Risoluzione dei problemi relativi alla quarantena centralizzata PVO su ESA e SMA

Sommario

Introduzione

Questo documento descrive come risolvere i problemi di consegna e connessione quando è abilitata la quarantena centralizzata per policy, virus ed epidemie.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Email Security Appliance (ESA) con AsyncOS 8.1 o versioni successive
- Security Management Appliance (SMA) con AsyncOS 8.0 o versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La funzionalità di quarantena Centralized Policy, Virus and Outbreak (PVO) è stata introdotta in AsyncOS 8.0 (ESA) / 8.1 (SMA). Questa funzionalità richiede ulteriori requisiti di connettività di rete e pone nuove sfide per la risoluzione dei problemi.

Comprendere la comunicazione

- La comunicazione CPQ utilizza SMTP, ma con alcuni comandi aggiuntivi per il trasferimento dei metadati
- L'SMA ascolterà le connessioni sull'interfaccia e sulla porta definite in Centralized Services ->

Policy, Virus and Outbreak Quarantines. Per impostazione predefinita, la porta è 7025, ma potrebbe essere stata modificata dall'utente admin.
- L'ESA ascolterà le connessioni sull'interfaccia e sulla porta definite in Security Services -> Policy, Virus and Outbreak Quarantines. Anche in questo caso, per impostazione predefinita, la porta è 7025, ma potrebbe essere stata modificata dall'utente admin.
- L'SMA utilizza anche SSH (tramite il client dei comandi) per ottenere le informazioni di configurazione dalle ESA. In particolare, viene utilizzato quando l'SMA consegna messaggi di posta elettronica all'ESA. Lo SMA utilizzerà il protocollo SSH per interrogare la configurazione ESA e determinare l'interfaccia o la porta a cui inviare l'e-mail rilasciata.

Listener

- Sia l'ESA che l'SMA avranno un listener nascosto chiamato 'cpq_listener' che resterà in ascolto sulla porta specificata.
- Questi listener possono essere visualizzati nel file di configurazione. Ad esempio:

```
<listener>
     <listener_name>cpq_listener</listener_name>
     <protocol>CPQ</protocol>
     <interface_name>Incoming Mail</interface_name>
     <port>7025</port>
     <listen_queue_size>50</listen_queue_size>
     <type>private</type>
     <hat>
$RELAYED
   RELAY {}
$BLOCKED
   REJECT {}
RELAYLIST:
   10.1.2.3
       $RELAYED (Only select hosts can relay from this box)
ALL
   $BLOCKED (Everyone else)
     </hat>
     <rat>
       <rat_entry>
         <rat_address>ALL</rat_address>
         <access>ACCEPT</access>
       </rat_entry>
     </rat>
```

- Questi listener verranno sospesi se l'utente amministratore utilizza 'suspendlisteners all' o 'suspend'. Se la porta non accetta connessioni, verificare che lo stato del sistema sia 'offline' e, se necessario, riprenderla.

Risoluzione dei problemi relativi alla consegna da ESA a SMA

- Verificare che l'ESA sia in grado di connettersi all'SMA sulla porta e sull'interfaccia configurate. A tale scopo, è possibile utilizzare telnet. Se la comunicazione ha esito positivo, si dovrebbe ottenere un banner 220.
- L'ESA disporrà di un oggetto di destinazione denominato 'the.cpq.host', che contiene i messaggi durante la relativa coda per il recapito all'SMA. È possibile visualizzare questo messaggio utilizzando 'tophosts' o Monitor -> Stato recapito. Non è possibile utilizzare

'hoststatus' con tale elemento, ma è possibile utilizzare 'showcontacts' e 'deleterecipients' se necessario.

