

Tài liệu đọc

Hỗ Trợ Công Nghệ Thông Tin

Khóa 4: Quản trị hệ thống và dịch vụ hạ tầng CNTT

Phần 1: Tài liệu đọc bổ trợ

<u>Bài đọc 1</u>	Quản trị hệ thống
	<ul style="list-style-type: none">1.1 KVM switch<ul style="list-style-type: none">- Các loại KVM Switch- Cách dùng KVM Switch1.2 Ghi lại hành động của bạn<ul style="list-style-type: none">- Script.- Start-Transcript.- Ghi lại các phiên làm việc với đồ họa
<u>Bài đọc 2</u>	Các dịch vụ mạng và cơ sở hạ tầng
	<ul style="list-style-type: none">2.1 Hệ điều hành máy chủ<ul style="list-style-type: none">- Định nghĩa- Các ứng dụng phổ biến- Cách tính chất của hệ điều hành mạng2.2 DNS server<ul style="list-style-type: none">- BIND- PowerDNS- Unbound- Dnsmasq- Eri-DNS
<u>Bài đọc 3</u>	Dịch vụ phần mềm và nền tảng
	<ul style="list-style-type: none">3.1 Các ứng dụng chat có thu phí

	<ul style="list-style-type: none"> - Slack - Microsoft Teams - Google Chat - Discord - Mattermost
	<p>3.2 Dịch vụ in</p> <ul style="list-style-type: none"> - Máy in - Công nghệ máy in - Xem máy in của bạn - Cài đặt máy in - Máy in ảo - Chia sẻ máy in - Máy in mạng - Máy chủ máy in
	<p>3.3 Quản lý tài nguyên đám mây</p> <ul style="list-style-type: none"> - Khái niệm tài nguyên đám mây - Các thiết lập cơ sở hạ tầng đám mây tiêu chuẩn: Autoscaling, Load Balancing, monitor, alerting
Bài đọc 4	Dịch vụ thư mục
	<p>4.1 Định dạng trao đổi dữ liệu LDAP</p> <ul style="list-style-type: none"> - Định dạng bản ghi nội dung - Các công cụ sử dụng LDIF - Các trường của LDIF - Ví dụ về LDIF <p>4.2 Phạm vi nhóm</p> <ul style="list-style-type: none"> - Khi nào sử dụng các nhóm có phạm vi domain local - Khi nào sử dụng các nhóm có phạm vi global - Khi nào sử dụng các nhóm có phạm vi universal - Thay đổi phạm vi nhóm <p>4.3 Các nguyên tắc bảo mật</p> <ul style="list-style-type: none"> - Tài khoản người dùng - Nhóm bảo mật - Các công nghệ liên quan đến các nguyên tắc bảo mật <p>4.4 Các đặc trưng của EFS</p> <ul style="list-style-type: none"> - Sự riêng tư - Hoạt động minh bạch - Tích hợp với File System - Hệ thống khôi phục dữ liệu
Bài đọc 5	Phục hồi và sao lưu dữ liệu

	<p>5.1 <u>Cách giải pháp sao lưu dữ liệu</u></p> <ul style="list-style-type: none">- Chức năng Back up and restore your PC trên Windows.- Sao lưu trong máy Mac với Time Machine- Sao lưu với rsync <p>5.2 <u>Các mức độ RAID (RAID Level)</u></p> <ul style="list-style-type: none">- RAID 0- RAID 1- RAID 4- RAID 5- RAID 6
--	---

Phần 2: Hướng dẫn trả lời câu hỏi - Quiz

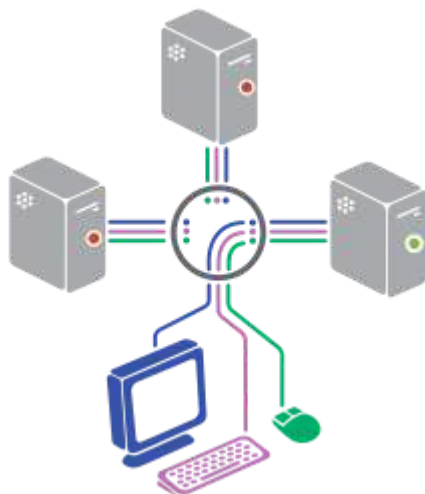
Phần 1

TÀI LIỆU ĐỌC BỔ TRỢ

Bài đọc 1: Quản trị hệ thống

1. KVM switch

KVM Switch (KVM là viết tắt của "keyboard, video and mouse" hay "bàn phím, màn hình và chuột") là một thiết bị phần cứng cho phép người dùng điều khiển nhiều máy tính từ một hoặc nhiều bộ bàn phím, màn hình và chuột.



Hình 1 - Minh họa KVM Switch. Máy tính bên phải đang được điều khiển bởi các thiết bị ngoại vi. [1]

Các loại KVM Switch

Với sự phổ biến của USB — bàn phím, chuột và thiết bị I/O kết nối USB vẫn là những thiết bị phổ biến nhất được kết nối với KVM switch. Cách phân loại KVM switch dựa trên các loại công nghệ cốt lõi khác nhau về cách KVM switch xử lý các thiết bị USB I/O — bao gồm bàn phím, chuột, màn hình cảm ứng, v.v.

USB Hub Based KVM

Còn được gọi là Enumerated KVM switch hoặc USB switch selector, thiết bị USB được kết nối, chia sẻ phải trải qua quá trình khởi tạo đầy đủ mỗi khi KVM được chuyển sang hệ thống, cổng đích khác. Việc chuyển đổi các cổng khác nhau cũng giống như bạn cắm và rút thiết bị USB vào hệ thống của mình.

KVM USB giả lập

Cổng USB console chuyên dụng được chỉ định để mô phỏng các bộ thông tin điều khiển chuyển đổi chuột hoặc bàn phím USB đặc biệt cho từng hệ thống được kết nối. USB giả lập cung cấp một hành động chuyển đổi tức thời và đáng tin cậy giúp cho các phím nóng trên bàn phím và chuột có thể chuyển đổi.

Semi-DDM USB KVM

Cổng bảng điều khiển USB chuyên dụng hoạt động với tất cả USB-HID (bao gồm cả bàn phím và chuột), nhưng không duy trì sự hiện diện của các thiết bị được kết nối với tất cả các hệ thống mục tiêu đồng thời.

DDM USB KVM

Dedicated Dynamic device. Ánh xạ các cổng USB console hoạt động với tất cả USB-HID (bao gồm cả bàn phím và chuột) và duy trì các chức năng và đặc điểm đặc biệt của thiết bị được kết nối cho từng hệ thống mục tiêu.

Sử dụng

KVM Switch là một thiết bị phần cứng, được sử dụng trong các trung tâm dữ liệu, cho phép điều khiển nhiều máy tính từ một bàn phím, màn hình và chuột (KVM). KVM Switch này cho phép nhân viên của trung tâm dữ liệu kết nối với bất kỳ máy chủ nào trong tủ rack.

Một ví dụ phổ biến về sử dụng tại nhà là cho phép sử dụng bàn phím, chuột và màn hình kích thước đầy đủ của máy PC để kết nối đến một thiết bị di động như máy tính xách tay, máy tính bảng, PDA hoặc máy tính sử dụng hệ điều hành khác.

KVM Switch khác nhau về số lượng máy tính có thể được kết nối. Cấu hình chuyển mạch truyền thống có từ 2 đến 64 máy tính có thể được gắn vào một thiết bị duy nhất. Các thiết bị cấp doanh nghiệp được kết nối với nhau thông qua phương pháp chuỗi hoặc xếp tầng có thể hỗ trợ tổng số 512 máy tính được truy cập như nhau bởi bất kỳ bảng điều khiển người dùng nhất định nào.

2. Ghi lại hành động của bạn

Trước khi thực hiện các thay đổi quan trọng trên máy tính, bạn cần phải có một kế hoạch rõ ràng về những gì sẽ làm và lưu trữ những hành động đó. Một cách làm phổ biến đối với các quản trị viên hệ thống là sử dụng hàng đợi lỗi (bug queue) hoặc hệ thống vé (ticketing system) bao gồm việc ghi nhận các lệnh được thực thi và kết quả thu được bug hoặc ticket tương ứng. Điều này được khuyến nghị nếu các lệnh cần được thực hiện ít và đơn giản.

Tuy nhiên, có những trường hợp bạn không biết chính xác lệnh nào mình sẽ cần thực hiện. Trong những trường hợp như vậy, có thể hữu ích khi sử dụng một lệnh như script cho Linux hoặc Start-Transcript cho Windows.

Script

Đối với lệnh script, có thể gọi như sau : `script session.log`

Thao tác này sẽ ghi nội dung phiên làm việc của bạn vào tập tin session.log. Khi bạn muốn dừng ghi, bạn có thể gõ exit hoặc nhấn Ctrl-D. tập tin được tạo sẽ ở định dạng ANSI bao gồm các màu được hiển thị trên màn hình. Để đọc chúng, bạn có thể sử dụng các lệnh như ansi2txt hoặc ansi2html để chuyển đổi nó thành văn bản thuần hoặc HTML tương ứng.

Start-Transcript

Đối với lệnh script, có thể gọi như sau : `Start-Transcript -Path C:\Transcript.txt`

Thao tác này sẽ ghi nội dung của phiên làm việc vào C:\Transcript.txt. Khi bạn muốn dừng ghi, bạn cần gọi Stop-Transcript. Tập tin được tạo là tập tin văn bản thuần, nơi các lệnh được thực thi và kết quả đầu ra của chúng được lưu trữ.

Ghi lại các phiên làm việc với đồ họa

Việc thực hiện các hành động quản trị hệ thống thông qua Giao diện người dùng đồ họa ít phổ biến hơn (vì khó tự động hóa và thực hiện từ xa hơn), nhưng đôi khi vẫn cần thiết.

Nếu bạn đang thực hiện một hành động cần được thực hiện bằng đồ họa và bạn muốn ghi lại những gì bạn đang làm, bạn có thể sử dụng một công cụ chuyên dụng như recordMyDesktop cho Linux hoặc các công cụ video như OBS hoặc VLC.

3. Tài liệu tham khảo

[1] https://en.wikipedia.org/wiki/KVM_switch

[2] <https://www.coursera.org/learn/system-administration-it-infrastructure-services/supplement/8Tt3K/recording-your-actions>

Bài đọc 2: Dịch vụ mạng và cơ sở hạ tầng

1. Hệ điều hành máy chủ

Hệ điều hành máy chủ là gì?

Hệ điều hành máy chủ được thiết kế để cung cấp nền tảng cho các ứng dụng mạng đa người dùng, thường xuyên, quan trọng của doanh nghiệp. Trọng tâm của các hệ điều hành mạng là: bảo mật, ổn định và cộng tác, hơn là giao diện người dùng.

Hệ điều hành máy chủ cung cấp nền tảng cho các ứng dụng nhiều người dùng và hầu hết đi kèm với một loạt các ứng dụng máy chủ phổ biến, chẳng hạn như máy chủ Web, e-mail và dịch vụ đầu cuối.

Các ứng dụng phổ biến cho hệ điều hành máy chủ

Chia sẻ tập tin và máy in: Chia sẻ tập tin liên quan đến việc thiết lập một điểm lưu trữ chung cho các tài liệu của công ty. Chia sẻ máy in cho phép nhiều máy tính sử dụng một máy in.

Dịch vụ ứng dụng (bao gồm cả cơ sở dữ liệu): khả năng chạy các ứng dụng bạn cần của hệ điều hành máy chủ rõ ràng là rất quan trọng. Máy chủ hoạt động như kho lưu trữ cơ sở dữ liệu quan trọng và môi trường chia sẻ cho các ứng dụng cộng tác

Dịch vụ trang web: Máy chủ giao thức truyền siêu văn bản (HTTP) được bao gồm trong nhiều hệ điều hành máy chủ, thông qua một ứng dụng tích hợp hoặc các ứng dụng HTTP khác như máy chủ nguồn mở Apache. Một số hệ điều hành cũng đi kèm với các tính năng nâng cao hơn, chẳng hạn như tích hợp cơ sở dữ liệu (để bạn có thể tự động xây dựng các trang Web dựa trên thông tin trong cơ sở dữ liệu), cá nhân hóa và viết kịch bản.

E-mail, phần mềm nhóm và nhắn tin: Máy chủ e-mail trung tâm cho phép bạn chuyển tiếp và nhận e-mail đến và đi từ doanh nghiệp của mình, cũng như kiểm soát các tài khoản e-mail cá nhân dựa trên một miền. Các ứng dụng phần mềm nhóm, chẳng hạn như Lotus Notes, Microsoft Exchange hoặc Novell GroupWise, cung cấp email cũng như sự cộng tác phức tạp hơn.

Dịch vụ đầu cuối: Cho phép khách hàng chạy ứng dụng làm việc trên máy chủ, đồng thời xem kết quả trực quan của ứng dụng trên màn hình của họ.

Bộ nhớ đệm (caching): Tăng tốc độ truy cập mạng (thường là truy cập Internet) bằng cách lưu trữ các tập tin đã tải xuống trước đó trong bộ nhớ đệm - giống như cách trình duyệt Internet giữ bộ nhớ cache của trang web bạn đã viếng thăm trước đây.

Cách tính chất của hệ điều hành mạng

- **Quản trị:** những công cụ nào có sẵn và sử dụng chúng dễ dàng hay không.
- **Bảo mật:** tính năng quan trọng nhất và khó đánh giá và làm đúng nhất. Nói chung, máy chủ càng thực hiện nhiều nhiệm vụ thì càng có nhiều lỗ hổng tiềm ẩn mà tin tặc xâm nhập.
- **Sự ổn định:** hạn chế downtime
- **Các tính năng:** nó có các dịch vụ cụ thể mà bạn muốn tích hợp sẵn không
- **Hiệu suất:** hệ điều hành máy chủ và nền tảng phần cứng chạy trên đó có đủ nhanh cho nhu cầu của bạn không?
- **Yêu cầu phần cứng:** hệ điều hành máy chủ có thể chạy trên phần cứng của Intel hay AMD hay nó yêu cầu một nền tảng độc quyền, ví dụ như hệ điều hành Solaris của Sun chỉ chạy trên phần cứng Sun
- **Khả năng mở rộng:** hệ điều hành có thể xử lý nhiều máy khách hơn trong tương lai hay không.
- **TCO:** chi phí phụ trợ của hệ điều hành là bao nhiêu - về năng suất, quản trị và thời gian ngừng hoạt động.
- **Ứng dụng của bên thứ ba:** những sản phẩm nào có sẵn cho các nền tảng không nằm trong bộ cơ bản có trong Hệ điều hành.

2. DNS server

Hệ thống tên miền - domain name system (DNS), có thể không phải là thứ bạn nghĩ đến hàng ngày. Tuy nhiên, DNS là một phần thiết yếu làm cho Internet có thể sử dụng được. Khi DNS hoạt động bình thường, chỉ cần nhập tên miền vào thanh URL để mở một trang web là đủ, nhưng nếu không có DNS, chúng ta phải nhập địa chỉ IP được liên kết với trang web đó để mở nó.

Các loại máy chủ DNS

Ngày nay có nhiều cách cài đặt khác nhau của hệ thống DNS. Mỗi máy chủ DNS đại diện cho việc cài đặt các đặc điểm khác nhau, chẳng hạn như giao diện, hỗ trợ nền tảng, đóng gói và các tính năng bổ sung.

