



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

Microsoft Windows

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ giáo trình: Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.



Chương 4: Bảo trì, khắc phục lỗi và giám sát hoạt động của Windows

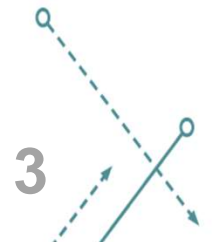
4.1 Cập nhật các bản vá Windows

4.2 Sao lưu và khôi phục dữ phòng

4.3 Khắc phục các sự cố trong Windows

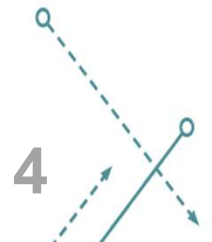
4.4 Giám sát hoạt động và kiểm toán Windows

4.5 Giới thiệu các công cụ quản trị Windows từ xa

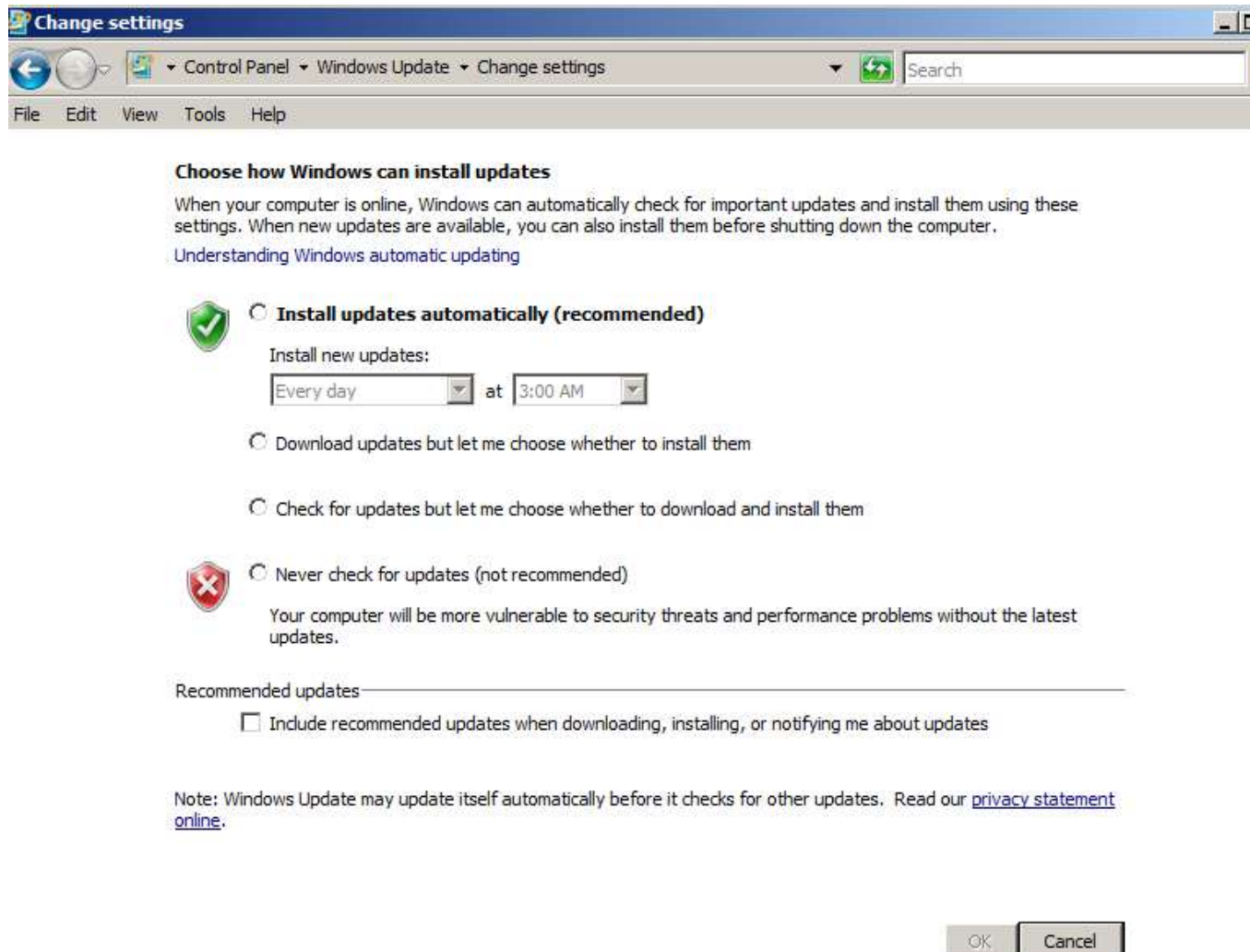


Cập nhật bản vá (1)

- Định kỳ chạy Windows update để kiểm tra bản bản cập nhật và vá lỗi.
- Lựa chọn cập nhật:
 - Định kỳ kiểm tra.
 - Tự động cập nhật/ nhắc nhở.
- Kiểm tra các gói dịch vụ - service pack.



Cập nhật bản vá (2)



Chương 4: Bảo trì, khắc phục lỗi và giám sát hoạt động của Windows

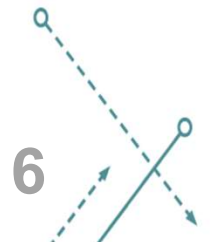
4.1 Cập nhật các bản vá Windows

4.2 Sao lưu và khôi phục dự phòng

4.3 Khắc phục các sự cố trong Windows

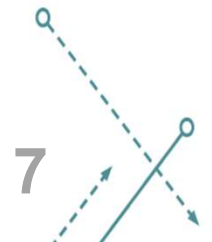
4.4 Giám sát hoạt động và kiểm toán Windows

4.5 Giới thiệu các công cụ quản trị Windows từ xa



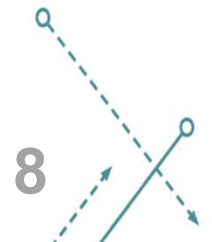
Sao lưu và khôi phục (1)

- Là các hoạt động tối quan trọng đảm bảo việc vận hành hệ thống được an toàn và tin cậy.
- Sao lưu back-up:
 - Tạo các bản sao của dữ liệu để có thể khôi phục dữ liệu gốc trong tình huống lỗi.
- Phương tiện sao lưu:
 - Ổ đĩa cứng
 - Ổ đĩa quang
 - Băng từ



Sao lưu và khôi phục (2)

- Băng từ đã từng là phương tiện sao lưu phổ biến cho khối lượng lớn dữ liệu. Tốc độ truy nhập chậm.
- Ổ cứng trở nên phổ biến do chi phí giảm, tốc độ truy nhập cao. Thường sử dụng ở dạng NAS hay SAN.
- Ổ đĩa quang: suy giảm chất lượng lưu trữ theo thời gian.



Băng từ VCR



Ổ cứng NAS



Ổ đĩa quang



Sao lưu và khôi phục (3)

- Lựa chọn mục sao lưu
 - Tách biệt chương trình và dữ liệu
 - Áp dụng chính sách sao lưu khác nhau

