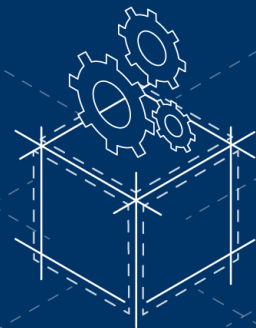


Container

AZURE - INSTALLATION & CONFIGURATION GUIDE



Contents

Introduction	3
Requirements.....	5
Step A – Deploy Clouddokit Container	6
Step 1 – Create a Storage Account and upload the license file.....	6
Step 2 – Create your container environment and start your container.....	7
Step B (Optional) – Configure Clouddokit Web UI	9
Step C (Optional) – Configure Clouddokit Container to support Scheduling.....	14
Start Clouddokit Scheduler Container.....	14
Set Settings in the settings file.....	14
Step D (Optional) – Configure Clouddokit Container to support the creation of Compliance Rules, Tailored Diagrams and Settings	15
Create (or re-use) an Azure Cosmos DB.....	15
Configure Clouddokit Container to use the Azure Comos DB.....	17
Step E – Understand Clouddokit API Container	18
Step F – Test your license.....	19
Activate and setup components for your license	19
Step G – Validate that you can authenticate to the environment that you want to scan	20
Step H – Test the document generation.....	22
Step I – Manage your document generation.....	23
/ListDocumentGeneration	23
/StopDocumentGeneration	23
Annex – Deploy multiple instances of Clouddokit Container.....	24
Step 1 – Create / Configure Azure Key Vault	25
Step 2 – Configure Azure Redis Cache	26
Step 3 – Define the Environment Variables required to run the Clouddokit Container	26
Annex – Troubleshooting.....	29

Introduction

The purpose of this document is to provide the detailed steps to run and configure Clouddokit Docker container images.

There are two types of images that you should run:

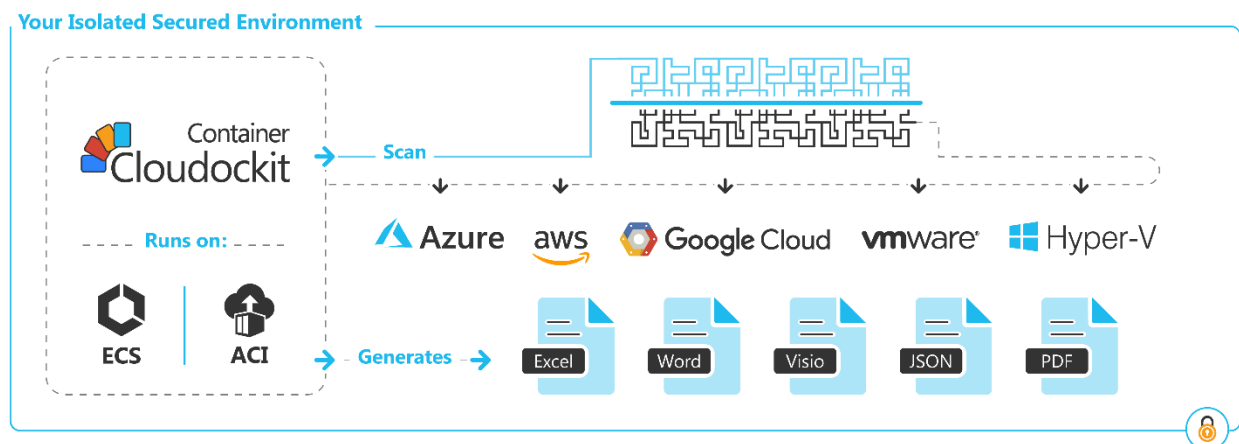
- **cdk-web-linux** that contains the Clouddokit API/Web interface. This is mandatory to run this container.
- **cdk-scheduler-linux** that contains the Clouddokit Scheduling features. This is an optional container you do not need to install if you do not want to use schedules.

The cdk-web image contains the Clouddokit API that you can call from your CI/CD processes or any other process / scenario which fits your business needs.

In addition to the API, we have integrated the complete Clouddokit Web UI in the image so that you can get all the features that you are accustomed to.

Clouddokit Docker container images provides you a way to run Clouddokit into your own isolated Cloud environment and gives you the exact same features as Clouddokit Website and Clouddokit Desktop.

Here is the high-level overview of the solution :



The following hosting environments are currently supported:

- Web App for Containers on Azure - Recommended
- ECS (Elastic Container Services) on AWS
- ACI (Azure Container Instance) on Azure
- GKE (Google Kubernetes Engine) on GCP

A few important things to note:

- These configurations are for the hosting of the container, not for the environment that you scan which means that you can scan a GCP project using the Clouddokit Container API even if the container runs on Azure.

- Depending on the hosting option that you choose, there could be some limitations. Those limitations are related to the hosting option and not the Cludockit Container itself.
- The current document does not detail networking configuration like isolation/https setup as this is highly dependent on your internal setup.
- Container is currently designed to have one node running which should be more than enough to generate all the documents you need.
- For production environment, we recommend 4vCPU + 8 Gb RAM
- Cludockit Web UI only supports Azure AD as SSO authentication. If you do not set it up, you will only be able to access the API portion.

The following sections contain the different steps to deploy the Cludockit Docker container image on the Azure Platform.

Here is an overview of the different steps you must do to deploy Cludockit Container:

Step A - Deploy Cludockit Container

- This Step is subdivided in 4 different steps
- Those steps have been scripted to ease the deployment process so we strongly advise to use the scripted approach

Step B (Optional) - Activate Cludockit Container UI

- Create an Azure AD Application

Step C (Optional) - Activate the Scheduling feature (cdk-scheduler)

- Set the appropriate settings to activate scheduling

Step D ... - Do some tests

- Test the license validity
- Start some documentation

Requirements

To install Clouddokit Container in your environment, you will need:

- A Storage Account
- An App Service or an Azure Container Instance to run the Container.
- (Optional) An Azure Active Directory Application if you want to activate Clouddokit Container Web UI

Important note

We highly recommend that you use the script (based on Azure CLI) provided by Clouddokit Team to provision the Clouddokit Container.

Step A – Deploy Cloudockit Container

Step 1 – Create a Storage Account and upload the license file.

To run Cloudockit Container, you need to have a Storage Account that will be used to store information (license file, settings...). As the license file is linked to this Storage Account, you need to choose a Storage Account Name (short name like *yourcompanycloudockit*) and send that name to Cloudockit Support Team (support@cloudockit.com) so that they generate a license file.

Once you receive your license file, you can upload the license file into a file named ***cloudockitinternal/license.json*** in the container.

Please note that the Json license file is tied to the storage account name so you need to create/use a storage account with a name that matches the name provided to Cloudockit Support Team.

