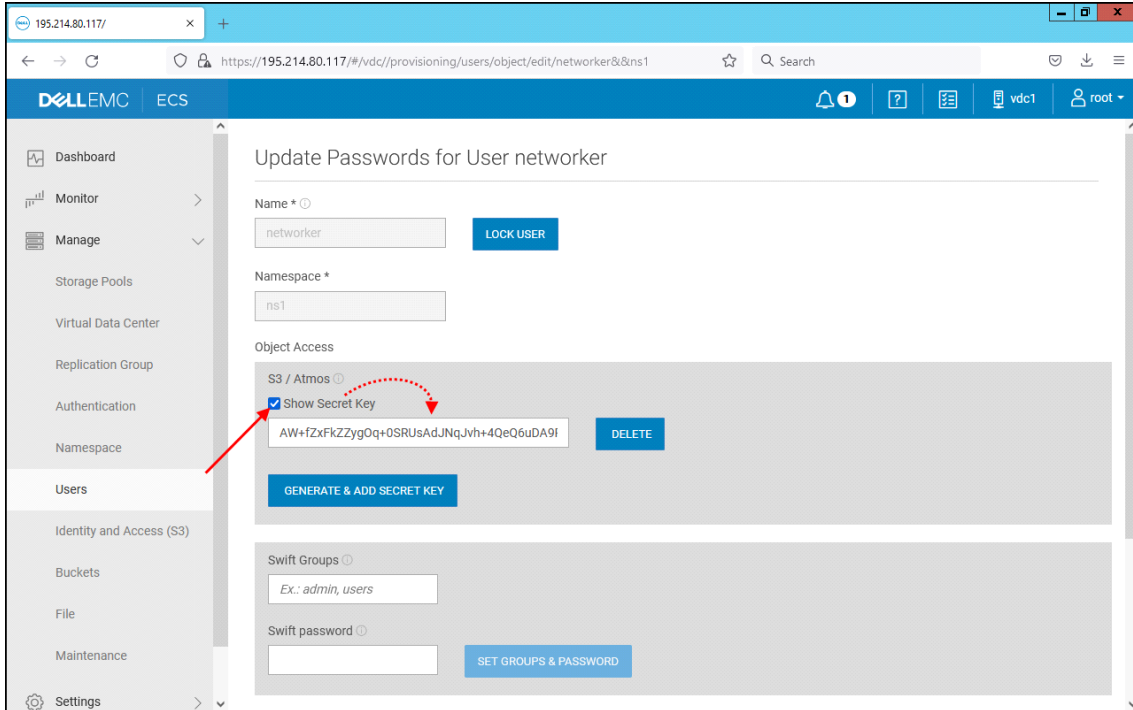
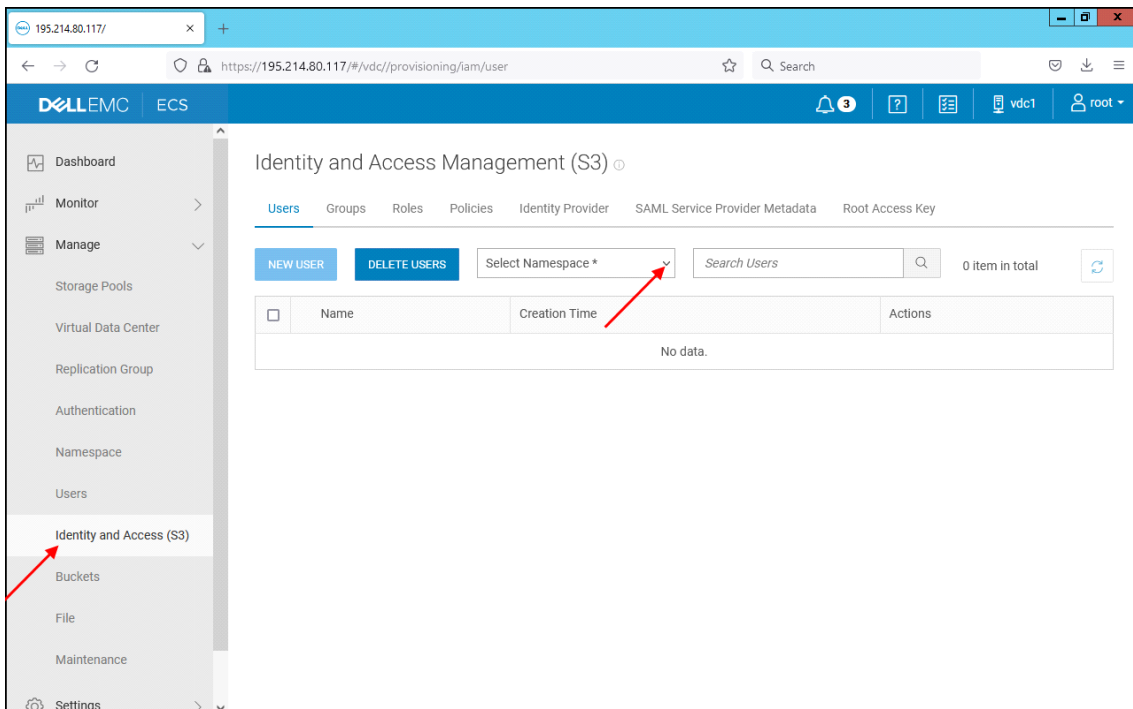


How to determine 'Secret Key' & 'Access Key'

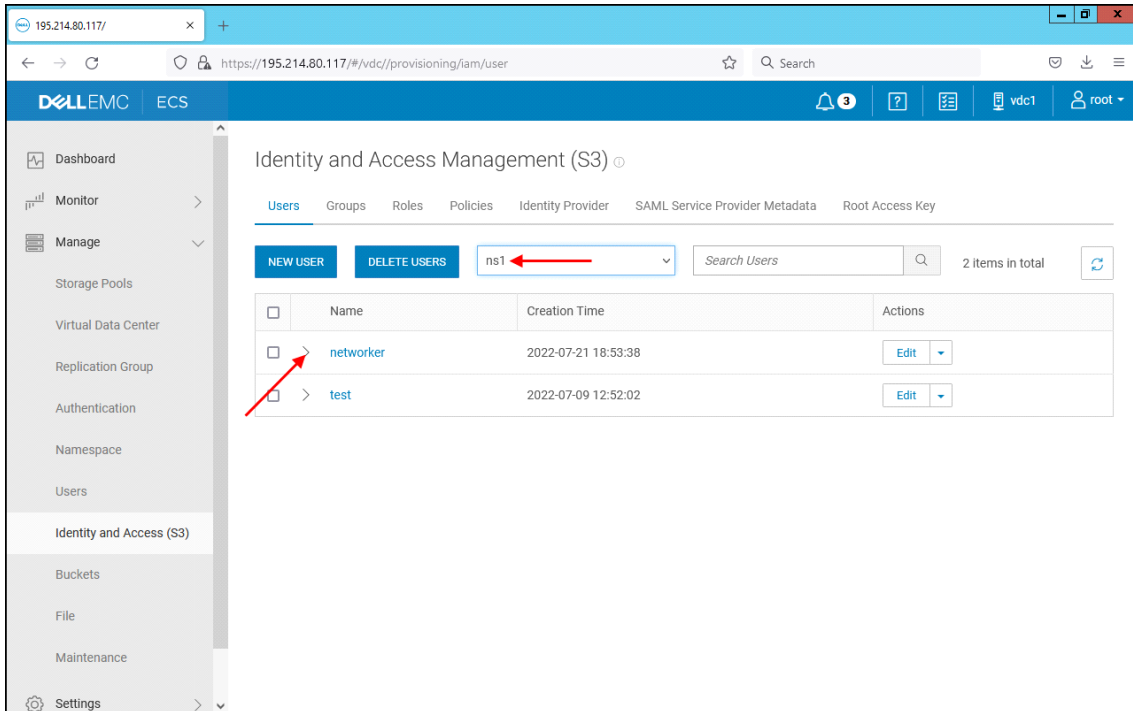
You will receive the *Secret Key* already if you create the user (here: *networker*):



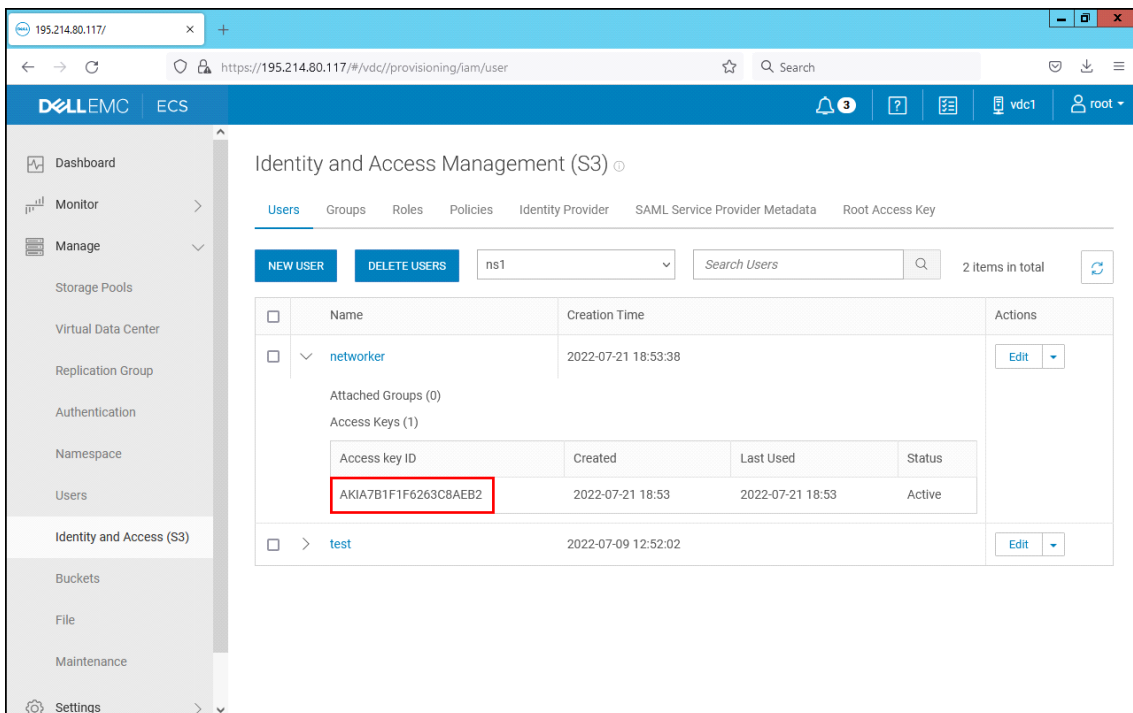
- You better save the **Secret Key** in a text file.
- For the **Access Key** you first have to go to **Manage > Identity and Access (S3) > Users** and open the list under **Select Namespace ***:



