Troubleshooting the Temporary ID Client

As part of configuring an IdP and an RP, you will be asked to run a TIDC command to verify that your RP proxy or IdP are able to contact the trust router correctly.

The command-line for TIDC is as follows:

```
Usage: tidc <server> <RP-realm> <target-realm> <community> [<port>]
```

The below cases are the most common errors experienced when attempting to run the TIDC command. If you have come across one not listed here, please get in touch with us with the command run and the subsequent output.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error when running the TIDC command:

```
Error returned by gss_init_sec_context:
      major error <1> Unspecified GSS failure. Minor code may provide more information
      minor error <1> Generic RADIUS failure
AuthenticateToServer failed: Generic RADIUS failure (err = 2109382928)
Error in tidc_open_connection.
```

Possible Solutions:

Check the following:

1. The RADIUS server specified in `/etc/radsec.conf` is running and can be reached over TLS or UDP (depending on your setting in radsec.conf).
2. Check that the `<RP-realm>` value in the `tidc` command-line is what you have registered for your organisation in your Trust Router operator's Moonshot portal.
3. There may be a problem with your Trust Router operator's APC or the trust router. Please contact your Trust Router operator.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error when running the TIDC command:

```
Error returned by gss_init_sec_context:
      major error <1> Unspecified GSS failure. Minor code may provide more information
      minor error <1> Missing default password or other credentials
AuthenticateToServer failed: Missing default password or other credentials (err = 2109382948)
Error in tidc_open_connection.
```

Possible Solutions:

Check the following:

1. You have the FreeRADIUS user (**freerad** on Debian systems, **radiusd** on RHEL systems) listed in `/etc/moonshot/flatstore-users`.
2. You are running the TIDC command as the FreeRADIUS user and that you have run the `unset DISPLAY` command before running the TIDC command.
3. You have imported the Trust Router credentials using the `moonshot-webp` command as the FreeRADIUS user in Section 4.4.1 of Install an IdP on Debian/Ubuntu/Raspbian or Install an IdP on RHEL/CentOS/SL. To verify you have, execute `ls -la ~/.local/share/moonshot-ui/identities.txt` as the FreeRADIUS user, and you should see the file listed.
4. If you use Network Address Translation (NAT), check that you are forwarding TCP ports 2083 and 12309 both in- and outbound, and that the public IP address is correct in the configuration of your Trust Router operator.
5. If your service is firewalled, check that TCP ports 2083 and 12309 are open both in- and outbound, and that the public IP address is correct in the configuration of your Trust Router operator. Your firewall should also support hairpinning.
6. You are running the newest version of the trust router and Moonshot software. If you were part of the Janet or GÉANT Moonshot Pilots, you must update your software to the newest versions.
7. You have installed the `dbus-x11` package. This package is not installed as part of the package dependencies, but it **is** part of the instructions in Section 2 of the platform-specific instructions for Install an Identity Provider. It is a client library and will not require the installation of the X11 system.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error when running the TIDC command:

```
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.
```

Possible Solutions:

Check the following:

1. Your hostname must resolve correctly. Check that the `hostname` and `hostname -f` commands return the same name.
2. Check that your hostname resolves with `nslookup`

Problem

I can't seem to be able to connect my service to the trust router infrastructure. I get the following error when running the TIDC command:

```
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.
```

Possible Solutions:

Check the following:

1. There may be a problem with your organisation's Trust Router network credentials:
    a. If you were part of the Janet Moonshot pilot, your credential will cease to function on March 20, 2015.
    b. After March 25, 2015, contact your Trust Router operator.
2. Check with your Trust Router operator that your organisation's Trust Router credential trust anchors are correct if you see a message similar to the below immediately before the error message:

```
CTRL-EVENT-EAP-TLS-CERT-ERROR reason=1 depth=0 subject='...' 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
```

Problem

I can't seem to be able to connect my service to the trust router infrastructure. It seems to start but then I get the following error when running the TIDC command:

```
tidc_open_connection: Opening GSS connection to tr.moonshot.ja.net:12309.gss_connect: Connecting to host 'tr.
moonshot.ja.net' on port 12309
CTRL-EVENT-EAP-STARTED EAP authentication started
:
:
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
tidc_fwd_request: Sending TID request: {"msg_type": "tid_request", "msg_body": {"rp_realm": "my RP realm",
"target_realm": "ov-apc.moonshot.ja.net", "community": "ov-apc.moonshot.ja.net", ...}
ReadBuffer failed: Connection reset by peer (err = 104)
ReadBuffer failed: Connection reset by peer (err = 104)
ReadBuffer failed: Connection reset by peer (err = 104)
```

Solution:

1. There may be a problem with your organisation's Trust Router network credentials.
2. Check that the values of your RP realm parameter in the TIDC command-line matches the `rp_realm` parameter in the FreeRADIUS `realm` module of your RP proxy and that the value is also present in the trust configuration of your Trust Router operator.
3. The trust router may be down. This should not be the case, but it occasionally happens. Give it a few minutes and then try again.

