

Clouddockit's Optimal Setup - Enterprise - AWS

Before you start, let us help you navigate all of the steps to Clouddockit Optimal Setup. Simply book a call with one of our experts.

[Book a call](#)

Introduction

The purpose of this document is to provide the detailed steps to install and configure Clouddockit Desktop in an optimal way so you can get going as quickly as possible with your automated documentation generation for your AWS environment.

Clouddockit desktop can be installed in many ways. On a workstation, on a server, on a virtual machine.

Based on our experience we have identified that the optimal way is to create an EC2 instance and install Clouddockit desktop to automate your document generation.

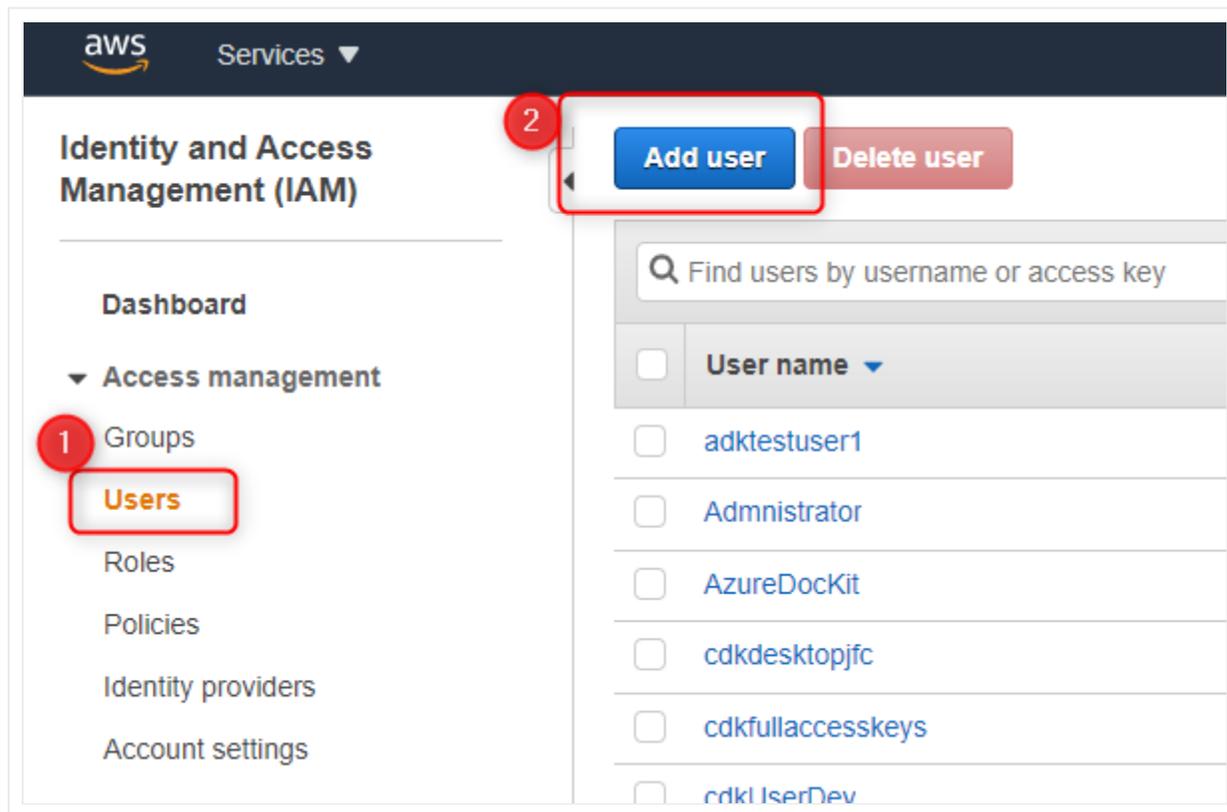
Step 1 – Create the IAM User

Your chosen IAM User will be used to list all of the accounts in the organization to enable Clouddockit Desktop to loop through the accounts and assume roles in each of them.

Create the User

Sign in to the AWS Console and open the IAM console: [Amazon IAM](#)

In the navigation panel, choose **Users**, press **Add** user.



Set User details and Select AWS access type

Enter a name

In Access Type, check **Programmatic access**

Click: Permissions

Add user



Set user details

You can add multiple ¹ users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these ² users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

- Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

Cancel **Next: Permissions**

Create the Policy

Select **Attach existing policies directly**.

Click: Create Policy

Add user

1 2 3 4 5

▼ Set permissions

Copy permissions from **Attach existing policies**

2  Add user to group

 existing user

 directly

Create policy



Filter policies   Search

Showing 646 results

	Policy name 		Used as
<input type="checkbox"/>	 accessToUmaknowAccount	Customer managed	Permissions policy (1)
<input type="checkbox"/>	 adkpascaltest1	Customer managed	None
<input type="checkbox"/>	 AdministratorAccess	Job function	Permissions policy (23)
<input type="checkbox"/>	 AlexaForBusinessDeviceSetup	AWS managed	Boundary (1)
<input checked="" type="checkbox"/>	  AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	 AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	  AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	 AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None

▶ Set permissions boundary

Cancel

Previous

Next: Tags

Make the following selections:

- In Service, select **Organizations**
- In action, select **Access Level / List Accounts and ListAccountsForParent**
- In Resources, select **All resources**

Click: Review Policy

Create policy

1

2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

[Expand all](#) | [Collapse all](#)

▼ Organizations (2 actions)

[Clone](#) | [Remove](#)

1 ▶ Service Organizations

2 ▶ Actions List
ListAccounts
ListAccountsForParent

3 ▼ Resources Specific
[close](#) All resources

As a best practice, define permissions for only specific resources. Alternatively, you can grant least privilege using condition keys.

[Learn more](#)

▶ **Request conditions** [Specify request conditions \(optional\)](#)

[+ Add additional permissions](#)

Character count: 172 of 6,144.

Cancel

Review policy

Give your Policy a unique name and press **Create Policy**.

Create policy

1

2

Review policy

Name*

Use alphanumeric and '+=, @-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Summary

Q Filter			
Service ▾	Access level	Resource	Request condition
Allow (1 of 241 services) Show remaining 240			
Organizations	Limited: List	All resources	None

* Required

Cancel

Previous

Create policy

Close the opened tab to create the new policy.

Go back to the user creation screen and refresh the list.

Select the newly created policy

Click: Tags

Add user

- 1
- 2
- 3
- 4
- 5

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Create policy

1



Filter policies ▼

cdk

Showing 5 results

	Policy name ▼	Type	Used as
<input type="checkbox"/>	▶ CDK-NoPermissionCostAndUsageReport	Customer managed	None
<input checked="" type="checkbox"/>	▶ cdkCostExplorerServiceMissingPermissions	Customer managed	Permissions policy (1)
<input type="checkbox"/>	▶ CDKOptimalMultipleAccountPolicy	Customer managed	None
<input type="checkbox"/>	▶ CDKOptimalSetupPolicy	Customer managed	None
<input type="checkbox"/>	▶ kinesis-analytics-service-cdkKinesisAnalytic-us-east-1	Customer managed	Permissions policy (1)

▶ Set permissions boundary

Add Tags

Add tags based on your organization's policies.

Click: Review

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

[Cancel](#)

Review

Review the parameters and create a user.

Add user



Review

Review your choices. After you create the user, you can [view and download the autogenerated password and access key](#).

User details

User name	CDKOptimalMultiAccountScan
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	CDKOptimalMultipleAccountPolicy

Tags

No tags were added.

[Cancel](#)[Previous](#)[Create user](#)

Save the Access key ID as well as the Secret access key in a safe place.

You will need them to authenticate the account for Cloudockit.

✔ **Success**

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://349224196492.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶ ✔	cdkoptimalsetup	AKIAI44781432LGGGLC6GMUJ	***** Show

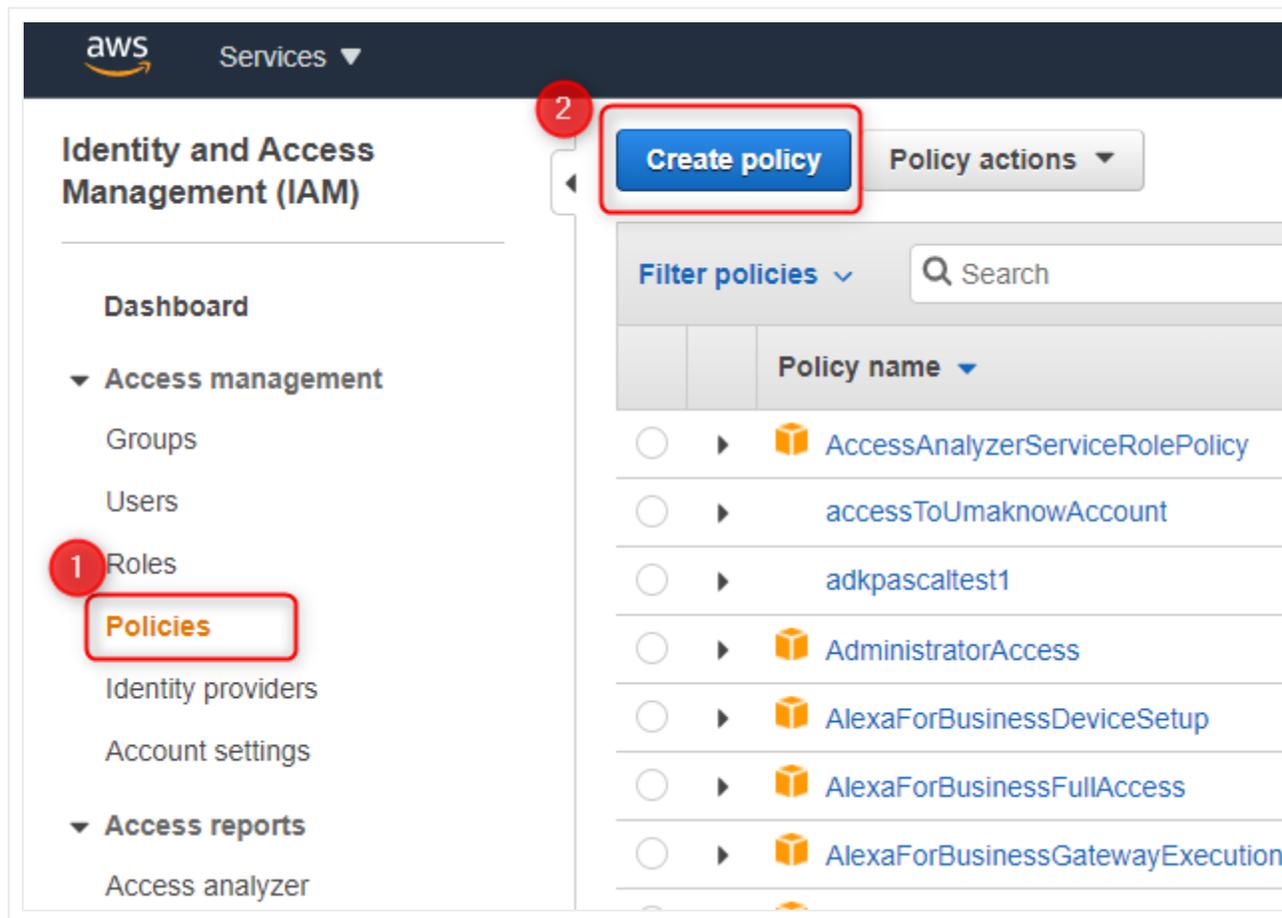
Step 2 – EC2 Instance Role and Policies

Let's create a policy and the role required for the EC2 instance to access the accounts and generate documentation.