Important note

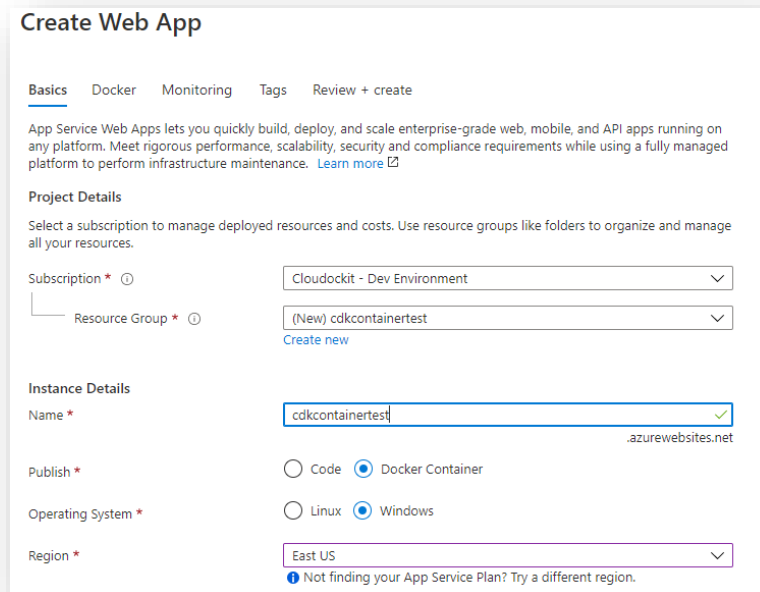
Ensure that the Storage Account exists in your environment before sending it to the Cloudockit Support Team.

The Json license file that you'll upload to your storage will be read by your Cloudockit Container when you start it. You will need to specify an Environment Variable / App Settings named `DockerStorageAzureCnxString` that will store a complete connection string to the storage account (cf. section below).

Step 2 – Create your container environment and start your container.

Once you have created your Storage Account, you need to create your container environment and start the container.

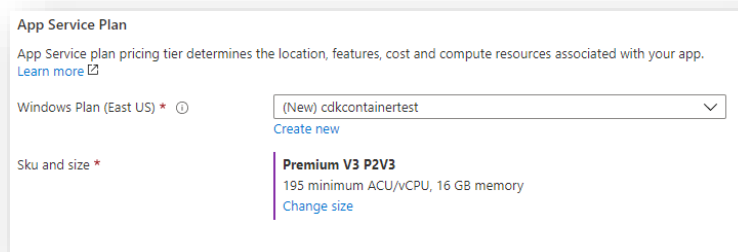
First, create a new Web App for Containers instance:



The screenshot shows the 'Create Web App' form in the Azure portal. The form has tabs for 'Basics', 'Docker', 'Monitoring', 'Tags', and 'Review + create'. The 'Basics' tab is selected. Below the tabs, there is a brief description of App Service Web Apps. The 'Project Details' section includes a 'Subscription' dropdown set to 'Clouddokit - Dev Environment' and a 'Resource Group' dropdown set to '(New) cdkcontainertest'. The 'Instance Details' section includes a 'Name' field with 'cdkcontainertest', a 'Publish' section with 'Docker Container' selected, an 'Operating System' section with 'Linux' selected, and a 'Region' dropdown set to 'East US'. A note at the bottom of the 'Region' section says 'Not finding your App Service Plan? Try a different region.'

Ensure that you have selected **Docker Container** and Linux for the Operating System.

Then create a new App Service Plan:



The screenshot shows the 'App Service Plan' form in the Azure portal. The form has a title 'App Service Plan' and a brief description. The 'Windows Plan (East US)' dropdown is set to '(New) cdkcontainertest'. The 'Sku and size' section shows 'Premium V3 P2V3' with '195 minimum ACU/vCPU, 16 GB memory' and a 'Change size' link.

Then, in the Docker Tab, select Private Registry and enter the following information:

Name	Value
Server URL	https://clouddockitcontainerregistry.azurecr.io
User Name	User provided by Clouddockit Team
Password	Password provided by Clouddockit Team
Image and Tag	clouddockitcontainerregistry.azurecr.io/cdk-web-linux:latest (linux)
Startup Command	Leave empty

Then, click on **Review+Create** and proceed.

Once done, you need to navigate to the Application Settings of the App Service that you have created and enter the following values:

Name	Value
WEBSITE_MEMORY_LIMIT_MB	Amount of RAM (in MB) that you have in your App Service Plan (1 GB is 1024) Minimum value is 2048 , recommended value is 4096
AppInsightKey (optional)	An Azure App Insight Instrumentation Key for advanced login
DockerStorageCloudProvider	Specify if your Storage Account is stored in Azure, AWS or GCP. Possible values are: <ul style="list-style-type: none">• Azure• GCP• AWS
DockerStorageAzureCnxString	Enter the complete connection string (Full access) of the Storage Account.
AuthenticationEndPoint (optional)	Specify if you want to use a different Azure endpoint. Possible values are: <ul style="list-style-type: none">• gov• de• cn Leave empty for default endpoint (Global).

Step B (Optional) – Configure Clouddokit Web UI

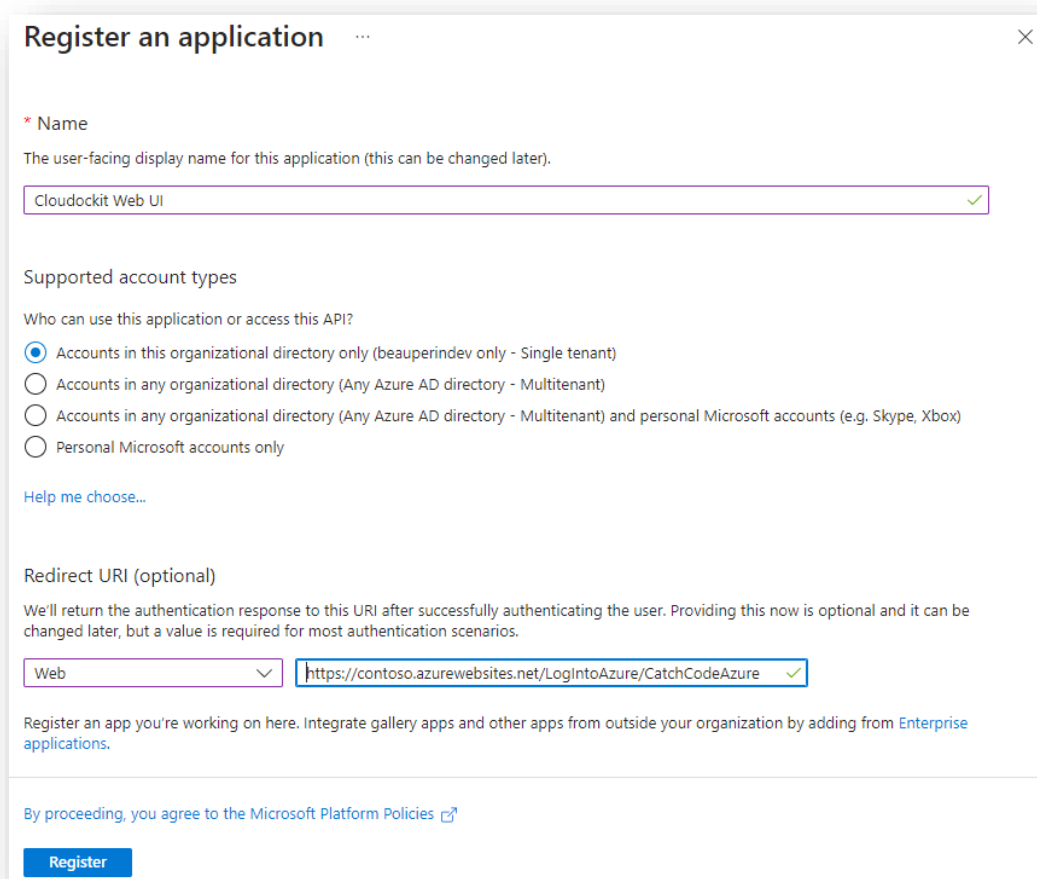
Clouddokit Container supports a Web UI that allows users to authenticate by using Azure AD or Azure User Authentication.

