**6. Đảm bảo hệ thống**

**6.1. Sao lưu và phục hồi**

**6.1.1. Cài đặt Windows Server Backup**

1. Server Manager/Add roles and features
2. Tại cửa sổ Before you begin, nhấp Next
3. Tại cửa sổ Select installation type, nhấp Next
4. Tại cửa sổ Select destination server
5. Tại cửa sổ Select server roles, nhấp Next
6. Tại cửa sổ Select features, chọn Windows Server Backup, nhấp Next
7. Nhấp Install
8. Nhấp Close

**6.1.2. Sao lưu với Windows Server Backup**

1. Server Manager/Tools/Windows Server Backup
2. Tại cửa sổ Windows Server Backup, Nhấp vào Local Backup bên cửa sổ trái, trong cửa sổ phải (Actions), nhấp vào Backup Schedule…
3. Tại cửa sổ Getting Started, nhấp Next
4. Tại cửa sổ Specify Backup Time, chọn mốc thời gian sao lưu định kỳ, nhấp Next
5. Tại cửa sổ Specify Destination Type, chọn nơi sao lưu phù hợp, nhấp Next
6. Hiển thị cửa sổ yêu cầu nhập Username, Password, điền thông tin và nhấp Ok,
7. Nhấp Finish
8. Nhấp Close

**6.1.3. Phục hồi từ Windows**

1. Server Manager/Tools/Windows Server Backup
2. Tại cửa sổ Windows Server Backup, Nhấp vào Local Backup bên cửa sổ trái, trong cửa sổ phải (Actions), nhấp vào Recover…
3. Tại cửa sổ Getting Started, nhấp vào tuỳ chọn A backup stored on another location, nhấp Next
4. Tại cửa sổ Specify Location Type, chọn Local drives, nhấp Next
5. Tại cửa sổ Select Backup Location chọn nơi lưu trữ hệ thống sao lưu, nhấp Next
6. Tai cửa sổ Select Server, chọn Server muốn khôi phục, nhấp Next
7. Tại cửa sổ Select Backup Data, chọn ngày phục hồi, nhấp Next
8. Tại cửa sổ Select Recovery Type, chọn nội dung cần phục hồi (ví dụ chọn file and folder), nhấp Next
9. Tại cửa sổ Select Items to Recover, chọn folder cần phục hồi, nhấp Next
10. Tại cửa sổ Specify Recovery Options, chọn vị trí khôi phục đến vị trí gốc hay vị trí mới, nhấp Next
11. Tại cửa sổ Confirmation, nhấp Recover
12. Nhấp Close

**6.2. An ninh, an toàn**

**6.2.1. Microsoft Defender Antivirus**

1. Server Manager/Add roles and features
2. Tại cửa sổ Before you begin, nhấp Next
3. Tại cửa sổ Select installation type, nhấp Next
4. Tại cửa sổ Select destination server
5. Tại cửa sổ Select server roles, nhấp Next
6. Tại cửa sổ Select features, chọn Microsoft Defender Antivirus, nhấp Next
7. Nhấp Install
8. Nhấp Close

**6.2.2. Windows Defender Security Center**

1. Nhấp vào Start/Settings/Update & Security/Windows Security rồi chọn Virus & Threat Protection.
2. Chọn liên kết Scan options
3. Đảm bảo nút radio ở chế độ Full scan và chọn nút Scan now
4. Quá trình quét sẽ mất một lúc. Sau khi quá trình quét hoàn tất, hãy đóng Defender Security Center.

**6.2.3. Configuring Windows Firewall**

1. Nhấp vào Start/Settings/Update & Security/Windows Security rồi chọn Firewall & Network Protection.
2. Sau đó, bạn có thể quyết định tùy chọn tường lửa nào bạn muốn đặt, như thay đổi thông báo tường lửa, bật hoặc tắt Tường lửa Windows, khôi phục mặc định, cấu hình cài đặt nâng cao và khắc phục sự cố
3. Hộp thoại cài đặt Tường lửa Windows cho phép bạn bật hoặc tắt Tường lửa Windows cho cả mạng riêng và mạng công cộng. Cài đặt Bật sẽ chặn các nguồn đến và cài đặt Tắt Tường lửa Windows sẽ cho phép các nguồn đến kết nối.

