Настройка логирования действий пользователя при работе с «С-Терра Шлюз»

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.
Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Назначение документа

Документ описывает настройку логирования действий (выполняемых команд) при работе в различных консолях (cisco-like, bash, vtysh) на криптошлюзах «С-Терра Шлюз» и «С-Терра Шлюз DP» версии 5.0.

Предварительные требования

Требования к квалификации администратора

Администратор должен обладать обширными знаниями в области сетевой информационной безопасности, иметь опыт работы с аналогичным оборудованием/программным обеспечением, знать и понимать syslog.

Требования к начальному состоянию «С-Терра Шлюз»

Устройство «С-Терра Шлюз» должно быть инициализировано (подробнее на https://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз 5.0 -> «Подключение ПАК и инициализация С-Терра Шлюз на вычислительных системах архитектуры Intel x86-64»).

Логирование действий в bash консоли

Данная настройка позволяет логировать в syslog выполняемые действия в Linux bash консоли криптошлюза. Настройка выполняется из bash консоли.

1. Откройте на редактирование файл `/etc/bash.bashrc` и добавьте в конец файла следующие строки:

```
# Log bash commands
LOG_SEVERITY="debug"
LOG_FACILITY="local6"

log_command() {
    export HISTIGNORE=
    export HISTCONTROL=
    local RETRN_VAL=$?
```

© 2003-2025 «С-Терра СиЭсПи»

```
    local whoami="$(whoami)@$(if [ -n "$SSH_CONNECTION" ]; then
        echo "$SSH_CONNECTION" | awk '{print $1}'
    else
        echo '127.0.0.1'
    fi)"

    local CURRENT_HISTNUM=$(HISTTIMEFORMAT="" history 1 | awk '{print $1}')

    if [[ -z "$LAST_HISTNUM" ]]; then
        LAST_HISTNUM=$CURRENT_HISTNUM
        return
    fi

    if [[ "$CURRENT_HISTNUM" -ne "$LAST_HISTNUM" ]]; then
        local COMMAND_TEXT=$(HISTTIMEFORMAT="" history 1 | sed 's/^[ ]*[0-
9]\+[ ]*//')
        logger -p "$LOG_FACILITY.$LOG_SEVERITY" -t "bash_logger" "$whoami [$$]
[$PWD]: $COMMAND_TEXT [$RETRN_VAL]"
        LAST_HISTNUM=$CURRENT_HISTNUM
    fi
}

export PROMPT_COMMAND='log_command'
```

2. Создайте конфигурационный файл `/etc/rsyslog.d/bash_logger.conf` для rsyslog, например, для логирования в локальный файл `/var/log/bash_commands.log`:

```
root@sterragate:~# vim.tiny /etc/rsyslog.d/bash_logger.conf
```

```
if ($programname == 'bash_logger') then {
    action(type="omfile" file="/var/log/bash_commands.log")
    stop
}
```

Для отправки лога на удаленный сервер можно использовать следующую директиву `action`:

```
action(type="omfwd" target="REMOTE_IP" port="REMOTE_PORT" protocol="PROTO")
```

Где:

- `REMOTE_IP` – IP адрес удаленного сервера;
- `REMOTE_PORT` – порт удаленного сервера;
- `PROTO` – протокол передачи (`tcp` или `udp`).

Можно указывать несколько директив `action` одновременно.

3. Перезапустите сервис `rsyslog`:

```
root@sterragate:~# systemctl restart rsyslog.service
```

4. Для того, чтобы выполняемые действия начали логироваться, необходимо переподключиться к bash консоли.

5. Убедитесь, что команды, введенные в bash консоли логируются:

```
root@sterragate:~# cat /var/log/bash_commands.log
```

```
2025-05-13T22:02:33.107059+03:00 sterragate bash_logger: root@192.168.100.100
[1587] [/root]: ls [0]
```

```
2025-05-13T22:02:45.930006+03:00 sterragate bash_logger: root@192.168.100.100
[1587] [/root]: vim.tiny /etc/rsyslog.d/bash_logger.conf  [0]
2025-05-13T22:02:57.005875+03:00 sterragate bash_logger: root@192.168.100.100
[1587] [/root]: cat /var/log/bash_commands.log  [0]
```

6. Для отключения логирования введенных команд в bash консоли удалите добавленные строки в файле `/etc/bash.bashrc`, удалите конфигурационный файл `/etc/rsyslog.d/bash_logger.conf` и перезапустите сервис `rsyslog`.

Логирование действий в cisco-like консоли

Данная настройка позволяет логировать в syslog выполняемые действия в cisco-like консоли. Настройка выполняется из cisco-like консоли.

