Вестник ЦЭМИ РАН. 2018

ISSN 1111-1111

URL - http://cemi.jes.su

Выпуск 2 Том . 2018

Использование сигнальных E-Mail-сообщений

Терентьев А. М.
Центральный экономико-математический институт РАН
Российская Федерация, Москва, Нахимовский проспект, 47

Аннотация

Предложен метод оповещения в проблемных ситуациях на антивирусном сервере. Для реализации метода использована специальная программа отправки E-Mail и созданный фиктивный аккаунт на почтовом сервере. Программа написана как консольная утилита на языке PowerBASIC. Описаны реальные случаи использования метода. Программа снабжена конфигурационным файлом, и поэтому легко переносима в любую необходимую Windows-среду. Внедрение программы на Антивирусном сервере ЦЭМИ РАН позволило исключить ежедневные дистанционные наблюдения за сервером во время обновления антивирусных областей и получения статистики в пол-ночь.

Ключевые слова: антивирус, сервер, Windows, E-Mail, MTA

Дата публикации: 13.12.2018

Ссылка для цитирования:

Терентьев А. М. Использование сигнальных E-Mail-сообщений // Вестник ЦЭМИ РАН. 2018. Выпуск 2 [Электронный ресурс]. Доступ для зарегистрированных пользователей. URL: http://cemi.jes.su/s111111110000007-0-1-ru (дата обращения: 17.12.2018). DOI: 10.18254/S0000007-0-1

1 Практика использования серверов в большинстве случаев не

предусматривает постоянного присутствия человека за клавиатурой и монитором сервера. Во многих случаях это невозможно не только вследствие круглосуточной работы сервера, но и из-за технических особенностей: ряд серверов эксплуатируется вообще без постоянно подключённых монитора и клавиатуры [9]. В полной мере это относится к Windows-серверам, и в том числе к Антивирусному серверу (АВ-серверу) ЦЭМИ РАН [8] [14] [9] [10] [11].

2 Между тем, в ряде случаев необходимо своевременное принятие решений, а зачастую и операторских действий при нештатных ситуациях на сервере. Если относительно сбоев электропитания можно что-то предпринять, например, осуществив резкое увеличение срока поддержки автономного питания [7] [6], то существуют ситуации, когда реагировать нужно незамедлительно.

3 Одна из такого рода ситуаций стала происходить на АВ-сервере в мае 2018 года, когда при принудительном завершении работы раздатчика web-информации Apache 1.3.23 [4] по непонятным причинам не удалялся текущий протокол работы (лог) программы Apache. Это приводило к тому, что на следующие сутки образовывался не новый протокол работы, а продолжался текущий за предыдущие сутки, причем такой эффект мог быть многодневным. При фиксации этого эффекта, автору работы приходилось ежедневно с 23:30 до 00:00 с помощью программы удалённого доступа Remote Administrator [3] контролировать корректность удаления лога, а в случаях невозможности его удаления («*Файл access.log занят посторонней программой*») перезагружать сервер, останавливать автоматически стартовавший при перезагрузке Apache, удалять лог и вновь стартовать Apache. Когда означенная ситуация повторилась в пятый раз за 10 дней, стала очевидной необходимость не только найти выход из ситуации без перезагрузки сервера, но и предусмотреть способ оповещения о такой ситуации.

4 Для завершения рассмотрения описанной ситуации следует сказать, что разблокировку лога оказалось возможным быстро осуществлять бесплатной программой ***IoBit Unlocker*** [1], которая показала присутствие пары несанкционированных процессов, запущенных якобы из каталога общего доступа. Каталог был исключён из разрешённых к доступу ботами добавлением строки в файл ROBOTS.TXT, и больше означенная проблема не возникала. Тем не менее, описанная ситуация навела автора на мысль создать внутри Антивирусной службы института сервис автоматической посылки E-Mail-сообщений с параметрической настройкой темы письма и текста сообщения.

