Oracle Audit Vault & FireWall Admin Guide

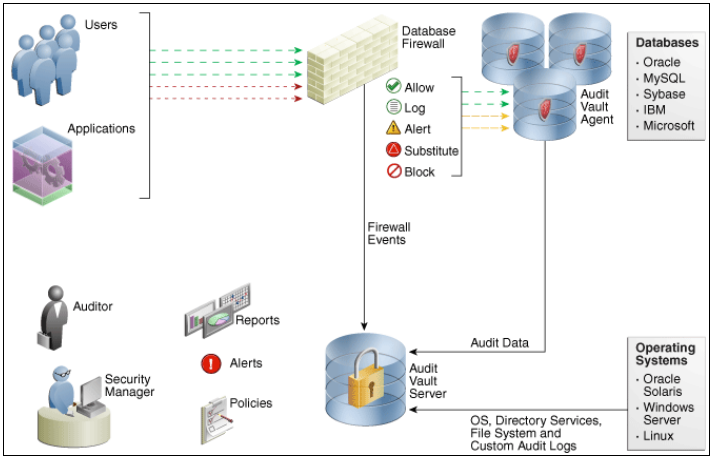
# Giới thiệu chung

## **Các thành phần của Oracle Audit Vault & FireWall**

Oracle Audit Vault & Database Firewall bảo vệ database và các thành phần liên quan bằng 3 cách:

* Cung cấp firewall có thể theo dõi, cho phép hoặc ngăn chặn các truy vấn SQL tới database ngay ở tầng mạng dựa trên cách chính sách của nó.
* Thu thập dữ liệu Audit từ các database và tạo báo cáo audit
* Cung cấp hàng chục build-in cho phép tùy chỉnh cấu hình các thông báo và cảnh báo phù hợp

### Kiến trúc tổng quan của AVDF



* Đôi với mỗi DB cần bảo vệ, sẽ có 1 Audit Vault Agent tương ứng và có 1 Fire Wall nằm ở trên mạng ( ngăn cách ứng dụng và DB)
* Dữ liệu từ AV Agent sẽ được gửi về tổng hợp ở Audit Vault Server
* Fire Wall có khả năng theo dõi lưu lượng dữ liệu tới DB, nó có khả năng cảnh báo hoặc chặn những truy vấn SQL dựa trên các polices có sẵn.

### Audit Vault Server

* Bao gồm các tool cần thiết cho quá trình cấu hình AVDF. Nó lưu trữ các file cấu hình của AVFW và thu thập các dữ liệu audit , có thể coi nó như 1 data warehouse nội bộ. Người sử dụng có thể cấu hình và tùy chỉnh báo cáo dựa trên nhưng thông tin có sẵn ở Audit Vault Server
* Sử dụng 1 Oracle Database nhúng để lưu trữ và quản lý dữ liệu. Database này được enable tính năng Database Vault dùng để quản lý truy cập người dùng. Người sử dụng được khuyến cáo không nên quản lý database này mà để tự nó quản lý

Các tính năng chính :

* Thu thập, quản lý dữ liệu audit
* Quản lý AV agent
* Quản lý FW
* Quản lý các chính sach bảo mật của AV&FW
* Quản lý các thông báo và cảnh báo
* Lưu trữ dữ liệu, các phương pháp audit
* Tạo, lưu báo cáo
* Quản lý User sử dụng
* Liên kết với các chương trình thứ 3

Phân loại user:

* Super Administrator:
  + Được phép tạo admin hoặc super admin
  + Cài đăt, cấu hình tham số
* Administrator
  + Chỉ được phép xem dữ liệu

### Audit Vault Agent

* Được cài đặt trên mỗi DB
* Làm nhiệm vụ thu thập audit file của mỗi DB và gửi về cho Audit Vault Server

### Oracle Database FireWall

* Là 1 hệ thống tường lửa có thể bảo vệ tính an toàn cho các database (Oracle, MySQL, Microsoft SQL Server, Sybase Adaptive Server Enterprise (ASE), Sybase SQL Anywhere SQL, and IBM DB2 SQL ) trên nền tảng (Linux, UNIX, and Microsoft Windows)
* Nó ngăn chặn các cuộc tấn công, ghi lại log của các hoạt động, cung cấp các tool tăng cường các tính năng bảo mật của DB hiện có như mã hóa dữ liệu và xác thực người dùng

Các chế độ hoạt động:

* DPE Mode: đưa ra cảnh báo và cho phép/ ngăn chăn các truy vấn SQL đến
* DAM Mode: chỉ cảnh báo
* Proxy: FW có thể hoạt động để điều khiển lưu lượng dữ liệu ( vào, ra ...) như 1 proxy trên mạng.

