

Come eseguire il rollback dalla versione corrente di AsyncOS su Cisco Email Security Appliance?

Domanda:

Ambiente: Cisco Email Security Appliance (ESA), tutte le versioni di AsyncOS

Riepilogo:

In AsyncOS, la funzione di ripristino consente di ripristinare una versione precedente dell'accessorio.

Non tutte le versioni precedenti saranno disponibili:

Gli aggiornamenti causano una trasformazione unidirezionale dei sottosistemi chiave che complica il processo di ripristino. Cisco certifica versioni specifiche di CASE, Sophos, VOF e McAfee su versioni AsyncOS, per garantire una conversione fluida, le build di versione target devono essere certificate da Cisco. Non tutte le compilazioni precedenti saranno disponibili; esisteranno soltanto possibilità di conversione limitate e predeterminate.

L'operazione di inversione richiede un tempo di aggiornamento pari a:

Per risparmiare le risorse del file system, i supporti di installazione non vengono conservati sugli accessori. Il processo di reversione richiede lo streaming, lo scaricamento completo e l'installazione.

L'inversione è distruttiva:

Tutti i messaggi nella coda di lavoro o nella coda di recapito vengono eliminati. Tutti i dati di reporting e i file di log vengono eliminati. Solo che i dati relativi alle chiavi delle feature vengono mantenuti e tutte le altre configurazioni vengono perse. Tutti i database e i dati di verifica messaggi andranno persi. Tutti i messaggi di quarantena della posta indesiderata e i dati dell'elenco indirizzi attendibili/elenco indirizzi bloccati dell'utente finale. Verranno mantenute solo le impostazioni di rete. È necessario disporre dell'accesso da console al box post-revert poiché l'IP tornerà al valore predefinito di 192.168.42.42. Il ripristino del dispositivo causa un riavvio immediato. Dopo il riavvio, l'accessorio viene reinizializzato e riavviato alla versione desiderata.

Preparare un'eventuale reversione prima dell'aggiornamento:

Come buona norma, Cisco consiglia di prepararsi per un aggiornamento attenendosi alla seguente procedura:

1. Salvare il file di configurazione XML (senza maschera delle password)
2. Se si utilizza la funzione Safelist/Blocklist, esportare la casella elenco
3. Sospendere i listener
4. Svuotare la coda di posta e la coda di recapito
5. Esportare il database dell'elenco di sicurezza/elenco di blocco per la quarantena della posta indesiderata in un altro computer (se applicabile)

Non dimenticare di riattivare i listener dopo l'aggiornamento.

Procedura:

1. Accedere alla CLI
2. Digitare "revert"
3. L'ESA presenterà un menu di versioni qualificate installate in precedenza
4. Selezionare la versione di ripristino
5. Riavvio
6. Primo riavvio - il sistema si accende, cancella i dischi, disimballaggio supporti di installazione
7. Secondo riavvio (automatico) - il sistema viene fornito utilizzando la versione selezionata, inizializza i dati aggiornati, l'accessorio viene avviato
8. Caricare il file di configurazione XML salvato durante l'aggiornamento
9. Se necessario, importare il file elenco indirizzi attendibili/elenco indirizzi attendibili