Validation et récupération des points d'accès Catalyst sur 17.12 affectés par une défaillance de mise à niveau

Table des matières

- Introduction
- Assistance interactive
- Contexte
- Détails de la cause première
- Codes et points d'accès affectés
  - Points d'accès affectés
  - Codes affectés
- Codes fixes
- Chemin de mise à niveau et applicabilité des bogues
  - Bogue non applicable et chemin de mise à niveau
  - Bogue applicable et chemin de mise à niveau
- Prévérifications de mise à niveau
  - Prévérification manuelle
  - Prévérification Automatisée
  - Prévérifie les résultats
- Récupération
  - Faible espace disponible dans la partition 2
    - Supprimer les fichiers principaux des points d'accès
    - Réinitialisation en usine des points d'accès
    - Supprimer le fichier cnssdaemon.log (Access Point devshell)
    - Échange de partition de démarrage d'image du point d'accès
  - Bootloop du point d'accès
- Quand ouvrir un dossier TAC
- FAQ

Introduction

Ce document décrit la procédure de validation et de récupération lorsque les points d'accès sont affectés par l'ID de bogue Cisco CSCwf25731 et CSCwf37271.

Assistance interactive

Si vous vous connectez avec vos informations d'identification CCO, Cisco AI Assistant for Support peut vous aider à déterminer de manière interactive si ce bogue est applicable à votre réseau et, le cas échéant, à déterminer les options de récupération. Pour commencer :

1. Cliquez sur l'icône Cisco AI Assistant for Support située dans le coin inférieur droit du document.
   - 

2. Connectez-vous à l'aide de vos identifiants Cisco.
3. Une fois connecté, actualisez l'onglet/le document de votre navigateur.
4. Cliquez sur l'icône de démarrage située dans le coin inférieur droit pour commencer à poser des questions sur ce document.
   - 

Pour obtenir les meilleurs résultats, commencez par des questions simples et augmentez progressivement la complexité. Si une réponse n'est pas satisfaisante, veuillez cliquer sur l'icône du pouce vers le bas pour nous faire part de vos commentaires. Vous pouvez toujours vous reporter à ce document si les réponses de Cisco AI Assistant for Support ne sont pas claires.

Contexte

Les mises à niveau ou les PASP appliquées aux systèmes qui exécutent actuellement 17.12.4/5/6/6a ou qui exécutaient précédemment ces versions pendant une période de temps considérable peuvent entraîner l'entrée en boucle de démarrage des modèles de points d'accès affectés (veuillez vérifier la liste des points d'accès affectés ci-dessous) dans certaines conditions, déclenchées par un échec d'installation de l'image en raison d'un espace disque insuffisant sur le stockage du point d'accès. Bien que cela n'affecte pas les opérations quotidiennes ou les SMU, il s'agit d'un risque critique lors des mises à niveau ISSU, des mises à niveau complètes du code du contrôleur ou des installations APSP, car ces procédures impliquent des mises à niveau d'image des points d'accès.

Il est nécessaire de suivre un processus supplémentaire qui nécessite des étapes obligatoires de vérification préalable de la mise à niveau mentionnées dans ce document, car il n'existe aucune solution de contournement de la configuration.

Pour résoudre ce problème, vous devez installer le correctif de version APSP spécifique (indiqué dans le tableau Codes fixes ci-dessous) dans le WLC avant que les points d'accès ne tentent de mettre à niveau, ou utiliser le correctif APSP de nettoyage (disponible pour 17.15.4d et 17.18.2) si

vous avez déjà déplacé vers une version ultérieure mais exécuté l'une des versions affectées. Même si vous n'êtes pas sûr de l'historique de votre système, il est fortement recommandé d'effectuer des vérifications de stockage avant toute mise à niveau ou installation d'APSP si les versions concernées ont déjà été présentes dans votre environnement.

Détails de la cause première

Les points d'accès exécutant les versions 17.12.4 à 17.12.6a sont affectés par un bogue de bibliothèque qui génère un fichier journal persistant : /storage/cnssdaemon.log. Ce fichier augmente de 5 Mo par jour et n'est pas effacé par les redémarrages, ce qui finit par épuiser l'espace de stockage du périphérique. Par conséquent, si le point d'accès s'exécute à partir de la partition de démarrage 1 (Partie 1) et que la partition de démarrage 2 (Partie 2) est saturée en raison du fichier journal, le processus de mise à niveau échoue car il ne peut pas stocker la nouvelle image dans la partition de démarrage 2, ce qui peut entraîner une boucle de démarrage. Pour éviter cela, vous devez effacer le stockage ou vous assurer que le point d'accès a démarré à partir de la partition 2 avant de tenter d'autres mises à niveau en exécutant les instructions de ce document.

Codes et points d'accès affectés

Points d'accès affectés

Les modèles de points d'accès suivants sont les seuls susceptibles de rencontrer ce problème. Si votre réseau n'utilise aucun de ces modèles spécifiques, votre environnement n'est pas affecté et aucune action supplémentaire n'est requise.

- Catalyst 9124 (I/D/E)
- Catalyst 9130 (E/S)
- Catalyst 9136I
- Catalyst 9162I
- Catalyst 9163E
- Catalyst 9164I
- Catalyst 9166 (I/D1)
- Catalyst IW9167 (I/E)

Codes affectés

Pour vérifier cela sur votre réseau, exécutez la commande suivante à partir de tous les WLC et vérifiez si le code présent dans vos WLC est répertorié dans le tableau ci-dessous.

```
WLC# show version | in Version
```

Vous pouvez également faire de même à partir des points d'accès. Vérifiez le résultat pour voir si l'image principale ou de sauvegarde exécute une image affectée parmi celles répertoriées dans le tableau.

```
AP# show version | in Image
```

Code affecté par le contrôleur	Image affectée par le point d'accès
17.12.4	De 17.12.4.0 à 17.12.4.212
17.12.5	De 17.12.5.0 à 17.12.5.208
17.12.6/6a	De 17.12.6.0 à 17.12.6.200

Remarque : Remarque : En général, si le réseau n'est pas en cours d'exécution et n'a pas exécuté 17.12.4, 17.12.5, 17.12.6/6a dans le passé, le problème n'est pas applicable.

Codes fixes

Le tableau suivant répertorie les versions du logiciel WLC et leurs APSP (Access Point Service Packs) correspondants qui contiennent le correctif pour ce bogue. Veuillez noter que pour les versions répertoriées ci-dessous, le correctif est actuellement disponible uniquement via l'installation d'APSP au moment de la rédaction de ce document.

Contrôleur et code fixe APSP	Image fixe du point d'accès
17.12.4 + APSP13	17.12.4.213
17.12.5 + APSP9	17.12.5.209
17.12.6a + APSP1	17.12.6.201
17.12.7 bis	17.12.7.13
17.15.3 + APSP12	17.15.3.212
17.15.4b + APSP6	17.15.4.206
17.15.4d + APSP1	17.15.4.225
17.15.5	17.15.5.36

17.18.1 + APSP3	17.18.1.203
17.18.2 + APSP2	17.18.2.202
17.18.3	17.18.3.18
26.1.1	26.1.1.11

Chemin de mise à niveau et applicabilité des bogues

Utilisez le tableau ci-dessous pour déterminer si vos versions logicielles actuelles de WLC et de points d'accès s'appliquent à ce bogue et quelles étapes de mise à niveau prendre. Si votre déploiement actuel correspond à l'une de ces versions dans la table Bug applicable et chemin de mise à niveau, vous devez effectuer les vérifications préalables du stockage expliquées dans la section Prévérifications de mise à niveau avant d'essayer d'autres mises à niveau.

Bogue non applicable et chemin de mise à niveau

Le tableau suivant indique si vos WLC et vos points d'accès ne s'appliquent pas à ce bogue :

Code actuel	Code cible	Applicabilité des bogues	Avant la mise à niveau - vérification préalable requise	Chemin cible/mise à niveau	Prévérification de mise à niveau	Commentaires
17,3 x / 17,6 x / 17,9 x	17.12.x	Non	Non	17.12.4 + APSPx 17.12.5 + APSPx17.12.6a + APSPx17.12.7	Non	Vérifier la destination Notes de version
17.9.x.	Tout (sauf 17.12.4/5/6/6a)	Non	Non	Suivre le chemin de mise à niveau	Non	17.9.1 à .5 ne prennent pas en charge la mise à niveau directe vers 17.15, utilisez 17.9.6 ou une version ultérieure pour plus d'informations, consultez les notes de version

17.12.1 à 17.12.3	Tout (sauf 17.12.4/5/6/6a)	Non	Non	Suivre le chemin de mise à niveau	Processus régulier	Vérifier la destination Notes de version
17,15+Nouveau déploiement	tous les modèles	Non	Non	tous les modèles	Non	
17.18.+Nouveau déploiement	tous les modèles	Non	Non	tous les modèles	Non	

Bogue applicable et chemin de mise à niveau

Le tableau suivant montre si vos WLC et points d'accès ne s'appliquent pas pour ce bogue :

Code actuel	Code cible	Applicabilité des bogues	Avant la mise à niveau - vérification préalable requise	Chemin cible/mise à niveau	Prévérification de mise à niveau	Commentaires
17.12.4/5/6/6a	17.12.x(4,5,6,6a, etc.), APSP	Oui	Oui: reportez-vous à la section Prévérification de mise à niveau	17.12.4 + APSP, 17.12.5 + APSP, 17.12.6a + APSP, 17.12.7	Oui	Après l'installation d'un APSP fixe, aucune vérification supplémentaire n'est nécessaire pour les futures mises à niveau de la version 17.12
17.12.4/5/6/6a	17.15.x / 17.18.x	Oui	Oui: reportez-vous à la section Prévérification de mise à niveau	Mettre à niveau l'APSP 17.12.x respectif, puis mettre à niveau vers 17.15.x + APSP ou 17.18.x + APSP	Oui pour la première mise à niveau APSP 17.12 et non pour les mises à niveau suivantes.	