Create a Policy

Connect to the AWS Console and select IAM.

Select **Policies** and press **Create Policy**.



Select the JSON tab and paste this JSON into the window.

Click: Review Policy

```
{  
  "Version": "2008-10-17",
```

```
"Statement": {  
  "Effect": "Allow",  
  "Action": "sts:AssumeRole",  
  "Resource": "*" }  
}
```

Create policy

1

2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

```
1 {  
2 "Version": "2012-10-17",  
3 "Statement": {  
4 "Effect": "Allow",  
5 "Action": "sts:AssumeRole",  
6 "Resource": "*" }  
7 }  
8 }  
9 |
```

Character count: 96 of 6,144.

Cancel

Review policy

Give the policy a unique name and press **Create policy**.

Create policy

1

2

Review policy

Name*

CDKOptimalAssumeRole|

Use alphanumeric and '+=, @-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Summary

Q Filter

Service ▾

Access level

Resource

Request condition

Allow (1 of 241 services) [Show remaining 240](#)

STS

Limited: Write

All resources

None

* Required

Cancel

Previous

Create policy

Add Tags

Add tags based on your organization's policies.

Click: Review

Add tags (optional)

Add tags are from existing policies you can add to your own. Tags can include user information such as an email address, or can be descriptive such as job

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

Cancel

Previous

Next: Review

Review

Give the policy a unique name and review to make sure everything is in order.

Click: Create Role

Create policy

1

2

Review policy

Name*

Use alphanumeric and '+=, @-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Summary

Service ▾	Access level	Resource	Request condition
Allow (1 of 241 services) Show remaining 240			
STS	Limited: Write	All resources	None

* Required

Cancel

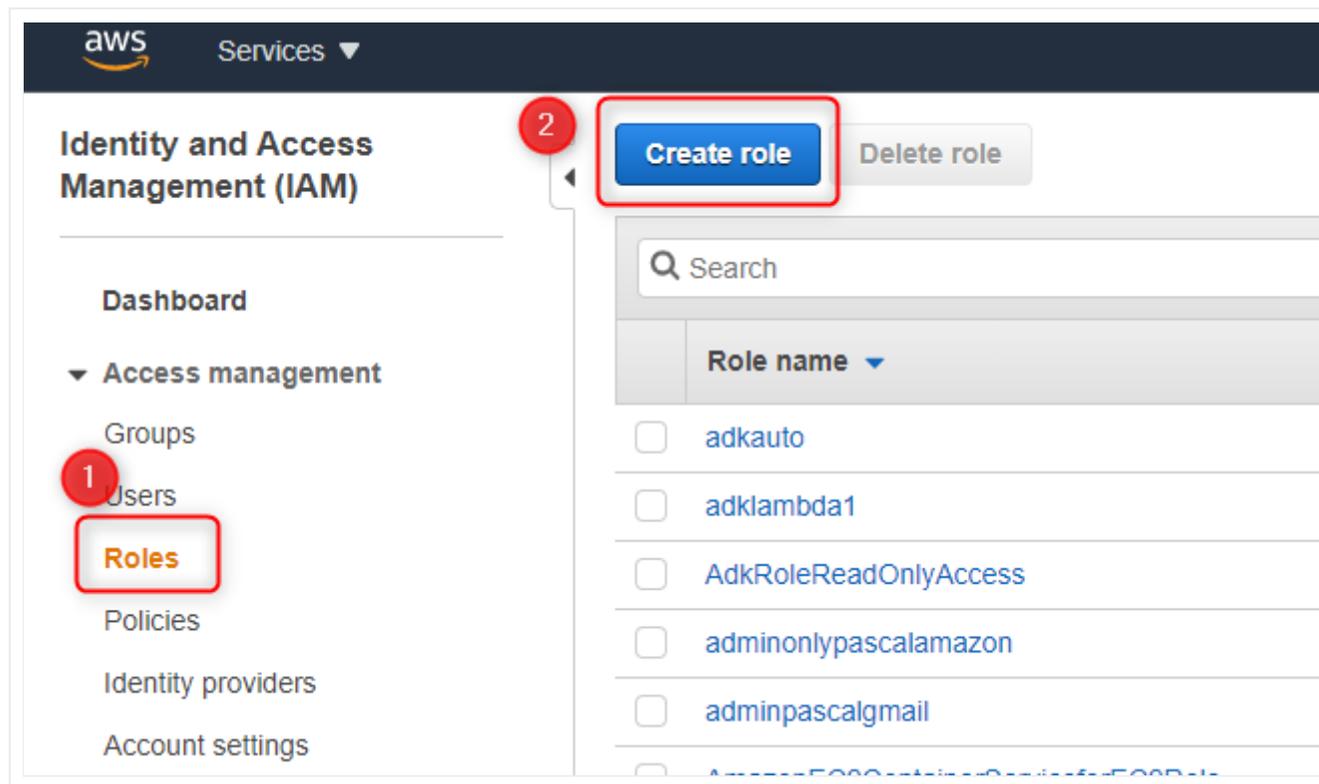
Previous

Create policy

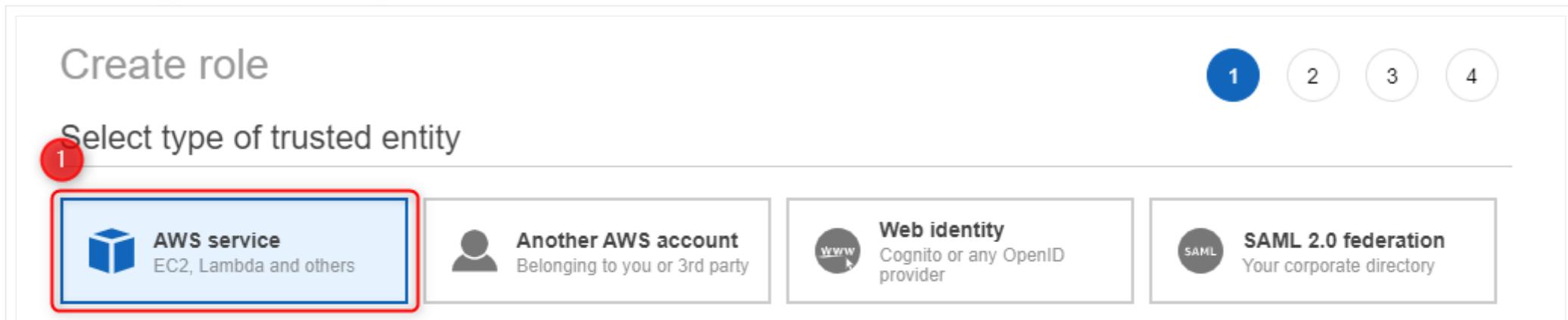
Create an EC2 Role for Cross-Account Documentation

Connect to the AWS Console and select IAM.

Select **Roles** and press **Create role**.



Under Select type of trusted entity, select AWS Service.



Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

2 Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway	CloudWatch Events	EKS	KMS	Rekognition
AWS Backup	CodeBuild	EMR	Kinesis	RoboMaker
AWS Chatbot	CodeDeploy	ElastiCache	Lake Formation	S3
AWS Marketplace	CodeGuru	Elastic Beanstalk	Lambda	SMS
AWS Support	CodeStar Notifications	Elastic Container Service	Lex	SNS
Amplify	Comprehend	Elastic Transcoder	License Manager	SWF
AppStream 2.0	Config	ElasticLoadBalancing	Machine Learning	SageMaker
AppSync	Connect	Forecast	Macie	Security Hub
Application Auto Scaling	DMS	GameLift	Managed Blockchain	Service Catalog
Application Discovery Service	Data Lifecycle Manager	Global Accelerator	MediaConvert	Step Functions
Batch	Data Pipeline	Glue	Migration Hub	Storage Gateway
	DataSync	Greengrass	OpsWorks	Systems Manager

* Required

Cancel

3 [Next: Permissions](#)

From the Attach permissions policies screen select the following policies:

- ReadOnlyAccess
- CDKOptimalAssumeRole (Name of the policy you have created in the previous setup)

Click: Tags

Create role

1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy ↻

Filter policies Showing 6 results

	Policy name	Used as
<input type="checkbox"/>	▶ CDK-NoPermissionCostAndUsageReport	None
<input type="checkbox"/>	▶ cdkCostExplorerServiceMissingPermissions	Permissions policy (1)
<input checked="" type="checkbox"/>	▶ CDKOptimalAssumeRole	None
<input type="checkbox"/>	▶ CDKOptimalMultipleAccountPolicy	Permissions policy (1)
<input type="checkbox"/>	▶ CDKOptimalSetupPolicy	None
<input type="checkbox"/>	▶ kinesis-analytics-service-cdkKinesisAnalytic-us-east-1	Permissions policy (1)

▸ Set permissions boundary

* Required

Cancel

Previous

Next: Tags

Add tags based on your organization's policies.

Click: Review

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
-----	------------------	--------

Add new key

You can add 50 more tags.

Cancel

Previous

Next: Review

Enter a unique name for your role.

Review the parameters and press **Create Role**.

Create role



Review

Provide the required information below and review this role before you create it.

Role name*

CDKOptimalEC2RoleCrossAccount

Use alphanumeric and '+=, @-_' characters. Maximum 64 characters.

Role description

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities

AWS service: ec2.amazonaws.com

Policies

 [ReadOnlyAccess](#) 

[CDKOptimalAssumeRole](#) 

Permissions boundary

Permissions boundary is not set

No tags were added.

