Atualização e rebaixamento dos controladores Catalyst 9800 : Dicas e truques

Contents

Referências

Introduction

Este documento descreve as coisas que devem ser observadas ao atualizar ou rebaixar um Catalyst 9800 Wireless LAN Controller (WLC) através de várias versões do Cisco IOS XE.

Antes de continuar

Este documento não tem como objetivo substituir as notas de versão que devem sempre ser o documento de entrada ao atualizar. O objetivo é facilitar a atualização através de várias versões, destacando as mudanças mais impactantes entre as versões.

Este documento não substitui a leitura das notas da versão do software de destino. Faça backup da sua configuração e tome todas as precauções necessárias antes de continuar com uma atualização.

Por padrão, o servidor http do 9800 não é mapeado estaticamente para um certificado/ponto de confiança específico que pode levar a alterações após a atualização. Defina o servidor HTTP como um ponto de confiança estático (de preferência, para um certificado emitido para o fim, ou para o certificado MIC de outra forma) na configuração antes de atualizar.

O caso especial das versões especiais de engenharia

Os edifícios especiais de engenharia não suportam a atualização do ISSU deles. Este documento concentra-se apenas em versões públicas publicadas em cisco.com, portanto, se você estiver em um build especial de engenharia, consulte as notas de versão que você recebeu juntamente com elas para receber suporte para todas as suas perguntas de atualização.

Atualização

Você pode ler diretamente as anotações sob a versão de software de destino desejada. As dicas aplicáveis através de várias versões são repetidas sempre para sua conveniência. Não faça upgrade por meio de mais de 3 versões de uma só vez. Por exemplo, a atualização de 16.12.1 para 17.3.2 é abordada neste documento, mas não é feita de atualizações de 16.12 para 17.4. Nesse cenário, passe pela seção 17.3 e verifique as notas na seção 17.3, faça a atualização, examine a seção 17.4 e prepare a segunda atualização. Como conclusão, as dicas listadas não são mais repetidas após 3 versões principais, mesmo que ainda válidas, como o documento pressupõe, você passa por versões principais intermediárias.

Gibraltar

16.12.2

- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s, e se sua rede sem fio usar a etiqueta de política padrão, ela será desativada devido à alteração de mapeamento

padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.

16.12.3

- 16.12.3 é a primeira versão que reforça o suporte somente dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados através da interface de usuário da Web.
- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s, e se sua rede sem fio usar a etiqueta de política padrão, ela será desativada devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.

16.12.4

- 16.12.3 e 17.2.1 são as primeiras versões para reforçar o suporte apenas dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados através da interface de usuário da Web.
- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s, e se sua rede sem fio usar a etiqueta de política padrão, ela será desativada devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.

16.12.5

- Igual a 16.12.4

Amsterdã

17.1.1

- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de

transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados através da interface de usuário da Web.
- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s e se sua rede sem fio usar a etiqueta de política padrão, ela ficará inativa devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.
- A partir dessa versão, uma nova verificação de acessibilidade do gateway é apresentada. Os APs enviam solicitações de eco ICMP (ping) periódicas ao gateway padrão para verificar a conectividade. Você precisa garantir que a filtragem de tráfego entre os APs e o gateway padrão (como ACLs) permita pings ICMP entre o AP e o gateway padrão. Se esses pings forem bloqueados, mesmo que a conectividade entre o controlador e o AP esteja ativa, os APs serão recarregados com um intervalo de 4 horas.

17.2.1

- 16.12.3 e 17.2.1 são as primeiras versões para reforçar o suporte apenas dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados através da interface de usuário da Web.
- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s, e se sua rede sem fio usar a marca de política padrão, ela poderá ficar inativa devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.
- A partir da 17.1, uma nova verificação de acessibilidade do gateway é apresentada. Os APs enviam solicitações de eco ICMP (ping) periódicas ao gateway padrão para verificar a conectividade. Você precisa garantir que a filtragem de tráfego entre os APs e o gateway padrão (como ACLs) permita pings ICMP entre o AP e o gateway padrão. Se esses pings forem bloqueados, mesmo se a conectividade entre o controlador e o AP estiver ativa, os APs serão recarregados com um intervalo de 4 horas.

17.3.1

- 16.12.3 e 17.2.1 são as primeiras versões para reforçar o suporte apenas dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados

através da interface de usuário da Web.

- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s e se sua rede sem fio usar a etiqueta de política padrão, ela ficará inativa devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.
- A partir da 17.1, uma nova verificação de acessibilidade do gateway é apresentada. Os APs enviam solicitações de eco ICMP (ping) periódicas ao gateway padrão para verificar a conectividade. Você precisa garantir que a filtragem de tráfego entre os APs e o gateway padrão (como ACLs) permita pings ICMP entre o AP e o gateway padrão. Se esses pings forem bloqueados, mesmo que a conectividade entre o controlador e o AP esteja ativa, os APs serão recarregados com um intervalo de 4 horas.
- Se você configurou o modo FIPS, certifique-se de remover a **configuração de segurança wpa wpa1 cipher tkip** de qualquer WLAN antes de atualizar o Cisco IOS XE Amsterdam 17.3.x de uma versão anterior. Se isso não for feito, a segurança da WLAN será definida como TKIP, que não é suportado no modo FIPS. Após a atualização, é necessário reconfigurar a WLAN com AES.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o Cisco Catalyst 9800-CL Wireless Controller requer 16 GB de espaço em disco para novas implantações.É possível aumentar o tamanho do espaço em disco somente através de uma reinstalação com uma imagem 17.3.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o nome do AP só pode ter até 32 caracteres.
- Para autenticação de endereço MAC local (de clientes ou APs), somente o formato aaaabbbccc (sem separador) é suportado a partir de 17.3.1. Isso significa que a autenticação falhará se você adicionar um endereço MAC com separadores na interface do usuário da Web ou na CLI.
- A partir dessa versão, os APs serão recarregados após 4 horas se não puderem se unir a uma WLC, não poderão fazer ping em seu gateway E ARP em seu gateway (Todos os 3 precisam falhar para que o AP seja reinicializado). Este é um aprimoramento (ID de bug da Cisco CSCvt89970) para a verificação anterior do gateway somente icmp das versões anteriores
- A partir da versão 17.3.1, a nova maneira de configurar o código do país para pontos de acesso é o comando "Wireless country <1 country code>", que você pode repetir várias vezes com diferentes códigos de país. Isso permite aumentar a quantidade máxima de código de país por mais de 20 anos. Os comandos "ap country" ainda estão presentes e ainda funcionarão. No entanto, considere alterá-los para os comandos "Wireless country", pois os comandos ap country serão obsoletos em uma versão futura

17.3.2

- 16.12.3 e 17.2.1 são as primeiras versões para reforçar o suporte apenas dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados

através da interface de usuário da Web.

- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s e se sua rede sem fio usar a etiqueta de política padrão, ela ficará inativa devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.
- A partir da 17.1, uma nova verificação de acessibilidade do gateway é apresentada. Os APs enviam solicitações de eco ICMP (ping) periódicas ao gateway padrão para verificar a conectividade. Você precisa garantir que a filtragem de tráfego entre os APs e o gateway padrão (como ACLs) permita pings ICMP entre o AP e o gateway padrão. Se esses pings forem bloqueados, mesmo que a conectividade entre o controlador e o AP esteja ativa, os APs serão recarregados com um intervalo de 4 horas.
- Se você configurou o modo FIPS, certifique-se de remover a **configuração de segurança wpa wpa1 cipher tkip** de qualquer WLAN antes de atualizar o Cisco IOS XE Amsterdam 17.3.x de uma versão anterior. Se isso não for feito, a segurança da WLAN será definida como TKIP, que não é suportado no modo FIPS. Após a atualização, é necessário reconfigurar a WLAN com AES.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o Cisco Catalyst 9800-CL Wireless Controller requer 16 GB de espaço em disco para novas implantações.É possível aumentar o tamanho do espaço em disco somente através de uma reinstalação com uma imagem 17.3.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o nome do AP só pode ter até 32 caracteres.
- Para autenticação de endereço MAC local (de clientes ou APs), somente o formato aaaabbbccc (sem separador) é suportado a partir de 17.3.1. Isso significa que a autenticação falhará se você adicionar um endereço MAC com separadores na interface do usuário da Web ou na CLI.
- A partir de 17.3.1, os APs serão recarregados após 4 horas se não puderem se unir a uma WLC, não poderão fazer ping no gateway E ARP no gateway (todos os 3 precisam falhar para que o AP seja reinicializado). Este é um aprimoramento (ID de bug da Cisco CSCvt89970) para a verificação anterior do gateway somente icmp das versões anteriores
- A partir da versão 17.3.1, a nova maneira de configurar o código do país para pontos de acesso é o comando "Wireless country <1 country code>", que você pode repetir várias vezes com diferentes códigos de país. Isso permite aumentar a quantidade máxima de código de país por mais de 20 anos. Os comandos "ap country" ainda estão presentes e ainda funcionarão. No entanto, considere alterá-los para os comandos "Wireless country", pois os comandos ap country serão obsoletos em uma versão futura.

