BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 3001 /BTTTT-CATTT V/v hướng dẫn bảo đảm an toàn thông tin cho hệ thống quản lý văn bản và điều hành	*Hà Nội, ngày 06 tháng 9 năm 2019*

Kính gửi:
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn kinh tế, tổng công ty Nhà nước.

Thực hiện chức năng quản lý nhà nước về an toàn thông tin của Bộ Thông tin và Truyền thông tại Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Thực hiện chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 28/2018/QĐ-TTg ngày 12 tháng 7 năm 2018 của Thủ tướng Chính phủ về gửi, nhận văn bản điện tử giữa các cơ quan trong hệ thống hành chính nhà nước;

Bộ Thông tin và Truyền thông hướng dẫn đảm bảo an toàn thông tin cho hệ thống Quản lý văn bản và điều hành của cơ quan, tổ chức nhà nước. Nội dung hướng dẫn bao gồm: Các thành phần cơ bản, các yêu cầu an toàn cơ bản và phương án thực thi để bảo đảm an toàn thông tin cho hệ thống Quản lý văn bản và điều hành.

Bản mềm tài liệu hướng dẫn có thể được tải về từ cổng thông tin điện tử của Bộ Thông tin và Truyền thông tại địa chỉ: http://www.mic.gov.vn hoặc từ cổng thông tin điện tử của Cục An toàn thông tin tại địa chỉ https://www.ais.gov.vn/huong-dan-bao-dam-an-toan-thong-tin-cho-he-thong-quan-ly-van-ban-dieu-hanh.

Chi tiết liên hệ ông Nguyễn Tiến Đức, Phòng Thẩm định và Quản lý giám sát, Cục An toàn thông tin, Điện thoại: 0934578162; Thư điện tử: ntduc@mic.gov.vn.

Trong quá trình thực hiện, nếu có điều gì vướng mắc, đề nghị các cơ quan, tổ chức, phản ánh về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để được hướng dẫn giải quyết./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử Chính phủ;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Đơn vị chuyên trách về CNTT của Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Kiểm toán nhà nước;
- Đơn vị chuyên trách về CNTT của Cơ quan Trung ương của các đoàn thể;
- Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương;
- Cổng thông tin điện tử Bộ TT&TT;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Thành Hưng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU HƯỚNG DẪN
BẢO ĐẢM AN TOÀN THÔNG TIN CHO HỆ THỐNG QUẢN LÝ VĂN BẢN VÀ ĐIỀU HÀNH CỦA CƠ QUAN, TỔ CHỨC NHÀ NƯỚC

(Kèm theo Công văn số 3001 /BTTTT-CATTT ngày 06 tháng 9 năm 2019 của Bộ Thông tin và Truyền thông)

Hà Nội, 2019

Chương I
PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG

1.1. Phạm vi áp dụng

a) Tài liệu này hướng dẫn các thành phần cơ bản, các yêu cầu an toàn cơ bản và phương án thực thi bảo đảm an toàn thông tin cho hệ thống Quản lý văn bản và điều hành (sau đây gọi là hệ thống QLVBĐH) chạy trên nền tảng ứng dụng Web, sử dụng trong các cơ quan, tổ chức nhà nước.

b) Tài liệu này đưa ra các yêu cầu an toàn thông tin cơ bản, hướng dẫn bảo đảm an toàn thông tin cho hệ thống QLVBĐH.

1.2. Đối tượng áp dụng

a) Tài liệu này áp dụng đối với các cơ quan, tổ chức, cá nhân có liên quan đến việc sử dụng, quản lý và vận hành hệ thống QLVBĐH trong các cơ quan, tổ chức nhà nước.

b) Khuyến khích cácdoanh nghiệp, tổ chức khác áp dụng hướng dẫn này để bảo đảm an toàn thông tin cho hệ thống QLVBĐH thuộc phạm vi quản lý.

1.3. Thuật ngữ, định nghĩa

a) An toàn dữ liệu (data security): Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm tính bảo mật, tính nguyên vẹn và tính khả dụng của thông tin, dữ liệu khi lưu trữ, xử lý, truy nhập, cung cấp, thu thập và truyền đưa dữ liệu qua môi trường mạng.

b) An toàn mạng (network security): Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm việc thiết lập, xây dựng, quản lý, vận hành hạ tầng mạng (bao gồm: kênh kết nối, thiết bị mạng, thiết bị bảo mật, thiết bị phụ trợ và các thành phần khác nếu có) bảo đảm an toàn.

c) An toàn máy chủ (server security): Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm an toàn cho máy chủ trong quá trình thiết lập, quản lý, vận hành và hủy bỏ.

d) An toàn ứng dụng (application security): Tập hợp các biện pháp quản lý và kỹ thuật nhằm bảo đảm các ứng dụng, dịch vụ cung cấp bởi hệ thống bảo đảm an toàn trong quá trình thiết lập, quản lý, vận hành và gỡ bỏ.

đ) Chống thất thoát dữ liệu (data leak prevention): Giải pháp giúp cơ quan, tổ chức bảo vệ dữ liệu quan trọng của mình tránh việc bị đánh cắp, rò rỉ hoặc khi dữ liệu bị vô ý mất mát, thất lạc thì bên thứ ba không thể khai thác dữ liệu đó trái phép.

e) Dự phòng nóng (hot standby): Khả năng thay thế chức năng của thiết bị khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

g) Giám sát an toàn hệ thống thông tin (information system security monitoring): Hoạt động lựa chọn đối tượng, công cụ giám sát, thu thập, phân tích thông tin trạng thái của đối tượng giám sát, báo cáo, cảnh báo hành vi xâm phạm an toàn thông tin hoặc có khả năng gây ra sự cố an toàn thông tin đối với hệ thống thông tin.

h) Giám sát hệ thống thông tin (information system monitoring): Biện pháp giám sát, theo dõi trạng thái hoạt động của hệ thống để phát hiện, cảnh báo sớm các sự cố có thể gây gián đoạn hoạt động của hệ thống và làm mất tính khả dụng của hệ thống thông tin.

i) Nhật ký hệ thống (system log): Những sự kiện được hệ thống ghi lại liên quan đến trạng thái hoạt động, sự cố, sự kiện an toàn thông tin và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

k) Phần mềm độc hại (malware): Phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

l) Phần mềm phòng chống mã độc (anti-malware software): Phần mềm có chức năng phát hiện, cảnh báo và xử lý phần mềm độc hại.

m) Quản lý tài khoản đặc quyền (privileged identity management - PIM): Biện pháp quản lý tập trung các tài khoản có quyền quản trị cao nhất (có đầy đủ các quyền hệ thống cung cấp) trên hệ thống.

n) Thiết bị mạng chính (core network device): Thiết bị gây gián đoạn hoạt động của toàn bộ hệ thống khi xảy ra sự cố. Ví dụ: thiết bị chuyển mạch trung tâm, thiết bị định tuyến biên, tường lửa trung tâm và các thiết bị khác có chức năng và vị trí tương đương.

o) Vùng DMZ (demilitarized zone): Vùng mạng được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.

p) Vùng máy chủ nội bộ (internal server zone): Vùng mạng được thiết lập để đặt các máy chủ nội bộ, cung cấp các ứng dụng, dịch vụ phục vụ hoạt động nội bộ của tổ chức và các hoạt động khác mà không cho phép truy cập trực tiếp từ các mạng bên ngoài.

q) Vùng quản trị (management zone): Vùng mạng được thiết lập để đặt các máy chủ, máy quản trị và các thiết bị chuyên dụng khác phục vụ việc quản lý, vận hành và giám sát hệ thống.

r) Vùng quản trị thiết bị hệ thống (device management zone): Vùng mạng riêng cho các địa chỉ quản trị của các thiết bị hệ thống cho phép thiết lập chính sách chung và quản lý tập trung các thiết bị hệ thống.

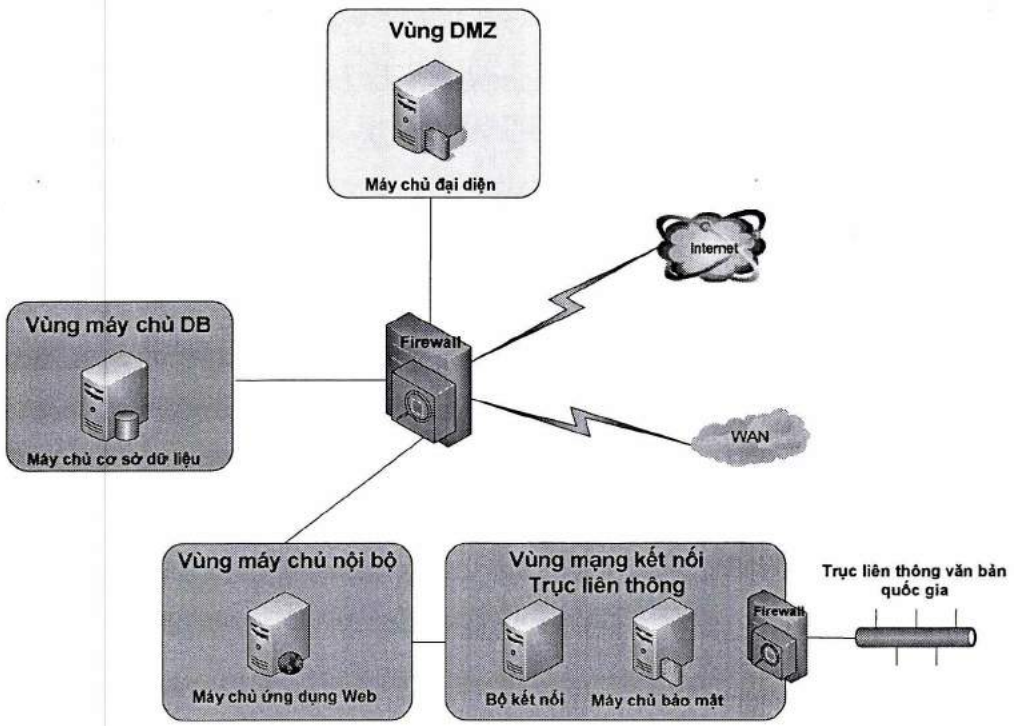
s) Vùng máy chủ cơ sở dữ liệu (database server zone): Vùng mạng được thiết lập để đặt các máy chủ cơ sở dữ liệu. Các máy chủ trong vùng này được triển khai tách biệt với các máy chủ ứng dụng cho phép quản lý chính sách truy cập hoặc thiết lập các biện pháp bảo vệ tập trung cho các máy chủ trong vùng mạng này.

t) Máy chủ đại diện (Reverse proxy): Máy chủ trung gian giữa một máy chủ web và các máy trạm. Máy chủ này kiểm soát yêu cầu từ các trạm để kiểm tra tính hợp lệ của yêu cầu trước khi gửi đến máy chủ web.

Chương II
TỔNG QUAN VỀ HỆ THỐNG QUẢN LÝ VĂN BẢN VÀ ĐIỀU HÀNH

2.1. Mô hình và thành phần cơ bản của hệ thống QLVBĐH

Thành phần cơ bản của hệ thống QLVBĐH bao gồm:



Hình 1. Thành phần cơ bản để phục vụ hoạt động của hệ thống QLVBĐH

a) Máy chủ đại diện (Reverse proxy) là máy chủ tiếp nhận yêu cầu trực tiếp từ các máy ngoài Internet. Máy chủ này đại diện cho các máy khách từ bên ngoài Internet để gửi yêu cầu tới máy chủ ứng dụng Web trong vùng mạng nội bộ. Việc sử dụng máy chủ Reverse proxy để hạn chế việc truy cập trực tiếp từ các máy

khách đến máy chủ ứng dụng Web làm giảm thiểu nguy cơ mất an toàn thông tin cho máy chủ này.

Máy chủ đại diện có thể được triển khai trên nhiều nền tảng khác nhau: (1) Triển khai dưới dạng máy chủ cài đặt hệ thống Reverse Proxy như: Nginx, Apache, IIS ARR...; (2) sử dụng thiết bị tường lửa ứng dụng web chuyên dụng như: Fortiweb, Big-IP LTM, NetScaler...

Máy chủ Reverse proxy được đặt tại vùng DMZ. Các máy chủ trong vùng DMZ được thiết lập hệ thống bảo vệ để kiểm soát truy nhập, phòng chống xâm nhập, tấn công mạng và tấn công từ chối dịch vụ DoS/DDoS.

b) Máy chủ ứng dụng web là máy chủ quản lý hoạt động của toàn bộ hệ thống QLVBĐH. Máy chủ này thực hiện chức năng tiếp nhận các yêu cầu gửi đến, xử lý, kết nối cơ sở dữ liệu và phản hồi yêu cầu gửi đến.

Máy chủ ứng dụng web có thể được triển khai trên nhiều nền tảng khác nhau như: IIS, Apache, Tomcat... tùy thuộc vào ứng dụng quản lý văn bản được phát triển.

Máy chủ ứng dụng được đặt tại vùng máy chủ nội bộ và không cho truy cập trực tiếp từ bên ngoài Internet. Các máy chủ trong vùng máy chủ nội bộ được thiết lập hệ thống bảo vệ để kiểm soát truy nhập, phòng chống xâm nhập và tấn công mạng.

c) Máy chủ cơ sở dữ liệu lưu trữ và quản lý cơ sở dữ liệu của hệ thống QLVBĐH. Máy chủ này được đặt trong một vùng mạng riêng cho các máy chủ cơ sở dữ liệu và không cho phép kết nối, truy cập trực tiếp từ các mạng bên ngoài. Thông thường, các máy chủ trong vùng mạng này chỉ cho phép truy cập từ vùng máy chủ nội bộ và vùng mạng quản trị.

Máy chủ cơ sở dữ liệu có thể được triển khai trên nhiều nền tảng khác nhau như: Oracle, MSSQL, MySQL...tùy thuộc vào ứng dụng quản lý văn bản được phát triển.

Các máy chủ trong vùng cơ sở dữ liệu được thiết lập hệ thống bảo vệ để kiểm soát truy nhập, phòng chống xâm nhập và tấn công mạng.

d) Thành phần kết nối tới Trục liên thông văn bản quốc gia (VBQG) bao gồm: Bộ kết nối (Local Adapter) và máy chủ bảo mật (Security Server). Căn cứ vào điều kiện thực tế của cơ quan, tổ chức mà thành phần này có thể chia thành hai máy chủ độc lập hoặc trên cùng một máy chủ.

Trường hợp bộ kết nối và máy chủ bảo mật nằm trên một máy chủ thì máy chủ đó phải có 02 giao diện. Một giao diện kết nối với máy chủ bảo mật của Trục liên thông VBQG và một giao diện kết nối với hệ thống QLVBĐH.

Trường hợp bộ kết nối và máy chủ bảo mật nằm trên 02 máy chủ khác nhau thì máy chủ bảo mật phải có 02 giao diện. Một giao diện kết nối với máy chủ bảo mật của Trục liên thông VBQG và một giao diện kết nối với hệ thống QLVBĐH và bộ kết nối.

Để giảm thiểu sự ảnh hưởng hoạt động giữa việc cung cấp dịch vụ quản lý văn bản và việc kết nối vào Trục liên thông VBQG, hệ thống cần thiết kế một vùng mạng riêng để kết nối giao diện bên trong của máy chủ bảo mật, máy chủ của hệ thống QLVBĐH và máy chủ của bộ kết nối.

2.2. Đối tượng kết nối và chia sẻ thông tin với hệ thống QLVBĐH

Về cơ bản, đối tượng kết nối và chia sẻ thông tin với hệ thống QLVBĐH bao gồm các đối tượng sau:

a) Người sử dụng truy cập vào hệ thống QLVBĐH để quản lý, vận hành và sử dụng dịch vụ của hệ thống thông qua mạng nội bộ hoặc qua kết nối mạng Internet.

b) Hệ thống Trục liên thông văn bản quốc gia để gửi nhận văn bản điện tử giữa các cơ quan, tổ chức nhà nước. Kết nối giữa hệ thống QLVBĐH với hệ thống Trục liên thông văn bản quốc gia sử dụng mạng TSLCD cấp I hoặc cấp II.

c) Hệ thống QLVBĐH của cơ quan, tổ chức khác trên địa bàn. Kết nối giữa hệ thống QLVBĐH với các hệ thống QLVBĐH của cơ quan, tổ chức khác sử dụng mạng thông tin diện rộng (mạng WAN) của địa phương đó.

2.3. Một số nguy cơ mất an toàn thông tin đối với hệ thống QLVBĐH

Nguy cơ mất an toàn đối với hệ thống QLVBĐH chủ yếu từ bên ngoài Internet qua giao diện mà hệ thống QLVBĐH cung cấp dịch vụ công cộng.

Ngoài ra, nguy cơ mất an toàn thông tin có thể xuất phát từ các thành phần khác bên trong hệ thống hoặc các hệ thống khác có kết nối trực tiếp với hệ thống QLVBĐH.

Về cơ bản, một số nguy cơ mất an toàn thông tin có thể xảy ra với hệ thống QLVBĐH bao gồm:

a) Tấn công từ chối dịch vụ làm mất tính khả dụng của hệ thống QLVBĐH trong việc cung cấp dịch vụ.

b) Tấn công khai thác điểm yếu, lỗ hổng chiếm quyền điều khiển, thay đổi giao diện… của máy chủ và ứng dụng triển khai hệ thống QLVBĐH.

c) Thực hiện các hình thức tấn công, nghe lén để đánh cắp thông tin, dữ liệu quan trọng, nhạy cảm.

d) Thực hiện tấn công mã độc vào các máy tính người sử dụng để lợi dụng chiếm quyền, nâng quyền kiểm soát đối với các hệ thống khác bên trong hệ thống.

đ) Tấn công vào nền tảng phần cứng (các thiết bị mạng và máy chủ) của hệ thống có tồn tại điểm yếu an toàn thông tin để chiếm quyền điều khiển hoặc tấn công từ chối dịch vụ.

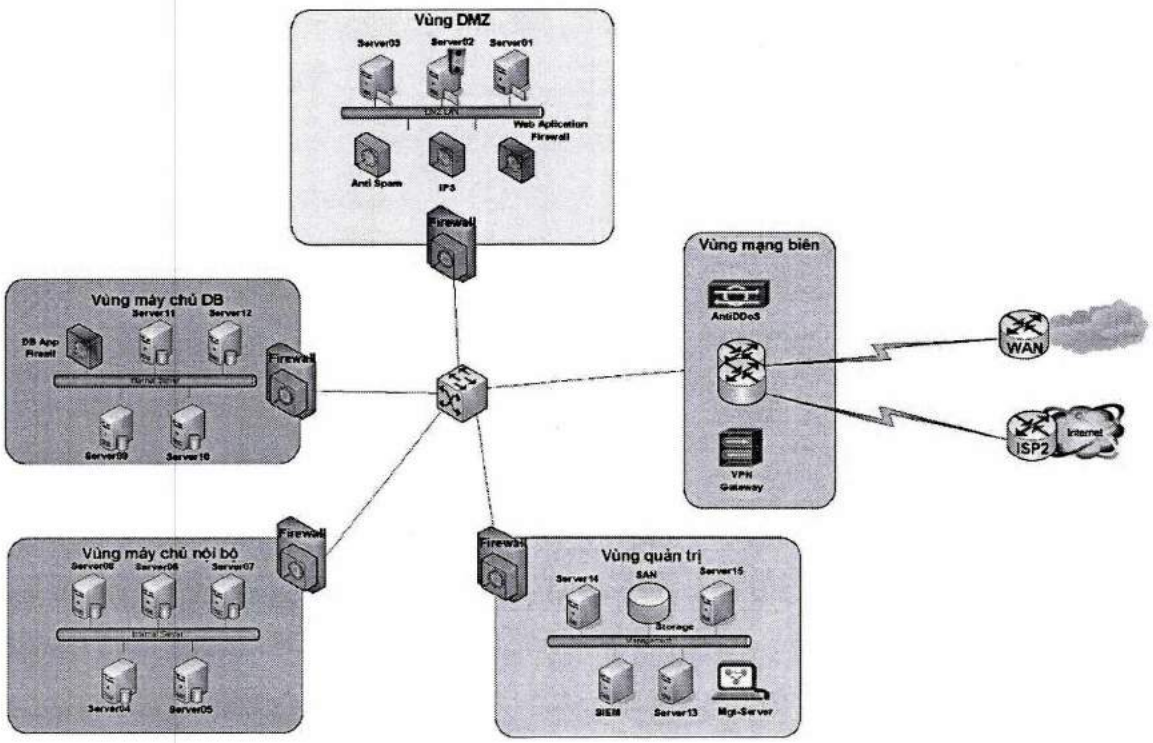
2.4. Thành phần cơ bản bảo đảm an toàn thông tin cho hệ thống QLVBĐH

Thành phần bảo đảm an toàn thông tin cho hệ thống QLVBĐH bao gồm các thành phần cơ bản sau:

a) Tường lửa: Sử dụng để quản lý truy cập giữa các mạng bên ngoài vào hệ thống mạng và giữa các vùng mạng trong hệ thống của cơ quan, tổ chức

Tùy thuộc vào năng lực thực tế của mỗi hệ thống thông tin, tường lửa có thể triển khai theo nhiều phương án khác nhau: (1) sử dụng thiết bị tường lửa tập trung và phân các vùng mạng bởi các giao diện của tường lửa; (2) chia thiết bị tường lửa vật lý và nhiều tường lửa logic và triển khai độc lập cho mỗi vùng mạng; (3) triển khai thiết bị tường lửa độc lập, chuyên dụng cho mỗi vùng mạng.

