TÀI LIỆU TRIỂN KHAI MỘT SỐ TÍNH NĂNG PAM-MINIORANGE

**Tên chủ đề: MiniOrange – Privileged Access Management (PAM)**



1. **THÔNG TIN CHUNG:**

|  |  |  |
| --- | --- | --- |
| STT | Họ và tên | Email |
| 1 | Nguyễn Hoài Phương | Phuongnguyen27102003@gmail.com |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| STT | Nội dung | Trang |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |

BÁO CÁO CHI TIẾT

# QUẢN LÝ QUYỀN TRUY CẬP CHO NGƯỜI DÙNG QUẢN TRỊ (ADMIN USERS) TRÊN WINDOWS VÀ LINUX

Vào dashboard admin 🡪 All Assets 🡪 Add Asset

Ảnh có chứa văn bản, ảnh chụp màn hình, số, phần mềm

Mô tả được tạo tự động

**2**

**1**

Sau đó pop up điền thông tin asset hiện ra. Tiến hành điền các thông tin và thông tin về System Users có thể bỏ trống.

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Sau đó chuyển sang tab System Users 🡪 Add system user

Ảnh có chứa ảnh chụp màn hình, văn bản, hàng, Phông chữ

Mô tả được tạo tự động

**2**

**1**

Điền các thông tin về tài khoản Administrator của Window sau đó gán System user này cho Asset Window vừa tạo ở bước trên, ví dụ như sau:

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Chuyển về tab asset và thêm thông tin System User tại Edit như hình dưới:

Ảnh có chứa ảnh chụp màn hình, văn bản

Mô tả được tạo tự động

**2**

**1**

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Tiếp theo để gán một tài khoản bất kì trong miniorange để cho phép user này có thể truy cập vào máy Window ta thực hiện các bước sau:

Asset 🡪 All asset 🡪 Allocate 🡪 Tick chọn user minorange mà ta muốn cấp quyền truy cập.

Ảnh có chứa ảnh chụp màn hình, văn bản

Mô tả được tạo tự động

**2**

**1**

Ảnh có chứa ảnh chụp màn hình, văn bản, hàng, số

Mô tả được tạo tự động

**3**

Tại đây cho phép tùy chọn các phương thức cấp quyền cho user. Trong ví dụ, chọn LIFE LONG ALLOCATION (Cho phép truy cập không giới hạn).

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

**5**

**4**

Sau khi setting thành công, tiến hành test thử bằng tài khoản miniorange user (WindowPC):

Ảnh có chứa ảnh chụp màn hình, văn bản, hàng

Mô tả được tạo tự động

Kết nối thành công

Ảnh có chứa phần mềm, Phần mềm đa phương tiện, Phần mềm đồ họa, Biểu tượng máy tính

Mô tả được tạo tự động

Đối với hệ điều hành Ubuntu tương tự.

Tạo system user

Ảnh có chứa văn bản, ảnh chụp màn hình, số, phần mềm

Mô tả được tạo tự động

Tạo Asset chạy Ubuntu OS và gắn system user cho asset này

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Sau đó allocate cho user miniorange

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, số

Mô tả được tạo tự động

Kiểm tra lại có user miniorange để xem có được cấp quyền truy cập vào máy Ubuntu hay chưa

Ảnh có chứa văn bản, số, hàng, Phông chữ

Mô tả được tạo tự động

Click Access để kiểm tra kết nối. Như hình dưới có nghĩa là kết nối thành công.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

# QUẢN LÝ QUYỀN TRUY CẬP TÀI KHOẢN ADMIN MYSQL BẰNG PAM

Trên máy Ubuntu cài đặt thêm dịch vụ MySQL. Có thể xem hướng dẫn tại [Cài đặt và cấu hình MySQL](https://quantrimang.com/cong-nghe/cai-mysql-tren-ubuntu-177449).