Toute version, mais l'image précédente était l'une de 17.12.4/5/6/6a	17.15.x	Oui	Oui: reportez-vous à la section Prévérification de mise à niveau	17.15.x + APSP	Oui	
Toute version, mais l'image précédente était l'une de 17.12.4/5/6/6a	17.18.x	Oui	Oui: reportez-vous à la section Prévérification de mise à niveau	17.18.x + APSP	Oui	

Prévérifications de mise à niveau

Pour s'assurer que les points d'accès disposent d'un espace libre suffisant dans la partition 2 (partie 2) pour l'installation du code ou de l'APSP, les étapes suivantes doivent être suivies pour récupérer en toute sécurité l'espace de stockage :

1. Identifier : Exécutez les vérifications préalables manuelles ou automatisées pour identifier les points d'accès spécifiques applicables au bogue. Une vérification préalable automatisée est fortement recommandée.
2. Récupérer : Pour tous les points d'accès marqués avec peu d'espace dans la partie 2, suivez les procédures de récupération mentionnées dans la section Récupération d'espace.
3. Vérifier : Réexécutez les vérifications préalables pour confirmer que tous les périphériques sont en bon état et que le problème de disponibilité de l'espace dans la partie 2 est résolu.
4. Mise à niveau: Procédez à la mise à niveau vers les APSP fixes répertoriés dans la section Codes fixes.

Il existe 2 méthodes de précontrôle :

- Manuel
- Automatisé

La méthode recommandée est la méthode automatisée, car elle permet de gagner du temps et d'éviter les erreurs humaines.

Prévérification manuelle

1. À partir du WLC, vous pouvez vérifier les colonnes d'image principale et de sauvegarde pour confirmer si vos points d'accès exécutent l'une des versions affectées (consultez la section Codes

affectés ci-dessus).

```
WLC# show ap image
Total number of APs  : 4

AP Name              Primary Image          Backup Image            Predownload Status   Predownload Ver
-------------------------------------------------------------------------------------------------------
Ap117.12.5.41        17.12.4.201                None                  0.0.0.0            N/A
Ap217.12.5.41        17.12.4.201                None                  0.0.0.0            N/A
Ap317.12.5.41        17.12.4.201                None                  0.0.0.0            N/A
Ap417.12.5.41        17.12.4.201                None                  0.0.0.0            N/A
```

Vous pouvez également effectuer une vérification similaire directement au niveau du point d'accès en exécutant la commande suivante pour vérifier les deux partitions d'image :

```
AP# show version
AP Running Image     :17.12.5.41
Primary Boot Image   : 17.12.5.41
Backup Boot Image    : 17.12.5.209
```

Vérifiez la partition de démarrage active. Utilisez la commande « show boot » et vérifiez que la « liste de chemins BOOT » pointe vers la partie 1 ; cela indique que le point d'accès s'exécute actuellement à partir de la partition principale et tente d'effectuer une mise à niveau vers la partie secondaire (partie 2), ce qui pourrait déclencher le problème.

```
AP# show boot
--- Boot Variable Table ---
BOOT path-list: part1
```

2. Vérifiez l'utilisation actuelle du système de fichiers en vérifiant la partition /dev/ubivol/part2. Si la colonne « Disponible » indique moins de 85 Mo, la partition n'a pas assez d'espace pour installer l'APSP, ce qui entraîne l'échec de la mise à niveau et peut potentiellement déclencher une boucle de démarrage.

```
AP# show filesystems
Filesystem                Size      Used Available Use% Mounted on
devtmpfs                880.9M         0    880.9M   0% /dev
/sysroot                883.8M    219.6M    664.1M  25% /
tmpfs                     1.0M     56.0K    968.0K   5% /dev/shm
tmpfs                   883.8M         0    883.8M   0% /run
tmpfs                   883.8M         0    883.8M   0% /sys/fs/cgroup
/dev/ubivol/part1       372.1M     79.7M    292.4M  21% /part1
/dev/ubivol/part2       520.1M    291.3M    228.9M  56% /part2
```

3. Vérifiez l'intégrité de l'image pour les deux partitions afin de vous assurer qu'elles ne sont pas endommagées. Tous les champs des images principale et de sauvegarde doivent afficher l'état "Bon"; Si un champ indique le contraire, arrêtez le processus et passez à la section Quand ouvrir un dossier TAC.

```
AP# show image integrity
/part1(Backup) 17.12.5.209
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good
/part2(primary) 17.12.5.41
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good
```

Répertoriez tous les points d'accès démarrant à partir de la partie 1 et affichant moins de 85 Mo disponibles dans /dev/ubivol/part2 car ils auront besoin de récupération d'espace. Vous pouvez passer à la section Récupération de ce document.

Prévérification Automatisée

Pour la vérification automatique préalable, utilisez l'outil WLANPoller. Cet outil vous permet d'exécuter les commandes nécessaires sur tous vos points d'accès simultanément pour identifier les points d'accès concernés ; vous pouvez le télécharger directement à partir du lien suivant : https://developer.cisco.com/docs/wireless-troubleshooting-tools/wlan-poller-wlan-poller/

Remarque : Téléchargez la version de WLANPoller compatible avec votre système d'exploitation (Windows, Intel Mac ou ARM Mac). Assurez-vous que l'ordinateur hôte dispose d'une connectivité SSH aux points d'accès.

Étapes:

0- SSH : ces étapes supposent que l'accès SSH est activé dans tous les profils de jointure AP et que SSH n'est pas bloqué vers les points d'accès.

1. Extraction - Décompressez le fichier WLANPoller dans votre répertoire préféré. Après la décompression, vous trouverez deux répertoires et une application nommée comme suit :

- données
- confd
- Interface graphique WlanPoller

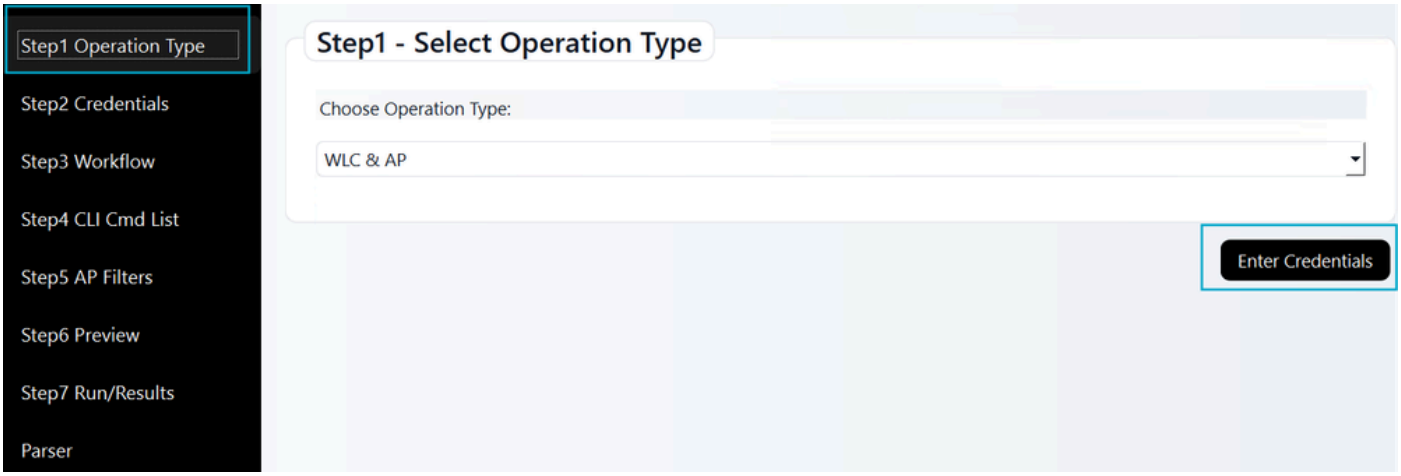
Remarque : Si vous rencontrez des erreurs lors de l'exécution de l'application après l'extraction avec des outils Windows natifs, veuillez utiliser un utilitaire tiers comme 7-Zip pour extraire les fichiers.

