Aquila Clouds

November 5, 2019

Getting Started Guide

Overview

The Aquila Clouds SAAS platform enables you to run your cloud with confidence and efficiency. Aquila clouds gathers configuration, cost and performance data from your cloud environment, analyzes it and provides summarized reports and recommendations in addition to automating some aspects of managing your cloud environment.

The platform's features can be broadly classified into three aspects

- Visibility
- Recommendations
- Actions.

Visibility provides insights into the cost and utilization of your environment summarized in a neat Dashboard by different dimensions of interest such as Sub account, groups , Services, Resource types etc.

Recommendations Dashboard offers suggestions to save cost and improve performance.

Actions are either one time tasks or continuous tasks that are automatically executed on schedule or based on certain conditions or events which the platform can perform on your behalf.

To use the platform, you need to SignUp and onboard the AWS account(s) that you wish to manage using Aquila Clouds. The SignUp process starts with a request for access to the software. It can occur via a manual interaction with a Aquila Clouds Sales contact or via our company portal at https://aquilaclouds.com. Once you SignUp an email will be sent to you with the URL for accessing the platform and onboarding your Cloud Environment to be managed by Aquila Clouds.

Basic Onboarding Steps

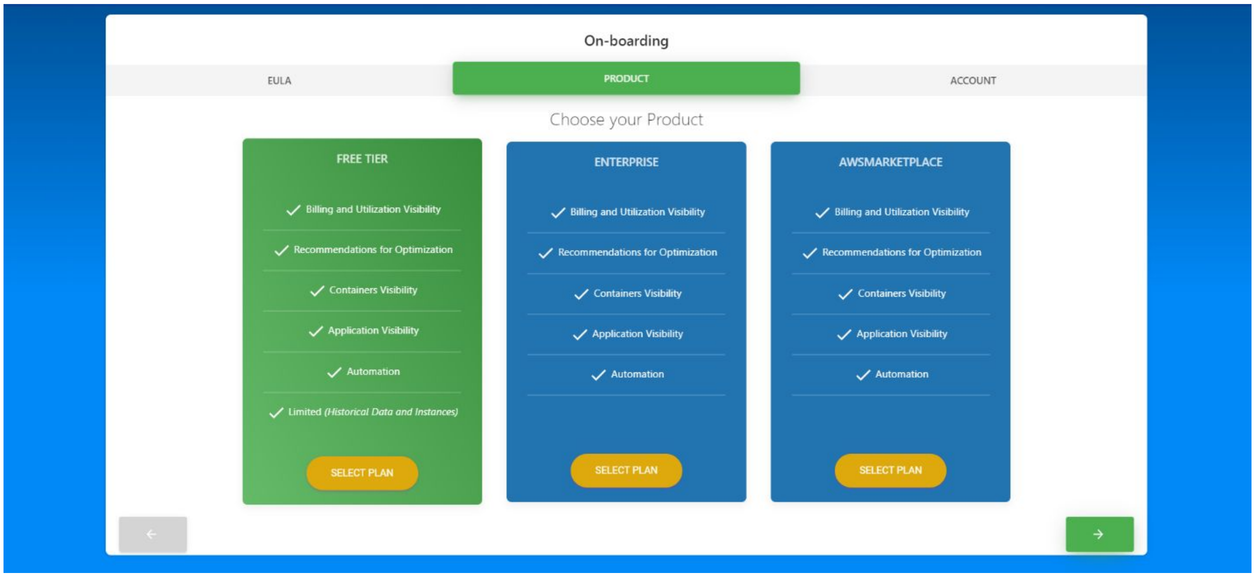
1. Agree to the Terms of Service/Software License Agreement
2. Select whether you wish to go with **Free Tier** *(Aquila Clouds Platform limits analysis to first 100 Instances and 3 month Data History for Free Tier)* OR **Enterprise Tier** *(Unlimited, 30 days Free Trial after which License needs to be purchased)*
3. Provide Company Email and Password

Step 1

Read the terms and Accept (if you agree) or Abort by killing the browser window (if you disagree to the terms)

Step 2

Choose your Product License type



On-boarding

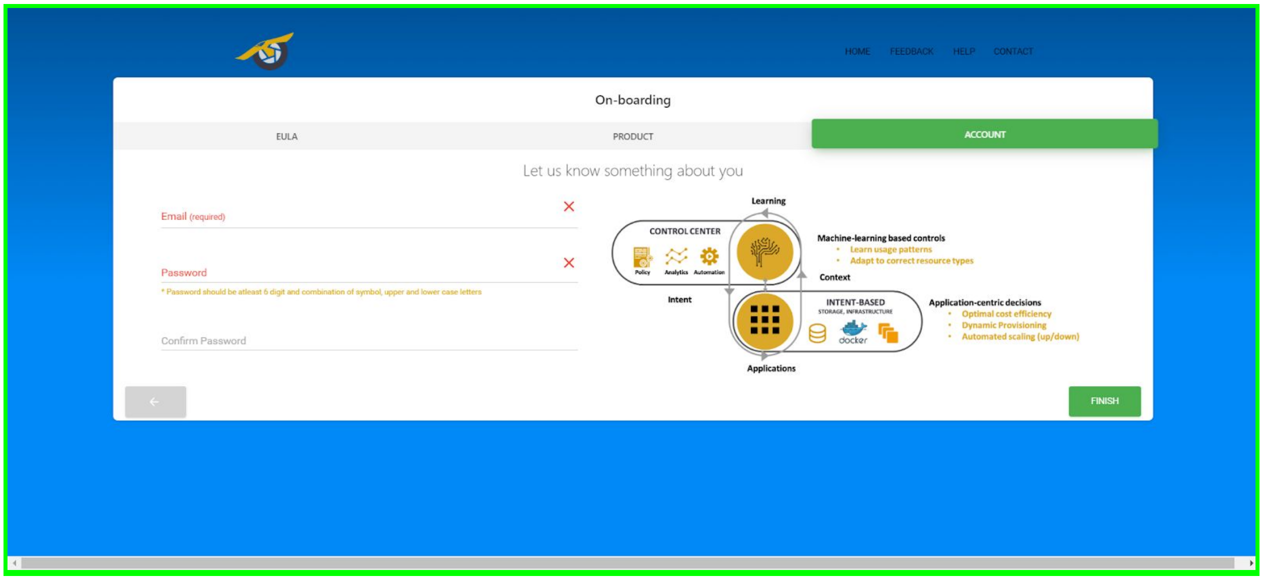
EULA | PRODUCT | ACCOUNT

Choose your Product

FREE TIER	ENTERPRISE	AWSMARKETPLACE
✓ Billing and Utilization Visibility	✓ Billing and Utilization Visibility	✓ Billing and Utilization Visibility
✓ Recommendations for Optimization	✓ Recommendations for Optimization	✓ Recommendations for Optimization
✓ Containers Visibility	✓ Containers Visibility	✓ Containers Visibility
✓ Application Visibility	✓ Application Visibility	✓ Application Visibility
✓ Automation	✓ Automation	✓ Automation
✓ Limited *(Historical Data and Instances)*		
SELECT PLAN	SELECT PLAN	SELECT PLAN

Step 3

Provide your company email id and create a password that you wish to use to signin.



On-boarding

EULA | PRODUCT | ACCOUNT

Let us know something about you

Email (required) ✕

Password ✕

* Password should be atleast 6 digit and combination of symbol, upper and lower case letters

Confirm Password

You are Onboarded Now.

Please note, Aquila Clouds discovers objects in your environment and retrieves utilization metrics from it via Cloudwatch API (*please note cloudwatch api use will incur charges from AWS. Please refer to AWS cloudwatch pricing information for charges incurred*). You can check those charges in AWS Console -> Billing -> Cost Explorer.

Before you login and start using the product, you need to add a cloud environment like AWS, Azure etc. And before we add the environment, we need to create an IAM role, a s3 bucket and an access policy in AWS console.

AWS Specific Instructions

Steps for creating IAM Role

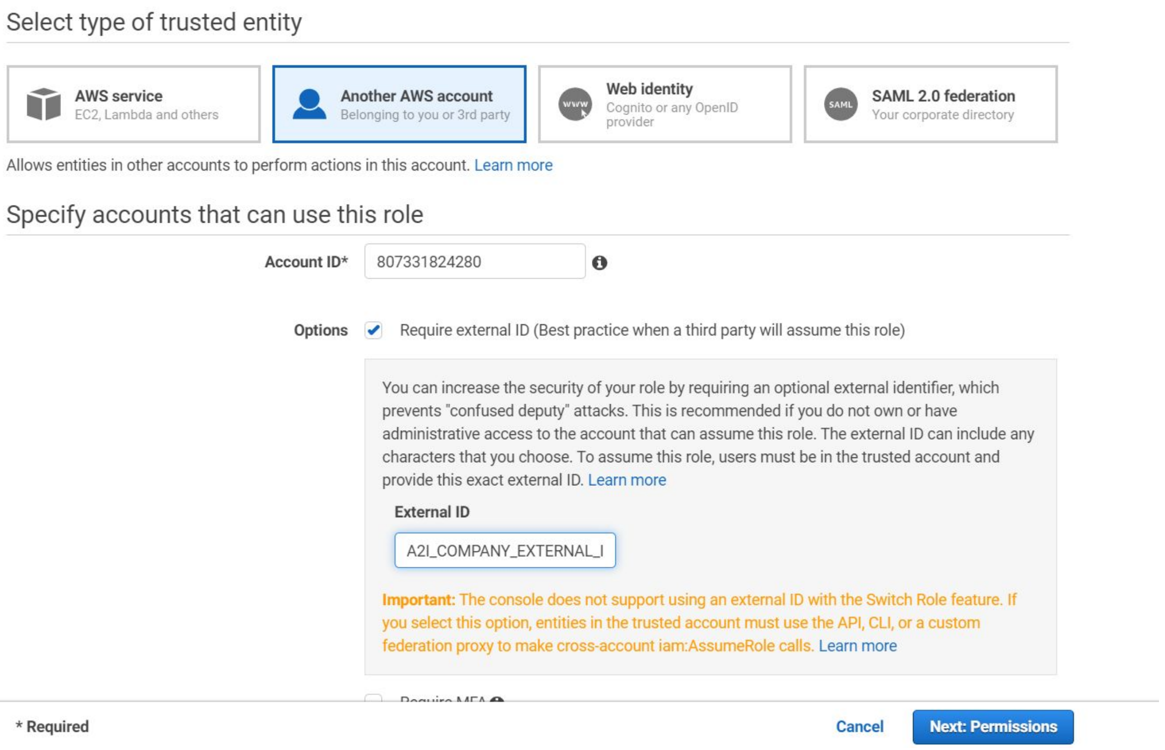
We recommend that you use the Role Creator Tool provided by us to create the role. Its easy and reliable way to create an IAM role for this application.
If you can not use the tool for some reason, please follow the steps elaborated below.