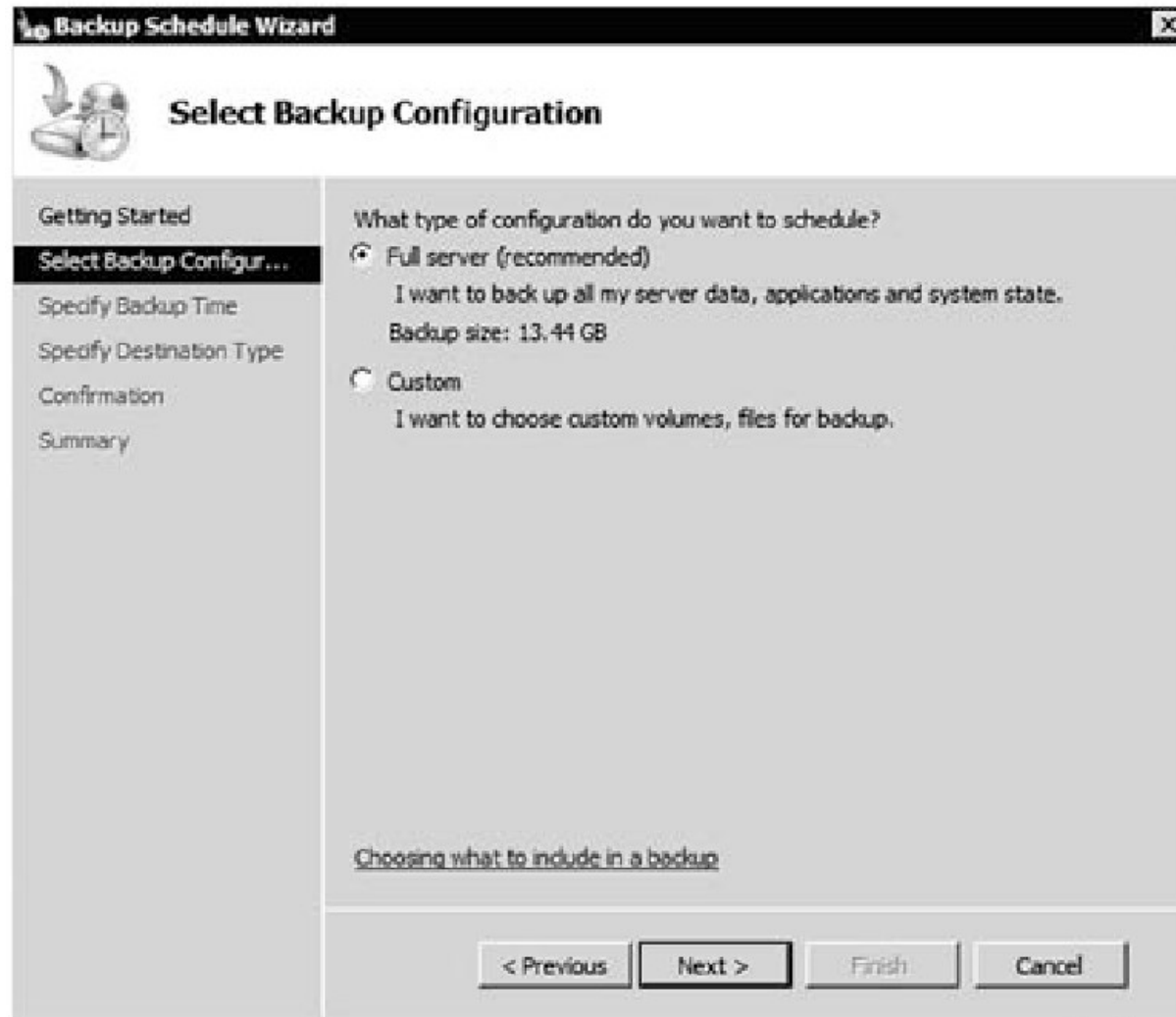
Sao lưu và khôi phục (4)

- Các phương pháp khác:
 - Trực tuyến: Dùng đĩa cứng hoặc chuỗi đĩa cứng có thể khôi phục ngay lập tức. Chi phí cao.
 - Cận trực tuyến: thường dùng băng từ, thời gian khôi phục lâu hơn.
 - Không trực tuyến: cần thao tác của người quản trị. Mất nhiều thời gian.
 - Sao lưu toàn bộ/sao lưu phòng thảm họa: sao lưu toàn bộ hệ thống phòng sự cố có thể chuyển sang vị trí khác để hoạt động.

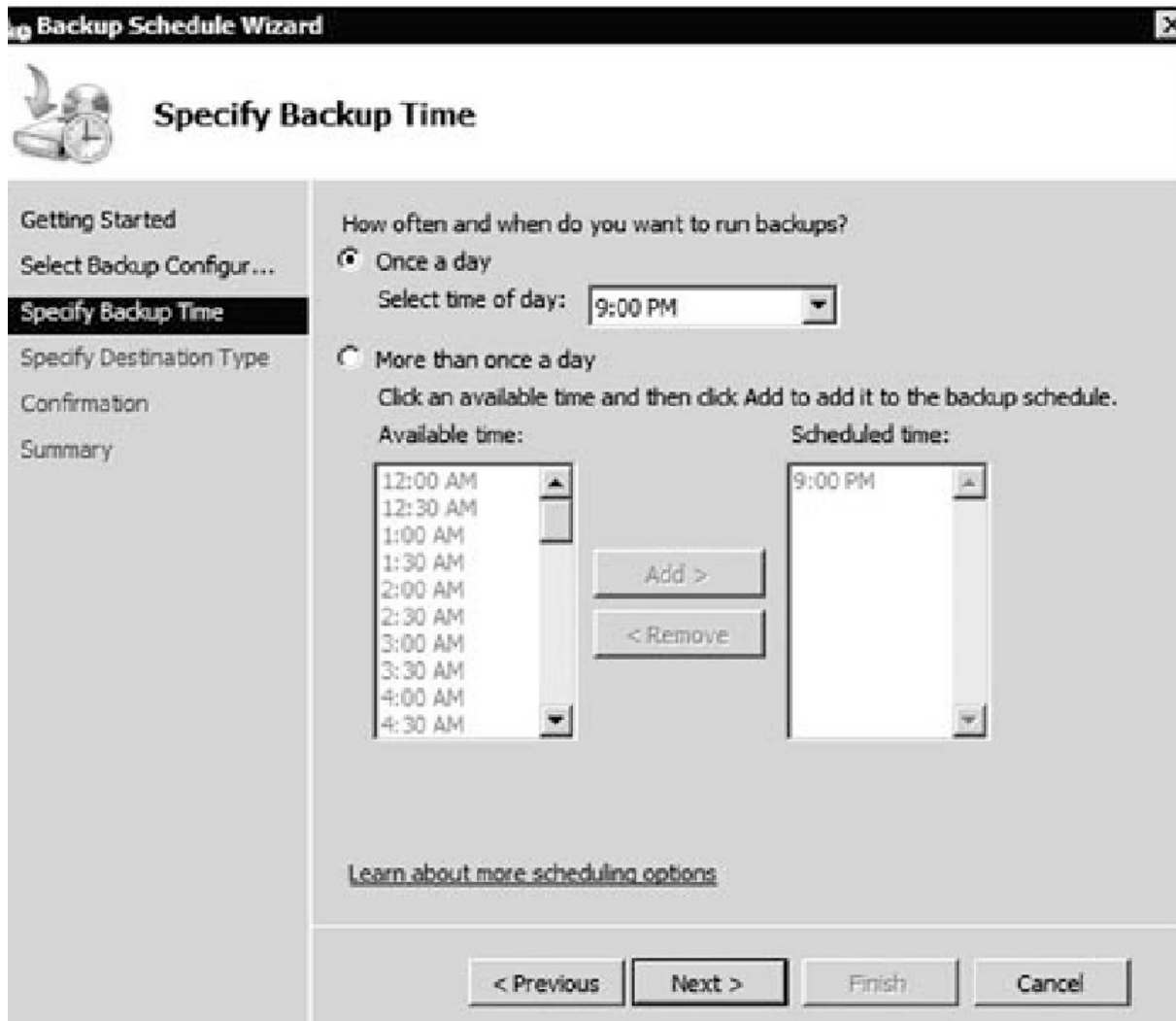
Các chính sách sao lưu

- Sao lưu toàn bộ
 - Tạo bản sao toàn bộ file và dữ liệu
- Sao lưu tăng dần
 - Sao lưu toàn bộ tiếp theo là sao lưu tăng dần
- Sao lưu khác biệt
 - Sao lưu toàn bộ tiếp theo là sao lưu các file và dữ liệu khác biệt

Windows Server Backup (1)



Windows Server Backup (2)



The screenshot shows the 'Specify Backup Time' step of the Windows Backup Schedule Wizard. The left sidebar contains the following steps: Getting Started, Select Backup Configur..., **Specify Backup Time**, Specify Destination Type, Confirmation, and Summary. The main area is titled 'Specify Backup Time' and contains the following text: 'How often and when do you want to run backups?'. There are two radio button options: 'Once a day' (selected) and 'More than once a day'. Under 'Once a day', there is a 'Select time of day:' dropdown menu showing '9:00 PM'. Under 'More than once a day', there is a text box that says 'Click an available time and then click Add to add it to the backup schedule.' Below this, there are two lists: 'Available time:' and 'Scheduled time:'. The 'Available time:' list contains times from 12:00 AM to 4:30 AM in 30-minute increments. The 'Scheduled time:' list is currently empty. Between the two lists are 'Add >' and '< Remove' buttons. At the bottom of the main area, there is a link that says 'Learn about more scheduling options'. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Chương 4: Bảo trì, khắc phục lỗi và giám sát hoạt động của Windows

4.1 Cập nhật các bản vá Windows

4.2 Sao lưu và khôi phục dự phòng

4.3 Khắc phục các sự cố trong Windows

4.4 Giám sát hoạt động và kiểm toán Windows

4.5 Giới thiệu các công cụ quản trị Windows từ xa



Khắc phục sự cố (1)

- Có hai cách tiếp cận khi xử lý lỗi
 - Kinh nghiệm: Xử lý vấn đề cụ thể đã gặp từ trước.
 - Hệ thống: nhằm xử lý triệt để vấn đề giảm thiểu việc dự đoán nguyên nhân.

