Working with S3-compatible credentials

When you want to interact with object storage in Cleura using tools that support an Amazon S3 compatible API (such as `s3cmd`, `rclone`, the `aws` CLI, or the Python `boto3` library), you need an S3-compatible access key ID and secret key.

Creating credentials

You can create a set of S3-compatible credentials with the following command:

```
openstack ec2 credentials create
```

This will return an `Access` and `Secret` key that you can use to populate the `AWS_ACCESS_KEY_ID` and `AWS_SECRET_ACCESS_KEY` environment variables (or whichever configuration options your application requires).

> Your S3-compatible credentials are always scoped to your Cleura *region* and *project*. You cannot reuse an access and secret key across multiple regions or projects.
>
> Also, your credentials are only "S3-compatible" in the sense that they use the same *format* as AWS S3 does. They are never valid against AWS S3 itself.

Listing credentials

You can list any previously-created credentials with:

```
openstack ec2 credentials list
```

Deleting credentials

If at any time you need to delete a set of AWS-compatible credentials, you can do so with the following command:

```
openstack ec2 credentials delete <access-key-id>
```

> Deleting a set of S3-compatible credentials will *immediately* revoke access for any applications that were using it.

Last update: 2022-04-19

Created: 2022-04-19

Authors: Florian Haas