# Upgrading a pilot site on Debian

This article describes the upgrade of a pilot site from Trust Router v1.2 or v1.3 and FreeRADIUS v3.0.1 and v3.0.3, as there are some significant changes within FreeRADIUS.

## Step-by-step guide

### Upgrading Trust Router:

Upgrade the trust router as per your operating system instructions:

```
$ apt-get install moonshot-trust-router
```

Trust Router now ships with a System V init script.

Open the file `/etc/default/trust_router` for editing (if necessary, create it) as follows:

```
ipaddr="[your TIDS host IP address]"               # IP address that the TIDS is reachable on
hostname="[your TIDS host name]"                       # The host name that the TIDS is known as
gssname="trustrouter@apc.moonshot.ja.net"       # The GSS service name for the TIDS APC

TIDS_USER="trustrouter"                                          # The user that the TIDS is running as
TIDS_GROUP="trustrouter"                                          # The group that the TIDS is running as
```

Enable the init script as per your operating system instructions, but do not start the server yet.

The SQLite database that contains the trust router keys has moved and changed:

1. If `/var/lib/trust_router/keys` exists after the upgrade and you **did not** originally create it there, you should not need to do anything and you can skip the next two steps.
2. If `/var/lib/trust_router/keys` exists after the upgrade and you **did** create it there, delete it, then follow the remaining steps.
3. If `/var/lib/trust_router/keys` **does not** exist after the upgrade, create it manually:

   ```
   # sqlite3 </usr/share/trust_router/schema.sql /var/lib/trust_router/keys
   # chown trustrouter:trustrouter /var/lib/trust_router/keys
   # chmod 660 /var/lib/trust_router/keys
   ```

4. Delete any old, obsolete copies of the keys database.

The user `trustrouter` must be able to read some information from directories owned by the `freerad` user and group, notably the FreeRADIUS certificates.

1. Run the `id trustrouter` command.
2. If you can see the `freerad` group in the `groups=` list in the output, you do not need to do anything.
3. If you **cannot** see the `freerad` group in the `groups=` list in the output, run the below commands:

   ```
   $ usermod -a -G freerad trustrouter
   $ id trustrouter
   ```

4. Verify that the `freerad` group is now in the `groups=` list in the output.

Start the TIDS service as per your operating system instructions, then check its log in `/var/log/trust_router` to ensure there were no errors during startup.

### Upgrading FreeRADIUS:

Upgrade FreeRADIUS as per your operating system instructions:

1. Run the command `apt-get install freeradius freeradius-config freeradius-abfab`
   The `freeradius-abfab` package will do much of the reconfiguration (such as enabling the sites and modules used by Moonshot, as well as creating and configuring users).
2. During the upgrade of the `freeradius-config` package, you may be asked to make decisions about modified configuration files. It is sensible to choose **`(N)`** or **`(O)`** to maintain your existing configuration.
   The corresponding updated files will be installed as `<filename>.dpkg-dist` and you can use a diffing tool afterwards to merge your existing and the updated files.
3. Repeat the `apt-get install` command for any other FreeRADIUS packages that you use in your installation, such as the LDAP, KRB5 and SQLite modules.
4. Do not start the server.

The FreeRADIUS user, `freerad`, must be able to read some information from directories owned by the `trustrouter` user and group, notably the SQLite database in `/var/lib/trust_router`.

1. Run the `id freerad` command.
2. If you can see the `trustrouter` group in the `groups=` list in the output, you do not need to do anything.
3. If you **cannot** see the `trustrouter` group in the `groups=` list in the output, run the below commands:

```
$ usermod -a -G trustrouter freerad
$ id freerad
```

4. Verify that the `trustrouter` group is now in the `groups=` list in the output.

Several items in FreeRADIUS have changed or been superseded:

1. Change to the `/etc/freeradius/sites-enabled` directory.
2. Check that the `channel_bindings`, `abfab-tls` and `abfab-tr-idp` symbolic links exist. If they **do not**, create them:

```
$ ln -s ../sites-available/channel_bindings
$ ln -s ../sites-available/abfab-tls
$ ln -s ../sites-available/abfab-tr-idp
```

3. Delete the obsolete `chbind` and `tls` symbolic links.
4. Change to the `/etc/freeradius/mods-enabled` directory.
5. Check that the `abfab_psk_sql` symbolic link exists. If it **does not**, create it:

```
$ ln -s ../mods-available/abfab_psk_sql
```

6. Delete the obsolete `psk` symbolic link.
7. Check that the `realm suffix` entries in the `realm` file are as they were before the upgrade:

```
realm suffix {
  format = suffix
  delimiter = "@"
  default_community = "apc.moonshot.ja.net"
  rp_realm = "your service realm as registered with the Janet Moonshot Community Portal"
  trust_router = "tr1.moonshot.ja.net"
}
```

8. Change to the `/etc/freeradius/sites-available` directory.
9. Open the file `abfab-tls` for editing, then update the `client default` stanza at the bottom of the file to match the below:

```
client default {
        ipaddr = 0.0.0.0/0
        proto = tls
        gss_acceptor_realm_name = "your service realm as registered with the Janet Moonshot Community
Portal"
        trust_router_coi = apc.moonshot.ja.net
}
```

   If you have any other client definitions here, please also update these.

10. **On the Moonshot IdP only**, keep the file `abfab-tr-idp` open for editing, then transfer the SAML assertion (as created per the Issue SAML Assertions section) from the `/etc/freeradius/sites-available/default` file into the `post-auth` section.

    > Alternatively, you can create a policy in `/etc/freeradius/policy.d` that you can call from the `post-auth` sections of the `abfab-tr-idp` and `default` files. To see how to do this, visit the Issuing SAML Assertions hard-coded in the RADIUS Server page.

11. Open the file `/etc/raddb/proxy.conf` for editing and check that the `proxy server` section contains the below keyword:

    ```
    dynamic = yes
    ```

    If it does not, either insert it at the top or the bottom of the section.
12. Start the server. It should start ok and continue to function as normal.

# Related articles

# Content by label

There is no content with the specified labels