Sau đó đăng nhập tài khoản root bằng câu lệnh mysql -u root -p

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Sau đó tạo user

CREATE USER 'DB\_Root'@'192.168.124.20' IDENTIFIED BY 'phuong2003';

Với 192.168.124.20 là IP Của **PAM Server.**

Kiểm tra thông tin user vừa tạo

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Tiếp theo thực hiện cấp quyền cho user

GRANT ALL PRIVILEGES ON test\_miniorange.\* TO 'DB\_Root'@'192.168.124.20';

Lưu ý: Truy cập vào file và tìm dòng bind-address. Đảm bảo rằng nó không chỉ định địa chỉ 127.0.0.1. Thay vào đó, bạn có thể đặt nó thành 0.0.0.0 để cho phép kết nối từ mọi địa chỉ IP:

sudo nano /etc/mysql/mysql.conf.d/mysqld.cnf

và chỉnh sửa bind-access

bind-address = 0.0.0.0

Để kiểm tra kết nối từ PAM server 🡪 MySQL server ta chuyển sang máy PAM server và thực hiện telnet để kiểm tra bằng câu lệnh sau:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Sau khi thiết lập thành công, tiến hành cấu hình tính năng quản lý tài khoản quản trị MySQL

Ảnh có chứa ảnh chụp màn hình, văn bản, số, Phông chữ

Mô tả được tạo tự động

**2**

**1**

Cài đặt thông tin MySQL để kết nối và bỏ trống giá trị System Users

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Tiếp theo ta sẽ tạo thêm tài khoản quản trị MySQL và gán nó cho App

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Sau đó allocate

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Phông chữ

Mô tả được tạo tự động

**2**

**1**

Ảnh có chứa ảnh chụp màn hình, văn bản, hàng, số

Mô tả được tạo tự động

**3**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

**5**

**4**

Đăng nhập bằng tài khoản UbuntuClient để test

Ảnh có chứa văn bản, trang phục, ảnh chụp màn hình

Mô tả được tạo tự động

Ảnh có chứa ảnh chụp màn hình, văn bản, hàng

Mô tả được tạo tự động

**1**

**2**

Kiểm tra thấy truy cập thành công

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

Admin site có thể thấy được toàn bộ chi tiết thông tin về câu truy vấn tại audit mode

Ảnh có chứa văn bản, phần mềm, số, Biểu tượng máy tính

Mô tả được tạo tự động

# QUẢN LÝ QUYỀN TRUY CẬP TÀI KHOẢN WEB APP BẰNG PAM

Demo triển khai với github:

Ảnh có chứa văn bản, số, Phông chữ, hàng

Mô tả được tạo tự động

**2**

**1**

Cài đặt như hình bên dưới

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Để truy cập được Web app Remote Access

Cần cài 1 máy Windows Server nâng cấp lên Domain Controller sau đó cài đặt dịch vụ RDS trên máy windows để cài đặt XecureAgentApp 1.0.

Chú ý:

Tại máy PAM cần chỉnh sửa lại thông tin như trong khung đỏ

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Tại máy Windows Server cần cài đặt add host entry tại path (**C:\Windows\System32\drivers\etc\hosts**) hoặc cài đặt dịch vụ DNS để phân giải tên miền.

# TẠO CHÍNH SÁCH ĐẶT MẬT KHẨU CHO USER (PASSWORD POLICIES)

Ảnh có chứa văn bản, ảnh chụp màn hình, số, phần mềm

Mô tả được tạo tự động

Kiểm tra bằng cách tạo 1 user mới thì có thể thấy chính sách đã được áp dụng

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

# XÁC THỰC 2FA CHO USER VÀ USERADMIN

Đối với user: Đăng nhập vào tài khoản và chuyển sang tab **Two-Factor** 🡪 **Configure**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Sau đó pop-up hiện ra yêu cầu nhập hoặc quét mã QR (yêu cầu tải app **Google Authenticator App** về điện thoại)

Ảnh có chứa văn bản, ảnh chụp màn hình, mẫu

Mô tả được tạo tự động

Test tính năng:

Sau khi đăng nhập tài khoản mật khẩu thành công sẽ được chuyển sang màn hình nhập mã OTP.

Ảnh có chứa trang phục, văn bản, người, ảnh chụp màn hình

Mô tả được tạo tự động

Để lấy mã vào app **Google Authenticator App** trên điện thoạivà kiểm tra mã OTP đã được gửi trong đó. Ví dụ như sau

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Sau đó nhập 6 số mã OTP này và kiểm tra đăng nhập thành công hay chưa

Ảnh có chứa ảnh chụp màn hình, văn bản, phần mềm, hàng

Mô tả được tạo tự động

Tương tự đối với tài khoản Admin

# AUTHENTICATION LDAP/SSO

[Cách cài đặt LDAP Server trên Ubuntu (viblo.asia)](https://viblo.asia/p/cach-cai-dat-ldap-server-tren-ubuntu-EoDGQoqxkbV)

