Troubleshoot a centralisé la quarantaine PVO sur l'ESA et le SMA

Contenu

Introduction

Ce document décrit comment dépanner la livraison et des problèmes de connexion quand le quarnatine centralisé policiy, de virus et d'épidémie est activé.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité du courrier électronique (ESA) avec AsyncOS 8.1 ou plus tard
- Appliance de Gestion de la sécurité (SMA) avec AsyncOS 8.0 ou plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Centralisé stratégie, virus et épidémie (PVO) quarantaine caractéristique était introduit dans AsyncOS 8.0) (ESA/8.1 (SMA). Cette caractéristique a des conditions requises supplémentaires de connexion réseau, et lance quelques nouveaux défis pour le dépannage.

Comprenez la transmission

- La transmission CPQ utilise le SMTP, mais avec quelques commandes supplémentaires pour transférer des métadonnées
- Le SMA écoutera des connexions sur l'interface et mettra en communication défini sous des

services centralisés - > des quarantaines de stratégie, de virus et d'épidémie. Par défaut, le port est 7025, mais ceci a pu avoir été changé par l'utilisateur d'admin !
- L'ESA écoutera des connexions sur l'interface et mettra en communication défini sous des Services de sécurité - > des quarantaines de stratégie, de virus et d'épidémie. De nouveau, par défaut, le port est 7025, mais ceci a pu avoir été changé par l'utilisateur d'admin !
- Le SMA emploie également le SSH (par l'intermédiaire du client de commande) pour obtenir les informations de configuration de l'ESAs. En particulier, ceci est utilisé quand le SMA fournit les emails libérés à l'ESA. Le SMA emploiera le SSH pour questionner la configuration ESA et pour déterminer à quels interface/port pour fournir l'email sorti.

Auditeurs

- L'ESA et le SMA auront un auditeur masqué appelé le « cpq_listener » qui écoutera sur le port spécifié.
- Ces auditeurs peuvent être vus dans le fichier de configuration. Exemple :

```
<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>
```

- Ces auditeurs seront interrompus si les utilisations « suspendlisteners tous » d'utilisateur d'admin ou « s'interrompent ». Si le port ne reçoit pas des connexions, vous devriez vérifier si l'état du système est « hors ligne » et reprise si nécessaire.

Dépannez la livraison de l'ESA à SMA

- Vérifiez que l'ESA peut se connecter au SMA sur le port et l'interface configurés. Ceci peut être fait utilisant le telnet. Vous devriez obtenir une bannière 220 si la transmission est réussie.
- L'ESA aura un objet de destination appelé le « the.cpq.host », qui contient des messages tandis qu'ils sont alignés pour la livraison au SMA. Vous pouvez voir ceci utilisant des « tophosts » ou surveiller - > état de la livraison. Vous ne pouvez pas utiliser le

« hoststatus » avec lui, mais vous pouvez utiliser des « showrecipients » et des « deleterecipients » s'il y a lieu.

Dépannez la livraison de SMA à l'ESA

- Vérifiez que le SMA peut se connecter à l'ESA sur le port et l'interface configurés. De nouveau, vous pouvez utiliser le telnet et verrez la bannière 220 si réussi.
- En utilisant des batteries, il est important que l'interface définie au niveau de batterie sous des Services de sécurité - > les quarantaines de stratégie, de virus et d'épidémie existe pour toutes les appliances au niveau d'ordinateur. (réseau de contrôle - > interfaces IP).
- Le SMA aura un objet de destination appelé le « the.cpq.release.host » qui contient les messages libérés tandis qu'ils sont alignés pour la livraison à l'ESA. Vous pouvez voir ceci utilisant des « tophosts ». Ceci ne semble pas fonctionner avec le « hoststatus » ou les « showrecipients », et je n'ai pas testé des « deleterecipients » avec lui, mais ceci ne fonctionne pas probablement l'un ou l'autre.
- Il peut également y avoir des problèmes avec la transmission de SSH entre le SMA et l'ESA. Ces questions ne sont pas toujours nécessairement réseau basé, par exemple dans CSCus29647 un composant interne du SMA sort de l'exécution. Les questions de ce type apparaîtront typiquement car des défauts d'application dans les logs de messagerie, et peuvent habituellement être résolues en redémarrant le SMA.

TLS/Certificates

- Toutes les connexions CPQ dans l'un ou l'autre de direction se fondent sur le TLS, et en conséquence la configuration de chiffrement peut jouer un rôle.
- Pour que la connexion de TLS réussisse, le périphérique ouvrant la connexion doit pouvoir vérifier que le périphérique récepteur utilise notre certificat hiddent CPQ. Il est possible que ceci échoue si l'appliance négocie un chiffrement anonyme. Ceci apparaîtrait dans les logs en tant que n'importe quoi de pareil :

```
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
```

- Vous pouvez réparer ces questions en retirant simplement des chiffrements anonymes de la liste sortante de chiffrement de la livraison, qui est faite en ajoutant « `: - aNULL` » à la fin de la liste de chiffrement. Exemple : `HAUTE : SUPPORT : - aNULL`

Fichier journal

- Si le SMA a un abonnement de logs de messagerie (il fait par défaut), vous pouvez passer en revue les logs de messagerie pour recueillir la vue supplémentaire.
- CPQ recevant des événements ressemblera à ceci pour des messages étant mis en quarantaine au SMA et des messages libérés à l'ESA

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

- Vous pouvez rechercher ces événements utilisant le grep, exemple : `grep mail_logs « CPQ ICID »`
- Les événements, chacun des deux qui mettent en quarantaine de l'ESA et la release de la livraison CPQ de la quarantaine de SMA, semblent semblables à n'importe quelle autre livraison, excepté que le port fait sur commande est répertorié et quelques lignes incluent le verbiage « quarantaine centralisée de stratégie ». Exemple ci-dessous :

```
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
```

- Vous pouvez trouver ces événements à l'aide du grep au seach pour le port, exemple : `mail_logs du port 7025" de grep «`

Bouton de « enable » ESA désactivé

En tentant d'activer PVO sur l'ESA, vous pouvez constater que le bouton de « enable » est grisé, en dépit de toute la configuration de condition préalable étant terminée. Quand l'ESA affiche la page PVO, il communique avec le SMA au-dessus du port 7025 pour vérifier que la configuration est prête à être activée. Si cette transmission échoue, le bouton de « enable » sera désactivé. Vous pouvez dépanner ceci juste comme n'importe quel ESA - > transmission du port 7025 SMA par grepping pour le « port 7025" sur l'ESA. Le pour en savoir plus se rapportent au TechNote répertorié dans les informations relatives.

Informations connexes

- Conditions requises pour l'assistant de transfert PVO quand l'ESA est groupé
- La stratégie de centralisation ESA, le virus, et la quarantaine d'épidémie (PVO) ne peuvent pas être activés