Trường hợp hệ thống QLVBĐH được xác định là hệ thống thông tin cấp độ 4 hoặc 5 thì hệ thống tường lửa trực tiếp quản lý truy cập và bảo vệ các vùng mạng DMZ, máy chủ nội bộ và cơ sở dữ liệu cần được triển khai dưới dạng thiết bị độc lập, chuyên dụng.



Hình 2. Mô hình hệ thống các thành phần bảo đảm an toàn thông tin

b) Phòng chống và phát hiện xâm nhập: Phát hiện xâm nhập và tấn công mạng từ các mạng bên ngoài vào hệ thống mạng và giữa các vùng mạng trong hệ thống của cơ quan, tổ chức

Tương tự như với cách triển khai đối với thiết bị tường lửa, thiết bị phòng chống xâm nhập cũng có thể triển khai theo 03 cách ở trên. Tuy nhiên, việc đặt thiết bị phòng chống xâm nhập sẽ làm giảm hiệu năng hoạt động của hệ thống mạng. Do đó, căn cứ vào khả năng xử lý của thiết bị phòng chống xâm nhập để triển khai vị trí phù hợp. Trường hợp thiết bị phòng chống xâm nhập có hiệu năng xử lý cao có thể triển khai tại vùng mạng biên để giám sát tổng thể lưu lượng mạng. Trường hợp năng lực xử lý hạn chế thì xem xét ưu tiên bảo vệ các vùng mạng như vùng DMZ, vùng máy chủ nội bộ, vùng máy chủ cơ sở dữ liệu.

c) Phòng chống tấn công từ chối dịch vụ: Bảo vệ, phòng chống tấn công từ chối dịch vụ (DoS/DDoS) vào hệ thống máy chủ dịch vụ của hệ thống

Thiết bị này được triển khai tại vùng mạng biên để phòng chống DoS/DDoS. Trên thực tế có nhiều thiết bị tường lửa có tích hợp chức năng phòng chống tấn công DoS/DDoS. Trường hợp hệ thống QLVBĐH được xác định là hệ thống thông tin cấp độ 4 hoặc 5 thì hệ thống phòng chống tấn công DoS/DDoS cần được triển khai dưới dạng thiết bị độc lập, chuyên dụng.

Một điểm cần chú ý là việc triển khai giải pháp phòng chống tấn công DoS/DDoS tại hệ thống thông tin cần bảo vệ chỉ hiệu quả khi lưu lượng tấn công nhỏ hơn băng thông kết nối mạng Internet của hệ thống (thường là các cuộc tấn công DoS/DDoS vào lớp ứng dụng). Do đó, để có phương án phòng chống tấn công DoS/DDoS tổng thể cần kết hợp giữa việc triển khai giải pháp tại hệ thống thông tin với thuê dịch vụ phòng chống tấn công DoS/DDoS chuyên nghiệp của doanh nghiệp.

d) Kết nối mạng riêng ảo VPN: Phục vụ việc thiết lập và quản lý kênh kết nối mạng an toàn, cho phép quản trị hệ thống từ xa.

Việc quản trị, cấu hình hệ thống hay quản lý dữ liệu cho hệ thống QLVBĐH khi thực hiện trực tiếp qua Internet là tiềm ẩn nhiều nguy cơ mất an toàn thông tin.

Để bảo đảm an toàn thông tin các máy chủ ứng dụng web và máy chủ cơ sở dữ liệu không cho phép kết nối trực tiếp từ mạng Internet mà thông thường phải thông qua một máy chủ quản trị trong vùng mạng quản trị. Do đó, cần thiết phải có thiết bị hoặc phương án kết nối VPN cho phép kết nối từ xa vào máy quản trị để từ máy đó thực hiện quản trị cấu hình và dữ liệu của hệ thống.

đ) Tường lửa chuyên dụng bảo vệ máy chủ cơ sở dữ liệu: Phục vụ việc quản lý và phòng chống tấn công vào máy chủ cơ sở dữ liệu thông qua các cấu truy vấn cơ sở dữ liệu độc hại để vượt quyền truy cập hoặc khai thác điểm yếu của hệ quản trị cơ sở dữ liệu.

Máy chủ cơ sở dữ liệu là máy chủ đặc biệt quan trọng của hệ thống. Bên cạnh các dạng tấn công mạng thông thường mà máy chủ này phải đối mặt thì còn có dạng tấn công riêng đối với ứng dụng cơ sở dữ liệu. Do đó, máy chủ này ngoài các giải pháp bảo vệ như tường lửa, phòng chống xâm nhập, mã độc thì cần triển khai thiết bị tường lửa chuyên dụng để phát hiện và phòng chống tấn công vào hệ thống cơ sở dữ liệu.

e) Hệ thống phòng chống phần mềm độc hại trên môi trường mạng: Phục vụ việc phát hiện và chặn lọc phần mềm độc hại trên môi trường mạng

Một trong các nguy cơ mất an toàn thông tin phổ biến là việc các máy tính/máy chủ bị lây nhiễm mã độc và bị điều khiển từ xa, bị lợi dụng để tấn công các thành phần bên trong của hệ thống thông tin.

Để triển khai phương án phòng chống phần mềm độc hại hiệu quả, giải pháp cần kết hợp giữa việc triển khai phần mềm phòng chống mã độc trên các máy với việc triển khai giải pháp trên môi trường mạng. Việc triển khai giải pháp trên môi trường mạng cho phép phát hiện các kết nối tới máy chủ C&C (Máy chủ điều khiển hoạt động của mạng máy tính ma – botnet, các máy tính bị nhiễm mã độc) và các hành vi mã độc khác tại các điểm có lưu lượng mạng tập trung.

Ngoài ra, một số thiết bị phần cứng cũng có khả năng bị nhiễm phần mềm độc hại và bị điều khiển từ xa. Trong khi các thiết bị này khó có thể cài đặt phần mềm phòng chống mã độc trên đó. Do đó, việc triển khai giải pháp phòng chống mã độc trong các trường hợp như vậy là rất cần thiết.

Phương án triển khai giải pháp này tương tự như với phương án triển khai hệ thống tường lửa và phát hiện xâm nhập. Căn cứ vào năng lực của thiết bị để lựa chọn vị trí triển khai giải pháp cho phù hợp. Trường hợp năng lực của thiết bị đủ lớn thì có thể triển khai thiết bị tại điểm giám sát tập trung toàn bộ lưu lượng mạng của hệ thống ra Internet. Trường hợp năng lực của hệ thống hạn chế thì ưu tiên triển khai giải pháp tại điểm tập trung lưu lượng mạng của người sử dụng ra Internet hoặc vùng mạng máy chủ mà có kết nối hoặc cho truy cập Internet.

g) Hệ thống giám sát hệ thống thông tin tập trung: Phục vụ giám sát, theo dõi thời gian thực hoạt động của hệ thống mạng nhằm bảo đảm tính khả dụng của hệ thống.

Hệ thống này nhận thông tin hoặc kết nối tới các thiết bị mạng, máy chủ và ứng dụng để thu thập các thông tin liên quan đến trạng thái, tài nguyên hệ thống, cho phép người quản trị theo dõi thời gian thực trạng thái của toàn hệ thống để đưa ra những hành động kiểm soát kịp thời. Hệ thống này được sử dụng để bảo đảm tính khả dụng của hệ thống trong quá trình vận hành, khai thác.

h) Hệ thống giám sát an toàn hệ thống thông tin tập trung: Phục vụ việc quản lý, phân tích, giám sát sự kiện an toàn thông tin tập trung để phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin.

Tương tự như đối với hệ thống giám sát hệ thống thông tin tập trung, hệ thống này cũng nhận thông tin hoặc kết nối tới các thiết bị mạng, máy chủ và ứng dụng để thu thập các thông tin liên quan đến sự kiện bảo mật, thay đổi chính sách hay truy nhập để phát hiện tấn công mạng và các hành vi dị thường. Hệ thống này cho phép người quản trị theo dõi, phát hiện và cảnh báo sớm các nguy cơ mất an toàn thông tin có thể xảy ra trên hệ thống.

i) Hệ thống lưu trữ tập trung: Phục vụ việc quản lý và sao lưu dự phòng tập trung.

Hệ thống này được sử dụng để lưu trữ dữ liệu của toàn bộ hệ thống bao gồm: các ảnh của hệ điều hành (nếu hệ thống triển khai trên nền ảo hóa), các tệp tin cấu hình hệ thống, cơ sở dữ liệu và các thông tin riêng của tổ chức, cá nhân nếu có.

Hệ thống này cho phép thiết lập chính sách mã hóa, quản lý truy cập, sao lưu dự phòng nhằm tăng cường khả năng bảo mật, tính khả dụng cho toàn bộ dữ liệu của hệ thống.

k) Hệ thống phòng chống mã độc trên máy chủ/máy trạm: Hệ thống phần mềm được cài đặt trên máy chủ/máy trạm và được quản lý bởi một hệ thống tập trung cho phép quản lý phát hiện và phòng chống mã độc trên các máy chủ/máy trạm.

l) Hệ thống phòng chống thất thoát dữ liệu: Phục vụ việc theo dõi, giám sát và phòng chống thất thoát thông tin/dữ liệu quan trọng qua môi trường mạng.

Hệ thống này được triển khai trên môi trường mạng hoặc dưới dạng phần mềm cài đặt trực tiếp trên máy chủ cho phép phát hiện nguy cơ lộ, lọt thông tin bí mật của hệ thống.

m) Hệ thống quản lý tài khoản đặc quyền: Phục vụ việc quản lý tài khoản và phân quyền truy nhập vào các thành phần của hệ thống tập trung.

Căn cứ vào việc xác định cấp độ an toàn thông tin cho hệ thống QLVBĐH để xác định thành phần bảo đảm an toàn cơ bản cho hệ thống này đáp ứng các yêu cầu an toàn tối thiểu theo quy định của pháp luật.

Chương III
YÊU CẦU AN TOÀN CƠ BẢN ĐỐI VỚI HỆ THỐNG QUẢN LÝ VĂN BẢN VÀ ĐIỀU HÀNH

Hệ thống QLVBĐH là hệ thống thông tin thành phần của hệ thống thông tin tổng thể. Do đó, căn cứ vào cấp độ của hệ thống QLVBĐH, phương án bảo đảm an toàn thông tin phải đáp ứng các yêu cầu an toàn tối thiểu theo quy định của pháp luật và các yêu cầu cụ thể tại hướng dẫn này.

3.1. Yêu cầu chung

Hệ thống QLVBĐH là một hệ thống thành phần trong hệ thống thông tin tổng thể. Để bảo đảm an toàn thông tin cho hệ thống này ngoài việc bảo đảm an toàn thông tin cho các thành phần trực tiếp phục vụ hoạt động của hệ thống này thì các thành phần khác liên quan đến hoạt động của hệ thống QLVBĐH trong hệ thống tổng thể cũng phải được bảo đảm an toàn. Do đó, yêu cầu an toàn thông tin tổng thể để bảo đảm an toàn thông tin cho hệ thống QLVBĐH bao gồm các yêu cầu dưới đây:

a) Yêu cầu an toàn thông tin đưa ra trong Tài liệu này bao gồm yêu cầu về quản lý và yêu cầu về kỹ thuật.

Yêu cầu về quản lý bao gồm các nhóm yêu cầu: (1) Thiết lập chính sách an toàn thông tin; (2) Tổ chức bảo đảm an toàn thông tin; (3) Bảo đảm nguồn nhân lực; (4) Quản lý thiết kế, xây dựng hệ thống; (5) Quản lý vận hành hệ thống.

Yêu cầu về kỹ thuật bao gồm: (1) Yêu cầu bảo đảm an toàn mạng; (2) Yêu cầu bảo đảm an toàn máy chủ; (3) Yêu cầu bảo đảm an toàn ứng dụng; (4) Yêu cầu bảo đảm an toàn dữ liệu.

b) Yêu cầu an toàn về quản lý đối với hệ thống QLVBĐH phải đáp ứng các yêu cầu quản lý chung đối với hệ thống thông tin với cấp độ tương ứng theo quy định tại điểm b, khoản 3, Điều 8 Thông tư số 03/2017/TT-BTTTT.

c) Yêu cầu an toàn về kỹ thuật đối với hệ thống QLVBĐH phải đáp ứng các yêu cầu quản lý chung đối với hệ thống thông tin với cấp độ tương ứng theo quy định tại điểm a, khoản 3, Điều 8 Thông tư số 03/2017/TT-BTTTT.

d) Cơ quan, tổ chức tham khảo Tiêu chuẩn quốc gia TCVN 11930:2017 và hướng dẫn dưới đây để xác định các yêu cầu an toàn cụ thể đối với hệ thống QLVBĐH.

3.2. Yêu cầu an toàn hạ tầng mạng

a) Phương án bảo đảm an toàn thông tin, thiết kế hệ thống và các thiết bị phục vụ hoạt động của hệ thống QLVBĐH cần được thiết kế, thiết lập, cấu hình bảo mật đáp ứng các yêu cầu tối thiểu sau:

- Các vùng mạng bao gồm: Có vùng mạng DMZ để đặt máy chủ đại diện; có vùng mạng máy chủ nội bộ để đặt máy chủ ứng dụng web; vùng máy chủ cơ sở dữ liệu để đặt máy chủ cơ sở dữ liệu; có vùng mạng quản trị để đặt máy quản trị các máy chủ và các thành phần khác bên trong hệ thống; có vùng mạng để kết nối hệ thống QLVBĐH với Trục liên thông văn bản quốc gia.

- Có hệ thống tường lửa tích hợp chức năng phát hiện xâm nhập và phòng chống mã độc trên môi trường mạng;

- Có tường lửa ứng dụng web;

- Phần mềm phòng chống mã độc trên các máy chủ.

b) Đối với hệ thống QLVBĐH được xác định là từ cấp độ 3 trở lên thì cần bổ sung các yêu cầu sau:

- Các thiết bị mạng chính được triển khai phương án cân bằng tải, dự phòng nóng;

- Có tường lửa cơ sở dữ liệu;

- Có hệ thống phòng chống tấn công từ chối dịch vụ;

- Có hệ thống giám sát an toàn hệ thống thông tin tập trung;

- Có hệ thống quản lý sao lưu dự phòng tập trung.

c) Ngoài ra yêu cầu an toàn hạ tầng mạng còn bao gồm các nhóm yêu cầu: (1) Thiết kế hệ thống; (2) Kiểm soát truy cập từ bên ngoài mạng; (3) Kiểm soát truy cập từ bên trong mạng; (4) Nhật ký hệ thống; (5) Phòng chống xâm nhập; (6) Phòng chống phần mềm độc hại trên môi trường mạng; (7) Bảo vệ thiết bị hệ thống.

Cơ quan, tổ chức có thể tham khảo tiêu chuẩn quốc gia TCVN 11930:2017 để lựa chọn, bổ sung thêm các yêu cầu an toàn cơ bản theo cấp độ của hệ thống QLVBĐH, như bảng dưới dây:

Bảng 1. Bảng tham chiếu yêu cầu an toàn cơ bản hạ tầng mạng theo Tiêu chuẩn TCVN 11930:2017

STT	Thiết kế hệ thống	Kiểm soát truy cập từ bên ngoài mạng	Kiểm soát truy cập từ bên trong mạng	Nhật ký hệ thống	Phòng chống xâm nhập	Phòng chống mã độc trên môi trường mạng	Bảo vệ thiết bị hệ thống
Cấp độ 1	5.2.1.1	5.2.1.2		5.2.1.3	5.2.1.4		5.2.1.5
Cấp độ 2	6.2.1.1	6.2.1.2	6.2.1.3	6.2.1.4	6.2.1.5		6.2.1.6
Cấp độ 3	7.2.1.1	7.2.1.2	7.2.1.3	7.2.1.4	7.2.1.5	7.2.1.6	7.2.1.7
Cấp độ 4	8.2.1.1	8.2.1.2	8.2.1.3	8.2.1.4	8.2.1.5	8.2.1.6	8.2.1.7
Cấp độ 5	9.2.1.1	9.2.1.2	9.2.1.3	9.2.1.4	9.2.1.5	9.2.1.6	9.2.1.7

3.3. Yêu cầu bảo đảm an toàn máy chủ

a) Hệ thống QLVBĐH cần được thiết kế thành các máy chủ độc lập bao gồm: Máy chủ đại diện, máy chủ ứng dụng web và máy chủ cơ sở dữ liệu. Tùy thuộc vào tài nguyên thực tế của hệ thống, các máy chủ này có thể triển khai trên các máy chủ vật lý độc lập hoặc máy chủ ảo để tận dụng và tối ưu tài nguyên hệ thống.

b) Các máy chủ phục vụ kết nối hệ thống QLVBĐH với Trục liên thông văn bản quốc gia bao gồm: Máy chủ bộ kết nối, máy chủ bảo mật. Tùy thuộc vào tài nguyên thực tế của hệ thống, các máy chủ này có thể triển khai trên các máy chủ vật lý độc lập hoặc máy chủ ảo để tận dụng và tối ưu tài nguyên hệ thống.

c) Việc bảo đảm an toàn thông tin cho máy chủ là bảo đảm an toàn thông tin cho hệ điều hành máy chủ và các ứng dụng, dịch vụ hệ thống và các thành phần khác liên quan. Do đó, sau khi hệ điều hành được cài đặt thì người quản trị cần thực hiện cấu hình, tối ưu, cứng hóa và triển khai các phương án bảo đảm an toàn thông tin khác để đáp ứng các yêu cầu cơ bản.

d) Yêu cầu cơ bản đối với máy chủ bao gồm: (1) Xác thực; (2) Kiểm soát truy cập; (3) Nhật ký hệ thống; (4) Phòng chống xâm nhập; (5) Phòng chống phần mềm độc hại; (6) Xử lý máy chủ khi chuyển giao.

Cơ quan tổ chức có thể tham khảo tiêu chuẩn quốc gia TCVN 11930:2017 để xác định các yêu cầu an toàn cơ bản theo cấp độ của hệ thống QLVBĐH, như bảng dưới dây:

Bảng 2. Bảng tham chiếu yêu cầu an toàn cơ bản cho máy chủ theo Tiêu chuẩn TCVN 11930:2017

STT	Xác thực	Kiểm soát truy cập	Nhật ký hệ thống	Phòng chống xâm nhập	Phòng chống phần mềm độc hại	Xử lý máy chủ khi chuyển giao
Cấp độ 1	5.2.2.1	5.2.2.2	5.2.2.3	5.2.2.4	5.2.2.5	
Cấp độ 2	6.2.2.1	6.2.2.2	6.2.2.3	6.2.2.4	6.2.2.5	
Cấp độ 3	7.2.2.1	7.2.2.2	7.2.2.3	7.2.2.4	7.2.2.5	7.2.2.6
Cấp độ 4	8.2.2.1	8.2.2.2	8.2.2.3	8.2.2.4	8.2.2.5	8.2.2.6
Cấp độ 5	9.2.2.1	9.2.2.2	9.2.2.3	9.2.2.4	9.2.2.5	9.2.2.6

đ) Cơ quan, tổ chức có thể tham khảo Phụ lục hướng dẫn thiết lập cấp hình bảo mật an toàn cho máy chủ Windows và Linux.

3.4. Yêu cầu bảo đảm an toàn ứng dụng

a) Ứng dụng phục vụ hoạt động của hệ thống QLVBĐH bao gồm các ứng dụng thành phần khác nhau bao gồm: Ứng dụng máy chủ web (IIS, Apache, Nginx, Tomcat…), Hệ quản trị cơ sở dữ liệu (MSSQL, MySQL, Oracle,…) và các ứng dụng nghiệp vụ cụ thể được triển khai trên các nền tảng khác nhau như ASP, PHP, JSP…

Việc bảo đảm an toàn thông tin cho hệ thống QLVBĐH thì cần bảo đảm an toàn thông tin cho các thành phần phục vụ hoạt động của các hệ thống này.

b) Yêu cầu cơ bản đối với ứng dụng bao gồm: (1) Xác thực; (2) Kiểm soát truy cập; (3) Nhật ký hệ thống; (4) Bảo mật thông tin liên lạc; (5) Chống chối bỏ; (6) An toàn ứng dụng và mã nguồn.