17.3.3

- 16.12.3 e 17.2.1 são as primeiras versões para reforçar o suporte apenas dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados através da interface de usuário da Web.

- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s e se sua rede sem fio usar a etiqueta de política padrão, ela ficará inativa devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.
- A partir da 17.1, uma nova verificação de acessibilidade do gateway é apresentada. Os APs enviam solicitações de eco ICMP (ping) periódicas ao gateway padrão para verificar a conectividade. Você precisa garantir que a filtragem de tráfego entre os APs e o gateway padrão (como ACLs) permita pings ICMP entre o AP e o gateway padrão. Se esses pings forem bloqueados, mesmo que a conectividade entre o controlador e o AP esteja ativa, os APs serão recarregados com um intervalo de 4 horas.
- Se você configurou o modo FIPS, certifique-se de remover a **configuração de segurança wpa wpa1 cipher tkip** de qualquer WLAN antes de atualizar o Cisco IOS XE Amsterdam 17.3.x de uma versão anterior. Se isso não for feito, a segurança da WLAN será definida como TKIP, que não é suportado no modo FIPS. Após a atualização, é necessário reconfigurar a WLAN com AES.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o Cisco Catalyst 9800-CL Wireless Controller requer 16 GB de espaço em disco para novas implantações.É possível aumentar o tamanho do espaço em disco somente através de uma reinstalação com uma imagem 17.3.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o nome do AP só pode ter até 32 caracteres.
- Para autenticação de endereço MAC local (de clientes ou APs), somente o formato aaaabbbccc (sem separador) é suportado a partir de 17.3.1. Isso significa que a autenticação falhará se você adicionar um endereço MAC com separadores na interface do usuário da Web ou na CLI.
- A partir de 17.3.1, os APs serão recarregados após 4 horas se não puderem se unir a uma WLC, não poderão fazer ping no gateway E ARP no gateway (todos os 3 precisam falhar para que o AP seja reinicializado). Este é um aprimoramento (ID de bug da Cisco CSCvt89970) a verificação anterior do gateway somente icmp das versões anteriores
- A partir da versão 17.3.1, a nova maneira de configurar o código do país para pontos de acesso é o comando "Wireless country <1 country code>", que você pode repetir várias vezes com diferentes códigos de país. Isso permite aumentar a quantidade máxima de código de país por mais de 20 anos. Os comandos "ap country" ainda estão presentes e ainda funcionarão. No entanto, considere alterá-los para os comandos "Wireless country", pois os comandos ap country serão obsoletos em uma versão futura.
- A WLC pode travar se seus APs tiverem nomes de host com mais de 32 caracteres (ID de bug da Cisco CSCvy11981)

17.3.4

- 16.12.3 e 17.2.1 são as primeiras versões para reforçar o suporte apenas dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados

através da interface de usuário da Web.

- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s e se sua rede sem fio usar a etiqueta de política padrão, ela ficará inativa devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.
- A partir da 17.1, uma nova verificação de acessibilidade do gateway é apresentada. Os APs enviam solicitações de eco ICMP (ping) periódicas ao gateway padrão para verificar a conectividade. Você precisa garantir que a filtragem de tráfego entre os APs e o gateway padrão (como ACLs) permita pings ICMP entre o AP e o gateway padrão. Se esses pings forem bloqueados, mesmo que a conectividade entre o controlador e o AP esteja ativa, os APs serão recarregados com um intervalo de 4 horas.
- Se você configurou o modo FIPS, certifique-se de remover a **configuração de segurança wpa wpa1 cipher tkip** de qualquer WLAN antes de atualizar o Cisco IOS XE Amsterdam 17.3.x de uma versão anterior. Se isso não for feito, a segurança da WLAN será definida como TKIP, que não é suportado no modo FIPS. Após a atualização, é necessário reconfigurar a WLAN com AES.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o Cisco Catalyst 9800-CL Wireless Controller requer 16 GB de espaço em disco para novas implantações.É possível aumentar o tamanho do espaço em disco somente através de uma reinstalação com uma imagem 17.3.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o nome do AP só pode ter até 32 caracteres.
- Para autenticação de endereço MAC local (de clientes ou APs), somente o formato aaaabbbccc (sem separador) é suportado a partir de 17.3.1. Isso significa que a autenticação falhará se você adicionar um endereço MAC com separadores na interface do usuário da Web ou na CLI.
- A partir de 17.3.1, os APsl são recarregados após 4 horas se não puderem se unir a uma WLC, não podem fazer ping no gateway E ARP no gateway (todos os 3 precisam falhar para que o AP seja reinicializado). Este é um aprimoramento (ID de bug da Cisco CSCvt89970) para a verificação anterior do gateway somente icmp das versões anteriores
- A partir da versão 17.3.1, a nova maneira de configurar o código do país para pontos de acesso é o comando "Wireless country <1 country code>", que você pode repetir várias vezes com diferentes códigos de país. Isso permite aumentar a quantidade máxima de código de país por mais de 20 anos. Os comandos "ap country" ainda estão presentes e ainda funcionam. No entanto, considere alterá-los para os comandos "Wireless country", pois os comandos ap country estão planejados para serem obsoletos em uma versão futura.
- Ao atualizar para 17.3.4 e posterior, recomenda-se que o bootloader/rommon 16.12.5r esteja instalado nos controladores onde for aplicável (9800-80. O 9800-40 não tem um rommong 16.12.5r no momento e não precisa de uma atualização rommon).
- A atualização do controlador, do Cisco IOS XE Bengaluru 17.3.x para qualquer versão usando ISSU, pode falhar se o comando **snmp-server enable traps hsrp** estiver configurado. Certifique-se de remover o comando **snmp-server enable traps hsrp** da configuração antes de iniciar uma atualização de ISSU porque o comando **snmp-server enable traps hsrp** é removido do Cisco IOS XE Bengaluru 17.4.x.
- Ao atualizar para o Cisco IOS XE 17.3.x e versões posteriores, se o comando ip http ative-session-modules none estiver ativado, você não poderá acessar a GUI do controlador usando HTTPS. Para acessar a GUI usando HTTPS, execute estes comandos:ip http session-module-list pkilist OPENRESTY_PKIip http ative-session-modules pkilist

17.3.5

- Devido à ID de bug da Cisco CSCwb13784 , se o MTU do seu caminho for inferior a 1500 bytes, os APs talvez não consigam ingressar. Baixe o patch SMU disponível para 17.3.5 para corrigir esse problema.
- 16.12.3 e 17.2.1 são as primeiras versões para reforçar o suporte apenas dos SFPs listados como suportados na documentação. Os SFPs não listados causam uma situação de inatividade de porta. Verifique a lista de SFP suportados e certifique-se de que os SFPs são compatíveis para evitar que as portas de dados fiquem inoperantes após a atualização
- O arquivo de atualização para esta versão pode ser muito grande para upload HTTP (ao fazer upgrade de IU da Web) se você estiver na versão 16.12.1. Use outro método de transferência ou passe por 16.12.2, que suporta arquivos maiores a serem carregados através da interface de usuário da Web.
- A partir do Cisco IOS XE Gibraltar 16.12.2s, o mapeamento automático da WLAN para o perfil de política padrão sob a marca de política padrão foi removido. Se você estiver atualizando de uma versão anterior à do Cisco IOS XE Gibraltar 16.12.2s e se sua rede sem fio usar a etiqueta de política padrão, ela ficará inativa devido à alteração de mapeamento padrão. Para restaurar a operação da rede, adicione a WLAN necessária aos mapeamentos de política sob a marca de política padrão.
- A partir da 17.1, uma nova verificação de acessibilidade do gateway é apresentada. Os APs enviam solicitações de eco ICMP (ping) periódicas ao gateway padrão para verificar a conectividade. Você precisa garantir que a filtragem de tráfego entre os APs e o gateway padrão (como ACLs) permita pings ICMP entre o AP e o gateway padrão. Se esses pings forem bloqueados, mesmo que a conectividade entre o controlador e o AP esteja ativa, os APs serão recarregados com um intervalo de 4 horas.
- Se você configurou o modo FIPS, certifique-se de remover a **configuração de segurança wpa wpa1 cipher tkip** de qualquer WLAN antes de atualizar o Cisco IOS XE Amsterdam 17.3.x de uma versão anterior. Se isso não for feito, a segurança da WLAN será definida como TKIP, que não é suportado no modo FIPS. Após a atualização, é necessário reconfigurar a WLAN com AES.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o Cisco Catalyst 9800-CL Wireless Controller requer 16 GB de espaço em disco para novas implantações.É possível aumentar o tamanho do espaço em disco somente através de uma reinstalação com uma imagem 17.3.
- A partir do Cisco IOS XE Amsterdam 17.3.1, o nome do AP só pode ter até 32 caracteres.
- Para autenticação de endereço MAC local (de clientes ou APs), somente o formato aaaabbbccc (sem separador) é suportado a partir de 17.3.1. Isso significa que a autenticação falhará se você adicionar um endereço MAC com separadores na interface do usuário da Web ou na CLI.
- A partir de 17.3.1, os APsl são recarregados após 4 horas se não puderem se unir a uma WLC, não podem fazer ping no gateway E ARP no gateway (todos os 3 precisam falhar para que o AP seja reinicializado). Este é um aprimoramento (ID de bug da Cisco CSCvt89970) para a verificação anterior do gateway somente icmp das versões anteriores
- A partir da versão 17.3.1, a nova maneira de configurar o código do país para pontos de acesso é o comando "Wireless country <1 country code>", que você pode repetir várias vezes com diferentes códigos de país. Isso permite aumentar a quantidade máxima de código de país por mais de 20 anos. Os comandos "ap country" ainda estão presentes e ainda funcionam. No entanto, considere alterá-los para os comandos "Wireless country", pois os