BIND

BIND được thiết kế vào đầu những năm 1980 tại Đại học California Berkeley. Được viết bởi bốn sinh viên, BIND đã và vẫn được nâng cấp liên tục và thường được coi tiêu chuẩn cho các máy chủ DNS thông thường. BIND có khả năng hoạt động như một máy chủ định danh có thẩm quyền cũng như một bộ đệ quy và hỗ trợ nhiều tính năng DNS nâng cao như DNSSEC, truyền TSIG, mạng IPv6. Nó có thể được quản lý thông qua dòng lệnh hoặc bằng giao diện web. Mặc dù nó chủ yếu được sử dụng trên các hệ điều hành giống Unix, nhưng BIND ngày nay hoàn toàn đa nền tảng.

PowerDNS

PowerDNS được tạo ra vào cuối những năm 1990 tại Hà Lan và nhanh chóng trở thành một trong những nhà cung cấp phần mềm và dịch vụ DNS hàng đầu. Máy chủ được viết bằng C++ và có một cộng đồng mạnh mẽ. PowerDNS cũng có đầy đủ tính năng như BIND, nhưng được quản lý độc quyền thông qua CLI. Nhiều người chọn triển khai PowerDNS vì nó là một máy chủ DNS ổn định và mạnh mẽ đồng thời được hỗ trợ bởi cộng đồng và hỗ trợ thương mại mạnh.

Unbound

Ban đầu được viết bằng Java vào năm 2006, Unbound được viết lại bằng C bởi NLnet Labs là phần mềm máy chủ DNS hiệu suất cao vào năm 2007. Điểm mạnh của Unbound là các thành phần mô-đun của nó với các tính năng hiện đại. Unbound là một trình phân giải DNS đệ quy và do đó không có khả năng hoạt động như một máy chủ định danh có thẩm quyền, nhưng các mô-đun có sẵn cho DNSSEC và một API trình phân giải ứng dụng khách tích hợp. Unbound ban đầu được tạo ra cho các hệ điều hành giống Unix, nhưng sau đó cũng đã được chuyển sang Windows.

Dnsmasq

Dnsmasq được phát hành lần đầu tiên vào năm 2001 theo GPL. Là phần mềm miễn phí, Dnsmasq là một phần của nhiều bản phân phối Linux ngày nay. Dnsmasq chủ yếu là một trình chuyển tiếp DNS và một máy chủ DHCP được quản lý thông qua dòng lệnh. Phần mềm này nhẹ và được coi là đặc biệt dễ cấu hình. Dnsmasq được khuyến nghị cho các mạng nhỏ trên tất cả các hệ điều hành, ngoại trừ Windows.

Erl-DNS

Erl-DNS là một máy chủ định danh chính thức được viết bằng Erlang. Nó cung cấp phản hồi truy vấn rất nhanh (30-65 μ s/phản hồi) và có thể được sử dụng như một máy chủ định danh có thẩm quyền với một số kỹ thuật lưu trữ cho dữ liệu vùng. Erl-DNS cho thấy bản thân nó rất độc đáo khi được mở rộng thông qua hệ thống mô-đun của Erlang và cũng có khả năng chịu lỗi khá cao do triết lý "let it crash" của Erlang.

3. Tài liệu tham khảo

[1]https://www.pcworld.idg.com.au/article/151491/server_operating_systems/#apps

[2] <https://blog.dnsimple.com/2015/02/top-dns-servers/>

Bài đọc 3: Các dịch vụ nền tảng và phần mềm

1. Các ứng dụng chat có thu phí

Ứng dụng trò chuyện nhóm không chỉ là công cụ — chúng còn là văn phòng hiện đại. Điều đó rõ ràng đúng với các nhóm làm việc từ xa, nhưng sự hấp dẫn còn vượt xa hơn thế. Các công ty có không gian làm việc chung ngày càng phụ thuộc vào việc chat tại nơi làm việc để hoàn thành công việc.

Một phần của điều này là về hiệu quả. Nhưng các ứng dụng trò chuyện doanh nghiệp cho phép mọi người đều có thể quyết định tham gia hoặc ít nhất là xem, các cuộc trò chuyện có liên quan, đồng thời cho phép mọi người bỏ qua các tin nhắn không liên quan đến họ.

Các ứng dụng chat nhóm tốt nhất hiện nay gồm:

- Slack: một nơi làm việc hỗ trợ trò chuyện
- Microsoft Teams: cho các tổ chức lớn được chia thành các nhóm
- Google Chat for Google Workspace (trước đây là G Suite) users
- Discord: cho voice chat
- Mattermost: cho trò chuyện nhóm tự tổ chức

Slack

Hoạt động trên nền tảng: Android, iOS, Windows, Mac, Linux, Web

Slack ra mắt vào năm 2013 và nhanh chóng trở thành định nghĩa của không gian trò chuyện văn phòng, một phần không nhỏ vì mọi người yêu thích sử dụng nó.

Mỗi nhóm Slack đều có một kênh Chung dành cho toàn bộ công ty, nhưng phần lớn các cuộc trò chuyện hàng ngày xảy ra trong các kênh liên quan đến một nhóm hoặc dự án cụ thể. Người dùng quyết định kênh nào trong số những kênh này họ muốn tham gia, có nghĩa là họ có thể tránh bị ngập trong các thông báo về các dự án không liên quan đến họ

Slack cũng giúp người dùng dễ dàng tìm thấy câu trả lời bằng tính năng tìm kiếm. Bạn có thể dễ dàng lọc theo kênh, người dùng, ngày tháng, v.v.

Nhược điểm lớn nhất của Slack có thể là giá của nó. Tuy nhiên, đối với các nhóm nghiêm túc về trò chuyện tại nơi làm việc, Slack cung cấp quá nhiều giá trị đáng giá.

Giá Slack: Miễn phí cho người dùng không giới hạn, cuộc gọi 1-1 trong nhóm của bạn và lịch sử tin nhắn 10k; gói trả phí từ \$ 8/người dùng/tháng (khi trả hàng tháng) cho lịch sử không giới hạn, chia sẻ màn hình, trò chuyện nhóm và cuộc gọi điện video nhóm.

Microsoft Teams

Hoạt động trên nền tảng: Android, iOS, Windows, Mac, Web

Mọi tài khoản Microsoft Teams được liên kết với một tổ chức duy nhất, đôi khi được gọi là org, đại diện cho toàn bộ công ty của bạn. Người dùng được mời vào một hoặc nhiều nhóm trong một công ty và mọi nhóm được chia thành các kênh.

Cuộc gọi video và âm thanh là một điểm nhấn lớn. Người dùng có thể lên lịch các cuộc họp, hoàn thành chương trình làm việc hoặc bắt đầu các cuộc gọi tự phát. Ngoài ra còn có các tính năng cộng tác mở rộng, bao gồm tích hợp chặt chẽ với bộ Microsoft Office để cộng tác trên tài liệu, lịch hẹn và ghi chú.

Nhược điểm chính của MS Team là quá nhiều công việc để triển khai. Nếu bạn không có nhân viên CNTT chuyên trách, sẽ rất khó để thiết lập, đặc biệt nếu bạn đang cố gắng thiết lập phiên bản miễn phí. Tuy nhiên, nếu quy mô của tổ chức lớn, Teams là sự lựa chọn phù hợp, đặc biệt nếu nhóm của bạn đã sử dụng bộ ứng dụng của Microsoft.

Giá của Microsoft Teams: Bao gồm với Microsoft 365 Business Basic và cao hơn từ \$6/ người dùng/tháng (khi thanh toán hàng năm) cho Sharepoint, OneDrive, các phiên bản đám mây của tất cả các ứng dụng Office và trò chuyện Microsoft Teams.

Google Chat

Hoạt động trên nền tảng: Web, iOS, Android

Phần mềm chat nhóm tốt nhất cho người dùng ứng dụng Google Workspace,

Google Chat, trước đây được gọi là Google Hangouts Chat, chia nhỏ các cuộc trò chuyện thành các phòng, tương tự như các kênh trong Slack. Các cuộc trò chuyện được buộc thành chuỗi, giúp giữ mọi thứ có tổ chức. Công ty của bạn có thể thêm bao nhiêu phòng tùy thích và người dùng có thể dễ dàng tham gia và rời khỏi phòng.

Google Chat thực sự tỏa sáng là nhờ sự tích hợp với hệ sinh thái ứng dụng của Google như: Google Doc, Google Meet, Google Tasks,...

Điểm yếu của Google Chat có lẽ là thiếu tính tế. Một số việc có vẻ đơn giản, chẳng hạn như duyệt danh sách các phòng công cộng để tham gia, bị che dấu sau nhiều lần nhấp chuột vì những lý do rõ ràng.

Giá của Google Chat: Được bao gồm trong các gói Google Workspace (trước đây là G Suite) từ \$ 6/người dùng/tháng cho Gmail trên miễn tùy chỉnh của bạn, các ứng dụng Google Workspace và Google Chat.

Discord

Hoạt động trên nền tảng: Android, iOS, Windows, Mac, Web

Discord là một ngoại lệ thực sự. Ban đầu nó được xây dựng cho người chơi game và ngày nay được quảng bá cho các cộng đồng trực tuyến chứ không phải các công ty. Không có nhiều tính năng dành riêng cho doanh nghiệp và việc tích hợp phần lớn là các bot do bên thứ ba xây dựng. Nhưng Discord có thể hoạt động để trò chuyện trong công việc vì một lý do chính: âm thanh luôn bật.

Discord cung cấp các kênh văn bản, tương tự như các kênh được thấy trong các ứng dụng trò chuyện nhóm khác. Bạn có thể thêm bao nhiêu tùy thích và có thể chia nhỏ các cuộc hội thoại hơn nữa bằng cách sử dụng các chuỗi. Tuy nhiên, điểm nổi bật ở đây là các kênh thoại (audio), đây là các cuộc gọi điện thoại luôn bật, nơi bạn có thể nói chuyện với bất kỳ ai trong nhóm của mình. Bạn có thể tắt micrô, sau đó nhấn một phím để bắt đầu nói bất cứ khi nào bạn muốn tham gia.

Một điểm quan trọng khác: Discord gần như hoàn toàn miễn phí. Có một số mở rộng có tính phí, nhưng về cơ bản chúng không liên quan đến trường hợp sử dụng trong doanh nghiệp. Discord cũng cung cấp chất lượng âm thanh tốt

nhất trên thị trường và chỉ riêng tính năng này đã khiến nó đáng xem nếu bạn đang tìm kiếm một giải pháp thay thế Slack và nói chuyện bằng âm thanh là cách bạn hoàn thành công việc.

Mattermost

Hoạt động trên nền tảng: Android, iOS, Windows, Mac, Linux, Web

Một số cuộc trò chuyện quá quan trọng để lưu trữ trên máy chủ của bên thứ ba, đó là lý do Mattermost xuất hiện. Đây là một ứng dụng trò chuyện mã nguồn mở, có nghĩa là bạn có thể tải xuống và cài đặt nó trên máy chủ của chính công ty mình. Đối với một số doanh nghiệp, điều này là hoàn toàn cần thiết.

Các cuộc hội thoại được chia thành các kênh, tương tự như các dịch vụ khác. Các chủ đề được cung cấp, mặc dù mọi bài đăng trong một chủ đề cũng được đăng lên kênh chính, điều này có thể hơi lộn xộn. Chức năng tìm kiếm hoàn chỉnh, cho phép bạn lọc theo người dùng, kênh và ngày. Trò chuyện video và âm thanh được xử lý bởi các dịch vụ của bên thứ ba, một số trong số đó bạn có thể cài đặt trên máy chủ của công ty mình và tích hợp trực tiếp trong giao diện người dùng.

Mattermost có thể xem như Slack chạy trên máy chủ của riêng mình.

Giá của Mattermost: Miễn phí nếu bạn tải xuống phiên bản mã nguồn mở và cài đặt nó trên máy chủ của riêng bạn. Các gói trả phí bắt đầu từ \$ 10/người dùng/tháng.

2. Dịch vụ in

Máy in

Đôi khi bạn cần tạo một hard copy của một thứ gì đó trên máy tính. Bạn cần có khả năng chuyển nó đi xung quanh, đánh dấu nó hoặc lưu trữ thứ gì đó dưới dạng bản sao vật lý. Đây là nơi máy in xuất hiện! Máy in hoạt động theo nhiều cách khác nhau. Trong mỗi trường hợp, máy in sử dụng một số loại công nghệ in để áp dụng hình ảnh lên bề mặt in như giấy, nhựa, vải hoặc bất kỳ loại bề mặt nào mà bạn có thể tưởng tượng!

Công nghệ máy in

Theo thời gian, nhiều loại công nghệ in đã được phát triển. Dưới đây là một số loại phổ biến nhất:

Máy in phun (Inkjet printer): sử dụng các dây vòi phun rất nhỏ để phun mực lên bề mặt in. Đây là những máy in rất linh hoạt có thể in trên nhiều bề mặt khác nhau.

Máy in laser: sử dụng tia laser để vẽ hình ảnh tĩnh điện trên trống cảm quang. Hình ảnh tích điện tĩnh trên trống sẽ thu hút một chất màu dạng bột gọi là bột mực, chất này được chuyển lên giấy và được hợp nhất tại chỗ!

Máy in tác động (Impact printer): giống như một máy đánh chữ. Ví dụ, một máy in kim có một loạt các chốt nhỏ ép vào giấy thông qua một dải ruy băng có mực. Máy in kim đã từng rất thông dụng nhưng hiện nay chỉ được sử dụng trong những trường hợp đặc biệt. Một ví dụ về điều này là khi bạn cần in trên giấy carbon

Máy in nhiệt (Thermal printer): áp dụng nhiệt cho giấy có màu nhiệt đặc biệt. Giấy nhiệt màu thay đổi màu sắc khi nó được làm nóng, vì vậy máy in nhiệt không cần bất kỳ loại mực nào! Máy in nhiệt được sử dụng rất phổ biến làm máy in hóa đơn.

Máy in 3D: không áp dụng hình ảnh lên chất nền. Máy in 3D từ từ tạo lớp vật liệu nhỏ tại một thời điểm để tạo ra các vật thể 3 chiều! Có rất nhiều loại công nghệ in 3D và bạn không chỉ cần trình điều khiển mà còn cần phần mềm đặc biệt khác để xây dựng hướng dẫn cho máy in 3D cụ thể của mình.

Xem máy in của bạn

Để xem những máy in nào đã được cài đặt trong hệ điều hành của bạn, hãy điều hướng đến cài đặt máy in của hệ điều hành. Bạn cũng có thể thêm máy in mới và quản lý các máy in hiện có từ đó.

- Trong Windows, bạn đi đến một trong hai nơi, tùy thuộc vào phiên bản Windows đã cài đặt. Bạn sẽ đi tới Settings > Devices > Printers & Scanners hoặc đến Control Panel > Printers and Devices.

- Trong MacOS, điều hướng đến System Preferences > Printers & Scanners.
- Có rất nhiều tiện ích khác nhau để định cấu hình cài đặt máy in trong Linux. Hãy xem tài liệu về phiên bản Linux của bạn để biết chắc chắn. Ví dụ, đối với một bản phân phối phổ biến của Linux, Ubuntu, bạn sẽ điều hướng đến Activities > Printers.

Mỗi máy in trong hệ điều hành của bạn có một hàng đợi in hoặc ống in. Nếu bạn gửi nhiều lệnh in đến một máy in, các lệnh đó sẽ xếp hàng chờ xử lý, mỗi lần một lệnh. Các lệnh in có thể được sắp xếp lại hoặc hủy bỏ khi chúng đang ở trong hàng đợi in.

