**PHỤ LỤC 01: HƯỚNG DẪN CHI TIẾT CẤU HÌNH ATTT CHO**

**HỆ ĐIỀU HÀNH**

# I. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH CENTOS 6.4

1. **Cài đặt và cập nhật bản vá cho hệ điều hành**

* Cài đặt phiên bản mới nhất và cập nhật bản vá của hệ điều hành, không mắc các lỗ hổng bảo mật đã được công bố.
* Kiểm tra phiên bản kernel với lệnh: “uname -a”. Yêu cầu kernel phải được nâng cấp lên phiên bản mới nhất tính tới thời điểm cài đặt.
* Trong trường hợp cập nhật bản vá, nâng cấp kernel:
* Trường hợp có kết nối Internet, thực hiện chạy lệnh sau để nâng cấp kernel:

|  |
| --- |
| *# yum upgrade kernel* |

* Trường hợp không có kết nối Internet, thực hiện chạy lệnh sau để tiến hành cài đặt:
* Bước 1: Cài đặt 1 máy ảo với hệ điều hành tương ứng với hệ điều hành cần nâng cấp kernel. *Chú ý máy ảo này phải có kết nối Internet.*
* Bước 2: Download toàn bộ các gói cần cài đặt nâng cấp kernel mà distro cung cấp về máy ảo:

|  |
| --- |
| *# mkdir /opt/upgrade*  *# yum install yum-downloadonly -y*  *# yum install kernel -y --downloadonly --downloaddir=/opt/upgrade* |

* Bước 3: Tải toàn bộ gói .rpm trong thư mục /opt/upgrade của máy tính lên máy chủ và thực hiện cài như cài gói .rpm như thông thường.

***Lưu ý***: Sau khi cài đặt xong cần khởi động lại máy chủ để hệ điều hành nhận kernel mới.

* Hệ điều hành phải được cập nhật các bản vá security đã được Tập đoàn cảnh báo.

1. **Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết**

Trong thực tế, một server (máy chủ) trong hệ thống sẽ đảm nhiệm một chức năng riêng biệt. Khi cài đặt hệ điều hành cho server, cần xóa hoặc disable tất cả các dịch vụ, ứng dụng, giao thức không cần thiết.

* Bước 1: Liệt kê toàn bộ các gói tin với câu lệnh “yum list”, tìm kiếm các gói tin không cần thiết và thực hiện gỡ bỏ bằng cách sau:

|  |
| --- |
| *# yum remove <package-name>* |

* Bước 2: Liệt kê các dịch vụ đang được chạy ở runlevel 3. Tìm kiếm và xoá bỏ các dịch vụ không cần thiết.

|  |
| --- |
| *# chkconfig --list | grep '3:on'*  *Tìm kiếm các dịch vụ chạy ở mức độ 3 không sử dụng, tiến hành tắt chúng bằng cách:*  *# chkconfig <serviceName> off* |

* Bước 3: Kiểm tra các cổng đang mở trên hệ thống và các dịch vụ đang lắng nghe trên các cổng đó, tiến hành tắt các dịch vụ không cần thiết:

|  |
| --- |
| *# netstat –tulpn*  *Kiểm tra danh sách các dịch vụ không cần thiết, tiến hành tắt các dịch vụ:*  *# service <serviceName> stop* |

1. **Thiết lập chính sách tài khoản**

* Xóa hoặc vô hiệu hóa các toàn khoản không sử dụng trên hệ thống.

|  |
| --- |
| *Bước 1: Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:*  *#cat /etc/passwd | grep /\*sh$ | awk -F: '{print $1}'*  *Bước 2: Kiểm tra xem trong danh sách tài khoản hiện ra xem tài khoản nào không sử dụng. Thực hiện xoá các tài khoản đó bằng lệnh sau:*  *#userdel –r username*  *Ví dụ: Trong danh sách có tài khoản user1 không sử dụng*  *#userdel –r user1* |

* Cấu hình chính sách mật khẩu cho tài khoản:
* Độ dài tối thiểu của mật khẩu phải lớn hơn hoặc bằng 8 ký tự.

|  |
| --- |
| *Bước 1: Mở tập tin /etc/pam.d/system-auth*  *#vi /etc/pam.d/system-auth*  *Bước 2: Thêm hoặc cập nhật cấu hình sau trong tập tin cấu hình của PAM:*  *password requisite pam\_cracklib.so [các option trước đó] 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.

|  |
| --- |
| *Bước 1: Mở tập tin /etc/pam.d/system-auth*  *#vi /etc/pam.d/system-auth*  *Bước 2: Thêm hoặc cập nhật cấu hình sau trong tập tin cấu hình của PAM:*  *password requisite pam\_cracklib.so [các option trước đó] ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1*  *Bước 3: Lưu lại tập tin cấu hình.* |

* Thời gian bắt buộc phải thay đổi mật khẩu: Thiết lập giá trị 90 ngày với hệ thống public và 180 ngày với hệ thống nội bộ. Ví dụ thiết lập với hệ thống public như sau:

|  |
| --- |
| *Mở tập tin /etc/login.defs, thay đổi tuỳ chọn PASS\_MAX\_DAYS, ví dụ:*  *PASS\_MAX\_DAYS 90*  *Với các tài khoản đã tồn tại, có thể sử dụng lệnh sau để thay đổi thời gian hết hạn mật khẩu:*  *#chage –M 90 username*  *Ví dụ, để thay đổi thời gian hết hạn mật khẩu cho tài khoản user1:*  *#chage –M 90 user1* |

* Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất: Thiết lập giá trị là 2 với hệ thống nội bộ và 5 với hệ thống public. Ví dụ thiết lập cho hệ thống nội bộ như sau:

|  |
| --- |
| *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 sufficient trong tập tin cấu hình của PAM:*  *password sufficient pam\_unix.so [các option trước đó] remember=2*  *Bước 3: Lưu lại tập tin cấu hình.* |

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

|  |
| --- |
| *Bước 1: Kiểm tra thuật toán mã hoá sử dụng:*  *#authconfig --test | grep hashing*  *password hashing algorithm is sha512*  *Bước 2: Nếu thuật toán mã hoá sử dụng không phải là sha512, thực hiện sửa đổi và kiểm tra lại:*  *#authconfig --passalgo=sha512 --update*  *#authconfig --test | grep hashing*  *password hashing algorithm is sha512* |

* Mật khẩu không dễ đoán: không bao gồm thông tin cá nhân (tài khoản, họ tên, số điện thoại, số chứng minh thư, ngày tháng năm sinh, mã nhân viên), không được bao gồm các thông tin thông dụng (tên tổ, nhóm, phòng ban, đơn vị, ngày tháng năm thiết lập mật khẩu), không được bao gồm các chuỗi ký tự liên tiếp (từ 4 ký tự trở lên), chuỗi các ký tự giống nhau (từ 4 ký tự trở lên).

Ví dụ: các mật khẩu không được phép: 123456a@, 1234567a@, 12345678a@, qwerty@A, 11112222a@, Hungnh17a@, …

1. **Quản trị từ xa qua kênh truyền an toàn**

Để đảm bảo yêu cầu bảo mật cho hệ thống, tránh trường hợp thất thoát dữ liệu trên đường truyền khi quản trị hệ thống từ xa yêu cầu thiết lập và sử dụng các dịch vụ quản trị an toàn. Cụ thể nếu sử dụng SSH để quản trị cho Centos 6.x thì thực hiện các thiết lập sau như sau:

* Yêu cầu 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 2: Lưu lại tập tin và khởi động lại dịch vụ ssh.* |

* 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.* |

* 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* |

1. **Phân quyền tập tin và thư mục**

* Xác thực đường dẫn các biến môi trường PATH:

|  |
| --- |
| *Để kiểm tra đường dẫn PATH, ta dùng lệnh sau:*  *#echo $PATH*  *Ví dụ:*  *PATH có chứa đường dẫn trống: /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin****::***  *PATH có chứa đường dẫn tương đối: /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:****./src/bin***  *PATH có chứa đường dẫn nguy hiểm: /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:****/tmp*** |

* 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: 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* |

1. **Cài đặt và cấu hình firewall mềm**

* Yêu cầu sử dụng firewall mềm trên hệ thống.

|  |
| --- |
| *Kiểm tra chế độ của iptables trên hệ thống để chắc chắn chế độ 3 đang là On (dịch vụ sẽ tự động khởi động cùng hệ điều hành):*  *# chkconfig --list | grep iptables*  *Nếu đang ở trạng thái Off thì cấu hình như sau để iptables khởi động cùng hệ thống:*  *#chkconfig –level 345 iptables on*  *Kiểm tra trạng thái hiện tại của iptables:*  *#service iptables status* |

* Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống.

Sử dụng 2 lệnh chính sau:

* iptables-save: lưu lại toàn bộ rule ra một file text có định dạng đặc biệt
* iptables-restore: load rule từ file text đã lưu trước đó.

Cú pháp sử dụng:

* Lệnh iptables-save:

|  |
| --- |
| *# iptables-save > /etc/iptables-save* |

Lưu ý: /etc/iptables-save là file lưu lệnh iptables, có thể thay đổi thành file bất kỳ.

* Lệnh iptables-restore:

|  |
| --- |
| *# iptables-restore < /etc/iptables-save* |

Tất cả các rule trong file /etc/iptables-save sẽ được load và áp dụng vào iptables.

Ý nghĩa của file được lưu bởi lệnh iptables-save:

|  |
| --- |
| *# Generated by iptables-save v1.4.7 on Fri Jul 10 22:34:12 2015*  *\*filter*  *:INPUT ACCEPT [0:0]*  *:FORWARD ACCEPT [0:0]*  *:OUTPUT ACCEPT [129895:7030615]*  *-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT*  *-A INPUT -p udp -m state --state NEW -m udp --dport 123 -j ACCEPT*  *-A INPUT -p icmp -j ACCEPT*  *-A INPUT -i lo -j ACCEPT*  *-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT*  *-A INPUT -j REJECT --reject-with icmp-host-prohibited*  *-A FORWARD -j REJECT --reject-with icmp-host-prohibited*  *COMMIT*  *# Completed on Fri Jul 10 22:34:12 2015* |

Trong đó:

* “\*filter”: Chỉ bắt đầu các rule của table filter, table dùng để viết các rule lọc gói tin.
* :INPUT ACCEPT [0:0]
  + INPUT: là chain của iptables, table filter có 3 chain là INPUT, OUTPUT, FORWARD. Trong đó INPUT là thời điểm gói tin đi vào hệ thống, OUTPUT là thời điểm gói tin đi ra hệ thống, còn FORWARD là thời điểm gói tin đi từ card mạng này sang card mạng khác.
  + ACCEPT: Chain policy của chain INPUT, OUTPUT và FORWARD. Ý nghĩa: Nếu gói tin sau khi được kiểm tra bởi tất cả các rule của iptables mà không có rule nào khớp thì sẽ được ACCEPT.
  + [0:0]: Số đầu tiên chỉ ra số lượng gói tin, số thứ 2 chỉ ra dung lượng của các gói tin. Đây là các thông số thống kê về các gói tin không khớp luật nào của iptables, và do đó được thực hiện Chain policy là ACCEPT.
* Các rule tiếp theo: Là rule lọc của iptables, sẽ áp dụng từ trên xuống dưới.
* COMMIT: Đánh dấu kết thúc bảng filter.

Cách sửa luật iptables:

Tạo một file có nội dung như sau, ví dụ là /etc/sysconfig/iptables:

|  |
| --- |
| *# Firewall configuration written by system-config-firewall*  *# Manual customization of this file is not recommended.*  *\*filter*  *:INPUT ACCEPT [0:0]*  *:FORWARD ACCEPT [0:0]*  *:OUTPUT ACCEPT [0:0]*  *### Cho phép các gói tin thuộc 1 kết nối đang tồn tại hoặc có liên quan đến 1 connection đang tồn tại đi vào, không cần kiểm tra ###*  *-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT*  *-A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT*  *### Cho phép ping echo request đến server ###*  *-A INPUT -p icmp --icmp-type 8 -j ACCEPT*  *### Nhứng gói tin từ card mạng loopback thì không cần lọc ###*  *-A INPUT -i lo -j ACCEPT*  *### Thêm nhưng luật lọc chiều INPUT tại đây ###*  *# Ví dụ luật cho phép 1 IP hay 1 dải IP SSH đến server #*  *-A INPUT -m state --state NEW -s 192.168.1.190 -m tcp -p tcp --dport 22 -j ACCEPT*  *-A INPUT -m state --state NEW -s 192.168.2.0/24 -m tcp -p tcp --dport 22 -j ACCEPT*  *# Ví dụ luật cho phép HTTP #*  *-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT*  *### Thêm các luật lọc chiều OUTPUT tại đây ###*  *### Chỉ khi server cần chủ động kết nối ra bên ngoài mưới thêm luật tiếp theo ###*  *# Ví dụ luật cho phép server hiện tại ssh đến server 10.10.10.10 #*  *-A OUTPUT -m state --state NEW -d 10.10.10.10 -m tcp -p tcp --dport 22 -j ACCEPT*  *### Chặn toàn bộ các kết nối còn lại, ghi log trước khi chặn ###*  *-A INPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"*  *-A FORWARD -j LOG --log-level 4 --log-prefix "IPTABLES DROP"*  *-A OUTPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"*  *-A INPUT -j REJECT --reject-with icmp-host-prohibited*  *-A FORWARD -j REJECT --reject-with icmp-host-prohibited*  *-A OUTPUT -j REJECT --reject-with icmp-host-prohibited*  *COMMIT* |

Cách cấu hình để iptables nạp các rule khi server khởi động lại:

|  |
| --- |
| *Thêm dòng sau vào cuối file /etc/rc.local:*  *iptables-restore < /etc/sysconfig/iptables* |

Cách tạm thời tắt tất cả các luật của iptables để troubleshoot:

|  |
| --- |
| *Sử dụng các lệnh sau:*  *# iptables –F*  *# iptables –X*  *# iptables –P INPUT ACCEPT*  *# iptables –P OUTPUT ACCEPT*  *# iptables –P FORWARD ACCEPT* |

Ý nghĩa các lệnh:

* Lệnh đầu tiên để xoá tất cả các rule trong tất cả các chain của iptables
* Lệnh thứ 2 xoá tất cả các chain do người dùng tự tạo
* Lệnh 3,4,5 thiết lập chain policy cho chain INPUT, OUTPUT, FORWARD là ACCEPT, khi đấy server cho phép toàn bộ kết nối vào/ra server.
* Ghi log những bản ghi vào/ra không hợp lệ.

|  |
| --- |
| *Lưu ý thêm các dòng sau vào file cấu hình iptables: -A INPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"*  *-A FORWARD -j LOG --log-level 4 --log-prefix "IPTABLES DROP"*  *-A OUTPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"* |

1. **Thiết lập chính sách quản lý log**

* Ghi log mặc định của hệ điều hành: Ghi log các hành vi quan trọng của máy chủ: Yêu cầu thiết lập cấu hình ghi log tối thiệu các loại sau: message log, dmesg log, secure log.

Cấu hình rotate log tối đa là 1 lần/tháng.

* Bước 1: Cấu hình nội dung tập tin /etc/rsyslog.conf với nội dung sau:

|  |
| --- |
| *$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)*  *$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*  *authpriv.\**  *mail.\**  *cron.\**  *\*.emerg*  *uucp,news.crit*  *local7.\** |

* Bước 2: 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 1*  *}*  */var/log/btmp {*  *missingok*  *monthly*  *create 0600 root utmp*  *rotate 1*  *}* |

* Bước 3: 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 4: Khởi động lại dịch vụ log:

|  |
| --- |
| *#/etc/init.d/rsyslog restart*  *Shutting down system logger: [ OK ]*  *Starting system logger: [ OK ]* |

* 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.
* Trên centOS 6.4, 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.
* Đồng bộ thời gian HĐH về máy chủ tập trung:

|  |
| --- |
| *Bước 1: Cài đặt:*   * + *Đối với máy chủ có kết nối Internet:*   *# yum install ntp*   * *Đối với máy chủ không có kết nối Internet:*   *Download gói ntp dạng rpm: ntp-4.2.6p5-1.el6.centos*  *Copy gói cài đặt lên máy chủ, chuyển tới thư mục chứa tập tin và chạy lệnh:*  *#rpm –ivh {Tên tập tin}*  *Bước 2: Cấu hình dịch vụ NTP*   * *Cấu hình dịch vụ ntpd luôn chạy khi khởi động máy chủ:*   *#chkconfig ntpd on*   * *Sửa tập tin cấu hình /etc/ntp.conf như sau:*   *restrict default kod nomodify notrap nopeer noquery*  *restrict -6 default kod nomodify notrap nopeer noquery*  *restrict 127.0.0.1*  *restrict -6 ::1*  *server ntp-server*   * *Đảm bảo file cấu hình ntp có cấu hình tham số serer, trong đó tham số ntp-server là hostname hoặc địa chỉ IP của NTP server.* * *Chạy dịch vụ ntpd và khởi động lại dịch vụ iptables bằng lệnh:*   *#service ntpd start*  *#service iptables restart*   * *Kiểm tra lại dịch vụ bằng lệnh:*   *#netstat -tulpn | grep ntpd* |

* Cấu hình lưu log command người dùng hệ thống:
* Bước 1: Thực hiện backup toàn bộ các file cấu hình phục vụ rollback khi cấu hình.
  + 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* |

* + Với Solaris server:

|  |
| --- |
| *#cp /etc/profile /etc/profile.back*  *#cp /etc/syslog.conf /etc/syslog.conf.back* |

* + 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
  + **Với Linux (CentOS, Redhat)**

Thêm vào cuối file **/etc/bashrc:**

|  |
| --- |
| *export PROMPT\_COMMAND='RETRN\_VAL=$?;logger -plocal6.debug "[cmdlog] $(whoami) [$$]: $(history 1 | sed "s/^[ ]\*[0-9]\+[ ]\*//" ) [$RETRN\_VAL] [$(echo $SS\_CLIENT | cut -d" " -f1)]"'* |

Cấu hình đẩy log vào file chứa logs:

Thêm dòng cấu hình sau vào file /etc/syslog.conf hoặc /etc/rsyslog.conf tùy thuộc vào server chạy syslog hay rsyslog (recommend 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* |

Các bước cấu hình cho rotate log, tạo file cmdlog trong /etc/logrotate.d có nội dung sau:

|  |
| --- |
| *# /etc/logrotate.d/cmdlog*  */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*  *}* |

* + **Với server Unix**

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

|  |
| --- |
| *PROMPT\_COMMAND='RETRN\_VAL=$?;logger -p local6.debug "[cmdlog] $/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 file /etc/syslog.conf (recommend thêm vào sau dòng local7.\* /var/log/boot.log, cho dễ kiểm soát).

|  |
| --- |
| *# Log cmdlog*  *local6.debug /var/log/cmdlog.log* |

Tạo file ghi log trong thư mục lưu trữ log

|  |
| --- |
| *Touch /var/log/cmdlog.log* |

Khởi động lại syslog bằng lệnh

|  |
| --- |
| */etc/init.d/syslog stop*  */etc/init.d/syslog start*  *Hoặc*  *Svcadm restart system-log* |

Kiểm tra việc ghi log trong files ghi 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/adm/cmdlog.log -z 0* |

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

|  |
| --- |
| *logadm -C 12 –p 1w –w /var/adm/cmdlog.log -z 0* |

* + **Với server Linux Suse**

Thêm vào cuối file **/etc/bashrc:**

|  |
| --- |
| *export PROMPT\_COMMAND='RETRN\_VAL=$?;logger -plocal6.debug "[cmdlog] $(whoami) [$$]: $(history 1 | sed "s/^[ ]\*[0-9]\+[ ]\*//" ) [$RETRN\_VAL] [$(echo $SSH\_CLIENT | cut -d" " -f1)]"'* |

Cấu hình đẩy log vào file chứa logs

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

|  |
| --- |
| *filter f\_cmdlog { level(debug) and facility(local6); };*  *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* |

Các bước cấu hình cho rotate log, tạo file cmdlog trong /etc/logrotate.d có nội dung sau:

|  |
| --- |
| */var/log/cmdlog.log*  *{*  *compress*  *weekly*  *rotate 12*  *sharedscripts*  *postrotate*  */etc/init.d/syslog reload*  *endscript*  *}* |

* 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/adm/cmdlog.log với Unix và var/log/cmdlog.log với Linux.

