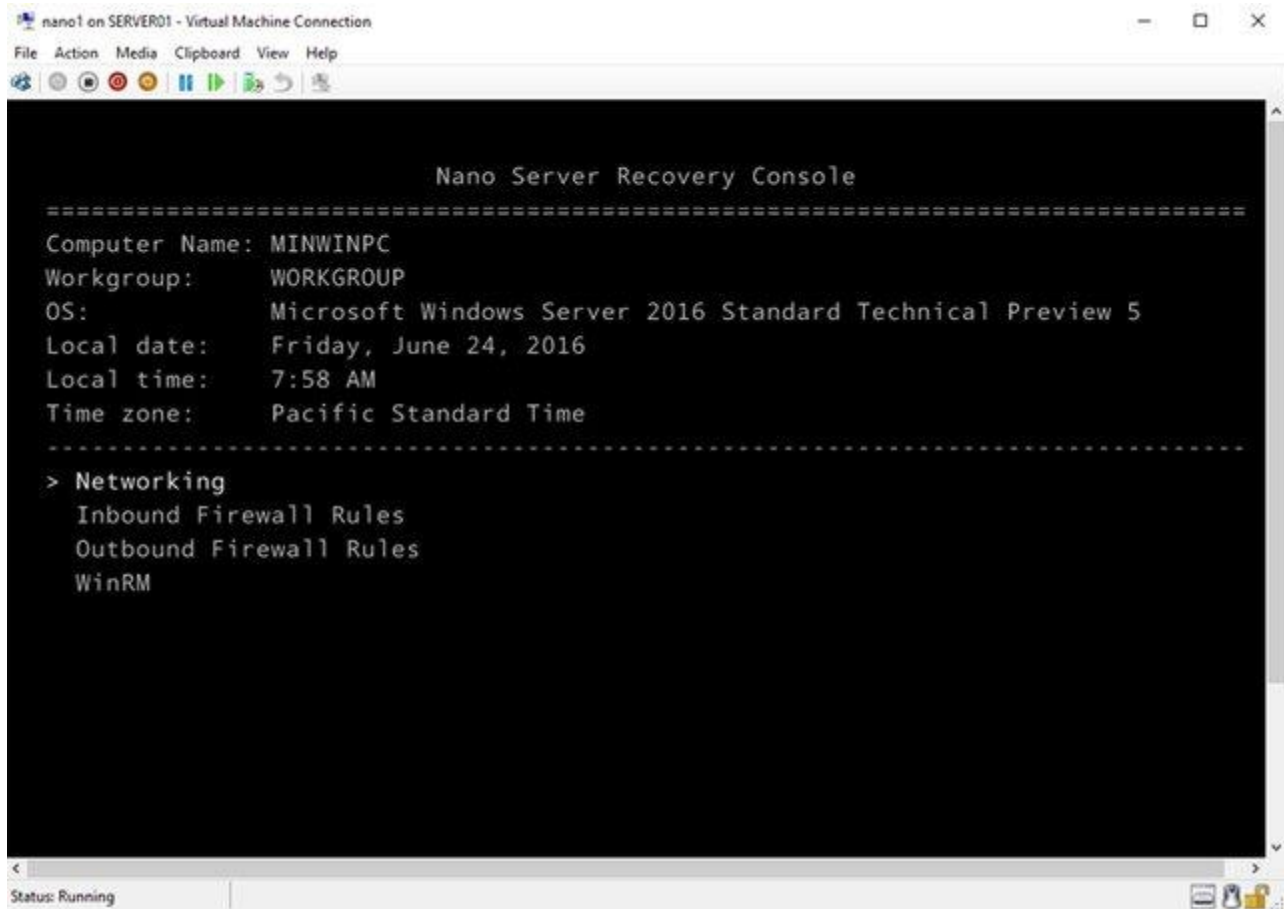


## 10 tính năng tốt nhất của Windows Server 2016

Hiện giờ, người dùng có thể sử dụng Windows Server 2016. Bản phát hành này phản ánh xu hướng công nghệ thông tin hiện đại và kết nối lai với các dịch vụ đám mây. Bài viết sẽ giới thiệu cho các bạn 10 tính năng tốt nhất của Windows Server 2016.

