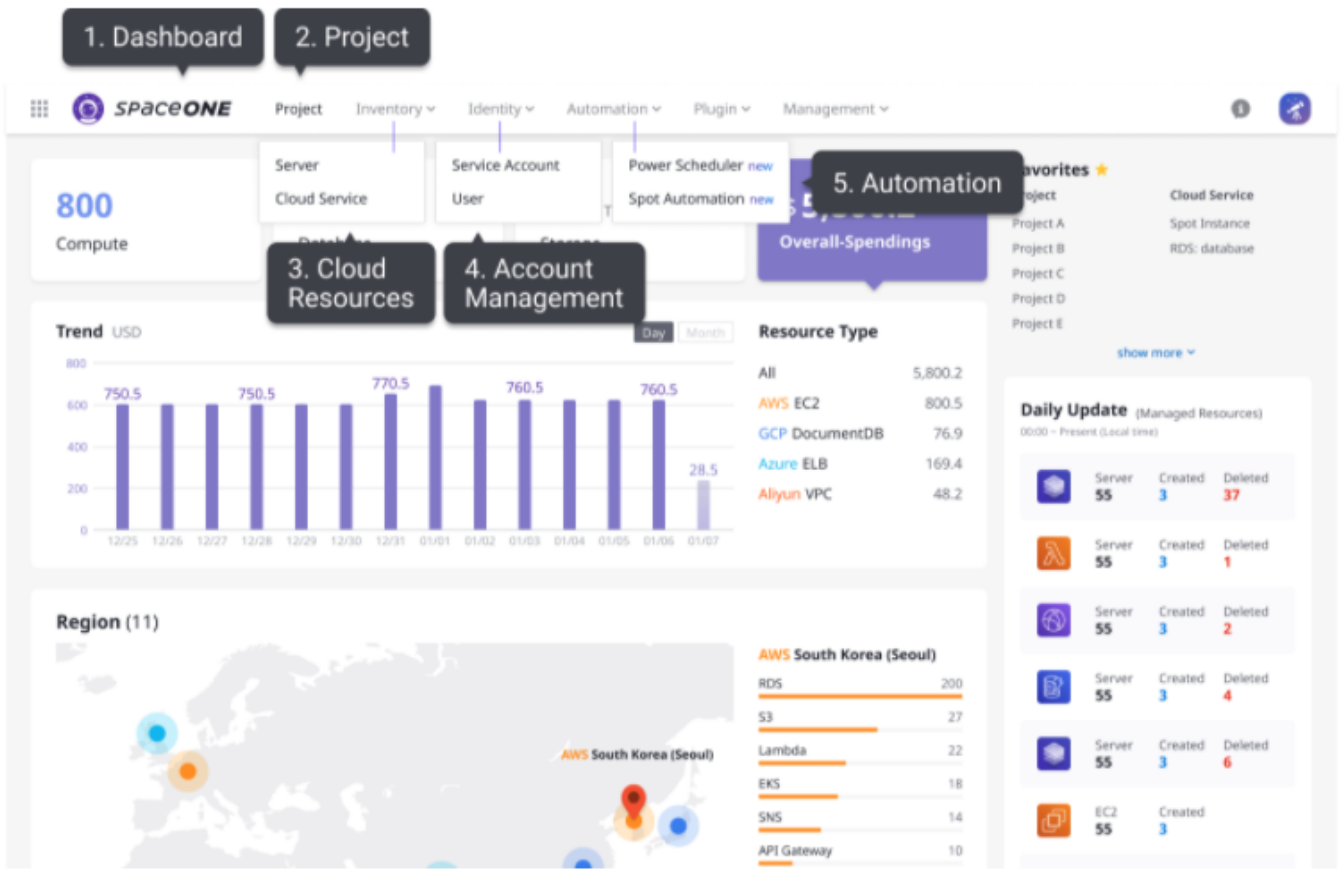
User Guide

User Guide of SpaceONE

Welcome aboard to SpaceONE

Introduction

SpaceONE, our mission is accelerate the **Cloud Native** Technology for sustainable Ecosystem.
SpaceONE is the Cloud management platform that enables integrating all **Multi-Clouds** regardless of the platforms which boosts and maximizes your operational efficiency in management.



1. Dashboard

Visualize your all cloud resources in one view.
About Domain Dashboard

2. Project

Consolidate your multi cloud resources by projects.
About Project

3. Cloud Resources

Discover & Classify your all cloud resources conveniently.
About Cloud Resources

4. Account Management

Managing credentials for cloud provider accounts.
About Service Account

5. Automation

Automate repetitive operational tasks, Optimize cloud resource costs.
About Power Scheduler

Learn how to use SpaceONE

Look up tasks and how to perform them using step by step guide.

Understand SpaceONE

Learn about SpaceONE and its fundamental concepts

SpaceONE

Key Differentiators

Try SpaceONE

Step by step guide for each user to user SpaceONE environment.

Basic Setup

Power Scheduler Quick Start

1 - Getting Started

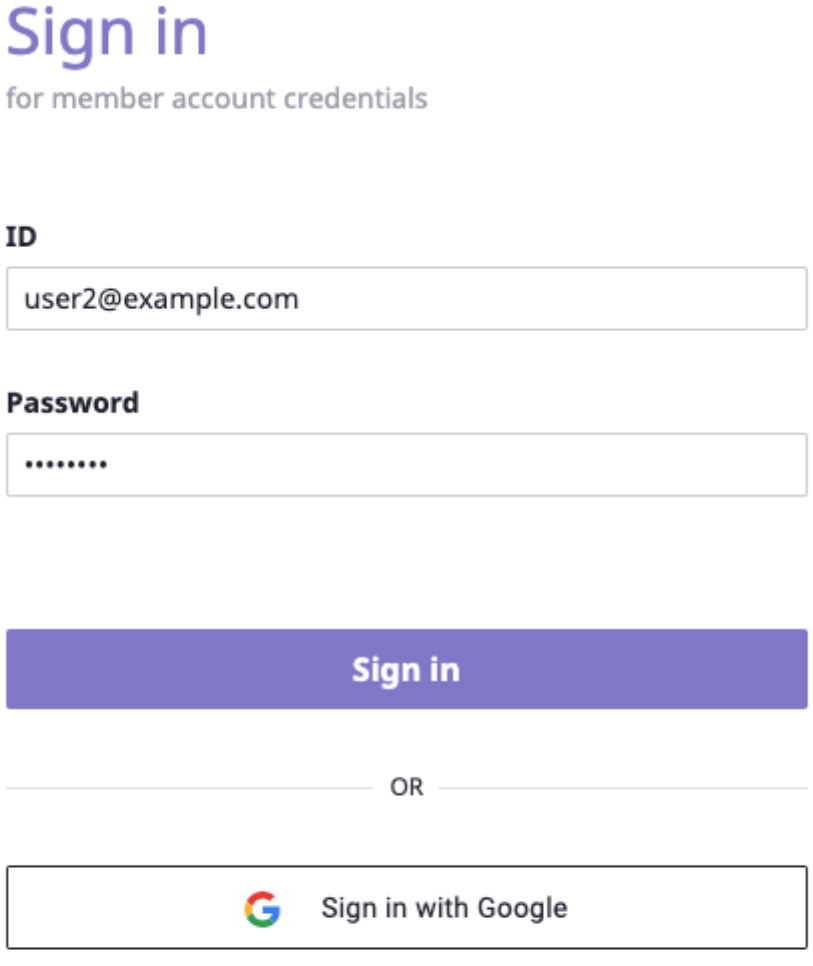
Step by Step Guide for Initial Setup

1.1 - Basic Setup

General user can manage resources by creating a project under the project group and registering a cloud account(service account) to created project.

Sign-in

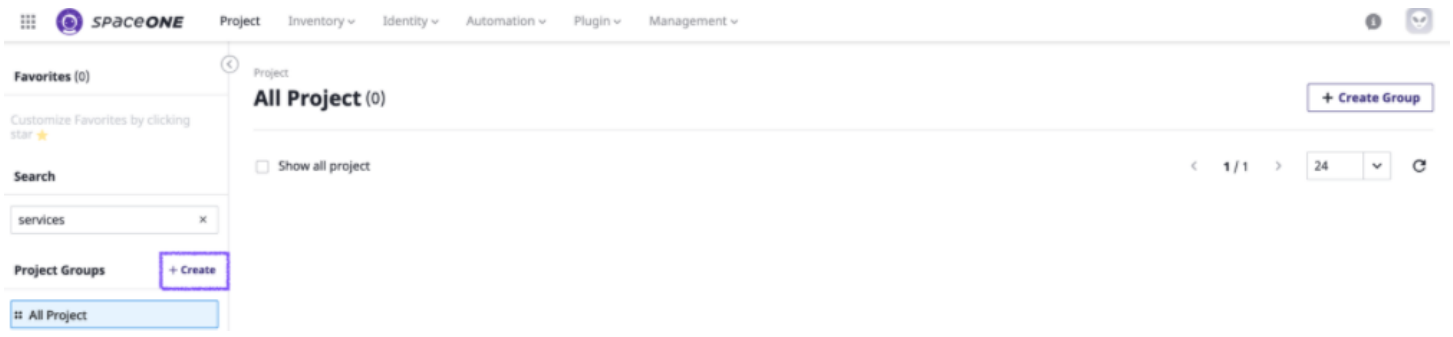
STEP 1: Drive to the domain of **SpaceONE** on the browser and type the given ID and Password.



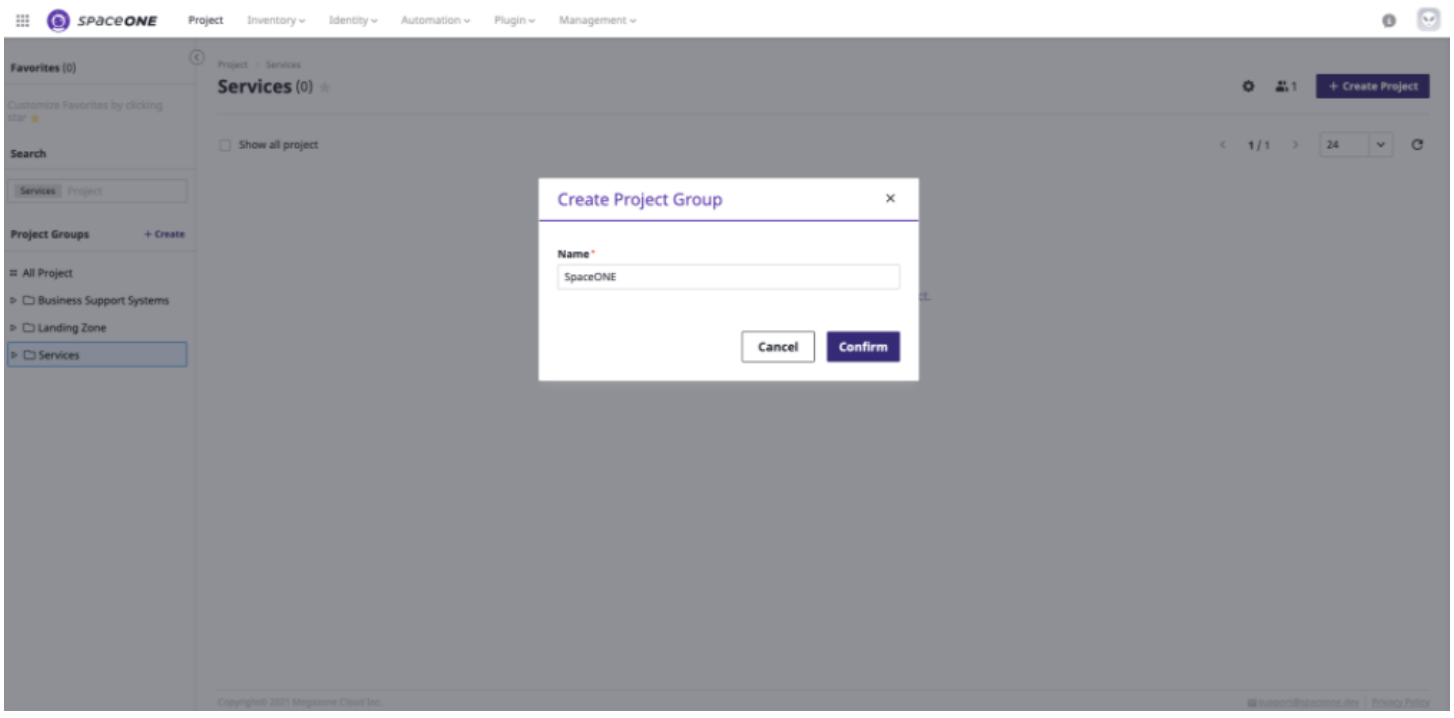
Create My Project Group and Project

> ### Note
> **General User** has a permission to control only the project group/project which they belong to.

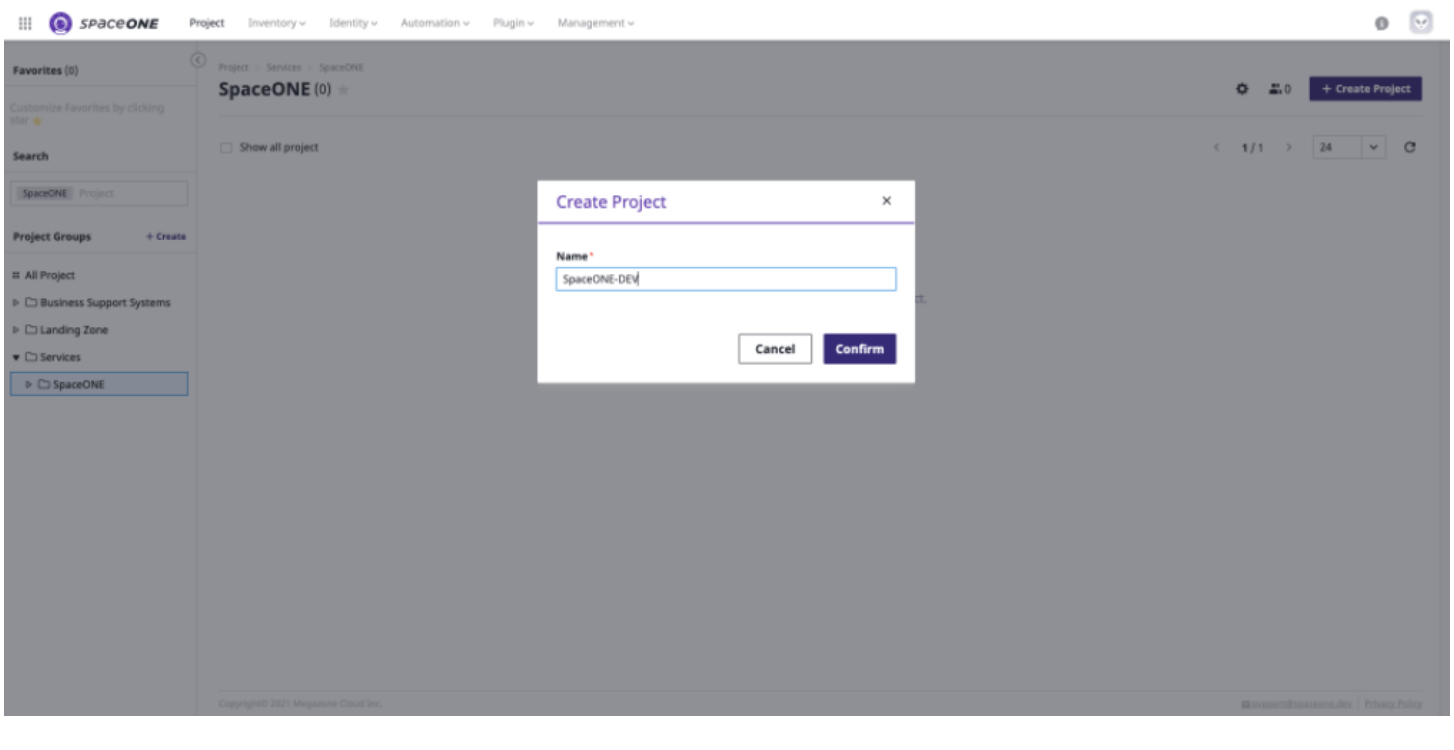
STEP 1: Drive to menu `Project` at top bar and click `+ Create` button as below.



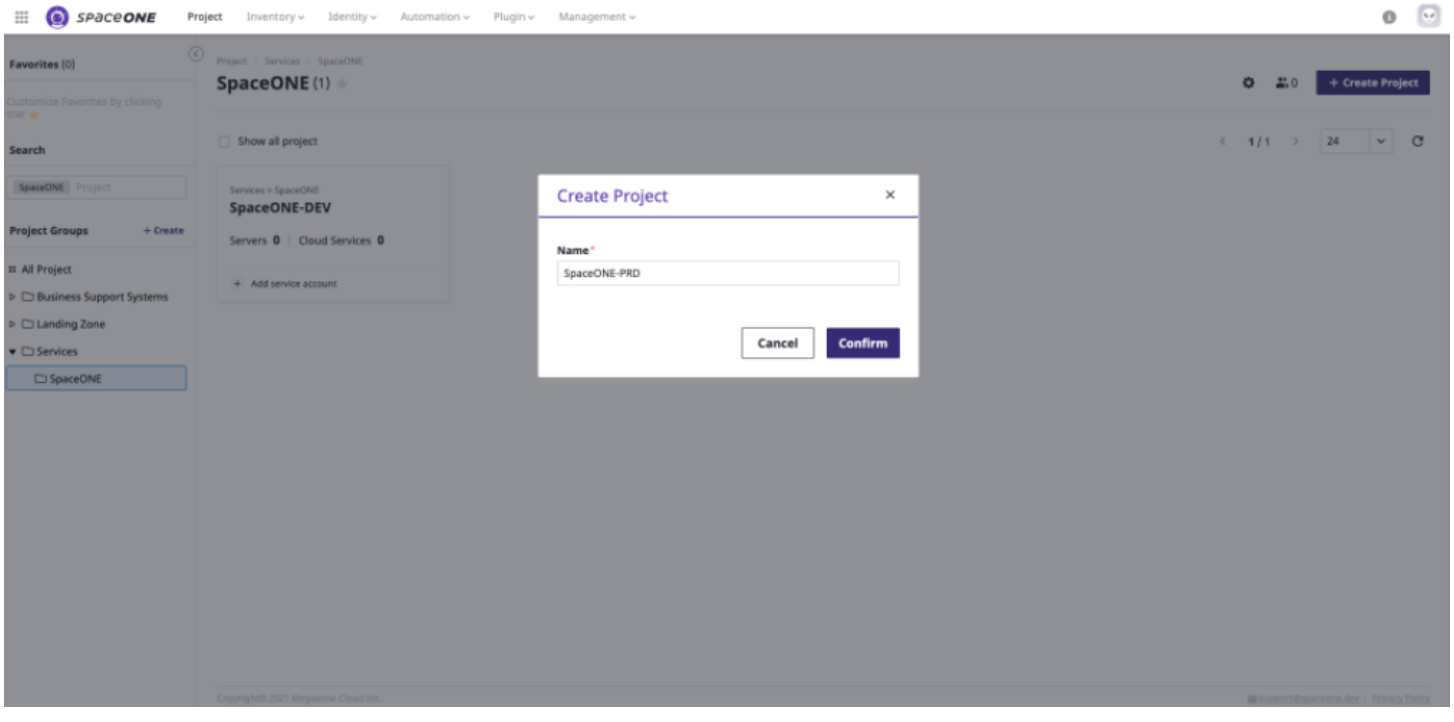
STEP 2: Name `Group` at top bar and click `Confirm` button as below.



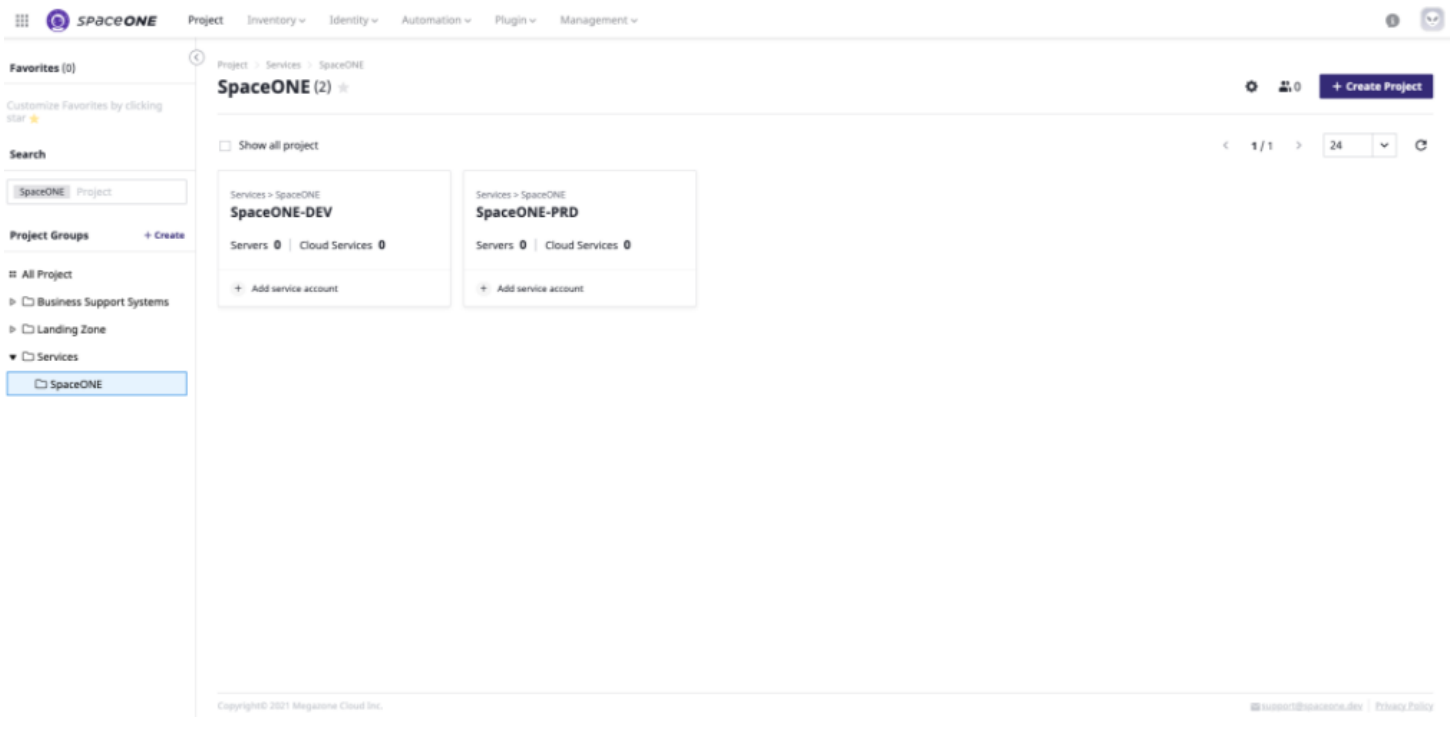
STEP 3: Select Project Group that you created in the previous step and click `+ Create Project` at the top right corner of the page. Name project and then click the** `Confirm` ** button. (sample case: **SpaceONE-DEV**)



STEP 4: Click `+ Create Project` at the top right corner of the page and then name project with a different name for your own use and then click `Confirm` button. (sample case: **SpaceONE-PRO**)

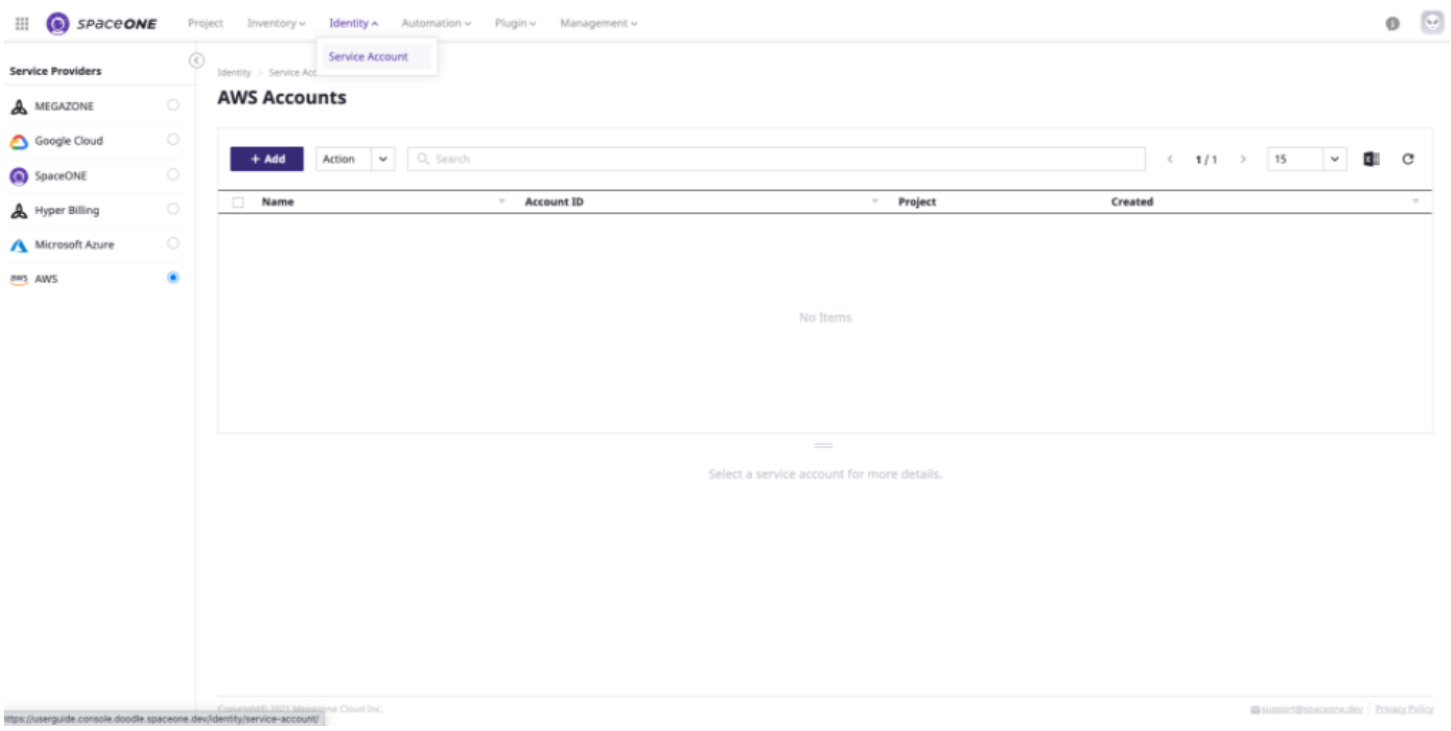


STEP 5: Check 2 sample Projects (**SpaceONE-DEV, SpaceONE-PRO**) have created under **SpaceONE** project group.
desc



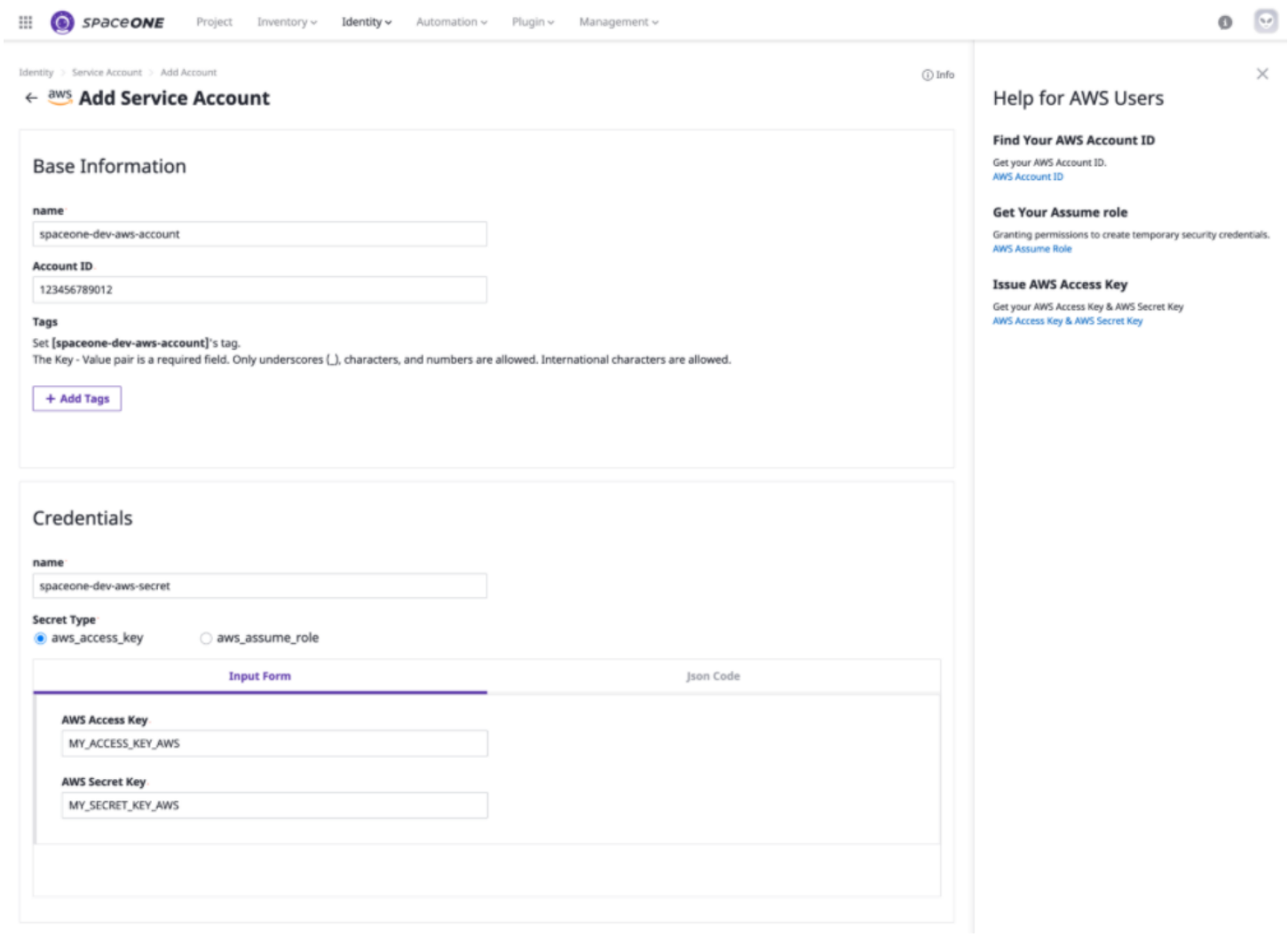
Register Service Account

Service accounts must be registered to run collectors which getting cloud resources from public clouds.
STEP 1: Drive to menu `Identity > Service Account` from the top bar and Click AWS from the provider panel on the left side menu.
Click `+ Add` button to add AWS service account.

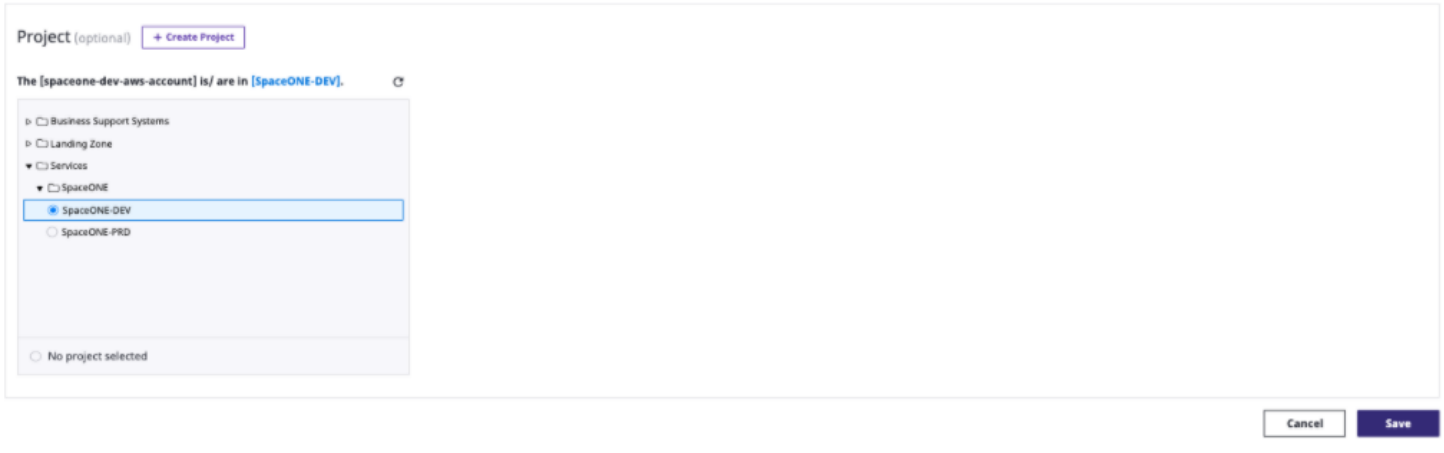


STEP 2: Fill out the name of Service Account and Account ID on base information fields. Please, fill out your **AWS Access Key** and **AWS Secret Key** as well.

> Please, Click links at Help for AWS Users panel if you have any issue to get Account id, Assume role, and AWS access key.



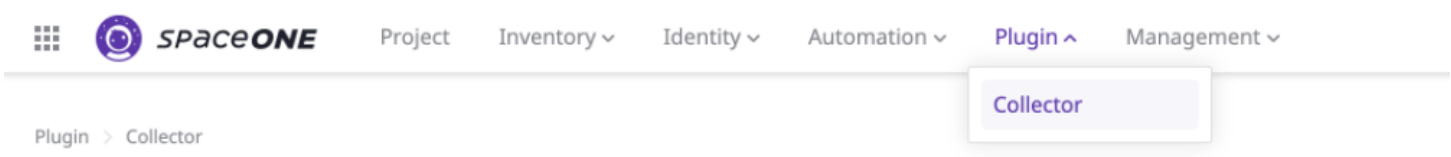
STEP 3: Please, select a project that you want to map with your service account.
We highly recommend mapping a project with Service Account for cloud resource management purposes.



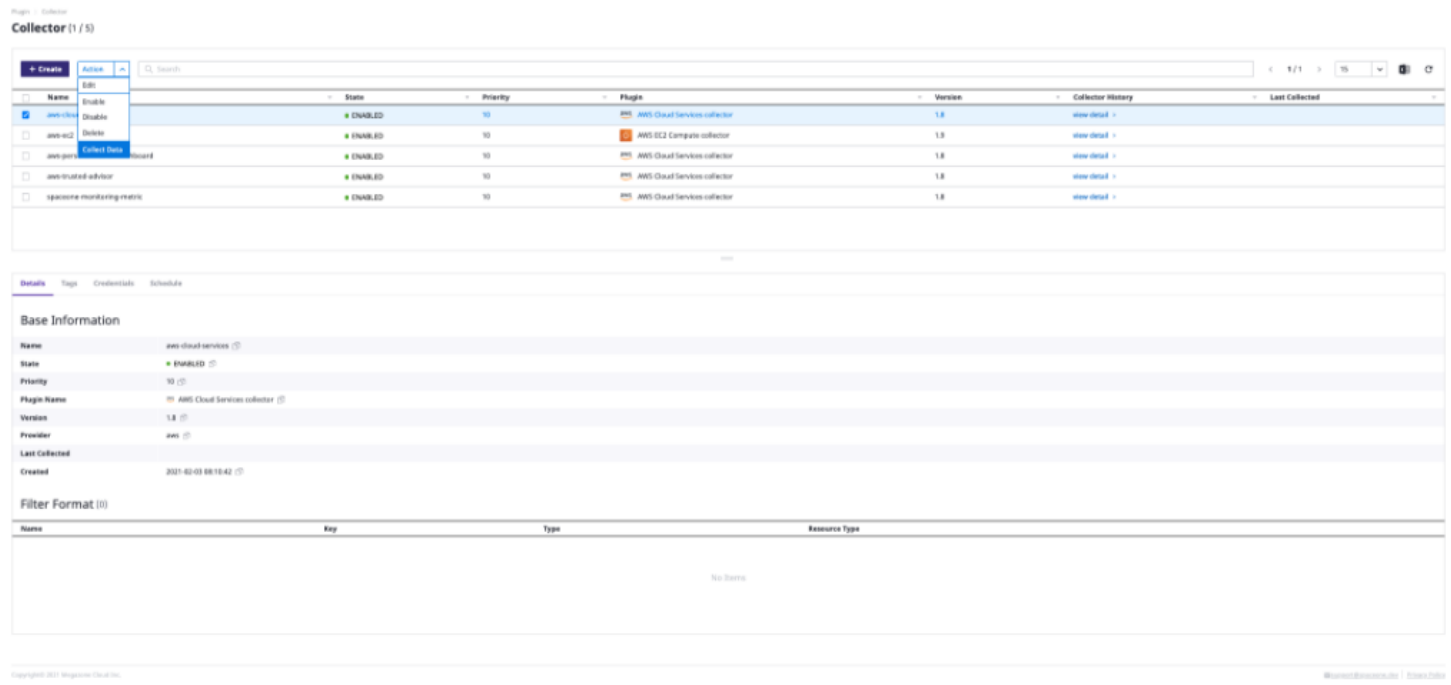
All cloud resources under the Service Account that you registered above will be shown on the selected project and I**nventory** menu.

Collect Resources

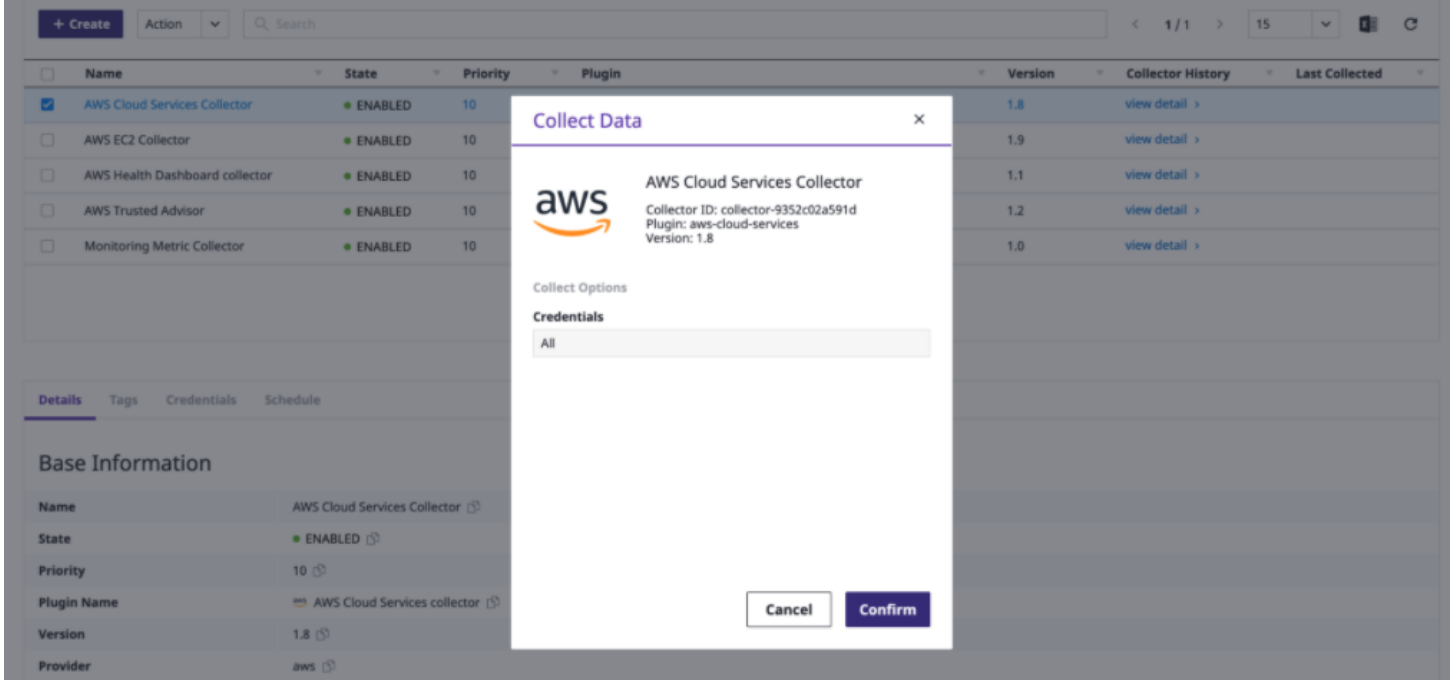
STEP 1: Drive to menu **`Plugin > Collector`** at the top menu bar.



STEP 2: Select collector and Select collect data from drop down option on Action.

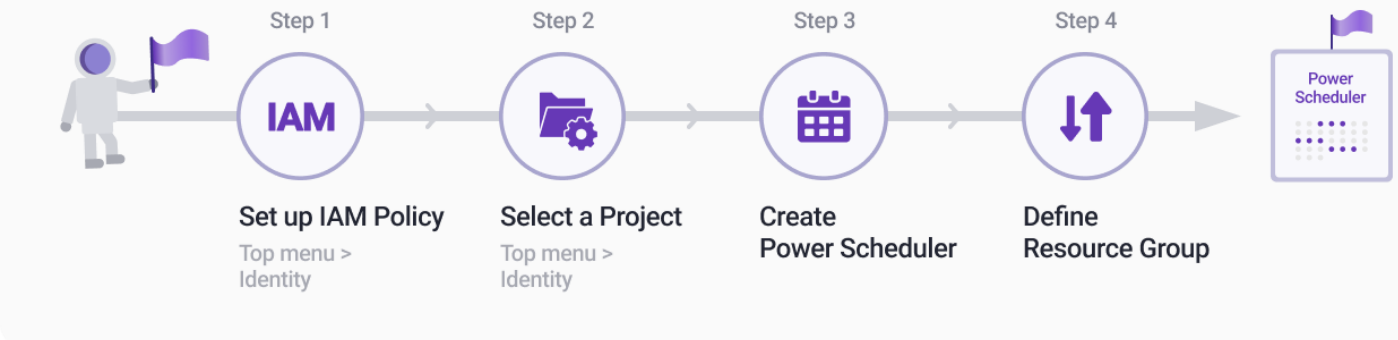


STEP 3: Click `Confirm` button on **Collect Data** pop-up window.



1.2 - Power Scheduler Quick Start

Quick Guide for user easier to set up Power Scheduler



How to Set up

Start your Power Scheduler after completing the following steps:

Prerequisites

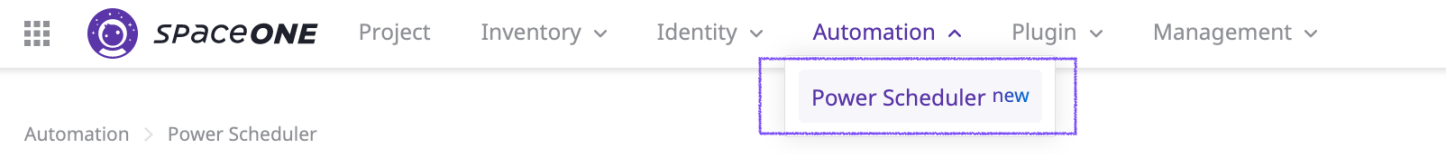
You can set up your IAM policy for power scheduler in SpaceONE with pre-defined credentials per cloud-provider to control resources with safety and prevent others to access resources without permission.
Please, assign corresponding access policies to SpaceONE from each provider's console as mentioned below, prior to create a Power Scheduler.

(AWS) Service Account Policy Management

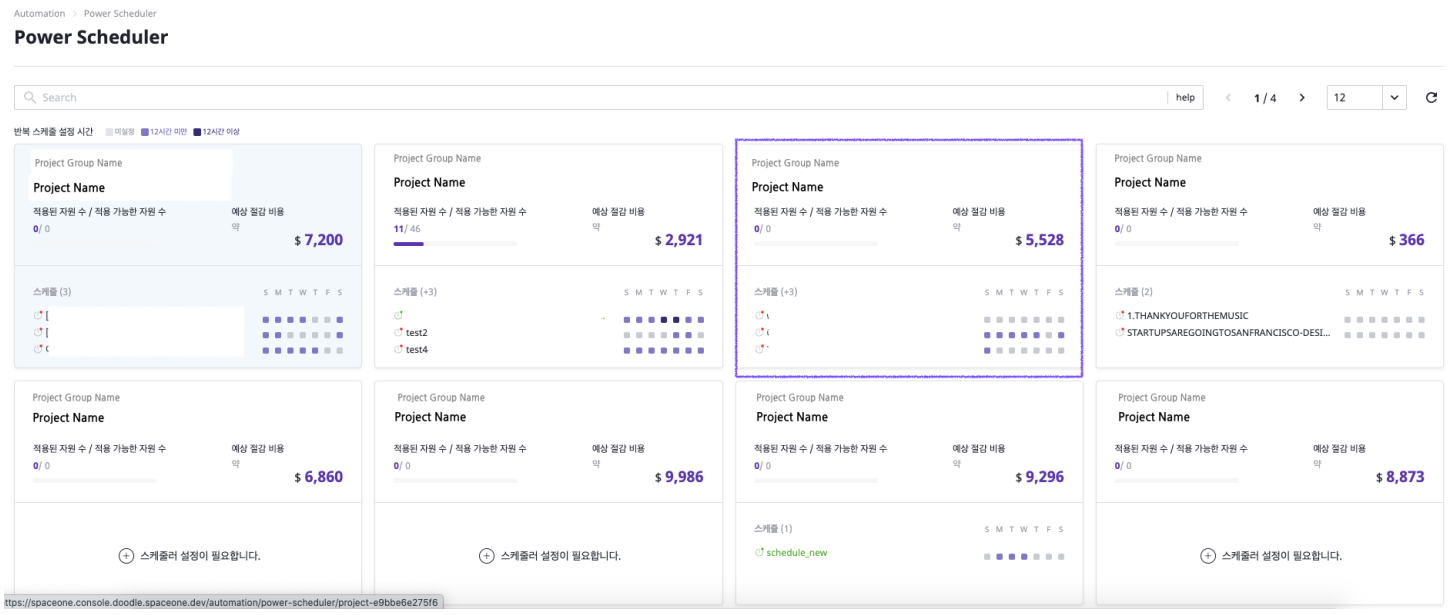
(Google Cloud) Service Account Policy Management

Set up Basic Scheduler Info

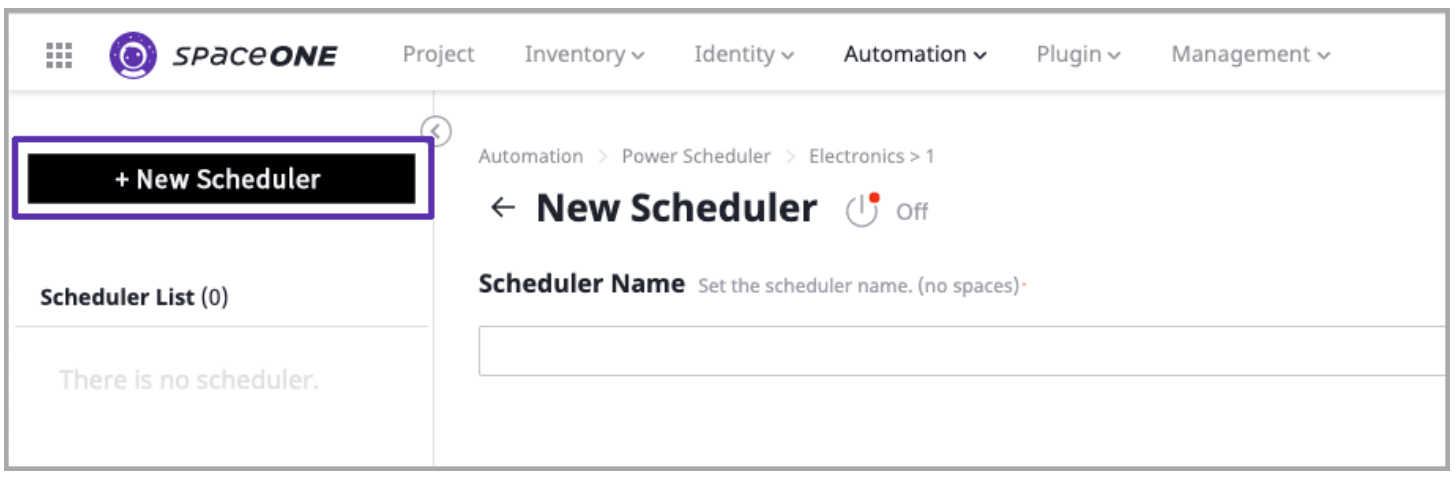
STEP 1: Select `Automation > Power Scheduler` on top header menu



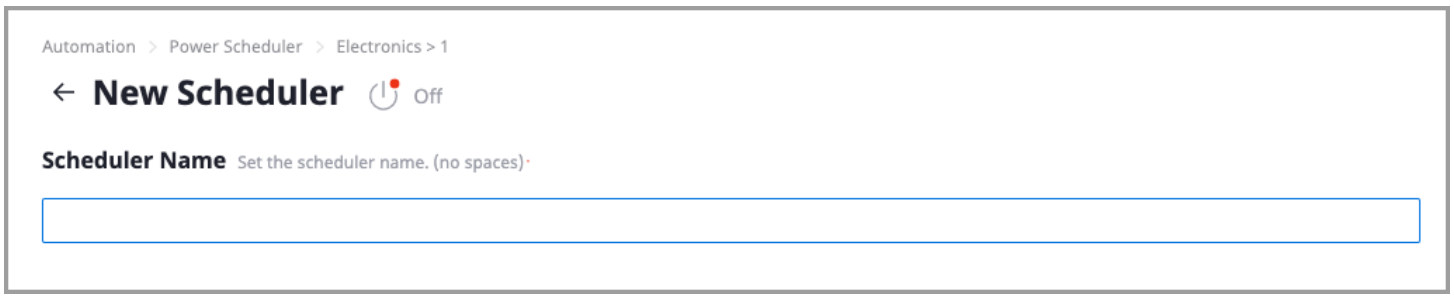
STEP 2: Select a project to set up Power Scheduler on the dashboard.



STEP 3: Click `+ New Scheduler` button at the top left corner. It is automatically changed to the creation mode if there is no previously created scheduler in the project.



STEP 4: Set the scheduler's name to create a scheduler. You can enter a string including letters and – . Scheduler name is required and blank spaces are not allowed.



