HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH BẢO MẬT HỆ ĐIỀU HÀNH ORACLE

I. Các phiên bản hỗ trợ:

TT	Phiên bản	Ghi chú
1	Oracle Linux 7	
2	Oracle Linux 8	
3	Oracle Linux 9	

II. Hướng dẫn thiết lập chính sách bảo mật

1. Cài đặt hệ điều hành

1.3. Biến môi trường $PATH không được chứa các đường tương đối, đường dẫn bất thường, đường dẫn trống

- Bước 1: Kiểm tra các đường dẫn trong biến môi trường, ta dùng lệnh sau:
  `su - root -c 'env | grep PATH' | cut -d '=' -f 2 | tr '\n' ' '`
- Bước 2: Biến môi trường không được chứa các đường dẫn:
  - PATH không chứa đường dẫn trống (::)
    `/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin::`
  - PATH không chứa đường dẫn tương đối (./)
    `/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:./src/bin`
  - PATH không chứa đường dẫn bất thường (/tmp)
    `/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmp`
- Bước 3: Nếu biến môi trường có chứa đường dẫn không cho phép, thực hiện loại bỏ theo hướng dẫn sau:
  - Truy cập file: `nano ~/.bashrc và nano ~/.bash_profile`
  - Tìm dòng lệnh sau và xóa các đường dẫn không hợp lệ
    `export PATH=$PATH:/path/to/folder`
  - Save lại và chạy lệnh để thay đổi cấu hình
    `source ~/.bashrc`
    `source ~/.bash_profile`

1.6. Thiết lập cấu hình dịch vụ CRON

- Bước 1: Thực hiện xóa File cron.deny:
  `#rm /etc/cron.deny`
- Bước 2: Thêm File cron.allow nếu hệ thống chưa có:
  `#touch /etc/cron.allow`
- Bước 3: Sửa file /etc/cron.allow, cập nhật hoặc thêm các tài khoản được phép sử dụng dịch vụ CRON:

```
User1
User2 …
```

- Bước 4: Sửa file /etc/cron.allow, hạn chế quyền sửa các file cấu hình của CRON:

```
#chown root:root /etc/crontab
#chmod 600 /etc/crontab
#chown -R root:root /etc/cron.hourly /etc/cron.daily
/etc/cron.weekly /etc/cron.monthly /etc/cron.d
#chmod -R go-rwx /etc/cron.hourly /etc/cron.daily
/etc/cron.weekly /etc/cron.monthly /etc/cron.d
```

2. Kiểm soát truy cập

2.1. Cấu hình tài khoản quản trị phải tuân thủ Phần V, Tiêu chuẩn Xác thực đăng nhập và quản lý mật khẩu hệ thống công nghệ thông tin số TC.CNVTQĐ.CNTT.26

Độ dài tối thiểu của mật khẩu phải lớn hơn hoặc bằng 8 ký tự

Đối với CentOS/RedHat

- Bước 1: Mở tập tin /etc/security/pwquality.conf và tìm tới dòng:

```
#minlen
```

- Bước 2: Thay đổi thành:

```
minlen = 8
```

- Bước 3: Lưu lại tập tin cấu hình

Mật khẩu phải chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt

Đối với CentOS/RedHat:

Mở file /etc/security/pwquality.conf và thêm vào:

```
lcredit=-1
ucredit=-1
dcredit=-1
ocredit=-1
```

Mật khẩu chỉ hợp lệ trong tối đa 90 ngày

Mở tập tin /etc/login.defs, thay đổi tuỳ chọn **PASS_MAX_DAYS**:

```
PASS_MAX_DAYS 90
```

Yêu cầu mật khẩu mới khác 5 mật khẩu gần nhất

- Bước 1: Mở tập tin /etc/pam.d/system-auth
  `#vi /etc/pam.d/system-auth`
  Bước 2: Thêm hoặc cập nhật cấu hình thuộc tính remember của tuỳ chọn
  `password required/sufficient/requisite pam_unix.so [các option trước đó] remember=5`
  Tùy theo yêu cầu của tổ chức, có thể đặt giá trị remember lớn hơn hoặc bằng 5
- Bước 3: Lưu lại tập tin cấu hình.

