Содержание

Введение

Этот документ описывает, как устранить неполадки доставки и проблем с подключением, когда централизовано policiy, вирус и вспышка quarnatine включены.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Email Security Appliance (ESA) с AsyncOS 8.1 или позже
- Устройство управления безопасностью (SMA) с AsyncOS 8.0 или позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Централизованная Политика, Вирус и Вспышка (PVO) Карантинная функция были представлены в (ESA) AsyncOS 8.0 / 8.1 (SMA). Эта функция имеет дополнительные требования сетевого подключения и ставит некоторые новые проблемы перед устранением проблем.

Поймите связь

- Связь CPQ использует SMTP, но с некоторыми дополнительными командами для передачи метаданных
- SMA прислушается к соединениям на интерфейсе и порту, определенном под Centralized Services-> Политика, Вирус и Карантин Вспышки. По умолчанию порт 7025, но это, возможно, было изменено пользователем с правами администратора!
- ESA прислушается к соединениям на интерфейсе и порту, определенном под

Сервисами безопасности-> Политика, Вирус и Карантин Вспышки. Снова, по умолчанию, порт 7025, но это, возможно, было изменено пользователем с правами администратора!
- SMA также использует SSH (через клиента команды) для получения сведений о конфигурации от ESA. В частности это используется, когда SMA отправляет освобожденные электронные почты ESA. SMA будет использовать SSH, чтобы сделать запрос конфигурации ESA и определить который интерфейс / порт для отправки освобожденной электронной почты.

Слушатели

- И ESA и SMA будут иметь вызванный 'cpq_listener' скрытого слушателя, который будет слушать на указанном порте.
- Эти слушатели могут быть замечены в файле конфигурации . Пример:

- Эти слушатели будут временно отстранены, если использование пользователя с правами администратора 'suspendlisteners все' или 'приостановит'. Если порт не принимает соединения, необходимо проверить, является ли состояние системы 'офлайновым' и резюме в случае необходимости.

Доставка устранения неполадок от ESA до SMA

- Проверьте, что ESA может соединиться с SMA на настраиваемом порте и интерфейсе. Это может быть сделано с помощью telnet. Если связь успешна, необходимо получить 220 баннеров.
- ESA будет иметь объект назначения названным 'the.cpq.host', который содержит сообщения, в то время как они помещены в очередь для доставки к SMA. Вы видите это использование 'tophosts' или Монитор-> Статус Доставки. Вы не можете использовать 'hoststatus' с ним, но можно использовать 'showrecipients' и 'deleterecipients' при необходимости.

Доставка устранения неполадок от SMA до ESA

- Проверьте, что SMA может соединиться с ESA на настраиваемом порте и интерфейсе. Снова, вы можете использовать telnet и будете видеть 220 баннеров, если успешный.
- При использовании кластеров важно, чтобы интерфейс, определенный на кластерном уровне под Сервисами безопасности-> Политика, Вирус и Карантин Вспышки, существовал для всех устройств на уровне машины. (проверьте Сеть-> IP - интерфейсы).
- SMA wil имеет объект назначения, названный 'the.cpq.release.host', который содержит освобожденные сообщения, в то время как они помещены в очередь для доставки к ESA. Вы видите это использование 'tophosts'. Это, кажется, не работает с 'hoststatus' или 'showrecipients', и я не протестировал 'deleterecipients' с ним, но это, вероятно, не работает также.
- Могут также быть проблемы со связью SSH между SMA и ESA. Эти проблемы являются не всегда обязательно сетевыми, например в CSCus29647, внутренний компонент SMA выходит из операции. Вопросы, такие как они будут, как правило, обнаруживаться как отказы приложения в почтовых журналах и могут обычно решаться путем перезагрузки

SMA.

TLS/Сертификаты

- Все соединения CPQ в любом направлении полагаются на TLS, и в результате конфигурация шифра может играть роль.
- Для TLS подключение для следования устройство, открывающее соединение, должно быть в состоянии проверить, что принимающее устройство использует наш hiddent CPQ сертификат. Если устройство выполняет согласование об анонимном шифре, для этого возможно отказать. Это появилось бы в журналах как что-то вроде этого:

- Можно устранить эти проблемы путем простого удаления анонимных шифров из исходящего списка шифра доставки, который сделан путем добавления `':-aNULL'` до конца списка шифра . Пример: `Высокий: Средний:-aNULL`

Файл журнала

- Если SMA имеет подписку журналов почты (он делает по умолчанию), можно рассмотреть почтовые журналы для сбора дополнительного понимания.
- CPQ получение событий будет похож на это и для сообщений, изолируемых к SMA и для сообщений, освобожденных к ESA

- Можно искать эти события с помощью grep, примера: `grep "CPQ ICID" mail_logs`
- События доставки CPQ, и изолирующие от ESA и выпуска от карантина от SMA, выглядят подобными любой другой доставке, за исключением того, что пользовательский порт перечислен, и несколько линий включают формулировку 'Централизованный Карантин Политики'. Пример ниже:

- Можно найти эти события при помощи grep к seach для порта, примера: `grep "порт 7025" mail_logs`

Кнопка 'Enable' ESA отключена

При попытке включить PVO на ESA, можно найти, что кнопка 'Enable' отображается серым, несмотря на всю необходимую как условие завершаемую конфигурацию. Когда ESA отображает страницу PVO, он связывается с SMA по порту 7025, чтобы проверить, что конфигурация готова быть включенной. Если эта связь откажет, то кнопка 'Enable' будет отключена. Можно устранить неполадки этого точно так же, как любой ESA-> связь порта 7025 SMA путем захвата для "порта 7025" на ESA. Для получения дополнительной информации обратитесь к TechNote, перечисленному в Дополнительных сведениях.

Дополнительные сведения

- Требования для Мастера Миграции PVO, когда кластеризован ESA
- Политика Централизации ESA, Вирус и Карантин Вспышки (PVO) не Могут быть Включены