STEP 1 : In AWS console go to IAM service. Click Roles -> Create Role

STEP 2 : Choose another AWS Account

STEP 3: Enter the AQUILA CLOUDS AWS ACCOUNT ID (807331824280)

STEP 4: Select the checkbox for require EXTERNALID and enter the ID (A2I_COMPANY_EXTERNAL_ID) as shown below



Select type of trusted entity

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

Account ID* 807331824280

Options ☑ Require external ID (Best practice when a third party will assume this role)

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more

External ID A2I_COMPANY_EXTERNAL_I

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. Learn more

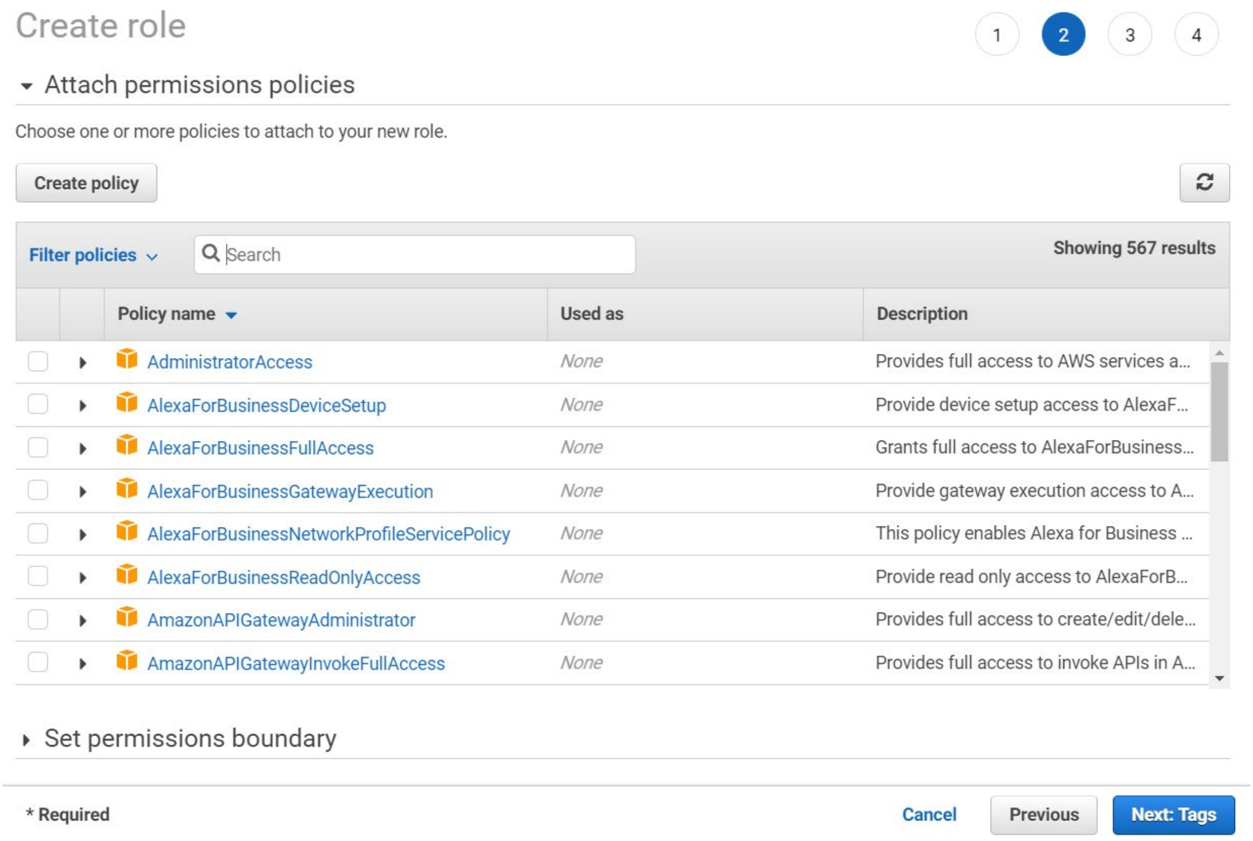
☐ Require MFA

* Required

Step 4

Assign all the required permissions for the platform by referring to the permissions section[Permissions needed in IAM Role to enable features](). In case you wish to limit the permissions to the lowest level ie Read Only then select these 2 permissions in the permissions screen. else please refer information below to provide other permissions required to realize the full power of the platform

- AmazonEC2ReadOnlyAccess
- CloudWatchReadOnlyAccess



Create role

▾ Attach permissions policies

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

Showing 567 results

		Policy name ▾	Used as	Description
□	▸	AdministratorAccess	None	Provides full access to AWS services a...
□	▸	AlexaForBusinessDeviceSetup	None	Provide device setup access to AlexaF...
□	▸	AlexaForBusinessFullAccess	None	Grants full access to AlexaForBusiness...
□	▸	AlexaForBusinessGatewayExecution	None	Provide gateway execution access to A...
□	▸	AlexaForBusinessNetworkProfileServicePolicy	None	This policy enables Alexa for Business ...
□	▸	AlexaForBusinessReadOnlyAccess	None	Provide read only access to AlexaForB...
□	▸	AmazonAPIGatewayAdministrator	None	Provides full access to create/edit/dele...
□	▸	AmazonAPIGatewayInvokeFullAccess	None	Provides full access to invoke APIs in A...

▸ Set permissions boundary

* Required

Step 5

Skip the Tags step and Give a name and create ROLE

Step 6

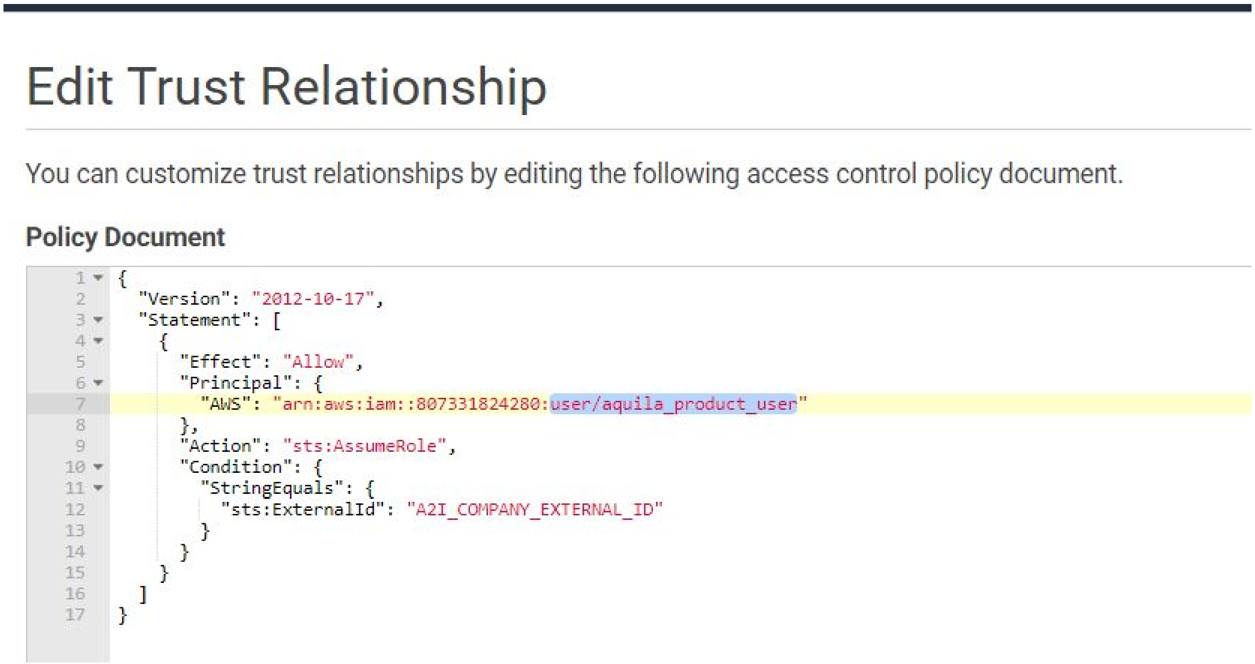
Go to the Roles Page and open the role you just created

