**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

**BÀI TẬP LỚN NHÓM 4**

Họ và tên các thành viên:

Đỗ Tiến Sĩ (B20DCAT153) (nhóm trưởng)

Trần Đăng Trọng (B20DCAT191)

Đào Thị Thảo (B20DCAT178)

Dương Ngô Hiếu(B20DCAT056)

Nguyễn Thị Trang(B20DCAT188)

Họ và tên giảng viên:

TS. Đinh Trường Duy

Mục lục

[**Chương 1: Dịch vụ DNS/ DHCP (so sánh cài đặt và quản trị trên Window với Linux) 2**](#_Toc117028960)

[**I) Dịch vụ DNS 2**](#_Toc117028961)

[**1. Giới thiệu 2**](#_Toc117028962)

[**2. So sánh cài đặt 2**](#_Toc117028963)

[**II) Dịch vụ DHCP 4**](#_Toc117028964)

[**1. Giới thiệu 4**](#_Toc117028965)

[**2. So sánh cài đặt 4**](#_Toc117028966)

[**Chương 2 . QUẢN LÝ NGƯỜI DÙNG VÀ MÁY TÍNH 5**](#_Toc117028967)

[**I. Trong hệ điều hành Windows 6**](#_Toc117028968)

[**1. Giới thiệu về phần mềm windows 6**](#_Toc117028969)

[**2. Trong hệ điệu hành Linux/Unix 8**](#_Toc117028970)

[**Chương 3: GIÁM SÁT HOẠT ĐỘNG VÀ KIỂM TOÁN: 10**](#_Toc117028971)

[**I) .Giám Sát Hoạt Động 10**](#_Toc117028972)

[**II) Kiểm Toán 12**](#_Toc117028973)

[**III) TÌM HIỂU VÀ PHÂN TÍCH CÁC LOẠI LOG: 13**](#_Toc117028974)

# Chương 1: Dịch vụ DNS/ DHCP (so sánh cài đặt và quản trị trên Window với Linux)

## I) Dịch vụ DNS

1. **Giới thiệu**

Dịch vụ tên miền là dịch vụ thiết yếu trong mạng Internet. Mỗi khi người dùng truy nhập tài nguyên trên mạng như trang Web, người dùng phải nhập vào địa chỉ trang web. Máy tính của người dùng sử dụng dịch vụ DNS để xác định vị trí vật lý (địa chỉ mạng) của máy tính chứa nội dung trang web mà người dùng muốn truy nhập đến.

Về mặt kỹ thuật, DNS là hệ thống quản lý cơ sở dữ liệu phân tán dựa trên mô hình phân cấp chủ/khách để chuyển đổi tên máy chủ hay tên miền thành địa chỉ mạng Internet.

1. **So sánh cài đặt**
   1. **Sự giống nhau**

Về cơ bản dịch vụ DNS trên Linux tương tự như trên Windows

- Có thể chia làm các loại máy chủ DNS: Máy chủ chính (primary server hay DNS Master, Máy chủ phụ (secondary server hay DNS Slave), Đệm (caching server).

- Các thông tin của máy chủ DNS được lưu vào các bản ghi có dạng: SOA, NS, CNAME, PTR, MX, A hoặc AAAA, SRV…

- Máy chủ DNS có thể quản lý hoặc miền chính (primary zone) hay miền thứ cấp (secondary zone) hay cả hai. Khi đặt cấu hình cho máy chủ DNS có hai kiểu vùng khác nhau: Forward Lookup Zone và Reverse Lookup Zone

**2.2 Sự khác nhau**

|  |  |
| --- | --- |
| Hệ điều hành Windows | Hệ điều hành Linux |
| Cung cấp dịch vụ DNS qua tiện ích “Server Manager”, rồi thêm role DNS.    Hình 2.1. Cài đặt DNS trên Windows | Cung cấp DNS qua gói phần mềm BIND (Berkeley Internet Name Daemon). Sử dụng câu lệnh: sudo apt-get install bind9    Hình 2.2. Cài đặt DNS trên Linux |
| Các file database được lưu trong *%systemroot%/System32/dns* | Các file cấu hình dịch vụ DNS được đặt trong thư mục */etc/bind.* |
| Các dạng bản ghi DNS: Các thông tin của máy chủ DNS được lưu vào các bản ghi có dạng như sau:  - Bản ghi khởi đầu SOA  - Bản ghi máy chủ  - Bản ghi CNAME  - Bản ghi NS  - Bản ghi dịch vụ SRV  - Bản ghi con trỏ PTR  - Bản ghi máy chủ thư | Các bản ghi theo các cấu trúc như sau:  - Bản ghi SOA  - Bản ghi NS  - Bản ghi A  - Bản ghi CNAME  - Bản ghi PTR |
| Cung cấp giao diện đồ họa cho việc cài đặt, cấu hình.  + Cài đặt các vùng tìm kiếm thuật, nghịch : trong “Server Manager”, vào *Tools -> DNS-> New zone*  +Chỉnh sửa các bản ghi cũng có thể thực hiện trong “DNS Manager”. | Cài đặt, cấu hình sử dụng giao diện dòng lệnh  + Người quản trị có thể sửa đổi file cấu hình qua *“/etc/bind/named.conf.local”*  + Chỉnh sửa các bản ghi qua file */etc/bind/db.192*  +Sau khi cài đặt, người dung cần khởi động lại dịch vụ DNS thông qua câu lệnh: *“sudo service bind9 restart”.* |
| Sau khi cài đặt người dung có thể sử dụng cmd để kiểm tra:  + *ping*: kiểm tra kết nối mạng  +*nslookup*: kiểm tra cấu hình DNS  +*ipconfig:* xem các tham số mạng được đặt cho máy tính như: IP, DNS Address, … | Kiểm tra cài đặt của dịch vụ DNS có thể sử dụng các câu lệnh sau:  +*ping*: kiểm tra máy trạm gắn với tên miền có hoạt động không  +*named-checkzone*: kiểm tra dữ liệu tên  +*nslookup*: kiểm tra tên Internet |

## II) Dịch vụ DHCP

1. **Giới thiệu**

Dịch vụ DHCP là dịch vụ mạng cho phép gán cấu hình mạng tự động cho các máy tính trong mạng. Điều này giúp cho việc triển khai và quản lý mạng được thuận tiện và nhanh chóng so với việc người quản trị phải thiết lập các tham số cho các máy tính một cách thủ công. Các điều chỉnh và sửa đổi chỉ cần thực hiện tại máy chủ cung cấp dịch vụ DHCP.

DHCP giúp việc quản lý và cấp phát tập trung và tự động địa chỉ mạng Internet cho các máy tính trong mạng. Ngoài ra, dịch vụ này còn giúp cài đặt các tham số khác một cách tự động cho các máy tính trong mạng như địa chỉ máy chủ DNS, cổng kết nối ra bên ngoài.

1. **So sánh cài đặt**
   1. **Giống nhau**

Về cơ bản dịch vụ DHCP trên Linux tương tự như trên Windows

- Máy chủ dịch vụ DHCP hỗ trợ các chế độ hoạt động như sau: Cấp phát tĩnh (thủ công), cấp phát động, cấp phát tự động.

- Tham số quan trọng cần xác định là

+ Dải địa chỉ mà máy chủ DHCP quản lý.

+ Các nhóm địa chỉ dành riêng không dùng để cấp phát cho các máy tính trong mạng.

+ Nhóm địa chỉ có thể phục vụ mục đích riêng như gán cố định cho các dịch vụ mạng.

+ Không gian địa chỉ còn lại dùng để cấp phát cho các máy trong mạng

**-** Các điều chỉnh và sửa đổi chỉ cần thực hiện tại máy chủ cung cấp dịch vụ DHCP. Về cơ bản, thông tin cấu hình gồm có: Địa chỉ IP và mạng con, địa chỉ IP của máy gateway, địa chỉ IP của máy chủ tên miền, 1 số dịch vụ khác: tên máy trạm, tên miền…

