Comment est-ce que je roule de retour de ma version en cours d'AsyncOS sur une appliance de sécurité du courrier électronique de Cisco ?

Question :

Environnement : Appliance de sécurité du courrier électronique de Cisco (ESA), toutes les versions d'AsyncOS

Résumé :

Dans AsyncOS, « retournez » la caractéristique tient compte du roulement soutiennent l'appliance à une version préalable.

Non toutes les versions préalables seront disponibles :

Les mises à jour entraînent la transformation à sens unique des sous-systèmes principaux compliquant le procédé d'inversion. Cisco certifie des versions spécifiques de CAS, de Sophos, de VOF et de McAfee aux versions d'AsyncOS, pour assurer une inversion sans couture, des constructions de version cible doivent être qualifiés par Cisco. Non toutes les constructions antérieures seront disponibles ; seulement les possibilités limitées et prédéterminées d'inversion existeront.

L'inversion prendra tant que la mise à jour :

Pour économiser des ressources système en fichier, des medias d'installation ne sont pas gardés sur des appliances. Le procédé d'inversion exige couler, faire-service informatique-tandis que-téléchargement, installation.

L'inversion est destructive :

Tous les messages dans la file d'attente de travail ou la file d'attente de la livraison sont supprimés. Tous les données et fichiers journal d'enregistrement sont supprimés. Seulement, des données de touche de fonction sont préservées, toutes autres configurations sont perdues. Toutes les bases de données et données de cheminement de message seront perdues. Tous les message de quarantaine de Spam et données de l'utilisateur safelist/blocklist. Seulement les paramètres réseau seront préservés. Vous devez avoir accès de console au courrier de case retourner car l'IP retournera au par défaut de 192.168.42.42. Le retour du périphérique fait avoir lieu une réinitialisation immédiate. Après réinitialisation, l'appliance se réinitialise et le redémarre de nouveau à la version désirée.

Préparez-vous à une inversion possible avant l'évolution :

Comme pratique recommandée, Cisco recommande la préparation à une mise à jour en prenant les mesures suivantes :

1. Sauvegardez le fichier de config XML outre de la case (les mots de passe étant démasqué)
2. Si vous utilisez la caractéristique Safelist/Blocklist, exportez la liste outre de la case

3. Interrompez les auditeurs
4. Videz la file d'attente de messagerie et la file d'attente de la livraison
5. Exportez la base de données de la quarantaine safelist/blocklist de Spam à un autre ordinateur (si c'est approprié)

N'oubliez pas réactivent la mise à jour de courrier d'auditeurs.

Comment :

1. Procédure de connexion au CLI
2. Le type « retournent »
3. L'ESA présentera un menu des versions précédemment installées et qualifiées
4. La sélection retournent la version
5. Réinitialisation
6. Première réinitialisation - le système est soulevé, des disques d'espaces libres, éclate le support d'installation
7. En second lieu le système de réinitialisation (automatique) - est livré utilisant la version sélectionnée, initialise des données fraîches, des débuts d'appareils
8. Chargez le fichier de config XML que vous vous êtes enregistré tout en améliorant
9. S'il y a lieu, importez le fichier Safelist/Blocklist