- 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]* |

1. **Cài đặt các hệ thống bảo vệ và giám sát hệ thống**

**8.1 Cài đặt phần mềm Server Endpoint hỗ trợ giám sát bất thường và vi phạm Baselines**

Điều kiện đảm bảo:

* Id cho agent được cài đặt phải được khai báo với hệ thống trước khi bắt đầu cài đặt cho agent. Id của agent là duy nhất.
* Id agent có format như sau: **TênHĐH\_Ipv4**. Ví dụ: **windows\_10.10.0.1**
* Các đơn vị khác VTNet, đề nghị khi tạo ID bổ sung prefix tên viết tắt của đơn vị (VD: vtidc, vtt, vttek,..). Ví dụ: **vtt\_centos\_10.30.58.164**
* Toàn bộ sử dụng chữ viết thường
* Tên hệ điều hành là windows, centos, redhat, oracle, solaris, suse …
* Địa chỉ IP theo chuẩn IP v4.
* Chương trình cài đặt bắt buộc chạy với user Administrator đối với hệ hiều hành Windows và user root với hệ điều hành Linux, Solaris.
* Đối với các agent tương ứng cần có các gói sau:

| **Linux** |  |
| --- | --- |
| wget | Download dữ liệu từ repository |
| unzip | Giải nén file nén chứa file cài đặt |
| **Windows** |  |
| powershell | Giao diện quản trị lệnh của Windows |
| vcredist | Lib c trên windows |

* Thông kết nối từ agent tới server tập trung (10.30.160.44, 10.30.160.45, 10.30.160.46) tương ứng các cổng sau: **80, 443, 4505, 4506, 6379.**
* Kiểm tra kết nối từ máy tính của người thực hiện tới địa chỉ portal của hệ thống SIRC (10.30.160.41) cổng 80 (http), 443 (https) và 8443 (https).
* Phân giải được các domain của hệ thống SIRC. Mặc định trên hệ thống DNS đã có cấu hình domain này, trong trường hợp chưa phân giải được, cấu hình file host trên máy tính của người thực hiện cài đặt để truy cập vào trang web quản trị:

|  |
| --- |
| 10.30.160.41 srm.sirc.viettel.com  10.30.160.41 se.sirc.viettel.com  10.30.160.41 cas.sirc.viettel.com |

**Bước 1:** Khai báo server\_id trên Portal <http://se.sirc.viettel.com/#/server/list>

Chú ý: Đối với các server cài lại cần vào Portal trên thực hiện thao tác **Reject**, sau đó khoảng 1 phút **Renew** lại cert của server cần cài lại, và cài đặt bình thường

**Bước 2:** Download file se-install.sh

wget http://10.30.160.44/serverendpoint/se-install.sh

**Bước 3:** Cài đặt theo cú pháp:

|  |
| --- |
| bash se-install.sh <server\_id> <master>  For example:  bash se-install.sh test\_192.168.10.10 10.30.160.44  bash se-install.sh test\_centos\_192.168.10.10 |

Trong đó:

* Server\_id: là server\_id đã được khai báo trên Hệ thống SE ở bước 1
* Master: là IP Address của Master, nếu bỏ qua không nhập, script sẽ tự hiểu mặc định là 10.30.160.44

**Bước 4:** Kiểm tra cài đặt thành công

|  |
| --- |
| /opt/se/salt-call vsm.status  ret:  local:  ----------  version:  2014.7.4 |

**8.2 Cài đặt filebeat**

a. Điều kiện kết nối

| **STT** | **Đích** | **Port** | **Ghi chú** |
| --- | --- | --- | --- |
| 1 | 10.30.160.44 | 80/TCP, 443/TCP | Kết nối đến repo (thường đã có khi cài SE Agent) |
| 2 | 10.30.160.41 | 514/TCP+UDP, 5044/TCP, 6379/TCP, 9092/TCP, 9080-9100 TCP | Kết nối đến hệ thống Log tập trung |

b. Cài đặt

 Tải bộ cài tương ứng từ SE-Repo [LogAgent - http://10.30.160.44/serverendpoint/logagent/](http://10.30.160.44/serverendpoint/logagent/)

* Debian/Ubuntu tải file deb, Centos/RedHat tải file rpm, tương đương với kiến trúc
* Các server linux khác thì tải bản se\_filebeat tương đương.

 Cài đặt bộ cài

* **Debian/Ubuntu**:
  + dpkg -i filebeat-xxx.deb
  + mkdir -p /etc/filebeat/filebeat.d
* **Centos/RedHat**:
  + rpm -Uvh fileabeat-xxx.rpm
  + mkdir -p /etc/filebeat/filebeat.d
* **Các Distro Linux khác**:
  + Giải nén unzip se\_filebeat-xxx.zip
  + Vào thư mục được giải nén ra cd filebeat-xxx
  + Install binary, create service ./install
  + Chạy câu lệnh mkdir -p /etc/filebeat/filebeat.

c. Cấu hình

* Dùng server\_id của **SE-Agent** làm tên của **LogAgent**, cấu hình trong shipper.name (server\_id xem trong /etc/salt/minion.d/id.conf, cấu hình cụ thể xem ở dưới cho từng OS)

name: vtt\_centos\_10.10.0.132

* Cấu hình gửi log lên server 10.30.160.41:5044/TCP với các dải mạng nội bộ của **SIRC** thì dùng IP cấu riêng để vào, phía server cần mở **Firewall**
* Tất cả các file cấu hình đều là định dạng yml, dùng dấu cách space thay vì tab, lưu ý về các khoảng cách này
* File cấu hình mặc định filebeat.yml được copy từ nội dung trong hướng dẫn, tất cả các cấu hình thêm sau này, thì nên đưa vào filebeat.d/extra.yml để tiện sửa chữa hay cài mới ko bị mất

|  |
| --- |
| # filebeat.d/filebeat.yml  # follow this hierachy  filebeat:  prospectors:  -  paths:  #- C:\Windows\System32\LogFiles\W3SVC3\ex??????.log  #- C:\salt\var\log\salt\minion  #- C:\ProgramData\VMware\vCenterServer\logs\vmware-vpx\vpxd-\*.log  input\_type: log |

Lấy toàn bộ log liên quan đến auth, audit, mail, access … của hệ thống, nếu có file không nằm trong thư mục chuẩn, thì chủ động thêm vào bằng tay. Sửa file /etc/filebeat/filebeat.yml

|  |
| --- |
| filebeat:  prospectors:  -  paths:  - /var/log/messages  - /var/log/authlog  - /var/log/auth.log  - /var/log/secure  - /var/log/secure.log  - /var/log/system.log  - /var/log/syslog  - /var/log/ipfilter.log  - /var/adm/ipsec.log  - /var/adm/syslog  - /var/adm/auth.log  - /var/adm/syslog.log  - /var/adm/messages  - /var/adm/syslog/syslog.log  - /var/log/userlog  - /var/log/security  - /var/log/xferlog  - /var/log/proftpd.log  - /var/log/vsftpd.log  - /var/log/radius.log  - /var/log/radius/radius.log  - /var/log/mail.info  - /var/log/mail.notice  - /var/log/maillog  - /usr/local/squid  - /var/logs/access.log  - /var/log/squid/access.log  - /var/log/horde.log  - /var/log/asl.log  - /var/log/dpkg.log  - /var/log/vmware/hostd.log  - /var/log/proftpd/proftpd.log  - /var/log/apache/error.log  - /var/log/apache/error\_log  - /var/log/apache/access.log  - /var/log/apache/access\_log  - /var/www/logs/access\_log  - /var/www/logs/error\_log  - /var/log/httpd/error\_log  - /var/log/httpd/access\_log  - /var/log/nginx/access.log  - /var/log/nginx/error.log  - /var/log/apache2/error.log  - /var/log/apache2/access.log  - /var/log/snort/alert  - /var/log/salt/minion  - /var/log/cmd.log  input\_type: log  registry\_file: /var/lib/filebeat/registry  config\_dir: /etc/filebeat/filebeat.d  output:  logstash:  hosts: ["10.30.160.41:5044"]  worker: 1  compression\_level: 3  index: beat\_agent  shipper:  name: <server\_id>  logging:  to\_syslog: false  to\_files: true  level: warning  files:  path: /var/log/filebeat  name: filebeat.log  rotateeverybytes: 10485760  keepfiles: 7 |

d. Chạy và kiểm tra

* Kiểm tra thông kết nối đến server Log bằng lệnh telnet

telnet 10.30.160.41 5044

* Chạy thử và kiểm tra cấu hình, chuyển thư mục đến chỗ có file chạy(trong CMD)
  + filebeat -e -v -c filebeat.yml
  + winlogbeat -e -v -c winlogbeat.yml
* Nếu output không có lỗi gì thì cấu hình là OK
* Chạy tiến trình dạng service:
  + Khởi động service /etc/init.d/filebeat start
  + Check kết quả đầu ra trên server
* Setup để service khởi động cùng hệ thống. Tùy theo OS để set thuộc tính này, có thể tham khảo cách sau
  + Chạy câu lệnh chkconfig filebeat on hoặc update-rc.d filebeat defaults

e. Tích hợp cho các loại log phổ biến

**Log Squid**

* Mặc định, sau khi cài đặt, squid có filelog ở /var/log/squid/access.log
* Cấu hình của filebeat mặc định đã lấy log từ file này
* Nếu cấu hình sang file khác, thêm đường dẫn tương ứng vào cấu hình
* Restart service filebeat /etc/init.d/filebeat restart

**Log SSO**

**SSO** là hệ thống Single Sign On của tập đoàn, được chạy trên nhiều node. Các server này, sau khi cài filebeat cần thêm đường dẫn tương ứng của file log vào để đẩy lên hệ thống Log tập trung. Đường dẫn nằm trong thư mục logs của ứng dụng, lấy file logUserAuthen.log, ví dụ:

/u01/app/SSO/Tomcat\_SSO\_PP\_8180/logs/logUserAuthen.log

Sau khi thêm vào cấu hình tương ứng, thì khởi động lại filebeat

**8.3 Cài đặt OSSEC Agent để hỗ trợ thu thập log webserver, log ứng dụng, log firewall, log command (đối với các OS không hỗ trợ filebeat CentOS <=5)**

**Chuẩn bị**

* File cài đặt ossec cho Linux phiên bản hiện tại là ossec-hids-2.5.1.tar.gz. Tải: http://www.ossec.net/files/ossec-hids-\<version>.tar.gz
* Key file: Được cung cấp bởi P. ATTT được sinh ra trên server, mục đích xác thực giữa server và agent, mỗi agent sẽ có 1 key khác nhau.
* Mở port 1514 UDP, 514 UDP trên firewall.
* Kiểm tra máy chủ đảm bảo có gcc
* which gcc

**Cài đặt**

Đăng nhập hệ thống với account **root**.

# Bước 1: Copy ossec-hids-.tar.gz lên server, thực hiện giải nén.

* cd vào thư mục chứa file ossec-hids-\<version>.tar.gz. Giải nén:
* tar -xzvf ossec-hids-<version>.tar.gz

# Bước 2: Sau khi thực hiện các bước trên sẽ xuất hiện thư mục

ossec-hids-<version>

* Thực hiện cd vào thư mục này, chạy file install.sh

cd ossec-hids-<version>

./install.sh

* Màn hình giới thiệu hiện ra, bấm [Enter] để tiếp tục.

Tùy chọn ngôn ngữ hiện ra gõ en để chọn ngôn ngữ là English.

Gõ agent [Enter] để chọn chế độ cài đặt là agent.

Gõ /var/ossec [Enter] để cài ossec vào thư mục /var/ossec

Nếu là các server có IP DCN:

10.60.97.12 [Enter]

Gõ y [Enter]

Gõ y [Enter]

[3.4 Do you want to enable active response?]: Chú ý chọn **n** trong tùy chọn này.

Gõ n [Enter]

Gõ [Enter] để sang bước 5, quá trình biên dịch bắt đầu. Quá trình biên dịch bắt đầu, đợi cho tới khi việc biên dịch mã nguồn hoàn thành. Sau 1 khoảng thời gian ngắn, quá trình biên dịch thành công bấm [Enter] để hoàn tất qúa trình cài đặt.

# Bước 3: Import key authentication cho ossec agent.

cd vào thư mục /var/ossec/bin. Chạy file /var/ossec/bin/manage\_agents

[Choose your action: I or Q:]

Gõ I [Enter]

[Paste it here(or '\q' to quit):] Mở Key.txt đã được cung cấp bởi P.ATTT copy vào paste vào dấu nhắc lệnh.

Trong trường hợp ví dụ này là chuỗi:

MDAxIGFnZW50MSAxOTIuMTY4LjEuMTAwIDg4MWQ4YWMxY2U1NDY0OGFlZTJiNWJkZTcxN2JlMjViN2Y3ZGNkOTM1MzVhMWU4ZGQyZWEwZTgxZGNiNjdkOTc=

Sau khi paste key vào và bấm Enter chương trình sẽ hiển thị thông tin về key như agent, name, IP. Nếu IP giống với IP agent thì sang bước tiếp theo.

Agent information:

ID: 001

Name: agent1

IP Address:192.168.1.100

[Comfirm adding it?(y/n)]

Gõ y [Enter]

Start ossec:

/var/ossec/bin/ossec-control start

Kiểm tra lại việc kết nối đến server đã thành công!!!

more /var/ossec/logs/ossec.log | grep Connected

Nếu xuất hiện dòng “Conmected to the server...” như hình bên dưới thì quá trình kết nối thành công.

# Bước 4: Cấu hình ossec.conf

Yêu cầu khi cài đặt ossec phải cấu hình ossec monitor đầy đủ các log(nếu có): Log Webserver(IIS, Apache, Ngnix, lightto, Tomcat....), log ứng dụng, log firewall...

Cấu hình OSSEC monitor log ứng dụng, hệ điều hành. Hai thông số cơ bản khi cấu hình là location và log\_format.

| **Thông số** | **Ý nghĩa** |
| --- | --- |
| \<location>**location**\</location> | Đường dẫn đến file log. |
| \<log\_format>**log\_format**\</log\_format> | Định dạng log |
| OSSEC hỗ trợ định dạng log của các ứng dụng phổ biến: snort-full, snort-fast, squid, iis, eventlog, mysql\_log, postgresql\_log, nmapg, apache. Ngoài ra OSSEC còn hỗ trợ định dạng syslog, mỗi mục log được ghi trên 1 dòng. |  |
| Ví dụ: log-2011-06-27.log có một đoạn như sau là định dạng syslog. |  |

|  |
| --- |
| 2011/06/27 14:50:29 ossec-execd(1350): INFO: Active response disabled. Exiting.  2011/06/27 14:50:29 ossec-agent(1410): INFO: Reading authentication keys file.  2011/06/27 14:50:29 ossec-agent: INFO: No previous counter available for 'agent' |

Ví dụ để monitor file log có đường dẫn Path\_to\_log\log-%y-%m-%d.log thì thêm dòng sau vào ossec.conf:

|  |
| --- |
| <localfile>  <location>Path\_to\_log\log-%y-%m-%d.log</location>  <log\_format>syslog</log\_format>  </localfile> |

Trong đó: + "Path\_to\_log": Thư mục ghi log (VD: /u03/tomcat/webapp/myweb/logs) + "log-%y-%m-%d.log": OSSEC monitor file log của ngày hiện tại.

%y: Năm hiện tại

%m: Tháng hiện tại

%d: Ngày hiện tại

VD: Ngày 27/6/2011 OSSEC sẽ monitor file log-2011-06-27.log trong thưc mục /u03/tomcat/webapp/myweb/logs

Cấu hình monitor log Apache. Theo mặc định Apache sẽ lưu log tại /var/log/httpd. Thêm các dòng sau vào ossec.conf

|  |
| --- |
| <localfile>  <location>/var/log/httpd/error.log</location>  <log\_format>apache</log\_format>  </localfile>  <localfile>  <location>/var/log/httpd/access.log</location>  <log\_format>apache</log\_format>  </localfile>  <localfile>  <location>/var/log/httpd/modsec\_audit.log</location> # Nếu có sử dụng  <log\_format>syslog</log\_format> # mod\_security  </localfile> # cho Apache |

Cấu hình ossec.conf monitor log hệ thống, iptables và cmdlog: Thêm các dòng sau vào ossec.conf

|  |
| --- |
| <localfile>  <location>/var/log/iptables/iptables.log</location>  <log\_format>syslog</log\_format>  </localfile>  <localfile>  <location>/var/log/cmdlog.log</location>  <log\_format>syslog</log\_format>  </localfile> |

Sau khi cấu hình xong khởi động lại ossec-agent để các thiết lập có hiệu lực. Restart ossec:

|  |
| --- |
| /var/ossec/bin/ossec-control restart |

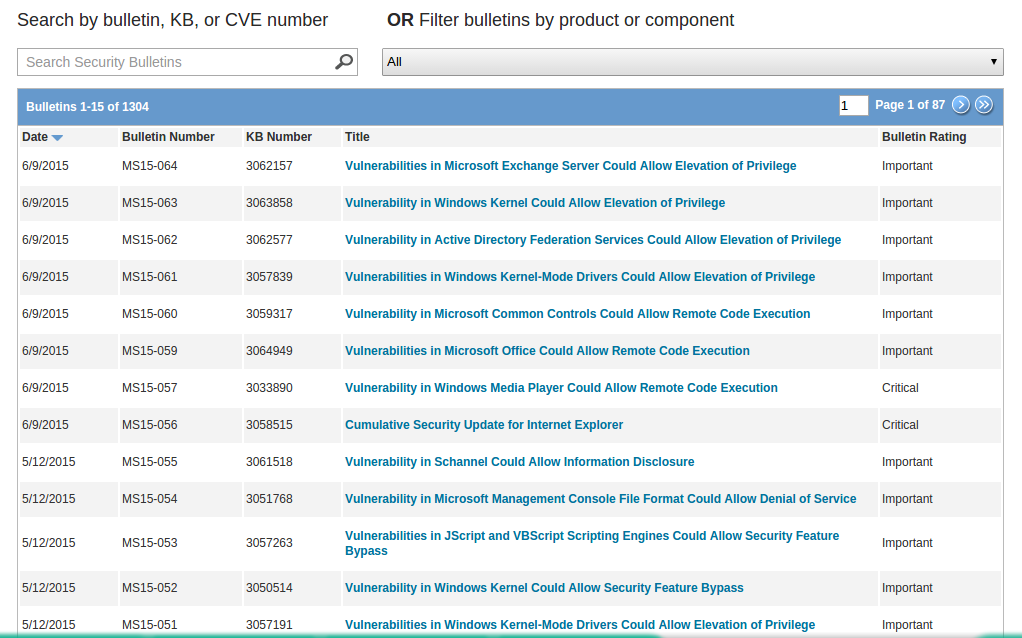
# II. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH WINDOWS SERVER 2008

1. **Cài đặt hệ điều hành và cập nhật bản vá**

Khi tiến hành cài đặt một hệ điều hành, một trong những yêu cầu đầu tiên phải thực hiện đó là cài đặt các bản vá hoặc upgrade version mới nhất nhằm tránh các lỗ hổng về bảo mật đã tồn tại trong các phiên bản cũ.

* Với mỗi phiên bản hệ điều hành Windows Server yêu cầu nâng cấp lên phiên bản Service Pack mới nhất.
* Đối với hệ điều hành Windows Server cài đặt mới, yêu cầu cài đặt phiên bản Windows Server 2008 R2 Service Pack 2 trở lên.
* Hệ điều hành phải được cập nhật các bản vá security đã được Tập đoàn cảnh báo.
* Trup cập trang: <https://technet.microsoft.com/en-us/security/bulletin/>

Thực hiện cập nhật bản vá mới nhất từ nhà phát triển cho hệ điều hành Windows Server tại đây.