**6.2.4. Windows Firewall with Advanced Security (WFAS)**

1. Nhấp vào Start/Settings/Update & Security/Windows Security/ Firewall & Network Protection
2. Click vào Advanced Settings.
3. Nhấp chuột phải vào Inbound Rules và chọn New Rule.
4. Chọn một loại quy tắc. Đối với bài tập này, hãy chọn Custom để bạn có thể thấy tất cả các tùy chọn có sẵn cho mình. Sau đó, nhấp vào Next.
5. Tại màn hình Program, hãy chọn All Programs. Sau đó, nhấp vào Next.
6. Chọn loại giao thức cũng như số cổng cục bộ và từ xa bị ảnh hưởng bởi quy tắc này. Đối với bài tập này, hãy chọn TCP và đảm bảo rằng All Ports được chọn cho cả Local Port và Remote Port. Nhấp vào Next để tiếp tục.
7. Tại màn hình Scope, hãy chọn Any IP Address cho cả local và remote. Sau đó, nhấp vào Next.
8. Tại màn hình Action, hãy chọn Allow The Connection Only If It Is Secure. Nhấp vào Next.
9. Tại màn hình Users, bạn có thể thử nghiệm các tùy chọn này nếu muốn bằng cách nhập người dùng vào cả hai phần. Khi bạn nhấp vào một trong các hộp kiểm, các nút Add và Remove sẽ khả dụng. Nhấp vào Next để tiếp tục.
10. Tại màn hình Computers, bạn có thể chọn máy tính nào bạn sẽ ủy quyền hoặc cho phép thông qua quy tắc này (ngoại lệ). Một lần nữa, bạn có thể thử nghiệm các tùy chọn này nếu muốn. Nhấp vào Next để tiếp tục.
11. Tại màn hình Profile, hãy chọn hồ sơ nào sẽ bị ảnh hưởng bởi quy tắc này. Chọn một hoặc nhiều hồ sơ và nhấp vào Next.
12. Đặt tên và mô tả cho hồ sơ của bạn, sau đó nhấp vào Finish. Quy tắc tùy chỉnh của bạn sẽ xuất hiện trong danh sách các quy tắc đến và quy tắc sẽ được bật.
13. Nhấp đúp vào quy tắc mới tạo của bạn. Lưu ý rằng bạn có thể thay đổi các tùy chọn mà bạn đã định cấu hình trước đó.
14. Xóa quy tắc bằng cách nhấp chuột phải vào quy tắc mới và chọn Delete. Một hộp thoại sẽ xuất hiện hỏi bạn có chắc chắn không. Nhấp vào Yes.
15. Đóng Tường lửa Windows.

**6.2.5. Installing Windows Defender Application Guard**

1. Nhấp chuột phải vào Start/Apps and Features, tại cửa sổ bên phải chọn Programs And Features.
2. Nhấp vào liên kết Turn Windows Features On Or Off.
3. Cuộn xuống và đánh dấu vào ô Windows Defender Application Guard, sau đó nhấp vào nút OK. Nếu đang cài trên Windows Server 2022 thì qua bước 4.
4. Tại màn hình Before You Begin, nhấp vào Next.
5. Màn hình Select Installation Type sẽ xuất hiện tiếp theo. Đảm bảo rằng nút radio Role-Based được chọn và nhấp vào Next.
6. Tại màn hình Select Destination Server, chọn Select a server from the server pool, chọn Server. Nhấp vào Next.
7. Tại màn hình Select Server Roles, nhấp vào hộp kiểm cho Windows Defender Application Guard.
8. Sau khi Windows Defender Application Guard được cài đặt, hãy đóng Control Panel.