Nguyên lý hoạt động:

* FW làm việc dựa trên việc phân tích ý nghĩa câu truy vấn mà client gửi tới. Điều này cung cấp 1 khả năng bảo vệ tốt hơn rất nhiều
* Không giới hạn độ dài độ dài của các câu truy vấn cần phải phân tích . Hiển thị 2000 ký tự đầu tiên và áp dụng cho mọi loại truy vấn ( ví dụ như ANSI SQL...)
* FW ko làm ảnh hưởng tới hiệu năng làm việc của hệ thống

Các tính năng chính của Firewall:

* Tạo các chính sách bảo mật ( policy file) đến và đi thông qua firewall
* Firewall sẽ dựa trên các chính sách bảo mật và thông tin của các truy vấn SQL để quyết định các hành động tiếp theo (cho phép, chặn, cảnh báo..)
* Firewall có khả năng tích lũy những kết quả từ trước ( lưu giữ nhưng cấu hình chính sách và kêt quả thực thi đối với những dữ liệu từ trước ) để sinh ra những chứng sách thích hợp.Từ đó,chúng chia những câu lệnh SQL thành các nhóm, mỗi nhóm sẽ áp dụng các chính sách riêng
* FireWall ghi lại log để:
  + Giám sát và tạo báo cáo
  + Tạo mới và cải tiến các chính sách bảo mật
  + Không phụ thuộc vào log của database ( ko ảnh hưởng tới DB)
* Các loại log bao gồm
  + Traffic log: ( user, ip, Os, client program...)
  + Event log ( các sự kiện xảy ra đối với FW)
  + Admin log ( các thao tác của admin đối vs FW)

## Kế hoạch cấu hình cho **Oracle Audit Vault & FireWall**

### Xác định mục tiêu của quá trình cấu hình:

Để xác định được mục tiêu của quá trình cấu hình, cần làm rõ những câu hỏi:

* Mục tiêu nào cẩn đảm bảo an toàn: database, hệ điều hành ( OS) ...
* Để bảo đảm an toàn cho mục tiêu thì cần phải triển khai Audit Vault Agent hoặc Database Firewalls hay cả hai?
* Nếu triển khai Audit Vault Agent thì những loại log nào cần phải thu thập, cấu hình để lấy log như thế nào?
* Nếu triển khai Database Firewalls thì đặt ở đâu, cấu hình để ở chế độ kiểm soát lưu lượng dữ liệu hay proxy
* Có cần thiết cấu hình HA ( high availability)
* Bổ nhiệm ai làm superadmin, admin...

### Các bước thực hiện

Bước 1: Cấu hình Audit Vault Server

Bước 2: Cấu hình Database FireWall

Bước 3: Triển khai Audit Vault Agent

Bước 4: Cấu hình Audit Trail

Bước 5: Kế hoạch cấu hình tùy chọn

Bước 6: Kế hoạch cấu hình HA ( High Availability )

Bước 7: Kế hoạch quản lý user và các quyền hạn truy cập

## Nguyên tắc bảo mật cơ bản

### Cài đặt an toàn

Audit Vault Server đã được cài đặt an toàn theo mặc định. Nếu muốn thay đổi các tham số mặc định thì phải cẩn thận vì nó có thể làm giảm độ an toàn đi.

Tham khảo tài liệu cài đặt để biết thêm chi tiết.

### Bảo vệ dữ liệu

Bảo vệ dữ liệu theo những cách sau:

* Account Names and Passwords: Đặt password cho Audit Vault Server console UI, root, support, và sys accounts một cách cẩn thận và giữ cho chúng an toàn.
* Administrator Accounts: Không chia sẻ Oracle AVDF Administrator accounts.
* Strong Password Policies: Sử dụng chính sách password tốt để user bắt buộc phải sử dụng 1 password mạnh
* Installed Accounts: Sử dụng account Oracle để install Oracle AVDF
* Secure Archiving: đảm bảo đường truyền và các địa điểm lưu trữ được bảo đảm an toàn
* Remote Access: Oracle AVDF cho phép được truy cập từ xa. Có thể cấp quyền truy cập từ xa đến giao diện web để điều khiển console, shell (ssh), and SNMP:
  + Chỉ cấp quyền truy cập khi cần thiết.
  + Hạn chế truy cập vào địa chỉ IP
  + Cấp quyền truy cập vào termial ( shell) khi thực thiên patch update.

### Các khuyến nghị để bảo vệ an toàn chung

Oracle đề nghị tuân theo các khuyến nghị sau:

* Nếu sử dụng tường lửa để ngăn chặn các truy cập không mong muốn vào Database thì phải đảm bảo rằng tất cả dữ liệu từ client có thể tới được DB thông qua FW và ngược lại. Bao gồm cả các yêu cầu và phản hồi
* Sử dụng các biện pháp an ninh thích hợp để kiểm soát quyền truy cập vào máy tính có chứa thiết bị AV Server và FW.
* Đảm bảo rằng mật khẩu phù hợp( tuân theo đúng chính sách đề ra)
* Phân chia nhiệm vụ giữa admin và auditor 1 cách rõ ràng
* Chỉ định rõ những user tương ứng với role admin, super admin,auditor, super auditor.

### Bảo mật mạng - Thực hiện mã hóa mạng

* Khi triển khái FW giữa tầng ứng dụng và tầng Database: FW có thể giải mã được các lượng truy cập đến và đi từ một Database Oracle. Tuy nhiên đối với những database không phải Oracle thì FW không thể thực hiện được
* FW không thể nắm bắt được các các truy vấn được thực hiện ngay tại server hay nhưng truy vấn gọi thực hiện những procedures được lưu trữ tại stored procedures trong server... Nên sử dụng tính năng audit để nắm bắt được những vấn đề này
* Các giao thức non-SQL được FW hỗ trợ:
  + Oracle Database: Oracle TTC/Net
  + Non-Oracle Database: Tabular Data Stream (TDS)
  + Không hỗ trợ IPv6: FW sẽ block mọi kết nối từ IPv6
  + Không hỗ trợ: non-TCP

### Bảo đảm an toàn cho các cấu hình đặc biệt

* Khi sử dụng share server: nên chỉ rõ các port đượ sử dụng và cấu hình cho FW có thể theo dõi các cổng đó. Cấu hình trong file init.ora
  + Ví dụ:

dispatchers="(PROTOCOL=tcp)(PORT=nnnn)"

* Khi sử dụng share listener giữa nhiều DB: FW không thể phân biệt lưu lượng truy cập trực tiếp đến từng cơ sở dữ liệu.
* Lưu ý khi sử dụng Client-side context

# Cấu hình Audit Vault Server

## Đăng nhập

* Sau khi cài đặt xong, user có thể đăng nhập vào AVServer
* Sử dụng trình duyệt internet và truy cập địa chỉ:

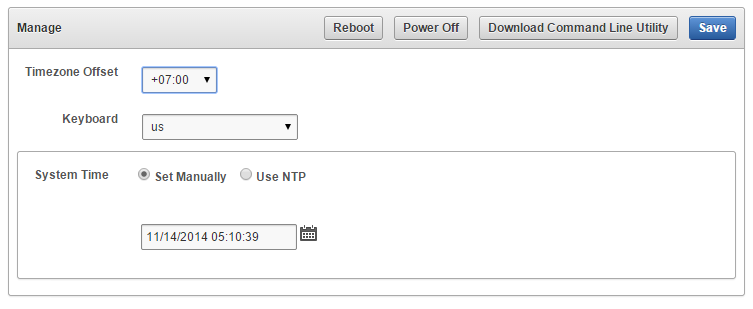
[*https://ip\_address*](https://ip_address)

## Cấu hình những tham số cần thiết

### Cấu hình thời gian

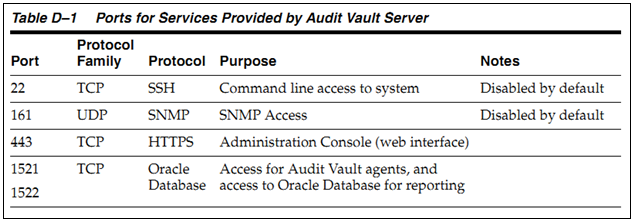
Cấu hình:

* Đăng nhập vào AVServer bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **System** menu, chọn **Manage**.
* Thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi
  + **Timezone Offset** chọn thời gian cho địa điểm 1 cách chính xác ( VietNam: UTC + 7)
  + **Keyboard** : định dạng keyboard ( US)
  + **System Time**,
    - Nếu chọn **Manually Set** ( lấy thời gian theo thời gian của máy local) hoặc tùy chỉnh theo ý muốn
    - Nếu chọn **NTP Synchronization** ( lấy thời gian theo server trên mạng) : điền **địa chỉ hoặc tên server** phù hợp và **apply**. Và lựa chọn: **Enable NTP Time Synchronization**



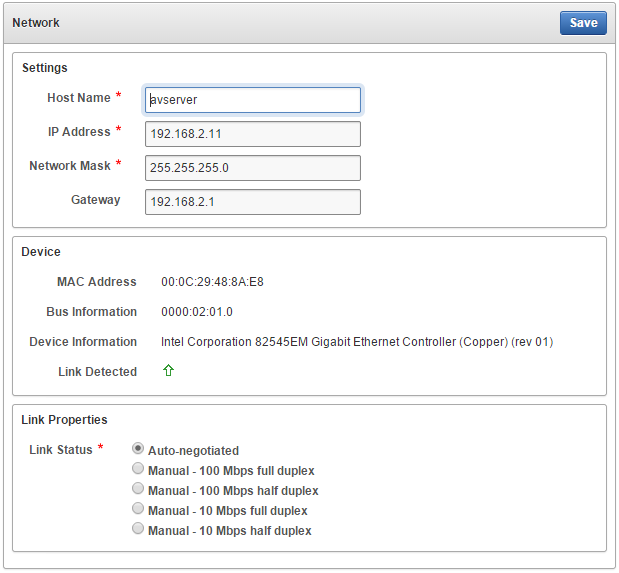
### Cấu hình mạng

Các cổng mạng được sử dụng theo mặc định



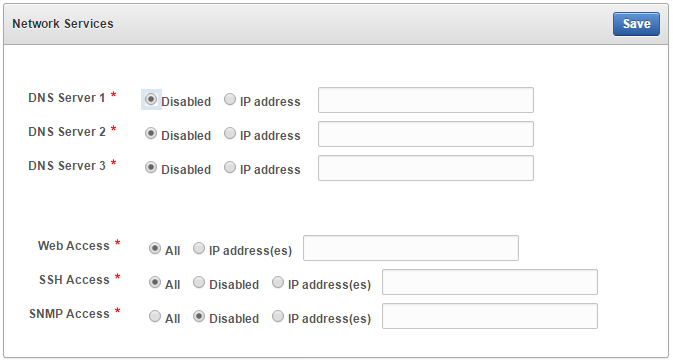
Cấu hình thông tin mạng

* Đăng nhập vào AVServer bằng user **super admin** hoặc **admin**
* Truy cập vào mục **Setting**
* Trong **System** menu, chọn **Network**
* Thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi
  + **Địa chỉ IP** ( yêu cầu reboot và cập nhât ở FireWall )
  + **Network Mask** ( chỉ super admin mới có thể thay đổi)
  + **Gateway** ( chỉ super admin mới có thể thay đổi)
  + **Host Name** ( yêu cầu reboot)
  + **Link properties** ( đề nghị giữ nguyên mặc đinh)



### Cấu hình các dịch vụ liên quan

* Đăng nhập vào AVServer bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **System** menu, chọn **Services**
* Thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi
  + **DNS Servers 1, 2, 3: địa chỉ máy chủ phân giải tên miền**
  + **Web Access:** Cấu hình để hạn chế những máy có thể truy cập
  + **SSH Access:** cho phép SSH tới AVServer
  + **SNMP Access:** cho phép SNMP tới AVServer

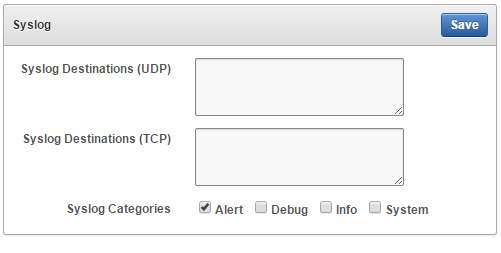


### Cấu hình địa chỉ nhận log từ AVServer

Có thể cấu hình địa chỉ để AVServer gửi log ( Alert,Debug, Info, System..) địa chỉ xác định để thuận tiện cho công việc quản lý

