Upgrading a pilot site on RHEL/CentOS/SL 6

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 package as per your operating system instructions:

```
$ yum update trust_router
```

Trust Router now ships with a System V init script.

Open the file `/etc/sysconfig/tids` for editing.

Adjust the `TIDS_SERVER_IP` and `TIDS_SERVER_NAME` entries to suit your host information.

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 `radiusd` user and group, notably the FreeRADIUS certificates.

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

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

4. Verify that the `radiusd` 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 `yum update freeradius`
2. Repeat the command for any other FreeRADIUS modules that you use in your installation, such as the LDAP, KRB5 and SQLite modules.
3. During the upgrade of the packages, copies of the configuration files that you have changed from the default will be installed as `<filename>.rpmnew` and you can use a diffing tool afterwards to merge your existing and the updated files.
4. Install the `freeradius-abfab` module; it will do much of the reconfiguration (such as enabling the sites and modules used by Moonshot, as well as creating and configuring users).

```
$ yum install freeradius-abfab
```

5. Do not start the server.

The FreeRADIUS user, `radiusd`, 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 radiusd` 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 radiusd
$ id radiusd
```

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

Alternatively, you can create a policy in `/etc/raddb/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
```

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

Before starting the server, ensure that SELinux is switched into **Permissive** mode!

Related articles

Content by label

There is no content with the specified labels