**6.2.6. Using Windows Defender Application Guard**

1. Mở Microsoft Edge.
2. Từ menu tùy chọn, chọn New Application Guard Window
3. Bạn sẽ cần phải đợi Application Guard thiết lập môi trường bị cô lập. Quá trình này có thể mất vài phút.
4. Mở trang web của Microsoft ở chế độ Application Guard và bạn có thể thấy điều đó ở góc trên bên trái của cửa sổ. Đóng Edge

**6.2.7. Windows Defender Application Guard Enterprise**

1. Cài đặt Application Guard bằng cách sử dụng đối tượng Group Policy, System Center hoặc MDM.
2. Trong Group Policy, hãy đặt các thiết lập Network Isolation mà bạn muốn tuân theo. Để đặt tùy chọn này, trong trình soạn thảo GPO của bạn, hãy đi tới Administrative Templates\Network\Network Isolation\Enterprise Resource Domains Hosted In The Cloud.
3. Tiếp theo, hãy vào Administrative Templates\Network\Network Isolation\Domains được phân loại là cả thiết lập công việc và cá nhân. Nhập các trang web mà bạn tin tưởng.
4. Tiếp theo, hãy vào Computer Configuration\Administrative Templates\Windows Components\Windows Defender Application Guard\Turn On Windows Defender Application Guard In Enterprise Mode.
5. Chọn nút tùy chọn Enabled, chọn Option 1 (xem Hình 17.16) và nhấp vào OK.
6. Close the GPO editor.

**6.2.8. Windows Defender Credential Guard**

1. Mở Group Policy Management Console trên Windows Server 2022.
2. Tạo GPO mới và nhấp vào GPO rồi chọn Edit.
3. Đi tới Computer Configuration/Administrative Templates/System/Device Guard.
4. Nhấp đúp vào tùy chọn Turn On Virtualization Based Security rồi chọn tùy chọn Enabled.
5. Trong tùy chọn Turn On Virtualization Based Security, hãy chọn hộp Platform Security Level, chọn Secure Boot hoặc Secure Boot and DMA Protection.
6. Trong hộp Credential Guard Configuration, hãy nhấp vào Enabled with UEFI lock, rồi nhấp vào nút OK.
7. Đóng Group Policy Management Console.

**6.2.9. Windows Defender Exploit Guard**

1. Mở trung tâm Cài đặt bằng cách nhấp vào nút Start và nhấp vào biểu tượng Settings (biểu tượng spoke).
2. Chọn Update And Security.
3. Nhấp vào n Windows Security và chọn e Virus & Threat Protection.
4. Chọn Ransomware Protection và đảm bảo cài đặt được bật.
5. Nhấp vào Protected Folders để xem những thư mục nào hiện đang được bảo vệ. Bạn có thể nhấp vào + Add A Protected Folder để thêm các thư mục khác.
6. Nếu bạn muốn một ứng dụng có quyền truy cập, bạn có thể nhấp vào liên kết Allow An App Through Controlled Folder Access. Sau khi nhấp vào liên kết, bạn có thể thêm ứng dụng sẽ được phép truy cập.
7. Đóng Security Center (khởi động lại nếu bạn thực hiện bất kỳ thay đổi nào).

**6.2.10. Chính sách mật khẩu chi tiết (Fine-Grained Password Policy - FGPP)**

1. Đăng nhập Domain Controller với quyền Domain Admin
2. Mở Server Manager → Tools → Active Directory Administrative Center (ADAC)
3. Vào: YourDomain | System | Password Settings Container
4. Chọn New → Password Settings
5. Đặt tên cấu hình và các thông số cấu hình, nhấp Add, Chọn nhóm người dùng áp dụng, nhấp OK
6. Nhấp Ok,

**6.3. Kiểm soát nhật ký**

**6.3.1. Xem và lọc sự kiện với Event Viewer**

1. Administrator Tools/Event Viewer
2. Xem log theo chế độ Windows Log, Application and Service Logs
3. Xem nhật ký hệ thống, Windows Logs/System
4. Cửa sổ giữa hiển thị tất cả các sự kiện

**6.3.2. Lọc sự kiện, lưu và xoá sự kiện**

1. Lọc sự kiện bằng cách, nhấp vào Filter Current Log… bên cửa sổ phải và chọn các tuỳ chọn để lọc sự kiện log
2. Lưu bộ lọc để xem lần sau, Cửa sổ phải chọn Save Filter to Custom … và đặt tên để lưu
3. Xoá bộ lọc, cửa sổ trái trong mục Custom Views, click chuột phải vào bộ lọc cần xoá và bấm Delete