Remarque : pour que MacOS exécute l'application, ouvrez un terminal avec un accès racine et naviguez jusqu'au répertoire où WLANPoller a été extrait. Exécutez la commande suivante : sudo ./Wpgui_Mac_Arm64_Ver505/WlanPollerGUI.app/Contents/MacOS/WlanPollerGUI

---

2. Configuration - Lancez l'application WlanPollerGUI et configurez les paramètres comme suit :

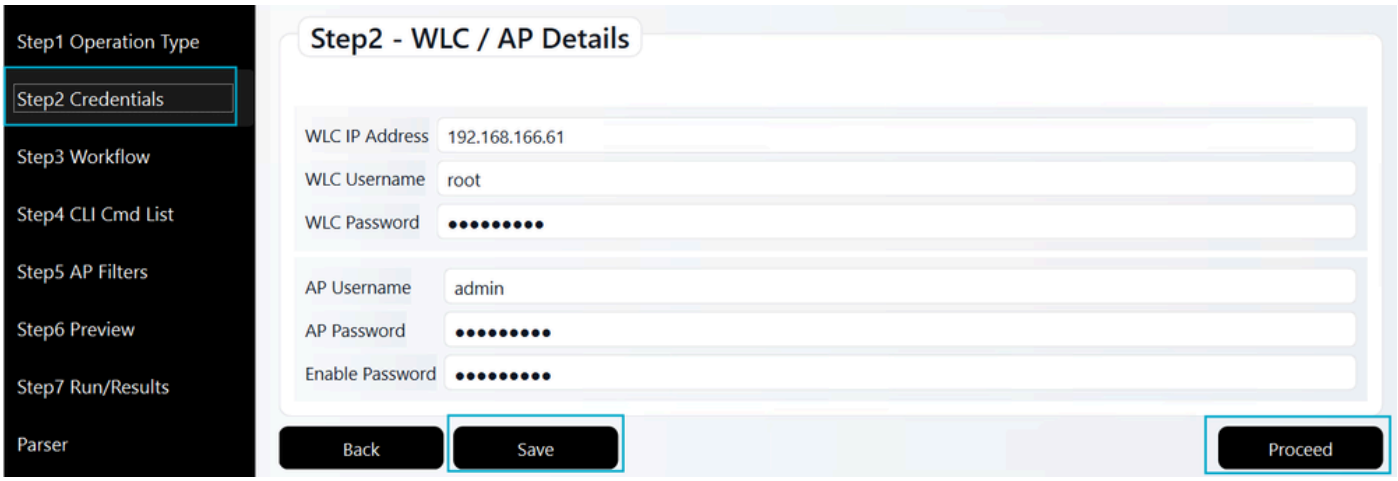
Type d'opération : Sélectionnez WLC et AP. Pour l'option Access PointOnly, téléchargez un fichier ".txt" répertoriant vos points d'accès dans un format séparé par des virgules (par exemple 192.168.166.105, Timpadil9166). Cliquez ensuite sur Enter Credentials.



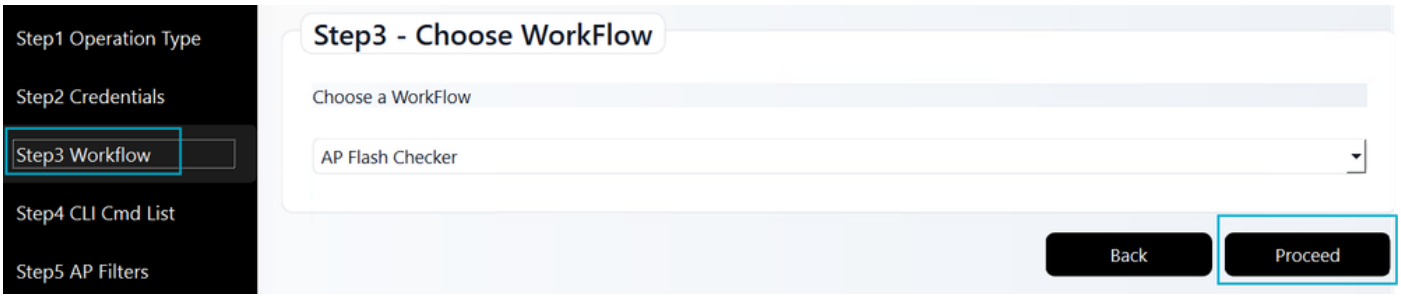
Pour le mode Access Point Only, assurez-vous que votre fichier ".txt" suit cet exemple :



Informations d'identification : Saisissez l'adresse IP et les informations d'identification du WLC. Incluez le nom d'utilisateur, le mot de passe et le mot de passe enable du point d'accès Join Profile. Cliquez sur Enregistrer, puis sur Continuer.

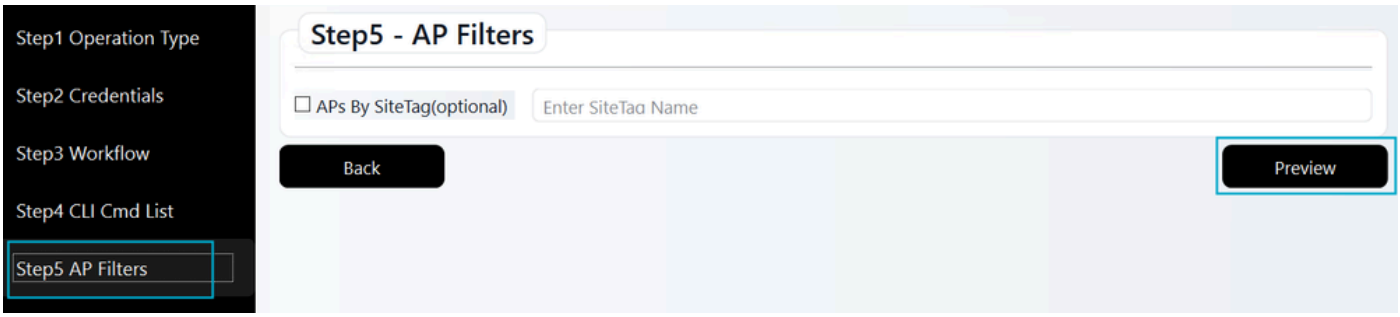


Workflow : Choisissez le workflow Vérificateur Flash du point d'accès pour exécuter les commandes de diagnostic requises. Cliquez ensuite sur Continuer.

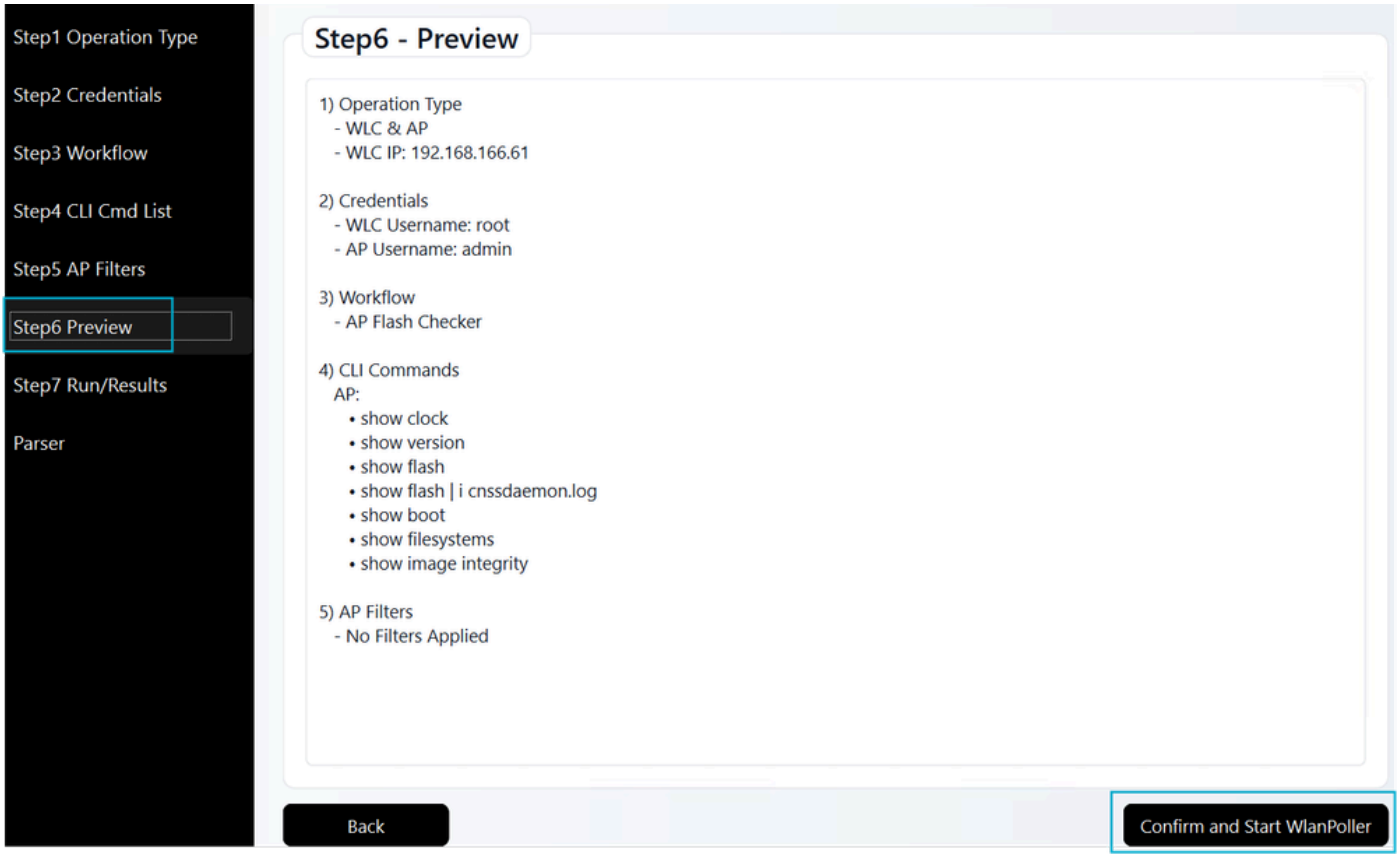


CLI Cmd List : cette étape est ignorée automatiquement ; la liste de commandes requise est déjà incluse dans le flux de travail Vérificateur Flash du point d'accès (étape 3).