### 1. Nano Server

Nano Server tự hào có cài đặt nhỏ hơn 92 phần trăm so với tùy chọn cài đặt giao diện đồ họa người dùng Windows Server (GUI). Ngoài ra, những lý do thuyết phục sau có thể khiến bạn bắt đầu chạy Nano cho các lượng công việc Windows Server:



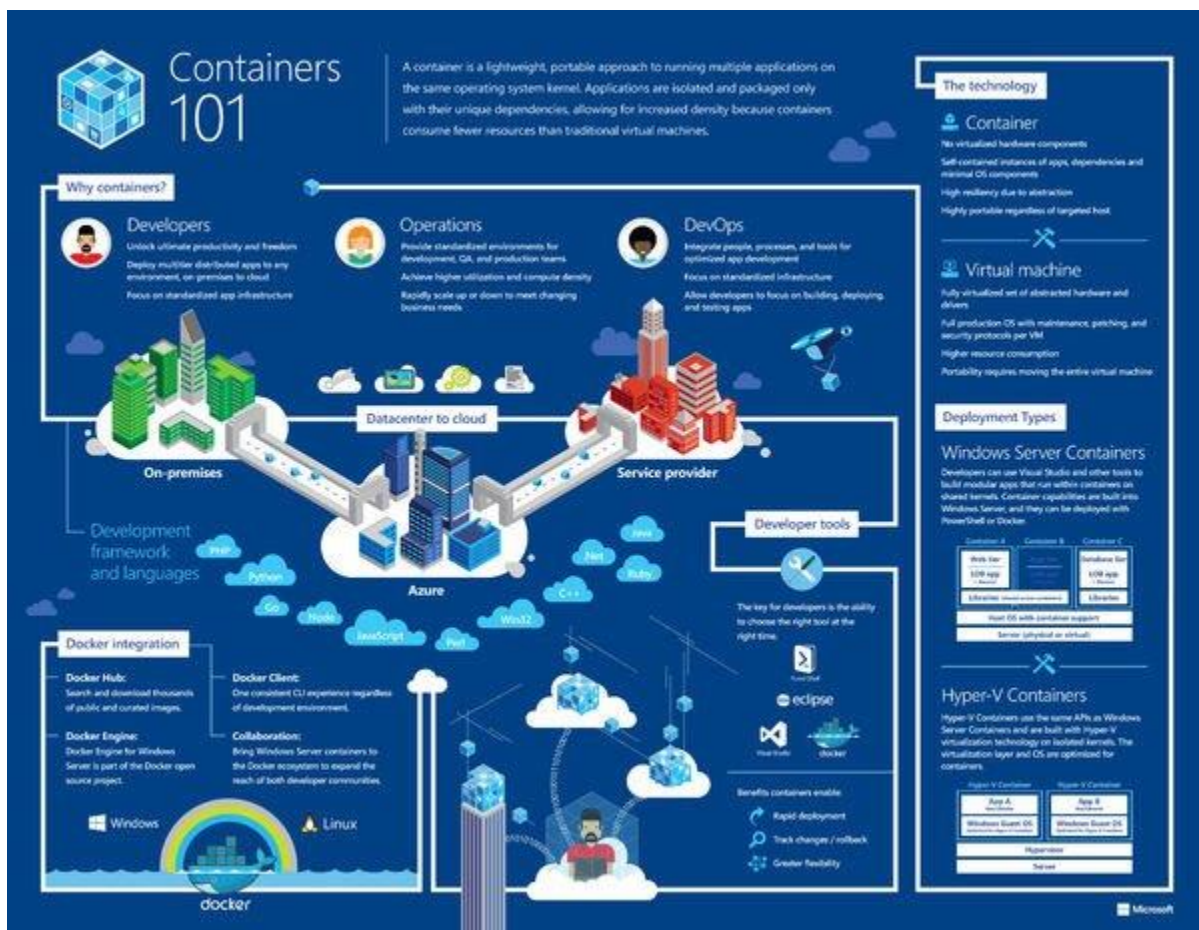
```
nano1 on SERVER01 - Virtual Machine Connection
File Action Media Clipboard View Help
Nano Server Recovery Console
=====
Computer Name: MINWINPC
Workgroup:      WORKGROUP
OS:             Microsoft Windows Server 2016 Standard Technical Preview 5
Local date:     Friday, June 24, 2016
Local time:     7:58 AM
Time zone:      Pacific Standard Time
-----
> Networking
  Inbound Firewall Rules
  Outbound Firewall Rules
  WinRM
```