This Web UI supports Azure Active Directory as a first step to authenticate users.

Once connected, you will be able to connect to Azure, AWS and GCP using Service Accounts (Azure AD App, GCP Service Credentials, AWS Access Keys).

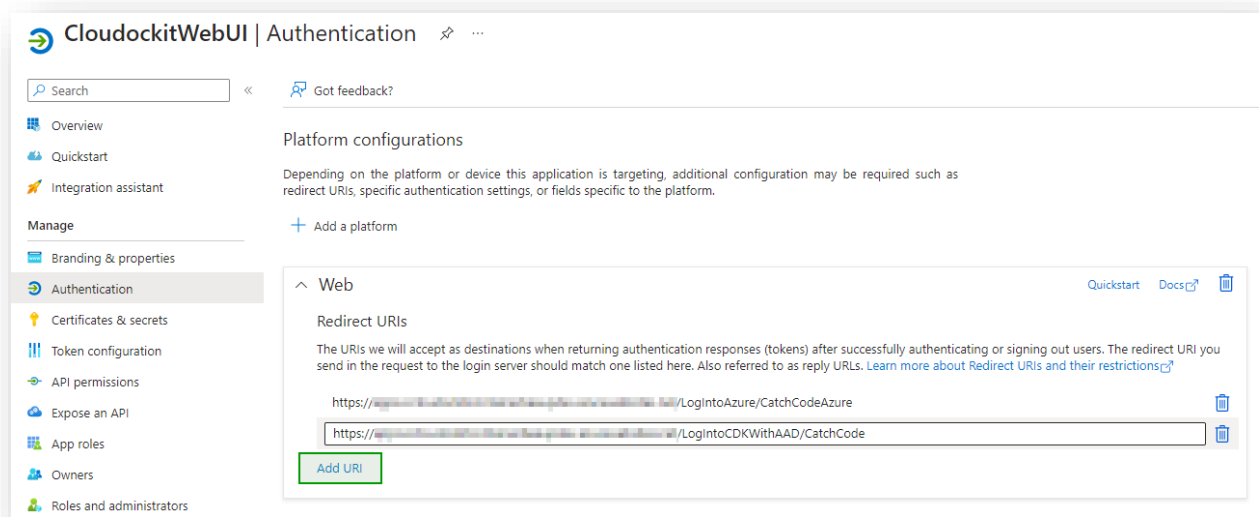
To activate Azure AD Authentication, you need to follow these steps:

- Go to your **Azure Active Directory**
- Click on **App Registration** and then click **New Registration**
- Enter a **Name** (any name you want) and select **Single Tenant**
- Enter the following **redirect URIs** (reply url):
 - `https://<AppSvcName>.azurewebsites.net/LogIntoAzure/CatchCodeAzure`
 - `https://<AppSvcName>.azurewebsites.net/LogIntoCDKWithAAD/CatchCode`where *AppSvcName* is the name of your App Service



The screenshot shows the 'Register an application' dialog in the Azure portal. The dialog has a title bar with a close button. The main content area is divided into sections. The first section is 'Name', with a label '* Name' and a description 'The user-facing display name for this application (this can be changed later)'. Below this is a text input field containing 'Clouddokit Web UI' and a green checkmark icon. The second section is 'Supported account types', with a label 'Supported account types' and a description 'Who can use this application or access this API?'. Below this are four radio button options: 'Accounts in this organizational directory only (beauperindv only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. Below these options is a link 'Help me choose...'. The third section is 'Redirect URI (optional)', with a label 'Redirect URI (optional)' and a description 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.'. Below this is a dropdown menu set to 'Web' and a text input field containing 'https://contoso.azurewebsites.net/LogIntoAzure/CatchCodeAzure' with a green checkmark icon. Below the input fields is a link 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.'. At the bottom of the dialog is a footer with the text 'By proceeding, you agree to the Microsoft Platform Policies' and a link to the policies. Below the footer is a blue button labeled 'Register'.

Note: the interface will not let you enter the 2nd URL before clicking on **Register** so you'll have to enter it after registration, in the Authentication page:




Then, go to **API Permissions**, click on **+Add a permission** and select :

- **Microsoft Graph**, then **Delegated permissions** and then select **User.Read**:
- **Azure Service Management**, then **Delegated permissions** and then select **user_impersonation**:

Request API permissions

< All APIs

 Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
> IdentityRiskyUser	
✓ User (1)	
<input checked="" type="checkbox"/> User.Read ⓘ Sign in and read user profile	No
<input type="checkbox"/> User.Read.All ⓘ Read all users' full profiles	Yes
<input type="checkbox"/> User.ReadBasic.All ⓘ Read all users' basic profiles	No
<input type="checkbox"/> User.ReadWrite ⓘ Read and write access to user profile	No

Add permissions

Discard

Click **Add permissions**. You should now see the following :

[Refresh](#) | [Got feedback?](#)

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, and user consent will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for UMAknow Solutions DEV Inc](#)

API / Permissions name	Type	Description	Admin consent req...
▼ Azure Service Management (1)			
user_impersonation	Delegated	Access Azure Service Management as organization use...	No
▼ Microsoft Graph (2)			
User.Read	Delegated	Sign in and read user profile	No

To view and manage permissions and user consent, try [Enterprise applications](#).

Then, click on **Grant Admin consent** for Default Directory (if you don't have the permissions to click on **Grant admin consent**, please contact your IT admin to do it for you):

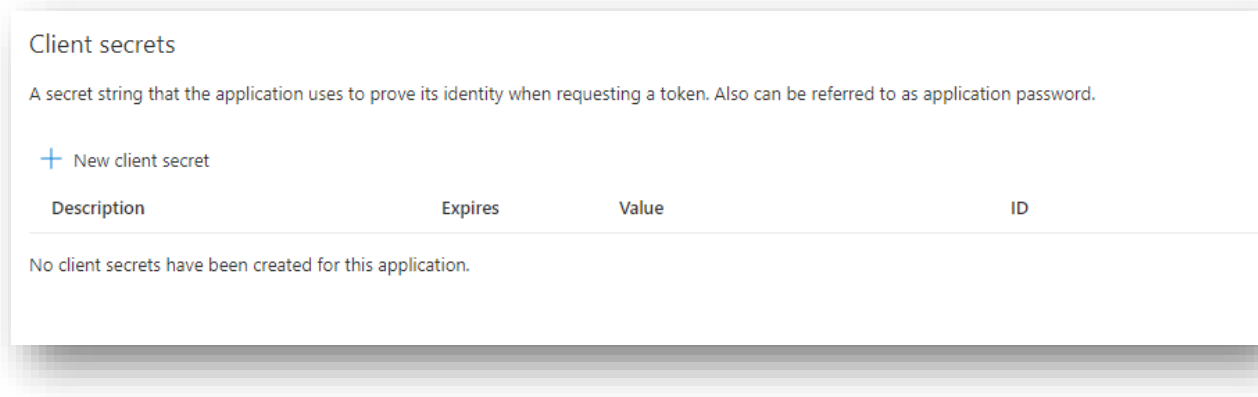
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for Default Directory](#)

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (2)				...
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for Default Dire... ...