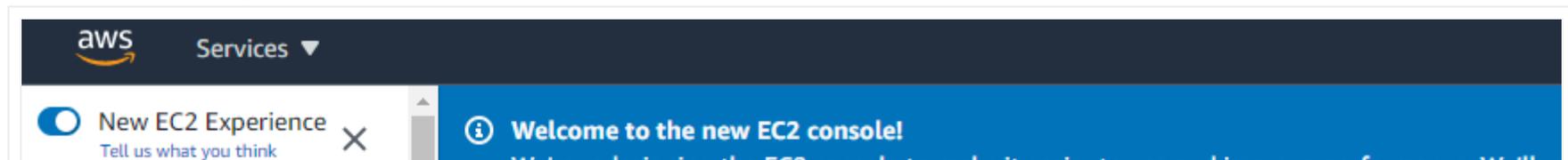
* Required

Cancel Previous Create role

Step 3 – Creation of the EC2 Instance

Connect to the AWS Console and go to the EC2.

From the EC2 Dashboard page Press the **Launch instance** button.



We're redesigning the EC2 console to make it easier to use and improve performance. We'll roll out the new console, use the New EC2 Experience toggle.

EC2 Dashboard New

Events New

Tags

Limits

▼ **Instances**

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Scheduled Instances

Capacity Reservations

▼ **Images**

AMIs

▼ **Elastic Block Store**

Volumes

Snapshots

Lifecycle Manager

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Running instances	1	Dedicated Hosts
Instances (all states)	14	Key pairs
Placement groups	0	Security groups
Volumes	14	

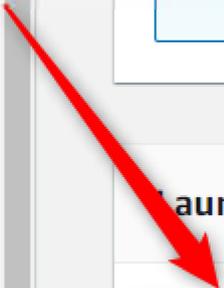
 Easily size, configure, and deploy Microsoft SQL Server Always On availability group

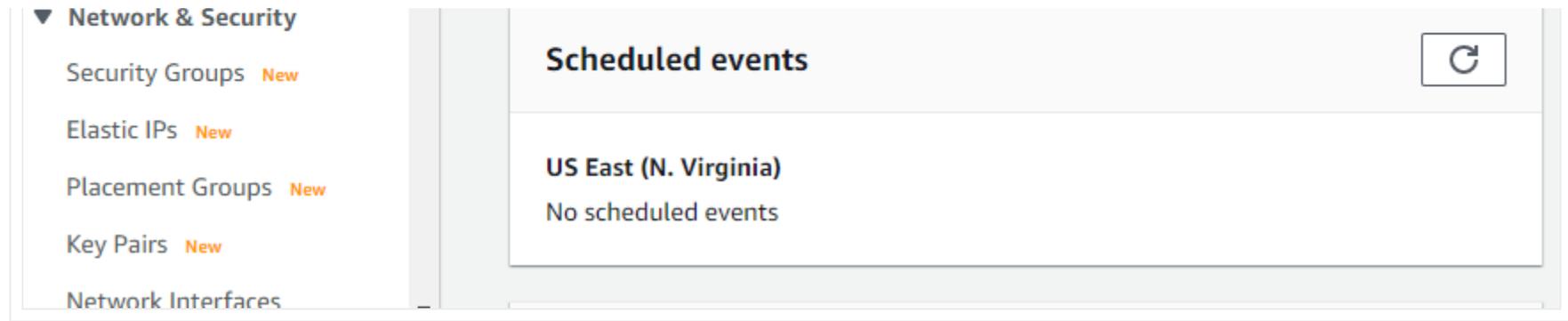
Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Note: Your instances will launch in the US East (N. Virginia) Region





Choose an Amazon Machine Image (AMI)

Select Microsoft Windows Server 2019 Base. (Linux OS is not supported).

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

Free tier eligible

Ubuntu Server 20.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes



Ubuntu Server 18.04 LTS (HVM), 5SD Volume Type - ami-0817d426a6f68645 (64-bit x86) / ami-0f2b111f0c1647818 (64-bit Arm)

Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Free tier eligible

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes



Amazon RDS

Are you launching a database instance? Try Amazon RDS.

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora**, **MariaDB**, **MySQL**, **Oracle**, **PostgreSQL**, and **SQL Server** databases on AWS. **Aurora** is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)

Hide

Launch a database using RDS



Windows

Microsoft Windows Server 2019 Base - ami-0412e100c0177fb4b

Free tier eligible

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes



Deep Learning AMI (Ubuntu 18.04) Version 36.0 - ami-063585f0e06d22306

MXNet-1.7.0, TensorFlow-2.3.1, 2.1.0 & 1.15.3, PyTorch-1.4.0 & 1.7.0, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA support. For fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes



Deep Learning AMI (Ubuntu 16.04) Version 36.0 - ami-0cc2702a48aac44ba

MXNet-1.7.0, TensorFlow-2.3.1, 2.1.0 & 1.15.3, PyTorch-1.4.0 & 1.7.0, EI, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA. For fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes



Amazon Linux

Deep Learning AMI (Amazon Linux 2) Version 36.0 - ami-0899888474ea45a9

MXNet-1.7.0, TensorFlow-2.3.1, 2.1.0 & 1.15.3, PyTorch-1.4.0 & 1.7.0, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA support. For fully managed experience, check: <https://aws.amazon.com/sagemaker>

64-bit (x86)

64-bit (Arm)

Select

64-bit (x86)

64-bit (Arm)

Select

64-bit (x86)

Select

64-bit (x86)

Select

64-bit (x86)

Select

64-bit (x86)

Choose an Instance Type

We have identified that Clouddockit Desktop performs at its best with 4 CPUs and 16 GiB of memory. You can however choose the type that you prefer.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families | Current generation | Show/Hide Columns

Currently selected: t2.large (- ECUs, 2 vCPUs, 2.3 GHz, -, 8 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

Configure Instance Details

Configure the instance based on your organization's best practices and make sure to select the CrossAccount IAM role created in the previous step.

1. Choose AMI 2. Choose Instance Type **3. Configure Instance** 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the

Number of instances ⓘ	<input type="text" value="1"/>	Launch into Auto Scaling Group ⓘ
Purchasing option ⓘ	<input type="checkbox"/> Request Spot instances	
Network ⓘ	<input type="text" value="vpc-9eff53e6 default-vpc (default)"/>	Create new VPC
Subnet ⓘ	<input type="text" value="No preference (default subnet in any Availability Zone)"/>	Create new subnet
Auto-assign Public IP ⓘ	<input type="text" value="Use subnet setting"/>	
Placement group ⓘ	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation ⓘ	<input type="text" value="Open"/>	
Domain join directory ⓘ	<input type="text" value="No directory"/>	Create new directory

IAM role ⓘ ↕ [Create new IAM role](#)

CPU options ⓘ Specify CPU options

Shutdown behavior ⓘ ↕

Stop - Hibernate behavior ⓘ Enable hibernation as an additional stop behavior

Enable termination protection ⓘ Protect against accidental termination

Monitoring ⓘ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy ⓘ ↕
[Additional charges will apply for dedicated tenancy.](#)

Elastic Graphics ⓘ Add Graphics Acceleration
[Additional charges apply.](#)

Credit specification ⓘ Unlimited

Add Storage

You can leave the default parameters.

Add Tags

Add the tags based on your organization's tagging policy.

Configure Security Group

Create or assign a security group based on your organization's security policies.

Review Instance Launch

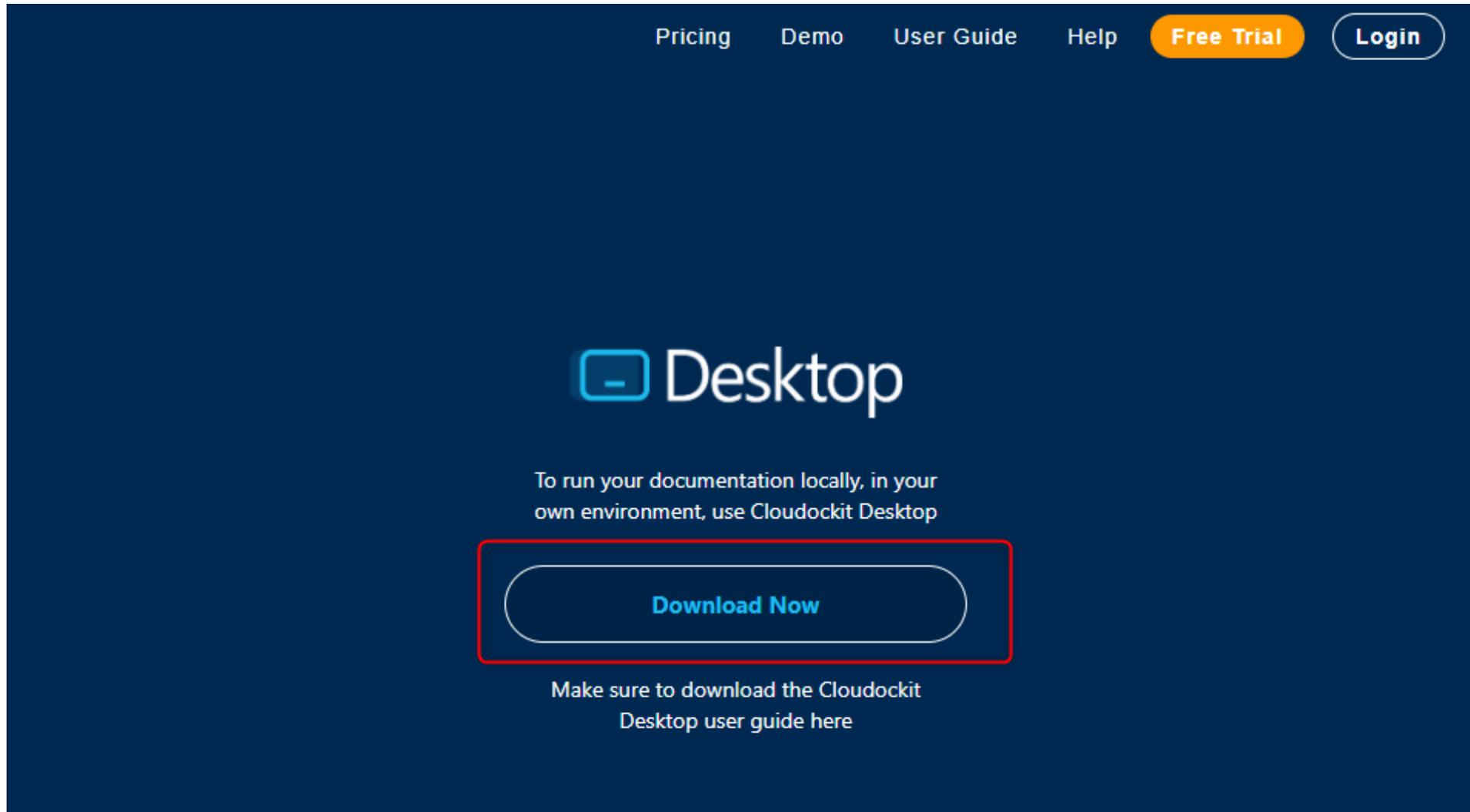
Review the parameters that have been set and press launch to create the instance.

