Fehlerbehebung: Zentralisierter PVO-Quarantäne auf ESA und SMA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie bei Bereitstellungs- und Verbindungsproblemen behoben werden können, wenn die zentrale Richtliniendurchsetzung, Viren- und Outbreak-Quarantäne aktiviert ist.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- E-Mail Security Appliance (ESA) mit AsyncOS 8.1 oder höher
- Security Management Appliance (SMA) mit AsyncOS 8.0 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Funktion für zentralisierte Richtlinien, Virus und Outbreak (PVO)-Quarantänen wurde in AsyncOS 8.0 (ESA)/8.1 (SMA) eingeführt. Diese Funktion stellt zusätzliche Netzwerkanbindungsanforderungen und neue Herausforderungen bei der Fehlerbehebung.

Verständnis der Kommunikation

- Die CPQ-Kommunikation verwendet SMTP, jedoch mit einigen zusätzlichen Befehlen zum Übertragen von Metadaten

- Die SMA überwacht Verbindungen auf der Schnittstelle und dem Port, die unter Zentrale Dienste -> Richtlinie, Virus- und Outbreak-Quarantäne definiert sind. Standardmäßig ist der Port 7025, dies kann jedoch vom Administrator-Benutzer geändert worden sein!
- Die ESA überwacht Verbindungen auf der Schnittstelle und dem Port, die unter Sicherheitsdienste -> Richtlinie, Virus- und Outbreak-Quarantäne definiert sind. Auch hier ist der Port standardmäßig 7025, aber dies kann vom Administrator-Benutzer geändert worden sein!
- Die SMA verwendet außerdem SSH (über den Befehls-Client), um Konfigurationsinformationen von den ESAs abzurufen. Dies wird insbesondere verwendet, wenn die SMA der ESA veröffentlichte E-Mails zustellt. Die SMA verwendet SSH, um die ESA-Konfiguration abzufragen und festzustellen, an welche Schnittstelle bzw. welchen Port die freigegebene E-Mail gesendet werden soll.

Listeners

- Sowohl die ESA als auch die SMA verfügen über einen ausgeblendeten Listener namens "cpq_listener", der den angegebenen Port überwacht.
- Diese Listener sind in der Konfigurationsdatei sichtbar. Beispiel:

```
<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>
```

- Diese Listener werden ausgesetzt, wenn der Admin-Benutzer 'Suspendierende Listener alle' oder 'Suspendierende' verwendet. Wenn der Port keine Verbindungen akzeptiert, sollten Sie überprüfen, ob der Systemstatus "offline" ist, und bei Bedarf fortfahren.

Fehlerbehebung bei der Bereitstellung von ESA zu SMA

- Überprüfen Sie, ob die ESA über den konfigurierten Port und die konfigurierte Schnittstelle eine Verbindung mit der SMA herstellen kann. Dies kann über Telnet erfolgen. Wenn die Kommunikation erfolgreich ist, sollten Sie ein 220-Banner bekommen.

- Die ESA verfügt über ein Zielobjekt namens "the.cpq.host", das Nachrichten enthält, während sie zur Übermittlung an die SMA in die Warteschlange gestellt werden. Sie können dies über "tophosts" oder "Monitor -> Delivery Status" sehen. Sie können nicht 'hoststatus' verwenden, aber Sie können bei Bedarf 'showhosts' und 'deleterecipients' verwenden.