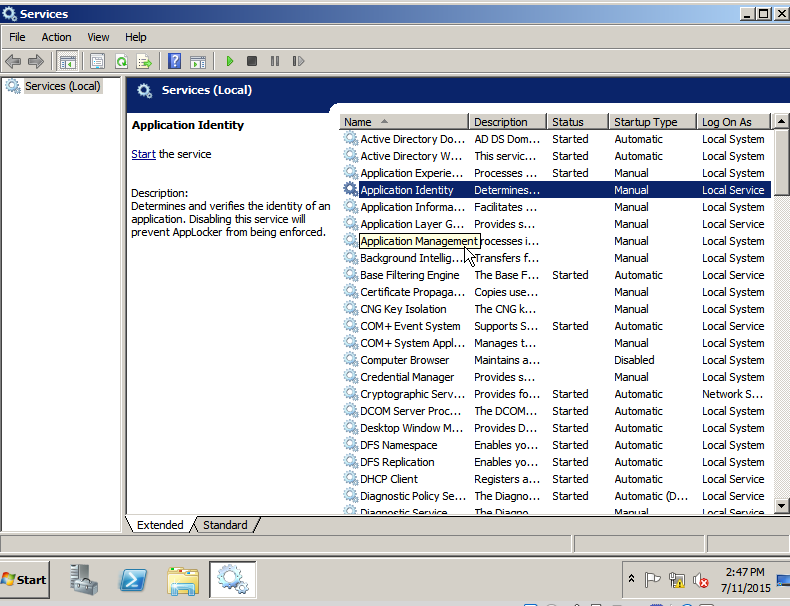


* Lưu ý: Phải tiến hành thử nghiệm trên hệ thống giả lập trước khi cập nhập bản vá và phải kiểm tra các lại dịch vụ của máy chủ sau khi thực hiện nâng cấp.

1. **Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết**

Trong thực tế, mỗi server (máy chủ) trong hệ thống sẽ đảm nhiệm một chức năng riêng biệt. Khi cài đặt hệ điều hành cho máy chủ, cần xóa hoặc disable tất cả các dịch vụ, ứng dụng, giao thức không cần thiết.

* Bước 1: Click chuột phải vào biểu tượng start của **Windows => Administrative Tools => Services.**
* Bước 2: Tìm và disabled các dịch vụ không cần thiết.



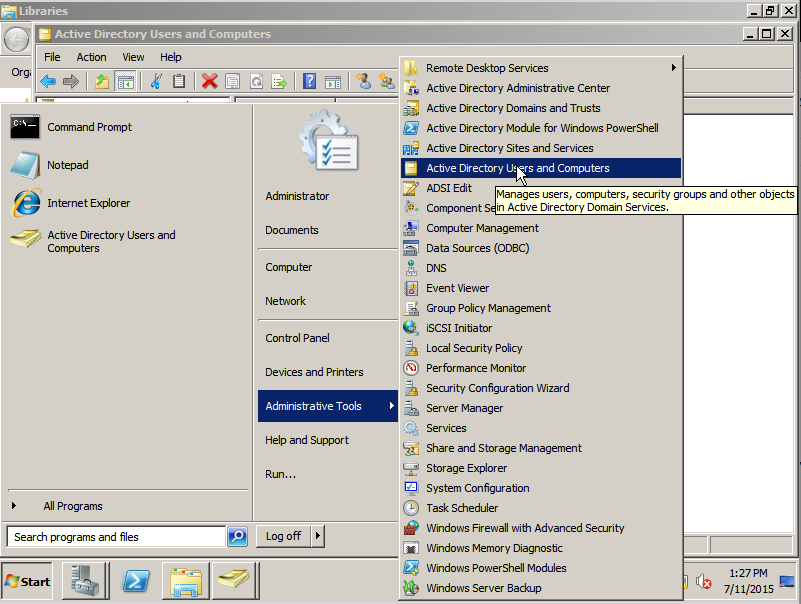
Thông thường, một số dịch vụ, ứng dụng, giao thức sau nên được xóa hoặc disable nếu không sử dụng:

* Dịch vụ chia sẻ file và printer: NFS, FTP, NetBios,..
* Wireless networking.
* Chương trình hỗ trợ remote control hoặc remote access không an toàn: telnet.
* Directory services: LDAP, NIS.
* Webserver, webservices.
* Email services: smtp.
* Language compilers, libraries.
* System development tools.
* System and network management tools and utilities: SNMP.

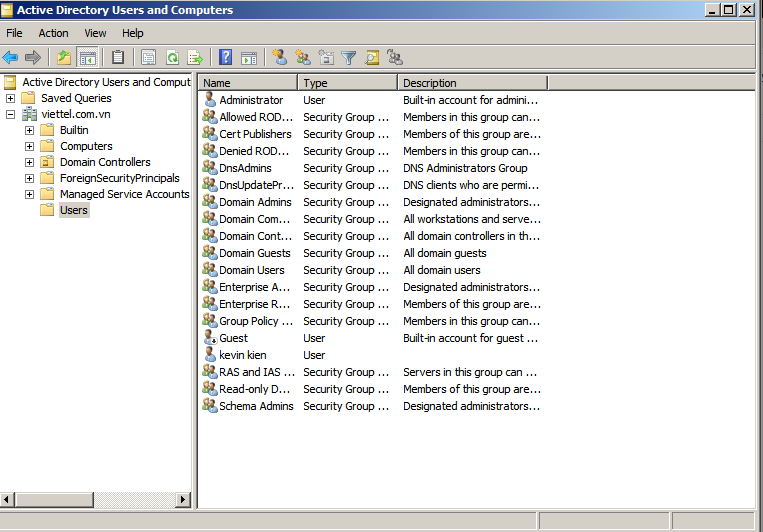
1. **Thiết lập chính sách tài khoản**

Các tài khoản mặc định của hệ thống, các tài khoản dễ đoán thường là mục tiêu tấn công, dò quét của các attacker. Mặc định hệ thống thường cung cấp các tài khoản như tài khoản guest, administrator,...với những mật khẩu mặc định.

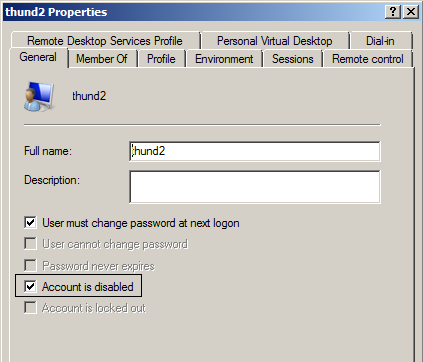
* Xóa hoặc vô hiệu hóa các toàn khoản không sử dụng trên hệ thống:
* Kiểm tra tài khoản trên Local:
* Bước 1: Click chuột phải vào My Computer => Mangager => Configuration => Local User and group => Users/Groups.
* Bước 2: Kiểm tra user nào không sử dụng xóa hoặc disable.
* Kiểm tra tài khoản trên máy domain controller:
  + Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Active Directory Users and Computers.



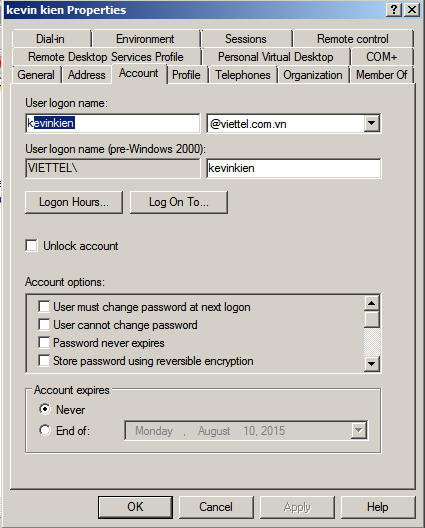
* Bước 2: Click vào User/Group. Xóa hoặc disable tài khoản không sử dụng.



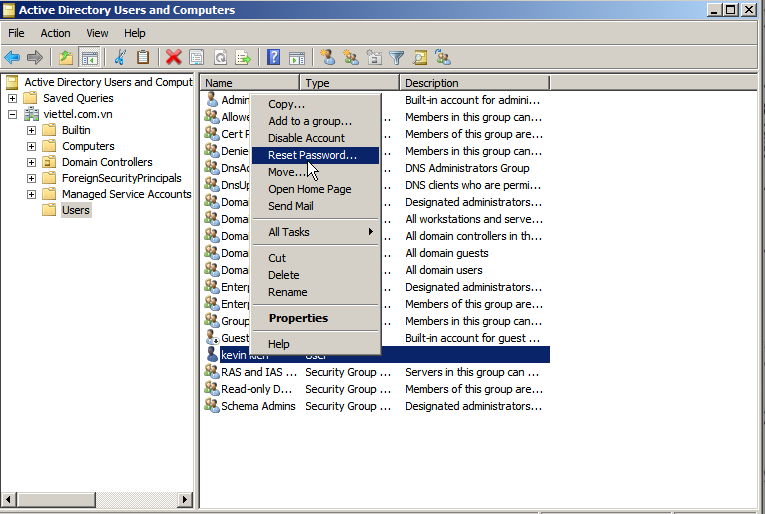
* Thay đổi tên, mật khẩu cho các tài khoản mặc định.
* Thay đổi user, password trên máy Local: Vào Start => Programs => Administrative Tools => Server Manager Configuration => Configure => Local Users and Group => Users => Click chuột phải vào user => Properties => Account is disabled.



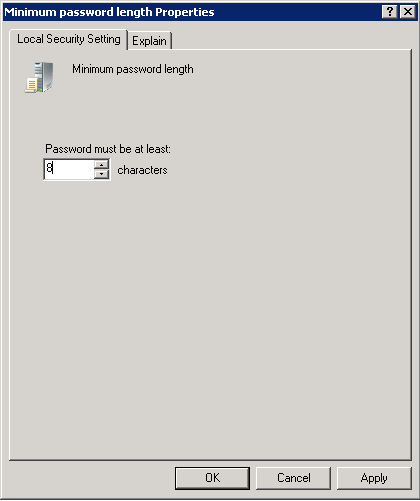
* Thay đổi tên, mật khẩu trên máy Domain Controller:
* Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Active Directory Users and Computers => User.
* Bước 2: Chọn tài khoản muốn thay đổi => Properties => Account. Thay đổi user muốn đổi.



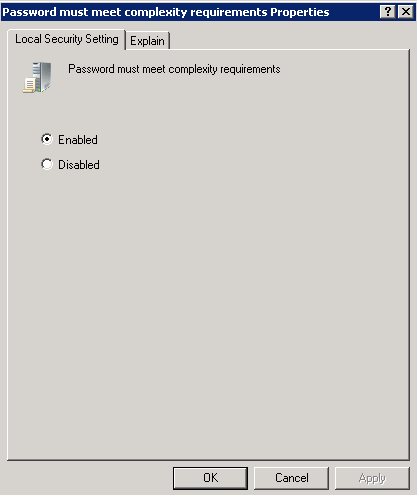
Chuột phải vào user muốn thay đổi => Reset Password. Và thực hiện thay đổi password.



* Cấu hình chính sách mật khẩu cho tài khoản:
* Độ dài tối thiểu của mật khẩu phải lớn hơn hoặc bằng 8 ký tự.
* Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
* Bước 2: Chọn *Minimum Password length* và đặt 8 kí tự.



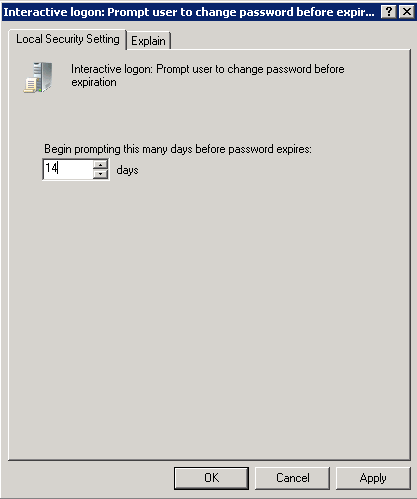
* Mật khẩu phải chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.
* Bước 1: Click chuột phải vào biểu tượng start của Windows > Administrative Tools => Local Security Policy => Account Policies => Password Policy.
* Bước 2: Chọn *Password must meet complexity* và tích vào Enabled.



* Thời gian bắt buộc phải thay đổi mật khẩu.
* Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
* Bước 2: Chọn *Maxnimum Password Age* và đặt 90 ngày (với hệ thống public) hoặc 180 ngày (với hệ thống nội bộ).



* + Bước 3: Cấu hình thông báo mật khẩu sắp hết hạn cho người dùng. Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Local Policies => Security Options. Thiết lập giá trị cho cấu hình *Interactive logon: Prompt user to change password before expire* là 14.

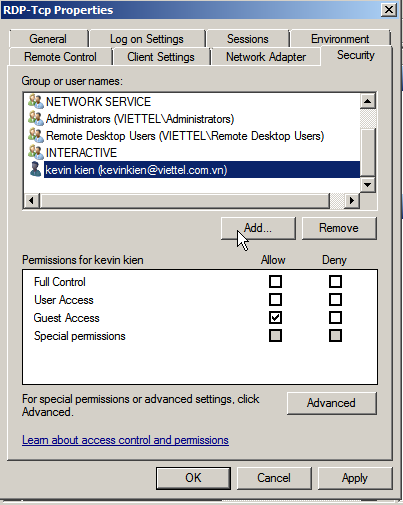


* Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất.
* Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
* Bước 2: Chọn *Enforce password history* và đặt giá trị là 02 (với hệ thống nội bộ) hoặc 05 (với hệ thống public).

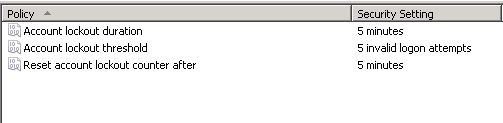


1. **Quản trị từ xa qua kênh truyền an toàn**

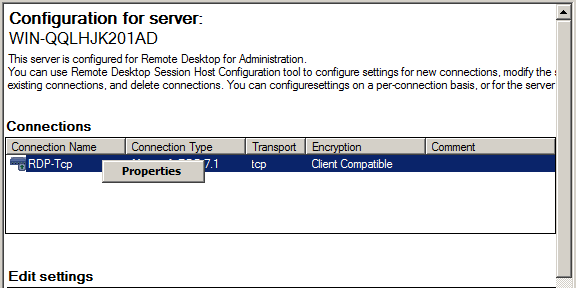
* Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa: Sử dụng ứng dụng Remote Desktop của Windows để quản trị từ xa.
* Cấu hình giới hạn tài khoản được phép sử dụng dịch vụ quản trị từ xa.
* Bước 1: Chọn Start => Administrative Tools => Server Manager => Roles => Remote Desktop Services.
* Bước 2: Chọn RD Session Host Configuration và click vào RDP-Tcp.
* Bước 3: Chọn mục Security và add thêm user muốn cho remote.



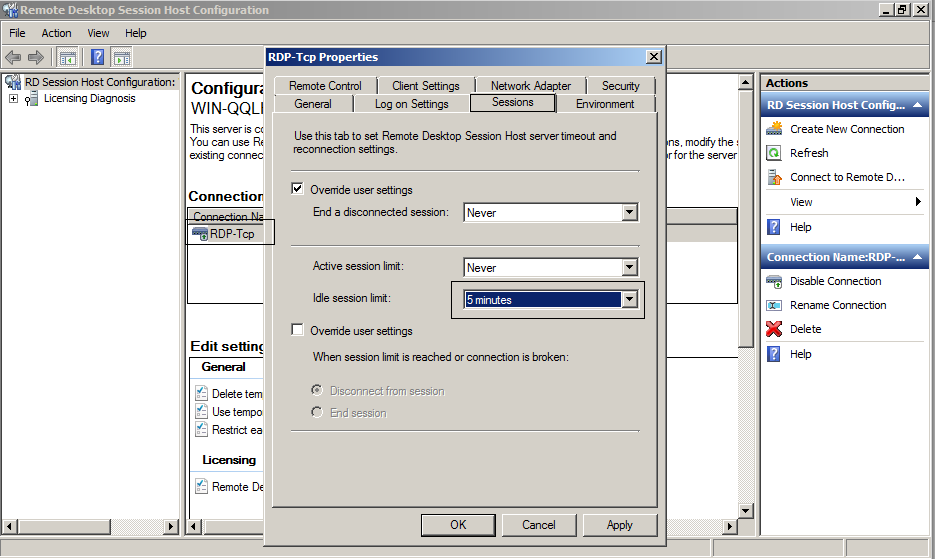
* Giới hạn số lần đăng nhập sai là 05 lần.
* Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
* Bước 2: Chọn *Account lockout threshold* và thiết lập giá trị là 5, *Account lockout duration* thiết lập là 5 và *Reset account lockout counter after* thiết lập giá trị là 5.



* Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 5 phút.
* Vào Start => Administrative Tools => Remote Desktop Services => Remote Desktop Session Host Configure. Click chuột phải vào RDP-TCP => Properties.

****

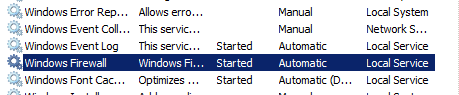
* Trong thẻ Sessionsthay đổi giá trị Idle session limit:



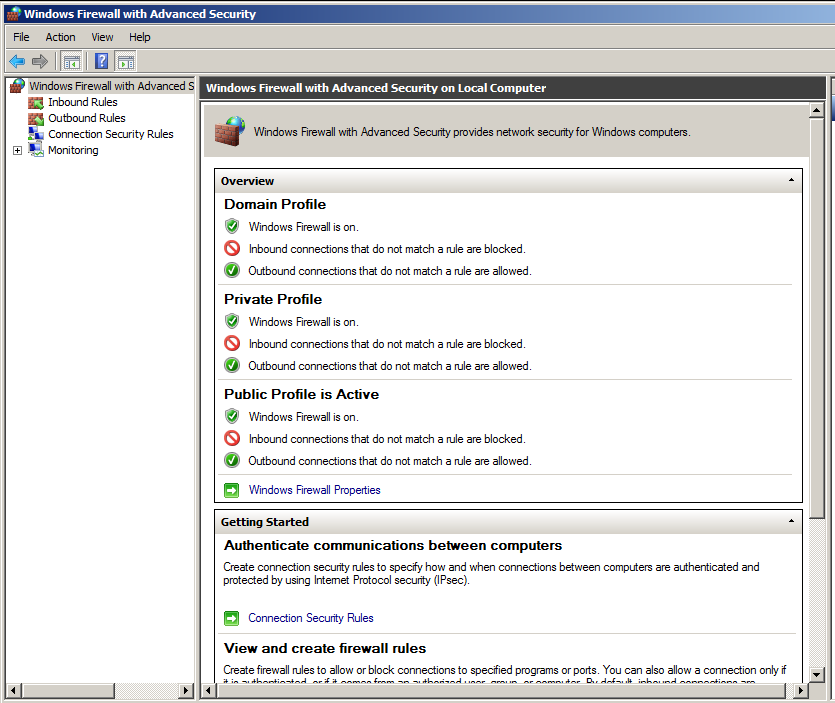
1. **Cài đặt và cấu hình firewall mềm**

Trên một server luôn có rất nhiều các dịch vụ đang chạy đồng thời, việc kiểm soát tất cả mọi truy cập vào ra trên hệ thống sẽ giúp hạn chế được các cuộc tấn công của attacker.

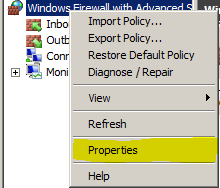
* Kích hoạt Windows Firewall: Run => services.msc => Chọn Windows Firewall => Chọn Automatic => Start.