**2.2. Khác nhau**

|  |  |
| --- | --- |
| Hệ điều hành Windows | Hệ điều hành Linux |
| Cài đặt thông qua giao diện của tiện ích “ServerManager”.    Hình 2.1.Cài đặt DHCP trên Windows | DHCP được cài đặt qua gói phần mềm của Ubuntu sử dụng công cụ quản lý phần mềm apt-get: *sudo apt-get install isc-dhcp-server*    Hình 2.2. Cài DHCP trên Linux |
| Database của DHCP được lưu ở đường dẫn *%systemroot%/System32/dhcp* | Các thông tin cài đặt cho máy chủ DHCP được lưu tại */etc/default/isc-dhcp-server*. |
| - Cấu hình cho dịch vụ DHCP khá thuận tiện nhờ giao diện đồ họa của phần quản trị DHCP: trong “Server Manager”, chọn *Tools -> DHCP .*  *+*Tại đây cần tạo một scope và range IP: trong “DHCP”, chọn *IPv4 -> New scope* | - Sử dụng giao diện dòng lệnh  -Thông tin về địa chỉ cấp cho các máy tính trong mạng, chỉnh sửa các thông tin mở file: */etc/dhcp/dhcpd.conf* |
| -Có thể sử dụng lệnh *netstat* để kiểm tra hoạt động của dịch vụ DHCP.  -Sử dụng câu lệnh: *ipconfig /all* để kiểm tra thông số TCP/IP do DHCP Server cấp phát trên máy Client. Hoặc trong “DHCP”, phần *Address Leases* kiểm tra trạng thái cấp phát dịch vụ cho các máy khách. | -Kiểm tra các yêu cầu được cấp phát qua file nhật ký: */var/lib/dhcpd/leases*  - Kiểm tra trạng thái dịch vụ: *service isc-dhcp-server status*  - Kiểm tra và khởi động lại dịch vụ DHCP:  *sudo service isc-dhcp-server status/restart* |

# Chương 2 . QUẢN LÝ NGƯỜI DÙNG VÀ MÁY TÍNH

Bất kì ai khi dùng máy tính thì đều phải thông qua một tài khoản người dùng. Mọi người khi sử dụng đều muốn có một tài khoản riêng.

Mỗi máy tính thì có thể tạo một hoặc nhiều tài khoản người dùng để bảo vệ máy tính. Máy tính có thể tạo ra nhiều User trong máy.

Khi có được nhiều tài khoản người dùng thì ta cần phải quản trị và khi đó thì vai trò của quản lý người dùng và máy tính thể hiện như sau:

* Giúp phân quyền trên máy tính được sử dụng ở trong công ty hoặc một nhóm người dùng chung trong máy tính.
* Giúp chia sẻ dữ liệu trong điều kiện bảo mật.
* Giúp bảo vệ dữ liệu máy tính.

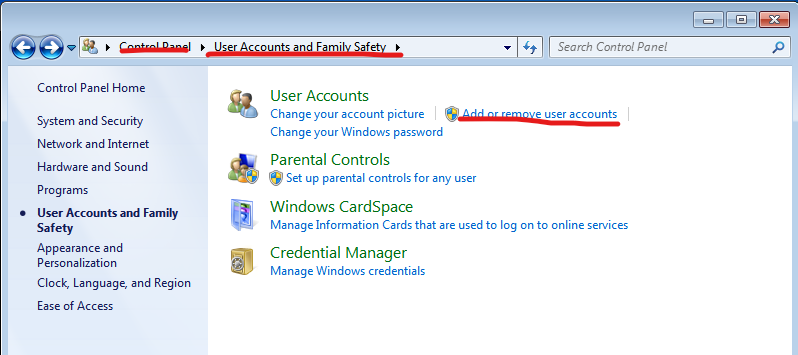
1. **Trong hệ điều hành Windows**
2. **Giới thiệu về phần mềm windows**