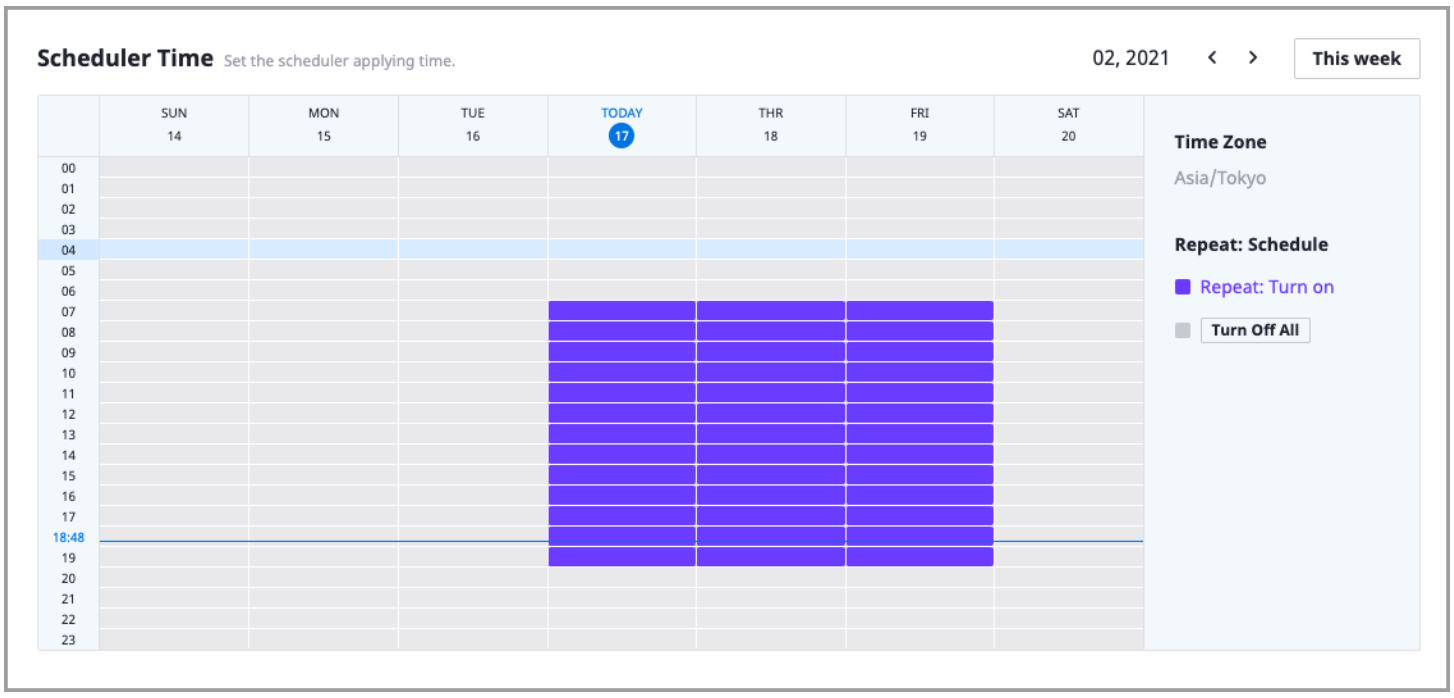
Configure scheduler runtime

Set the time for applying a scheduler.
The calendar grid breaks the week down by day on the horizontal axis and has 24-hour basis segments in portrait orientation. You can click `This week` button to set the scheduled time for this week.
You can move between month through `< >` at the upper right of the graph.

There are three types of scheduler mode.

Mode	State	Description	Color
Repeated Schedule		Timer repeated by every week. Selected area became On, Otherwise(Non selected) became Off.	반복 켜기 편집하기
One Time Schedule	ON	Created specified time range. Resource became On selected area.	켜기 편집하기
	OFF	Created specified time range. Resource became Off selected area.	끄기 편집하기

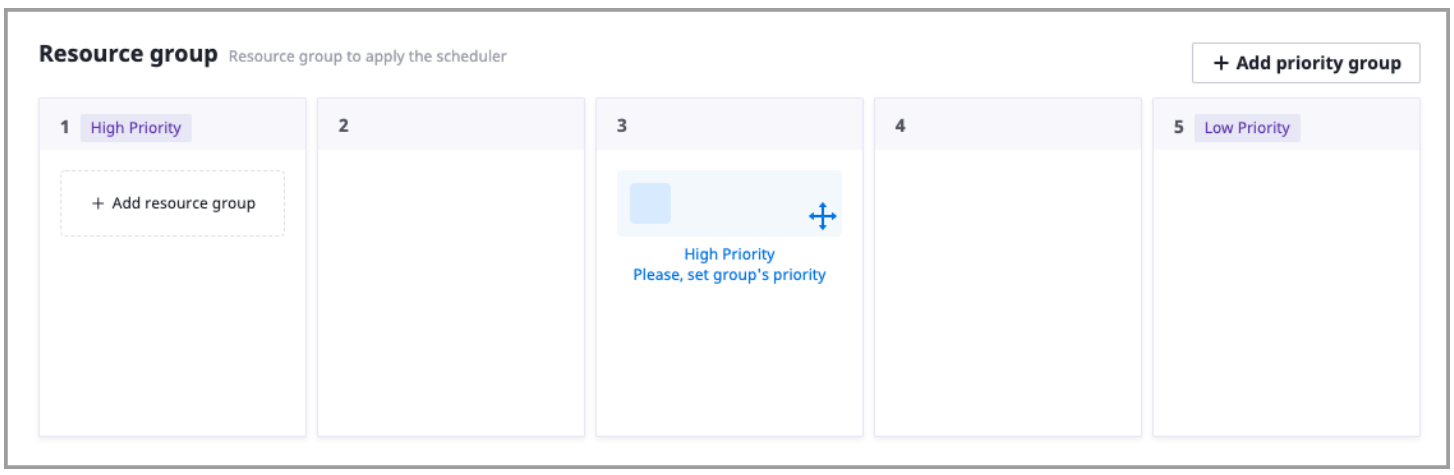
STEP 1: Click&drag to select certain time segments to set time for the scheduler to run.



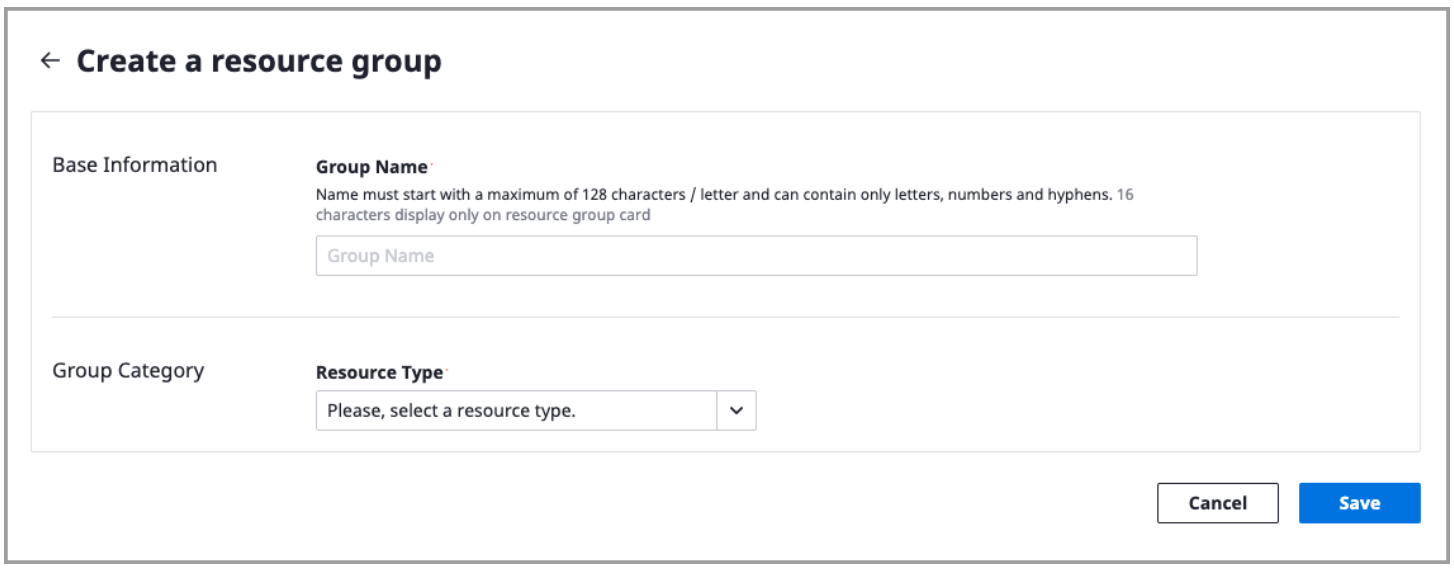
Please, be advised
Without any setting of Scheduler Time, it recognizes scheduler as `Turn Off All` which causes all resource to stop working immediately.

Define Resource Group

Set the resource group for applying defined schedule



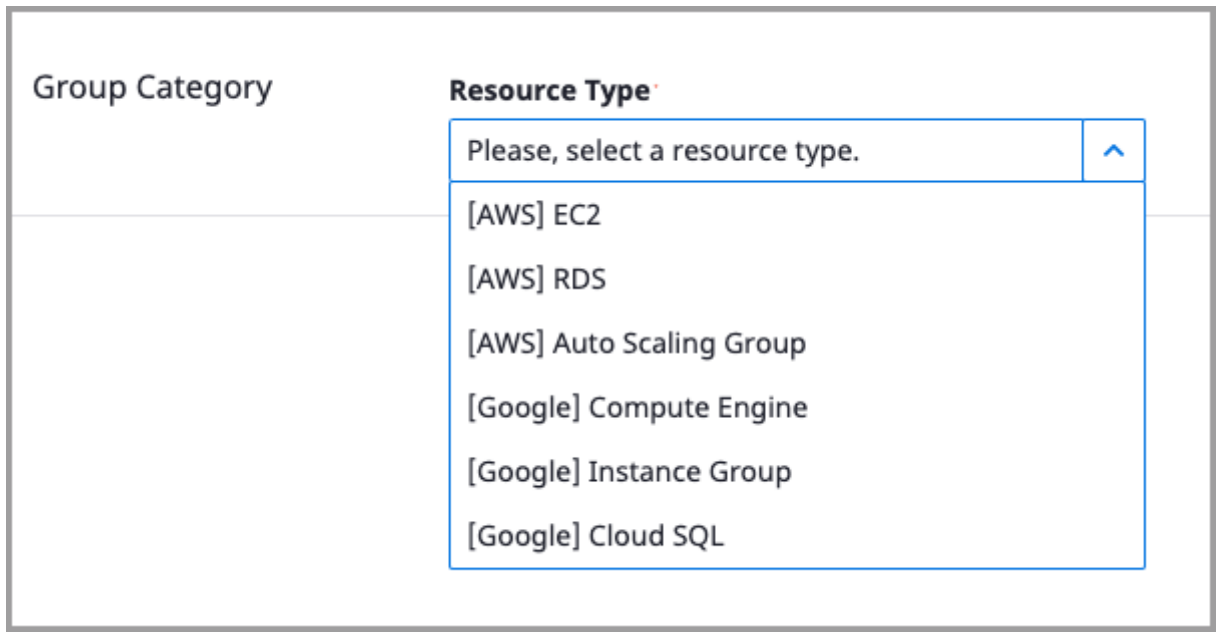
By clicking **`+ Add Resource Group`** , user can move to **Create a resource group** page.



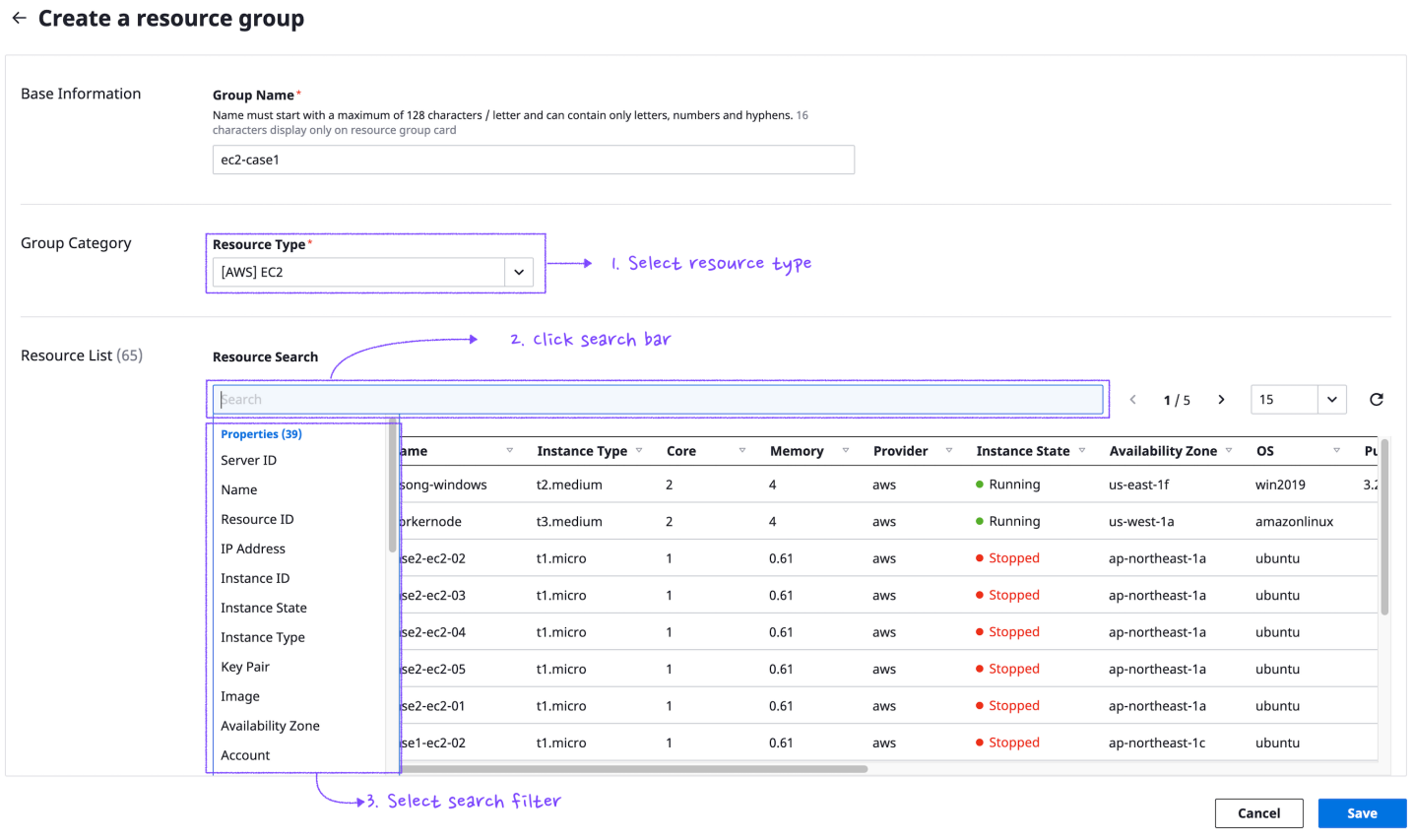
The Naming Rules of Resource Group is below.

> Max 128 character
> Start with character
> Character, Number, & Hyphen – available

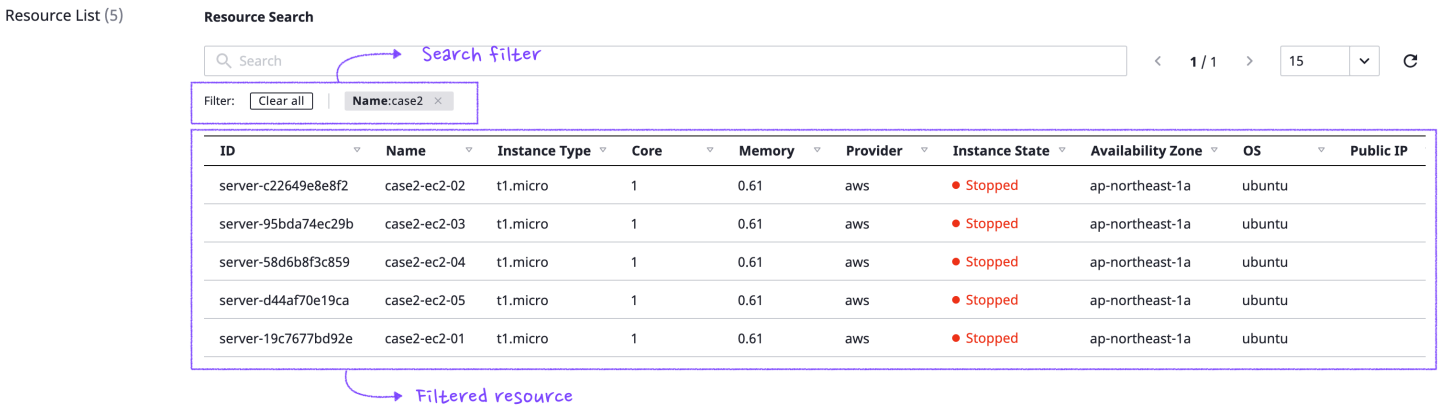
Select resource type



Then, Targeting resource is needed.
Enter search keyword to grouping resources. By clicking search bar available search properties pops up. Default property is name.
Supported search filter is listed here. Usually name or tag filter is preferred.

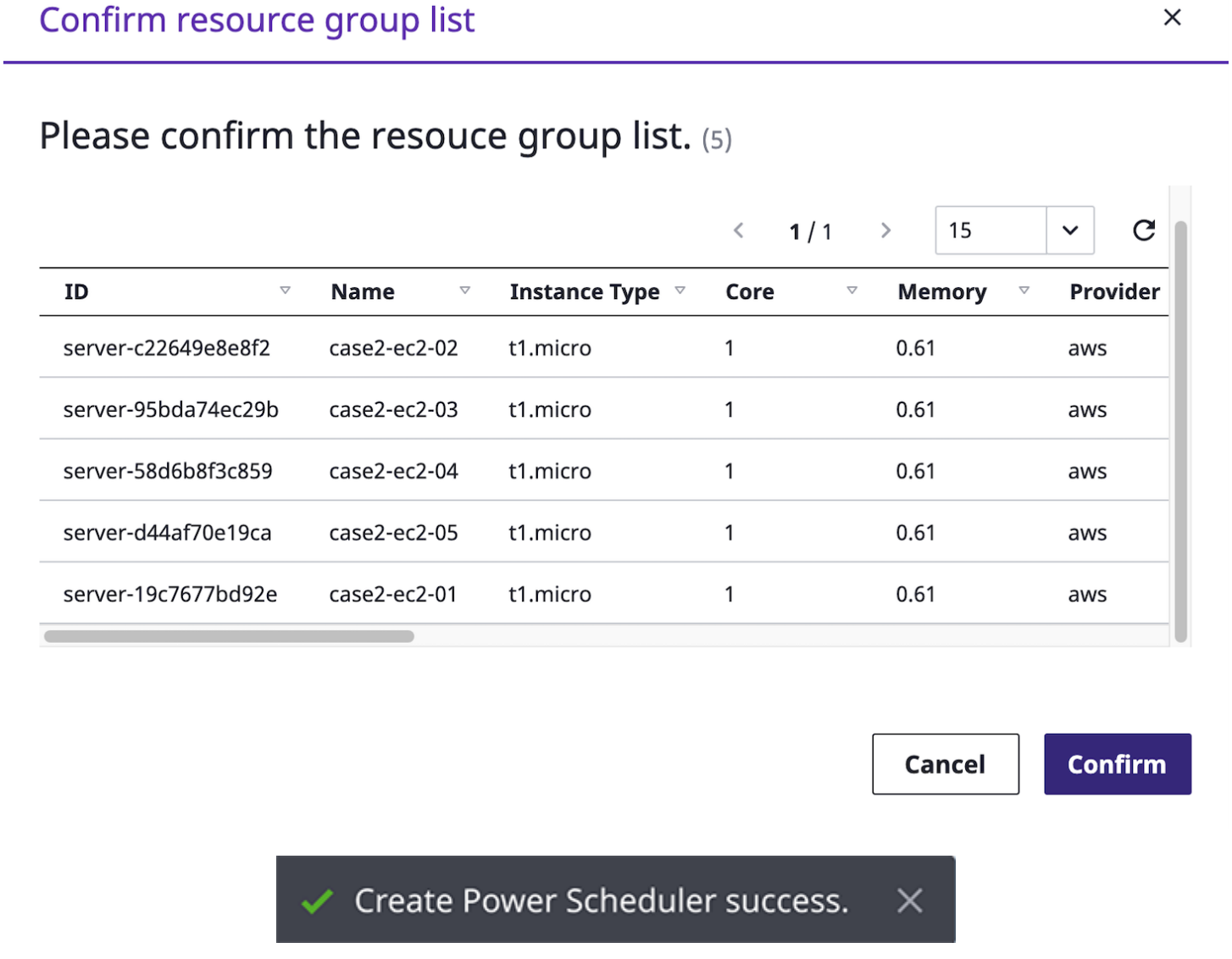


To apply search filter, You need to press ***Enter***. Then filtered resources will be appeared.



Enter all information, then click the save button below.

Get ***creating success*** message pops up when all creation process is done successfully.



Limitation & Restriction

Some type of resources are not controlled by power scheduler services. They are listed here.

1.3 - Alert Manager Quick Start

Quick guide for user to set up alert manager more easily.

How to Set up

SpaceONE Alert Manager는 다양한 모니터링 시스템에서 발생하는 Event를 체계적으로 통합관리할 수 있는 Tool 입니다. 자세한 설명은 링크를 참고해주세요. Alert Manager 소개
Alert Manager를 사용하기 위해서는 크게 두가지 설정이 필요합니다.
첫번째는, 외부의 다양한 모니터링 시스템들이 전달하는 Event를 SpaceONE Alert Manager가 수신 받기 위한 설정이고
두번째는, Alert이 임계치를 넘었을 경우 발생되는 Alarm Message를 수신받기 위한 Notification 설정 입니다.

> ### About Notification
>
> SpaceONE Notification 서비스는 Alarm Message를 다양한 매체를 통해 수신자들에게 전송합니다. 자세한 설명은 Notificaiton 소개 을 참고 하세요

이 페이지에서는 Alert Manager를 기본 설정하기 위한 방법에 대해 살펴 보도록 하겠습니다. 전체 순서는 아래와 같습니다.
사전 준비
Event 수신 설정
Alarm 수신 설정

사전 준비

Alert Manager를 사용하기 위해서는 사전에 아래와 같은 준비가 필요 합니다.

Project를 선택

Event를 수신 받을 Project를 지정해야 합니다. Alert Manager는 지정된 ***Endpoint*** 로 수신되는 Event를 Project의 ***Alert*** 으로 등록 합니다. 그러므로, 사전에 Event를 수신 받고자 하는 Project를 지정해 두어야 합니다.
또한, Project 내에 Alert로 인한 Alarm을 수신받기 위한 사용자들도 ***Member*** 로서 추가 되어 있어야 합니다.
Project에 사용자 추가하기

Event를 전달하기 위한 Monitoring Tool을 선택

Event를 감지하여 Alert Manager에게 전달하기 위한 Monitoring Tool이 필요합니다. SpaceONE은 주요 Monitoring Tool을 지원하는 Webhook Plugin을 지원하고 있습니다. 현재 MarketPlace에 등록된 Monitoring Webhook Plugin List는 링크를 참고해주세요.
Webhook Plugin List 보러가기

Notification 을 수신받기 위한 매체를 선택

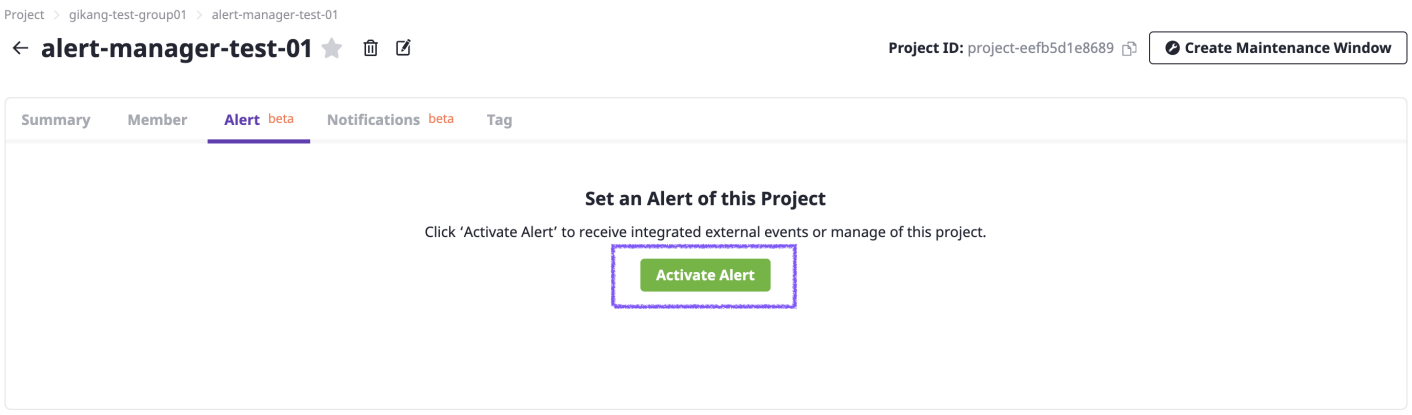
Alert이 등록된 후 정해진 규칙에 따라 Alarm 이 발생합니다. 발생된 Alarm은 지정된 Level에 따라 Notification Plugin 을 통해 사용자 채널에 발송됩니다. 현재 MarketPlace에 등록된 Notification Protocol Plugin List는 링크를 참고해주세요.
Notification Protocol List 보러가기

Event 수신 설정

Alert Manager Enable

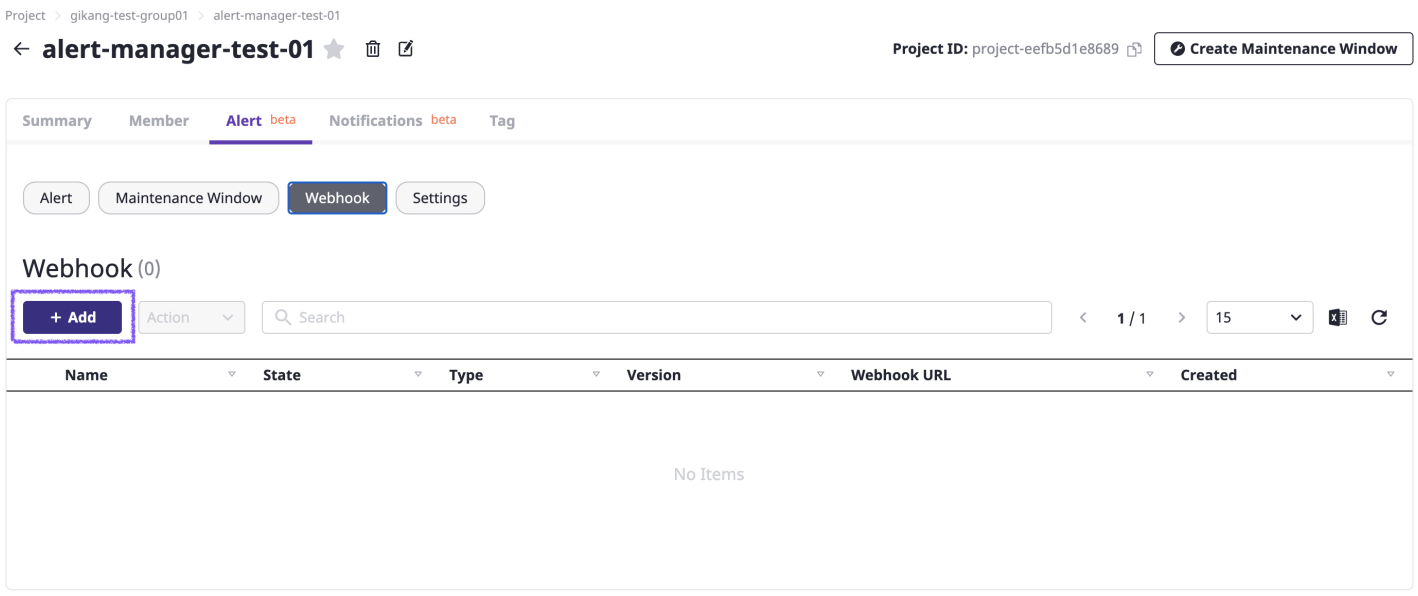
Alert를 수신하고자 하는 Project를 선택하여 ***`Project Dashboard > Alert`*** 탭을 클릭 합니다.

Activate Alert 를 클릭하여 Project내의 Alert을 활성화 합니다.

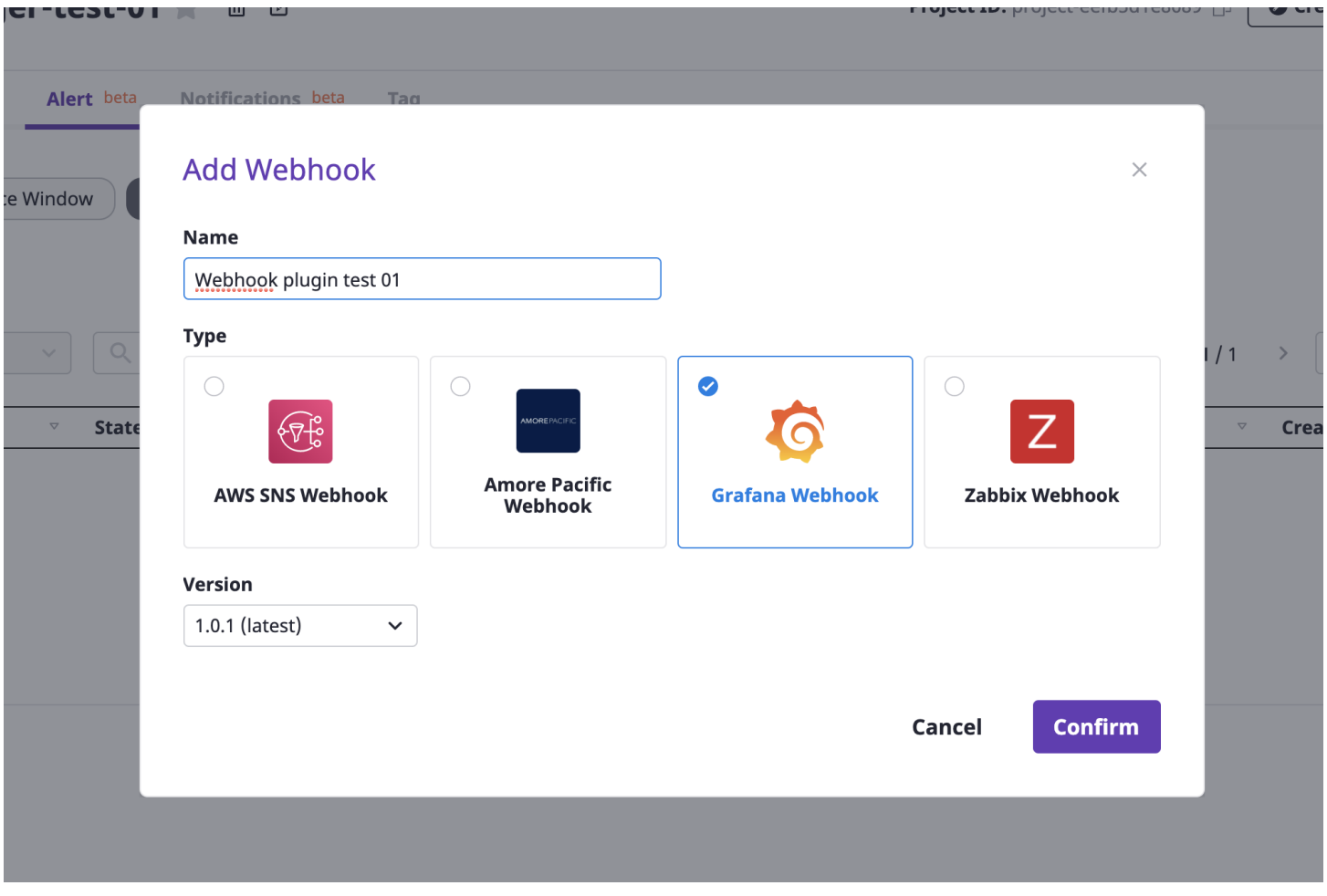


Configure Webhook Plugin

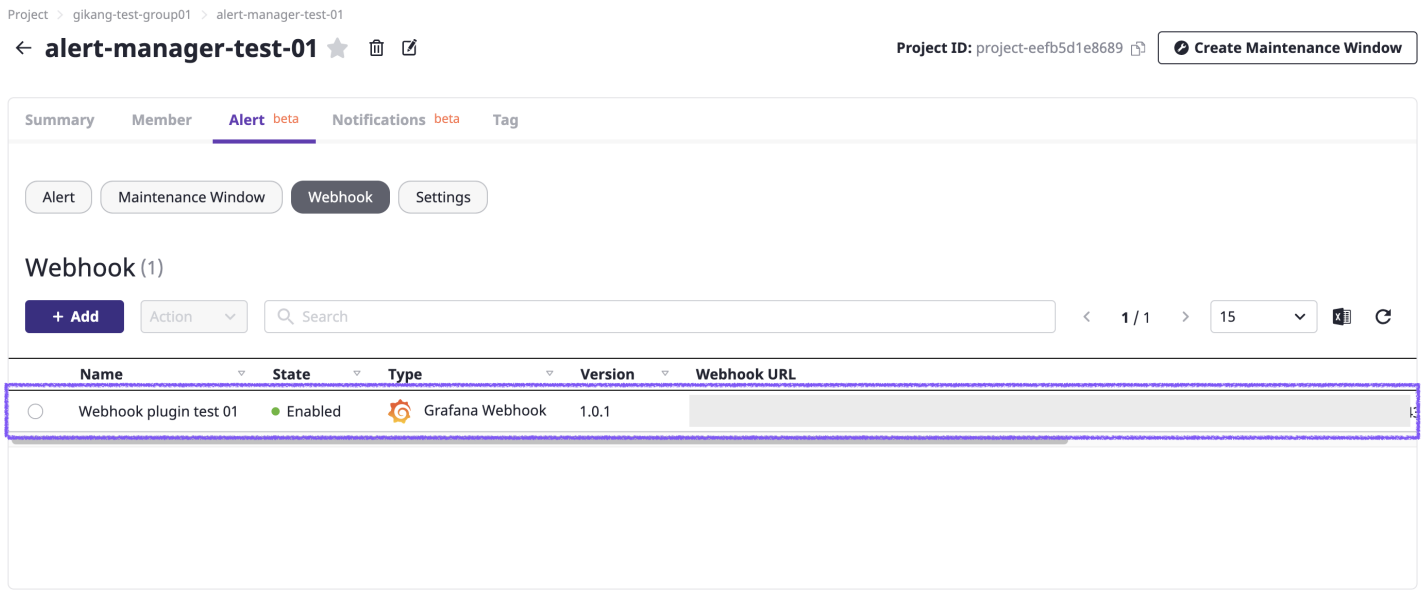
`Project Dashboard > Alert > Webhook` 탭을 클릭 합니다.
Add 버튼을 클릭합니다.



Event를 수신받고자 하는 Monitoring Tool을 선택 하고 ***Name*** 과 ***Version*** 을 입력 후, ***Confirm*** 버튼을 클릭 합니다.



아래와 같이 ***Webhook List*** 에 정상적으로 추가 되었다면, Monitoring Tool에서 생성한 Plugin으로 Event를 보낼 수 있도록 설정이 필요합니다.



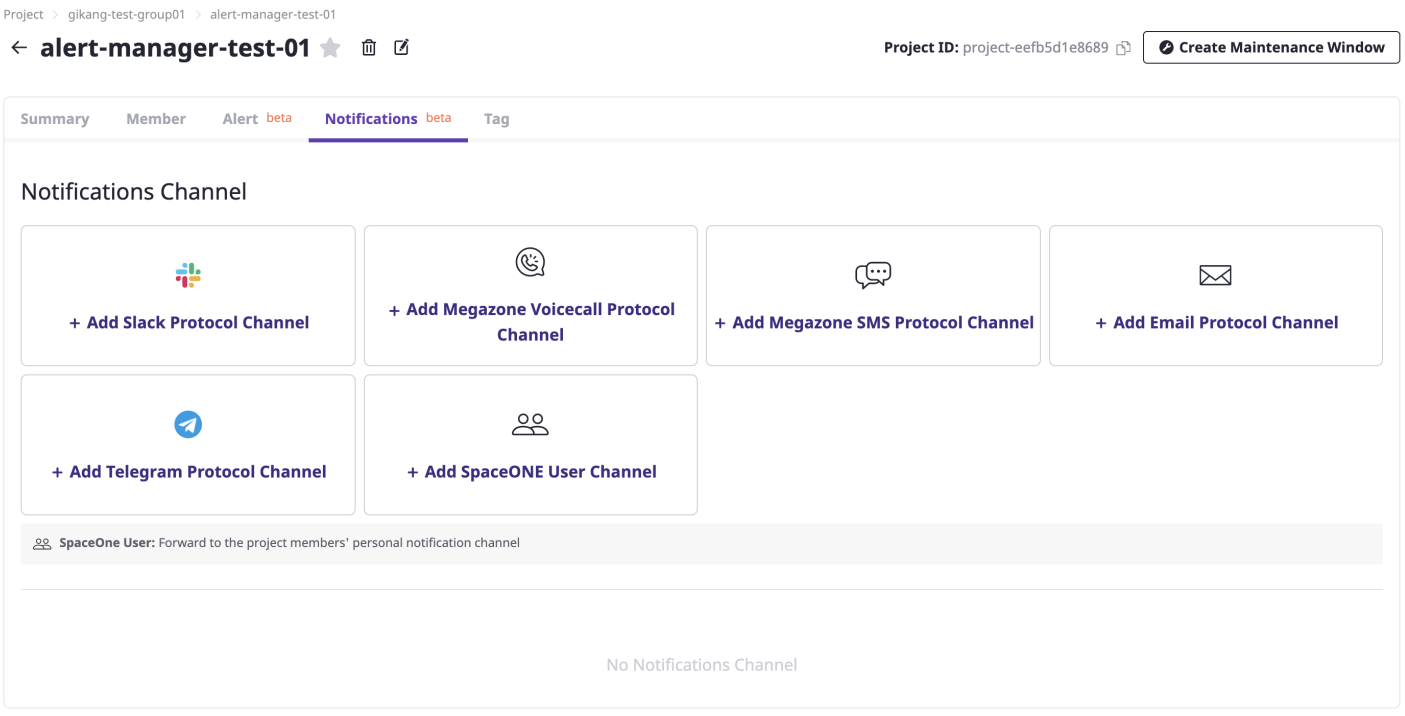
> ## Webhook Plugin Details
>
> 각 Tool 별로 설정을 위한 방법은 Monitoring Tool Webhook Plugin Configuration Guide 를 참고해주세요.

Alarm 수신 설정

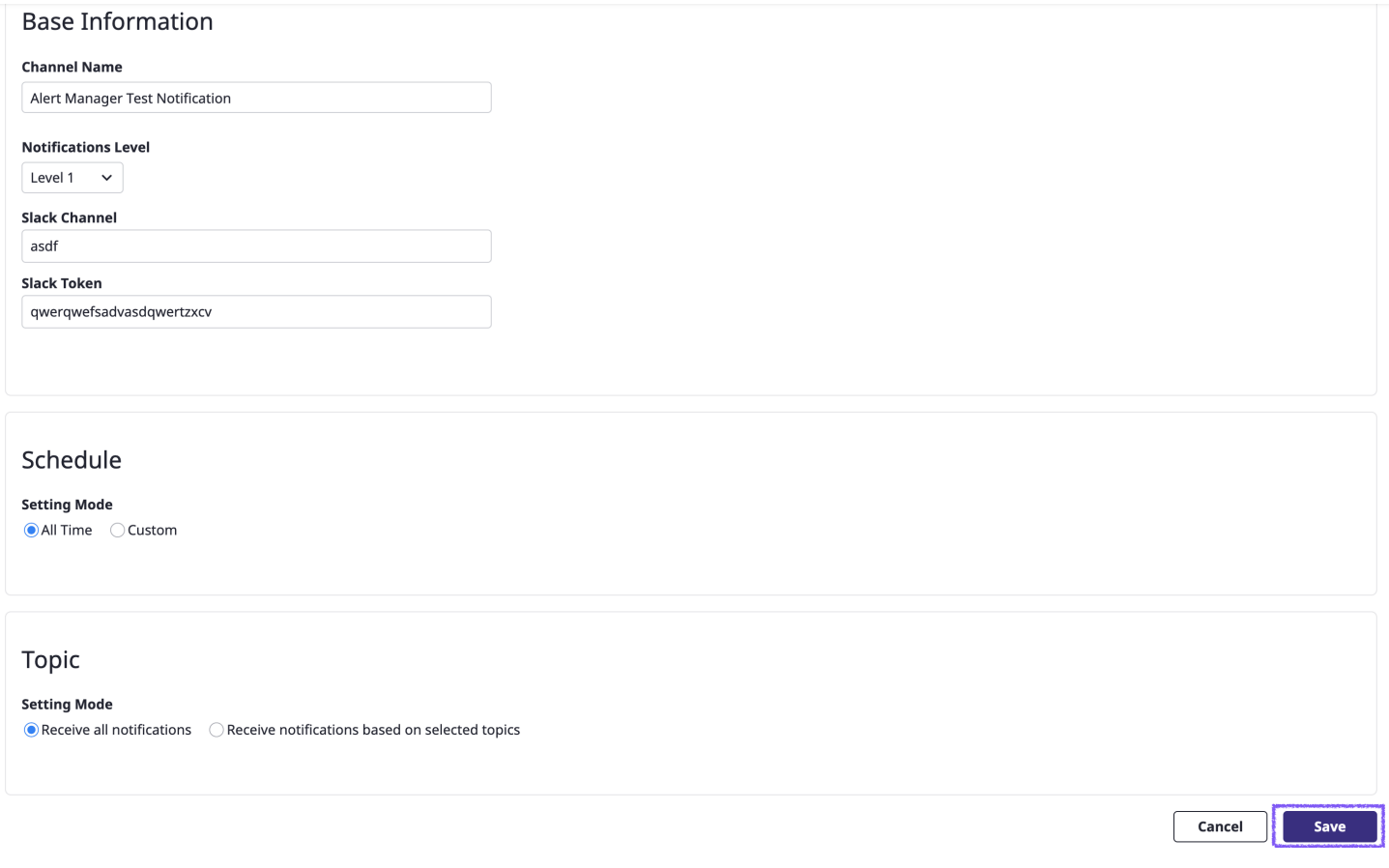
Alert 에 대하여 지정된 조건시 다양한 채널을 통해 ***Alarm*** 을 발생시킬 수 있도록 설정 합니다.

Notifications Channel 설정

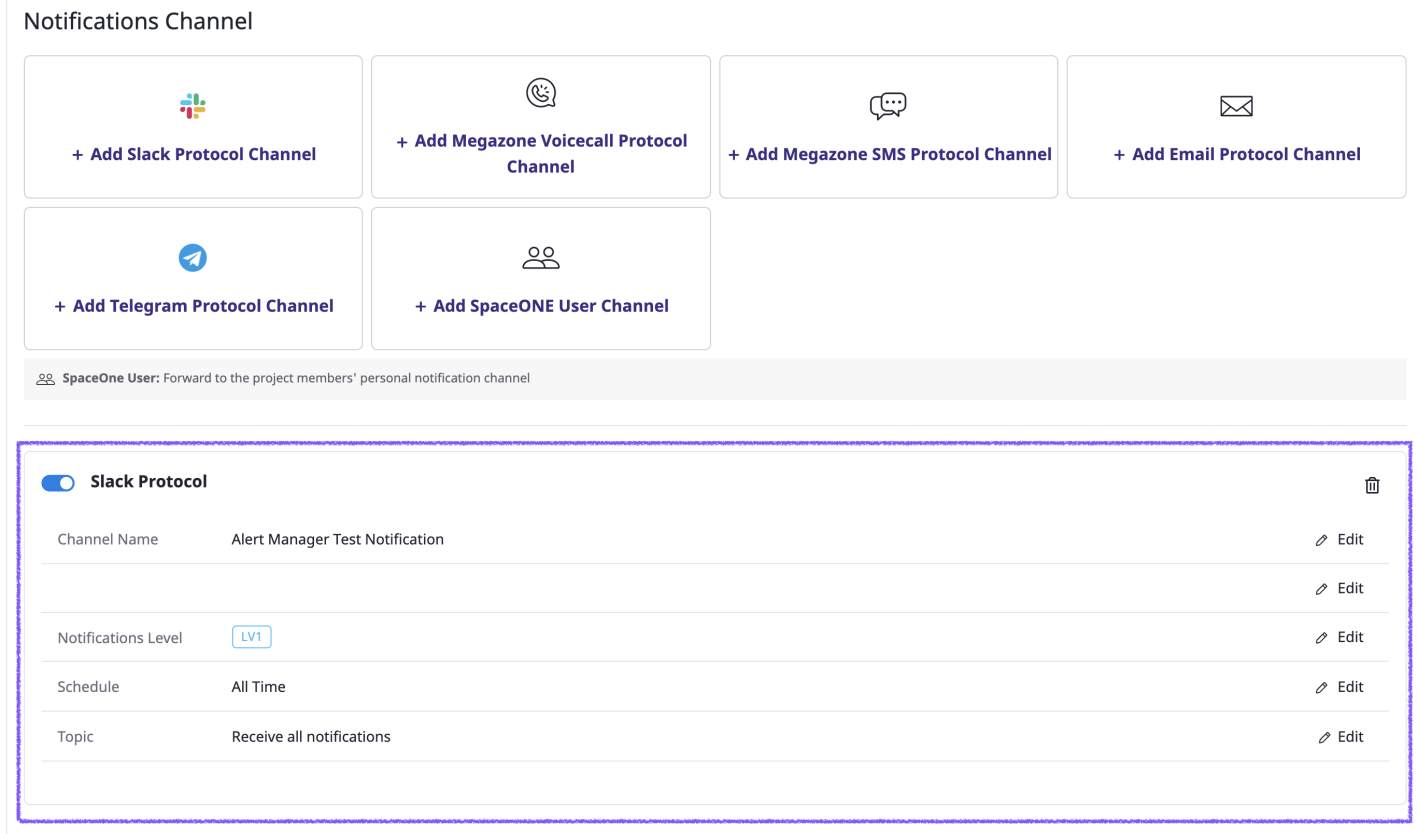
`Project Dashboard < Notifications` 로 이동합니다.
추가 하고자 하는 Channel 을 선택 합니다.



각 입력 항목의 내용을 입력 후 ***Save*** 버튼을 클릭 하여 생성을 완료 합니다.



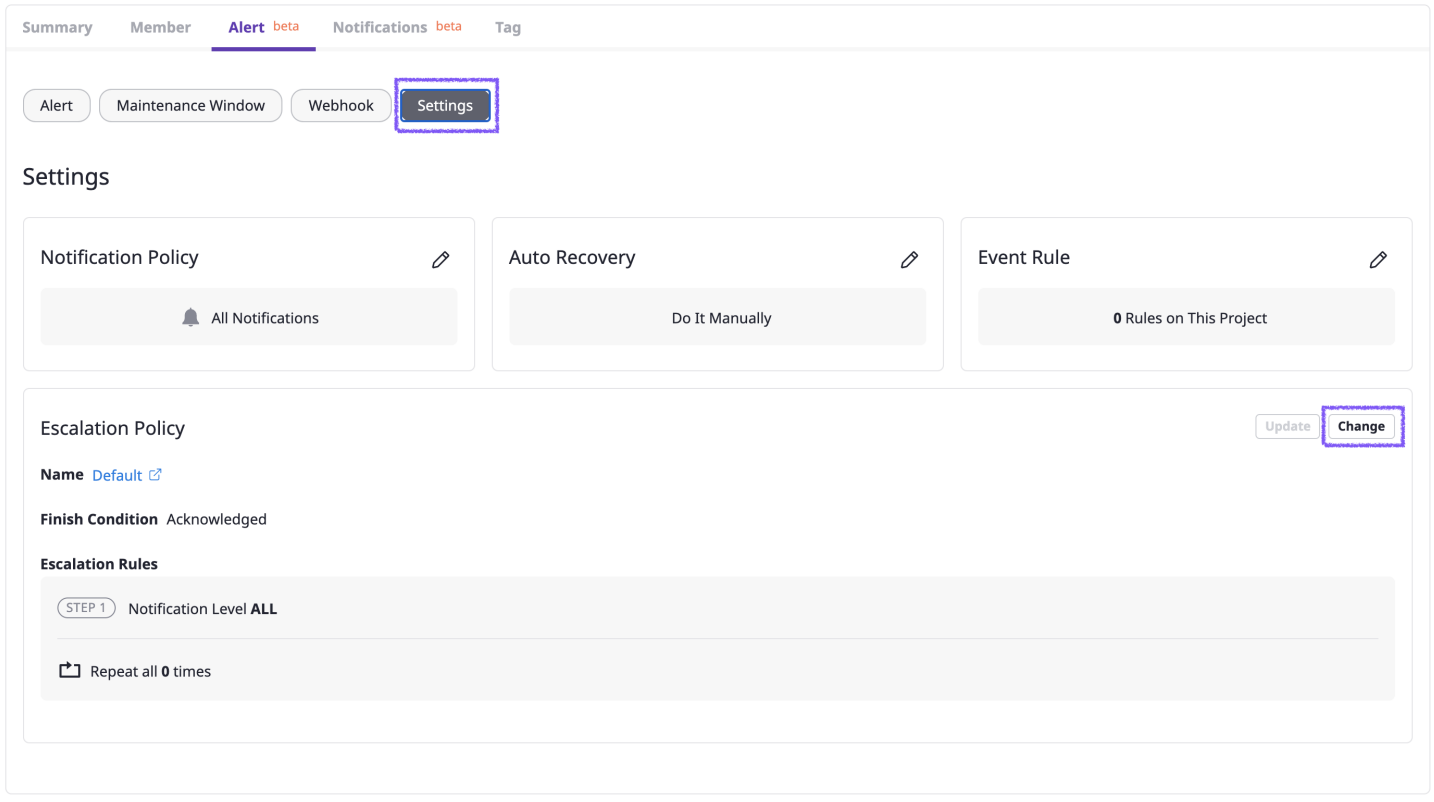
아래와 같이 추가된 ***Notification Channel*** 을 확인할 수 있습니다.



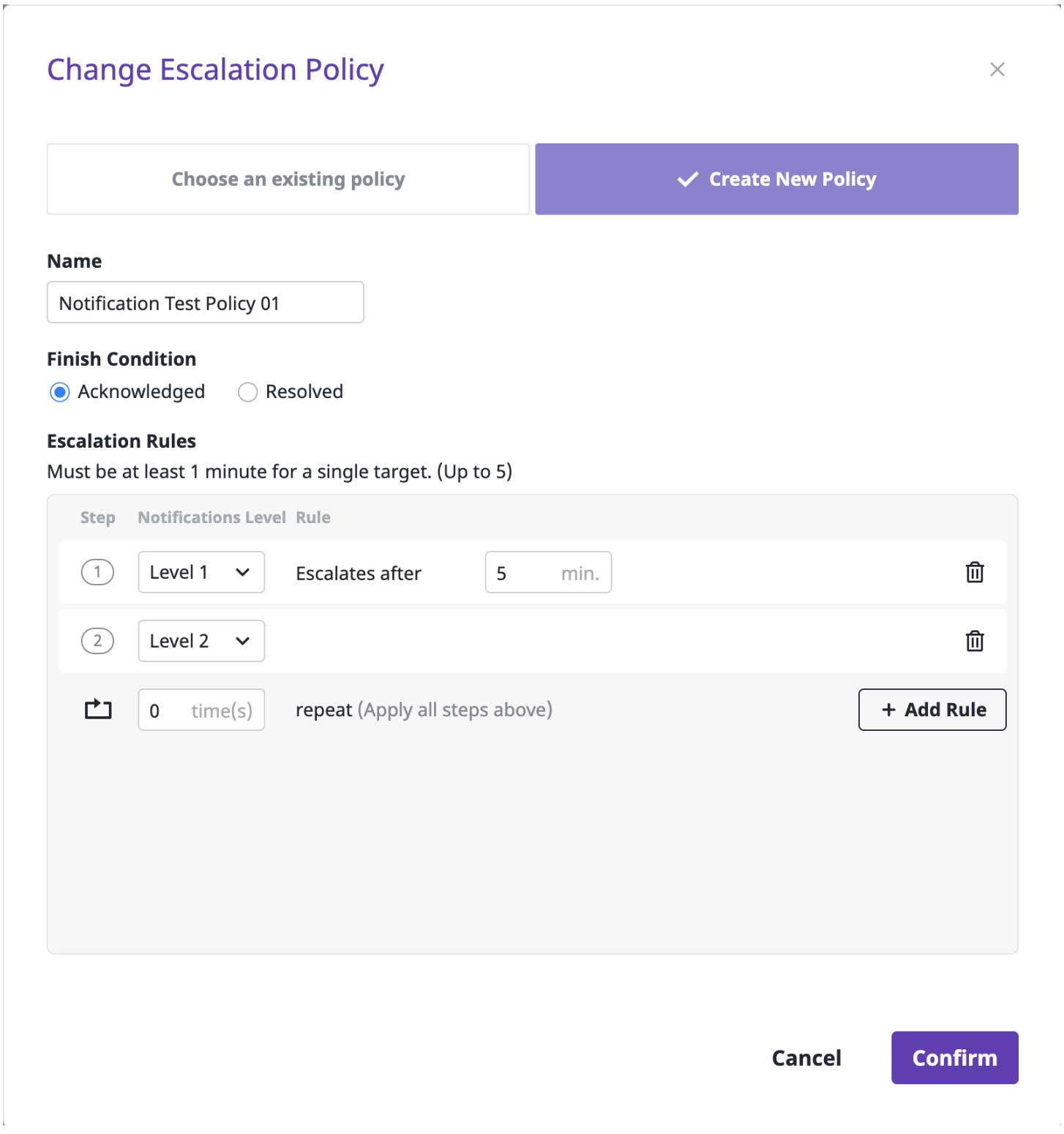
> ## Notification Plugin Details
>
> 각 Plugin별 Channel 설정에 대한 상세한 방안은 Notification Protocol Plugin 설정 가이드를 참고 해주세요.