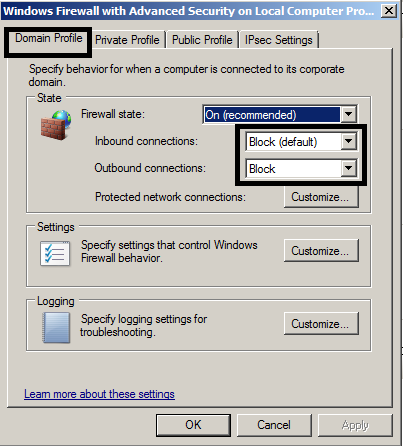
* Mặc định Windows Firewall cấm các kết nối vào và không cấm các kết nối ra đối với cả Domain Profile, Private Profile và Public Profile:
* Domain Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với các máy khác trong cùng một domain.
* Private Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với mạng riêng.
* Public Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với mạng công cộng.
* Local IP: là địa chỉ trên máy chủ đang chấp nhận kết nối hoặc địa chỉ được sử dụng với tư cách là địa chỉ nguồn để gửi các kết nối gửi đi.
* Remote IP: là địa chỉ IP của máy chủ điều khiển xa mà máy chủ này đang muốn kết nối đến (trong kịch bản truy cập gửi đi), hoặc địa chỉ IP nguồn của máy tính đang muốn kết nối với máy chủ (trong trường hợp kịch bản truy cập gửi đến).
* Local Port: các cổng nội bộ trên máy chủ mà rule của tường lửa sử dụng. Nếu rule là Inbound Rules thì đây sẽ là cổng để máy chủ lắng nghe. Nếu rule là Outbound Rules thì đây sẽ là cổng nguồn để máy chủ sử dụng kết nối tới máy khác.
* Remote Port: đây là cổng điều khiển từ xa để sử dụng cho rule. Trong trường hợp rule kết nối gửi đi thì đây sẽ là cổng mà máy chủ kết nối với một máy tính khác. Trong trường hợp rule kết nối đến thì đây chính là cổng nguồn của máy tính muốn kết nối với máy chủ.



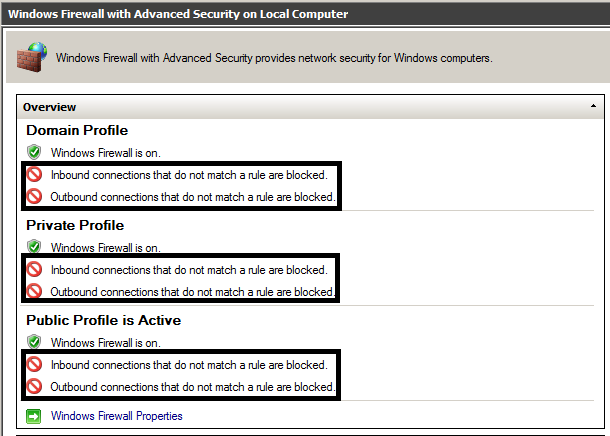
* Cấu hình block các kết nối ra ngoài:



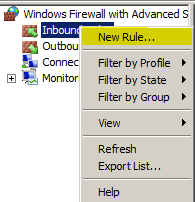
* Cấu hình Block Outbound Connection trong tab Domain Profile (làm tương tự đối với tab Private Profile và Public Profile).



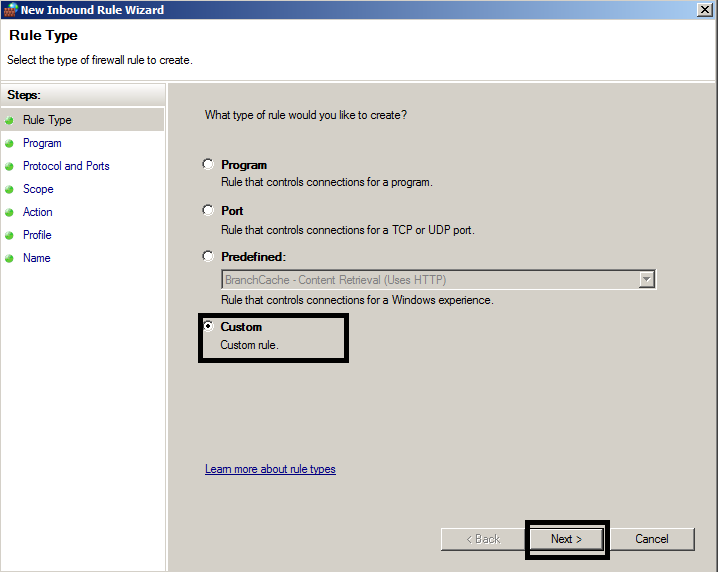
* Kiểm tra lại cấu hình xem đã được kích hoạt chưa:



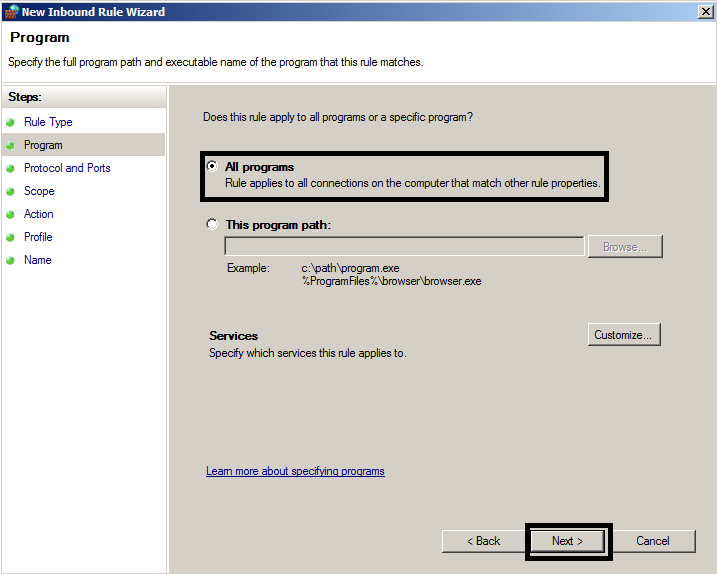
* Thiết lập kết nối chiều ra/vào theo đặc quyền:
* Thiết lập chính sách kết nối từ ngoài vào máy chủ (Inbound Rule): Click chọn Inbound Rule => New Rule…



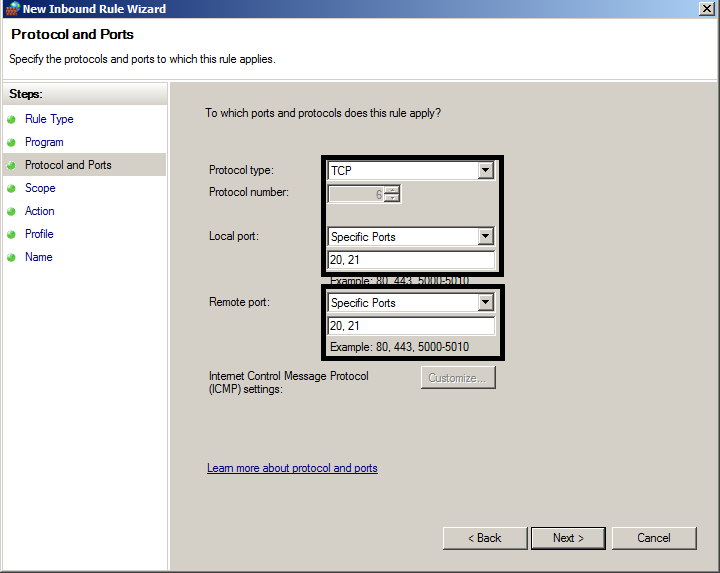
* Chọn Custom và click Next:



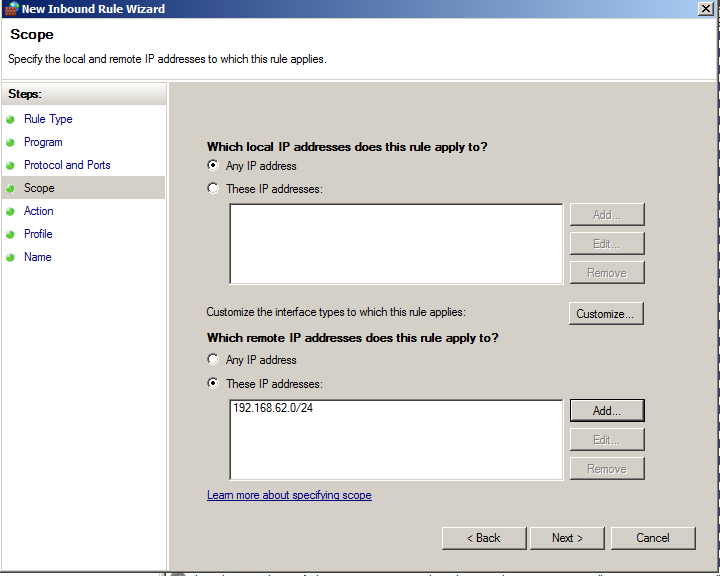
* Chọn chương trình kết nối => All Programs => Next.



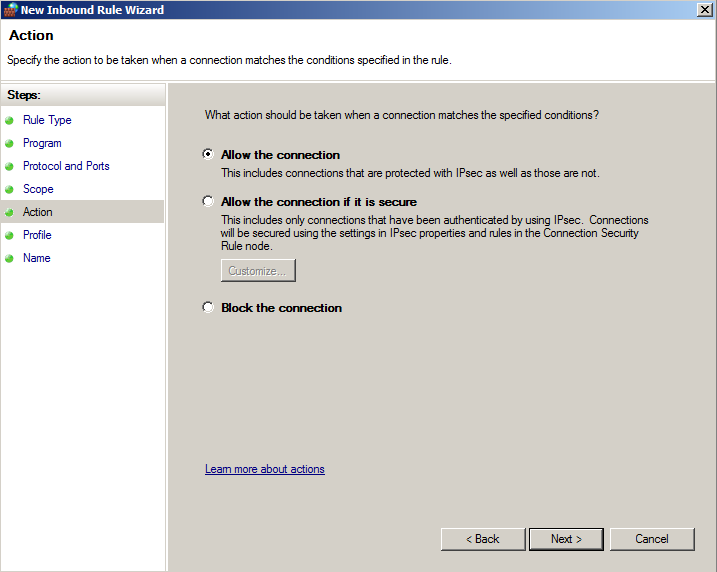
* Chọn giao thức và cổng tương ứng cần mở kết nối từ ngoài vào máy chủ. Ví dụ chọn giao thức TCP, cổng 20, 21 => Click Next.



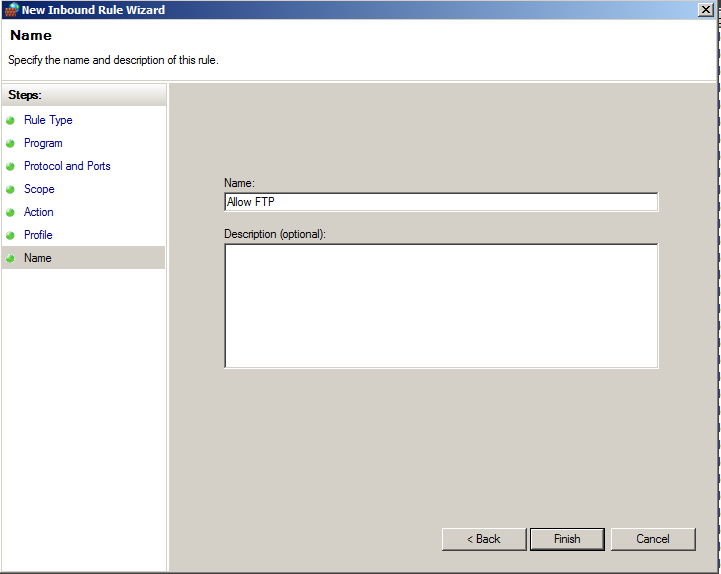
* Thiết lập IP được phép kết nối => Click Next:



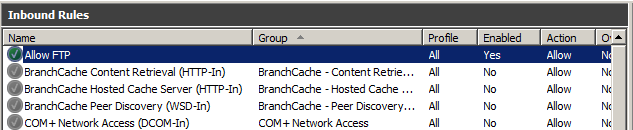
* Chọn Allow the connection => Click Next:



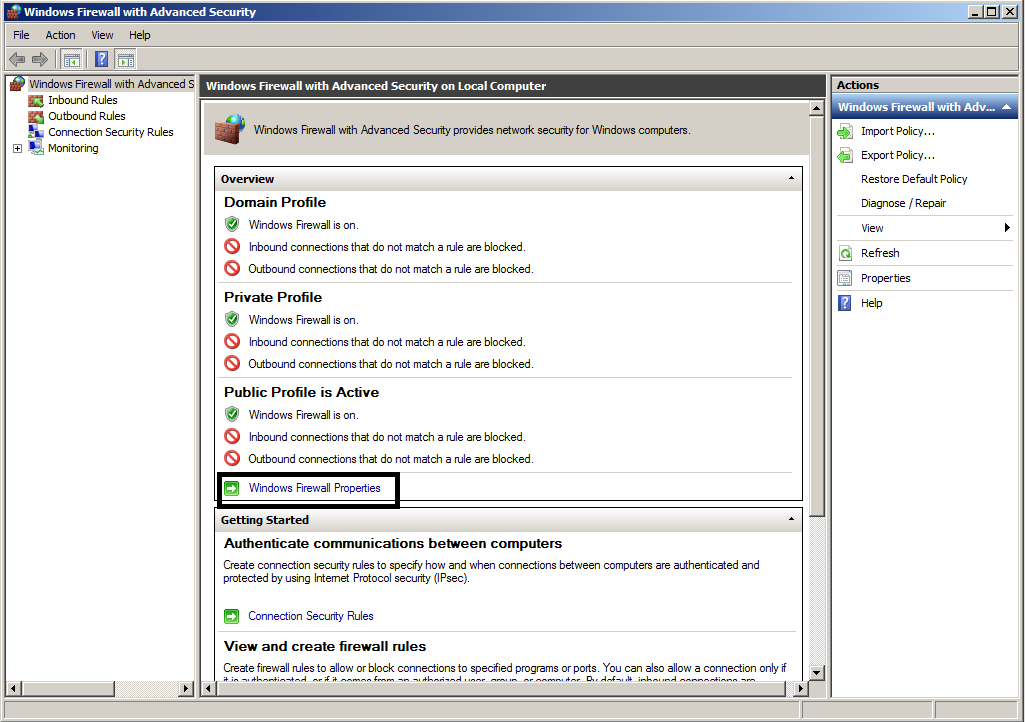
* Để mặc định => Next => Đặt tên cho Rule => Click Finish:



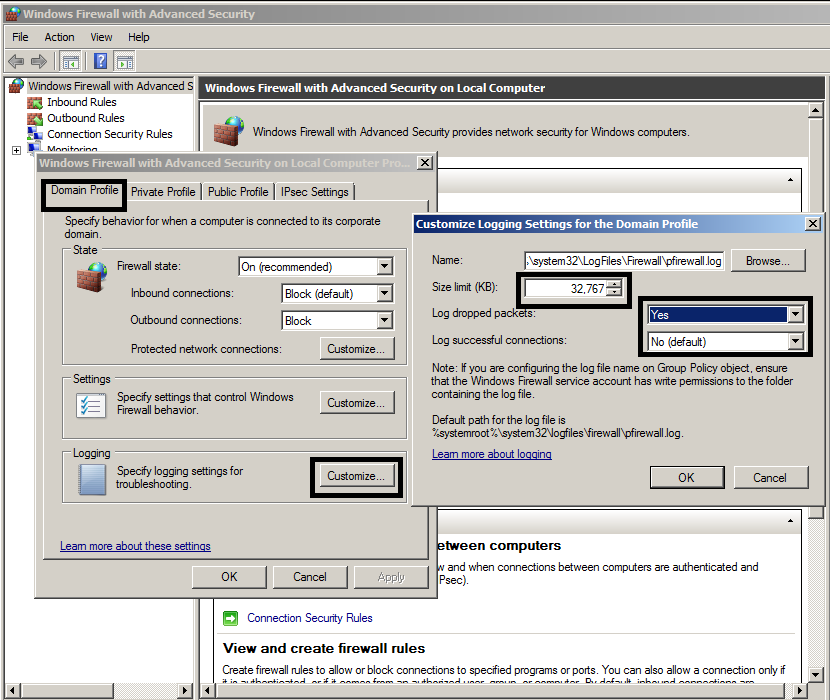
* Ta có được luật vừa tạo:



* Thiết lập chính sách kết nối từ máy chủ ra ngoài (Outbound Rule): Cách thiết lập tương tự như trên.
* Yêu cầu ghi log toàn bộ các gói tin vi phạm luật tường lửa.
* Vào Start => Administrative Tools => Windows Firewall with Advanced Security.

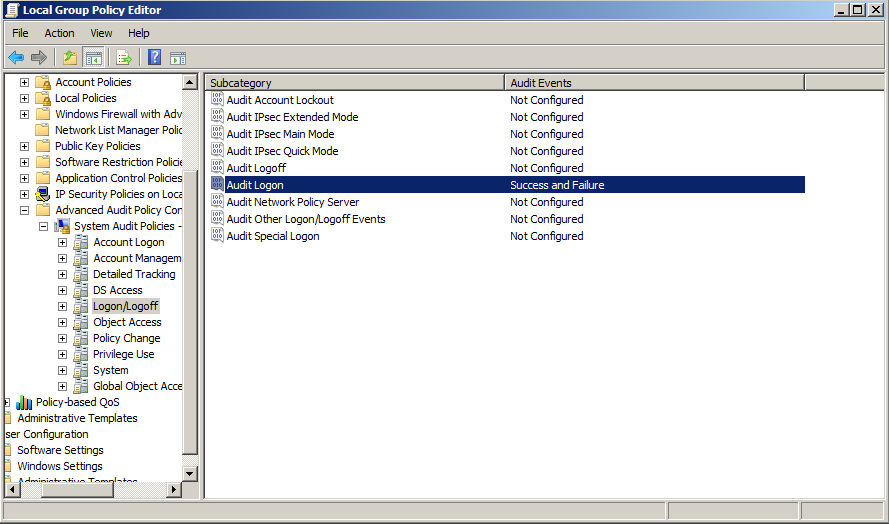


* Click Windows Firewall Properties => mở Customize… Logging của các tab Domain Profile, Private Profile và Public Profile => Click Yes cho Log dropped packets.

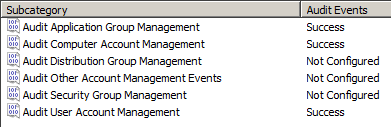


1. **Thiết lập chính sách quản lý log**

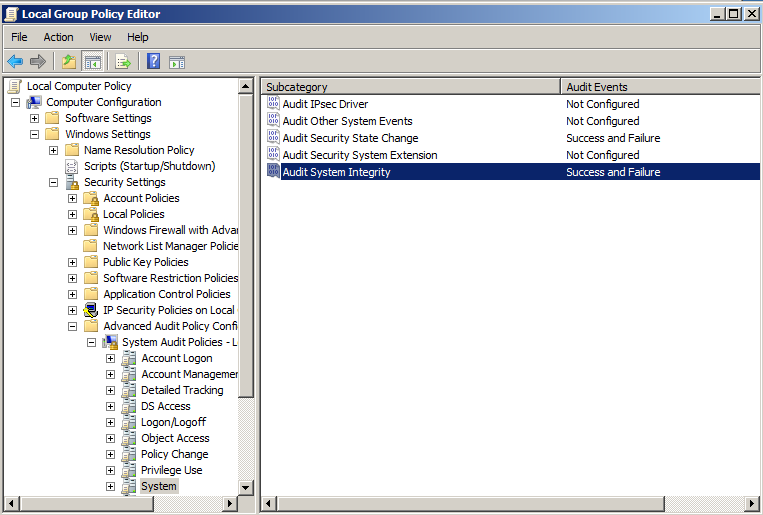
* Ghi log các sự kiện đăng nhập vào máy chủ.
* Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => Logon/logoff => Audit Logon => Configure the following audit event => Chọn Failure và Success.

