Ghi lại log

HƯỚNG DẪN CẤU HÌNH GHI LOG COMMAND.

Chú ý đặc biệt quan trọng, khi copy từ Word có thể phải sửa ký tự:

Ký tự	Sửa thành	Ghi chú
‘	'	Sửa mở nháy đơn tròn thành nháy đơn thẳng.
’	'	Sửa đóng nháy đơn tròn thành nháy đơn thẳng.
“	"	Sửa mở nháy kép tròn thành nháy kép thẳng.
”	"	Sửa đóng nháy kép tròn thành nháy kép thẳng.

Bước 1: Thực hiện backup toàn bộ các file cấu hình phục vụ rollback khi cấu hình.

a. Với Linux Centos, Redhat:

```
    cp /etc/bashrc /etc/bashrc.back
    cp /etc/syslog.conf   /etc/syslog.conf.back
    cp /etc/rsyslog.conf    /etc/rsyslog.conf.back
```

b. Với Solaris server:

```
    cp /etc/profile /etc/profile.back
    cp /etc/syslog.conf /etc/syslog.conf.back
```

c. Với Linux Suse

```
    cp /etc/bash.bashrc /etc/bash.bashrc.back
    cp /etc/syslog-ng/syslog-ng.conf   /etc/syslog-ng/syslog-
ng.conf.back
```

Bước 2: Cấu hình ghi log command.

2.1 Các bước thực hiện cấu hình ghi log command với server Linux (Centos, Redhat).

- Thêm vào cuối file **/etc/bashrc**

```
export PROMPT_COMMAND='RETRN_VAL=$?;logger -p local6.debug
"[cmdlog] $(whoami) [$$]: $(history 1 | sed "s/^[ ]*[0-9]
\+[ ]*//" ) [$RETRN_VAL] [$(echo $SSH_CLIENT | cut -d" " -
f1)]"'
```

  - Cấu hình đẩy log vào file chưa logs.

Thêm dòng cấu hình sau vào file **/etc/syslog.conf** hoặc **/etc/rsyslog.conf** tùy thuộc vào server chạy syslog hay rsyslog (recomment thêm vào sau dòng local7.* /var/log/boot.log, cho dễ kiểm soát).

```
# Log cmdlog
local6.*        /var/log/cmdlog.log
```

  - Khởi động lại syslog

    /etc/init.d/syslog restart hoặc

    /etc/init.d/rsyslog restart - Kiểm tra việc ghi log trong files ghi log.

    cat /var/log/cmdlog.log - Cấu hình rotate log trên Linux CentOS, Redhat, tạo file **/etc/logrotate.d/cmdlog** có nội dung như file bên dưới.

    /var/log/cmdlog.log { compress weekly rotate 12 sharedscripts

    postrotate /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true endscript }

2.2 Các bước thực hiện cấu hình ghi log command với server Unix.

- Thêm vào **/etc/profile** 02 dòng cấu hình sau:

```
PROMPT_COMMAND='RETRN_VAL=$?;logger -p local6.debug "[cmdl
og] $(/usr/ucb/whoami) [$$]: $(history 1 | sed "s/^[ ]*[0-
9]\+[ ]*//" ) [$RETRN_VAL] [$(echo $SSH_CLIENT | cut -d" "
-f1)]"'
export  PROMPT_COMMAND
```

  - Cấu hình đẩy log vào file chứa logs. Thêm dòng cấu hình sau vào cuối file **/etc/syslog.conf** (recomment thêm vào sau dòng local7.* /var/log/boot.log, cho dễ kiểm soát).

    local6.debug /var/log/cmdlog.log

`Chú ý: Do khi thực hiện copy dấu TAB giữa local6.debug và /var/log/cmdlog.log chuyển thành dấu SPACE gây ra lỗi không ghi được log. Vì vậy khi cấu hình cần gõ dấu TAB bằng tay.`

- Tạo file ghi log trong thư mục lưu trữ log.

```
touch /var/log/cmdlog.log
```

  - Khởi động lại syslog bằng câu lệnh sau:

Với solaris 8 & 9:

```
/etc/init.d/syslog stop
/etc/init.d/syslog start
```

Với Solaris 10:

```
svcadm  restart   system-log
```

  - Kiểm tra việc ghi log câu lệnh ra **/var/log/cmdlog.log**

    cat /var/log/cmdlog.log - Cấu hình rotate Log trong Solaris.

Thực hiện câu lệnh để check systax:

```
logadm -C 12 -p 1w  -n -w /var/log/cmdlog.log -z 0
```

Sau đó thực hiện câu lệnh, để update vào file logadm.conf.

```
logadm -C 12 -p 1w -w /var/log/cmdlog.log -z 0
```

2.3 Các bước thực hiện cấu hình ghi log command với server Linux Suse.

- Thêm vào cuối file **/etc/bash.bashrc**

```
export PROMPT_COMMAND='RETRN_VAL=$?;logger -p local6.debug
"[cmdlog] $(whoami) [$$]: $(history 1 | sed "s/^[ ]*[0-9]
\+[ ]*//" ) [$RETRN_VAL] [$(echo $SSH_CLIENT | cut -d" " -
f1)]"'
```

  - Cấu hình đẩy log vào file chưa logs.

Thêm các dòng cấu hình sau vào cuối file /etc/syslog-ng/syslog-ng.conf

```
filter f_cmdlog   { level(debug)      and facility(local
6); };
destination cmdlog { file("/var/log/cmdlog.log"); };
log { source(src); filter(f_cmdlog ); destination(cmdlog);
};
```

  - Khởi động lại syslog-ng

    /etc/init.d/syslog restart - Kiểm tra việc ghi log trong files ghi log.

    cat /var/log/cmdlog.log - Cấu hình rotate log trên Linux Suse, tạo file **/etc/logrotate.d/cmdlog** có nội dung như file bên dưới.

    /var/log/cmdlog.log { compress weekly rotate 12 sharedscripts

postrotate /etc/init.d/syslog reload endscript }

2.3 Các bước thực hiện cấu hình ghi log command với server AIX.

- Thêm vào cuối file etc/profile 2 dòng:

```
PROMPT_COMMAND='RETRN_VAL=$?;logger -p local6.debug "[cmdl
og] $(/usr/ucb/whoami) [$$]: $(history 1 | sed "s/^[ ]*[0-
9]\+[ ]*//" ) [$RETRN_VAL] [$(echo $SSH_CLIENT | cut -d" "
-f1)]"'
export  PROMPT_COMMAND
```

- Cấu hình đẩy log vào file chưa logs.

  Thêm các dòng cấu hình sau vào cuối file /etc/syslog.conf

```
local6.debug    /var/log/cmdlog.log rotate size 4096k file
s 12 time 1w compress
```

`Chú ý: Do khi thực hiện copy dấu TAB giữa local6.debug và /var/log/cmdlog.log chuyển thành dấu SPACE gây ra lỗi không ghi được log. Vì vậy khi cấu hình cần gõ dấu TAB bằng tay.`

- Tạo file log /var/log/cmdlog.log

```
touch /var/log/cmdlog.log
```

- Khởi động lại syslog bằng câu lệnh sau

```
refresh -s syslogd
```

Bước 3: Kiểm tra việc ghi log đã thành công chưa.

- Thử gõ một số lệnh như: "ls -al", "pwd"

- Kiểm tra nội dung file /var/log/cmdlog.log. Nếu kết quả như sau là thành công:

```
Apr 18 18:06:12 sv241 root: [cmdlog] root [12411]: ls -al
[0]
Apr 18 18:06:13 sv241 root: [cmdlog] root [12411]: pwd [0]
```