> If the problem persists, please get in touch with your Trust Router operator!

Problem

I can't seem to be able to connect my service to the trust router infrastructure. It seems to start but then I get the following error when running the TIDC command:

```
tidc_open_connection: Opening GSS connection to tr.moonshot.ja.net:12309.gss_connect: Connecting to host 'tr.
moonshot.ja.net' on port 12309
CTRL-EVENT-EAP-STARTED EAP authentication started
:
:
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
tidc_fwd_request: Sending TID request: {"msg_type": "tid_request", "msg_body": {"rp_realm": "my RP realm",
"target_realm": "ov-apc.moonshot.ja.net", "community": "ov-apc.moonshot.ja.net", ...}
tidc_fwd_request: Response Received (226 bytes).
{"msg_type": "tid_response", "msg_body": {"result": "error", "comm": "ov-apc.moonshot.ja.net", "target_realm":
"ov-apc.moonshot.ja.net", "rp_realm": "target_realm", "err_msg": "Can't open connection to next hop TIDS"}}
tr_msg_decode_tidresp(): Error! result = error.
Response received! Realm = ov-apc.moonshot.ja.net, Community = ov-apc.moonshot.ja.net.
tidc_resp_handler: Response is an error.
```

Solution:

1. Check that the TIDS service is running and, if you are using firewalls, that the port on tcp/12309 is open to accept traffic from the outside world, and that services on your server can reach port tcp/12309 anywhere in the outside world.
2. Check that you have imported the credentials file as the FreeRADIUS user, that you are running the TIDC command as the FreeRADIUS user, and that you have run the `unset DISPLAY` command before running the TIDC command.
3. Check that the value of your RP realm is correct and that it is also in the configuration of your Trust Router operator.
4. There appears to be a problem either with your organisation's Trust Router network credentials or with the RP realm that you specified on the command-line.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. It seems to start but then I get the following error when running the TIDC command:

```
tidc_open_connection: Opening GSS connection to tr.moonshot.ja.net:12309.gss_connect: Connecting to host 'tr.
moonshot.ja.net' on port 12309
CTRL-EVENT-EAP-STARTED EAP authentication started
:
:
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
tidc_fwd_request: Sending TID request: {"msg_type": "tid_request", "msg_body": {"rp_realm": "my RP realm",
"target_realm": "ov-apc.moonshot.ja.net", "community": "ov-apc.moonshot.ja.net", ...}
tidc_fwd_request: Response Received (198 bytes).
{"msg_type": "tid_response", "msg_body": {"result": "error", "err_msg": "RP Realm filter error", "rp_realm": "my
RP realm", "target_realm": "ov-apc.moonshot.ja.net", "comm": "ov-apc.moonshot.ja.net"}, "msg_type":
"tid_response"}
tr_msg_decode_tidresp(): Error! result = error.
Response received! Realm = ov-apc.moonshot.ja.net, Community = ov-apc.moonshot.ja.net.
tidc_resp_handler: Response is an error.
```

Solution:

1. There appears to be a problem with the RP realm that you specified.
2. Check that:
    a. the value of your RP realm is correct and that it is also in the configuration of your Trust Router operator.
    b. the value of your RP realm is specified in the second parameter of the TIDC command-line.
    c. you have not specified your ID Provider realm by accident, if it differs from your RP realm.

Problem

I can't seem to be able to connect my service to the trust router infrastructure. It seems to start but then I get the following error when running the TIDC command:

```
tidc_open_connection: Opening GSS connection to tr.moonshot.ja.net:12309.gss_connect: Connecting to host 'tr.
moonshot.ja.net' on port 12309
CTRL-EVENT-EAP-STARTED EAP authentication started
:
:
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
tidc_fwd_request: Sending TID request: {"msg_type": "tid_request", "msg_body": {"rp_realm": "my RP realm",
"target_realm": "my IdP realm", "community": "ov-apc.moonshot.ja.net", ...}
tidc_fwd_request: Response Received (198 bytes).
{"msg_type": "tid_response", "msg_body": {"result": "error", "err_msg": "No path to AAA Server(s) for realm",
"rp_realm": "my RP realm", "comm": "ov-apc.moonshot.ja.net", "target_realm": "my IdP realm"}}
tr_msg_decode_tidresp(): Error! result = error.
Response received! Realm = ov-apc.moonshot.ja.net, Community = ov-apc.moonshot.ja.net.
tidc_resp_handler: Response is an error.
```

Solution:

1. There appears to be a problem with the ID Provider realm that you specified.
2. Check that:
    a. the value you specified on the command-line matches the ID Provider realm you specified or asked your Trust Router operator to register for you.
    b. the ID Provider server name and IP address you specified in the portal or to your Trust Router operator are correct for your IdP server, and that they are accessible from anywhere on ports tcp/2083 and tcp/12309. This is very important!
    c. you have not specified your RP realm by accident, if it differs from your ID Provider realm.

More to come...