$\frac{\text{UNH}}{\text{CSC}}$ Team Guide: Teleport

Evan Parker

March 13, 2025

If you do not have an account to log in, SSH into the server and run:

```
sudo tctl users add <YOUR-USERNAME> --roles=editor,
   access --logins=root,ubuntu,ec2-user
```

Make sure you add your username to it, and correct roles when needed. Open the link provided, and utilize an authenticator app to link yourself to it.

User Management

To view users, go to `Zero Trust Access` → `Users`.

To lock a user out:

1. Go to the `Options` menu on the right.
2. Select `Reset Authentication...`.
3. Select `Generate Reset URL`.

The user will no longer be able to log in unless they get that new link. **This is preferable to deleting a user as it retains the option to give them access back if needed.**

Checking Logs

1. Go to `Audit` → `Audit Log`.
2. Click on `Details` on an entry to expand it.

Locking it Down

Join Tokens

By default, there are no Join Tokens created. These could give the ability for a device or resource to join the Teleport network, creating possible security vulnerabilities.

Roles

These are the default roles, and some notes on them. If there are any other roles, they should be treated as possible security vulnerabilities and be reviewed by the team.

- **access**:
  The role allows someone to connect and view setups, should **not** have any edit permissions. By default, only has `list` and `read` permissions.

- **auditor**:
  This role allows someone to `list` and `read` the resources tagged `session` and `event`. It should do nothing else.

- **editor**:
  This allows someone to edit everything. Be careful with this role.

- **terraform-provider**:
  This role is dangerous. It has a lot of permissions. Make sure it is not assigned to users.

- **wildcard-workload-identity-issuer**:
  Apparently, it issues workload identities as part of the API. It should not be assigned to users.

Auth Connectors

By default, Teleport comes with only the "Local Connector" enabled, with the ability to add GitHub as an alternative. The others, like Google, Microsoft, GitLab, etc., all require the enterprise subscription.

Integrations

By default, there are no enabled Integrations.

Clusters & Trusted Root Clusters

This will vary based on setup. Make sure all clusters are local and manageable by you.