INTRODUCTION

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol, operating on port 1812 that provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service. FreeRADIUS is an open source project and as such depends on contributions from its users.

Note:- It is recommended to disable the SELinux as it restricts the radiusd.service (explained later) from starting.

```
# setenforce 0
```

This command disables the SELinux.

```
# getenforce
> Disable
```

This will tell the current status of SELinux.

PREREQUISITES

Installation of httpd:

```
# yum update install          /for updating all the existing libraries
# yum groupinstall “Development Tools” -y
# yum -y install httpd httpd-devel
```

All the httpd related required libraries are installed and now we’ll start and enable the httpd server.

```
# systemctl enable httpd
# systemctl start httpd
```

Checking for the current status can be done by the command #systemctl status httpd
This will show *Active (Running)* if the server is running properly.

Installing and Configuring MariaDB:

```
# vim /etc/yum.repos.d/MariaDB.repo
```

A file will be opened and the following contents are needed to be added to the file.

```
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.1/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

Update the system and install MariaDB to configure Database server.

```
# yum -y update
# yum install -y mariadb-server mariadb
```

Start and enable MariaDB to run on boot and then check the status for it to be running.

```
# systemctl start mariadb
# systemctl enable mariadb
# systemctl status mariadb
```

Now we'll configure the initial MariaDB settings to secure it. Set the root password. For security purposes, consider removing anonymous users and disallowing remote root login. Press y for the questions popped during the configuration after using command.

```
# mysql_secure_installation
```

Allow only local connection to mysql server. This is a security mechanism.

```
# vim /etc/my.cnf      /Enter the following in the opened file
[mysqld]
bind-address=127.0.0.1                  /the IP of NAS
```

Configure Database for freeRADIUS:

```
# mysql -u root -p
MariaDB [(none)]> CREATE DATABASE radius;
MariaDB [(none)]> show databases;
MariaDB [(none)]> use radius;
MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY
"radiuspassword";
/////where the first radius is the database name, second radius (radius@localhost) is the
username and radiuspassword is the password for the database.
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> \q
> Bye
```

Installing php:

Check the php version to confirm if it is php 7 or php 5 using the command # php -v

If php is not present try installing it using the following commands:

```
# cd ~
# curl 'https://setup.ius.io/' -o setup-ius.sh
# sudo bash setup-ius.sh
```

If this command shows an error like "Peer Certificate has expired", check for the current date (using # date) and if the date is wrong, try syncing it with ntp server using this given link. Once the date is synced, this error won't appear.

```
# sudo yum remove php-cli mod_php php-common
# sudo yum -y install mod_php70u php70u-cli php70u-mysqlnd php70u-devel php70u-gd
php70u-mcrypt php70u-mbstring php70u-xml php70u-pear
```

This is the installation for php 7. If it fails, we'll try to install php 5 using the following command.

```
# yum -y install php-pear php-devel php-mysql php-common php-gd php-mbstring
php-mcrypt php php-xml
```

For redhat 8 the command for php 7 installation would be:

```
#yum install php php-mysqlnd php-pdo php-gd php-mbstring

# sudo apachectl restart
```

INSTALLING FREERADIUS

```
# yum -y install freeradius freeradius-utils freeradius-mysql
```

This will install freeradius 3 as well as the required add-ons. Then we'll start and enable freeradius to start at boot up and check the status of it.

```
# systemctl start radiusd.service
# systemctl enable radiusd.service
# systemctl status radiusd.service
```

Now we'll configure firewall to allow radius and httpd packets in and out. For this, we'll start and enable the firewall and then check the status for it to be running.

```
# systemctl enable firewalld
# systemctl start firewalld
# systemctl status firewalld
```

Confirm that firewall is running.

```
#firewall-cmd --state
> running
```

Add permanent rules to default zone to allow http, https and radius services.

```
# firewall-cmd --get-services | egrep 'http|https|radius' # firewall-cmd
--add-service={http,https,radius} --permanent
> success
```

Reload firewall for changes to take effect.

```
#  firewall-cmd --reload
```

Confirm that services were successfully added to the default zone.

```
#  firewall-cmd --get-default-zone
> public
# firewall-cmd --list-services --zone=public
> dhcpv6-client http https radius ssh
```

We can see the three services present hence we're good to proceed. Test radius server by running it in debug mode with option **-X.**

```
# ss -tunlp | grep radiusd
```

If it's running, debug mode will fail to bind to ports, you may have to kill radius server daemon first.

```
# pkill radius
```

Then start radius server in debugging mode to see if it runs successfully:

```
# radiusd -X                    /-X refers to the debug mode.
> ……...Ready to process requests
```

CONFIGURING FREERADIUS

To configure the RADIUS first we need to populate the MariaDB database using the schema that is already present in the mysql folder of freeradius. So, we'll import the Radius database scheme to populate radius database.

```
#mysql -u root -p radius < /etc/raddb/mods-config/sql/main/mysql/schema.sql
```

Now, for configuring it further, we need to create a soft-link for the SQL in the /etc/raddb/mods-enabled/. Always the files are in the mods-available where all the essential files are present and the files that are required are called from the mods-enabled therefore we have to create a soft so that all the changes done in the file of mods-available are then reflected in the mods-enabled.

```
# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/
```

Configure SQL module /raddb/mods-available/sql and change the database connection parameters to suite your environment:

```
# vim /etc/raddb/mods-available/sql
```

The sql{} section should look similar to this:

```
sql {
        driver = "rlm_sql_mysql"
        dialect = "mysql"

        # Connection info:
        server = "localhost"_________________
        port = 3306
        login = "radius"
        password = "radiuspassword"
        radius_db = "radius"
}

# Set to 'yes' to read radius clients from the database ('nas' table)
# Clients will ONLY be read on server startup.
read_clients = yes
```

```
# Table to keep radius client info
client_table = “nas”
```

Then change group right of /etc/raddb/mods-enabled/sql to radiusd:

```
# chgrp -h radiusd /etc/raddb/mods-enabled/sql
```