Then, take note of the client ID from the Overview tab and then go to **Certificates & Secrets** and generate a new Client Secret, take note of it.



Update the settings file from your storage account (in the clouddockitinternal folder) with the value of the previously created Azure AD Application:

```
{  
  "AzureADTenant": "mytenant.onmicrosoft.com",  
  "AzureADAppID": "zzzzz",  
  "AzureADAppKey": "zzzzz"  
}
```

Step C (Optional) – Configure Clouddokit Container to support Scheduling.

Clouddokit Container supports a Scheduling Web UI that allows users to choose when they want to schedule the document generation.

To activate scheduling, you need to spin-up a new container based on the **clouddokitscheduler** image and set the appropriate settings in your settings file.

Start Clouddokit Scheduler Container

You need to follow the same procedure as you did in the previous step to spin up a new Scheduling container. You need to use the **clouddokitscheduler** image. This scheduler is basically reading the schedules files created from the UI and calling the API according to the schedule.

Here are the settings for the container:

- CPU : 1+
- RAM : 1.5GB+
- No inbound networking is required
- Outbound networking needs access to the storage account where the settings are stored and the API URL where Clouddokit is deployed.
- The following 3 environment variables are required:

Name	Value
DockerStorageCloudProvider	Specify if your Storage Account is stored in Azure, AWS or GCP. Possible values are: <ul style="list-style-type: none">• Azure (select this value)• GCP• AWS
DockerStorageAzureCnxString	Enter the complete connection string (Full access) of the Storage Account.
DockerUrlForSchedulingStarts	Enter the URL of your API that hosts Clouddokit like: <code>https://testcdkapi.azurewebsites.net/</code>

Set Settings in the settings file

To activate the scheduling, you need to update the settings file from your storage account (in the *clouddokitinternal* folder) to specify the URL of your Clouddokit Container:

```
{  
  "DockerUrlForSchedulingStarts" : "https://myclouddokitcontainer"  
}
```

This information will be used by Clouddokit Scheduling feature to specify which Web API to call.

Note: the **Scheduling** menu will only appear in the interface if you login with an App Registration.

Step D (Optional) – Configure Clouddokit Container to support the creation of Compliance Rules, Tailored Diagrams and Settings

Clouddokit Container supports the creation of new Compliance Rules, new Tailored Diagram and new Settings.

This feature requires that you deploy an Azure Cosmos DB to save the Compliance Rules and Tailored Diagrams.

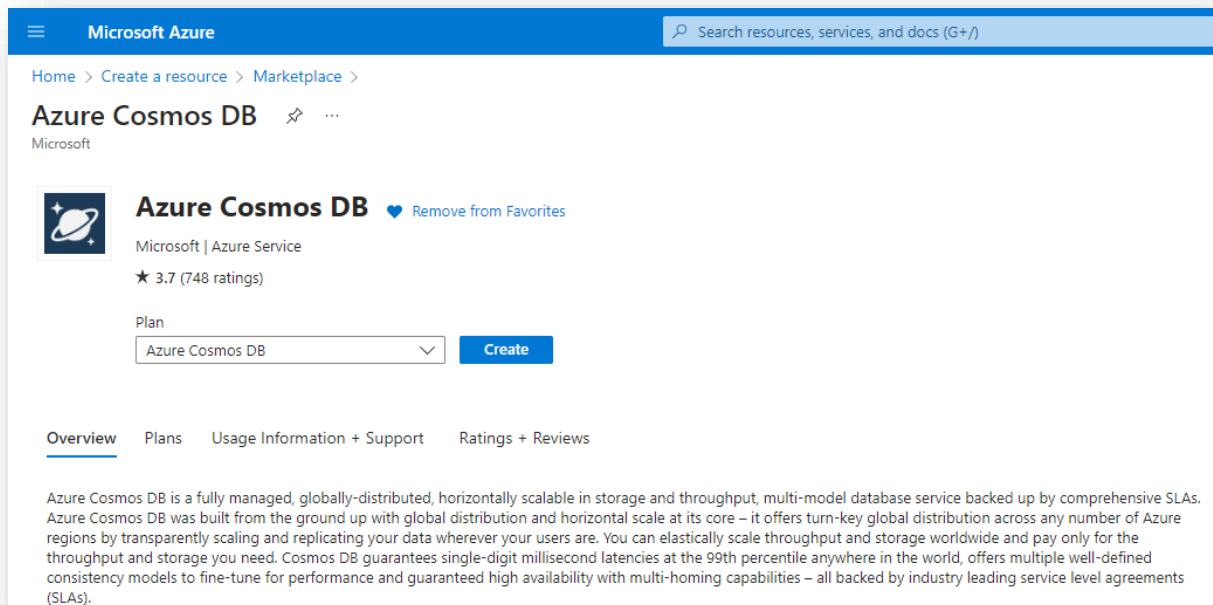
There are two steps required:

- Create (or re-use) an Azure Cosmos DB
- Add environment variables to the Clouddokit Container to specify which Azure Cosmos Database to use

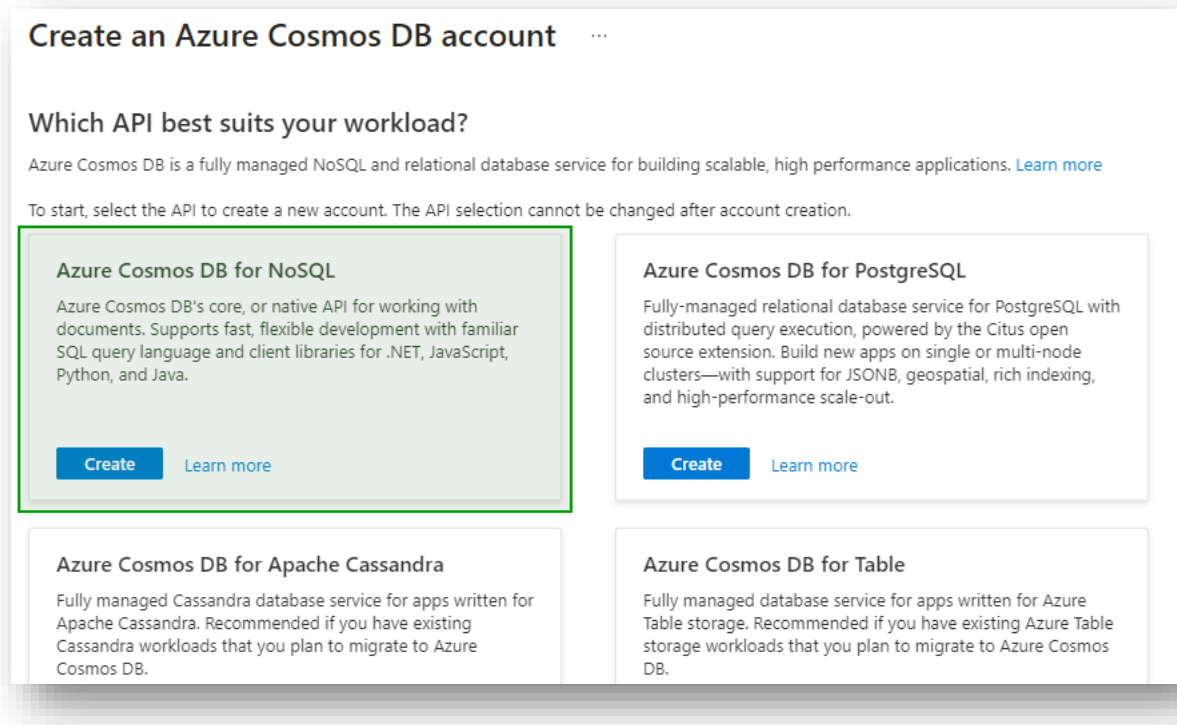
Create (or re-use) an Azure Cosmos DB

From the Azure Portal, create a new Cosmos DB: (you can skip those steps if you already have a Cosmos DB that you want to reuse)