- Hệ điều hành Bare-metal có nghĩa là người dùng sẽ phải ít cập nhật và khởi động lại.
- Bởi vì người dùng phải vào các vai trò máy chủ từ bên ngoài Nano, nên máy chủ sẽ có một bề mặt tấn công giảm nhiều khi so với GUI Windows Server.

- Nano nhỏ đến mức nó có thể được chuyển dễ dàng qua các máy chủ, trung tâm dữ liệu và các trang web vật lý.
- Nano lưu trữ các khối lượng công việc Windows Server phổ biến nhất bao gồm máy chủ Hyper-V.

Nano được thiết kế để quản lý hoàn toàn từ xa. Tuy nhiên, Nano bao gồm một giao diện quản lý cục bộ tối thiểu được gọi là "Nano Server Recovery Console" cho phép thực hiện các tác vụ cấu hình ban đầu.

## 2. Container (vật chứa)



Microsoft đang làm việc với nhóm phát triển Docker để mang container dựa trên Docker vào Windows Server. Cho đến nay, container đã tồn tại gần như hoàn toàn trong thế giới mã nguồn mở Linux/UNIX. Chúng cho phép bạn tách các ứng dụng

và dịch vụ một cách nhanh chóng để dễ quản lý. Windows Server 2016 cung cấp hai loại dịch vụ chứa Windows Sever khác nhau:

- **Windows Server Container.** Loại container này dành cho các khối lượng công việc có độ tin cậy thấp và không cần quan tâm khi dịch vụ container (container instance) chạy trên cùng một máy chủ có thể chia sẻ một số tài nguyên thông thường.
- **Hyper-V Container.** Đây không phải là máy chủ lưu trữ Hyper-V hoặc máy ảo. Dịch vụ chứa Windows Server của nó “hoàn toàn tách biệt với các container khác và máy chủ lưu trữ khác. Các container Hyper-V thích hợp với khối lượng công việc có độ tin tưởng cao.

### 3. Chế độ Secure Boot Linux

Chế độ Secure Boot là một phần thông số giao diện firmware mở rộng hợp nhất (Unified Extensible Firmware Interface - UEFI) bảo vệ môi trường khởi động của máy chủ chống lại việc lây nhiễm rootkit hoặc các phần mềm độc hại khởi động khác.

Vấn đề với Secure Boot dựa trên Windows Server là máy chủ của bạn sẽ gặp sự cố nếu cố tạo một máy ảo Hyper-V thế hệ 2 dựa trên Linux vì driver hạt nhân Linux không phải là thiết bị đáng tin cậy. Về mặt kỹ thuật, firmware UEFI của máy ảo hiển thị lỗi "Failed Secure Boot Verification" (Không xác thực khởi động bảo mật) và dừng khởi động.

Các đội ngũ kỹ sư của Windows Server và Azure dường như rất yêu thích Linux. Vì vậy, bây giờ chúng ta có thể triển khai các máy ảo Linux trong Windows Server 2016 Hyper-V mà không bắt cứ vấn đề gì mà không cần phải vô hiệu hóa tính năng Secure Boot.