Cơ quan tổ chức có thể tham khảo tiêu chuẩn quốc gia TCVN 11930:2017 để xác định các yêu cầu an toàn cơ bản theo cấp độ của hệ thống QLVBĐH, như bảng dưới dây:

Bảng 3. Bảng tham chiếu yêu cầu an toàn cơ bản cho ứng dụng theo Tiêu chuẩn TCVN 11930:2017

STT	Xác thực	Kiểm soát truy cập	Nhật ký hệ thống	Bảo mật thông tin liên lạc	Chống chối bỏ	An toàn ứng dụng và mã nguồn
Cấp độ 1	5.2.3.1	5.2.3.2	5.2.3.3			
Cấp độ 2	6.2.3.1	6.2.3.2	6.2.3.3			6.2.3.4
Cấp độ 3	7.2.3.1	7.2.3.2	7.2.3.3	7.2.3.4	7.2.3.5	7.2.3.6
Cấp độ 4	8.2.3.1	8.2.3.2	8.2.3.3	8.2.3.4	8.2.3.5	8.2.3.6
Cấp độ 5	9.2.3.1	9.2.3.2	9.2.3.3	9.2.3.4	9.2.3.5	9.2.3.6

3.5. Yêu cầu bảo đảm an toàn dữ liệu

a) Dữ liệu cần được bảo vệ bao gồm 02 nhóm dữ liệu: (1) Nhóm dữ liệu của hệ thống và (2) Dữ liệu nghiệp vụ.

Nhóm dữ liệu hệ thống là những dữ liệu phục vụ hoạt động của hệ thống hoặc được tạo ra trong quá trình quản lý vận hành như: tệp tin cấu hình hệ thống, ảnh hệ điều hành, nhật ký hệ thống…

Nhóm dữ liệu nghiệp vụ là những dữ liệu của cơ quan, tổ chức tạo ra như: thông tin riêng, thông tin cá nhân và có thể bao gồm thông tin bí mật nhà nước.

b) Để bảo đảm an toàn dữ liệu cho hệ thống QLVBĐH, hệ thống lưu trữ tập trung cần được triển khai để quản lý và lưu trữ tập trung các dữ liệu hệ thống và dữ liệu nghiệp vụ.

c) Các máy chủ cần được triển khai trên nền tảng ảo hóa để thuận tiện trong việc sao lưu, dự phòng và khôi phục sau sự cố.

d) Yêu cầu cơ bản đối với dữ liệu bao gồm: (1) Nguyên vẹn dữ liệu; (2) Bảo mật dữ liệu; (3) Sao lưu dự phòng.

Cơ quan tổ chức có thể tham khảo tiêu chuẩn quốc gia TCVN 11930:2017 để xác định các yêu cầu an toàn cơ bản theo cấp độ của hệ thống QLVBĐH, như bảng dưới dây:

Bảng 4. Bảng tham chiếu yêu cầu an toàn cơ bản cho dữ liệu theo Tiêu chuẩn TCVN 11930:2017

STT	Nguyên vẹn dữ liệu	Bảo mật dữ liệu	Sao lưu dự phòng
Cấp độ 1	5.2.4.1		
Cấp độ 2	6.2.4.1		6.2.4.2
Cấp độ 3	7.2.4.1	7.2.4.2	7.2.4.3
Cấp độ 4	8.2.4.1	8.2.4.2	8.2.4.3
Cấp độ 5	9.2.4.1	9.2.4.2	9.2.4.3

Chương IV
HƯỚNG DẪN ĐẢM BẢO AN TOÀN THÔNG TIN CHO HỆ THỐNG QUẢN LÝ VĂN BẢN VÀ ĐIỀU HÀNH

4.1. Trách nhiệm bảo đảm an toàn thông tin cho hệ thống QLVBĐH

a) Chủ quản hệ thống thông tin, đơn vị vận hành có trách nhiệm: (1) Trách nhiệm đối với những sự cố mất an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý nói chung và hệ thống QLVBĐH nói riêng; (2) Trách nhiệm đối với các sự cố mất an toàn thông tin xảy ra xuất phát từ hệ thống của mình tới các hệ thống thông tin của cơ quan, tổ chức khác; (3) Trách nhiệm phối hợp với cơ quan, tổ chức có thẩm quyền trong công tác bảo đảm an toàn thông tin cho hệ thống thông tin thuộc phạm vi quản lý nói chung và hệ thống QLVBĐH nói riêng.

b) Trách nhiệm cụ thể của chủ quản hệ thống thông tin liên quan đến công tác bảo đảm an toàn thông tin được quy định theo quy định tại Điều 20 Nghị định số 85/2016/NĐ-CP.

c) Trách nhiệm cụ thể của đơn vị vận hành liên quan đến công tác bảo đảm an toàn thông tin được quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP.

4.2. Phương án triển khai bảo đảm an toàn thông tin cho hệ thống QLVBĐH

a) Chủ quản hệ thống thông tin thành lập hoặc chỉ định đơn vị chuyên trách về an toàn thông tin mạng để làm công tác tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, xử lý khắc phục sự cố, giám sát công tác bảo đảm an toàn, an ninh mạng theo quy định của pháp luật.

b) Mỗi hệ thống thông tin cần chỉ định bộ phận thực thi nhiệm vụ giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin theo các phương án sau: Tự thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ

thống thông tin thuộc quyền quản lý hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực để thực hiện.

c) Mỗi hệ thống thông tin cần chỉ định bộ phận thực thi nhiệm vụ kiểm tra, đánh giá an toàn thông tin mạng theo các phương án sau: Lựa chọn tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin thuộc quyền quản lý hoặc đột xuất khi có yêu cầu theo quy định của pháp luật.

d) Cơ quan, tổ chức có thể căn cứ vào quy định liên quan tại Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng để có sở cứ lập dự toán triển khai các phương án bảo đảm an toàn thông tin cho hệ thống QLVBĐH.

4.3. Triển khai giám sát an toàn thông tin

Việc triển khai giám sát an toàn thông tin nhằm bảo đảm tính khả dụng của hệ thống và khả năng phát hiện sớm nguy cơ mất an toàn thông tin có thể xảy ra đối với hệ thống. Cơ quan, tổ chức có thể triển khai giám sát an toàn thông tin theo hướng dẫn sau:

a) Thực hiện phương án giám sát: (1) Giám sát hoạt động của hệ thống để có được thông tin trạng thái hoạt động của hệ thống về hiệu năng, trạng thái tăng/giảm (Up/Down), băng thông kết nối; (2) Giám sát an toàn thông tin để phát hiện và cảnh báo sớm tấn công mạng và các nguy cơ mất an toàn thông tin.

b) Xác định đối tượng giám sát: Là các thiết bị mạng, lưu lượng mạng, máy chủ, ứng dụng, dịch vụ có trong hệ thống. Đối với hệ thống QLVBĐH thì đối tượng giám sát tối thiểu bao gồm: (1) Máy chủ đại diện, máy chủ ứng dụng web, máy chủ cơ sở dữ liệu, bộ kết nối, máy chủ bảo mật; (2) Các thiết bị mạng, thiết bị bảo mật trực tiếp phục vụ hoạt động của hệ thống QLVBĐH.

c) Xây dựng các quy định, quy trình quản lý hoạt động giám sát, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát; Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát.

d) Cơ quan, tổ chức tham khảo văn bản "Hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước " do Bộ Thông tin và Truyền thông công bố để có phương án triển khai giám sát an toàn toàn thông tin tổng thể.

4.4. Kiểm tra, đánh giá an toàn thông tin

Việc kiểm tra đánh giá an toàn thông tin nhằm rà soát, kiểm tra các nguy cơ mất an toàn thông tin thông qua việc khai thác điểm yếu, lỗ hổng bảo mật trên hệ thống. Cơ quan, tổ chức có thể triển khai kiểm tra, đánh giá an toàn thông tin theo hướng dẫn sau:

a) Xác định đối tượng được kiểm tra, đánh giá an toàn thông tin tối thiểu bao gồm: (1) Hạ tầng mạng, (2) Hệ thống máy chủ, (3) Ứng dụng dịch vụ, (4) Hệ thống cơ sở dữ liệu.

b) Hệ thống QLVBĐH cần thực hiện kiểm tra đánh giá tối thiểu các đối tượng sau: Máy chủ đại diện, máy chủ ứng dụng web, máy chủ cơ sở dữ liệu, bộ kết nối, máy chủ bảo mật; Các thiết bị mạng, thiết bị bảo mật trực tiếp phục vụ hoạt động của hệ thống QLVBĐH.

c) Nội dung kiểm tra, đánh giá an toàn thông tin bao gồm: Đối với hạ tầng mạng cần kiểm tra việc thiết kế hệ thống, thiết lập cấu hình trên các thiết bị và có điểm yếu an toàn thông tin trên các thiết bị mạng hay không. Đối với máy chủ cần kiểm tra việc thiết lập cấu hình bảo mật và các điểm yếu an toàn thông tin trên hệ điều hành máy chủ và các dịch vụ hệ thống chạy cùng hệ điều hành. Đối với ứng dụng cần kiểm tra việc thiết lập cấu hình bảo mật và các điểm yếu an toàn thông tin cho ứng dụng và hệ thống cơ sở dữ liệu.

d) Hệ thống QLVBĐH cấp độ 3 trở lên thì các thành phần của hệ thống yêu cầu thực hiện kiểm tra đánh giá an toàn thông tin trước khi đưa vào sử dụng, các hệ thống ở cấp độ khác khuyến nghị thực hiện để tăng cường bảo đảm an toàn thông tin. Hoạt động kiểm tra, đánh giá phải được thực hiện thường xuyên, định kỳ theo quy định của pháp luật.

đ) Cơ quan, tổ chức tham khảo văn bản "Hướng dẫn triển khai hoạt động kiểm tra, đánh giá an toàn thông tin trong cơ quan, tổ chức nhà nước " do Bộ Thông tin và Truyền thông công bố để có phương án kiểm tra, đánh giá an toàn toàn thông tin tổng thể.

4.5. Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng

Việc xây dựng phương án ứng cứu sự cố an toàn thông tin mạng giúp cơ quan, tổ chức chủ động hơn trong việc xử lý sự cố và khôi phục hệ thống sau sự cố. Cơ quan, tổ chức có thể triển khai phương án ứng cứu sự cố an toàn thông tin mạng theo hướng dẫn sau:

a) Xây dựng phương án quản lý sự cố an toàn thông tin có thể xảy ra đối với hệ thống QLVBĐH, tối thiểu bao gồm các nội dung: Đưa ra chính sách/quy trình

thực hiện quản lý sự cố an toàn thông tin của tổ chức, bao gồm: Phân nhóm sự cố an toàn thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch ứng phó sự cố an toàn thông tin; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường; Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

b) Thực hiện phân nhóm sự cố an toàn thông tin mạng; Xây dựng hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; và thực hiện các trách nhiệm liên quan được quy định tại Quyết định số 05/2017/NĐ-CP ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

c) Định kỳ hàng năm tổ chức diễn tập bảo đảm an toàn thông tin và thực hành phương án xử lý sự cố an toàn thông tin có thể xảy ra đối với hệ thống QLVBĐH.

PHỤ LỤC:
HƯỚNG DẪN CẤU HÌNH BẢO MẬT CHO MÁY CHỦ

Hướng dẫn cấu hình bảo mật cho máy chủ dưới đây mang tính chất tham khảo. Các giá trị được thiết lập trong hướng dẫn này được thay đổi cho phù hợp với yêu cầu của từng hệ thống cụ thể.

Việc thực hiện cấu hình bảo mật cho máy chủ cần thực hiện trước khi đưa máy chủ vào sử dụng. Không thực hiện cấu hình máy chủ khi máy chủ đang cung cấp dịch vụ để không ảnh hưởng đến việc cung cấp dịch vụ của máy chủ.

Việc thực hiện cấu hình bảo mật cho máy chủ như hướng dẫn dưới đây.

1. Hướng dẫn thiết lập cấp hình bảo mật an toàn cho máy chủ Windows

1.1. Hardening Window Server

1.1.1. Partitioning

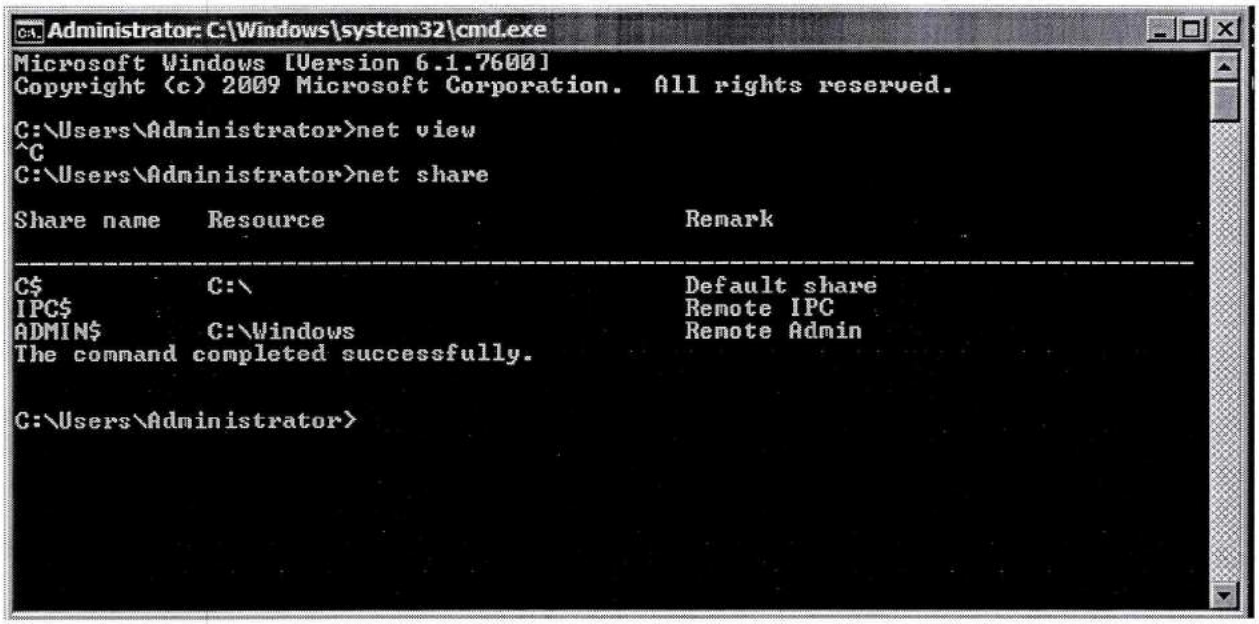
Partion	Kích thước khuyến nghị	Định dạng	Lưu ý
C:\	100GB	NTFS	Chứa hệ điều hành, Profiles và các ứng dụng cài đặt
D:\	Kích cỡ còn lại của ổ đĩa	NTFS	Chứa dữ liệu ứng dụng, dữ liệu khác

1.1.2. Vô hiệu hóa các share không cần thiết

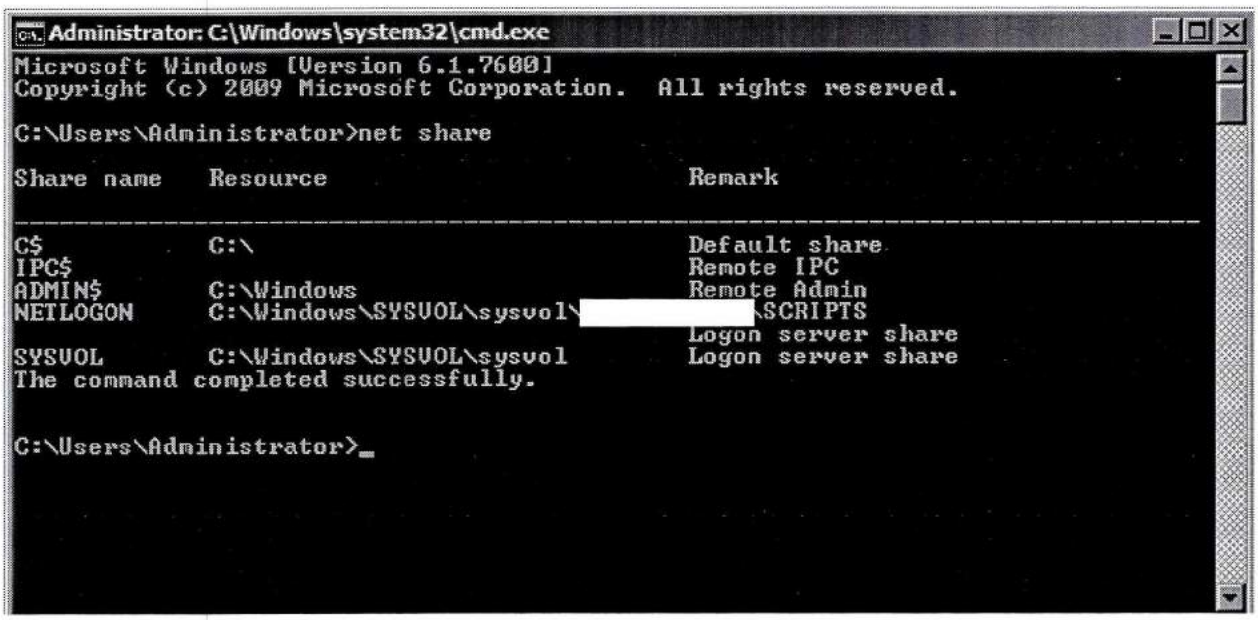
Các thư mục share hệ thống và share phục vụ mục đích quản trị yêu cầu share ẩn (Có dấu $ đằng sau tên thư mục share).

Sử dụng Command line : Net share để hiển thị các thư mục chia sẻ trên máy chủ.

Danh mục chia sẻ độc lập đối với máy chủ độc lập (Standalone) sau:



Danh mục các thư mục chia se đối với máy chủ Domain (Domain Controller) sau:

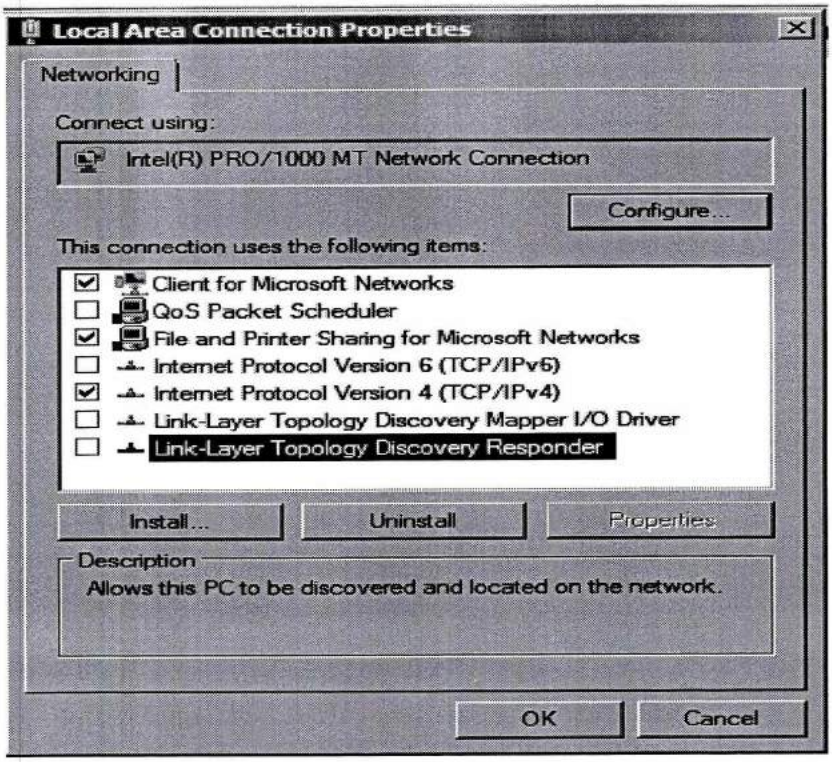


1.2. Cấu hình mạng

1.2.1. Đối với máy chủ Domain Controller và máy chủ chia sẻ file

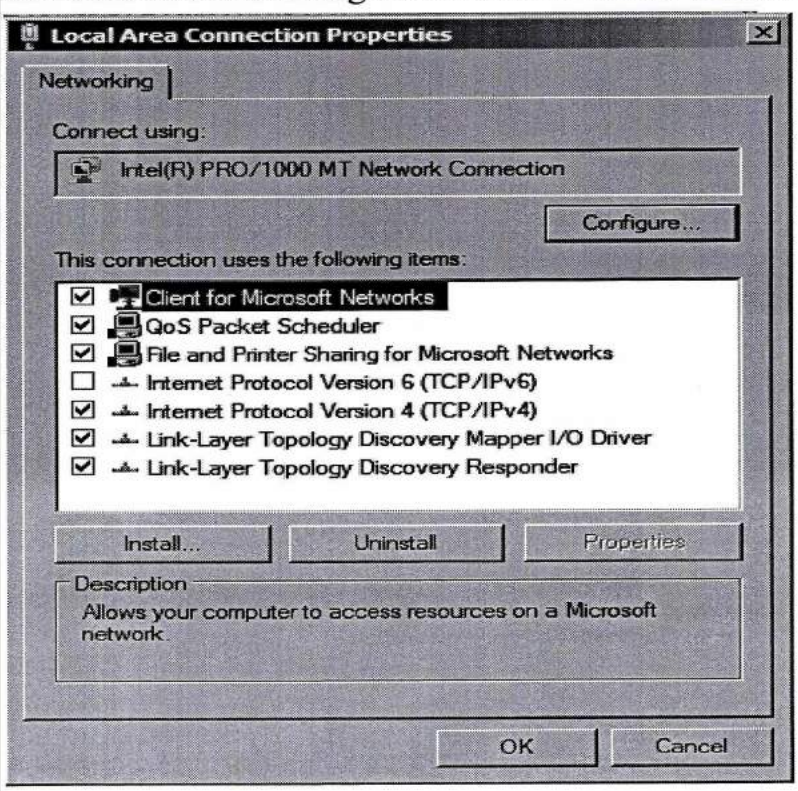
Chỉ cho phép các tính năng:

- Client for Microsoft Networks;
- File and Printer Sharing of Microsoft Networks;
- Internet Protocol Version 4 (TCP/IP).