Risoluzione dei problemi relativi alla consegna da SMA a ESA

- Verificare che l'SMA sia in grado di connettersi all'ESA sulla porta e sull'interfaccia configurate. Anche in questo caso, è possibile utilizzare telnet e visualizzare il banner 220 se l'operazione riesce.
- Quando si utilizzano i cluster, è importante che l'interfaccia definita a livello di cluster in Security Services -> Policy, Virus and Outbreak Quarantines sia disponibile per tutti gli accessori a livello di computer. (selezionare Rete -> Interfacce IP).
- L'SMA avrà un oggetto di destinazione chiamato 'the.cpq.release.host' che contiene i messaggi rilasciati mentre sono in coda per il recapito all'ESA. Per visualizzarlo, utilizzare 'tophosts'. Non sembra funzionare con 'hoststatus' o 'showreceive' e non è stato testato con 'deleterecipients', ma probabilmente non funziona.
- Possono inoltre verificarsi problemi nella comunicazione SSH tra l'SMA e l'ESA. Questi problemi non sono sempre necessariamente basati sulla rete, ad esempio in CSCus29647 un componente interno dell'SMA non è più operativo. Problemi di questo tipo vengono in genere visualizzati come errori dell'applicazione nei log di posta e possono in genere essere risolti riavviando l'SMA.

TLS/Certificati

- Tutte le connessioni CPQ in entrambe le direzioni si basano su TLS, e di conseguenza la configurazione cifratura può svolgere un ruolo.
- Affinché la connessione TLS abbia esito positivo, il dispositivo che apre la connessione deve essere in grado di verificare che il dispositivo ricevente stia utilizzando il certificato CPQ nascosto. È possibile che l'operazione non riesca se l'accessorio esegue la negoziazione di una cifratura anonima. Nei log viene visualizzato un messaggio simile al seguente:

```
Mon Apr  1 12:00:00 2014 Info: New SMTP DCID 123456 interface 10.0.0.2 address 10.0.0.1 port
7025
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS failed: verify error: no certificate from
server
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS was required but could not be successfully
negotiated
```

- Per risolvere questi problemi, è sufficiente rimuovere le cifrature anonime dall'elenco di cifratura in uscita. A tale scopo, aggiungere ':-aNULL' alla fine dell'elenco di cifratura. Ad esempio: HIGH:MEDIO:**-NULL**

File di log

- Se l'SMA dispone di una sottoscrizione ai log di posta (impostazione predefinita), è possibile esaminare i log di posta per ottenere ulteriori informazioni.
- Il CPQ che riceve gli eventi avrà questo aspetto sia per i messaggi messi in quarantena al SMA che per i messaggi rilasciati all'ESA

```
New CPQ ICID 12345 interface Management (10.10.10.1) address 10.10.20.1 reverse dns host
unknown verified no
```

- Èpossibile cercare questi eventi utilizzando grep, ad esempio: grep "CPQ ICID" mail_logs
- Gli eventi di consegna CPQ, sia in quarantena dall'ESA che in quarantena dal SMA, sono simili a qualsiasi altra consegna, con l'eccezione che la porta personalizzata è elencata e alcune righe includono la parola 'Centralized Policy Quarantine'. Esempio:

```
Fri Sep 13 15:08:02 2013 Info: New SMTP DCID 12345 interface 10.10.20.1 address 10.10.10.1
port 7025
Fri Sep 13 15:08:02 2013 Info: DCID 12345 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Fri Sep 13 15:08:02 2013 Info: Delivery start DCID 12345 MID 23456 to RID [0] to Centralized
Policy Quarantine
Fri Sep 13 15:08:02 2013 Info: Message done DCID 12345 MID 23456 to RID [0] (centralized
policy quarantine)
Fri Sep 13 15:08:07 2013 Info: DCID 12345 close
```

- Èpossibile trovare questi eventi utilizzando grep per cercare la porta, ad esempio: log_di_posta "porta 7025" grep

Pulsante ESA 'Attiva' disattivato

Quando si tenta di abilitare il PVO sull'ESA, il pulsante 'Abilita' è disattivato, nonostante tutte le operazioni di configurazione dei prerequisiti siano state completate. Quando l'ESA visualizza la pagina PVO, comunica con l'SMA sulla porta 7025 per verificare che la configurazione sia pronta per essere abilitata. Se la comunicazione non riesce, il pulsante 'Abilita' verrà disabilitato. È possibile risolvere questo problema proprio come qualsiasi comunicazione ESA -> SMA port 7025 saltando per "port 7025" sull'ESA. Per ulteriori informazioni, fare riferimento alla nota tecnica riportata in Informazioni correlate.

Informazioni correlate

- Requisiti per la Migrazione guidata di UCS quando l'ESA è raggruppata
- Non è possibile abilitare la policy di centralizzazione ESA, la quarantena per virus ed epidemie (PVO)