Applies to **SUSE Linux Enterprise Server 15 SP2**

8 Setting Up a FreeRADIUS Server

The RADIUS (Remote Authentication Dial-In User Service) protocol has long been a standard service for manage network access. It performs authentication, authorization, and accounting (AAA) protocol for very large businesses such as Internet service providers and cellular network providers, and is also popular for small networks. It authenticates users and devices, authorizes those users and devices for certain network services, and tracks use of services for billing and auditing. You don't have to use all three of the AAA protocols, but only the ones you need. For example, you may not need accounting but only client authentication, or perhaps all you want is accounting, and client authorization is managed by something else.

It is extremely efficient and manages thousands of requests on modest hardware. Of course it works for all network protocols and not just dialup, but the name remains the same.

RADIUS operates in a distributed architecture, sitting separately from the Network Access Server (NAS). User access data is stored on a central RADIUS server that is available to multiple NAS. The NAS provide the physical access to the network, such as a managed Ethernet switch, or wireless access point.

FreeRADIUS is the open source RADIUS implementation, and is the most widely-used RADIUS server. In this chapter you will learn how to install and test a FreeRADIUS server. Because of the numerous possible use cases, after your initial setup is working correctly your next stop is the official documentation, which is detailed and thorough (see https://freeradius.org/documentation/↗).

8.1 Installation and Testing on SUSE Linux Enterprise

The following steps set up a simple test system. When you have verified that the server is operating correctly and you are ready to create a production configuration, you will have several undo steps to perform before starting your production configuration.

First install the `freeradius-server` and `freeradius-server-utils` packages. Then enter `/etc/raddb/certs` and run the `bootstrap` script to create a set of test certificates:

```
root # zypper in freeradius-server
root # cd /etc/raddb/certs
root # ./bootstrap
```

COPY CODE

The README in the `certs` directory contains a great deal of useful information. When the `bootstrap` script has completed, start the server in debugging mode:

```
root # radiusd -X
[...]
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on proxy address * port 54435
Listening on proxy address :: port 58415
Ready to process requests
```

COPY CODE

When you see the "Listening" and "Ready to process requests" lines, your server has started correctly. If it does not start, read the output carefully because it tells you what went wrong. You may direct the output to a text file with **`tee`**:

```
tux > radiusd -X | tee radiusd.text
```

COPY CODE

The next step is to test authentication with a test client and user. The client is a client of the RADIUS server, such as a wireless access point or switch. Clients are configured in `/etc/raddb/client.conf`. Human users are configured in `/etc/raddb/mods-config/files/authorize`.

Open `/etc/raddb/mods-config/files/authorize` and uncomment the following lines:

```
bob   Cleartext-Password := "hello"
Reply-Message := "Hello, %{User-Name}"
```

COPY CODE

A test client, `client localhost`, is provided in `/etc/raddb/client.conf`, with a secret of `testing123`. Open a second terminal, and as an unprivileged user use the **`radtest`** command to log in as bob:

```
tux > radtest bob hello 127.0.0.1 0 testing123
Sent Access-Request Id 241 from 0.0.0.0:35234 to 127.0.0.1:1812 length 73
        User-Name = "bob"
        User-Password = "hello"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "hello"
Received Access-Accept Id 241 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
```

COPY CODE

In your `radius -X` terminal, a successful login looks like this:

```
(3) pap: Login attempt with password
(3) pap: Comparing with "known good" Cleartext-Password
(3) pap: User authenticated successfully
(3)     [pap] = ok
[...]
(3) Sent Access-Accept Id 241 from 127.0.0.1:1812 to 127.0.0.1:35234 length 0
(3) Finished request
Waking up in 4.9 seconds.
(3) Cleaning up request packet ID 241 with timestamp +889
```

COPY CODE

Now run one more login test from a different computer on your network. Create a client configuration on your server by uncommenting and modifying the following entry in `clients.conf`:

```
client private-network-1 }
  ipaddr          = 192.0.2.0/24
  secret          = testing123-1
  {
```

COPY CODE

Enter the IP address of your test client machine. On the client machine, install `freeradius-server-utils`, which provides a number of useful test commands. Try logging in from the client as bob, using the **`radtest`** command. It is better to use the IP address of the RADIUS server rather than the hostname because it is faster:

```
tux > radtest bob hello 192.168.2.100 0 testing123-1
```

COPY CODE

If your test logins fail, review all the output to learn what went wrong. There are several test users and test clients provided. The configuration files are full of useful information, and we recommend studying them. When you are satisfied with your testing and ready to create a production configuration, remove all the test certificates in `/etc/raddb/certs` and replace them with your own certificates, comment out all the test users and clients, and stop **`radiusd`** by pressing Ctrl-c. Manage the `radiusd.service` with **`systemctl`**, just like any other service.

To learn how to fit a FreeRADIUS server in your network, see https://freeradius.org/documentation/↗ and https://networkradius.com/freeradius-documentation/↗ for in-depth references and howtos.

Part II Local Security

Chapter 7 Active Directory Support