Các bước phát hiện sự cố

1. Tìm ra vấn đề:
 - Xác định và ghi lại các triệu chứng của sự cố và tìm trong thư viện kỹ thuật như Microsoft Knowledge Base.
2. Đánh giá cấu hình hệ thống:
 - Tìm hiểu các thay đổi cấu hình (kiểm tra trong Event viewer).
3. Liệt kê hay theo dõi các giải pháp có thể và cố gắng cách ly vấn đề bằng cách loại bỏ phần cứng và phần mềm:
 - Chạy phần mềm kiểm tra hoặc theo dõi log file.
4. Thực hiện kế hoạch:
 - Thử các giải pháp tiềm năng và có kế hoạch với sự việc bất ngờ khi giải pháp không có tác dụng hay ảnh hưởng tiêu cực đến hệ thống.
5. Kiểm tra kết quả:
 - Nếu vấn đề vẫn tồn tại thì thực hiện các bước từ đầu.
6. Chủ động:
 - Ghi lại các thay đổi thực hiện trong khi xử lý sự cố.



Công cụ

- System Information
- Event Viewer
- Task Manager
- Resource Monitor
- Performance Monitor
- System Configuration
- Memory Diagnostics tool
- Troubleshooting Wizard
- Boot Menu including Safe mode
- Windows Repair

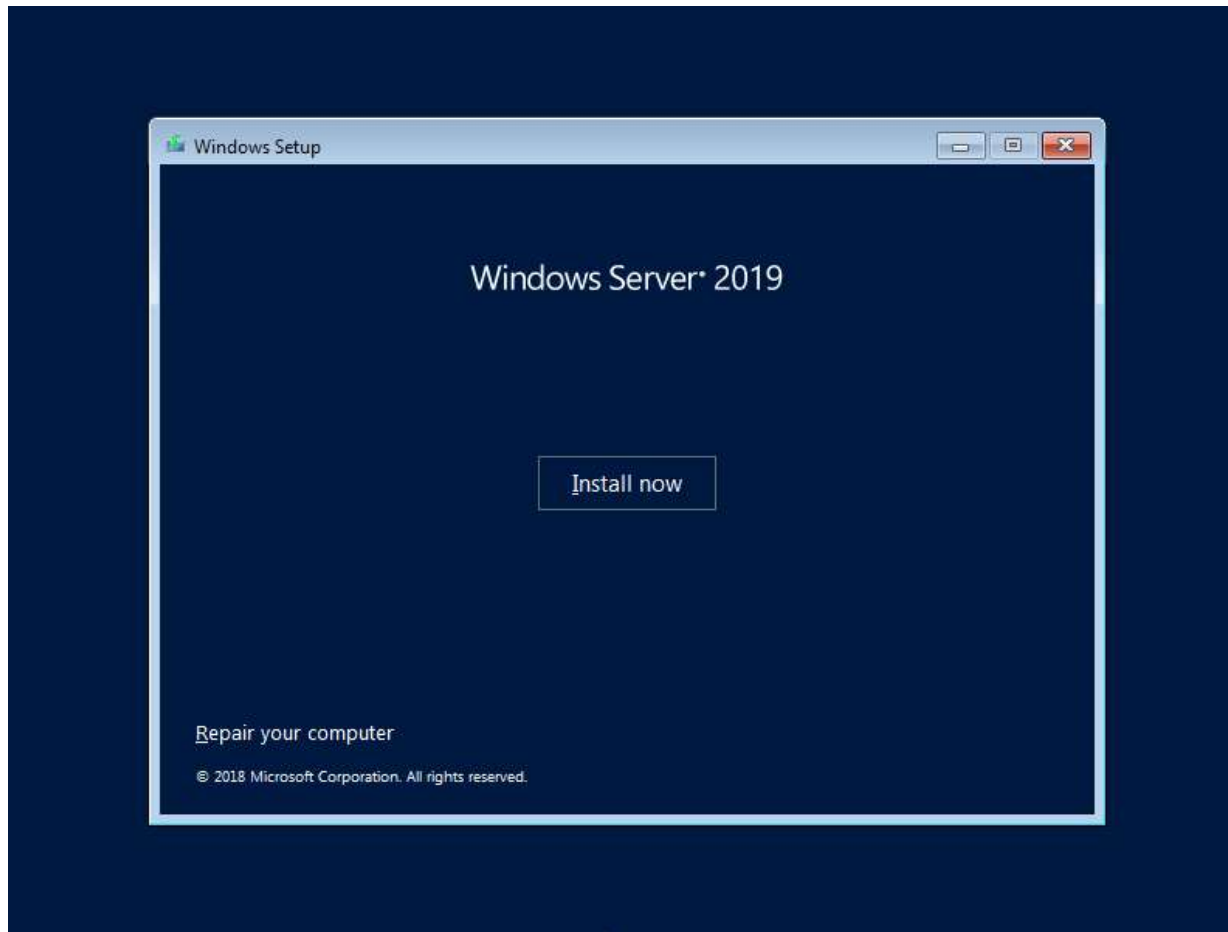


Khắc phục sự cố (2)

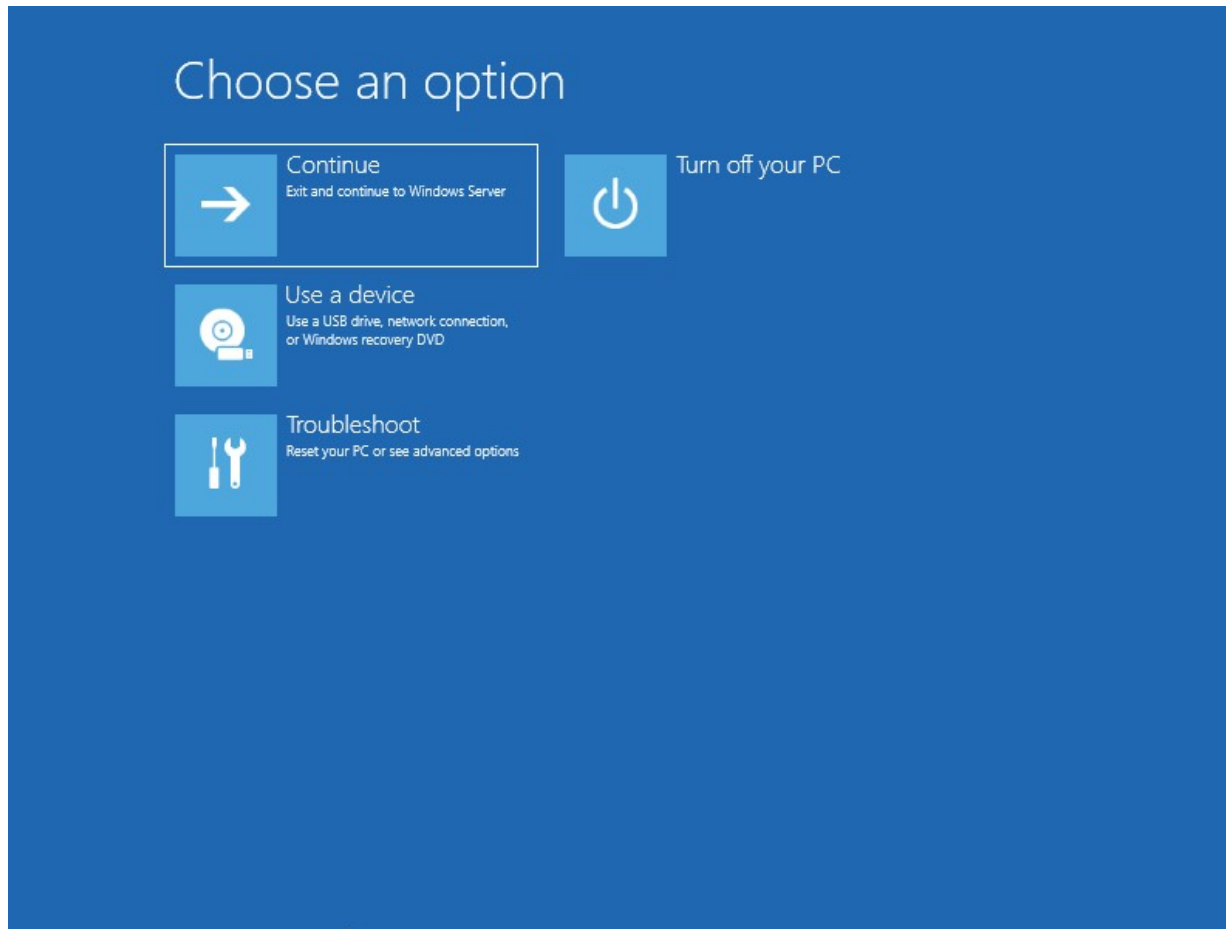
- Microsoft cung cấp Recovery Console để giúp quản trị xử lý trường hợp hệ thống không khởi động được.
- Chương trình Recovery console có thể được sử dụng qua giao diện dòng lệnh hoặc đồ họa