5

```
ECHO OFF
REM !accnt1.bat = Catch Apache access log - Part1
tamdatew "accnt-1 bat-file issues OK" >>accnt.log
if exist accname.$$ DEL accname.$$>>accnt.log
tamdatnw accname.$$ a
"D:\Program Files\Apache Group\Apache\Apache.exe" -w -n "Apache"
     -k stop
if exist access.log del access.log>>accnt.log
ECHO F|XCOPY "D:\Program Files\Apache
     Group\Apache\logs\access.log" E:\STAT\SITE\access.log /Y
     /F>>accnt.log
copy /b acc1.ba + accname.$$ + acc2.ba accnty.bat
REM Занесение дневного лога с нужним именем в каталог
call accnty.bat
REM Удаление дневного лога
del "D:\Program Files\Apache Group\Apache\logs\access.log"
     >>accnt.log
IF NOT EXIST "D:\Program Files\Apache
     Group\Apache\logs\access.log" GOTO OkDel
tamdatew =!!= Accnt-1 Current Apache log IS NOT deleted!
     >>accnt.log
tamsmtp /GO
GOTO TstFlg
:OkDel
tamdatew =++= Accnt-1 Current log moved. >>accnt.log
:TstFlg
if exist tampst3.flg goto IssueX
tamdatew Accnt1 - Flag is NOT present ! >>accnt.log
tamsmtp /GO /txt=Flag
goto No
:IssueX
if exist accessx.log del accessx.log >>accnt.log
copy /b access.log accessx.log >>accnt.log
REM Наконец можно выполнить полноценную обработку дневного лога
call accntx.bat
:No
tamwait 10
```

Рис. 1. BAT-файл завершения дневной работы Apache

6 Такой блок уже был однажды запрограммирован и включён в программу постоянного пингования связи с роутером локальной сети [13]. Теперь этот блок был выделен в самостоятельную программу, к которой возможно обращение из BAT-файла. Большинство параметров (путь создаваемого файла отчёта, адрес (URL) почтового сервера, поля From, To, Subj, Text и Password) обычно хранятся в конфигурационном файле рядом с вызываемой программой в системном каталоге, а изменяемые Subj и/или Text могут дополнительно задаваться параметрами вызова.

7 Теперь соответствующие строки проверки реального удаления лога Apache вставлены в BAT-файл ежедневного завершения работы Apache (рис. 1). В случае неудаления лога исполняется обращение **tamsmtp /GO**, информирующее о необходимости вмешаться в ситуацию.

8 Второе обращение, ниже, **tamsmtp /GO /TXT=Flag** предусмотрено для ситуации, когда вследствие некорректной работы блока **accntx.bat** обработки дневного лога в предшествующие дни (например, из-за переполнения таблицы пользователей) оказывается убранным флаг-файл **tampst3.flg**.

Конфигурационный файл программы **tamsmtp.exe** показан на рис. 2. Из него видно, что поле Subj содержит текст-идентификацию основного АВ-сервера “**[AV_Server_LOG]**”, текстом по умолчанию является “**Log_NOT_Deleted_Today**”. При втором вызове текст меняется на “**Flag**”.

9

```
' TAMSMTP.CFG - конфигуратор SMTP
FullRepName=TAMSMTP.REP
server=vs1.cemi.rssi.ru
from=avir@cemi.rssi.ru
to=tam@cemi.rssi.ru
subj=[AV_Server_LOG]
text=Log_NOT_Deleted_Today
```

Рис. 2. Конфигурационный файл программы TamSmtp.exe

10 Для реализации приведённой схемы оказалось необходимым на общеинститутском почтовом сервере создать фиктивный аккаунт **avir**, чтобы существующий Mail Transport Agent (MTA) принимал посланные от этого имени сообщения. Поскольку на сервере **vs1.cemi.rssi.ru** не предусмотрена схема парольного доступа, принимаемые сообщения ограничены не аутентификацией, а разрешёнными фиксированными исходящими IP, включающими все АВ-сервера и постоянно включённый рабочий ПК Антивирусной службы. Адрес назначения является основным адресом администратора АВ-серверов.

11 Результат реализации значительно сокращает объём работы по администрированию АВ-сервера [5]. В частности, вместо ежедневного дистанционного наблюдения в 23:30 за процессом завершения дневной работы по раздаче антивирусных обновлений достаточно скачать текущую почту.