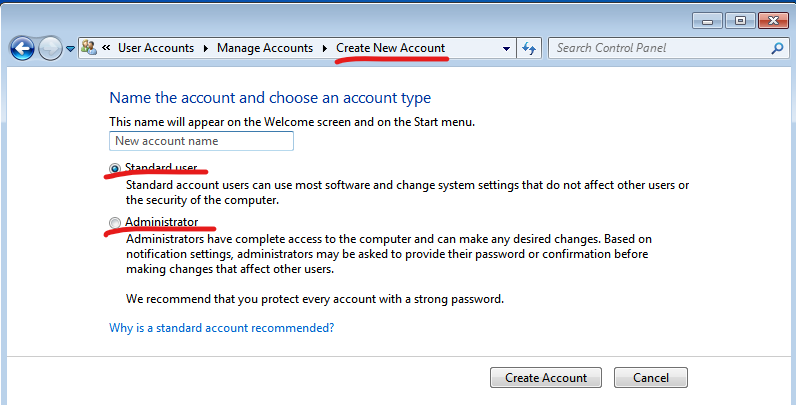
Ưu điểm: giao diện đẹp, dễ thao tác và sử dụng cho người dùng.

* Có 2 kiểu tài khoản;
* Người dùng truy cập vào máy tính thì gọi là tài khoản cục bộ
* Người dùng truy cập các tài nguyên trong mạng người dùng thì cần phải tài khoản miền.
* Các kiểu người dùng phổ biến:
* Người quản lý: người có thể cài đặt bất cứ gì và thay đổi ảnh hưởng đến tất cả người dùng trong PC đó.
* Tiêu chuẩn (standard): người chỉ có thể sử dụng phần mềm được quản trị viên cài đặt và không thể làm thay đổi hệ thống người dùng khác.
* Trẻ em: tài khoản này sẽ dùng khi cho trẻ em sử dụng thì sẽ an toàn khi truy cập Internet.
* Khách: người dùng này chỉ sử dụng khi được người người quản trị cài đặt và không làm thay đổi gì ở trên hệ thống.
* Khi ta sử dụng chung một máy tính thì ta có thể chuyển qua lại giữa 1 tài khoản Microsoft.
* Để quản trị người dùng cục bộ thì ta dùng quản trị truy nhật “Local User and Group” của Server manager”.
* Còn khi ta muốn sử dụng nhóm người mà dùng chung tài nguyên trong miền thì ta sử dụng Active Directory Users and Computers”

**Demo:**

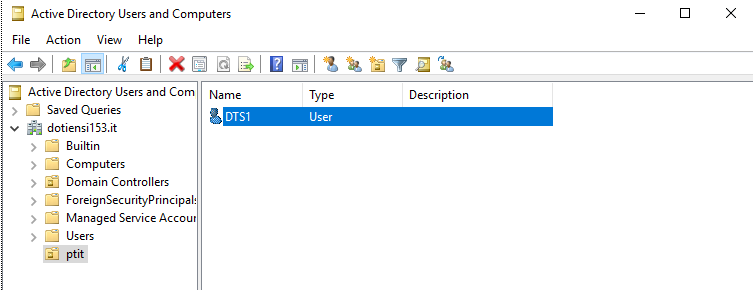
* Phần tài khoản người dùng cục bộ:

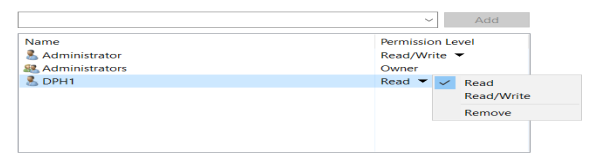
****

****

Ta sử dụng bằng win7.

* Ta sử dụng người dùng trên miền





1. **Trong hệ điệu hành Linux/Unix**

**Giới thiệu chung :**

Về bản chất, Ubuntu được cài đặt dành cho 1 người duy nhất sử dụng trên hệ thống, nhưng nếu yêu cầu có nhiều hơn 1 người, cách tốt nhất là tạo nhiều tài khoản tương ứng với số người dùng. Do đó, mỗi người sẽ có những thiết lập và thư mục lưu trữ riêng biệt, không ảnh hưởng cũng như liên quan đến tài khoản khác.