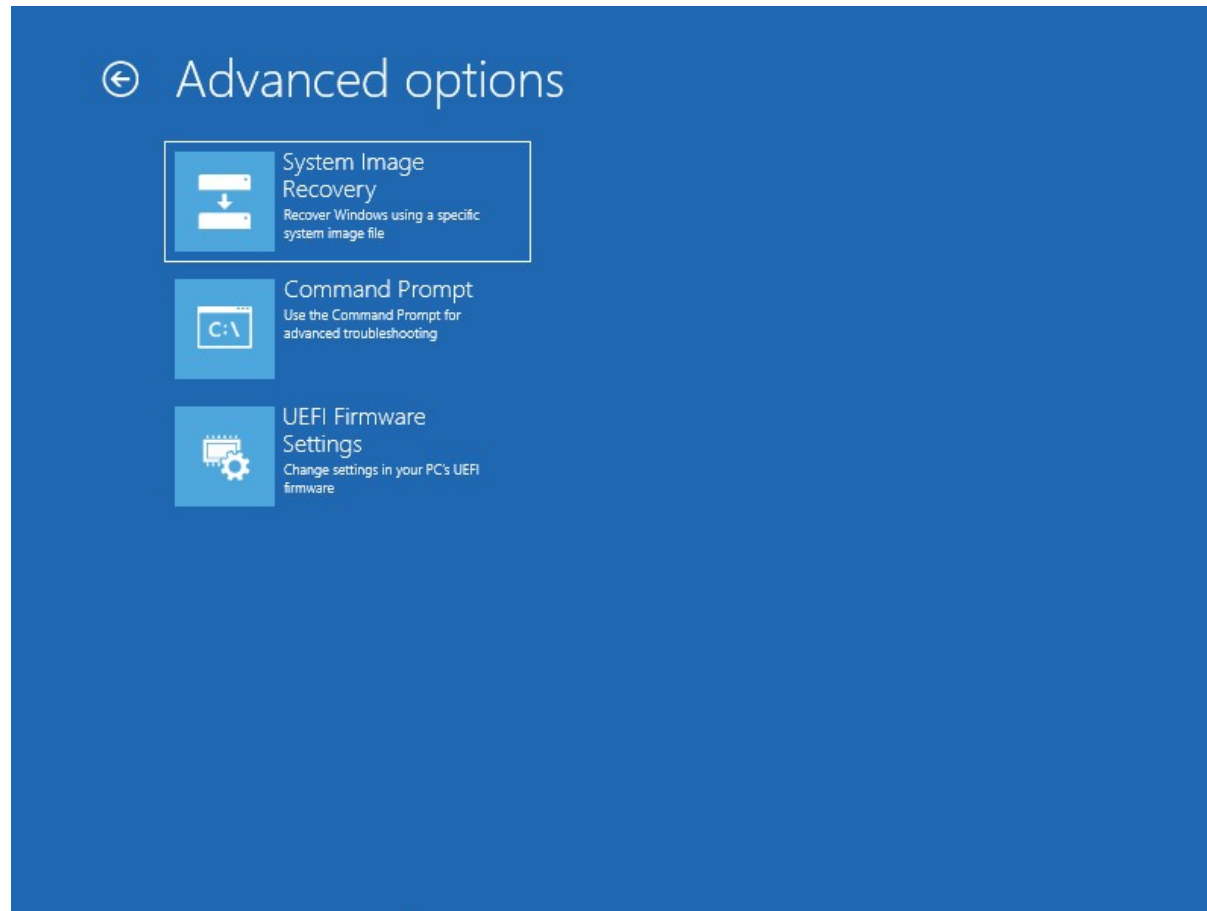
Giao diện cài đặt



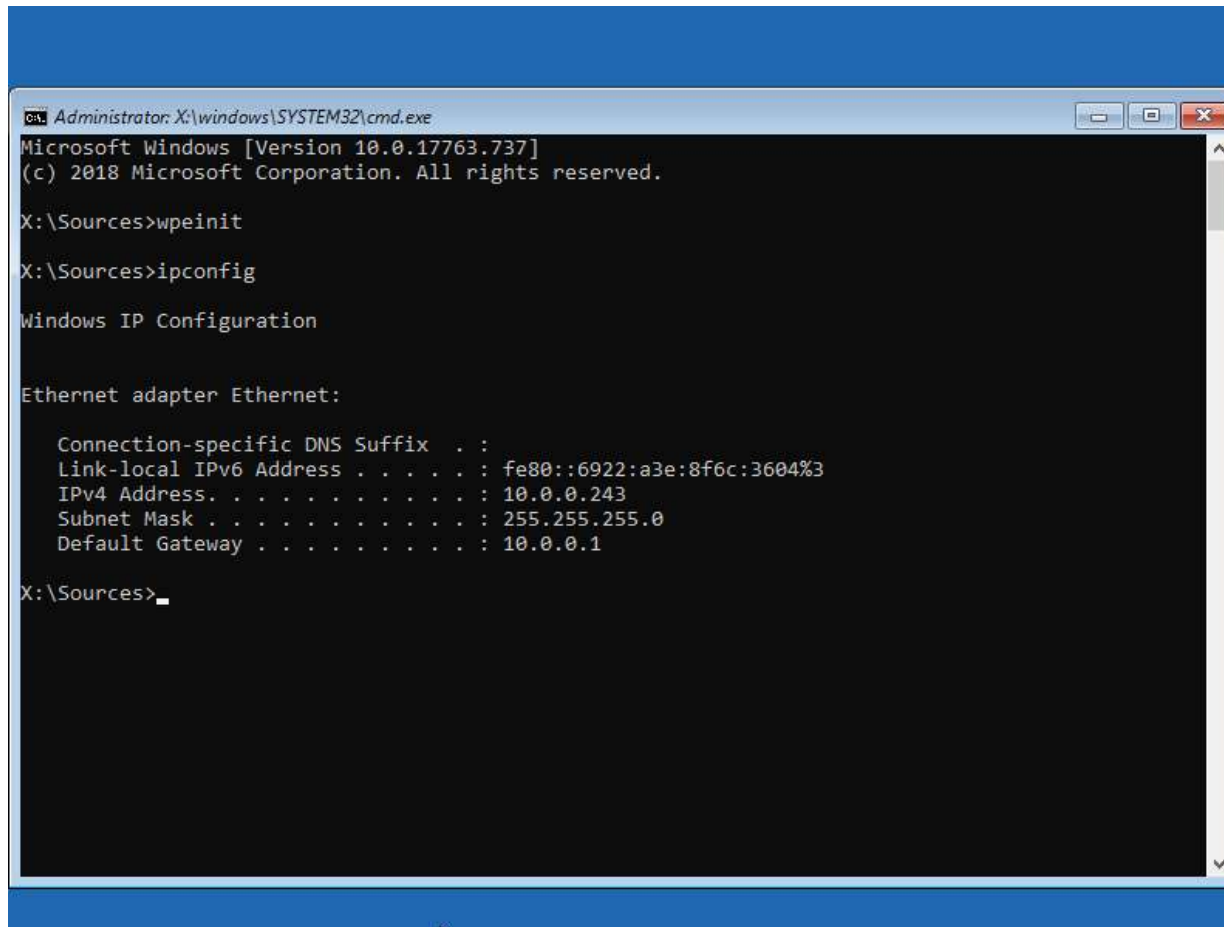
Khắc phục sự cố (3)



