faire face à l'assistant du jour 0 si vous avez configuré la commande « wireless country » car elle n'existait pas avant 17.3.
- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.
- Il n'est pas possible d'arrêter le profil de stratégie WLAN lorsque vous effectuez une mise à niveau de Cisco IOS XE Amsterdam 17.3.x (prenant en charge la commutation locale IPv6 AVC) vers Cisco IOS XE Gibraltar 16.12.x (où la commutation locale IPv6 AVC n'est pas prise en charge). Dans ce cas, il est recommandé de supprimer le profil de stratégie WLAN existant et d'en créer un nouveau.

Commutateurs 17.3.3

- Si vous rétrogradez de cette version à une version inférieure, le WLC peut se retrouver dans une boucle de démarrage si la télémétrie a été configurée en raison de l'ID de bogue Cisco CSCvt6990/ID de bogue Cisco CSCvv87417.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.3.1 vers une version antérieure, les canaux de port configurés avec une plage supérieure disparaissent.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.3.1 vers une version antérieure, vous pouvez à nouveau faire face à l'assistant du jour 0 si vous avez configuré la commande « wireless country » car elle n'existait pas avant 17.3.
- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.
- Il n'est pas possible d'arrêter le profil de stratégie WLAN lorsque vous effectuez une mise à

niveau de Cisco IOS XE Amsterdam 17.3.x (prenant en charge la commutation locale IPv6 AVC) vers Cisco IOS XE Gibraltar 16.12.x (où la commutation locale IPv6 AVC n'est pas prise en charge). Dans ce cas, il est recommandé de supprimer le profil de stratégie WLAN existant et d'en créer un nouveau.

Commutateurs 17.4.1

- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.4.1 vers une version antérieure à 17.3, vous pouvez à nouveau faire face à l'assistant du jour 0 si vous avez configuré la commande « wireless country » car elle n'existait pas avant 17.3.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.4.1 vers une version antérieure, vous perdez la connexion de télémétrie car 17.4 utilise des destinations de télémétrie nommées qui n'étaient pas prises en charge dans les versions antérieures. Vous devez recréer la connexion de télémétrie.
- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.

Commutateurs 17.5.1

- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.4.1 vers une version antérieure à 17.3, vous pouvez à nouveau faire face à l'assistant du jour 0 si vous avez configuré la commande « wireless country » car elle n'existait pas avant 17.3.
- Si vous rétrogradez de Cisco IOS XE Amsterdam 17.4.1 vers une version antérieure, vous perdez la connexion de télémétrie car 17.4 utilise des destinations de télémétrie nommées qui n'étaient pas prises en charge dans les versions antérieures. Vous devez recréer la connexion de télémétrie.
- Un rechargement continu est observé lorsque le contrôleur sans fil Cisco Catalyst 9800 est rétrogradé de 17.x à 16.12.4a. Il est recommandé de procéder à une mise à niveau vers Cisco IOS XE Gibraltar 16.12.5 au lieu de 16.12.4a.

17.9.x.

- Les mots de passe 802.1x ne sont pas visibles en texte clair dans cette version, car ils sont chiffrés. Si vous rétrogradez vers une image antérieure qui ne prend pas en charge un mot de passe chiffré, les AP sont bloqués et échouent à plusieurs reprises l'authentification dot1x en raison d'informations d'identification erronées. Vous devez désactiver 802.1x sur le port du commutateur AP afin de permettre au point d'accès de joindre le contrôleur avant de définir le mot de passe en texte clair.

Commutateurs 17.10.1

- Vous ne pouvez pas voir les mots de passe 802.1x en texte clair dans cette version, car ils sont chiffrés. Si vous rétrogradez vers une image antérieure qui ne prend pas en charge un mot de passe chiffré, les AP sont bloqués et échouent à plusieurs reprises l'authentification dot1x en raison d'informations d'identification erronées. Vous devez désactiver 802.1x sur le

port du commutateur AP afin de permettre au point d'accès de joindre le contrôleur avant de définir le mot de passe en texte clair.

Commutateurs 17.11.1

- Vous ne pouvez pas voir les mots de passe 802.1x en texte clair dans cette version, car ils sont chiffrés. Si vous rétrogradez vers une image antérieure qui ne prend pas en charge un mot de passe chiffré, les AP sont bloqués et échouent à plusieurs reprises l'authentification dot1x en raison d'informations d'identification erronées. Vous devez désactiver 802.1x sur le port du commutateur AP afin de permettre au point d'accès de joindre le contrôleur avant de définir le mot de passe en texte clair.

17.12.x

- Vous ne pouvez pas voir les mots de passe 802.1x en texte clair dans cette version, car ils sont chiffrés. Si vous rétrogradez vers une image antérieure qui ne prend pas en charge un mot de passe chiffré, les AP sont bloqués et échouent à plusieurs reprises l'authentification dot1x en raison d'informations d'identification erronées. Vous devez désactiver 802.1x sur le port du commutateur AP afin de permettre au point d'accès de joindre le contrôleur avant de définir le mot de passe en texte clair.

Informations connexes

- 17.1 correctif à chaud et guide de mise à niveau des points d'accès
- 17.3 correctifs à chaud et guide de mise à niveau ISSU.
- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.