Cấu hình:

* Đăng nhập vào hệ thống bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **System** menu, chọn **Connectors,** cuộn xuống mục **Syslog**



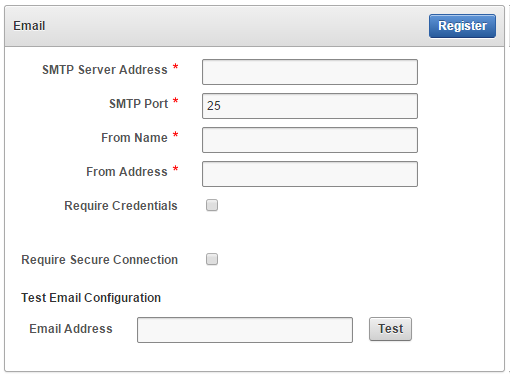
* Thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi
  + **Syslog Destinations (UDP):** điền địa chỉ IP của máy đích được gửi log bằng giao thức UDP
  + **Syslog Destinations (TCP):** điền địa chỉ IP của máy đích được gửi log bằng giao thức UDP
  + **Syslog Categories**: Chọn những log cần gửi:
    - **Alert**: Cảnh báo dựa trên những alert log ở trên AVDF Server
    - **Debug**: Thổng tin sửa lỗi
    - **Info**: Thông tin thay đổi các thuộc tính của AVServer
    - **System**: Thông tin System được tạo bới Oracle AVDF hoặc các software khác

## Cấu hình dịch vụ gửi mail ( SMTP)

Có thể cấu hình AV Server để gửi mail khi có những cảnh báo được tạo ra. Email thông báo sẽ được gửi bằng định dạng text tới các thiết bị đầu cuối cần thiết

Cấu hình:

* Đăng nhập vào AVServer bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **System** menu, chọn **Connectors,** xem mục **Email**



* Điền những thông tin cần thiết và chọn **Register** để đăng kí
  + **SMTP Server Address:** điền địa chỉ IP của SMTP server
  + **SMTP Port:** điền cổng của SMTP server
  + **From Username**: điền user gửi email
  + Chọn mục **Require Credentials** và điền thông tin của **Username, Password,** và **Re-enter Password.**
  + Chọn **Require Secure Connection** để đảm bảo phương thức xác thực

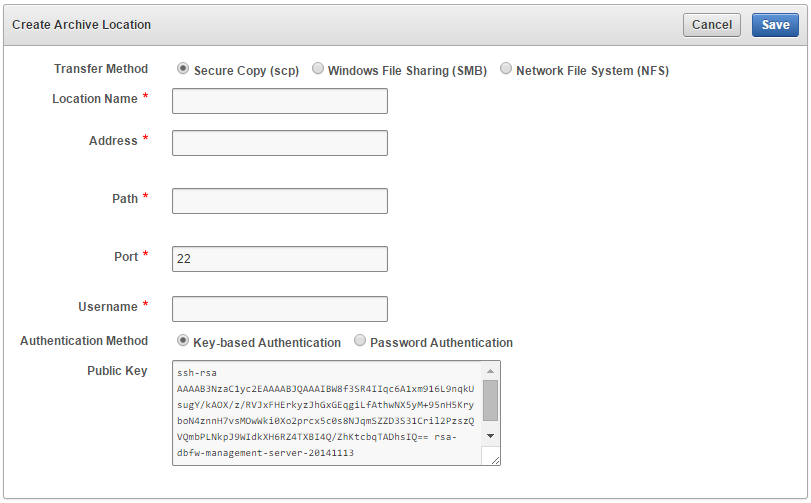
## Cấu hình địa chỉ Archive và các chính sách (Retention Policies )

Có thể cấu hình archive cho các file dữ liệu để thuận tiện cho quá trình sử dụng và quản lý. Công việc cấu hình archive có thể bằng tay hoặc theo chính sách, lịch...