Filtres de point d'accès : Cette étape facultative vous permet de filtrer par site spécifique. Si vous l'utilisez, cochez la case et entrez le nom de la balise de site (sensible à la casse). Une fois terminé, ou si vous ignorez cette étape, cliquez sur Aperçu.

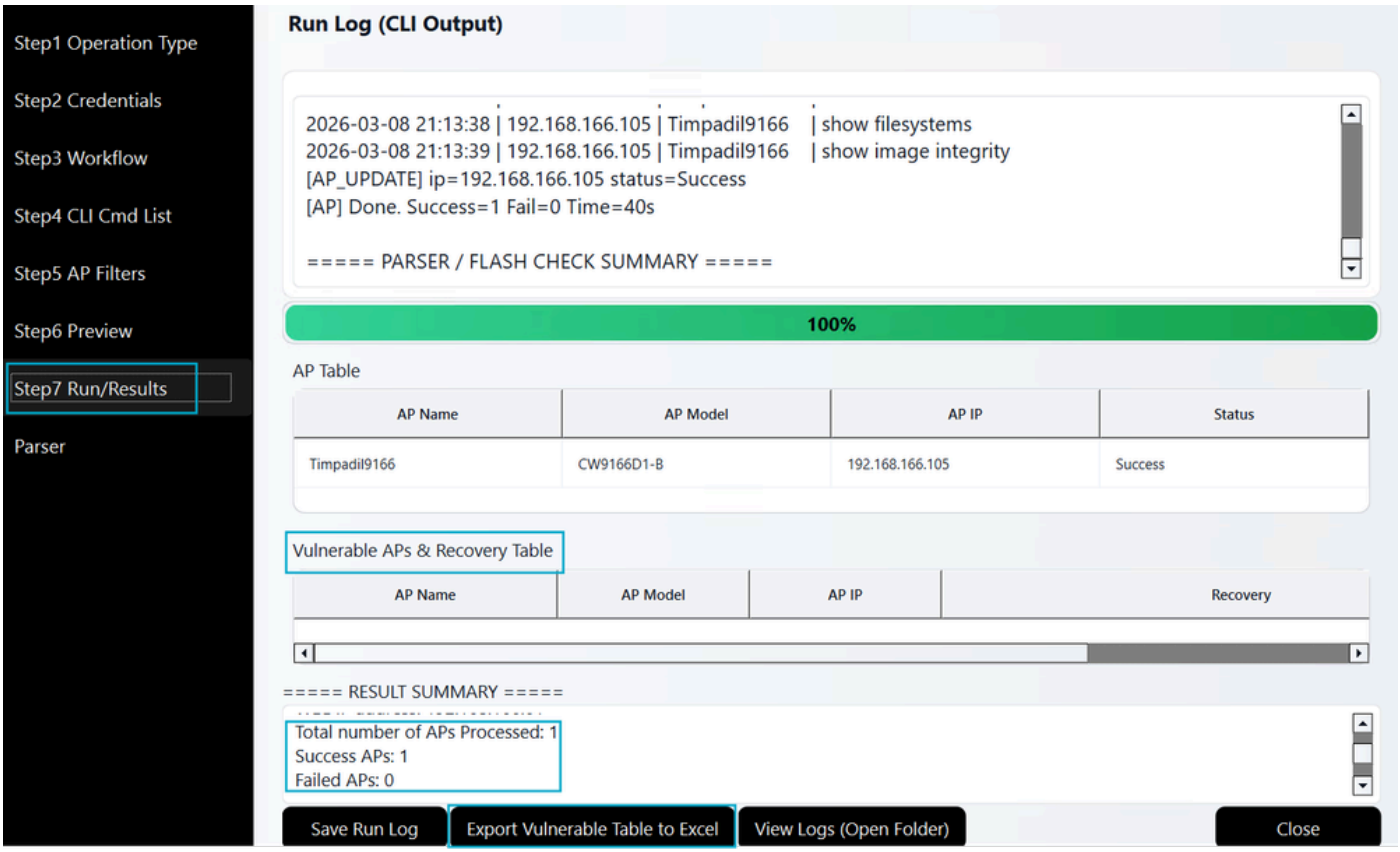


Preview : vérifiez vos paramètres WLANPoller ici. Les commandes CLI requises sont préremplies à partir de l'étape précédente du workflow. Après avoir confirmé les détails, cliquez sur Confirm and Start WLANPoller pour commencer la connexion SSH et la collecte de données.



3. Résultats : L'outil établit des connexions SSH à vos points d'accès pour exécuter les commandes nécessaires. Les résultats s'affichent pour vous aider à identifier les points d'accès nécessitant une récupération. Un enregistrement de ces données est automatiquement enregistré dans le sous-dossier data dans votre répertoire d'extraction WLANPoller.

Remarque : La fonctionnalité Exporter le tableau des failles vers Excel répertorie uniquement les points d'accès nécessitant une récupération. Si un point d'accès n'est pas répertorié, cela signifie qu'il n'est pas affecté.



Prévérifie les résultats

En fonction de l'analyse, WLANoller classe les points d'accès affectés dans l'une des options suivantes :

- État sûr, mais le point d'accès a une image boguée dans la partition de sauvegarde : Le point d'accès est actuellement sûr pour la mise à niveau et vous pouvez poursuivre l'installation du code/de l'APSP. Cependant, sachez que la partition de sauvegarde contient toujours une image sensible.
- Récupérer avec échange de partition d'image : Le point d'accès est actuellement amorcé à partir de la partition 1, mais la partition 2 ne dispose pas de suffisamment d'espace pour la mise à niveau. Un échange de partition de démarrage de point d'accès est requis.
- Récupérer avec devshell : Le point d'accès nécessite une récupération via devshell car l'espace est insuffisant dans l'une ou l'autre partition pour installer le nouveau code ou APSP.
- La vérification de l'intégrité de l'image a échoué pour ce point d'accès : La vérification d'intégrité de l'image de la partition 1 ou 2 a échoué. Une intervention manuelle peut être nécessaire.

Récupération

En fonction des résultats de la vérification préalable, vous pouvez sélectionner l'option de récupération appropriée qui convient le mieux à votre réseau, comme suit :

Résultat	Options de récupération
État sûr, mais le point d'accès a une image boguée dans la partition de sauvegarde	Pour plus d'informations, vous pouvez poursuivre l'installation du code/du protocole APSP
Récupération avec échange de partition d'image	Il existe 4 options : 1. Supprimez les fichiers principaux du point d'accès. 2. Réinitialisez les points d'accès en usine. 3. Échange de partition de démarrage d'image de point d'accès. 4. Supprimez le fichier cnssdaemon.log (Access Point devshell). Choisissez l'option de récupération la mieux adaptée à votre environnement et à la disponibilité de vos ressources.
Récupérer avec devshell	Il existe 2 options : 1. Supprimez le fichier cnssdaemon.log (Access Point devshell). 2. Réinitialisez les points d'accès en usine. Choisissez l'option de récupération la mieux adaptée à votre environnement et à la disponibilité de vos ressources.
La vérification de l'intégrité de l'image a échoué pour ce point d'accès	Suivez la procédure : Quand ouvrir un dossier TAC

Il existe deux chemins de récupération en fonction de l'état actuel de vos points d'accès. L'état des points d'accès peut être :

1. Faible espace disponible dans la partition 2 : Cela se produit lors de la phase de pré-mise à niveau (trouvée lors des vérifications préalables de la mise à niveau) lors d'une tentative d'installation de code/APSP.
2. Bootloop du point d'accès : Cela se produit après la mise à niveau si l'installation du code/APSP a été tentée malgré un espace insuffisant.

Les étapes de récupération détaillées pour chacun des états possibles des points d'accès sont décrites ci-dessous.

Faible espace disponible dans la partition 2

Si la vérification préalable de mise à niveau identifie des points d'accès démarrant avec la partition 1 et avec un espace insuffisant dans la partition 2, utilisez l'une des méthodes suivantes pour faire de l'espace dans la partition.