Step 4 – Installing Clouddockit Desktop

Downloading the Document

You can get the Clouddokit installation file from our [website](#).

Press the Download Now button to get the MSI.



Launch your instance and copy the MSI file on the instance.

Double click the Clouddokit icon to start the installation.

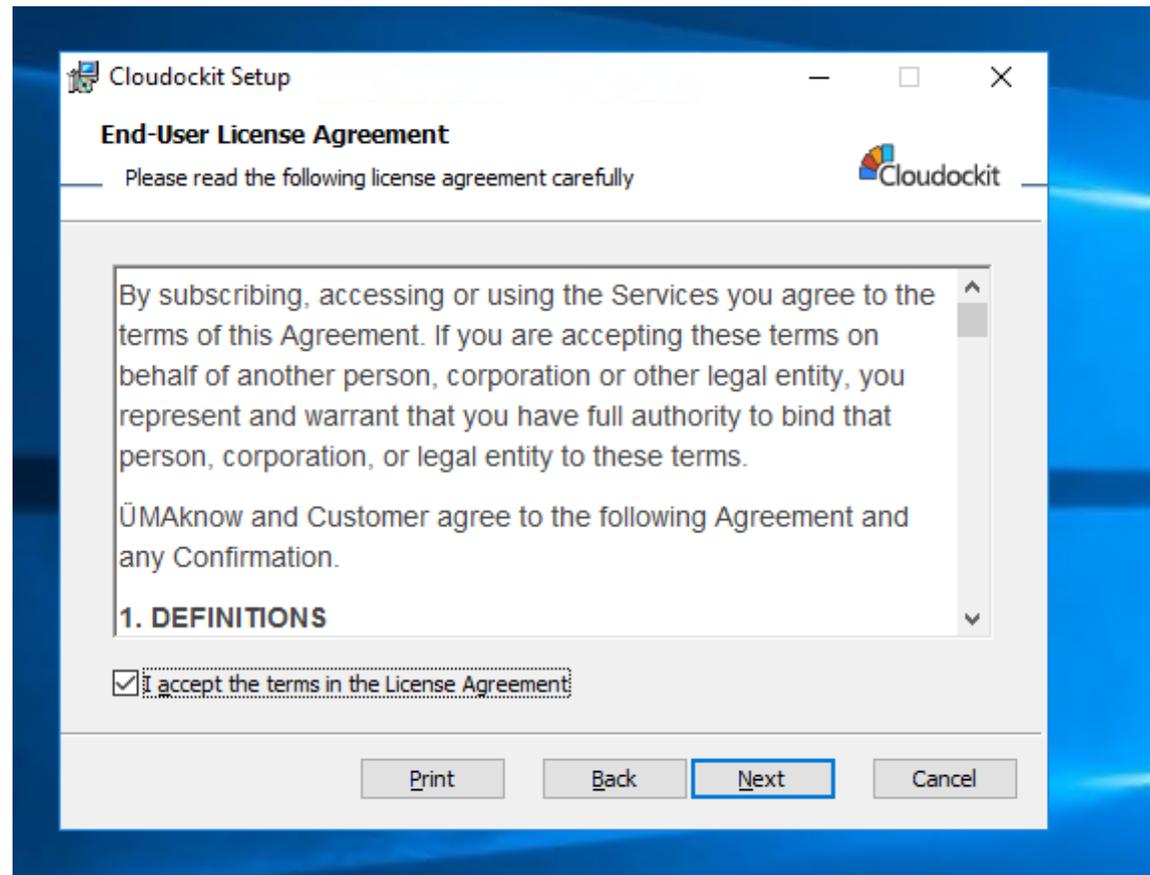
Click: Next



Carefully read the terms in the license agreement.

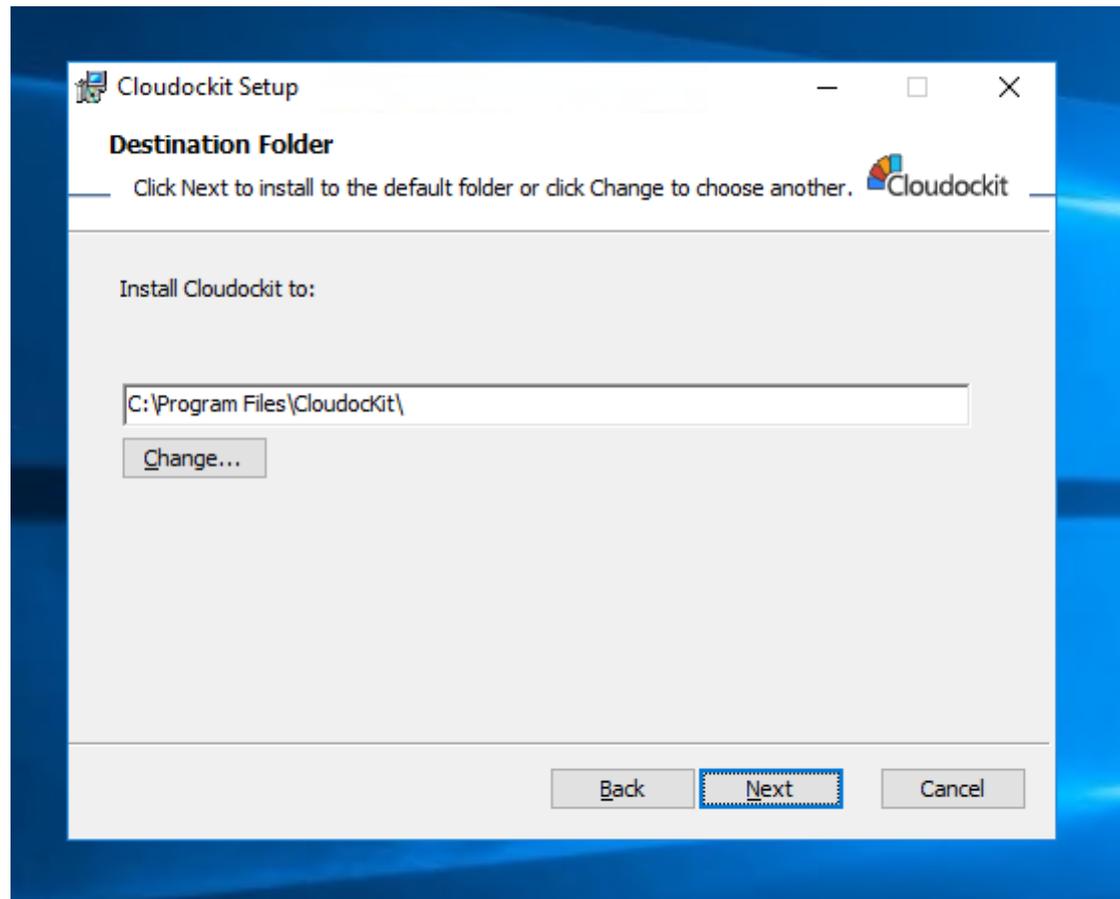
Check the box "I accept the terms in the License Agreement".

Click: Next

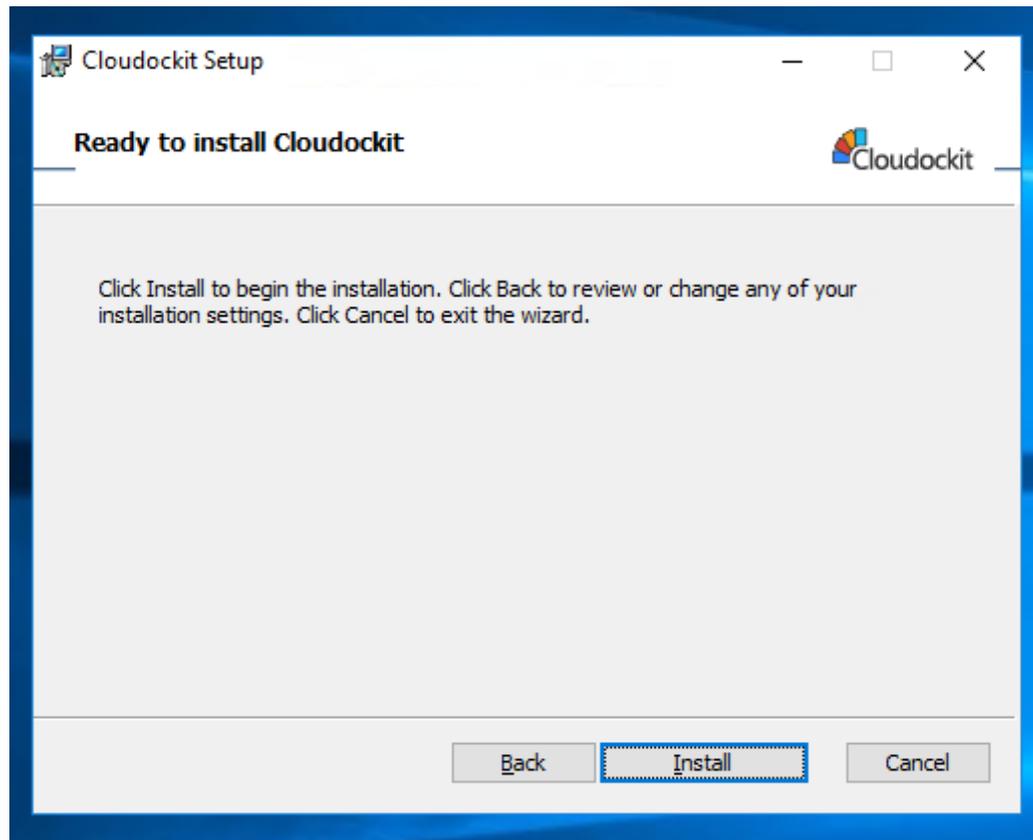


Select the path where you want to install Cludockit Desktop.