**

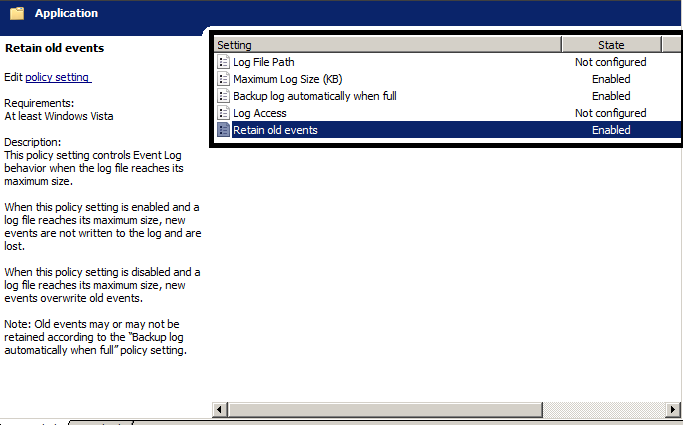
* Ghi log các sự kiện liên quan đến quản lý tài khoản và nhóm tài khoản.
* Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => Account Management.
* Cấu hình như sau:
* Audit Application Group Management => Chọn Success.
* Audit Computer Account Management => Chọn Success.
* Audit User Account Management => Chọn Success.

**

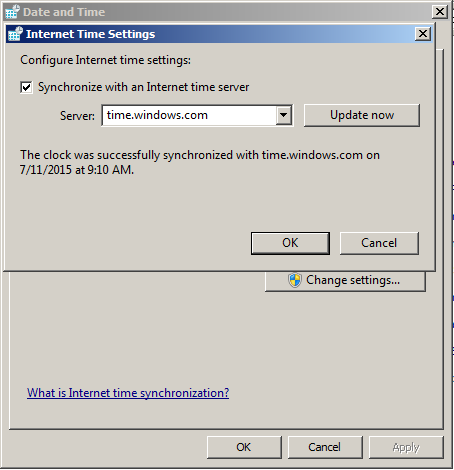
* Ghi log những thay đổi trong “Security State Change” và “System Integrity”.
* Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => System:
* Audit Security State Change => Chọn Failure và Success.
* Audit System Integrity => Chọn Failure và Success.



* Thiết lập kích cỡ và sao lưu file log Application, Security, System.
* Vào Run => gpedit.msc => Computer Configuration => Administrative Templates => Windows Components => Event Log Service. Đối với cả 3 mục Application, Security, System thiết lập như sau:
* Application => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
* Security => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
* System => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
* Bật: Backup log automatically when full.



* Cấu hình đồng bộ thời gian cho hệ thống:
* Vào Start Menu => Control Panel => Date and Time => Internet Time => Change Setting => chọn “Synchronize with an Internet Time Server” => nhập địa chỉ Time Server => Update now.

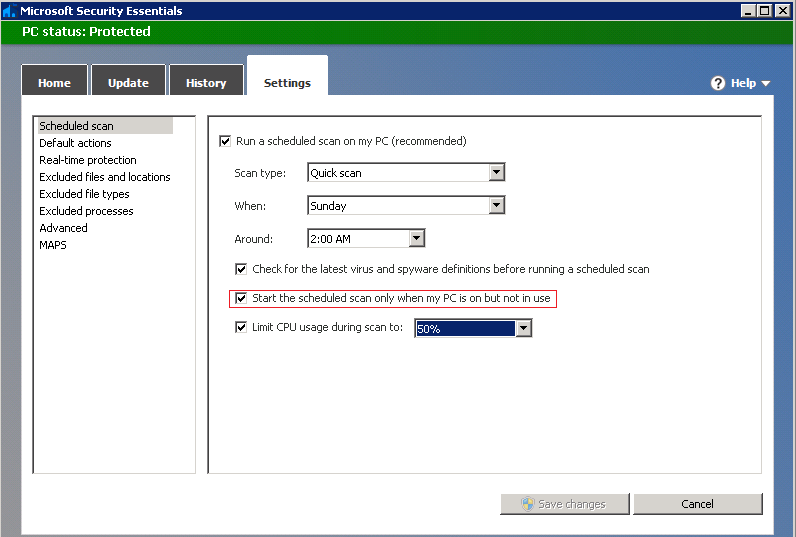


1. **Cài đặt các hệ thống bảo vệ và giám sát hệ thống**

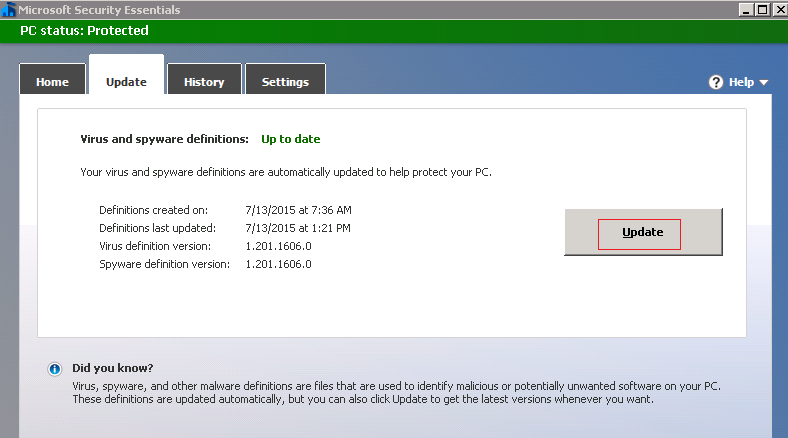
**7.1 Cài đặt phần mềm diệt virus Kaspersky**

Yêu cầu cài đặt các phần mềm antiVirus nhằm ngăn ngừa, phát hiện các cuộc tấn công của attacker vào hệ thống. Trong phần này, phụ lục chi tiết hướng dẫn cấu hình phần mềm diệt virus Microsoft Security Essentials (MSE) theo các đầu mục của baseline.

* Yêu cầu sử dụng phần mềm diệt virus luôn ở chế độ bảo vệ.



* Cập nhật các mẫu diệt virus mới hàng ngày.



**7.2 Cài đặt phần mềm Server Endpoint**

## Điều kiện đảm bảo

* Id cho agent được cài đặt phải được khai báo với hệ thống trước khi bắt đầu cài đặt cho agent. Id của agent là duy nhất.
* Id agent có format như sau: **TênHĐH\_Ipv4**. Ví dụ: **windows\_10.10.0.1**
* Các đơn vị khác VTNet, đề nghị khi tạo ID bổ sung prefix tên viết tắt của đơn vị (VD: vtidc, vtt, vttek,..). Ví dụ: **vtt\_centos\_10.30.58.164**
* Toàn bộ sử dụng chữ viết thường
* Tên hệ điều hành là windows, centos, redhat, oracle, solaris, suse …
* Địa chỉ IP theo chuẩn IP v4.
* Chương trình cài đặt bắt buộc chạy với user Administrator đối với hệ hiều hành Windows và user root với hệ điều hành Linux, Solaris.
* Đối với các agent tương ứng cần có các gói sau:

| **Linux** |  |
| --- | --- |
| wget | Download dữ liệu từ repository |
| unzip | Giải nén file nén chứa file cài đặt |
| **Windows** |  |
| powershell | Giao diện quản trị lệnh của Windows |
| vcredist | Lib c trên windows |

* Thông kết nối từ agent tới server tập trung (10.30.160.44, 10.30.160.45, 10.30.160.46) tương ứng các cổng sau: 80, 443, 4505, 4506, 6379.
* Kiểm tra kết nối từ máy tính của người thực hiện tới địa chỉ portal của hệ thống SIRC (10.30.160.41) cổng 80(http), 443(https) và 8443(https).
* Phân giải được các domain của hệ thống SIRC. Mặc định trên hệ thống DNS đã có cấu hình domain này, trong trường hợp chưa phân giải được, cấu hình file host trên máy tính của người thực hiện cài đặt để truy cập vào trang web quản trị:

10.30.160.41 srm.sirc.viettel.com

10.30.160.41 se.sirc.viettel.com

10.30.160.41 cas.sirc.viettel.com

**Bước 1:** Khai báo server\_id trên Portal <http://se.sirc.viettel.com/#/server/list>

Chú ý: Đối với các server cài lại cần vào Portal trên thực hiện thao tác **Reject**, sau đó khoảng 1 phút **Renew** lại cert của server cần cài lại, và cài đặt bình thường

**Bước 2:** Download bộ cài <http://10.30.160.44/serverendpoint/se_setup_windows.zip>

**Bước 3:** Unzip se\_setup\_windows.zip

**Bước 4:** Chạy file se-install.bat

Nhập ID, Master IP (default là 10.30.160.44) và run.

"\*\*\*\*\*\*\* WINDOWS INSTALL SE \*\*\*\*\*\*\*"

Server ID: test\_server\_id

Master IP Address [10.30.160.44]: 10.30.160.44

Chú ý: Đối với server bị lỗi **The application has failed to start because its side-by-side configuration...** hoặc **The system cannot find the path specified.** , nguyên nhân do thiếu VCredist, cài đặt bộ cài tương ứng tại: [*http://10.30.160.44/serverendpoint/vcredist/*](http://10.30.160.44/serverendpoint/vcredist/)

**Bước 5:** Kiểm tra cài đặt thành công

C:\salt\salt-call.exe vsm.status

ret:

local:

----------

version:

2014.7.4

**7.3 Cài đặt winlogbeat**

**Để đẩy log lên hệ thống, cần làm Policy kết nối như sau:**

| **STT** | **Đích** | **Port** | **Ghi chú** |
| --- | --- | --- | --- |
| 1 | 10.30.160.44 | 80/TCP, 443/TCP | Kết nối đến repo(thường đã có khi cài SE Agent) |
| 2 | 10.30.160.41 | 514/TCP+UDP, 5044/TCP, 6379/TCP, 9092/TCP, 9080-9100 TCP | Kết nối đến hệ thống Log tập trung |

**Cài đặt**

* Tải bộ cài tương ứng từ SE-Repo [LogAgent - http://10.30.160.44/serverendpoint/logagent/](http://10.30.160.44/serverendpoint/logagent/)
  + Debian/Ubuntu tải file deb, Centos/RedHat tải file rpm, tương đương với kiến trúc
  + Các server linux khác thì tải bản se\_filebeat tương đương
  + Window thì tải winlogbeat và filebeat\_windows phiên bản 5.00
* Cài đặt bộ cài
  + **Window**:
    - Giải nén winlogbeat và filebeat\_windows.xxx.zip vào thư mục C:\Program Files\WinlogBeat
    - Mở Powershell với quyền Administrator
    - Enable scripting, mở Powershell, run: Set-ExecutionPolicy RemoteSigned
    - Chuyển thư mục hiện tại vào C:\Program Files\WinlogBeat
    - Tạo 01 thư mục rỗng filebeat.d
    - Chạy script install .\install-service-winlogbeat.ps1 .\install-service-filebeat.ps1
    - Nếu mà ko chạy được thì chỉ chuột phải vào file ps1 đó, chọn Properties, ấn UnBlock sau đó chạy lại

**Cấu hình**

* Dùng server\_id của **SE-Agent** làm tên của **LogAgent**, cấu hình trong shipper.name(server\_id xem trong /etc/salt/minion.d/id.conf, cấu hình cụ thể xem ở dưới cho từng OS)

name: vtt\_centos\_10.10.0.132

* Cấu hình gửi log lên server 10.30.160.41:5044/TCP với các dải mạng nội bộ của **SIRC** thì dùng IP cấu riêng để vào, phía server cần mở **Firewall**
* Tất cả các file cấu hình đều là định dạng yml, dùng dấu cách space thay vì tab, lưu ý về các khoảng cách này
* File cấu hình mặc định filebeat.yml được copy từ nội dung trong hướng dẫn, tất cả các cấu hình thêm sau này, thì nên đưa vào filebeat.d/extra.yml để tiện sửa chữa hay cài mới ko bị mất

|  |
| --- |
| # filebeat.d/filebeat.yml  # follow this hierachy  filebeat:  prospectors:  -  paths:  #- C:\Windows\System32\LogFiles\W3SVC3\ex??????.log  #- C:\salt\var\log\salt\minion  #- C:\ProgramData\VMware\vCenterServer\logs\vmware-vpx\vpxd-\*.log  input\_type: log |

Window cần phải cấu hình cả winlogbeat và filebeat.

* **WinlogBeat**: Lấy toàn bộ event log của các loại Application, Security, System, Kaspersky Event Log. File C:/Program File/winlogbeat/winlogbeat.yml

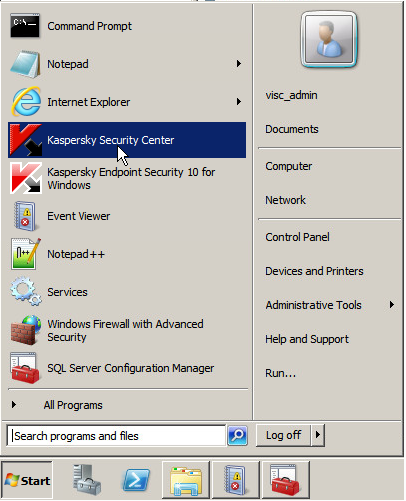
|  |
| --- |
| winlogbeat:  registry\_file: C:/ProgramData/winlogbeat/.winlogbeat.yml  event\_logs:  - name: Application  ignore\_older: 72h  - name: Security  - name: System  - name: "Kaspersky Event Log"  output:  logstash:  hosts: ["10.30.160.41:5044"]  worker: 1  compression\_level: 3  index: beat\_agent  name: <server\_id>  logging:  to\_files: true  level: warning  files:  path: C:/ProgramData/winlogbeat/Logs  name: winlogbeat.log  rotateeverybytes: 10485760  keepfiles: 7 |

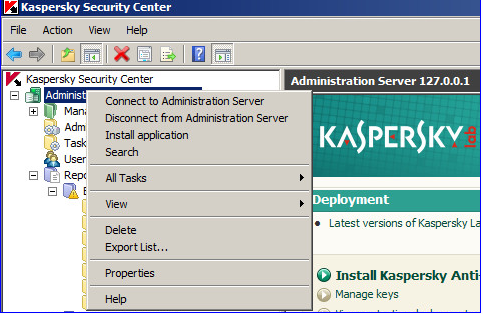
* **Filebeat**: Lấy log của IIS nếu có, hoặc các ứng dụng khác từ file. Chạy trong powershell: .\add-iis-log.ps1
* Thêm file bằng cách thêm vào paths, cấu hình cụ thể từng file tham khảo trên doc của filebeat. File C:/Program File/winlogbeat/filebeat.yml

|  |
| --- |
| filebeat:  prospectors:  -  paths:  - C:\Windows\System32\LogFiles\W3SVC3\ex??????.log  - C:\salt\var\log\salt\minion  input\_type: log  registry\_file: "C:/ProgramData/filebeat/registry"  config\_dir: "C:/Program Files/Winlogbeat/filebeat.d"  output:  logstash:  hosts: ["10.30.160.41:5044"]  worker: 1  compression\_level: 3  index: beat\_agent  name: <server\_id>  logging:  to\_syslog: false  to\_files: true  level: warning  files:  path: C:/ProgramData/winlogbeat/Logs  name: filebeat.log  rotateeverybytes: 10485760  keepfiles: 7 |

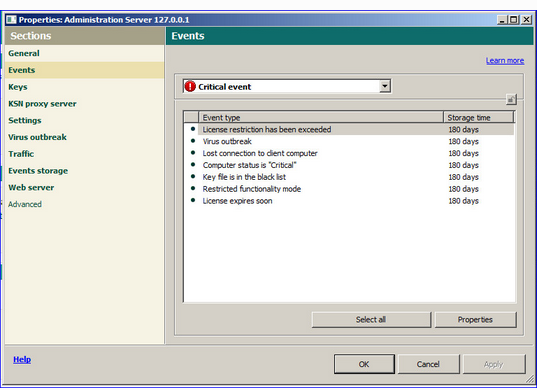
# Tích hợp cho các loại log phổ biến

* **Log KAV**

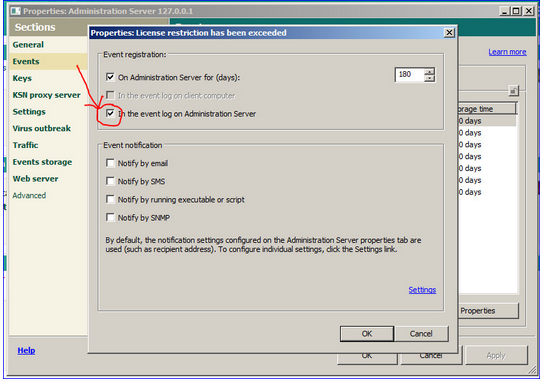




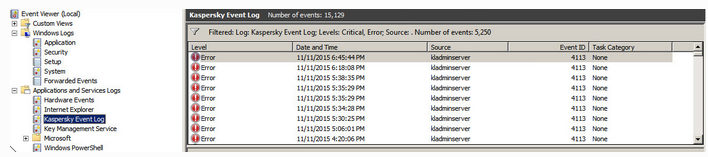
Chọn Properties



Chọn Events => Critical Event => (Chọn cả Virus outbreak + Computer status is critical) => Properties

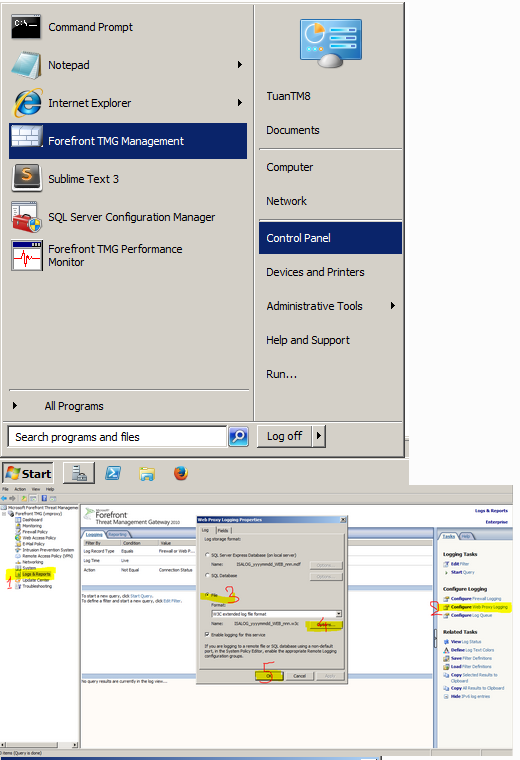


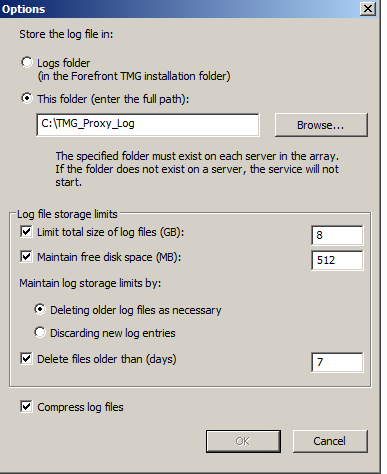
Chọn In the event log on Administrator Server

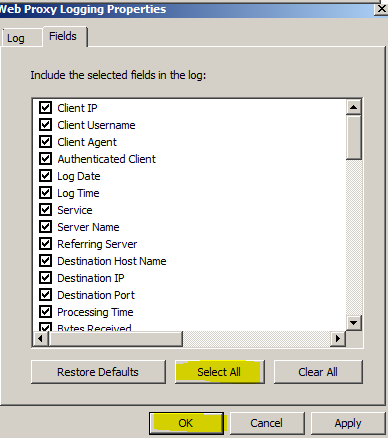


Sau khi cấu hình thì log **KAV** sẽ được lấy qua Window EventLog

* **Log TMG**







Cấu hình filebeat: Thêm filelog vào trong cấu hình filebeat.d/extra.yml(tạo mới nếu chưa có), theo đúng cấu trúc cây thư mục

|  |
| --- |
| filebeat:  prospectors:  -  paths:  - C:\TMG\_Proxy\_Log\\*.log  - C:\Windows\System32\LogFiles\W3SVC3\ex??????.log  input\_type: log |

