Troubleshooting the Temporary ID Server

As part of configuring an IdP and an RP, you will be asked to run a TIDS command to verify that your RP proxy or IdP can be contacted correctly by the trust router and other hosts in the trust router infrastructure.

The command-line of TIDS is as follows:

```
Usage: tids <ip-address> <trust-router gss-name> <hostname> <database-name>
```

The below cases are the most common errors seen in the TIDS logs in `/var/log/trust_router`. If you have come across one not listed here, please get in touch with us with the output, and, if possible, any commands that may have led to this.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error in my TIDS window or log when attempting to authenticate:

```
In gsscon_passive_authenticate(), inNameBuffer = trustidentity@your_rp_realm
SSL: error:0200100D:system library:fopen:Permission denied
SSL: error:20074002:BIO routines:FILE_CTRL:system lib
SSL: error:140DC002:SSL routines:SSL_CTX_use_certificate_chain_file:system lib
tlscreatectx: Error initialising SSL/TLS (certfile issues) in TLS context gss-eap
tids: util_radius.cpp:880: OM_uint32 gssEapRadiusMapError(OM_uint32*, rs_error*): Assertion `(err != __null)'
failed.
```

Solution:

Check that the user that TIDS runs as (typically `trustrouter`) has access to the certificates specified in `/etc/radsec.conf`:

1. You have `/etc/radsec.conf` configured as per Section 3.1.3 of Install an Identity Provider of the operating system of your choice. It must be configured for TLS for TIDS to function correctly.
2. Add the user to the group (`freerad` on Debian systems, `radiusd` on RHEL systems) under which FreeRADIUS is running, if you choose to use the certificates stored in the FreeRADIUS directory.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error in my TIDS window or log when attempting to authenticate:

```
Error returned by gss_acquire_cred:
      major error <1> Unspecified GSS failure. Minor code may provide more information
      minor error <1> /etc/radsec.conf: unable to open configuration file
Authenticate failed: Unknown code FF 164 (err = 100004)
tids_auth_connection: Error from gsscon_passive_authenticate(), rc = 100004.
```

Solution:

Check the following:

1. You have `/etc/radsec.conf` present. Without this file, TIDS will start but will not be able to function.
2. You have `/etc/radsec.conf` configured as per Section 3.1.3 of Install an Identity Provider of the operating system of your choice. It must be configured for TLS for TIDS to function correctly.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error in my TIDS window or log when attempting to authenticate:

```
In gsscon_passive_authenticate(), inNameBuffer = trustidentity@your_rp_realm
ReadBuffer failed: Connection reset by peer (err = 104)
ReadToken failed: Connection reset by peer (err = 104)
Authenticate failed: Connection reset by peer (err = 104)
tids_auth_connection: Error from gsscon_passive_authenticate(), rc = 100004
```

Solution:

Check the following:

1. You have FreeRADIUS configured correctly for TLS. If you are behind a firewall, make sure that both your firewall and your FreeRADIUS server accept connections on port tcp/2083.
2. Your `rp_realm` in the FreeRADIUS `realm` module is correctly configured for the host to use. If you have a separate IdP to your RP proxy, the `rp_realm` values between the IDP and the RP proxy may differ.
   Check your realm configuration at your Trust Router operator, including service realms and domain constraints.
3. The name of your host is registered in DNS and resolves back to an IP address. Manual resolution in /etc/hosts is not sufficient.
4. The name of your host in the management portal is not an IP address.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error in my TIDS window or log when attempting to authenticate:

```
Error returned by gss_accept_sec_context:
      major error <1> Invalid credential was supplied
      minor error <1> Authentication rejected by RADIUS server
Authenticate failed: Authentication rejected by RADIUS server (err = 2109382925)
tids_auth_connection: Error from gsscon_passive_authenticate(), rc = 2109382925.
```

Possible Solutions:

This means that the trust router credential your server is supplying is incorrect, or no credential is being passed along, or another error occurred that prevents passing the credentials along.

Check the following:

1. You are running the `freeradius -fxx -l stdout` or `radiusd -fxx -l stdout` command as the FreeRADIUS user and you have executed the `unset DISPLAY` command beforehand. Without running `unset DISPLAY`, the TID client (TIDC) connection will fail. Additionally, you may see something similar to the below in your FreeRADIUS debug output.

   ```
   (3) suffix : Looking up realm "ov-apcmoonshot.ja.net" for User-Name = "@ov-apc.moonshot.ja.net"
   Openning TIDC connection to tr.moonshot.ja.net:0Error in tidc_open_connection.
   (3) suffix : No such realm "ov-apc.moonshot.ja.net"
   (3) [suffix] = noop
   ```

2. On RHEL-based systems only, there currently exists a problem with the SELinux contexts. If you see this while your FreeRADIUS server is running as daemon (i.e. has been started with init.d), check whether SELinux is in Enforcing mode:

   ```
   # getenforce
   ```

   You should receive a message that it is either in Enforcing or in Permissive mode. Ensure that SELinux is either switched to Permissive mode, or see this article: Troubleshooting SELinux