Click: Next

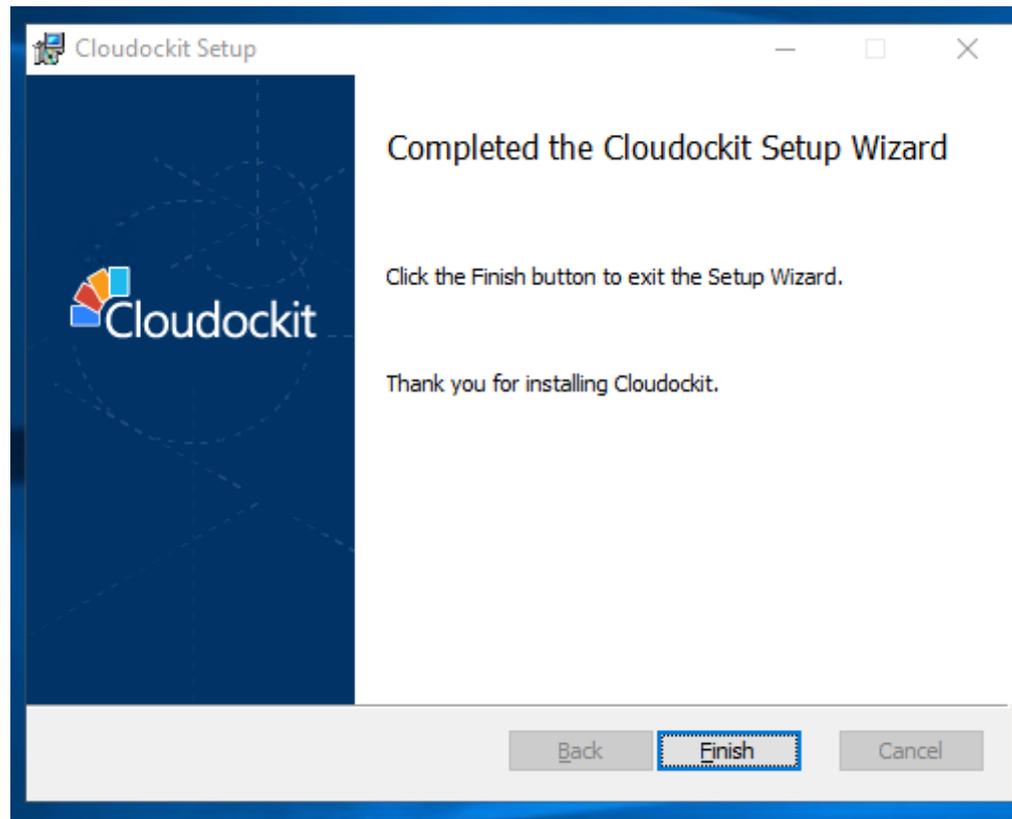


Click: Instal



Once the installation is complete.

Click: Finish

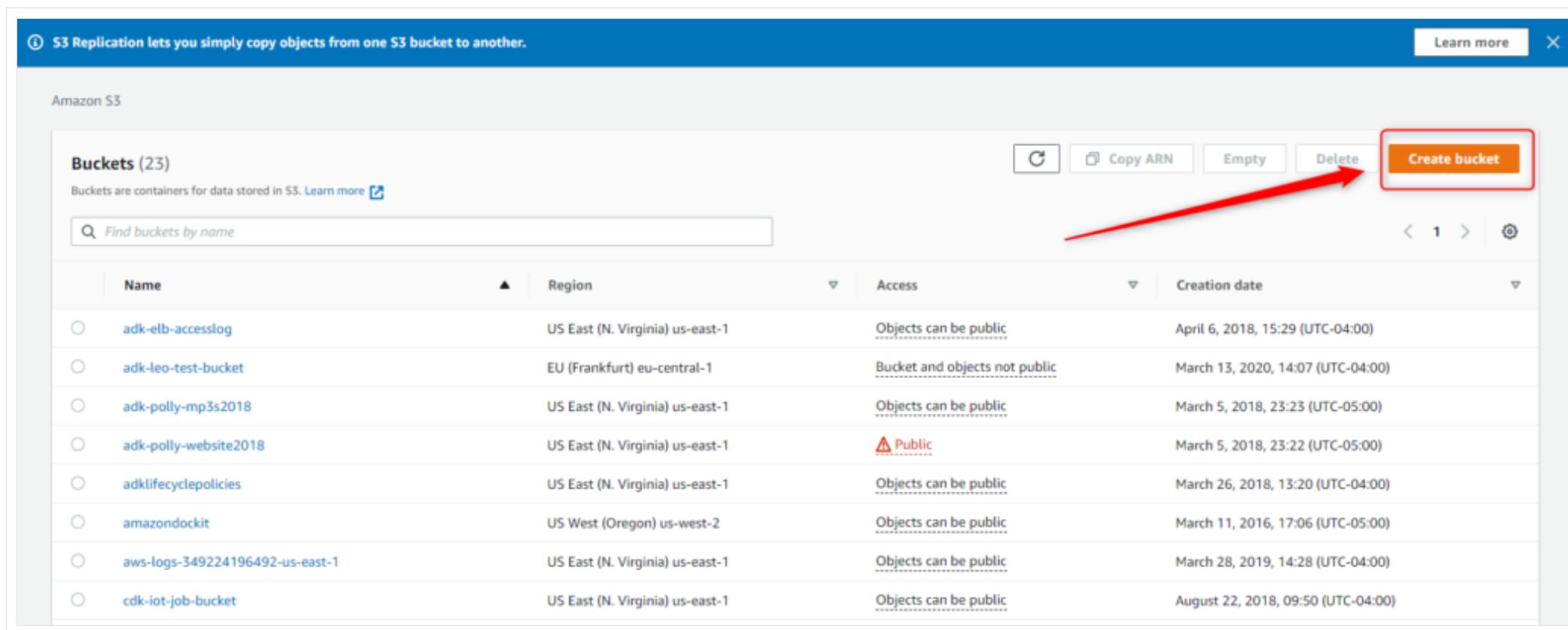


Step 5 – Creation of the Bucket

The bucket will allow you to save the documentation and be available to employees in your organization.

From the AWS Console, select **S3**

Press **Create bucket** in the upper right corner.



The screenshot shows the Amazon S3 console interface. At the top, there is a blue banner with the text "S3 Replication lets you simply copy objects from one S3 bucket to another." and a "Learn more" button. Below the banner, the page title "Amazon S3" is visible. The main content area is titled "Buckets (23)" and includes a search bar with the placeholder text "Find buckets by name". To the right of the search bar are several action buttons: "Refresh", "Copy ARN", "Empty", "Delete", and "Create bucket". The "Create bucket" button is highlighted with a red box, and a red arrow points to it from the right. Below the buttons is a table listing the buckets. The table has columns for Name, Region, Access, and Creation date. The buckets listed are: adk-elb-accesslog, adk-leo-test-bucket, adk-polly-mp3s2018, adk-polly-website2018, adklifecyclepolicies, amazondockit, aws-logs-349224196492-us-east-1, and cdk-iot-job-bucket.

Name	Region	Access	Creation date
adk-elb-accesslog	US East (N. Virginia) us-east-1	Objects can be public	April 6, 2018, 15:29 (UTC-04:00)
adk-leo-test-bucket	EU (Frankfurt) eu-central-1	Bucket and objects not public	March 13, 2020, 14:07 (UTC-04:00)
adk-polly-mp3s2018	US East (N. Virginia) us-east-1	Objects can be public	March 5, 2018, 23:23 (UTC-05:00)
adk-polly-website2018	US East (N. Virginia) us-east-1	Public	March 5, 2018, 23:22 (UTC-05:00)
adklifecyclepolicies	US East (N. Virginia) us-east-1	Objects can be public	March 26, 2018, 13:20 (UTC-04:00)
amazondockit	US West (Oregon) us-west-2	Objects can be public	March 11, 2016, 17:06 (UTC-05:00)
aws-logs-349224196492-us-east-1	US East (N. Virginia) us-east-1	Objects can be public	March 28, 2019, 14:28 (UTC-04:00)
cdk-iot-job-bucket	US East (N. Virginia) us-east-1	Objects can be public	August 22, 2018, 09:50 (UTC-04:00)

General Configuration

Name your bucket and select the Region of your choice.

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#) 

Region

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Bucket Settings for Block Public Access

Define the public access based on your organization's best practices.

Bucket settings for Block Public Access

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

- I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#) 

Bucket Versioning

- Disable
- Enable

You can enable or disable bucket versioning based on your preferences.

Tags

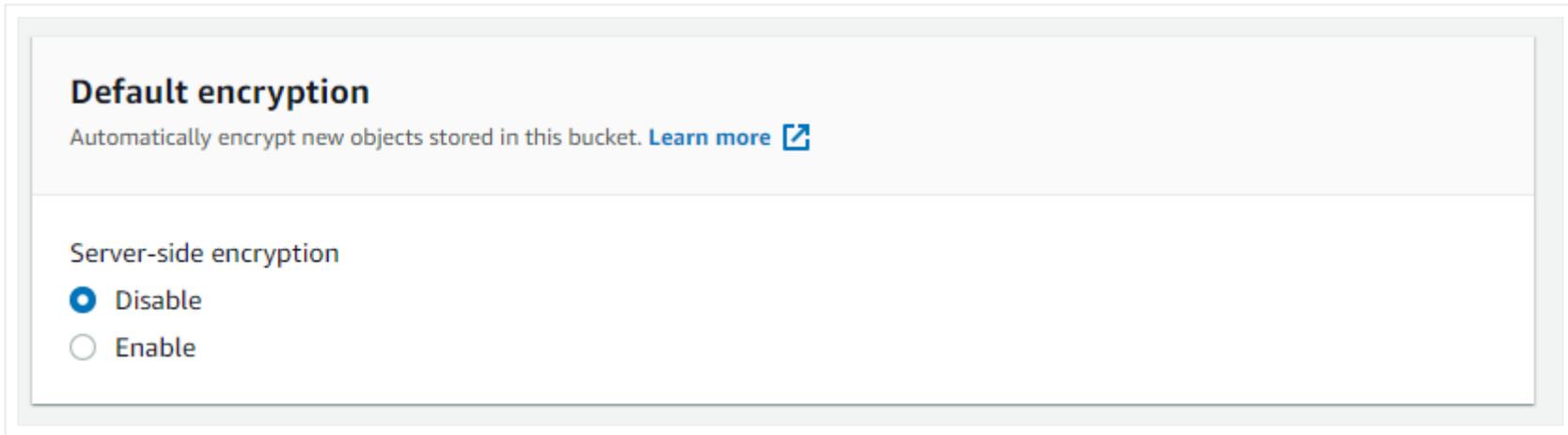
Add tags based on your organization practices.