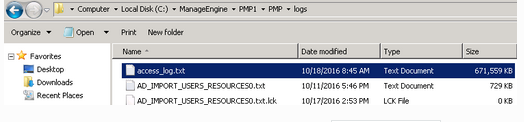
Restart service filebeat net stop filebeat net start filebeat

* **Log Password Manager**

Trong Password Manager cần thu thập 2 loại log: access log và audit log. Cụ thể:

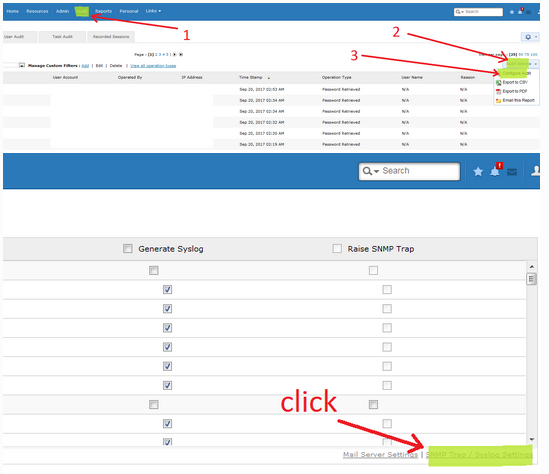
**Access Log** là log của webapp, ghi nhận các kết nối đến PasswordManager. Access Log lấy bằng filebeat cấu hình thêm đường dẫn file vào cấu hình của filebeat vào filebeat.d/extra.yml cụ thể:

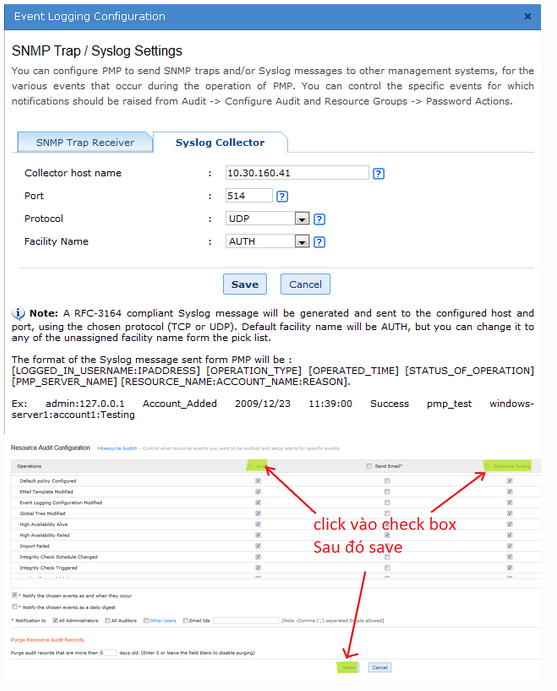
* + Windows: Trong thư mục cài đặt, logs



* + Linux: Trong thư mục cài đặt, logs (tìm file access\_log.txt trong thư mục của PMP)

**Audit Log** là log tác động của user đối với các tài nguyên trong PasswordManger như user A lấy mật khẩu của tài khoản X. Audit Log không lấy qua file được, mà cấu hình bắn vào Syslog server từ giao diện quản trị của PasswordManager. Cấu hình cụ thể như sau:





* **Log Vcenter, ESXi**

Log ESXi và VCenter được lấy bằng filebeat, trong đó cấu hình lấy thêm những file cụ thể được liệt kê ở dưới, chi tiết cho từng OS(Lưu ý khi thêm vào phải kiểm tra cú pháp của file cấu hình): - ESXi: Là một server Linux, cài đặt phiên bản filebeat tương ứng và thêm các file vào cấu hình

/var/log/dhclient.log

/var/log/hostd.log

/var/log/shell.log

* Log Vcenter tùy thuộc vào phiên bản nằm ở các thư mục:
  + Windows XP, 2000, 2003: %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter\Logs\
  + Windows Vista, 7, 2008: C:\ProgramData\VMware\VMware VirtualCenter\Logs\
  + vCenter Server Appliance 5.x: /var/log/vmware/vpx/
  + vCenter Server Appliance 5.x UI: /var/log/vmware/vami
  + vCenter 6: C:\ProgramData\VMware\vCenterServer\logs\vmware-vpx\
  + **Trong các trường hợp không thấy, hoặc version lạ, tìm file có cụm từ vpxd trong filesystem để tìm thư mục**

Trong các thư mục đó, cần lấy những file sau:

vpxd.log

vpxd-\*.log

manager.\*.log

host-manager.\*.log

# III. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH IBMAIX

## Cài đặt hệ điều hành và cập nhật bản vá

**Yêu cầu khắc phục:**

* Cài đặt phiên bản mới nhất tại khi cài đặt mới.
* Cập nhập các bản vá lỗi cho hệ điều hành: Bao gồm các bản vá lỗ hổng bảo mật đã được công bố và các bản vá theo yêu cầu của Tập đoàn.

## Hệ thống chỉ chạy các phần mềm tối thiểu đúng với chức năng được thiết kế

**Yêu cầu khắc phục:**

* Cài đặt tối thiểu các phần mềm, dịch vụ theo đúng chức năng được thiết kế của server.
* Gỡ bỏ hoặc vô hiệu hóa các gói dịch vụ không cần thiết, các gói dịch vụ lỗi thời có nguy cơ bị mất an toàn thông tin:Telnet, rcp, rsh, rlogin, nis, ftp...
* Kiểm tra các dịch vụ đang chạy trên hệ điều hành. Nếu dịch vụ nào không cần thiết chạy thì thực hiện vô hiệu hóa hoặc xóa bỏ.
* Bước 1: Xác định các dịch vụ đang hoạt động.

|  |
| --- |
| *# lssrc -a | grep active* |

* Bước 2: Xác định các dịch vụ thừa, không cần thiết để disable.

|  |
| --- |
| *#stopsrv -s <service>* |

* Nếu trong trường hợp dịch vụ là một trong những dịch vụ con của inetd. Thì thực hiện như sau:

|  |
| --- |
| *# vi /etc/inetd.conf*  *Comment dòng bên dưới (thêm dấu # vào đầu dòng tương ứng với service), ví dụ :*  ***telnet stream tcp6 nowait root /usr/sbin/telnetd telnetd -a***  *Restart lại dịch vụ inetd:*  *# refresh -s inetd* |

## Thiết lập chính sách tài khoản

#### Xóa hoặc vô hiệu tất cả các tài khoản không sử dụng trên hệ thống

**Yêu cầu khắc phục:** Rà soát hệ thống, liệt kê những tài khoản đang hoạt động trên hệ thống rồi tìm và xóa hoặc vô hiệu những tài khoản không sử dụng ra khỏi hệ thống.

* Bước 1: Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:

|  |
| --- |
| *# lsuser ALL | awk ’{print $1}’* |

* Bước 2: Kiểm tra xem các tài khoản này tài khoản nào không sử dụng. Thực hiện khóa các tài khoản đó bằng lệnh sau:

|  |
| --- |
| *# chuser account\_locked=true <username>* |

#### Cấu hình chính sách mật khẩu cho tài khoản

#### Mật khẩu phải có độ dài tối thiểu 8 ký tự chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt

**Yêu cầu khắc phục:** Mật khẩu có độ dài tối thiểu 8 ký tự, đảm bảo phải bao gồm ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.

|  |
| --- |
| *# vi /etc/security/user*  *minalpha = 5 (yêu cầu mật khẩu có ít nhất 5 kí tự là chữ)*  *minother = 3 (yêu cầu mật khẩu có ít nhất 3 kí tự đặc biệt)*  *minlen = 8 (yêu cầu mật khẩu có ít nhất 8 ký tự)* |

#### Thời gian bắt buộc phải thay đổi mật khẩu người dùng

**Yêu cầu khắc phục:** Đối với mật khẩu người dùng, thiết lập thời gian tối đa bắt buộc phải đổi mật khẩu là 90 ngày.

Thay đổi giá trị maxage=13 và giá trị maxexpired=-1 trong file /etc/security/user. Thực hiện như sau:

|  |
| --- |
| *# vi /etc/security/user*  *maxage = 13*  *maxexpired = -1* |

* **Chú** ý: Trong file /etc/security/user, giá trị maxage=13 (tuần) sẽ tương đương với thời hạn hết hạn mật khẩu là =< 90 ngày.

#### Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất

**Yêu cầu khắc phục:** Đối với mật khẩu người dùng, thiết lập bắt buộc mật khẩu mới phải không trùng với 5 mật khẩu gần nhất. Thay đổi giá trị histsize=1 trong file /etc/security/user. Thực hiện như sau:

|  |
| --- |
| *# vi /etc/security/user*  *histsize = 5* |

#### Mật khẩu phải được lưu dưới dạng mã hóa sử dụng thuật toán băm SHA-512

**Yêu cầu khắc phục:** Kiểm tra và nâng cấp phương thức mã hóa mật khẩu, sử dụng thuật toán băm SHA-512.

* Sử dụng lệnh sau để kiểm tra OS và TL (Technology Level):

|  |
| --- |
| *#oslevel -r*  *<OS Ver>-<TL>-<SP>-<BUILD DATE>* |

* Nếu tham số TL>7 sẽ thực hiện các bước thiết lập mã hóa password bằng sha-512 bên dưới, nếu không ta bỏ qua;
* Ví dụ: #oslevel –r cho kết quả: 5300-02-07-1207

Tức là OS Version=5.3, TL=2, Build tuần thứ 07 của năm 2012 ( TL < 7: bỏ qua phần thiết lập mã hóa password.)

* Kiểm tra nếu thỏa mãn điều kiện về OS. Thực hiện lệnh sau để đảm bảo hệ thống có hỗ trợ thuật toán băm sha-512.

|  |
| --- |
| *# cat /etc/security/pwdalg.cfg | grep sha*  *ssha512:*  *lpa\_module = /usr/lib/security/ssha*  *lpa\_options = algorithm=sha512* |

* Nếu kết quả trả về xuất hiện như ví dụ trên thì hệ điều hành có hỗ trợ mã hóa sha-512. Thực hiện các bước sau để thiết lập lưu password dưới dạng thuật toán băm sha-512:
* Lưu password dưới dạng thuật toán băm sha-512. Thêm tùy chọn sau vào file /etc/security/login.cfg. Cụ thể:

|  |
| --- |
| *# vi /etc/security/login.cfg*  *Thêm hoặc sửa dòng như sau vào phần thiết lập (thường ở cuối file và có khoảng tab ở đầu dòng):*  *pwd\_algorithm = ssha512* |

* **Chú ý:**
* Nếu hệ điều hành không hỗ trợ mã hóa sha512, sử dụng mã hóa md5 để thay thế:

|  |
| --- |
| *# vi /etc/security/login.cfg*  *Thêm hoặc sửa dòng như sau vào phần thiết lập (thường ở cuối file):*  *pwd\_algorithm = smd5* |

* Với những tài khoản đang tồn tại trên hệ thống phải thực hiện các bước sau để chính sách được áp dụng:
* Bước 1: Liệt kê các tài khoản đang tồn tại trên hệ thống, sử dụng lệnh:

|  |
| --- |
| *# lsuser ALL | awk '{print $1}'* |

* Bước 2: Buộc người dùng phải đổi mật khẩu ở lần đăng nhập tiếp theo, sử dụng lệnh.

|  |
| --- |
| *# pwdadm –f ADMCHG <username>* |

## Quản trị từ xa qua kênh truyền an toàn

**Yêu cầu khắc phục:** Để đảm bảo an toàn yêu cầu chỉ sử dụng công cụ quản trị từ xa có mã hóa đường truyền. Chỉ sử dụng SSH để quản trị máy chủ, khi sử dụng SSH cần thực hiện các thiết lập sau *(Yêu cầu khởi động lại dịch vụ SSH khi thiết lập xong cấu hình):*

#### Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa.

***Chỉ cho phép sử dụng giao thức SSH version 2.***

|  |
| --- |
| *Mở file cấu hình /etc/ssh/sshd\_config, sửa lại tùy chọn:*  *Protocol 2* |

***Cấu hình chỉ cho phép tài khoản người dùng được phép SSH.***

|  |
| --- |
| *Mở file cấu hình /etc/ssh/sshd\_config, thêm tùy chọn sau:*  *AllowUsers user1 user2* |

***Không cho phép tài khoản root đăng nhập trực tiếp từ xa.***

|  |
| --- |
| *Mở file cấu hình /etc/ssh/sshd\_config, sửa hoặc thêm tùy chọn sau:*  *PermitRootLogin no* |

#### Không cho phép tài khoản đăng nhập sai là 05 lần

|  |
| --- |
| *N/A* |

#### Thiết lập thời gian tự động ngắt phiên nếu phiên không có hoạt động trong 5 phút

|  |
| --- |
| *Mở file cấu hình /etc/profile, thêm 3 dòng sau vào cuối file:*  *TMOUT=300*  *readonly TMOUT*  *export TMOUT* |

* **Lưu ý:** Trong trường hợp máy chủ chưa được cài đặt SSH, xem phụ lục 07.

## Phân quyền tệp tin và thư mục

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

**Yêu cầu khắc phục:** Kiểm tra biến môi trường PATH không được chứa các đường tương đối, đường dẫn bất thường, đường dẫn trống.

|  |
| --- |
| *Để ki km tra biến môi trường PAT, ta dùng lệnh sau:*  *# echo $PATH*  *Ví dụ:*  *PATH chứa đường dẫn trống: PATH /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin****::***  *PATH chứa đường đẫn tương đối: /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:****./src/bin***  *PATH chứa đường dẫn nguy hiểm: /bin:/us: /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:****/tmp*** |

#### Thiết lập cấu hình dịch vụ CRON

**Yêu cầu khắc phục:**

* Giới hạn tài khoản được phép chạy dịch vụ CRON bởi whitelist danh sách người dùng.
* Bước 1:

|  |
| --- |
| *# rm /var/adm/cron/cron.deny* |

* Bước 2: Thêm file cron.allow nếu hệ thống chưa có:

|  |
| --- |
| *# touch /var/adm/cron/cron.allow* |

* Bước 3: Sửa file /var/adm/cron/cron.allow, cập nhật hoặc thêm các tài khoản được phép sử dụng dịch vụ CRON:

|  |
| --- |
| *User1*  *User2*  *…* |

* Hạn chế quyền sửa các file cấu hình của CRON

|  |
| --- |
| *# chown -R root:root /var/spool/cron/crontabs/*  *# chmod -R 600 /var/spool/cron/crontabs/*  *# chown -R root:root /var/adm/cron/*  *#chmod -R go-rwx /cron.d* |

## Cấu hình tường lửa mềm

#### Yêu cầu sử dụng tường lửa mềm trên hệ thống

**Yêu cầu khắc phục:** Thực hiện bật tường lửa mềm cho hệ thống (Chi tiết tham khảo mục 8). Cấu hình chính sách tường lửa theo các mục bên dưới Giới hạn địa chỉ IP quản trị được phép truy cập đến máy chủ.

#### Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống

**Yêu cầu khắc phục:** Sử dụng tường lửa chỉ mở kết nối giới hạn.

* Đối với hệ thống nội bộ:
* Chỉ mở vừa đủ các kết nối vào (Chiều INPUT).
* Đối với hệ thống public:
* Yêu cầu mở vừa đủ các kết nối vào (Chiều INPUT).
* Yêu cầu mở vừa đủ các kết nối ra (Chiều OUTPUT).

***Chú ý:*** Người quản trị cần phải cấu hình tường lửa ở chế độ ghi log các gói tin trong vòng 1-2 tuần. Sau đó sẽ phân tích logs và thiết lập rule tương ứng. Thực hiện theo ”Hướng dẫn cấu hình ipfilter cho AIX”.

#### Ghi log toàn bộ những bản tin vào ra không hợp lệ.

* Yêu cầu khắc phục: Ghi toàn bộ log vào/ra hệ thống không hợp lệ. Thực hiện theo ”Hướng dẫn cấu hình ipfilter cho AIX”.

## Thiết lập chính sách quản lý log

#### Ghi log mặc định của hệ điều hành

**Yêu cầu khắc phục:** Thiết lập lưu log của hệ điều hành, log truy cập và log tác động.

* Bước 1: Tìm và sửa file /etc/syslog.conf tại dòng sau:

|  |
| --- |
| *# vi /etc/syslog.conf*  *\*.debug;local4.none;auth.none /var/log/syslog/syslog.out rotate size 4096k files 12 time 1w compress*  *\*.crit /var/log/syslog/syslog.out rotate size 4096k files 12 time 1w compress*  *auth.debug /var/log/syslog/faillogin rotate size 4096k files 12 time 1w compress* |

* Bước 2: Nếu chưa có file /var/log/syslog/syslog.out thì tạo ra bằng lệnh sau:

|  |
| --- |
| *# mkdir /var/log/syslog*  *# touch /var/log/syslog/syslog.out* |

* Bước 3: khởi động lại dịch vụ syslog

|  |
| --- |
| *# refresh -s syslogd* |

* Bước 4: kiểm tra lại /var/log/syslog/syslog.out để chắc chắn đã có log:

|  |
| --- |
| *# tail –f /var/log/syslog/syslog.out* |

* + Chú ý: Theo quy định của Tập đoàn thời gian tối thiểu lưu log là 3 tháng. Tuy nhiên nếu máy chủ hiện tại không đủ dung lượng ổ cứng để lưu log trong 3 tháng. Còn số này quản trị có thể thiết lập lại để phù hợp với thực tế tránh log đầy làm cheo máy chủ.
* Bước 5: Thực hiện ghi log Firewall.

|  |
| --- |
| *# touch /var/log/firewall* |

* Bước 6: Thêm dòng giá trị sau vào file /etc/syslog.conf.

|  |
| --- |
| *local4.debug /var/log/firewall rotate size 4096k files 12 time 1w compress* |

* Bước 7: Khởi động lại hệ thống syslog.

|  |
| --- |
| *# refresh -s syslogd* |

* Bước 8: Kiểm tra trạng thái dịch vụ syslog: Nếu dịch vụ ở trạng thái active tức là dịch vụ đã hoạt động.

|  |
| --- |
| *# lssrc -a | grep log*  *syslogd ras 168238 active* |

#### Cấu hình thời gian lưu log tối thiểu là 3 tháng

**Yêu cầu khắc phục:** Thiết lập cấu hình thời gian lưu log tối thiểu 03 tháng.

Đối với hệ điều hành AIX cấu hình rotate log nằm trong file cấu hình */etc/syslog.conf như ở mục 7.1 tham số cấu hình ”****12 time 1w”*** chỉ định log được rotate hàng tuần (1w) và lưu trữ 12 file gần nhất (12 time).

|  |
| --- |
| *# vi /etc/syslog.conf*  *\*.debug;local4.none;auth.none /var/log/syslog/syslog.out rotate size 4096k files* ***12 time 1w*** *compress*  *\*.crit /var/log/syslog/syslog.out rotate size 4096k files* ***12 time 1w*** *compress*  *auth.debug /var/log/syslog/faillogin rotate size 4096k files* ***12 time 1w*** *compress* |

#### Đồng bộ thời gian HĐH về máy chủ tập trung

**Yêu cầu khắc phục:** Bật dịch vụ NTP để đồng bộ thời gian từ máy chủ thời gian chuẩn.

* Cách **1: Đồng bộ bằng dịch vụ ntp.**
* Bước 1: Sửa file /etc/ntp.conf, đảm bảo đã có những dòng sau:

|  |
| --- |
| *# vi /etc/ntp.conf*  *restrict default kod nomodify notrap nopeer noquery*  *restrict -6 default kod nomodify notrap nopeer noquery*  *restrict 127.0.0.1*  *restrict -6 ::1*  *Thêm dòng sau vào phía dưới dòng* ***#broadcastclient***  ***server 192.168.181.50 prefer***  *(Lưu ý: dòng* ***driftfile*** *và* ***tracefile*** *giữ nguyên)* |

* Bước 2: Kiểm tra trạng thái dịch vụ ntpd:

|  |
| --- |
| *# lssrc -a | grep xntp*  *xntpd tcpip 225286 active* |

* Bước 3: Nếu dịch vụ xntpd chưa chạy thì dùng lệnh

|  |
| --- |
| *# startsrc -s xntpd* |

* Bước 4: Để dịch vụ tự khởi động khi reboot:

|  |
| --- |
| *# vi /etc/rc.tcpip*  *Bỏ dấu # ở đầu dòng bên dưới để dịch vụ NTP khởi động cùng máy chủ sau khi reboot.*  *start /usr/sbin/xntpd "$src\_running"* |

* **Cách 2: Đồng bộ bằng crontab (Yêu cầu máy chủ phải cài đặt chương trình ntpdate).**
* Bước 1: Sửa crontab của root.

|  |
| --- |
| # *export EDITOR=vi*  *# crontab -e*  *# Bổ sung một crontab*  \*/5 \* \* \* \* ntpdate -u 192.168.181.50 |

#### Cấu hình ghi log command

Thực hiện backup tương tự các bước đối với hệ điều hành Linux ở Phụ lục 01.