Khắc phục sự cố (4)



Khắc phục sự cố (5)



```
Administrator: X:\windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

X:\Sources>wpeinit
X:\Sources>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6922:a3e:8f6c:3604%3
    IPv4 Address. . . . . : 10.0.0.243
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

X:\Sources>
```



Một số câu lệnh

- Bootcfg: thay đổi tham số khởi động
- Chkdsk: Kiểm tra ổ đĩa
- Diskpart: Quản lý các phân vùng trên ổ đĩa cứng
- Format: định dạng ổ đĩa
- Listsvc: Liệt kê các dịch vụ và trình điều khiển trên máy tính.
- Fixmbr: Chữa phân vùng khởi động



Chương 4: Bảo trì, khắc phục lỗi và giám sát hoạt động của Windows

4.1 Cập nhật các bản vá Windows

4.2 Sao lưu và khôi phục dự phòng

4.3 Khắc phục các sự cố trong Windows

4.4 Giám sát hoạt động và kiểm toán Windows

4.5 Giới thiệu các công cụ quản trị Windows từ xa



Giám sát và kiểm toán

- Microsoft cung cấp một số công cụ cho người quản trị theo dõi hiệu năng và việc sử dụng tài nguyên hệ thống:
 - Performance Monitor
 - Task Manager
 - Resource Monitor
 - Event Viewer

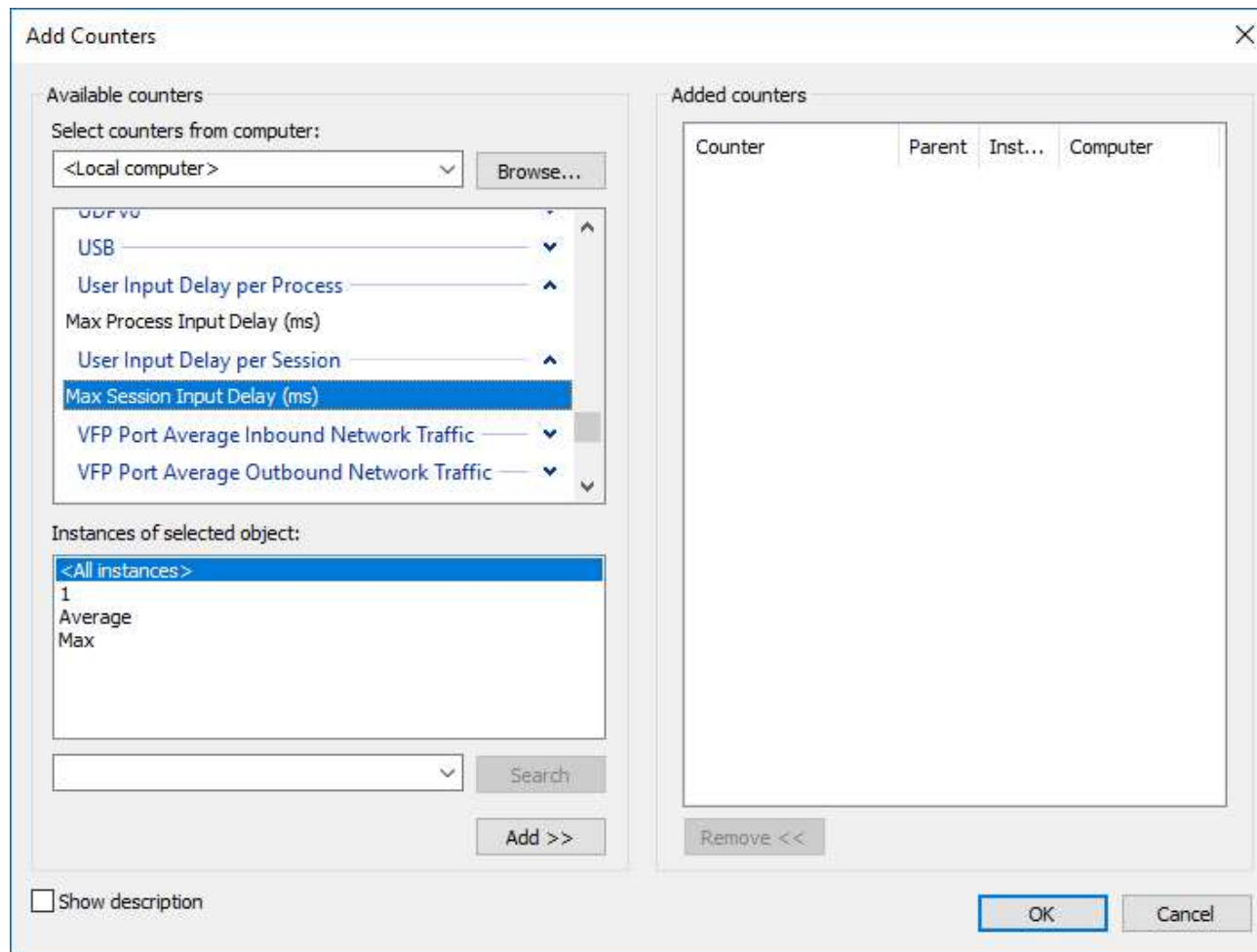


Giám sát hiệu năng (1)

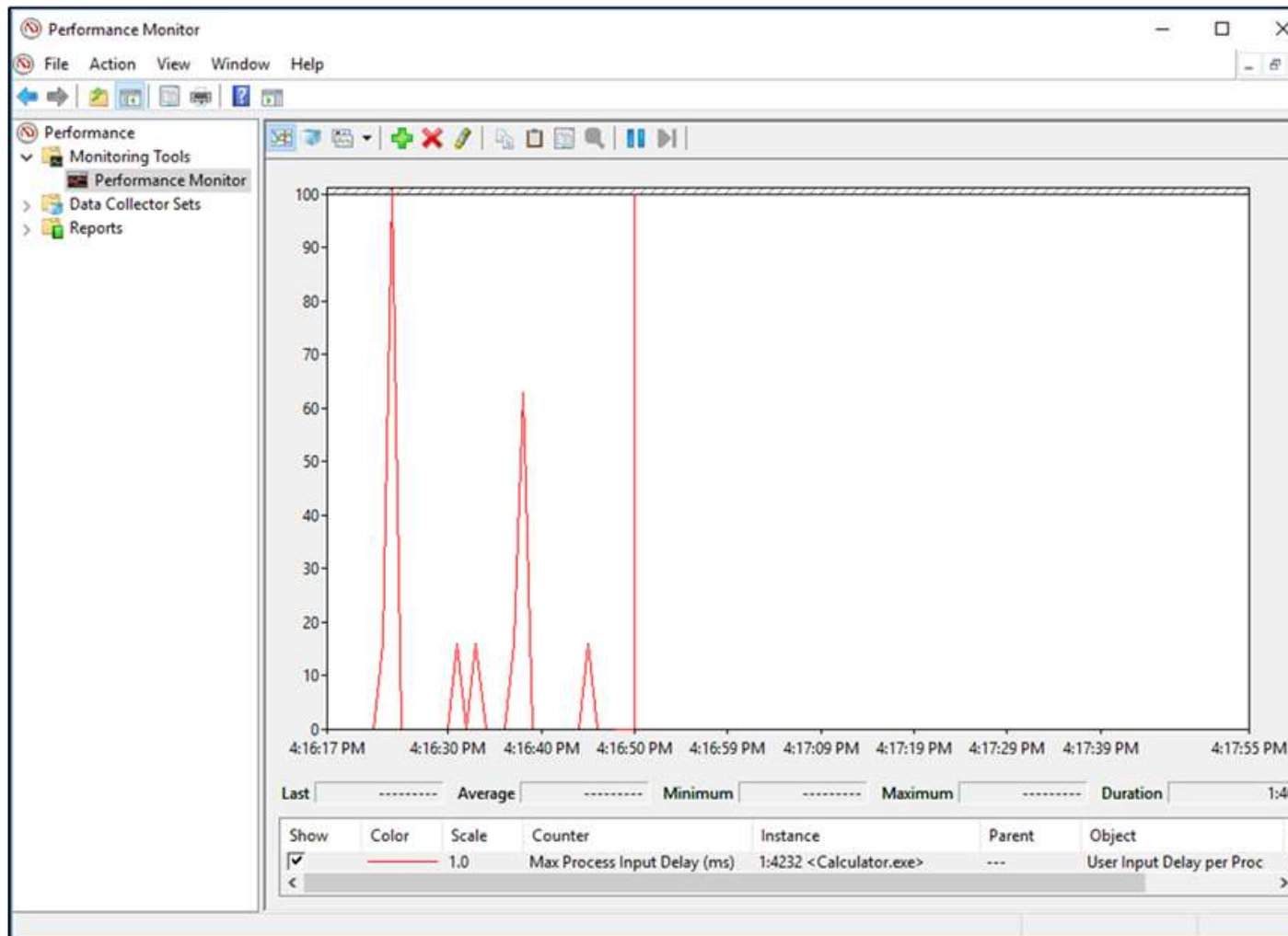
- Thực hiện thông qua dữ liệu thu thập từ các bộ đếm (counter):
 - Đếm hiệu năng: Là các đối tượng được giám sát bởi chức năng giám sát hiệu năng như bộ xử lý, bộ nhớ, ổ đĩa.
 - Thể hiện: Cho phép xem dữ liệu một cách chi tiết thu được từ các bộ đếm.