Hệ điều hành của bạn sẽ có một máy in mặc định. Nếu bạn chỉ có một máy in, thì đó sẽ là máy in mặc định. Nếu bạn có nhiều máy in được định cấu hình, thì bạn có thể chọn một máy in để sử dụng theo mặc định!

Cài đặt máy in

Máy in có thể là thiết bị khá phức tạp, với nhiều cài đặt. Có hàng chục thương hiệu máy in phổ biến và hàng nghìn kiểu máy in. Hệ điều hành của bạn có dịch vụ máy in và biết cách nói chuyện với nhiều máy in, nhưng nó có thể không biết cách nói chuyện với máy in của bạn. Hệ điều hành có **trình điều khiển thiết bị máy in** (device driver) chung sẽ hoạt động cho nhiều kiểu máy in phổ biến. Ngoài ra, các hệ điều hành chính cũng sẽ hiểu cách tìm kiếm danh mục trình điều khiển thiết bị để tìm trình điều khiển chính xác cho một máy in nhất định. Nếu hệ điều hành của bạn không tự động định vị trình điều khiển cho máy in mà bạn đang cố gắng cài đặt, thì nơi tốt nhất để tìm là trên trang web hỗ trợ của nhà sản xuất máy in. Hãy đảm bảo sử dụng đúng trình điều khiển cho hệ điều hành của bạn.

Một điều bạn có thể nhận thấy khi xem trình điều khiển thiết bị máy in là một số máy in có thể nói nhiều hơn một ngôn ngữ mô tả trang. Phổ biến nhất của những ngôn ngữ này là **PostScript** (PS) và **Ngôn ngữ Lệnh Máy in** (Printer Command Language - PCL). Một số máy in sẽ hoạt động tốt hơn với ngôn ngữ này so với ngôn ngữ khác. Đa số trường hợp, hãy chọn thiết lập mặc định hoặc được khuyến nghị bởi nhà sản xuất máy in. Đôi khi, các ứng dụng mà bạn đang in sẽ thích ngôn ngữ này hơn ngôn ngữ khác. Nếu máy in của bạn hỗ trợ

nhiều ngôn ngữ và không in được một số tài liệu nhất định hoặc không in được từ một số ứng dụng nhất định, bạn có thể thử một ngôn ngữ khác.

Máy in ảo

Bạn sẽ làm gì nếu có một tài liệu quan trọng mà bạn muốn lưu lại nhưng lại không cần đến một bản giấy? Bạn có thể sử dụng một máy in ảo. Máy in ảo là một trình điều khiển máy in trông giống như một máy in thực với hệ điều hành, nhưng thay vì in lệnh in ra giấy, nó sẽ tạo ra một tập tin! Máy in ảo có các tên như "Print to PDF" hoặc "Print to File". Bạn có thể sử dụng máy in ảo để tạo các tài liệu như tập tin PDFs hoặc tập tin XPS hoặc bất kỳ loại tập tin hình ảnh nào!

Chia sẻ máy in

Điều gì sẽ xảy ra nếu bạn có một máy in được gắn vào máy tính của mình và bạn muốn chia sẻ máy in đó với một người đang sử dụng một máy tính khác? Bạn có thể! Bạn có thể chia sẻ máy in của mình! Khi bạn chia sẻ máy in của mình, bạn cung cấp nó cho các máy tính khác như một máy in dùng chung. Với một máy in dùng chung, các máy tính khác sẽ gửi lệnh in qua mạng đến máy tính được gắn với máy in.

Máy in mạng

Một số máy in có thể được gắn trực tiếp vào mạng mà không cần phải chia sẻ hệ điều hành của máy tính. Đây là những máy in mạng độc lập. Bạn có thể thêm máy in mạng vào máy tính của mình theo cách tương tự như máy in chia sẻ.

Lưu ý, một số máy in mạng chứa ổ cứng hoặc bộ lưu trữ khác được sử dụng để lưu trữ các công việc trong hàng đợi in. Bộ nhớ này cuối cùng có thể giữ một số thông tin khá nhạy cảm! Đảm bảo kiểm soát quyền truy cập vào bộ nhớ này. Phá hủy bộ nhớ hoặc xóa an toàn mọi dữ liệu khỏi bộ lưu trữ này trước khi bảo dưỡng, bán hoặc vứt bỏ máy in mạng!

Máy chủ máy in

Điều gì sẽ xảy ra nếu bạn chỉ có một vài máy in và một vài người cần chia sẻ những máy in đó? Bạn có thể cần một máy chủ in! Máy chủ in hoạt động tương tự như chia sẻ máy in cục bộ, nhưng ở quy mô lớn hơn. Chúng có thể chấp nhận nhiều lệnh in cùng một lúc và sẽ xếp hàng hoặc cuộn các lệnh in để chúng có thể được xử lý từng lệnh một bởi (các) máy in.

3. Quản lý tài nguyên đám mây

Nếu bạn đang cân nhắc lưu trữ một số dịch vụ trong Đám mây, bạn sẽ cần tìm hiểu ý nghĩa của các thuật ngữ khác nhau được sử dụng để cấu hình dịch vụ.

Khi triển khai một dịch vụ lên đám mây, bạn thường sẽ tạo một số máy ảo đóng vai trò là máy chủ lưu trữ dịch vụ của bạn. Trong trường hợp thông thường, bạn sẽ bắt đầu bằng cách tạo một máy duy nhất để chạy dịch vụ, tạo cấu hình liên quan đến máy đó, xác minh rằng nó hoạt động, sau đó biến nó thành một mẫu có thể được sử dụng để tạo các máy khác khi cần thiết.

Để làm được điều này, bạn sẽ sử dụng cả **Tự động mở rộng (Autoscaling)** và **Cân bằng tải (Load Balancing)**. Tự động mở rộng nghĩa là có thể tự động tạo các phiên bản máy ảo mới khi tải tăng và tự động bỏ chúng khi tải giảm. Để thực hiện được điều này, bạn cần đảm bảo rằng các phiên bản của bạn có thể được định cấu hình hoàn toàn tự động và không có dữ liệu nào được lưu giữ trong các phiên bản đó (dữ liệu có thể được lưu trữ trong cơ sở dữ liệu hoặc trong các ổ đĩa riêng biệt).

Cân bằng tải có nghĩa là phân phối tải giữa nhiều máy chủ. Có các cách tiếp cận khác nhau để thực hiện cân bằng tải, nhưng khái niệm chính đó là có một dịch vụ cân bằng tải sẽ định tuyến lưu lượng truy cập đến các máy chủ theo cách mà mỗi máy chủ có thể phục vụ một phần người dùng, mà người dùng không nhận ra rằng họ đang kết nối với các máy chủ khác nhau. Nói cách khác, người dùng sẽ truy cập vào một địa chỉ duy nhất (ví dụ: <http://www.example.com>), địa chỉ này có thể được phục vụ bởi các máy chủ khác nhau, ở các khu vực khác nhau trên thế giới, mà người dùng không cần quan tâm đến điều đó.

Sau khi bạn đã thiết lập dịch vụ của mình để tự động mở rộng và cân bằng tải, bạn cũng sẽ muốn thiết lập **Giám sát (monitor)** và **Cảnh báo (alerting)** cho dịch vụ đó. Giám sát có nghĩa là kiểm tra xem dịch vụ có hoạt động tốt không, dịch vụ có phản hồi các truy vấn như mong đợi và không tạo ra các lỗi bất thường hay không. Cảnh báo có nghĩa là gửi cảnh báo khi mọi thứ không diễn ra như mong đợi.

Đối với một dịch vụ đơn giản, bạn có thể sử dụng tính năng giám sát đã được tích hợp sẵn bởi nhà cung cấp dịch vụ đám mây, điều này sẽ cho phép bạn kiểm tra xem phiên bản của mình có hoạt động tốt hay không, nhưng nó sẽ không đi sâu vào chi tiết về việc liệu nội dung có đang bị phục vụ một cách chính xác. Nếu dịch vụ của bạn phức tạp hơn, bạn có thể đầu tư nhiều thời gian để có thể theo dõi các thông số bổ sung của dịch vụ.

Tùy thuộc vào dịch vụ cụ thể mà bạn đang triển khai, có thể có nhiều khái niệm hơn mà bạn cần hiểu trước khi thực sự có thể thực hiện nó. Bạn nên đọc tài liệu được cung cấp bởi nhà cung cấp đám mây mà bạn đã chọn để tìm ra những gì bạn cần làm.

4. Tài liệu tham khảo

[1] <https://zapier.com/blog/best-team-chat-app/>

[2] <https://www.coursera.org/learn/system-administration-it-infrastructure-services/supplement/4YiCM/managing-cloud-resources>

[3] <https://www.coursera.org/learn/system-administration-it-infrastructure-services/supplement/Ne1xo/supplemental-reading-for-print-services>

Bài đọc 4: Các dịch vụ thư mục

1. Định dạng trao đổi dữ liệu LDAP

Định dạng trao đổi dữ liệu LDAP (LDAP Data Interchange Format - LDIF) là định dạng trao đổi dữ liệu văn bản thuần tiêu chuẩn để thể hiện nội dung thư mục Giao thức truy cập thư mục hạng nhẹ (LDAP) và các yêu cầu cập nhật. LDIF truyền tải nội dung thư mục dưới dạng một tập hợp các bản ghi, một bản ghi cho mỗi đối tượng (hoặc mục nhập). Nó cũng đại diện cho các yêu cầu cập nhật, chẳng hạn như Thêm, Sửa đổi, Xóa và Đổi tên, dưới dạng một tập hợp các bản ghi, một bản ghi cho mỗi yêu cầu cập nhật.

LDIF được thiết kế vào đầu những năm 1990 bởi Tim Howes, Mark C. Smith và Gordon Good tại Đại học Michigan. LDIF đã được cập nhật và mở rộng vào cuối những năm 1990 để sử dụng với Phiên bản 3 của LDAP. Phiên bản mới hơn của LDIF này được gọi là phiên bản 1 và được chỉ định chính thức trong RFC 2849, một RFC theo dõi tiêu chuẩn IETF. RFC 2849 được tác giả bởi Gordon Good và được xuất bản vào tháng 6 năm 2000. Nó hiện là một Tiêu chuẩn Đề xuất.

Một số phần mở rộng cho LDIF đã được đề xuất trong những năm qua. Một phần mở rộng đã được IETF chính thức chỉ định và xuất bản. RFC 4525 tạo ra bởi Kurt Zeilenga, đã mở rộng LDIF để hỗ trợ phần mở rộng LDAP Modify-Increment. Các phần mở rộng bổ sung sẽ được IETF công bố trong tương lai.

Định dạng bản ghi nội dung

Mỗi bản ghi nội dung được biểu diễn dưới dạng một nhóm thuộc tính, với các bản ghi được phân tách với nhau bằng các dòng trống. Các thuộc tính riêng lẻ của một bản ghi được biểu diễn dưới dạng các dòng logic đơn (được biểu diễn dưới dạng một hoặc nhiều đường vật lý thông qua cơ chế gấp dòng), bao gồm các cặp "tên: giá trị". Dữ liệu giá trị không nằm trong tập con di động của các ký tự ASCII được đánh dấu bằng ':' sau tên thuộc tính và được mã hóa thành ASCII bằng cách sử dụng mã hóa base64. Định dạng bản ghi nội dung là một tập hợp con của loại Thông tin Thư mục Internet RFC 2425.

Các công cụ sử dụng LDIF

- Các tiện ích OpenLDAP bao gồm các công cụ để xuất dữ liệu từ máy chủ LDAP sang bản ghi nội dung LDIF (ldapsearch), nhập dữ liệu từ bản ghi nội dung LDIF vào máy chủ LDAP (ldapadd) và áp dụng bản ghi thay đổi LDIF cho máy chủ LDAP (ldapmodify).
- LDIF là một trong những định dạng để nhập và xuất dữ liệu số địa chỉ trong Netscape Communicator và trong Bộ ứng dụng hỗ trợ Mozilla .
- Microsoft Windows 2000 Server và Windows Server 2003 bao gồm một công cụ dòng lệnh dựa trên LDIF có tên là LDIFDE để nhập và xuất thông tin trong Active Directory.
- JXplorer là một ứng dụng java mã nguồn mở đa nền tảng có thể duyệt và chỉnh sửa cơ bản các tập tin LDIF.

Các trường của LDIF

dn - distinguished name (Tên phân biệt). Trường này đề cập đến tên xác định duy nhất một mục nhập trong thư mục.

dc - domain component (Thành phần miền). Trường này đề cập đến từng thành phần của miền. Ví dụ: www.mydomain.com sẽ được viết là DC = www, DC = mydomain, DC = com

ou - organizational unit (đơn vị tổ chức). Trường này đề cập đến đơn vị tổ chức (hoặc đôi khi là nhóm người dùng) mà người dùng là thành viên. Nếu người dùng là một phần của nhiều nhóm, bạn có thể chỉ định, ví dụ: OU = Luật sư, OU = Thẩm phán.

cn - common name (tên gọi chung). Trường này đề cập đến đối tượng cá nhân (tên người; phòng họp; tên công thức nấu ăn; chức danh công việc; v.v.) cho đối tượng mà bạn đang truy vấn.

Ví dụ về LDIF

Đây là một ví dụ về một mục nhập thư mục đơn giản với một số thuộc tính, được biểu diễn dưới dạng bản ghi trong LDIF:

```
dn: cn=The Postmaster,dc=example,dc=com
objectClass: organizationalRole
cn: The Postmaster
```

Đây là ví dụ về bản ghi LDIF sửa đổi nhiều thuộc tính có giá trị đơn cho hai mục nhập thư mục khác nhau (định dạng này được sử dụng bởi công cụ LDIFDE của Microsoft):

```
dn: CN=John Smith,OU=Legal,DC=example,DC=com
changetype: modify
replace: employeeID
employeeID: 1234
-
replace: employeeNumber
employeeNumber: 98722
-
replace: extensionAttribute6
extensionAttribute6: JSmith98
-

dn: CN=Jane Smith,OU=Accounting,DC=example,DC=com
changetype: modify
replace: employeeID
employeeID: 5678
-
replace: employeeNumber
employeeNumber: 76543
-
replace: extensionAttribute6
extensionAttribute6: JSmith14
-
```

Lưu ý: ký tự "-" giữa mỗi lần thay đổi thuộc tính là bắt buộc. Mỗi mục nhập thư mục kết thúc bằng dấu "-" theo sau là một dòng trống. Dấu "-" cuối cùng được yêu cầu bởi công cụ LDIFDE của Microsoft, nhưng không cần thiết đối với hầu hết các triển khai ldif.

Đây là ví dụ về tập tin LDIF thêm số điện thoại cho người dùng hiện có:

```
dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
changetype: modify
```



```
add: telephonenumber
telephonenumber: +1 415 555 0002
```

2. Phạm vi nhóm:

Bất kỳ nhóm nào, cho dù đó là nhóm bảo mật hay nhóm phân phối, được đặc trưng bởi một phạm vi xác định mức độ mà nhóm được áp dụng trong miền của cây hoặc rừng. Ranh giới hoặc phạm vi tiếp cận của phạm vi nhóm cũng được xác định bởi cài đặt cấp chức năng miền của miền mà nhóm đó cư trú. Có ba phạm vi nhóm: **phổ quát (universal)**, **toàn cầu (global)** và **miền cục bộ (domain local)**.