Cấu hình:

* Thêm vào cuối file etc/profile 2 dòng:

PROMPT\_COMMAND='RETRN\_VAL=$?;logger -p local6.debug "[cmdlog] $(/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 files 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

## HƯỚNG DẪN CẤU HÌNH IPFILTER CHO AIX

* 1. **Giải nghĩa 1 số option trong quá trình thiết lập tường lửa trên hệ thống sử dụng điều hành AIX:**
* **lsfilt**: liệt kê các rule đang tồn tại.
* **genfilt:** tạo ra một rule mới, nếu câu lệnh không có option -n thì rule mới sẽ được thêm vào cuối của bảng.
* **chfilt:** sửa một rule đã tồn tại. Khi sử dụng lệnh này cần đưa cụ thể option -n tương ứng với ID của rule cần sửa. Rule có ID bằng 0,1,2 là các default rule và không thể sửa bằng lệnh này.
* **rmfilt:** xóa một rule tương ứng với ID đưa ra.
* **mkfilt:** câu lệnh dùng để active/deactive rules, enable/disable việc ghi log hoặc dùng để thay đổi default rule.
* **-v**: IP version, giá trị là “4” hoặc “6”.
* **-n**: Đưa ra số thứ tự của rule. Nếu không đưa giá trị cụ thể cho option này, rule sẽ mặc định gán vào cuối của tập luật.
* **-a**: "action" của rule. Giá trị "P" (permit) và "D" (deny).
* **-s**: Địa chỉ IP nguồn.
* **-m**: Subnet mask IP nguồn.
* **-d**: Địa chỉ IP đích.
* **-M**: Subnet mask IP đích.
* **-c**: Giao thức. Giá trị là "udp", "icmp", "tcp", "tcp/ack", và "all".
* **-o**: Source port/ICMP, là các toán tử so sánh giá trị port nguồn. Giá trị là "lt" (less than: nhỏ hơn), "le" (less than or equal to: nhỏ hơn hoặc bằng), "gt" (greater than: lớn hơn), "ge" (greater than or equal to: lớn hơn hoặc bằng), "eq" (equal), "neq" (not equal), hoặc "any".
* **-O**: Destination port/ICMP, là các toán tử so sánh giá trị port đích. Giá trị là "lt" (less than: nhỏ hơn), "le" (less than or equal to: nhỏ hơn hoặc bằng), "gt" (greater than: lớn hơn), "ge" (greater than or equal to: lớn hơn hoặc bằng), "eq" (equal), "neq" (not equal), hoặc "any".
* **-p**: Source port/ICMP , giá trị port nguồn được dùng để so sánh.Giá trị 0 cho tất cả các port.
* **-P**: Destination port/ICMP, giá trị port đích được dùng để so sánh.Giá trị 0 cho tất cả các port.
* **-w**: Chỉ ra rule sẽ áp dụng cho chiều incoming (I), outgoing (O) hay cả 2 (B).
* **-l**: Ghi log. Các giá trị là "Y" (yes) và "N" (no).
* **-i**: Interface, chỉ ra card mạng sẽ được áp dụng rule này.  Giá trị “all” cho tất cả card mạng.
  1. **Thiết lập cấp hình tường lửa**
  + B1: Thiết lập Policy Default:
* Xóa hết những rule đang tồn tại nếu có bằng lệnh:

|  |
| --- |
| *# rmfilt -n all -v4* |

* Chỉnh sửa các policy default:

|  |
| --- |
| *# smit ips4\_start* |

* + Chú ý: Lựa chọn các giá trị:

**Start IP Security**: Chọn ***Now and After Reboot*** để firewall có hiệu lực ngay lập tức và sau khi hệ thống reboot.

**Deny All Non\_Secure IP Packets**: Chú ý chọn ***No***. Nếu chọn Yes thì có thể sẽ bị mất kết nối sau khi cấu hình.

Sau đó nhấn Enter để khởi động firewall.

* List các giá trị: ***F4***, chọn giá trị sau đó ***Enter (bắt buộc phải thực hiện bước này để đảm bảo khởi động device cho IPSecurity)***.
* Thoát ra bằng lệnh ***Esc+0***
* Liệt kê các rule mặc định:

|  |
| --- |
| *# lsfilt -v4 -O*  *1|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|no|udp|eq|4001|eq|4001|both|both|no|all packets|0|all|0|||Default Rule*  *2|\*\*\* Dynamic filter placement rule for IKE tunnels \*\*\*|no*  *0|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|yes|all|any|0|any|0|both|both|no|all packets|0|all|0|||Default Rule* |

* + Chú ý: 3 rule trên là mặc định, không nên thay đổi giá trị gì.
  + B2: Tạo một file có tên ruleIPSec.sh trong folder root/backup/<date>:

*# vi /root/backup/<date>/ruleIPSec.sh*

|  |
| --- |
| #!/bin/ksh  # Khong thiet lap chan cac goi tin chieu vao tu loopback interface (lo0).  # Chu y: neu thiet lap bao invalid interface ”lo0” thi co the bo qua cau hinh nay  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c all -o any -p 0 -O any -P 0 -w B -l N -i lo0  # Không thiết lập chặn các gói tin chiều vào từ các internal interface  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c all -o any -p 0 -O any -P 0 -w B -l N -i en2  # Cho phep giao thuc ICMP  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c icmp -o any -p 0 -O any -P 0 -w I -l N –i en0  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c icmp -o any -p 0 -O any -P 0 -w O -l N –i en0  # Cho phep Server ket noi toi Server khac o cong 22 (SSH)  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp -o any -p 0 -O eq -P 22 -w O -l N -i en0  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp/ack -o eq -p 22 -O any -P 0 -w I -l N -i en0  # Cho quan tri IP 192.168.1.0/24 ket noi toi Server qua SSH  genfilt -v 4 -a P -s 192.168.1.0 -m 255.255.255.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp -o any -p 0 -O eq -P 22 -w I -l N -i en0  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 192.168.1.0 -M 255.255.255.0 -c tcp/ack -o eq -p 22 -O any -P 0 -w O -l N -i en0  # cho phep giao thuc HTTP va HTTPS  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp -o any -p 0 -O eq -P 80 -w I -l N -i en0  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp/ack -o any -p 0 -O eq -P 443 -w I -l N -i en0  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp -o eq -p 80 -O any -P 0 -w O -l N -i en0  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp/ack -o eq -p 443 -O any -P 0 -w O -l N -i en0  # Cho phep giao thuc dong bo thoi gian NTP  genfilt -v 4 -a P -s 192.168.181.50 -m 255.255.255.255 -d 0.0.0.0 -M 0.0.0.0 -c udp -o eq -p 123 -O eq -P 123 -w I -l N -i en0  genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 192.168.181.50 -M 255.255.255.255 -c udp -o eq -p 123 -O eq -P 123 -w O -l N -i en0  # Thiết lập ghi log và drop gói tin vi phạm  genfilt -v 4 -a D -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c all -o any -p 0 -O any -P 0 -w I -l Y -i en0 |
|  |

Chú ý:

* IPFilter không phải là tường lửa trạng thái do vậy muốn mở 1 kết nối thì cần phải mở cả chiều vào và chiều ra (xem ví dụ về rule mở cho phép telnet/ssh/http/https ở trên).
* IPFilter không cho phép mở 1 dải port ví dụ (từ 1024-2098) nó chỉ cho phép mở các port (>1024 hoặc <1024 hoặc =1024). Do vậy với các dịch vụ FTP server chạy ở chế độ passive cần phải cấu hình lại FTP chạy ở chế độ active mới có thể thiết lập được IPFilter.
  + B3: Thực thi file ruleIPSec.sh như sau:

|  |
| --- |
| *# cd /root/backup/<date>*  *# chmod +x ruleIPSec.sh*  *# ./ruleIPSec.sh* |

* + B4: Đưa các rule đã thiết lập vào thực thi:

|  |
| --- |
| *# mkfilt -v4 –u* |

* + B5: Kiểm tra lại các rule đang active bằng lệnh sau:

|  |
| --- |
| *# lsfilt -v4 -O –a* |

* + B6: Sau đó bắt đầu việc ghi log bằng lệnh:

|  |
| --- |
| *# mkfilt -v4 -g start* |

* Lưu ý: Nếu muốn dừng việc ghi log thì dùng lệnh sau:

|  |
| --- |
| *# mkfilt -v4 -g stop* |

## HƯỚNG DẪN CÀI ĐẶT OPENSSH TRÊN AIX

**Tải gói cài đặt OpenSSL và OpenSSH:**

**Tải OpenSSL:**

[*https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixbp*](https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixbp)

**Tải OpenSSH:**

[*http://sourceforge.net/projects/openssh-aix/files/*](http://sourceforge.net/projects/openssh-aix/files/)

Lưu ý là chọn đúng phiên bản OpenSSL và OpenSSH tương ứng với phiên bản hệ điều hành. Nếu không sẽ xảy ra lỗi trong quá trình cài đặt.

**II. Cài đặt OpenSSL và OpenSSH:**

Đầu tiên là cài đặt OpenSSL.

|  |
| --- |
| *# uncompress openssl-0.9.8.2500.tar.Z*  *# tar -xvf openssl-0.9.8.2500.tar*  *# cd openssl-0.9.8.2500*  *# smitty install* |

Chọn Install and Update Software > Install Software.

Nhập ‘.’ để chọn thư mục chứa file cài đặt là thư mục hiện tại.

Di chuyển xuống “ACCEPT new license agreements” và nhấn tab để đổi giá trị từ ‘No’ thành ‘Yes’.

Nhấn Enter để thực hiện quá trình cài đặt.

Tương tự với OpenSSH:

|  |
| --- |
| *# uncompress openssh\_5.4p1.tar.Z*  *# tar -xvf openssh\_5.4p1.tar*  *# smitty install* |

***Chú ý:*** Thực hiện cấu hình ssh theo yêu cầu mục 5 “Quản trị từ xa qua kênh truyền mã hóa”.

Restart lại dịch vụ sshd sau khi cài đặt và cấu hình xong để các thiết lập có hiệu lực:

|  |
| --- |
| # stopsrc –s sshd  # startsrc –s sshd |

## Cài đặt các hệ thống bảo vệ và giám sát hệ thống

Thực hiện tương tự các bước với hệ điều hành Linux ở Phụ lục 01

# IV. HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH SOLARIS

1. **Cài đặt hệ điều hành và cập nhật bản vá**

**Yêu cầu khắc phục:**

* Cài đặt phiên bản mới nhất tại khi cài đặt mới.
* Cập nhập các bản vá lỗi cho hệ điều hành: Bao gồm các bản vá lỗ hổng bảo mật đã được công bố và các bản vá theo yêu cầu của Tập đoàn.

**Chú ý:**

* Yêu cầu này chỉ áp dụng với các hệ thống đã mua bản quyền hệ điều hành Solaris.
* Thực hiện backup hệ thống trước khi cập nhật bản vá để giảm thiểu rủi ro.

1. **Hệ thống chỉ chạy các phần mềm tối thiểu đúng với chức năng được thiết kế**

**Yêu cầu khắc phục:**

* Cài đặt tối thiểu các phần mềm, dịch vụ theo đúng chức năng được thiết kế của server.
* Gỡ bỏ hoặc vô hiệu hóa các gói dịch vụ không cần thiết, các gói dịch vụ lỗi thời có nguy cơ bị mất an toàn thông tin:Telnet, rcp, rsh, rlogin, nis, ftp...
* Kiểm tra các dịch vụ đang chạy trên hệ điều hành. Nếu dịch vụ nào không cần thiết chạy thì thực hiện vô hiệu hóa hoặc xóa bỏ.

|  |
| --- |
| ***Phương án 1:*** *Vô hiệu hóa dịch vụ không cần thiết.*  *# svcs -a*  *#svcadmin disable < Tên dịch vụ cần tắt>*  *Ví dụ: # svcadmin disable network/telnet*  ***Phương án 2:*** *Gõ bỏ dịch vụ không cần thiết.*  *#* *pkgrm <Tên gói cần xóa>* |

1. **Thiết lập chính sách tài khoản**

**3.1 Xóa hoặc vô hiệu tất cả các tài khoản không sử dụng trên hệ thống**

**Yêu cầu khắc phục:** Rà soát hệ thống, liệt kê những tài khoản đang hoạt động trên hệ thống rồi tìm và xóa hoặc vô hiệu những tài khoản không sử dụng ra khỏi hệ thống.

|  |
| --- |
| *Bước 1: Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:*  *# passwd -s -a | grep PS*  *Bước 2: Kiểm tra xem các tài khoản này tài khoản nào không sử dụng. Thực hiện 1 trong 2 phương án:*  ***Phương án 1:*** *Vô hiệu các tài khoản:*  *# passwd -l username*  ***Phương án 2:*** *Xóa tài khoản:*  *#userdel username*  *Ví dụ: Trong danh sách có tài khoản game không sử dụng*  *#userdel game* |

**3.2 Cấu hình chính sách mật khẩu cho tài khoản**

**3.2.1 Mật khẩu phải có độ dài tối thiểu 8 ký tự chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt**

**Yêu cầu khắc phục:** Mật khẩu có độ dài tối thiểu 8 ký tự, đảm bảo phải bao gồm ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.

|  |
| --- |
| *#* *chmod u+w /etc/default/passwd*  *# export EDITOR=vi*  *# vi /etc/default/passwd*  *PASSLENGTH=8 (yêu cầu mật khẩu phải có ít nhất 8 ký tự)*  *MINALPHA=1 (yêu cầu mật khẩu phải có ít nhất 1 ký tự chữ)*  *MINDIGIT=1 (yêu cầu mật khẩu phải có ít nhất 1 ký tự số)*  *MINSPECIAL=1 (yêu cầu mật khẩu phải có ít nhất 1 ký tự đặc biệt)*  *MINUPPER=1 (yêu cầu mật khẩu phải có ít nhất 1 ký tự hoa)*  *# chmod u-w /etc/default/passwd* |

***Chú ý:*** Nếu không có quyền sửa file /etc/default/passwd thì gõ lệnh sau để có quyền sửa file:

|  |
| --- |
| *#* *chmod u+w /etc/default/passwd* |

**3.2.2 Thời gian bắt buộc phải thay đổi mật khẩu người dùng**

**Yêu cầu khắc phục:** Đối với mật khẩu người dùng, thiết lập thời gian tối đa bắt buộc tối đã 3 tháng (90 ngày)

Thay đổi giá trị MAXWEEKS=13 trong file /etc/default/passwd. Thực hiện như sau:

|  |
| --- |
| *# chmod u+w /etc/default/passwd*  *# export EDITOR=vi*  *# vi /etc/default/passwd*  *MAXWEEKS=13*  *# chmod u-w /etc/default/passwd*  *# passwd -s -a | grep PS*  *# passwd -x 91 <user\_name>* |

***Chú ý:***

* Trong file /etc/default/passwd không có tùy chọn MAXDAY=90 do vậy với tùy chọn MAXWEEKS=13 sẽ tương đương với thời hạn hết hạn mật khẩu là 91 ngày.
* Câu lệnh passwd -s -a | grep PS có ý nghĩa liệt kê toàn bộ tài khoản có khả năng đăng nhập vào hệ thống. Một số tài khoản đang bị khóa hoặc không có quyền đăng nhập vào hệ thống sẽ không được liệt kê.

**3.2.3 Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất**

**Yêu cầu khắc phục:** Đối với mật khẩu người dùng, thiết lập bắt buộc mật khẩu mới phải không trùng với 5 mật khẩu gần nhất.

Thay đổi giá trị HISTORY=5 trong file /etc/default/passwd. Thực hiện như sau:

|  |
| --- |
| *# chmod u+w /etc/default/passwd*  *# export EDITOR=vi*  *# vi /etc/default/passwd*  *HISTORY=5* |

**3.2.4 Mật khẩu phải được lưu dưới dạng mã hóa sử dụng thuật toán băm SHA-512**

**Yêu cầu khắc phục:** Kiểm tra và nâng cấp phương thức mã hóa mật khẩu, sử dụng thuật toán băm SHA-512.

Thực hiện 02 lệnh sau để đảm bảo hệ thống có hỗ trợ thuật toán băm sha-512.

|  |
| --- |
| *# cat /etc/security/policy.conf | grep CRYPT\_ALGORITHMS\_ALLOW | grep -v ^#*  *Kết quả trả về : CRYPT\_ALGORITHMS\_ALLOW=1,2a,md5,5,****6***  *# cat /etc/security/crypt.conf | grep crypt\_sha512*  *Kết quả trả về :* ***6***  *crypt\_sha512.so.1* |

* Nếu kết quả trả về giống như ví dụ trên thì hệ điều hành có hỗ trợ mã hóa sha-512. Thực hiện các bước sau để thiết lập lưu password dưới dạng thuật toán băm sha-512:

Lưu password dưới dạng thuật toán băm sha-512. Thực hiện sửa hoặc thêm tùy chọn sau vào file /etc/security/policy.conf. Cụ thể:

|  |
| --- |
| *# export EDITOR=vi*  *# vi /etc/security/policy.conf*  *CRYPT\_DEFAULT=6* |

***Chú ý:***

* Sau khi thiết lập tham số phải đăng nhập thử vào hệ thống. Nếu không đăng nhập được nghĩa là hệ thống không hỗ trợ thuật toán mã hóa SHA-512. Phải cấu hình tham số ”CRYPT\_DEFAULT=MD5” nghĩa là sử dụng thuật toán MD5 để thay thế.
* Với những tài khoản đang tồn tại trên hệ thống phải thực hiện các bước sau để chính sách được áp dụng:

|  |
| --- |
| 1. Liệt kê danh sách mật khẩu   *# passwd -s -a | grep PS*   1. Xóa mật khẩu cũ của tài khoản   *# password -d username*   1. Đặt lại mật khẩu mới cho tài khoản   *# passwd username*   1. Buộc người dùng phải đổi mật khẩu ở lần đăng nhập tiếp theo   *# passwd -f username* |

1. **Quản trị từ xa qua kênh truyền an toàn.**

**Yêu cầu khắc phục:** Để đảm bảo an toàn yêu cầu chỉ sử dụng công cụ quản trị từ xa có mã hóa đường truyền. Chỉ sử dụng SSH để quản trị máy chủ, khi sử dụng SSH cần thực hiện các thiết lập sau *(Yêu cầu khởi động lại dịch vụ SSH khi thiết lập xong cấu hình):*

**4.1 Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa**

***Chỉ cho phép sử dụng giao thức SSH version 2.***

|  |
| --- |
| *Mở file cấu hình /etc/ssh/sshd\_config, sửa lại tùy chọn:*  *Protocol 2* |

***Cấu hình chỉ cho phép tài khoản người dùng được phép SSH.***

|  |
| --- |
| *Mở file cấu hình /etc/ssh/sshd\_config, thêm tùy chọn sau:*  *AllowUsers user1 user2* |

***Không cho phép tài khoản root đăng nhập trực tiếp từ xa.***

|  |
| --- |
| *Mở file cấu hình /etc/ssh/sshd\_config, sửa hoặc thêm tùy chọn sau:*  *PermitRootLogin no* |

**4.2 Không cho phép tài khoản đăng nhập sai là 05 lần**

|  |
| --- |
| *Mở file cấu hình /etc/default/login, sửa hoặc thêm tùy chọn sau:*  *RETRIES=5* |

**4.3 Thiết lập thời gian tự động ngắt phiên nếu phiên không có hoạt động trong 5 phút**

|  |
| --- |
| *Mở file cấu hình /etc/profile, thêm 3 dòng sau vào cuối file:*  *TMOUT=300*  *readonly TMOUT*  *export TMOUT* |

1. **Phân quyền tệp tin và thư mục**

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

**Yêu cầu khắc phục:** Kiểm tra biến môi trường PATH không được chứa các đường tương đối, đường dẫn bất thường, đường dẫn trống.

|  |
| --- |
| *Để ki km tra biến môi trường PAT, ta dùng lệnh sau:*  *# echo $PATH*  *Ví dụ:*  *PATH chứa đường dẫn trống: PATH /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin****::***  *PATH chứa đường đẫn tương đối: /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:****./src/bin***  *PATH chứa đường dẫn nguy hiểm: /bin:/us: /usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:****/tmp*** |

**5.2 Thiết lập cấu hình dịch vụ CRON**

**Yêu cầu khắc phục:**

* Giới hạn tài khoản được phép chạy dịch vụ CRON bởi whitelist danh sách người dùng.
* Bước 1: Thực thi lệnh xóa file cron.deny:

|  |
| --- |
| *# rm /etc/cron.d/cron.deny* |

* Bước 2: Thêm file cron.allow nếu hệ thống chưa có:

|  |
| --- |
| *#touch /etc/cron.d/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*  *…* |

* Hạn chế quyền sửa các file cấu hình của CRON

|  |
| --- |
| *# chown -R root:root /var/spool/cron/crontabs/*  *# chmod -R 600 /var/spool/cron/crontabs/*  *# chown -R root:root /etc/cron.d*  *#chmod -R go-rwx /cron.d* |

1. **Cấu hình tường lửa mềm**

**6.1 Yêu cầu sử dụng tường lửa mềm trên hệ thống**

**Yêu cầu khắc phục:** Kiểm tra đảm bảo tường lửa mềm được bật.

|  |
| --- |
| *# svcs -a | grep ipf*  *online 10:06:55 svc:/network/ipfilter:default* |

* Nếu câu lệnh trả về có giá trị là ”online” thì dịch vụ đang được bật, Ngược lại nghĩa là tường lửa chưa được bật. Và phải cấu hình rule và bật theo các mục bên dưới.