- Select the existing namespace **ns1**
That will make all its existing users appear:



- Now click the arrow left to its name to verify his details.
Now you will see his **Access key ID** :



Be careful - this is **not** the Access Key, but only its internal ID, the number which is used within the management system.
It would be logical, that the user **Name** would be the true **Access Key**.

Unfortunately, the older (DDOS 6.1) *Administration Guide* does not really shed the light.

The technical writers could have easily omitted this statement:

Adding an S3 Flexible provider cloud unit

The Cloud Tier feature supports additional qualified S3 cloud providers under an S3 Flexible provider configuration option..

The S3 Flexible provider option supports the standard and standard-infrequent-access storage classes. The endpoints will vary depending on cloud provider, storage class and region. Be sure that DNS is able to resolve these hostnames before configuring cloud units.

Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click **Add**.
The Add Cloud Unit dialog is displayed.
3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.
The remaining fields in the Add Cloud Unit dialog pertain to the cloud provider account.
4. For **Cloud provider**, select **Flexible Cloud Tier Provider Framework for S3** from the drop-down list.
5. Enter the provider **Access key** as password text.
6. Enter the provider **Secret key** as password text.
7. Specify the appropriate **Storage region**.
8. Enter the provider **Endpoint** in this format: `http://<ip/hostname>:<port>`. If you are using a secure endpoint, use `https` instead.
9. For **Storage class**, select the appropriate storage class from the drop-down list.
10. Ensure that port 443 (HTTPS) is not blocked in firewalls. Communication with the S3 cloud provider occurs on port 443.
11. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.
Enter the proxy hostname, port, user, and password.
12. Click **Add**.

The File System main window now displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.

However, the current (DDOS 7.7) *Administration Guide* is really clear:

Adding a cloud unit for Elastic Cloud Storage (ECS)

About this task

A protection system or DDVE instance requires a close time synchronization with the ECS system to configure a DD cloud unit. Configuring NTP on the protection system or DDVE instance, and the ECS system addresses this issue.

Steps

1. Select **Data Management > File System > Cloud Units**.
2. Click **Add**.
The **Add Cloud Unit** dialog box appears.
3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.
The remaining fields in the Add Cloud Unit dialog pertain to the cloud provider account.
4. For **Cloud provider**, select **EMC Elastic Cloud Storage (ECS)** from the list.
5. In the **Bucket** field, optionally specify a pre-existing, empty bucket to use the for the cloud unit.
6. Enter the provider **Access key** as password text.
NOTE: Use the ECS username as the access key.
7. Enter the provider **Secret key** as password text.
8. Enter the provider **Endpoint** in this format: **http://<ip/hostname>:<port>**. If you are using a secure endpoint, use **https** instead.
NOTE: Implementing cloud storage on ECS requires a load balancer.

By default, ECS runs the S3 protocol on port 9020 for HTTP and 9021 for HTTPS. With a load balancer, these ports are sometimes remapped to 80 for HTTP and 443 for HTTPS, respectively. Check with your network administrator for the correct ports.
9. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure** for **HTTP Proxy Server**.
Enter the proxy hostname, port, user, and password.
NOTE: There is an optional step to run the cloud provider verify tool before adding the cloud unit. This tool performs pre-check tests to ensure that all requirements are met before to adding the actual cloud unit.
10. Click **Add**.
The File System main window displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.



This supports my assumption that when you define the cloud unit for an ECS the *User Name* shall be used as the *Access Key* .