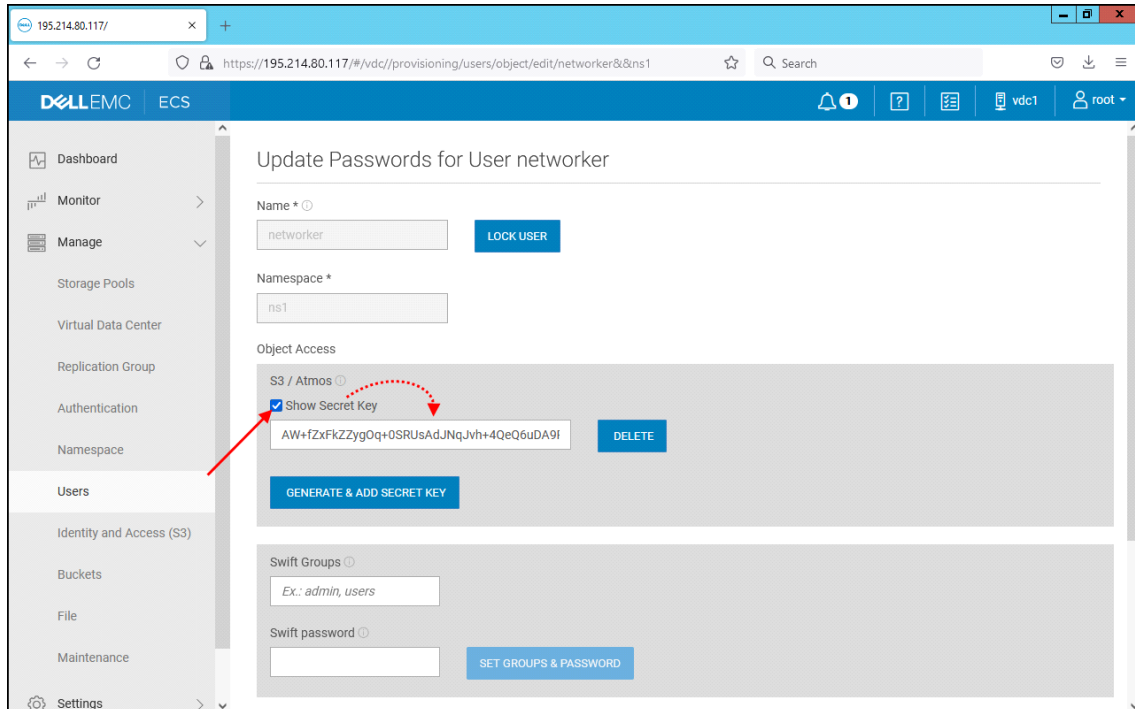
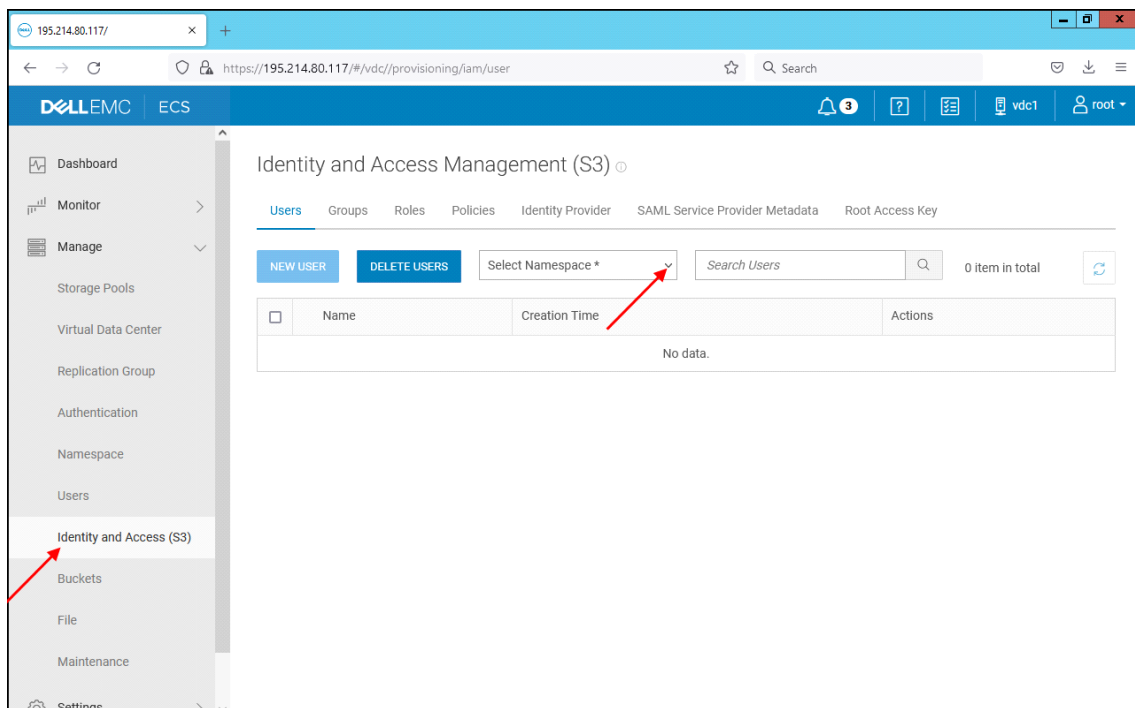


So ermitteln Sie 'Secret Key' & 'Access Key'

Den *Secret Key* erhalten Sie bereits bei der Erstellung des Users (hier: *networker*):



- Kopieren Sie sich den **Secret Key** in einer Textdatei.
- Für den **Access Key** müssen Sie zunächst **Manage > Identity and Access (S3) > Users** auswählen und die Liste unter **Select Namespace *** öffnen:



- Wählen Sie darin jetzt bereits benutzten Namespace **ns1** aus.
Hierdurch werden die bereits für ihn definierten **User** zugänglich:

The screenshot shows the Dell EMC ECS IAM console. The left sidebar contains navigation options like Dashboard, Monitor, Manage, Storage Pools, etc. The main content area is titled 'Identity and Access Management (S3)' and shows the 'Users' tab for namespace 'ns1'. A table lists two users: 'networker' (created 2022-07-21 18:53:38) and 'test' (created 2022-07-09 12:52:02). A red arrow points to the 'ns1' dropdown menu, and another red arrow points to the 'networker' user name.

- Klicken Sie den Pfeil links neben seinem Namen an, um seine Details abzufragen.
Jetzt sehen Sie auch seine **Access key ID** :

The screenshot shows the details for the 'networker' user. The 'Access Keys (1)' section is expanded, showing a table with one entry: 'Access key ID' AKIA7B1F1F6263C8AEB2, 'Created' 2022-07-21 18:53, 'Last Used' 2022-07-21 18:53, and 'Status' Active. The 'Access key ID' is highlighted with a red box.



Das ist allerdings nicht der **Access Key**, sondern 'nur' seine ID, also die "Nummer der Resource", unter der der offensichtliche Access Key verwaltet wird. Logischerweise wäre dann der User **Name** der eigentliche **Access Key**.

In einem älteren (DDOS 6.1) *Administration Guide* trägt leider die beschreibende Textstelle nicht wirklich zur Aufklärung bei.

Die entsprechende Passage hätten sich die Technical Writer auch wirklich sparen können:

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.

Zum Glück wird der aktuelle (DDOS 7.7) *Administration Guide* dann doch wirklich eindeutig:

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.



Somit bestätigt sich meine Annahme, daß bei der Definition der Cloud Unit für eine ECS der *User Name* auch wirklich als *Access Key* einzutragen ist.