1.2.2. Đối với máy chủ Standalone

Trong phần cấu hình Networking bỏ Internet Protocol Version 6 (TCP/IP).



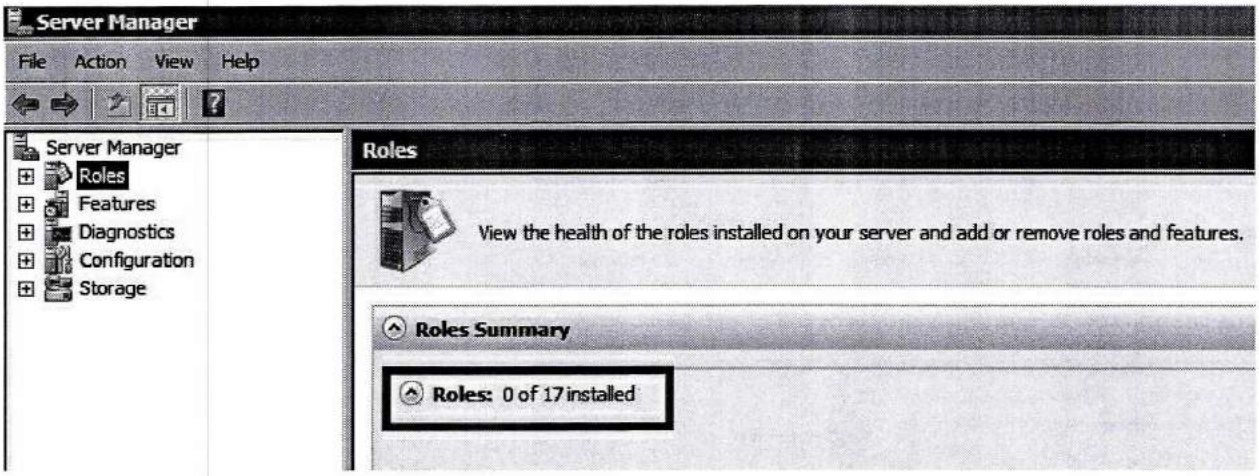
1.3. Xóa bỏ các role không cần thiết

Mảy chủ chạy dịch vụ gì thì cài Role dịch vụ đó, không cài thừa – Roles chuẩn của máy chủ là:

Không có roles nào được kích hoạt

Sử dụng hộp thoại Run gõ lệnh : **servermanager.msc.**

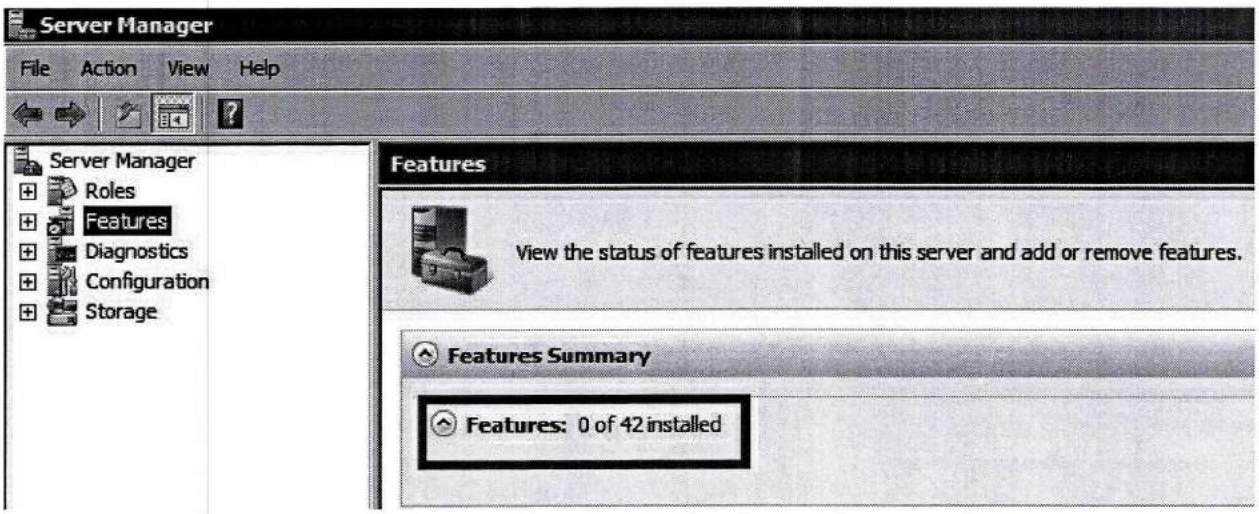
Sau đó chon **Roles** để xem danh sách các role đã được cài đặt.



1.4. Xóa bỏ các Features không cần thiết

Máy chủ cần Features gì thì chỉ cài đặt Features đó không cài thừa – Features chuẩn của máy chủ là:

Không có Features nào được kích hoạt



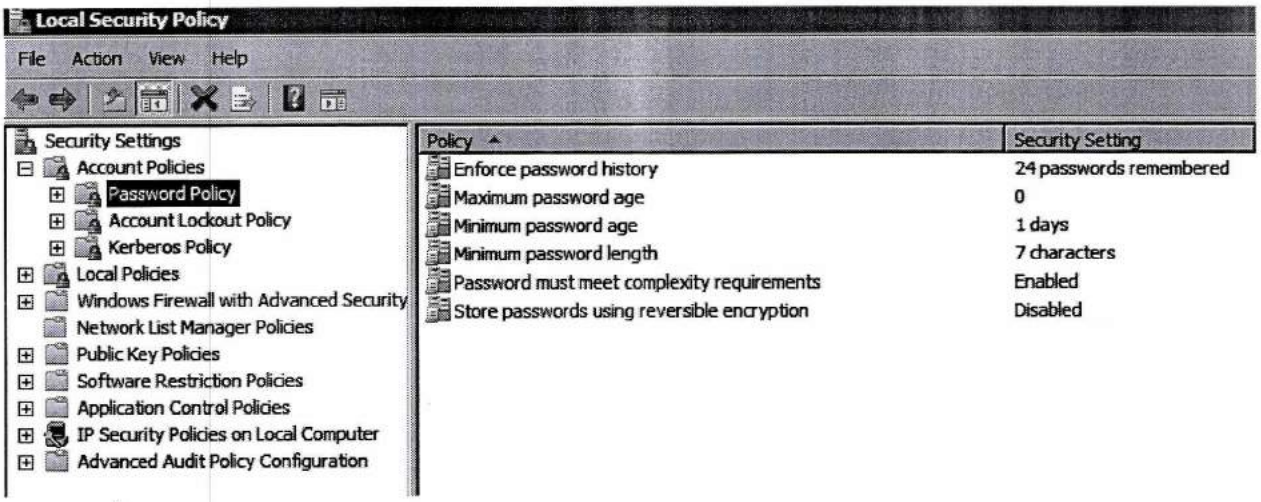
1.5. Chính sách tài khoản và mật khẩu

1.5.1. Cấu hình chính sách mật khẩu:

Đối với máy chủ Standalone cấu hình ở " Local Policy" với máy chủ Domain cấu hình ở " Domain Security Policy" .

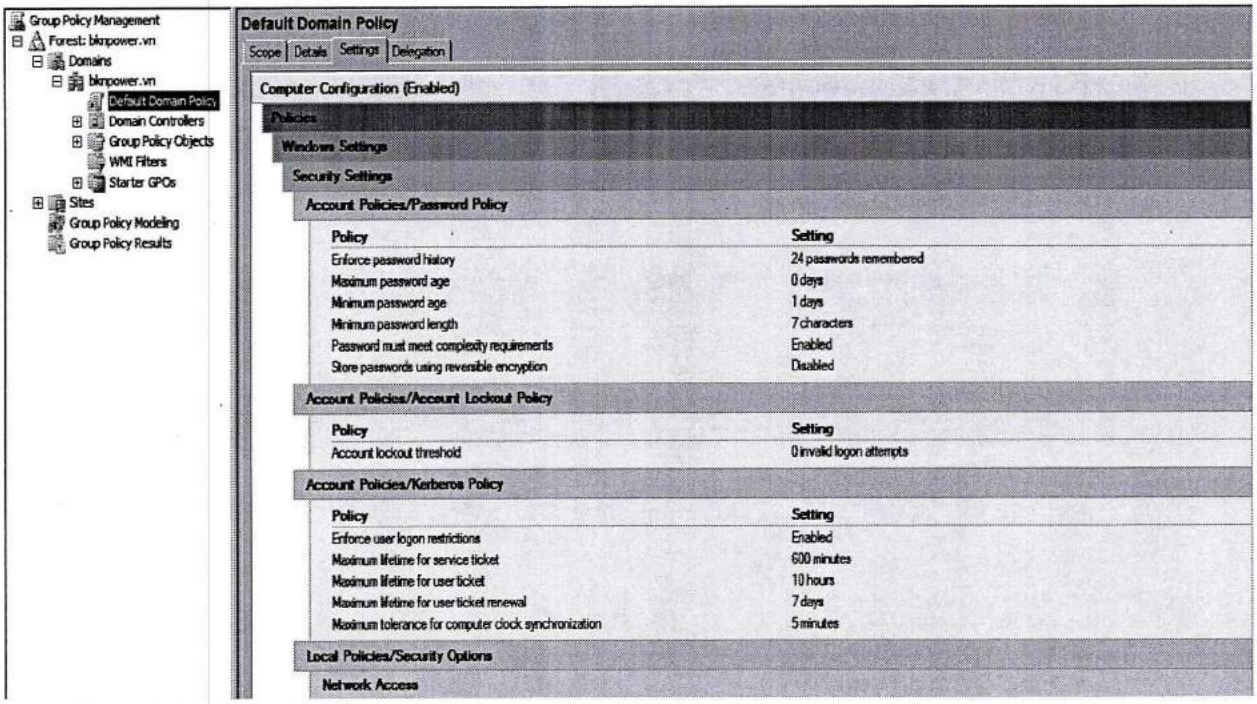
Để truy cập Local Policy sử dụng lệnh : **secpol.msc.**

Rồi thay đổi các thông tin.

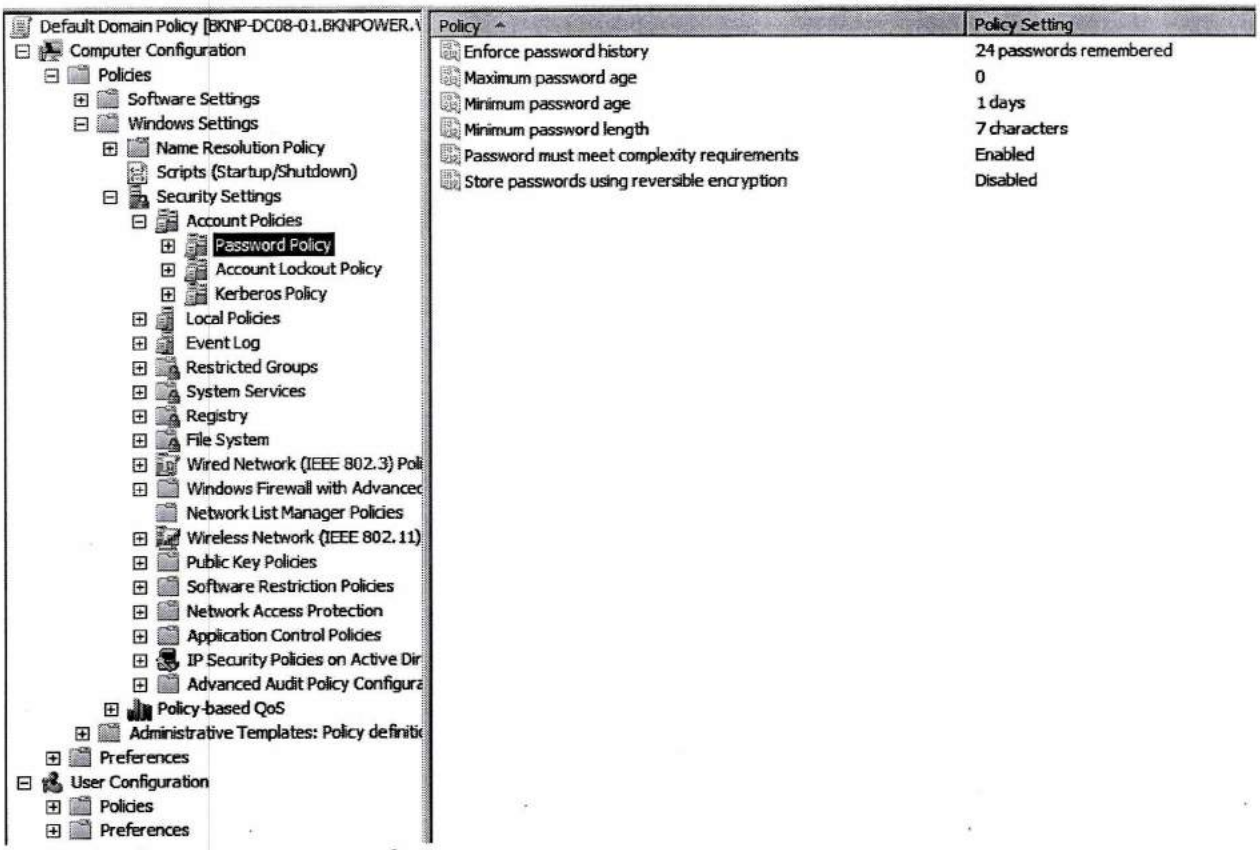


Để truy cập Domain Security Policy sử dụng lệnh: **gpmc.msc.**

Sau đó chọn **Default Domain Policy -> Chọn Tab Settings** để view setting.



Sau đó Click chuột phải vào **Default Domain policy** chọn **Edit**



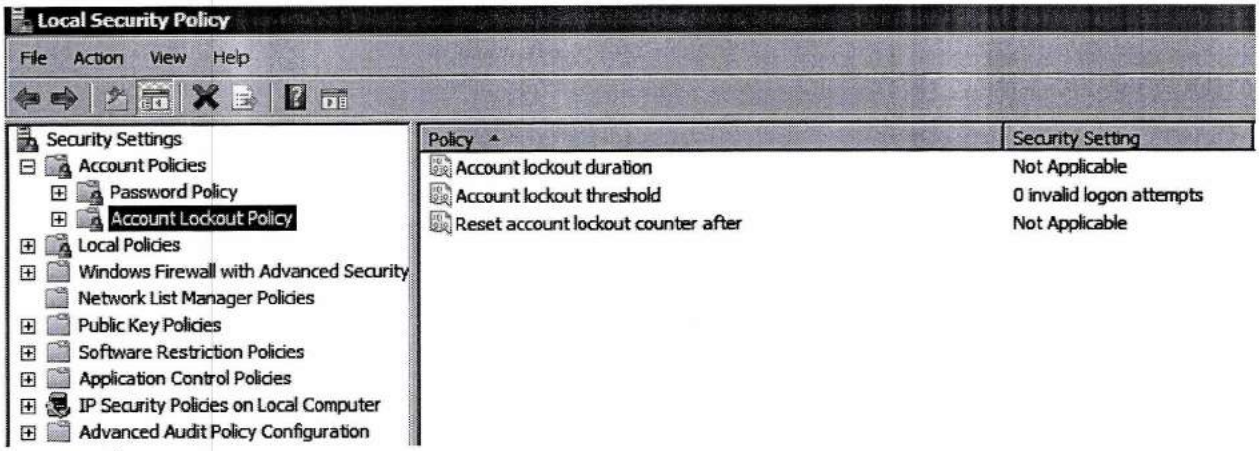
Thiết lập các tham số theo chính sách an toàn thông tin

Policy	Setting
Enforce password history	4 password remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

1.5.2. Cấu hình chính sách tài khoản

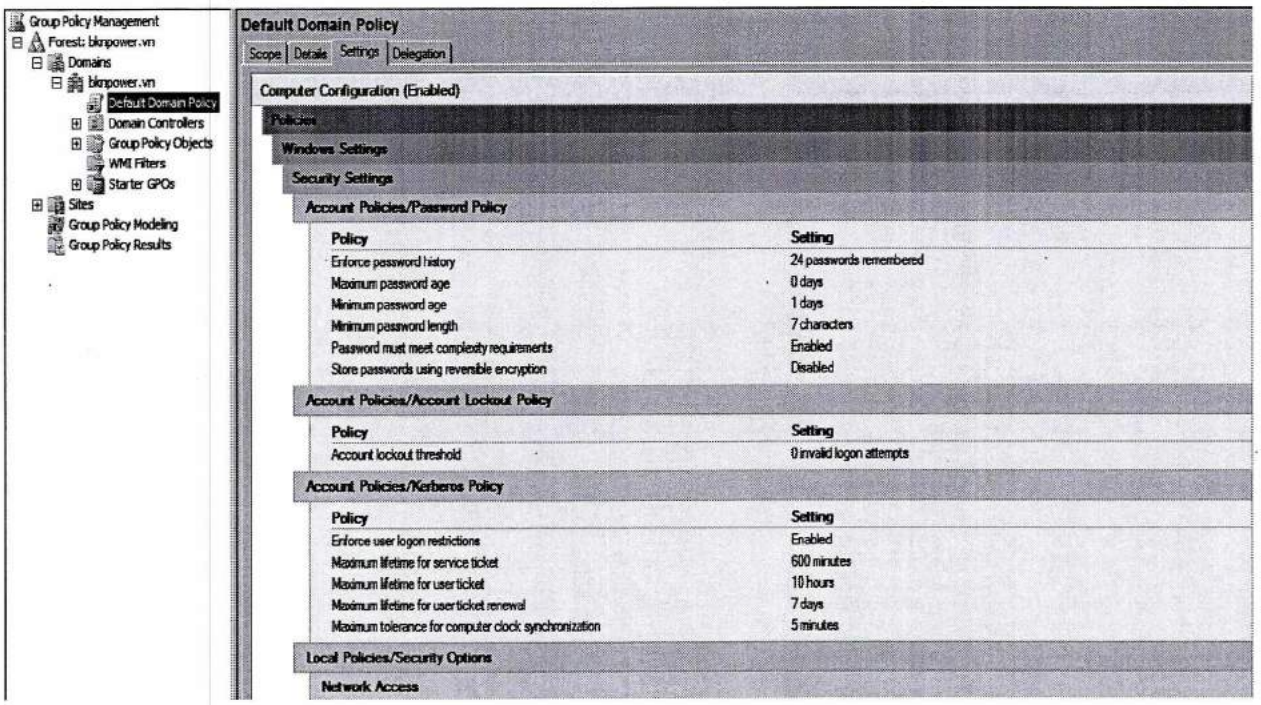
Đối với máy chủ standalone cấu hình ở " Local Policy" với máy chủ Domain cấu hình ở " Domain Security Policy"

