

Содержание

[Введение](#)

[Общие сведения](#)

[Решение](#)

[Как можно препятствовать тому, чтобы произошли почтовые петли?](#)

Введение

Этот документ описывает, как определить почтовую петлю на Email Security Appliance (ESA).

Общие сведения

Почтовые Петли могут быть обозначены сообщениями с тем же Идентификатором сообщения, которые были введены больше чем 3 раза. Почтовые Петли могут вызвать признаки Высокой загрузки CPU, медленных проблем доставки и общей производительности. Обычно идентификаторы сообщения, введенные несколько раз, указали бы на цикличное выполнение, но иногда они введены несколько раз из-за проблем, или это мог быть неаккуратный спаммер, который продолжает вводить то же сообщение спама с тем же Идентификатором сообщения.

Более, как правило, почтовая петля вызвана почтовой проблемой инфраструктуры, которая передает то же сообщение или набор сообщений, мчащихся вокруг вашей сети от почтового сервера до почтового сервера бесконечно. В то время как эти сообщения могут поддержать себя развлеченными таким образом в течение очень долгого времени, это не хорошая вещь или для вашей пропускной способности сети или для понесенных затрат на обработку ESA.

Решение

Определение почтовой петли, если вы подозреваете, что это может быть проблемой, обычно довольно легко, хотя вам будет нужен к главному яблоку он.

Войдите в интерфейс командной строки (CLI) системы и выполните одну из этих команд или обоих, поскольку вы находите лучшие преимущества вами:

Особенно для поиска на Идентификаторе сообщения, если вы видите повторяющиеся экземпляры точно того же ID тогда, вы будете знать, что у вас есть почтовая петля. Однако, иногда это недостаточно, потому что один из почтовых серверов, сплывающих назад то же сообщение, мог бы услужливо изменять или удалять заголовок Идентификатора сообщения. Таким образом, если вы не получаете ничего идентифицируемого с разрешением проверки Идентификатора сообщения и пробуете Подчиненную проверку.

Предположение, что вы управляли найти сообщение цикличного выполнения Идентификатором сообщения, вы также захотите узнать другую информацию о сообщении и его родительском соединении (ICID). Учитывая Идентификатор сообщения и MID в той же

строке журнала можно выполнить:

Учитывая результирующие выходные данные там можно найти соответствующий ICID и DCID и выполнить:

Теперь вы должны иметь завершенное соединение - транзакция сообщения и видеть, куда это прибыло из и куда это было отправлено (если это уже произошло). Как только вы определили сообщение циклического выполнения, ваш следующий шаг должен получить взгляд на сообщение так, чтобы можно было решить проблему. Не исправляя причину петли, вероятно, что это сообщение и другие продолжат циклично выполняться или что скоро повторно произойдет проблема.

Создайте фильтр сообщения, подобный этому:

Теперь передача, которые изменяют и выполняют эту команду для проверки сообщения:

С информацией можно получить об удаленной системе путем рассмотрения почтовых журналов и другой информации, которую можно получить путем рассмотрения самого сообщения, должна существовать возможность для определения, где проблема.

Как можно препятствовать тому, чтобы произошли почтовые петли?

В сложных средах это может быть трудно - понимающий, как почта течет в вашей среде и как новое сетевое изменение, или на ESA или к другому устройству, будет влиять на тот трафик, является ключевым. Одна типичная причина безудержных почтовых петель является удалением Полученного заголовка. ESA автоматически обнаружит и остановит почтовую петлю, когда он будет видеть 100 Полученных заголовков в сообщении, но ESA действительно обеспечивает удаление этого заголовка, которые часто приводят к плохой почтовой петле. Пока нет *действительно* достаточное основание к, не выключайте Полученный заголовок или заставляйте их быть удаленными.

Ниже пример фильтра, который может помочь или предотвращать или исправлять почтовую петлю: