

## Microsoft Windows Server 2003 [11/28/2003 9:35:00 AM]

Vào ngày 24/4/2003, Microsoft sẽ tung ra thị trường hệ điều hành (HĐH) Windows Server 2003. Đây là sản phẩm thế hệ kế tiếp của Windows 2000 Server và là HĐH đặt nền móng cho sự tiếp nhận rộng rãi các dịch vụ Web. Họ sản phẩm Windows Server 2003 thừa hưởng những công nghệ tốt nhất của Windows 2000. Nó bao hàm tất cả những tính năng ưu việt mà khách hàng chờ đợi từ một HĐH máy chủ Windows như bảo mật, độ tin cậy cao, tính sẵn sàng và khả năng có thể mở rộng

Vào ngày 24/4/2003, Microsoft sẽ tung ra thị trường hệ điều hành (HĐH) Windows Server 2003. Đây là sản phẩm thế hệ kế tiếp của Windows 2000 Server và là HĐH đặt nền móng cho sự tiếp nhận rộng rãi các dịch vụ Web. Họ sản phẩm Windows Server 2003 thừa hưởng những công nghệ tốt nhất của Windows 2000. Nó bao hàm tất cả những tính năng ưu việt mà khách hàng chờ đợi từ một HĐH máy chủ Windows như bảo mật, độ tin cậy cao, tính sẵn sàng và khả năng có thể mở rộng. Windows Server 2003 còn tích hợp chặt chẽ với Microsoft .NET [1], khả năng hỗ trợ có sẵn cho .NET Framework [1] để phát triển và triển khai các ứng dụng và dịch vụ Web. Các tính năng mới cũng như những cải tiến đã nâng cao khả năng của họ Windows Server trong việc hỗ trợ các hệ thống mạng và những ứng dụng cao cấp và tối quan trọng.

Phiên bản cho sản phẩm Windows Server mới này còn được biết dưới tên Windows .NET Server 2003. Sản phẩm cuối cùng có tên là Windows Server 2003. Do sự hỗ trợ các dịch vụ Web được tích hợp vào trong toàn bộ dòng sản phẩm, Microsoft quyết định đổi tên là nhằm đơn giản hoá việc đặt tên sản phẩm và thực hiện chiến lược thương hiệu .NET mới của họ. Dòng sản phẩm Windows Server 2003, cũng như các sản phẩm có khả năng .NET của Microsoft, khi đưa ra thị trường sẽ mang biểu tượng "Microsoft .NET Connected", thay vì cụm từ ".NET?" trước đó.

### 1. Tổng quan về Windows Server 2003

Với những tính năng mới được nâng cao cùng với những cải tiến các dịch vụ, Windows Server 2003 chuyên giao một nền tảng cao cấp để cung cấp nguồn lực cho các ứng dụng, các mạng và các dịch vụ Web từ nhóm làm việc đến trung tâm dữ liệu. Dễ dàng khi triển khai, quản lý và sử dụng, Windows Server 2003 cung cấp một nền tảng server hoàn chỉnh cho phép tạo ra các giải pháp được kết nối với nhau một cách thông suốt. Để thực hiện những khả năng đó, trước hết Windows Server 2003 phải thể hiện vai trò như những server dưới đây.

#### 1.1. Vai trò Server

Windows Server 2003 là một HĐH đa dụng có khả năng quản lý một tập những vai trò server (phục vụ), tùy thuộc vào nhu cầu của những tổ chức khác nhau, theo kiểu tập trung hay phân tán. Sau đây là một số vai trò server của Windows Server 2003:

- ❖ File server (phục vụ tập tin) và Print server (phục vụ in ấn).  
Web Server (phục vụ Web) và Web Application Server (phục vụ ứng dụng Web).  
Mail server (phục vụ thư tín) và Terminal server (phục vụ thiết bị đầu cuối).  
Remote access/virtual private network [VPN] server (phục vụ truy cập từ xa/mạng riêng ảo).  
Directory services (các dịch vụ thư mục), Domain Name System [DNS] (hệ thống tên miền),  
Dynamic Host Configuration Protocol [DHCP] server (phục vụ giao thức cấu hình địa chỉ động)  
và Windows Internet Naming Service [WINS] (dịch vụ đặt tên Internet trên Windows).  
Streaming media server (phục vụ phương tiện truyền thông theo luồng).
- ❖ Một số cải tiến trong công nghệ lõi của Windows Server 2003  
Sau đây là những tính năng mới mà Microsoft hy vọng sẽ biến Windows Server 2003 thành một nền tảng server lý tưởng cho mọi tổ chức với mọi cấp độ.

Tính sẵn sàng: H? Windows Server 2003 □43; c?i thi?n tónh s?n s□ thụng qua s? h? tr? clustering (x?p nhóm) □ c?i tí?n. Các dịch vụ clustering đã trở thành thiết yếu cho các tổ chức triển khai các ứng dụng

đánh giá kinh doanh và thương mại điện tử bởi chúng có những cải tiến quan trọng cho khả năng sẵn sàng, tính có thể mở rộng và khả năng quản lý. Họ Windows Server 2003 hỗ trợ các nhóm server đến 8 nút. Nếu một trong các nút trong nhóm hỏng hóc hay do bảo trì, một nút khác ngay lập tức thế chỗ để cung cấp dịch vụ. Windows Server 2003 cũng hỗ trợ NBL (Network Load Balancing, cân bằng tải mạng) để cân bằng lưu lượng IP đến các nút trong một cluster.

Khả năng có thể mở rộng: Họ Windows Server 2003 cho phép khả năng có thể mở rộng thông qua ?scale-up? [2], được cho phép bởi SMP (symmetric multiprocessing, đa xử lý đối xứng) và ?scale-out? [2], được cho phép bởi clustering (tạo nhóm). Những thử nghiệm bên trong cho thấy khi so sánh với Windows 2000 Server, Windows Server 2003 chuyển giao hiệu suất thực hiện đến 140% tốt hơn trong hệ thống file và hiệu suất tốt hơn đáng kể trong các tính năng khác như Microsoft Active Directory service, Web server và các thành phần Terminal Server cũng như các dịch vụ kết nối mạng. Windows Server 2003 hỗ trợ tới 32 đường SMP thông qua ?scale-up? và hỗ trợ cả hai bộ xử lý 32-bit và 64-bit.

Tính an toàn: Những doanh nghiệp ngày nay đang mở rộng mạng LAN truyền thống của họ. Như một hệ quả tất yếu, an ninh hệ thống đang bị đe dọa. Để đảm bảo sự chắc chắn, độ an toàn và tính tin cậy, Microsoft đã xem xét, cân nhắc, cải tiến và đưa vào Windows Server 2003 nhiều tính năng bảo mật mới và quan trọng:

The common language runtime [1] (CLR - bộ thực thi ngôn ngữ chung) : CLR cải tiến tính tin cậy và giúp đảm bảo một môi trường tính toán an toàn. Nó làm giảm số lượng lỗi kỹ thuật và những lỗ hổng về bảo mật được tạo ra bởi những lỗi lập trình phổ thông. CLR cũng xác minh rằng các ứng dụng có thể chạy mà không có lỗi và kiểm tra những ?giấy phép? bảo mật có thích hợp hay không.

Internet Information Services (IIS) 6.0: Để tăng an toàn cho Web server, IIS 6.0 được cấu hình cho sự bảo mật tối đa. IIS 6.0 và Windows Server 2003 cung cấp giải pháp Web server đáng tin cậy, hiệu quả, kết nối thông suốt và tích hợp nhất với sự chịu đựng lỗi, yêu cầu hàng đợi, giám sát ứng dụng, vòng lặp chu kỳ ứng dụng tự động, cất giữ (caching) và những thứ khác. Những tính năng mới trong IIS 6.0 cho phép bạn quản lý doanh nghiệp an toàn trên mạng.

Kết nối thông suốt Windows Server 2003 có thể tạo ra cơ sở hạ tầng cho những giải pháp kinh doanh để kết nối tốt hơn với những người làm thuê, những đối tác, những hệ thống và khách hàng. Cụ thể, Windows Server 2003 cung cấp một Web server tích hợp và streaming media server giúp tạo ra nhanh chóng và bảo mật các Website động trên intranet và Internet. Kể đến nó cung cấp một application server tích hợp cho phép dễ dàng phát triển, triển khai và quản lý những dịch vụ Web XML. Cuối cùng là việc cung cấp các công cụ cho phép bạn kết nối với các dịch vụ Web XML tới những ứng dụng nội bộ, những nhà cung cấp và những đối tác.

XML Web Services (các dịch vụ Web XML): IIS 6.0 là một thành phần quan trọng trong dòng sản phẩm Windows Server 2003. Những người quản trị và các nhà phát triển yêu cầu một nền tảng Web nhanh, đáng tin cậy, khả năng mở rộng và bảo mật. Những cải tiến đáng kể về kiến trúc trong IIS bao gồm một mô hình tiến trình mới cải thiện rất nhiều tính tin cậy, khả năng mở rộng và hiệu suất thực hiện. An toàn bảo mật được tăng lên do người quản trị hệ thống cho phép hay vô hiệu hoá những tính năng hệ thống dựa trên những yêu cầu ứng dụng.

Kết nối mạng và truyền thông: Những cải tiến và những tính năng mới cho kết nối mạng và truyền thông trong họ Windows Server 2003 mở rộng tính linh hoạt, khả năng quản lý và độ tin cậy của các cơ sở hạ tầng mạng. Phần này chúng tôi sẽ khảo sát chi tiết trong mục 2 của bài báo dưới đây. Các dịch vụ Enterprise UDDI: Windows Server 2003 bao hàm các dịch vụ Enterprise UDDI [3], một cơ sở hạ tầng động và linh hoạt cho các dịch vụ Web XML. Giải pháp dựa trên cơ sở những chuẩn này cho phép các công ty chạy dịch vụ UDDI nội bộ của họ cho việc sử dụng intranet hay extranet. Những nhà phát triển có thể tìm thấy dễ dàng và nhanh chóng các dịch vụ Web có sẵn trong phạm vi tổ chức đó. Các nhà quản trị IT có thể phân loại và quản lý những tài nguyên có khả năng chương trình hoá trong mạng của họ. Với các dịch vụ Enterprise UDDI, các công ty có thể xây dựng và triển khai các ứng dụng nhanh chóng và đáng tin cậy hơn.

Các dịch vụ Web XML và .NET[1]

Như đã được đề cập trong phần giới thiệu, Microsoft .NET được tích hợp sâu trong dòng sản phẩm Windows Server 2003. Nó cho thấy một mức độ tích hợp chưa từng thấy của phần mềm sử dụng các dịch vụ Web XML. Ngắm vào trong các sản phẩm tạo ra nền tảng Microsoft, .NET cung cấp khả năng để xây dựng, host, triển khai nhanh chóng và tin cậy và sử dụng an toàn những giải pháp kết nối thông suốt thông qua các dịch vụ Web XML. Nền tảng Microsoft cung cấp một bộ các công cụ phát triển, các ứng dụng client, các dịch vụ Web XML và các server cần thiết để tham gia vào trong thế giới kết nối thông suốt này. Muốn tìm hiểu sâu hơn về Nền tảng .NET và những lợi ích của nó trong họ Windows Server 2003 các bạn có thể tìm hiểu trong các bài viết chuyên đề về .NET đã được đăng trong các số tháng 12/2002 và 02/2003.

Các dịch vụ quản lý : Windows Server 2003 đưa ra nhiều công cụ quản lý tự động hoá mới bao gồm Microsoft Software Update Services (SUS) và các Server Configuration Wizard để giúp tự động hoá công việc triển khai. Việc quản lý Group Policy được thực hiện dễ dàng với Group Policy Management Console (GPMC) mới, cho phép nhiều tổ chức tận dụng tốt hơn dịch vụ Active Directory và nắm lấy lợi thế của chúng. Ngoài ra, những công cụ command-line (dòng lệnh) cho phép người quản trị thực hiện nhiều tác vụ ?command console?.

Quản lý lưu giữ : Windows Server 2003 có chứa những đặc tính mới và nâng cao khả năng quản lý công việc cất giữ, quản lý và bảo trì đĩa và dung lượng đĩa, dự trữ và phục hồi dữ liệu và kết nối với các Storage Area Network (SAN).

Terminal Services (các dịch vụ thiết bị đầu cuối): Thành phần Terminal Services trong Microsoft Windows Server 2003 xây dựng trên chế độ ?solid application server mode? trong Terminal Services của Windows 2000. Terminal Services cho phép bạn chuyển giao các ứng dụng trên nền Windows, hay bản thân Windows desktop, tới bất cứ một thiết bị tính toán nào ?bao gồm cả những ứng dụng không chạy trên Windows.

## 2. Những cải tiến và tính năng mới cho kết nối mạng và truyền thông

Những tính năng mới và cải tiến cho kết nối mạng và truyền thông trong họ Windows Server 2003 cho thấy tính linh hoạt, khả năng quản lý và tính đáng tin cậy của những cơ sở hạ tầng mạng, mở rộng trên nền tảng được thiết lập với họ Windows 2000 Server. Sau đây chúng tôi sẽ giới thiệu tổng quan về các lợi ích, các tính năng mới cũng như những cải tiến cho dịch vụ kết nối mạng và truyền thông trong họ Windows Server 2003.

### 2.1. Cải thiện tính đa năng

Internet Protocol version 6 (IPv6) : Đây là giao thức Internet phiên bản 6. IPv6 [4] là thế hệ kế tiếp của các giao thức tầng Internet của bộ giao thức TCP/IP. IPv6 giải quyết những vấn đề hiện tại của IPv4, (giao thức Internet đang sử dụng) về vấn đề thiếu hụt địa chỉ, an toàn bảo mật, tự động cấu hình, khả năng mở rộng và hơn thế nữa. Trình điều khiển giao thức IPv6 được cung cấp bởi Windows Server 2003 là một sản phẩm chất lượng và chứa đựng những tiện ích thiết thực, hỗ trợ API trong phạm vi rộng (như Windows Sockets, Remote Procedure Call [RPC] và IPHelper) và các thành phần hệ thống có khả năng IPv6 (IPv6-enabled) như Microsoft Internet Explorer, Telnet client, FTP client, IIS 6.0, chia xê tập tin và máy in và những thứ khác. IPv6 trong Windows Server 2003 cũng có khả năng hỗ trợ những công nghệ cùng tồn tại IPv6/IPv4 [4] như ?6to4? [4] và ISATAP [5] (Intra-site Automatic Tunnel Addressing Protocol).

Point-to-Point Protocol over Ethernet (PPPoE) [13] : Windows Server 2003 chuyên giao một trình điều khiển PPPoE để thực hiện những kết nối băng rộng cho những nhà cung cấp dịch vụ Internet (ISP) nào đó mà không cần phần mềm bổ sung. Những doanh nghiệp nhỏ hay những văn phòng chi nhánh tự hạch toán có thể cũng dùng những khả năng dial (quay số) theo yêu cầu của PPPoE để tích hợp với dịch vụ Routing and Remote Access (định hướng và truy nhập từ xa) và NAT [6].

Network Bridging : Network Bridging (bắc cầu qua mạng) cho phép những nhà quản trị ?nối liền? các đoạn mạng với nhau khi sử dụng máy tính chạy Windows Server 2003. Trong một mạng gồm nhiều đoạn (multi-segment network), một hay nhiều máy tính có thể có bộ tiếp hợp như một bộ tiếp hợp không dây, một bộ tiếp hợp gọi quay số (dial-up) hay một bộ tiếp hợp Ethernet. Công việc bắc cầu qua những bộ tiếp

hợp này cho phép các máy tính và các thiết bị trên mỗi đoạn của các đoạn mạng liên lạc với nhau thông qua cầu nối hoặc truyền thông với Internet khi Internet Connection Sharing (ICS) [7] được trao quyền.

Internet Protocol Security (IPSec) qua NAT [6]: Điều trở ngại khi sử dụng các VPN [10] trên cơ sở IPSec [8] hoặc những ứng dụng được bảo vệ bởi IPSec (IPSec-protected) đi qua một NAT được loại trừ. Windows Server 2003 cho phép một L2TP [14] (Layer Two Tunneling Protocol) qua IPSec (L2TP/IPSec) hay một kết nối IPSec [8] đi qua một NAT. Khả năng này dựa trên các chuẩn IETF gần đây nhất. Một người quản trị có thể cũng sử dụng đặc tính này để bảo đảm lưu lượng Microsoft Exchange Server trên mạng vành đai (perimeter network) đến một mạng nội bộ (internal network) chạy Exchange Server hay một server ứng dụng mạng vành đai tới một server ứng dụng của đối tác trên Internet mà không đòi hỏi một server VPN [10].

## 2.2. Khả năng quản lý mềm dẻo

Những bổ sung cho Group Policy : Những cải tiến mới cho Group Policy (chính sách nhóm) trong Windows Server 2003 giúp người quản trị điều khiển thông qua đa số các thiết lập cấu hình mạng. Chẳng hạn, người quản trị bây giờ có thể cấu hình một số thiết lập DNS client trên các máy tính chạy Windows Server 2003 có sử dụng Group Policy. Hơn nữa, tính năng Group Policy có thể được sử dụng để cho phép hay hạn chế sự truy cập cấu hình người dùng tới những thành phần cá nhân của giao diện người dùng mạng.

Connection Manager Administration Kit (CMAK) được nâng cao : CMAK [12] đã cho những người quản trị khả năng để xác định trước những hiện trạng kết nối cho những người dùng truy cập từ xa có chạy Windows XP, Windows 2000, Microsoft Windows NT 4.0, Windows Millennium Edition (Windows Me) và Windows 98. Windows Server 2003 chuyển giao những tính năng mới và những cải tiến cho CMAK, cho phép người quản trị cung cấp nhiều hơn một server VPN [10] cho các kết nối, mở đăng nhập cho người dùng cuối, tự động cấu hình những thiết đặt ủy quyền (proxy) trình duyệt trên những máy tính client, cho phép hoặc vô hiệu hóa ?split tunneling? [15] được thực hiện trên máy trạm client và cấu hình các ?key? chia sẻ trước cho các kết nối L2TP/IPSec.

Những cải tiến IAS [11] : Những triển khai mạng không dây làm tăng thêm đáng kể nhu cầu cho nhiều máy server RADIUS [16] và những công cụ tốt hơn để chẩn đoán những vấn đề chứng thực (authentication) và quản lý điều khiển truy cập mạng. Windows Server 2003 đã để tâm đến vấn đề này với những tính năng mới cho phép IAS [11] gửi thông tin đăng ký tới một server chạy Microsoft SQL Server để cho phép các truy vấn SQL cao cấp (advanced SQL) để phòng những trường hợp truy cập mạng đi qua xí nghiệp, những tính năng chứng thực 802.1X [9] mới, chứng thực ?cross-forest? và nhiều tính năng khác. Khi sử dụng IAS [11], Windows Server 2003 thực hiện triển khai dễ dàng các giải pháp cao cấp cho sự điều khiển truy cập mạng được chứng thực trong những trường hợp có dây, không dây và truy cập từ xa.

Những sự mở rộng quản lý và tích hợp : Họ Windows Server 2003 chuyển giao những tính năng kết nối mạng mới để đơn giản hóa việc quản lý mạng. Một Network Load Balancing Manager mới có chức năng quản lý cân bằng tải mạng. Sự hỗ trợ RFC 2734 cho phép lưu lượng TCP/IP trên một kênh nối tiếp IEEE 1394. Với sự xúc tiến cam kết bảo mật, Windows Server 2003 cung cấp sự hỗ trợ cho nhóm Diffie-Hellman 2048-bit. Nhóm này cung cấp một sự trao đổi khóa Diffie-Hellman chắc chắn và an toàn hơn.

## 2.3. Những cải tiến nâng cao độ tin cậy

Internet Connection Firewall (ICF, tường lửa kết nối Internet): ICF [17] được thiết kế để sử dụng cho doanh nghiệp nhỏ, cung cấp sự bảo vệ cơ bản trên những máy tính được kết nối trực tiếp vào Internet hay trên những đoạn mạng cục bộ (LAN). ICF có thể dùng được cho LAN, dial-up, VPN [10] hay các kết nối PPPoE [13]. ICF tích hợp với ICS [7] hay với dịch vụ định tuyến và truy cập từ xa (Routing and Remote Access service).

IPSec Network Load Balancing (cân bằng tải mạng IPSec [8]): Network Load Balancing được cung cấp bởi Windows Server 2003 và hỗ trợ cả lưu lượng IPSec. Người quản trị có thể sử dụng Network Load

Balancing cho một nhóm các server để cung cấp độ tin cậy ?scale-out? [2] và năng lực cho những triển khai các ứng dụng được bảo vệ bởi IPSec [8] và những triển khai công VPN [10] Windows. Cho các công VPN, những cải tiến NLB [18] hỗ trợ cả các VPN L2TP [14] được bảo vệ bởi mã hoá IPSec và những kết nối VPN trên nền PPTP (Point-to-Point Tunneling Protocol).

Network Access Security với 802.1X (bảo mật truy cập mạng với 802.1X): Các công ty có thể chuyển sang một mô hình bảo mật đảm bảo tất cả sự truy nhập vật lý được chứng thực và mã hoá, trên cơ sở hỗ trợ 802.1X [9] trong Windows Server 2003. Khi sử dụng những điểm truy cập không dây trên nền 802.1X hay các switch, các công ty có thể đảm bảo rằng chỉ có những hệ thống được ủy thác mới cho phép kết nối và trao đổi những gói dữ liệu với những mạng được bảo mật.

IAS RADIUS Proxy và Load Balancing : IAS [11] hỗ trợ những khả năng ủy quyền RADIUS [16] (RADIUS proxy), có tính đến sự chuyển tiếp dựa trên cơ sở quy tắc mềm dẻo, sự chuyển tiếp có chọn lọc cho chứng thực và những yêu cầu về tính toán đến các server RADIUS [16] khác và khả năng ép buộc client sử dụng một ?tunnel? (đường hầm) bắt buộc có hay không có sự chứng thực người dùng. Năng lực chuyển tiếp có thể được sử dụng khi những người dùng đang kết nối từ những ?forest? hay những ?domain? không được ủy thác.

## Lời kết

Windows Server 2003 hiện đã sẵn sàng cho người sử dụng. Microsoft đã hoàn tất việc đóng gói 4 phiên bản của Windows Server 2003 : Datacenter Edition (dành cho ứng dụng nghiệp vụ tối quan trọng, đòi hỏi khả năng mở rộng và khả năng sẵn sàng cao nhất), Enterprise Edition (có độ tin cậy và hiệu năng rất cao), Standard Edition (dành cho doanh nghiệp) và Web Edition (phục vụ lưu trữ và trang web).

Các phiên bản của Windows Server 2003 đã thừa hưởng những công nghệ tiên tiến của Windows 2000 Server. Với sự bổ sung những tính năng mới và những cải tiến mang tính cách mạng, khi sử dụng Windows Server 2003 các tổ chức có thể nhanh chóng được lợi từ những nền tảng tích hợp dễ triển khai, quản lý và sử dụng, làm cho hệ thống mạng trở thành một tài sản chiến lược trong thời buổi cạnh tranh ngày hôm nay.

ThS. Nguyễn Hoàng Linh  
Trung tâm VTQT KV-1/VTI  
Chú thích

[1] .NET, CLR : xem bài ?Tổng quan về Microsoft .NET? (số tháng 12/2002) và ?Nền tảng .NET? (số tháng 02/2003).

[2] Scale-out, Scale-up : Scale-out được hiểu là tăng số lượng máy chủ của một nhóm máy chủ (cluster) ứng dụng riêng biệt. Scale-up là một khái niệm để tăng số lượng bộ xử lý trong một máy chủ đơn.

[3] UDDI: Đặc tả Universal Description, Discovery and Integration ? một sáng kiến tạo ra một khung (framework) mở, không phụ thuộc vào nền tảng, toàn cầu cho phép những doanh nghiệp khám phá lẫn nhau, định rõ chúng tương tác với nhau như thế nào qua Internet và chia sẻ thông tin trong một nơi đăng ký (registry) toàn cầu.

[4] IPv6, IPv4, IPv6/IPv4, ?6to4?: xem bài ?IPv6: Những vấn đề công nghệ & giải pháp? (số tháng 11/2002).

[5] ISATAP : Intra-site Automatic Tunnel Addressing Protocol.

[6] NAT: Network Address Translation - Dịch địa chỉ mạng.

[7] ICS : Internet Connection Sharing ? Chia sẻ kết nối Internet.

[8] IPSec: Internet Protocol Security : Bảo mật giao thức Internet.

[9] IEEE 802.1X: Extensible Authentication Protocol over LAN ? Giao thức chứng thực có thể mở rộng.

Xem bài ?Mạng Wireless LAN và chuẩn IEEE 802.11b? (số tháng 12/2002)

[10] VPN : Virtual Private Network - Mạng riêng ảo.

[11] IAS : Internet Authentication Service - Dịch vụ chứng thực Internet.

[12] CMAK : Connection Manager Administration Kit : Bộ quản trị quản lý kết nối.

[13] PPPoE: Point-to-Point Protocol over Ethernet ? Giao thức điểm - điểm qua Ethernet.

[14] L2TP : Layer Two Tunneling Protocol ? Giao thức ?tạo đường hầm? lớp hai.

[15] split tunneling : Đây là một tính năng cho phép những kết nối VPN [10] được thực hiện trên máy trạm client để định tuyến lưu lượng trên cơ sở công tác (corporate-based) qua kết nối VPN, trong khi cô lập lưu lượng trên cơ sở Internet (Internet-based) tới kết nối Internet cục bộ của người dùng, bằng cách đó ngăn ngừa sự sử dụng dải tần công tác cho sự truy cập tới các vị trí Internet. Những công ty nhạy cảm với vấn đề bảo mật có thể lựa chọn mô hình ?non-split? mặc định để đảm bảo rằng tất cả truyền thông của client cho những client của VPN được bảo vệ bởi tường lửa công tác.

[16] RADIUS : Remote Authentication Dial-In User Service - Dịch vụ người dùng quay số chứng thực từ xa.

[17] ICF : Internet Connection Firewall - Tường lửa kết nối Internet.

[18] NLB : Network Load Balancing - Cân bằng tải mạng. [Quản trị File trong WINNT](#) [11/23/2003 3:03:00 AM]

Thay đổi trong File Manager Thay đổi quan trọng nhất trong Windows NT File Manager là File Manager bây giờ là ứng dụng 32 bit và File Manager hiện đã hỗ trợ hệ thống file cài đặt được, chẳng hạn như NTFS.

1. Đa luồng Windows NT File Manager đã được cải tiến và một số chức năng hiện nay là đa luồng. Chẳng hạn tìm kiếm file và lên khuôn dạng đĩa mềm hiện có thể được thực hiện dưới ngầm trong khi thực hiện các công việc khác trong File Manager.

2. Menu File Dưới Properties, hiện đã có nút Open By. Nút này chỉ xuất hiện dưới File Properties khi file đã được chọn trước khi File Properties được chọn. Nó sẽ mở một hộp đối thoại gồm total opens, total locks, ai có file mở, và đặt tùy chọn.

3. File Associate File Associate hiện bao gồm cả các chức năng được cung cấp cho Windows 3.1, bởi chương trình REGEDIT trong Windows 3.1. Các thiết lập của nó được lưu trong Windows NT Registry dưới HKEY\_CLASSES\_ROOT.

4. Menu Disk

Không còn tùy chọn để tạo một system disk nữa.

Connect và Disconnect là các mục riêng biệt trên menu.

Share As - cho phép chia sẻ các thư mục.

Stop Sharing - ngừng chia sẻ thư mục.

Menu Options

Cá thể hoá thành công cụ

Thanh công cụ có thể được cho phép hoặc không cho phép  
- Drivebar có thể được cho phép hoặc không cho phép  
- Open New Windows on Connect - khi nối với ổ mạng, tùy chọn này tạo một cửa sổ để hiển thị nội dung của ổ.

6. Menu Window

Tile Horizontally -sắp xếp các cửa sổ ổ đĩa đang mở theo chiều ngang

Tile Vertically -sắp xếp các cửa sổ ổ đĩa theo chiều dọc

7. Menu Security

- Permissions - cho phép thiết lập quyền trên thư mục và file
- Auditing - cho phép kiểm soát được thiết lập trên thư mục và file
- Owner - cho phép quyền chủ sở hữu được lấy ra từ thư mục và file

## 8. The new Toolbar

Thanh công cụ của Windows NT File Manager rất giống Windows for Workgroup File Manager. Thanh công cụ này có thể cấu hình hoá được, tuy nhiên sẽ không bao bọc đối với những nút không đặt vừa màn hình. Vì vậy nếu có quá nhiều mục trong thanh công cụ thì chúng sẽ bị nằm ngoài màn hình. Có thể sẽ có vấn đề nếu người dùng chuyển từ driver màn hình phân giải cao (1024x768) sang độ phân giải thấp hơn (640x480) bởi vì họ sẽ không thể cho tất cả các mục vào trong màn hình.

Khác biệt chính giữa thanh công cụ mặc định trong Windows NT và Windows for Workgroups là trong Windows NT có nút an toàn.

## II. Hỗ trợ hệ thống file

Windows NT hỗ trợ nhiều hệ thống file tích cực có thể được nạp về như bất kỳ driver nào. Điều này khiến Windows NT có khả năng hỗ trợ bất cứ hệ thống file nào chừng nào một driver được phát triển cho nó. Theo mặc định Windows NT hỗ trợ những hệ thống file sau:

- Hệ thống tệp MS-DOS FAT
- Hệ thống tệp OS/2 HPFS

Hệ thống tệp Windows NT NTFS mới

- Hệ thống tệp CD
- Hệ thống tệp Named Pipe
- Hệ thống tệp Mailslot

Để phục vụ mục đích thảo luận, chúng ta sẽ chỉ tập trung trên ba hệ thống tệp được sử dụng trong các ổ đĩa cứng đọc/ghi: FAT, HPFS và NTFS.

### 1. Chọn hệ thống tệp

NTFS là hệ thống tệp thông thường, tuy nhiên trong một số trường hợp cũng có thể cần sử dụng các hệ thống tệp khác. Chẳng hạn, nếu hệ thống chạy một hệ điều hành khác thì ít nhất một phân vùng-partition phải được lên khuôn dạng theo cách của hệ điều hành đó. Trong trường hợp MS-DOS, thì partition thứ nhất phải được lên khuôn dạng bằng hệ thống tệp FAT. Hệ thống tệp FAT có một lợi điểm là nó được sử dụng rộng rãi và được nhiều hỗ trợ của các hệ điều hành khác.

Để xác định chính xác sử dụng hệ thống file nào, cần thiết phải có một số hiểu biết về mỗi hệ thống file đang được hỗ trợ.

Btrees (Bcây) là cấu trúc cây nhị phân với một gốc và một số các nốt. Dữ liệu được tổ chức theo kiểu logic sao cho dễ duyệt. Gốc chứa một ánh xạ tới phần còn lại của cấu trúc và các nốt chứa dữ liệu.

### 2. Hỗ trợ POSIX

NTFS tuân thủ nhất POSIX.1 của các hệ thống file được hỗ trợ vì nó hỗ trợ các yêu cầu sau của POSIX.1:

- Đặt tên phân biệt chữ hoa chữ thường. Trong POSIX, README.TXT, Readme.txt, và readme.txt là các file khác nhau
- Tem thời gian bổ sung. Tem thời gian bổ sung cung cấp thời gian khi file được truy nhập lần cuối cùng.
- Liên kết cứng. Một liên kết cứng là khi hai tên file khác nhau, có thể nằm ở các thư mục khác nhau trở tới cùng một dữ liệu.

### 3. Loại bỏ các hạn chế

Trước hết là NTFS đã tăng đáng kể kích thước của các file và các volume sao cho chúng có thể lớn tới 264. NTFS cũng quay về khái niệm cluster của FAT để tránh vấn đề của HPFS đối với kích thước sector cố định. Điều này được thực hiện bởi vì Windows NT là một hệ điều hành khá chuyển và hỗ trợ các công nghệ đĩa khác nhau. Do vậy, 512 byte một sector dường như được coi là chưa chắc đã phải luôn luôn khớp với các định vị. Điều đó được thực hiện bởi cho phép cluster được định nghĩa như tích của kích thước định vị tự nhiên của phần cứng. Cuối cùng, trong NTFS tất cả các tên file là Unicode và tên kiểu 8.3 được giữ cùng với tên dài.

#### 4. Ưu điểm của NTFS

NTFS là giải pháp tốt nhất khi sử dụng các volume kích thước 400 MB hoặc hơn. Lý do là vì hiệu năng hệ thống không giảm đi trong NTFS như là trong FAT khi kích thước volume tăng lên.

Tính có thể phục hồi được thiết kế trong NTFS sao cho người dùng không bao giờ phải chạy bất kỳ một kiểu tiện ích sửa đĩa nào trong một partition NTFS.

#### 5. Nhược điểm của NTFS

Nói chung không NTFS không được khuyến cáo sử dụng đối với các volume có kích thước nhỏ hơn 400 MB vì không gian lưu chuyển trong NTFS thường lớn. Không gian lưu chuyển này dưới dạng của các file hệ thống NTFS thông thường sử dụng ít nhất 4 MB ổ đĩa trong một partition có kích thước 100 MB.

Đồng thời, không có mã hoá file trong NTFS. Do đó, ai đó có thể khởi động dưới MS-DOS, hoặc hệ điều hành khác và sử dụng các tiện ích soạn thảo đĩa mức thấp để nhìn dữ liệu được lưu trong volume của NTFS.

Không thể lên khuôn dạng cho một đĩa mềm trong hệ thống file NTFS, Windows NT lên khuôn dạng tất cả các đĩa mềm với hệ thống file FAT. Lý do là bởi vì thông tin lưu chuyển trong NTFS sẽ không đặt vừa trong một đĩa mềm.

#### 6. Quy ước đặt tên của NTFS

- Tên file và thư mục có thể dài đến 255 ký tự, và có thể gồm bất cứ mở rộng nào.

- Các tên vẫn duy trì chữ hoa chữ thường, nhưng không phân biệt chữ hoa chữ thường. NTFS không phân biệt tên file dựa trên chữ hoa chữ thường.

- Tên có thể chứa bất kỳ ký tự nào ngoài các ký tự: ? " \ < > \* | :

Chú ý Hiện nay, từ dòng lệnh chỉ có tên file dài 253 ký tự có thể được tạo.

#### 7. Các tên file phân biệt chữ hoa chữ thường được quản lý như thế nào

Như đã nói ở trên một trong những yêu cầu của POSIX được NTFS hỗ trợ là cách đặt tên phân biệt chữ hoa chữ thường. NTFS, một phân hệ POSIX và các ứng dụng POSIX không có vấn đề gì trong việc sử dụng tên file phân biệt chữ hoa chữ thường. Tuy nhiên, WOW, VDM, OS/2 và Win32 hiện không hỗ trợ các đặt tên phân biệt chữ hoa chữ thường. Do đó, bất kỳ ứng dụng nào chạy trong bất kỳ môi trường nào trong số này có thể nhầm lẫn vì các file sử dụng các tên phân biệt chữ hoa chữ thường.

Giả sử có một thư mục trên một volume NTFS, trong đó có ba file chẳng hạn như: readme.txt, Readme.txt và README.TXT - CMD.EXE và File Manager sẽ hiển thị cả ba file. Tuy nhiên khi thao tác các file này thông qua dấu nhắc dòng lệnh Windows NT hoặc File Manager các file sẽ đung độ với nhau.

Giả dụ copy những file này về thư mục gốc, nó sẽ copy toàn bộ cả ba file, nhưng chúng sẽ copy lên trên mỗi file khác và sẽ có một file readme.txt trong thư mục gốc với nội dung của file thứ ba được copy.