Đối với Local Policy cũng sử dụng lệnh : **secpol.msc**

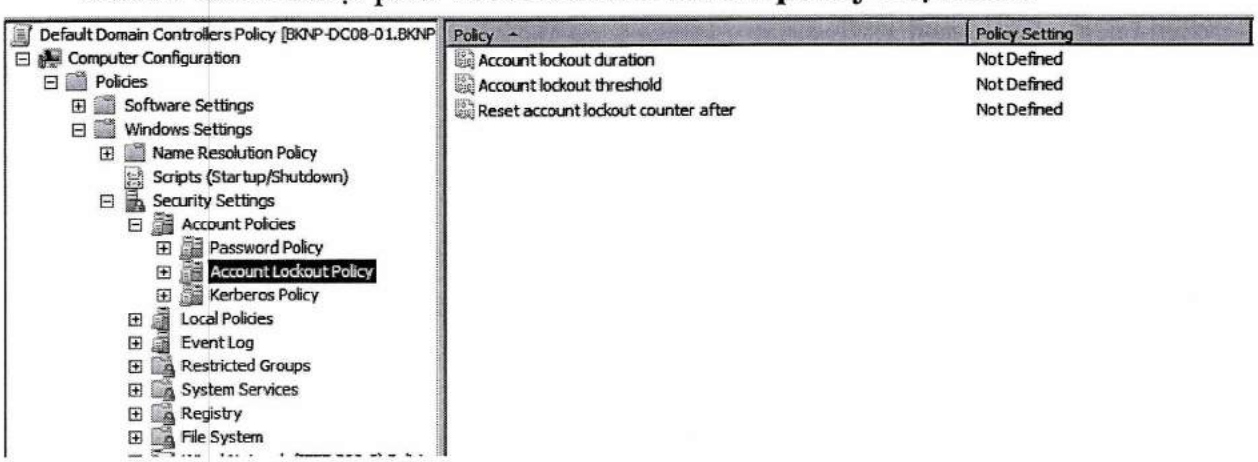


Để truy cập Domain Security Policy sử dụng lệnh: **gpmc.msc**

Sau đó chọn **Default Domain Policy -> Chọn Tab Settings** để view setting



Sau đó Click chuột phải vào **Default Domain policy** chọn **Edit**

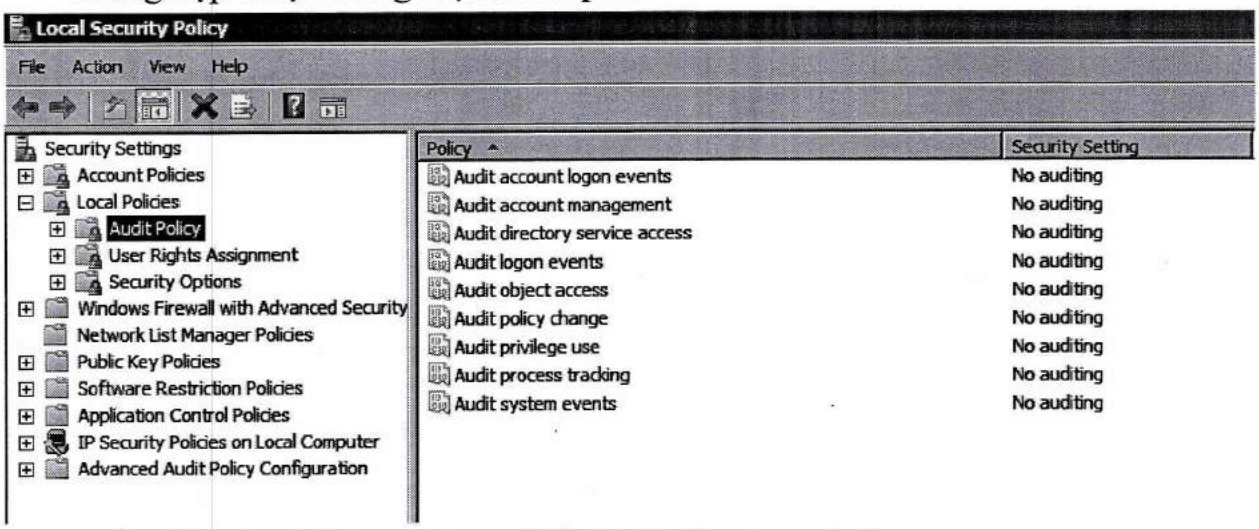


Thiết lập các thông số theo chính sách an toàn thông tin

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	6 invalid logon attempts
Reset account lockout counter after	30 minutes

1.6. Chính sách kiểm soát (Audit policy)

Dùng hộp thoại Run gõ lệnh : **secpol.msc**

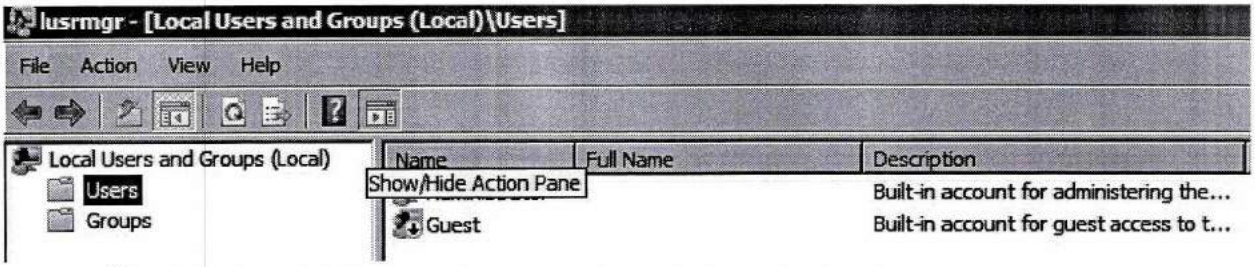


Đối với máy chủ Standalone thiết lập Policy Local như sau

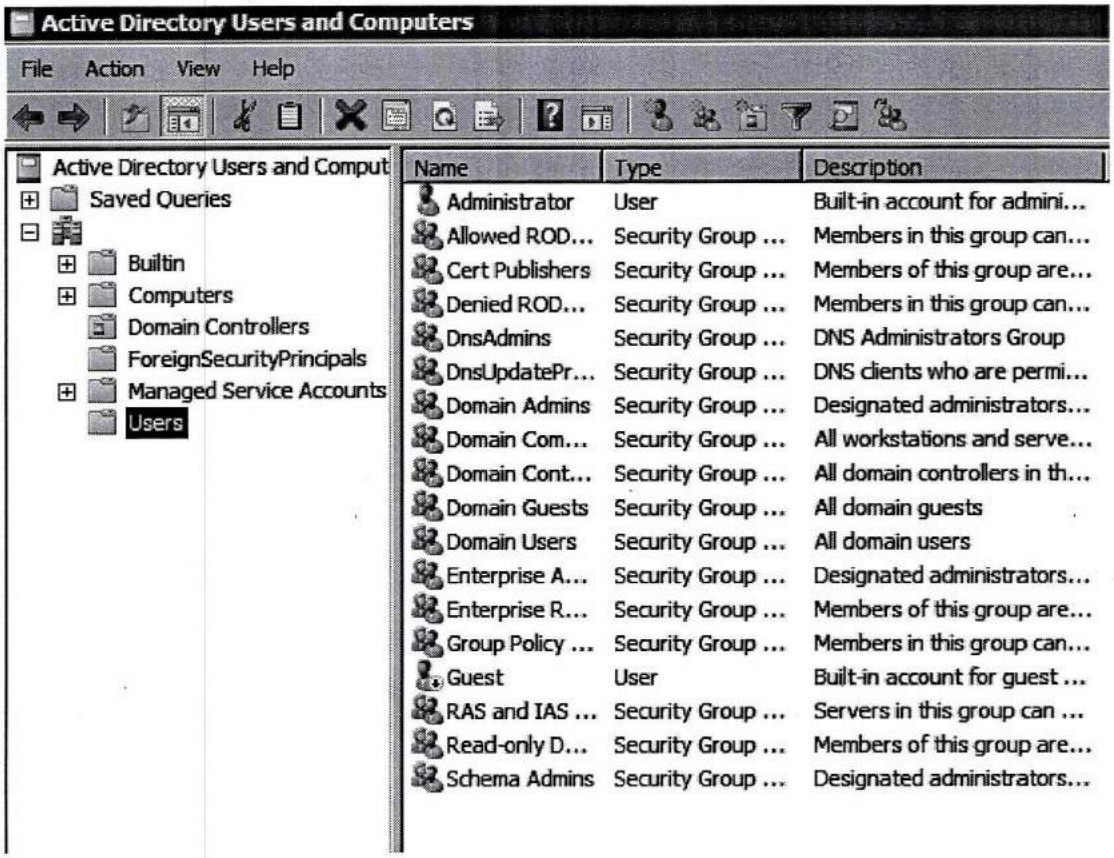
Policy	Recommended Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

1.7. Disable hoặc xóa các tài khoản không cần thiết

Đối với máy chủ Standalone thì thực hiện với tài khoản Local sử dụng lệnh : **lusrmgr.msc**



Đối với máy chủ là domain controller sử dụng lệnh **dsa.msc**

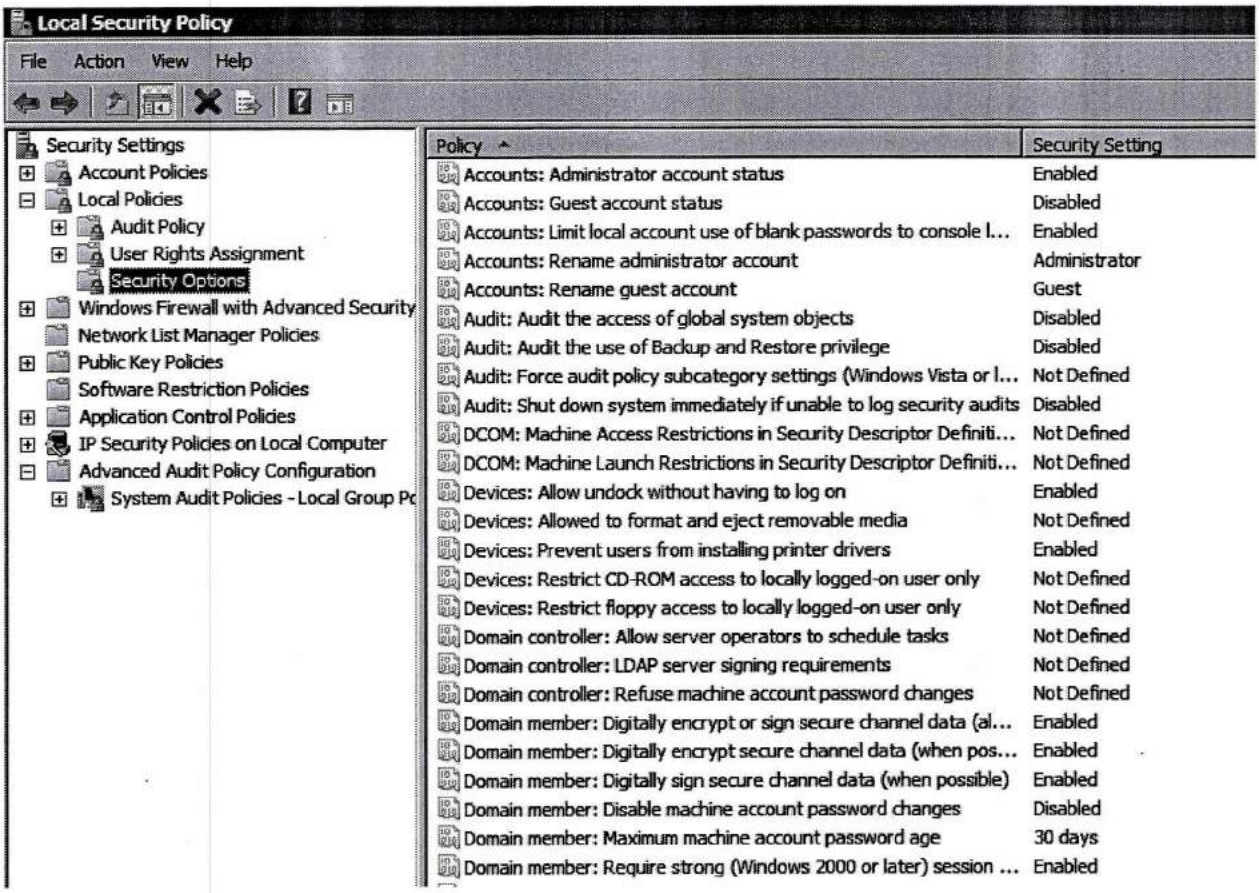


- Disable tài khoản Guest và tài khoản Help Assistant
- Rename tài khoản Administrator thành "adm"
- Xóa các tài khoản "test" trên hệ thống
- Xóa các tài khoản đã nghỉ việc
- Disable các tài khoản quá 90 days không truy cập hệ thống
- Tài khoản truy cập vào hệ điều hành phải là tài khoản định danh của mỗi cá nhân, không được sử dụng chung một tài khoản admin của hệ điều hành

1.8. Thiết lập bảo mật (Security Options)

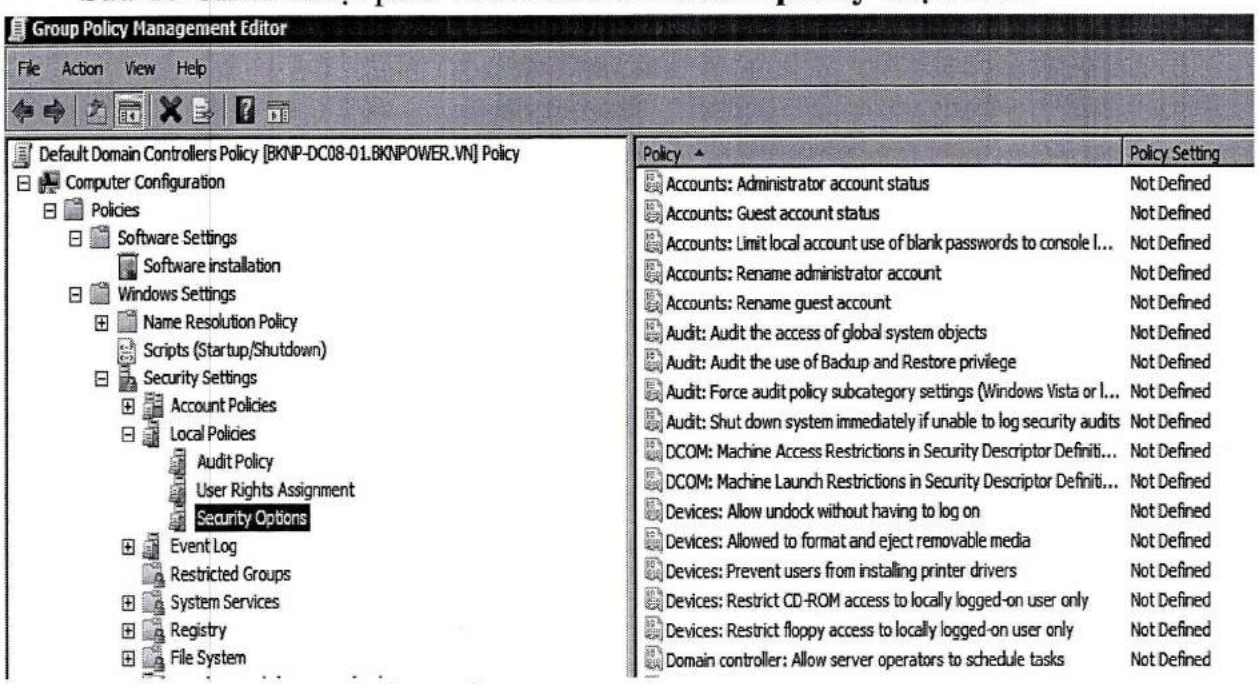
Đối với máy chủ Standalone thực hiện ở Local Policy

Dùng lệnh: **secpol.msc**



Đối với máy chủ là domain controller sử dụng lệnh **: gpmc.msc**

Sau đó Click chuột phải vào **Default Domain policy** chọn **Edit**



Thiết lập các tham số chuẩn như sau

No.	Policy	Recommended Setting

Major Security Settings		
1	Network Access: Allow Anonymous SID/Name Translation:	Disabled
2	Network Access: Do not allow Anonymous Enumeration of SAM Accounts	Disabled
3	Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares	Disabled
Minor Security Settings		
1	Accounts: Administrator Account Status	Not Defined
2	Accounts: Guest Account Status	Disabled
4	Accounts: Limit local account use of blank passwords to console logon only	Enabled
5	Accounts: Rename Administrator Account	Non-Standard
6	Accounts: Rename Guest Account	Non-Standard
7	Audit: Audit the access of global system objects	<Not Defined>
8	Audit: Audit the use of backup and restore privilege	<Not Defined>
9	Audit: Shut Down system immediately if unable to log security alerts	<Not Defined>
10	DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	<Not Defined>
11	DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	<Not Defined>
12	Devices: Allow undock without having to log on	<Not Defined>
13	Devices: Allowed to format and eject removable media	Administrator

14	Devices: Prevent users from installing printer drivers	Enabled
15	Devices: Restrict CD-ROM Access to Locally Logged-On User Only	Enabled
16	Devices: Restrict Floppy Access to Locally Logged-On User Only	Enabled
17	Devices: Unsigned Driver Installation Behavior	Warn But Allow installation
18	Domain Controller: Allow Server Operators to Schedule Tasks	Disabled
19	Domain Controller: LDAP Server Signing Requirements	Require Signing
20	Domain Controller: Refuse machine account password changes	Disabled
21	Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	<Not Defined>
22	Domain Member: Digitally Encrypt Secure Channel Data (When Possible)	Enabled
23	Domain Member: Digitally Sign Secure Channel Data (When Possible)	Enabled
24	Domain Member: Disable Machine Account Password Changes	Disabled
25	Domain Member: Maximum Machine Account Password Age	30 Days
26	Domain Member: Require Strong (Windows or later) Session Key	Enabled
27	Interactive logon: Display user information when the session is locked	<Not Defined>
28	Interactive Logon: Do Not Display Last User Name	Enabled
29	Interactive Logon: Do not require CTRL+ALT+DEL	Disabled
30	Interactive Logon: Message Text for Users Attempting to Log On	********** ***Welcome to OurServer ********** ***

		NOTICE TO USERS WARNING! The use of this system is restricted to authorized users, unauthorized access is forbidden and will be prosecuted by law. All information and communications on this system are subject to review, monitoring and recording at any time, without notice or permission. Users should have no expectation of privacy. ********** ***
31	Interactive Logon: Message Title for Users Attempting to Log On	Welcome
32	Interactive Logon: Number of Previous Logons to Cache	<Not Defined>
33	Interactive Logon: Prompt User to Change Password Before Expiration	14
34	Interactive Logon: Require Domain Controller authentication to unlock workstation	Enabled
35	Interactive Logon: Require Smart Card	<Not Defined>
36	Interactive Logon: Smart Card Removal Behavior	Lock Workstation
37	Microsoft Network Client: Digitally sign communications (always)	<Not Defined>
38	Microsoft Network Client: Digitally sign communications (if server agrees)	Enable

39	Microsoft Network Client: Send Unencrypted Password to Connect to Third-Part SMB Server	Disable
40	Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session	15 Minutes
41	Microsoft Network Server: Digitally sign communications (always)	<Not Defined>
42	Microsoft Network Server: Digitally sign communications (if client agrees)	Enable
43	Microsoft Network Server: Disconnect clients when logon hours expire	Enable
44	Network access: Allow anonymous SID/Name translation	Disabled
45	Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
46	Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
47	Network Access: Do not allow storage of credentials or .NET passports for network authentication	Enabled
48	Network Access: Let Everyone permissions apply to anonymous users	Enabled
49	Network Access: Named pipes that can be accessed anonymously	<None>
50	Network Access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\WindowsNT\CurrentVersion
51	Network Access: Remotely accessible registry paths and subpaths	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows

		NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers , System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server , System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\ Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib , System\CurrentControlSet\Services\SysmonLog
52	Network Access: Restrict anonymous access to Named Pipes and Shares	Enabled
53	Network Access: Shares that can be accessed anonymously	<None>
54	Network Access: Sharing and security model for local accounts	Classic
55	Network Security: Do not store LAN Manager password hash Rule on next password change	Eanbled
56	Network Security: Force logoff when logon hours expire	<Not Defined>