Escalation Policy 설정

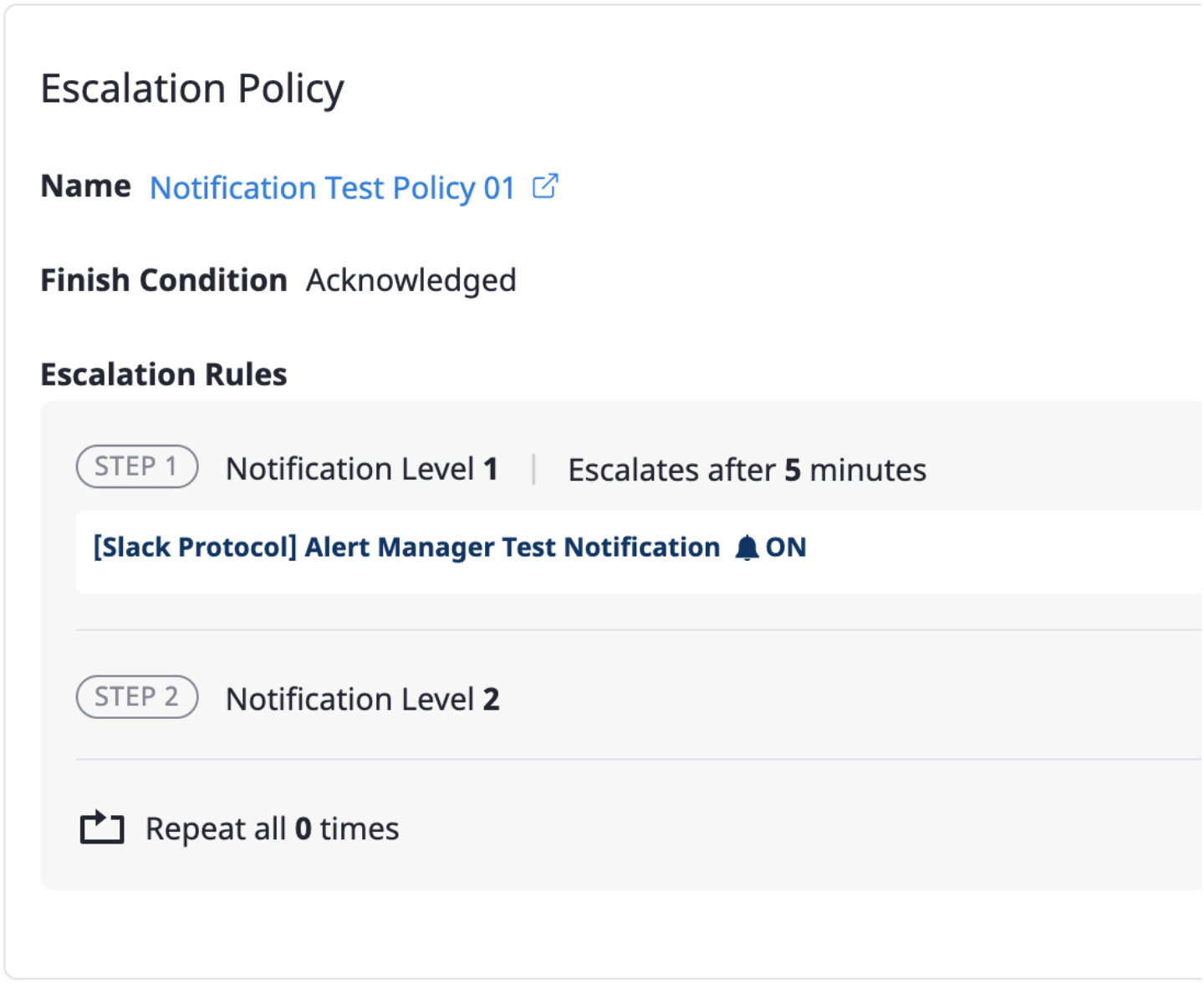
`Project Dashboard > Alert > Settings` 로 이동합니다.
Escalation Policy 의 ***Change*** 버튼을 클릭 합니다.



Create New Policy 버튼을 클릭 합니다.
아래와 같이 ***Name*** , ***Finish Condition*** , ***Escalation Rules*** 을 선택한 뒤 ***Confirm*** 을 클릭 하여 완료 합니다.



적용된 Policy를 확인 합니다.



Escalation Policy Details

Escalation Policy의 상세 설명은 Escalation Policy 상세 설정 가이드를 참고 해주세요.

2 - Dashboard

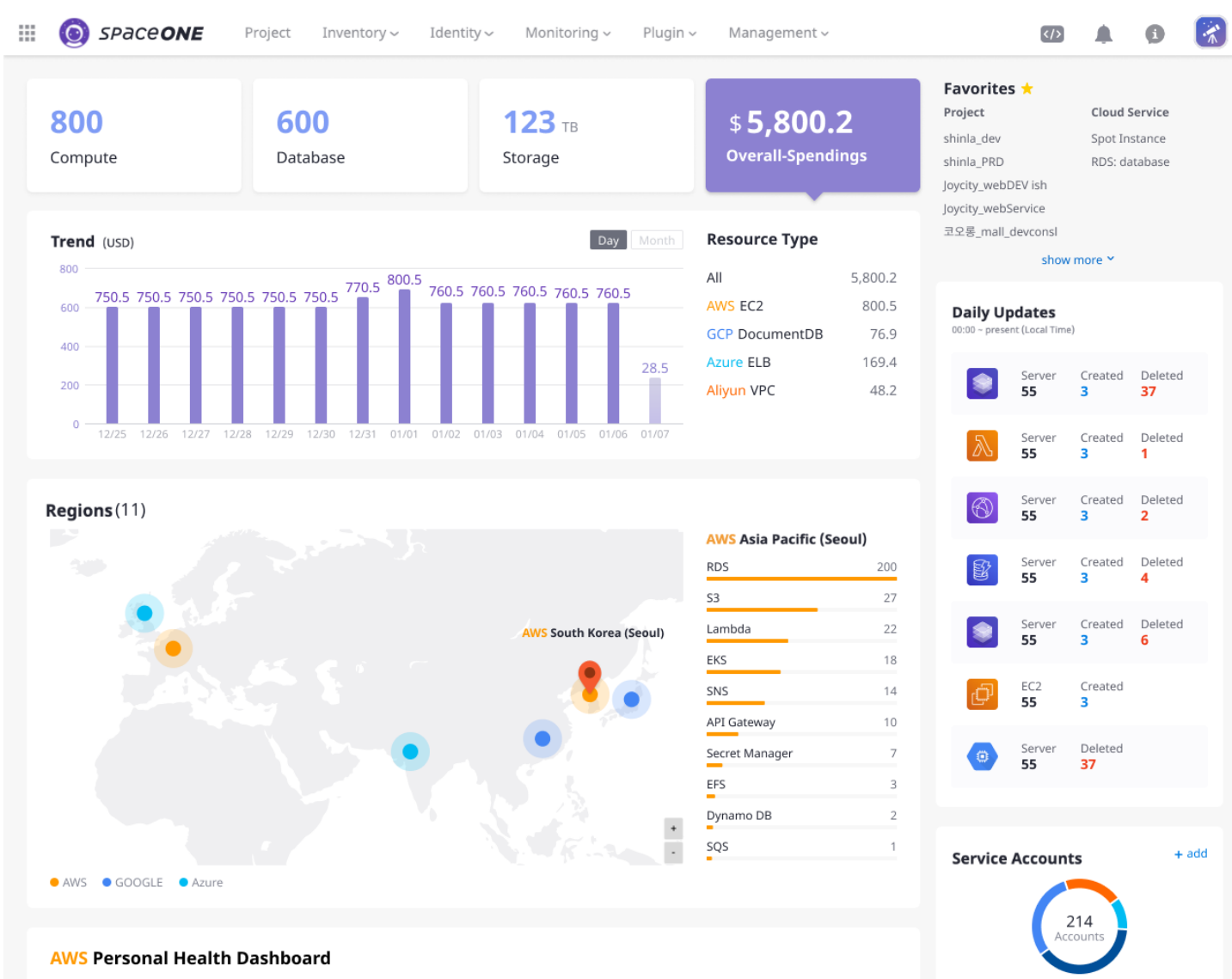
About Dash board

2.1 - Domain Dashboard

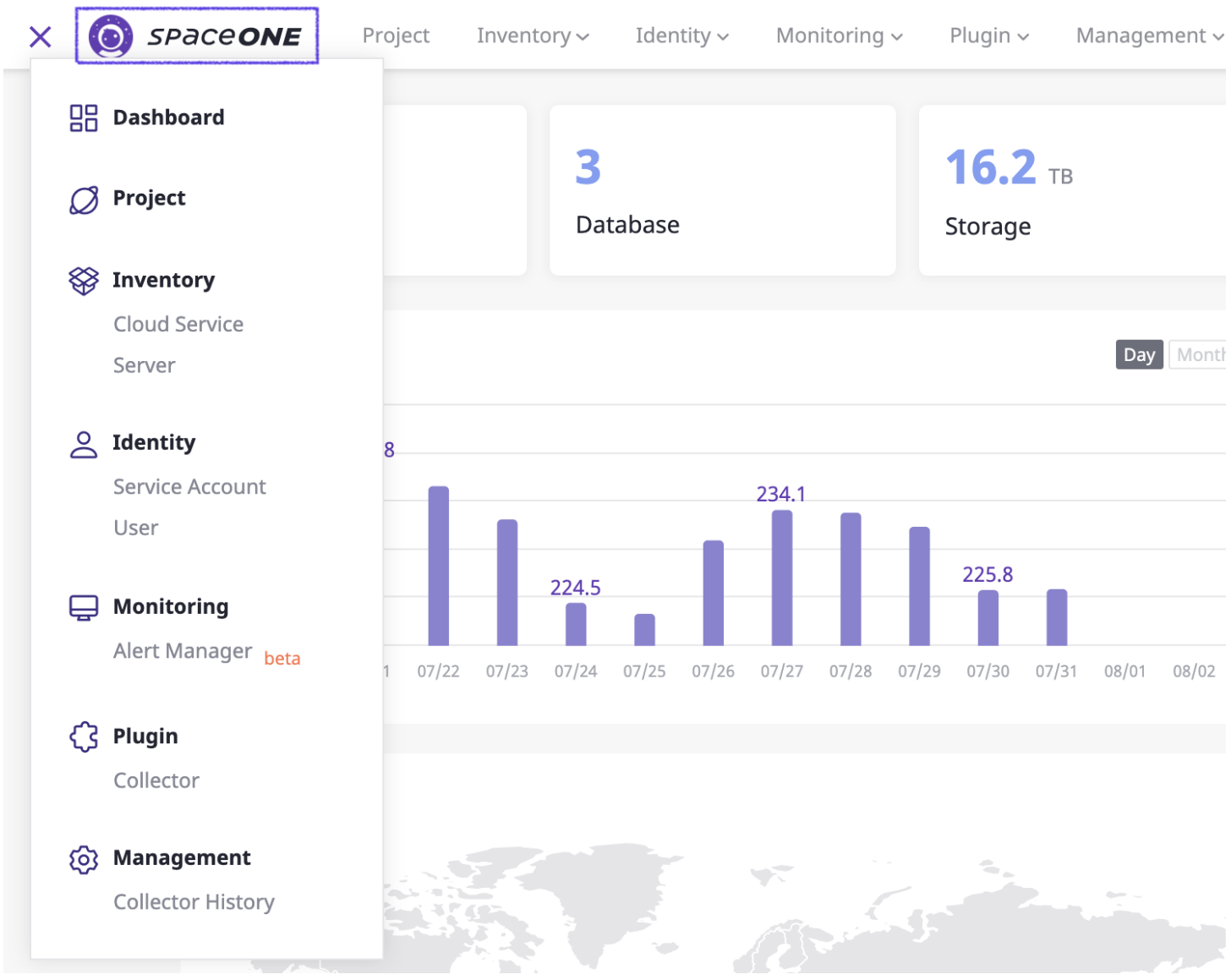
Domain Dashboard provides the full status of the Cloud Resources in your domain.

Overview

The Dashboard is the first screen you will see when connecting to the **SpaceONE** service.
It allows you to look through the status of the entire service being used by the domain.
When you click an item, you can navigate to the corresponding service.

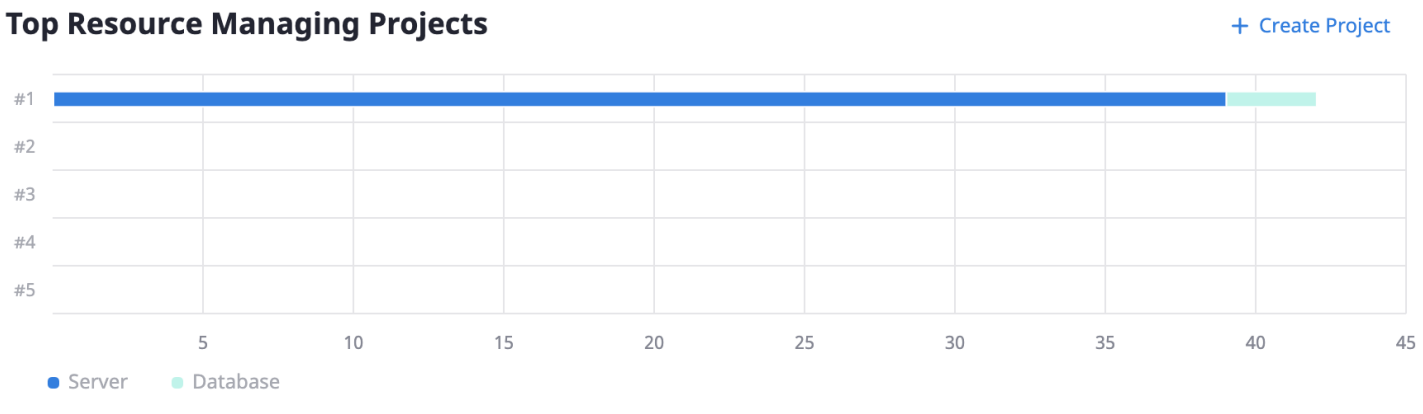


You can use the navigation bar at the top left corner of the screen to quickly navigate to each page.



Top Resource Managing Projects

You can see the status of projects that use **`Resources`** the most.
If you click on each **`Project group / Project`** , you will be taken to the corresponding page.



Rank	Project Group	Project	Compute	Database	Storage
# 1	Project Group 1	AWS	39	3	16.18 TB

Service Accounts

You can see the number of **`Service Accounts`** registered in the domain.
Following **`Service Providers`** are currently available:
Alibaba Cloud

AWS

Azure

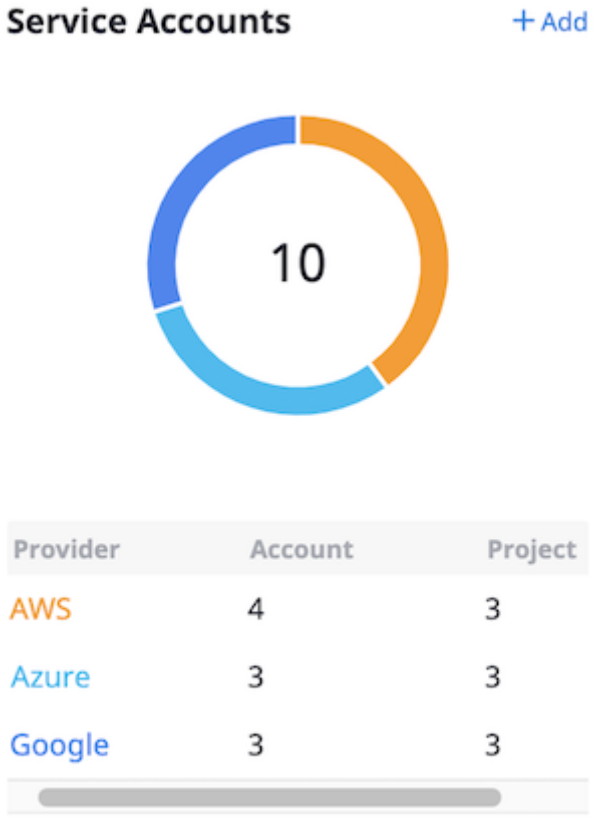
Google

Hyper Billing

Oracle Cloud

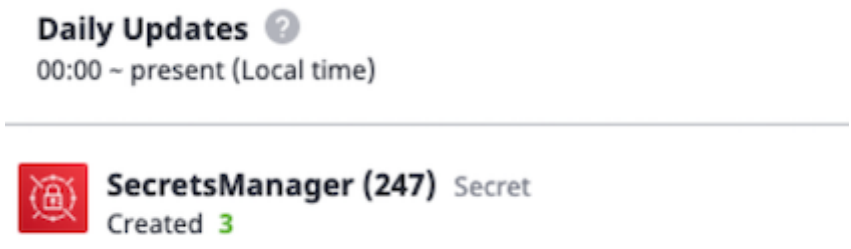
SpaceONE

Also, you can see the current number of **`Service Accounts`** registered for each cloud.



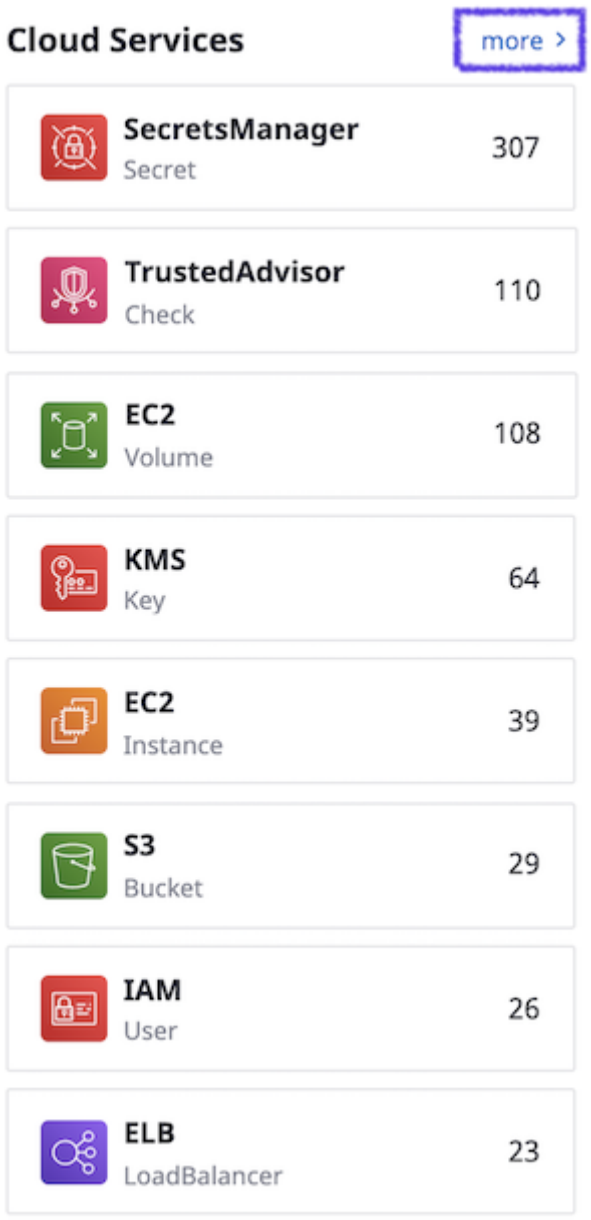
Daily Updates

It shows details about increased/decreased resources on a daily basis.
You can browse the history of changes from **0** to the **present**.



Cloud Services

You can see the number and type of collected cloud service resources at a glance.
If you click the `more` button, you will be taken to the `Cloud Service` page.

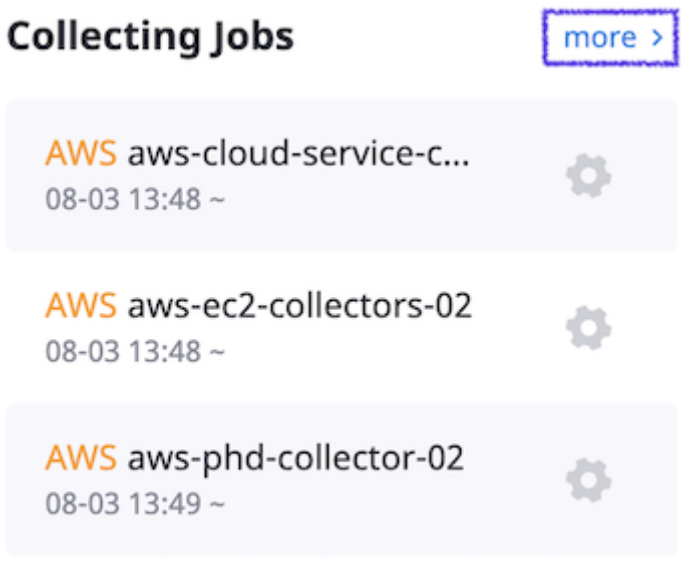


Collection

You can explore the history of **`collector`** execution and the status of **`collectors`** which currently run.

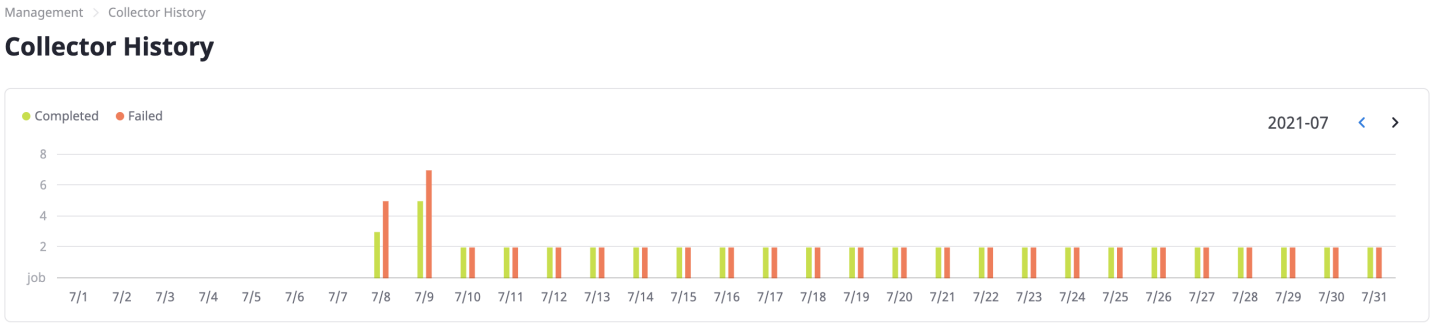
Collector Jobs

`Collecting jobs` shows jobs that are currently being collected.
The **`more`** button links you to the **`Collector history`** page.



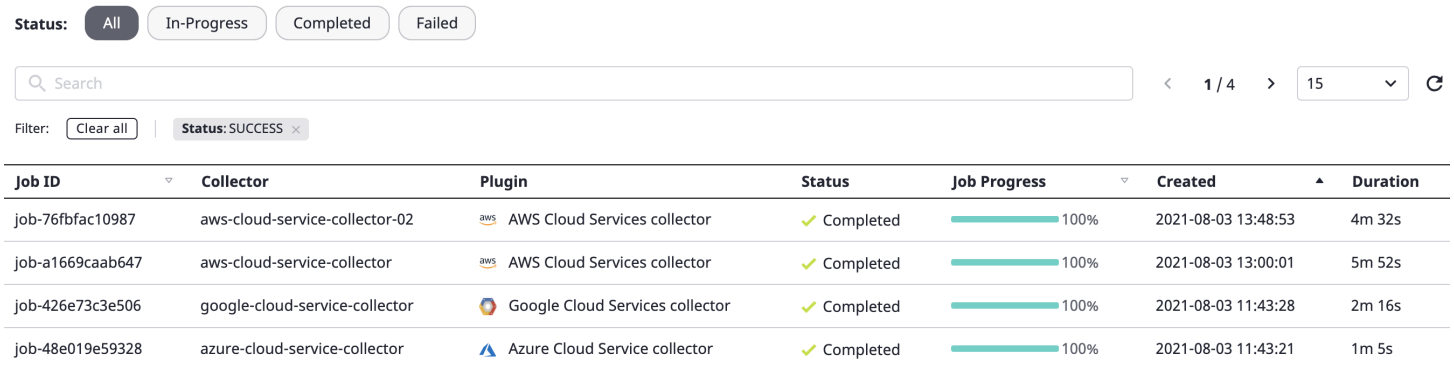
Collector History

`Collector history` shows the completed/failed history of collectors on a monthly basis.



Collecting Progress

You can also check a list of in-progess, completed, and failed collectors.



Job ID	Collector	Plugin	Status	Job Progress	Created	Duration
job-76fbfac10987	aws-cloud-service-collector-02	AWS Cloud Services collector	Completed	100%	2021-08-03 13:48:53	4m 32s
job-a1669caab647	aws-cloud-service-collector	AWS Cloud Services collector	Completed	100%	2021-08-03 13:00:01	5m 52s
job-426e73c3e506	google-cloud-service-collector	Google Cloud Services collector	Completed	100%	2021-08-03 11:43:28	2m 16s
job-48e019e59328	azure-cloud-service-collector	Azure Cloud Service collector	Completed	100%	2021-08-03 11:43:21	1m 5s

3 - Project

About Project Management

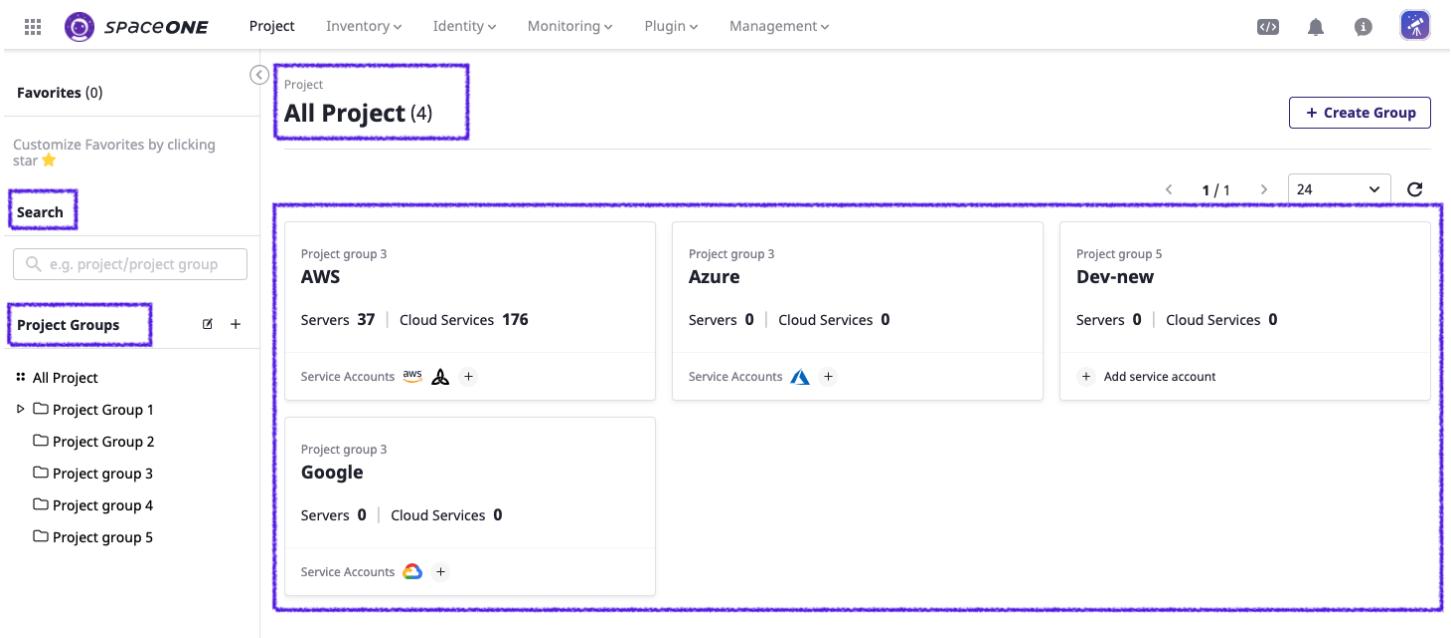
3.1 - Project Group Management

View and manage Project Groups.

Overview

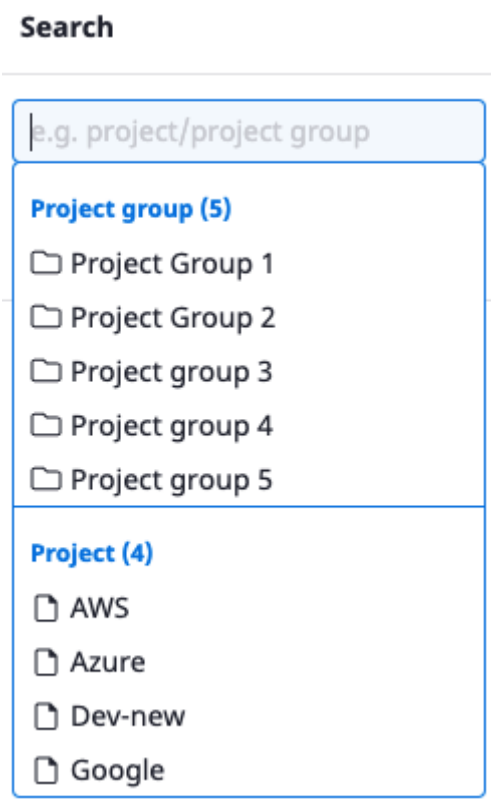
The **`Project`** menu, allows users to manage **`Project groups`** and **`Projects`** .
The Project page consists **`Project Group Management`** and **`Project Management`** as shown below.
It allows company users to participate in projects, and manage authorization through roles in projects.

When you enter the first page of **`Project`** , you can see the entire project list aka the **`All Project`** .



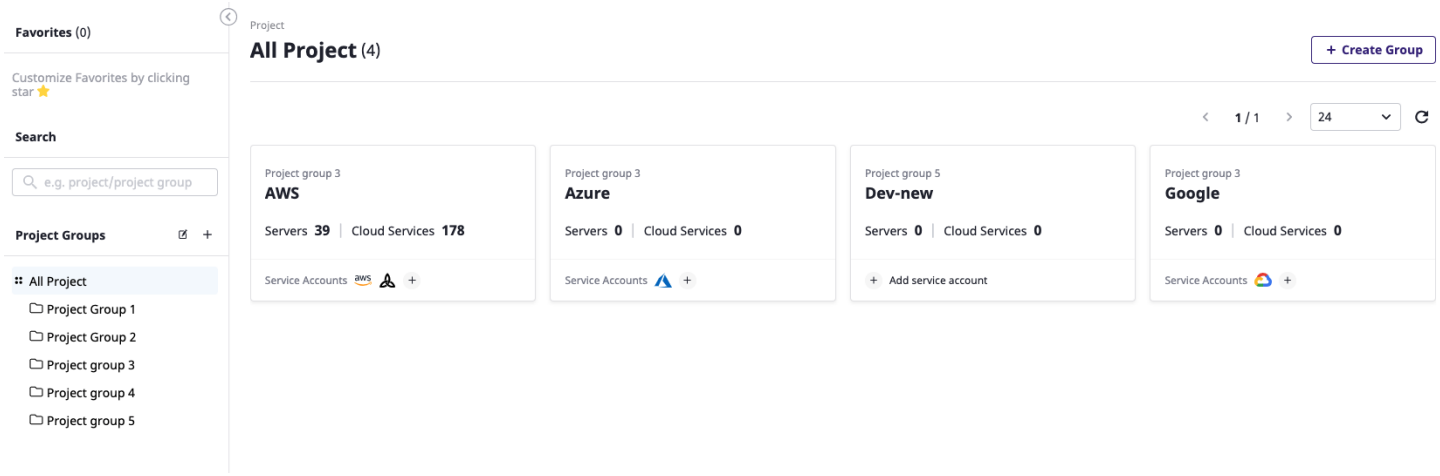
Project Group Management

The search bar on the left allows you to search and move through **`Project Groups / Projects`** .
The search field, helps you easily search / create / edit the **`Project Group Tree`** .

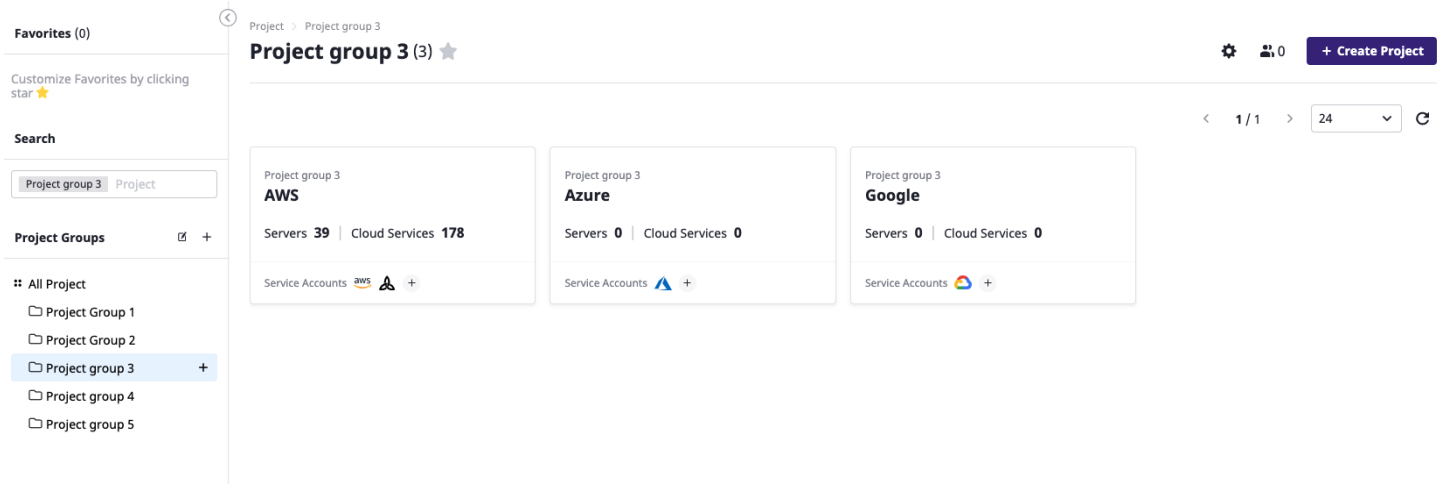


View Project Group

`All Project` shows the list of all projects at once.
You can also select a target project to navigate to the **`Project Dashboard`** .

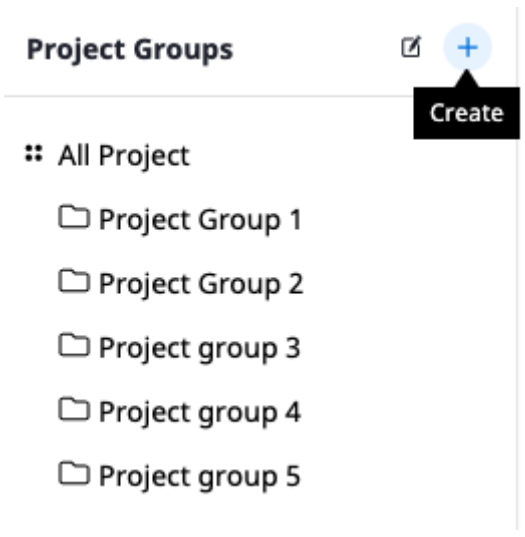


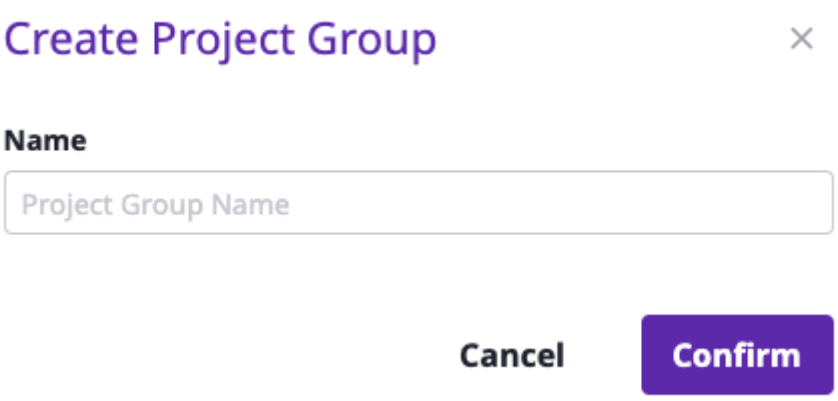
When you select a **`Project group`** , you can see all the projects that belong to the group at once.



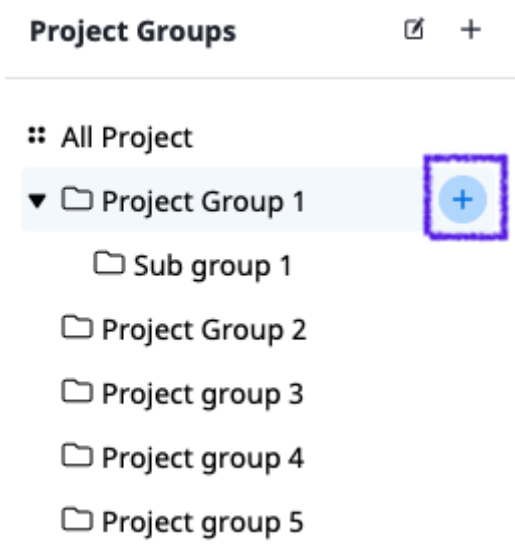
Create Project Group

You can create **`Project Groups`** through the **`Create`** button.



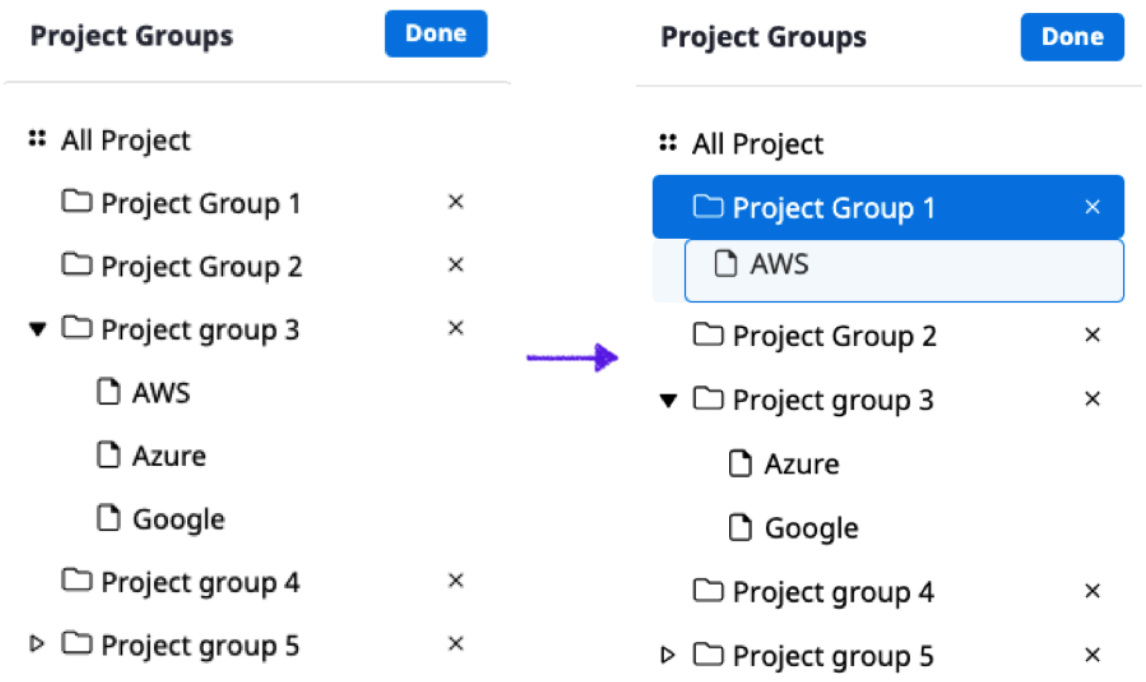


`Project Groups` can have hierarchical relationships.
If you want to create a **`Sub Project Group`** under a parent **`Project Group`** ,
click the **`+`** button like the following image :



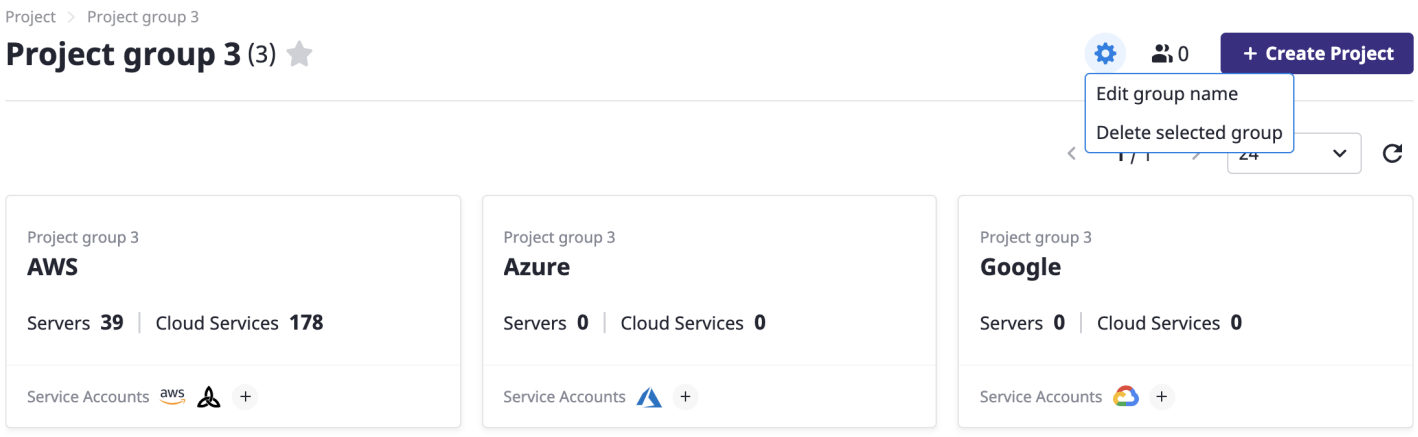
Edit Directory

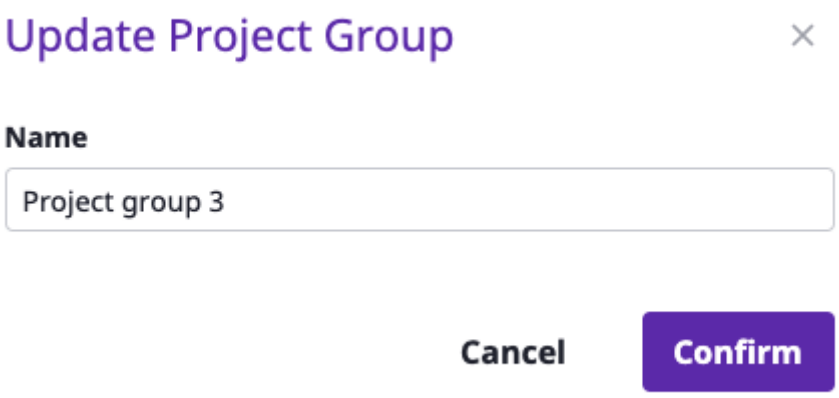
From the `Project Groups` side bar, you can edit the directory of your **Project Groups and Projects**. Simply ***drag and drop*** projects and groups to change the tree structure. After changing the directory please click `Done` to save.



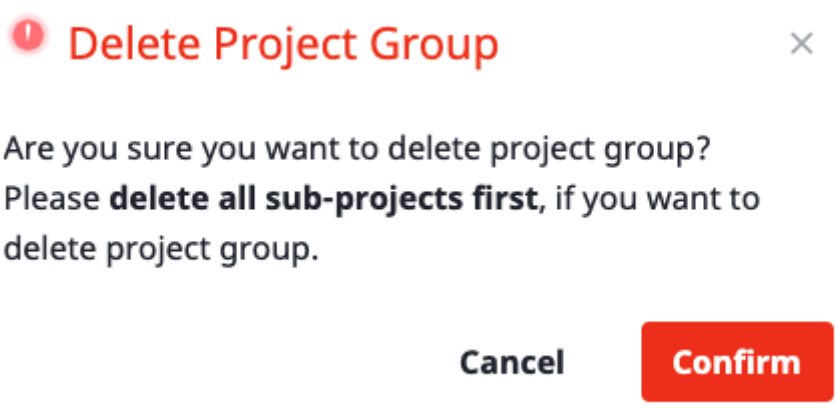
Edit / Delete Project Group

If you want to edit / delete **Project Groups**, Click the ⚙ button at the top right corner of the page.



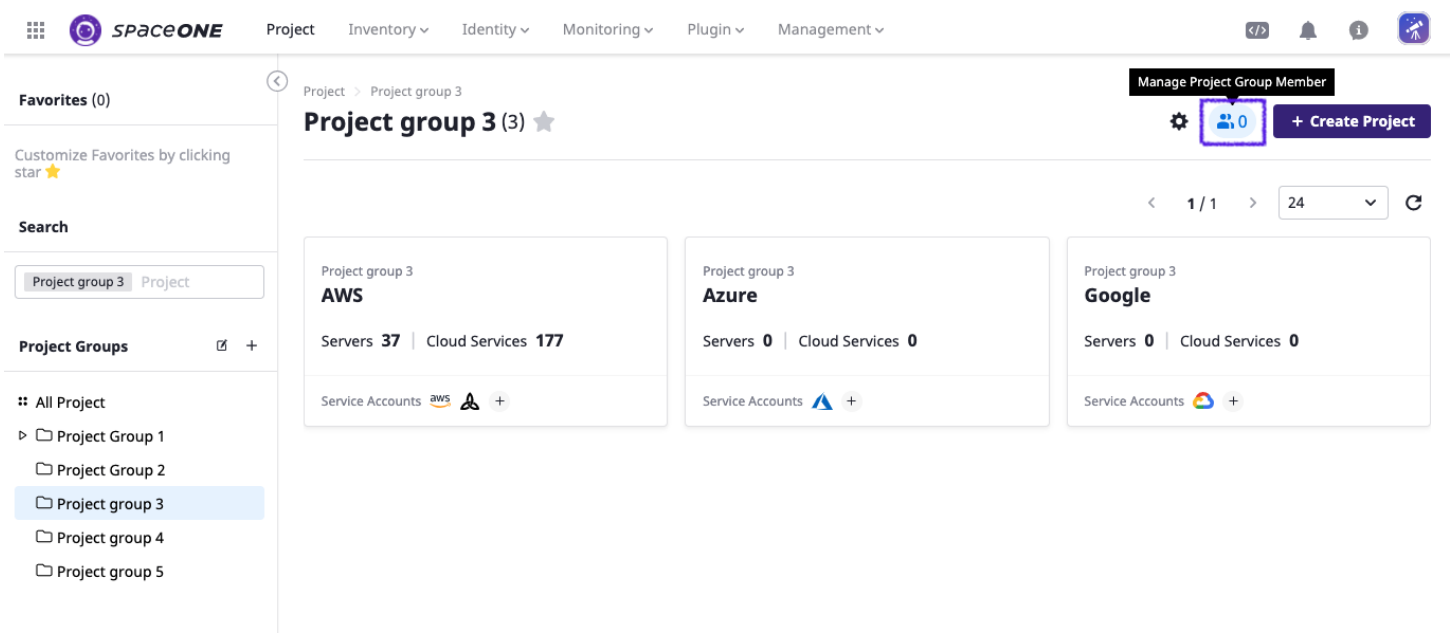


To delete a **Project Group**, you must delete all of the projects that are included in the target group in advance.