Bảng sau đây mô tả sự khác biệt giữa các phạm vi của mỗi nhóm:

Phạm vi nhóm	Nhóm có thể bao gồm các thành viên...	Nhóm có thể được chỉ định quyền trong...	Phạm vi nhóm có thể được chuyển đổi thành...
Universal	<ul style="list-style-type: none"> Tài khoản từ bất kỳ miền nào trong rừng mà Nhóm Universal này cư trú Các nhóm Global từ bất kỳ miền nào trong rừng mà Nhóm Universal này cư trú Nhóm Universal từ bất kỳ miền nào trong rừng mà Nhóm Universal này cư trú 	Bất kỳ miền hoặc rừng nào	<ul style="list-style-type: none"> Domain local Global (miền là không có nhóm universal nào khác tồn tại với tư cách là thành viên)
Global	<ul style="list-style-type: none"> Các tài khoản từ cùng một miền với nhóm global cha Nhóm global từ cùng một miền với nhóm global cha 	Quyền thành viên có thể được chỉ định trong bất kỳ miền nào	Universal (miền là nó không phải là thành viên của bất kỳ nhóm)

			global nào khác)
Domain local	<ul style="list-style-type: none"> Tài khoản từ bất kỳ miền nào Nhóm global từ bất kỳ miền nào Nhóm universal từ bất kỳ miền nào Nhóm Domain local nhưng chỉ từ cùng một miền với nhóm Domain local cha 	Quyền thành viên chỉ có thể được chỉ định trong cùng một miền với nhóm Domain local cha	Universal (miền là không có nhóm domain local nào khác tồn tại với tư cách là thành viên)

Khi nào sử dụng các nhóm có phạm vi domain local

Các nhóm có phạm vi domain local giúp bạn xác định và quản lý quyền truy cập vào các tài nguyên trong một miền duy nhất. Ví dụ: để cấp cho năm người dùng quyền truy cập vào một máy in cụ thể, bạn có thể thêm tất cả năm tài khoản người dùng trong danh sách quyền của máy in. Tuy nhiên, nếu sau này bạn muốn cấp cho năm người dùng quyền truy cập vào một máy in mới, bạn phải chỉ định lại tất cả năm tài khoản trong danh sách quyền cho máy in mới.

Bạn có thể đơn giản hóa tác vụ quản trị thông thường này bằng cách tạo một nhóm với phạm vi domain local và gán quyền truy cập vào máy in cho nhóm đó. Đặt năm tài khoản người dùng vào một nhóm có phạm vi global, sau đó thêm nhóm này vào nhóm có phạm vi domain local. Khi bạn muốn cấp cho năm người dùng quyền truy cập vào một máy in mới, hãy chỉ định nhóm có quyền phạm vi cục bộ miền để truy cập máy in mới. Tất cả các thành viên của nhóm có phạm vi toàn cầu sẽ tự động nhận được quyền truy cập vào máy in mới.

Khi nào sử dụng các nhóm có phạm vi global

Sử dụng các nhóm có phạm vi để quản lý các đối tượng thư mục yêu cầu bảo trì hàng ngày, chẳng hạn như tài khoản người dùng và máy tính. Bởi vì các nhóm có phạm vi toàn cầu không được sao chép bên ngoài miền riêng của họ,

bạn có thể thay đổi tài khoản trong nhóm có phạm vi toàn cầu thường xuyên mà không cần tạo lưu lượng sao chép vào danh mục chung

Mặc dù việc gán quyền và cho phép trong miền mà chúng được chỉ định, bằng cách áp dụng thống nhất các nhóm có phạm vi global trên các miền thích hợp, bạn có thể hợp nhất các tham chiếu đến các tài khoản có mục đích tương tự. Điều này đơn giản hóa và hợp lý hóa việc quản lý nhóm trên các miền. Ví dụ: trong mạng có hai miền, Europe và UnitedStates, nếu bạn có một nhóm có phạm vi toàn cầu được gọi là GLAccounting trong miền UnitedStates, hãy tạo một nhóm có tên GLAccounting trong miền Europe (trừ khi chức năng kế toán không tồn tại trong miền Europe).

Bên sử dụng nhóm global hoặc nhóm universal thay vì nhóm domain local khi bạn chỉ định quyền trên các đối tượng thư mục miền được sao chép vào danh mục chung

Khi nào sử dụng các nhóm có phạm vi universal

Sử dụng các nhóm có phạm vi universal để hợp nhất các nhóm trải dài các miền. Để thực hiện việc này, hãy thêm tài khoản vào các nhóm có phạm vi global, sau đó lồng các nhóm này vào các nhóm có phạm vi universal. Khi bạn sử dụng chiến lược này, bất kỳ thay đổi thành viên nào trong các nhóm có phạm vi global sẽ không ảnh hưởng đến các nhóm có phạm vi universal.

Ví dụ: trong một mạng có hai miền, Europe và UnitedStates và một nhóm có phạm vi global được gọi là GLAccounting trong mỗi miền, hãy tạo một nhóm có phạm vi chung được gọi là UAccounting. Các thành viên của nó có hai nhóm GLAccounting, UnitedStates\GLAccounting và Europe\GLAccounting. Sau đó, nhóm UAccounting có thể được sử dụng ở bất kỳ đâu trong doanh nghiệp. Bất kỳ thay đổi nào về tư cách thành viên của các nhóm GLAccounting riêng lẻ sẽ không gây ra sự sao chép lên nhóm UAccounting.

Thay đổi phạm vi nhóm

Khi bạn tạo một nhóm mới, theo mặc định, nhóm mới được định cấu hình là nhóm bảo mật với phạm vi global, bất kể mức chức năng miền hiện tại là bao nhiêu. Mặc dù việc thay đổi phạm vi nhóm không được phép trong các miền có mức chức năng miền hỗn hợp của Windows 2000, các chuyển đổi sau được

phép trong các miền có mức chức năng miền của Windows 2000 gốc hoặc Windows Server 2003:

- Global thành universal. Việc chuyển đổi này chỉ được phép nếu nhóm bạn muốn thay đổi không phải là thành viên của một nhóm phạm vi global khác.
- Domain local thành universal. Việc chuyển đổi này chỉ được phép nếu nhóm bạn muốn thay đổi không có nhóm domain local khác làm thành viên.
- Universal thành global. Việc chuyển đổi này chỉ được phép nếu nhóm bạn muốn thay đổi không có một nhóm universal nào khác là thành viên.
- Universal thành domain local. Không có hạn chế cho hoạt động này.

3. Các nguyên tắc bảo mật (Security Principals)

Tài khoản và Nhóm bảo mật

Các tài khoản và nhóm bảo mật được tạo trong miền Active Directory là các đối tượng thư mục và chúng có thể được sử dụng để quản lý quyền truy cập vào tài nguyên miền.

Tài khoản người dùng cục bộ và nhóm bảo mật được tạo trên máy tính cục bộ và chúng có thể được sử dụng để quản lý quyền truy cập vào tài nguyên trên máy tính đó. Tài khoản người dùng cục bộ và nhóm bảo mật được Trình quản lý tài khoản bảo mật (Security Accounts Manager - SAM) lưu trữ và quản lý trên máy tính cục bộ.

Tài khoản người dùng

Tài khoản người dùng nhận dạng duy nhất một người sử dụng hệ thống máy tính, do đó cho phép hệ thống thực thi quyền thích hợp để cho phép hoặc từ chối quyền truy cập vào tài nguyên. Tài khoản người dùng có thể được tạo trong Active Directory và cả trên các máy tính cục bộ. Tài khoản người dùng được sử dụng để:

- Đại diện, xác định và xác thực danh tính của người dùng. Tài khoản người dùng cho phép người dùng đăng nhập vào máy tính và miền có danh tính duy nhất có thể được xác thực bởi máy tính hoặc miền.
- Phân quyền (cấp hoặc từ chối) quyền truy cập vào tài nguyên. Sau khi người dùng đã được xác thực, người dùng được phép (cấp hoặc từ chối) quyền

truy cập vào tài nguyên dựa trên các quyền được chỉ định cho người dùng đó trên tài nguyên.

Nhóm bảo mật

Nhóm bảo mật là một tập hợp các tài khoản người dùng, tài khoản máy tính và các nhóm khác có thể được quản lý như một đơn vị duy nhất từ góc độ bảo mật. Các nhóm có thể dựa trên Active Directory hoặc cục bộ cho một máy tính cụ thể. Trong Windows Server 2003, có một số nhóm bảo mật tích hợp được cấu hình sẵn với các quyền và quyền thích hợp để thực hiện các tác vụ cụ thể. Ngoài ra, bạn có thể tạo một nhóm bảo mật cho từng tổ hợp yêu cầu bảo mật duy nhất áp dụng cho nhiều người dùng trong tổ chức của bạn.

Bạn sử dụng các nhóm trong Active Directory để quản lý quyền đối với tài nguyên miền.

Nhóm cục bộ tồn tại trong cơ sở dữ liệu SAM trên máy tính cục bộ (trên tất cả các máy tính chạy Windows) ngoại trừ bộ điều khiển miền. Bạn sử dụng các nhóm cục bộ để quản lý các quyền và quyền chỉ đối với các tài nguyên trên máy tính cục bộ.

Sử dụng nhóm bảo mật để quản lý kiểm soát truy cập giải quyết các vấn đề sau. Sử dụng các nhóm bảo mật:

- Đơn giản hóa việc quản trị. Bạn có thể chỉ định một nhóm quyền chung cho nhiều tài khoản cùng một lúc, thay vì chỉ định chúng cho từng tài khoản riêng lẻ. Ngoài ra, khi người dùng chuyển công việc hoặc rời khỏi tổ chức, quyền không bị ràng buộc với tài khoản người dùng của họ, giúp việc chuyển lại hoặc xóa quyền dễ dàng hơn.
- Cho phép bạn triển khai mô hình kiểm soát truy cập dựa trên vai trò để cấp quyền bằng cách sử dụng các nhóm có phạm vi khác nhau (cục bộ, toàn cục, miền cục bộ và phổ quát) cho các mục đích thích hợp.
- Giảm thiểu kích thước của danh sách kiểm soát truy cập (ACL) và tăng tốc độ kiểm tra bảo mật. Một nhóm bảo mật có SID riêng; do đó, SID nhóm có thể được sử dụng để chỉ định quyền cho một tài nguyên. Trong môi trường có hơn vài nghìn người dùng, nếu SID của các tài khoản người dùng cá nhân được sử dụng để chỉ định quyền truy cập vào một tài nguyên, thì ACL của tài nguyên

đó có thể trở nên lớn không thể quản lý và cần thời gian để hệ thống kiểm tra quyền đối với tài nguyên có thể trở nên không thể chấp nhận được.

Các công nghệ liên quan đến các nguyên tắc bảo mật

Các nguyên tắc bảo mật có liên quan chặt chẽ đến các thành phần và công nghệ sau trong Windows Server 2003.

Các thành phần kiểm soát quyền truy cập và ủy quyền

- **SID.** Mỗi nguyên tắc bảo mật được tự động gán một SID khi nó được tạo.
- **Mã thông báo truy cập (Access Tokens).** Sau khi người dùng đăng nhập và được xác thực, hệ thống sẽ tạo mã thông báo truy cập cho người dùng chứa SID của người dùng, SID của tất cả miền và nhóm bảo mật cục bộ mà người dùng là thành viên và một số SID nổi tiếng. Mọi quy trình mà người dùng tạo đều kế thừa mã thông báo truy cập của người dùng, mã này sau đó được sử dụng để xác định xem có cấp cho người dùng đó quyền truy cập vào tài nguyên hệ thống trong một phiên đăng nhập nhất định hay không.
- **Bộ mô tả bảo mật và ACL.** Bộ mô tả bảo mật là một cấu trúc dữ liệu được liên kết với từng đối tượng bảo mật. Bộ mô tả bảo mật chứa danh sách kiểm soát truy cập tùy ý (discretionary access control list - DACL), với các SID cho người dùng và các nhóm được phép hoặc bị từ chối quyền truy cập vào đối tượng đó.
- **Quyền hạn.** Quyền truy cập các đối tượng bảo mật như đối tượng Active Directory, tập tin và cài đặt sổ đăng ký được cấp cho các nguyên tắc bảo mật.

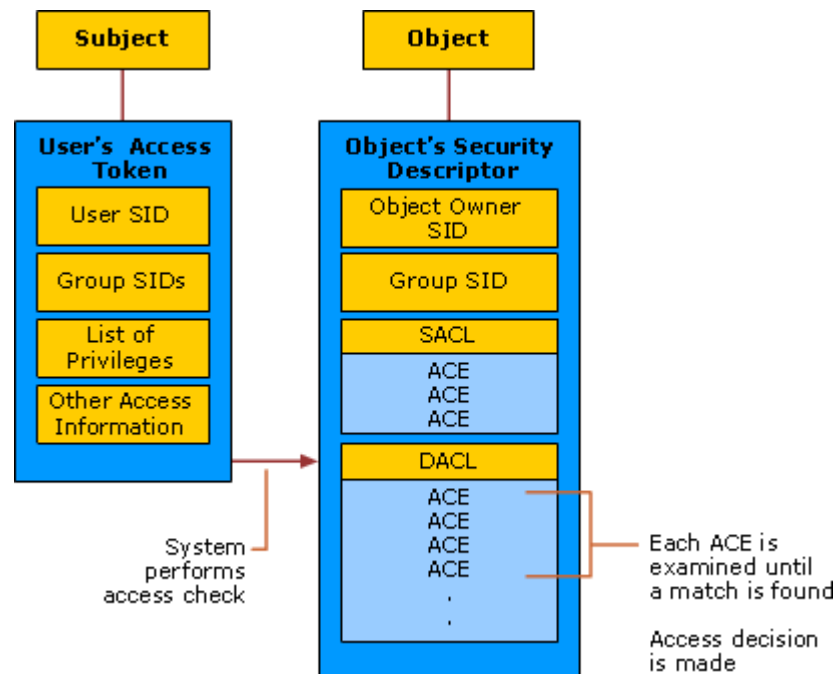
Authentication

Tài khoản người dùng cho phép người dùng đăng nhập vào máy tính và miền có danh tính có thể được xác thực bởi máy tính hoặc miền.

Active Directory

Các tài khoản và nhóm bảo mật được tạo trong miền Active Directory được lưu trữ trong cơ sở dữ liệu Active Directory và được quản lý bằng các công cụ Active Directory.

Sơ đồ sau đây cho thấy quy trình kiểm soát truy cập và ủy quyền Windows Server 2003. Trong sơ đồ này, chủ đề (một chuỗi trong một quy trình do người dùng bắt đầu) cố gắng truy cập một đối tượng, chẳng hạn như một thư mục được chia sẻ. Thông tin trong mã thông báo truy cập của người dùng được so sánh với các mục nhập kiểm soát truy cập (ACE) trong bộ mô tả bảo mật của đối tượng và quyết định truy cập được đưa ra. SID của các nguyên tắc bảo mật được sử dụng trong mã thông báo truy cập người dùng và trong ACE của bộ mô tả bảo mật của đối tượng.



4. Các đặc trưng của EFS

EFS cung cấp cho người dùng **quyền riêng tư, hoạt động minh bạch** và **phương tiện khôi phục dữ liệu**. Ngoài ra, nó đảm bảo rằng mã hóa không vô tình bị đánh bại bởi việc sao chép hoặc di chuyển tập tin.