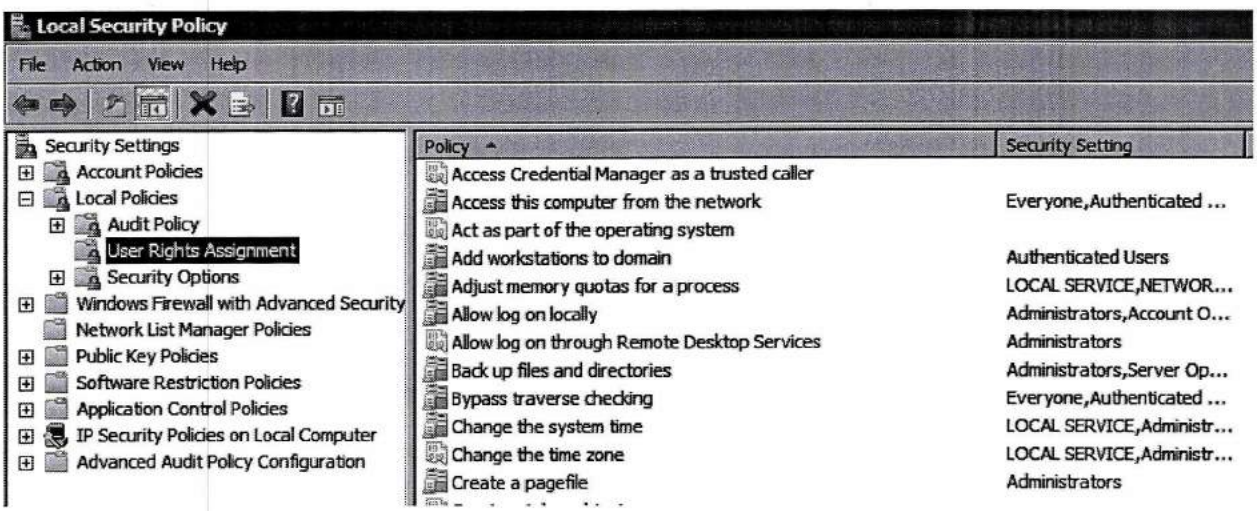
57	Network Security: LAN Manager Authentication Level	Send NTLMv2, refuse LM
58	Network Security: LDAP client signing requirements	Negotiate Signing or Require Signing
59	Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption
60	Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption
61	Recovery Console: Allow Automatic Administrative Logon	Disabled
62	Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders	Disabled
63	Shutdown: Allow System to be Shut Down Without Having to Log On	Disabled
64	Shutdown: Clear Virtual Memory Pagefile	Enabled
65	System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key
66	System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	<Not Defined>
67	System objects: Default owner for objects created by members of the Administrators group	Object Creator
68	System objects: Require case insensitivity for non-Windows subsystems	<Not Defined>
69	System objects: Strengthen default permissions of internal system objects	Enabled
70	System settings: Optional subsystems	<None>

71	System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	<Not Defined>
71	System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	<Not Defined>
71	System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	<Not Defined>
71	MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications	

1.9. Gán quyền User (User Rights Assignment)

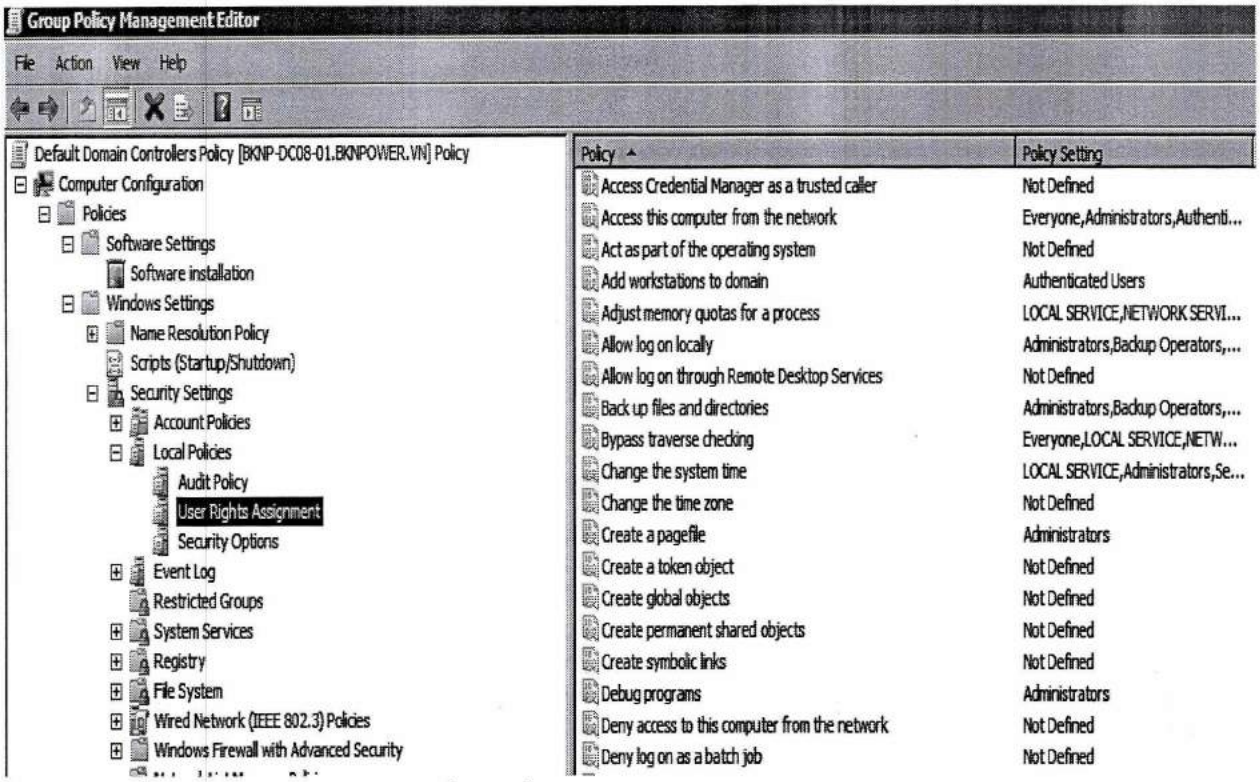
Đối với máy chủ Standalone thực hiện ở Local Policy .

Dùng lệnh: **secpol.msc.**



Đối với máy chủ là domain controller sử dụng lệnh **: gpmc.msc**

Sau đó Click chuột phải vào **Default Domain policy** chọn **Edit**



Thiết lập với các tham số chuẩn như sau

No	Policy	Recommended Setting
1	Access this computer from the network	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS
2	Act as part of the operating system	<None>
3	Add workstations to domain	<Not Defined>
4	Adjust memory quotas for a process	NETWORK SERVICE, LOCAL SERVICE, Administrators
5	Log on locally	Administrators, Authenticated Users
6	Allow logon through terminal services	Administrators
7	Back up files and directories	<Not Defined>
8	Bypass traverse checking	<Not Defined>
9	Change the system time	Administrators
10	Create a pagefile	Administrators
11	Create a token object	<None>
12	Create a global object	<Not Defined>
13	Create permanent shared objects	<None>

14	Debug Programs	<None>
15	Deny access to this computer from the network	ANONOYMOUS LOGON, Guests
16	Deny logon as a batch job	<Not Defined>
17	Deny logon as a service	<Not Defined>
18	Deny logon locally	<Not Defined>
19	Deny logon through Terminal Service	<Not Defined>
20	Enable computer and user accounts to be trusted for delegation	<None>
21	Force shutdown from a remote system	Administrators
22	Generate security audits	Local Service, Network Service
23	Impersonate a client after authentication	SERVICE
24	Increase scheduling priority	Administrators
25	Load and unload device drivers	Administrators
26	Lock pages in memory	Administrators
27	Log on as a batch job	<None>
28	Log on as a service	<Not Defined>
29	Manage auditing and security log	Administrators
30	Modify firmware environment values	Administrators
31	Perform volume maintenance tasks	Administrators
32	Profile single process	Administrators
33	Profile system performance	Administrators
34	Remove computer from docking station	Administrators
35	Replace a process level token	NETWORK SERVICE, LOCAL SERVICE
36	Restore files and directories	Administrators
37	Shut down the system	Administrators, Authenticated Users
38	Synchronize directory service data	<None>
39	Take ownership of file or other objects	Administrators

1.10. Cấu hình kiểm soát (Configure Auditing)

Cấu hình kiểm soát và log lại các sự kiện sau:

- Kiểm soát sự kiện Account logon
- Kiểm soát quản lý Account

- Kiểm soát truy cập dịch vụ thư mục
- Kiểm soát sự kiện Logon
- Kiểm soát truy cập đối tượng
- Kiểm soát thay đổi chính sách
- Kiểm soát sử dụng đặc quyền
- Kiểm soát giám sát tiến trình
- Kiểm soát sự kiện hệ thống

Cấu hình:

Đối với máy chủ Standalone thực hiện ở Local Policy, đối với máy chủ Domain thực hiện ở Domain security Policy

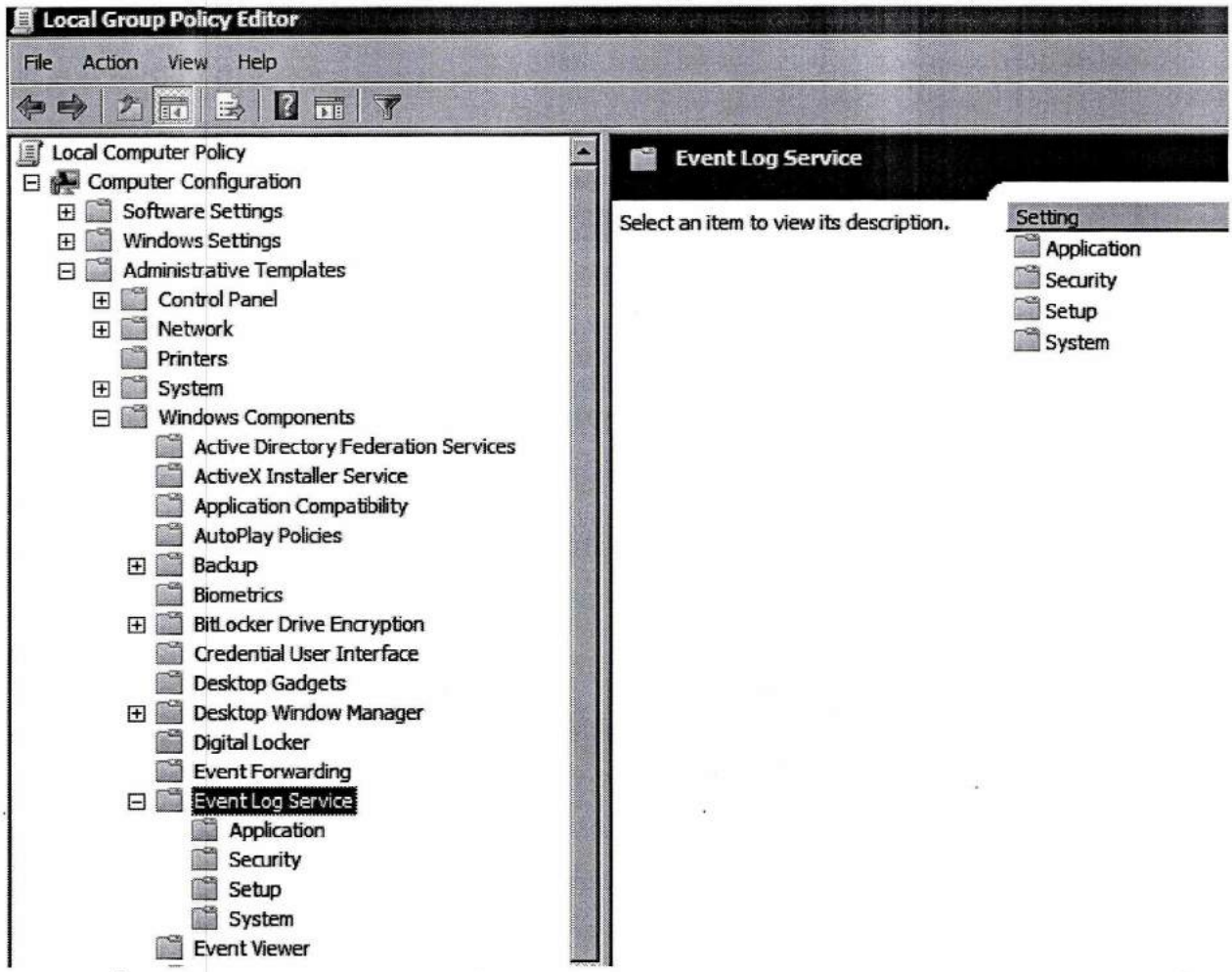
Thiết lập các tham số theo chuẩn:

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

1.11. Thiết lập Log sự kiện (Event Log Setting)

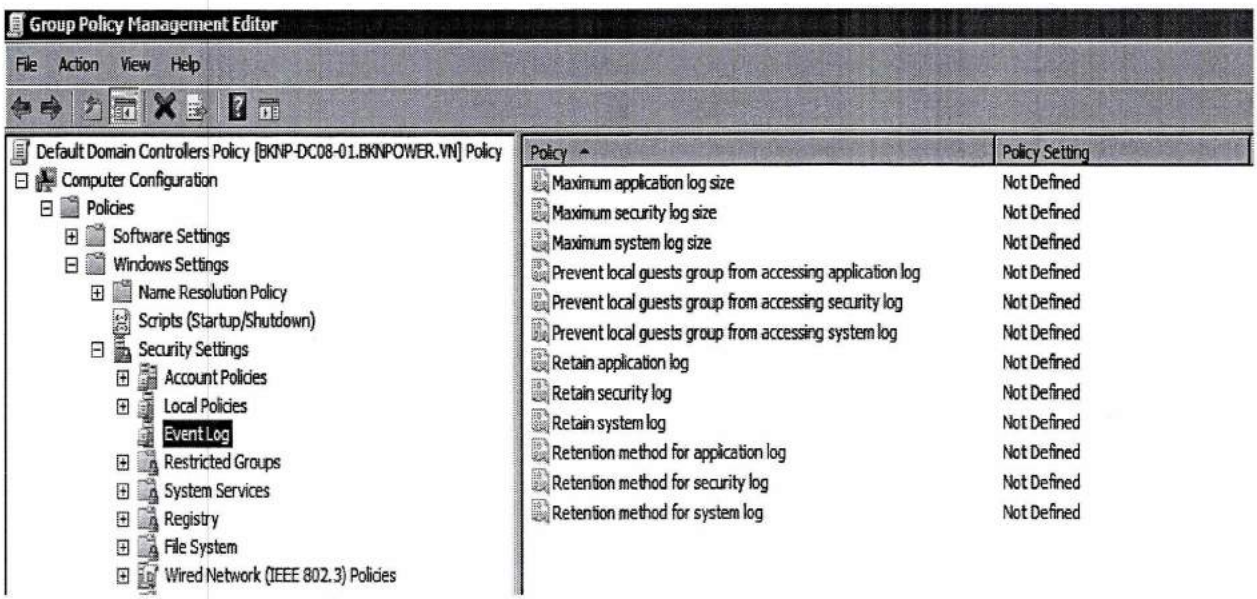
Đối với máy chủ Standalone thực hiện ở Local Policy dùng lệnh : **secpol.msc**

Truy cập theo đường dẫn **Computer Configuration -> Administrative Templates -> Windows Components -> Event Log Service**



Đối với máy chủ là domain controller sử dụng lệnh **: gpmc.msc**

Sau đó Click chuột phải vào **Default Domain policy** chọn **Edit**



Thiết lập tham số theo bảng sau.

Application Log	
Policy	**Setting**

Maximum Event Log Size	16 MB
Restrict Guest Access	Enabled
Log Retention Method	<Not Defined>
Log Retention	<Not Defined>

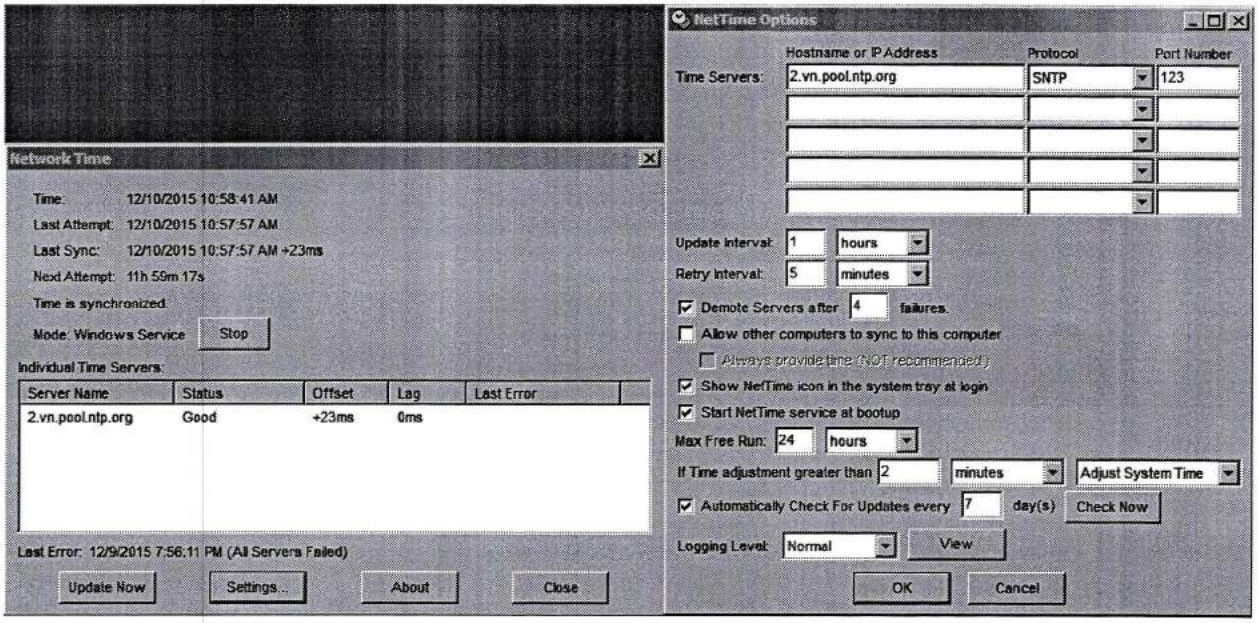
Security Log	
Policy	**Setting**
Maximum Event Log Size	80 MB
Restrict Guest Access	Enabled
Log Retention Method	<Not Defined>
Log Retention	<Not Defined>

System Log	
Policy	**Setting**
Maximum Event Log Size	16 MB
Restrict Guest Access	Enabled
Log Retention Method	<Not Defined>
Log Retention	<Not Defined>

1.12. Thiết lập giờ hệ thống

Với máy chủ vật lý độc lập cài đặt phần mềm NetTime, thiết lập giờ hệ thống thiết lập cập nhật từ máy chủ Time tập trung của tổ chức nếu có hoặc chọn 1 server có độ tin cậy cao **2.vn.pool.ntp.org** (máy ảo thì cài vmware tool để cập nhật giờ theo máy chủ vật lý)

Download http://www.timesynctool.com/

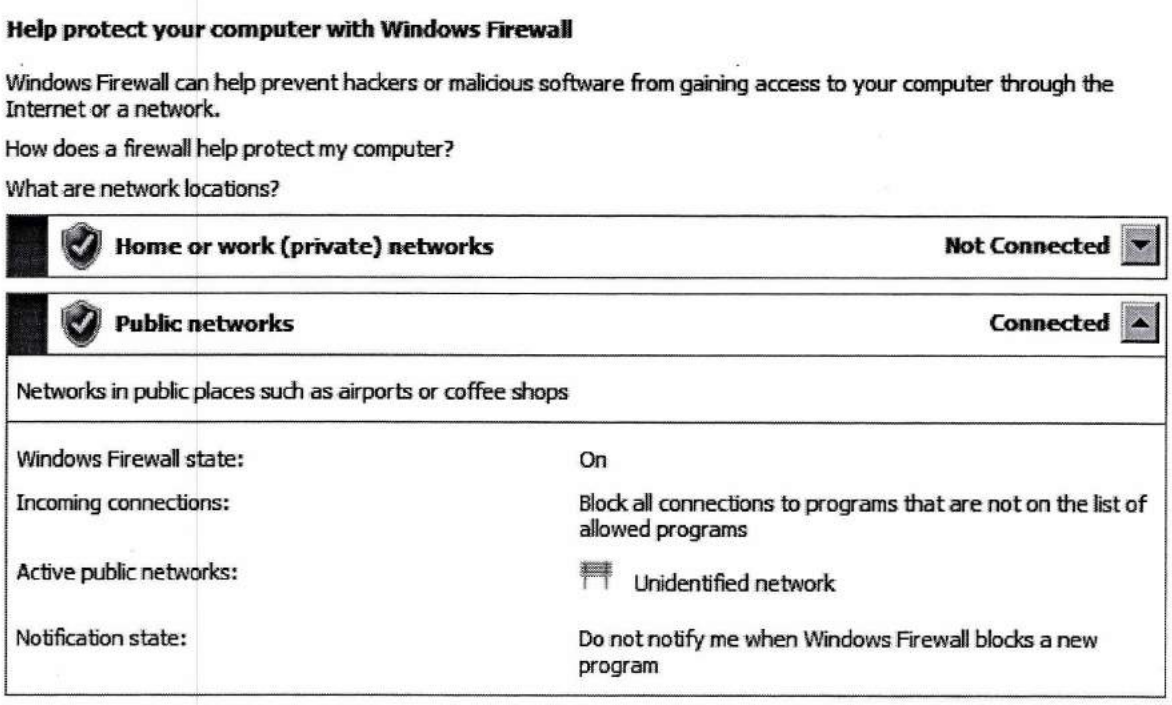


1.13. Disable Remote Registry

Cấu hình không cho phép truy cập Registry qua mạng :

Kiểm tra xem Firewall của HT có bật hay không có thể dùng lệnh **firewall.cpl** hoặc

Start --> Control Panel --> Windows firewall --> ON



Giới hạn quyền truy cập registry từ xa:

Start --> RUN --> **regedit** --> Chọn tới:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\

Chọn "winreg" --> Click chuột phải --> "Permissions" chọn user root(administrator) quyền "Full" còn lại bỏ hết quyền đi --> OK and exit.

