troubleshoot集中了在ESA和SMA的PVO检疫

目录

简介

当集中化policiy，病毒和爆发quarnatine启用时，本文描述如何排除故障交付和连接问题。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 给安全工具(ESA)发电子邮件有AsyncOS 8.1或以上的
- 安全管理设备(SMA)有AsyncOS 8.0或以上的

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

集中化策略，病毒和爆发(PVO)检疫功能是介绍在AsyncOS 8.0 (ESA)/8.1 (SMA)。 此功能有另外的网络连通性需求，并且摆在一些排除故障的新建的挑战。

了解通信

- CPQ通信以一些额外的命令使用SMTP，但是转接元数据
- SMA将细听在接口和端口的连接定义在集中式服务下- >Policy、病毒和爆发检疫。 默认情况下，端口是7025，但是这可能由管理员用户更改!
- ESA将细听在接口和端口的连接定义在安全服务下- >Policy、病毒和爆发检疫。 再次，默认情况下，端口是7025，但是这可能由管理员用户更改!
- SMA也使用SSH (通过client命令)从ESAs获得配置信息。 特别是，这，当SMA传送发布的电子邮件对ESA时，使用。 SMA将使用SSH查询ESA配置和确定传送发布的电子邮件的哪接口/端口。

听众

- ESA和SMA将有隐藏的监听程序呼叫‘在指定的端口将侦听的cpq_listener’。
- 这些监听程序在配置文件能被看到。 例如：

```
<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>
```

- 这些监听程序将被暂停，如果管理员用户用途‘suspendlisteners全部’或‘挂起’。 如果端口不接受连接，您应该检查系统状态若需要是否是‘脱机’和恢复。

排除故障交付从ESA到SMA

- 检查ESA能连接到在配置端口和接口的SMA。 使用telnet，这可以执行。 如果通信是成功的，您应该获得220标语。
- ESA将有呼叫‘the.cpq.host的’一目的地目标，包含消息，当他们为对SMA时的交付排队。 您能看到此使用‘tophosts’或监控- >传送状态。 您不能以它使用‘hoststatus’，但是您能使用‘showrecipients’和‘deleterecipients’如果需要。

排除故障交付从SMA到ESA

- 检查SMA能连接到在配置端口和接口的ESA。 再次，您能使用telnet，并且请参阅220标语，如果成功。
- 当曾经集群时，重要的是接口定义在集群级别下面安全服务- >Policy、病毒和爆发检疫为所有设备存在级的计算机。 (检查Network-> IP接口)。
- SMA wil有呼叫‘包含发布的消息的the.cpq.release.host的’一目的地目标，当他们为对ESA时的交付排队。 您能看到此使用‘tophosts’。 这不看上去与‘hoststatus’或‘showrecipients一起使用’，并且我未测试‘deleterecipients’与它，但是这很可能不运作二者之一。
- 可能也有与SSH通信的问题SMA和ESA之间。 这些问题总是不必要网络基础，例如在 CSCus29647 SMA的内部组件出去操作。 问题例如这些将典型地出现作为在邮件日志的应用程序故障，并且可能通过重新启动SMA通常解决。

TLS/Certificates

- 所有CPQ连接在任何一个方向依靠TLS，结果，并且密码器配置能扮演角色。
- 为了TLS连接能成功，打开连接的设备一定能验证接收设备使用我们的hiddent CPQ证书。 如果设备协商一匿名密码器，发生故障此是可能的。 这在日志将出现作为如此物：

```
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
```

- 您能通过删除匿名密码器调整这些问题从流出的交付密码器列表，由添加完成‘- aNULL’对结尾的密码器列表。 例如：**- aNULL**

日志文件

- 如果SMA有邮件日志订阅(默认情况下)，您能检查邮件日志采集另外的见解。
- 接收事件如下所示:两个消息被检疫对SMA和消息的CPQ发布对ESA

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

- 使用grep，您能搜索这些事件，示例：grep “CPQ ICID” mail_logs
- CPQ从检疫的交付事件，两个检疫从ESA的和版本从SMA，看起来类似于其他交付，除之外自定义端口是列出的，并且一些条线路包括冗余‘集中化策略检疫’。下面示例：

```
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
```

- 您能找到这些事件通过使用grep到端口的seach，示例：grep “7025" mail_logs

ESA ‘禁用的Enable (event)’按钮

当尝试启用在ESA时的PVO，您可以尽管完成的所有前提配置发现‘Enable (event)’按钮变灰。当ESA显示PVO页时，与在端口7025的SMA联络验证配置准备启用。 如果此通信发生故障，‘Enable (event)’按钮将禁用。 您能排除故障此正如所有ESA - > SMA端口7025通信通过grepping “ESA的端口的7025"。欲知参考在相关信息列出的TechNote的更多信息。

相关信息

- PVO迁移向导的需求，当ESA是集群
- 集中策略、病毒和爆发检疫(PVO)的ESA不可能启用