ODS
SAVE TIME - IMPROVE VALUE

12 GỢI Ý

GIÚP IT TĂNG CƯỜNG BẢO MẬT CHO SERVER LINUX

Lời nói đầu

Trên thế giới đã có hơn 50% các doanh nghiệp lớn và nhỏ sử dụng ít nhất một nền tảng công nghệ đám mây - Cloud Server để chuyển đổi kỹ thuật số. Đây được xem là giải pháp máy chủ tốt nhất hiện nay khi giải quyết được rất nhiều vấn đề cho doanh nghiệp như: Chi phí, năng suất hoạt động, nhân sự vận hành,...

Từ những lợi ích vượt trội mà công nghệ điện toán mang lại khiến việc dịch chuyển “lên mây” được diễn ra như một lẽ tất yếu đối với các doanh nghiệp ngày nay. Điều đó làm dấy lên nhiều lo lắng và tranh cãi xung quanh tính bảo mật cho dữ liệu.

Dữ liệu “trên mây”

Mục tiêu tấn công hàng đầu của tin tặc

Một đặc tính của công nghệ điện toán đám mây chính là khả năng sao lưu tự động liên tục, điều này đồng nghĩa với việc một nguồn dữ liệu có giá trị cao sẽ “luôn có mặt” trên mây với sự tăng trưởng mỗi ngày theo cấp số nhân.

Bằng việc upload và download dữ liệu liên tục, điện toán đám mây trở thành một hệ thống thông tin khổng lồ. Chính vì vậy, đây được xem là mục tiêu tấn công hàng đầu của các tin tặc.

Đã có không ít trường hợp dữ liệu bị xâm phạm trong đám mây, bao gồm nhiều dữ liệu quan trọng như thông tin cá nhân của khách hàng, hồ sơ sức khỏe, dữ liệu kinh doanh, thông tin bầu cử,... Điều này gây thiệt hại không hề nhỏ cho đơn vị sở hữu các dữ liệu này. Từ đó cho thấy tầm quan trọng của bảo mật đám mây và nhu cầu toàn vẹn dữ liệu.

12 GỢI Ý

GIÚP IT TĂNG CƯỜNG BẢO MẬT CHO SERVER LINUX

Linux là hệ điều hành phổ biến và chuyên dụng, có thiết kế giao diện mang tính ứng dụng cao, tuy nhiên vẫn sẽ có nhiều nguy cơ bảo mật tiềm ẩn. Dưới đây là 12 gợi ý giúp bạn nhanh chóng bảo vệ và tăng cường bảo mật cho Server Linux.

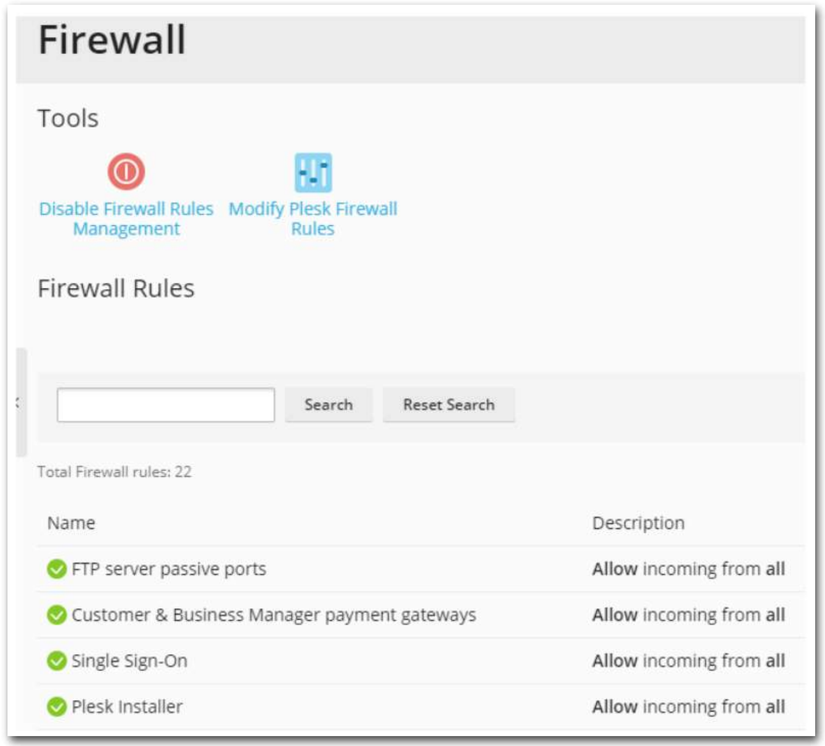
Tăng cường bảo mật bằng Tường lửa (Firewall)

Xây dựng tường lửa là bước phòng thủ đầu tiên và quan trọng hàng đầu khi thiết lập hệ thống bảo mật cho doanh nghiệp.

Chúng sẽ lọc truy cập mạng hiệu quả, tiến hành xác minh tên máy chủ, đăng nhập tiêu chuẩn và bảo vệ dữ liệu khỏi những tác động gây hại khác.

Một vài gợi ý về bảo mật bằng tường lửa:
IPtables - Ứng dụng tường lửa tiêu chuẩn được cấu hình, tích hợp trong hầu hết các bản phân phối của Linux (CentOS, Ubuntu...)
FirewallD - Giải pháp tường lửa mạnh mẽ được cài đặt mặc định trên RHEL 7 và CentOS 7 thay thế cho IPTables

Trong trường hợp bạn gặp khó khăn khi sử dụng những dòng lệnh phức tạp của các phần mềm trên thì bạn có thể sử dụng **PLESK** - Phần mềm quản trị Hosting được đánh giá là thích hợp đến 90% với Server Linux, cho phép quản lý và triển khai đa tác vụ trên Website một cách đơn giản và dễ dàng.



PLESK giúp Website hoạt động ổn định và liên tục với khả năng bảo mật mạnh mẽ, giữ cho hệ thống không bị tấn công bởi mã độc. Bạn có thể thiết lập Tường lửa (Fire-wall) qua các bước sau:

- Vào mục Công cụ & Cài đặt --> Chọn Tường lửa trong phần bảo mật.
- Click bật Quản lý tường lửa cho nút bên cạnh chuyển màu xanh.
- Tiếp tục nhấp Sửa đổi tường lửa Plesk --> Chọn những sửa đổi mà bạn muốn, bật nút xanh. Chẳng hạn như, bật từ chối các kết nối bên ngoài đến hệ thống.
- Cuối cùng, click Áp dụng để hoàn tất thao tác một cách nhanh chóng, đơn giản.

Ngoài ra, vài dịch vụ Plesk riêng lẻ còn có các quy tắc với phạm vi hẹp hơn như SMTP hoặc MySQL. Có tác dụng chi phối những liên kết từ ngoài muốn tiến vào hệ thống.

Xóa bớt các dữ liệu không cần thiết

Xem xét và loại bỏ những dữ liệu không cần thiết vì đây có có thể trở thành mục tiêu tấn công của tin tặc.

Bên cạnh đó, bằng việc xóa bớt dữ liệu không dùng tới sẽ giúp hệ thống của bạn hoạt động mượt mà hơn. Đây cũng chính là một trong những cách hạn chế lỗ hổng an ninh, bảo mật tuyệt vời nhất. Bạn nên tìm hiểu, tham khảo và ứng dụng triệt để nhé!

Thường xuyên cập nhập hệ thống

Việc luôn giữ cho Server ở trạng thái Update sẽ nâng cao tính năng mới, vá lại những lỗ hỏng và sửa lỗi hoàn chỉnh, nâng cấp phần nhân hệ thống ngay lập tức. Từ đó, hệ thống trở nên hoàn thiện, các hacker cũng không còn khả năng lợi dụng những yếu tố lỗi nào để xâm nhập, tấn công được. Sử dụng những lệnh sau để cập nhật Server nhanh:

```
# yum update

# yum check-update
```

Sử dụng Kernel Care để tự động vá lỗi thường xuyên

Kernel Care là dịch vụ giúp tăng cường bảo mật máy chủ bằng cách áp dụng các bản vá lỗi trực tiếp cho Kernel của hệ điều hành Linux.

- Thiết lập hệ thống an toàn bằng cách phát hiện, thiết lập chế độ phòng vệ bằng tính năng kiểm tra liên tục 4 tiếng/lần.
- Vá lỗi trực tiếp trên hệ điều hành Linux mà không cần phải khởi động lại máy chủ.
- Luôn tự động cập nhật những phiên bản mới nhất, hoàn toàn không mất nhiều thời gian cài đặt như nhiều hệ điều hành khác.

Khuyến khích sử dụng những mật khẩu mạnh hơn

Chọn mật khẩu có tính bảo mật cao được xem là bước tạo "hàng phòng thủ" chắc chắn để giúp bạn loại bỏ sự tấn công của tin tắc khỏi những dữ liệu quan trọng. Sử dụng ***Module Cracklib (PAM)*** sẽ buộc người dùng phải sử dụng cho mình những mật khẩu mạnh và an toàn hơn. Hãy thêm những dòng sau bằng một trình biên soạn

```
# vi etc/pam.d/system-auth
```

và thêm dòng sau (lcredit,ucredit, dcredit hay ocredit tương ứng với chữ thường, chữ hoa, chữ số và các ký tự khác)

/lib/security/$ÍA/pam_cracklist.so retry = 3 minlen=8 lcredit =-1 ucredit=-2 dcredit=-2 ocredit=-1

Hạn chế sử dụng mật khẩu cũ

Bằng việc hạn chế sử dụng mật khẩu cũ bạn sẽ giảm thiểu nguy cơ bị tin tặc tiếp cận hoặc người dùng trước đặt lại mật khẩu. Các mật khẩu sẽ được lưu trữ tại ***/etc/pam.d/system-auth***, file này chỉ có thể truy cập trong chế độ PAM. Mở file ***'etc/pam.d/system-auth'*** trong RHEL/CentOS/Fedora.

```
# vi /etc/pam.d/system-auth
```

Thêm dòng lệnh sau vào mục 'auth'

```
auth        sufficient      pam_unix.so likeauth nullok
```

Mở file 'etc/pam.d/common-password' trong Ubuntu/Debian/Linux Mint

```
# vi /etc/pam.d/common-password
```

Thêm dòng lệnh sau vào mục 'password' để ngăn người dùng sử dụng lại 1 trong 5 password gần nhất của họ

```
password    sufficient      pam_unix.so nullok use_authtok md5 shadow remember=5
```

Nếu như người dùng muốn sử dụng lại bất kỳ mật khẩu nào trong số 5 cái mới nhất, họ sẽ nhận được một dòng cảnh báo

```
Password has been already used. Choose another.
```

Cấu hình bảo mật cho kết nối SSH

Về tiêu chuẩn, mặc định cấu hình SSH sử dụng Port 22 để kết nối. Đó là một lợi thế cho kẻ tấn công vào Server của bạn. Do đó, hãy cố gắng cải thiện bằng việc thay đổi Port SSH. Ngoài ra, hãy áp dụng giới hạn chỉ cho phép đăng nhập bằng key vào Server. Tuy có hơi phức tạp với nhiều lệnh, nhưng hiệu quả của phương pháp này là không cần bàn cãi.

Cụ thể, bạn mở file ***/etc/ssh/sshd_config*** và sửa các dòng sau:
- Port 2020
- PubkeyAuthentication yes
- PasswordAuthentication no

Tiếp theo, tiến hành thực hiện thêm bước Public key lên Server Linux là hoàn thành. Sau đó, bắt đầu khởi động lại dịch vụ SSH bằng lệnh:

 # /etc/init.d/ssh restart

hoặc

 # systemctl restart sshd.service

Liên tục giữ kết nối hiện tại và mở thêm một kết nối mới sử dụng key tới Server với port 2020 để kiểm tra.

Thường xuyên Kiểm tra và Tắt các cổng dịch vụ không sử dụng

Thường xuyên kiểm tra, giảm thiểu tối đa các cổng dịch vụ không dùng đến để tăng hiệu năng cho máy tính hoạt động trơn tru hơn cũng như giảm thiểu các lỗ hổng bảo mật mà tin tặc có thể tiếp cận.
Để thực hiện, bạn có thể sử dụng câu lệnh ***'netstat'*** để xem tất cả các cổng đang mở và các chương trình có kết nối mạng. Sau đó, tiến hành rà soát, nếu có phát hiện phải nhanh chóng dùng lệnh ***'chkconfig'*** để tắt các dịch vụ đó đi.

Không nên chạy nhiều dịch vụ trên cùng một Server

Việc sử dụng nhiều dịch vụ mạng khác nhau trên cùng một Máy chủ vật lý hoặc VPS sẽ mang đến cho bạn nhiều nguy cơ bị xâm phạm thông tin bảo mật hơn.
Giả sử bạn đang có các dịch vụ là: Web, Database, Email và File Sharing đều được chạy trên cùng một Server. Khi một trong các dịch vụ này có lỗ hổng bảo mật, kẻ tấn công sẽ dễ dàng khai thác và chiếm quyền sở hữu toàn bộ thông tin của các dịch vụ còn lại trên Server này.
Vì vậy, bạn nên cân nhắc việc dịch chuyển từ Server Vật lý lên Cloud Server. Điều này làm tăng khả năng đảm bảo an toàn dữ liệu khi chạy các dịch vụ khác nhau trên mỗi Cloud Server riêng biệt.

Hạn chế dịch vụ FTP, Telnet và Rlogin/ Rsh trên Linux

Chỉ với một gói Sniffer, bất cứ ai cũng có thể nhận được tên người dùng, mật khẩu, lệnh FTP, Telnet và Ssh và các tệp từ hệ thống của bạn truyền đến nếu sử dụng cùng một mạng. Do đó, cần có sự chuẩn bị, hạn chế tối thiểu việc dùng các dịch vụ này trên hệ điều hành Linux. Ngoài ra, bạn cũng nên vận dụng giải pháp sử dụng OpenSSH, SFTP hoặc FTPS (FTP qua SSL), bổ sung mã hóa SSL hoặc TLS vào FTP nữa.

Chỉ với mã lệnh sau, mọi người đều xóa được NIS, Rsh và các dịch vụ lỗi lạc hậu khác nhanh chóng:

Đối với hệ điều hành thường:

```
# yum erase xinetd ypserv tftp-server telnet-server rsh-server
```

Với hệ điều hành Debian/ Ubuntu Linux, hãy thử lệnh:

```
$ sudo apt-get --purge remove xinetd nis yp-tools tftpd atftpd tftpd-hpa telnetd
rsh-server rsh-redone-server
```

Bảo mật nâng cao với SELinux

Sử dụng thêm ***SELinux*** và các phần mở rộng bảo mật Linux khác để thiết lập thêm một lớp lá chắn an toàn nữa cho hệ thống, bên cạnh những bản vá bảo mật khác. Chúng sẽ tăng cường bảo mật cho ***Server Linux*** ở mức độ lớn hơn, mạnh hơn với nhiều chính sách bảo đảm an ninh hữu hiệu.

Khóa tài khoản người dùng sau khi đăng nhập thất bại

Tại hệ điều hành Linux, người ta đã nghiên cứu và phát triển lệnh ***Faillog***, cho phép bạn nhìn thấy các tài khoản đã từng đăng nhập thất bại trước đó.
Hãy tận dụng tính năng này để khóa ngay những người dùng từng Login vào hệ thống máy chủ, loại bỏ triệt để ngay từ những bước đầu.
Faillog hiển thị đầy đủ các bản ghi, thậm chí có chế độ giới hạn lỗi đăng nhập. Vì vậy, bạn hãy thường xuyên dùng đến cách này để nâng cao sự bảo mật cho hệ thống.
Lưu ý, sau khi đã kích hoạt chế độ khóa tài khoản này, nếu muốn mở lại, bạn dùng lệnh: ***faillog -r -u userName.***

6 TIÊU CHÍ CHỌN LỰA NHÀ CUNG CẤP SERVER LINUX TỐT NHẤT

Trong thời công nghệ số phát triển mạnh mẽ như hiện nay, việc dịch chuyển "lên mây" đang trở thành một xu hướng tất yếu mà các doanh nghiệp bắt buộc phải thực hiện. Đây chính là nguyên nhân thúc đẩy sự hình thành của rất nhiều nhà cung cấp Cloud Server để đáp ứng nhu cầu sử dụng ngày càng lớn.