Step 7

Select the Trust Relationships tab and click Edit Trust Relationship

Step 8

replace the word root with this string *user/aquila_product_user* as done in the image below and click update trust policy button



Edit Trust Relationship

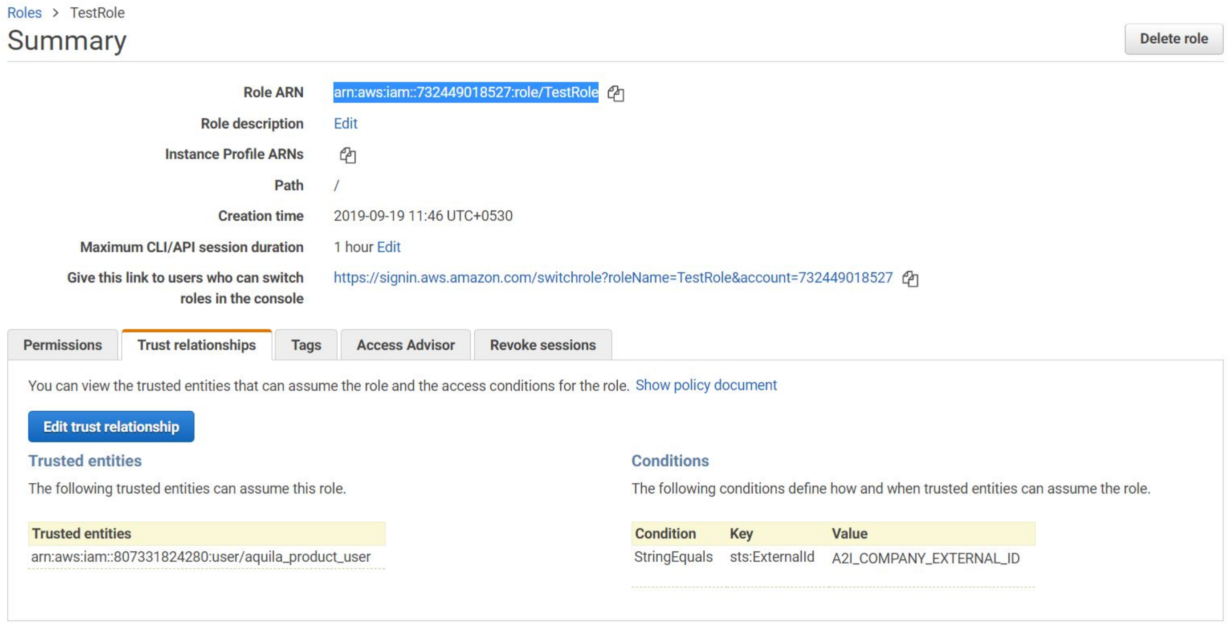
You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::807331824280:user/aquila_product_user"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "A2I_COMPANY_EXTERNAL_ID"
        }
      }
    }
  ]
}
```

Step 9

Copy the *Role ARN* (highlighted in the example image below) . This is the string you need to enter in the Add Environment screen of Aquila.



Roles > TestRole

Summary

Role ARN	arn:aws:iam::732449018527:role/TestRole
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2019-09-19 11:46 UTC+0530
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=TestRole&account=732449018527

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Trusted entities

The following trusted entities can assume this role.

Trusted entities
arn:aws:iam::807331824280:user/aquila_product_user

Conditions

The following conditions define how and when trusted entities can assume the role.

Condition	Key	Value
StringEquals	sts:ExternalId	A2I_COMPANY_EXTERNAL_ID

Permissions needed in IAM Role to enable features

Users can choose to grant various levels of permissions to access different Aquila Clouds features. We strongly suggest that all permissions be granted as listed to derive maximum value from the platform.

Enabling Billing

Enabling access to detailed Billing data as detailed in the steps below.

Refer AWS S3 doc: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-s3.html.

Steps to activate S3 based billing

Steps:

1) Create an S3 bucket to store the daily billing reports of your AWS resources that are generated by AWS. Log in to the Amazon S3 console to create a bucket: https://console.aws.amazon.com/s3

2) To create billing report and schedule the AWS Cost and Usage report to be generated daily.

a) *Open the Billing and Cost Management console:* *https://console.aws.amazon.com/billing/*

b) Click Reports > Create report.

c) On the Select Content page, configure the following properties:

Report name: *Type a name for the report*

Time unit: *Select Daily to aggregate report data every day.*

Include:

Enable **Include the Resource IDs** check box to associate the resources with the business services.

Enable **Automatically refresh your Cost & Usage Report when charges are detected for previous months with closed bills** checkbox

d) Click Next.

3) On the Report details page, configure the following properties:

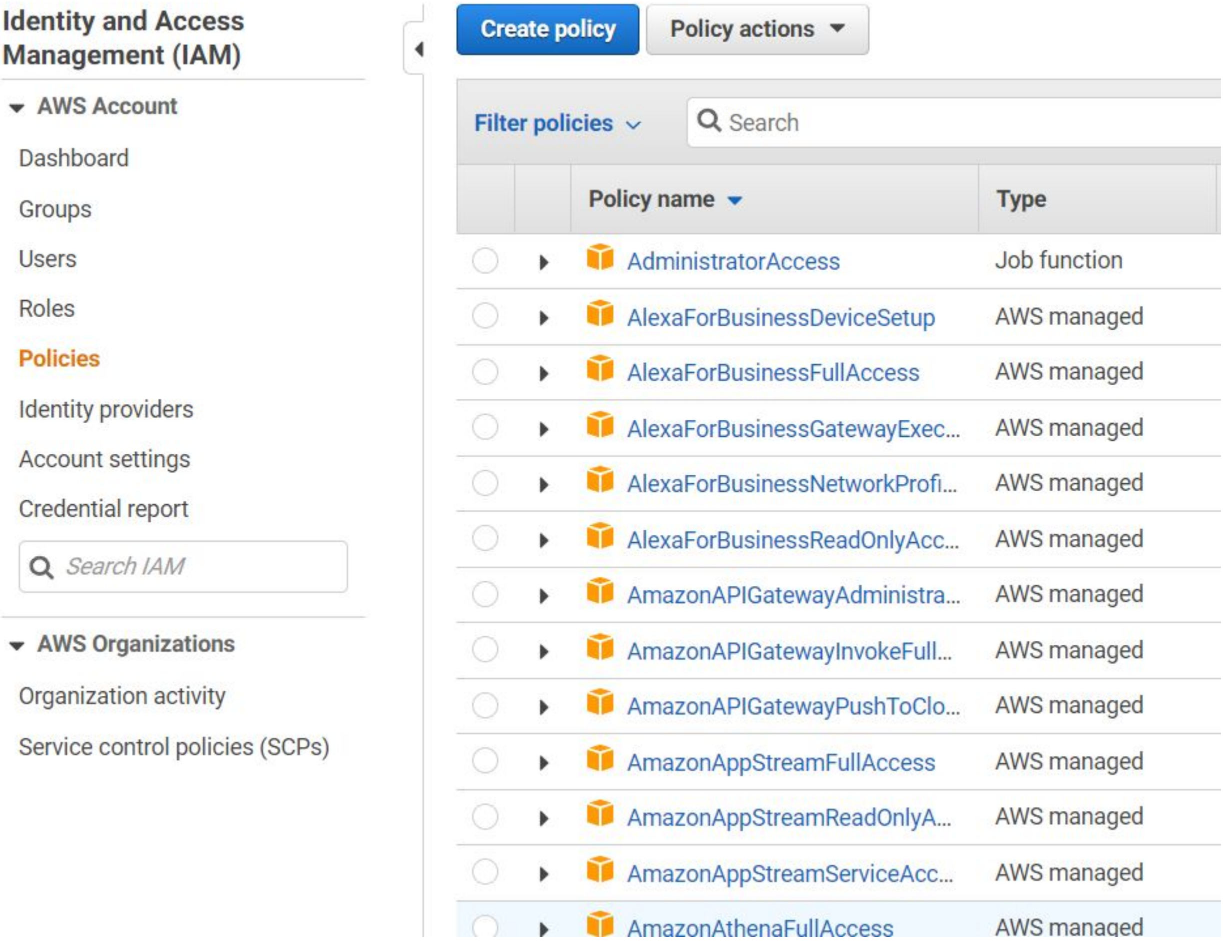
a) Click on the Configure and select the s3 bucket we just created. Verify whether the bucket has appropriate permissions to store the reports and click Save.

b) In the Report path prefix box, type the prefix that you want to append to the report name. Select *Daily* time granularity and *Create new report version.*

c) Click Next.

d) Review the settings, and click Review and Complete

4) Create a policy that grants access to the s3 bucket we created. Go to AWS console -> IAM -> Policies -> Create Policy.

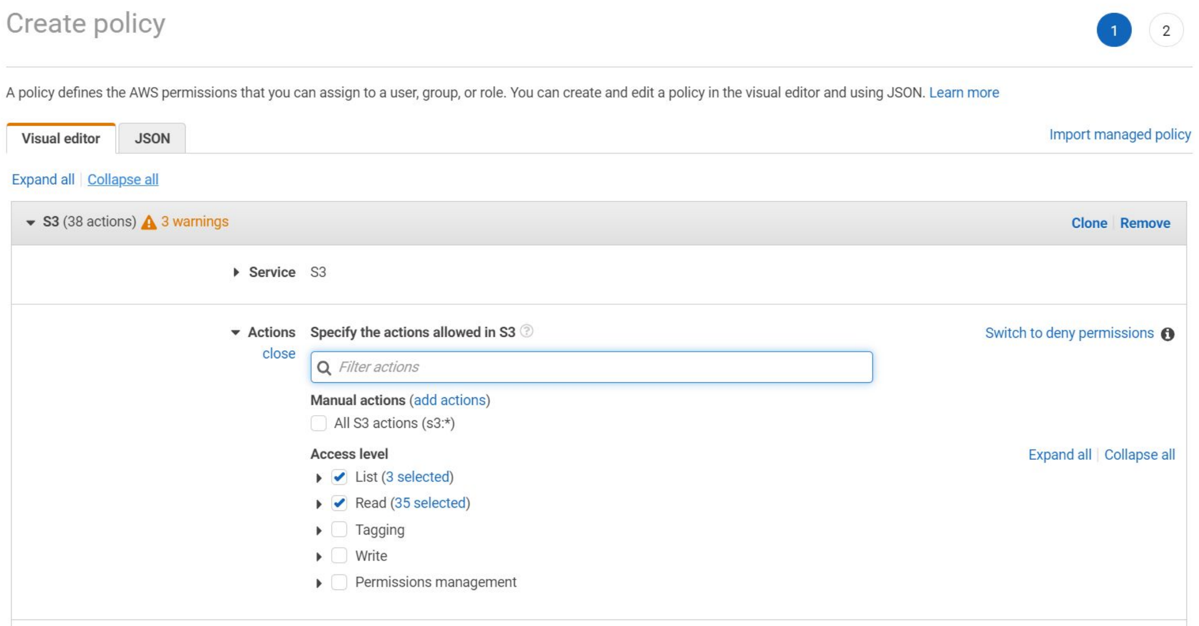


Identity and Access Management (IAM)

- AWS Account
  - Dashboard
  - Groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Credential report
- Search IAM
- AWS Organizations
  - Organization activity
  - Service control policies (SCPs)

		Policy name ▾	Type
○	▸	AdministratorAccess	Job function