Mỗi người dùng được phân biệt thông qua tên hay định danh người dùng UID, được xác thực nhờ cơ chế kiểm tra mật khẩu. Mặc định, các thông tin người dùng này được lưu trong file */etc/passwd.*

- File passwd nằm ở thư mục */etc* chứa danh sách tài khoản trên hệ thống, cung cấp thông tin về mỗi tài khoản như: User ID, Group ID, Home Directory, Shell…

* Gắn với file */etc/passwd* là file */etc/shadow*. Thông tin được lưu tại đây sẽ an toàn hơn so với cách lưu trong tập tin /etc/passwd do tập tin này chỉ có tài khoản root hoặc có quyền sudo mới có thể truy cập.

Các loại tài khoản người dùng :

* Người dùng root: có quyền cao nhất trên hệ thống Linux thực hiện quản trị hệ thống.
* Người dùng thường xuyên: để hoàn thiện những công việc thường ngày. Họ bị giới hạn trong quyền truy cập vào hệ thống và phải dùng quyền của sudoer để thực hiện những tác vụ quản trị
* Người dùng hệ thống: được tạo ra bởi hệ thống để chạy các processes hoặc daemons. Mỗi users có những files và resources riêng.
  1. **Ưu điểm:**
* Linux/Unix là hệ điều hành hỗ trợ nhiều người dùng ngay cả khi hệ thống chỉ có một người sử dụng, nó vẫn được cấu hình như là hệ thống đa người dùng, vậy nên:
  + Đảm bảo an ninh và ngăn chặn phần mềm độc hại nhờ việc các ứng dụng chạy bằng tài khoản người dùng thông thường chứ không phải với đặc quyền quản trị hệ thống.
  + Trong trường hợp hệ thống cần cho nhiều người dùng, chỉ cần tạo thêm người dùng vào hệ thống.
  + Dễ dàng sao lưu các file của người dùng vì chúng được lưu bên trong thư mục riêng của từng người dùng.
  1. **Demo**

Tạo người dùng mới:

Text

Description automatically generated

Đặt mật khẩu cho người dùng:

Text

Description automatically generated

Tạo nhóm người dùng mới:



Thêm người dùng vào nhóm:



Tạo thư mục filedemo.txt:

Graphical user interface, application, Word

Description automatically generated

Thêm quyền cho mọi người đều có quyền thực thi với filedemo.txt:



1. **So Sánh**

|  |  |
| --- | --- |
| Windows | Linux |
| Windows hỗ trợ giao diện đồ hòa dễ dàng sử dụng. | Linux thiên về dòng lệnh giúp quản lý người dùng và máy tính. |
| Có 4 loại người dùng | Có 3 loại người dùng (được nêu ở trên) |
| Window thì có các nhóm tạo sẵn   * Domain Admins: dùng cho các thành viên quản trị. * DomainUsers: nhóm người dùng miền   …. | Người dùng được lưu trong file /etc/group. Người quản trị sử dụng các câu lệnh thêm, xóa , sửa thong tin người dùng. - useradd, userdel, usermod: nhóm quản lý người dùng.   * Groupadd, groupdel, groupmod: quản lý nhóm * Passwd: thay đổi mật khẩu người dùng. |
| Bảo mật còn kém. Tin tặc có thể loại dụng quản trị của người dùng và qua trình chia sẻ tài nguyên để tấn công. | An ninh chặt, ngăn các phần mềm độc hại. Ta cần phải cẩn thận khi đăng nhập bằng root. |
| Có 4 loại kiểm soát người dùng:   * Toàn quyền kiểm soát(Full control): * Sửa(modify): cho phép đọc và suera tài nguyên. * Đọc(read) : chỉ hiển thị dữ liệu thuộc tính và chủ sở hữu. * Ghi(Write): ghi dữ liệu và tài nguyện và đọc để thay đổi thuộc tính tài nguyên. | Hệ thống file cho phép cài đặt một số quyền với file:  Các quyền như đọc(r), ghi(w), thực thi(x).   * Để tang cường tính an toàn Linux/Unix cho phép cài đặt 3 kiểu đặc quyền: * Chủ sở hữu file * Nhóm sở hữu file * Người còn lại. * Thay đổi quyền thì thực hiện chown và chmod.   …. |