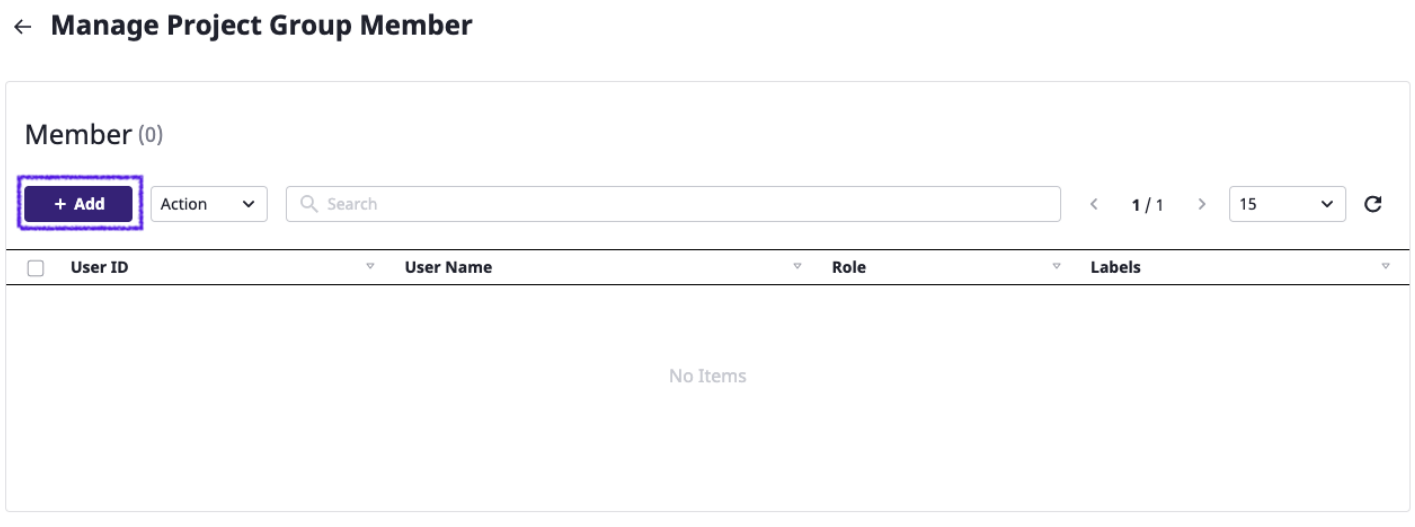


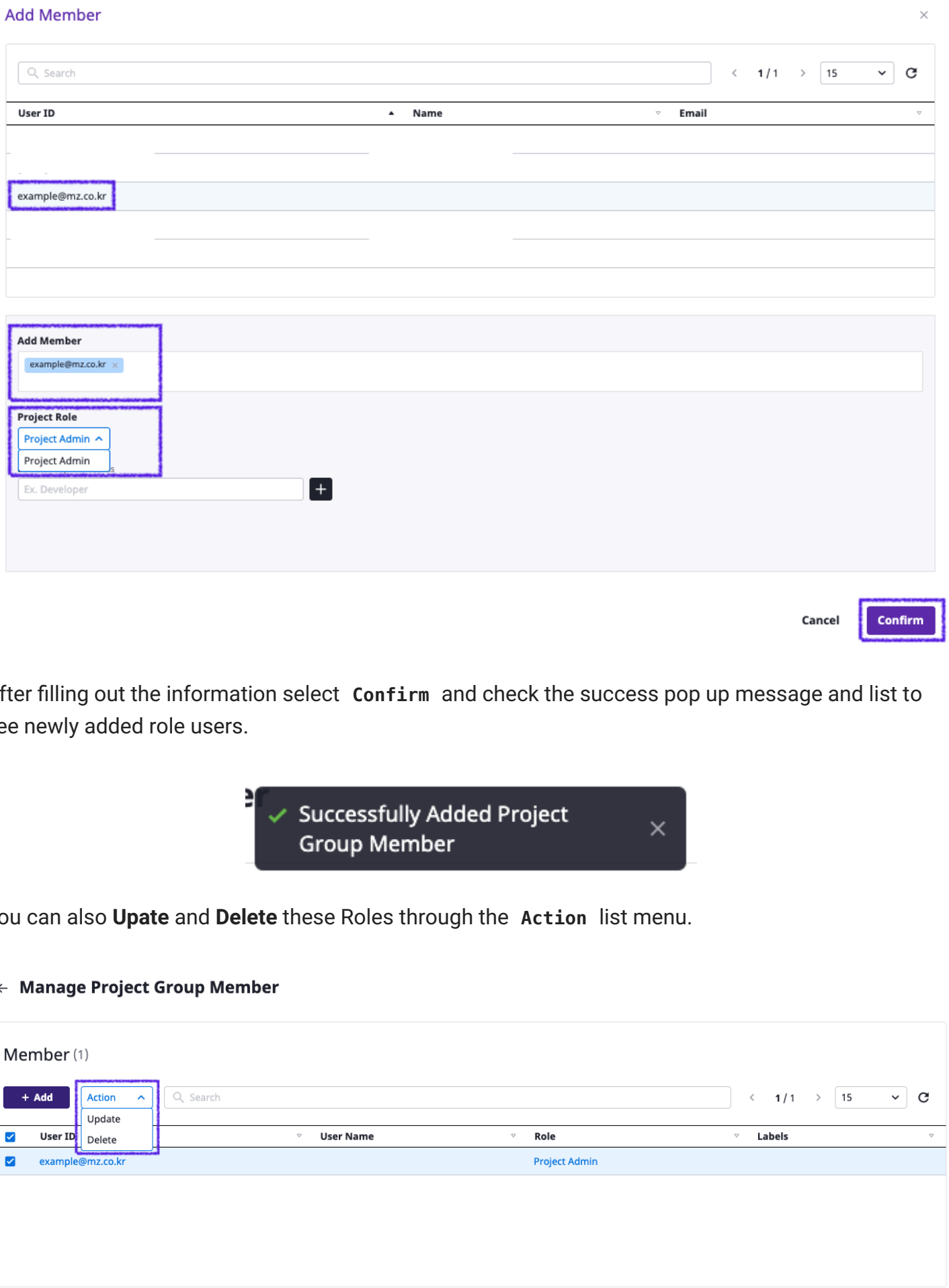
Set Project Group Roles

At SpaceONE users can not only set `Roles` for individual projects/users but also `Project Groups`. Select a `Project Group` and click on the `Manage Project Group Member` icon.



From the `Manage Project Group Member` page select `+ Add`. Then select user IDs that you'd like to give **Project Admin** roles to.





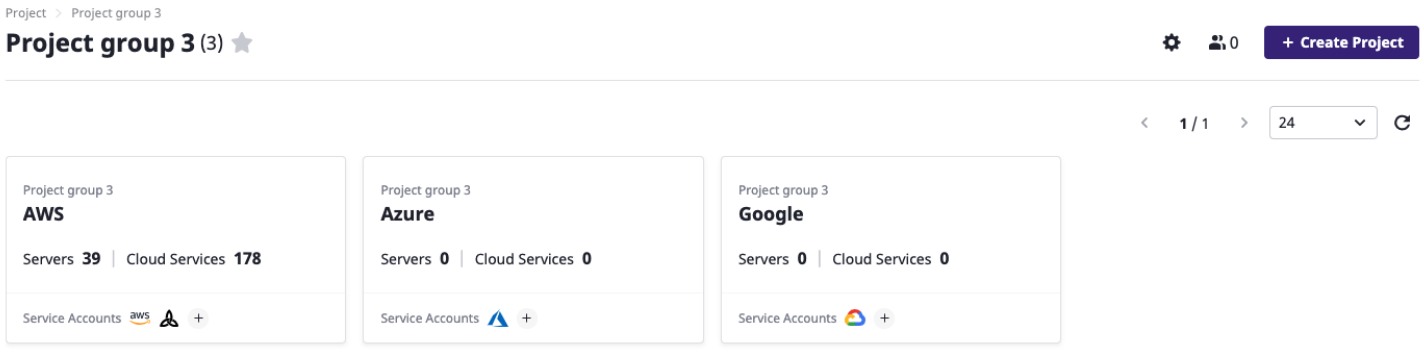
After filling out the information select `Confirm` and check the success pop up message and list to see newly added role users.

You can also **Upate** and **Delete** these Roles through the `Action` list menu.

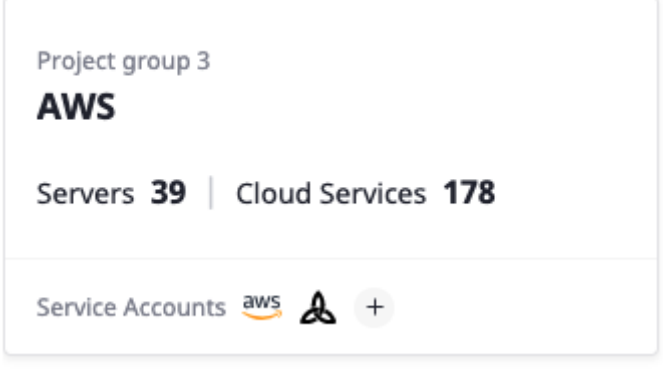
> During this process you can only grant users **Project Admin** roles.
> However if you would like to see further details about different **Users Role types** and **Users Role Settings**, please visit here.

View Project

To see a summary of the projects included in a group, select a **Project Group**.

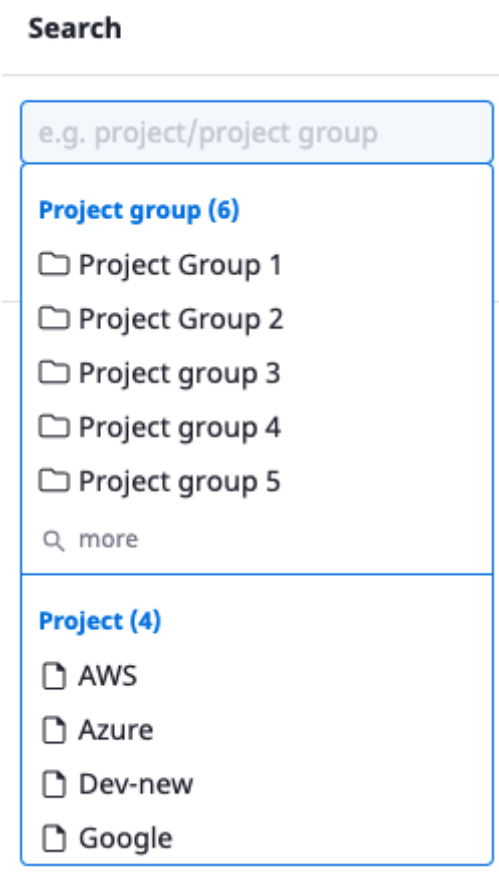


You can see a brief summary on how many **`Servers / Cloud services`** each project has.
You can also check your **Cloud `Service Account` Type**.



Search Project Group

The **`Search Bar`** helps you move quickly through **`Project Groups / Projects.`**



The **`Search bar`** enables the following actions:
Search **`Project Group / Project`** by simple keywords.
Provides links to project pages
Shows all projects when clicking the **`more`** button.

3.2 - Project Management

View overall status of each project and Navigate to detailed cloud resources.

Overview

The `Project` page allows you the following features:

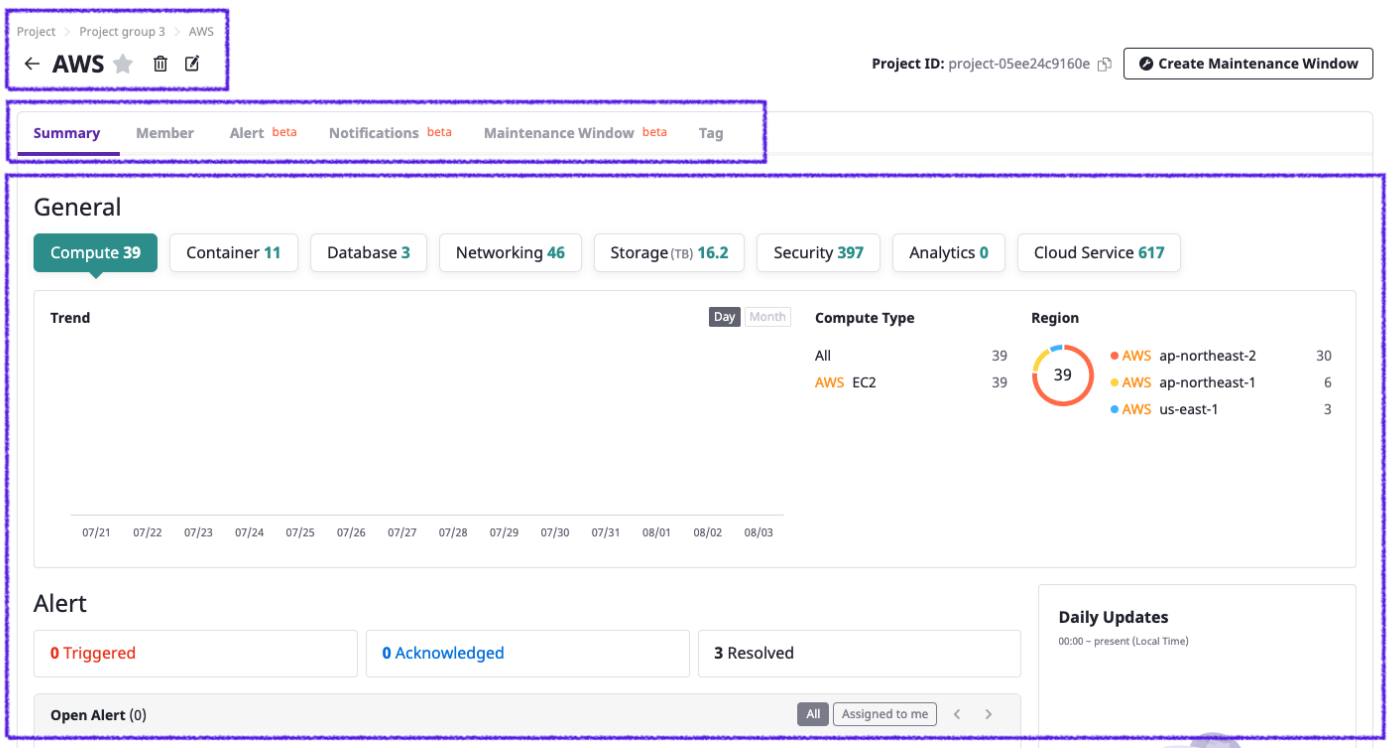
View and edit projects.

View project details

View Summary, Member, Alert, Notifications, Maintenance Window, and Tags.

Project Dashboard

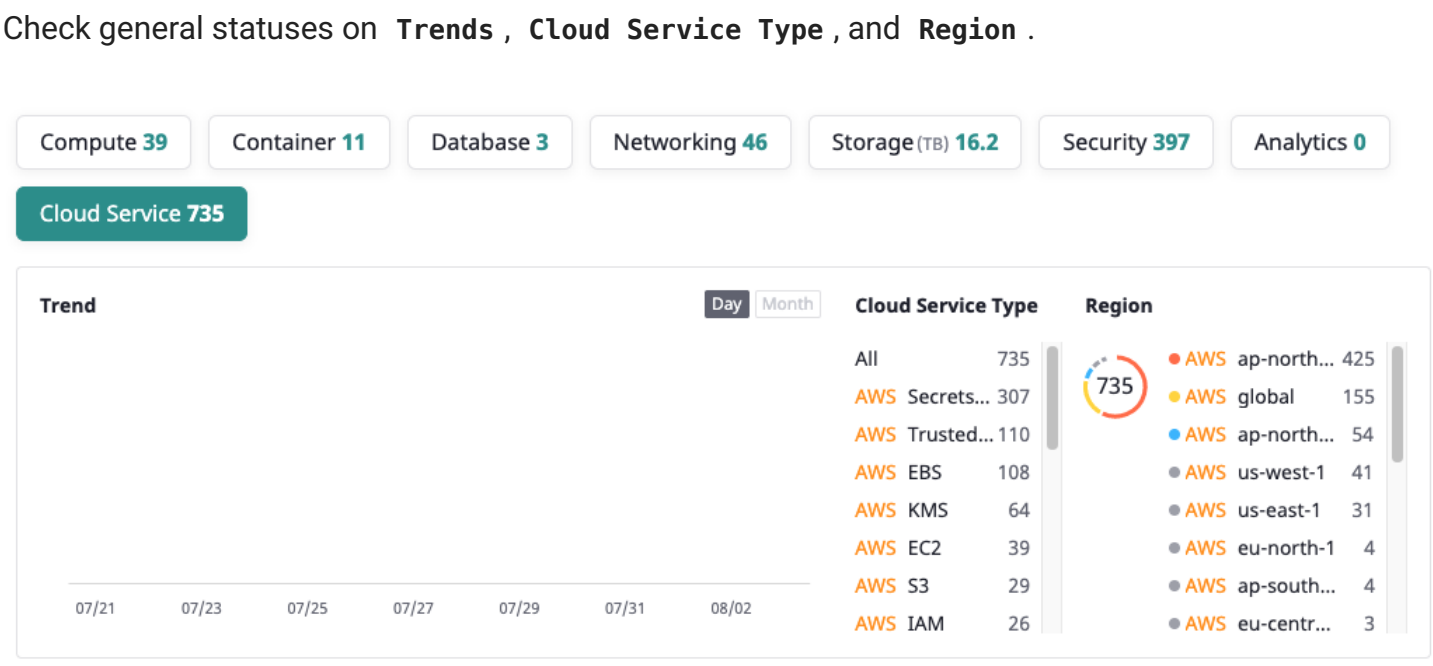
View overall usage of projects. Users can check usage by resource classifications. Click on each classification icon to see the detailed informations.



Summary

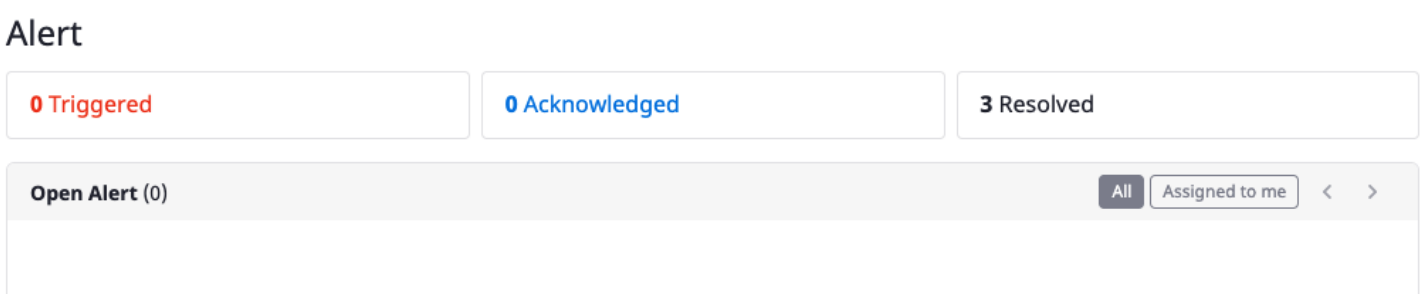
General

Check general statuses on `Trends`, `Cloud Service Type`, and `Region`.



Alert

You can easily check on `Alerts` by their statuses.

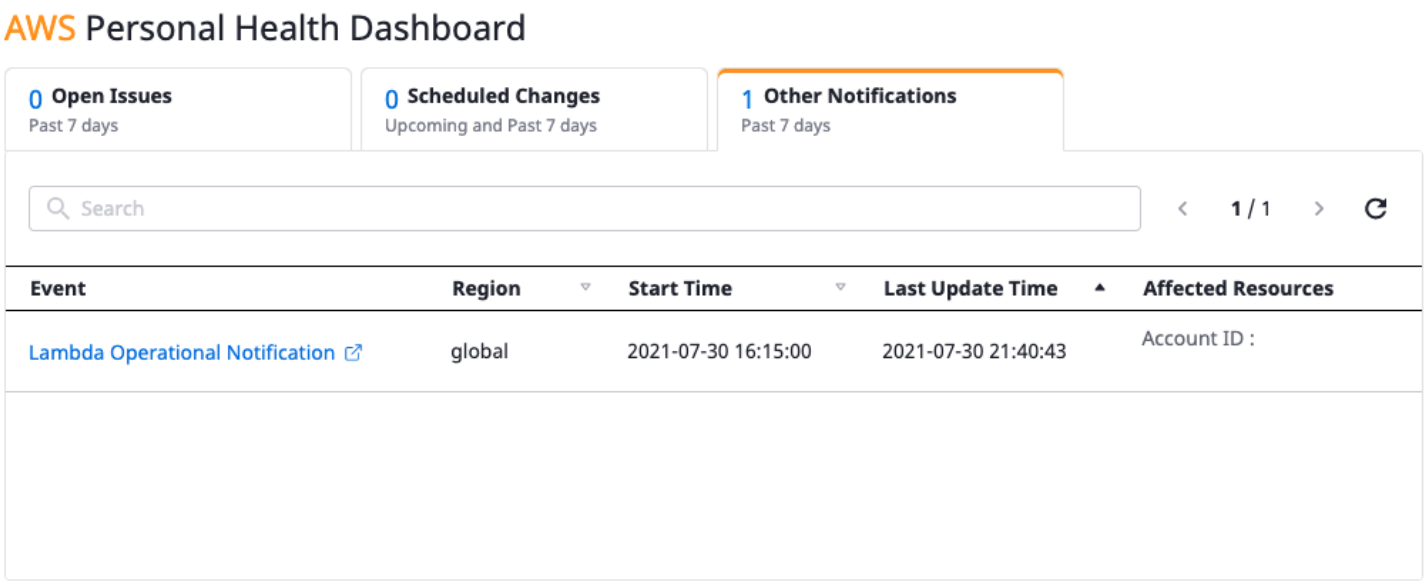


Billing

You can easily check **`Billing Trends`** . Click on each service names to see details.

Personal Health Dashboard

You can check **`Open Issues`** , **`Scheduled Changes`** and **`Other Notifications`** on the **`Personal Health Dashboard`** .

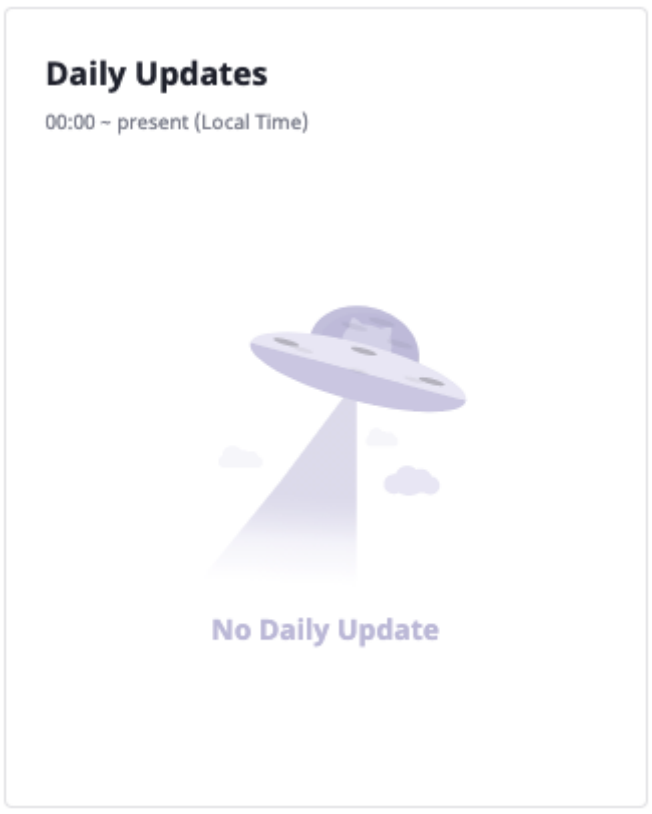


Service Accounts

You can check resource usages from **`Service Accounts`** within the project. You can also check the amount of resources registered.

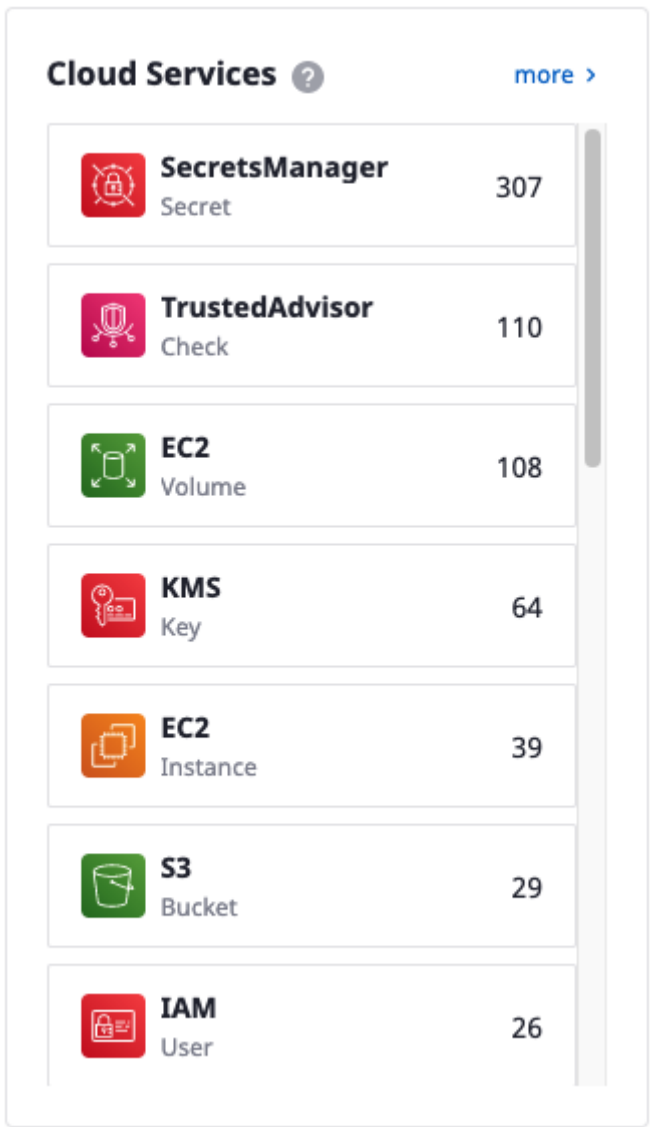
Daily Updates

`Daily updates` shows the history of changes in your cloud resources.
Click on each update to go to the detailed status page.



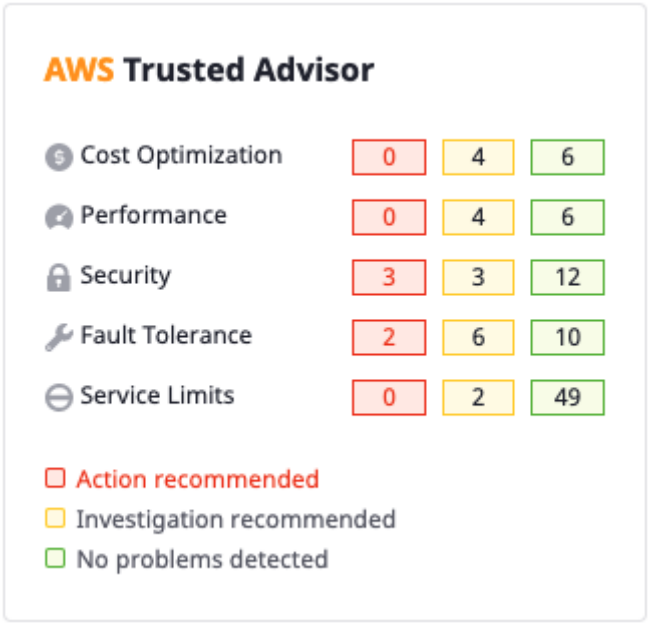
Cloud Services

You can check the major services from the **`Cloud Services`** .
To see further details you can click on each service or the **`more >`** button.



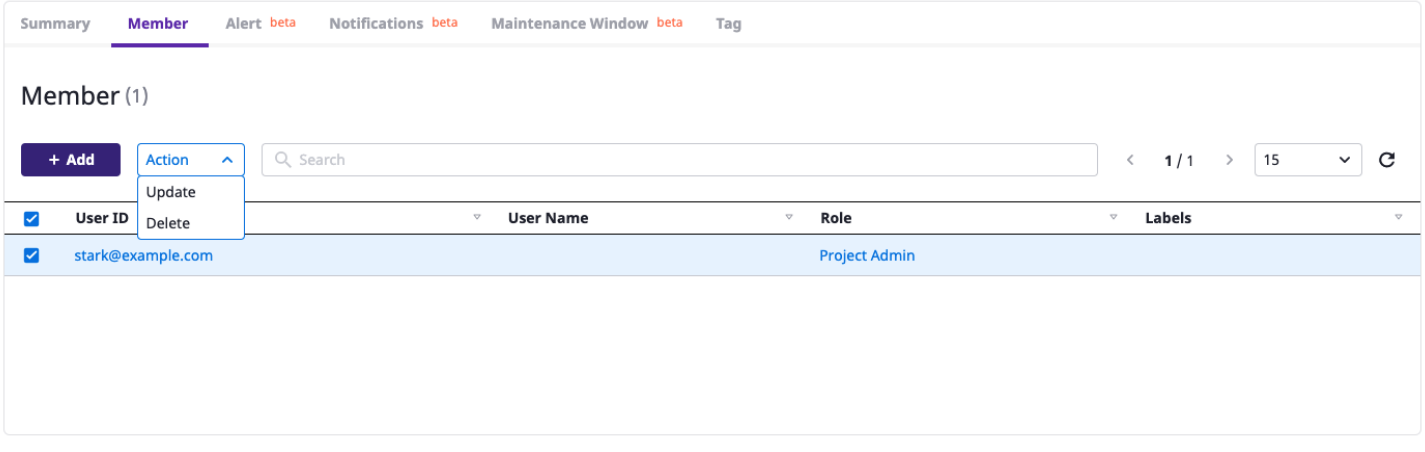
Trusted Advisor

You can easily check Advises on **`Cost Optimization`** , **`Performance`** , **`Security`** , **`Fault Tolerance`** , and **`Service Limits`** from the **`Trusted Advisor`** .



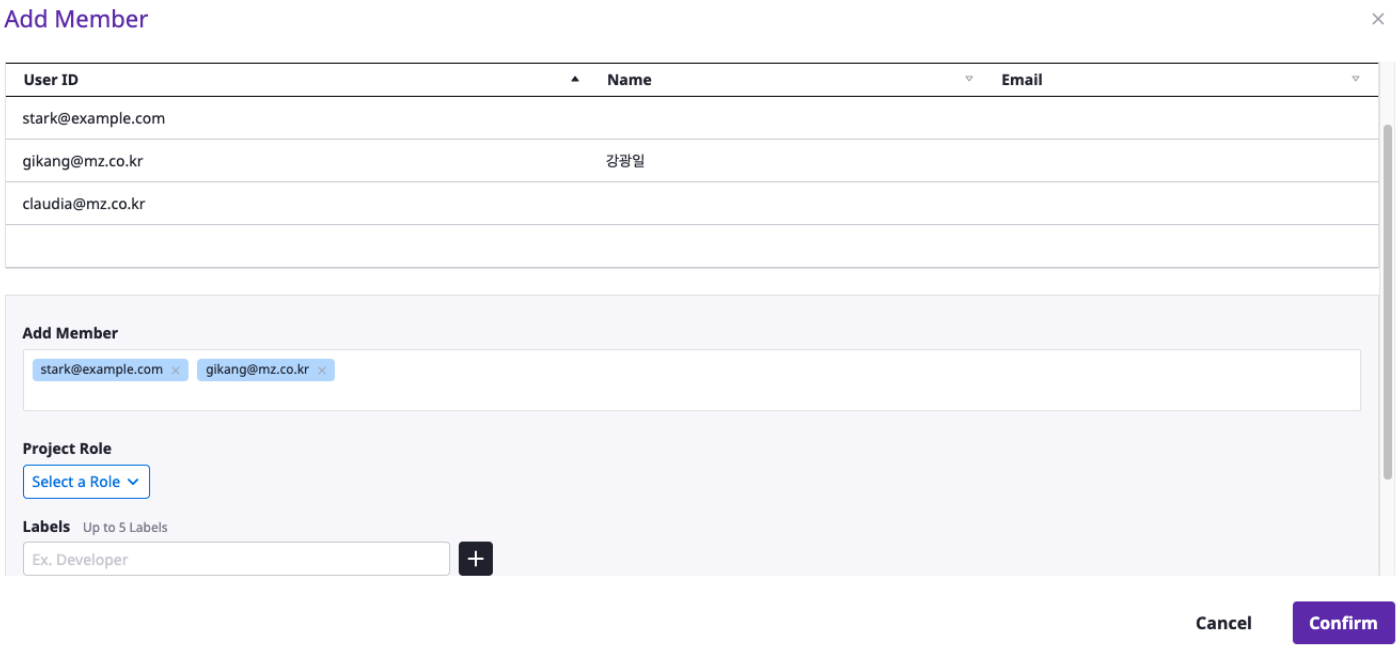
Member

`Add` or **`Delete`** users who can view and manage the project.
To do so, the users should be registered as a **`Project Admin`** in advance.



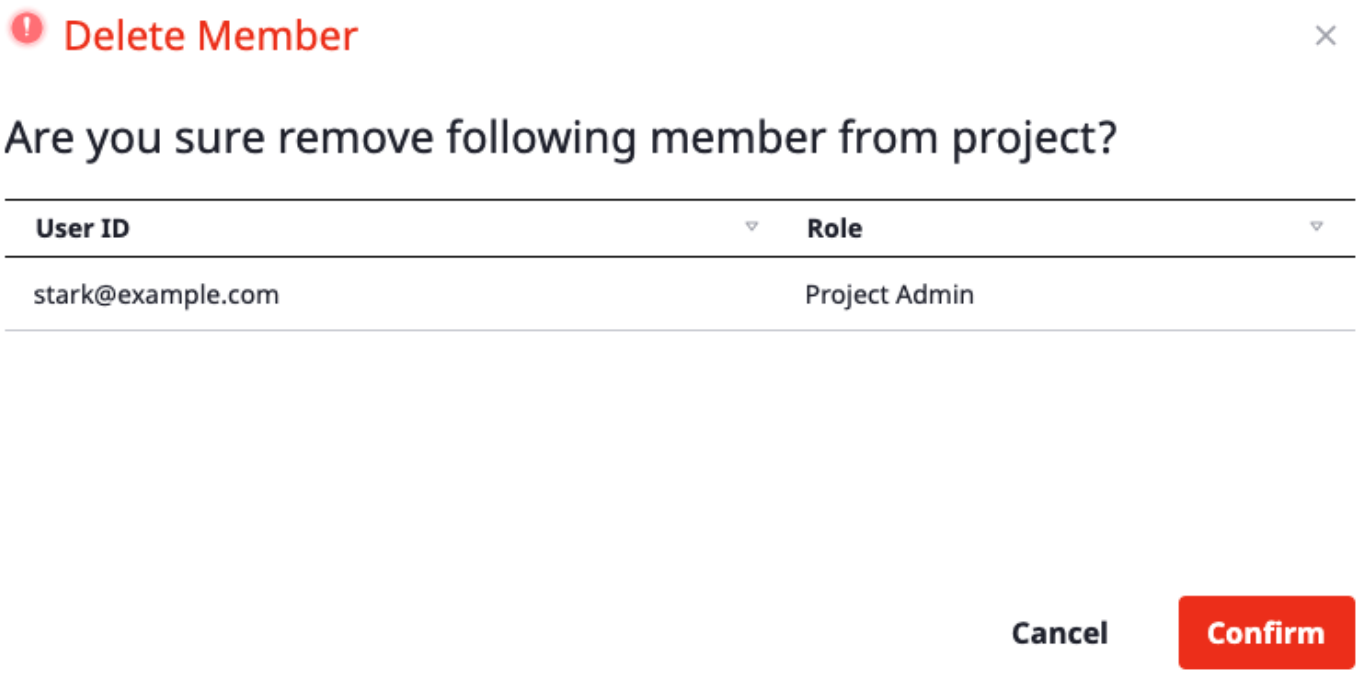
Add member

When you click the **`Add`** button, you can see the **`Add Member`** pop up. You can add multiple users at once.



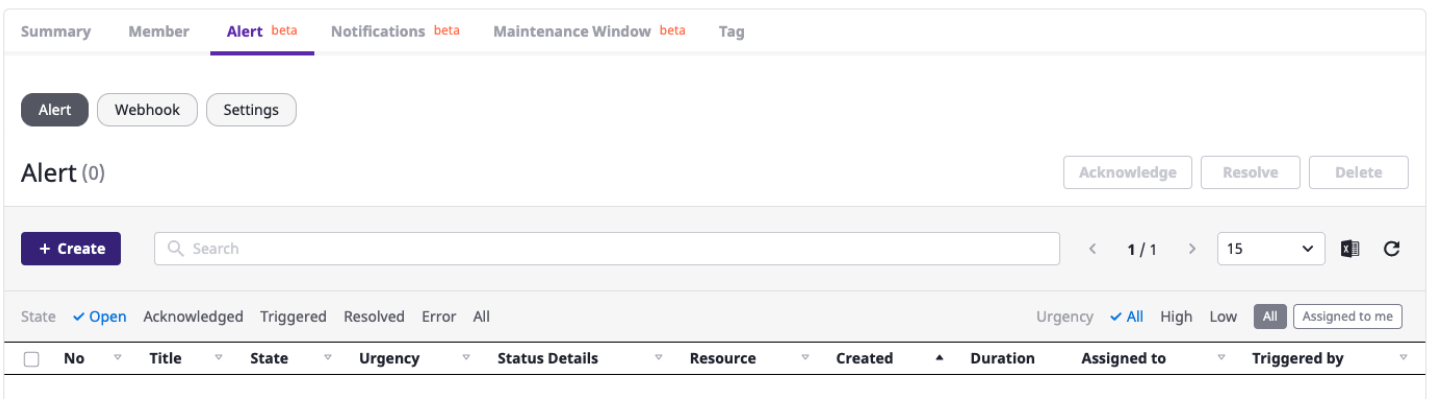
Delete member

Select users you want to delete and click **`Action > Delete`** .



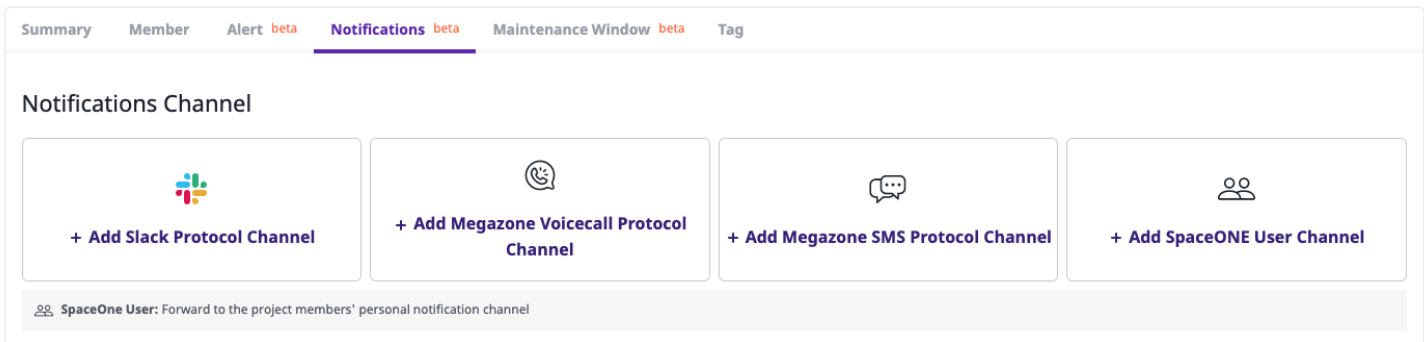
Alert

`Create` , **`Acknowledge`** , **`Resolve`** , **`Delete`** Alerts and Webhooks.
You can also manage Rules and Escalation Policies from **`Settings`** .



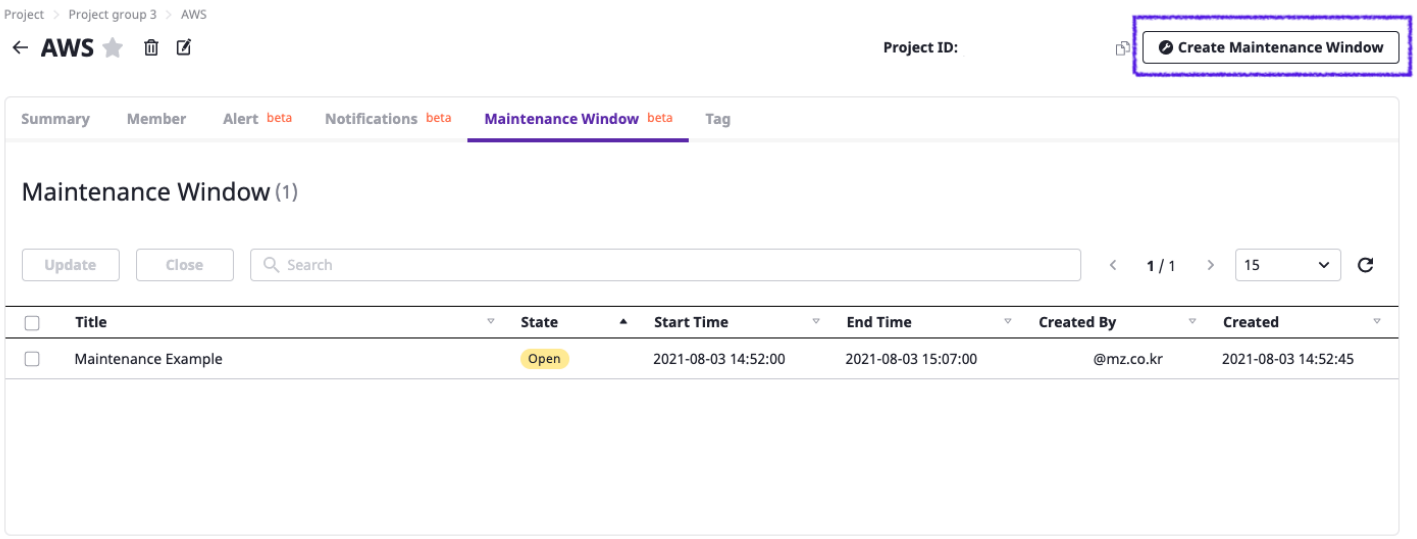
Notifications

Add notification channels such as, **`Slack Protocol`** **`Megazone Voice Call Protocol`** **`Megazone SMS Protocol`** **`SpaceONE User Channel`** .



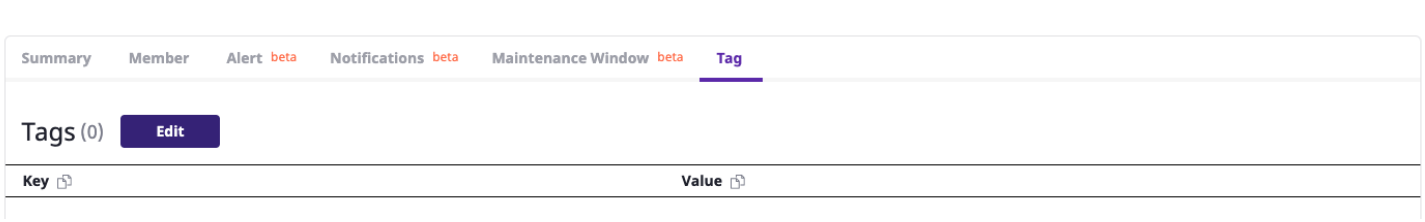
Maintenance Window

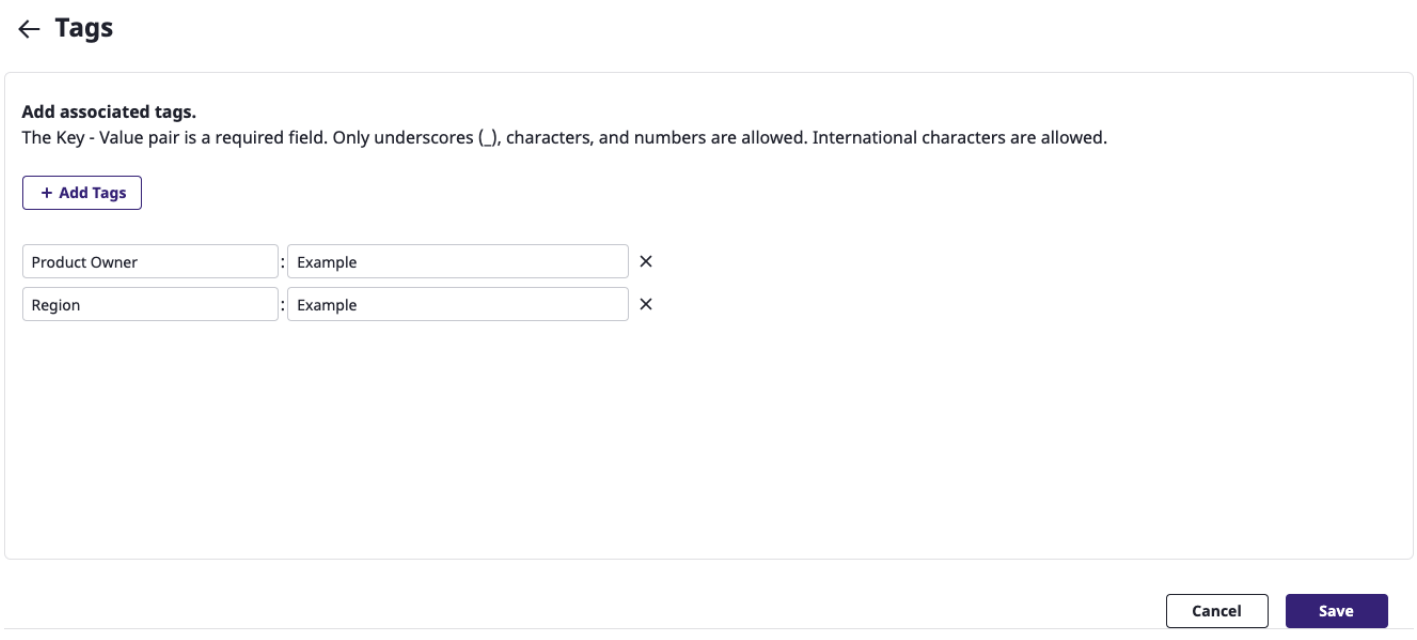
During maintenances you can create or close a **`Maintenance Window`** to prevent new alerts on a project.
Click **`Create Maintenance Window`** and select a schedule.



Tag

You can **`add`** or **`delete`** Tags in your project. Click the **`Edit`** button to do so.



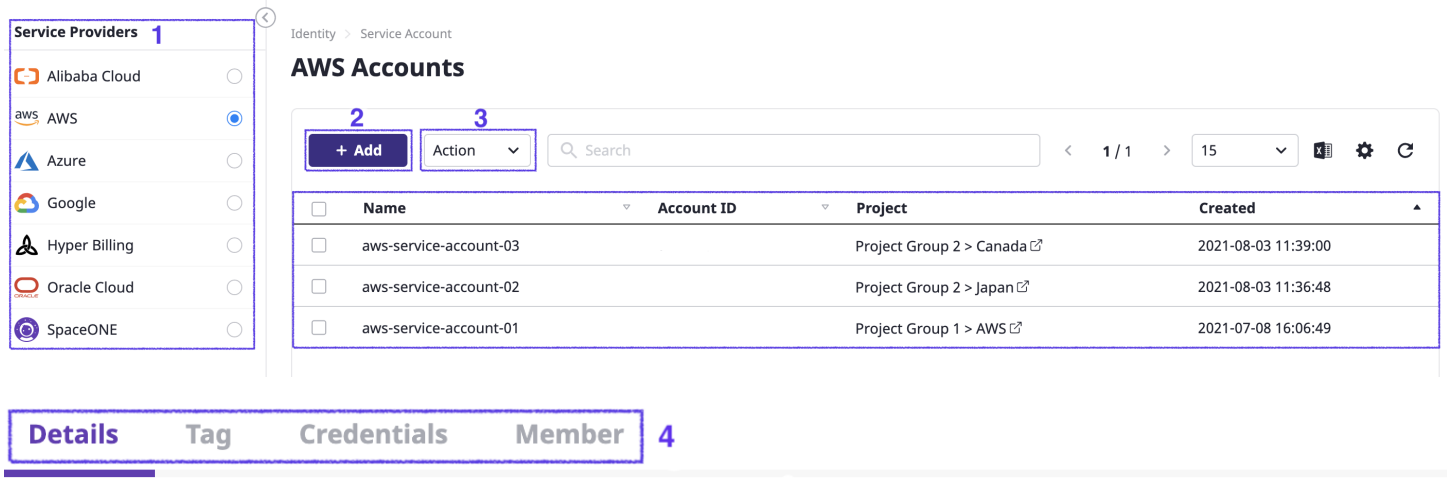


4 - Service Account

Credential information for each cloud providers.

Overall

On the service account page, you can easily manage credentials for each service provider. Multi cloud resources are collected based on these credentials.



1. A list of **Service Providers**
2. Adding **Service Account**
3. Deleting **Service Account** /Changing **Project**/Connecting to **Console**
4. Details, **Tag**/**Credentials** Management, **Member**

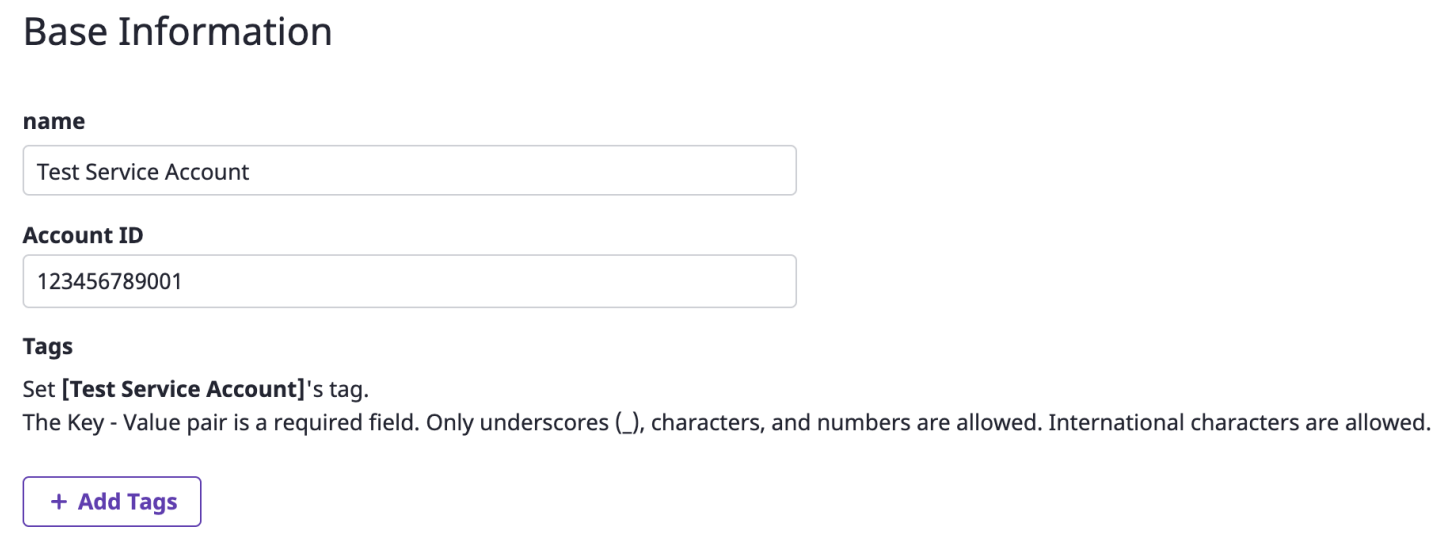
SpaceONE supports the following service providers:

Alibaba Cloud
AWS
Azure
Google
Hyper Billing
Oracle Cloud
SpaceONE

Add Service Account

You can add a **Service Account** simply by selecting a service provider and clicking the **+ Add** button.
For the upcoming steps, we will focus on AWS`s IAM.
To add a **Service Account**, you need to enter a **Name** and an **Account ID** first.