○	▸	AlexaForBusinessDeviceSetup	AWS managed
○	▸	AlexaForBusinessFullAccess	AWS managed
○	▸	AlexaForBusinessGatewayExec...	AWS managed
○	▸	AlexaForBusinessNetworkProfi...	AWS managed
○	▸	AlexaForBusinessReadOnlyAcc...	AWS managed
○	▸	AmazonAPIGatewayAdministra...	AWS managed
○	▸	AmazonAPIGatewayInvokeFull...	AWS managed
○	▸	AmazonAPIGatewayPushToClo...	AWS managed
○	▸	AmazonAppStreamFullAccess	AWS managed
○	▸	AmazonAppStreamReadOnlyA...	AWS managed
○	▸	AmazonAppStreamServiceAcc...	AWS managed
○	▸	AmazonAthenaFullAccess	AWS managed

b) Select s3 service and choose List & Read Actions as shown below.



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

S3 (38 actions) 3 warnings — Clone | Remove

Service: S3

Actions (close) — Specify the actions allowed in S3 — Switch to deny permissions

Filter actions

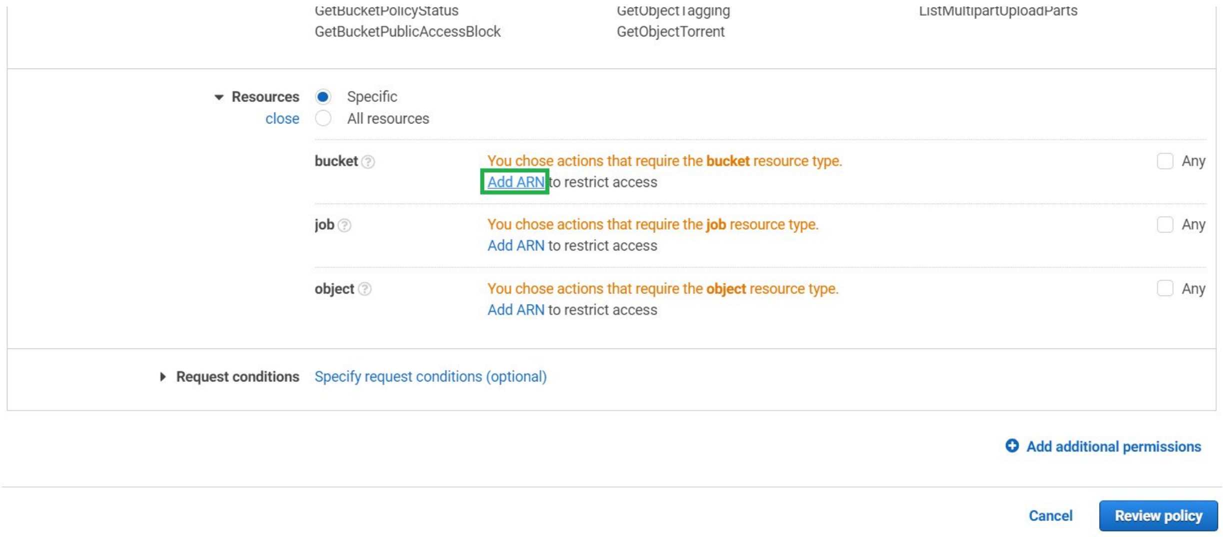
Manual actions (add actions)

☐ All S3 actions (s3:*)

Access level — Expand all | Collapse all

- ☑ List (3 selected)
- ☑ Read (35 selected)
- ☐ Tagging
- ☐ Write
- ☐ Permissions management

c) Click on resources and then on ‘Add ARN’ from the *bucket* section highlighted below



GetBucketPolicyStatus GetObjectTagging ListMultipartUploadParts

GetBucketPublicAccessBlock GetObjectTorrent

Resources (close)

● Specific

○ All resources

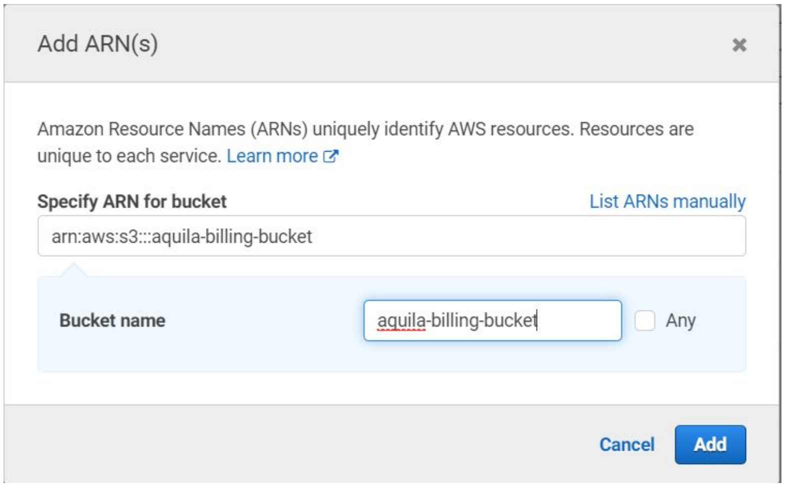
bucket	You chose actions that require the **bucket** resource type. Add ARN to restrict access	☐ Any
job	You chose actions that require the **job** resource type. Add ARN to restrict access	☐ Any
object	You chose actions that require the **object** resource type. Add ARN to restrict access	☐ Any

Request conditions — Specify request conditions (optional)

Add additional permissions

Cancel | Review policy

d) Enter the Bucket name and click on Add.



Add ARN(s)

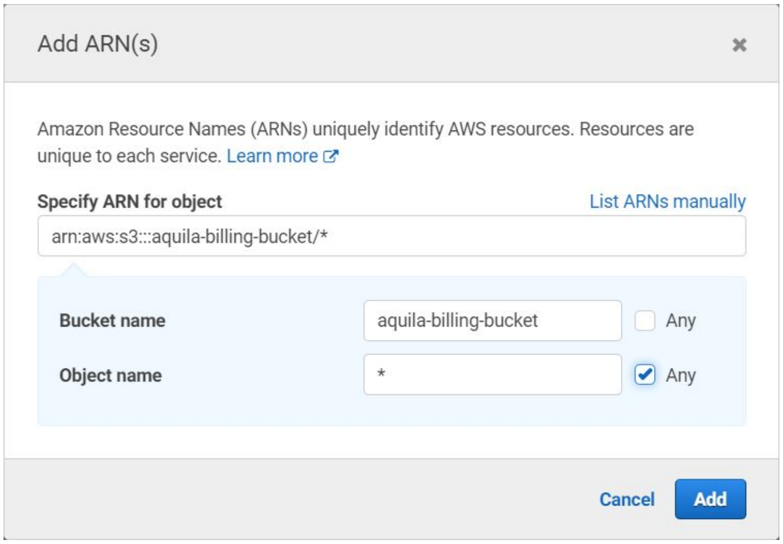
Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for bucket

arn:aws:s3:::aquila-billing-bucket

Bucket name: aquila-billing-bucket □ Any

e) Now click on Add ARN' from *object* section and fill in detail as shown below & click Add.



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

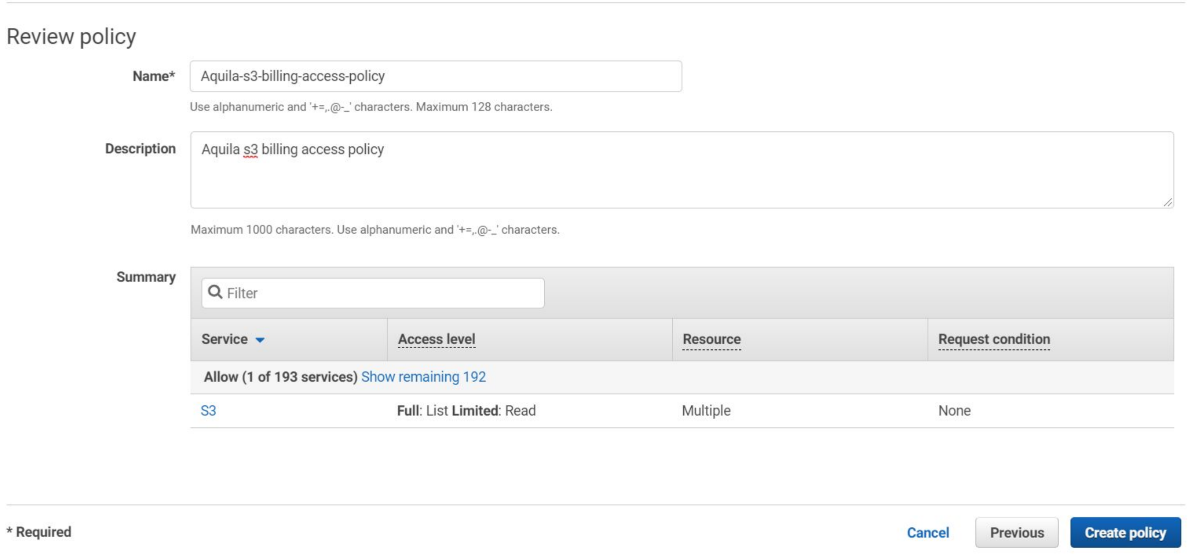
Specify ARN for object

arn:aws:s3:::aquila-billing-bucket/*

Bucket name: aquila-billing-bucket □ Any

Object name: * ☑ Any

f) Now, click on Review Policy and enter Name & Description before clicking on Create Policy.



Review policy

Name* Aquila-s3-billing-access-policy

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

Description Aquila s3 billing access policy

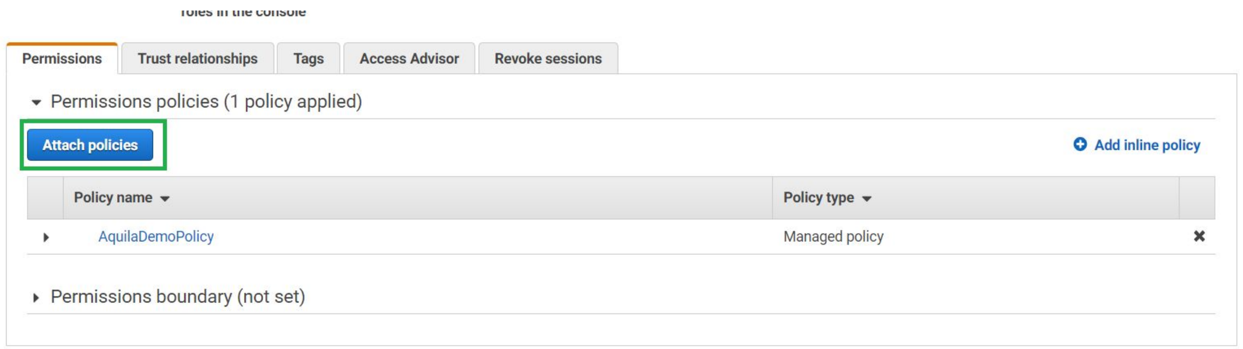
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 193 services) Show remaining 192			
S3	**Full**: List **Limited**: Read	Multiple	None

* Required

g) Next step is to attach this policy to the role we created for Aquila. Go to IAM -> Roles, select the role and click on Attach Policies

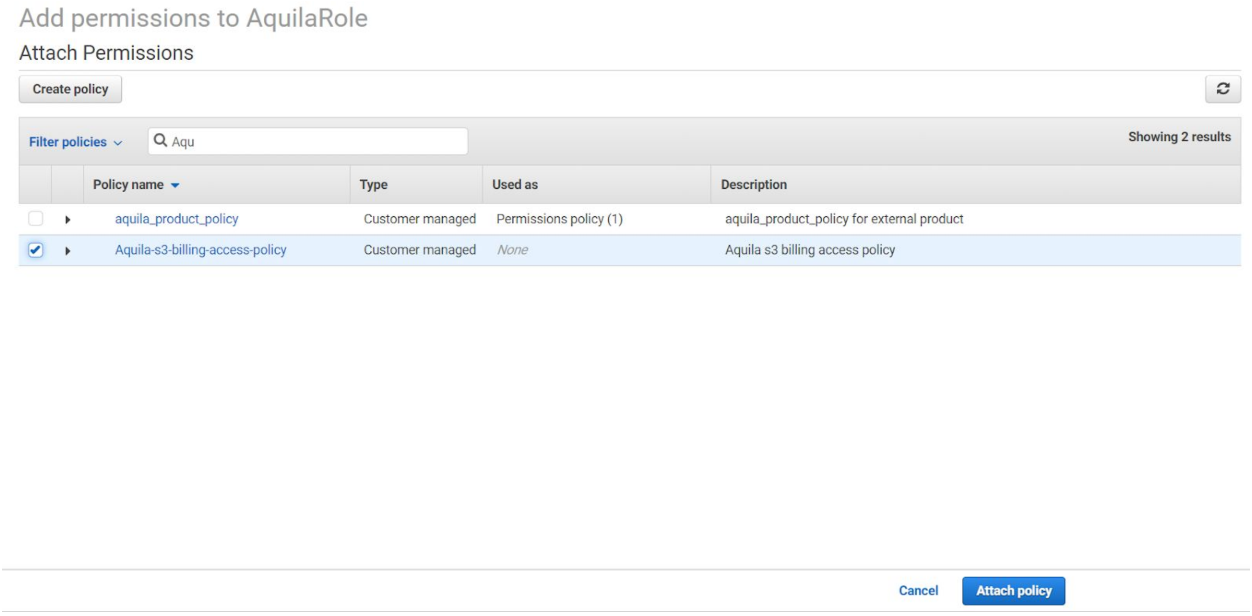


Permissions policies (1 policy applied)

Policy name	Policy type
AquilaDemoPolicy	Managed policy

Permissions boundary (not set)

h) Select the newly created policy from list and click on Attach policy



Add permissions to AquilaRole

Attach Permissions

		Policy name	Type	Used as	Description
□	▸	aquila_product_policy	Customer managed	Permissions policy (1)	aquila_product_policy for external product
☑	▸	Aquila-s3-billing-access-policy	Customer managed	None	Aquila s3 billing access policy

5) Go s3 -> Buckets and make sure that our bucket json permissions look something like below:

```
{
Version: 2012-10-17,
  Statement: [
  {
Effect: Allow,
Principal: {
  AWS: 386209384616
},
Action: [
  s3:GetBucketAcl,
  s3:GetBucketPolicy
],
Resource: arn:aws:s3:::<bucketname>
  },
  {
Effect: Allow,
Principal: {
  AWS: 386209384616
},
Action: s3:PutObject,
Resource: arn:aws:s3:::<bucketname>/*
  }
  ]
}
```

Replace <bucketname> with the name of your bucket.

Do not change the Principal number 386209384616. AWS uses it to send reports to your bucket.

Feature-wise breakup of Permissions

Permissions required for Visibility,Recommendation, Alerts (Cost, Recommendation, Alerts, Utilization, Container and Application Dashboards). This is apart from billing permissions stated above

```
ec2:DescribeSnapshots,
ec2:DescribeVolumes,
ec2:DescribeVolumeStatus,
ec2:DescribeSnapshotAttribute,
ec2:DescribeInstances,
ec2:DescribeVolumeAttribute,
ec2:DescribeInstanceStatus,
ec2:DescribeTags,
ecs:List*,
ecs:Describe*,
eks:List*,
eks:Describe*,
ec2:Describe*,
elasticloadbalancing:Describe*,
cloudwatch:ListMetrics,
cloudwatch:GetMetricStatistics,
cloudwatch:GetMetricData,
cloudwatch:Describe*,
autoscaling:Describe*,
```

Permissions required for Actions/Automation features of Aquila Clouds (Actions enabled in Recommendation Dashboard, Action Console). These are in addition to those needed for Visibility/Recommendation Dashboards and Billing mentioned above.