comandos ap country estão planejados para serem obsoletos em uma versão futura.
- Ao atualizar para 17.3.4 e posterior, recomenda-se que o bootloader/rommon 16.12.5r esteja instalado nos controladores onde for aplicável (9800-80. O 9800-40 não tem um rommong 16.12.5r no momento e não precisa de uma atualização rommon).
- A atualização do controlador, do Cisco IOS XE Bengaluru 17.3.x para qualquer versão usando ISSU, pode falhar se o comando **snmp-server enable traps hsrp** estiver configurado. Certifique-se de remover o comando **snmp-server enable traps hsrp** da configuração antes de iniciar uma atualização de ISSU porque o comando **snmp-server enable traps hsrp** é removido do Cisco IOS XE Bengaluru 17.4.x.
- Ao atualizar para o Cisco IOS XE 17.3.x e versões posteriores, se o comando ip http ative-session-modules none estiver ativado, você não poderá acessar a GUI do controlador usando HTTPS. Para acessar a GUI usando HTTPS, execute estes comandos:ip http session-module-list pkilist OPENRESTY_PKIip http ative-session-modules pkilist

Bengaluru

17.4.1

- A partir de 17.4.1, os APs baseados no Cisco IOS Wave 1 não são mais suportados (1700.2700.3700.1570), com exceção do IW3700.
- Suas WLANs podem ser desligadas após a atualização se forem SSIDs não-WPA (convidado, aberto ou CWA) e tiverem FT adaptável configurada. A solução é remover a configuração de FT adaptável antes da atualização (ID de bug da Cisco CSCvx34349). A configuração de FT adaptável não faz sentido em SSID não-WPA, portanto, não há perda de nada removendo-o.
- A WLC pode travar se seus APs tiverem nomes de host com mais de 32 caracteres (ID de bug da Cisco CSCvy11981)

17.5.1

- A partir de 17.4.1, os APs baseados no Cisco IOS Wave 1 não são mais suportados (1700.2700.3700.1570), com exceção do IW3700.
- A partir do Cisco IOS XE Bengaluru Versão 17.4.1, a solução de telemetria fornece um nome para o endereço do receptor em vez do endereço IP para os dados de telemetria. Esta é uma opção adicional. Durante o downgrade da controladora e a atualização subsequente, é provável que haja um problema - a versão de upgrade usa os receptores recém-nomeados, que não são reconhecidos no downgrade. A nova configuração é rejeitada e falha na atualização subsequente. A perda de configuração pode ser evitada quando a atualização ou o rebaixamento é realizado a partir do Cisco DNA Center.
- Suas WLANs podem ser desligadas após a atualização se forem SSIDs não-WPA (convidado, aberto ou CWA) e tiverem FT adaptável configurada. A solução é remover a configuração de FT adaptável antes da atualização (ID de bug da Cisco CSCvx34349). A configuração de FT adaptável não faz sentido em SSID não-WPA, portanto, não há perda de nada removendo-o.
- A WLC pode travar se seus APs tiverem nomes de host com mais de 32 caracteres (ID de bug da Cisco CSCvy11981)
- Ao atualizar a GUI de uma versão para outra, recomendamos que você limpe o cache do

navegador para que todas as páginas da GUI sejam recarregadas corretamente.
- Ao atualizar para o Cisco IOS XE 17.3.x e versões posteriores, se o comando ip http ative-session-modules none estiver ativado, você não poderá acessar a GUI usando HTTPS. Para acessar a GUI usando HTTPS, execute estes comandos:ip http session-module-list pkilist OPENRESTY_PKIip http ative-session-modules pkilist
- Se você encontrar o erro ERR_SSL_VERSION_OR_CIPHER_MISMATCH na GUI após uma reinicialização ou travamento do sistema, recomendamos que você regenere o certificado do ponto de confiança.O procedimento para gerar um novo ponto confiável autoassinado é o seguinte:
```
configure terminal no crypto pki trustpoint
```