Dưới đây là 6 tiêu chí giúp bạn có được một quyết định đúng đắn, hữu hiệu và không lãng phí ngân sách khi lựa chọn Nhà cung cấp Cloud Server phù hợp với doanh nghiệp của mình.

1 Đánh giá uy tín, tên tuổi của Nhà cung cấp dịch vụ

Dù trong bất kỳ lĩnh vực nào, tên tuổi và độ uy tín của Nhà cung cấp là điều bạn nên quan tâm đầu tiên trước khi quyết định.

Những đơn vị được thành lập lâu năm, có kinh nghiệm chuyên biệt về dịch vụ, khẳng định được chất lượng và hình ảnh của mình trên thị trường sẽ là những yếu tố cực kỳ có ích giúp bạn ***"chọn mặt gửi vàng"***.

Thực tế, nhiều các Nhà cung cấp thường hoạt động, xây dựng uy tín thông qua chất lượng và phản hồi của khách hàng. Do đó, bạn nên tham gia một cộng đồng nào đó quan tâm đến dịch vụ Cloud Server để có thể tiếp cận được những phản hồi chân thật nhất của các khách hàng thực tế.

2 Đánh giá tốc độ, hiệu suất, sự ổn định

Chất lượng dịch vụ là điều mà chúng ta không nên bỏ qua khi lựa chọn Nhà cung cấp Cloud Server. Tốc độ, hiệu suất chạy, sự ổn định hệ thống,... là những tiêu chí đánh giá chất lượng của Nhà cung cấp Cloud Server mà bạn nên chú ý.

Bên cạnh đó, hãy chọn những nơi cung cấp Cloud Server có chính sách dùng thử để trải nghiệm dịch vụ. Đừng ngần ngại đặt ra thắc mắc cho nhân viên hỗ trợ, đây chính là quyền lợi của bạn. Chúng góp phần giúp bạn đem về một dịch vụ tốt nhất, hoàn chỉnh nhất cho công ty mình.

3 Hệ thống An toàn và Bảo mật cho dữ liệu

Nói đến dịch vụ đám mây thì an ninh là mối quan tâm hàng đầu, quan trọng nhất. Một Nhà cung cấp Cloud Server uy tín, đặt lợi ích của khách trước tiên thì sẽ bảo đảm được vấn đề này. Bởi, khách hàng không ai muốn cơ sở dữ liệu của mình bị lộ ra ngoài, ảnh hưởng đến kinh doanh.

Muốn đánh giá được ở đâu có chi tiết, điều khoản bảo mật tốt, bạn nên xem phần cam kết. Những nhà cung cấp tốt, chân chính họ sẽ có quy tắc riêng mình, khẳng định không truy cập trái phép vào Cloud Server nếu chưa được sự cho phép của khách hàng.

Tiêu chí này cũng vô cùng cần thiết, bởi nếu lỡ dính vào phốt an ninh, nhà cung cấp sẽ khó giữ được uy tín trong thị trường.

4 Kênh giám sát tài nguyên Cloud Server

Để đánh giá một Nhà cung cấp Cloud Server có uy tín hay không, bạn cần hỏi, liệu họ có cung cấp một kênh giám sát tình trạng tài nguyên của Cloud Server để bạn theo dõi hay không.

Việc có thể theo dõi hệ thống dữ liệu của doanh nghiệp như tài nguyên CPU, RAM, Traffic của Cloud Server sẽ giúp bạn có được cái nhìn tổng quan để điều chỉnh và xử lý kịp thời những sự cố bất ngờ.

Một Nhà cung cấp tốt, sẽ có yếu tố ***Cloud Monitoring*** này, bạn nên chú ý nhé!

5

Chi phí

Cloud Server nổi bật nhất chính là khả năng tùy biến thông số phần cứng với giá cả hiển thị trực quan. Vậy, đánh giá Nhà cung cấp Cloud Server qua chi phí như thế nào?