Windows NT Notepad nhìn thấy cả ba file và hiển thị chúng theo đúng chữ hoa chữ thường trong hộp đối thoại mở file. Tuy nhiên, dù file nào được mở, Notepad sẽ luôn luôn mở và ghi vào readme.txt và hiển thị README.TXT trong thanh tên. EDIT.COM của MS-DOS 5.0 cũng hoạt động như Notepad.

Windows NT có cả hai tùy chọn tên phân biệt và không phân biệt chữ hoa chữ thường. Mặc dù NTFS hỗ trợ tên phân biệt chữ hoa chữ thường, hiện nay chỉ có phân hệ POSIX là sử dụng tên phân biệt chữ hoa chữ thường.

#### 8. Cách quản lý sự khác nhau trong cách đặt tên file

Cả HPFS và NTFS đều tương thích với FAT, tức là đều chấp nhận và sử dụng các tên file chuẩn FAT 8.3, nhưng chúng cũng đều hỗ trợ tên file dài. Tuy nhiên, chỉ có NTFS giữ tên file 8.3 cùng với tên file dài (được tự động). Tên file 8.3 của NTFS có thể được thể hiện trong File Manager (chi tiết-File Details) hay bằng dòng lệnh "DIR/X"

Chú ý: Vì HPFS chỉ có tên file dài và FAT chỉ chứa tên file 8.3, nên lệnh DIR /X sẽ có cột trắng ở cột thứ 2 của tên file nếu phân vùng của nó là HPFS hay FAT.

NTFS cho phép các ứng dụng MS-DOS và Windows 3.x nhận biết hay nạp các file thậm trí cả tên file dài NTFS. Thêm nữa ứng dụng MS-DOS/Windows 3.x cất file trên volume NTFS, cả tên file 8.3 và NTFS được chấp nhận.

Chú ý: Khi cất file từ ứng dụng MS-DOS/ Windows 3.x trên volume NTFS, nếu ứng dụng lưu nó ra file

tạm, xoá file ban đầu, đổi tên file tạm thành file ban đầu, TÊN FILE DÀI ĐƯỢC PHÉP! Hơn nữa các quyền trên file này cũng được đảm bảo trên file mới.

Khi sử dụng tên file dài cho các biểu tượng trong Program Manager, nếu có dấu trắng trong đường dẫn thì phải đặt đường dẫn trong dấu nháy kép "". Ví dụ Word for Windows trong thư mục D:\Word for Windows, thì dòng Command Line là: "D:\Word for Windows\winword.exe".

COPY, XCOPY, và tên file dài

Ngâm định COPY XCOPY sao chép file với tên dài của nó khi sao tên file dài từ NTFS hay HPFS sang FAT sẽ có lỗi:

The filename, directory name, or volume label syntax is incorrect.

và lệnh này sai khi gặp phải tên file dài.

Có thể dùng COPY/XCOPY, từ phân vùng NTFS sang FAT với thông số mới /n. Thông số này cho COPY/XCOPY sử dụng tên file 8.3 NTFS sinh ra.

Tên file NTFS 8.3 được sinh ra thế nào ?

NTFS sinh ra tên file NTFS 8.3 theo cách:

- Bỏ các ký tự trắng.

- Các dấu chấm được loại trừ dấu chấm cuối ở tên file mà nó có một ký tự tiếp theo. NTFS hiểu dấu chấm cuối và ba ký tự tiếp theo là phần mở rộng của tên file.

- Thay tất cả các ký tự trong DOS không hợp cách bởi dấu gạch dưới (\_).

- Gộp tên file tới 6 ký tự (không có phần mở rộng), với ký tự (~), và số tuần tự để phân biệt duy nhất. Các số đơn được thử đầu tiên. Nếu xung đột thì số có hai chữ số được thử. Trong quá trình so sánh tên file, nó cũng xác định được phần mở rộng tên file.

- Nối phần mở rộng với 3 ký tự.

File System Drivers và Registry Entries

Mỗi file trong 3 hệ thống file đều được tạo từ các phần sau:

- Trình điều khiển hệ thống file (File System Driver)

- Đó chính là một phần của hệ thống file là trình điều khiển hệ thống file trong hệ thống . Các trình điều khiển hệ thống file có thể được cấu hình trong Control Panel ở phần Devices, ngâm định giá trị khởi động (startup) là Disabled. Vùng cho File System Drivers có thể thấy trong:

\HKEY\_LOCAL\_MACHINE

\SYSTEM

\CurrentControlSet

\Services

\

- Trình xác nhận hệ thống file (File System Recognizer) Là một phần trong hệ thống file để nhận biết xem một hệ thống file có cần thiết phải được nạp trên hệ thống hay không. Khi một ổ đầu tiên được truy nhập, nếu trình xác nhận hệ thống file đang chạy, trình xác nhận sẽ khởi động hệ thống file tương ứng và sau đó nó tự kết thúc (chết). Tương tự nó cũng có thể được cấu hình trong Control Panel Devices và có giá trị ngâm định khởi động là System. Vùng cho File System Recognizers có thể thấy trong:

\HKEY\_LOCAL\_MACHINE

\SYSTEM

\CurrentControlSet

\Services

\

- Thư viện liên kết động tiện ích hệ thống file (File System Utility Dynamic Link Library-DLL) Là một phần của hệ thống file chứa các thực thể (entry) đặc tả hệ thống file cho các tiện ích như CHKDSK và FORMAT. Để cho hệ thống file được cài đặt mới làm việc với những tiện ích này thì tiện ích hệ thống file DLL cần được cung cấp.

Loại phân vùng FAT HPFS NTFS

File System Driver FASTFAT.SYS PINBALL.SYS NTFS.SYS

File System FAT\_REC.SYS HPFS\_REC.SYS NTFS\_REC.SYS  
Recognizer  
File System UFAT.DLL UHPFS.DLL UNTFS.DLL  
Utility DLL

Tất cả các file hệ thống file có thể tìm trong thư mục con \\System32

## **Giải Pháp Quản Lý Mạng Từ Xa Cho Microsoft** [12/9/2003 5:03:00 AM]

Một trong những vấn đề nan giải mà các nhà quản trị Microsoft đang đương đầu là làm sao quản lý hệ thống từ xa theo cách an toàn hơn? Trong thế giới UNIX thì câu trả lời khá đơn giản: dùng giao thức SSH. Nhờ có SSH, chúng ta có thể quản lý những hệ thống từ xa không những trong chế độ văn bản (text mode), mà còn có thể chạy những trình ứng dụng X-Window từ xa bằng cách dùng kỹ thuật đường hầm giao thức (protocol tunneling). Và tất cả những cái đó đều dùng mật mã vững chắc để bảo vệ việc truyền dữ liệu đi từ việc truy cập trái phép.

Không may, để bảo vệ an toàn việc truy cập từ xa đến hệ thống MS Windows thì không dễ dàng một chút nào. Tại sao? Thứ nhất, chỉ có NT Terminal Server, 2000 Server và XP được trang bị những dịch vụ quản lý từ xa (Terminal Services). Thứ hai, giải pháp quản lý hệ thống MS Windows có khả năng là không mã hoá dữ liệu truyền đi (giống như VNC), hoặc là sự bổ sung của họ thường đi liền với những chi phí thêm vào khá đáng kể.

Bài viết này sẽ mô tả phương pháp chung cho việc quản lý từ xa mà có thể được dùng để quản lý hầu hết tất cả hệ thống của MS Windows: từ Windows 95 lên đến XP. Phương pháp này không những chỉ dùng chi phí thấp nhất, mà còn có sự bảo mật tương đối cao hơn.

### **Giải Pháp**

Những đặc điểm nào mà giải pháp quản lý mạng từ xa nên có? Thứ nhất, là phải thiết thực. Mặc dầu trong trường hợp của hệ thống Unix, việc sử dụng phương pháp này để quản lý MS Windows khá xa vời ý tưởng trên. Bởi vì MS Windows là một hệ thống dựa trên môi trường đồ hoạ, việc quản lý từ xa cũng nên thực hiện trong một chế độ đồ hoạ. Bên cạnh đó cũng phải an toàn hơn. Giải pháp này không những cung cấp sự thẩm quyền cho người sử dụng, mà còn phải đảm bảo tính cần mật và toàn vẹn hơn cho việc truyền dữ liệu.

Trong giải pháp này, tất cả những yêu cầu trên sẽ được gặp ở đây bằng cách dùng phần mềm có mã nguồn mở sau:

+ VNC - VNC (Virtual Network Computing) cung cấp sự quản lý đồ hoạ cho những hệ thống từ xa. Ở trường hợp của chúng ta, phần mềm VNC sẽ là phần "cốt lõi" của toàn bộ giải pháp này. Nó sẽ cũng cấp một bàn giao tiếp đồ hoạ (graphic console) đến hệ thống MS Windows từ xa.

+ Stunnel - Mục đích chính của tiện ích Stunnel là tạo ra những đường hầm SSL để truyền dữ liệu, thường là những giao thức không mã hoá. Ở giải pháp đang miêu tả ở đây, công cụ này sẽ được dùng để bảo vệ giao thức VNC. Nhờ có Stunnel, nó không những bảo đảm được tính cần mật và toàn vẹn trong việc truyền dữ liệu, mà còn xác thực máy khách của và máy chủ VNC.