Base Information



Name : Name of **Service Account**

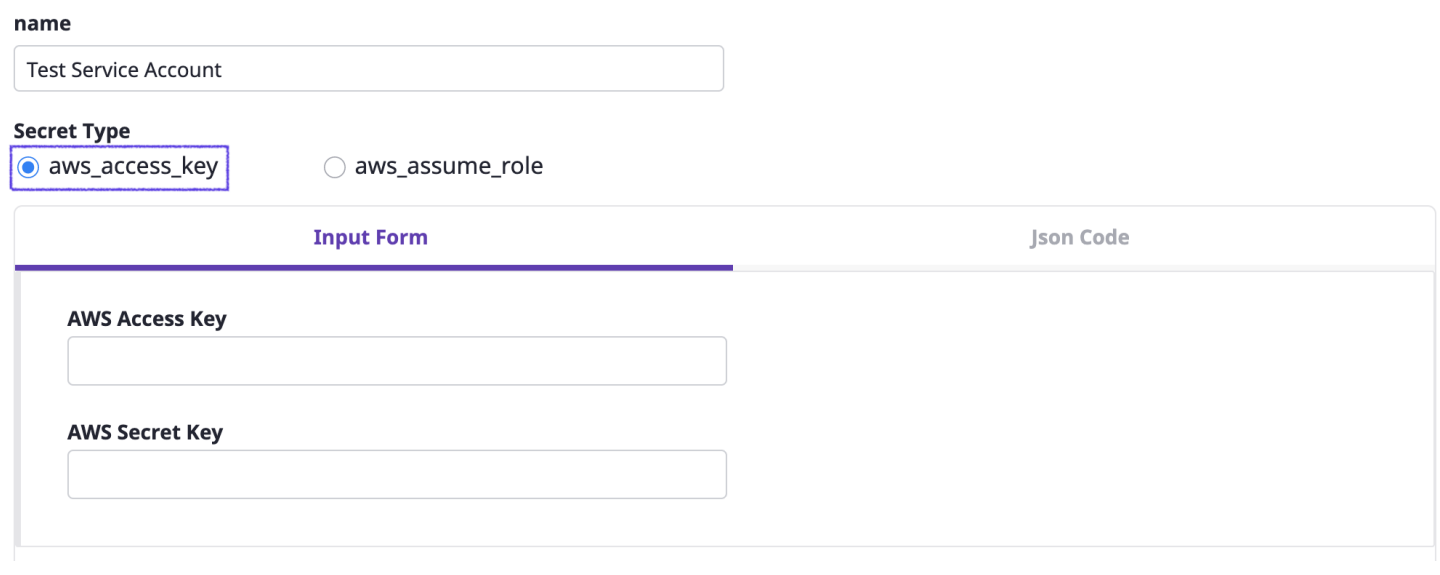
Account ID : Root Account ID (12-digits)

Tags : Additional **Service Account**`s tag

Credentials

Two types of **Service Accounts** are available: aws_access_key, aws_assume_role.

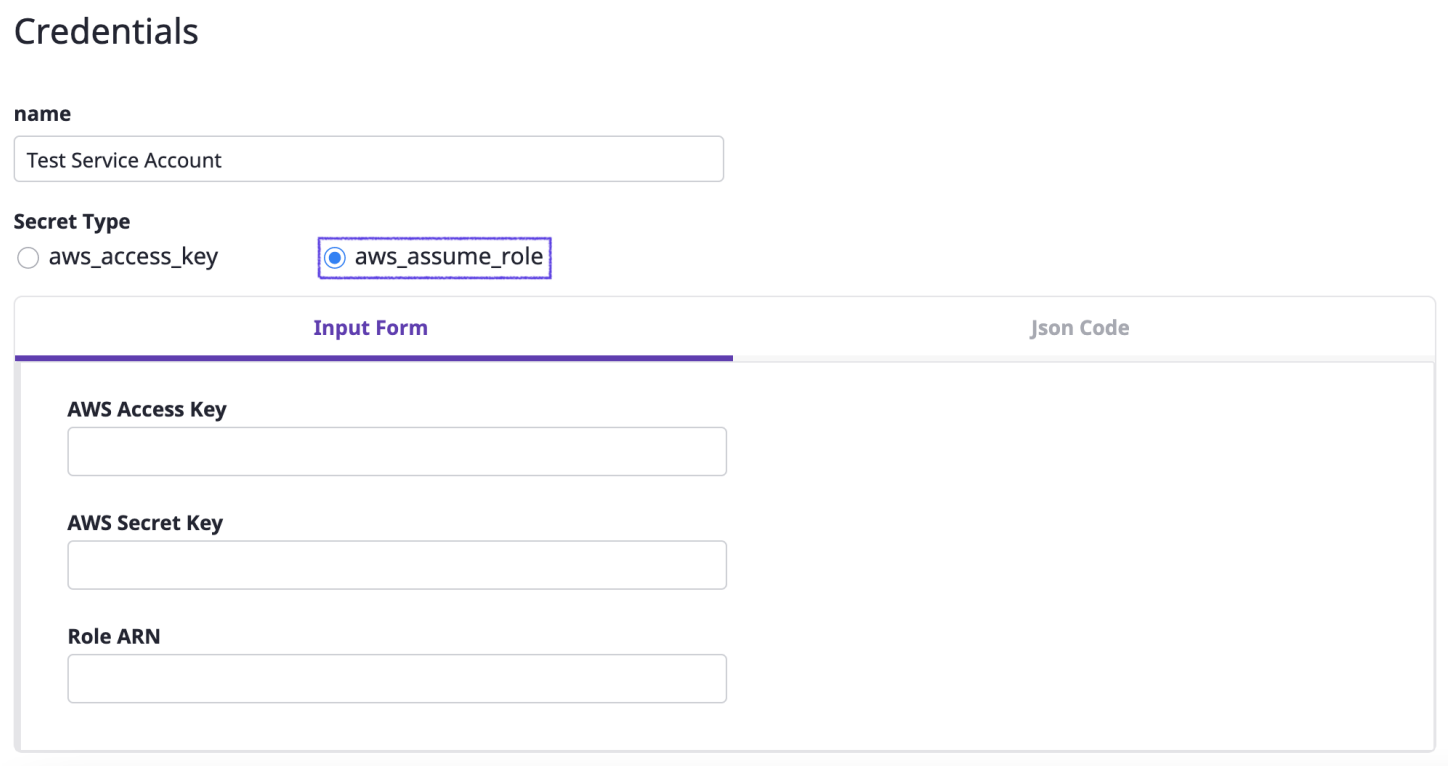
aws_access_key



AWS Access Key (Required) : Access Key from IAM (Read Only policy is strongly recommended).

AWS Secret Key (Required) : Secret key from IAM

aws_assume_role



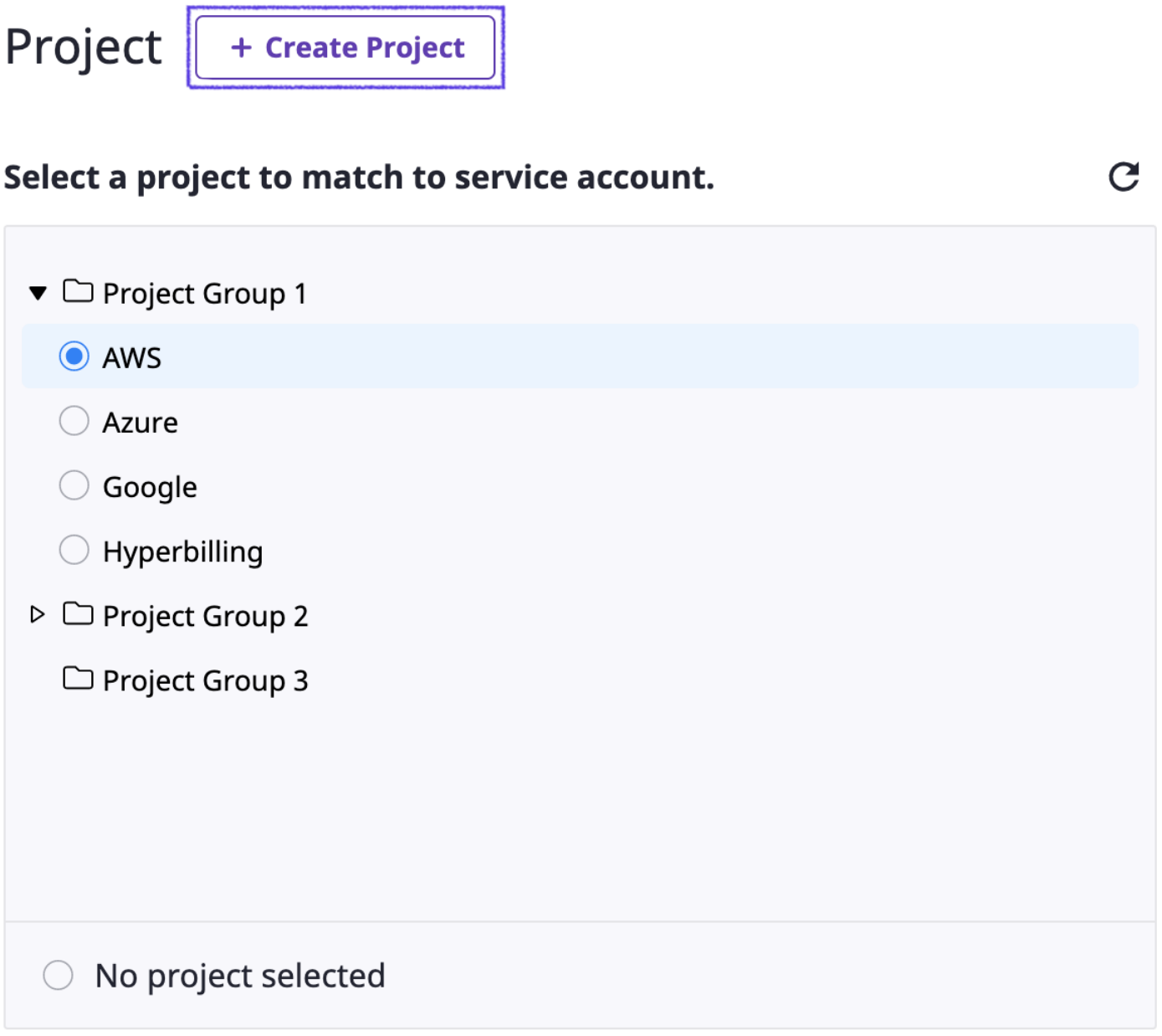
AWS Access Key (Required) : Access key from IAM to assume a role

AWS Secret Key (Required) : Secret key from IAM to assume a role

Role ARN (Required) : Role ARN from IAM to assume a role

Select Project

Select a project in which a **Service Account** will be placed. Collected resources from the **Service Account** will be included to the project automatically.



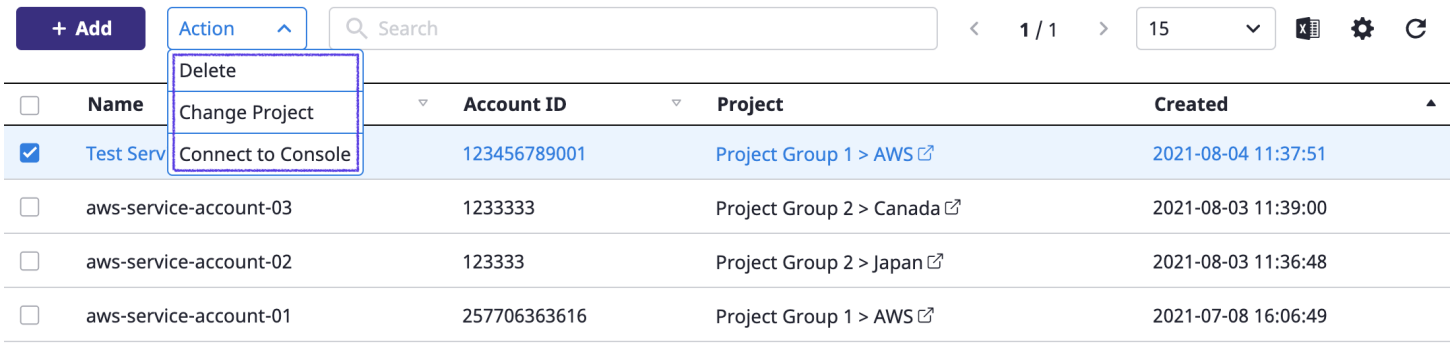
To create a **Project**, click the **+ Create Project** button.
For a more detailed process on creating a project, refer to the link below.

Project Group Management

Select a project you want, then click the **Save** button.

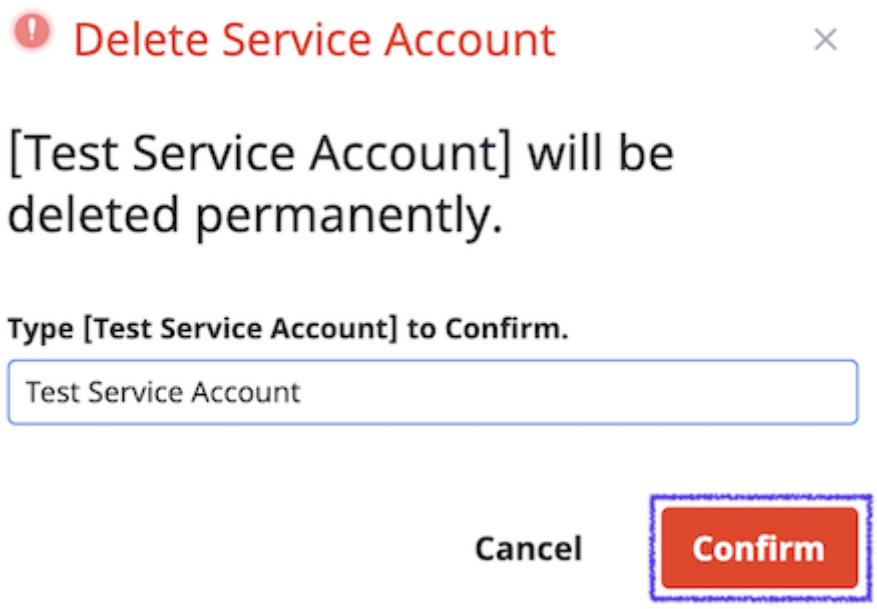
Delete Service Account/Change Project

You can delete a **Service Account** or change a **Project** linked to a certain **Service Account**.
Select the target **Service Account**, then click **Action > Delete/Change Project**.



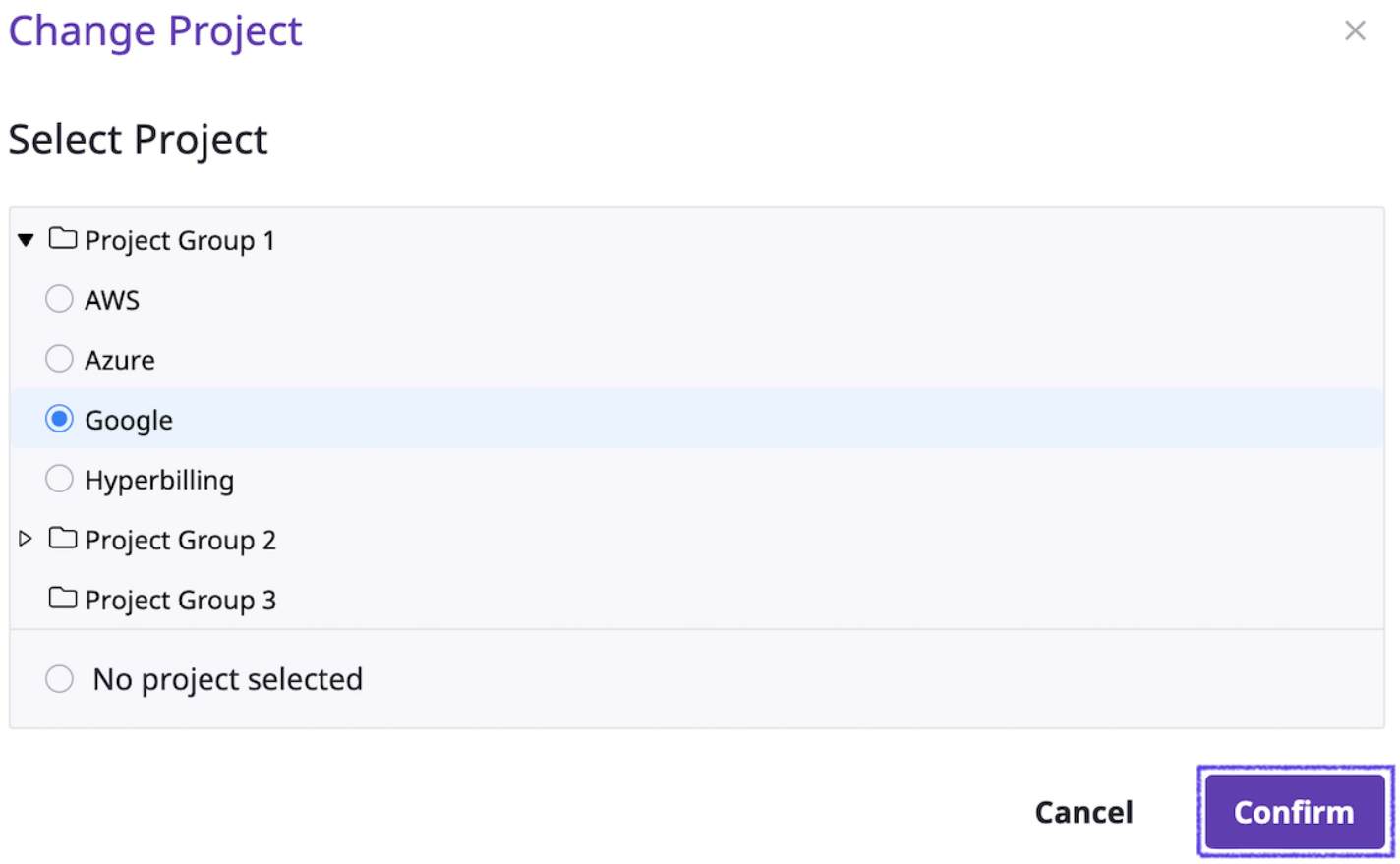
Delete Service Account

Enter a name of a **Service Account** you want to delete, then click the **Confirm** button.



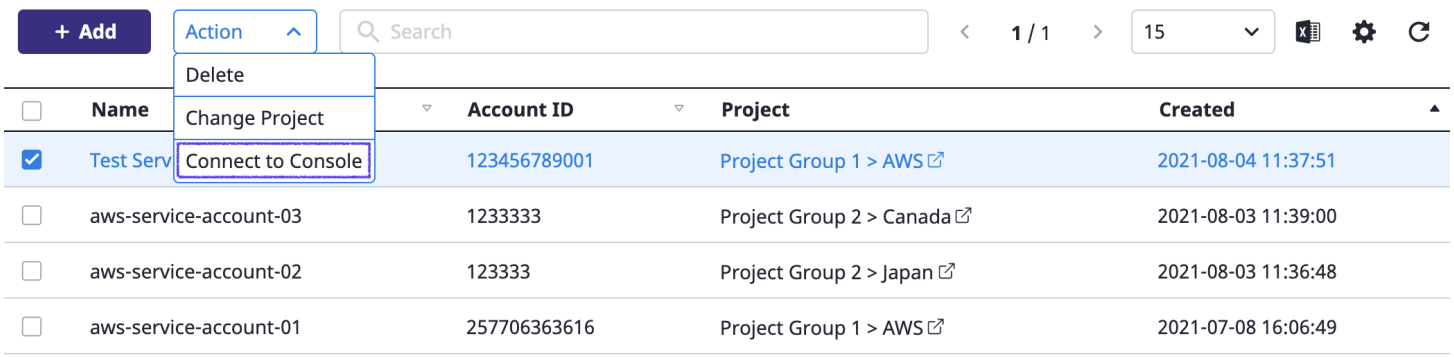
Change Project

Select a project you want to newly link a **Service Account**, then click the **Confirm** button.



Link to AWS Console

Select the target **Service Account**, then click **Action > Connect to Console**.



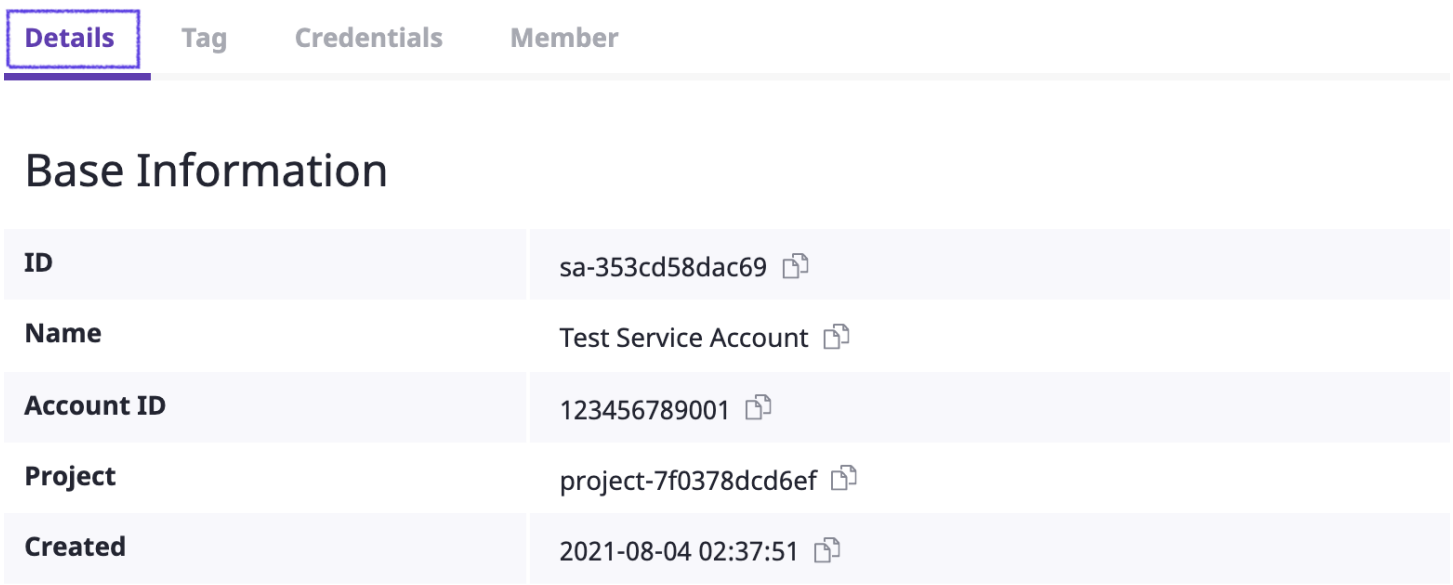
To access AWS console, you must be logged into AWS console in advance. (AWS Console SSO is not available.)

Status Tab

Using the **Status** tab, you can browse details of a **Service Account**.

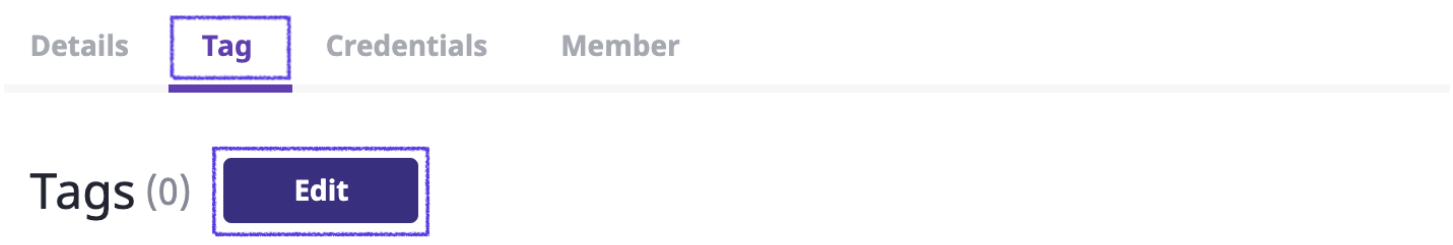
Details

You can see detailed information of a **Service Account** on the **Details** tab.

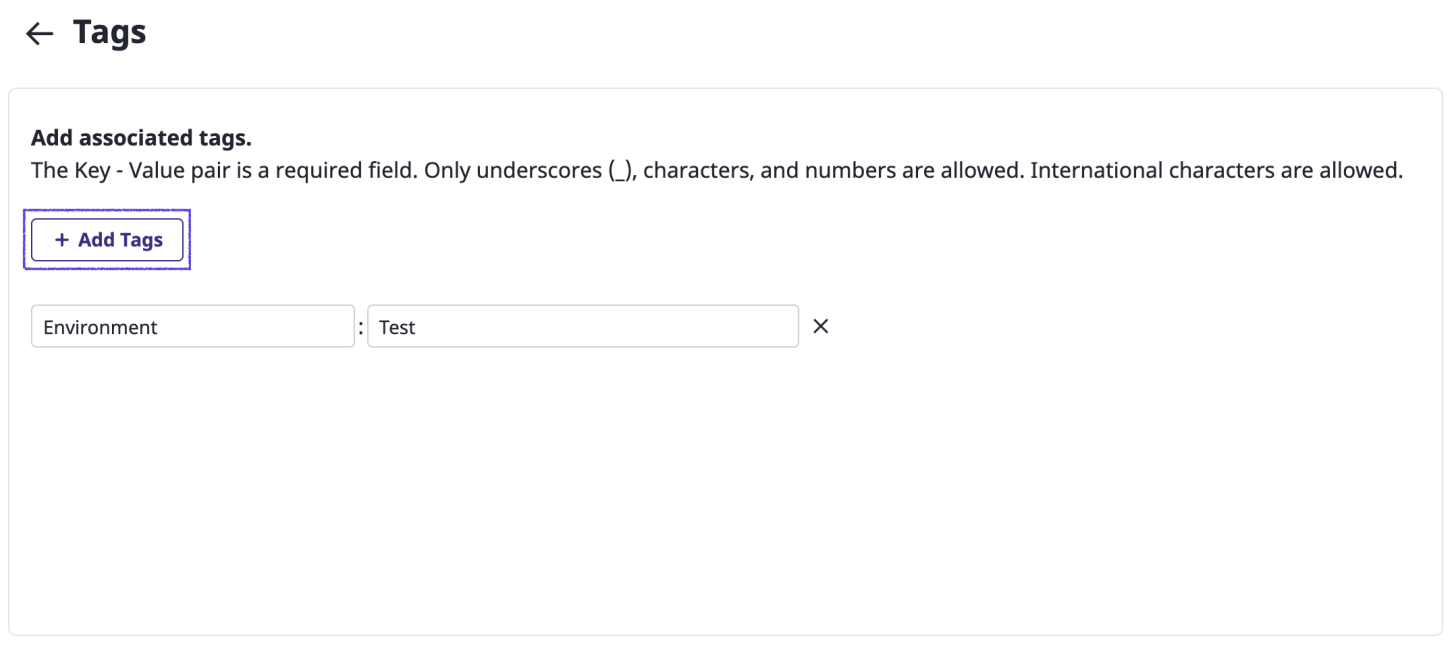


Tag

By clicking the **Edit** button, **Tags** for a **Service Account** can be added or deleted.

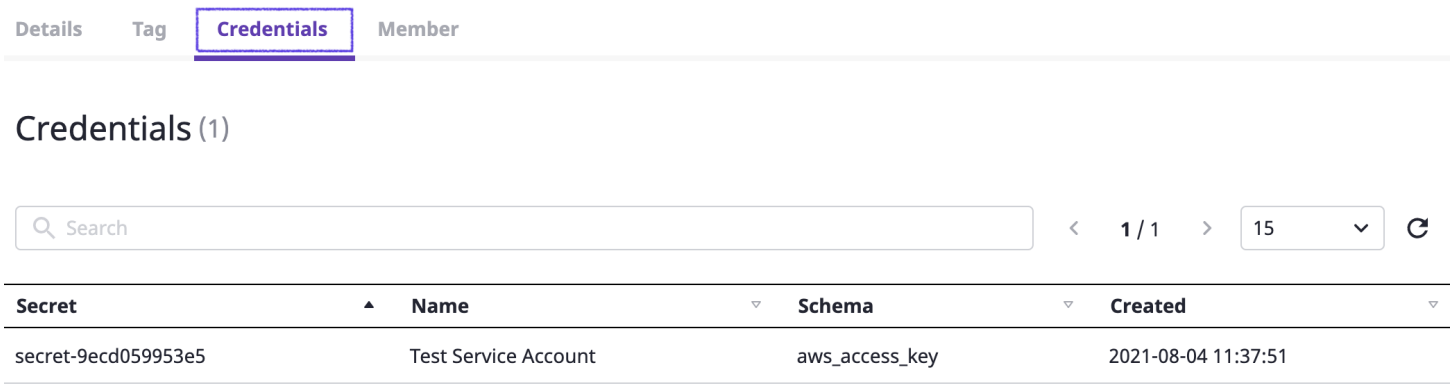


Afer clicking the **+ Add Tags** button, enter a **Key** and a **Value**, then click the **Save** button.



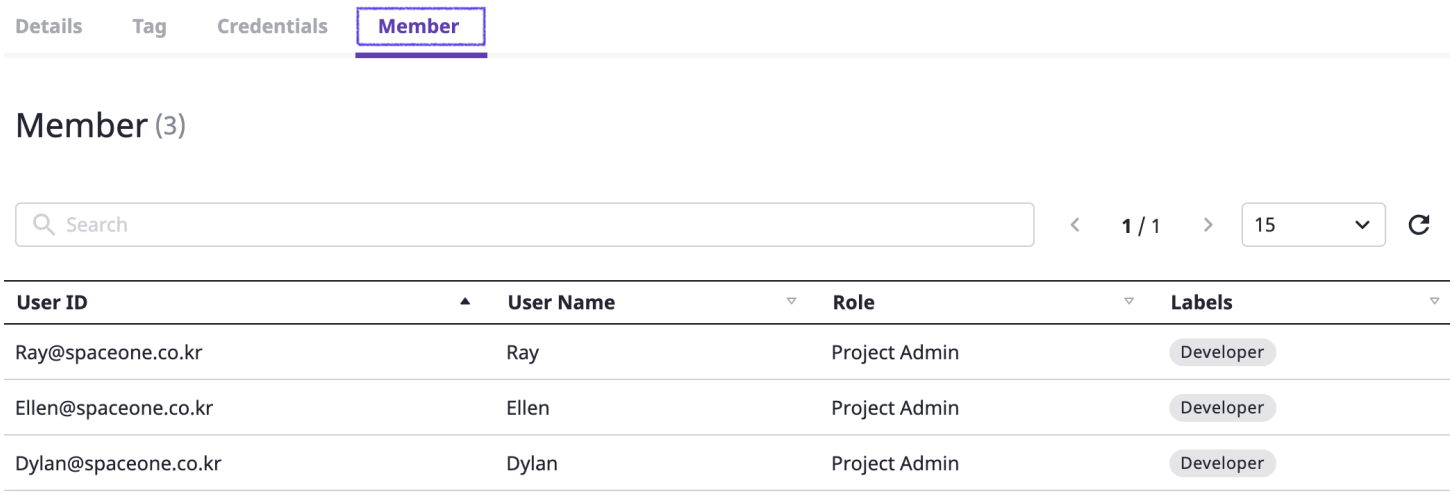
Credentials

Credentials that contain key information can be added or deleted.



Member

On the **Member** tab, you can see who is participating in the project.



4.1 - (AWS) Service Account Policy Management

Details of API Security policy to use SpaceONE plugin

Service Account Policy

Before creating a **Service Account**, you can modify your existing API policies.
This will guarantee that your resources are isolated from other non power-scheduled items. It can also prevent malfunctions caused by misconfigurations of power scheduling.
To create API for each use case, follow directions below.
General Collector

Power Scheduler Service

Personal Health Dashboard/Trusted Advisor Collector

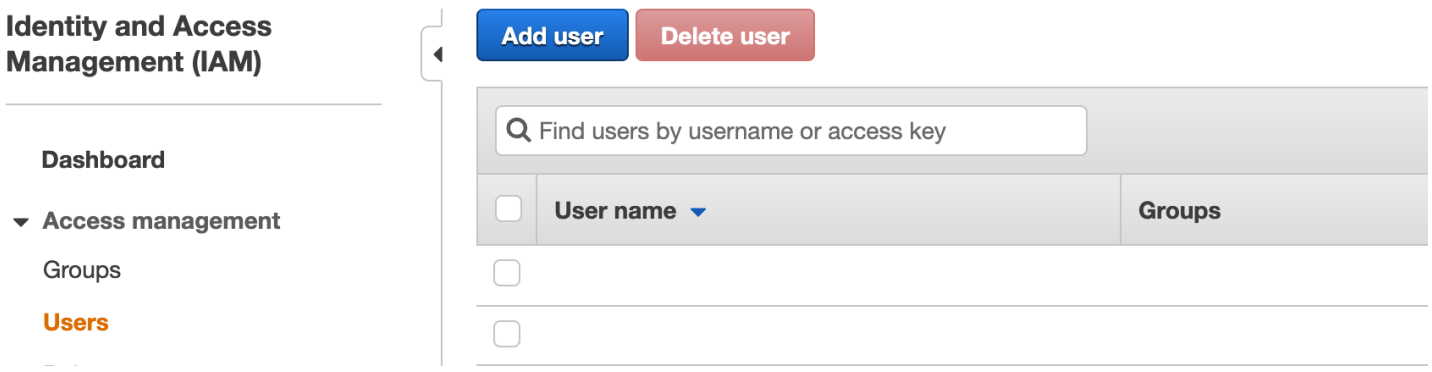
In case of internal regulations, create the policy below and attach it when creating an API user.

Overall IAM Policy Superset

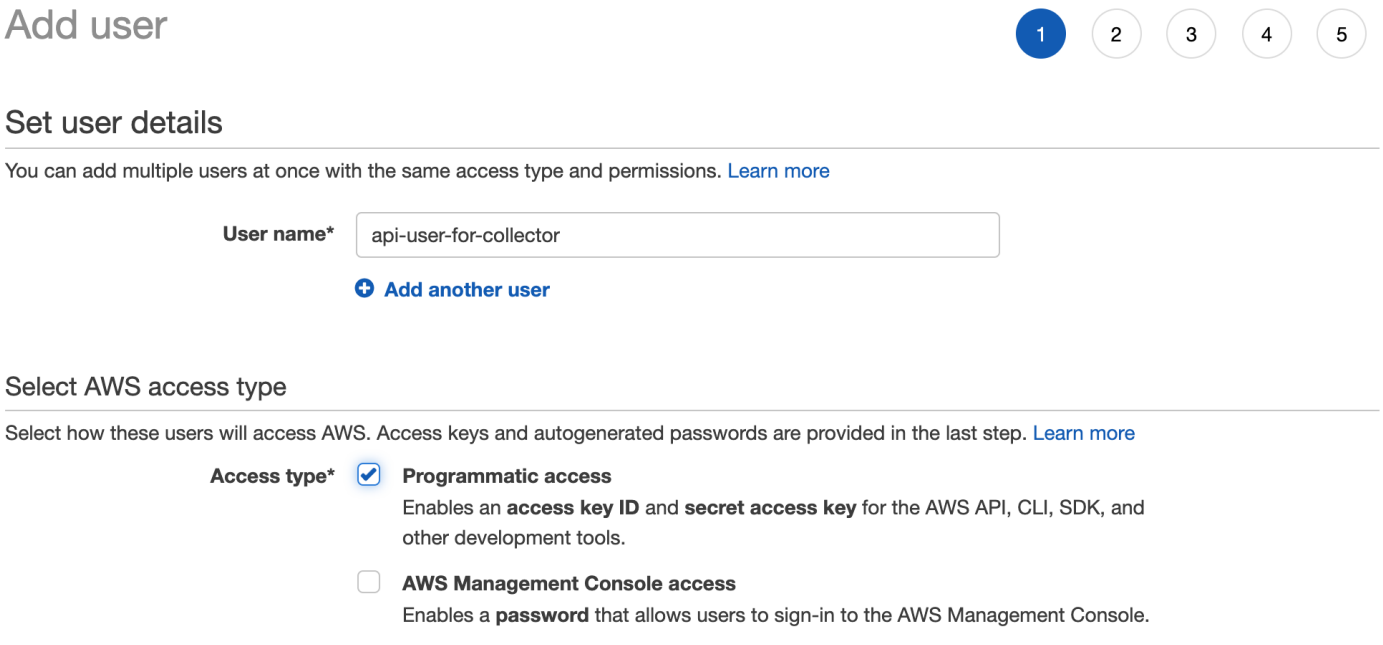
General Collector

Collectors do not require any types of permissions, except for the read permission. So we strongly recommend you to restrict permissions to **read-only access**.
Or, you can add more restrictions based on regions and resources. One of the useful examples is to restrict permissions within regions.
In order to experience more powerful functions of SpaceONE collectors, we highly recommend using managed **read-only policies**.

Step 1. Log into AWS Console > IAM
Go to IAM > Users > Add user.



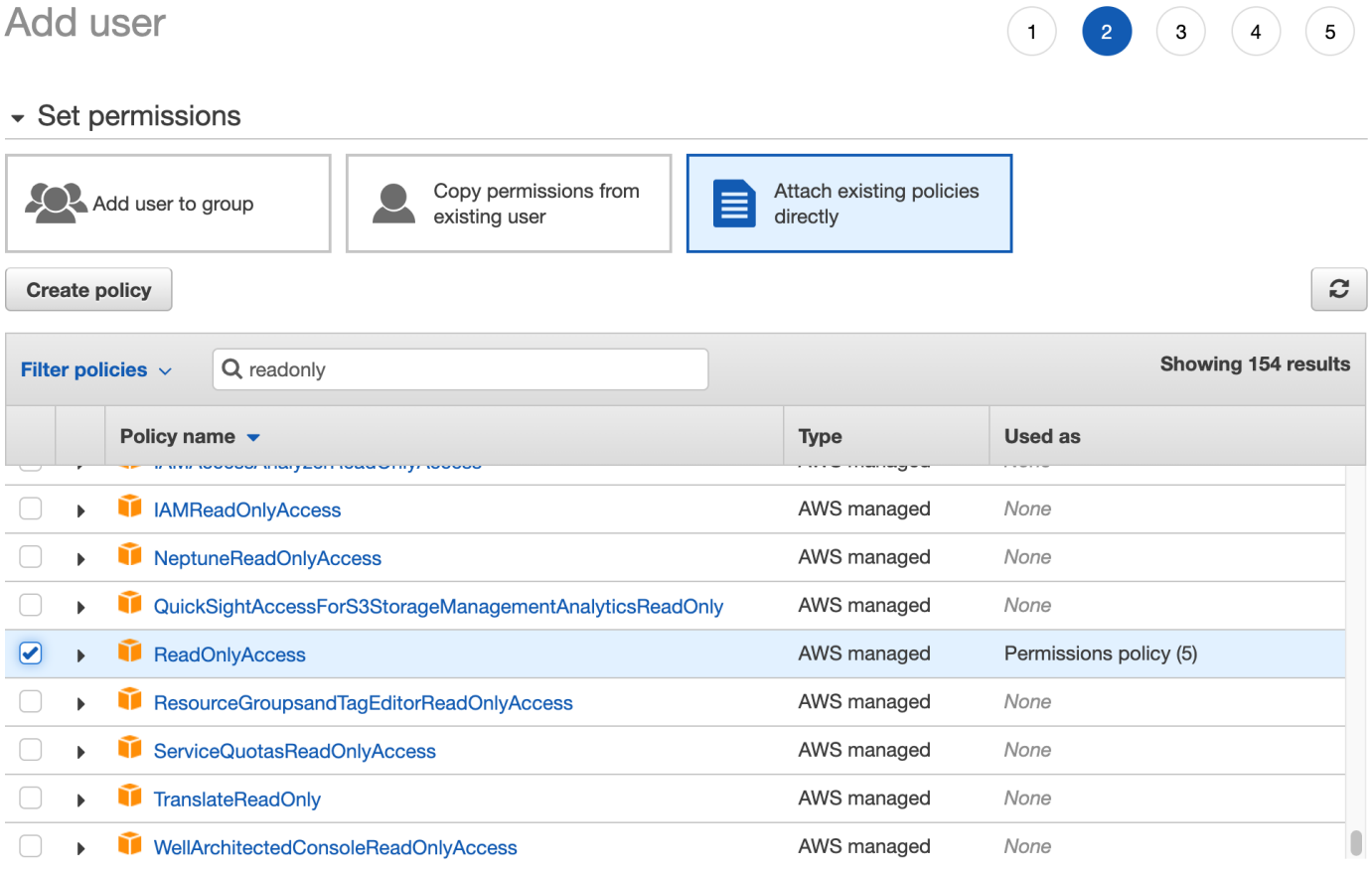
Step 2. Set User Details
Enter ***User name***, and set ***Access type*** to ***Programmatic access***.



Step 3. Set API Permission

Click ***Attach existing policies directly***, and enter "***readonly***" in the policy search bar.

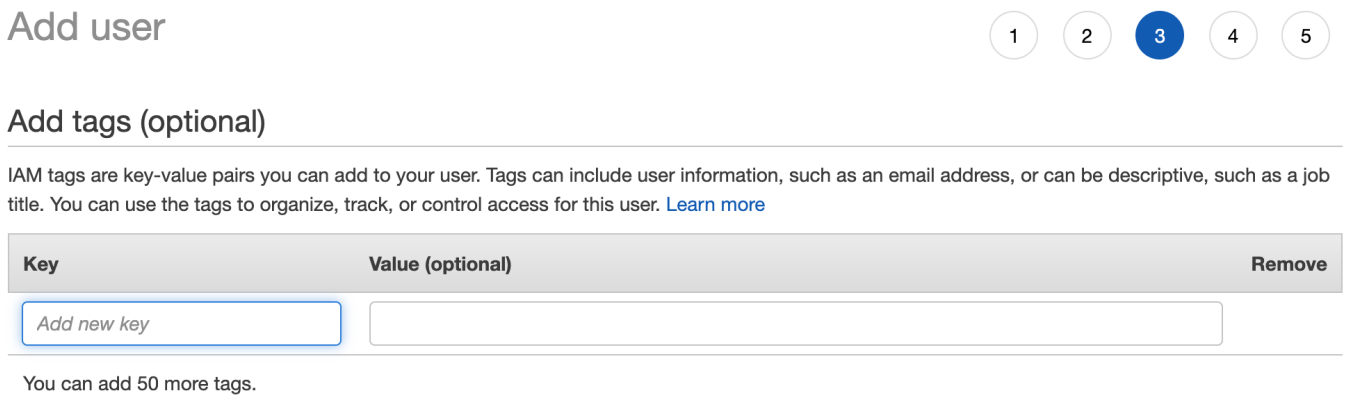
Select ***ReadOnlyAccess*** managed policy as shown below.



Step 4. Add Tags

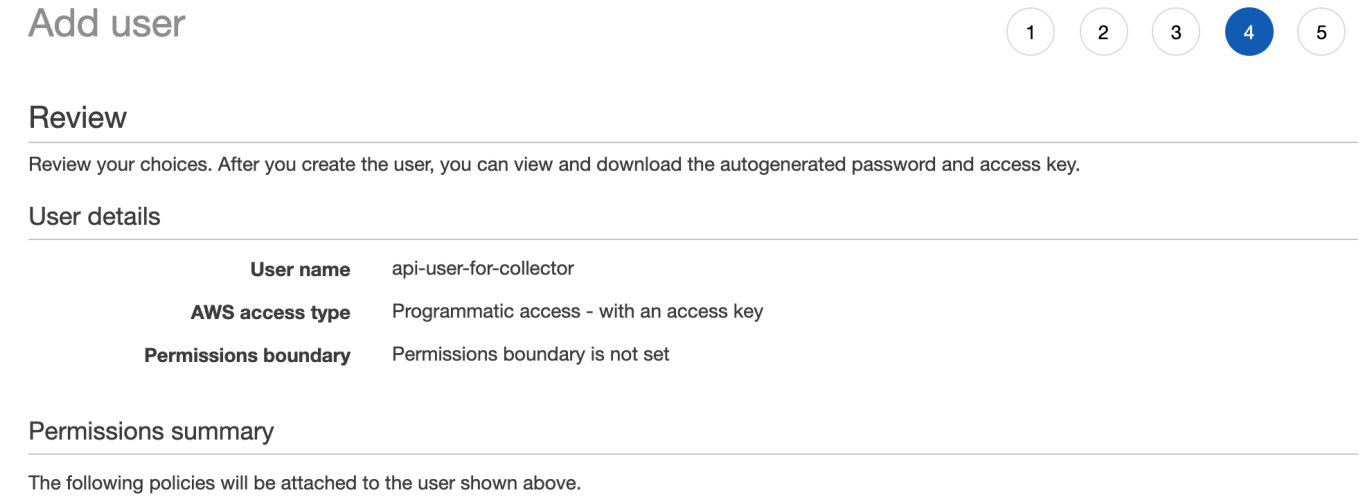
You can skip this process and move to the next step.

SpaceONE collectors are not related to tags in IAM.



Step 5. Review

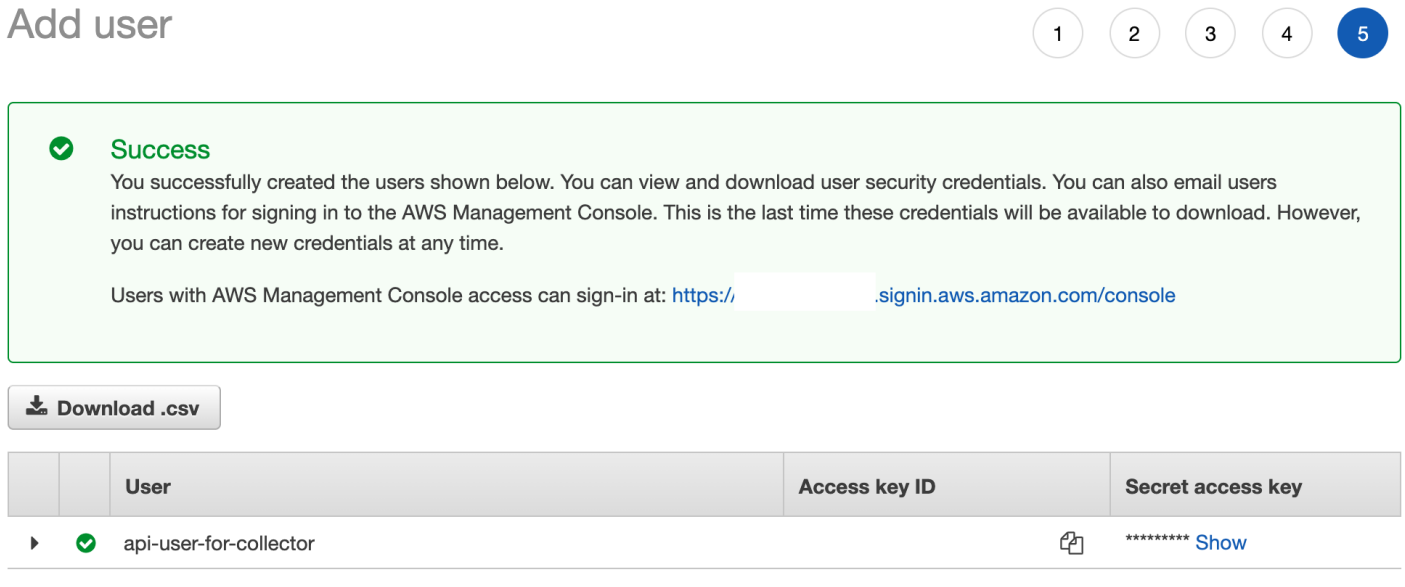
Check the details you have added. Then click ***Create users*** at the bottom of the page.



Step 6. Copy Key Pair

After the IAM key pair is created, ***make sure to copy the Access key ID/Secret access key and keep them safely***.

If you forget to copy them, there is no way to have them again (you have to start over from step 1).

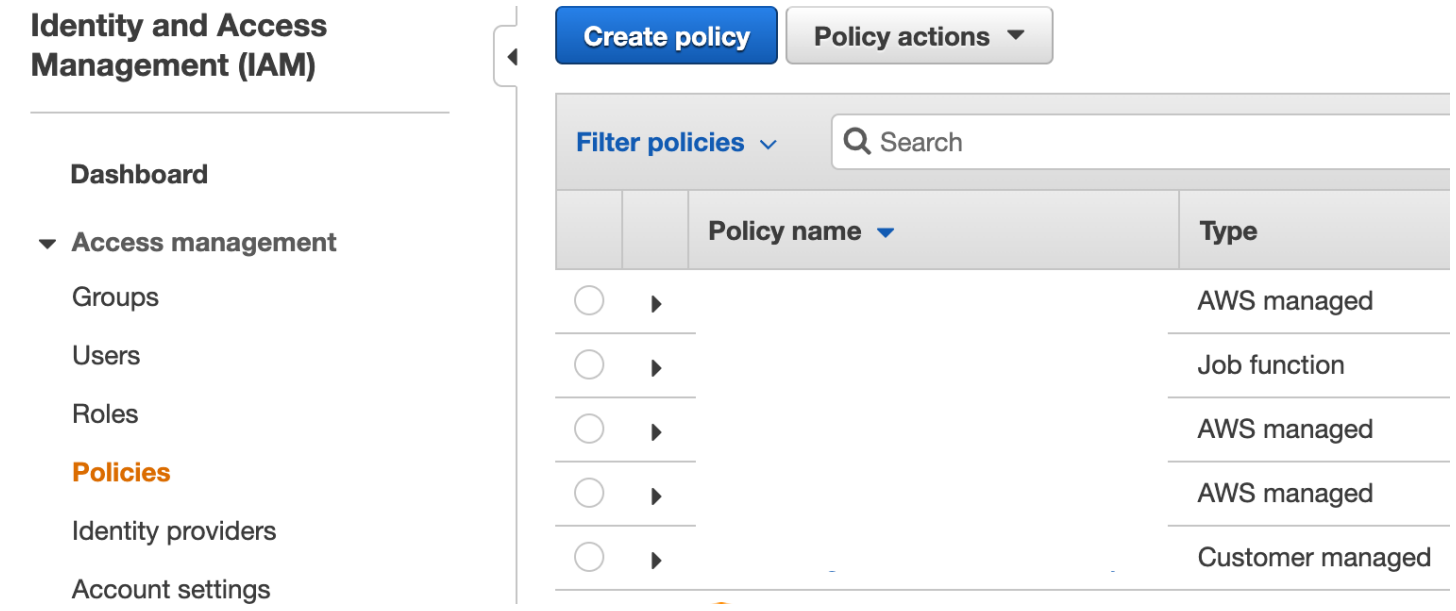


PowerScheduler

Suggested IAM policices for each cloud provider to use ***SpaceONE Power Scheduler*** service are described below.

Step 1. Create Policy

Go to IAM > Policies > Create policy.



Step 2. Attach Policy Definitions

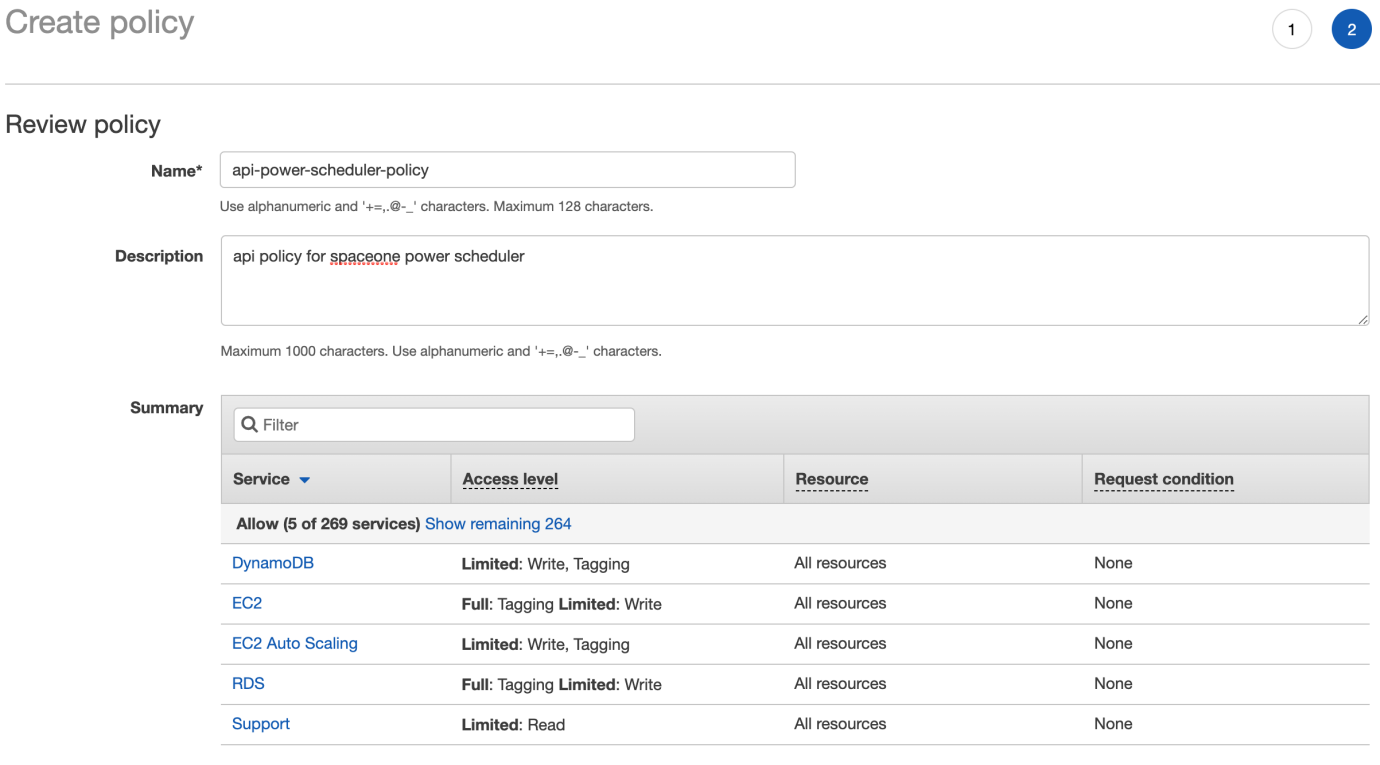
Move to the JSON tab, and attach the policy definition as shown below. Then click ***Review policy***.

AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "rds:StartDBCluster",
                "rds:StopDBCluster",
                "rds:StartDBInstance",
                "rds:StopDBInstance",
                "rds:RebootDBInstance",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "autoscaling:SetDesiredCapacity",
                "autoscaling:UpdateAutoScalingGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

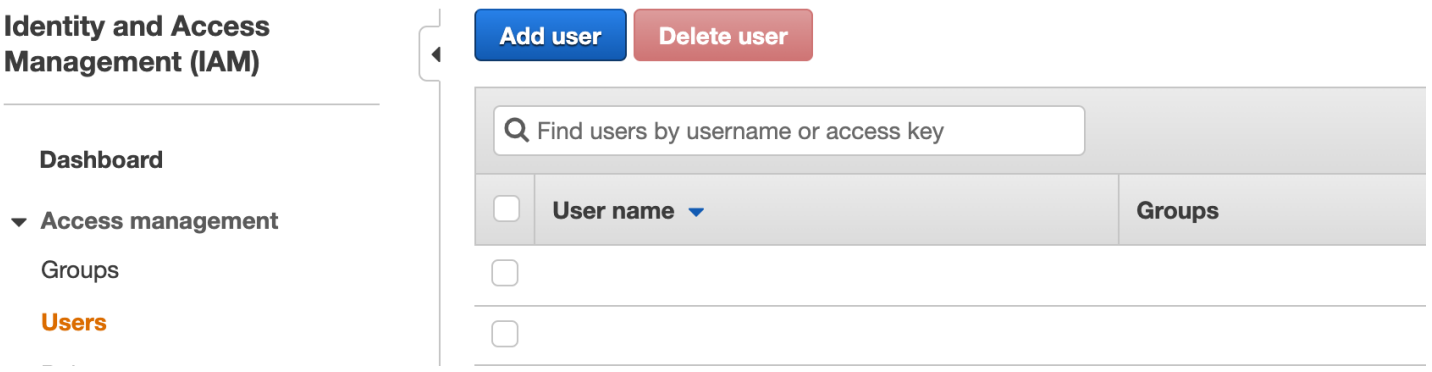
Step 3. Review Policy

Enter policy ***Name*** and ***Description***. Then click ***Create policy***.



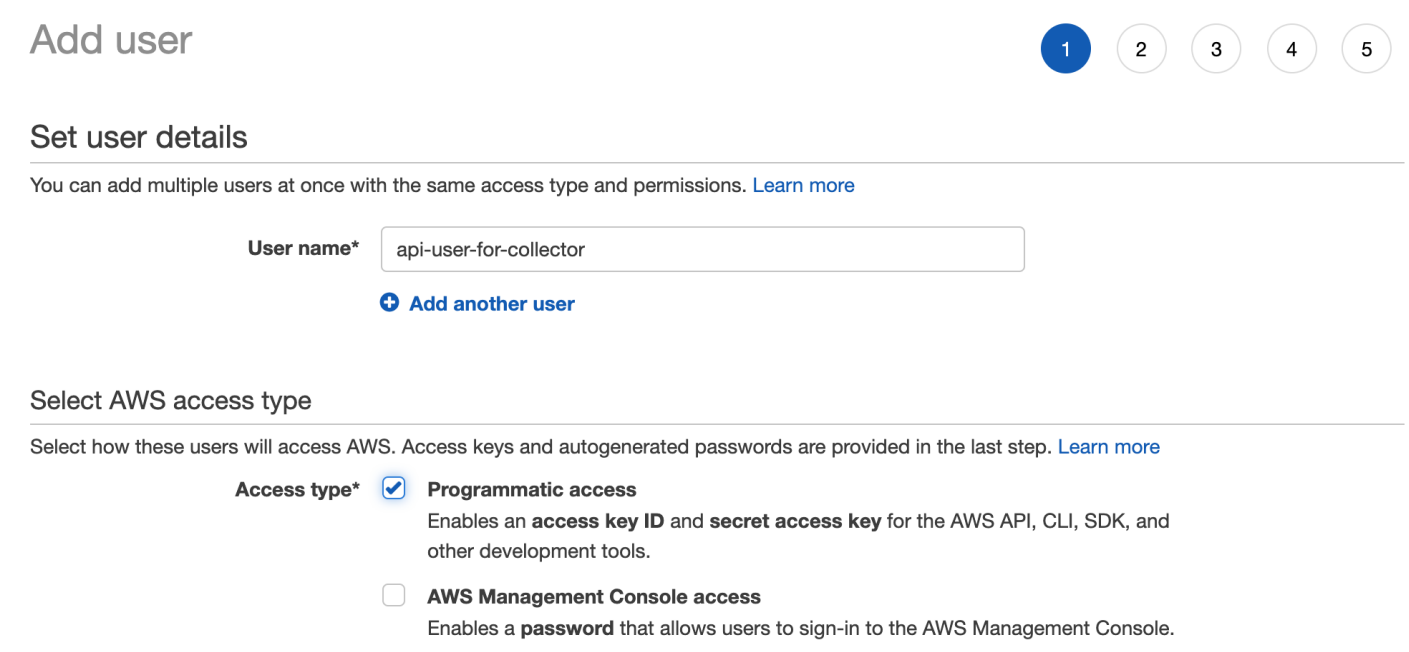
Step 4. Log into AWS Console > IAM

Go to IAM > Users > Add user.



Step 5. Set User Details

Enter ***User name***, and set ***Access type*** to ***Programmatic access***.



Step 6. Set API Permission

Add all policies below. They should be included to guarantee successful actions.

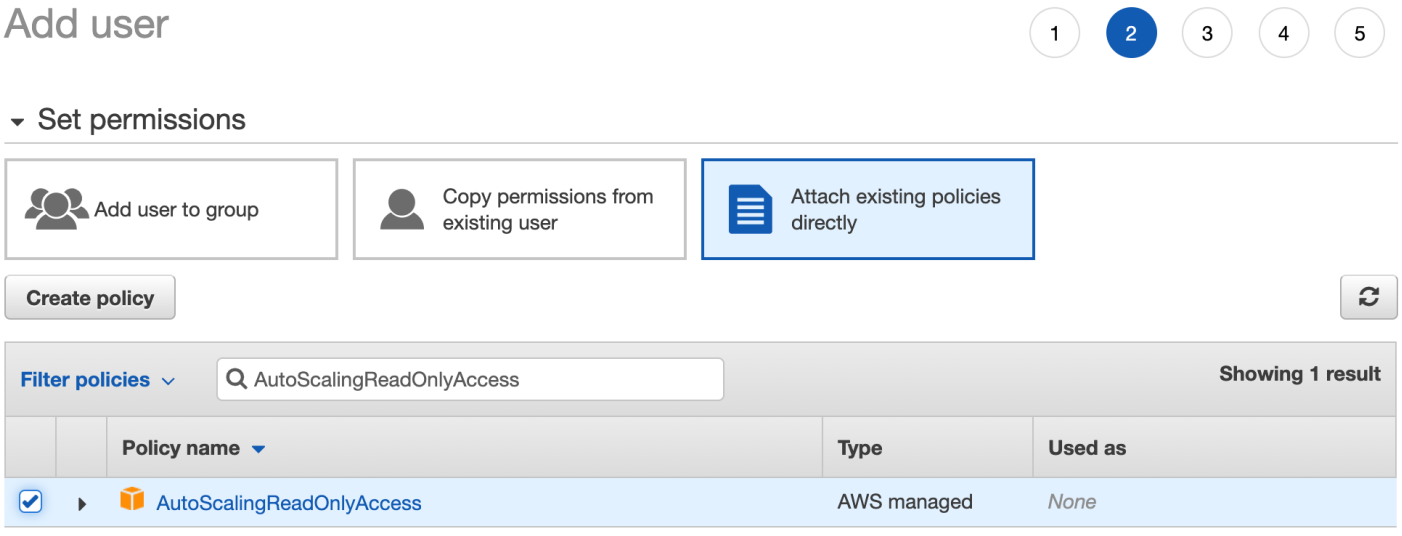
AmazonDynamoDBReadOnlyAccess

AmazonEC2ReadOnlyAccess

AmazonRDSReadOnlyAccess

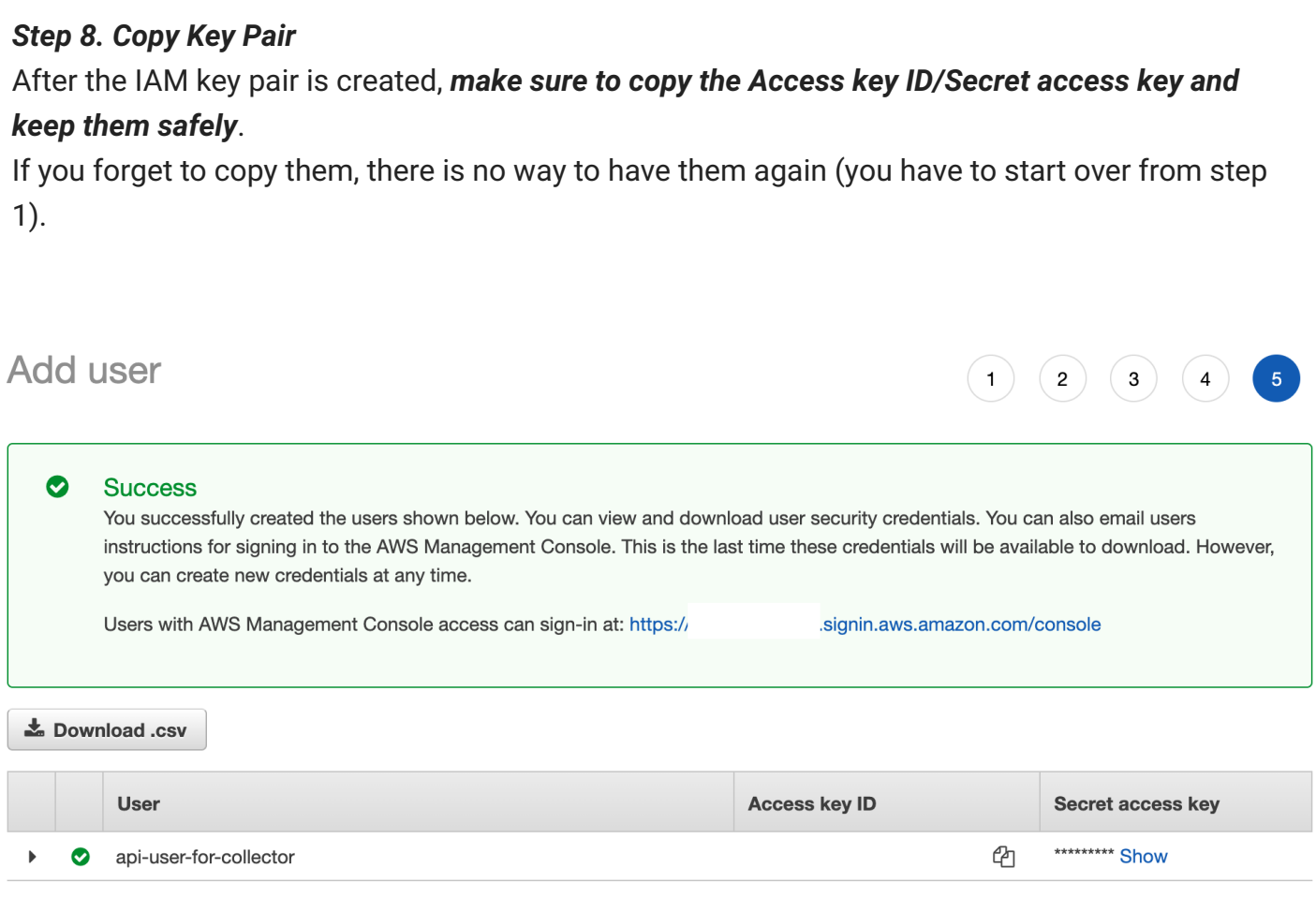
AutoScalingReadOnlyAccess

Policy created in step 3



Step 7. Review

Make sure to include all policies from Step 4. Then click ***Create user***.



Step 8. Copy Key Pair

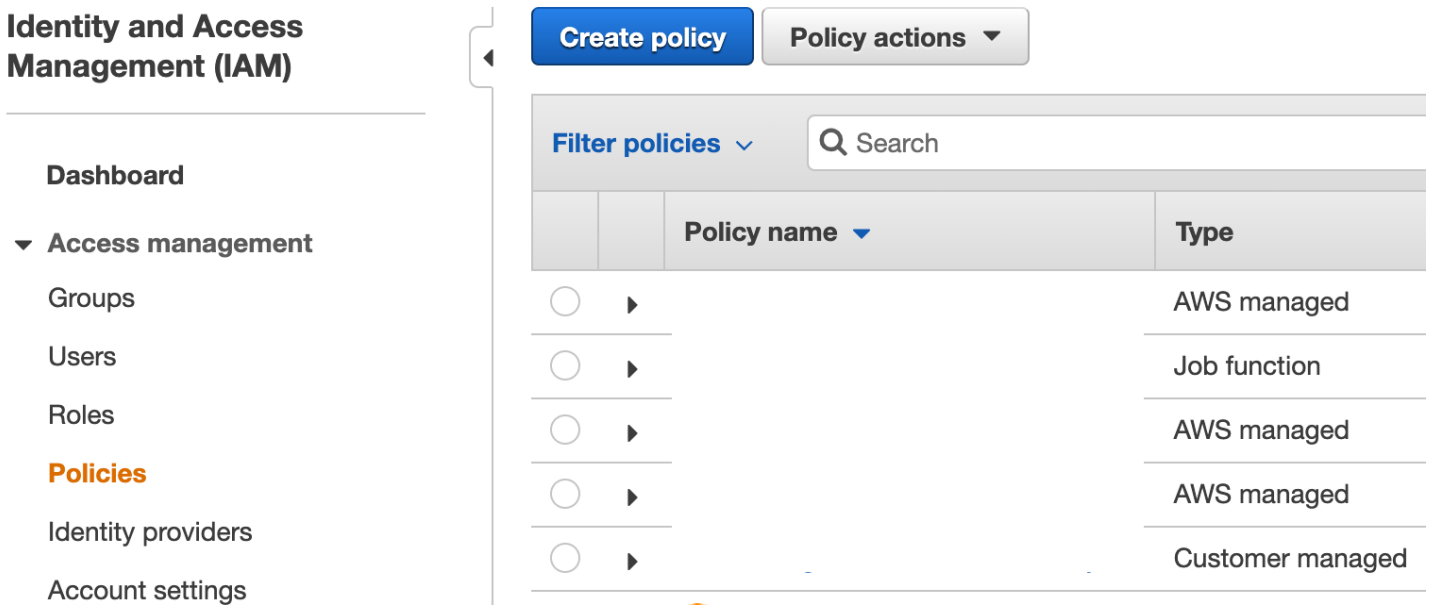
After the IAM key pair is created, ***make sure to copy the Access key ID/Secret access key and keep them safely***.

If you forget to copy them, there is no way to have them again (you have to start over from step 1).

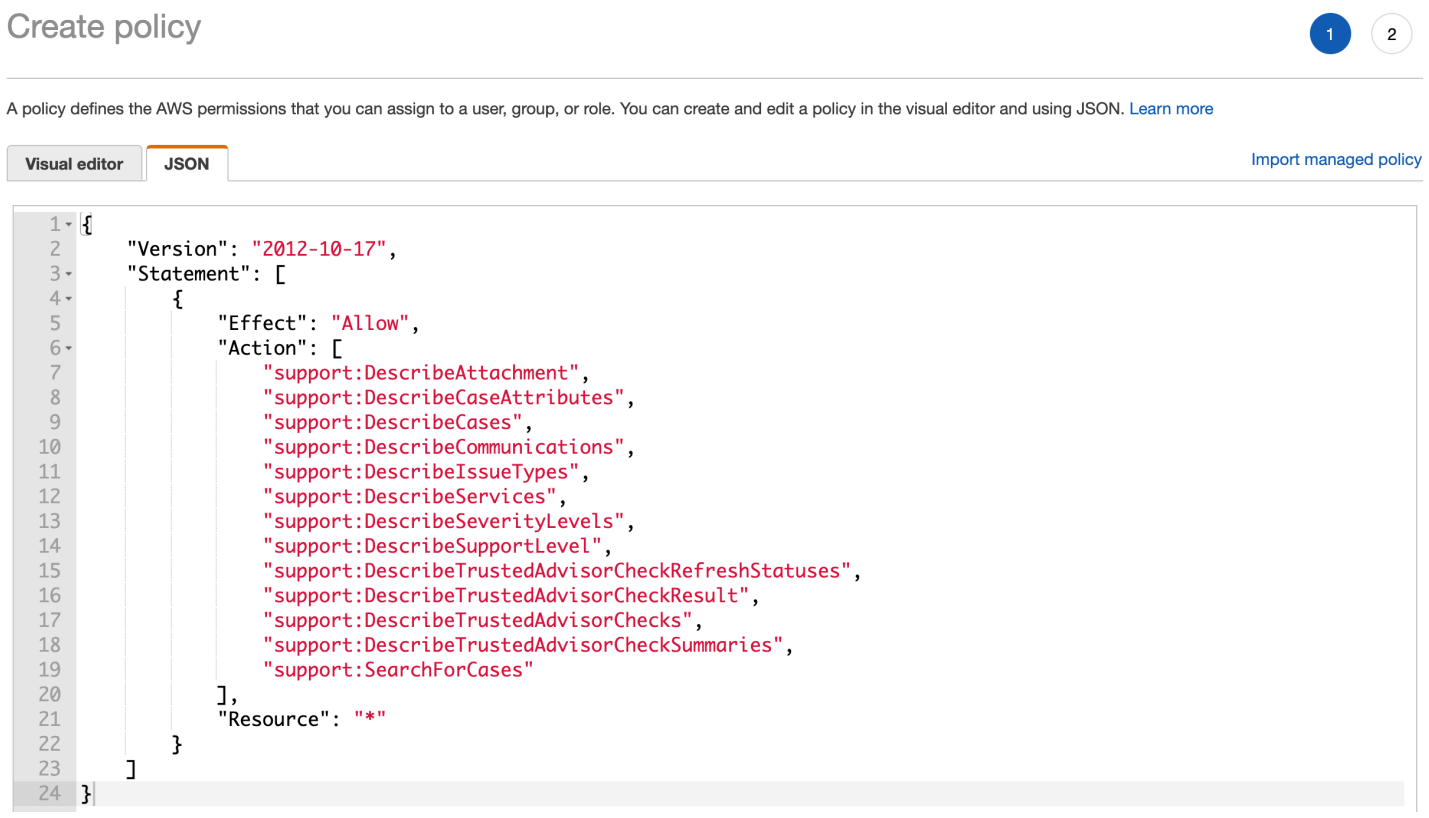
AWS Personal Health Dashboard/Trusted Advisor

To use AWS advanced collectors such as AWS ***Personal Health Dashboard/Trusted Advisor***, the user account support level should be above ***business*** and additional IAM policies need to be attached.

Step 1. Create Policy
Go to IAM > Policies > Create policy.



Step 2. Attach Policy Definitions
Move to the JSON tab, and attach the policy definition as shown below. Then click ***Review policy***.

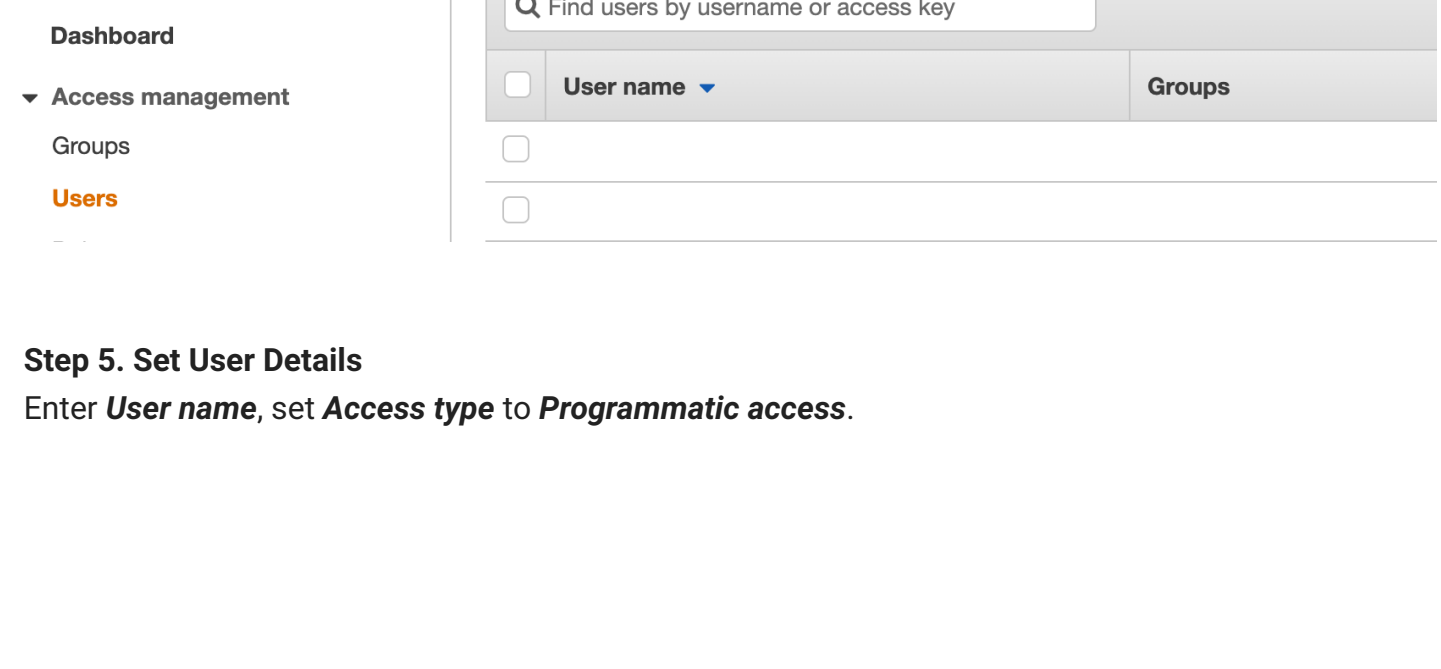



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeAttachment",
                "support:DescribeCaseAttributes",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeIssueTypes",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
```

```
                "support:DescribeSupportLevel",
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:SearchForCases"
            ],
            "Resource": "*"
        }
    ]
}
```

Step 3. Review Policy

Enter policy ***Name*** and ***Description***. Then click ***Create policy***.

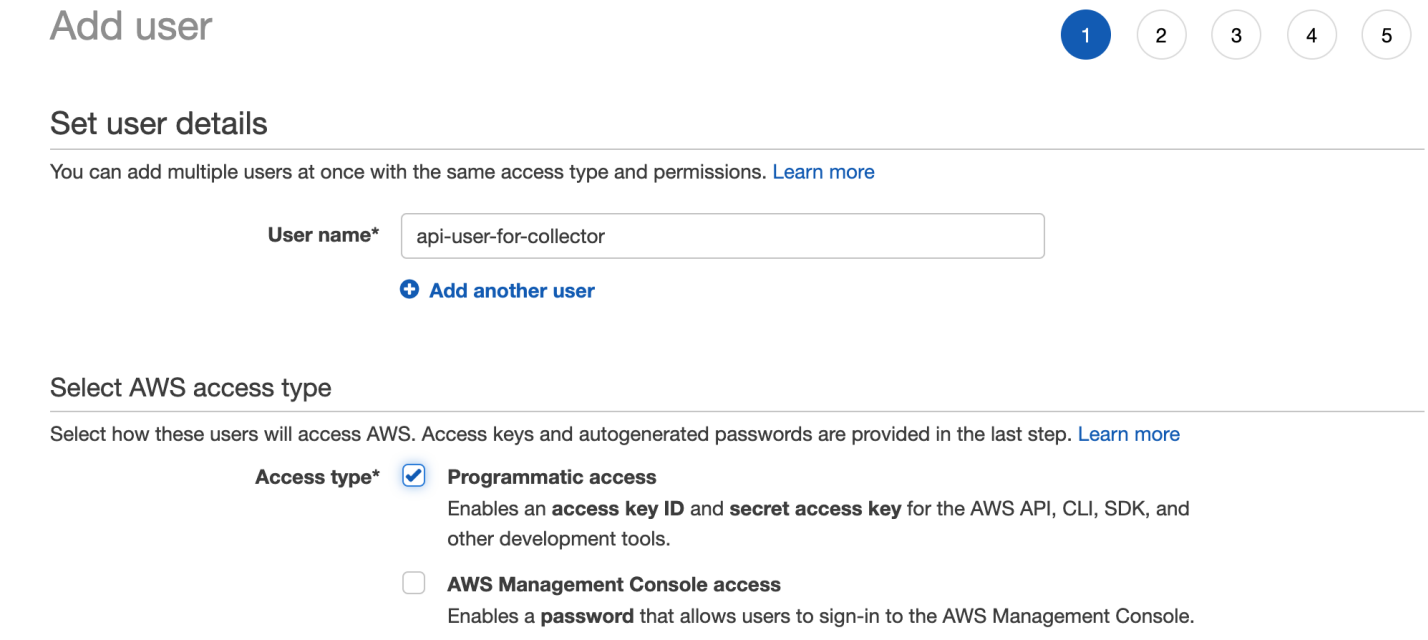


Step 4. Log into AWS Console > IAM

Go to IAM > Users > Add user.

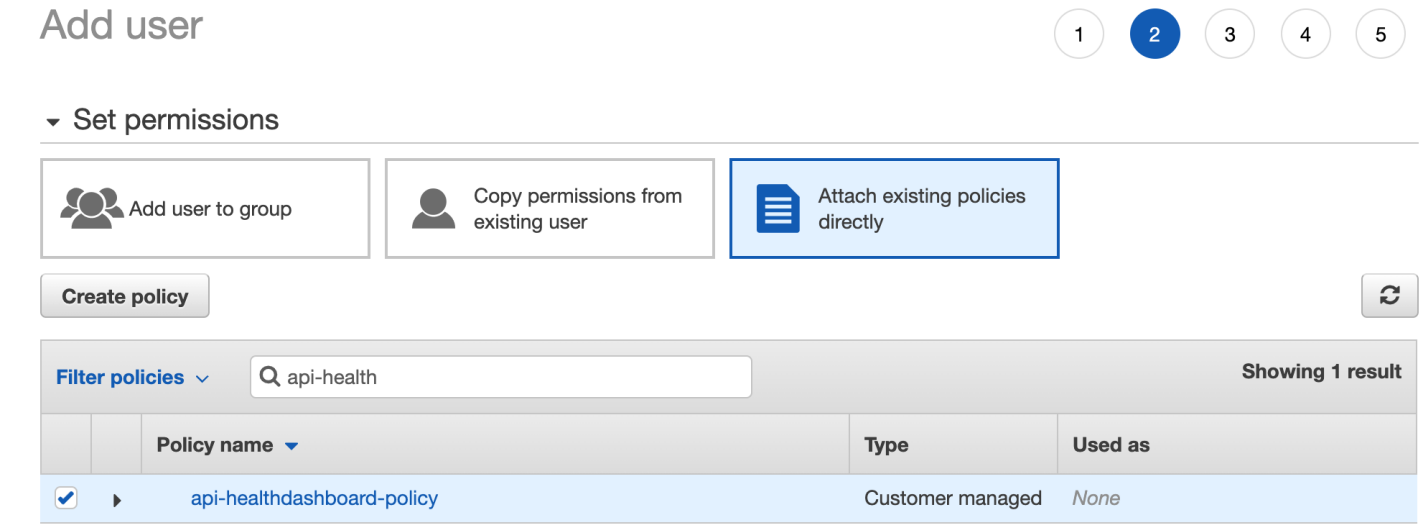
Step 5. Set User Details

Enter ***User name***, set ***Access type*** to ***Programmatic access***.



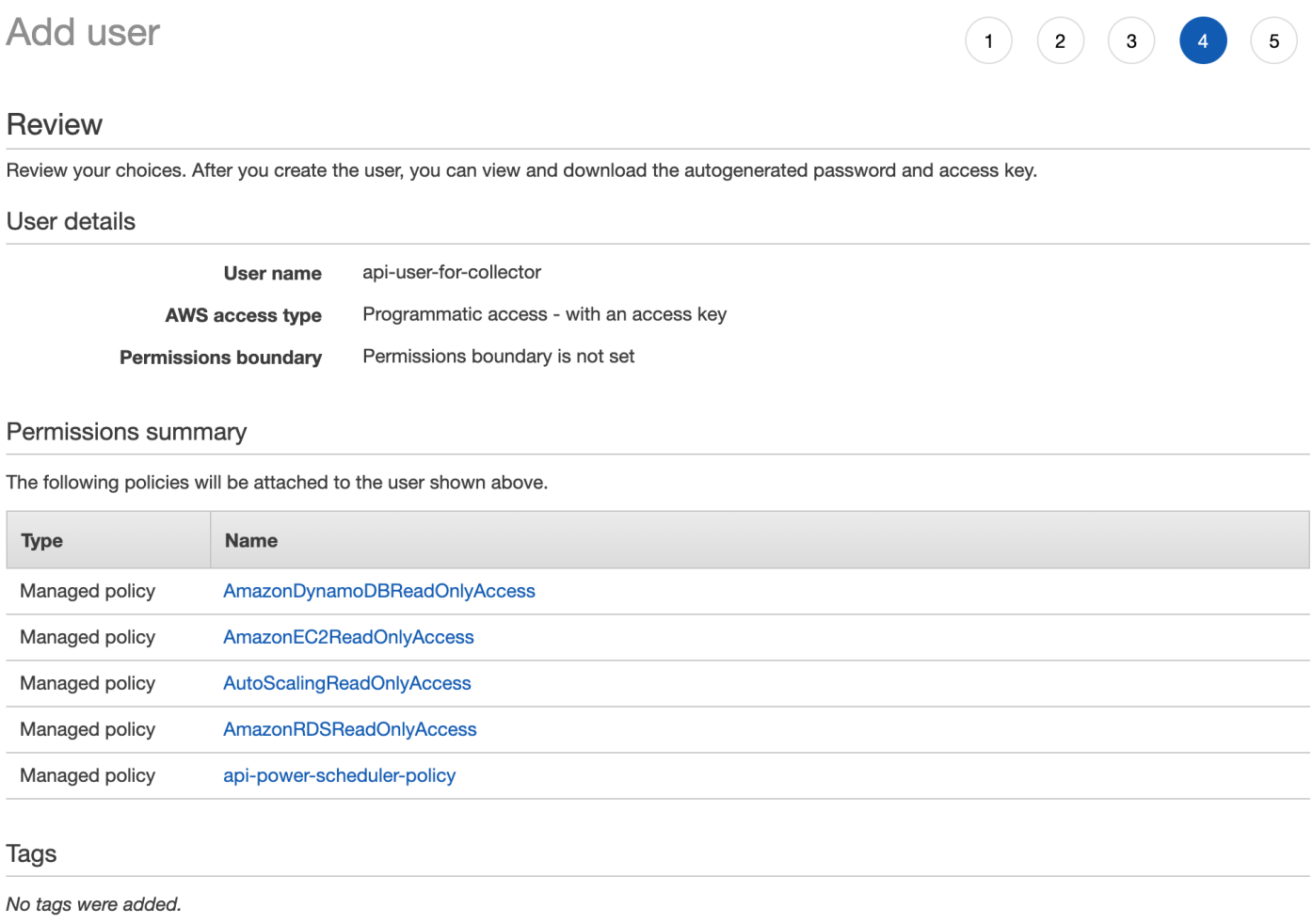
Step 6. Set API Permission

Add all policies below. They should be included to guarantee successful actions.



Step 7. Review

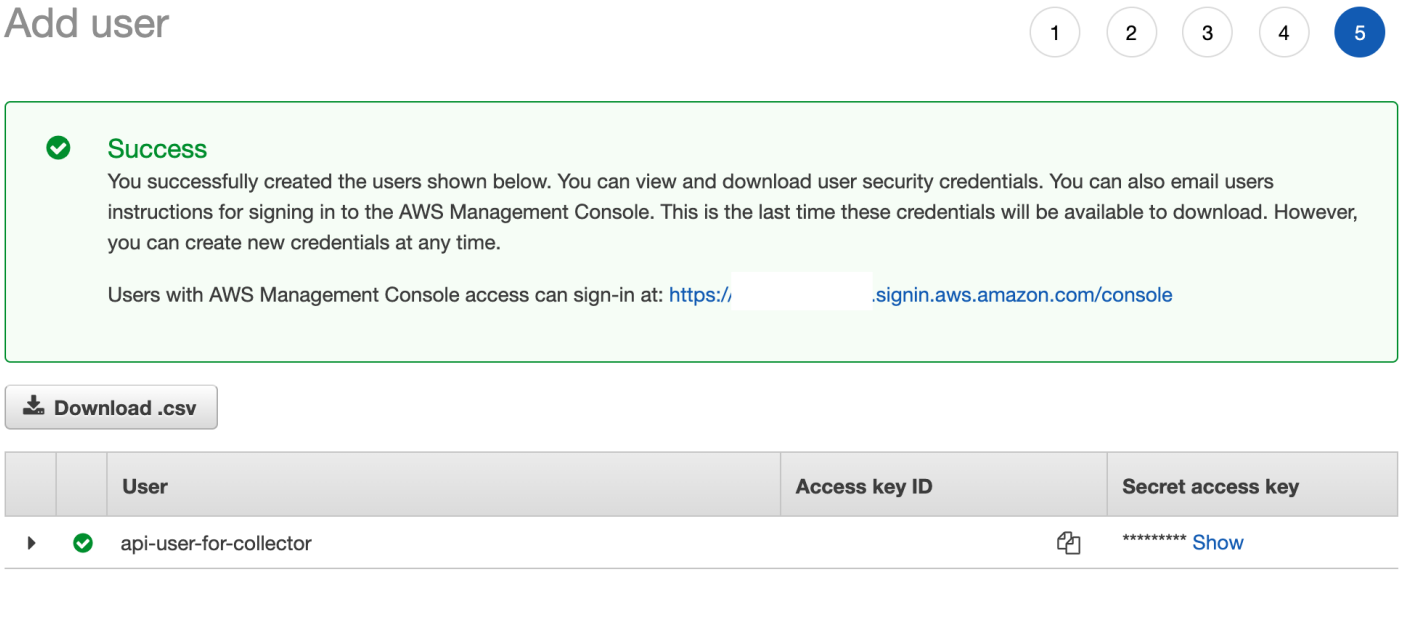
Make sure to include all policies from Step 4. Then click ***Create user***.



Step 8. Copy Key Pair

After the IAM key pair is created, ***make sure to copy the Access key ID/Secret access key and keep them safely***.

If you forget to copy them, there is no way to have them again (you have to start over from step 1).



Overall IAM Policy Superset

If you want to use a managed policy, you can refer to the policy below.
Region Code in resource parameters needs to be changed. ***AWS Region Code*** or ******* character is available.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GeneralReadOnlyPolicyForCollectors",
            "Effect": "Allow",
            "Resource": "arn:aws:*:{aws region code}:*:*"
            "Action": [
                "acm:Describe*",
                "acm:Get*",
                "acm:List*",
                "acm-pca:Describe*",
                "acm-pca:Get*",
                "acm-pca:List*",
                "apigateway:GET",
                "autoscaling:Describe*",
                "autoscaling-plans:Describe*",
                "autoscaling-plans:GetScalingPlanResourceForecastData",
                "athena:List*",
                "athena:Batch*",
                "athena:Get*",
                "cassandra:Select",
                "cloudfront:Get*",
                "cloudfront:List*",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*",
                "connect:List*",
                "connect:Describe*",
                "connect:GetFederationToken",
                "directconnect:Describe*",
                "dynamodb:BatchGet*",
                "dynamodb:Describe*",
                "dynamodb:Get*",
                "dynamodb:List*",
                "dynamodb:Query",
```

```
                "dynamodb:Scan",
                "ec2:Describe*",
                "ec2:Get*",
                "ec2:SearchTransitGatewayRoutes",
                "ec2messages:Get*",
                "ecr:BatchCheck*",
                "ecr:BatchGet*",
                "ecr:Describe*",
                "ecr:Get*",
                "ecr:List*",
                "ecs:Describe*",
                "ecs:List*",
                "eks:Describe*",
                "eks:List*",
                "elasticache:Describe*",
                "elasticache:List*",
                "elasticfilesystem:Describe*",
                "elasticloadbalancing:Describe*",
                "es:Describe*",
                "es:List*",
                "es:Get*",
                "es:ESHttpGet",
                "es:ESHttpHead",
                "health:Describe*",
                "iam:Generate*",
                "iam:Get*",
                "iam:List*",
                "iam:Simulate*",
                "kafka:Describe*",
                "kafka:List*",
                "kafka:Get*",
                "lambda:List*",
                "lambda:Get*",
                "rds:Describe*",
                "rds:List*",
                "rds:Download*",
                "redshift:Describe*",
                "redshift:GetReservedNodeExchangeOfferings",
                "redshift:View*",
                "route53:Get*",
                "route53:List*",
                "route53:Test*",
                "route53domains:Check*",
                "route53domains:Get*",
                "route53domains:List*",
                "route53domains:View*",
                "route53resolver:Get*",
                "route53resolver:List*",
                "s3:Get*",
                "s3:List*",
                "secretsmanager:List*",
                "secretsmanager:Describe*",
                "secretsmanager:GetResourcePolicy",
                "sns:Get*",
                "sns:List*",
                "sns:Check*",
                "sqs:Get*",
                "sqs:List*",
                "sqs:Receive*",
                "storagegateway:Describe*",
                "storagegateway:List*",
                "tag:Get*",
                "trustedadvisor:Describe*",
                "workspaces:Describe*"
            ]
        },
        {
            "Sid": "PowerSchedulerController",
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ec2:{aws region code}:*:instance/*",
                "arn:aws:rds:{aws region code}:*:db:*",
```

```
                "arn:aws:rds:{aws region code}:*:cluster:*",
                "arn:aws:autoscaling:{aws region code}:*:autoScalingGroup:*"
            ],
            "Action": [
                "rds:StartDBCluster",
                "rds:StopDBCluster",
                "rds:StartDBInstance",
                "rds:StopDBInstance",
                "rds:RebootDBInstance",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "autoscaling:SetDesiredCapacity",
                "autoscaling:UpdateAutoScalingGroup"
            ]
        },
        {
            "Sid": "PHDandTACollector",
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "support:DescribeAttachment",
                "support:DescribeCaseAttributes",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeIssueTypes",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:DescribeSupportLevel",
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:SearchForCases"
            ]
        }
    ]
}
```

4.2 - (Google Cloud) Service Account Policy Management

Details of API Security policy to use SpaceONE plugin

Service Account Policy

SpaceONE highly recommends, setting appropriate permissions to **Service Accounts** for each purpose.
General Collector
(Retrieve Google Cloud Resources into **SpaceONE** Inventory)
Google Compute VM Collector - **google-cloud compute**

Google Cloud Service Collector - **google-cloud-services**

Google power state Collector - **google-cloud-power-state**

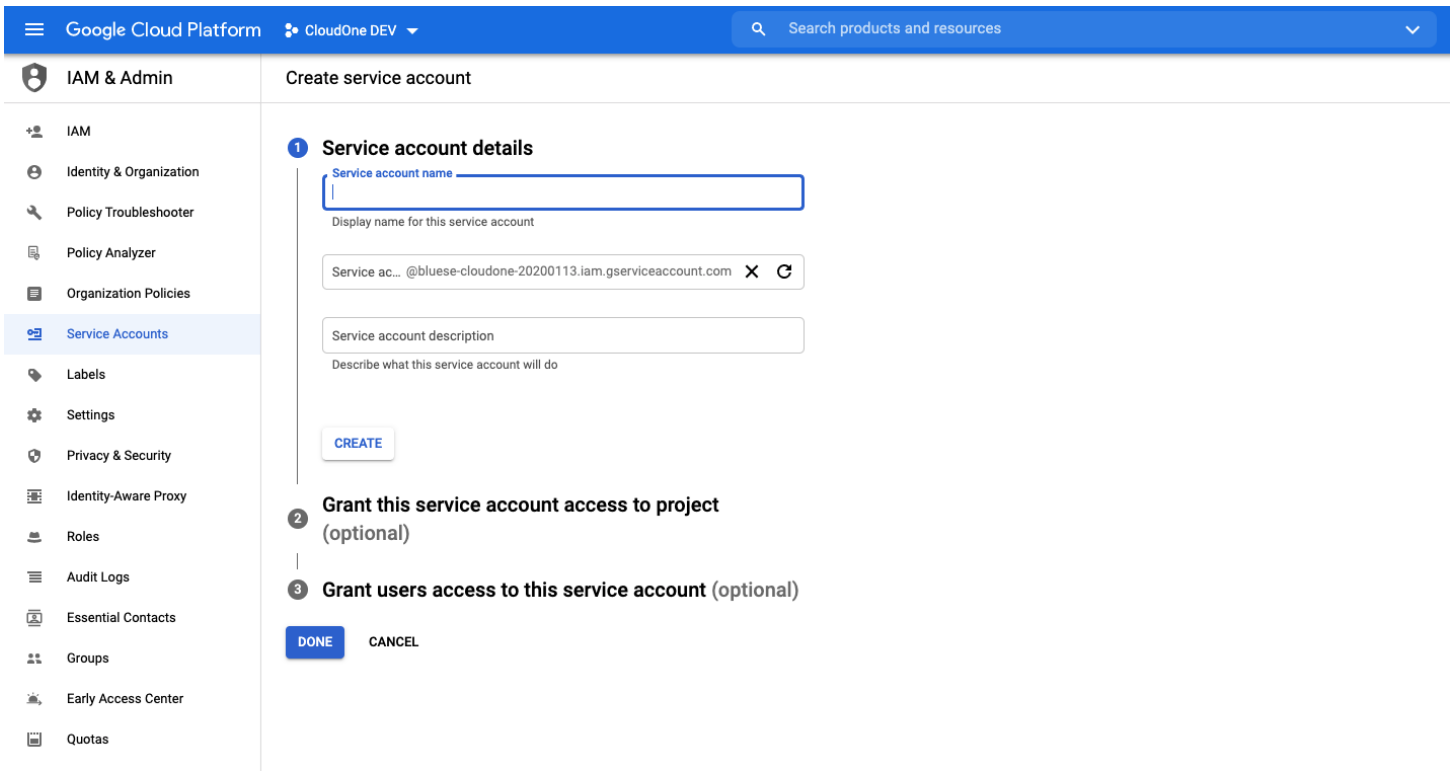
Power-scheduler
(Post Action to Google Cloud resources to turn on/off for following resources : Compute VMs, Instance group, Cloud SQL) with Power-scheduler > Scheduler Management
Google Cloud power Controller

STEP 1. Please, Set Service Accounts to Create API for each Use Case
General Collector
Special Roles
Power Controller
STEP 2. Register Your Service Account into SpaceONE
Register Service Account into SpaceONE

General Collector

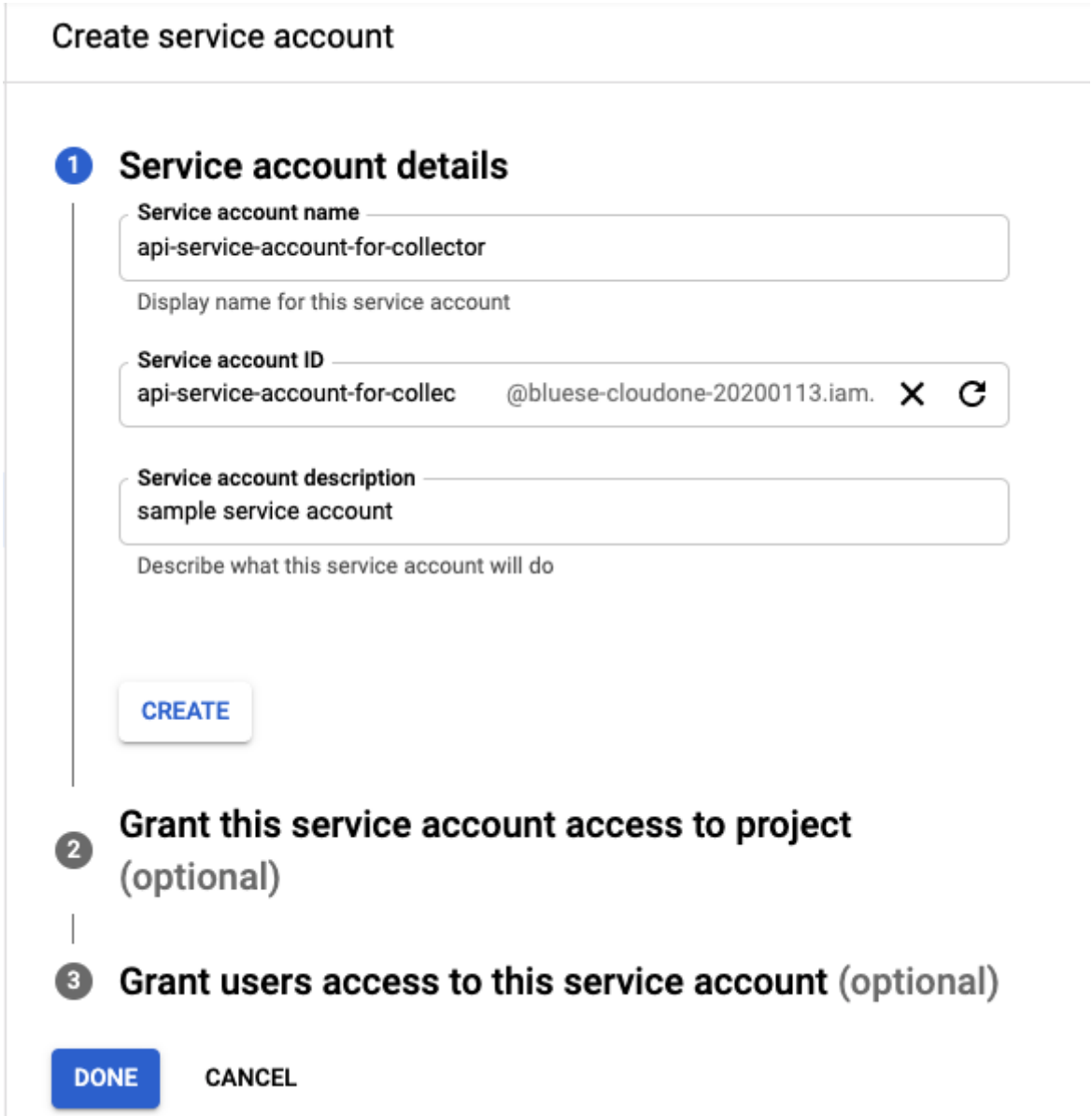
Collectors require appropriate authorities to collect cloud resources. We strongly recommend limiting the collector's service account permission to `read only access`. Or you can add more restrictions per resources or actions. One useful example is to restrict its rights within region.

STEP 1. Sign in to Google Cloud Console > IAM
Go to **IAM > Service Account** and click `+ CREATE SERVICE ACCOUNT`.



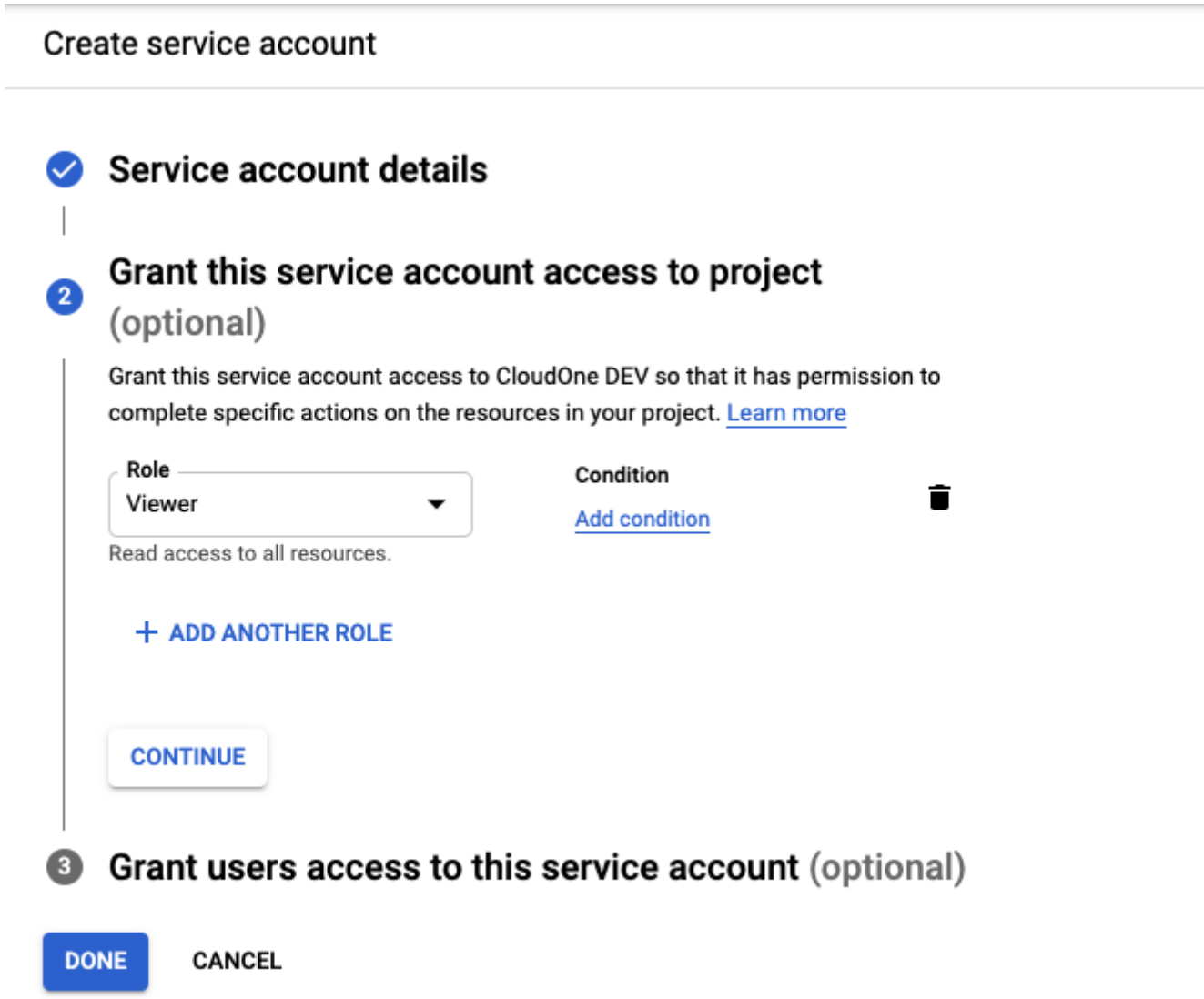
STEP 2. Set Service account details

Enter ***Service account name***, and ***Service account description***.



