

Wie kann ich auf einer Cisco E-Mail Security Appliance von meiner aktuellen Version von AsyncOS zurücksetzen?

Frage:

Umgebung: Cisco Email Security Appliance (ESA), alle Versionen von AsyncOS

Zusammenfassung:

In AsyncOS ermöglicht die Funktion "Zurücksetzen" das Zurücksetzen der Appliance auf eine vorherige Version.

Nicht alle früheren Versionen sind verfügbar:

Upgrades führen zu einer unidirektionalen Transformation wichtiger Subsysteme, die den Reversion-Prozess verkomplizieren. Cisco zertifiziert spezifische Versionen der Versionen CASE, Sophos, VOF und McAfee zu AsyncOS, um eine nahtlose Umkehr sicherzustellen, dass Zielversionen von Cisco qualifiziert werden müssen. Es werden nicht alle früheren Builds verfügbar sein. Es gibt nur begrenzte, vorab festgelegte Reversionsmöglichkeiten.

Die Reversion dauert so lange, wie das Upgrade durchgeführt wird:

Um Dateisystemressourcen zu speichern, werden Installationsmedien nicht auf Appliances gespeichert. Der Reversionsvorgang erfordert Streaming, Herunterladen von Dateien und die Installation.

Reversion ist destruktiv:

Alle Nachrichten in der Arbeitswarteschlange oder in der Zustellungwarteschlange werden gelöscht. Alle Berichtsdaten und Protokolldateien werden gelöscht. Nur Feature-Schlüsseldaten bleiben erhalten, alle anderen Konfigurationen gehen verloren. Alle Datenbanken und Nachrichtenverfolgungsdaten gehen verloren. Sämtliche Spam-Quarantäne-Nachrichten und Daten zu Listen sicherer Absender/Sperrlisten für Endbenutzer. Nur die Netzwerkeinstellungen bleiben erhalten. Sie müssen über Konsolenzugriff auf den Posteingang verfügen, da die IP-Adresse auf den Standardwert 192.168.42.42 zurückgesetzt wird. Durch das Zurücksetzen des Geräts wird ein sofortiger Neustart durchgeführt. Nach dem Neustart wird die Einheit neu initialisiert und wieder zur gewünschten Version neu gestartet.

Bereiten Sie vor dem Upgrade auf eine mögliche Reversion vor:

Als Best Practice empfiehlt Cisco, sich auf ein Upgrade vorzubereiten. Gehen Sie dazu wie folgt vor:

1. Deaktivieren Sie das Kontrollkästchen XML-Konfigurationsdatei speichern (ohne Kennwörter).
2. Wenn Sie die Funktion "Listen sicherer Absender/Sperrlisten" verwenden, exportieren Sie die Liste aus dem Feld
3. Aussetzen der Listener

4. Löschen der Mailwarteschlange und der Zustellwarteschlange
5. Exportieren der Datenbank der Spam-Quarantäne für Listen sicherer Absender/Sperrlisten auf ein anderes System (falls zutreffend)

Vergessen Sie nicht, die Listener nach dem Upgrade erneut zu aktivieren.

Vorgehensweise:

1. Melden Sie sich bei der CLI an.
2. Geben Sie "vertauschen" ein.
3. ESA stellt ein Menü von bereits installierten, qualifizierten Versionen vor.
4. Version zurücksetzen auswählen
5. Neustart
6. Erster Neustart - System wird hochgefahren, Datenträger gelöscht, Datenträger deinstalliert
7. Zweiter Neustart (automatisch) - System wird mit ausgewählter Version gestartet, initialisiert neue Daten, Appliance startet
8. Laden Sie die XML-Konfigurationsdatei, die Sie während des Upgrades gespeichert haben.
9. Importieren Sie ggf. die Datei Listen sicherer Absender/Sperrlisten.