17.6.1

- A partir de 17.4.1, os APs baseados no Cisco IOS Wave 1 não são mais suportados (1700.2700.3700.1570), com exceção do IW3700.
- A partir do Cisco IOS XE Bengaluru Versão 17.4.1, a solução de telemetria fornece um nome para o endereço do receptor em vez do endereço IP para os dados de telemetria. Esta é uma opção adicional. Durante o downgrade da controladora e a atualização subsequente, é provável que haja um problema - a versão de upgrade usa os receptores recém-nomeados, que não são reconhecidos no downgrade. A nova configuração é rejeitada e falha na atualização subsequente. A perda de configuração pode ser evitada quando a atualização ou o rebaixamento é realizado a partir do Cisco DNA Center.
- Suas WLANs podem ser desligadas após a atualização se forem SSIDs não-WPA (convidado, aberto ou CWA) e tiverem FT adaptável configurada. A solução é remover a configuração de FT adaptável antes da atualização (ID de bug da Cisco CSCvx34349). A configuração de FT adaptável não faz sentido em SSID não-WPA, portanto, não há perda de nada removendo-o.
- Ao atualizar a GUI de uma versão para outra, recomendamos que você limpe o cache do navegador para que todas as páginas da GUI sejam recarregadas corretamente.
- Um AP que ingressou em uma WLC 17.6.1 ou posterior não pode mais ingressar em uma WLC AireOS a menos que ela execute o código 8.10.162 ou posterior, ou 8.5.176.2 ou posterior ao código 8.5.
- Ao atualizar para 17.6,1 e posterior, é aconselhável ter o bootloader 16.12.5r/rommon instalado nos controladores onde for aplicável (9800-80. O 9800-40 não tem um rommong 16.12.5r no momento e não precisa de uma atualização rommon).
- A atualização do controlador, do Cisco IOS XE Bengaluru 17.3.x para qualquer versão usando ISSU, pode falhar se o comando **snmp-server enable traps hsrp** estiver configurado. Certifique-se de remover o comando **snmp-server enable traps hsrp** da configuração antes de iniciar uma atualização de ISSU porque o comando **snmp-server enable traps hsrp** é removido do Cisco IOS XE Bengaluru 17.4.x.
- Durante a atualização para o Cisco IOS XE 17.3.x e versões posteriores, se o comando ip http ative-session-modules none estiver ativado, o acesso HTTPS à GUI do controlador não funcionará. Para acessar a GUI usando HTTPS, execute estes comandos:ip http session-module-list pkilist OPENRESTY_PKIip http ative-session-modules pkilist
- Se você encontrar o erro ERR_SSL_VERSION_OR_CIPHER_MISMATCH na GUI após uma reinicialização ou travamento do sistema, recomendamos que você regenere o certificado do ponto de confiança.O procedimento para gerar um novo ponto confiável autoassinado é o seguinte:

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

17.6.2

- A partir de 17.4.1, os APs baseados no Cisco IOS Wave 1 não são mais suportados (1700.2700.3700.1570), com exceção do IW3700.
- A partir do Cisco IOS XE Bengaluru Versão 17.4.1, a solução de telemetria fornece um nome para o endereço do receptor em vez do endereço IP para os dados de telemetria. Esta é uma opção adicional. Durante o downgrade da controladora e a atualização subsequente, é provável que haja um problema - a versão de upgrade usa os receptores recém-nomeados, que não são reconhecidos no downgrade. A nova configuração é rejeitada e falha na atualização subsequente. A perda de configuração pode ser evitada quando a atualização ou o rebaixamento é realizado a partir do Cisco DNA Center.
- Suas WLANs podem ser desligadas após a atualização se forem SSIDs não-WPA (convidado, aberto ou CWA) e tiverem FT adaptável configurada. A solução é remover a configuração de FT adaptável antes da atualização (ID de bug da Cisco CSCvx34349) A configuração de FT adaptável não faz sentido em SSID não-WPA, portanto, não há perda de nada removendo-o.
- Ao atualizar a GUI de uma versão para outra, recomendamos que você limpe o cache do navegador para que todas as páginas da GUI sejam recarregadas corretamente.
- Um AP que ingressou em uma WLC 17.6.1 ou posterior não pode mais ingressar em uma WLC AireOS a menos que ela execute o código 8.10.162 ou posterior, ou 8.5.176.2 ou posterior ao código 8.5.
- Ao atualizar para 17.6,1 e posterior, é aconselhável ter o bootloader 16.12.5r/rommon instalado nos controladores onde for aplicável (o 9800-80. O 9800-40 não tem um rommong 16.12.5r no momento e não precisa de uma atualização rommon).
- A atualização do controlador, do Cisco IOS XE Bengaluru 17.3.x para qualquer versão usando ISSU, pode falhar se o comando **snmp-server enable traps hsrp** estiver configurado. Certifique-se de remover o comando **snmp-server enable traps hsrp** da configuração antes de iniciar uma atualização de ISSU porque o comando **snmp-server enable traps hsrp** é removido do Cisco IOS XE Bengaluru 17.4.x.
- Durante a atualização para o Cisco IOS XE 17.3.x e versões posteriores, se o comando ip http ative-session-modules none estiver ativado, o acesso GUI do controlador HTTPS não funcionará. Para acessar a GUI usando HTTPS, execute estes comandos:ip http session-module-list pkilist OPENRESTY_PKIip http ative-session-modules pkilist
- Não use mais de 31 caracteres para nomes de AP. Se o nome do AP tiver 32 caracteres ou mais, pode ocorrer um travamento do controlador.
- Se você encontrar o erro ERR_SSL_VERSION_OR_CIPHER_MISMATCH na GUI após uma reinicialização ou travamento do sistema, recomendamos que você regenere o certificado do ponto de confiança.O procedimento para gerar um novo ponto confiável autoassinado é o seguinte:
```
configure terminal no crypto pki trustpoint
```

Cupertino

Esta seção pressupõe que você esteja iniciando em 17.6.1 ou posterior e atualizando para uma versão Cupertino. Se estiver atualizando diretamente de uma versão anterior (que pode ser suportada, verifique as notas de versão para ter certeza), leia as advertências da seção 17.3 e

17.6.

17.7.1

- Não use mais de 31 caracteres para nomes de AP. Se o nome do AP tiver 32 caracteres ou mais, pode ocorrer um travamento do controlador.
- 17.7.1 exige que o código de país do AP seja configurado nos perfis de união do AP.
- Devido à ID de bug da Cisco CSCvu22886 , se você tiver 9130 ou 9124 APs, precisará passar por 17.3.5a ao atualizar para 17.7.1 ou posterior de uma versão anterior a 17.3.4

17.8.1

- Não use mais de 31 caracteres para nomes de AP. Se o nome do AP tiver 32 caracteres ou mais, pode ocorrer um travamento do controlador.
- 17.7.1 exige que o código de país do AP seja configurado nos perfis de união do AP.
- Devido à ID de bug da Cisco CSCvu22886 , se você tiver 9130 ou 9124 APs, precisará passar por 17.3.5a ao atualizar para 17.7.1 ou posterior de uma versão anterior a 17.3.4

Desatualizar

Não há suporte oficial para downgrades e pode ocorrer perda de configuração de novos recursos. No entanto, à medida que podem ocorrer downgrades no mundo real, este documento ainda lista as armadilhas mais comuns a serem evitadas ao fazer o downgrade. Para encontrar as informações necessárias, verifique a versão da qual você está fazendo o downgrade (a versão anterior ao downgrade)

Gibraltar

16.12.2

- Nada a apontar aqui.

16.12.3

- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.

16.12.4

- Se você fizer o downgrade dessa versão para uma versão inferior, a WLC poderá terminar em um loop de inicialização se a telemetria tiver sido configurada devido ao bug da Cisco ID CSCvt69990 / ID de bug da Cisco CSCvv87417
- O Cisco Catalyst 9800 Wireless Controller pode ser recarregado se baixado de 17.x para 16.12.4a. Para evitar isso, recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a

Amsterdã

17.1.1

- Se você fizer o downgrade dessa versão para uma versão inferior, a WLC poderá terminar em um loop de inicialização se a telemetria tiver sido configurada devido ao bug da Cisco ID CSCvt69990 / CSCvv8741
- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.