Khi các file dữ liệu được archive thì nội dung của nó không được luu trữ trên AVServer nữa ( chỉ còn thông tin file). Nhưng nếu cần thiết thì có thể khôi phục lại để làm báo cáo ( mục XII)

### Cấu hình địa chỉ Archive

* Đăng nhập vào AVServer bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **Archiving** menu, chọn **Manage Archive Locations**
* Chọn **Create**



* Thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi:
  + **Transfer Method**: Phương thức sử dụng để chuyển dữ liệu từ AVServer
    - **Secure Copy (scp):** Chọn nếu đích là 1 máy Linux
    - **Windows File Sharing (SMB)**: Chọn nếu đích là 1 máy Window ne
    - **Network File Storage (NFS): (**AVDF 12.1.2 trở lên **)** Chọn nếu sử dụng chia sẻ file hoặc NAS
  + **Location Name**: Tên của địa chỉ đích
  + **Remote Filesystem** ( khi chọn NFS): chọn file system
  + **Address**: Địa chỉ IP của đích.
  + **Export Directory**: (NFS) : điền thư mục export . Ví dụ: /export\_dir.
  + **Path**: Địa chỉ thư mục để lưu trữ archive
  + **Port**: Cổng để thực hiện copy file ( SCP-22, SMB: 445)
  + **Username**: tên user đăng nhập trên máy đích
  + **Password** và **Confirm Password**: password tương ứng với user

### Tạo mới và xóa chính sách archive

Tạo mới chính sách archive

* Đăng nhập vào AVServer bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **Archiving** menu, chọn **Manage Policies**
* Chọn **Create**
* Thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi:
  + **Name**: Tên của chính sách
  + **Months Online:** Số tháng dữ liệu được dữ lại trước khi archive.

Mặc định là 1 (tháng)

* + **Months Archived:** Số tháng dữ liệu có thể được khôi phục sau khi archive**.** Mặc định là 6 (tháng)

Xóa chính sách archive

* Đăng nhập vào hệ thống bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **Archiving** menu, chọn **Manage Policies**
* Tìm chính sách muốn xóa và **Delete**

## Đăng kí Database FireWall với Audit Vault Server

Nếu cài đặt cả AVServer và Firewall thì cần phải đăng kí Firewall với AVServer để cả hai thành phần có thể giao tiếp với nhau

Để đăng kí FireWall với AVServer thì làm theo những bước sau:

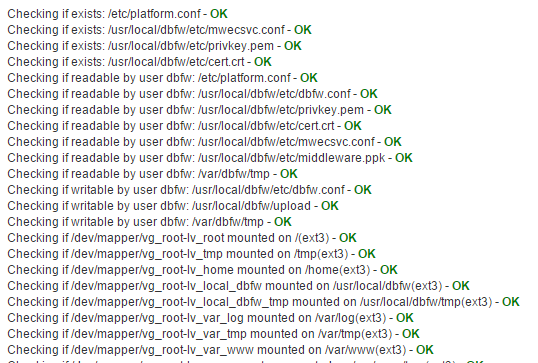
* Cấu hình FireWall (mục III)
* Cung cấp chứng chỉ và địa chỉ IP của AVServer cho FireWall ( mục III )
* Đăng nhập vào hệ thống bằng user **super admin**
* Truy cập vào mục **FireWall**
* **FireWall** được đăng kí sẽ hiện thị
* Chọn **Register**
* Điền địa chỉ **Database Firewall,** và **IP Address**
* Chọn **Save**

## Kiểm thử hệ thống Audit Vault Server

Nên kiểm thử hệ thống hàng ngày để khắc phục các sự cố ếu

Thực hiện:

* Đăng nhập vào AVServer bằng user **super admin**
* Truy cập vào mục **Setting**
* Trong **System** menu, chọn **Status**
* Chọn **Test Diagnostics:** Đảm bảo mọi thứ **OK**
* Chọn mục **Home** để xem trạng thái của các **Database Firewalls** và **Hosts**



# Cấu hình Database FireWall

## Đăng nhập

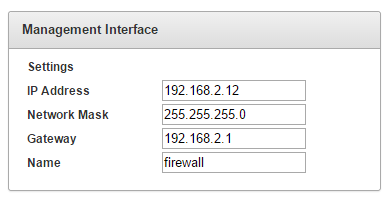
* Sau khi cài đặt xong, user có thể đăng nhập vào FireWall
* Sử dụng trình duyệt internet và truy cập địa chỉ:

[*https://ip\_address*](https://ip_address)