Sự riêng tư

EFS được thiết kế để bảo vệ quyền riêng tư của dữ liệu nhạy cảm. Ngoài người dùng mã hóa tập tin, chỉ những nhân viên khôi phục được chỉ định mới có thể giải mã tập tin đó. Các tài khoản hệ thống khác có quyền đối với tập tin

đó - ngay cả quyền Sở hữu - không thể mở tập tin mà không có khóa riêng của người mã hóa.

EFS đặc biệt hữu ích để bảo mật dữ liệu nhạy cảm trên máy tính được chia sẻ bởi một số người dùng và trên máy tính xách tay. Cả hai loại hệ thống đều dễ bị tấn công bởi các kỹ thuật phá vỡ các hạn chế của danh sách kiểm soát truy cập (access control lists - ACL) Trong một hệ thống dùng chung, có thể đạt được quyền truy cập bằng cách khởi động một hệ điều hành khác. Với một chiếc máy tính xách tay, kẻ trộm có thể chỉ mất một lúc để lấy trộm nó. Sau đó, kẻ trộm có thể tháo ổ đĩa cứng, cắm ổ đĩa cứng vào máy tính khác và đọc các tập tin. Tuy nhiên, các tập tin EFS xuất hiện dưới dạng các ký tự khó hiểu khi kẻ trộm không có khóa giải mã.

Hoạt động minh bạch

Trong EFS, mã hóa tập tin không yêu cầu chủ sở hữu tập tin phải giải mã và mã hóa lại tập tin trong mỗi lần sử dụng. Quá trình giải mã và mã hóa tập tin diễn ra minh bạch khi nó được đọc và ghi vào đĩa.

Ngược lại, các dịch vụ mã hóa trong hầu hết các sản phẩm không minh bạch đối với người dùng. Người dùng phải giải mã tập tin trước mỗi lần sử dụng và mã hóa lại khi hoàn tất. Nếu người dùng quên mã hóa một tập tin, tập tin đó sẽ không được bảo vệ. Và, bởi vì người dùng phải gặp rắc rối khi chỉ định rằng một tập tin được mã hóa và giải mã trong mỗi lần sử dụng, nên nó không khuyến khích việc sử dụng mã hóa.

Tích hợp với File System

EFS được tích hợp chặt chẽ với NTFS. Bạn đặt thuộc tính mã hóa cho các thư mục hoặc tập tin khi bạn đặt các thuộc tính khác, chẳng hạn như chỉ đọc, nén hoặc ẩn. Khi mã hóa được đặt cho một thư mục, EFS sẽ tự động mã hóa những điều sau:

- Tất cả các tập tin mới được tạo trong thư mục
- Tất cả các tập tin văn bản thuần đã được sao chép vào thư mục
- Tùy chọn, tất cả các tập tin và thư mục con hiện có trong thư mục

Khi EFS được triển khai ở cấp thư mục, các bản sao tạm thời của tập tin được mã hóa trong cùng một thư mục (chẳng hạn như những tập tin được tạo trong quá trình chỉnh sửa) cũng được mã hóa, cũng như các bản sao lưu được tạo trong cùng một thư mục. Mã hóa vẫn tồn tại khi di chuyển và đổi tên, với điều kiện tất cả các tập tin đều nằm trên ổ đĩa NTFS của Windows 2000.

Hệ thống khôi phục dữ liệu

Việc mã hóa một tập tin luôn làm tăng nguy cơ không thể đọc lại được. Chủ sở hữu khóa cá nhân có thể rời khỏi doanh nghiệp. Nếu không hài lòng, chủ sở hữu có thể mã hóa tất cả các tập tin của mình một cách ác ý trước khi rời đi. Tệ hơn nữa, người đó có thể mã hóa các tập tin được chia sẻ quan trọng để không ai khác có thể sử dụng chúng. Vì lý do này, EFS được thiết kế để chỉ được sử dụng nếu hệ thống được cấu hình với một hoặc nhiều quản trị viên tác nhân khôi phục.

Tài khoản người dùng được chỉ định, được gọi là tài khoản recovery agent > được cấp chứng chỉ tác nhân khôi phục với các khóa công khai và khóa riêng được sử dụng cho các hoạt động khôi phục dữ liệu EFS. Tài khoản tác nhân khôi phục được chỉ định bởi chính sách khôi phục của EFS. Theo mặc định, tài khoản tác nhân khôi phục là tài khoản Quản trị viên cấp cao nhất. Trên một máy tính độc lập, đây là Quản trị viên cục bộ. Trong miền, quản trị viên miền cho bộ điều khiển miền đầu tiên được cài đặt trong miền là tài khoản tác nhân khôi phục mặc định cho tất cả các máy tính trong miền. Các tài khoản tác nhân khôi phục khác nhau có thể được chỉ định bằng cách thay đổi chính sách khôi phục EFS và các chính sách khôi phục khác nhau có thể được định cấu hình cho các bộ phận khác nhau của doanh nghiệp. Khóa riêng tư cho tài khoản tác nhân khôi phục phải được đặt trên máy tính nơi các hoạt động khôi phục sẽ được tiến hành.

Khi chứng chỉ tác nhân khôi phục được cấp, chứng chỉ và khóa cá nhân được cài đặt trong hồ sơ người dùng cho tài khoản người dùng đã yêu cầu chứng chỉ. Bạn cũng có tùy chọn xuất chứng chỉ tác nhân khôi phục và khóa cá nhân để lưu trữ chúng trong kho lưu trữ hoặc chuyển chứng chỉ và khóa cá nhân sang tài khoản người dùng và máy tính khác.

Có thể có nhiều tài khoản tác nhân khôi phục cho một tập tin EFS, mỗi tài khoản có một khóa riêng tư khác nhau. Khôi phục dữ liệu chỉ tiết lộ dữ liệu được mã hóa, không tiết lộ khóa riêng tư của người dùng đã được sử dụng để mã hóa khóa mã hóa hàng loạt hoặc bất kỳ khóa riêng tư nào khác để khôi phục. Điều này đảm bảo rằng không có thông tin cá nhân nào khác vô tình bị tiết lộ cho quản trị viên tác nhân khôi phục.

Nếu bạn chọn định cấu hình chính sách khôi phục EFS mà không có chứng chỉ tác nhân khôi phục, thì EFS sẽ bị vô hiệu hóa. Do tính năng này, thông thường bạn không thể sử dụng EFS để mã hóa dữ liệu nên không thể khôi phục dữ liệu - cho dù việc mã hóa được thực hiện do vô tình hay do ác ý. Tuy nhiên, sau đó bạn có thể hủy khóa cá nhân để khôi phục để ngăn việc khôi phục dữ liệu.

5. Tài liệu tham khảo

- [1] https://en.wikipedia.org/wiki/LDAP_Data_Interchange_Format
- [2] [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s-server-2003/cc755692\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s-server-2003/cc755692(v=ws.10)?redirectedfrom=MSDN)
- [3] [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s-server-2003/cc780957\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s-server-2003/cc780957(v=ws.10)?redirectedfrom=MSDN)
- [4] [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s-2000-server/cc962100\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s-2000-server/cc962100(v=technet.10)?redirectedfrom=MSDN)

Bài đọc 5: Phục hồi và sao lưu dữ liệu

1. Cách giải pháp sao lưu dữ liệu

Chức năng Back up and restore your PC trên Windows

Back up

Có một số cách để sao lưu PC của bạn.

1. Chọn nút Start, sau đó chọn **Control Panel > System and Maintenance > Backup and Restore**.

2. Làm một điều trong số sau đây:

- Nếu bạn chưa từng sử dụng Windows Backup trước đây hoặc gần đây đã nâng cấp phiên bản Windows của mình, hãy chọn **Set up backup**, sau đó làm theo các bước trong trình hướng dẫn.
- Nếu bạn đã tạo bản sao lưu trước đó, bạn có thể đợi bản sao lưu theo lịch định kỳ xảy ra hoặc bạn có thể tạo bản sao lưu mới theo cách thủ công bằng cách chọn **Back up Now**.
- Nếu bạn đã tạo bản sao lưu trước đó, nhưng muốn tạo bản sao lưu mới, đầy đủ thay vì cập nhật bản sao lưu cũ, hãy chọn **Create new, full backup**, sau đó làm theo các bước trong trình hướng dẫn.

Tạo ảnh hệ thống

Ảnh hệ thống chứa tất cả thông tin trên PC của bạn ở một trạng thái cụ thể. Bấm chuột phải vào nút **Start**, sau đó chọn **Control Panel > System and Maintenance > Backup and Restore**. Trong panel bên trái, chọn **Create a system image**, sau đó làm theo các bước trong trình hướng dẫn. Cần có quyền quản trị viên nếu bạn được yêu cầu nhập mật khẩu quản trị viên để xác nhận, hãy nhập mật khẩu.

Tạo điểm khôi phục (restore point)

Bạn có thể sử dụng điểm khôi phục để khôi phục các tệp tin hệ thống của máy tính về thời điểm sớm hơn. Các điểm khôi phục được System Restore tự

động tạo mỗi tuần và khi PC của bạn phát hiện thấy sự thay đổi, chẳng hạn như khi bạn cài đặt ứng dụng hoặc driver.

Cách tạo điểm khôi phục

1. Bấm chuột phải vào nút Start , sau đó chọn Control Panel > System and Maintenance > System.
2. Trong panel bên trái, chọn System protection.
3. Chọn tab System Protection, sau đó chọn Create.
4. Trong hộp thoại System Protection, nhập mô tả, sau đó chọn Create.

Phục hồi

1. Bấm chuột phải vào nút **Start**, sau đó chọn **Control Panel > System and Maintenance > Backup and Restore**.
2. Thực hiện một trong số những điều sau:
 - Để khôi phục tập tin của bạn, hãy chọn **Restore my files**.
 - Để khôi phục tập tin của tất cả người dùng, hãy chọn **Restore all users' files**.
3. Thực hiện một trong số những điều sau:
 - Để xem qua nội dung của bản sao lưu, hãy chọn **Browse for files** hoặc **Browse for folders**. Khi đang duyệt các thư mục, bạn sẽ không thể thấy các tập tin riêng lẻ trong một thư mục. Để xem các tập tin riêng lẻ, hãy sử dụng tùy chọn **Browse for files**.

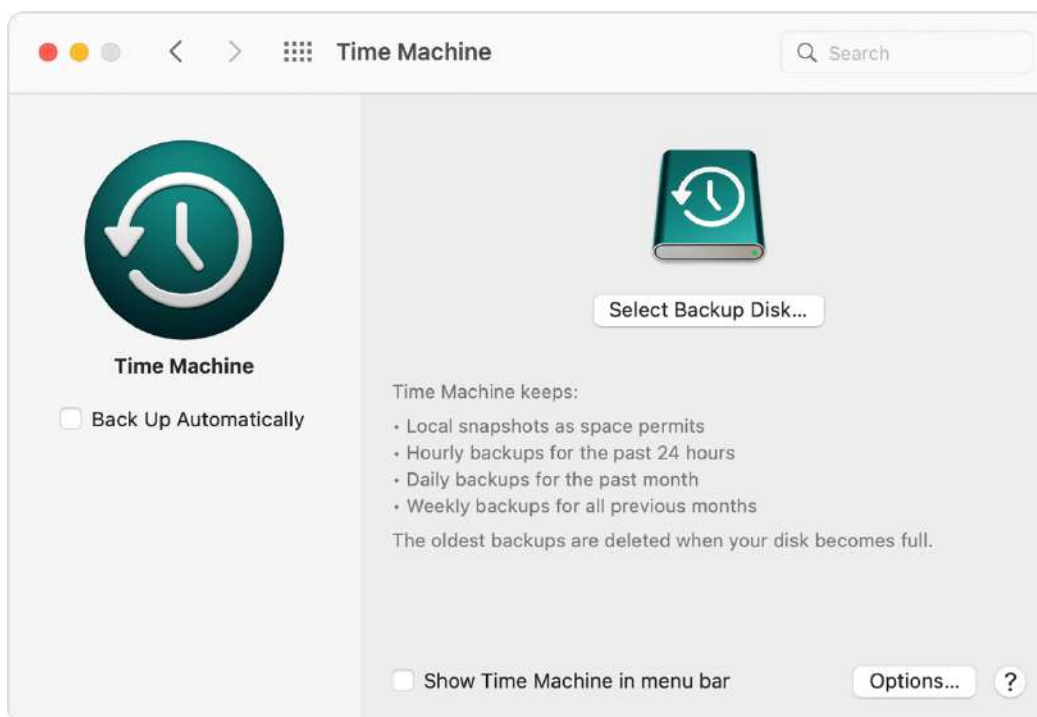
Để tìm kiếm nội dung của bản sao lưu, hãy chọn **Search**, nhập tất cả hoặc một phần của tên tập tin, sau đó chọn **Search**.

Sao lưu trong máy Mac với Time Machine

Sử dụng Time Machine, tính năng sao lưu tích hợp của máy Mac, để tự động sao lưu dữ liệu cá nhân, bao gồm ứng dụng, nhạc, ảnh, email và tài liệu. Có một bản sao lưu cho phép bạn khôi phục các tập tin mà sau này bạn xóa hoặc không thể truy cập

Tạo bản sao lưu Time Machine

1. Kết nối thiết bị lưu trữ bên ngoài, chẳng hạn như USB hoặc ổ Thunderbolt.
2. Mở tùy chọn Time Machine từ menu Time Machine trong thanh menu. Hoặc chọn menu Apple > System Preferences, sau đó nhấp vào Time Machine.
3. Chọn Select Backup Disk



4. Chọn tên đĩa của bạn, sau đó nhấp vào Use Disk. Time Machine ngay lập tức bắt đầu thực hiện sao lưu định kỳ — tự động và bạn không cần thực hiện thêm hành động nào.

Nếu bạn muốn bắt đầu sao lưu theo cách thủ công mà không cần đợi đến lần sao lưu tự động tiếp theo, hãy chọn Back Up Now từ menu Time Machine trên thanh menu.

Sử dụng cùng một menu để kiểm tra trạng thái của một bản sao lưu hoặc bỏ qua một bản sao lưu đang được tiến hành. Ví dụ: nếu một quá trình sao lưu đang được tiến hành, menu sẽ hiển thị mức độ hoàn thành của quá trình đó. Khi chưa tiến hành sao lưu, menu hiển thị ngày và giờ của bản sao lưu mới nhất.

Sao lưu với rsync

rsync là một tiện ích mã nguồn mở cung cấp khả năng truyền tập tin gia tăng nhanh chóng (incremental file transfer)

Cài đặt

Trước hết cần cài đặt gói [rsync](#)

Tự động sao lưu

Trong ví dụ này, tập lệnh được tạo trong thư mục `/etc/cron.daily` và sẽ được chạy hàng ngày nếu một daemon cron được cài đặt và định cấu hình đúng cách. Cấu hình và sử dụng cron nằm ngoài phạm vi của bài viết này.