```
ec2:CopySnapshot
ec2:ModifyVolumeAttribute,
ec2:CreateImage,
ec2:ResetInstanceAttribute,
ec2:CopyImage,
 ec2:StartInstances,
 ec2:StopInstances
 ec2:ImportSnapshot,
ec2:CreateLaunchTemplateVersion,
ec2:CreateLaunchTemplate,
ec2:ModifyInstanceCreditSpecification,
ec2:AssociateIamInstanceProfile
ec2:UnmonitorInstances
ec2:MonitorInstances,
ec2:ReportInstanceStatus,
ec2:DeleteVolume,
ec2:ModifySnapshotAttribute,
ec2:StartInstances,
ec2:CreatePlacementGroup,
ec2:ImportImage,
ec2:DetachVolume,
ec2:ModifyVolume,
ec2:ResetImageAttribute,
ec2:CreateTags,
ec2:RegisterImage,
ec2:ModifyInstanceEventStartTime,
ec2:RunInstances,
ec2:StopInstances,
ec2:CreateVolume,
ec2:EnableVolumeIO,
ec2:AttachVolume,
ec2:ImportVolume,
ec2:RequestSpotInstances,
ec2:DeleteTags,
ec2:RunScheduledInstances,
ec2:RequestSpotFleet,
ec2:ModifyImageAttribute,
ec2:CreateSnapshot,
ec2:ModifyInstanceAttribute,
ec2:ModifyReservedInstances,
ec2:RebootInstances,
ec2:CreateInstanceExportTask,
ec2:ModifyInstancePlacement,
ec2:TerminateInstances,
ec2:ImportInstance,
ec2:ResetSnapshotAttribute,
ec2:ModifyInstanceCapacityReservationAttributes
```

,

Comprehensive set of Permissions required for entire set of features as single list (This is a cumulative list of both the distinct lists above)

```
{
   Version: 2012-10-17,
   Statement: [
      {
         Sid: VisualEditor0,
         Effect: Allow,
         Action: [
            ec2:CopySnapshot,
            ec2:DescribeInstances,
            ec2:UnmonitorInstances,
            ec2:ModifyVolumeAttribute,
            ec2:MonitorInstances,
            ec2:CreateImage,
            ec2:ResetInstanceAttribute,
            ec2:CopyImage,
ec2:DescribeSnapshots,
ec2:ReportInstanceStatus,
ec2:DeleteVolume,
ec2:DescribeVolumeStatus,
ec2:ModifySnapshotAttribute,
ec2:StartInstances,
ec2:CreatePlacementGroup,
ec2:DescribeVolumes,
ec2:ImportImage,
ec2:DetachVolume,
ec2:ModifyVolume,
ec2:ResetImageAttribute,
ec2:CreateTags,
ec2:DescribeSnapshotAttribute,
ec2:RegisterImage,
ec2:ModifyInstanceEventStartTime,
ec2:RunInstances,
ec2:StopInstances,
ec2:DescribeVolumeAttribute,
ec2:CreateVolume,
ec2:EnableVolumeIO,
ec2:ModifyInstanceCapacityReservationAttributes,
ec2:AttachVolume,
ec2:ImportVolume,
ec2:RequestSpotInstances,
ec2:DeleteTags,
ec2:RunScheduledInstances,
ec2:RequestSpotFleet,
ec2:ModifyImageAttribute,
ec2:CreateSnapshot,
ec2:ModifyInstanceAttribute,
ec2:ModifyReservedInstances,
ec2:DescribeInstanceStatus,
ec2:RebootInstances,
ec2:CreateInstanceExportTask,
ec2:ModifyInstancePlacement,
ec2:TerminateInstances,
ec2:ImportInstance,
ec2:DescribeTags,
ec2:ResetSnapshotAttribute,
ec2:ImportSnapshot,
                ec2:CreateLaunchTemplateVersion,
                ec2:CreateLaunchTemplate,
                ec2:ModifyInstanceCreditSpecification,
                ec2:AssociateIamInstanceProfile,


                ecs:List*,
                ecs:Describe*,
                eks:List*,
                eks:Describe*,


                 ec2:Describe*,


                 elasticloadbalancing:Describe*,

                 cloudwatch:ListMetrics,
                cloudwatch:GetMetricStatistics,
                cloudwatch:GetMetricData,
                cloudwatch:Describe*,

                autoscaling:Describe*,


                ec2:DescribeInstances,
                ec2:StartInstances,
                ec2:StopInstances