+ OpenSSL - OpenSSL là một thư viện mã hoá mà có thể được dùng để nâng cao những ứng dụng bởi chức năng mã hoá dữ liệu. Dùng OpenSSL chúng ta cũng có thể tạo ra, ký hiệu và huỷ bỏ chứng nhận mà có thể được dùng trong giải pháp dựa trên kiến trúc khóa công cộng (public key infrastructure). Ở phương pháp bên dưới công cụ này sẽ được dùng để tạo và ký hiệu chứng nhận cần thiết để xác thực cả máy khách lẫn máy chủ của VNC.

Hình sau đây cho thấy cách mà phần mềm đề cập ở trên được dùng để cung cấp sự quản lý vững chắc mạng từ xa:

Bây giờ, hãy thực hành giải pháp được miêu tả ở đây.

## Cài đặt phần mềm

Giai đoạn đầu tiên của việc quản lý an toàn từ xa là phải cài đặt phần mềm.

### VNC

Để dùng VNC, ta phải tải về ([www.uk.research.att.com/vnc/](http://www.uk.research.att.com/vnc/)) và cài đặt nó trên máy chủ mà ta muốn quản lý ở xa mà sẽ được đề cập dưới đây. Tiếp theo, ta phải đăng ký dịch vụ VNC (Start Menu ® RealVNC ® VNC Server ® Register VNC Server Service) và khởi động lại hệ thống.

Sau khi khởi động lại hệ thống, ta phải đặt vài tham số cơ bản của dịch vụ VNC. Quan trọng nhất là gõ một mật khẩu phù hợp để bảo vệ dịch vụ VNC chống lại sự truy cập trái phép. Bước tiếp theo là tắt tùy chọn "Enable Java Viewer" (nó không được sử dụng kể từ khi tùy chọn này yêu cầu hai đường hầm SSL riêng biệt), theo như hình bên dưới.

Sau khi định xong cấu hình cho máy chủ VNC, ta nên tải phần mềm máy khách VNC (vncviewer.exe) và đặt nó ở máy chủ mà nó sẽ là máy khách của VNC.

Ở điểm này ta nên kiểm tra nếu máy khách VNC có thể thiết lập một nối kết đến máy chủ VNC. Nếu những chương trình có thể liên lạc lẫn nhau được, thì ta hoàn thành việc định cấu hình

Bởi vì máy chủ VNC chỉ có khả năng truy cập bởi một Stunnel cục bộ, những mục nhập theo sau nên được thêm vào Windows Registry trên máy chủ VNC:

#### CODE

```
Key: HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3Name: LoopbackOnly
Type: REG_DWORD
Value: 1
```

Những mục nhập ở trên làm cho nó có khả năng dùng kết nối loopback, và chỉ giới hạn listen ở cổng 5900/tcp đến localhost (127.0.0.1). Nhờ đó, máy chủ VNC sẽ không bị truy cập trực tiếp từ mạng máy tính. Nếu ta không muốn người sử dụng tắt dịch vụ VNC trên host của máy chủ VNC, thì nhập vào Registry:

#### CODE

```
Key: HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3\Default
Name: AllowShutdown
Type: REG_DWORD
Value: 0
```

Để kích hoạt những sự thay đổi ở trên, ta phải khởi động lại dịch vụ VNC.

### Stunnel

Bước tiếp theo là cài đặt tiện ích Stunnel. Để cài đặt, ta tải xuống và đặt nó trên máy chủ và máy khách của VNC, trong thư mục: C:\Program Files\Stunnel. Ta cũng nên tải thêm hai thư viện của Stunnel: libeay32.dll, libssl32.dll.

Nếu ta muốn cho Stunnel tự động bắt đầu khi hệ thống khởi động, thì thêm vào Windows Registry mục sau:

## CODE

Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\  
Microsoft\Windows\CurrentVersion\Run  
Name: Stunnel  
Type: REG\_SZ  
Value: "C:\Program Files\Stunnel\stunnel-4.04.exe"

## OpenSSL

Lúc này thư viện OpenSSL phần lớn được cài đặt như mặc định trong hầu hết Linux phân phối, bởi vì nó phụ thuộc vào OpenSSH. Tuy nhiên, một vài người biết rằng có phiên bản OpenSSL cho MS Windows có chức năng gần như giống nhau. Bởi vì bài viết dành cho nền tảng MS Windows, nên ta sẽ sử dụng phiên bản OpenSSL này.

Để cài đặt và định cấu hình ch phần mềm OpenSSL, ta phải thực hiện những bước sau:

Phiên bản của OpenSSL (openssl.exe) có thể tải về từ <http://www.stunnel.org/download/binaries.html> . Giống như chương trình Stunnel, ta cũng phải tải thêm hai thư viện: libeay32.dll và libssl32.dll. Phần mềm tải về phải đặt trong thư mục C:\Program Files\OpenSSL.

Hai file khác cũng phải được tải về là: file cấu hình, openssl.conf (<http://www.securityfocus.com/data/tools/openssl.conf>) và script ca.bat (<http://www.securityfocus.com/data/tools/ca.bat>), mà sẽ được dùng để cấp sự chứng nhận. Hai file đó đặt trong thư mục C:\Program Files\OpenSSL. Nội dung cuối cùng của thư mục phải tương tự như sau:

Bước tiếp theo cấp sự chứng nhận, mà được dùng để xác thực máy chủ và máy khách của VNC.

Chìa khóa và việc tạo ra Bằng chứng nhận (Certificates)

### Certification Authority

Quy trình cấp chứng nhận nên bắt đầu bằng việc tạo một cặp khoá private/public và chứng nhận cho nhóm thứ ba, hay CA (Certification Authority). Chìa khóa private của CA sẽ được dùng sau này để ký hiệu chứng nhận cho máy chủ và máy khách VNC. Sự chứng nhận CA sẽ được thay thế trên tất cả máy chủ và máy khách VNC. Bởi vì chìa khóa private của CA là một trong những yếu tố quan trọng của mọi sự thi hành PKI, chìa khoá phải được bảo vệ bằng cụm mật khẩu tốt và tránh xa những người dùng bình thường.

Để tạo ra một cặp chìa khoá private/public và chứng nhận cho CA, ta chạy script ca.bat như sau:

```
C:\progra~1\OpenSSL\ca genca
```

Sau khi thực hiện những bước trên, văn bằng CA sẽ được bảo quản ở file C:\CA\CAcert.pem, và cặp chìa khoá private/public sẽ được bảo quản ở file C:\CA\private\CAkey.pem.

### Máy chủ VNC

Bước tiếp theo là generate cặp chìa khoá private/public và chứng nhận cho máy chủ VNC:

```
C:\progra~1\OpenSSL\ca server
```

Theo kết quả, những file sau sẽ được tạo ra trong thư mục C:\CA\temp\vnc\_server:

server.key - cặp chìa khoá private/public

server.crt - chứng nhận máy chủ

server.pem - server.key + server.crt (yêu cầu bởi Stunnel)

Máy khách VNC

Bước cuối cùng là tạo ra cặp chìa khóa private/public và chứng nhận cho máy khách VNC:

C:\progra~1\OpenSSL\ca client

Giống như ở bước trước, những file sau sẽ được tạo trong thư mục C:\CA\temp\vnc\_client:

+ client.key - cặp chìa khóa private/public

+ client.crt - chứng nhận máy khách (client's certificate)

+ client.pem - client.key + client.crt (yêu cầu bởi Stunnel)

Cấu hình Stunnel

VNC Server

Trước khi thử thiết lập một sự kết nối an toàn giữa máy chủ và máy khách của VNC, ta phải định cấu hình cho tiện ích Stunnel, và trang bị với tất cả những chìa khoá và chứng nhận mà nó đòi hỏi.

Để làm điều đó, ta nên tạo một file "C:\Program Files\Stunnel\stunnel.conf" với nội dung sau:

CODE

CAfile = CAcert.pem

CAPath = certificates

cert = server.pem

client = no

verify = 3

[vnc]

accept = 443

connect = 127.0.0.1:5900

Cấu hình ở trên sẽ làm cho tất cả những kết nối vào cổng 443/tcp sẽ được chuyển tiếp đến cổng cục bộ 5900/tcp.

Bước tiếp theo là thay thế cả CA's certificate (C:\CA\CAcert.pem) và cặp chìa khóa private/public của máy chủ VNC, chứng nhận (C:\CA\temp\vnc\_server\server.pem) vào thư mục C:\Program Files\Stunnel.

Cuối cùng ta phải nhập chứng nhận của máy khách VNC vào. Để cho Stunnel tìm certificate trong suốt quá trình thẩm định, ta phải thay đổi tên của nó như sau (lệnh theo sau phải chạy trên máy chủ mà certificates đã generate; value phải được thay thế bằng kết quả của lệnh "openssl x509"):

cd C:\CA\temp\vnc\_client

C:\progra~1\openssl\openssl x509 -hash -noout -in client.crt

value

copy client.crt value.0

File value.0 nên đặt vào thư mục C:\Program Files\Stunnel\certificates.

