

# Comment restaurer ma version actuelle d'AsyncOS sur un dispositif de sécurité de la messagerie Cisco ?

## Question :

Environnement : Appareil de sécurité de la messagerie Cisco (ESA), toutes les versions d'AsyncOS

## Résumé:

Dans AsyncOS, la fonction de restauration permet de restaurer la version précédente de l'appliance.

## Toutes les versions précédentes ne seront pas disponibles :

Les mises à niveau provoquent une transformation unidirectionnelle des sous-systèmes clés qui complique le processus de réversion. Cisco certifie des versions spécifiques de CASE, Sophos, VOF et McAfee vers AsyncOS, pour garantir une réversion transparente, les versions cibles doivent être qualifiées par Cisco. Toutes les versions antérieures ne seront pas disponibles ; il n'y aura que des possibilités limitées de réversion prédéterminées.

## La réversion prendra autant de temps que la mise à niveau :

Pour enregistrer les ressources du système de fichiers, les supports d'installation ne sont pas conservés sur les appliances. Le processus de reversion nécessite la diffusion en continu, le téléchargement en cours, l'installation.

## La réversion est destructrice :

Tous les messages de la file d'attente de travail ou de remise sont supprimés. Toutes les données de rapport et les fichiers journaux sont supprimés. Seules les données de clé de fonction sont conservées, toutes les autres configurations sont perdues. Toutes les bases de données et les données de suivi des messages seront perdues. Tous les messages de quarantaine du spam et les données de liste sécurisée/de liste de blocage de l'utilisateur final. Seuls les paramètres réseau seront préservés. Vous devez disposer d'un accès console à la case post revert, car l'adresse IP revient à la valeur par défaut 192.168.42.42. La restauration du périphérique entraîne un redémarrage immédiat. Après le redémarrage, la solution matérielle-logicielle se réinitialise et redémarre vers la version souhaitée.

## Préparez-vous à une éventuelle réversion avant la mise à niveau :

En tant que meilleure pratique, Cisco recommande de se préparer à une mise à niveau en procédant comme suit :

1. Enregistrer le fichier de configuration XML dans la zone désactivée (avec les mots de passe non masqués)
2. Si vous utilisez la fonction de liste sécurisée/de blocage, exportez la liste dans la case

correspondante.

3. Suspendre les écouteurs
4. Réduire la file d'attente de messagerie et la file d'attente de remise
5. Exporter la base de données sécurisée/de liste de blocage de quarantaine du spam vers une autre machine (le cas échéant)

N'oubliez pas de réactiver la mise à niveau post-écoute.

Comment :

1. Se connecter à l'interface de ligne de commande
2. Entrez « revert ».
3. ESA présentera un menu de versions qualifiées précédemment installées
4. Choisir la version de rétablissement
5. Redémarrez
6. Premier redémarrage : le système démarre, efface les disques, désinstalle les supports
7. Deuxième redémarrage (automatique) : le système utilise la version sélectionnée, initialise les données fraîches, l'apppliance démarre
8. Charger le fichier de configuration XML que vous avez enregistré lors de la mise à niveau
9. Si nécessaire, importez le fichier de liste sécurisée/de blocage