            ],
            Resource: *
        }
    ]
}
```

Billing

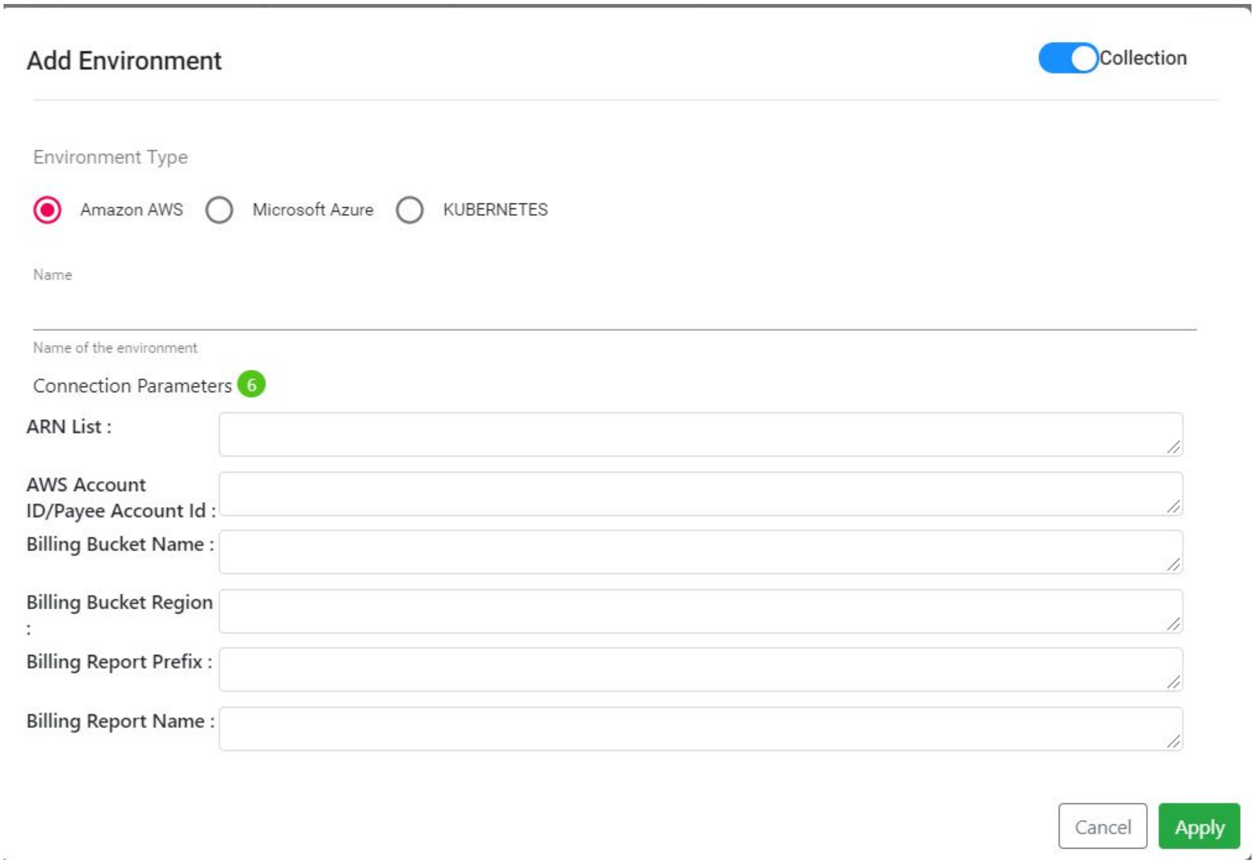
```
{
   “Version”: 2012-10-17,
   “Statement”: [
      {
            “Effect”: “Allow”,
            “Action”: [
                “s3:Get*”,
                “s3:List*”
            ],
            “Resource”: [
                “arn:aws:s3:::billing-a2i”,
                “arn:aws:s3:::billing-a2i/*”
            ]
        }
    ]
}
```

Add Environment

Below section explains how to add AWS and Azure environments to Aquila.

Add AWS Environment

To start deriving value from the Aquila Clouds Cloud Management Product, you must add one or more environment such as Amazon AWS Cloud Account, Microsoft Azure Cloud Account.
The example below is for Amazon AWS. Go to Administrator -> Manage Environments -> Add Environment.



Add Environment

Collection

Environment Type

● Amazon AWS ○ Microsoft Azure ○ KUBERNETES

Name

Name of the environment

Connection Parameters 6

ARN List :

AWS Account ID/Payee Account Id :

Billing Bucket Name :

Billing Bucket Region :

Billing Report Prefix :

Billing Report Name :

.

Description of Fields

1. **List of Role ARNs :** Provide the Role ARN or List of Role ARNs corresponding to the cross account roles permitting access to your Cloud accounts for Aquila Clouds. You would typically have a list of role ARNs when a set of related accounts (Root and it's Sub accounts together) need to be managed by Aquila Clouds. The role ARNs for another set of related accounts wouid be added as part of different Environment altogether. More information here.

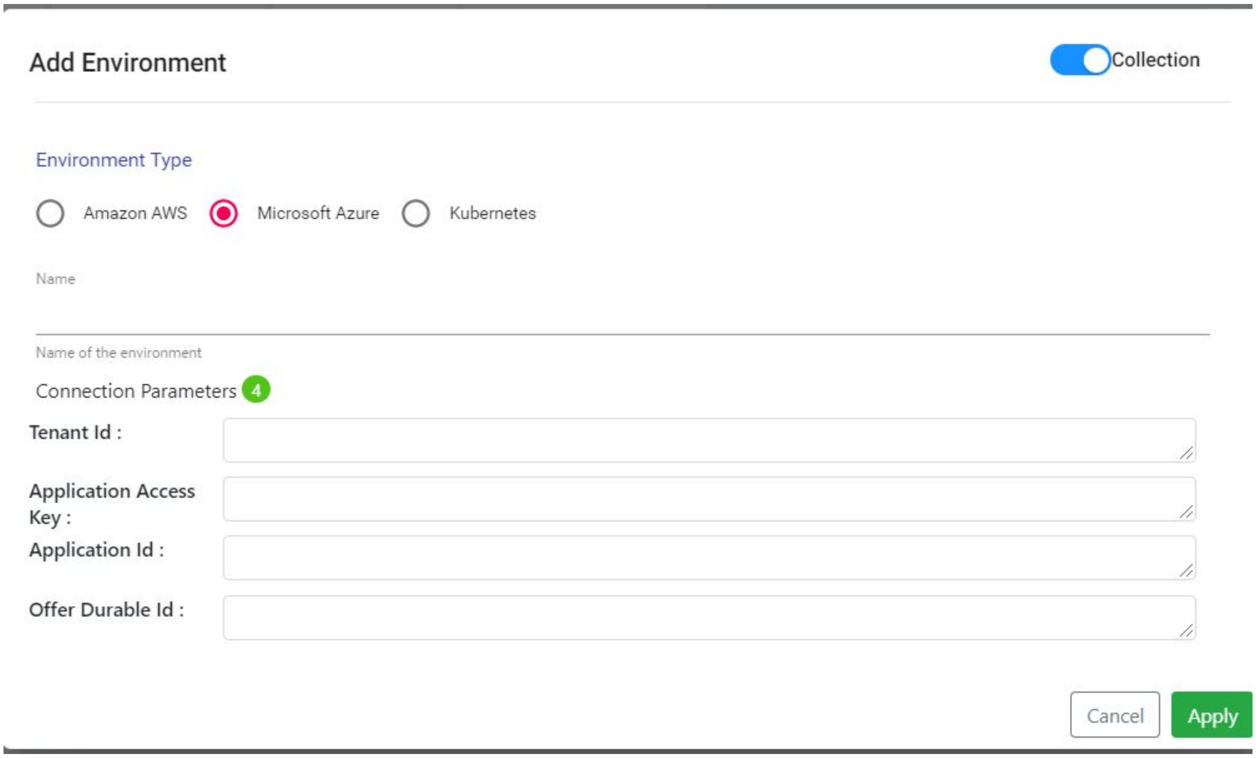
2. **Payee Account ID/Root Account ID:** Provide the Payee Account ID for the AWS Cloud environment you wish to manage using Aquila Clouds. In the case where a explicit Payee Account is not designated, you can provide the Root Account.

3. Billing information :
    a. Provide the Billing S3 Bucket Name (more info here),
    b. Billing S3 Bucket Region (AWS Region code(e.g., us-east-2 for Ohio))
    c. Billing Report Prefix (Billing prefix name without '/' as mentioned in steps here.)
    d. Billing Name to be used by the Aquila Clouds platform to analyze cost incurred for your Cloud environment.

Click Apply and confirm. Your AWS environment is now added.

Add Azure Environment

.



Add Environment

Environment Type

○ Amazon AWS ● Microsoft Azure ○ Kubernetes

Name

Name of the environment

Connection Parameters 4

Tenant Id :

Application Access Key :

Application Id :

Offer Durable Id :

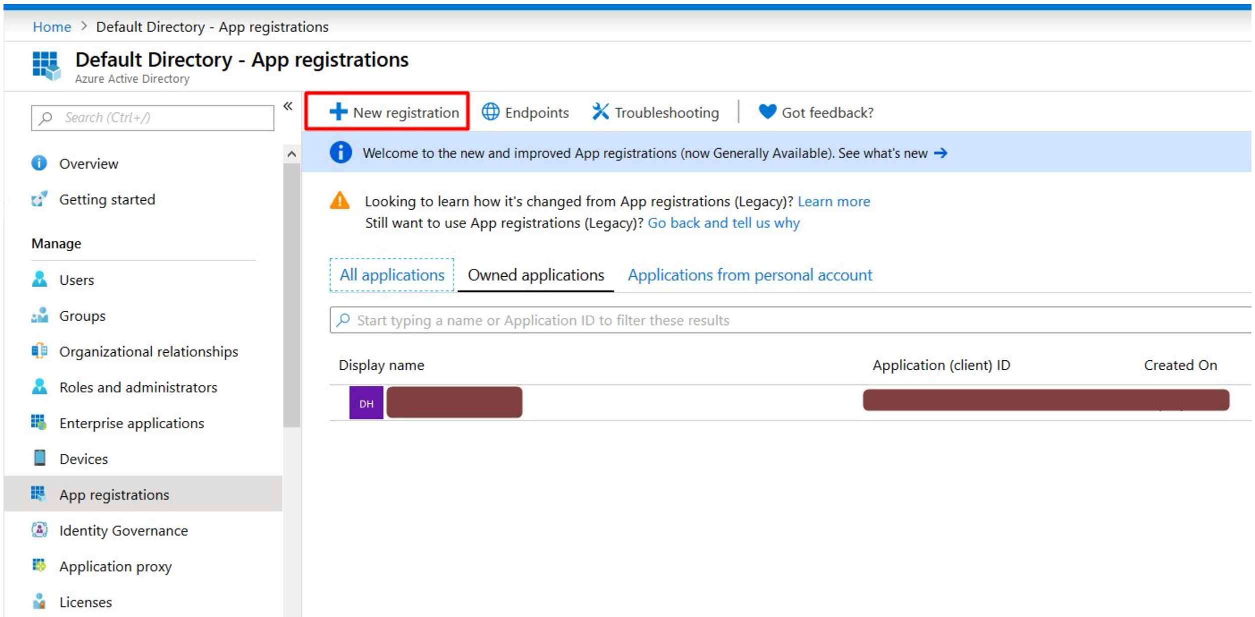
Description of fields:

1) Name: Name for your Azure environment like *Azure - <Company name>*.
2) Tenant ID: Navigate to Azure Portal -> Azure Active Directory -> Properties -> The Directory ID in there is your Tenant ID.
3) Application Access Key: This key needs to be copied and saved somewhere when its created while registering the application. If you do not this key ready, it can be created by registering a new application for

the sole purpose of on-boarding it on Aquila. Below are the steps to follow to register an application.

a) Go to Azure Portal -> Azure Active Directory -> App registrations

b) Click on +New Registration