Tags (0) - optional
Track storage cost or other criteria by tagging your bucket. [Learn more](#) 

No tags associated with this bucket.

[Add tag](#)

Default Encryption



Ensure to copy the Bucket ARN in a secure place. You will need it later.

Click: Finish

S3 Bucket Policy

You must now give your IAM user the policy to allow the S3 bucket to drop the files that Clouddokit will create.

Sign in to the AWS Console and open the IAM console at <https://console.aws.amazon.com/iam/>.

In the navigation panel, choose **Users** and search for the user you created.

Select the username

The screenshot shows the AWS IAM console interface. At the top, there is a dark header with the AWS logo and a 'Services' dropdown menu. Below the header, the page is titled 'Identity and Access Management (IAM)'. On the left side, there is a navigation sidebar with the following items: 'Dashboard', 'Access management' (expanded), 'Groups', 'Users' (highlighted in orange), 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports' (expanded), 'Access analyzer', 'Archive rules', 'Analyzers', and 'Settings'. The main content area on the right contains two buttons: 'Add user' (blue) and 'Delete user' (red). Below these buttons is a search bar with the text 'cdk'. A table of users is displayed below the search bar, with the following entries:

<input type="checkbox"/>	User name ▾
<input type="checkbox"/>	cdkdesktopjfc
<input type="checkbox"/>	cdkfullaccesskeys
<input checked="" type="checkbox"/>	CDKOptimalMultiAccountScan
<input type="checkbox"/>	cdkUserDev
<input type="checkbox"/>	cdkUserReadOnly

Click: Add Permissions

Add Permissions to Users

Select Attach existing policies directly.

Click: Create Policy

Add permissions to cdkoptimalsetup 1 2

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy 1 or create a new one.

2 Add user to group Copy permissions from existing user **Attach existing policies directly**

Create policy ↻

Filter policies Showing 644 results

	Policy name	Type	Used as
<input type="checkbox"/>	accessToUmaknowAccount	Customer managed	Permissions policy (1)
<input type="checkbox"/>	adkpasctest1	Customer managed	None
<input type="checkbox"/>	AdministratorAccess	Job function	Permissions policy (23)
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	Boundary (1)
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None

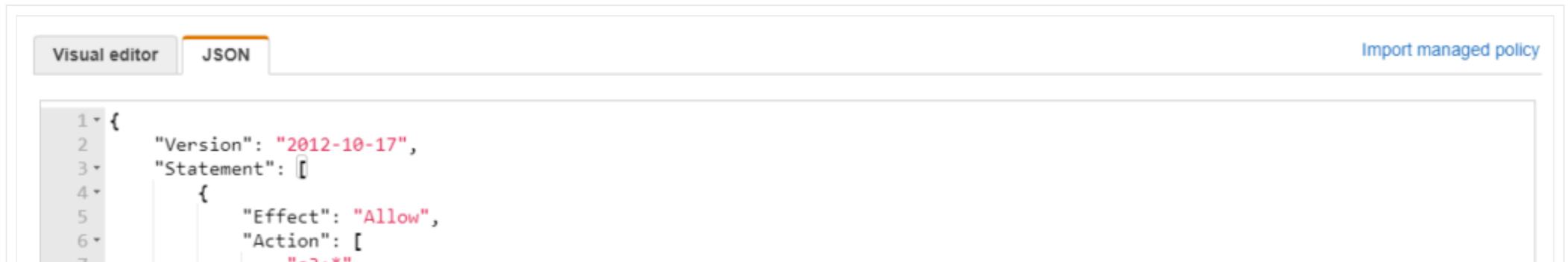
Create Policy

Select JSON tab and paste the following code in the window.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "s3:*" ],
      "Resource": [ "arn:aws:s3:::cdkoptimalsetup" ]
    }
  ]
}
```

Under the Resource value, make sure you replace `arn:aws:s3:::cdkoptimalsetup` with the Bucket ARN saved in the previous step.

Click: Review Policy



```
7
8 ],
9 "Resource": [
10   "arn:aws:s3:::cdkoptimalsetup"
11 ]
12 }
13 ]
14 }
```

Character count: 119 of 6,144.

Cancel

Review policy

Review Policy

Give your policy a unique name, a description and click **Create Policy**.

Create policy

1 2

Review policy

Name*

Use alphanumeric and '+=, @-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Summary

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining**. [Learn more](#)

Service ▾	<u>Access level</u>	<u>Resource</u>	<u>Request condition</u>
Allow (1 of 241 services) Show remaining 240			
S3	Limited: List, Read, Write, Permissions management, Tagging	BucketName string like cdkoptimalsetup	None

* Required

Cancel

Previous

Create policy

Storage Account

From the Storage Account, click on **Permissions** and then **Bucket Policy**. Ensure you have the following statement: replace the IAM User Arn and Resource.

```
{
  "Version": "2008-10-17",
  "Id": "Policy1335892530063",
  "Statement": [
    {
      "Sid": "Stmt1335892526597",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::xxxx:user/xxxxxxx"
      }
    }
  ]
}
```

```
    },  
    "Action": "s3:PutObject",  
    "Resource": "arn:aws:s3:::yourS3Bucket/*"  
  }  
]  
}
```

Step 6 – Policies

Now that we have a user created, an EC2 Instance created as well as a storage account, it is time to apply the policies. Policies were already given to the user account in the previous step, therefore it has read access at the account level.

AWS Billing

To read billing information from AWS, the credentials used to generate the documentation must have “**aws-portal:ViewBilling**” policy.

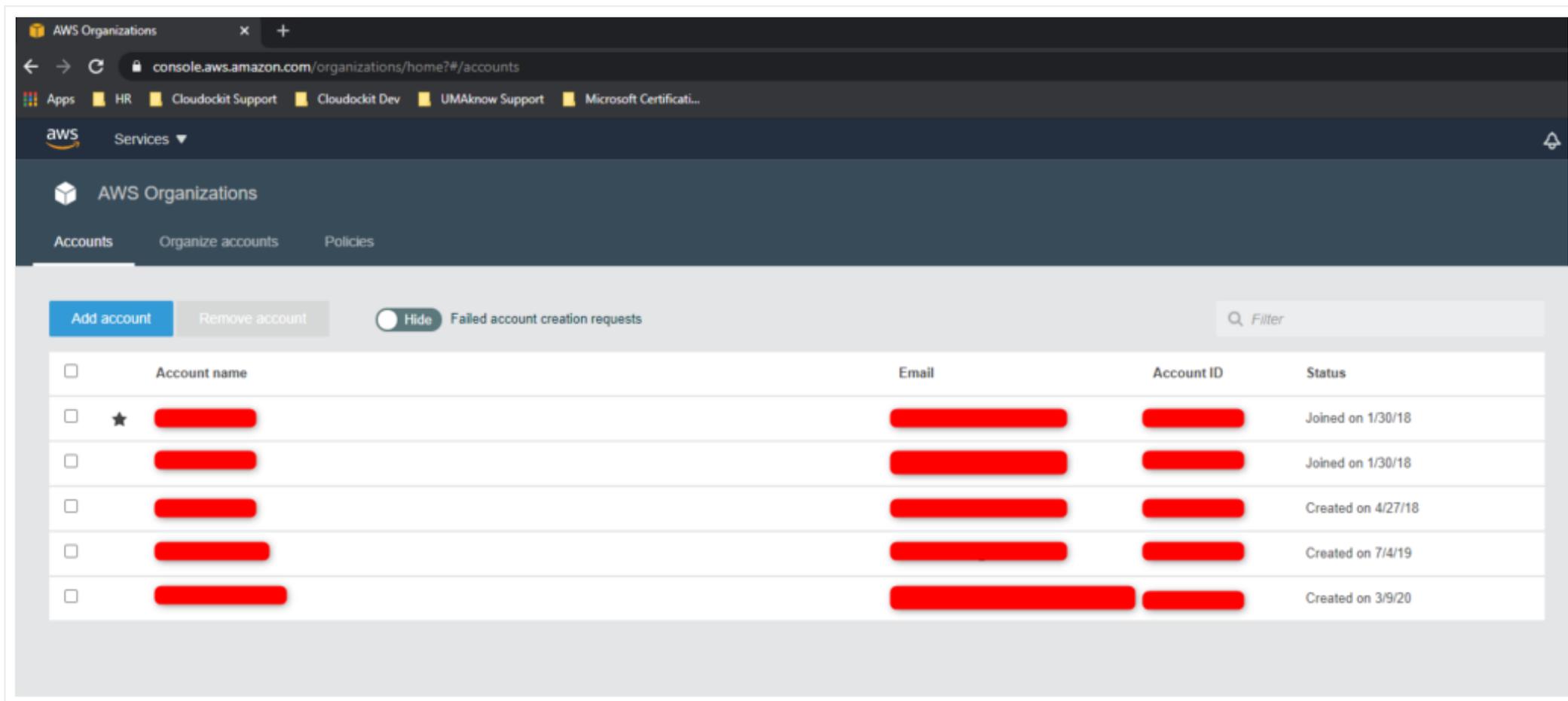
AWS Trusted Advisor

To read information from AWS Trusted Advisor, the credentials used to generate the documentation must have the following policy.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ce:Get*",
        "ce:List*",
        "ce:Describe*"
      ],
      "Resource": [ "*" ]
    }
  ]
}
```

AWS Organizations Accounts

In the generated documents, if you want to view details of the accounts from your organization, you will need to choose an AWS master account when logging on Cloudockit website.



AWS Organizational Units and Accounts

If you want to view details of the organizational units and accounts of your organization in the generated documents, you will need to choose an AWS master account when logging on Cloudockit website.

AWS Organizations

Accounts

Organize accounts

Policies

Root

⊖ Root



↳ cloudockit-ou

TREE VIEW

🔍 Filter

Organizational units (2)

↳ New organizational unit

[Redacted]

cloudockit-ou

Accounts (2)

CloudockitProduction
CloudockitAWSMarketplac...

Cloudockit-Test-2
[Redacted]

AWS Member Account

When you choose an AWS member account, the generated documents will display the information of your organization and minimum information about your account (e.g.: Id, ARN).

Step 7 – AWS Cross-Account Roles

In each AWS Account you want to scan, you need to create a role named CloudockitScanRole (or any name that you prefer).

Here are the steps to create this role:

From IAM console, click on Roles and then Create role.