Đầu tiên, hãy tạo một tập lệnh chứa các tùy chọn lệnh thích hợp:

<code>/etc/cron.daily/backup</code>
<code>#!/bin/sh</code>
<code>rsync -a --delete --quiet /path/to/backup /location/of/backup</code>

`-a`: cho biết rằng các tập tin nên được lưu trữ, có nghĩa là hầu hết các đặc tính của chúng được giữ nguyên (nhưng không phải ACL, liên kết cứng hoặc các thuộc tính mở rộng như khả năng)

`--delete`: có nghĩa là các tập tin bị xóa trên nguồn cũng sẽ bị xóa trên bản sao lưu

Cuối cùng cần thực thi file script trên

Tự động sao lưu với SSH

Nếu thực hiện sao lưu với SSH, dùng đoạn script sau

<code>/etc/cron.daily/backup</code>
<code>#!/bin/sh</code>
<code>rsync -a --delete --quiet -e ssh /path/to/backup</code>
<code>remoteuser@remotehost:/location/of/backup</code>

-e ssh: chỉ dẫn rsync sử dụng SSH

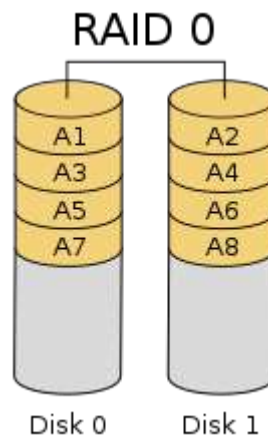
remoteuser: là người dùng trên máy chủ từ xa

-a: nhóm tất cả các tùy chọn này -rlptgoD (recursive, links, perms, times, group, owner, devices)

2. Các mức độ RAID (RAID Level)

Các mức độ RAID bao gồm một bộ cấu hình RAID cơ bản (redundant array of independent disks) sử dụng các kỹ thuật phân dải (stripping), sao chép (mirroring) hoặc chẵn lẻ (parity) để tạo ra các kho lưu trữ dữ liệu đáng tin cậy lớn từ nhiều ổ đĩa cứng máy tính đa dụng

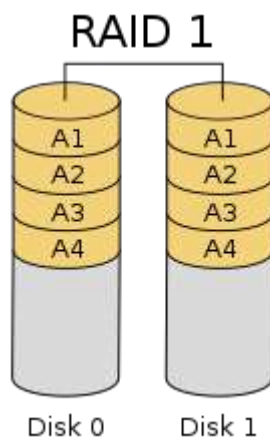
RAID 0



Hình 1 - Mô hình RAID 0 [4]

RAID 0 chia dữ liệu đồng đều trên hai hoặc nhiều đĩa mà không có thông tin chẵn lẻ, dự phòng hoặc khả năng chịu lỗi. Vì RAID 0 không cung cấp khả năng chịu lỗi hoặc dự phòng, sự cố của một ổ đĩa sẽ khiến toàn bộ mảng bị lỗi. Cấu hình này thường được triển khai để tăng tốc độ đọc ghi, nó cũng có thể được sử dụng để tăng khối lượng lưu trữ logic từ hai hoặc nhiều đĩa vật lý.

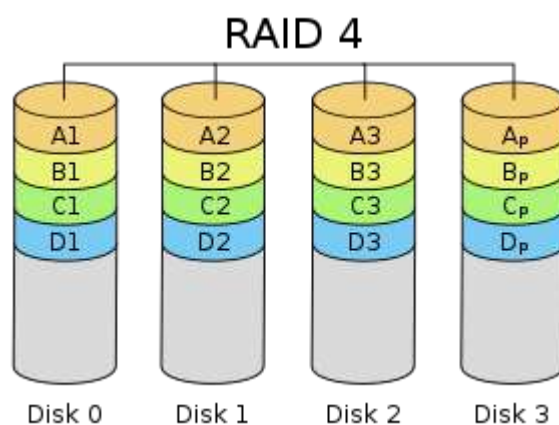
RAID 1



Hình 2 - Mô hình RAID 1[4]

RAID 1 bao gồm một bản sao chính xác của một tập hợp dữ liệu trên hai hoặc nhiều đĩa; một cặp RAID 1 được cổ điển chứa hai đĩa. Cấu hình này hữu ích khi hiệu suất đọc hoặc độ tin cậy quan trọng hơn hiệu suất ghi hoặc dung lượng lưu trữ dữ liệu kết quả

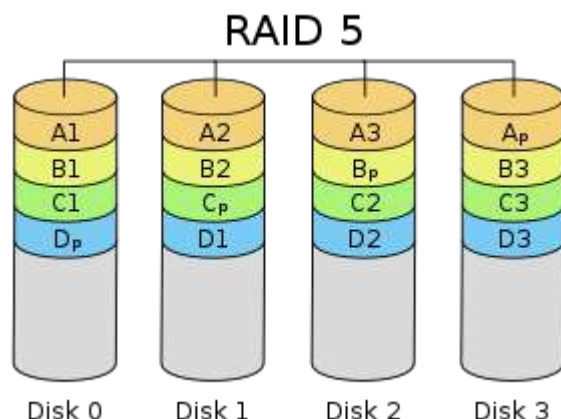
RAID 4



Hình 3-Mô hình RAID 4[4]

RAID 4 bao gồm dải cấp khối với một đĩa lưu chẵn lẻ chuyên dụng. Do bố cục của nó, RAID 4 cung cấp hiệu suất tốt khi đọc ngẫu nhiên, trong khi hiệu suất ghi ngẫu nhiên thấp do nhu cầu ghi tất cả dữ liệu chẵn lẻ vào một đĩa duy nhất

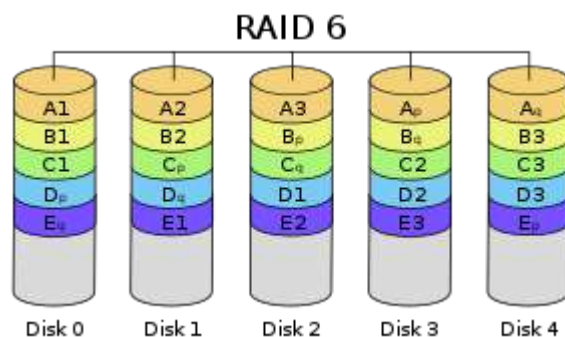
RAID 5



Hình 4- Mô hình RAID 5[4]

RAID 5 bao gồm dải cấp khối với tính chẵn lẻ phân tán. Không giống như trong RAID 4, thông tin chẵn lẻ được phân phối giữa các ổ đĩa. Nó yêu cầu tất cả các ổ đĩa trừ một ổ đĩa phải có mặt để hoạt động. Khi một ổ đĩa bị lỗi, các lần đọc tiếp theo có thể được tính toán từ tính chẵn lẻ được phân phối sao cho không có dữ liệu nào bị mất.

RAID 6



Hình 5 - Mô hình RAID 6[4]

RAID 6 mở rộng RAID 5 bằng cách thêm một khối chẵn lẻ khác; do đó, nó sử dụng dải cấp khối với hai khối chẵn lẻ được phân phối trên tất cả các đĩa thành viên

3. Tài liệu tham khảo

- [1] <https://support.microsoft.com/en-us/help/17127/windows-back-up-restore>
- [2] <https://support.apple.com/en-us/HT201250>
- [3] https://wiki.archlinux.org/index.php/rsync#As_a_backup_utility
- [4] https://en.wikipedia.org/wiki/Standard_RAID_levels

Phần 2

HƯỚNG DẪN

TRẢ LỜI CÂU HỎI

Quản trị hệ thống

Câu hỏi về quản trị viên hệ thống

1. Quản trị viên hệ thống chịu trách nhiệm cho tác vụ nào sau đây?

- A. Thiết lập tài khoản người dùng và thiết bị mới
- B. Bảo trì máy chủ
- C. Khắc phục sự cố người dùng
- D. Tất cả những điều trên

Đáp án: D

2. Yếu tố nào sau đây tạo nên cơ sở hạ tầng CNTT?

- A. Phần cứng và phần mềm
- B. Mạng
- C. Hệ điều hành
- D. Tất cả những điều trên

Đáp án: D

3. Câu nào trong số này được coi là máy chủ (server) ? Chọn tất cả các câu phù hợp.

- A. Phần mềm cung cấp dịch vụ cho các máy khác
- B. Phần mềm chỉ khả dụng cho máy tính được cài đặt trên đó
- C. Một máy tính cung cấp dịch vụ cho các máy tính khác
- D. Một phần mềm cung cấp dịch vụ cho phần mềm khác

Đáp án: A, C, D

4. KVM Switch được sử dụng để:

- A. Bộ chuyển đổi giữa nhiều máy tính sử dụng một màn hình, bàn phím và chuột

- B. Cho phép bạn nhận các kết nối SSH đến.
- C. Gắn nhiều máy chủ vào một giá đỡ máy chủ.
- D. Cho phép bạn cung cấp nội dung web cho nhiều khách hàng.

Đáp án: A

5. Phần cứng máy chủ nào trong số những phần cứng này bạn có thể xếp chồng lên nhau trong giá đỡ máy chủ?

- A. Rack
- B. Blade
- C. Tower
- D. Desktop

Đáp án: A, B

6. Với _____, bạn có thể truy cập dữ liệu của mình, sử dụng các ứng dụng và hơn thế nữa từ mọi nơi trên thế giới, miễn là bạn có kết nối Internet.

- A. Điện toán đám mây
- B. Mạng LAN
- C. Mạng PAN

Đáp án: A

7. Lợi ích của điện toán đám mây so với điện toán cục bộ là gì? Chọn tất cả các câu phù hợp.

- A. Dịch vụ có thể truy cập từ mọi nơi trên thế giới.
- B. Các bản cập nhật phần mềm được xử lý bởi công ty cung cấp dịch vụ.
- C. Điện toán đám mây có thể có các khoản phí cần phải trả trong thời gian dài.
- D. Điện toán đám mây có chi phí ban đầu nhỏ.

Đáp án: A, B, D

8. Lợi ích của điện toán cục bộ so với điện toán đám mây là gì? Chọn tất cả các câu phù hợp.

- A. Có những chi phí dài hạn tiềm ẩn liên quan đến điện toán cục bộ.
- B. Các dịch vụ được xử lý bởi một tổ chức khác, do đó, tổ chức của bạn phụ thuộc vào bên thứ ba.
- C. Bạn có toàn quyền kiểm soát cơ sở hạ tầng CNTT.
- D. Có thể tiến hành cập nhật bất cứ lúc nào.

Đáp án: C, D

Câu hỏi về các tác vụ quản trị hệ thống

1. Chính sách nào sau đây là chính sách tốt để áp dụng đối với mật khẩu? Chọn tất cả các câu phù hợp.

- A. Độ dài mật khẩu lớn
- B. Sử dụng các từ thông dụng
- C. Hỗn hợp các ký hiệu và số
- D. Độ dài mật khẩu ngắn

Đáp án: A, C

2. Cái nào trong số này là một phần của vòng đời phần cứng? Chọn tất cả các câu phù hợp.

- A. Nghỉ hưu (Retirement)
- B. Mua sắm (Procurement)
- C. Triển khai (Deployment)
- D. Kết nối mạng (Network Connectivity)

Đáp án: A, B, C

Câu hỏi tổng hợp

1. Máy đang gặp sự cố, vì vậy người dùng có trách nhiệm đưa máy đi bảo dưỡng. Kịch bản này thuộc về giai đoạn nào của vòng đời phần cứng?

- A. Procurement
- B. Deployment
- C. Maintenance
- D. Retirement

Đáp án: C

2. Bộ phận CNTT gửi đơn đặt hàng mua máy tính mới từ nhà cung cấp. "Đơn đặt hàng" là chứng từ do người mua phát hành cho biết họ muốn mua hàng từ người bán. Kịch bản này thuộc về giai đoạn nào của vòng đời phần cứng?

- A. Procurement
- B. Deployment
- C. Maintenance
- D. Retirement

Đáp án: A

3. Bộ phận CNTT thiết lập một tài khoản người dùng và phần mềm. Tình trạng này thuộc về giai đoạn nào của vòng đời phần cứng?

- A. Procurement
- B. Deployment
- C. Maintenance
- D. Retirement

Đáp án: B

4. Máy phải được trả lại cho nhà cung cấp để tái chế. Kịch bản này thuộc về

giai đoạn nào của vòng đời phần cứng?

- A. Procurement
- B. Deployment
- C. Maintenance
- D. Retirement

Đáp án: D

5. Loại phần cứng máy chủ nào tiết kiệm không gian nhất?

- A. Máy chủ Blade
- B. Máy chủ Rack
- C. Công tắc KVM
- D. Máy chủ Tower

Đáp án: B

6. Điều nào trong số này có thể là những cân nhắc để phát triển chính sách máy tính? Đánh dấu vào tất cả các câu phù hợp.

- A. Liệu người dùng có thể cài đặt phần mềm hay không
- B. Bạn có nên đặt mật khẩu thiết bị trên điện thoại công ty của nhân viên hay không
- C. Liệu người dùng có thể xem các trang web không liên quan đến công việc, như Facebook hay không
- D. Người dùng có nên chia sẻ mật khẩu của họ hay không

Đáp án: A, B, C

7. Một nhân viên sắp rời khỏi công ty của bạn. Những bước nào sau đây là thích hợp để thực hiện trong quá trình này? Đánh dấu vào tất cả các câu phù hợp.

- A. Làm sạch máy để sử dụng sau này

- B. Tạo bản sao các tập tin của người dùng
- C. Yêu cầu người dùng cung cấp thông tin đăng nhập của họ
- D. Xóa quyền truy cập của người dùng vào tài nguyên CNTT

Đáp án: A, D

8. Một số yếu tố quan trọng khi làm việc với các nhà cung cấp với tư cách là một sysadmin là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Tạo mối quan hệ độc lập với nhà cung cấp mà không cần sự cho phép của ban quản lý
- B. Lên lịch bảo trì tại công ty
- C. Thiết lập mối quan hệ với các nhà cung cấp
- D. Mua sắm phần cứng

Đáp án: B, C, D

9. Những phương pháp nào thường được sử dụng bởi sysadmins để sắp xếp các vấn đề? Đánh dấu vào tất cả các câu phù hợp.

- A. Kiểm tra máy ngẫu nhiên
- B. Hệ thống vé (ticketing system)
- C. Kiểm tra hàng ngày trên mỗi máy
- D. Cảnh báo giám sát dịch vụ

Đáp án: B, D

10. Loại máy chủ nào giống với máy tính để bàn nhất về ngoại hình?

- A. Máy chủ DNS
- B. Máy chủ Rack
- C. Máy chủ Blade
- D. Máy chủ Tower

Đáp án: D

11. Cơ sở hạ tầng CNTT nào có thể do một người điều hành?

- A. Google
- B. Apple
- C. Facebook
- D. Hometown Independent Computer Company, LLC

Đáp án: D

12. Những trách nhiệm có thể của một sysadmin là gì? (Đánh dấu vào tất cả các câu phù hợp)

- A. Quản trị cơ sở dữ liệu
- B. Hỗ trợ kỹ thuật
- C. Quản trị mạng
- D. Quản lý tiền lương

Đáp án: A, B, C

Dịch vụ mạng và cơ sở hạ tầng

Câu hỏi về Giới thiệu dịch vụ hạ tầng CNTT

1. Dịch vụ nào sau đây được coi là dịch vụ cơ sở hạ tầng vật lý? Đánh dấu vào tất cả các câu phù hợp.

- A. Máy tính xách tay
- B. Máy tính để bàn
- C. Máy chủ Rack
- D. Hệ điều hành

Đáp án: A, B, C

2. Dịch vụ nào trong số này được coi là dịch vụ mạng? Đánh dấu vào tất cả các câu phù hợp.

- A. Mạng không dây
- B. DNS
- C. Máy chủ Blade
- D. Cáp Ethernet

Đáp án: A, B

3. Dịch vụ nào trong số này được coi là dịch vụ phần mềm? Đánh dấu vào tất cả các câu phù hợp.

- A. Ứng dụng trò chuyện
- B. Trình xử lý văn bản
- C. Ứng dụng email
- D. Mạng không dây

Đáp án: A, B, C

Câu hỏi về Dịch vụ hạ tầng vật lý

1. Nếu bạn đang chạy một máy chủ, hệ điều hành nào sau đây sẽ phù hợp nhất cho máy chủ của bạn?

- A. Windows 10
- B. Ubuntu server
- C. MacOS
- D. Ubuntu

Đáp án: B

2. Lợi ích của việc ảo hóa máy chủ là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Sử dụng tài nguyên phần cứng tốt hơn
- B. Bảo trì dễ dàng hơn
- C. Giá rẻ hơn
- D. Hiệu suất tốt hơn máy chủ chuyên dụng

Đáp án: A, B, C

3. Bạn cần điều nào sau đây để SSH cho một máy? Đánh dấu vào tất cả các câu phù hợp.

- A. Máy khách SSH trên máy bạn muốn kết nối
- B. Kết nối VPN
- C. Máy chủ SSH trên máy bạn muốn kết nối
- D. Một máy chủ ảo để kết nối với

Đáp án: A, C

Câu hỏi về Dịch vụ mạng

1. Một lợi ích của việc sử dụng TFTP hơn SFTP là gì?

- A. Thêm bảo mật
- B. Chuyển đơn giản hơn mà không cần xác thực
- C. Truyền dữ liệu được mã hóa
- D. Yêu cầu xác thực người dùng

Đáp án: B

2. Bạn có thể sử dụng dịch vụ nào để giữ cho thời gian được đồng bộ hóa giữa các máy trong tổ chức của bạn?

- A. FTP
- B. Kerberos
- C. NTP
- D. SFTP

Đáp án: C

3. Proxy cung cấp những tính năng nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Quyền riêng tư của mạng
- B. Giám sát lưu lượng mạng
- C. Lọc lưu lượng truy cập Internet
- D. Khả năng chia sẻ thông tin của nhân viên dễ dàng hơn

Đáp án: A, B, C

4. Nếu bạn muốn trở một tên miền đến một máy chủ web hoặc sử dụng các tên máy chủ trong công ty của mình, bạn có thể sử dụng giao thức mạng nào?