Giám sát hiệu năng (2)



Giám sát hiệu năng (3)

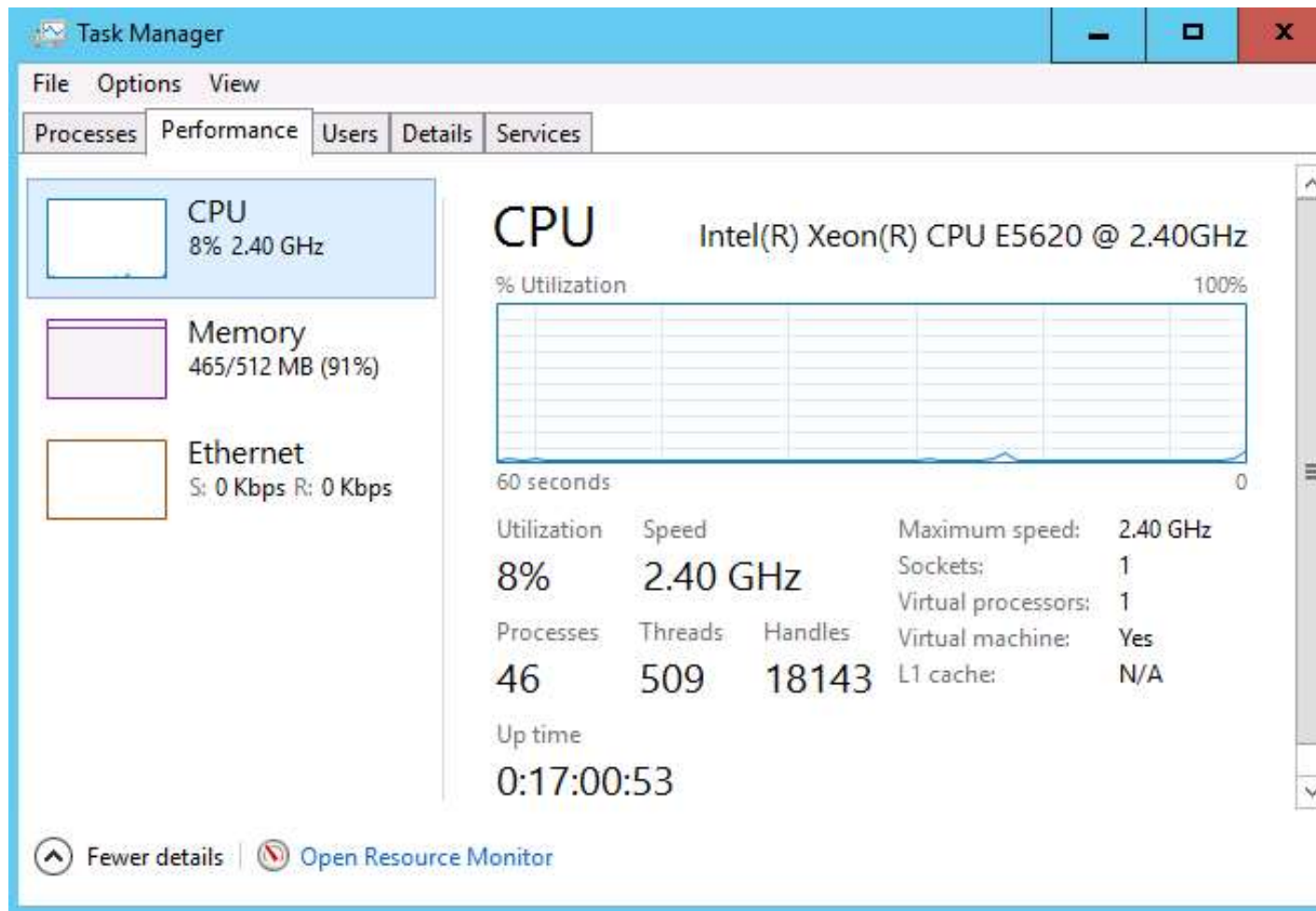


Giám sát công việc và tài nguyên (1)

- Giám sát công việc (Windows task manager)
 - Theo dõi thông tin hiệu năng, các ứng dụng và tiến trình đang chạy, danh sách người dùng đăng nhập vào hệ thống
 - Mục ứng dụng:
 - Danh sách ứng dụng đang chạy và trạng thái
 - Tiến trình
 - Các tiến trình của người dùng
 - Dịch vụ
 - Các dịch vụ Windows đang chạy
 - Hiệu năng
 - Theo dõi việc sử dụng CPU
 - Kết nối mạng
 - Giám sát các card mạng được cài đặt và việc sử dụng chúng
 - Người dùng



Giám sát công việc và tài nguyên (2)