[Cách cài đặt LDAP Server trên Ubuntu (P2) (viblo.asia)](https://viblo.asia/p/cach-cai-dat-ldap-server-tren-ubuntu-p2-Ljy5VdW3Zra)

[php - Unrecognized error number: 8192: trim(): Passing null to parameter #1 ($string) of type string is deprecated - Stack Overflow](https://stackoverflow.com/questions/74384236/unrecognized-error-number-8192-trim-passing-null-to-parameter-1-string)

# THEO DÕI VÀ GHI NHẬN HOẠT ĐỘNG

Tại góc phải Admin user chọn Switch to Audit Dashboard để chuyển sang mode thống kê

Ảnh có chứa văn bản, Phông chữ, số, ảnh chụp màn hình

Mô tả được tạo tự động

Tại dashboard mặc định, admin có thể xem được số lượng user, số lần đăng nhập thành công, thất bại,… và tài nguyên user đó truy cập là gì vào thời điểm nào.

Ảnh có chứa văn bản, số, Phông chữ, phần mềm

Mô tả được tạo tự động

Các app được truy cập nhiều bởi user miniorange

Ảnh có chứa văn bản, hàng, Phông chữ, số

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Số lượng commands mà user thực hiện khi truy cập vào tài nguyên.

Và số lần đăng nhập thành công/ thất bại vào 1 resource

# QUẢN LÝ PHIÊN ĐĂNG NHẬP

Tại đây admin có thể xem các phiên đang hoạt động ở real time hoặc các các session trong quá khứ nhờ vào recorded session.

Ảnh có chứa ảnh chụp màn hình, văn bản, hàng, Phông chữ

Mô tả được tạo tự động

Trong tab real-time Sessions cho phép admin dừng phiên hoạt động của user đó bất kì lúc nào

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng

Mô tả được tạo tự động

Trong tab recorded Sessions cho phép xem lại toàn bộ quá trình hoạt động của user thực hiện tại thời điểm bắt đầu đăng nhập.

# TẠO REPORT VÀ TICKET

Report cho phép admin xuất các file báo cáo liên quan đến hoạt động của user và các hoạt động chỉnh sửa của admin. Các loại report bao gồm:

|  |  |
| --- | --- |
| Tên Báo Cáo | Mô Tả |
| App Access Report | Báo cáo chi tiết về quyền truy cập vào các ứng dụng, bao gồm người dùng, thời gian và hành động. |
| App Allocation Report | Thông tin về việc phân bổ ứng dụng cho người dùng và nhóm, giúp theo dõi việc sử dụng ứng dụng. |
| Assets Report | Thống kê về các tài sản trong hệ thống, bao gồm địa điểm và tình trạng sử dụng. |
| Asset Access Report | Ghi nhận quyền truy cập vào các tài sản, bao gồm người dùng và thời gian truy cập. |
| Asset Allocation Report | Thông tin về cách các tài sản được phân bổ cho người dùng hoặc nhóm. |
| Web Apps Report | Thống kê về các ứng dụng web đang được sử dụng, bao gồm thông tin về người dùng và quyền. |
| Web App Access Report | Chi tiết về quyền truy cập vào các ứng dụng web, bao gồm thời gian và hành động của người dùng. |
| Web App Allocation Report | Thông tin về việc phân bổ ứng dụng web cho người dùng, giúp quản lý hiệu quả hơn. |
| User Login Report | Ghi nhận tất cả các lần đăng nhập của người dùng, bao gồm thời gian và địa điểm. |
| Tickets Report | Thống kê về các yêu cầu hỗ trợ (tickets), bao gồm trạng thái và thời gian xử lý. |

Ticket cho phép user xin phép cấp quyền truy cập/gia hạn truy cập vào 1 asset/app/webapp mà admin đã gắn cho user này trước đó . Dưới đây là cách thực hiện:

Tại giao diện user WindowPC 🡪 My Tickets 🡪 Create Ticket

Ảnh có chứa ảnh chụp màn hình, văn bản, hàng, số

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Sau khi tạo thành công ta có thể thấy trạng thái của ticket vừa tạo



Tại giao diện của Admin có thể thấy được thông báo của ticket này từ user WindowPC

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Click vào Accept để đồng ý cấp quyền hoặc từ chối bằng Reject

Ảnh có chứa văn bản, số, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

Một pop-up hiện ra yêu cầu chọn vào tài khoản System User. Sau khi chọn xong thì click Confirm

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Check lại trạng thái của ticket lại phía user WindowPC ta có thể thấy ticket này đã được chấp nhận  