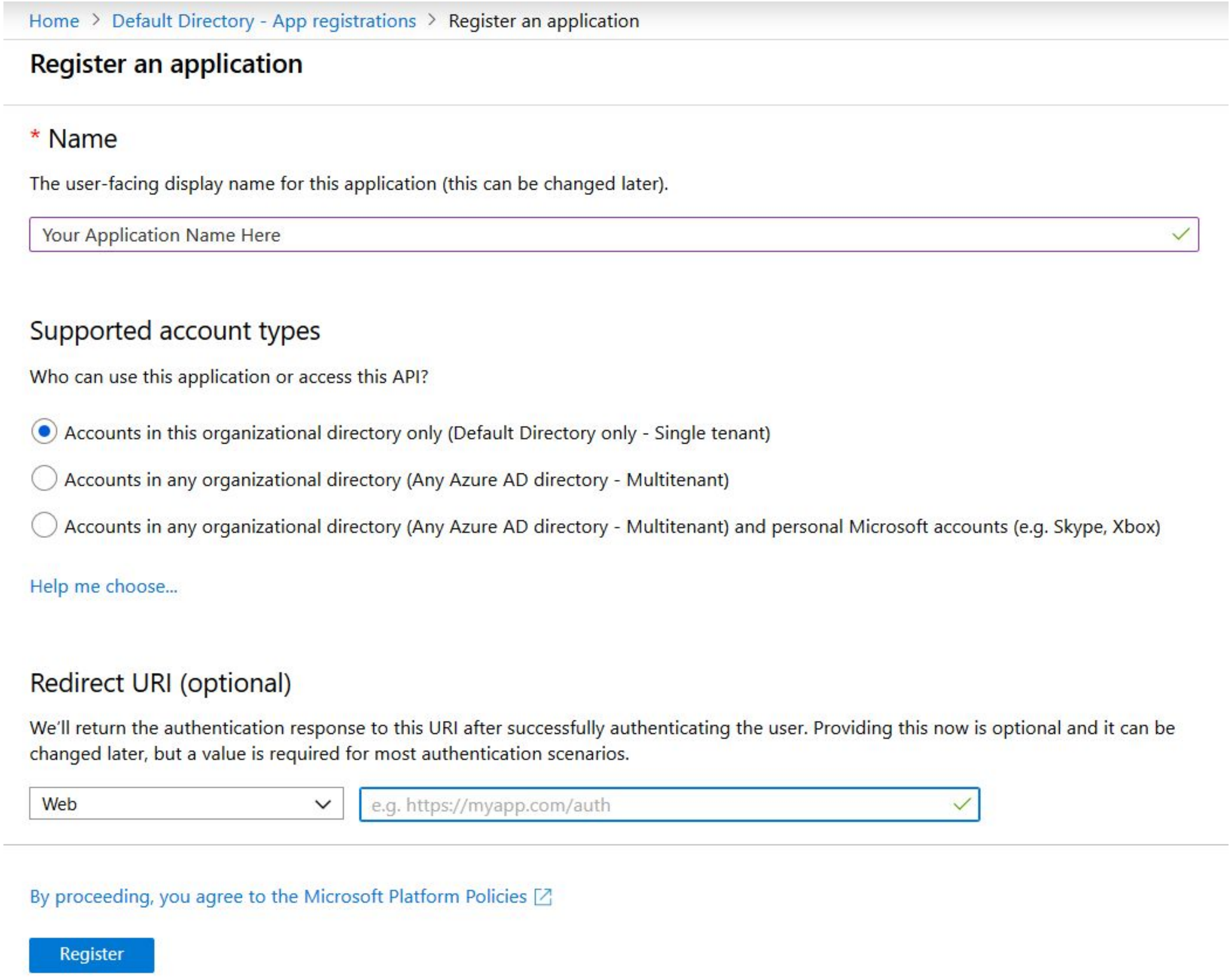


Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

Display name	Application (client) ID	Created On
DH [redacted]	[redacted]	

c) Enter your application name and click on Register



Home > Default Directory - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Your Application Name Here ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant)

○ 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)

Help me choose...

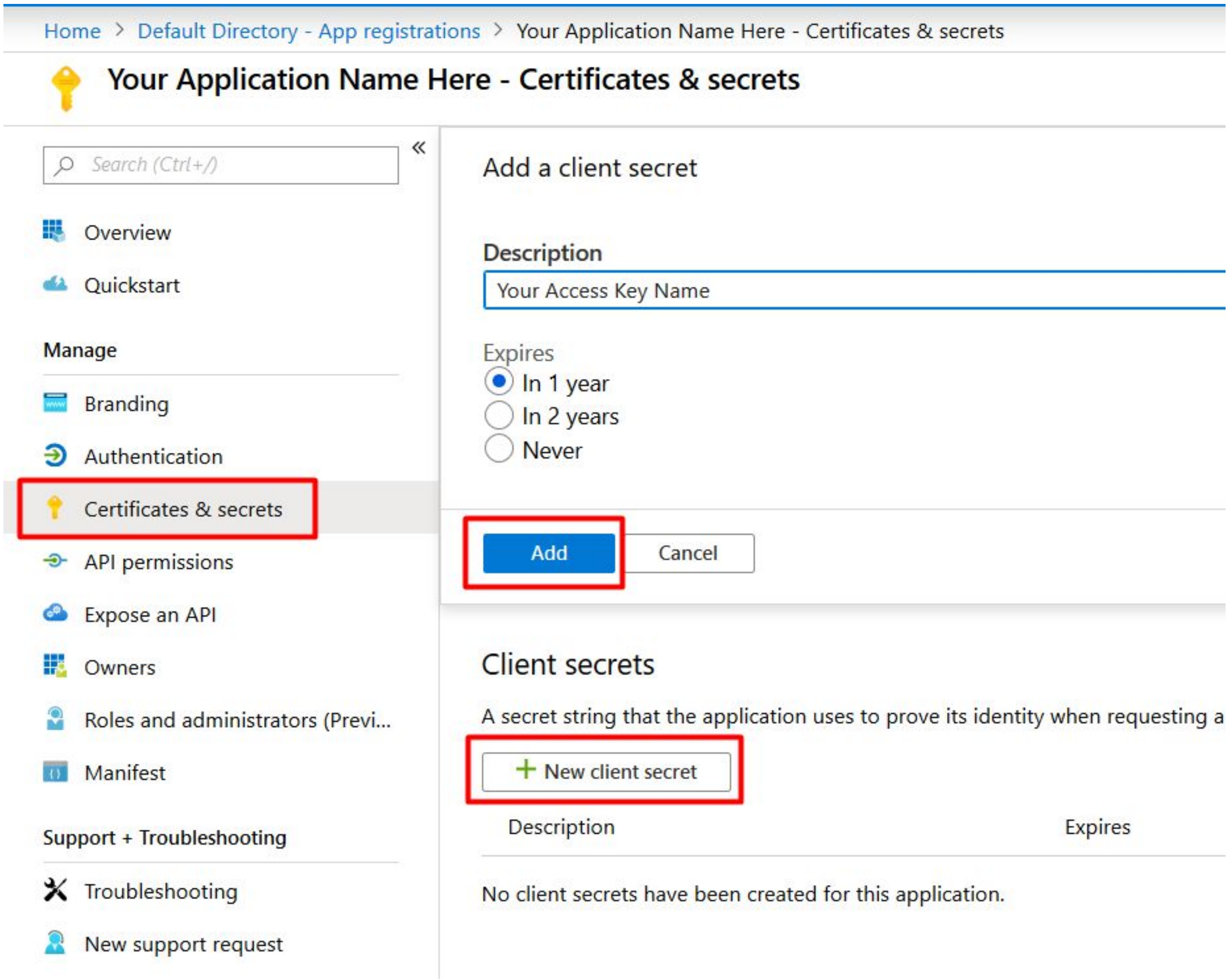
Redirect URI (optional)

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.

Web | e.g. https://myapp.com/auth ✓

By proceeding, you agree to the Microsoft Platform Policies

d) Click on Certificates & secrets, then on +New client secret and then after naming the client secret, selecting the desired duration it stays alive for, click on Add.



Home > Default Directory - App registrations > Your Application Name Here - Certificates & secrets

Your Application Name Here - Certificates & secrets

Add a client secret

Description: Your Access Key Name

Expires
● In 1 year
○ In 2 years
○ Never

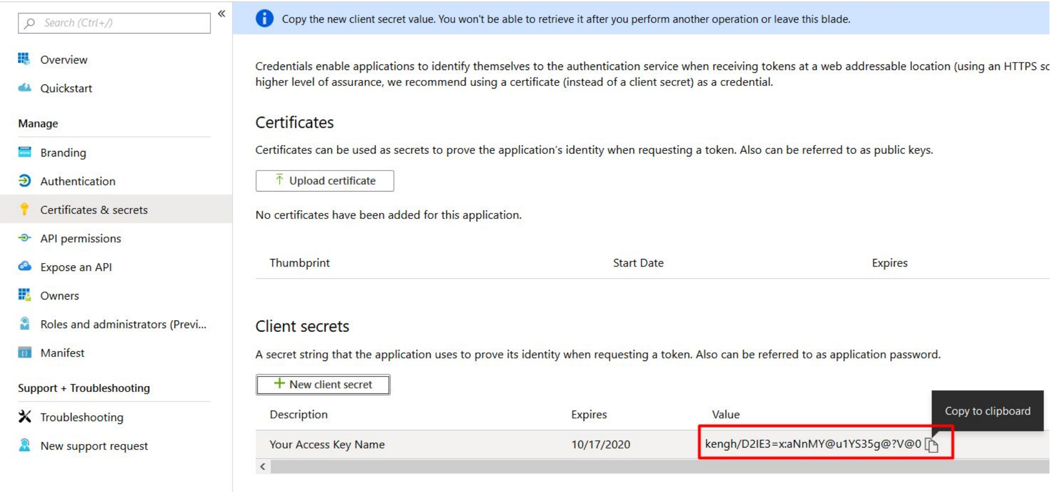
Client secrets

A secret string that the application uses to prove its identity when requesting a

Description	Expires

No client secrets have been created for this application.

e) **Please make sure you copy the secret key value and save it**. It'll be used to on-board the account on Aquila.



Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS sc higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

Client secrets

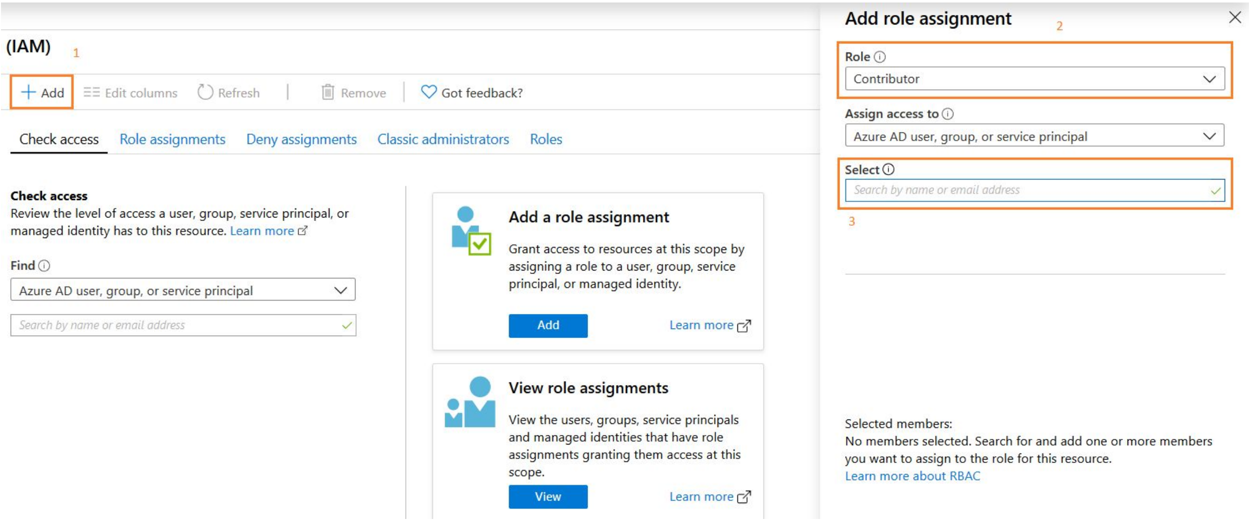
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
Your Access Key Name	10/17/2020	kengh/D2IE3=x:aNnMY@u1YS35g@?V@0

4) Application ID: Go to Azure Portal -> Azure Active Directory -> App registrations. Select the ID for desired registered App
5) Offer Durable ID: Go to Azure Portal -> Subscriptions -> Properties. The Offer ID is your offer Durable ID.
6) Role assignment

Though there is no Role Assignment field on the Add Environment form we need to assign an Azure IAM role to the application in order to get the data into Aquila. Below is how to do it:

a) Go to *All Services -> Subscriptions* and click on your subscription.
b) Now go to *Access Control (IAM)* & click on *+Add.* Then select the **Contributor** role as shown below.



Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: Azure AD user, group, or service principal

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

Role: Contributor

Assign access to: Azure AD user, group, or service principal

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

The **Contributor role** is needed when actions are to be performed like, starting & shutting off the VMs, changing VM types, deleting disks etc through Aquila.

Choose the **Reader role** when all you need is to read the data and not perform any actions on it.

c) Search and select the desired application in the third highlighted field in above screenshot and hit the Save button. A message saying '*Added Role assignment'* should be displayed.

7) Using all above inputs, fill in the fields on Add Environment form/window and click Apply & confirm.