- Select Another AWS Account. Enter the Account ID where you are installing the EC2 instance that will run Cloudockit Desktop.
- Click Next and select the *ReadOnlyAccess*
- Click Next: Review
- Enter the name: CDKOptimalScanRole (Or which ever name you gave it)
- Click on create role
- Repeat those steps in all AWS Accounts

Step 8 – Launch Clouddockit Desktop and Schedule a Document Generation

Connect to the EC2 Instance created.

Launch Clouddockit Desktop.

Activating Clouddockit

Click on the desktop shortcut of Clouddockit to launch the application.

You will need to enter your product key to activate Clouddockit Desktop.

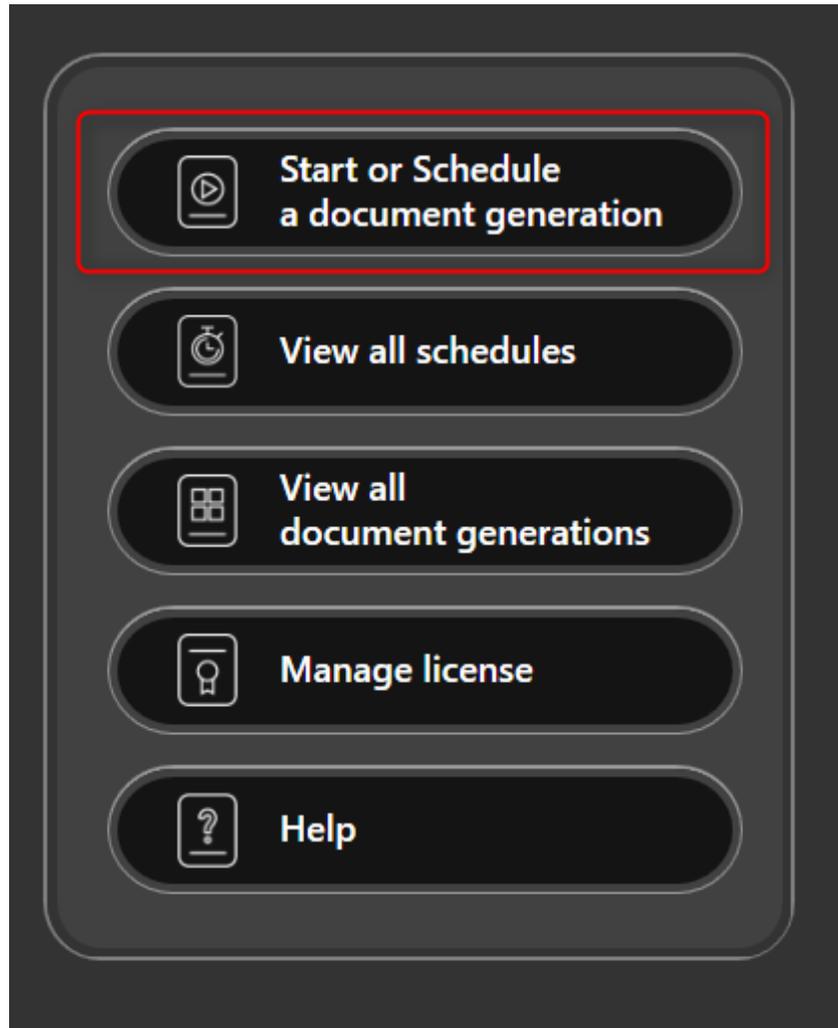
If you haven't purchased a product key, please visit <https://www.clouddockit.com/pricing/>

You will see a message confirming that the activation was done successfully.

Click: OK

Connecting to an AWS Platform

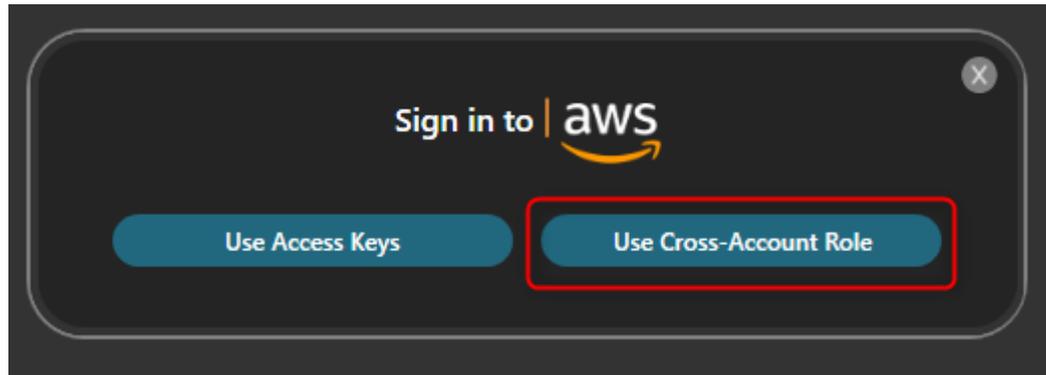
Select Start or Schedule a Document Generation



Select Cross-Account Role.

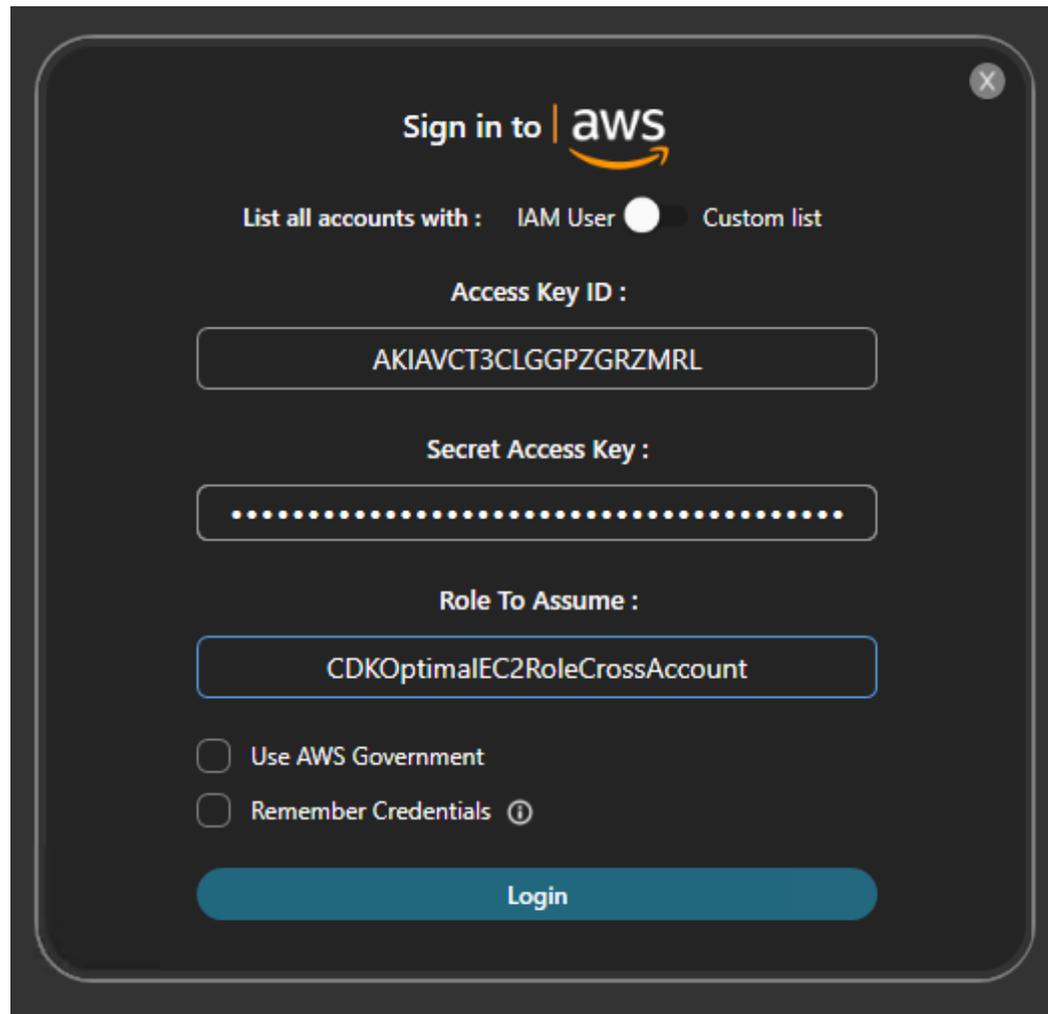


Select AWS from the list of platforms.



Enter the Access Key ID, Secret Access Key, and Role to Assume.

Click: Login

A dark-themed dialog box for signing into AWS. At the top center is the text "Sign in to | aws" with the AWS logo. Below this, there are two radio buttons: "IAM User" (selected) and "Custom list". The "Access Key ID" field contains the text "AKIAVCT3CLGGPZGRZMRL". The "Secret Access Key" field is masked with dots. The "Role To Assume" field contains the text "CDKOptimalEC2RoleCrossAccount". At the bottom, there are two unchecked checkboxes: "Use AWS Government" and "Remember Credentials" (with an information icon). A blue "Login" button is at the very bottom.

Sign in to | aws

List all accounts with : IAM User Custom list

Access Key ID :

AKIAVCT3CLGGPZGRZMRL

Secret Access Key :

.....