- Supprimer les fichiers principaux du point d'accès : Les points d'accès stockent les vidages principaux dans /dev/ubivol/part2. Si ces fichiers existent, leur suppression peut libérer suffisamment d'espace. Après la suppression, vous devez réexécuter la vérification préalable de mise à niveau pour valider que l'espace disponible répond aux exigences d'installation.
- Réinitialisation du point d'accès : La réinitialisation d'usine rétablit la configuration par défaut du point d'accès. Ce processus efface temporairement le fichier cnssdaemon.log du stockage, en fournissant généralement assez d'espace dans la partition 2 (partie 2) pour installer correctement le code/APSP.
- Supprimez le fichier cnssdaemon.log (Access Point devshell) : Ce processus implique l'accès au devshell des points d'accès pour supprimer manuellement le fichier cnssdaemon.log. Notez que cela nécessite un accès administratif et une coordination avec le TAC pour entrer dans l'environnement devshell.
- Remplacement de la partition de démarrage : Si la partition 2 (partie2) n'a pas assez d'espace pour installer le code/APSP mais contient déjà une image fonctionnelle, vous pouvez démarrer le point d'accès à partir de la partie2 et cibler l'installation sur la partition 1 (partie1), qui dispose généralement d'espace disponible.

Veuillez vérifier les détails de chacune des options pour vous assurer que vous comprenez les exigences. Sélectionnez la méthode la mieux adaptée à votre environnement réseau et à vos besoins opérationnels.

Supprimer les fichiers principaux des points d'accès

Les fichiers principaux peuvent être supprimés manuellement en accédant à chaque point d'accès via SSH. Vous pouvez également utiliser WLANPoller pour automatiser ce processus et effectuer des suppressions en mode bulk pour plusieurs points d'accès simultanément.

Mode manuel

Accédez à chaque point d'accès via SSH et exécutez les commandes suivantes :

```
AP# delete /force cores
AP# reload
Proceed with reload? [confirm] yes
```

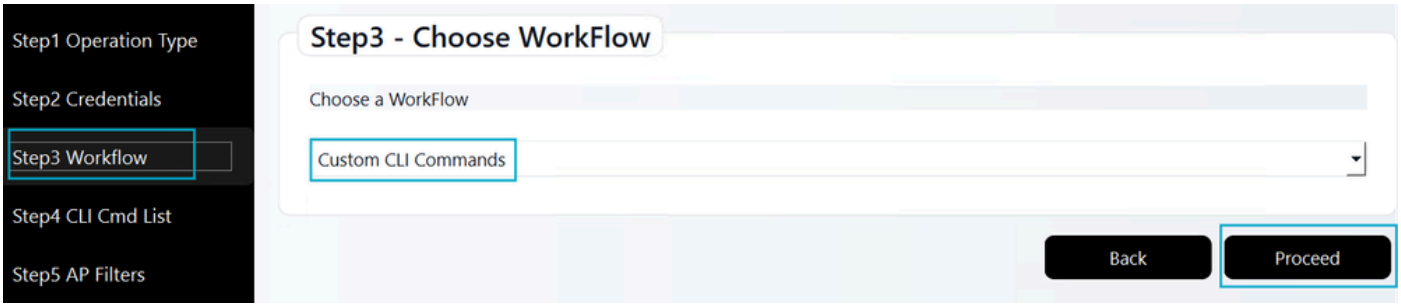
Mode automatisé

Lancez l'application WLANPoller et procédez comme suit :

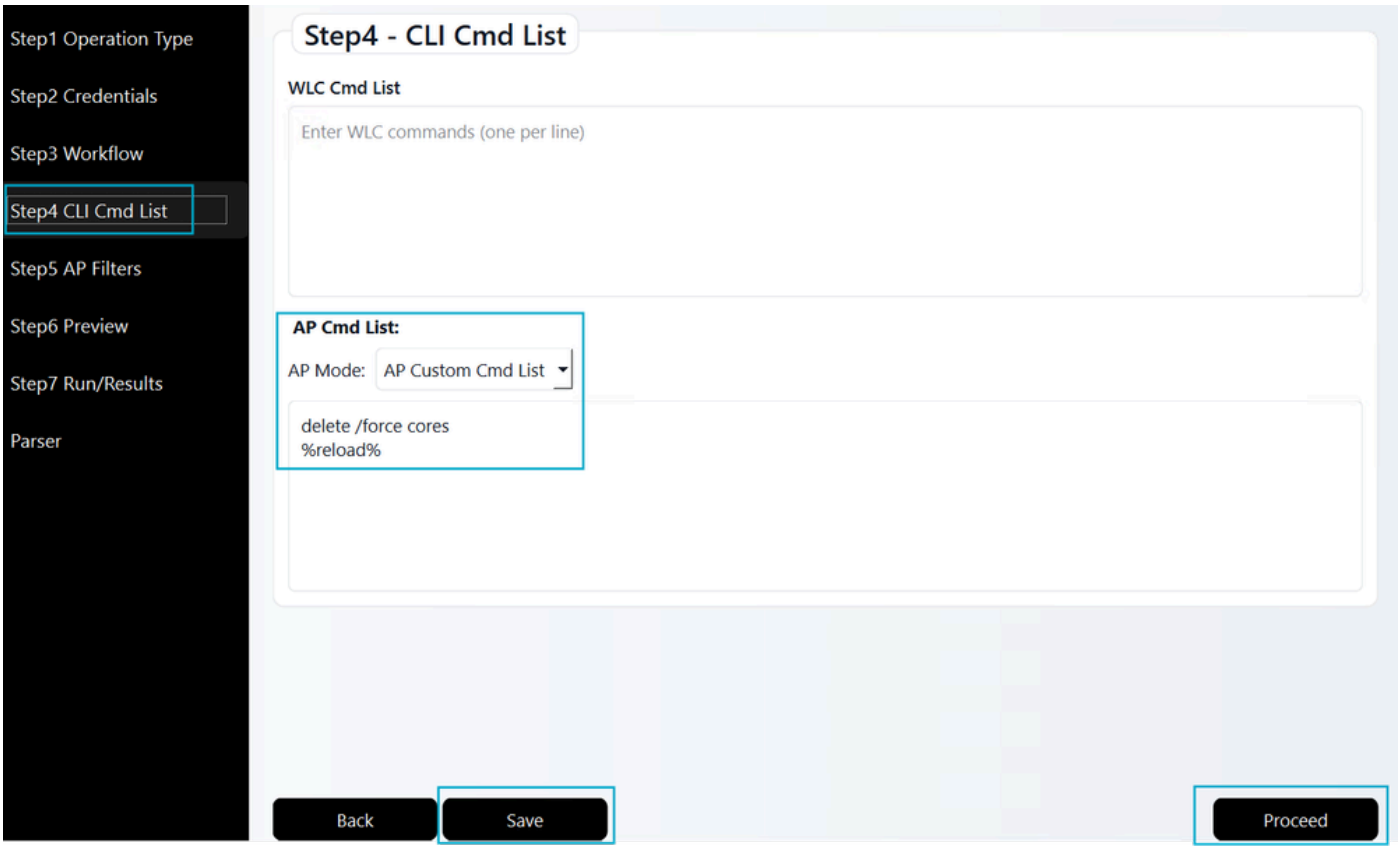
Type d'opération : Sélectionnez le type d'opération WLC & AP.

Informations d'identification : Saisissez les informations d'identification WLC et Access Point.

Workflow : Mettez à jour la sélection vers Commandes CLI personnalisées et cliquez sur Continuer.



Liste des commandes CLI : Entrez les commandes de point d'accès suivantes exactement comme elles s'affichent. Cliquez sur Enregistrer, puis sur Continuer.



Filtres de point d'accès : Ne cochez pas toutes les cases sauf si un filtre spécifique est requis pour votre environnement, puis cliquez sur Aperçu.

Aperçu : Vérifiez le résumé, puis cliquez sur Confirm and Start WLANPoller.

Résultats : Vérifiez que l'exécution de WLANPoller s'est correctement terminée pour tous les points d'accès ciblés.

Après la récupération, répétez la vérification préalable de mise à niveau comme décrit dans cette section. Vérifiez si les points d'accès affectés affichent toujours une faible disponibilité de l'espace. Si c'est le cas, passez à la recherche des options suivantes qui correspondent mieux à vos ressources ; s'ils sont effacés de la liste, la récupération est réussie et vous pouvez poursuivre avec le code/APSP dans ces points d'accès.

Réinitialisation en usine des points d'accès

La réinitialisation des paramètres d'usine du point d'accès supprime temporairement le fichier cnssdaemon.log. Pour garantir la réussite de l'installation du code/de l'APSP, veuillez poursuivre l'installation du code/de l'APSP dans les 48 heures suivant la réinitialisation en usine.

Il existe trois façons de réinitialiser en usine les points d'accès :

- Via le WLC (CLI ou GUI).
- Via la CLI du point d'accès,
- Via le bouton de réinitialisation physique du point d'accès.



