Probleemoplossing gecentraliseerde PVO-quarantaine op ESA en SMA

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij het leveren van uw oplossing en bij het oplossen van problemen wanneer een gecentraliseerd beleid, een virus en een uitbraken in de lucht zijn.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- E-mail security applicatie (ESA) met AsyncOS 8.1 of hoger
- Security Management-applicatie (SMA) met AsyncOS 8.0 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De optie Gecentraliseerde Policy, Virus en Outbreak (PVO) Quarantines is geïntroduceerd in AsyncOS 8.0 (ESA) / 8.1 (SMA). Deze optie heeft extra vereisten voor netwerkconnectiviteit en stelt een aantal nieuwe uitdagingen voor het oplossen van problemen voor.

Begrijp de communicatie

- CPQ communicatie gebruikt MTP, maar met sommige extra opdrachten voor het overdragen van metagegevens
- SMA zal luisteren naar verbindingen op de interface en poort die worden gedefinieerd onder

Gecentraliseerde services -> Beleids-, virussen- en Outdoorkleding. Standaard is de poort 7025 maar deze kan door de beheerder gewijzigd zijn!
- Het ESA zal luisteren naar aansluitingen op de interface en poort gedefinieerd onder Security Services -> Policy, Virus en Outbreak Quarantines. Opnieuw, standaard, is de poort 7025, maar dit kan door de beheerder gewijzigd zijn!
- De SMA gebruikt ook SSH (via opdrachtclient) om configuratieinformatie van de ESA's te verkrijgen. Dit wordt met name gebruikt wanneer de SMA vrijgegeven e-mails aan de ESA aflevert. De SMA zal SSH gebruiken om de ESA-configuratie te bevragen en te bepalen welke interface/poort wordt gebruikt om de vrijgegeven e-mail aan te leveren.

Lijsten

- Zowel de ESA als de SMA zullen een verborgen luisteraar hebben genaamd 'cpq_lister' die zal luisteren op de gespecificeerde poort.
- Deze luisteraars kunnen worden gezien in het configuratiebestand. Bijvoorbeeld:

```
<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>
```

- Deze luisteraars worden geschorst als de beheerder 'alle luisteraars schorst' of 'schorst' gebruikt. Als de haven geen verbindingen accepteert, zou u moeten controleren of de systeemstatus "offline" is en indien nodig hervat.

Levering van probleemoplossing van ESA aan SMA

- Controleer of de ESA op de geconfigureerde poort en interface een verbinding met de SMA kan maken. Dit kan worden gedaan met telnet. Een 220-banner als de communicatie succesvol is.
- Het ESA zal een doelobject hebben genaamd 'the.cpq.host', dat berichten bevat terwijl ze in de wachtrij staan voor levering aan het SMA. U kunt dit zien met 'tophosts' of monitor -> Delivery Status. Je kunt er geen "hoststatus" mee gebruiken, maar je kunt 'showontvangers'

en 'deleterecipients' indien nodig gebruiken.

Levering van probleemoplossing van SMA aan ESA

- Controleer of de SMA in de geconfigureerde poort en interface op de ESA kan worden aangesloten. Opnieuw, kunt u telnet gebruiken en zal de 220 banner zien indien succesvol.
- Bij gebruik van clusters is het belangrijk dat de interface die op clusterniveau is gedefinieerd onder Beveiligingsservices -> Beleids-, virussen- en uitbraakstandaarden bestaan voor alle apparaten op machineniveau. (Controleer netwerk -> IP-interfaces).
- De SMA zal een doelobject hebben dat "the.cpq.release.host" wordt genoemd en dat vrijgegeven berichten bevat terwijl ze in de wachtrij staan voor levering aan de ESA. Je kunt dit zien met 'tophosts'. Dit lijkt niet te werken met "hoststatus" of "showontvangers", en ik heb er geen "deleterecipients" mee getest, maar dat werkt waarschijnlijk ook niet.
- Er kunnen ook problemen zijn met de communicatie tussen het SMA en het ESA over SSH. Deze kwesties zijn niet altijd netwerkgebaseerd, bijvoorbeeld in CSCus29647 wordt een interne component van de SMA buiten werking gesteld. Vraagstukken zoals deze verschijnen meestal als applicatiefouten in de maillogbestanden en kunnen doorgaans worden opgelost door de SMA te hervatten.

TLS/certificaten

- Alle CPQ-verbindingen in beide richtingen zijn afhankelijk van TLS, zodat de algoritmische configuratie een rol kan spelen.
- Om de TLS-verbinding te laten slagen, moet het apparaat dat de verbinding opent, kunnen verifiëren dat het ontvangende apparaat ons verborgen CPQ-certificaat gebruikt. Het is mogelijk dat dit mislukt als het apparaat over een anoniem algoritme onderhandelt. Dit staat in de blogs als iets dergelijks:

```
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
```

- U kunt deze problemen oplossen door anonieme ciphers uit de lijst van de vertrekkende leveringspaconcentratie te verwijderen, wat gebeurt door 'a-aNULL' aan het einde van de lijst van het algoritme toe te voegen. Bijvoorbeeld: HOOG:MEDIUM:**-NULL**

Logbestand

- Als SMA een abonnement op maillogs heeft (dit gebeurt standaard), kunt u de maillogbestanden bekijken om extra inzicht te verkrijgen.
- CPQ-berichten die worden ontvangen, zien er zo uit voor zowel berichten die in quarantaine worden geplaatst met de SMA als berichten die worden vrijgegeven aan de ESA

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

- U kunt deze gebeurtenissen zoeken met behulp van grip, bijvoorbeeld: g "CPQ ICID" mail_logs
- CPQ-leveringsgebeurtenissen, zowel quarantaine vanuit het ESA als vrijgave van quarantaine vanuit het SMA, lijken op elke andere levering, met uitzondering van het feit dat de douanehaven is vermeld en enkele regels omvatten de term "gecentraliseerde beleidsquarantaine". Voorbeeld hieronder:

```
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
```

- U kunt deze gebeurtenissen vinden door grep te gebruiken om naar de haven te zoeken, bijvoorbeeld: gros "port 7025" mail_logs

De knop ESA 'Enable' uitgeschakeld

Wanneer u probeert PVO op de ESA in te schakelen, ziet u wellicht dat de knop Enable wordt weergegeven, ondanks dat alle vereiste configuratie is voltooid. Wanneer het ESA de PVO-pagina weergeeft, communiceert het met het SMA over poort 7025 om te controleren of de configuratie klaar is om te worden ingeschakeld. Als deze communicatie mislukt, wordt de knop 'Inschakelen' uitgeschakeld. U kunt dit oplossen net zoals elke ESA -> SMA poort 7025 communicatie door "port 7025" op de ESA te typen. Raadpleeg voor meer informatie de Technische opmerking die in Verwante informatie staat.

Gerelateerde informatie

- Vereisten voor de PVO-migratiewizard wanneer ESA zich heeft gevestigd
- ESA Centralizing Policy, Virus en Outbreak Quarantine (PVO) kunnen niet worden ingeschakeld