Role To Assume :

CDKOptimalEC2RoleCrossAccount

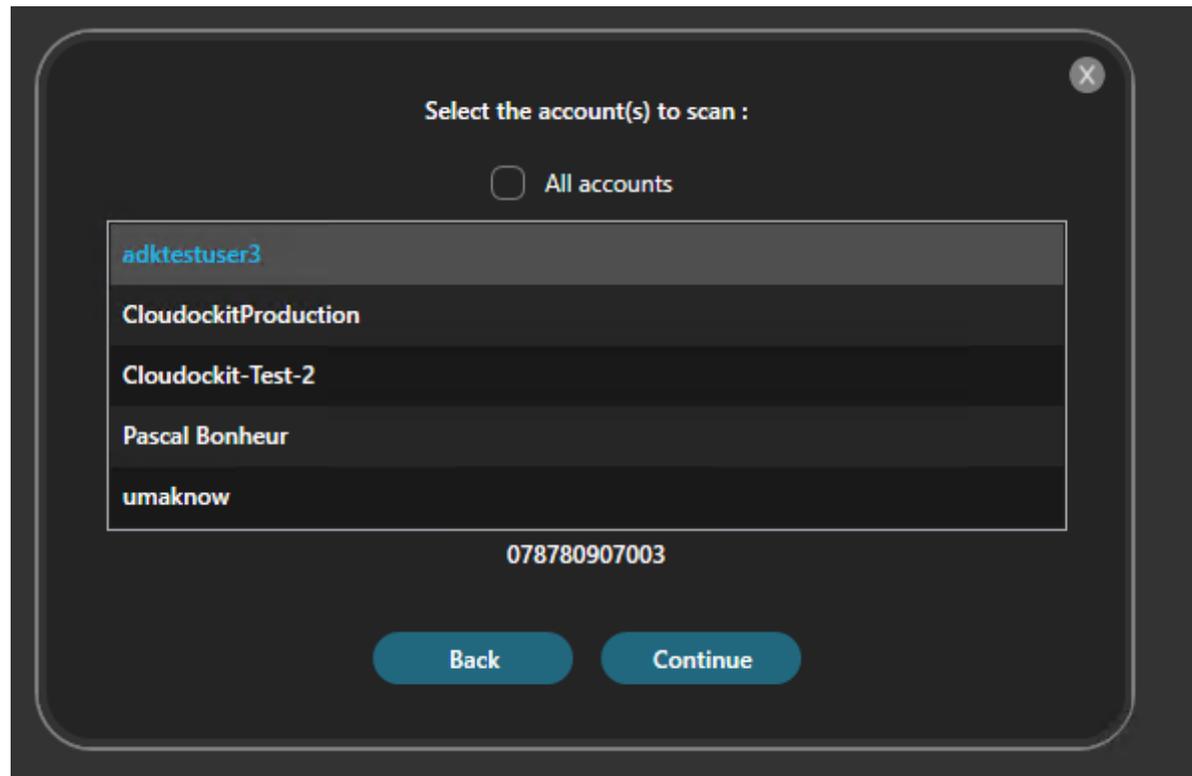
Use AWS Government

Remember Credentials ⓘ

Login

You now need to select the accounts you want to document.

Click: Continue



Schedule a Document Generation

Now that you are logged in, it is time to define what information you want to generate using Clouddokit.

Set the desired parameters under Documents, Workloads, and Organize Content.

Track Changes

Use the storage account created previously for track changes. This will allow you to see the differences that have occurred between a previous document generation and the one running right now.

Select **Track Changes** from the left menu.



Clouddockit - Options

Documents

Workloads

Organize Content

Track Changes

Drop-off

Compliance

Generate

Scheduling

Manage Configurations

Compare with previous versions

Track Changes feature saves a snapshot of your current environment and allows you to compare it with a previous snapshot. The snapshot will be saved in your selected storage.

Please choose the type of storage you'd like to use: Cloud Storage Local Folder Storage

Please note that the storage type for 'Your Storage' Drop-Off, and for Track Changes will be the same. If no value is entered or the storage is invalid. The default local folder will be used.

Cloud Storage

Account Name (ex: companynamedclouddockit)

cdkoptimalsetup

Please note that the cloud storage, once validated, will also be applied to 'Your Storage' Drop-Off. Please create and use a dedicated storage as CORS rules will be applied to this storage.

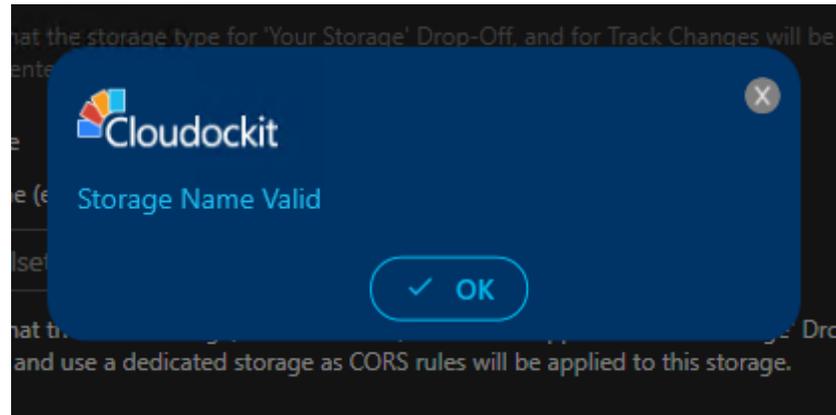
3

Validate

Clear

Enter the name of the bucket in the Account Name box and press **validate**.

A confirmation message will display that the bucket is valid.



Check the box **Save a snapshot for comparison.**

This will save a JSON file in the storage account every time a document generation runs.



Clouddockit - Options

Documents

Workloads

Organize Content

Track Changes

Drop-off

Compliance

Generate

Scheduling

Manage Configurations

Compare with previous versions

Track Changes feature saves a snapshot of your current environment and allows you to compare it with a previous snapshot. The snapshot will be saved in your selected storage.

Please choose the type of storage you'd like to use : Cloud Storage Local Folder Storage

Please note that the storage type for 'Your Storage' Drop-Off, and for Track Changes will be the same. If no value is entered or the storage is invalid. The default local folder will be used.

Cloud Storage

Account Name (ex: companynameclouddockit)

Validate

Clear

Please note that the cloud storage, once validated, will also be applied to 'Your Storage' Drop-Off. Please create and use a dedicated storage as CORS rules will be applied to this storage.

Save snapshot for future comparisons

Compare with a previously generated document

If you want to compare to latest snapshot available, please select the first empty row

Check the box **Compare with a previously generated document**.

Select the first empty row that appears below.

This will always select the most recent file in the storage account to compare.

- Save snapshot for future comparisons
- Compare with a previously generated document (in the selected directory)

If you want to compare to latest snapshot available, please select the first empty row

Thursday, November 5, 2020 8:19:26 PM

Thursday, November 5, 2020 8:15:48 PM

Thursday, November 5, 2020 8:05:47 PM

Thursday, November 5, 2020 7:53:28 PM

Thursday, November 5, 2020 7:46:00 PM

Thursday, November 5, 2020 7:36:20 PM

Drop-Off

In the Drop-Off settings, the same bucket as defined in the Track changes section is selected.

aws

Cloudockit - Options

- Documents
- Workloads
- Organize Content
- Track Changes
- Drop-off**
- Compliance
- Generate**
- Scheduling
- Manage Configurations

Drop-Off Settings

How should Cloudockit deliver your documents and notify you ?

- Send Email
- Your Storage
- Sharepoint Online
- CallBack URL

Your Storage

Please choose the type of storage you'd like to use : Cloud Storage Local Folder Storage

Please note that the storage type for 'Your Storage' Drop-Off, and for Track Changes will be the same. If no value is entered or the storage is invalid, The default local folder will be used.

Cloud Storage

For the Cloud Storage, only AWS and Azure storage are supported.
You can also enter an Azure Storage Connection String (works for Azure, AWS and GCP scans).

Scheduling

Define the desired schedule for your documentation to run and save your schedule.

Cloudockit - Options

- Documents
- Workloads
- Organize Content
- Track Changes
- Drop-off
- Compliance

Generate

Scheduling

Manage Configurations

Schedule the documents generation

Minutes Hourly Daily Weekly Monthly

Every 01 hour(s)

Next 5 Scheduled Dates

Tuesday, 10 November 2020 14:00
Tuesday, 10 November 2020 15:00
Tuesday, 10 November 2020 16:00
Tuesday, 10 November 2020 17:00
Tuesday, 10 November 2020 18:00

Enter a description for scheduling. This will allow you to identify the scheduling easily

Save Schedule

Subscription	Schedule Description	Send To	Schedule	Next Run	Actions
--------------	----------------------	---------	----------	----------	---------

Configuration

Enter a unique name in the parameters you have set and press **Save Current Configuration**.

Your configuration is saved, you can load or edit it in the future.

The screenshot shows the AWS Cloudockit 'Manage Configurations' page. On the left is a sidebar with navigation options: Documents, Workloads, Organize Content, Track Changes, Drop-off, Compliance, Generate (highlighted), and Scheduling. The main area is titled 'Manage Configurations' and contains instructions: 'Use this screen to save your current configuration. This will save the configurations like Documents output, Selected Workloads, Organize Content, etc. This will not save your authentication settings and currently selected environments.'

Under 'Save Configuration', there is a text input field and a 'Save Current Configuration' button. Below this is the 'Existing Configurations' section, which is currently empty. On the right side, there are two sections: 'Export Configuration' with a checked 'Encrypt Configuration File' option, a 'Browse...' button, and an 'Export' button; and 'Import Configuration' with a 'Browse...' button and an 'Apply' button.

Configuration Description	Actions
---------------------------	---------



Step 9 – Validate that Documents are Successfully Generated

Once your scheduled document generation is complete, let's validate that it has been scheduled properly.

From the main menu, select **View All schedules**.

You will see in the list the scheduled documentation you configured.

You can press run now to generate a manual document generation or wait for the schedule to run its course.

Once your document will be completed, you will be able to access it from the Storage Account or from the desktop application.



This is the list of all your current schedules

Subscription	Schedule Description	Send To	Schedule	Next Run	Actions
349224196492	AWS Optimal Setup		0 0 0 ? * MON *	11/16/2020 00:00	Run Now Delete
Microsoft Azure Sponsorship - Clouddockit Development	Unique Name		0 0 16 ? * MON,FRI *	11/13/2020 16:00	Run Now Delete

Click **View all document generations** from the main menu.

You have the list of all generated documents.

You can access the documents from the View Documents button on the right.

List of all document generations

Status All [Refresh List](#)

Subscription(s)	Platform	Generation Type	Status	Process ID	Start Time	Actions
Clouddokit - Test Environment 4	Azure	Manual	Successful	1028	10/1/2020 6:02:21 PM	View Documents
349224196492	AWS	Manual	Successful	3724	10/1/2020 5:13:45 PM	View Documents
349224196492	AWS	Manual	Stopped	3028	10/1/2020 3:13:47 PM	
CDK Test Environment 1	GCP	Manual	Successful	4520	10/1/2020 3:08:10 PM	View Documents
adkproject1	GCP	Manual	Successful	6328	10/1/2020 3:03:39 PM	View Documents
349224196492	AWS	Manual	Successful	5884	10/1/2020 1:29:00 PM	View Documents
Microsoft Azure Sponsorship - Clouddokit Development	Azure	Scheduled	Successful	5624	9/20/2020 10:00:00 AM	View Documents
Microsoft Azure Sponsorship - Clouddokit Development	Azure	Manual	Successful	716	9/18/2020 7:05:02 PM	View Documents
Microsoft Azure Sponsorship - Clouddokit Development	Azure	Manual	Successful	8336	9/18/2020 7:00:40 PM	View Documents

LATEST ON OUR BLOG

Great new Clouddokit Features Including Compliance Rules, AWS Backups, Google Cloud Billing, and More.

Great new features for Azure and AWS users plus download Clouddokit Desktop easily

© 2020 Clouddokit - by UMAknow Solutions inc.