Avertissement : Une réinitialisation d'usine supprime toutes les configurations persistantes (par exemple, nom d'hôte, paramètres HA, balises, LSC, etc.). Vous devez reconfigurer le point d'accès après qu'il ait rejoint le WLC. Assurez-vous que la détection CAPWAP (DHCP Option 43, DNS, etc.) est fonctionnelle pour que le point d'accès puisse trouver et joindre le contrôleur après la réinitialisation.

Via CLI WLC

```
WLC# clear ap config <APNAME> keep-ip-config
```

Via l'interface graphique WLC

Accédez à Configuration > Wireless > Access Points. Sélectionnez le point d'accès souhaité, puis accédez à Advanced > Set to Factory Default. Choisissez l'option Clear Config sauf Static IP et cliquez sur Update & Apply to Device.

Via la CLI du point d'accès

```
AP# capwap ap erase all
WARNING :" capwap ap erase all" is altered to perform DATA WIPE on COS AP.
The following files will be cleared as part of this process
1) Config ,Bak config files
2) Crashfiles
3) syslogs
4) Boot variables
5) Pktlogs
6) Manually created files
Are you sure you want continue? [confirm] yes
AP# reload
Proceed with reload command (cold)? [confirm] yes
```

Bouton Via le mode Point d'accès

1. Débranchez le point d'accès de sa source d'alimentation.

2. Appuyez sur le bouton Mode et maintenez-le enfoncé.

3. Reconnectez la source d'alimentation tout en maintenant le bouton enfoncé.

4. Une fois que le voyant d'état du point d'accès devient rouge fixe, maintenez le bouton Mode enfoncé pendant 10 secondes supplémentaires.

5. Relâchez le bouton.

6. Le point d'accès redémarre avec les paramètres d'usine par défaut.

Remarque : Le moment où vous appuyez sur le bouton Mode est critique. Si vous appuyez sur le bouton pendant moins de 20 secondes, le fichier cnssdaemon.log ne sera pas supprimé. Inversement, s'il est maintenu pendant plus de 60 secondes, le point d'accès ne réinitialise pas les paramètres d'usine. Veuillez vous assurer que le bouton est maintenu entre 30 et 50 secondes pour une réinitialisation réussie

---

Supprimer le fichier cnssdaemon.log (Access Point devshell)

Le Centre d'assistance technique (TAC) peut effectuer une récupération manuelle en effaçant le fichier cnssdaemon.log directement à partir de devshell sur les points d'accès affectés. Selon l'échelle de l'impact, il existe deux méthodes :

- Petit nombre de points d'accès concernés : Pour un petit nombre de points d'accès concernés, le TAC peut procéder selon l'une des deux approches suivantes :
    - Accès manuel au devshell : Accédez à chaque point d'accès individuellement via devshell pour effacer manuellement le fichier cnssdaemon.log.
    - Accès automatisé (en masse) au devshell : Utilisez l'outil RADKit pour automatiser le processus de nettoyage du fichier cnssdaemon.log vers tous les points d'accès concernés.
- Grand nombre de points d'accès affectés : le centre d'assistance technique doit utiliser l'outil RADKit, ce qui permet un accès en masse par devshell à tous les points d'accès affectés de manière automatisée afin d'exécuter le processus de nettoyage efficacement.

Remarque : Nous vous recommandons d'utiliser RADKit pour la procédure de

---

récupération du devshell du point d'accès afin d'assurer une efficacité et une cohérence opérationnelle maximales dans votre environnement.

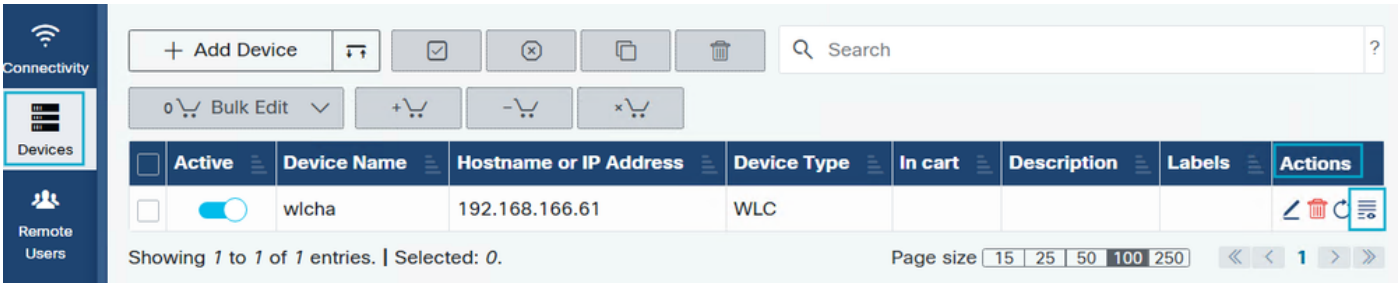
Accédez aux instructions de téléchargement et d'installation de RADKit via les liens ci-dessous :

- Téléchargement RADKit
- Installation de RADKit

Pour supprimer le fichier cnssdaemon.log dans les points d'accès via RADKit, assurez-vous que tous les points d'accès sont répertoriés dans l'inventaire. Il s'agit d'une tâche réservée aux administrateurs qui ne peut pas être effectuée à distance par le TAC. Pour ajouter en masse des points d'accès à l'inventaire RADKit, procédez comme suit :

1. WLC dans RADKit : Assurez-vous que le WLC est déjà ajouté à l'inventaire RADKit. Si vous avez besoin d'aide avec ce processus, veuillez suivre la section Ajout de périphériques ici de la documentation officielle de RADKit

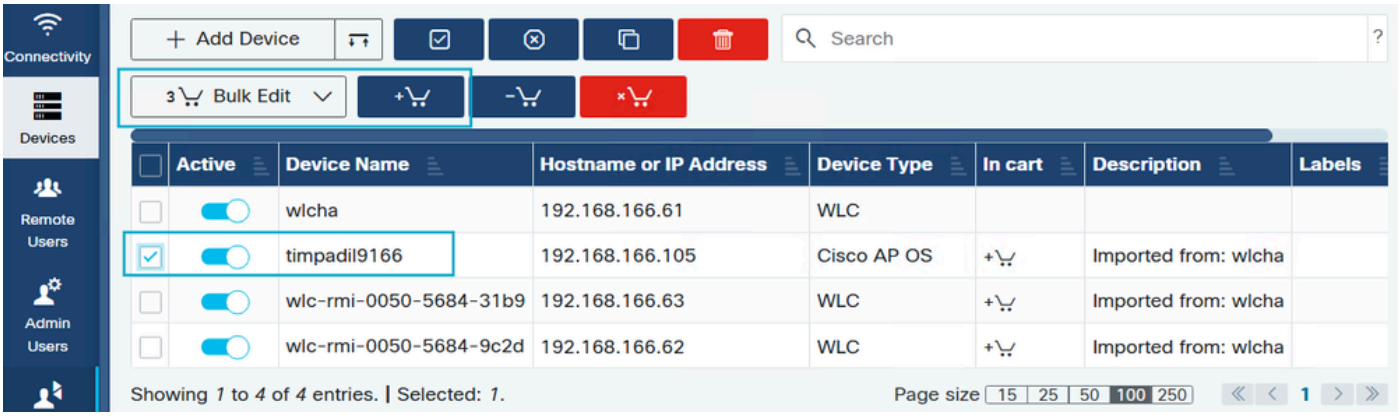
2. Icône d'inventaire WLC : Sous l'onglet Devices, localisez votre WLC et cliquez sur l'icône Inventory dans la colonne Actions.