1. Перейдите в режим конфигурирования:

```
sterragate#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
sterragate(config)#
```

2. Установите уровень логирования `debugging`:

```
sterragate(config)#logging trap debugging
```

3. Примените настройки:

```
sterragate(config)#end
```

4. После этого все команды, выполненные в cisco-like консоли, будут по умолчанию записаны в файл `/var/log/cspvpngate.log`, например:

```
2025-05-13T23:00:20.814118+03:00 sterragate cs_console: 00725001 Cisco-like
console started by user "root"
2025-05-13T23:00:21.940912+03:00 sterragate cs_console: 00727001 User "root":
Start interpreting command: "enable "
2025-05-13T23:00:23.005611+03:00 sterragate cs_console: 00725007 User "root"
has entered into the privileged EXEC mode
2025-05-13T23:00:23.005698+03:00 sterragate cs_console: 00727002 User "root":
Command "enable " processed with status OK
2025-05-13T23:00:25.197485+03:00 sterragate cs_console: 00727001 User "root":
Start interpreting command: "show running-config"
2025-05-13T23:00:25.203832+03:00 sterragate cs_console: 00727002 User "root":
Command "show running-config" processed with status OK
2025-05-13T23:00:26.773370+03:00 sterragate cs_console: 00725002 Cisco-like
console exited (user "root")
```

Для отправки лога на удаленный сервер можно использовать следующую команду в конфигурационном режиме в cisco-like консоли (это не отключит запись в локальный файл `/var/log/cspvpngate.log`):

```
sterragate(config)#logging host REMOTE_IP transport PROTO port REMOTE_PORT
```

Где:

- `REMOTE_IP` – IP адрес удаленного сервера;
- `REMOTE_PORT` – порт удаленного сервера;
- `PROTO` – протокол передачи (`udp`, `tcp` или `relp`).

Для отключения отправки лога на удаленный сервер используйте эту же команду с приставкой no.

© 2003-2025 «С-Терра СиЭсПи»

5. Для отключения логирования введенных команд используйте следующую команду в конфигурационном режиме в cisco-like консоли (эта команда восстановит уровень логирования по умолчанию):

```
sterragate(config)#no logging trap
```

Логирование действий в vtysh (FRR) консоли

Данная настройка позволяет логировать в syslog выполняемые действия в консоли vtysh сервиса FRR.

1. Запустите сервис FRR (если не запущен):

```
root@sterragate:~# systemctl start frr.service
```

2. Войдите в консоль vtysh:

```
root@sterragate:~# vtysh
```

```
Hello, this is FRRouting (version 9.0.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

sterragate#
```

3. Убедитесь, что логирование в syslog включено (по умолчанию включено):

```
sterragate# show running-config
```

```
...
log syslog informational
...
```

4. Перейдите в режим конфигурирования:

```
sterragate# configure
```

```
sterragate(config)#
```

5. Включите логирование команд:

```
sterragate(config)# log commands
```

6. Примените настройки:

```
sterragate(config)# end
```

7. Сохраните настройки и выйдите из консоли vtysh:

```
sterragate# write
```

```
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
```

```
sterragate# exit
```

```
root@sterragate:~#
```

8. После этого все команды, выполненные в консоли vtysh, будут записываться в файл `/var/log/frr/frr.log`, например (команды могут дублироваться):

```
2025-05-14T11:17:19.542533+03:00   sterragate   zebra[2205]:   [M7Q4P-46WDR]
vty[59]@> enable
2025-05-14T11:17:28.530353+03:00   sterragate   zebra[2205]:   [M7Q4P-46WDR]
vty[59]@# do write terminal
```

```
2025-05-14T11:18:39.005203+03:00 sterragate zebra[2205]: [M7Q4P-46WDR]
vty[59]@# configure terminal
```

9. Для отправки лога на удаленный сервер откройте на редактирование конфигурационный файл `/etc/rsyslog.d/45-frr.conf`, найдите строку

```
    then :omfile:$frr_log
```

и замените ее на следующую конструкцию:

```
    then {
        :omfile:$frr_log
        action(type="omfwd" target="REMOTE_IP" port="REMOTE_PORT"
protocol="PROTO")
    }
```

Где:

- `REMOTE_IP` – IP адрес удаленного сервера;
- `REMOTE_PORT` – порт удаленного сервера;
- `PROTO` – протокол передачи (`tcp` или `udp`).

Затем перезапустите сервис `rsyslog`:

```
root@sterragate:~# systemctl restart rsyslog.service
```

10. Для отключения логирования введенных команд используйте следующую команду в конфигурационном режиме в консоли vtysh:

```
sterragate(config)# no log commands
```

Приложение

Настройка ротации логов

В случаях, когда логирование было настроено в новый локальный файл, рекомендуется настроить ротацию этого файла для избежания ситуации с переполнением дискового пространства. Ротация файлов выполняется с помощью сервиса `logrotate`.

1. Создайте конфигурационный файл logrotate, например для ротации лога `/var/log/bash_commands.log`:

   ```
   root@sterragate:~# vim.tiny /etc/logrotate.d/bash_commands
   ```

   ```
   /var/log/bash_commands.log
   {
       rotate 3
       size 10M
       missingok
       notifempty
       compress
       delaycompress
       postrotate
           /usr/lib/rsyslog/rsyslog-rotate
       endscript
   }
   ```