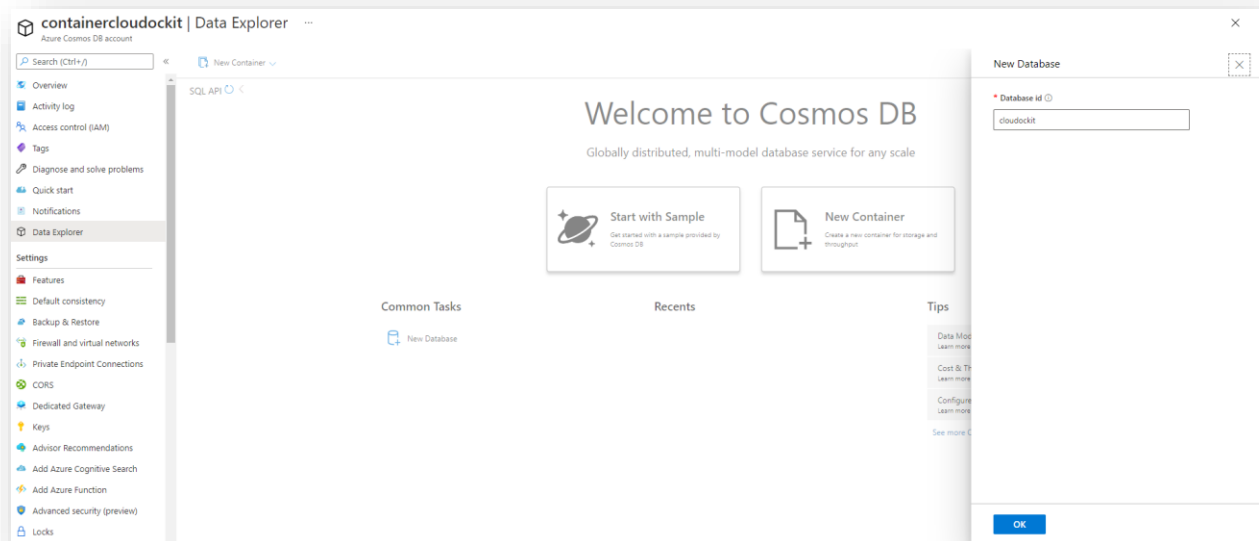
- Create a Cosmos DB



- Choose Azure Cosmos DB for NoSQL for the type



Once the Cosmos DB is created, you need to create a new Database named **clouddokit** :



Configure Clouddockit Container to use the Azure Cosmos DB

To ensure that the container can connect to the Database, you need to start the container and specify the following 2 required environment variables:

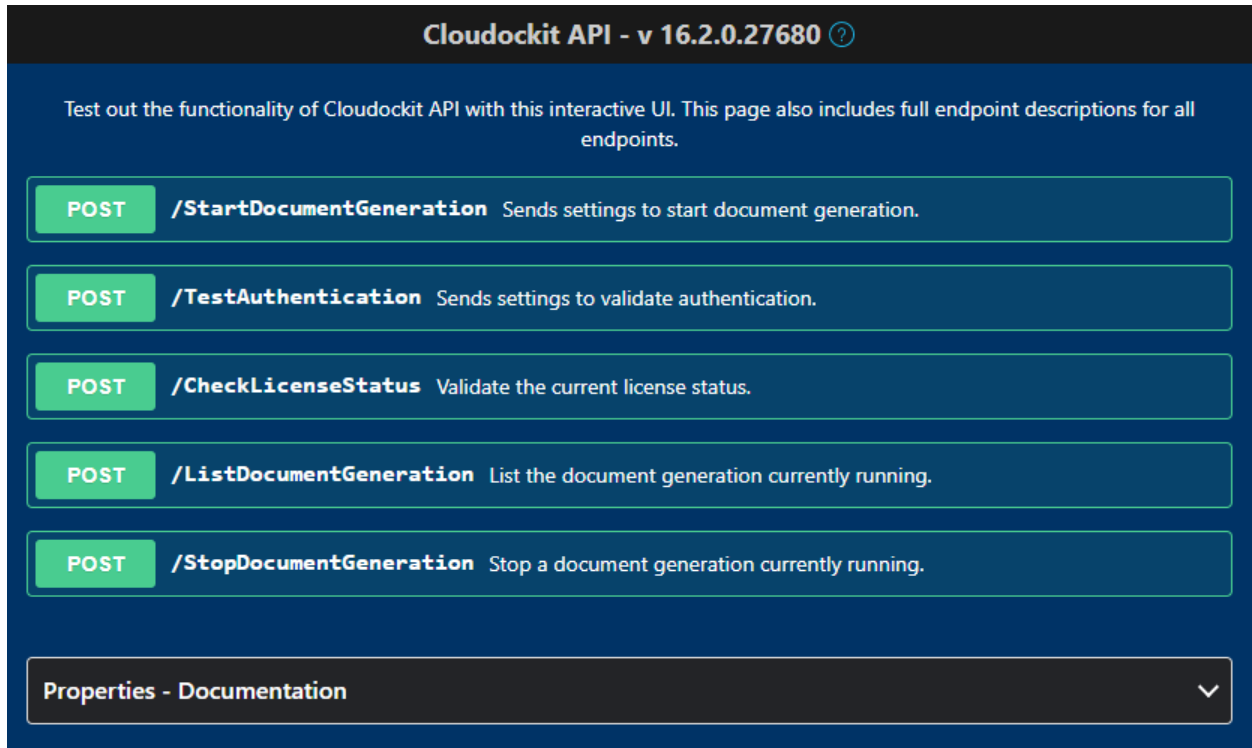
Name	Value
CosmosDb__DatabaseName	Enter the name of the Database that you have created in the previous step (clouddockit in the example)
ConnectionStrings__CosmosDb	Azure CosmosDB Connection string

Step E – Understand Clouddokit API Container

Once you have installed the Clouddokit Container, you can navigate to the Container Home Page and you will see the following screen.

It gives you the option to test the different endpoints offered by Clouddokit API.

Please note that you can do everything from command lines/scripts and not use the interface if you prefer.



For simplicity of usage, all the endpoint are POST endpoints. Not all settings are mandatory for each endpoint and you can refer to that section to see which endpoints require which parameters.