3. Importation en masse : Cliquez sur le bouton Bulk Import pour lancer le processus d'ajout de points d'accès à RADKit.

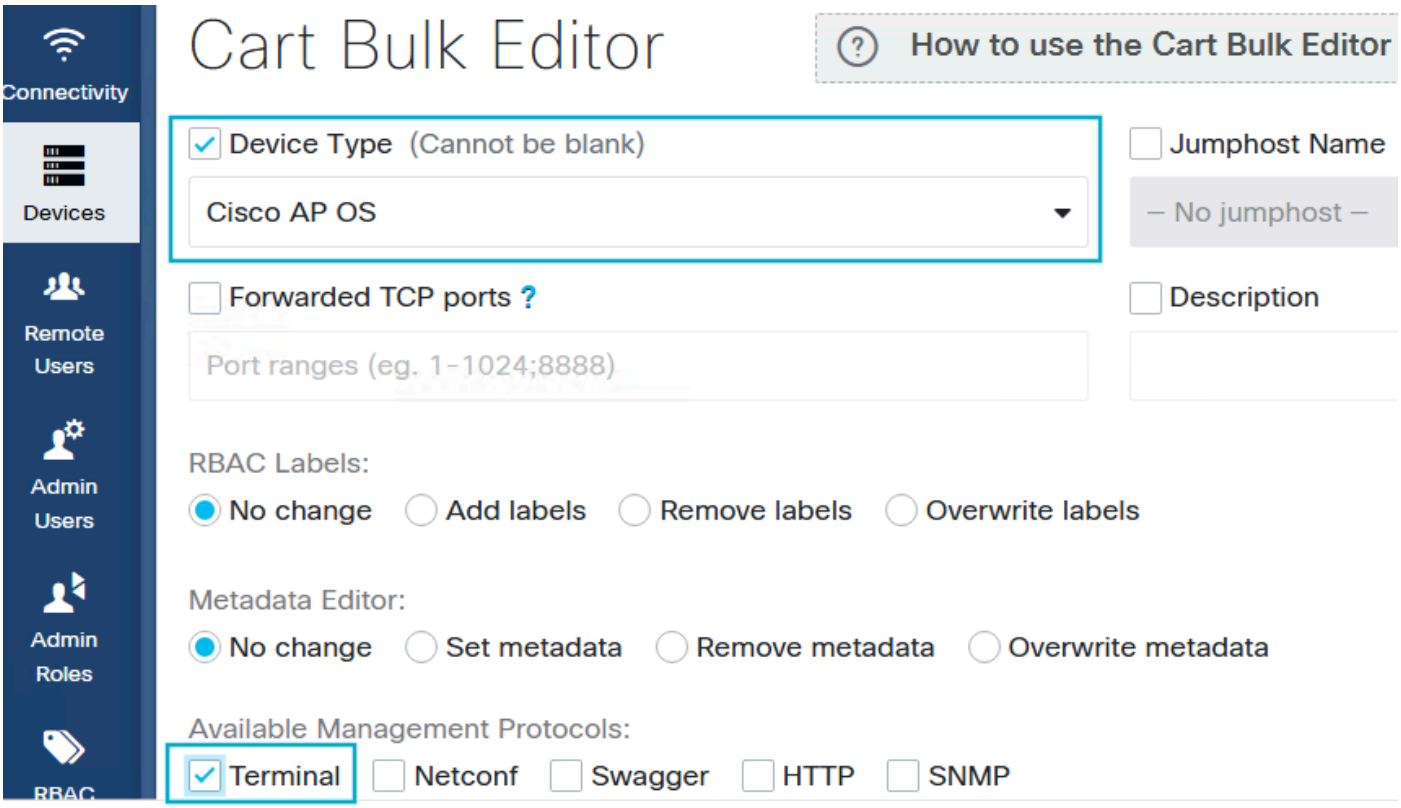


4. Configuration en bloc : Cochez les cases de tous les points d'accès nécessitant la suppression du fichier cnssdaemon.log. Cliquez sur l'icône Ajouter au panier (panier avec un signe plus), puis sélectionnez le bouton Modifier en bloc.

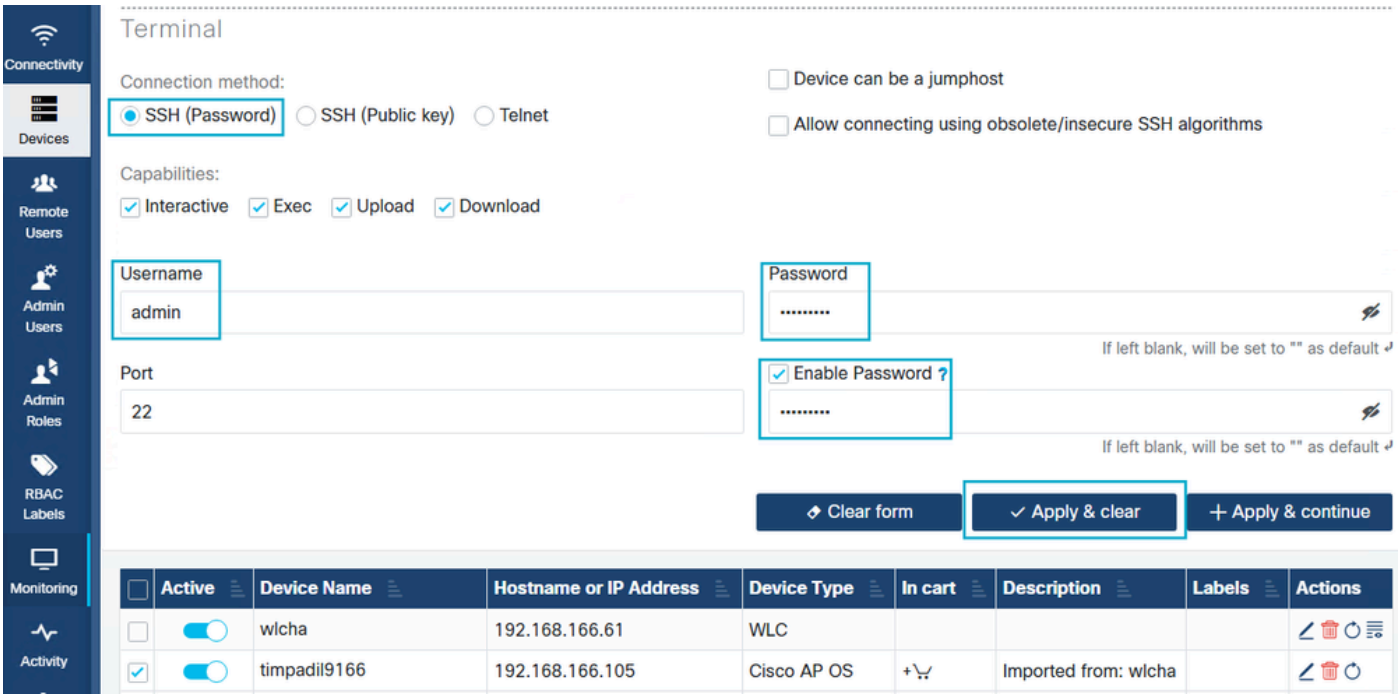


5. Activer le terminal et configurer SSH : Dans l'Éditeur en masse du chariot, cochez Type de périphérique et sélectionnez Cisco AP OS. Activez le bouton Terminal pour permettre la configuration SSH pour les points d'accès.

Remarque : Si le contrôle d'accès basé sur les rôles (RBAC) est activé, cliquez sur Ajouter des étiquettes et assurez-vous que Lecture seule est présent dans le champ Étiquettes sélectionnées (créez cette étiquette si elle n'existe pas déjà). Si le RBAC est désactivé, cette étape d'étiquetage n'est pas requise.



6. Configurez les informations d'identification SSH : Cliquez sur SSH (Mot de passe) et entrez les informations d'identification du point d'accès. Cochez la case Activer le mot de passe et entrez le mot de passe. Cliquez sur Appliquer et effacer pour enregistrer ces paramètres et fermer la fenêtre. Vérifiez que SSH est activé dans le WLC via AP Join Profile et que le nom d'utilisateur et le mot de passe sont à jour et corrects.



7. Ajouter un utilisateur distant : Ajoutez l'ID CCO Cisco de l'ingénieur affecté à votre dossier TAC

en suivant les étapes Ajout d'utilisateurs distants ici dans la documentation officielle de RADKit.

8. Liste des points d'accès ciblés : Collectez les noms exacts des points d'accès concernés (remarque : (sensible à la casse) dans un fichier, puis téléchargez le fichier dans votre dossier TAC.

Après l'installation et le téléchargement des fichiers avec les noms des points d'accès, le centre d'assistance technique de Cisco disposera de l'accès à distance nécessaire via RADKit pour effectuer la suppression en bloc des fichiers cnssdaemon.log.



Remarque : Le TAC peut également utiliser l'outil de nettoyage RADKit même si vous disposez d'un radkit d'entrefer. Cependant, vous devez toujours exécuter le client radkit à partir d'un ordinateur qui peut accéder aux API webex pour que les défis de devshell soient signés par un ingénieur du centre d'assistance technique Cisco.

Échange de partition de démarrage d'image du point d'accès

L'échange de la partition de démarrage peut être fait soit manuellement point d'accès par point d'accès ou automatisé via l'accès point d'accès en masse avec WLANPoller.

Manuellement

Établissez une connexion SSH avec les points d'accès et exécutez les commandes suivantes :

```
AP# config boot path 2
AP# reload
Proceed with reload? [confirm] yes
```

Automatisé

Utilisez WLANPoller pour exécuter la commande boot part en masse vers différents points d'accès.

1. Isoler les points d'accès affectés - assurez-vous que les points d'accès affectés n'ont aucune connectivité avec le WLC :
    - Assurez-vous que SSH est activé dans le profil de jointure des points d'accès et que les points d'accès sont accessibles par SSH (ou utilisez la console)

- Assurez-vous que les points d'accès n'ont pas de connectivité avec le WLC, mais, vous avez toujours un accès SSH aux points d'accès. Pour ce faire, il suffit de disposer d'une liste de contrôle d'accès dans la passerelle ou de déplacer les points d'accès vers un VLAN isolé. Si les points d'accès obtiennent l'accès au WLC, le point d'accès pourrait revenir à la partition de démarrage 1 (partie1) et sera de retour à l'état affecté.