STEP 3: Grant Service account to Project

Set Permission to Viewer (Role): Read Access to All Resources, and click **`CONTINUE`** .

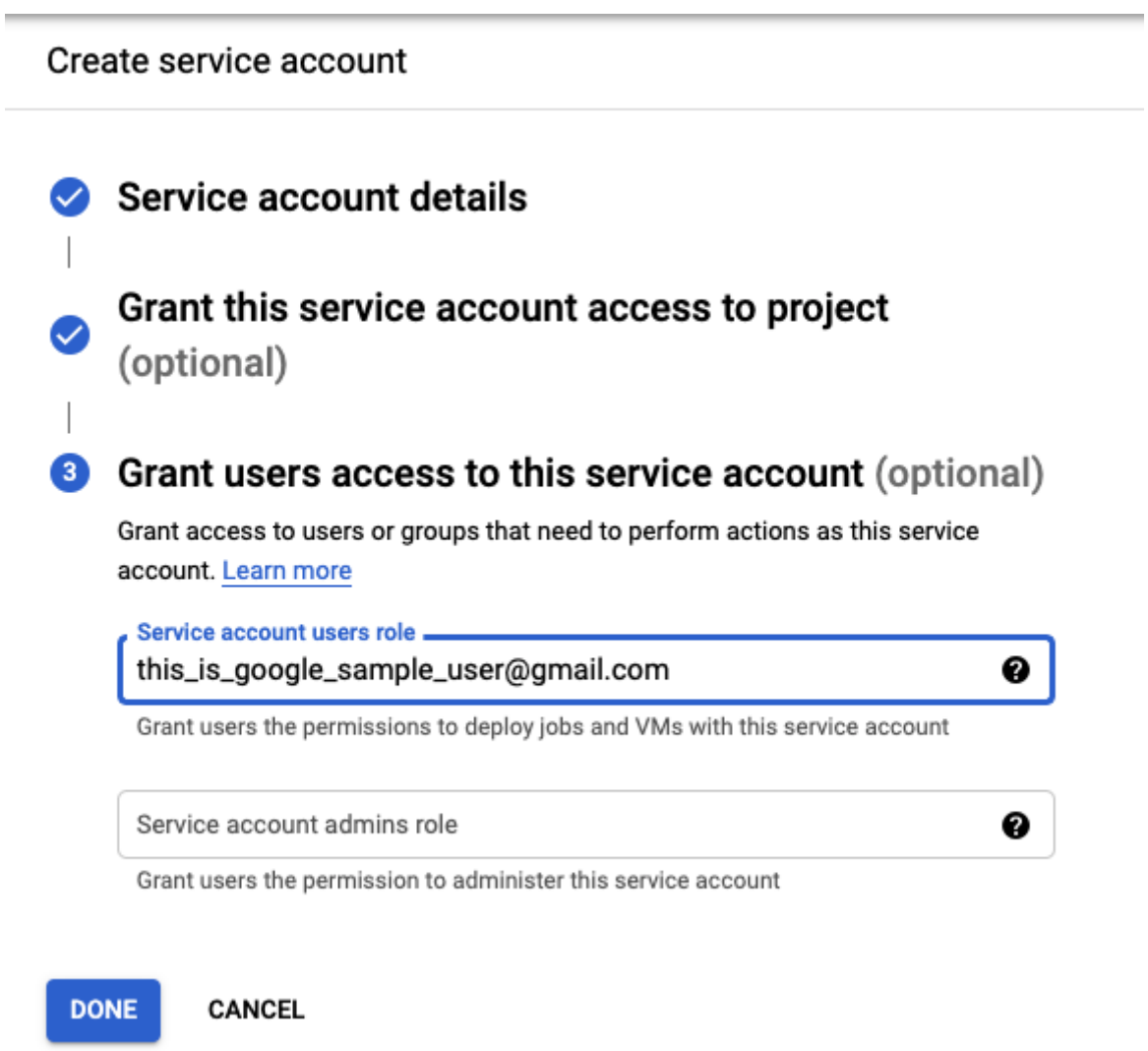


STEP 4: Grant Users access to this service Account (Optional)

You can skip this process and move to the next.

Set *Service account users role* and *Service account admin role*.

Click **`DONE`** when everything is finished.

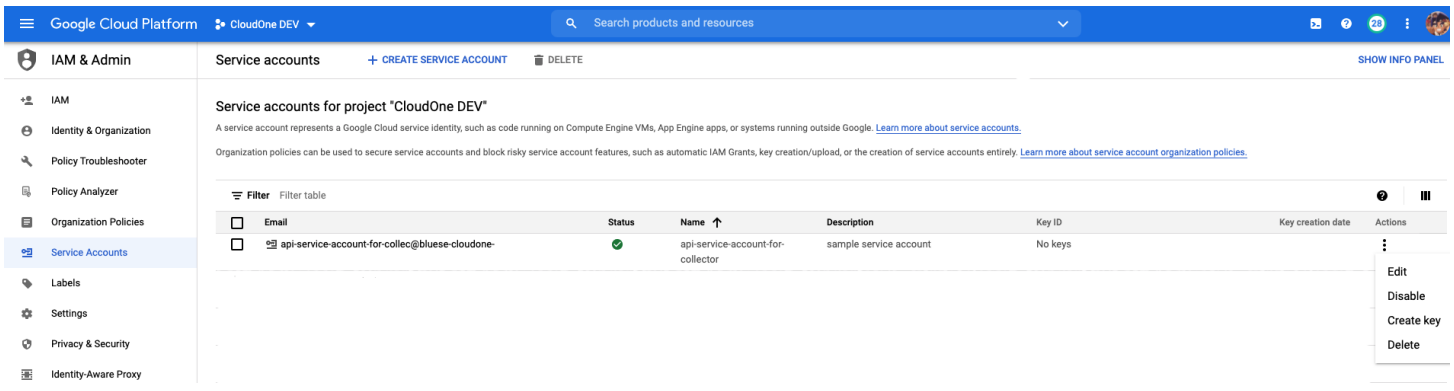


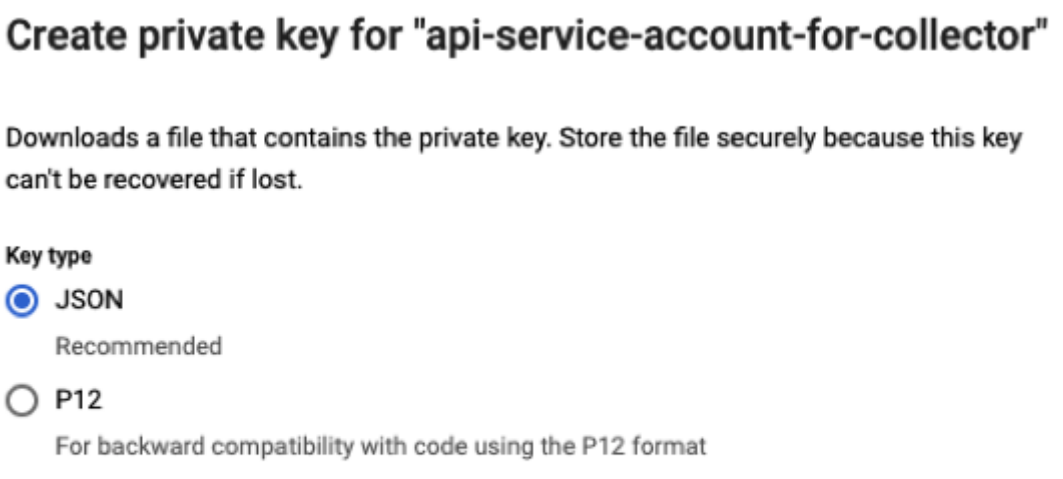
STEP 5: CREATE KEY

Find the Service account that you created in the previous step.

Click the Action button and Select **`Create Key`** .

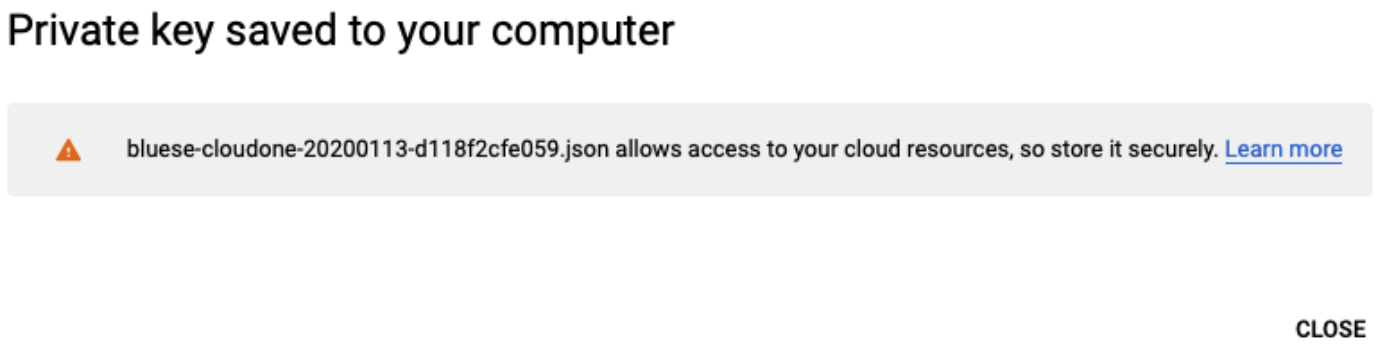
Select a Key Type and click the **`CREATE`** button. We recommend type JSON.

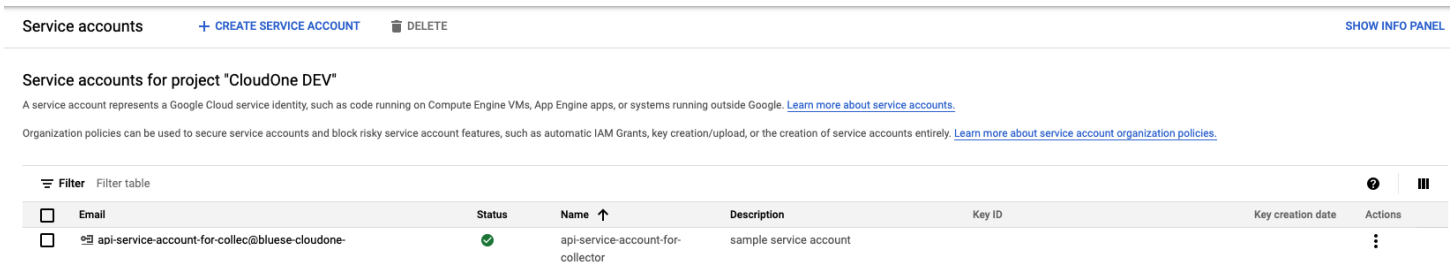




STEP 6: Review

After step 5, you'll be able to see the Key ID on the list and also its service account JSON on your local.





Special Roles

SpaceONE's ***General Collector*** requires permission to access the following services:

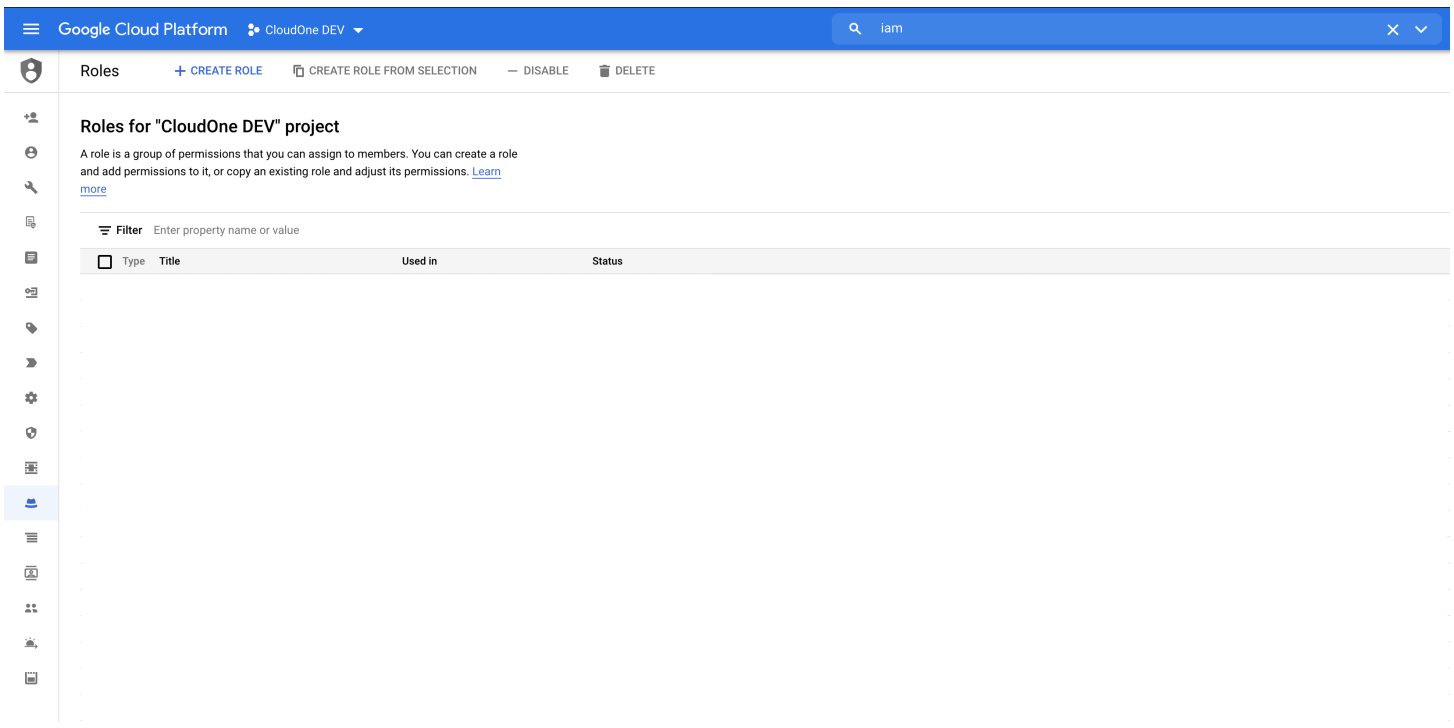
> **Google Cloud APIs are categorized as its types, and therefore it is essential to set up a Special Role that collects others types, rather than just the general cloud services.**

Cloud Storage
Object
list
get
getIamPolicy

Bucket
list
get
getIamPolicy
Big Query
Resource Viewer
Data Viewer

Step 1. Create Role

Go to **IAM > Role >** `+ Create Role` .

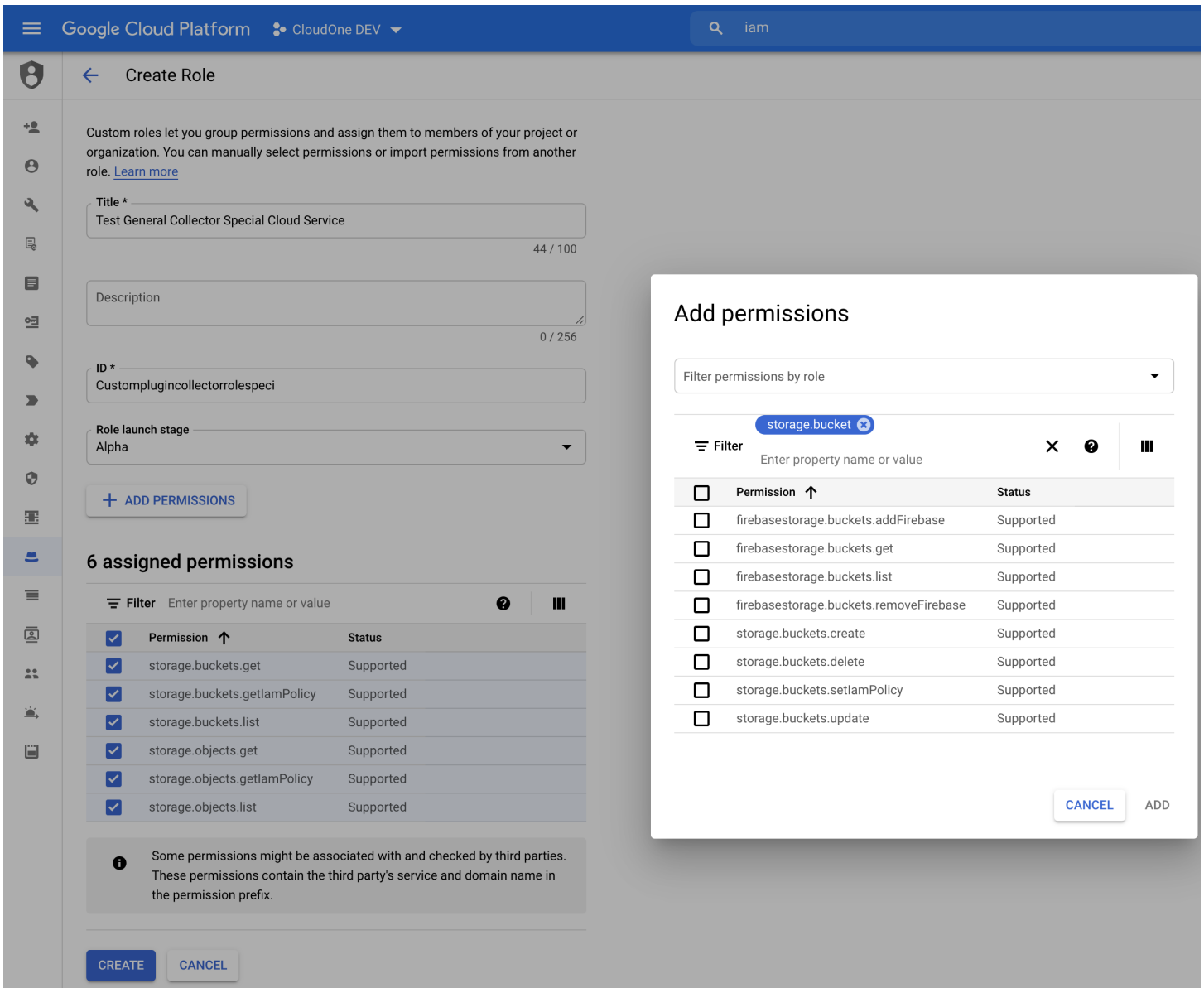


Step 2. Add Permissions to Role

Please, find an appropriate permission within the cloud service.

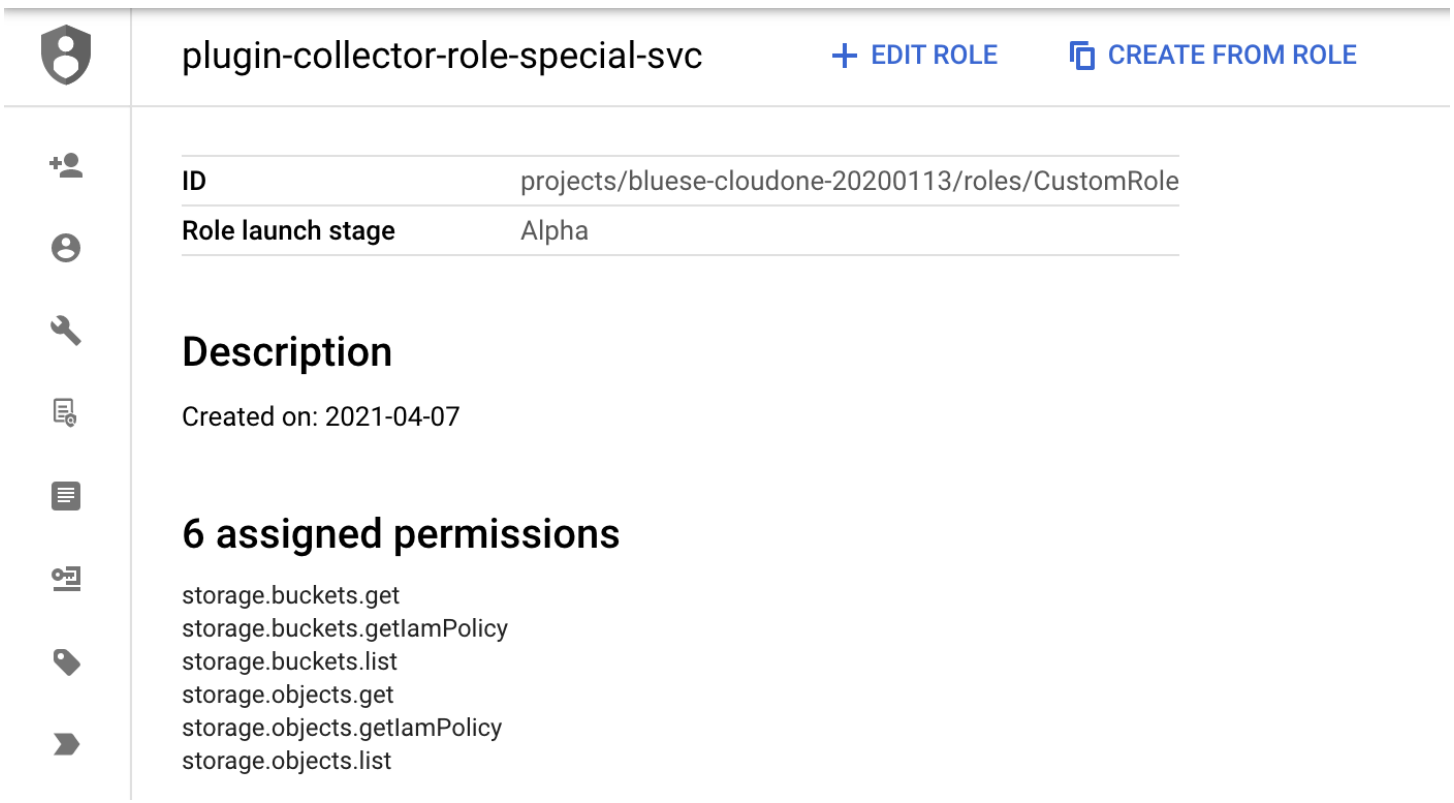
storage.buckets.get
storage.buckets.getIamPolicy
storage.buckets.list
storage.objects.get
storage.objects.getIamPolicy
storage.objects.list

Then click the `ADD` button.



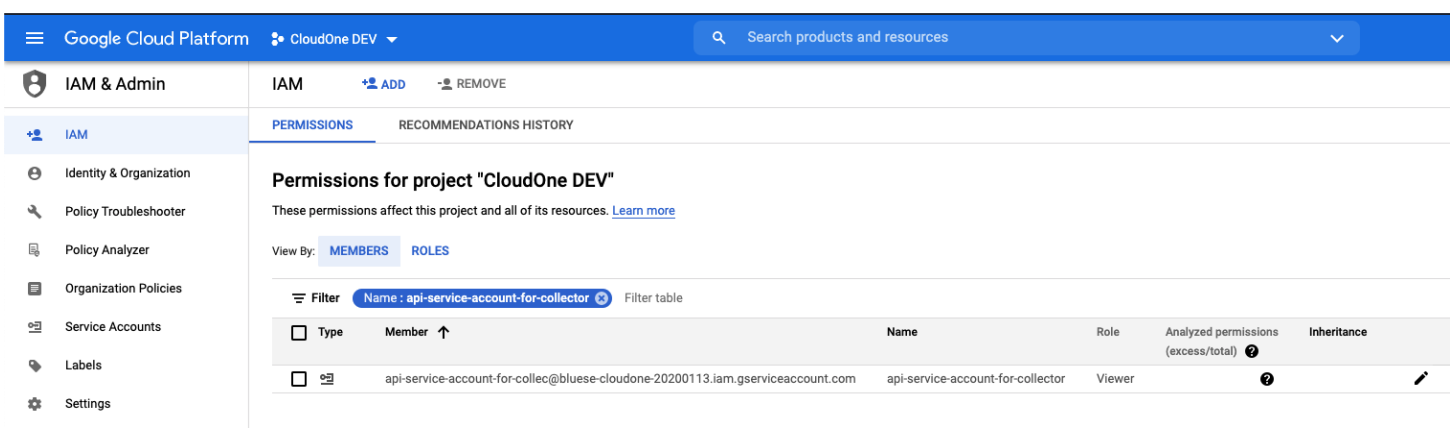
STEP 3: Review Permissions

Review the permissions once you've created a role.

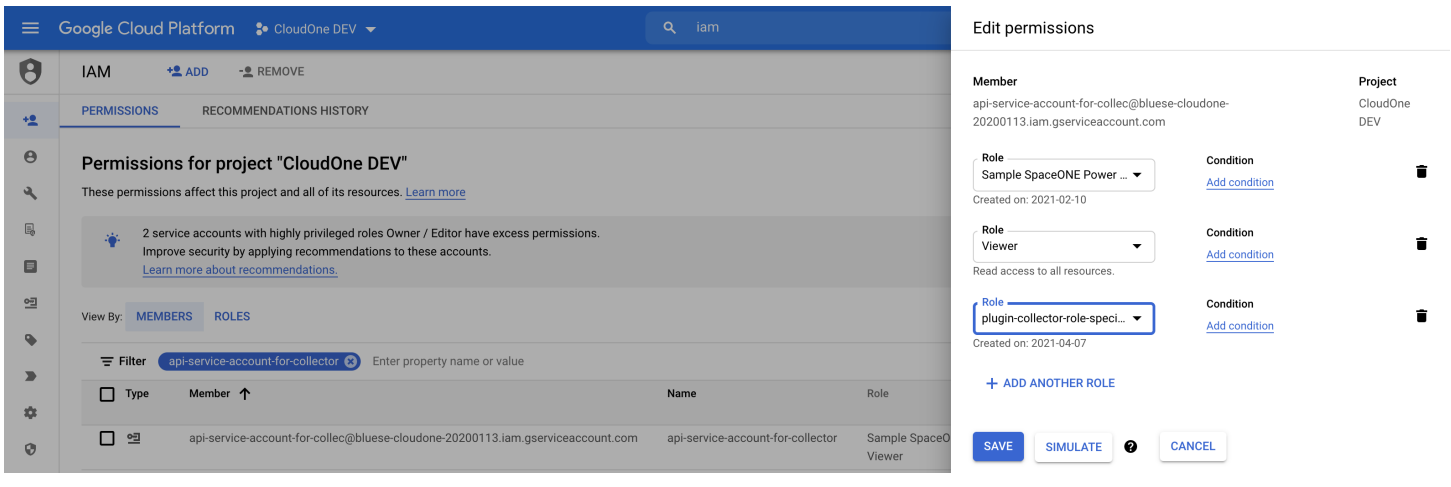


STEP 4: Set Created Role into the Service Account

Move to menu **IAM > IAM**.

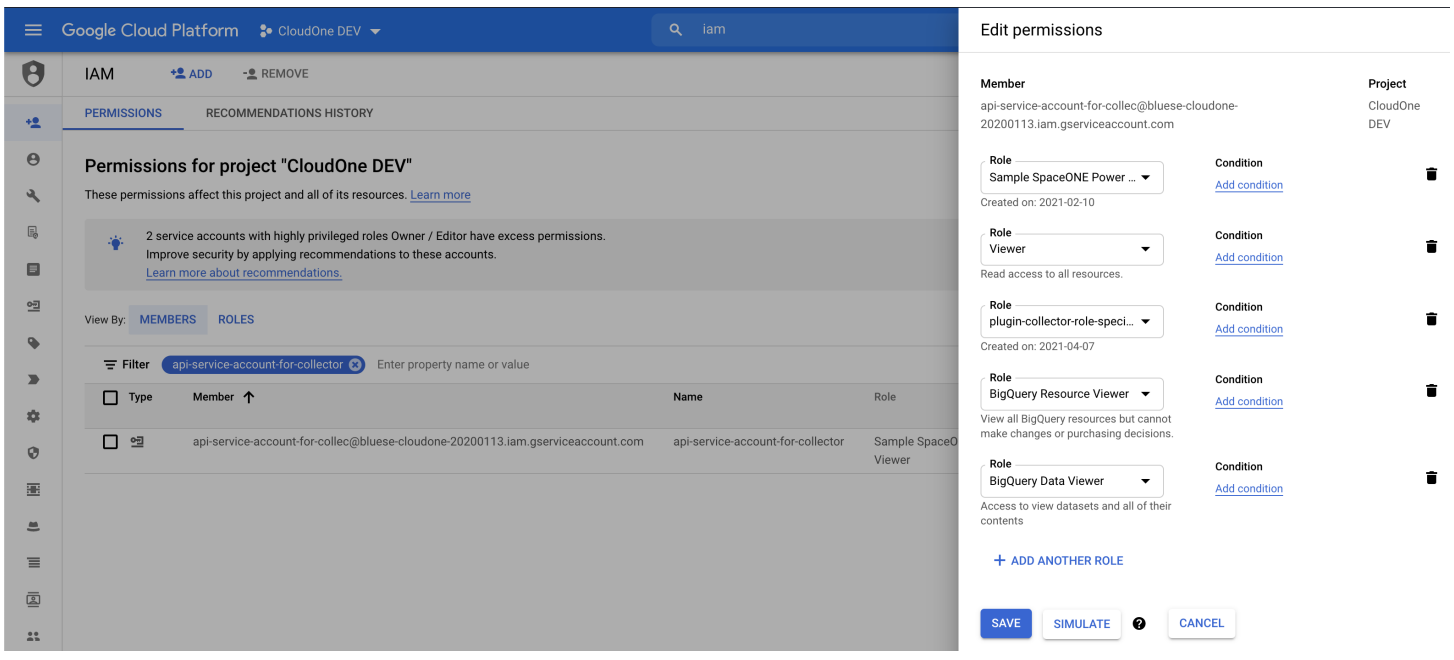


Click the ***pencil icon*** to move to **Edit permissions**. Then add the New Role created from the previous step.



STEP 5: Set BigQuery Permission into the Service Account

Use the `+ ADD ANOTHER ROLE` and add BigQuery roles. When you are done, click the `Save` button.



Power Controller

SpaceONE's ***Power Scheduler*** requires editing permissions to update the following Cloud Services:

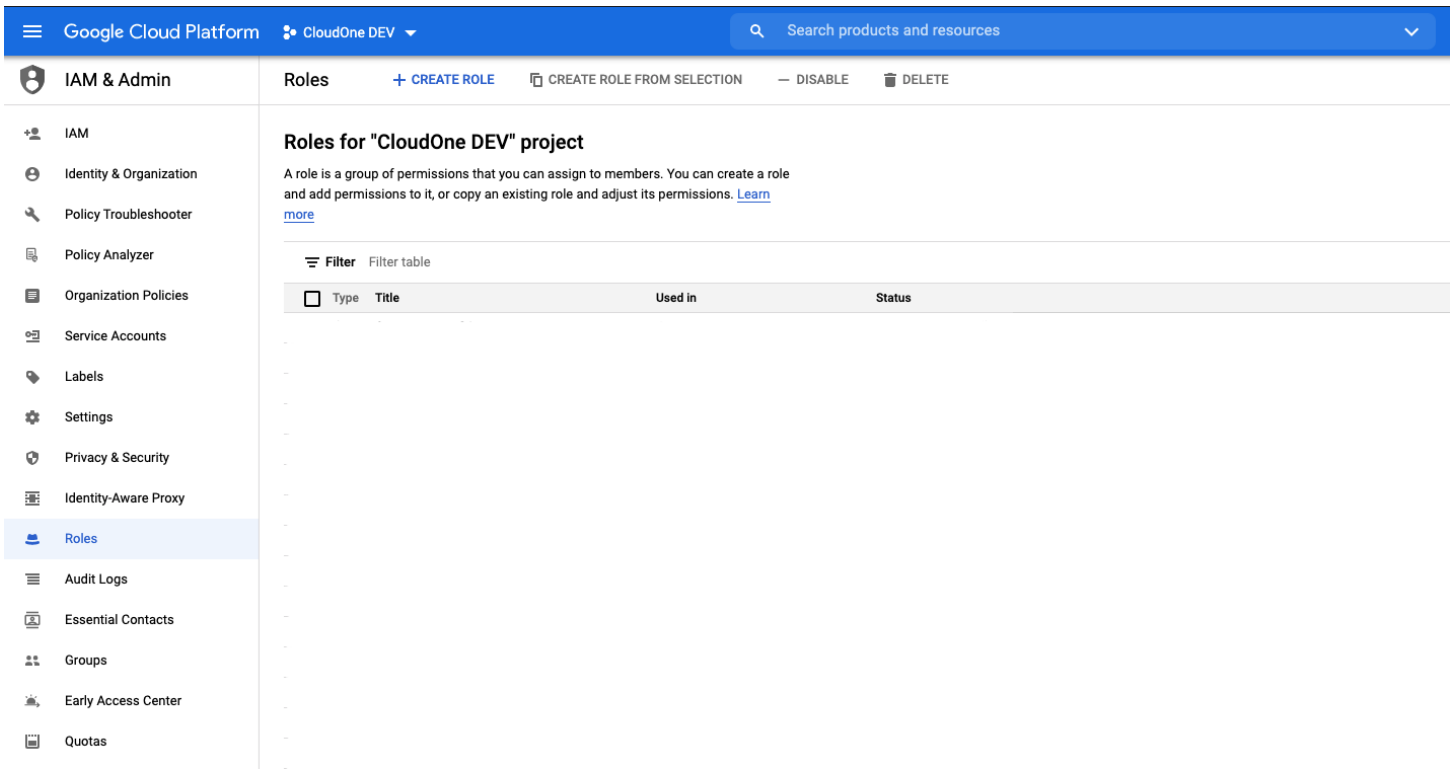
VM Instance

Instance Group

Cloud SQL

Step 1. Create Role

Go to **IAM > Role >** `+ Create Role` .



Step 2. Add Permissions to Role

Please, find an appropriate permission within the cloud services then click the **`ADD`** button.

VM Instance

Start

Stop

Reset

Instance Group (Manager)

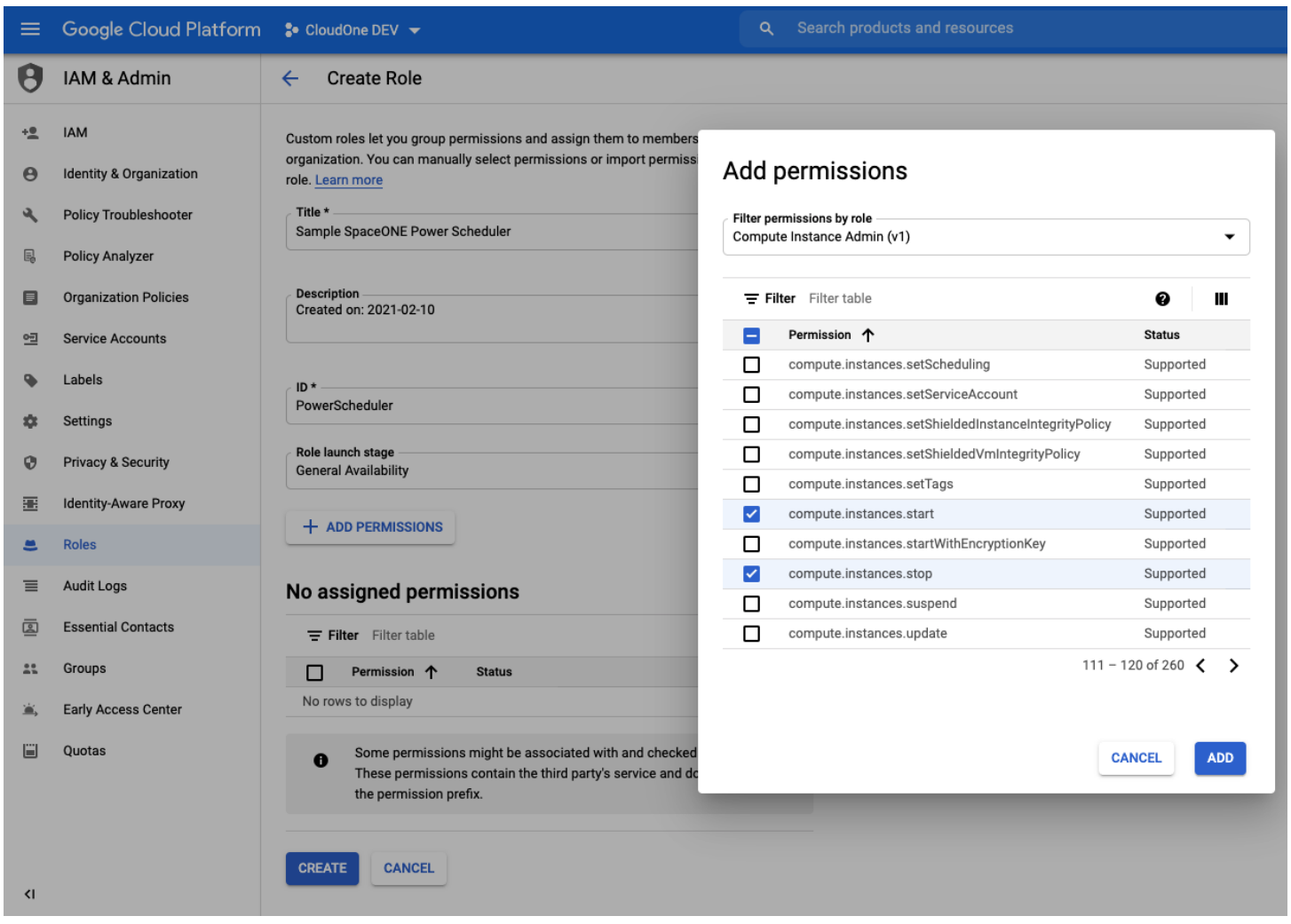
Resize

Autoscaler

Update

Cloud SQL

Update

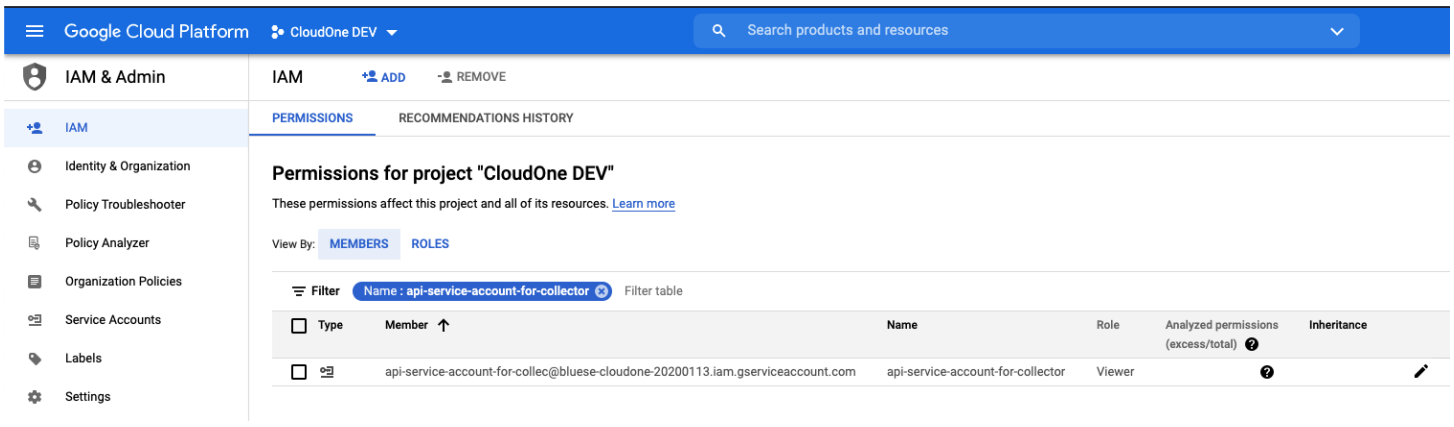


STEP 3: Review Permission

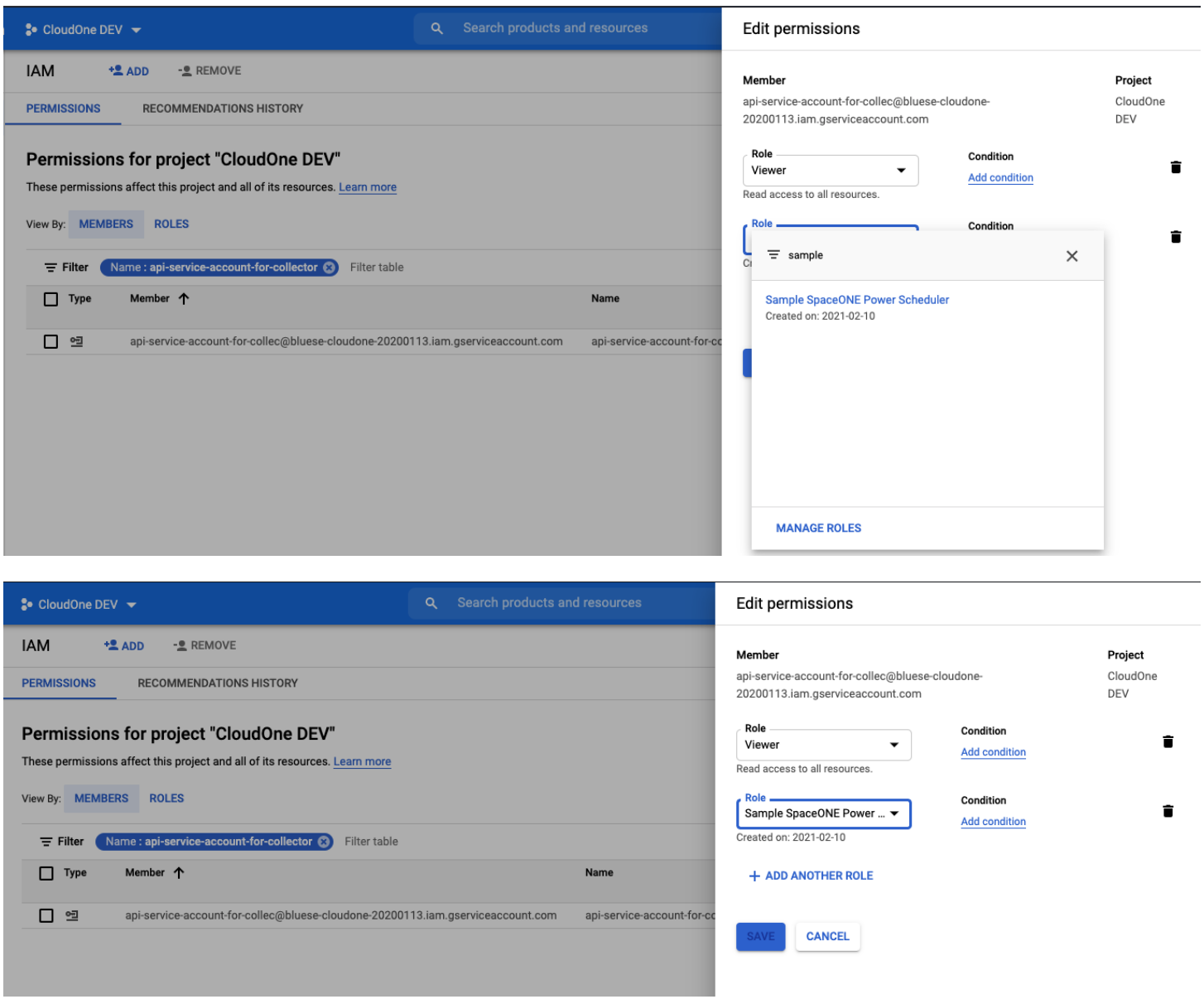
Review the permissions in the role you've created.

STEP 4: Set Created Role into the Service Account

Drive to menu **IAM > IAM**.

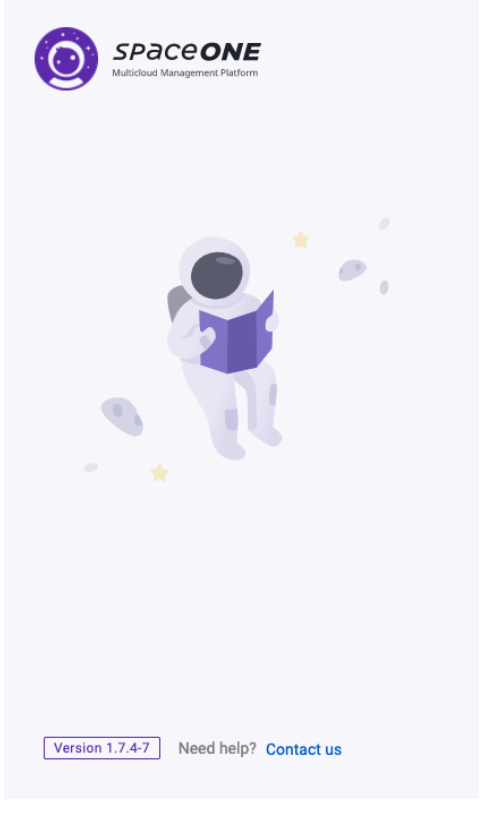


Click the ***pencil icon*** to move to **Edit permissions**. Then add the New Role created from the previous step.
After finishing the edit click the **`Save`** button.



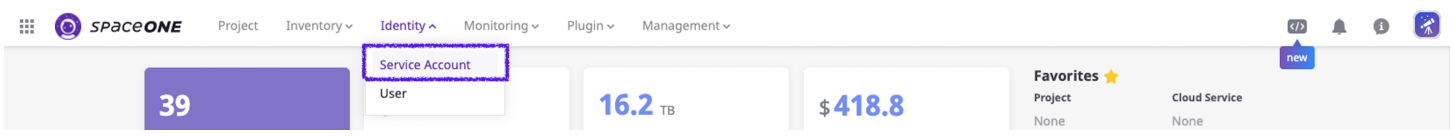
Register Your Service Account into SpaceONE

Step 1: Please, `Sign In` to the SpaceONE portal.



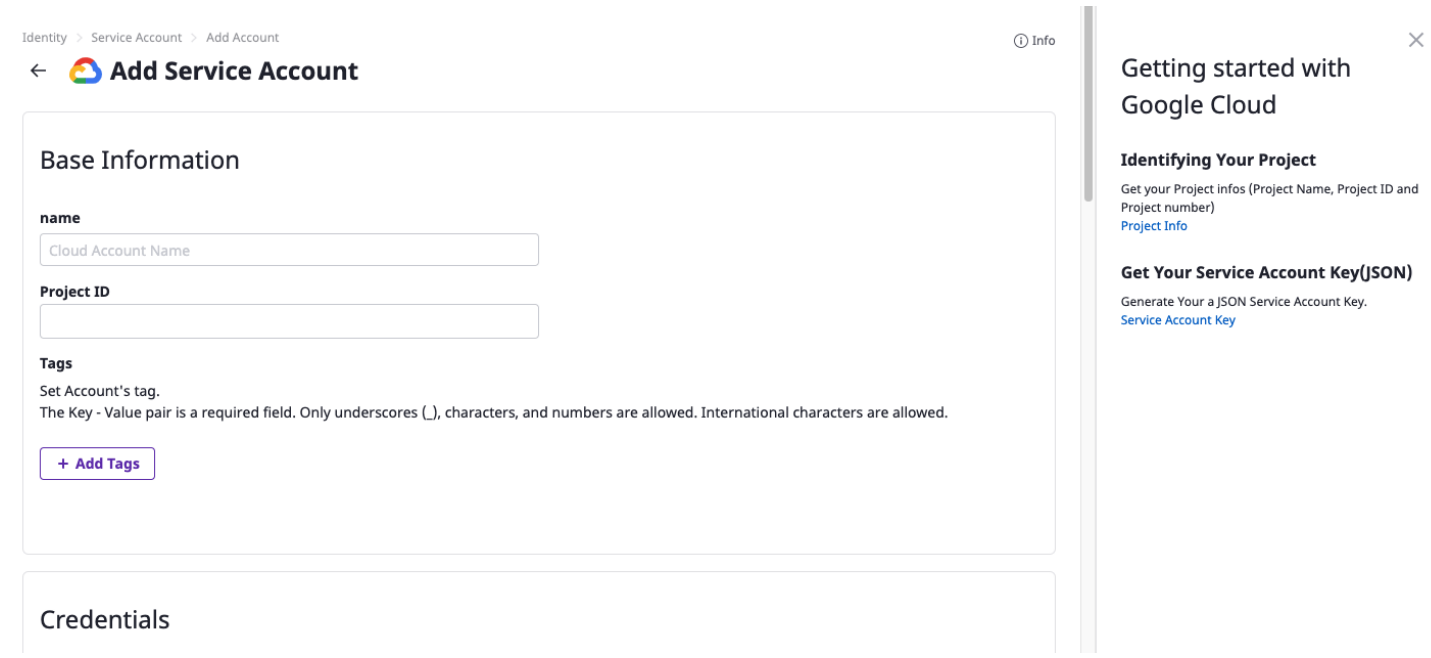
Step 2: Move to the menu's Service Account

Follow **`Identity > Service Account`** from the Top Menu bar.