VNC Client

Đầu tiên, ta phải tạo một file "C:\Program Files\Stunnel\stunnel.conf" với nội dung sau:

CODE

CAfile = CAcert.pem

CAPath = certificates

cert = client.pem

client = yes

verify = 3

[vnc]

accept = 127.0.0.1:5900

connect = VNC\_server\_IP\_address:443

Bước tiếp theo là cất giữ CA's Certificate (C:\CA\CAcert.pem) và cặp chìa khóa private/public và chứng nhận của máy khách VNC (C:\CA\temp\vnc\_client\client.pem) trong thư mục C:\Program Files\Stunnel.

Cuối cùng, ta phải đổi tên của file chứng nhận máy chủ VNC theo cách sau:

cd C:\CA\temp\vnc\_server

C:\progra~1\openssl\openssl x509 -hash -noout -in server.crt

value

copy server.crt value.0

và cất nó vào thư mục C:\program files\Stunnel\certificates.

Nội dung cuối cùng của thư mục C:\Program Files\Stunnel phải tương tự như sau:

Kiểm tra việc kết nối

Lúc này tất cả các phần mềm đã sẵn sàng được dùng. Để kiểm tra nó, ta phải chạy Stunnel trên cả máy chủ, máy khách, và chạy dịch vụ VNC.

Sau đó, ở host máy khách VNC ta chạy vncviewer.exe. Ta nhập vào địa chỉ: 127.0.0.1. Nếu mọi thứ được định hình chính xác, việc kết nối với máy chủ VNC sẽ được thiết lập, và Stunnel sẽ hiển thị những thông tin sau:

Ở máy chủ VNC:

Ở máy khách VNC:

Nếu vì một vài lý do nào đó mà sự kết nối bị hỏng, ta nên tăng mức độ log của Stunnel, và cố gắng thử tìm ra nguyên nhân. Để làm điều đó ta thêm vào file stunnel.conf:

```
debug = 7
```

Sau đó khởi động Stunnel và thử thiết lập kết nối một lần nữa.

Kết nối đảo ngược

Phương pháp trên hoạt động tốt, nhưng chỉ khi máy chủ VNC hợp lệ, địa chỉ IP ở bên ngoài hay nó được đặt trong cùng mạng LAN, giống như máy khách VNC. Nhưng điều gì sẽ xảy ra nếu máy chủ VNC được đặt trong NAT hay những kết nối vào host này bị drop bởi firewall?

Như tôi đã đề cập ở trước, VNC có khả năng thiết lập sự kết nối đảo ngược. Để dùng tùy chọn đó, những thay đổi sau phải được áp dụng cho file stunnel.conf trên máy chủ VNC:

CODE

```
CAfile = CAcert.pem
```

```
CApath = certificates
```

```
cert = server.pem
```

```
client = yes
```

```
verify = 3
```

```
[vnc]
```

```
accept = 127.0.0.1:5500
```

```
connect = VNC_client_IP_address:443
```

và ở máy khách VNC:

```
CAfile = CAcert.pem
```

```
CApath = certificates
```

```
cert = client.pem
```

```
client = no
```

```
verify = 3
```

```
[vnc]
```

```
accept = 443
```

connect = 127.0.0.1:5500

Lưu ý rằng vai trò của tiện ích Stunnel bây giờ đã đảo ngược. Stunnel ở máy chủ trở thành máy khách SSL, và Stunnel ở máy khách lại thành máy chủ SSL.

Cũng có một sự thay đổi trong cách thiết lập kết nối bằng phần mềm VNC. Ở phương pháp này, nên chạy vncviewer.exe đầu tiên, ở chế độ listen (Start Menu ® RealVNC ® VNC Viewer ® Run Listening VNC Viewer). Sau đó, ở máy chủ VNC, ta phải dùng tùy chọn "Add New Client" theo sau:

Sau khi thực hiện xong những bước trên, ta thiết lập sự kết nối giữa máy chủ và máy khách VNC.

Giải pháp trên là một cách rất hiệu quả để hạn chế việc bỏ sót NAT; tuy nhiên nó cũng có một cái bất lợi rất quan trọng: để thiết lập một sự kết nối đảo ngược, sự can thiệp thủ công lên máy chủ được đòi hỏi. Câu hỏi phát sinh là có cách nào thiết lập sự kết nối mà không cần đến sự can thiệp bằng thủ công?

Để hiển thị, nó phải được dùng trong hệ điều hành MS Windows "Task Scheduler Service", để giải quyết vấn đề can thiệp bằng thủ công. Hình ảnh bên dưới là một ví dụ của "Task Scheduler", mà máy chủ VNC cố gắng thiết lập một kết nối với máy khách VNC hàng ngày giữa 9 giờ sáng và 9 giờ chiều, trong khoảng 10 phút. Nếu muốn thiết lập một kết nối với máy chủ VNC, tất cả những gì ta cần làm là chạy VNC ở chế độ listen và chờ đến khi máy chủ kết nối. Phần lớn trong 10 phút đó, bàn giao tiếp hình ảnh (graphics console) sẽ được "gửi" đến chúng ta.

Phương pháp mô tả ở trên có nhiều giới hạn và bất lợi. Tuy nhiên, đây cũng là một cách hay để quản lý một host mà ta không thể thiết lập kết nối trực tiếp.

Tóm tắt

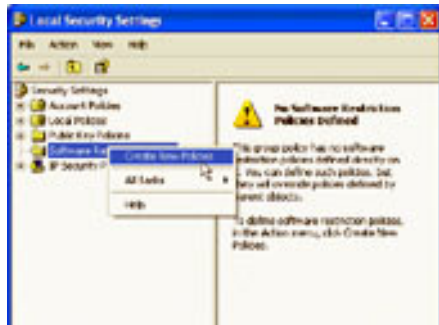
Có nhiều chương trình quản lý từ xa MS Windows. Không may, một số lượng lớn trong đó không bảo vệ an toàn việc truyền dữ liệu hoặc việc thực hiện chúng thì tổn rất nhiều. Phương pháp phác thảo ở trên là một giải pháp không mất tiền cho việc quản lý MS Windows từ xa một cách an toàn hơn. Nhờ có giao thức SSL và sự thẩm quyền dựa trên việc chứng nhận, giải pháp này không những đủ sức có cơ hội cạnh tranh với những giải pháp thương mại, mà còn trong cả việc bảo mật hoàn hảo hơn.

## **Bí mật security của Windows XP** [12/23/2003 2:18:00 AM]

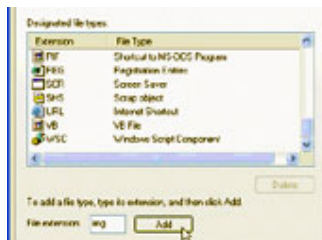
Trong MS Outlook tất cả các file có phần mở rộng là exe, vb, chm.....v..v đều không mở được và bị block lại vì lý do an toàn cho hệ thống vì có một số chương trình có thể tự động chạy mà không cần bạn kích hoạt nó lên nhưng nó vẫn chạy trong máy của bạn ngoại trừ các file nén dạng zip hay rar...vv . thứ hai nữa là Java Script và VB không còn được hỗ trợ trong Windows XP nữa bạn có thể thấy được trong Frontpage và MS Outlook.

Để thêm vào hoặc bớt đi phần mở rộng của file này các bạn hãy làm như sau :

Vào Start >> Control panel >> Administrative Tool>> Local security settings >> bấm chuột phải vào Software restriction policies >> chọn Create New Policies



>> chọn Dword tên là Designated File Types >> Double click vào file này và bạn có thể xoá các phần mở rộng bằng phím delete hay thêm vào bằng cách thêm vào trong phần file extension và bấm nút add như vậy là phần mở rộng đã được đưa vào phần cấm chạy của Windows XP.



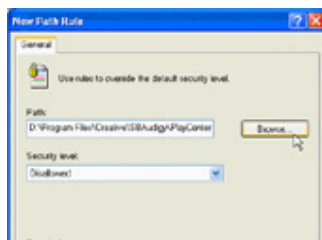
Phần kè: Không cho một chương trình ứng dụng nào đó chạy khi vắng mặt chủ nhân và không muốn ai đó sử dụng CD hoặc là Floppy của bạn

Không cho một chương trình ứng dụng nào đó chạy khi vắng mặt chủ nhân:

Vào Start >> Control panel >> Administrative Tool >> Local security settings >> bấm chuột phải vào Additional Rules (phần này chỉ có khi bạn đã làm phần trên “Create New Policies”) chọn New Path Rule



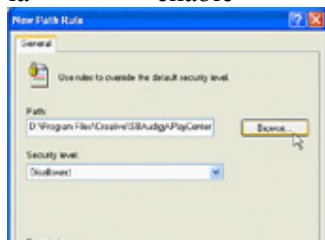
>> Chọn chương trình mà bạn không muốn cho nó chạy khi bạn đi công tác xa chẳng hạn như là Internet Explorer trong phần browse trong phần Security hãy để là disallowed và khi cần mở bạn chỉ việc chọn nó là unrestricted là nó sẽ mở thôi nhưng bạn phải restart máy lại cho nó có hiệu lực nhé.