**Chương 3: GIÁM SÁT HOẠT ĐỘNG VÀ KIỂM TOÁN:**

1. **.Giám Sát Hoạt Động**

Đối với hai hệ điều hành Windows và hệ điều hành Linux/Unix, giám sát và tinh chỉnh hiệu năng đều là quá trình theo dõi việc vận hành của hệ thống để xác lập tiêu chuẩn cơ sở, xác định và xử lý vấn đề tiềm năng. So sánh việc giám sát và hoạt động của hai hệ điều hành ta có bảng sau:

|  |  |
| --- | --- |
| **Hệ Điều Hành Windows** | **Hệ điều hành Linux/Unix** |
| Microsoft cung cấp một số công cụ cho người quản trị theo dõi hiệu năng và việc sử dụng tài nguyên hệ thống như giám sát hiệu năng (Performance Monitor), quản lý công việc (Task Manager), giám sát tài nguyên (Resource Monitor), và xem bản ghi sự kiện (Event Viewer).  Screenshot (225) | Các file nhật ký cung cấp thông tin về tình trạng hoạt động chung của các dịch vụ và hệ thống máy chủ và được lưu trong thư mục “var/log/” như:  - syslog: nhật ký về hoạt động chung của hệ thống  - mail: nhật ký về hệ thống thư điện tử  Screenshot (234) |
| Người quản trị có thể xác định được tình trạng chung của hệ thống thông qua chương trình quản lý nhiệm vụ theo dõi thông tin.  Về chức năng, chương trình cung cấp các thông tin như sau: Mục ứng dụng, tiến trình, dịch vụ, hiệu năng, kết nối mạng, người dùng.  Có hai kiểu file nhật ký sự kiện là: Nhật ký Windows và nhật ký dịch vụ và ứng dụng: lưu lại việc sử dụng của ứng dụng cụ thể.  Với nhật ký sự kiện, người quản trị sử dụng chương trình “Event Viewer”, mỗi sự kiện chương trình sẽ đánh dấu tương ứng như sau:  - Thông tin: Thông báo thông thường về thao tác được thực hiện thành công.  - Cảnh báo: Mô tả sự kiện không nghiêm trọng nhưng cần chú ý để tránh các vấn đề xa hơn.  - Lỗi: Cho biết một lối hay vấn đề không nghiêm trọng xảy ra.  - Nghiêm trọng: Cho thấy một lỗi nghiêm trọng hay vấn đề rất đáng kể xảy ra.  - Kiểm toán thành công: Mô tả sự kiện kiểm toán an ninh thành công như yêu cầu.  - Kiểm toán thất bại: Mô tả sự kiện kiểm toán an ninh không thành công như yêu cầu. | Linux/Unix cung cấp một số công cụ cho phép theo dõi tình trạng sử dụng các tài nguyên hệ thống của các chương trình và dịch vụ qua các câu lệnh:  - ps: liệt kê các chương trình đang hoạt động và số lượng tài nguyên hệ thống chúng sử dụng  Screenshot (232)  - df: cho biết dung lượng lưu trữ đã được sử dụng trong hệ thống  Screenshot (232)  - netstat: cho biết thông tin về các cổng và các giao thức mạng đang hoạt động của hệ thống  Screenshot (233)  - Để lấy thông tin về các thao tác vào/ra, người quản trị có thể sử dụng câu lệnh *sar –b*.  Screenshot (237) |
| **Ưu điểm:**  Bằng cách sử dụng các chương trình  Performance Monitor, Task Manager, Resource Monitor, Event Viewer người quản trị có thể dễ dàng theo dõi hiệu năng và giám sát, quản lý công việc. | **Ưu điểm:**  Chỉ với thư mục“var/log/” người quản trị có thể dễ dàng giám sát hoạt động. |
| **Nhược điểm:**  Quá nhiều chương trình thực hiện chức năng giám sát máy tính cũng dễ khiến người dùng nhầm lẫn giữa các công dụng của các chương trình. | **Nhược điểm:**  - Có nhiều câu lệnh khiến người quản trị dễ nhầm lẫn giữa các câu lệnh.  - Ít thân thiện với người dùng |