- A. DHCP
- B. DNS
- C. NTP
- D. SFTP

Đáp án: B

5. Nếu bạn không muốn sử dụng địa chỉ IP tĩnh mà muốn gán địa chỉ IP động cho máy tính, bạn có thể sử dụng giao thức mạng nào?

- A. TFTP
- B. Kerberos
- C. NTP
- D. DHCP

Đáp án: D

Câu hỏi tổng hợp

1. Giả sử rằng bạn xử lý việc quản trị hệ thống CNTT cho công ty. Có một máy chủ bên trong tổ chức của bạn kiểm tra tần suất các máy khách truy cập vào nó.

Nếu một máy khách không truy cập vào máy chủ trong ba tháng, máy chủ sẽ không cho phép máy khách truy cập tài nguyên của nó nữa. Bạn có thể dùng gì để đảm bảo rằng máy khách của bạn và thời gian máy chủ được đồng bộ hóa?

- A. FTP
- B. NTP
- C. Proxy
- D. Intranet

Đáp án: B

2. Giả sử bạn là nhân viên CNTT duy nhất trong công ty của bạn và sếp của bạn muốn có một cách để chặn một số trang web nhất định với nhân viên. Bạn có thể thiết lập gì để thực hiện yêu cầu này?

- A. Intranet
- B. FTP
- C. Proxy server
- D. DNS

Đáp án: C

3. Khi bạn thực hiện truy vấn DNS, máy tính của bạn sẽ kiểm tra ở đâu trước tiên để tìm địa chỉ IP để ánh xạ tên?

- A. Máy chủ DNS ISP
- B. Máy cục bộ của bạn
- C. Máy chủ gốc
- D. Miền cấp cao nhất

Đáp án: B

4. Ưu điểm của việc sử dụng hệ điều hành máy chủ là gì? Chọn tất cả câu đúng

- A. Thêm RAM và dung lượng lưu trữ

- B. Giao diện người dùng được đơn giản hóa
- C. Các tính năng bảo mật bổ sung và dịch vụ mạng được tích hợp ngay trong
- D. Nhiều kết nối mạng hơn

Đáp án: A, C, D

5. Một kỹ thuật viên mạng thiết lập một máy chủ DNS nội bộ cho mạng cục bộ của mình. Khi anh ấy nhập URL, cái nào được kiểm tra đầu tiên?

- A. Máy chủ DNS cục bộ
- B. Máy chủ DNS ISP bên ngoài
- C. Local host file
- D. Máy chủ DNS công cộng bên ngoài

Đáp án: C

6. Ưu điểm chính của việc sử dụng DHCP là gì?

- A. Ánh xạ địa chỉ IP thành các URL có thể đọc được của con người
- B. Cho phép bạn đặt địa chỉ IP theo cách thủ công
- C. Cho thuê địa chỉ IP, loại bỏ nhu cầu chỉ định địa chỉ theo cách thủ công
- D. Cho phép sử dụng địa chỉ IP tĩnh

Đáp án: C

7. PXE Boot là viết tắt của gì?

- A. Past Boot Examination
- B. Post Boot Extraction
- C. Pre Boot Execution
- D. Pay-to-Boot Extortion

Đáp án: C

8. Một sysadmin đang tìm cách sử dụng Pre Boot Execution qua mạng bằng cách giữ các tập tin cài đặt hệ điều hành trên máy chủ. Loại máy chủ này có khả năng là loại máy chủ nào nhất?

- A. Máy chủ TFTP
- B. máy chủ DNS
- C. Máy chủ SFTP
- D. Máy chủ FTP

Đáp án: A

Các dịch vụ nền tảng và phần mềm

Câu hỏi Về Dịch vụ phần mềm

1. Bạn có thể sử dụng dịch vụ giao tiếp nào trong tổ chức của mình? Đánh dấu vào tất cả các câu phù hợp.

- A. E-mail
- B. Ứng dụng trò chuyện
- C. DNS
- D. Điện thoại

Đáp án: A, B

2. Sự khác biệt giữa POP3 và IMAP là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. POP3 chỉ có thể tải email xuống một thiết bị cục bộ.
- B. IMAP chỉ có thể tải email xuống một thiết bị cục bộ.
- C. POP3 được sử dụng để gửi email.
- D. IMAP có thể tải email xuống nhiều thiết bị.

Đáp án: A, D

3. Giấy phép phần mềm sử dụng cho mục đích thương mại và sử dụng cá nhân về cơ bản là giống nhau.

- A. Đúng
- B. Sai

Đáp án: B

4. Sự khác biệt giữa TLS và SSL là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. TLS là sự kế thừa của SSL.
- B. TLS an toàn hơn SSL.
- C. SSL an toàn hơn TLS.
- D. SSL là sự kế thừa của TLS.

Đáp án: A, B

Câu hỏi Về Dịch vụ tập tin, in ấn, và nền tảng

1. Lợi ích của việc thiết lập một máy chủ NFS là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Kết nối với máy in
- B. Lưu trữ tập tin trên ổ đĩa mạng
- C. Cho phép chia sẻ tập tin qua mạng
- D. Cung cấp nội dung web

Đáp án: B, C

2. Bạn có thể sử dụng những phương pháp nào để thiết lập in ấn trong một tổ chức? Đánh dấu vào tất cả các câu phù hợp.

- A. Kết nối trực tiếp máy in
- B. Thiết lập máy chủ in
- C. Sử dụng dịch vụ đám mây để thiết lập máy in

D. Thiết lập máy chủ NFS

Đáp án: A, B, C

3. Khi bạn có máy chủ web, dịch vụ nào được sử dụng để cho phép xử lý các yêu cầu HTTP?

A. Máy chủ HTTP

B. Máy chủ web

C. Mã trạng thái HTTP

D. Một máy chủ cơ sở dữ liệu

Đáp án: A

4. Bạn có thể sử dụng _____ để lưu trữ một lượng lớn dữ liệu khách hàng cho một trang web.

A. Máy chủ NFS

B. Máy chủ HTTP

C. máy chủ cơ sở dữ liệu

D. máy chủ DNS

Đáp án: C

Câu hỏi Về Chuẩn đoán lỗi trang web

1. Mã trạng thái HTTP bắt đầu bằng 4xx, như 404, cho biết lỗi trên:

A. Phía khách hàng

B. Phía máy chủ

C. Không phải lỗi, đây là mã thành công

D. Chuyển hướng

Đáp án: A

2. Mã trạng thái HTTP bắt đầu bằng 5xx, như 501, cho biết lỗi trên:

- A. Phía khách hàng
- B. Phía máy chủ
- C. Không phải lỗi, đây là mã thành công
- D. Chuyển hướng

Đáp án: B

Câu hỏi tổng hợp

1. Nếu bạn đang duyệt một trang web, cách nhanh chóng để biết rằng trang đó an toàn là gì?

- A. Trang web có biểu ngữ nói rằng nó an toàn
- B. URL bắt đầu bằng https
- C. URL bắt đầu bằng tls
- D. URL bắt đầu bằng http

Đáp án: B

2. Bạn là nhân viên CNTT duy nhất tại công ty của bạn. Hầu hết các máy tính trong nhóm của bạn là máy Windows. Sếp của bạn muốn bạn thiết lập một bộ lưu trữ tập tin mạng. Bạn nên sử dụng dịch vụ tập tin nào?

- A. Máy chủ Samba
- B. Máy chủ NFS
- C. Máy chủ HTTP
- D. Máy chủ cơ sở dữ liệu

Đáp án: A

3. Cái nào trong số này KHÔNG phải là giao thức email?

- A. IRC

- B. SMTP
- C. POP3
- D. IMAP

Đáp án: A

4. Những giao thức hệ thống tập tin nào được thiết kế để sử dụng mạng? Đánh dấu vào tất cả các câu phù hợp.

- A. SMB
- B. Samba
- C. FAT32
- D. NFS

Đáp án: A, D

5. Phương pháp nào sau đây là phương pháp hợp lệ để quản lý dịch vụ máy in trong môi trường thương mại?

- A. Trên Linux, sử dụng CUPS để quản lý các dịch vụ in
- B. Trên máy chủ Windows, bật “Print and Document Services”, và thêm máy in
- C. Quản lý nhiều máy in riêng biệt
- D. Sử dụng nhà cung cấp dịch vụ đám mây để quản lý máy in của bạn thông qua trình duyệt web

Đáp án: A, B, D

6. Thông tin khách hàng, chẳng hạn như các bài báo, video, một lượng lớn văn bản, hình ảnh hoặc tập tin âm thanh, thường được lưu trữ cho các dịch vụ web ở đâu?

- A. Trên máy chủ web
- B. Trên cơ sở dữ liệu

- C. Chỉ trên máy cục bộ
- D. Trên máy chủ FTP

Đáp án: B

7. Chức năng chính của hệ thống cơ sở dữ liệu là gì?

- A. Cơ sở dữ liệu là một máy chủ vật lý lưu trữ các tập tin web và phần mềm máy chủ HTTP.
- B. Cơ sở dữ liệu cho phép lưu trữ, truy vấn, lọc và quản lý một lượng lớn dữ liệu.
- C. Cơ sở dữ liệu lưu trữ và truy xuất tập tin qua mạng.
- D. Cơ sở dữ liệu là một cách bảo mật thông tin liên lạc giữa máy chủ web và máy khách.

Đáp án: B

Các dịch vụ thư mục

Câu hỏi về giới thiệu dịch vụ thư mục

1. Máy chủ thư mục cung cấp gì?

- A. Dịch vụ giao tiếp thời gian thực
- B. Dịch vụ thời gian mạng
- C. Dịch vụ tra cứu cho một tổ chức
- D. Dịch vụ sao chép

Đáp án: C

2. Sự sao chép (replication) mang lại những lợi ích gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Trùng lắp (redundancy)
- B. Bảo mật nâng cao

C. Tăng công suất

D. Giảm độ trễ

Đáp án: A, D

3. Giao thức dịch vụ thư mục phổ biến nhất được sử dụng ngày nay là gì?

A. Directory Access Protocol

B. Directory System Protocol

C. Lightweight Directory Access Protocol

D. Directory Operational Binding Management Protocol

Đáp án: A, D

Câu hỏi về Quản lý tập trung hóa và LDAP

1. Ví dụ nào sau đây là quản lý tập trung? Đánh dấu vào tất cả các câu phù hợp.

A. Kiểm soát truy cập dựa trên vai trò

B. Quản lý cấu hình tập trung

C. Sao chép cấu hình sang các hệ thống khác nhau

D. Xác thực cục bộ

Đáp án: A, B

2. Cái nào trong số này là các thành phần của mục nhập LDAP? Đánh dấu vào tất cả các câu phù hợp.

A. Tên không phổ biến

B. Tên gọi phổ biến

C. Người dùng tổ chức

D. Tên phân biệt

Đáp án: B, D

3. Chính xác thì hoạt động Liên kết LDAP làm gì?

A. Sửa đổi các mục nhập trong máy chủ thư mục

- B. Tra cứu thông tin trong máy chủ thư mục
- C. Xác thực một máy khách đến máy chủ thư mục
- D. Thay đổi mật khẩu cho tài khoản người dùng trên máy chủ thư mục

Đáp án: C

4. Loại xác thực nào sau đây được hoạt động Liên kết LDAP hỗ trợ? Đánh dấu vào tất cả các câu phù hợp.

- A. Ẩn danh (Anonymous)
- B. Đơn (Simple)
- C. Phức (Complex)
- D. SASL

Đáp án: A, B, C

Câu hỏi về Active Directory

1. Active Directory là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Dịch vụ thư mục mã nguồn mở
- B. Một phần mềm dịch vụ thư mục chỉ dành cho Windows
- C. Một phần mềm của Microsoft về dịch vụ thư mục
- D. Dịch vụ thư mục tương thích với LDAP

Đáp án: C, D

2. Đơn vị tổ chức (Organizational Unit) khác với một vùng chứa thông thường như thế nào?

- A. Không khác. Nó chỉ là một tên khác cho vùng chứa
- B. Nó có thể chứa các đối tượng khác
- C. Nó chỉ có thể chứa các thùng chứa khác
- D. Nó có thể chứa các thùng chứa bổ sung

Đáp án: D

3. Khi bạn tạo miền Active Directory, tên của tài khoản người dùng mặc định là gì?

- A. Superuser
- B. Root
- C. Username
- D. Administrator

Đáp án: D

4. Máy trong Domain Controller cũng là thành viên của nhóm Domain Computer:

- A. Đúng
- B. Sai

Đáp án: B

5. Security group khác với distribution group ở điểm nào?

- A. Chúng giống hệt nhau.
- B. Security group được sử dụng cho máy tính, trong khi distribution group được sử dụng cho người dùng.
- C. Security group được sử dụng cho người dùng, trong khi distribution group được sử dụng cho máy tính.
- D. Security group có thể được sử dụng để cung cấp quyền truy cập vào tài nguyên, trong khi distribution group chỉ được sử dụng để liên lạc qua email.

Đáp án: D

6. Sự khác biệt giữa việc thay đổi mật khẩu (changing) và đặt lại mật khẩu

(resetting) là gì?

- A. Thay đổi mật khẩu yêu cầu mật khẩu trước đó.
- B. Thay đổi mật khẩu không yêu cầu mật khẩu trước đó.
- C. Đặt lại mật khẩu sẽ khóa tài khoản.
- D. Chúng giống nhau.