Step F – Test your license

Activate and setup components for your license

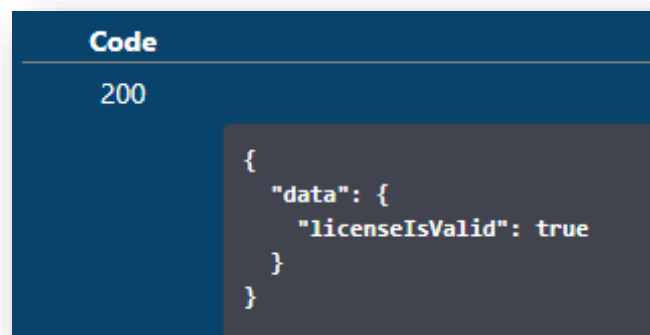
Once you get the API Key from Clouddokit team and you have the appropriate credentials for the license validation, you can check that your API Key is working by using the **/CheckLicenseStatus** endpoint.

First, navigate to the home page of the container and click on **CheckLicenseStatus** and Try it now. Then, replace the following values in the JSON that you are sending to Clouddokit API:

```
{
  "ApiKey": "API Key provided by Clouddokit Team"
}
```

Click on Execute.

You should receive the following response body:



Step G – Validate that you can authenticate to the environment that you want to scan

Once the license validation is successful, you need to test that the authentication to the environment you want to scan is working.

To do that, you need to use the `/TestAuthentication` endpoint.

First, you need to ensure that you specify the values from the above Step 2 for license validation.

Then, you need to specify the following additional values:

Name		Value
ADKCloudType		Azure/AWS/GCP depending on the platform that you want to scan.
SubscriptionID		Id/Alias of the subscription (Azure) or account (AWS) or project (GCP) that you want to scan.
(for AWS)	AWSAccessKeyId	AWS Access Key
	AWSSecretAccessKey	AWS Secret Access Key
(for Azure)	TenantID	Tenant name of the Azure Subscription to scan
	AppClientIdForAutomation	AAD App ID for the scan
	AppClientKeyForAutomation	AAD App Key for the scan
(for GCP)	GCPServiceAccountCredentials	Content of the JSON Service Credential file
AzureStorageNameForDropOff		Do not change the name of the parameter for AWS, this is also called AzureStorageNameForDropOff You should specify <u>one</u> of these values: <ul style="list-style-type: none">the Azure Storage Account Name (it can be the unique Storage Account name that is in the same tenant as the subscription that you scan <i>or</i> the complete Azure Storage Account Connection String)AWS S3 bucketGCP Bucket where Clouddokit should store the documents generated.

Example of Payload for an AWS environment scan:

```
{
  "ApiKey": "xxxx",
  "AWSAccessKeyId": "XXXX",
  "AWSSecretAccessKey": "8PoBo+4XXXX+/k/MzQ",
```

```

    "SubscriptionID": "34XXXX2",
    "AzureStorageNameForDropOff": "XXXdockit",
    "ADKCloudType": "AWS"
}

```

Example of Payload for an Azure environment scan:

```

{
  "ApiKey": "xxxx",
  "TenantID": "X2.onmicrosoft.com",
  "AppClientIdForAutomation": "XXXXX",
  "AppClientKeyForAutomation": "mln/XXXXX=",
  "SubscriptionID": "XXX",
  "AzureStorageNameForDropOff": "XXX",
  "ADKCloudType": "Azure"
}

```

Example of Payload for an GCP environment scan:

```

{
  "ApiKey": "xxxx",
  "GCPServiceAccountCredentials": {"type":
    "service_account", "project_id": "cdkXXXX", "private_key_id":
    "XXXXX", "private_key": "-----BEGIN PRIVATE KEY-----
    nMIIEvQIXXXXXZGy5PArVQS"n2buDji0URXCkoeWnukG9Cl0fHlP8rFK6+XXXXXX+kJm0Y
    xuFOWxdbgpSln38mQyez7EK"nObnp9wP05ynOxKXJqJx0r1k="n-----END PRIVATE
    KEY-----"n", "client_email":
    "XXXX@cdkproject1.iam.gserviceaccount.com", "client_id":
    "XXXXX", "auth_uri":
    "https://accounts.google.com/o/oauth2/auth", "token_uri":
    "https://oauth2.googleapis.com/token", "auth_provider_x509_cert_url"
    :
    "https://www.googleapis.com/oauth2/v1/certs", "client_x509_cert_url":
    "https://www.googleapis.com/robot/v1/metadata/x509/test-
    XXXX.iam.gserviceaccount.com"}, "SubscriptionID": "XXXX",
    "AzureStorageNameForDropOff": "XXXX",
    "ADKCloudType": "GCP"
}

```

Step H – Test the document generation

Once all the tests above have been done, you can start the document generation.

To do that, you need to use the `/StartDocumentGeneration` endpoint.

First, you need to ensure that you specify the same values as the above steps for `CheckLicenseStatus` and `TestAuthentication` endpoints.

Then, you need to specify additional values based on the type of document you want to generate and which option you would like to use.

You get a list of all options from the properties list at the bottom of the screen:

Properties - Documentation					
Show 10 entries		Search:			
Category	Title	Internal Name to use	Description	Type	Value must be one of the following
Authentication	GCP Service Account JSON Credentials	GCPServiceAccountJSONCredentials	Specify the Service Account JSON credentials to use. This is mandatory when using the API for GCP	String	
Authentication	Tenant ID	TenantID	Specify your Azure Active Directory Tenant ID	String	
Authentication	Azure AD Application Client ID	AppClientIdForAutomation	Specify the AAD App Client ID to use for the authentication. This is mandatory when using the API for Azure	String	
Authentication	Azure AD Application Secret Key	AppClientKeyForAutomation	Specify the AAD App Secret Key to use for the authentication. This is mandatory when using the API for Azure	String	
Authentication	AWS Access Key ID	AWSAccessKeyId	Specify the AWS Access Key ID to use. This is mandatory when using the API for AWS	String	
Authentication	AWS Secret Access Key	AWSSecretAccessKey	Specify the AWS Secret Access Key to use. This is mandatory when using the API for AWS	String	
Authentication	License Code	LicenseCode	Specify your license code	String	
Billing	Dataset that contains the billing data	GCPBigQueryDataSet	Specify the name of the BigQuery Dataset that contains billing data	String	
Billing	Table that contains the billing data	GCPBigQueryTable	Specify the name of the BigQuery Table that contains the billing data.	String	
Billing	Billing Type	BillingOfferID	Specify the type of billing to use (Standard, EA or CSP)	String	
Showing 1 to 10 of 296 entries				Previous	1 2 3 4 5 ... 30 Next

As there are many options that you can provide, we strongly advise that you use Clouddokit Website to generate the JSON file with the options.

One of the options that is particularly useful in this scenario are the `CallbackURL` and `CallbackUrlRequired` parameters that gives you the ability to be notified once document generation have been done.

When you hit Execute, you get the state URL of the current document generation:

Server Response	
Code	Details
202	<div>Response body</div> <pre>{ "data": { "stateUrl": "https://amazondockit.s3.us-west-2.amazonaws.com/3408512af03d8fcfe32-state.json?X-Amz-Expires=172800&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA647780789684405620201102T192525Z&X-Amz-SignedHeaders=host&X-Amz-Signature=5a37e76cf072a0266fa28ff423207f01c0fb494b7b37e802694fd5b035ba2fb4", "processId": 8420 }, "message": "Documentation generation was successfully started" }</pre>

For Payload example, you can simply re-use the previous ones.

Step I – Manage your document generation

The Clouddokit API offers two endpoints to facilitate the management of document generation.