Fehlerbehebung bei der Bereitstellung von SMA zu ESA

- Stellen Sie sicher, dass die SMA-Einheit über den konfigurierten Port und die konfigurierte Schnittstelle eine Verbindung zur ESA herstellen kann. Auch hier können Sie Telnet verwenden und sehen das 220-Banner, wenn erfolgreich.
- Bei der Verwendung von Clustern ist es wichtig, dass die auf Clusterebene unter Sicherheitsdienste -> Richtlinie, Virus- und Outbreak-Quarantäne definierte Schnittstelle für alle Appliances auf Computerebene vorhanden ist. (Aktivieren Sie Netzwerk -> IP-Schnittstellen).
- Die SMA verfügt über ein Zielobjekt namens "the.cpq.release.host", das freigegebene Nachrichten enthält, während sie zur Übermittlung an die ESA in die Warteschlange gestellt werden. Sie können dies mithilfe von 'tophosts' sehen. Dies scheint nicht mit 'hoststatus' oder 'showhosts' zu funktionieren, und ich habe noch keine 'Deleterecipients' getestet, aber das funktioniert wahrscheinlich auch nicht.
- Auch bei der SSH-Kommunikation zwischen SMA und ESA können Probleme auftreten. Diese Probleme müssen nicht immer netzwerkbasiert sein, z. B. in CSCus29647 ist eine interne Komponente der SMA außer Betrieb. Probleme wie diese werden in der Regel als Anwendungsfehler in den E-Mail-Protokollen angezeigt und können in der Regel durch einen Neustart des SMA behoben werden.

TLS/Zertifikate

- Alle CPQ-Verbindungen in beide Richtungen basieren auf TLS. Daher kann die Verschlüsselungskonfiguration eine Rolle spielen.
- Damit die TLS-Verbindung hergestellt werden kann, muss das Gerät, das die Verbindung öffnet, überprüfen können, ob das empfangende Gerät unser verstecktes CPQ-Zertifikat verwendet. Dies kann fehlschlagen, wenn die Appliance einen anonymen Chiffren aushandelt. Dies wird in den Protokollen wie folgt angezeigt:

```
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
```

- Sie können diese Probleme beheben, indem Sie einfach anonyme Chiffren aus der Liste der ausgehenden Verschlüsselungen entfernen. Dies geschieht durch Hinzufügen von ':-aNULL' am Ende der Verschlüsselungsliste. Beispiel: HOCH:MITTEL:**-NULL**

Protokolldatei

- Wenn die SMA über ein Abonnement für Mail-Protokolle verfügt (dies ist standardmäßig der Fall), können Sie die E-Mail-Protokolle überprüfen, um weitere Informationen zu sammeln.

- CPQ-Empfangsereignisse sehen für Nachrichten, die in die SMA-Quarantäne gestellt werden, und für Nachrichten, die an die ESA weitergeleitet werden, wie folgt aus:

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

- Sie können diese Ereignisse mithilfe von grep suchen, z. B.: grep "CPQ ICID" mail_logs
- CPQ-Bereitstellungsereignisse, sowohl die Quarantäne der ESA als auch die Freigabe der Quarantäne aus der SMA, ähneln jeder anderen Zustellung, mit der Ausnahme, dass der benutzerdefinierte Port aufgeführt ist und einige Posten die Überschrift "Zentrale Richtlinienquarantäne" enthalten. Beispiel unten:

```
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
```

- Sie können diese Ereignisse mithilfe von grep finden, um nach dem Port zu suchen, z. B.: grep "port 7025" mail_logs

ESA-Schaltfläche "Aktivieren" deaktiviert

Beim Versuch, PVO auf der ESA zu aktivieren, wird die Schaltfläche "Enable" (Aktivieren) trotz der erforderlichen Konfiguration möglicherweise abgeblendet angezeigt. Wenn die ESA die PVO-Seite anzeigt, kommuniziert sie mit dem SMA über Port 7025, um zu überprüfen, ob die Konfiguration aktiviert werden kann. Wenn diese Kommunikation fehlschlägt, wird die Schaltfläche 'Aktivieren' deaktiviert. Sie können diese Probleme wie jede ESA -> SMA-Port 7025-Kommunikation beheben, indem Sie auf der ESA "Port 7025" (Port 7025) als Fehlerbehebung verwenden. Weitere Informationen finden Sie im technischen Hinweis, der unter Zugehörige Informationen aufgeführt ist.

Zugehörige Informationen

- Anforderungen für den PVO Migration Wizard (PVO-Migrationsassistent) bei Clustering der ESA
- ESA Zentralisierung von Policy, Virus und Outbreak Quarantine (PVO) kann nicht aktiviert werden