### 4. ReFS

Resilient File System (ReFS) đã có được một thời gian dài trên Windows Server. Trong Windows Server 2016, cuối cùng người dùng cũng có thể sử dụng được phiên bản ReFS ổn định. ReFS là một hệ thống tệp tin hiệu suất cao, có khả năng khôi phục tốt được sử dụng với Storage Spaces Direct và khối lượng công việc của Hyper-V.

## **5. Tính năng Storage Spaces Direct**

Storage Spaces là một tính năng Windows Server tuyệt vời giúp các quản trị viên tạo ra dung lượng đĩa dự phòng linh hoạt hơn. Tính năng Storage Spaces Direct trong Windows Server 2016 là tính năng nâng cấp từ Storage Spaces cho phép các node trong failover cluster sử dụng bộ nhớ cục bộ bên trong cluster này, không cần dùng bộ lưu trữ dùng chung (storage fabric).

## **6. ADFS v4**

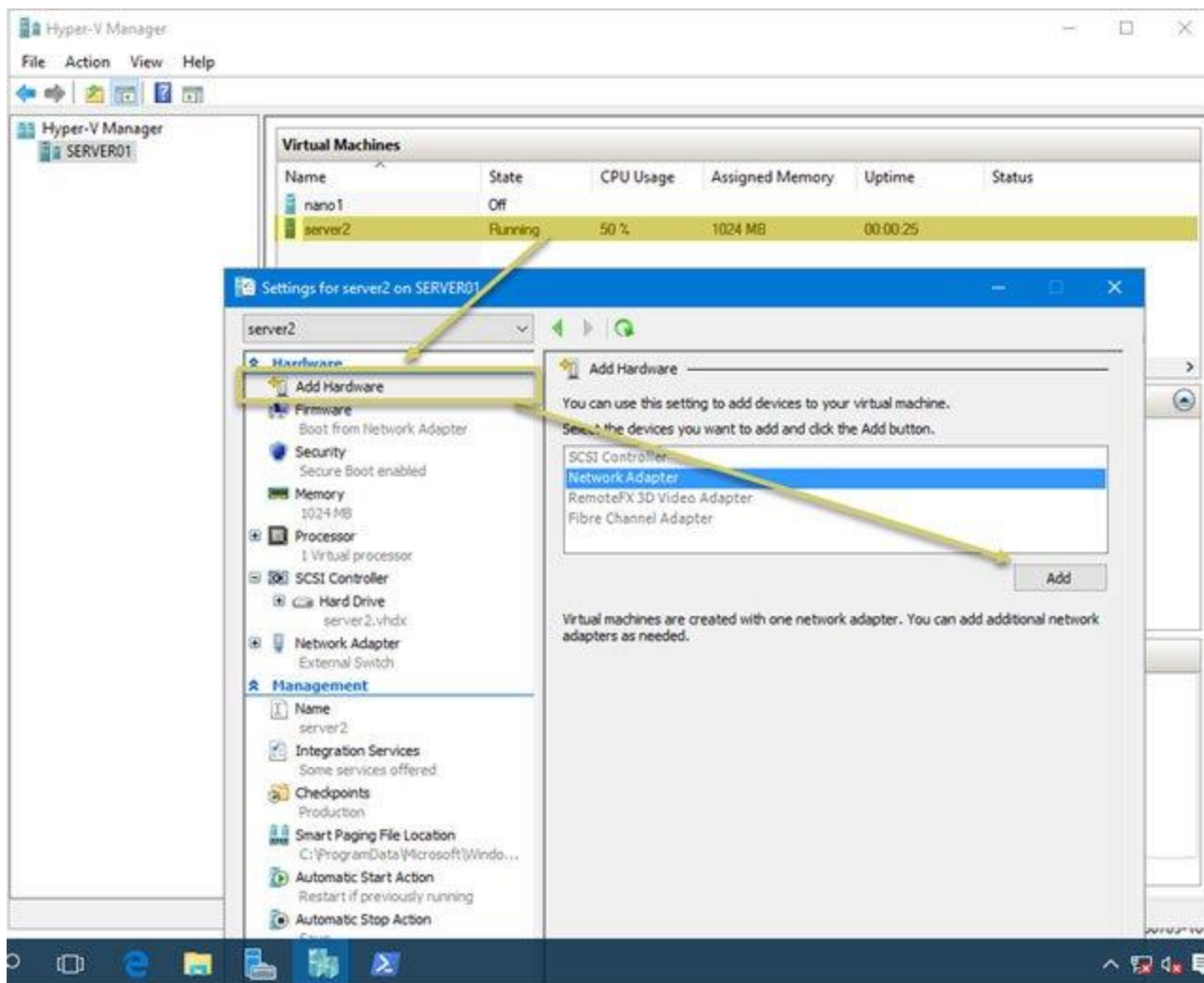
Active Directory Federation Services (ADFS) là một vai trò Windows Server hỗ trợ nhận dạng dựa trên tuyên bố (Claims -based identity) (token). Xác định danh tính dựa trên tuyên bố là rất quan trọng nhờ sự cần thiết phải xác thực một lần (SSO) giữa Active Directory tại chỗ và các dịch vụ dựa trên đám mây khác nhau.