Mã hóa mật khẩu sử dụng thuật toán mã hóa an toàn

Mở tệp tin /etc/login.defs, thêm hoặc cập nhật cấu hình
`ENCRYPT_METHOD SHA512  # hoặc YESCRYPT nếu hệ thống hỗ trợ`

Mở tệp tin /etc/pam.d/system-auth thêm hoặc cập nhật cấu hình:

- Nếu sử dụng SHA512:

`password sufficient pam_unix.so **sha512** shadow [existing options]`

- Nếu sử dụng yescrypt:

`password sufficient pam_unix.so **yescrypt** shadow [existing options]`

2.4. Cấu hình giới hạn tài khoản được phép sử dụng dịch vụ quản trị từ xa

- Bước 1: Mở tập tin cấu hình /etc/ssh/sshd_config
  `#vi /etc/ssh/sshd_config`
- Bước 2: Thêm tuỳ chọn AllowUsers để cấu hình tài khoản được phép truy cập từ xa:
  `AllowUsers username`
  Ví dụ nếu muốn cho phép tài khoản sshuser được phép sử dụng dịch vụ truy cập từ xa, ta cấu hình như sau:
  `AllowUsers sshuser`
- Bước 3: Không cho phép tài khoản root đăng nhập quản trị từ xa.
  `PermitRootLogin no`
- Bước 3: Lưu lại cấu hình và khởi động lại dịch vụ ssh.
  `systemctl restart sshd`

2.5. Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 05 phút

- Bước 1: Thêm nội dung sau vào cuối cấu hình file /etc/profile
  `TMOUT=300`
  `readonly TMOUT`

```
export TMOUT
```

- Bước 2:Khởi động lại dịch vụ ssh

```
systemctl restart sshd
```

2.11. Thiết lập hệ thống chỉ cho phép quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa

- Bước 1: Mở tập tin cấu hình /etc/ssh/sshd_config:

```
#vi /etc/ssh/sshd_config
```

- Bước 2: Sửa lại tuỳ chọn Protocol như bên dưới:

```
Protocol 2
```

- Bước 3: Lưu lại tập tin và khởi động lại dịch vụ ssh.

3. Phòng chống xâm nhập

3.1. Ghi log những bản ghi vào/ra không hợp lệ. Mặc định phải có rule chặn tất cả với những bản ghi vào/ra không hợp lệ

Cách 1: Cấu hình iptables (Áp dụng cho Oracle7/8)

Bước 1: Cài đặt:

- Đảm bảo máy chủ có kết nối Internet. Thực hiện cài dịch vụ dưới quyền root:

```
yum install -y iptables-services
systemctl enable iptables --now
```

- Kiểm tra trạng thái dịch vụ:

```
systemctl status iptables
```

Bước 2: Cấu hình iptables:

- Kiểm tra các rule hiện tại:

```
iptables -L -n -v
```

- Thêm Rule cho kết nối hợp lệ. Ví dụ:

```
# cho phép các kết nối đã thiết lập
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
# cho phép loopback (localhost)
iptables -A INPUT -i lo -j ACCEPT
# cho phép SSH (cổng 22)
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -
j ACCEPT
```

- Thêm Rule để ghi log và chặn kết nối không hợp lệ. Sửa file cấu hình iptables:

```
nano /etc/sysconfig/iptables
```

Thêm các dòng sau:

```
-A INPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP:
"
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A OUTPUT -j LOG --log-level 4 --log-prefix "IPTABLES
DROP: "
-A OUTPUT -j REJECT --reject-with icmp-host-prohibited
```

Bước 3: Nạp lại file cấu hình:

```
iptables-restore < /etc/sysconfig/iptables
```

Cách 2: Cấu hình nftables

Kể từ kernel Linux 4.x trở lên (mặc định từ CentOS 8), nftables trở thành công cụ lọc gói tin mặc định, thay thế iptables, ip6tables, arptables, và ebtables.