3. You have configured the `realm` module in FreeRADIUS correctly. By default, the module sets the trust router to `localhost`. Additionally, you may see something similar to the below in your FreeRADIUS debug output:

```
(0)  suffix : Looking up realm "ov-apc.moonshot.ja.net" for User-Name = "@ov-apc.moonshot.ja.net"
Opening TIDC connection to localhost:0
tidc_open_connection: Opening GSS connection to localhost:12309.gss_connect: Connecting to host
'localhost' on port 12309
Waking up in 0.3 seconds.
Error returned by gss_init_sec_context:
      major error <1> Invalid token was supplied
      minor error <1> Acceptor identity different than expected
AuthenticateToServer failed: Acceptor identity different than expected (err = 2109382938)
Error in tidc_open_connection.
(0)  suffix : No such realm "ov-apc.moonshot.ja.net"
(0)   [suffix] = noop
```

4. If you are using the `attr_filter` module, add the `GSS-Acceptor-Host-Name`, `GSS-Acceptor-Service-Name`, `GSS-Acceptor-Realm-Name` and `GSS-Acceptor-Service-Specifics` attributes to your `pre-proxy` and `post-proxy` filters. Modify the `/etc/freeradius/mods-config/attr_filter/pre-proxy` and `post-proxy` files and add the following lines under `DEFAULT`:

```
DEFAULT
<tab>GSS-Acceptor-Service-Name =* ANY,
<tab>GSS-Acceptor-Host-Name =* ANY,
<tab>GSS-Acceptor-Service-Specifics =* ANY,
<tab>GSS-Acceptor-Realm-Name =* ANY,
```

   The trust router requires the `GSS-Acceptor-*` attributes to be present in trust router authentication attempts.

   ⚠ These entries are currently not in the standard distribution, but they will be soon.

5. You may be using a trust router credential whose trust anchor information does not match the certificate that was received from the APC. You may see something similar to the below in your FreeRADIUS debug output:

```
TLS: Certificate verification failed, error 19 (Server certificate mismatch) depth 0 for '/C=GB
/ST=Oxfordshire/O=Jisc Collections and Janet Ltd./CN=Moonshot Workshop APC/emailAddress=netman@dev.ja.
net'
CTRL-EVENT-EAP-TLS-CERT-ERROR reason=1 depth=0 subject='/C=GB/ST=Oxfordshire/O=Jisc Collections and
Janet Ltd./CN=Moonshot Workshop APC/emailAddress=netman@dev.ja.net' err='Server certificate mismatch'
SSL: SSL3 alert: write (local SSL3 detected an error):fatal:unknown CA
OpenSSL: openssl_handshake - SSL_connect error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:
certificate verify failed
Error returned by gss_init_sec_context:
      major error <1> Invalid credential was supplied
      minor error <1> Authentication rejected by RADIUS server
AuthenticateToServer failed: Authentication rejected by RADIUS server (err = 2109382925)
Error in tidc_open_connection.
(0)  suffix : No such realm "ov-apc.moonshot.ja.net"
(0)   [suffix] = noop
```

   Contact your Trust Router operator to check whether the TLS certificates have changed.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error in my TIDS window or log when attempting to authenticate:

```
Error returned by gss_accept_sec_context:
      major error <1> Unspecified GSS failure.  Minor code may provide more information
      minor error <1> error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed (tcp.c:
235)
Authenticate failed: Unknown code rse 14 (err = 46882574)
tids_auth_connection: Error from gsscon_passive_authenticate(), rc = 46882574.
```

Solution:

Check whether your FreeRADIUS certificates have expired:

1. The `ca.cnf`, `client.cnf` and `server.cnf` files in `/etc/freeradius/certs` or `/etc/raddb/certs` directories specify a default expiry date of **60** days. You must extend that time to something for the length of your pilot or a year.

   ⚠ You must remember to renew the certificates after that time.

2. The error in the TIDS window will include the message `Certificate has expired` with the details of the expired certificate.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error in my TIDS window or log when attempting to authenticate:

```
Error returned by gss_accept_sec_context:
      major error <1> Unspecified GSS failure.  Minor code may provide more information
      minor error <1> peer disconnected (tcp.c:216)
Authenticate failed: Unknown code rse 20 (err = 46882580)
tids_auth_connection: Error from gsscon_passive_authenticate(), rc = 46882580.
```

Solution:

1. Check whether your FreeRADIUS server is running
2. If your FreeRADIUS server is running, it may be expecting a client certificate. If you are not providing a client certificate, change the option `require_client_certificate` to no.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error in my TIDS window or log when attempting to authenticate:

```
Authenticate failed: Operation not permitted (err = 1)
tids_auth_connection: Error from gsscon_passive_authenticate(), rc = 1.
tids_handle_connection: Error authorizing TID Server connection.
Error in tids_start(), rc = 0. Exiting.
```

Possible Solutions:

Check the following:

1. If you are using the `attr_filter` module, you must not filter out the `User-Name` attribute. Check the `/etc/raddb/mods-config/attr_filter/pre-proxy` and `post-proxy` files and check that the `User-Name` attribute appears in both files.
2. If you are using the `cui` module in the `post-auth` section of your `default` server (not the `inner-tunnel` server), check `/etc/raddb/policy.d/cui` for the below lines in the `cui.post-auth` stanza:

   ```
   update reply {
       User-Name -= "%{reply:User-Name}"
   }
   ```

   Comment them out, or move them to above the previous closing curly bracket. TIDS requires the trust router's username to be in its Access-Accept reply from the RADIUS server.

3. Alternatively, wrap the `cui` call in the `post-auth` section into a piece of unlang that prevents the `cui` module from running for trust router replies:

   ```
   if (&request:GSS-Acceptor-Service-Name != 'trustidentity' && \
       &request:GSS-Acceptor-Host-Name == '[hostname of your identity provider]')) {
    cui
   }
   ```

More to come...