1. **Kiểm Toán**

Việc kiểm toán cho phép người quản trị theo dõi cả truy nhập thực tế và cố thử truy nhập hay các sửa đổi các đối tượng và chính sách của hệ thống. Các đối tượng có thể là thư mục và file cũng như các đối tượng an ninh của hệ thống. Mục tiêu cơ bản của việc kiểm toán là đảm bảo hệ thống được vận hành một cách an toàn, giảm thiểu các rủi ro, và ứng phó một cách hữu hiệu khi có trục trặc xảy ra. Cụ thể ta có bảng so sánh:

|  |  |
| --- | --- |
| **Hệ Điều Hành Windows** | **Hệ điều hành Linux/Unix** |
| Cách chính sách kiểm toán hỗ trợ việc đảm bảo an toàn cho hệ thống, theo dõi các sửa đổi các dữ liệu nhạy cảm hay các tài khoản cần để ý:  - Đăng nhập: theo dõi việc xác thực thông tin đăng nhập  - Quản lý tài khoản: theo dõi các thao tác thay đổi tài khoản như người dùng, máy tính…  - Theo dõi chi tiết: theo dõi việc chạy chương trình, các lời gọi hàm từ xa…  - Truy nhập thư mục động: theo dõi việc truy nhập hay các chức năng của thư mục động.  - Truy nhập đối tượng: theo dõi việc truy nhập các file, thư mục hay ứng dụng. | Việc kiểm toán hệ thống cho phép người quản trị thực hiện các nhiệm vụ tiêu biểu như sau:  - Theo dõi truy nhập file và thay đổi  - Giám sát các lời gọi và chức năng hệ thống  - Phát hiện các bất thường như các tiến trình bị hỏng/ngưng.  - Các câu lệnh thực hiện bởi người dùng |
| **Ưu điểm**  Người dùng có thể dễ dàng sử dụng chương trình Group Policy Management Editor để giúp dễ dàng hiểu, triển khai, quản lý, khắc phục sự cố triển khai Group Policy, tự động hóa các hoạt động Group Policy thông qua tập lệnh. | **Ưu điểm**  Người quản trị có thể thao tác kiểm toán bằng bộ công cụ auditd được cài đặt qua câu lệnh *sudo apt-get install auditd.*  Screenshot (239) |
|  | **Nhược điểm**  - Sử dụng giao diện dòng lệnh khiến người quản trị khó nhớ được dòng lệnh.  - Cần phải cài đặt mới có thể sử dụng |