Ngoài ra nếu bạn không muốn ai đó sử dụng CD hoặc là Floppy của bạn thì hãy làm như sau:

Vào Start >> Control panel >> Administrative Tool >> Local security settings >> Local Policies >> Security Options >> chọn Dword :Devices: Restrict CD-ROM access to locally logged-on user only hoặc là Devices: Restrict Floppy access to locally logged-on user only >> hãy bấm double click vào nó và chọn

là enable xong rồi khởi động lại máy.



Và vẫn còn một số tính năng khác khá rất hay trong phần này các bạn hãy thử đi nhé

## Hạn chế quyền hạn của các Users trong Windows XP [12/25/2003 1:32:00 AM]

Máy của bạn được chia sẻ cho nhiều người sử dụng, trong đó, bạn là “sếp sòng” (administrator) còn những người khác (users) đều “dưới trướng” của bạn hết và đương nhiên, quyền “sinh sát” là ở ở trong tay bạn. Sau đây là vài biện pháp bảo vệ sự riêng tư của các thông tin trong máy, hạn chế quyền hạn của các users.

Khoá chức năng Folder Views trong Folder Options (mở Windows Explorer/Tools/Folder Options): chức năng này giúp bạn lựa chọn những tùy chọn cho sự hiển thị của các thông tin trong thư mục như: hiển thị/dấu những file ẩn, hiển thị kích thước, đường dẫn của thư mục,....

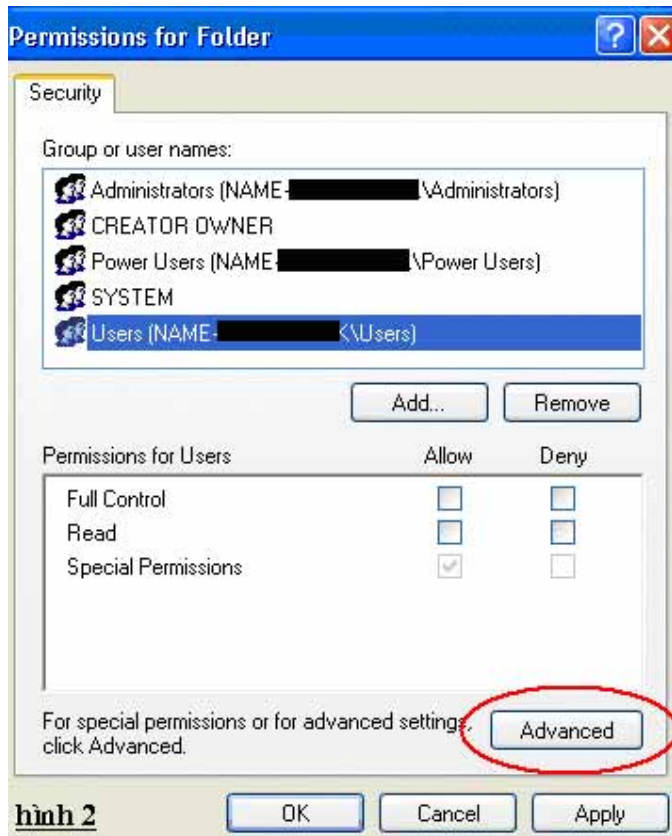
Để khoá chức năng này, đầu tiên, bạn khởi động Registry Editor, và tìm đến khóa: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder.

Click chuột phải vào khóa Folder và chọn Permissions.



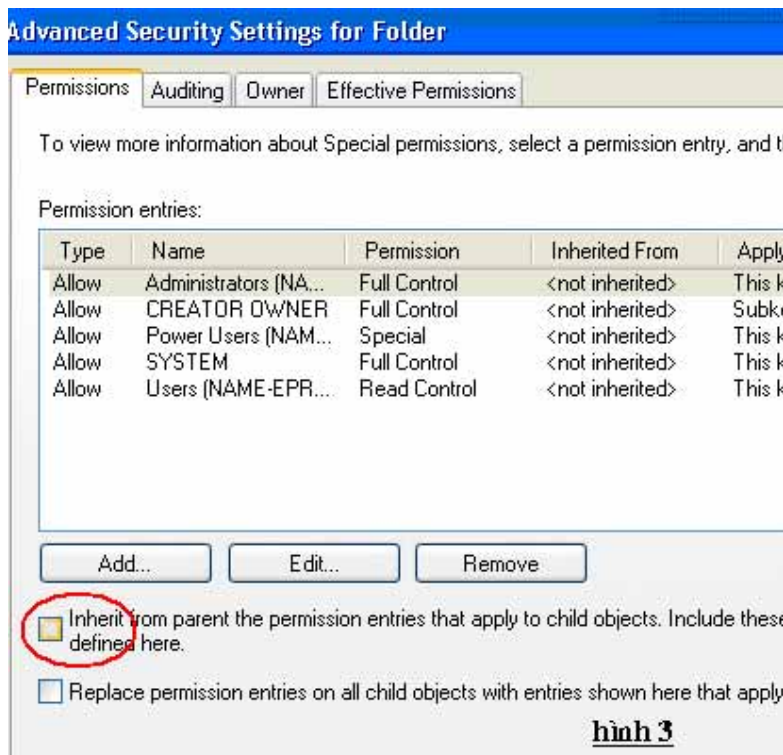
**hình 1**

Trong trình đơn Permissions for Folder mới mở ra, bạn chọn Advanced.

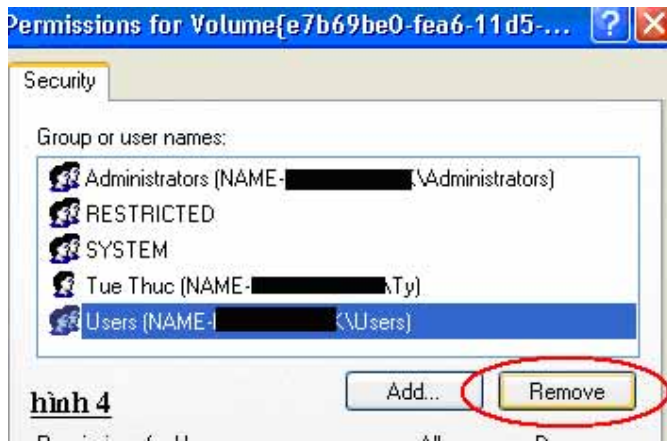


**hình 2**

Tùy chọn Inherit from parents the permissions... đang được đánh dấu, click vào đó để bỏ chọn options này.



Khi đó, một cửa sổ thông báo sẽ hiện lên, bạn chỉ cần click vào nút Copy. Click OK. Trở lại trình đơn Permissions for Folder, trong khung Groups and Users name, bạn chọn Users [.....] vào click nút Remove.



Click OK và khởi động máy. Từ đây, ngoài bạn ra, không users nào có thể “táy máy” gì được trong Folder Views.

Dấu một ổ đĩa: đầu tiên, bạn khởi động Registry Editor và tìm đến khoá: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer. Click phải vào khoá Explorer, chọn New/DWORD Value và đặt tên cho nó là NoDrive. Double click vào giá trị mới tạo. Trong khung Base, bạn chọn Decimal. Trong khung Value Data, bạn gõ vào giá trị thập phân của các ký tự mà bạn đặt tên cho các ổ đĩa (A, B, C,...) theo bảng sau. Click OK và khởi động lại máy.

Ổ đĩa Số của ổ đĩa Số phải gõ trong khung Value Data

- A 0 (20=)1
- B 1 (21=)2
- C 2 (22=)4
- D 3 (23=)8
- E 4 (24=)16

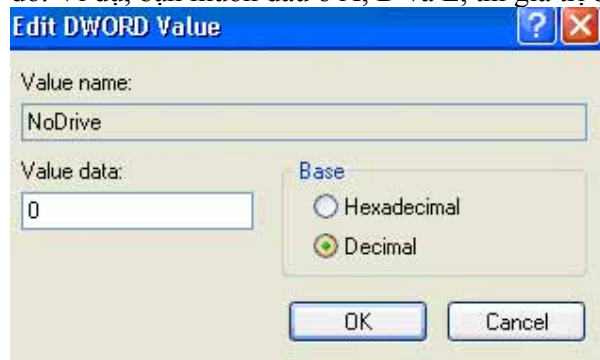
.....

Ghi chú:

· Nếu bạn muốn “ra uy” dấu 1 ổ đĩa, không cho 1 user nào đó sử dụng một ổ đĩa nào đó, bạn chỉ cần login vào phiên làm việc của user đó (bằng cách gõ password) và thực hiện nhiệm vụ. Bạn có thể áp đặt những “lệnh cấm vận” khác nhau lên những users khác nhau. Ví dụ như, bạn có thể không cho người này sử dụng ổ đĩa C; E, đồng thời không cho người kia sử dụng ổ A; R;.....

Nếu bạn muốn dấu nhiều ổ đĩa bạn chỉ cần gõ vào khung Value Data tổng giá trị thập phân của các ổ đĩa

đó. Ví dụ, bạn muốn dấu ổ A, D và E, thì giá trị bạn phải nhập là: 19 (20+21+24).



 In bài này | [Trao đổi - Nhận xét bài viết](#)

Theo TN