Secrets top-level elements

Table of contents

Secrets are a flavor of Configs focusing on sensitive data, with specific constraint for this usage.

Services can only access secrets when explicitly granted by a `secrets` attribute within the `services` top-level element.

The top-level `secrets` declaration defines or references sensitive data that is granted to the services in your Compose application. The source of the secret is either `file` or `environment`.

- `file`: The secret is created with the contents of the file at the specified path.
- `environment`: The secret is created with the value of an environment variable.

Example 1

`server-certificate` secret is created as `<project_name>_server-certificate` when the application is deployed, by registering content of the `server.cert` as a platform secret.

```
secrets:
 server-certificate:
   file: ./server.cert
```

Example 2

`token` secret is created as `<project_name>_token` when the application is deployed, by registering the content of the `OAUTH_TOKEN` environment variable as a platform secret.

```
secrets:
 token:
   environment: "OAUTH_TOKEN"
```

Additional resources

For more information, see How to use secrets in Compose.