Configuring minimum Permissions for NetApp account

For regular functionality, CyberSnap requires access to the NetApp to oversee processes within the NetApp environment during scanning and recovery.

The most efficient approach involves creating a dedicated user account with administrative privileges.

In cases where customers need to restrict account privileges, specific and granular permissions must be assigned to dedicated user accounts.

To set up the minimum required privileges for a dedicated NetApp account, follow these steps:

1. Log in to the NetApp system.
2. Navigate to "Cluster" and then select "Settings."
3. Within "Settings," click on "User and Roles."
4. Under "Roles," click on the "Add" button to open a new window.
5. In the "Add Role" window:

1. Enter the role name.
2. Choose the REST API PATH by selecting "/api."
3. Leave the secondary path blank.

4. Select the access level, and choose “Read/Create/Modify”.

6. Click on the "Save" button to apply the changes.

Upon the creation of a customized role, proceed to create a user and assign them the newly created role.

1. Log in to the NetApp system.

2. Navigate to "Cluster" and then select "Settings."

3. Within "Settings," click on "User and Roles."

4. Under "Users," click on the "Add" button to open a new window.

5. In the "Add User" window:

1. Enter desire username.

2. In the Role dropdown menu choose role that you created in previous step

3. In “User Login Methods”

- In Application
  - choose HTTP from dropdown menu
  - Select “Password” as “AUTHENTICATION”
  - Click on Plus sign to add new application
  - choose HTTP from dropdown menu
  - Select “Password” as “AUTHENTICATION”

- Configure desire password for user
- Click on Save button

Now you have configured a dedicated NetApp account with the minimum privileges required for CyberSnap to operate effectively.

If you require further assistance, please feel free to submit a support ticket here.