Bước 1: Cài đặt:

- Đảm bảo máy chủ có kết nối Internet. Thực hiện cài dịch vụ dưới quyền root:

```
yum install -y nftables
```

- Kiểm tra trạng thái dịch vụ:

```
systemctl status nftables     # Kiểm tra trạng thái
systemctl enable nftables     # Bật khi khởi động
systemctl start nftables      # Khởi động ngay
```

Bước 2: Cấu hình nftables:

- Kiểm tra các rule hiện tại:

```
nft list ruleset
```

- Thêm Rule cho kết nối hợp lệ tùy nhu cầu sử dụng. Ví dụ:

```
# tạo table
nft add table inet firewall
# tạo các chain INPUT, OUTPUT, FORWARD
nft add chain inet firewall INPUT { type filter hook input
priority 0\; policy accept\; }
nft add chain inet firewall FORWARD { type filter hook
forward priority 0\; policy accept\; }
nft add chain inet firewall OUTPUT { type filter hook
output priority 0\; policy accept\; }

# cho phép SSH từ một IP cụ thể
```

```
nft add rule inet firewall INPUT ip saddr 10.0.0.1 ct
state new tcp dport 22 counter accept comment "Allow SSH
from 10.0.0.1"

# cho phép truy cập ra ngoài đến nhiều cổng
nft add rule inet firewall OUTPUT ip daddr 192.168.1.1 ct
state new tcp dport {80, 443, 514, 4505, 4506, 5044, 6379,
9092, 9080-9100} counter accept comment "Allow external
services"

# ghi log và drop các kết nối không hợp lệ
nft 'add rule inet firewall INPUT log prefix "INPUT DROP:
" level debug'
nft 'add rule inet firewall INPUT drop'
nft 'add rule inet firewall OUTPUT log prefix "OUTPUT
DROP: " level debug'
nft 'add rule inet firewall OUTPUT drop'

# lưu lại các rule sau khi cấu hình xong
nft list ruleset > /etc/sysconfig/nftables.conf
```

- Cấu hình ghi log và drop các kết nối không hợp lệ. Kiểm tra file cấu hình **/etc/sysconfig/nftables.conf**.
  nano /etc/sysconfig/nftables.conf

Đảm bảo có các cấu hình sau trong table inet (Phần in đậm là bắt buộc):

Option 1:

```
    chain INPUT {
        counter packets 0 bytes 0 log prefix "Dropped input by firewall:
" level debug
        counter packets 0 bytes 0 drop
    }

    chain OUTPUT {
        counter packets 0 bytes 0 log prefix "Dropped output by
firewall: " level debug
        counter packets 0 bytes 0 drop
    }
```

Option 2:

```
    chain INPUT {
        counter packets 0 bytes 0 log prefix "Dropped input by firewall:
" level debug drop
```

```
    }

    chain OUTPUT {
        counter packets 0 bytes 0 log prefix "Dropped output by
firewall: " level debug drop
    }
```

Bước 3: Load lại cấu hình nftables:

```
systemctl reload nftables
```

3.4. Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng, cổng kết nối không sử dụng

Kiểm tra trạng thái của Bluetooth

```
systemctl status bluetooth
```

Nếu trạng thái đang là Active, dùng lệnh sau để vô hiệu hóa

```
systemctl stop bluetooth
systemctl disable bluetooth
```

Kiểm tra trạng thái của Cups

```
systemctl status cups
```

Nếu trạng thái đang là Active, dùng lệnh sau để vô hiệu hóa

```
systemctl stop cups
systemctl disable cups
```

4. Nhật ký hệ thống

4.1. Mặc định ghi log thông tin đăng nhập vào máy chủ

Ghi log mặc định của hệ điều hành: Yêu cầu thiết lập cấu hình ghi tối thiểu các loại sau: message log, dmesg log, secure log (Mặc định Suse ghi log message và secure vào cùng file log /var/log/ message).