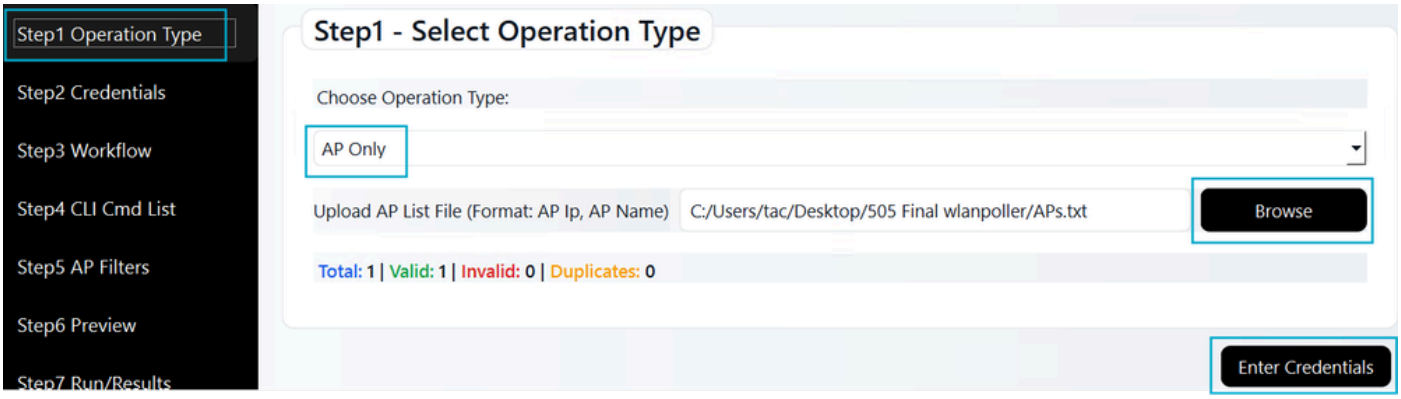
2. Configurez le chemin d'amorçage 2 et redémarrez les points d'accès affectés - Configurez WlanPoller pour indiquer aux points d'accès affectés via la ligne de commande de changer la partie d'amorçage de 1 à 2, puis redémarrez.

Type d'opération : Sélectionnez l'option AP Only, puis dans un éditeur de texte (de préférence) ajoutez les adresses IP et le nom des points d'accès (sensibles à la casse), cliquez sur Browse et sélectionnez le fichier avec les adresses IP et les noms des points d'accès. Cliquez ensuite sur Enter Credentials.

Format de liste de points d'accès :



Sélection du type d'opération :

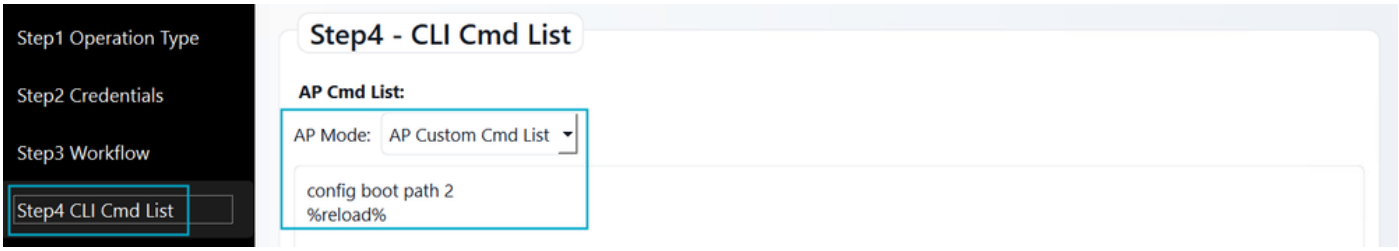


Informations d'identification : Saisissez les informations d'identification des points d'accès, cliquez sur Enregistrer, puis sur Continuer.

Workflow : Sélectionnez Commandes CLI personnalisées, puis cliquez sur Continuer.

Liste des commandes CLI : Configurez les commandes pour que le point d'accès démarre avec

part2 et redémarre. Cliquez ensuite sur Save, puis sur Proceed.



Aperçu : L'aperçu vous montre les 2 commandes qui seront exécutées sur les points d'accès. Cliquez sur Confirm and Start WlanPoller.

3. Mise à niveau - Installez dans le WLC l'APSP nécessaire dans votre code actuel, ou, si vous deviez mettre à niveau le code, passez à un nouveau code et assurez-vous que l'APSP est également installé.

4. Reconnect - Une fois la mise à niveau du contrôleur terminée, supprimez l'arrêt de communication entre le point d'accès et le WLC. Le point d'accès se connectera au WLC et téléchargera automatiquement la nouvelle image fixe dans la Partie1 de démarrage.

Bootloop du point d'accès

Si vous avez effectué une installation de code/APSP sans suivre les vérifications préalables de mise à niveau et que vos points d'accès se sont retrouvés dans une boucle d'amorçage, il y a 2 options à suivre :

1. Réinitialisez le point d'accès en usine à l'aide du bouton Mode, comme expliqué dans la section Réinitialisez en usine les points d'accès.
2. Obtenez un accès à la console et ouvrez un dossier TAC afin que le TAC puisse procéder à la récupération du point d'accès.

Quand ouvrir un dossier TAC

Ouvrez un dossier TAC si l'une des situations suivantes se présente :

- Échec de la récupération : Si les procédures de récupération ne peuvent pas être implémentées dans votre environnement ou si elles échouent.
- Problèmes d'intégrité : Les prévérifications manuelles ou automatisées renvoient une « Vérification de l'intégrité de l'image : Mauvais".
- Épuisement du stockage : Si, après la mise à niveau/l'installation d'APSP, la partition

"/dev/ubivol/part2" montre toujours une utilisation très élevée.

FAQ

Q : Ce problème s'applique-t-il uniquement aux mises à niveau de code complètes ou affecte-t-il également les installations APSP ?

A : Ce problème affecte les deux scénarios. Si votre environnement répond aux critères de ce bogue, le problème peut se produire pendant une mise à niveau complète du code ou l'installation d'APSP (y compris l'APSP avec le correctif de bogue). Veuillez compléter la section Prévérifications de mise à niveau pour déterminer si vous devez suivre les étapes de récupération avant d'appliquer des mises à jour ou des PASP.

Q : Mon WLC et mes points d'accès sont sur 17.9.x (ou antérieure) et je dois mettre à niveau vers 17.12.x, Que dois-je faire ?

A : Vous pouvez effectuer une mise à niveau directe de 17.9.x vers 17.12.x. Cependant, si vos modèles de point d'accès sont sensibles à ce bogue, assurez-vous d'installer l'APSP recommandé immédiatement après la mise à niveau.

Q : Mon WLC et mes points d'accès sont sur 17.9.x (ou antérieur) et je dois mettre à niveau vers 17.15.x ou supérieur.

A : Deux scénarios sont possibles :

- Mise à niveau directe : Si votre environnement permet une mise à niveau directe (veuillez vérifier via les notes de publication pour votre code cible), poursuivez la mise à niveau, puis installez l'APSP pour ce code cible.
- Mise à niveau intermédiaire : Si vous devez suivre un chemin de mise à niveau (par exemple, 17.9.x → 17.12.x → 17.15.x), nous vous recommandons de terminer la séquence complète vers 17.15.x dans le même jour. Étant donné que le fichier cnssdaemon.log augmente de 5 Mo par jour, l'achèvement de la mise à niveau empêche rapidement le fichier d'atteindre une taille critique. Si une mise à niveau le jour même n'est pas possible, vous devez installer l'APSP à l'étape 17.12.x avant de passer à l'étape 17.15.x et d'installer son APSP respectif.

Q : Je suis déjà sur 17.15.x. Cela signifie-t-il que je ne suis pas affecté par ce bogue ?

A : Pas nécessairement. Si vos points d'accès exécutaient précédemment la version 17.12.4, 17.12.5 ou 17.12.6/6a (sur 9800-L/40/80/CL), le fichier journal problématique a peut-être déjà été

généré et reste stocké. Nous vous recommandons vivement de suivre la section Prévérifications de mise à niveau pour vous assurer que les fichiers résiduels sont nettoyés.

Q : J'utilise les plates-formes 9800-M, 9800-H1 ou 9800-H2, qui ont été prises en charge pour la première fois dans la version 17.15. Suis-je concerné ?

A : Deux scénarios sont possibles :

- Première connexion au WLC : Si vos points d'accès ont rejoint un 9800-M/H1/H2 en tant que premier contrôleur, vous n'êtes pas affecté.
- Les WLC précédents ont rejoint : Si ces points d'accès étaient précédemment reliés à un autre contrôleur exécutant une version affectée (17.12.4/5/6/6a) avant de passer au 9800-M/H1/H2, ils peuvent toujours transporter le fichier problématique. Dans ce cas, veuillez suivre la section Prévérifications de mise à niveau.

Q : Nous avons des WLC séparés pour les tests en laboratoire et les mises à niveau échelonnées, Comment les gérer ?

A : Assurez-vous que tous les WLC de votre environnement exécutent l'APSP approprié. Étant donné que le fichier cnssdaemon.log augmente de 5 Mo par jour, tout point d'accès qui rejoint un WLC exécutant du code affecté, même temporairement pour le test, devient potentiellement sensible à ce bogue.

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.