➢ Hãy đánh giá thị trường chung, đừng chọn những dịch vụ mà Nhà cung cấp đưa ra mức chi phí cho mỗi đơn vị phần cứng quá thấp. Vì việc giảm giá có thể mang tính cạnh tranh không lành mạnh. Đồng thời, chất lượng dịch vụ của họ không như mong đợi là điều tất nhiên.

➢ Đừng nên so sánh giá của Cloud Server trong nước và nước ngoài. Đây là một sự cân nhắc khập khiễng. Bạn chỉ nên chọn các Nhà cung cấp Cloud Server cùng ở một quốc gia thì mới đưa ra được kết luận đúng.

➢ Chỉ chọn các Nhà cung cấp công khai giá cả minh bạch, rõ ràng bao gồm cả VAT cho khách hàng biết cần chi trả bao nhiêu ngay trên Website. Vì có những Nhà cung cấp đánh vào tâm lý ham rẻ của khách hàng bằng cách không cộng thuế vào bảng giá.

6

Chất lượng dịch vụ hỗ trợ khách hàng

Tiêu chí chất lượng của dịch vụ chăm sóc, tư vấn và hỗ trợ khách hàng được xem là một trong những yếu tố tiên quyết khi lựa chọn dịch vụ.

Bạn hãy quan sát để xem bộ phận kỹ thuật hỗ trợ khách hàng như thế nào thông qua các điểm chủ yếu sau:

- Thời gian hỗ trợ xuyên suốt, sẵn sàng 24/7, xem việc của khách là việc của mình. Chỉ cần 1 cú điện thoại thông báo, đội ngũ nhân viên sẽ có mặt, ngay lập tức phản hồi để trao đổi vấn đề.

- Thái độ hỗ trợ như cách giao tiếp, tinh thần trách nhiệm, sự nhiệt tình, tâm huyết chính là điểm dễ lấy lòng khách hàng.

- Trình độ chuyên môn, hiệu quả hỗ trợ kỹ thuật cao.

ODS
SAVE TIME - IMPROVE VALUE

TỰ HÀO LÀ ĐƠN VỊ CUNG CẤP DỊCH VỤ CLOUD SERVER HÀNG ĐẦU

Đơn vị uy tín cung cấp dịch vụ quản trị Cloud Server chất lượng

Hệ thống Cloud Server của ODS mang đến giải pháp công nghệ thông tin tối ưu cho doanh nghiệp, được xây dựng dựa trên nền tảng hạ tầng của Microsoft. Đảm bảo được sự hoạt động thông suốt, liên tục, với mức chi phí tốt nhất thị trường.

Hệ thống chăm sóc khách hàng được đánh giá là tốt nhất trên thị trường Việt Nam

Hỗ trợ kỹ thuật xuyên suốt, liên tục phòng sự cố xảy ra 24/7/365 ngày 1 năm. Quy trình tư vấn và hỗ trợ kỹ thuật khi có sự cố xảy ra cực kỳ chuyên nghiệp và nhanh chóng. Đảm bảo hoạt động của doanh nghiệp không bị gián đoạn.

Tích hợp phần mềm *Kernel Care* trong các Gói dịch vụ

Trong các gói dịch vụ của Nhà cung cấp Cloud Server này còn có phần mềm **Kernel Care**. Đây là ưu điểm riêng biệt chỉ có riêng ở ODS mang đến cho bạn giải pháp bảo vệ máy chủ linux chống lại các lỗ hổng bảo mật hiệu quả. Bạn có thể dùng chung sản phẩm này với Plesk để tăng cao mức độ an toàn cho dữ liệu quan trọng.

ODS
SAVE TIME - IMPROVE VALUE

THÔNG TIN LIÊN HỆ

Trụ sở chính:

Tầng 12, Tòa nhà trụ sở điều hành và trung tâm thương mại Viettel, 285 Cách Mạng Tháng 8, Phường 12, Quận 10, TP.HCM.

Văn phòng đại diện:

Số 54 Đường C1, Phường 13, Quận Tân Bình, TP.HCM.

1900 6634 (84-28) 7300 7788