1. Cấu hình log sshd trong file /etc/rsyslog.conf

```
$ModLoad imuxsock # provides support for local system logging
(e.g. via logger command)

$ModLoad imklog # provides kernel logging support (previously
done by rklogd)
```

```
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

$IncludeConfig /etc/rsyslog.d/*.conf

*.info;mail.none;authpriv.none;cron.none /var/log/messages

authpriv.* /var/log/secure

mail.* -/var/log/maillog

cron.* /var/log/cron

uucp,news.crit /var/log/spooler

local7.* /var/log/boot.log

#logging iptables:

#kern.* /var/log/kernel
```

4.6. Yêu cầu cấu hình lưu log command người dùng hệ thống với HĐH Linux

Lưu ý: Chỉ cần thao tác với 1 trong 2 services: syslog hoặc rsyslog, bỏ qua các commands với service còn lại

Kiểm tra service nào đang chạy

```
service rsyslog status
service syslog status
```

Bước 1: Thực hiện backup file cấu hình

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

Bước 2: Cấu hình ghi log command

- Thêm vào cuối file /etc/bashrc (lưu ý câu lệnh dưới đây nằm trên 1 dòng)

```
export PROMPT_COMMAND='RETRN_VAL=$?;logger -p
local6.debug "[cmdlog] $(whoami) [$$]: $(history 1 | sed
```

```
   "s/^[  ]*[0-9]\+[ ]*//" ) [$RETRN_VAL] [$(if [ -z
   "$SSH_CLIENT" ]; then ctty=$(echo $(tty) | cut -d"/"
   -f3,4);who | grep $ctty | cut -d"(" -f2 | sed "s/)//";
   else echo $(echo $SSH_CLIENT | cut -d" " -f1); fi)]"'
```

- Apply cấu hình

```
source /etc/bashrc
```

- 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 service syslog restart
```

Hoặc

```
/etc/init.d/rsyslog restart hoặc service rsyslog restart
```

- Kiểm tra việc ghi log trong files ghi log.

```
cat /var/log/cmdlog.log
```

4.7. Cấu hình thời gian lưu log tối thiểu là 03 tháng (HĐH Linux)

- Bước 1: Cấu hình nội dung tập tin /etc/logrotate.conf với nội dung sau:

```
weekly
rotate 12
create
dateext
include /etc/logrotate.d
/var/log/wtmp {
    monthly
    create 0664 root utmp
    minsize 1M
    rotate 2
}
/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 2
}
```

- Bước 2: Cấu hình log cho các tập tin messagelog, syslog, kernel.log… như sau:

```
- Tạo tập tin syslog trong /etc/logrotate.d/
#vi /etc/logrotate.d/syslog
- Sửa nội dung tập tin thành:
/var/log/cron
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
{
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2>
/dev/null` 2> /dev/null || true
    endscript
}
```

- Bước 3: Khởi động lại dịch vụ rsyslog:

```
systemctl restart rsyslog
```

- Kiểm tra đảm bảo tất cả các sự kiện quan trọng đều được ghi lại log. Quản trị viên có thể phân nhóm các sự kiện và ghi ra thành các tập tin riêng biệt để thuận tiện trong việc theo dõi và giám sát.

- Hệ thống sẽ kiểm tra thời gian rotate cho tất cả các file cấu hình có trong thư mục **/etc/logrotate.d/**, vì vậy cần đảm bảo đã **cập nhật rotate cho tất cả các file cấu hình có trong thư mục này**.

- Trên CentOS, có 2 dịch vụ log được sử dụng, là syslog và rsyslog. Tuy nhiên syslog có nhiều hạn chế trong việc lưu trữ từ xa an toàn, do vậy rsyslog được khuyến nghị sử dụng.
- Cấu hình các sự kiện ghi log được lưu trong tập tin /etc/syslog.conf đối với syslog và /etc/rsyslog.conf đối với rsyslog.
- Syslog và rsyslog hỗ trợ nhiều loại log hệ thống với nhiều mức log, cụ thể như sau:
  - kern – kernel
  - user – log các ứng dụng của người dùng
  - mail/news/UUCP/cron – Email/NNTP/UUCP/cron
  - daemon – system daemons
  - auth – log liên quan tới xác thực người dùng
  - lpr – log liên quan đến dịch vụ in
  - mark – thêm timestamp vào dữ liệu log

- local0-local7-8 log cho các tuỳ chọn kiểm tra, thanh tra
- syslog – các log khác của dịch vụ syslog
- authpriv – các log xác thực không thuộc hệ thống

Log hệ điều hành có các mức: emerg, alert, crit, warning, notice, info, debug

- Dựa vào các cấu hình trong bảng để xác định thời gian log sẽ được lưu trữ trên hệ thống trước khi bị xóa

Cấu hình	Giải thích
Interval	Một trong các giá trị daily, weekly, monthly, và yearly. Để đơn giản hóa, các giá trị daily, weekly, monthly, và yearly tương đương với 1, 7, 30, và 365 ngày
Rotate	Số lượng file log sẽ được giữ lại sau mỗi lần rotate. Ví dụ với **rotate** 7 và **interval** daily, sẽ giữ lại log trong 7 ngày trước đó (file.log.1 đến file.log.7) ngoài file hiện tại (file.log). Khi xoay vòng lần thứ 8, file file.log.7 sẽ bị xóa và các bản còn lại sẽ được đẩy lên. Nếu **rotate** là 0 các file log cũ sẽ không được giữ lại sau khi xoay vòng - chúng sẽ bị xóa ngay. Chỉ log hiện tại (file.log) được giữ lại.

- Thời gian log được giữ lại sẽ bằng **Interval * Rotate** . Cấu hình cần thiết để đạt được 90 ngày lữu trữ log được ghi ở bảng dưới đây:

Cấu hình Interval	Cấu hình Interval theo ngày	Cấu hình Rotate	Thời gian lưu trữ log (Ngày)
daily	1	>= 90	>= 90
weekly	7	>= 13	>= 91
monthly	30	>= 3	>= 90
yearly	365	>= 1	>= 365

4.8. Đồng bộ thời gian HĐH về máy chủ thời gian tập trung (NTP server)

Cách 1: Đồng bộ bằng dịch vụ NTP (Áp dụng cho Oracle7)

Bước 1: Cài đặt:

- Đảm bảo máy chủ có kết nối Internet. Thực hiện cài dịch vụ dưới quyền root:

```
yum install ntp -y
```

Bước 2: Cấu hình đồng bộ thời gian:

- Cấu hình địa chỉ NTP server đồng bộ thời gian:

```
nano /etc/ntp.conf
```

- Ví dụ cấu hình file **ntp.conf**: (Thay địa chỉ domain/IP bằng địa chỉ khả dụng)

```
# /etc/ntp.conf
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst

# /etc/ntp.conf
peer 192.168.1.1 iburst
peer 192.168.1.2 iburst
```

Bước 3: Kích hoạt và chạy tiến trình:

```
systemctl enable ntpd --now
```

Cách 2: Đồng bộ bằng dịch vụ Chrony (Áp dụng cho Oracle7/8/9)

Bước 1: Cài đặt:

- Đảm bảo máy chủ có kết nối Internet. Thực hiện cài dịch vụ dưới quyền root:

```
yum install -y chrony
```

Bước 2: Cấu hình đồng bộ thời gian:

- Cấu hình địa chỉ NTP server đồng bộ thời gian:

```
nano /etc/chrony.conf
```

- Ví dụ cấu hình file **chrony.conf**: (Thay địa chỉ domain/IP bằng địa chỉ khả dụng)

```
# /etc/chrony.conf
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst

# /etc/chrony.conf
peer 192.168.1.1 iburst
```

```
peer 192.168.1.2 iburst
```

Bước 3: Kích hoạt và chạy tiến trình:

```
systemctl enable chronyd --now
```

Cách 3: Đồng bộ bằng ntpdate và crontab (Áp dụng cho Oracle7)

Bước 1: Cài đặt:

- Đảm bảo máy chủ có kết nối Internet. Thực hiện cài dịch vụ dưới quyền root:

```
yum install -y ntpdate
```

Bước 2: Cấu hình crontab định kỳ đồng bộ thời gian:

- Chỉnh sửa cấu hình crontab:

```
crontab -e
```

- Thêm cấu hình định kỳ đồng bộ thời gian. Ví dụ:

```
# crontab -e
*/5 * * * * /usr/sbin/ntpdate -u pool.ntp.org >>
/var/log/ntpdate.log 2>&1
```

- Lưu crontab