12 К настоящему времени проведена работа по модификации всех BAT-файлов АВ-серверов с включением туда оповещений в случае аварийных или критических ситуаций.

13 Поскольку существуют и другие службы, используемые сервером (например, UPS [7]), которые предусматривают оповещение через E-Mail, теперь возможно их задействовать через тот же аккаунт **avir**, повысив информативность сервера и рабочего ПК в критических ситуациях.

14 Программа **tamsmtp.exe** написана на языке PowerBASIC Console Conpiler 5.05 [2] и достаточно тривиальна. Однако, уточнённый протокол отправки E-Mail был определён с помощью имеющейся системы наблюдения циркулирующих в локальной сети пакетов [12].

15 Внедрение в практику сигнальных E-Mail-сообщений подняло работу администратора АВ-сервера на качественно новый уровень. Замещая

необходимость постоянного наблюдения за процессами актуализации областей антивирусных обновлений и ежедневной статистики, такая технология существенно экономит время обслуживания. Наличие конфигуратора в программе отправки E-Mail и самодокументированность программы позволяет легко внедрить описанную технологию на других институтских Windows-серверах.

Библиография:

1. https://www.radmin.ru/985-6516-85-4 (рус.).

2. http://av.cemi.rssi.ru

3. "Национальные интересы: приоритеты и безопасность". - М.: Издательский дом "Финансы и кредит", N32(221), 2013, с.56-60, ISSN 2073-2872.

4. "Национальные интересы: приоритеты и безопасность". - М.: Издательский дом "Финансы и кредит", N30(219), 2013, с.46-53, ISSN 2073-2872.

5. "Использование и развитие современных информационных технологий в научных исследованиях." Сб. статей под ред. М.Д. Ильменского - М: ЦЭМИ РАН, 2003, с. 64-73.

6. "Национальные интересы: приоритеты и безопасность". - М.: Издательский дом "Финансы и кредит", N17(206), 2013, с.41-48, ISSN 2073-2872.

7. "Национальные интересы: приоритеты и безопасность". - М.: Издательский дом "Финансы и кредит", N19(208), 2013, с.40-45, ISSN 2073-2872.

8. "Национальные интересы: приоритеты и безопасность". - М.: Издательский дом "Финансы и кредит", N20(209), 2013, с.41-46, ISSN 2073-2872.

9. "Развитие и использование средств сетевого мониторинга и аудита. Выпуск 1". - Сб.статей под ред. А.М.Терентьева. - М., ЦЭМИ РАН, 2004, с.75-87, ISBN 5-8211-0317-7.

10. XXIV Международная научная конференция "Современные концепции научных исследований" - М.: "Евразийское научное объединение", N2(24). 2017. Т.1, с.37-39. ISSN 2411-1899.

11. "Развитие и использование средств сетевого мониторинга и аудита. Выпуск 1". - Сб.статей под ред. А.М.Терентьева. - М., ЦЭМИ РАН, 2004, с.47-59, ISBN 5-8211-0317-7

Using signal e-Mail messages

A. Terentjev
CEMI RAS
Russian Federation, Moscow, Nachimovky prospect 47

Abstract

The method of notification is offered in problem situations on a anti-virus server. The special program of dispatch of e-Mail, and fictitious account on MTA has made for method realisation. The program realised on the PowerBASIC algorithmicus language as console' utility. The real cases of the use of method are described. The program is equipped with a configuration file, and is therefore easily portable to any necessary Windows environment. The implementation of the program on the anti-Virus server of CEMI RAS allowed to exclude daily remote monitoring of the server during the update of anti-virus areas and obtaining statistics at midnight.

Keywords: antivirus, server, Windows, e-Mail, MTA

Date of publication: 13.12.2018

Citation link:

Terentjev A. Using signal e-Mail messages // Vestnik CEMI RAS. 2018. Issue 2 [Electronic resource]. Access for registered users. URL: http://cemi.jes.su/s111111110000007-0-1-ru (circulation date: 17.12.2018). DOI: 10.18254/S0000007-0-1