17.2.1

- Se você fizer o downgrade dessa versão para uma versão inferior, a WLC poderá terminar em um loop de inicialização se a telemetria tiver sido configurada devido ao bug da Cisco ID CSCvt69990 / ID de bug da Cisco CSCvv87417
- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.3.1 para uma versão anterior, os canais de porta configurados com intervalo superior a 4 desaparecerão
- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.

17.3.1

- Se você fizer o downgrade dessa versão para uma versão inferior, a WLC poderá terminar em um loop de inicialização se a telemetria tiver sido configurada devido ao bug da Cisco ID CSCvt69990 / CSCvv8741
- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.3.1 para uma versão anterior, os canais de porta configurados com intervalo mais alto desaparecerão
- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.3.1 para uma versão anterior, poderá enfrentar o assistente de dia 0 novamente se tiver o comando "país sem fio" configurado, pois ele não existia antes de 17.3
- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.
- Não é possível desligar o perfil da política de WLAN quando você faz o downgrade do Cisco IOS XE Amsterdam 17.3.x (suportando o IPv6 AVC de switching local) para o Cisco IOS XE Gibraltar 16.12.x (onde o IPv6 AVC de switching local não é suportado). Nesses casos, recomendamos que você exclua o perfil de política de WLAN existente e crie um novo.

17.3.2

- Se você fizer o downgrade dessa versão para uma versão inferior, a WLC terminará em um loop de inicialização se a telemetria tiver sido configurada devido ao bug da Cisco ID CSCvt69990 / ID de bug da Cisco CSCvv87417
- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.3.1 para uma versão anterior, os canais de porta configurados com intervalo mais alto desaparecerão

- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.3.1 para uma versão anterior, poderá enfrentar o assistente de dia 0 novamente se tiver o comando "país sem fio" configurado, pois ele não existia antes de 17.3
- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.
- Não é possível desligar o perfil da política de WLAN quando você faz o downgrade do Cisco IOS XE Amsterdam 17.3.x (suportando o IPv6 AVC de switching local) para o Cisco IOS XE Gibraltar 16.12.x (onde o IPv6 AVC de switching local não é suportado). Nesses casos, recomendamos que você exclua o perfil de política de WLAN existente e crie um novo.

17.3.3

- Se você fizer o downgrade dessa versão para uma versão inferior, a WLC poderá terminar em um loop de inicialização se a telemetria tiver sido configurada devido ao bug da Cisco ID CSCvt69990 / ID de bug da Cisco CSCvv87417
- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.3.1 para uma versão anterior, os canais de porta configurados com intervalo mais alto desaparecerão
- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.3.1 para uma versão anterior, poderá enfrentar o assistente de dia 0 novamente se tiver o comando "país sem fio" configurado, pois ele não existia antes de 17.3
- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.
- Não é possível desligar o perfil da política de WLAN quando você faz o downgrade do Cisco IOS XE Amsterdam 17.3.x (suportando o IPv6 AVC de switching local) para o Cisco IOS XE Gibraltar 16.12.x (onde o IPv6 AVC de switching local não é suportado). Nesses casos, recomendamos que você exclua o perfil de política de WLAN existente e crie um novo.

17.4.1

- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.4.1 para uma versão anterior antes de 17.3, poderá enfrentar o assistente de dia 0 novamente se tiver configurado o comando "país sem fio", pois ele não existia antes de 17.3
- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.4.1 para uma versão anterior, você perderá a conexão de telemetria, pois 17.4 usa o destino de telemetria nomeado, que não eram comandos suportados em versões anteriores. Você precisa recriar a conexão de telemetria.
- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.

17.5.1

- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.4.1 para uma versão anterior antes de 17.3, poderá enfrentar o assistente de dia 0 novamente se tiver configurado o comando "país sem fio", pois ele não existia antes de 17.3

- Se você fizer o downgrade do Cisco IOS XE Amsterdam 17.4.1 para uma versão anterior, você perderá a conexão de telemetria, pois 17.4 usa o destino de telemetria nomeado, que não eram comandos suportados em versões anteriores. Você precisa recriar a conexão de telemetria.
- A recarga contínua é observada quando o Cisco Catalyst 9800 Wireless Controller é baixado de 17.x para 16.12.4a. Recomendamos que você faça o downgrade para o Cisco IOS XE Gibraltar 16.12.5 em vez de 16.12.4a.

Referências

17.1 aplicação de patches a quente e guia de atualização do AP em execução

17.3 aplicação de hot patching e guia de atualização de ISSU.