ADFS v4 trong Windows Server 2016 cuối cùng đã mang đến sự hỗ trợ cho xác thực dựa trên kết nối OpenID, xác thực đa yếu tố (MFA) và "truy cập có điều kiện kết hợp". Công nghệ này cho phép ADFS phản hồi khi các thuộc tính của người dùng hoặc thiết bị không tuân thủ các chính sách bảo mật ở cả hai điểm cuối của mối quan hệ tin cậy (trust relationship).

## **7. Nested Virtualization (ảo hóa lồng nhau)**

Ảo hóa lồng nhau đề cập đến khả năng của một máy ảo đối với máy chủ ảo. Ảo hóa lồng nhau có tác dụng khi một doanh nghiệp muốn triển khai các máy chủ Hyper-V bổ sung và nhu cầu để giảm thiểu chi phí phần cứng.

## **8. Phần cứng ảo Hyper-V**



Hyper-V Server cho phép thêm phần cứng ảo hoặc điều chỉnh RAM được phân bổ cho một máy ảo. Tuy nhiên, trước đây để thực hiện những thay đổi này cần phải tắt máy ảo trước. Bây giờ, trong Windows Server 2016, chúng ta có thể thêm phần cứng ảo trong khi các máy ảo đang trực tuyến và đang chạy.

## 9. PowerShell Direct

Trong Windows Server 2012 R2, các quản trị viên Hyper-V thường thực hiện quản lý từ xa cho máy ảo dựa trên Windows PowerShell theo cách tương tự với các máy chủ vật lý. Trong Windows Server 2016, các lệnh từ xa của PowerShell giờ đây có các tham số `-VM *` cho phép gửi PowerShell trực tiếp vào các máy ảo của máy chủ Hyper-V.

```
Invoke-Command -VMName 'server2' -ScriptBlock {Stop-Service -Name Spooler} -Credential 'tomsitprotim' -Verbose
```

Chúng ta đã sử dụng tham số **-VMName** mới của các lệnh Invoke-Command để chạy các lệnh Stop-Service trên máy ảo Hyper-V có tên server2.

## **10. Máy ảo được bảo vệ (Shielded VM)**

Vai trò máy chủ Host Guardian Service mới là lưu trữ tính năng máy ảo được bảo vệ. Windows Server 2016 đã bảo vệ các máy ảo, cho phép kiểm soát sâu hơn, tinh vi hơn đối với truy cập máy ảo Hyper-V.

Ví dụ, máy chủ Hyper-V có thể có các máy ảo từ nhiều người dùng và cần đảm bảo rằng các nhóm quản trị viên Hyper-V khác nhau chỉ có thể truy cập vào các máy ảo được chỉ định. Bằng cách sử dụng BitLocker Drive Encryption để mã hóa các đĩa cứng ảo của máy ảo, các máy ảo được bảo vệ có thể giải quyết được vấn đề đó.