**6.2 Giới hạn địa chỉ IP quản trị được phép truy cập đến máy chủ**

**6.3 Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống**

**Yêu cầu khắc phục:** Sử dụng tường lửa chỉ mở kết nối giới hạn.

* Đối với hệ thống nội bộ:
* Chỉ mở vừa đủ các kết nối vào (Chiều INPUT).
* Đối với hệ thống public:
* Yêu cầu mở vừa đủ các kết nối vào (Chiều INPUT).
* Yêu cầu mở vừa đủ các kết nối ra (Chiều OUTPUT).

***Chú ý:*** Người quản trị cần phải cấu hình tường lửa ở chế độ ghi log các gói tin trong vòng 1-2 tuần. Sau đó sẽ phân tích logs và thiết lập rule tương ứng. Thực hiện theo ”Hướng dẫn cấu hình ipfilter cho Solaris”.

**6.4 Ghi log toàn bộ những bản tin vào ra không hợp lệ**

**Yêu cầu khắc phục:** Ghi toàn bộ log vào/ra hệ thống không hợp lệ. Thực hiện theo ”Hướng dẫn cấu hình ipfilter cho Solaris”.

1. **Thiết lập chính sách quản lý log**

**7.1 Ghi log mặc định của hệ điều hành**

**Yêu cầu khắc phục:** Yêu cầu thiết lập cấu hình ghi log tối thiểu các loại sau: message log, dmesg log, secure log.

* Bước 1: Cấu hình log đăng nhập failed:

|  |
| --- |
| *# export EDITOR=vi*  *# vi /etc/default/login*  *SYSLOG\_FAILED\_LOGINS=0*  *# touch /var/adm/authlog* |

* Bước 2: Thêm vào đầu file /etc/syslog.conf dòng sau:

|  |
| --- |
| *# export EDITOR=vi*  *# vi /etc/syslog.conf*  *auth.notice;auth.crit;auth.info /var/adm/authlog* |

* Bước 3: Resart lại dịch vụ syslog:

|  |
| --- |
| *# svcadm disable system/system-log*  *# svcadm enable system/system-log* |

Kiểm tra lại trạng thái của dịch vụ system-log xem đã chắc chắn được bật chưa. Sử dụng câu lệnh sau:

|  |
| --- |
| *# svcs system-log*  *STATE STIME FMRI*  ***online***  *15:13:31 svc:/system/system-log:default* |

Nếu có STATE là ”Online” nghĩa là dịch vụ đang hoạt động bình thường.

**7.2 Cấu hình thời gian lưu log tối thiểu là 3 tháng**

**Yêu cầu khắc phục:** Thiết lập cấu hình thời gian lưu log tối thiểu 03 tháng.

Mở file /etc/logadm.conf, kiểm tra cấu hình sẵn có và thêm vào cấu hình cho các file log /var/log/firewall, /var/adm/messages như sau:

|  |
| --- |
| *# export EDITOR=vi*  *# vi /etc/logadm.conf*  */var/adm/messages -A 3m -C 10 -s 10m -z 0 -a 'kill -HUP `cat /var/run/syslog.pid`'*  */var/log/firewall -A 3m -C 10 -s 10m -z 0 -a 'kill -HUP `cat /var/run/syslog.pid`'* |

***Trong đó:***

* A là số ngày tối đa lưu file logs đơn vị là ”h” chỉ số giờ, ”d” chỉ số ngày, ”m” chỉ số tháng, ”y” chỉ số năm.
* C là số file log cũ tối đa sẽ giữ lại.
* s là kích cỡ tối đa 1 file logs (ở đây là 10 MB).

***Chú ý:*** Theo quy định của Tập đoàn thời gian tối thiểu lưu log là 3 tháng. Tuy nhiên nếu máy chủ hiện tại không đủ dung lượng ổ cứng để lưu log trong 3 tháng. Còn số này quản trị có thể thiết lập lại để phù hợp với thực tế tránh log đầy làm treo máy chủ.

* Bước 1: Kiểm tra lại kết quả

|  |
| --- |
| *# logadm -V* |

* Bước 2: Kiểm tra logadm đã có trong crontab chưa

|  |
| --- |
| *# crontab -l* |

* Nếu kết quả trả về chưa có dòng ”***10 3 \* \* \* /usr/sbin/logadm***” thì thực hiện câu lệnh sau để thêm vào.

|  |
| --- |
| *# export EDITOR=vi*  *# crontab -e*  *10 3 \* \* \* /usr/sbin/logadm* |

* Bước 3: Thêm dòng bên dưới vào tệp tin ***/etc/syslog.conf***

|  |
| --- |
| *local0.debug /var/log/firewall* |

* Bước 4: Tạo file firewall bằng câu lệnh sau

|  |
| --- |
| *# touch /var/log/firewall*  *# chmod 600 /var/log/firewall* |

* Bước 5: Restart lại dịch vụ syslog

|  |
| --- |
| *# svcadm restart system-log* |

**7.3 Đồng bộ thời gian HĐH về máy chủ tập trung**

**Yêu cầu khắc phục:** Bật dịch vụ NTP để đồng bộ thời gian từ máy chủ thời gian chuẩn.

* **Cách 1: Đồng bộ bằng dịch vụ ntp.**
* Bước 1: Tạo file /etc/inet/ntp.conf

|  |
| --- |
| *# cp /etc/inet/ntp.client /etc/inet/ntp.conf* |

* Bước 2: Sửa file /etc/inet/ntp.conf
* Thay thế ***multicastclient 224.0.1.1***
* Bằng ***server 192.168.181.50***
* Bước 3: Chạy dịch vụ ntpd và khởi động lại dịch vụ bằng lệnh:

|  |
| --- |
| *# service disable network/ntp*  *# service enable network/ntp* |

Kiểm tra việc đồng bộ có thành công hay không, sử dụng lệnh:

|  |
| --- |
| *# ntpq -p*  *remote refid st t when poll reach delay offset disp*  *======================================================*  *192.168.181.50 0.0.0.0 2 u 21 64 3 376.54 -71.105 7889.14* |

* **Cách 2: Đồng bộ bằng crontab (Yêu cầu máy chủ phải cài đặt chương trình ntpdate).**
* Bước 1: Sửa crontab của root.

|  |
| --- |
| # *export EDITOR=vi*  *# crontab -e*  *# Bổ sung một crontab*  \*/5 \* \* \* \* ntpdate -u 192.168.181.50 |

1. **HƯỚNG DẪN CẤU HÌNH IPFILTER CHO SOLARIS**
   1. **Cấu hình tường lửa ở chế độ ghi logs**

* Trước khi thiết lập tường lửa chặn hết chiều vào/ra của hệ thống. Cần phải thống kê được các kết nối mà máy chủ cần kết nối tới đâu… Do đó quản trị phải thiết lập rule để ghi logs các kết nối vào/ra trên máy chủ từ 1-2 tuần để phân tích.
* Bước 1: Mở file /etc/ipf/ipf.conf

|  |
| --- |
| *# vi /etc/ipf/ipf.conf* |

* Sửa nội dung file như sau:

|  |
| --- |
| *## Allow all loopback (local) traffic*  *pass in quick on lo0*  *pass out quick on lo0*  *# Allow IP: 192.168.80.1 SSH to server.*  *pass in quick proto tcp from 192.168.80.1/32 to any port = 22 flags S keep state*  *#Allow public DNS*  *pass in quick proto tcp from any to any port = 53 flags S keep state*  *pass in quick proto udp from any to any port = 53*  *#Allow public Web*  *pass in quick proto tcp from any to any port = 80 flags S keep state*  *pass in quick proto tcp from any to any port = 443 flags S keep state*  *#Allow public FTP active*  *pass in quick proto tcp from any to any port = 21 flags S keep state*  *pass out quick proto tcp from any to any port = 20 flags S keep state*  *#Allow public FTP passive*  *# Them dong “passive ports 0.0.0.0/0 29000 29500” vào file /etc/ftpd/ftpaccess*  *# dinh nghia port passive tu 29000 toi 29500 va mo tren tuong lua cac port nay.*  *pass in quick proto tcp from any to any port = 21 flags S keep state*  *pass out quick proto tcp from any to any port = 20 flags S keep state*  *pass in quick proto tcp from any to any port 29000><29500 flags S keep state*  *# Allow ping to server*  *pass in quick proto icmp from any to any icmp-type 8 keep state*  *# Set a default* ***allow*** *policy and log all dropped traffic*  *pass in quick log all*  *pass out quick log all* |

**Trong đó:**

* “pass in quick on lo0” và “pass out quick on lo0”: 02 rule này cho phép mở cả chiều vào và ra trên card loopback.
* “pass in quick proto tcp from 192.168.80.1/32 to any port = 22 keep state”: Rule này cho phép địa chỉ 192.168.80.1 được phép kết nối tới máy chủ với port là 22.
* “pass in quick proto icmp from any to any icmp-type 8 keep state” **:** Rule này cho phép các máy khác có thể ping được tới máy chủ.
* “pass in quick log all” và “pass out quick log all”: 02 rule này cho phép mở cả chiều vào/ra trên hệ thống đồng thời ghi logs toàn bộ các rule **không** được khai báo ở trên.
* Chú ý: Nếu thêm rule mới vào file /etc/ipf/ipf.conf. Các rule này phải nằm ở trước 2 rule “pass in quick log all” và “pass out quick log all”
* Bước 2: Sau khi tạo file /etc/ipf/ipf.conf với nội dung trên. Tiến hành bật firewall để ghi log với câu lệnh.

|  |
| --- |
| *# svcadm adisable svc:/network/ipfilter:default*  *# svcadm enable svc:/network/ipfilter:default* |

* Bước 3: Kiểm tra lại xem ipfilter đã thực sự bật chưa

|  |
| --- |
| *# svcs -a | grep ipf*  *online 10:38:21 svc:/network/ipfilter:default* |

* Nếu kết quả trả về là online nghĩa là tường lửa đã được bật.
* Bước 4: Kiểm tra xem tường lửa đã ghi lại logs đúng theo cấu hình chưa.

|  |
| --- |
| *# tail -f /var/log/firewall* |

**8.2 Cấu hình tường lửa chỉ cho phép vừa đủ các kết nối vào/ra đảm bảo dịch vụ**

* Bước 1: Lên máy chủ lấy file /var/log/firewall về kiểm tra logs để thống kê các kết nối cần mở trên firewall.
* Bước 2: Bổ sung các rule cần mở theo thống kê ở bước 1 vào file /etc/ipf/ipf.conf.
* Bước 3: Sửa lại rule trong file /etc/ipf/ipf.conf để chặn toàn bộ các kết nối không được phép. Cụ thể như sau:

|  |
| --- |
| *## Allow all loopback (local) traffic*  *pass in quick on lo0*  *pass out quick on lo0*  *# Allow IP: 192.168.80.1 SSH to server.*  *pass in quick proto tcp from 192.168.80.1/32 to any port = 22 keep state*  *#Allow public DNS*  *pass in quick proto tcp from any to any port = 53 keep state*  *pass in quick proto udp from any to any port = 53 keep state*  *#Allow public Web*  *pass in quick proto tcp from any to any port = 80 keep state*  *pass in quick proto tcp from any to any port = 443 keep state*  *#Allow public FTP active*  *pass in quick proto tcp from any to any port = 21 keep state*  *pass out quick proto tcp from any to any port = 20 keep state*  *#Allow public FTP passive*  *# Them dong “passive ports 0.0.0.0/0 29000 29500” vào file /etc/ftpd/ftpaccess*  *# dinh nghia port passive tu 29000 toi 29500 va mo tren tuong lua cac port nay.*  *pass in quick proto tcp from any to any port = 21 keep state*  *pass out quick proto tcp from any to any port = 20 keep state*  *pass in quick proto tcp from any to any port 29000><29500 keep state*  *#Allow server request DNS*  *pass out quick proto udp from any to any port = 53 keep state*  *#Allow ntpclient request*  *pass out quick proto udp from any to any port = 123 keep state*  *# Allow ping to server*  *pass in quick proto icmp from any to any icmp-type 8 keep state*  *#Allow ping from server*  *pass out quick proto icmp from any to any icmp-type 8 keep state*  *# Set a default* ***block*** *policy and log all dropped traffic*  ***block*** *in quick log all*  ***block*** *out quick log all* |

* Bước 4: Trước khi chuyển qua bước 5 khởi động lại dịch vụ IPFilter để tường lửa lấy cấu hình mới. Cần phải thiết lập crontab lập lịch sau 1 phút tự động stop tường lửa loại trừ trường hợp ta thiết lập rule sai không truy cập được vào server. Thực hiện thêm chạy câu lệnh sau:

|  |
| --- |
| *# export EDITOR=vi*  *# crontab -e*  *\* \* \* \* \* /usr/sbin/svcadm disable svc:/network/ipfilter:default* |

* Bước 5: Khởi động lại dịch vụ IPFilter để tường lửa nhận cấu hình mới.

|  |
| --- |
| *# svcadm disable svc:/network/ipfilter:default*  *# svcadm enable svc:/network/ipfilter:default*  *# ipfstats -io* |

* Bước 6: Kiểm tra lại dịch vụ. Chú ý: Phải kiểm tra dịch vụ khi lệnh trong crontab chưa kịp tắt tường lửa vì tường lửa sẽ tự động tắt sau 1 phút.
* Bước 7: Nếu sau khi khởi động lại dịch vụ ipfilter các dịch vụ vẫn hoạt động bình thường. Tiến hành thêm dấu ”#” vào trước câu lệnh disable firewall trong crontab, cụ thể như sau:

|  |
| --- |
| *# export EDITOR=vi*  *# crontab -e*  *#\* \* \* \* \* /usr/sbin/svcadm disable svc:/network/ipfilter:default* |

* Bước 8: Khởi động lại ipfilter lần cuối để chắc chắn tường lửa được bật.

|  |
| --- |
| *# svcadm disable svc:/network/ipfilter:default*  *# svcadm enable svc:/network/ipfilter:default*  *# ipfstats -io* |

1. **Cài đặt các hệ thống bảo vệ và giám sát hệ thống**

**9.1 Cài đặt phần mềm Server Endpoint hỗ trợ giám sát bất thường và vi phạm baselines**

## Điều kiện đảm bảo

* Id cho agent được cài đặt phải được khai báo với hệ thống trước khi bắt đầu cài đặt cho agent. Id của agent là duy nhất.
* Id agent có format như sau: **TênHĐH\_Ipv4**. Ví dụ: **windows\_10.10.0.1**
* Các đơn vị khác VTNet, đề nghị khi tạo ID bổ sung prefix tên viết tắt của đơn vị (VD: vtidc, vtt, vttek,..). Ví dụ: **vtt\_centos\_10.30.58.164**
* Toàn bộ sử dụng chữ viết thường
* Tên hệ điều hành là windows, centos, redhat, oracle, solaris, suse …
* Địa chỉ IP theo chuẩn IP v4.
* Chương trình cài đặt bắt buộc chạy với user Administrator đối với hệ hiều hành Windows và user root với hệ điều hành Linux, Solaris.
* Đối với các agent tương ứng cần có các gói sau:

| **Linux** |  |
| --- | --- |
| wget | Download dữ liệu từ repository |
| unzip | Giải nén file nén chứa file cài đặt |
| **Windows** |  |
| powershell | Giao diện quản trị lệnh của Windows |
| vcredist | Lib c trên windows |

* Thông kết nối từ agent tới server tập trung (10.30.160.44, 10.30.160.45, 10.30.160.46) tương ứng các cổng sau: 80, 443, 4505, 4506, 6379.
* Kiểm tra kết nối từ máy tính của người thực hiện tới địa chỉ portal của hệ thống SIRC (10.30.160.41) cổng 80 (http), 443 (https) và 8443 (https).
* Phân giải được các domain của hệ thống SIRC. Mặc định trên hệ thống DNS đã có cấu hình domain này, trong trường hợp chưa phân giải được, cấu hình file host trên máy tính của người thực hiện cài đặt để truy cập vào trang web quản trị:

10.30.160.41 srm.sirc.viettel.com

10.30.160.41 se.sirc.viettel.com

10.30.160.41 cas.sirc.viettel.com

**Bước 1:** Khai báo server\_id trên Portal <http://se.sirc.viettel.com/#/server/list>

**Bước 2:** Chuẩn bị cài đặt

mkdir /opt/se

cd /opt/se

wget http://10.30.160.44/serverendpoint/salt\_setup-2015.7.0.solaris.zip

unzip salt\_setup-2015.7.0.solaris.zip -d /opt/se

**Bước 3:** Tạo file config.txt trong thư mục /opt/se

echo id: <server\_id> >> /opt/se/config.txt

echo salt\_repos: http://10.30.160.44/serverendpoint/ >> /opt/se/config.txt

Chú ý: Sau ký tự ":" phải có dấu cách

**Bước 4:** Install

su root

chmod a+x -R /opt/se

sh /opt/se/se-setup.sh install

**Bước 5:** Kiểm tra cài đặt thành công

/opt/se/salt-call vsm.status

ret:

local:

----------

version:

2014.7.4