

10 LÝ DO ĐỂ CÀI ĐẶT WINDOWS SERVER 2008

Hệ điều

Hệ điều hành máy chủ mới được Microsoft đưa ra gần đây: Windows Server 2008 (Windows Longhorn) có thực sự là một hệ điều hành tốt nhất, bảo mật hiệu quả nhất dành cho máy chủ không? Câu trả lời còn phụ thuộc tùy vào từng người dùng cụ thể nhưng dù sao thì 10 lý do sau cũng giúp bạn thấy rõ được có thực sự cần cài đặt Windows Server 2008 trên máy chủ của mình không và nó có những tính năng gì khác so với các hệ điều hành máy chủ trước đây của Microsoft.

Windows Server Virtualization

Windows Server 2008 gồm có Windows Server Virtualization (WSv), một công nghệ mạnh, hiệu quả và ảo hóa với sự quản lý mạnh và các tính năng bảo mật cao. Windows Server Virtualization sẽ giúp các doanh nghiệp giảm được chi phí, tăng khả năng linh hoạt và tính sẵn có của hệ thống trong việc hợp nhất máy chủ, khôi phục thảm họa, kiểm tra và phát triển, được kết hợp với System Center Virtual Machine Manager và sự quản lý xuyên suốt của các trung tâm dữ liệu động.

World-Class Web và nền ứng dụng

Windows Server 2008 cung cấp sự bảo mật, nền tảng dễ quản lý cho việc phát triển và khả năng tin cậy vào các ứng dụng chủ và dịch vụ được cung cấp từ máy chủ hoặc trên Web. Các tính năng mới gồm đơn giản hóa sự quản lý, tăng bảo mật, cải thiện hiệu suất và khả năng mở rộng cao, cung cấp một nền tảng hợp nhất cho việc xuất bản Web có tích hợp Internet Information Services 7.0 (IIS7), ASP.NET, Windows Communication Foundation và Microsoft Windows SharePoint Services.

Cải thiện hiệu suất kết nối mạng

Windows Server 2008 đưa ra một thay đổi lớn nhất trong ngăn xếp kết nối mạng kể từ Windows NT 4.0. Các công nghệ như Receive Window Auto-tuning, Receive Side Scaling và Quality of Service (QOS) cho phép các tổ chức có nhiều thuận lợi trong việc kết nối mạng nhiều Gigabit ngày nay. Integrated IPsec và Windows Firewall mới có tính năng bảo mật nâng cao cho phép các tổ chức bảo đảm và kiểm soát toàn bộ được lưu lượng mạng.

Bảo mật nâng cao

Windows Server 2008 đã được phát triển với mong muốn tạo ra sự bảo mật chặt chẽ nhất từ trước đến nay. Nó chỉ cài đặt các dịch vụ cần thiết cho vai trò mà máy chủ đang thực hiện. Thảm định nâng cao, mã hóa ổ đĩa, chuyển tiếp sự kiện và Rights Management Services là một trong số những công nghệ giúp tổ chức tham gia vào các chuẩn IT ngày nay.

Lấy lại sự kiểm soát trên những chi nhánh văn phòng của bạn

Các máy chủ quản lý, các dịch vụ và sự bảo mật tại vị trí từ xa là một trong những thách thức đang diễn ra đối với các chuyên gia CNTT. Windows Server 2008 đã đơn giản hóa sự quản trị của các máy chủ trong chi nhánh văn phòng với những cải tiến trong Active Directory, những cải tiến này gồm có Read-Only Domain Controller và sự phân biệt vai trò quản trị. Các công nghệ như tùy chọn cài đặt BitLocker và Server Core ở những tính năng cụ thể tăng độ bảo mật và nhằm vào những cần thiết duy nhất chỉ có của các chi nhánh văn phòng.

Quản trị máy chủ dễ dàng hơn

Đơn giản hóa sự phức tạp của việc quản trị máy chủ là một trong những chủ đề chính được cải tiến của Windows Server 2008. Công cụ quản lý mới như Server Manager Console cung cấp giao diện quản lý đơn giản, hợp nhất cho việc quản lý cấu hình của máy chủ, các thông tin hệ thống, hiển thị trạng thái máy chủ và quản lý tất cả các vai trò đã cài đặt trên máy chủ.

Nâng cao kịch bản và tự động hóa nhiệm vụ

Các công nghệ mới như Windows PowerShell, tiện ích dòng lệnh và ngôn ngữ kịch bản giúp chuyên gia CNTT giải quyết các nhiệm vụ chung một cách tự động. Với ngôn ngữ kịch bản tập trung quản lý mới, với hơn 120 công cụ dòng lệnh chuẩn, cú pháp và các tiện ích nhất quán, Windows PowerShell hoàn toàn lý tưởng với chuyên gia CNTT trong việc quản trị hệ thống.

Truy cập ứng dụng tập trung

Với Windows Sever 2008, người dùng sẽ an toàn khi truy cập vào các ứng dụng bên trong thông qua các cổng tường lửa thân thiện. Với Windows Server Terminal Services RemoteApp, các cửa sổ ứng dụng (không phải toàn bộ máy truy cập từ xa) có thể bắt đầu khởi chạy trong chính cửa sổ tương tác trên nền máy khách.

Bảo vệ các máy tính “không an toàn” khi truy cập mạng

Network Access Protection (NAP) nhằm vào vấn đề khi các máy tính “không an toàn” truy cập và gây tổn hại cho mạng của một tổ chức. NAP được sử dụng để bảo đảm bất kỳ máy tính nào kết nối vào mạng đều phải có được chính sách công ty với yêu cầu về “sự an toàn”, điều này nhằm hạn chế sự truy cập của các máy tính không có chính sách được định nghĩa trước, cung cấp dịch vụ điều chỉnh lại để đưa các máy tính trở về trạng thái “an toàn” và cung cấp cách thức kiểm tra chặt chẽ.

Hoạt động tốt hơn với Windows Vista

Windows Vista và Windows Server 2008 được xây dựng có chia sẻ với nhau một số công nghệ mới trong vấn đề kết nối mạng, lưu trữ, bảo mật và quản lý. Chính vì vậy các tổ chức sẽ thấy được những ưu điểm ngay lập tức khi chạy Windows Server 2008 và Windows Vista trong giải pháp máy chủ và máy khách của họ.

Văn Linh