Please note that for these endpoints, you need to specify an Admin API Key for the ApiKey value.

[/ListDocumentGeneration](#)

This will allow you to see which scans are running. It gives you the list of running processes with their Process ID and State:

Server Response	
Code	Details
202	<div>Response body<div><pre>{ "data": { "processes": [{ "stateURL": "https://amazondockit.s3.us-west-2.amazonaws.com/s3/aws4_request&X-Amz-Date=20201102T192525Z&X-Amz-SignedHeader= "processID": 8420 }] } }</pre></div></div>

[/StopDocumentGeneration](#)

This endpoint is used to kill a running document generation.

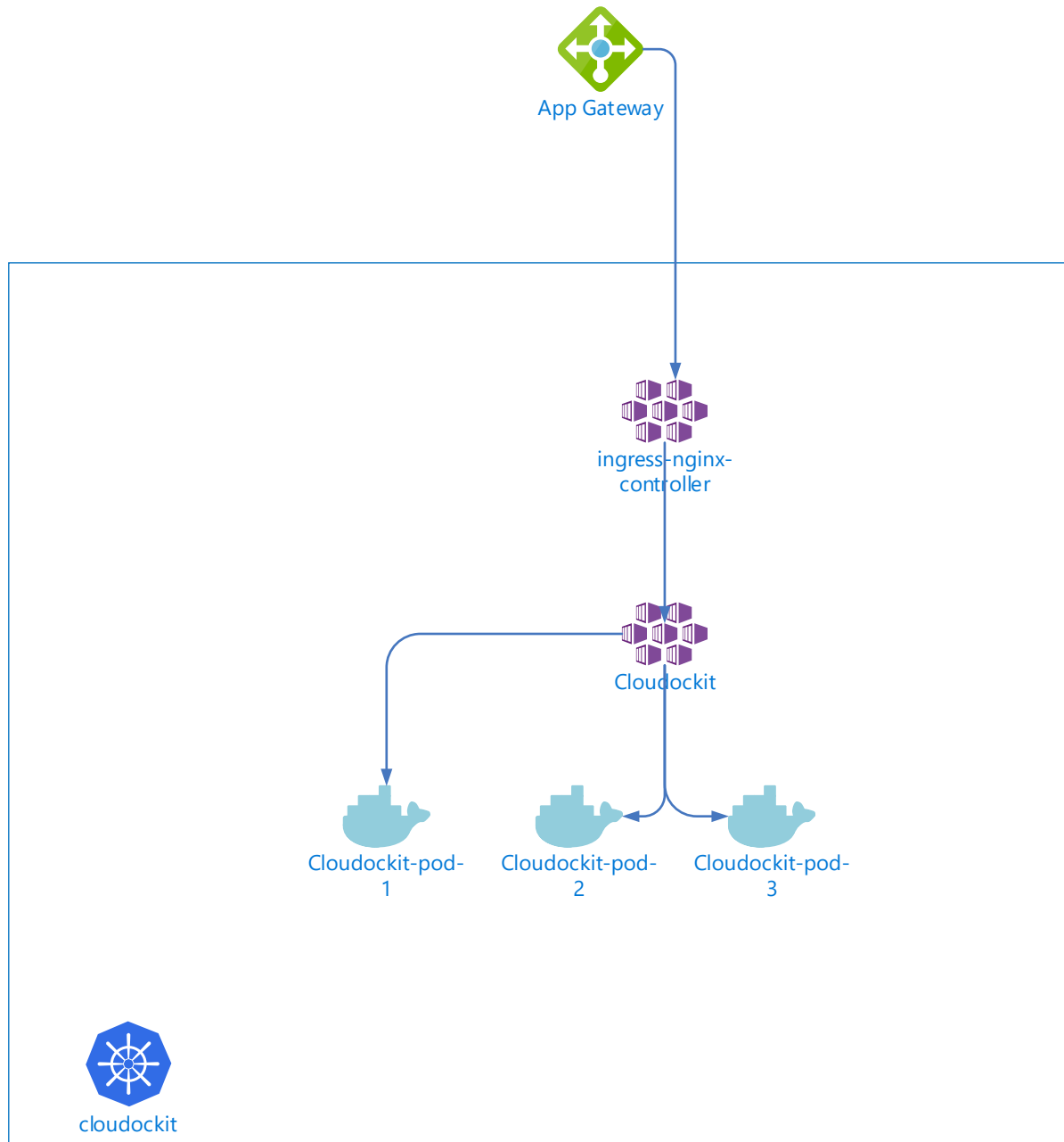
Name	Value
DockerProcessToKill	Value of the process ID to kill

It will reply with a confirmation message that the process has been killed.

Server Response	
Code	Details
202	<div>Response body<div><pre>{ "data": { "processKilled": true }, "message": "Process was killed" }</pre></div></div>

Annex – Deploy multiple instances of Clouddokit Container

Clouddokit can be deployed in multiple instances in scenarios like this one:



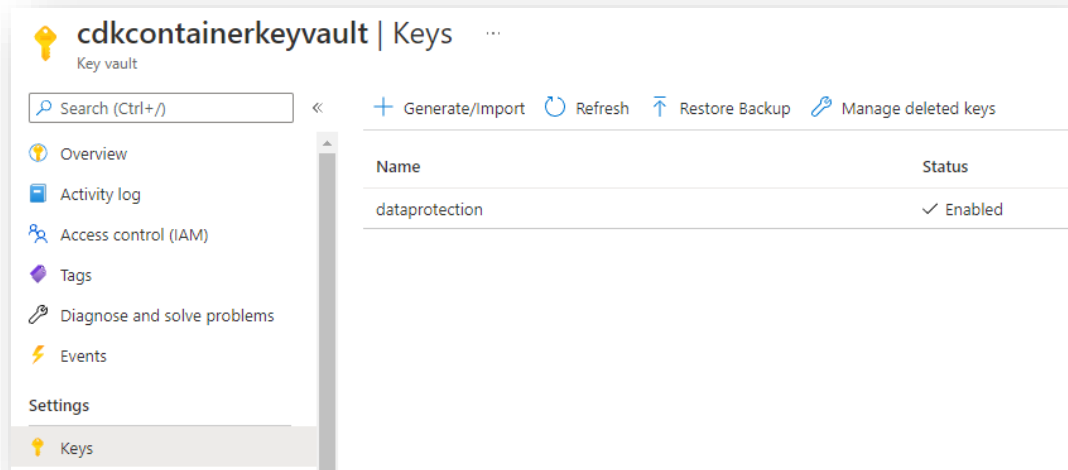
If you plan to use Clouddokit Container in a multi-pods environment, you need to configure some extra components. If you plan to use Clouddokit Containers in multiple instances with sticky session (for example App Services with a Traffic Manager), you do not need those extra components.

Here are the components that you need to configure.

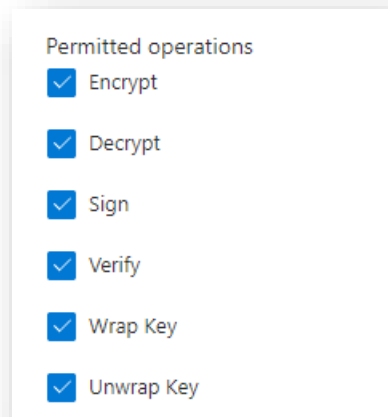
Step 1 – Create / Configure Azure Key Vault

To encrypt the anti-forgery keys used by ASPNETCore, an Azure Key Vault is required. You can create a new Azure Key vault or reuse an existing one.