1. **TÌM HIỂU VÀ PHÂN TÍCH CÁC LOẠI LOG:**

|  |  |
| --- | --- |
| Window   1. Application log   Nhật ký ứng dụng là một tệp các sự kiện được ứng dụng phần mềm ghi lại. Nó chứa các lỗi, sự kiện thông tin và cảnh báo.  Screenshot (241)   1. Security log   Nhật ký bảo mật được sử dụng để theo dõi thông tin liên quan đến bảo mật trên hệ thống máy tính. Những ví dụ bao gồm: Nhật ký bảo mật Windows Nhật ký bảo mật tường lửa kết nối Internet  Nhật ký bảo mật Windows chứa các bản ghi hoạt động đăng nhập / đăng xuất hoặc các sự kiện liên quan đến bảo mật khác được chỉ định bởi chính sách kiểm toán của hệ thống. Kiểm toán cho phép quản trị viên cấu hình Windows để ghi lại hoạt động của hệ điều hành trong Nhật ký bảo mật.  Screenshot (242)  Windows Nhật ký bảo mật tường lửa kết nối Internet có một số loại tính năng ghi nhật ký ghi lại cách tường lửa xử lý các loại lưu lượng khác nhau. Các nhật ký này có thể cung cấp thông tin có giá trị như địa chỉ IP nguồn và đích, số cổng và giao thức,giám sát các kết nối và gói TCP và UDP bị tường lửa chặn.     1. Setup log   xem xét các sự Windows setup logs trong trình xem Windows event log viewer. Điều này cho phép dễ dàng xem lại các hành động đã xảy ra trong quá trình Thiết lập Windows và xem lại thống kê hiệu suất cho các phần khác nhau của Thiết lập Windows     1. System log   Nhật ký hệ thống (syslog) chứa bản ghi các sự kiện của hệ điều hành (OS) cho biết cách hệ thống xử lý và trình điều khiển đã được tải. Nhật ký hệ thống hiển thị các sự kiện thông tin, lỗi và cảnh báo liên quan đến hệ điều hành máy tính. Bằng cách xem xét dữ liệu có trong nhật ký, quản trị viên hoặc người dùng khắc phục sự cố hệ thống có thể xác định nguyên nhân của sự cố hoặc liệu các quy trình hệ thống có đang tải thành công hay không.     1. Forwarded events log   Windows cho phép chuyển tiếp sự kiện từ máy chủ này sang máy chủ khác và theo mặc định, sự kiện được chuyển tiếp sẽ được lưu trữ trong thư mục Windows Logs -> Forwarded Events nhưng có thể chỉ định một thư mục khác. | Linux(Ubuntu)  System logs (syslog)  Các tệp nhật ký hệ thống là cần thiết để Linux hoạt động. Riêng nó, nó chứa lượng thông tin quan trọng nhất về chức năng hệ thống.    1.messages  **/ var / log / messages** - Chứa các thông báo hệ thống toàn cầu, bao gồm các thông báo được ghi lại trong quá trình khởi động hệ thống. Có một số thứ được đăng nhập / var / log / messages bao gồm mail, cron, daemon, kern, auth, v.v.    2.boot.log  **/var/log/boot.log**: Nhật ký khởi động hệ thống (nhật ký khởi động lưu trữ tất cả thông tin liên quan đến hoạt động khởi động)    3.auth.log  **/var/log/auth.log**: Nhật ký xác thực (nhật ký xác thực lưu trữ tất cả nhật ký xác thực, bao gồm cả lần thử thành công và thất bại)    4.deamon.log  **/var/log/daemon.log**: Nhật ký daemon (nhật ký daemon chứa thông tin về các sự kiện liên quan đến việc chạy hoạt động Linux)    5.dpkg.log  **/var/log/dpkg.log/:** Liệt kê tất cả các cài đặt, nâng cấp, xóa và xóa trên hệ thống.    6.kern.log  **/var/log/kern.log**: Nhật ký hạt nhân (nhật ký hạt nhân lưu trữ thông tin từ nhân Linux Ubuntu)    7.htttpd  **/var/log/httpd/**: Nhật ký lỗi và truy cập Apache    8.mysqld.log  **/var/log/mysqld.log**: Tệp nhật ký máy chủ cơ sở dữ liệu MySQL  9.maillog  **/var/log/maillog**: Nhật ký máy chủ thư (nhật ký thư lưu trữ thông tin liên quan đến máy chủ thư và lưu trữ email)  10.debug  **/var/log/debug**: Nhật ký gỡ lỗi (nhật ký gỡ lỗi lưu trữ các thông báo chi tiết liên quan đến gỡ lỗi và hữu ích để khắc phục sự cố hoạt động hệ thống cụ thể)    11.secure  **/var/log/secure**: Chứa thông tin liên quan đến các đặc quyền xác thực và ủy quyền. Ví dụ: sshd ghi lại tất cả các tin nhắn ở đây, bao gồm cả việc đăng nhập không thành công.  12.yum.log  **/var/log/yum.log**: Chứa thông tin được ghi lại khi một gói được cài đặt bằng yum  13. alternatives.log  **/var/log/alternatives.log** : Thông tin của các lựa chọn thay thế cập nhật được đăng nhập vào tệp nhật ký này. Trên Ubuntu, các lựa chọn thay thế cập nhật duy trì các liên kết tượng trưng xác định các lệnh mặc định.    14.btmp  **/ var / log / btmp** : Tệp này chứa thông tin về các lần đăng nhập không thành công    15.user.log  **/var/log/user.log** : Chứa thông tin về tất cả nhật ký cấp người dùng    16.wtmp  **/ var / log / wtmp** hoặc **/ var / log / utmp** : Chứa các bản ghi đăng nhập. Sử dụng wtmp bạn có thể tìm ra ai đã đăng nhập vào hệ thống. lệnh ai sử dụng tệp này để hiển thị thông tin. |