Đáp án: A

7. Liên kết máy tính vào Active Directory liên quan đến việc liên kết máy tính vào một workgroup.

- A. Đúng
- B. Sai

Đáp án: B

8. Việc tham gia máy tính vào miền AD mang lại lợi ích nào sau đây? Đánh dấu vào tất cả các câu phù hợp.

- A. Xác thực tập trung
- B. Nhật ký (logging) chi tiết hơn
- C. Quản lý tập trung với GPO
- D. Hiệu suất tốt hơn

Đáp án: A, C

9. Đối tượng chính sách nhóm là gì?

- A. Các loại thùng chứa đặc biệt
- B. Các loại nhóm máy tính đặc biệt
- C. Các loại nhóm người dùng đặc biệt
- D. Cài đặt cho máy tính và tài khoản người dùng trong AD

Đáp án: D

10. Sự khác biệt giữa chính sách (policy) và tùy chọn (preference) là gì?

- A. Chúng giống hệt nhau.
- B. Một chính sách được sử dụng để đặt một tùy chọn.
- C. AD thực thi một chính sách, trong khi người dùng cục bộ có thể sửa đổi tùy chọn.
- D. Người dùng cục bộ có thể sửa đổi chính sách, trong khi AD thực thi một tùy chọn.

Đáp án: C

11. Với miền AD mới, bạn cần thay đổi gì trước khi có thể nhắm mục tiêu nhóm người dùng và máy móc với GPO?

- A. Không cần. Có thể dùng cấu hình mặc định.
- B. Bạn cần đặt người dùng và máy tính vào OU mới.
- C. Bạn cần tạo một tài khoản quản trị viên.
- D. Bạn cần đổi tên các nhóm mặc định.

Đáp án: B

12. Chọn đúng thứ tự thực thi của GPO:

- A. Site-> Tên miền -> OU
- B. OU -> Tên miền -> Site
- C. Tên miền -> Site -> OU
- D. Site -> OU -> Tên miền

Đáp án: A

13. Chúng ta có thể sử dụng gì để xác định những chính sách nào sẽ được áp dụng cho một máy nhất định?

- A. gpupdate

- B. Bảng điều khiển
- C. Miền thử nghiệm
- D. Một báo cáo RSOP

Đáp án: D

14. Làm cách nào để khách hàng phát hiện ra địa chỉ của bộ điều khiển miền?

- A. Nó được đẩy qua AD GPO.
- B. Nó gửi một chương trình phát đến mạng cục bộ.
- C. Nó thực hiện một truy vấn DNS, yêu cầu bản ghi SRV cho miền.
- D. Nó được cung cấp qua DHCP.

Đáp án: C

15. Điều nào sau đây có thể ngăn bạn đăng nhập vào máy tính đã tham gia miền? Đánh dấu vào tất cả các câu phù hợp.

- A. Bạn không thể kết nối với bộ điều khiển miền.
- B. Máy tính của bạn được kết nối với Wifi.
- C. Tài khoản người dùng đã bị khóa.
- D. Ngày và giờ không chính xác.

Đáp án: A, C, D

Câu hỏi Tổng Hợp

1. Máy chủ thư mục đóng những vai trò gì trong quản lý tập trung? Đánh dấu vào tất cả các câu phù hợp.

- A. Bảo mật
- B. Cấp quyền
- C. Kế toán
- D. Xác thực tập trung

Đáp án: B, C, D

2. Khi có các GPO xung đột, thứ tự chúng được đánh giá và áp dụng là gì?

- A. OU, Site, Domain
- B. Site, OU, Domain
- C. Site, Domain, OU
- D. OU, Domain, Site

Đáp án: C

3. Thành phần nào của mục nhập LDAP chứa tên mục nhập duy nhất?

- A. Common name
- B. Organizational unit
- C. Distinguished name

Đáp án: C

4. Các dịch vụ thư mục lưu trữ thông tin theo cấu trúc thứ bậc. Phát biểu nào về Đơn vị tổ chức (OU) của hệ thống phân cấp dịch vụ thư mục là đúng? Đánh dấu vào tất cả các câu phù hợp.

- A. Có thể thực hiện các thay đổi đối với một OU con mà không ảnh hưởng đến các OU con khác trong cùng một cha.
- B. Các OU cha kế thừa các đặc điểm của các thành viên con.
- C. Các tập tin cụ thể trong OU hoặc vùng chứa, được gọi là "đối tượng".
- D. Các OU thành viên con kế thừa các đặc điểm của OU cha

Đáp án: A, C, D

5. Ví dụ về phần mềm máy chủ thư mục Lightweight Directory Access Protocol (LDAP) là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. OpenLDAP
- B. RDP
- C. ADUC

D. Active Directory của Microsoft

Đáp án: A, D

6. Cách nào sau đây là những cách phổ biến để xác thực truy vấn thư mục LDAP? Đánh dấu vào tất cả các câu phù hợp.

A. Private

B. SASL Authentication

C. Anonymous

D. Simple

Đáp án: A, C, D

7. Câu nào sau đây là đúng về Bộ điều khiển miền (DC)? Đánh dấu vào tất cả các câu phù hợp.

A. Bạn nên luôn sử dụng Domain Admin hoặc Enterprise Admin cho hoạt động hàng ngày.

B. Đơn vị tổ chức (OU) mặc định được gọi là Domain Controllers chứa tất cả Bộ điều khiển miền trong miền.

C. Ủy quyền có thể được sử dụng trong Active Directory.

D. Các thay đổi an toàn được thực hiện bằng cách nhân Domain * Controllers cùng một lúc được giao nhiệm vụ cấp cho chúng Flexible Single-Master Operations.

Đáp án: C

8. Sự khác biệt giữa chính sách nhóm và tùy chọn chính sách nhóm là gì?

A. Các tùy chọn được áp dụng lại sau mỗi 90 phút và các chính sách giống với một mẫu cài đặt hơn.

B. Chỉ quản trị viên mới có thể chỉnh sửa tùy chọn nhưng bất kỳ ai cũng có thể chỉnh sửa chính sách.

C. Chỉ quản trị viên mới có thể chỉnh sửa chính sách nhưng bất kỳ ai cũng

có thể chỉnh sửa tùy chọn chính sách nhóm.

- D. Các chính sách được áp dụng lại sau mỗi 90 phút và các tùy chọn là một mẫu cài đặt.

Đáp án: D

9. Bạn muốn thay đổi chính sách độ dài mật khẩu tối thiểu trong Chính sách miễn mặc định (GPO) Default Domain Policy. Cách tốt nhất để làm điều này là gì?

- A. Mở ADAC và chỉnh sửa cài đặt chính sách ở đó
- B. Mở Bảng điều khiển quản lý chính sách nhóm bằng cách chạy gpmmc.msc từ CLI
- C. Chỉnh sửa Windows Registry để thay đổi cài đặt chính sách nhóm
- D. Chỉnh sửa thủ công các tập tin cấu hình trong SYSVOL

Đáp án: B

10. Để quản lý các chính sách OpenLDAP qua Giao diện Dòng lệnh (CLI), cần có một loại tập tin nhất định. Loại tập tin này được gọi là gì?

- A. Tập tin TXT
- B. Tập tin LDIF
- C. Tập tin cấu hình LDAP
- D. Tập tin ADL

Đáp án: B

Phục Hồi và Sao Lưu Dữ Liệu

Câu hỏi về lên kế hoạch phục hồi dữ liệu

1. Làm thế nào bạn có thể khôi phục sau sự kiện mất dữ liệu không mong muốn? Chọn tất cả các câu phù hợp.

- A. Viết post-mortem report.
- B. Khôi phục dữ liệu từ các thiết bị bị hỏng.

- C. Khôi phục dữ liệu từ các bản sao lưu.
- D. Thiết kế một kế hoạch khắc phục thảm họa.

Đáp án: B, C

2. Về mặt vật lý, nơi nào là tốt nhất để lưu trữ các bản sao lưu?

- A. Cục bộ tại công ty
- B. Ngoài công ty
- C. Trong két sắt
- D. Trên nhiều địa điểm khác nhau

Đáp án: D

3. Dữ liệu nào sau đây nên được sao lưu? Chọn tất cả các câu phù hợp.

- A. Cấu hình tường lửa
- B. Thư mục các file đã tải xuống
- C. Hình ảnh kỳ nghỉ gia đình
- D. Cơ sở dữ liệu bán hàng

Đáp án: A, D

4. Phương tiện sao lưu băng từ phù hợp nhất với?

- A. Dữ liệu lưu trữ dài hạn
- B. Dữ liệu được lưu trong bộ nhớ cache có độ trễ thấp
- C. Hệ thống sao lưu giá rẻ
- D. Sao lưu nhanh chóng và hiệu quả

Đáp án: A

5. Tại sao kiểm tra các thủ tục sao lưu và khôi phục lại quan trọng? Chọn tất cả các câu phù hợp.

- A. Để giảm kích thước của dữ liệu sao lưu
- B. Để tăng tốc quá trình sao lưu và khôi phục
- C. Để đảm bảo sao lưu hoạt động và dữ liệu có thể được khôi phục từ chúng
- D. Để đảm bảo rằng dữ liệu có liên quan được đưa vào các bản sao lưu

Đáp án: C, D

6. Loại sao lưu nào sau đây tiết kiệm dung lượng nhất?

- A. Sao lưu toàn bộ
- B. Sao lưu khác biệt
- C. Sao lưu tăng dần

Đáp án: C

7. Bạn có thể sử dụng mảng RAID và sử dụng rsync để sao chép dữ liệu quan trọng vào đó để sao lưu.

- A. Đúng
- B. Sai

Đáp án: B

Câu hỏi về lên kế hoạch phục hồi sau thảm họa

1. Kế hoạch phục hồi sau thảm họa cần bao gồm những yếu tố nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Biện pháp phát hiện
- B. Biện pháp phòng ngừa
- C. Biện pháp phục hồi
- D. Biện pháp mạnh

Đáp án: A, B, C

2. Tại sao các **biện pháp phát hiện** lại được đưa vào kế hoạch phục hồi sau thảm họa ?

- A. Chúng không được đưa vào
- B. Bởi vì điều quan trọng là phải biết khi nào thảm họa xảy ra
- C. Vì chúng ngăn ngừa mất dữ liệu
- D. Vì chúng giúp khôi phục sau khi mất dữ liệu dễ dàng hơn

Đáp án: B

3. Các **biện pháp phòng ngừa** nào là tốt để áp dụng trong tổ chức của bạn? Đánh dấu vào tất cả các câu phù hợp.

- A. Hệ thống giám sát và cảnh báo
- B. Hệ thống dự phòng
- C. Sao lưu thường xuyên
- D. Tài liệu có thể truy cập và cập nhật

Đáp án: B, C, D

4. Các **biện pháp phát hiện** tốt để áp dụng trong tổ chức của bạn là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Giám sát môi trường
- B. Sao lưu các quy tắc tường lửa
- C. Nguồn điện dự phòng
- D. Giám sát hiệu suất hệ thống

Đáp án: A, D

5. Các biện pháp phục hồi tốt để áp dụng trong tổ chức của bạn là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Khôi phục cấu hình máy chủ từ bản sao lưu
- B. Tuân theo tài liệu kế hoạch khôi phục chi tiết
- C. Giám sát sự cố mất đường truyền internet
- D. Duy trì các máy chủ dự phòng

Đáp án: A, B

Câu hỏi về post-mortem

1. Mục đích đằng sau việc viết post-mortem là gì?

- A. Để đổ lỗi cho những sai lầm
- B. Phân bổ trách nhiệm pháp lý
- C. Để học hỏi từ những sai lầm và cải thiện trong tương lai
- D. Để khiến mọi người sợ hãi tránh hành vi nguy hiểm

Đáp án: C

2. Tiến trình thực hiện viết post-mortem bao gồm những gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Các hành động được thực hiện trước, trong và sau sự cố
- B. Phân tích chi tiết về sự cố, bao gồm nguyên nhân gốc rễ và phạm vi
- C. Ngày và giờ chi tiết
- D. Tóm tắt sự cố và nó kéo dài bao lâu

Đáp án: A, C

Câu hỏi Tổng Hợp

1. Có những loại chiến lược sao lưu nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Sao lưu đầy đủ
- B. Sao lưu khác biệt
- C. Sao lưu gia tăng

D. Sao lưu một phần

Đáp án: A, B, C

2. Các biện pháp bao gồm trong kế hoạch khắc phục hậu quả thiên tai là gì?

A. Phòng ngừa

B. Phát hiện

C. Thử nghiệm

D. Phục hồi

Đáp án: A, B, D

3. Phần nào thường bị bỏ qua của báo cáo post-mortem?

A. Tổng kết

B. Dòng thời gian

C. Điều gì đã diễn ra kém

D. Điều gì đã diễn ra tốt đẹp

Đáp án: D

4. Loại sao lưu nào chỉ sao lưu các tập tin đã thay đổi kể từ lần chạy trước?

A. Sao lưu đầy đủ

B. Sao lưu khác biệt

C. Sao lưu gia tăng

D. Sao lưu một phần

Đáp án: C

5. Ưu điểm của sao lưu tại chỗ là gì? Đánh dấu vào tất cả các câu phù hợp.

A. Có quyền truy cập dữ liệu nhanh hơn.

B. Dữ liệu an toàn hơn vì lưu lượng gửi đi ít hơn.

C. Sử dụng ít băng thông hơn.

D. Dữ liệu được an toàn trong trường hợp thảm họa.

Đáp án: A, B, C

6. Bạn có thể cân nhắc công cụ sao lưu nào sau đây khi thiết kế giải pháp sao lưu? Đánh dấu vào tất cả các câu phù hợp.

- A. Time Machine
- B. Regedit
- C. Backup and Restore
- D. Rsync

Đáp án: C

7. Loại sao lưu nào chỉ lưu các bản sao của tập tin đã được thay đổi hoặc tạo kể từ lần sao lưu cuối cùng?

- A. Sao lưu khác biệt
- B. Mảng RAID
- C. Sao lưu gia tăng
- D. Sao lưu toàn bộ

Đáp án: A

8. Dịch vụ đám mây là tùy chọn sao lưu lý tưởng cho các tập tin người dùng. Nền nào trong số này không phải là một trong những nền tảng lưu trữ đám mây phổ biến hiện nay?

- A. Dropbox
- B. Google Drive
- C. Rsync
- D. iCloud của Apple

Đáp án: C

9. Bạn đang thực hiện đánh giá rủi ro mạng để phát triển kế hoạch khắc phục thảm họa của mình. Đây là ví dụ nào về các biện pháp phát hiện? Đánh dấu vào

tất cả các câu phù hợp.

- A. Sử dụng hệ thống cảnh báo khi mất điện
- B. Kiểm tra kiến thức và sự sẵn sàng của chính bạn (và của người dùng) đối với thảm họa
- C. Giám sát kiểm tra hệ thống
- D. Tiến hành sao lưu thường xuyên, tự động

Đáp án: A, B, C

10. Một số mục đích của post-mortem là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Để nuôi dưỡng một nền văn hóa, nơi có thể phạm sai lầm
- B. Chia sẻ post-mortem với các nhóm khác tại một tổ chức giúp khuyến khích văn hóa học hỏi từ những sai lầm.
- C. Để hiểu nguyên nhân của sai lầm và cách phòng tránh
- D. Để xấu hổ và trừng phạt những sai lầm
- E. Để học hỏi và điều chỉnh các quy trình để đạt hiệu quả cao hơn

Đáp án: A, B, C