1.14. Cấu hình Window Firewall

Yêu cầu luôn phải bật để kiểm tra traffic in

1.15. Cài đặt phần mềm Antivirus

- Cài đặt phần mềm Antivirus
- Lập lịch Update định nghĩa virus hàng ngày
- Thiết lập ở chế độ tự động phát hiện và bảo vệ
- Lập lịch quét hàng ngày

1.16. Service Packs Hot fixes và hệ thống

Yêu cầu cài đặt các gói cập nhật:

- Cài đặt Service Pack mới nhất
- Cài đặt Critical và Important Hotfixes mới nhất

2. Hướng dẫn thiết lập cấp hình bảo mật an toàn cho máy chủ Linux

2.1. Hardening Linux Centos

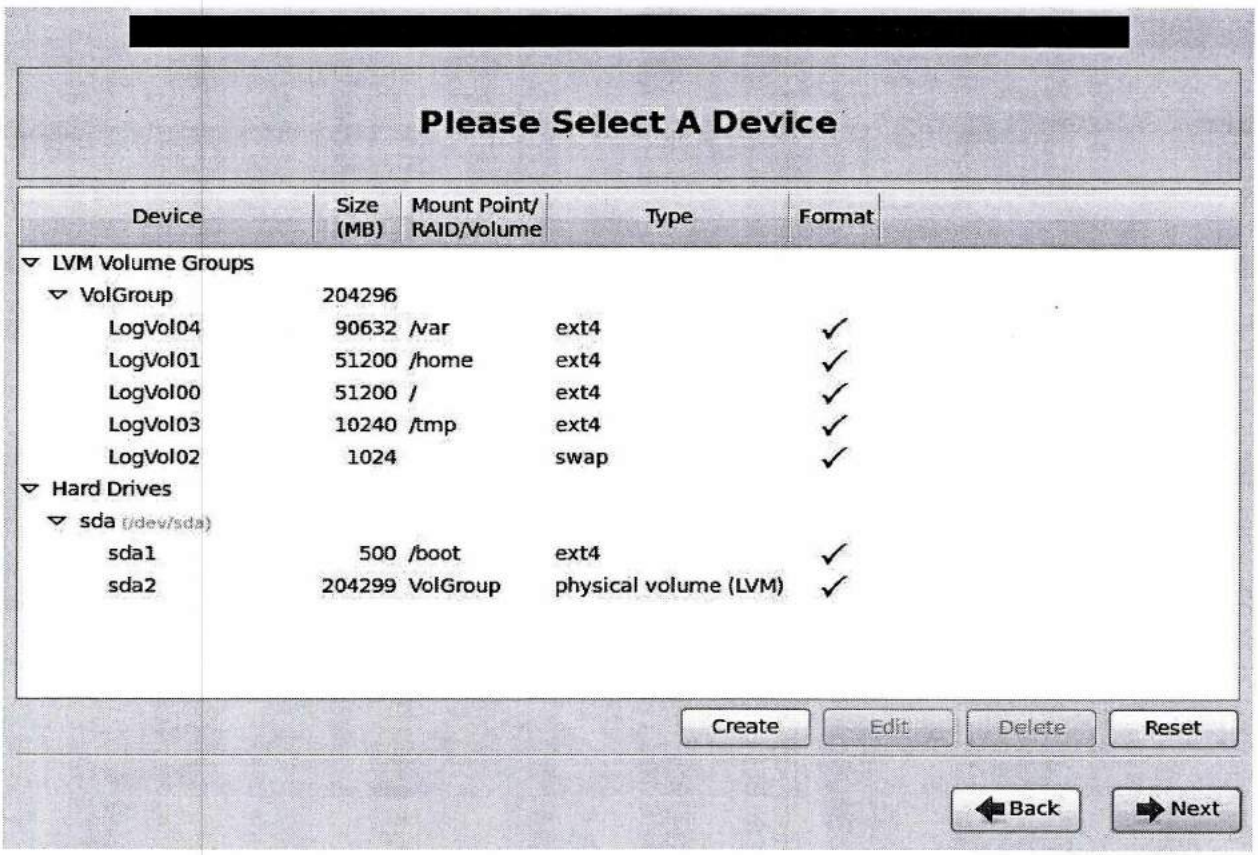
2.1.1. Tối ưu partitioning và mounting

Sử dụng bản cài Centos-6.5-minimal 64bit

a. Tối ưu Partitioning

Volume name	**Kích thước khuyến nghị**	**Lưu ý**
Partition thông thường		
/boot	500MB	Chứa Image boot, Primary, RAID1 (nếu có)
LVM partion	Toàn bộ kích thước đĩa còn lại	
LVM Volgroup		
/	50GB	Không cần tạo lớn vì chỉ chứa chương trình và các thư mục hệ thống

/home	50GB	Không chứa dữ liệu của hệ thống, chỉ lưu dữ liệu user. Không tạo nếu là máy ảo guest.
swap	2x kích thước RAM, nhưng: - max 2GB với máy vật lý - max 1GB với máy ảo.	Không tạo swap lớn quá kích thước Max
/tmp	10GB	
/var	Toàn bộ dung lượng đĩa còn lại	



b. Tối ưu Mounting Point

- **noexec**: không cho phép thực thi trực tiếp mã thực thi ở mount point được set option (Options này không ngăn cản scripts đang chạy).
- **Nodev**: thiết lập option này ở mọi mount point trừ "/" và các Partitions được chroot (nodev option cấm sử dụng device files trên file hệ thống)

- **Nosetuid**: thiết lập ở mọi mount point trừ "/" (nosuid sẽ cấm setuid bit có hiệu lực)

```
[root@localhost ~]# vi /etc/fstab
[root@localhost ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Fri Dec  4 08:59:20 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-LogVol00 /                       ext4    defaults        1 1
UUID=0c396b7a-bba4-49c9-8b9a-ba8986bf3099 /boot                   ext4    defaults,nosuid,noexec,nodev        1 2
/dev/mapper/VolGroup-LogVol01 /home                   ext4    defaults,nosuid,nodev        1 2
/dev/mapper/VolGroup-LogVol03 /tmp                    ext4    defaults,nosuid,noexec,nodev        1 2
/dev/mapper/VolGroup-LogVol04 /var                    ext4    defaults,nosuid        1 2
/dev/mapper/VolGroup-LogVol02 swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults,nosuid,noexec,nodev        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
[root@localhost ~]#
```

2.2. Tối ưu cấu hình mạng

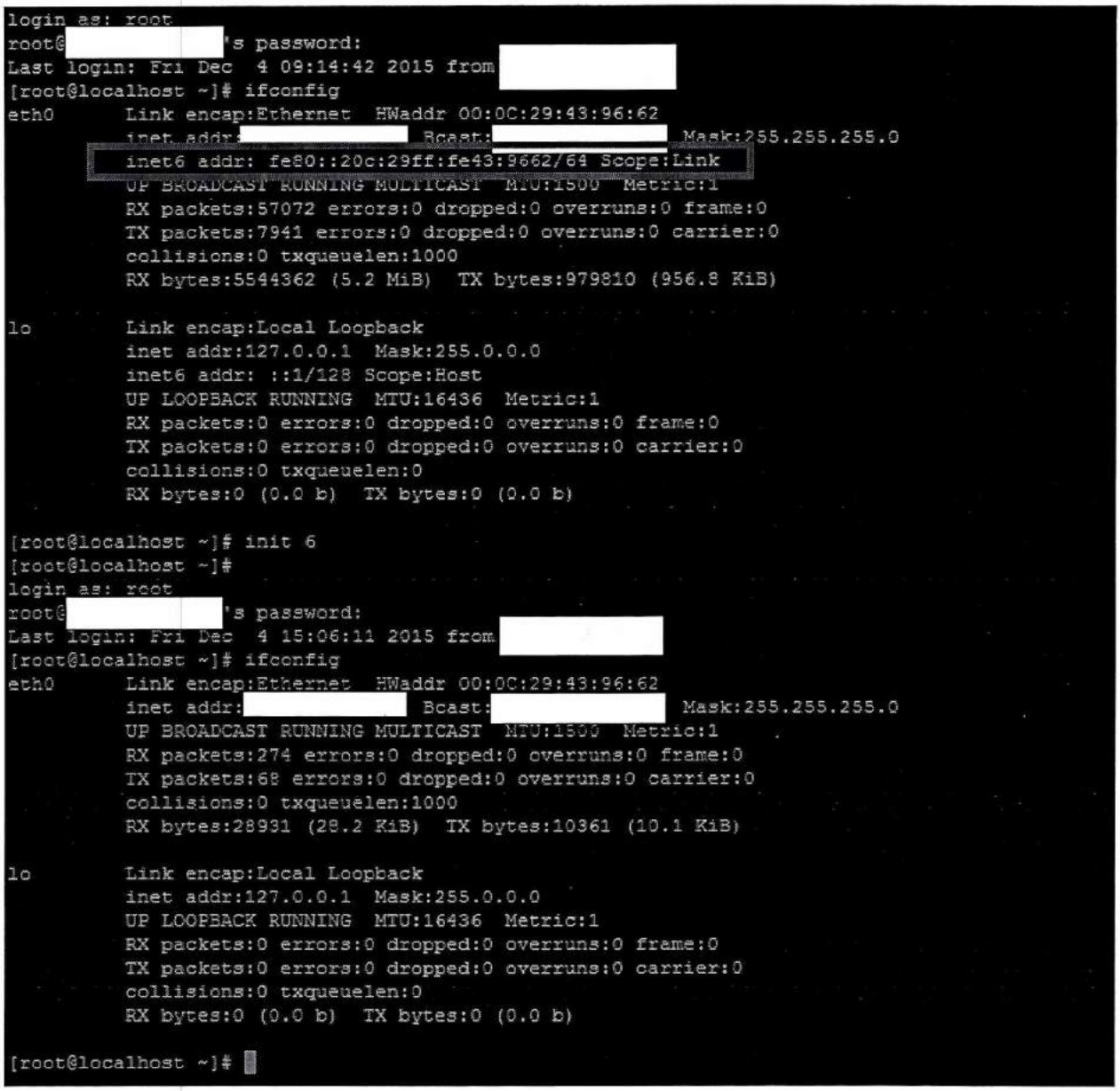
Trường hợp hệ thống không sử dụng IPv6 thì tắt dịch vụ này trên máy chủ.

a. Disable IPv6

- Tạo file **/etc/modprobe.d/ipv6.conf** thêm vào dòng:
  - **install ipv6 /bin/true**
- Thay đổi: **/etc/sysconfig/network** thêm dòng:
  - **NETWORKING_IPV6=no**
  - **IPV6INIT=no**

```
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=00:0C:29:43:96:62
TYPE=Ethernet
UUID=a0eeea3a-fd0e-418e-9a7f-6e240d9e340b
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
IPADDR=
NETMASK=255.255.255.0
GATEWAY=
NETWORKING_IPV6=no
IPV6INIT=no
[root@localhost ~]#
```

Kiểm tra sau khi reboot: **ifconfig | grep inet6** hoặc **lsmod | grep ipv6**



b. Disable Zeroconf

Sửa: **/etc/sysconfig/network** thêm vào cuối file dòng: **NOZEROCONF=yes**

Kiểm tra xem có gói "**avahi**" trong hệ thống sử dụng lệnh

- rpm –qa avahi

Nếu hệ thống có tồn tại gói này thì **Remove** gói

- yum remove avahi-autoipd avahi-libs avahi

c. Tối thiểu hóa các services(daemons) không cần thiết

Gõ Lệnh : chkconfig --list để kiểm tra danh sách service và trạng thái

```
[root@localhost ~]# chkconfig --list
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
blk-availability        0:off   1:on    2:on    3:on    4:on    5:on    6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
ip6tables       0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
iscsi           0:off   1:off   2:off   3:on    4:on    5:on    6:off
iscsid          0:off   1:off   2:off   3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mdmonitor       0:off   1:off   2:on    3:on    4:on    5:on    6:off
multipathd      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
postfix         0:off   1:off   2:on    3:on    4:on    5:on    6:off
rdisc           0:off   1:off   2:off   3:off   4:off   5:off   6:off
restorecond     0:off   1:off   2:off   3:off   4:off   5:off   6:off
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
saslauthd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
udev-post       0:off   1:on    2:on    3:on    4:on    5:on    6:off
```

- ***Runlevel-1***: chế độ chạy đơn người dùng (single-user mode).
- ***Runlevel-2***: chế độ chạy đa người dùng (multi-user mode).
- ***Runlevel-3***: chế độ đa người người, hỗ trợ mạng (multi-user and networking mode).
- ***Runlevel-5***: X11 (runlevel 3 + X Windows System). Thông thường, các dịch vụ chạy ở chế độ đồ họa (dựa trên X-Server như startx) thì runlevel ở mức 5 và các dịch vụ không chạy ở chế độ đồ họa thì runlevel ở mức 3. Bình thường, không có dịch vụ nào chạy ở runlevel 1. Để xác định runlevel mà bạn đang sử dụng thì bạn sử dụng lệnh sau:

Code:

```
# /sbin/runlevel
```

d. Vô hiệu hóa các dịch vụ lắng nghe mạng (network listen)

- Cách kiểm tra : netstat –tunlp (kiểm tra tất cả các port đang lắng nghe trên interfaces trên cả TCP/UDP)
- Khi mới cài đặt tối thiểu chỉ có các service sau được phép lắng nghe trên cổng mạng và trên các địa chỉ như sau:

```
[root@localhost ~]# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1119/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1199/master
```

2.3. Thiết lập iptables Firewall

- Thiết lập /etc/sysconfig/iptables theo mẫu sau.

```
[root@localhost ~]# cat /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]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
[root@localhost ~]#
```

2.4. Thiết lập đồng bộ giờ hệ thống

a. Thiết lập với máy chủ vật lý độc lập

- Cài đặt ntpdate : **yum install ntpdate**
- Sửa file /etc/ntp/step-stickers thêm vào địa chỉ máy chủ NTP local nếu có hoặc sử dụng NTP public có độ tin cậy cao

 # List of servers used for initial synchronization.

<IP NTP Server>

- Cập nhật giờ lần đầu : **ntpdate <IP(ntp server)>**

b. Thiết lập với máy chủ HOSTING máy ảo

2.5. Chính sách truy cập và tài khoản

a. Cấu hình chính sách mật khẩu tài khoản local và đăng nhập chung

Thiết lập file cấu hình: **/etc/login.defs** với các tham số chuẩn như sau:

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   90
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  500
UID_MAX                60000
#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  500
GID_MAX                60000
#
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD    /usr/sbin/userdel_local
#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is overridden with the -m flag on
# useradd command line.
#
CREATE_HOME     yes
#
# The permission mask is initialized to this value. If not specified,
# the permission mask will be initialized to 022.
UMASK           077
#
# This enables userdel to remove user groups if no members exist.
#
USERGROUPS_ENAB yes
#
# Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512
```

Thiết lập file cấu hình: **/etc/pam.d/system-auth** bằng cách thêm sửa các tham số chuẩn như sau :

```
[root@localhost ~]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_tally2.so onerr=fail deny=6 unlock_time=1800
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type= minlen=8 ucredit=-1 lcredit=-1 dcredit=-1
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=4
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
[root@localhost ~]#
```

Các tham số trên cho phép xác thực sai bị khóa, thời gian mở khóa, độ phức tạp của mật khẩu, lưu trữ mật khẩu ….

Chú ý : Check xem file lưu tạm mật khẩu có tồn tại trong hệ thống hay không, nếu không tồn tại cần phải tạo mà phân quyền đúng như sau

```
[root@localhost ~]# ls -l /etc/security/opasswd
-rw-------. 1 root root 0 Nov 22  2013 /etc/security/opasswd
```

- Thiết lập Console logout thêm các tham số sau vào cuối file : **/etc/bashrc**

```
# vim:ts=4:sw=4
# set a 5 min timeout policy for bash shell
TMOUT=300
readonly TMOUT
export TMOUT
[root@localhost ~]#
```

b. Chính sách truy cập từ xa qua ssh

- Thiết lập file cấu hình: **/etc/ssh/sshd_config** thêm/sửa với các tham số chuẩn như sau

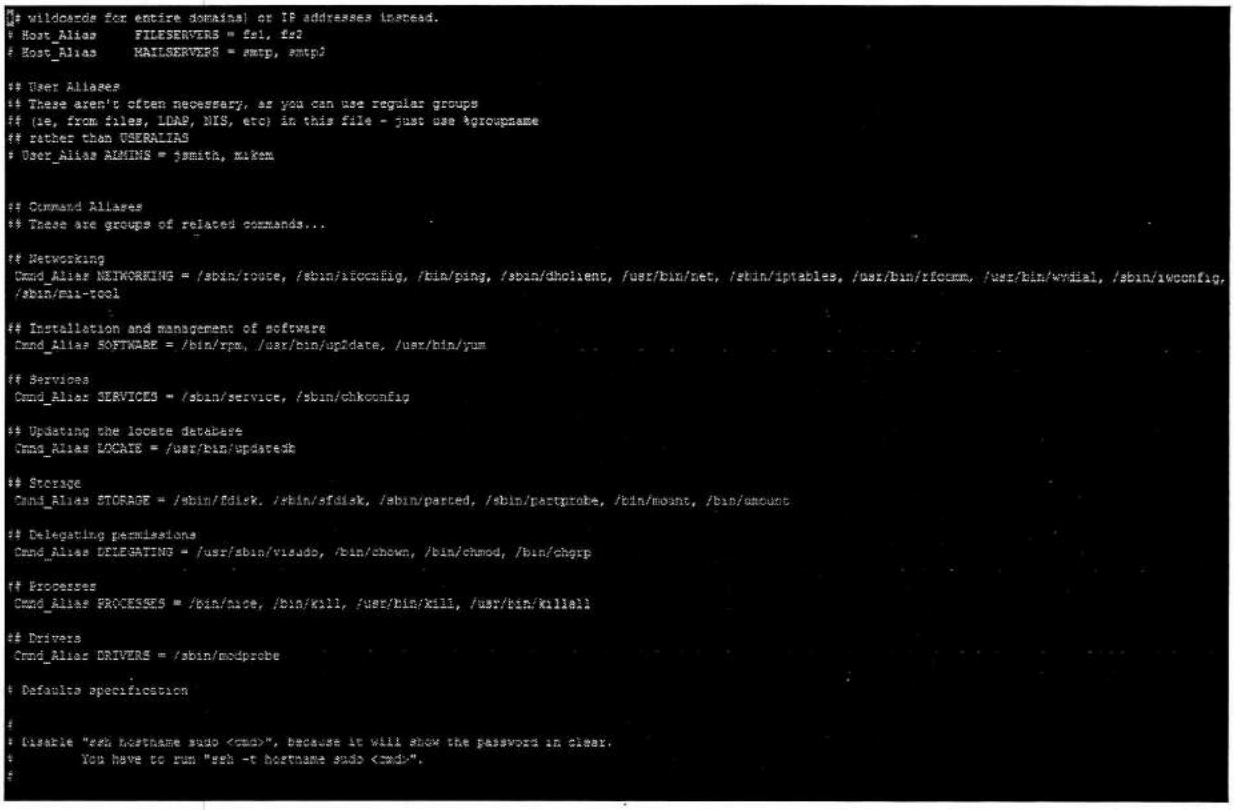
```
Port 22
ListenAddress 0.0.0.0
Protocol 2                                          # Yêu cầu SSHv2