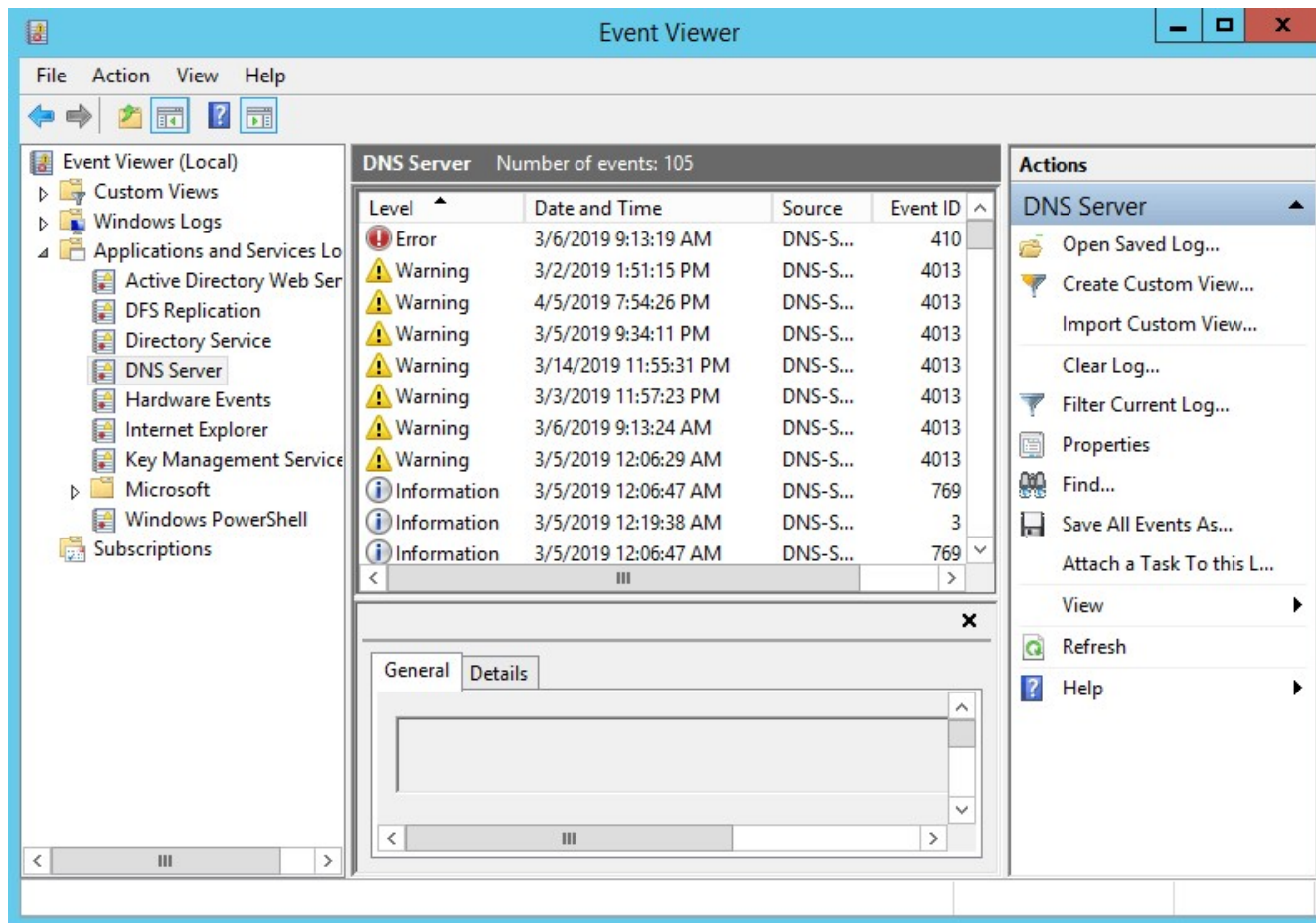


Nhật ký Windows

- Lưu lại các sự kiện phục vụ mục đích theo dõi. Có hai kiểu file nhật ký sự kiện là:
 - Nhật ký Windows.
 - Nhật ký dịch vụ và ứng dụng.



Nhật ký Windows



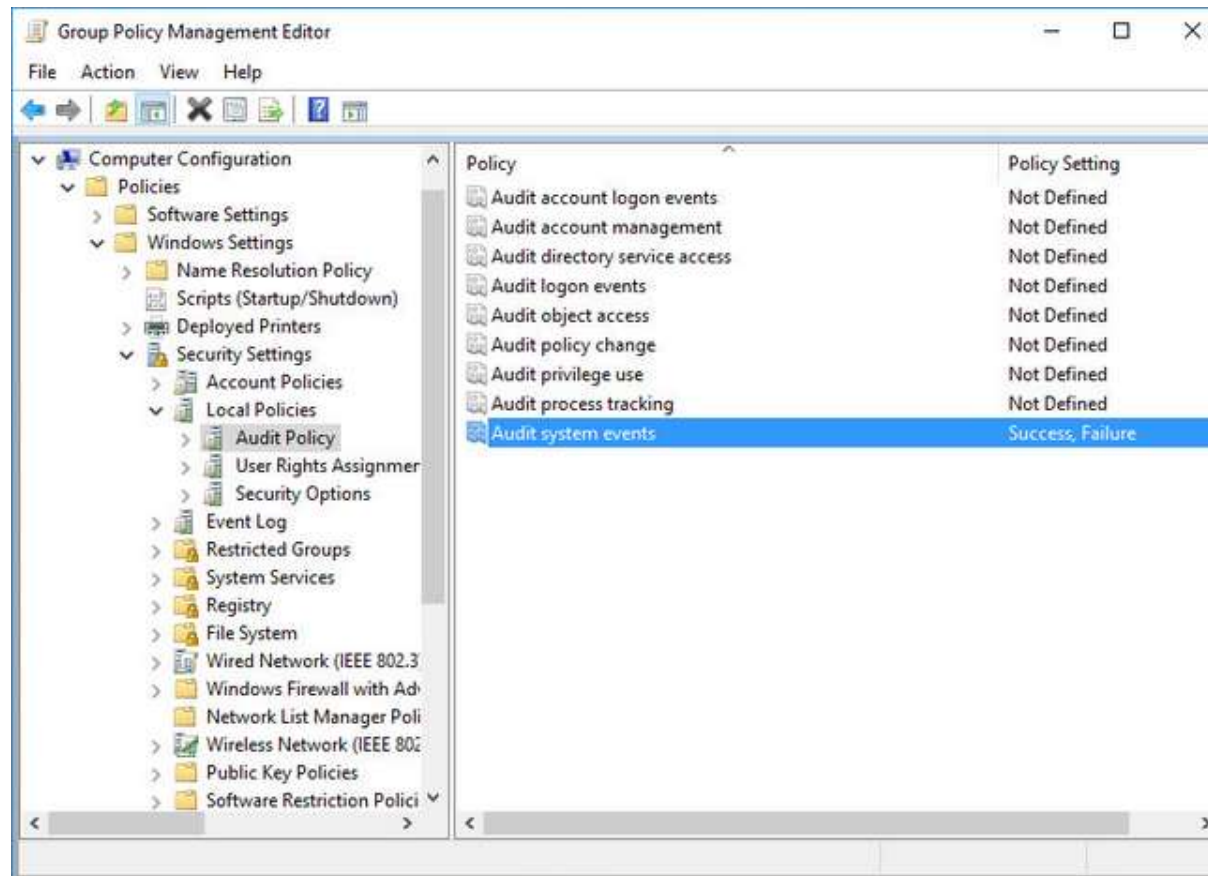
Kiểm toán Auditing

- Lưu lại thông tin về người dùng đăng nhập và tài nguyên mà người dùng đó sử dụng
- Thông tin kiểm toán gồm có:
 - Người đăng nhập thành công,
 - Người cố đăng nhập không thành công,
 - Người thay đổi tài khoản trong thư mục động,
 - Người truy nhập và sửa đổi file,
 - Người sử dụng máy in,
 - Người khởi động lại hệ thống,
 - Người thay đổi tham số hệ thống.



Kiểm toán

- Kiểm toán được kích hoạt qua Group Policy
 - Security Settings\Local Policies\Audit Policy



Chương 4: Bảo trì, khắc phục lỗi và giám sát hoạt động của Windows

4.1 Cập nhật các bản vá Windows

4.2 Sao lưu và khôi phục dự phòng

4.3 Khắc phục các sự cố trong Windows

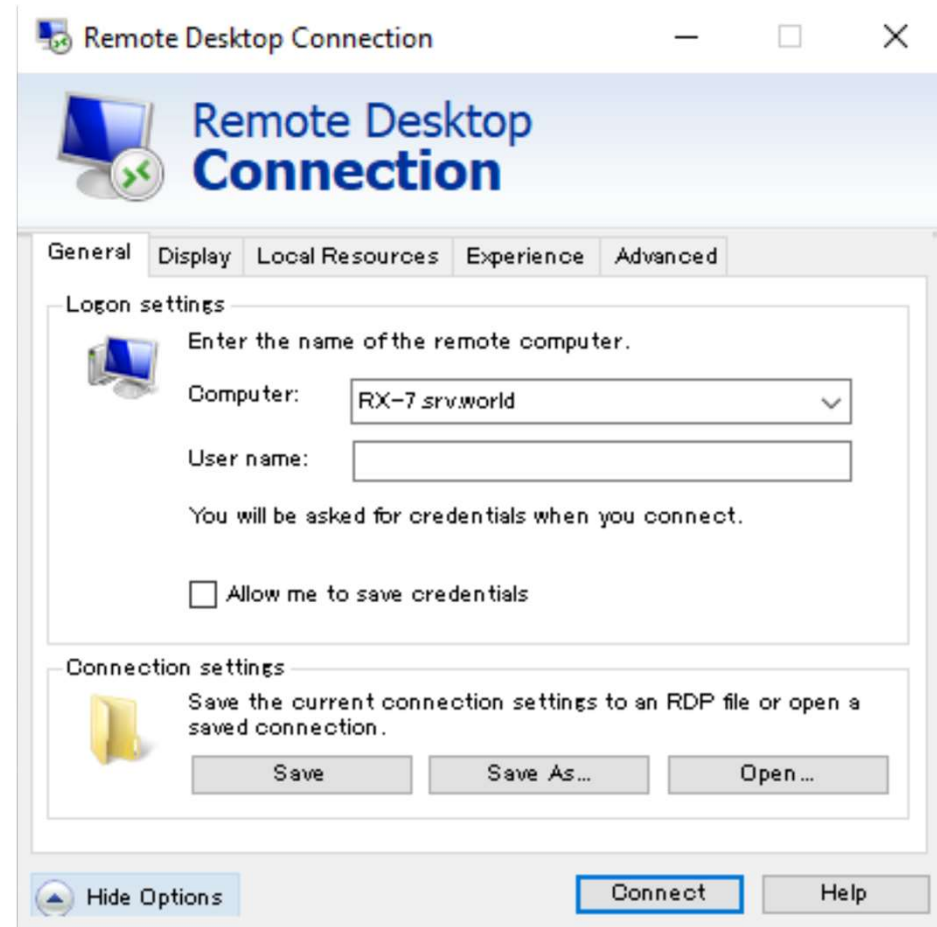
4.4 Giám sát hoạt động và kiểm toán Windows