## Cấu hình những tham số cần thiết

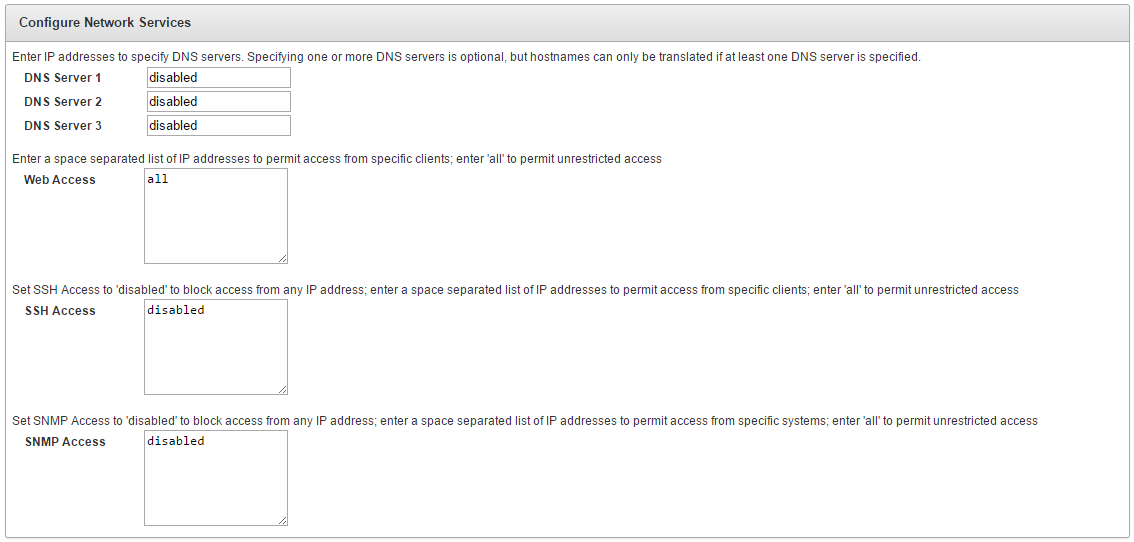
### Cấu hình mạng

* Đăng nhập vào FireWall bằng user **admin**
* Trong **System** menu, chọn **Network**
* Chọn nút **Change** ( ở cuối trang) để thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi:
  + **Địa chỉ IP** ( yêu cầu reboot và cập nhât ở FireWall )
  + **Network Mask** ( chỉ super admin mới có thể thay đổi)
  + **Gateway** ( chỉ super admin mới có thể thay đổi)
  + **Name** ( yêu cầu reboot)
  + **Link properties** ( đề nghị giữ nguyên mặc đinh)



### Cấu hình các dịch vụ liên quan

* Đăng nhập vào FireWall bằng user **admin**
* Trong **System** menu, chọn **Services**
* Chọn nút **Change** để thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi
  + **DNS Servers 1, 2, 3: địa chỉ máy chủ phân giải tên miền**
  + **Web Access:** Cấu hình để hạn chế những máy có thể truy cập
  + **SSH Access:** cho phép SSH tới AVServer
  + **SNMP Access:** cho phép SNMP tới AVServer



### Cấu hình thời gian

* Đăng nhập vào FireWall bằng user **admin**
* Trong **System** menu, chọn **Date and Time**.
* Chọn nút **Change** để thay đổi những thông tin cần thiết và chọn **Save** để lưu những thay đổi
  + **System Time:** cài đặt thời gian cho hệ thống
  + **Time Synchronization** Nếu chọn **NTP Synchronization** ( lấy thời gian theo server trên mạng) : điền **địa chỉ hoặc tên server** phù hợp và **apply**. Và lựa chọn: **Enable NTP Time Synchronization**

## Đăng kí Database FireWall với Audit Vault Server

Thao tác với AVServer

* Đăng nhập vào **AVServer** bằng user **admin**
* Chọn tab **Setting,** trong **Security** menu, chọn **Certificate**.
* Copy **certificate** của AVServer

Thao tác với FireWall

* Đăng nhập vào **FireWall** bằng user **admin**
* Trong **System** menu, chọn **Audit Vault Server**.
* Điền **IP Address** của AVServer và paste chứng chỉ vào
* Chọn **Apply.**