Once you have the Azure Key Vault, you need to create a Key named **dataprotection**



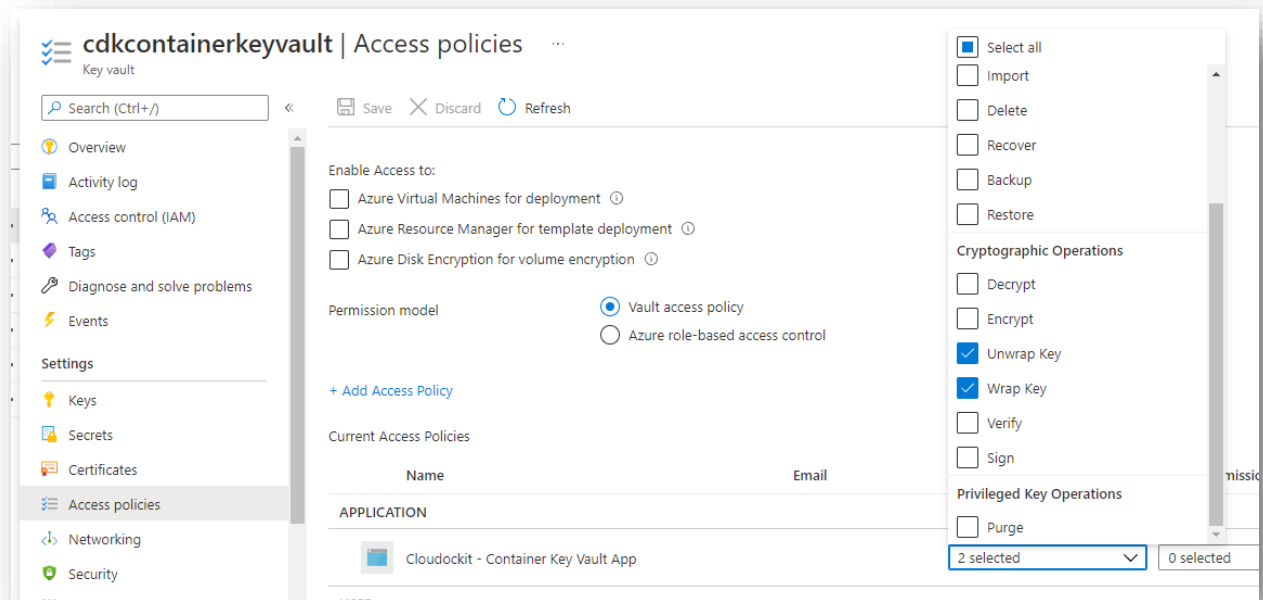
Please ensure that the Key have the following Permitted Operations (by default permissions)



Once you have done that, you need to create an Azure App Registration that will have access to this key. (you can also reuse the Azure AD App that you have created in the steps to configure Clouddockit Web UI if you prefer)

To do that, create a new App Registration (leave default settings) and note the Client ID and Client Secret as you will need that in the next steps.

Go back to the Azure Key Vault and give the Permissions to Unwrap Key / Wrap Key to the App that you just created



Step 2 – Configure Azure Redis Cache

As sessions can sprawl to multi pods, Azure Redis Cache is required to have consistent cache across all nodes.

Create a new Azure Cache for Redis (you can also reuse an existing one if you prefer) and select the Basic CO (250MB Cache) as only small elements will be cached. Ensure that you select a region that is close to the one where Clouddokit will run for performance optimization.

Once created, take note of the Redis Connection String.

Step 3 – Define the Environment Variables required to run the Clouddokit Container

In addition to the environment variables defined in the step above, you now need to add the following environment variables.

Name	Description	Example
DataProtection__EncryptionKeyUrl	URL of the key vault Key that you have created. You need to specify the Full Path to the key , not only the key vault.	https://cdkcontainerkeyvault.vault.azure.net/keys/data-protection
DataProtection__VaultClientId	Id of the Azure AD App that has privileges to Wrap / Unwrap key	760fb963-57a4-2303-1450-1b2dab513854

DataProtection__VaultSecret	Secret of the Azure AD App	SF7Q~NvuAYKF6.IB Fjdewdewd
CacheSettings__UseRedis	Set to true to use redis instead of memory cache	true
ConnectionStrings__Redis	Connection String to the Redis	cdkmultipods.redis .cache.windows.ne t:6380,password=x x=,ssl=True,abortC onnect=False

For reference, here is a sample yaml file to deploy that configuration

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: clouddockit
spec:
  replicas: 4
  selector:
    matchLabels:
      app: clouddockit
  template:
    metadata:
      labels:
        app: clouddockit
    spec:
      containers:
        - name: clouddockit
          image: cdkmultipods.azurecr.io/cdk-web-linux:dev
          ports:
            - containerPort: 80
          env:
            - name: DockerStorageCloudProvider
              value: "Azure"
            - name: "DockerStorageAzureCnxString"
              value:
                "DefaultEndpointsProtocol=https;AccountName=clouddockitcontainerdebug;AccountKey=xxx==;EndpointSuffix=core.windows.net"
            - name: AzureADTenant
              value: "umaknowdev.onmicrosoft.com"
            - name: AzureADAppID
              value: "9548a025-xxxx"
            - name: AzureADAppKey
              value: "W6UXfqC~xxxx"
            - name: Data__ProtectionEncryptionKeyUrl
```

```

        value:
"https://cdkcontainerkeyvault.vault.azure.net/keys/dataprotection"
      - name: DataProtection__VaultClientId
        value: "760fb9xxxx"
      - name: DataProtection__VaultSecret
        value: "VSF7xxxx"
      - name: CacheSettings__UseRedis
        value: "true"
      - name: ConnectionStrings__Redis
        value:
"cdkmultipods.redis.cache.windows.net:6380,password=xxxxk9g=,ssl=True,abortConnec
t=False"
      - name: APPINSIGHTS_INSTRUMENTATIONKEY
        value: "c07069xxxx"
      - name: TriggerDeployCount
        value: "5"
---
apiVersion: v1
kind: Service
metadata:
  name: cloudockit
spec:
  type: ClusterIP
  ports:
    - port: 80
  selector:
    app: cloudockit

```

Annex – Troubleshooting

Here are resolutions to common cases and how you can help find errors in Clouddokit Container.

- If you activate Clouddokit Container Web UI and noticed that in the upper right corner you have a Welcome message without your name, please check the AAD Credentials in the settings file
- If you are using Private endpoint for your App Service and Storage, please ensure that you activate vNET integration so that the App Service can communicate with the Storage Account
- You can specify an environment variable in your container named `AppInsightKey` that contains an Azure App Insight Instrumentation key so that you can see the logs.
- You can use the `-logs.txt` file in the storage that you have specified to see what is happening during document generation.
- If you get an error when the document generation starts, please ensure that you have Write privileges to your storage account
- If you see the message that the document generation is starting but do not see any progress, please verify that you have a CORS rule for GET Verb and origin that is your Clouddokit container website (should be done automatically).
- If you get an exception when starting the container that says “APPCMD failed with error code 87”, check that the variables that you are providing do not contain quotes.