4.5 Giới thiệu các công cụ quản trị Windows từ xa

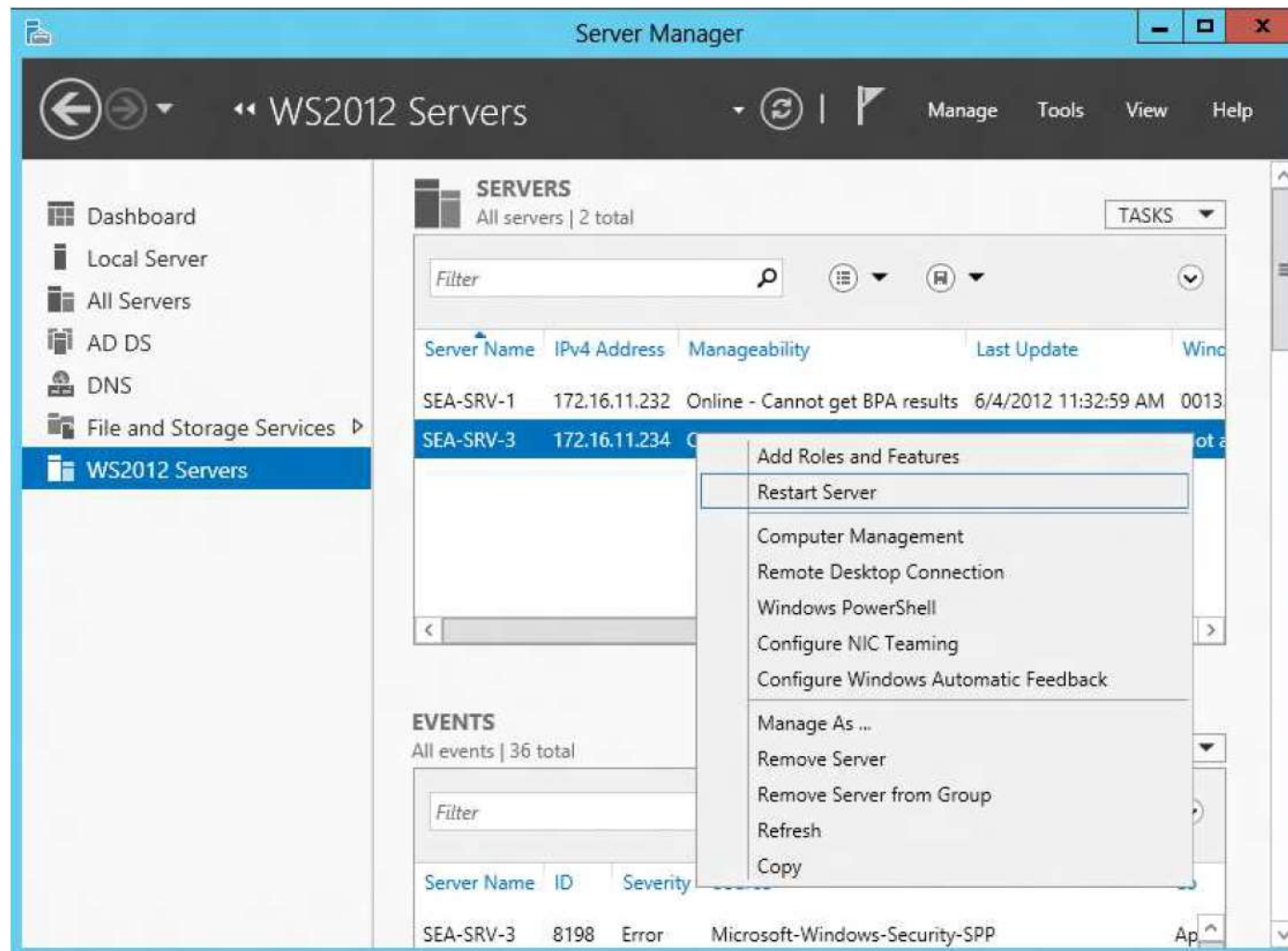


Quản trị từ xa (1)

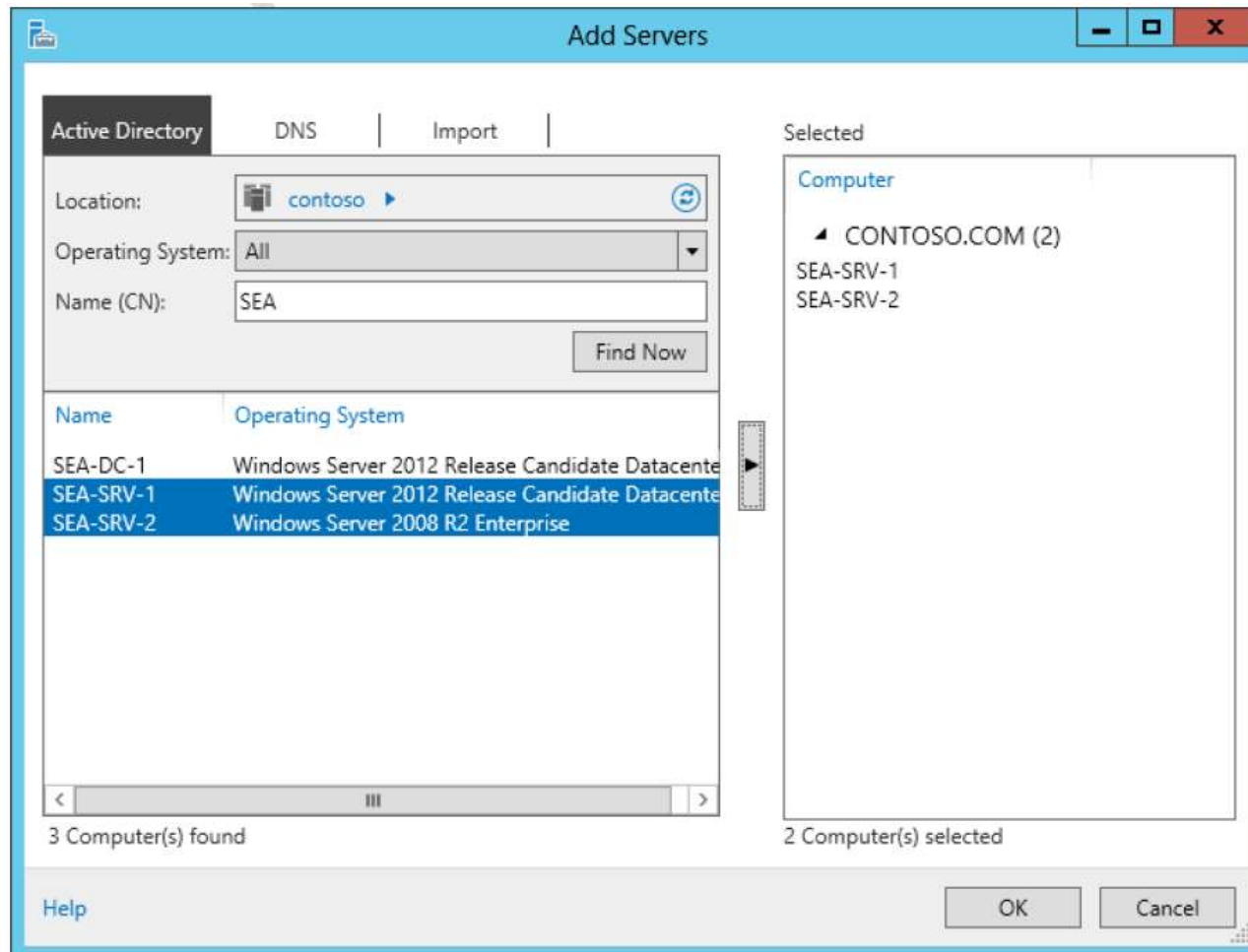
- Remote Desktop Services (Terminal Services) cho phép người dùng truy nhập ứng dụng và dữ liệu trên máy tính mạng
- Ngầm định hỗ trợ 2 phiên làm việc



Quản trị từ xa (2)



Quản trị từ xa (3)



Remote Desktop Web

- Chạy ứng dụng và dữ liệu từ xa qua trình duyệt