## Vị trị của FireWall trong mạng

Cấu hình FireWall trong mạng, nằm giữa ứng dụng và Database nhằm kiểm soát luồng thông tin giữa chúng

Yêu cầu: 3 card mạng

* 1 card mạng dùng để quản trị (N1)
* 2 card mạng dùng để kết nối với database và ứng dụng (N2-N3) ( nên thuộc 2 mạng khác nhau)

Sau khi install thì mặc định FireWall đã tự động cấu hình Traffic Sources cho 2 card mạng (N2-N3), tuy nhiên có thể tùy chỉnh:

* Đăng nhập vào **FireWall** bằng user **admin**
* Trong **System** menu, chọn **Network**.
* Chọn nút Change để thay đổi các thông số và **Save** để lưu:
  + **Remove:** xóa cấu hình
  + **IP address:** địa chỉ IP
  + **Network Mask:** mặt nạ mạng
  + **Unallocated Network Devices:** thêm card mạng khác vào
  + Chọn **Bridge Enabled:** để các card mạng có thể nối được với nhau

## Kiểm thử hệ thống FireWall

Nên kiểm thử hệ thống hàng ngày để khắc phục các sự cố ếu

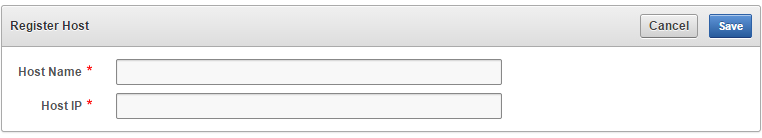
Thực hiện:

* Đăng nhập vào FireWall bằng user **admin**
* Trong **System** menu, chọn **Status**
  + **Show Report** : Xem các thông tin về diagnostic status
  + **Download Diagnostics:** tải tất cả các file **diagnostics files**

# Đăng kí địa chỉ đích với AVServer và cài đặt agent

## Đăng kí địa chỉ đích với AVServer

* Đăng nhập vào **AVServer** bằng user **admin**
* Chọn tab **Host**
* Chọn nút **Register**
* Điền **Host Name** và **Host IP**
* Chọn **Save** để lưu những thay đổi



## Cài đặt Agent lên các host

Thao tác với AVServer

* Đăng nhập vào **AVServer** bằng user **admin**
* Chọn tab **Host**
* Trong menu Host chọn **Agent**
* Download file **agent.jar** về và cài đặt trên các máy đích



Thao tác với máy đích

* Đăng nhập vào user oracle trên máy đích
* Tại thư mục chứa file agent.jar, khởi động agent:

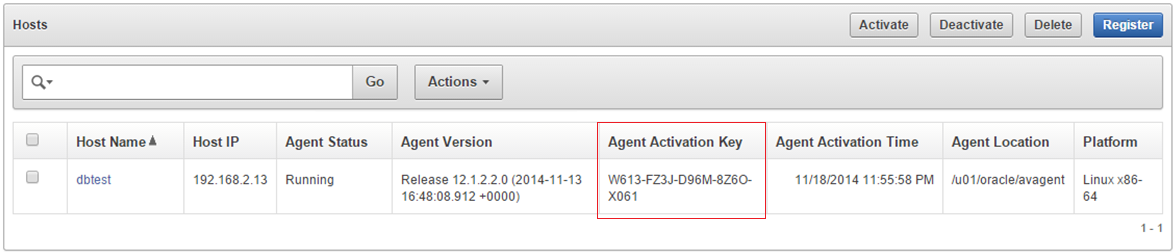
$ java -jar agent.jar -d *Agent\_Home*

* Kích hoạt agent để đăng kí tới AVServer

$ agentctl activate

Thao tác với AVServer

* Sau khi agent đăng kí tới AVServer, có 1 key được tự sinh ra để xác thực giữa 2 bên ( Agent Activation Key)
* Copy key này



Thao tác với máy đích

* Khởi động agent :

$ agentctl start –k

Enter Activation Key:

# Cấu hình Secured Targets, Audit Trails và Enforcement Points

## Đăng kí va tạo các nhóm Secured Targets với AVServer

## Cấu hình Secured Targets để thu thập dữ liệu Audit

## Cấu hình và quản lý dữ liệ Audit thu thâp được

## Cấu hình Enforcement Points

## Cấu hình và sử dụng Database Interrogation