SyslogFacility AUTHPRIV
LoginGraceTime 1m

PermitRootLogin no                  # cấm Root login
MaxAuthTries 6                        # Xác thực sai quá 6 lần sẽ ngắt kết nối

RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile      .ssh/authorized_keys

PermitEmptyPasswords no                 # Không cho phép đặt pass trống
PasswordAuthentication yes
ChallengeResponseAuthentication no
KerberosAuthentication no
GSSAPIAuthentication no
GSSAPICleanupCredentials yes

UsePAM yes
AllowTcpForwarding no
X11Forwarding no
PrintLastLog yes
TCPKeepAlive yes

ClientAliveInterval 45                  # Client ssh sẽ tự động out, sau 45s ko làm gì
ClientAliveCountMax 3

UseDNS no
PermitTunnel no
Banner /etc/ssh/banner                # Thiết lập Banner cảnh báo user khi truy cập
```

- Thiết lập thông báo khi user truy cập bổ sung vào file sau : **/etc/ssh/banner**

```
[root@localhost ~]# vi /etc/ssh/banner
[root@localhost ~]# cat /etc/ssh/banner
*******************************************************************************
#                            Welcome to SSH                                   #
#              All connections are monitored and recorded                     #
#         Disconnect IMMEDIATELY if you are not an authorized user!           #
#       Unauthorized access is forbidden and will be prosecuted by law        #
*******************************************************************************
[root@localhost ~]#
```

2.6. Cấu hình ủy quyền quản trị (SUDO)

Đầu tiên chỉnh sửa file cấu hình sudo: **/etc/sudoers.** Bỏ dấu '#' trước các dòng khởi tạo các nhóm lệnh.



Sau đó khởi tạo file thiết lập quyền cho group "adm"

```
[root@server ~]# cat /etc/sudoers.d/sysadmin
## View any file for Auditing

Cmnd_Alias VIEWER = /bin/cat, /bin/grep, /usr/bin/less, /usr/bin/tail, /usr/bin/tailf

## Editor config
Cmnd_Alias EDITOR = /bin/vi

## File manipulation
Cmnd_Alias FILE_MAN = /bin/mv, /bin/rm, /bin/cp, /bin/tar
%root        ALL=(ALL) NOPASSWD: ALL

%adm    ALL= NOPASSWD: VIEWER, EDITOR, NETWORKING, SOFTWARE, SERVICES, PROCESSES, LOCATE, DELEGATING, PASSWD: FILE_MAN

[root@server ~]#
```

Tiếp theo đó khởi tạo user rồi thêm vào nhóm "adm"

```
[root@server ~]# useradd -g adm manage
[root@server ~]# passwd manage
Changing password for user manage.
New password:
BAD PASSWORD: it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server ~]#
```

Để kiểm tra ta gõ lệnh kiểm tra file **/var/log/secure** nếu không thực hiện **sudo**

Ta sẽ thấy truy cập bị từ chối

Ex:

[manage@server ~]$ vi /var/log/secure

~

~

"/var/log/secure" [Permission Denied]

Sau đó thử lại lệnh với sudo : **sudo vi /var/log/secure**

Ta thấy được file log và log của sudo đã được lưu vào log của hệ thống

```
Dec  7 15:32:11 server sshd[1106]: Accepted password for root from 192.166.177.1 port 3437 ssh2
Dec  7 15:32:11 server sshd[1106]: pam_unix(sshd:session): session opened for user root by (uid=0)
Dec  7 15:32:34 server sshd[1121]: Accepted password for manage from 192.165.177.1 port 3438 ssh2
Dec  7 15:32:34 server sshd[1121]: pam_unix(sshd:session): session opened for user manage by (uid=0)
Dec  7 15:33:10 server sudo:   manage : TTY=pts/1 ; PWD=/home/manage ; USER=root ; COMMAND=/bin/vi /etc/sysconfig/network-scripts/ifcfg-eth0
Dec  7 15:33:38 server sudo:   manage : TTY=pts/1 ; PWD=/home/manage ; USER=root ; COMMAND=/bin/vi /var/log/secure
Dec  7 15:34:22 server sudo:   manage : TTY=pts/1 ; PWD=/home/manage ; USER=root ; COMMAND=/bin/vi /var/log/secure
Dec  7 15:38:55 server sudo:   manage : TTY=pts/1 ; PWD=/home/manage ; USER=root ; COMMAND=/bin/vi /var/log/secure
```

2.7. Thiết lập Local Email cho việc gửi báo cáo

Trên máy chủ mặc định đã cài gói postfix có thể dùng lệnh **rpm –qa postfix**. Nếu gói chưa được cài đặt dùng lệnh **yum install postfix** để cài đặt.

Sau cài đặt xong sửa trong file cấu hình **/etc/postfix/main.cf** các tham số sau

Line 83 – bỏ dấu '#' and và đặt tên miền

mydomain = example.com

Line 99 – bỏ dấu '#'

myorigin = $mydomain

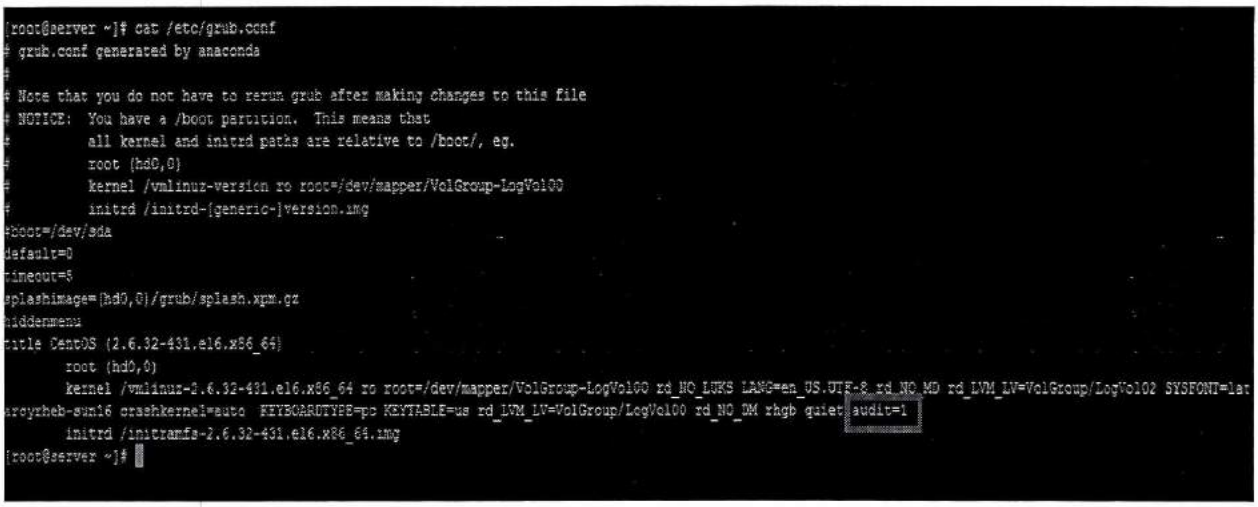
Sau đó khởi động lại dịch vụ bằng lệnh: **service postfix restart**

Và cho phép dịch vụ khởi động sau mỗi lần reboot : **chkconfig pofstfix on**

2.8. Thiết lập Audit, aureport và LogWatch

a. Cấu hình Audit

Thêm tham số "**audit=1"** vào cuối dòng kernel **:/etc/grub.conf**



Copy cấu hình mẫu Audit Rule

cp /usr/share/doc/audi-VERSION/stig.rules /etc/audit/audit.rules

Sửa cấu hình : **/etc/audit/audit.rules (** comment các dòng chứa arch= 32/64 không đúng với kiến trúc của máy chủ đang chạy)

Để check kiến trúc của máy chủ đang chạy có thể dùng lệnh : **uname –r hoặc uname –i**

VD:

```
## Things that could affect time
#-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
#-a always,exit -F arch=b32 -S clock_settime -F a0=0 -k time-change
-a always,exit -F arch=b64 -S clock_settime -F a0=0 -k time-change
```

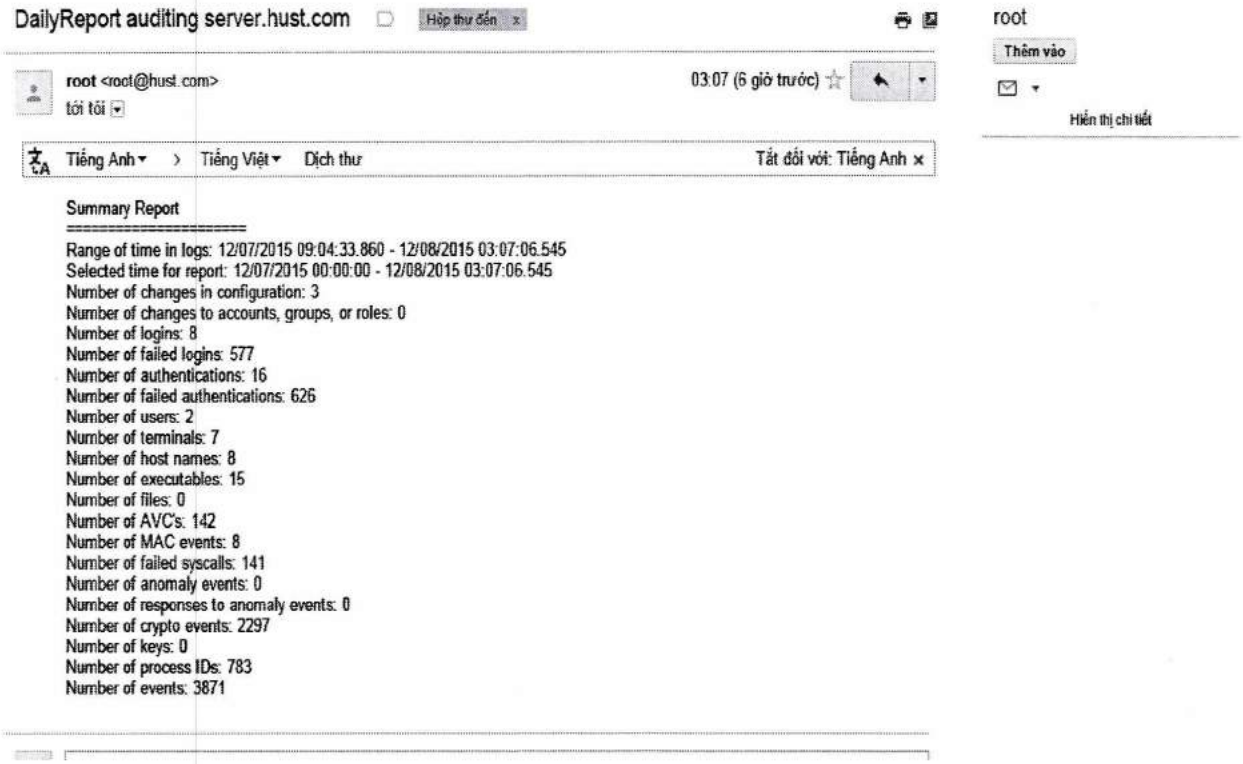
b. Cấu hình gửi mail aureport summary hàng ngày về mail nhóm quản trị

- Tạo file: **/etc/cron.daily/aureport** với nội dung như sau

```
#!/bin/sh

d=`date -d 'now -1 day' '+%m/%d/%Y'`

/sbin/aureport --start $d 00:00:00 | mail -s "DailyReport auditing $HOSTNAME" [redacted]@gmail.com
```

⇨ Trong đó có email là tài khoản của nhóm hoặc người quản trị

- Phân quyền: **chmod 755 /etc/cron.daily/aureport**



c. Thiết lập cấu hình Logwatch gửi email tới hòm mail nhóm hoặc người quản trị phục vụ việc gửi email report service tới admin

- Cài đặt logwatch: **yum install logwatch**
- Phân quyền: **chmod 755 /etc/cron.daily/0logwatch**

Tiếp theo đó phải cấu hình logwatch cho phép gửi mail tới địa chỉ mail của admin. Mặc định file cấu hình của LogWatch nằm theo đường dẫn :

/usr/share/logwatch/default.conf/logwatch.conf

Sửa dòng 35 để chỉnh hòm thư admin nhận thông tin từ LogWatch : **Mailto =**

Sửa dòng 44 chỉ người gửi trong server : **MailFrom =**

```
# Default person to mail reports to.  Can be a local account or a
# complete email address.  Variable Print should be set to No to
# enable mail feature
MailTo = [redacted]@gmail.com
# When using option --multiemail, it is possible to specify a different
# email recipient per host processed.  For example, to send the report
# for hostname host1 to user@example.com, use:
#Mailto_host1 = user@example.com
# Multiple recipients can be specified by separating them with a space.

# Default person to mail reports from.  Can be a local account or a
# complete email address.
MailFrom = root@hust.com
```

Sau đây là một vài thông tin có trong mail gửi từ LogWatch.

Logwatch for server.hust.com (Linux) Hộp thư đến x

root@hust.ecom 10:23 (24 phút trước)
tới tôi

Tiếng Anh > Tiếng Việt Dịch thư Tắt đối với: Tiếng Anh x

```
################### Logwatch 7.3.6 (05/19/07) ####################
        Processing Initiated: Tue Dec  8 10:23:53 2015
        Date Range Processed: yesterday
                              ( 2015-Dec-07 )
                              Period is day.
      Detail Level of Output: 0
            Type of Output: unformatted
          Logfiles for Host: server.hust.com
##################################################################

---------- Selinux Audit Begin ----------

Number of audit daemon stops: 2

---------- Selinux Audit End ----------


---------- Cron Begin ----------



---------- SSHD Begin ----------

SSHD Killed: 2 Time(s)

SSHD Started: 3 Time(s)

Failed logins from:
   14.161.37.177: 3 times
   118.71.255.34: 1 time
   149.154.65.151 (adobedrive.ru): 23 times
   195.154.58.76 (195-154-58-76.ggsmarket.net): 5 times
   212.83.177.88 (212-83-177-88.ggsmarket.net): 3 times

Illegal users from:
   14.161.37.177: 5 times
   149.154.65.151 (adobedrive.ru): 2 times
   195.154.58.76 (195-154-58-76.ggsmarket.net): 18 times
   212.83.177.88 (212-83-177-88.ggsmarket.net): 13 times

Users logging in through sshd:
   root:
      .              7 times
      .              : 1 time


Received disconnect:
   11: Bye Bye : 25 Time(s)
   3: com.jcraft.jsch.JSchException: Auth fail : 47 Time(s)
   3: java.net.SocketTimeoutException: Read timed out : 2 Time(s)
```

d. Thiết lập cấu hình Logrotate để toàn bộ Log quay vòng Log mỗi ngày, Lưu giữ 180 ngày có compress theo mẫu sau:

Chỉnh sửa file cấu hình Logrotate theo đường dẫn **/etc/logrotate.conf**

```
# see "man logrotate" for details
# rotate log files weekly
daily

# keep 4 weeks worth of backlogs
rotate 180

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
        minsize 1M
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}

# system-specific logs may be also be configured here.
```

2.9. Phần mềm Antivirus

Cài đặt phần mềm Clamav: **yum install clamav**

Nếu xuất hiện lỗi như sau

```
[root@server log]# yum install clamd
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.readyspace.com
 * extras: centos-hn.viettelidc.com.vn
 * updates: centos.usonyx.net
base
extras
updates
Setting up Install Process
No package clamd available.
Error: Nothing to do
```

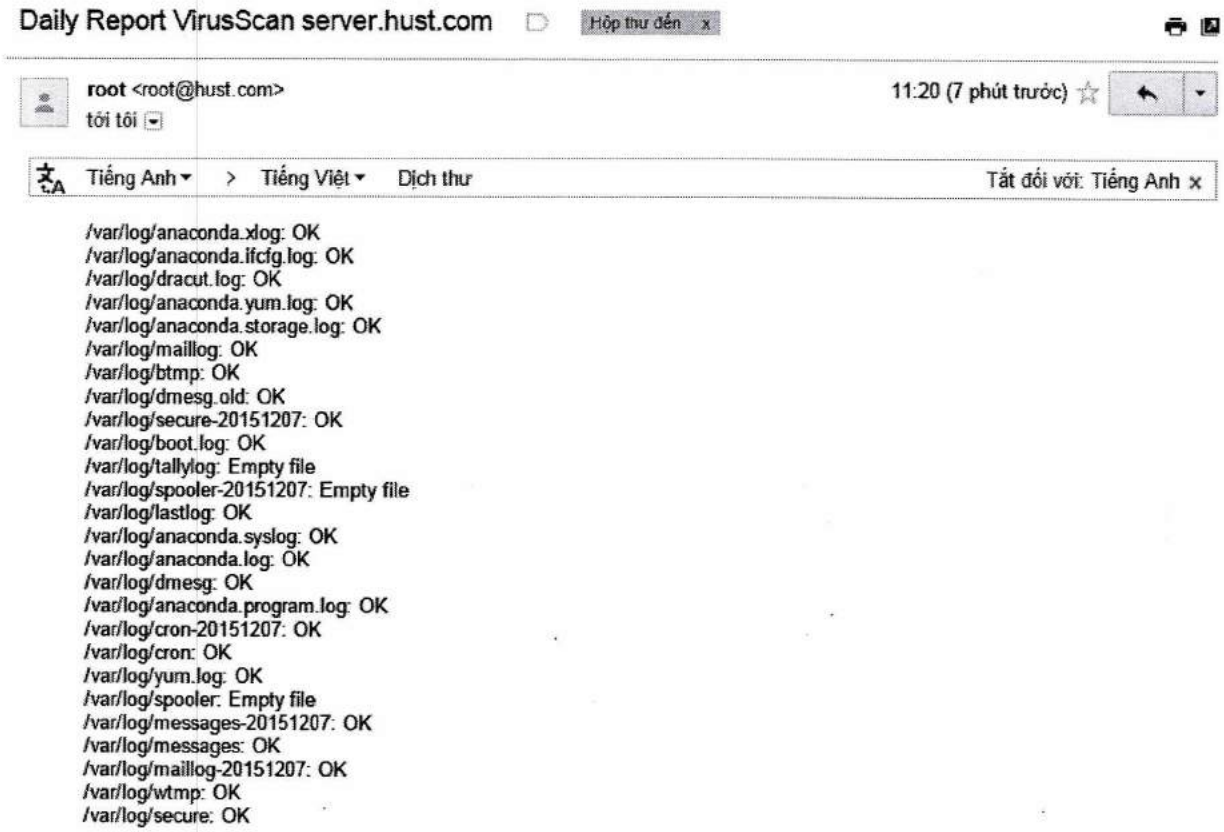
Sử dụng lệnh cập nhật Repositories : **yum install epel-release** sau đó chạy lại câu lệnh cài đặt.

Sau đó lập lịch quét tự động

- Tạo file : **/etc/cron.daily/clamscan** nội dung như sau:

#!/bin/bash

clamscan [đường dẫn thư mục muốn quét] –remove | mail –s "Daily Report VirusScan $HOSTNAME" mail-notify@domain.com



Daily Report VirusScan server.hust.com Hộp thư đến x

root <root@hust.com> 11:20 (7 phút trước)
tới tôi

Tiếng Anh > Tiếng Việt Dịch thư Tắt đối với: Tiếng Anh x

/var/log/anaconda.xlog: OK
/var/log/anaconda.ifcfg.log: OK
/var/log/dracut.log: OK
/var/log/anaconda.yum.log: OK
/var/log/anaconda.storage.log: OK
/var/log/maillog: OK
/var/log/btmp: OK
/var/log/dmesg.old: OK
/var/log/secure-20151207: OK
/var/log/boot.log: OK
/var/log/tallylog: Empty file
/var/log/spooler-20151207: Empty file
/var/log/lastlog: OK
/var/log/anaconda.syslog: OK
/var/log/anaconda.log: OK
/var/log/dmesg: OK
/var/log/anaconda.program.log: OK
/var/log/cron-20151207: OK
/var/log/cron: OK
/var/log/yum.log: OK
/var/log/spooler: Empty file
/var/log/messages-20151207: OK
/var/log/messages: OK
/var/log/maillog-20151207: OK
/var/log/wtmp: OK
/var/log/secure: OK