SSM Parameter Store & Secrets Manager reference

This page contains a reference of all of the SSM parameters in use by the pipeline and the Helm chart

Parameter store & Secrets manager layout

First of all, in the old pipelines everything was stored as Azure Devops variables. In this pipeline this has been replaced by using the AWS SSM Parameter Store for everything that is considered to be non-sensitive, and the Secrets Manager for everything that is considered to be sensitive (think things like passwords, tokens, access keys, etc). Both are created with a path-like naming convention. The general convention is as follows:

`/dsm/mendix/apps/<app_name>/<section>/<parameters>`

In here, `app_name` is the unique name of the Mendix application and must be consistently used everywhere in the various pipelines and scripts. It is very important to keep this name consistent everywhere.

`section` has a couple of options:

- `config` refers to the helm chart configuration for this Mendix app. Please see the next paragraph for this
- `vcs` refers to Version Control System, or in this case the remote Mendix hosted VCS, which is either Subversion or Git. The following `parameters` are defined here
  - `branch`: The branch to checkout
  - `url`: The Mendix VCS URL
  - `revision`: This contains state of the revision of the latest triggered pipeline used by the polling script in `mendix-vcs-polling`
- `azure` refers to (meta)data related to the Azure Devops pipeline with the following `parameters`:
  - `pipeline` contains a dictionary of the original pipeline ID and the sanitized name of this pipeline. Not actively used in any script at this time of writing.

Secrets are generally managed by the CDK with a few exceptions. Typically all secrets are created under the `/dsm/mendix/apps/<app_name>/config` section so the secrets can be picked up by the Helm chart. The following secrets are created manually and don't follow the path-style convention. They are expected to be present in the AWS account running all the scripts and the scripts will fail without them.

- mendix-service-account
- mendix-license-key
- azure-devops-token

Helm chart parameters usage

The Helm chart always has a `values.yaml` which provides the default values for the Helm chart. If no configuration parameter is provided by any other way it falls back to the default value specified here. Most parameters in this helm chart are expected to be overriden, however, and we are doing this by calling `scripts/generate_helm_values.py` to retrieve parameters out of the SSM Parameter Store and secrets out of the Secret Manager. This python script is essentially providing the glue between Helm and the AWS resources. Providing this as an additional values file to the Helm chart means that the values specified here will overwrite the default values (the flags must be set in the right order). It's adviced you read the comments in the `values.yaml` itself to get more insights on what can be configured.

The `scripts/generate_helm_values.py` script that lives in the *kubernetes-mendix-runtime* repository assumes the AWS parameters and secrets to be in the format specified above and writes it to `helm/values_generated.yaml` Each sub-parameter under `/config` is mapped accordingly. To give an example that combines both secrets and parameters (as the password comes out of the Secrets Manager):

`/dsm/mendix/apps/<app_name>/config/database/host`
`/dsm/mendix/apps/<app_name>/config/database/username`
`/dsm/mendix/apps/<app_name>/config/database/password`
`/dsm/mendix/apps/<app_name>/config/database/name`

Translates to:

```
database:
    host: myhost
```

```
    username: myuser
    password: mypassword
    name: myname
```

You can use this to your advantage to provide specific configuration parameters for specific use cases and specific applications. Always keep in mind that you will to take other apps into account when adding new parameters; add sane default values and make exceptions where needed.

SSM Parameter reference

This is an incomplete list of parameters. Note that it's incomplete because the assumption is made that parameters are added over time but this page not being kept up to date as they are added (hopefully this is proven wrong!)

Parameter	Description
/dsm/mendix/apps/<app_name>/config/aws/bucket_name	The name of the AWS bucket to use. Must be according to the naming convention of the bucket and as defined by the CDK codebase
/dsm/mendix/apps/<app_name>/config/aws/iam_access_key_id	The access key ID of the user. This gets automatically set and updated by the CDK code each time a deployment is done
/dsm/mendix/apps/<app_name>/config/database/username	The database user. If not set, this gets implicitly set by `generate_helm_values.py` (it is always the mendix app name)
/dsm/mendix/apps/<app_name>/config/database/host	The database host. If not set, this gets implicitly set by `generate_helm_values.py`. This then references the SSM parameter /dsm/mendix/db-1/host
/dsm/mendix/apps/<app_name>/config/database/name	The database name. If not set, this gets implicitly set by `generate_helm_values.py` (it is always the mendix app name)
/dsm/mendix/apps/<app_name>/config/ingress/certificate_arn	The ARN of the certificate. This gets created and set by the CDK

/dsm/mendix/apps/<app_name>/config/ingress/group_name	The Ingress group name. This is a way to share ALBs by grouping ingress objects to a specific ALB. Set this to a team name or any other value that makes sense to group objects with
/dsm/mendix/apps/<app_name>/config/ingress/http_headers	The HTTP headers which must be set on the nginx sidecar container of the Mendix application (so not the ingress object - this location may change in the future). This is important for CORS and other headers required by the Mendix application
/dsm/mendix/apps/<app_name>/config/ingress/waf_acl_arn	The ARN of the AWS WAF. If not set, no WAF is used
/dsm/mendix/apps/<app_name>/config/jvm/heapspace	The heap space of the Mendix application. By default this is 512MB
/dsm/mendix/apps/<app_name>/config/jvm/options	Any additional options to pass along to the JVM
/dsm/mendix/apps/<app_name>/config/mendix/clustering	Enable clustering mode in Mendix. This is only done in acceptance and production by default, but can be explicitly enabled / disabled per app here. If not set, no clustering is used.
/dsm/mendix/apps/<app_name>/config/mendix/sameSiteCookies	The sameSiteCookie setting for the Mendix Runtime. Can be None, Lose or Strict (None is the default)
/dsm/mendix/apps/<app_name>/vcs/url	The URL of the Mendix application. Must be a https://teamserver.sprintr.com or https://git.api.mendix.com URL
/dsm/mendix/apps/<app_name>/vcs/branch	The branch of the Mendix application to use. This must be set and no default is assumed.
/dsm/mendix/apps/<app_name>/vcs/revision	The SVN revision / Git commit hash as last seen by `mendix-vcs-polling`. This is the state on how the pipeline is being triggered.
/dsm/environment	The name of the environment. Must be dt, acc or prd

/dsm/public-zone-name	The FQDN of the public Route53 zone to use. Used to determine the FQDN of the Mendix applications
/dsm/public-zone-id	The ID of the public route53 zone. Used in automation.

Secrets manager reference

Some secrets are not following a path-style. This is done on purpose to indicate they are manually created and not created as part of automation. These are used by `generate_helm_values.py` as well.

Secret name	Description
/dsm/mendix/apps/<app_name>/config/aws/iam_secret_access_key	The secret access key for this app. Gets created and updated by the CDK each time the pipeline runs
/dsm/mendix/apps/<app_name>/config/mendix/mxadmin_password	The password to login as MxAdmin / dsmadmin in a Mendix application when local user authentication is enabled in the Mendix app
/dsm/mendix/apps/<app_name>/config/database/password	The password of the database user
mendix-license-key	The license key used for Mendix applications. Manually created and must exist on every environment.
azure-devops-token	The token used by `mendix-vcs-polling` to launch pipeline runs. Only used on the dev environment
mendix-service-account	The credentials and token for the Mendix service account. Used by `checkout_mendix_repo.py` to checkout the repository. Only used on the dev environment.