Step 3: Select Provider and Add Service Account

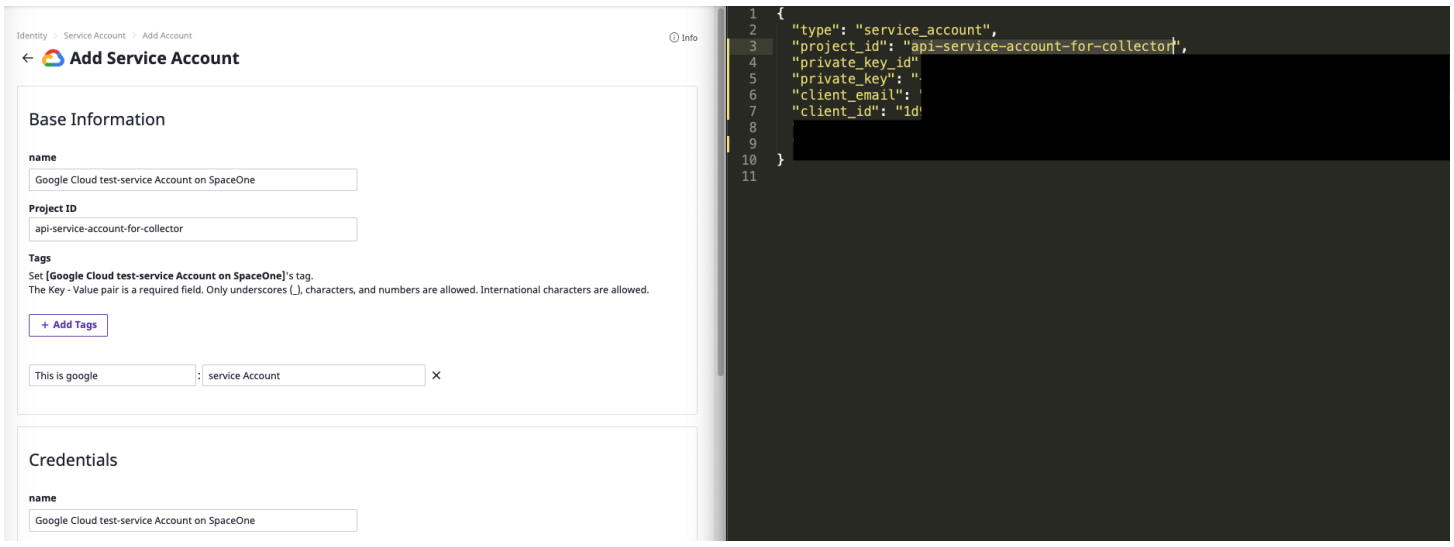
Select Google for the Service Provider and then click the **`+ Add`** Button



Step 4: Fill out the Base Information and Credentials

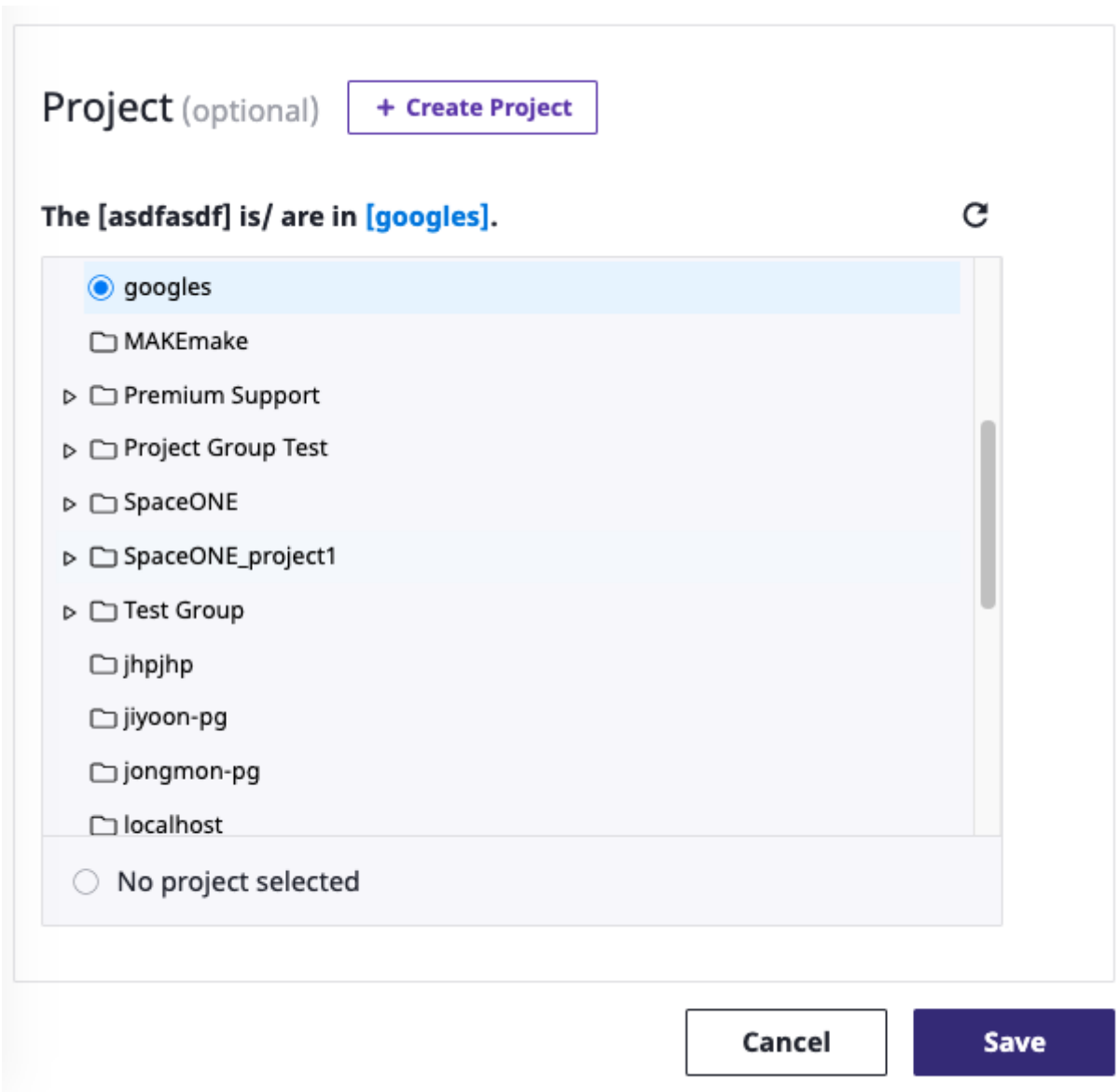
Please, fill out all required fields. Use your Service Account JSON that you issued at **General Collector Step** .

You can also just simply copy and paste the JSON.



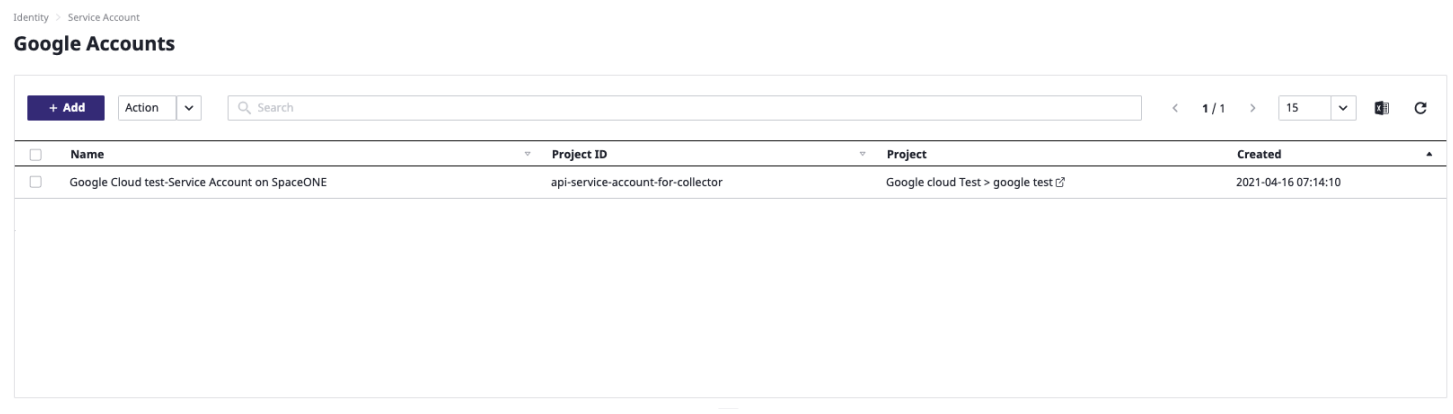
Step 5: Select a Project to Map the Service Account

Select a Project that you want to map the service account on. Then click the **`Save`** button.



Step 6: Confrim your Registration

Finally check the Service Account's **Google Account List** to confirm your registration.



4.3 - (Azure) Access Control (IAM) Policy Management

Details of API Security policy to use SpaceONE plugin

Access Control Policy

SpaceONE highly recommends, setting appropriate permissions to Resource groups for each purpose.
Please set service accounts to Create APIs for each Use Case:
General Collector

General Collector

Collectors require appropriate authorities to collect cloud resources. We strongly recommend limiting the collector's service account permission to `read only access`. Or you can add more restrictions per resources or actions. One useful example is to restrict its rights within region.

Prerequisites

This user guide tutorial assumes that a `subscription id` is already created. Assuming that the `subscription id` is created, you now need to allow permission from Azure Resources so SpaceONE can collect them.
There are two ways to do so.
Grant *Reader role* to Resource Groups
Grant `Reader role` to Resource Groups where the resources are located. If you give a role to the resource group, *SpaceONE* will only collect resources located in this resource group.

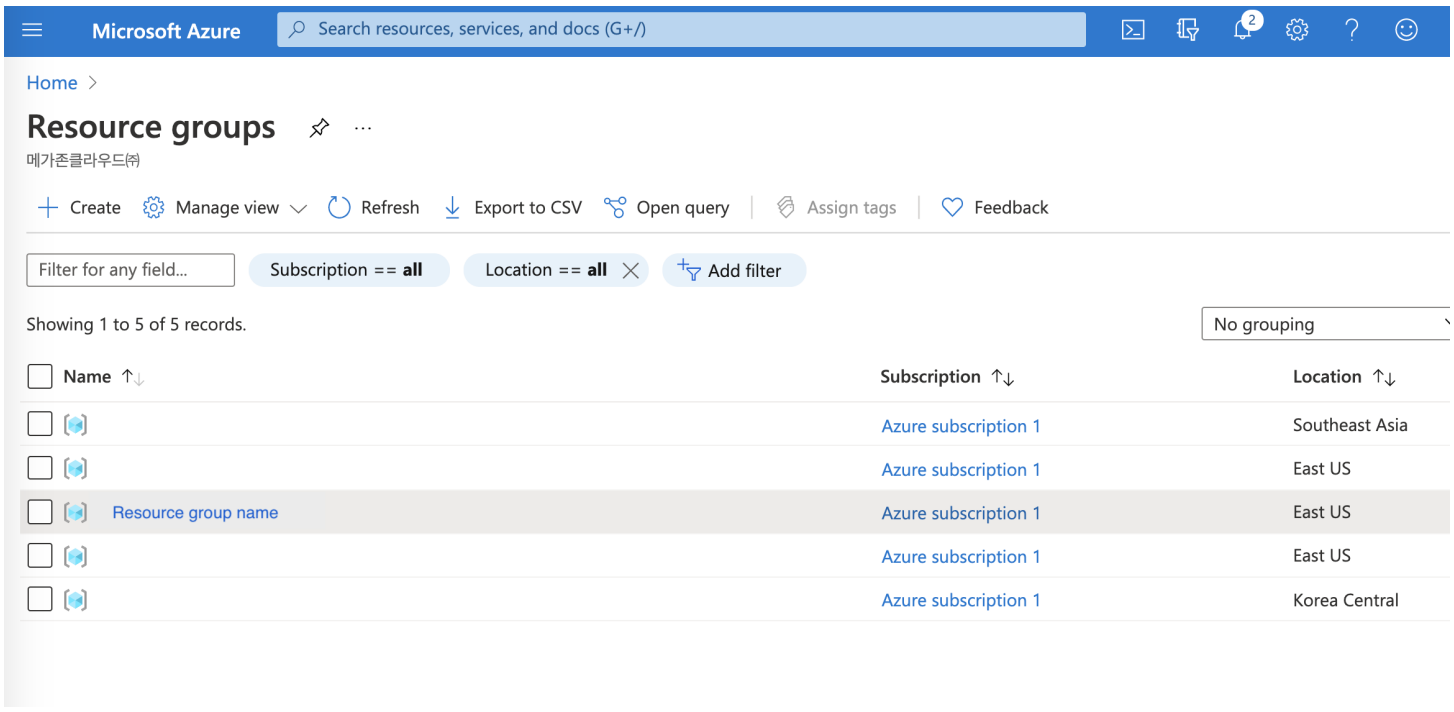
Grant *Reader role* to Subscriptions
Grant `Reader role` to Subscriptions where resources are located. If you give a role to the subscription, *SpaceONE* will collect resources from all the resource groups in this subscription.

If you want to know more about Azure's access control policies, visit this link .

Granting Roles

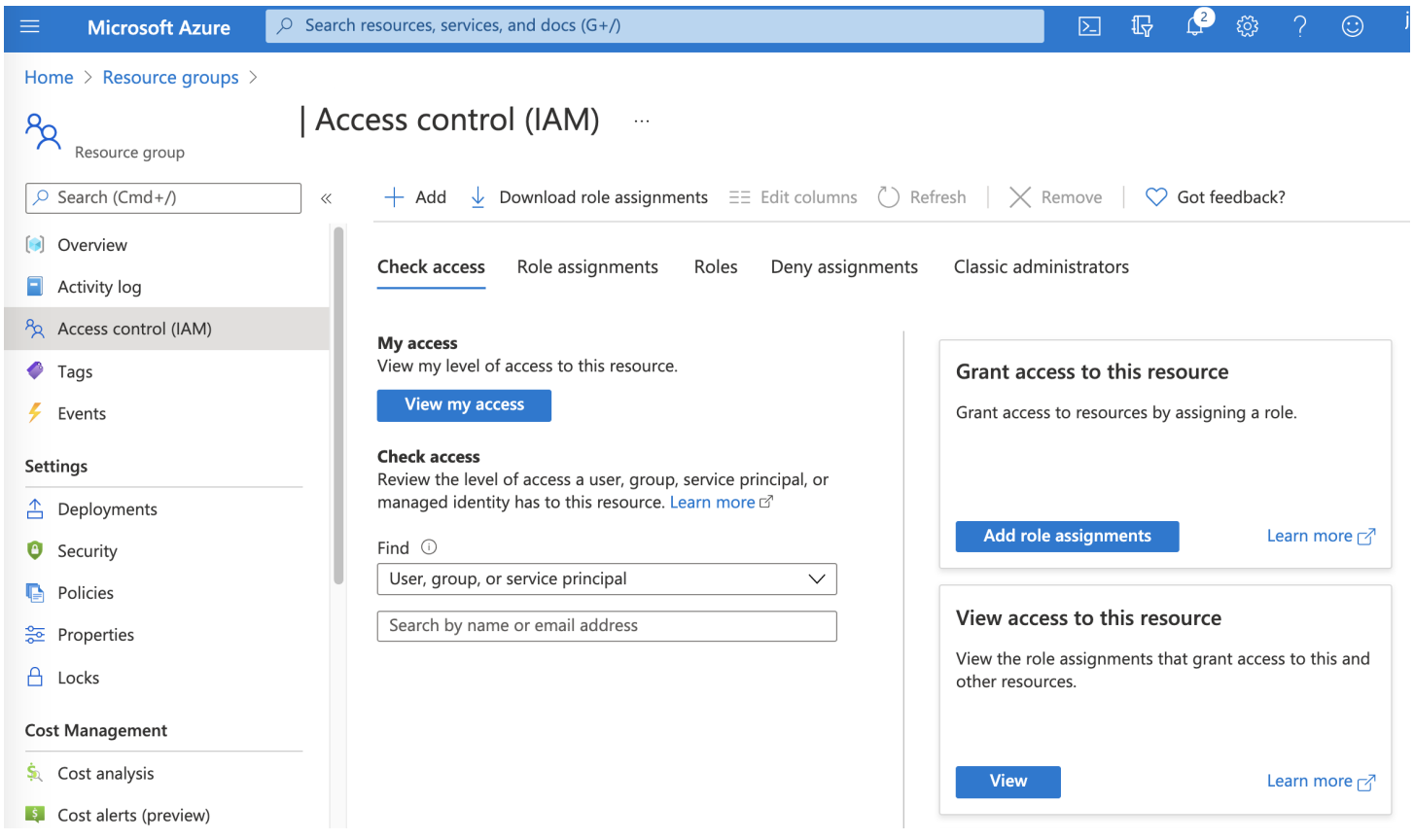
Grant Roles to Resource Groups

STEP 1. Sign in and move to Azure Portal > Resource groups
Select a Resource Group for which the Collector will collect resources from.



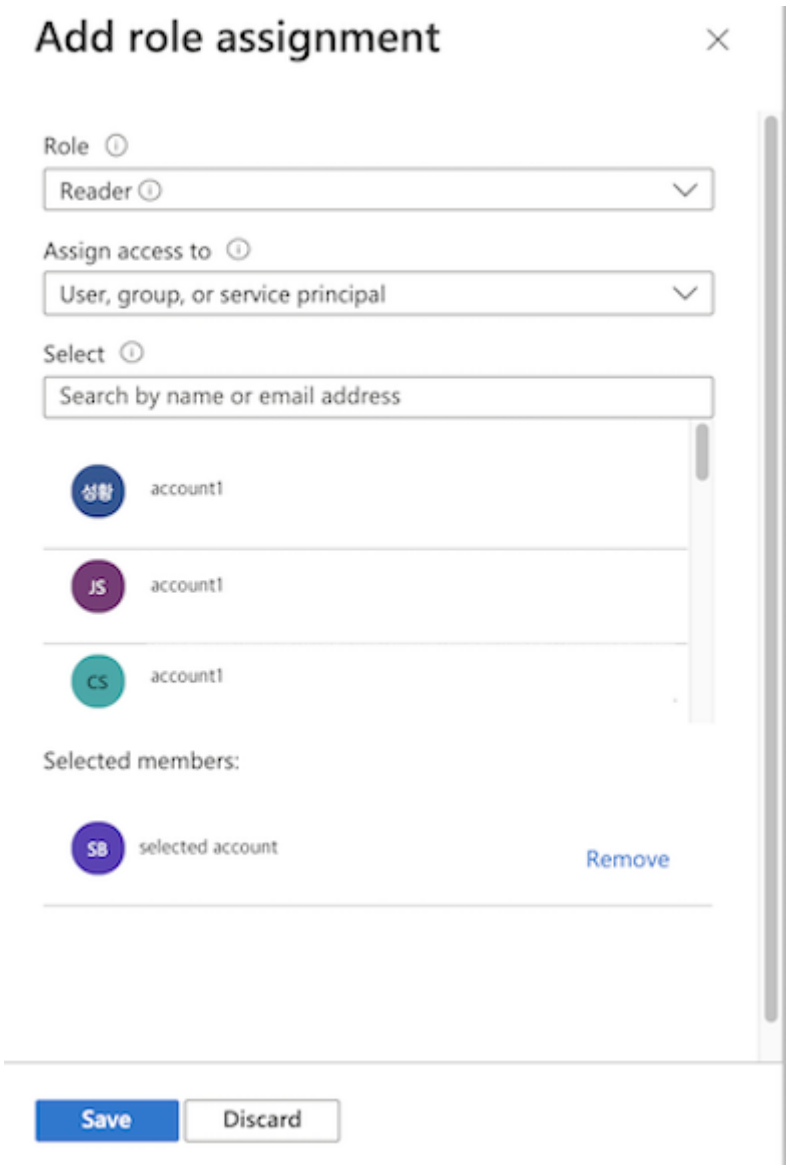
STEP 2. Add Access Control (IAM)

Click `Access control (IAM)` from the Navigation tab, and then select the `+Add` button.



STEP 3: Assign `Reader role`

Assign the **Reader Role** to the account. The account should have access permission in this resource group.



Troubleshooting

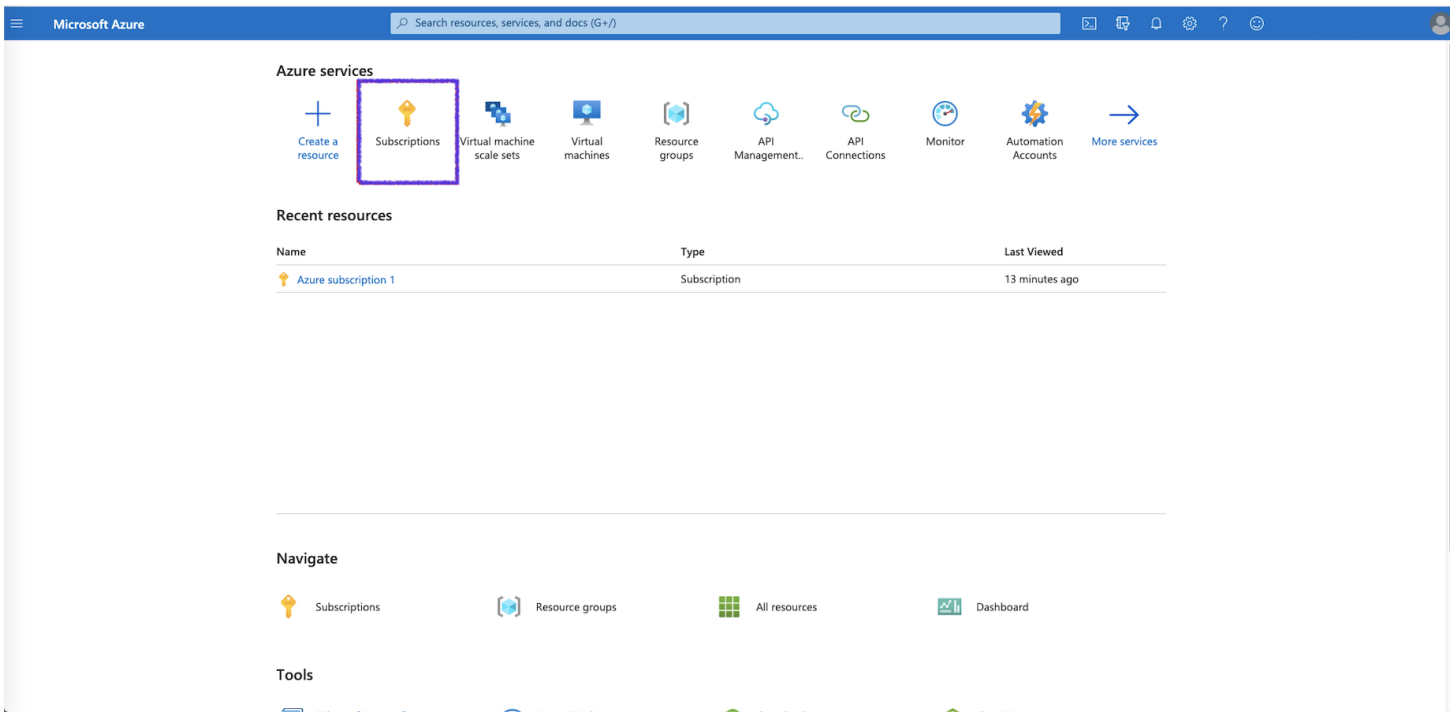
If you face Error messages when following the steps above, please follow this TroubleShooting Guide.

Authorization

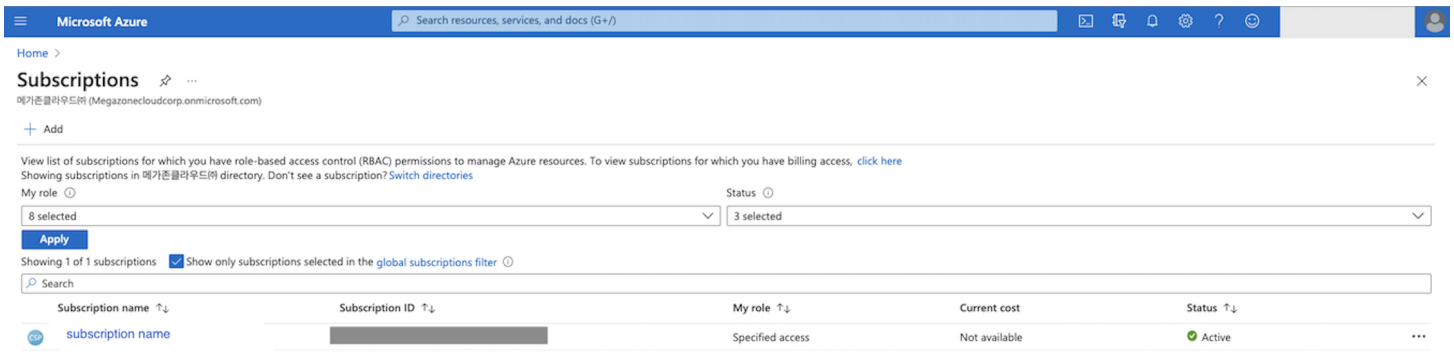
1. (AuthorizationFailed) Client does not have authorization

> The client (`client_id`) with object id (`object_id`) does not have authorization to perform action 'Microsoft.Resources/subscriptions/resourcegroups/read' over scope (`subscription_id`), or the scope is invalid. If access was recently granted, please try refreshing your credentials.

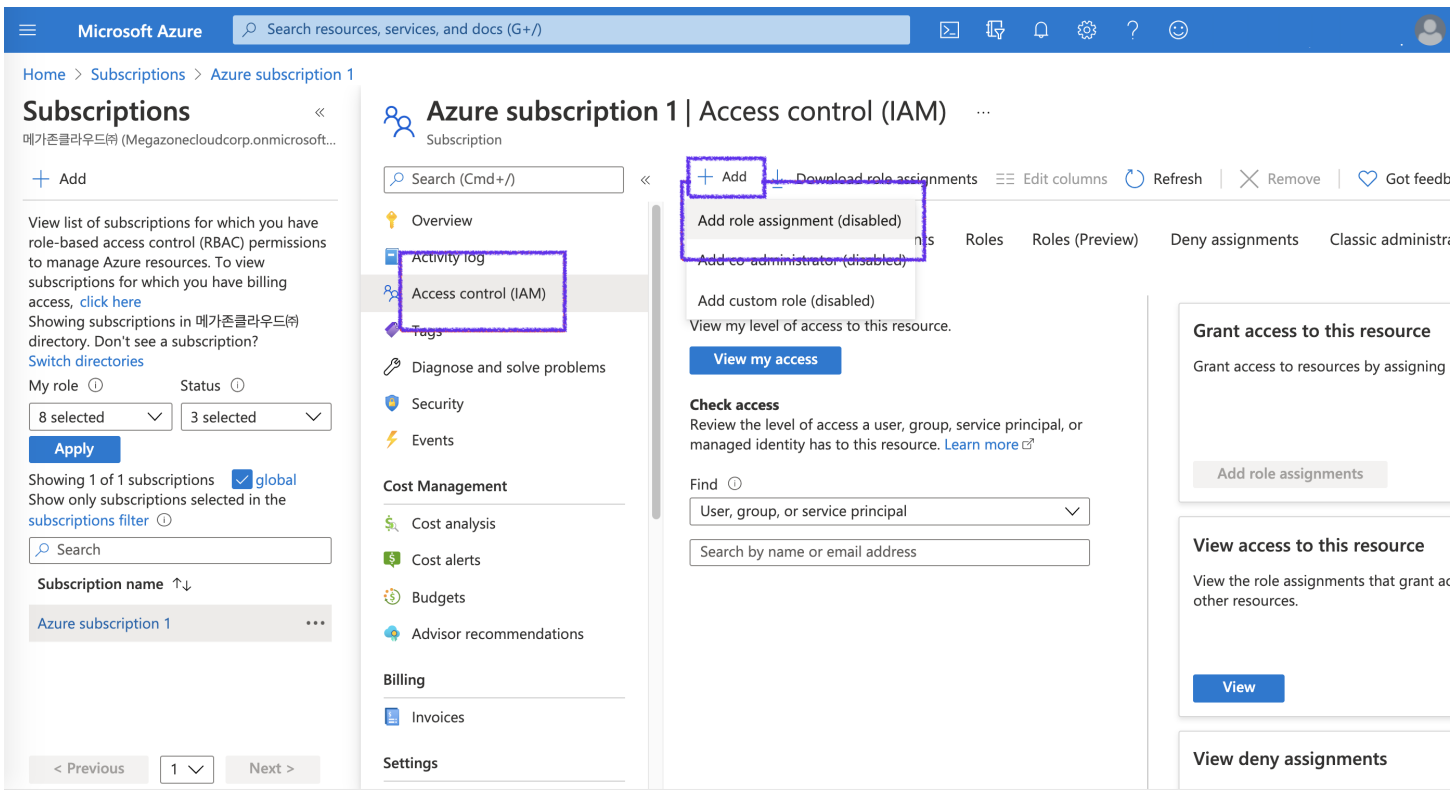
STEP 1: Log in to the Azure Portal and move to Subscriptions



STEP 2: Click on the subscription Name where the resources are located.



STEP 3: Click the `+Add role assignment` button.



STEP 4: Add role assignments

Add the Role Assignments like the following description and image.

Role

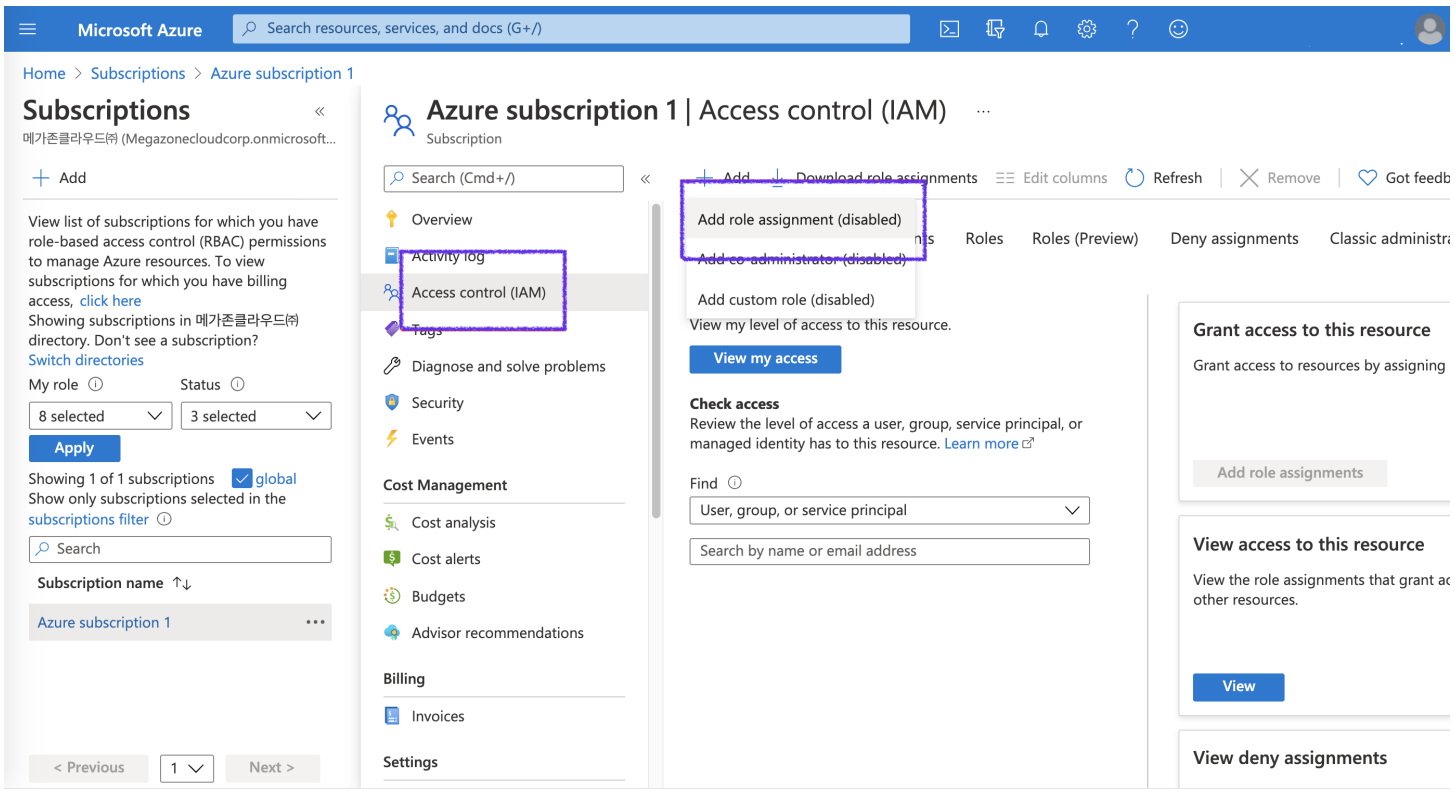
`Reader`

Assign access to

`User, group, or service principal`

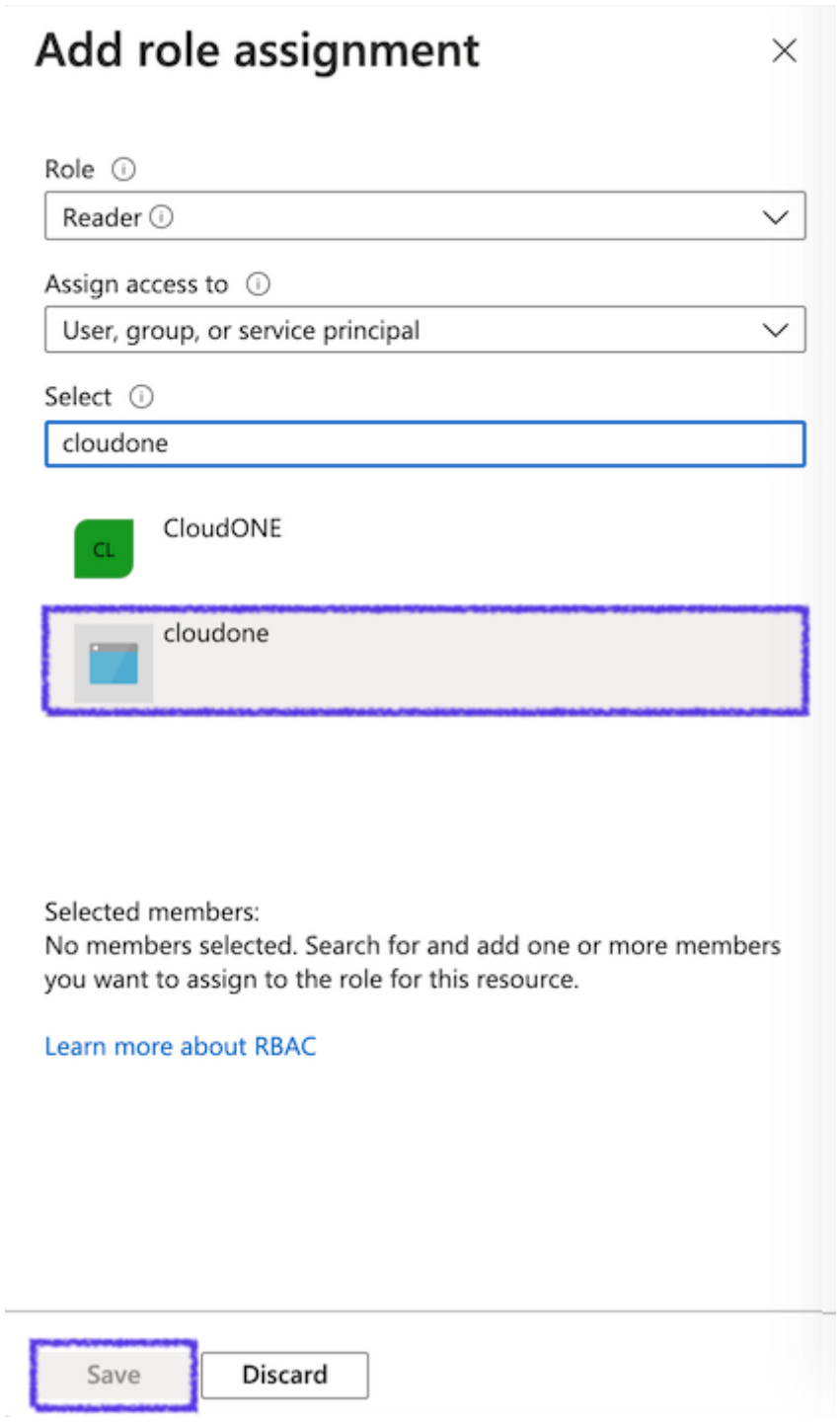
Select

`App that has registered on Active directory` at **Azure ActiveDirectory > Registered App**



Note

'Service Account names' and 'Registered App names' are easily confused.
Please, Select Registered App as shown below (Check the Icon Differences).



4.4 - (Oracle Cloud Infrastructure) Identity and Access Management(IAM) Policy Management

Details of API Security policy to use SpaceONE plugin

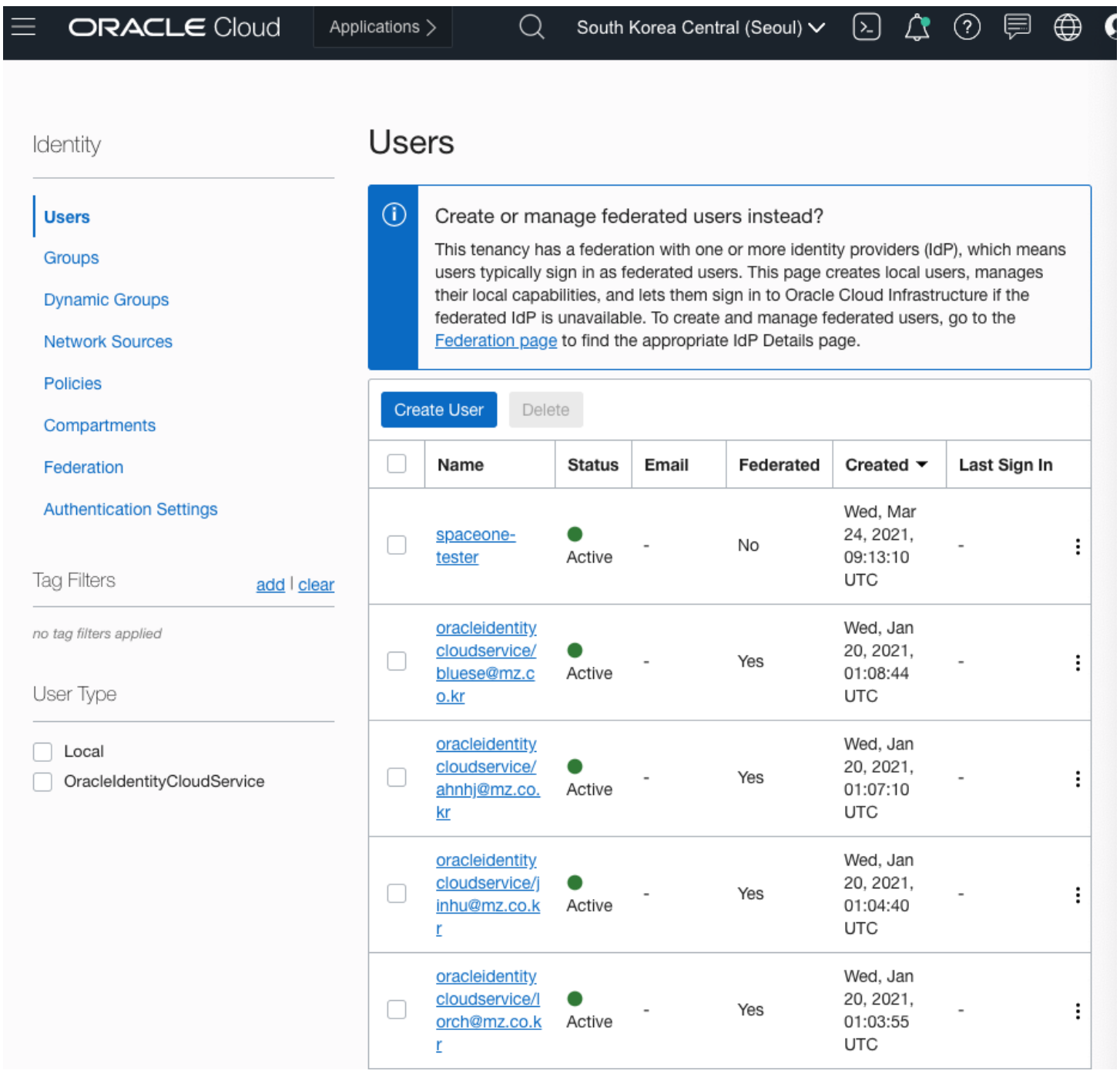
IAM Policy

SpaceONE highly recommends to set appropriate permissions to access your ***cloud resources*** for each purpose.
Please, Set service account, To Create API for each use case
General Collector

General Collector

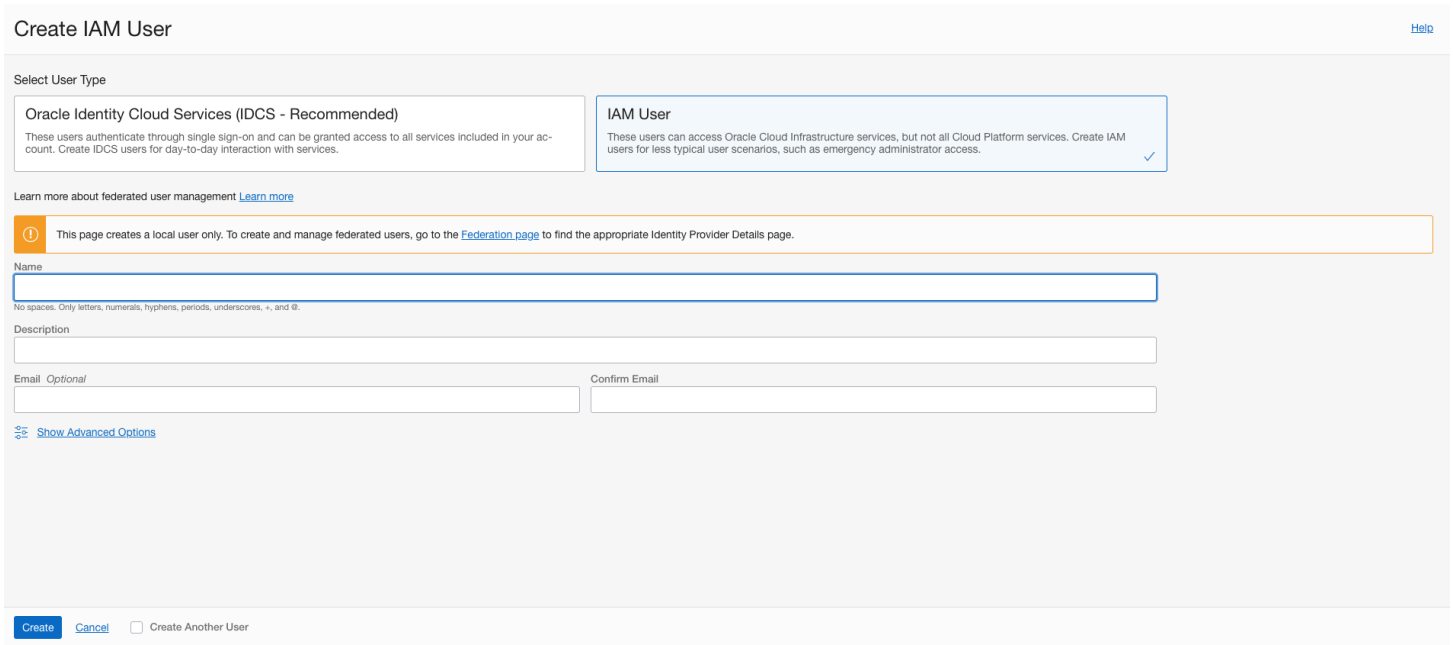
Collector requires appropriate authorities to collect cloud resources. We strongly recommend to limit collector's service account its permission to **read only access**.
Otherwise, you can add more restrictions per resources or actions. One of the useful example is to restrict its rights within region.

STEP 1. Log in Oracle Cloud Infrastructure Console > Identity
Go to Identity > Users and Click `CREATE USER`



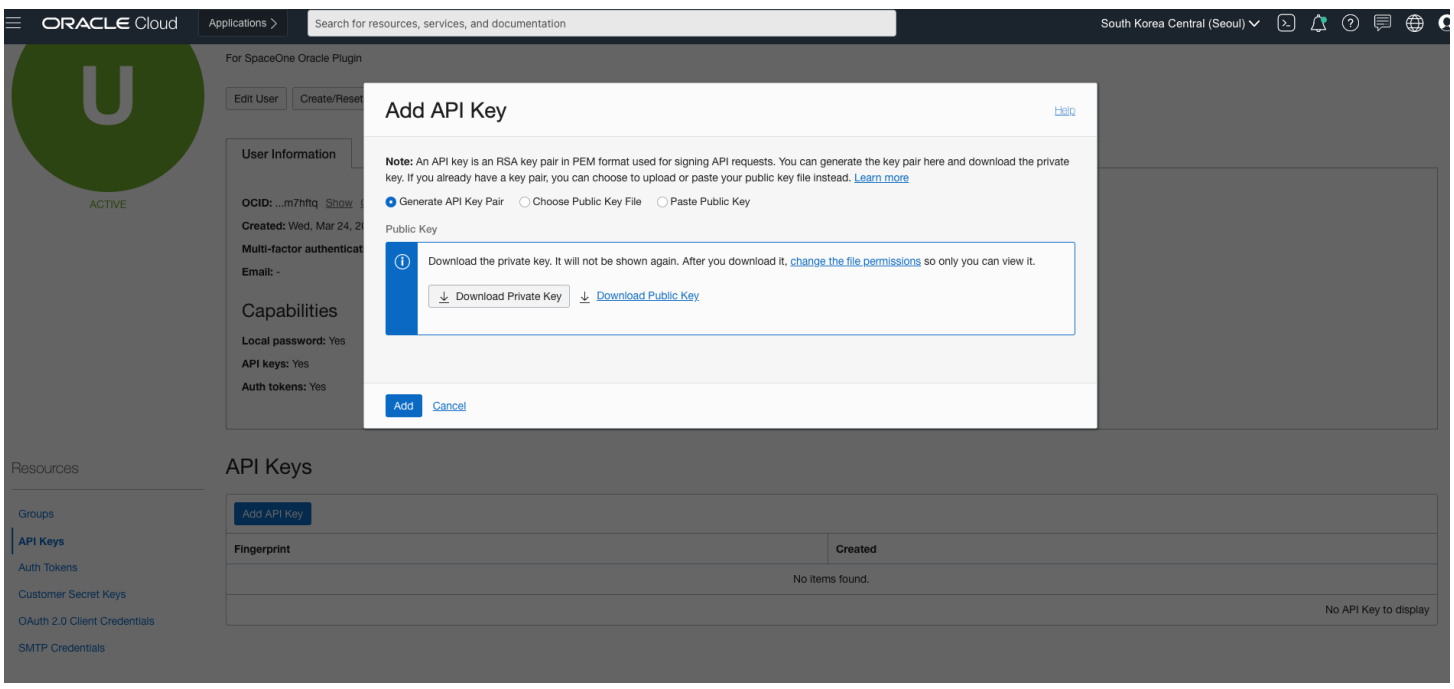
STEP 2. Set IAM User details

Click `IAM User` and Enter ***User name*** and ***Description***



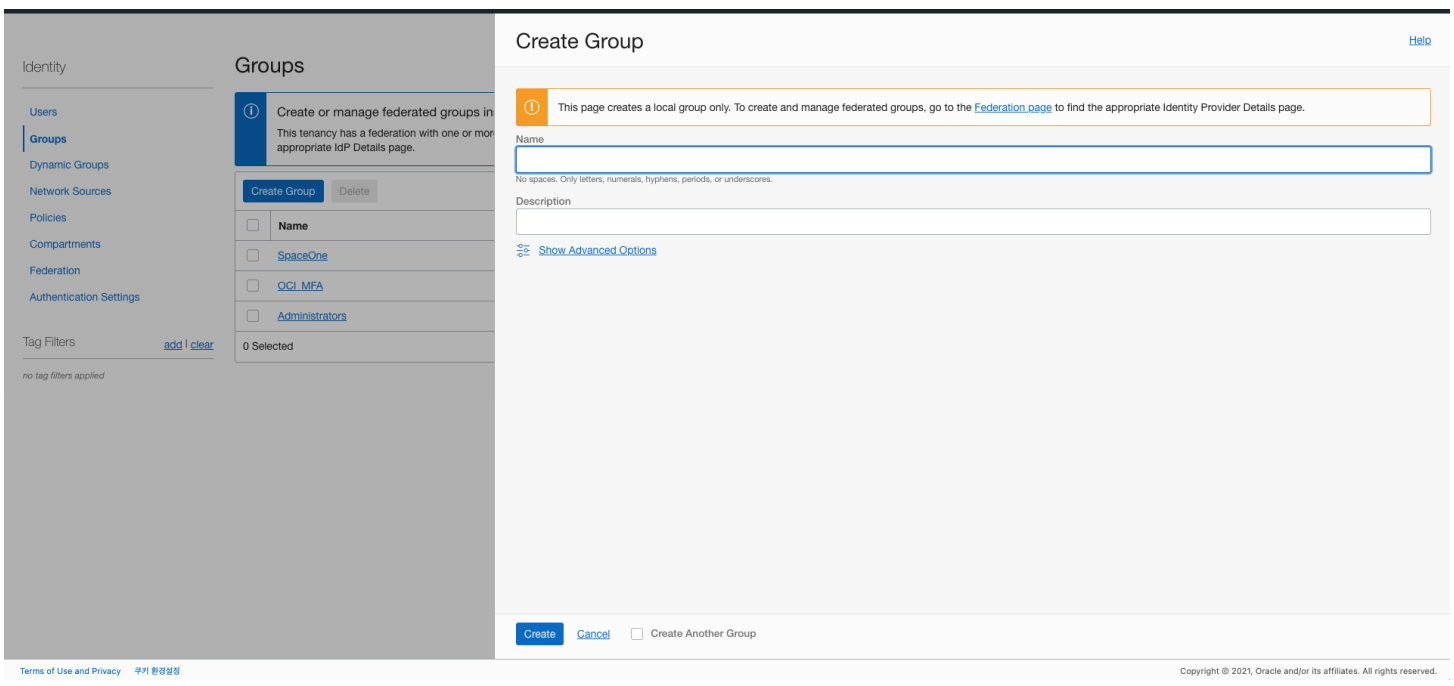
STEP 3. Set API Keys to IAM User

Go to Identity > Users > User > Details > API Keys. Click `Add API Key` and add or Generate API Key.



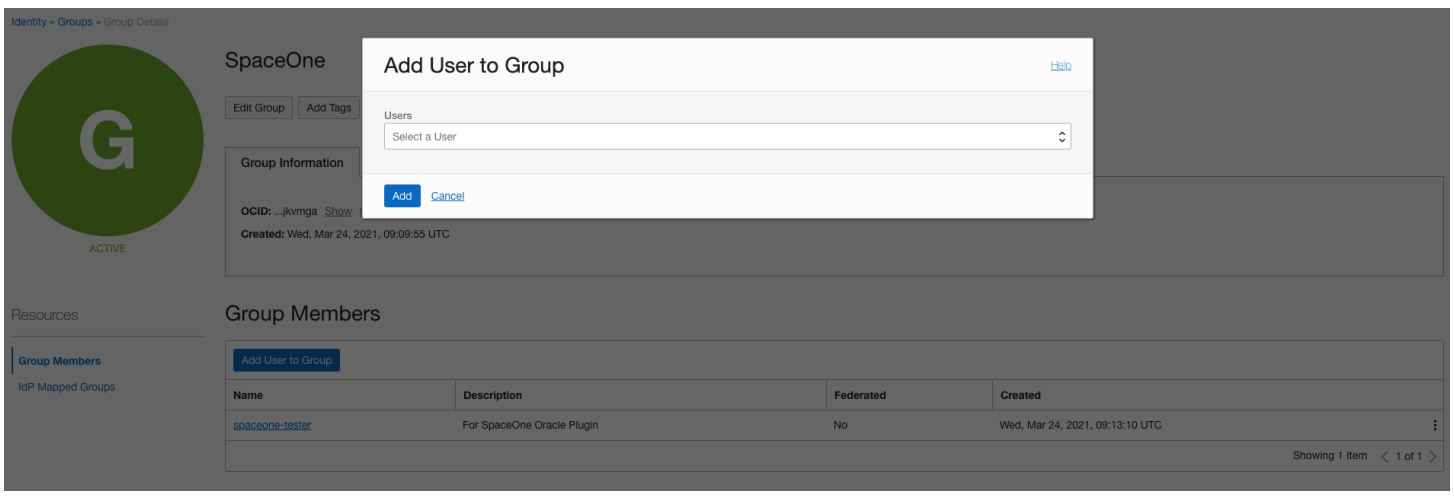
STEP 4. Create Group for IAM User

Go to Identity > Groups and Click `Create Group` Button. Enter ***Name*** and ***Description***.



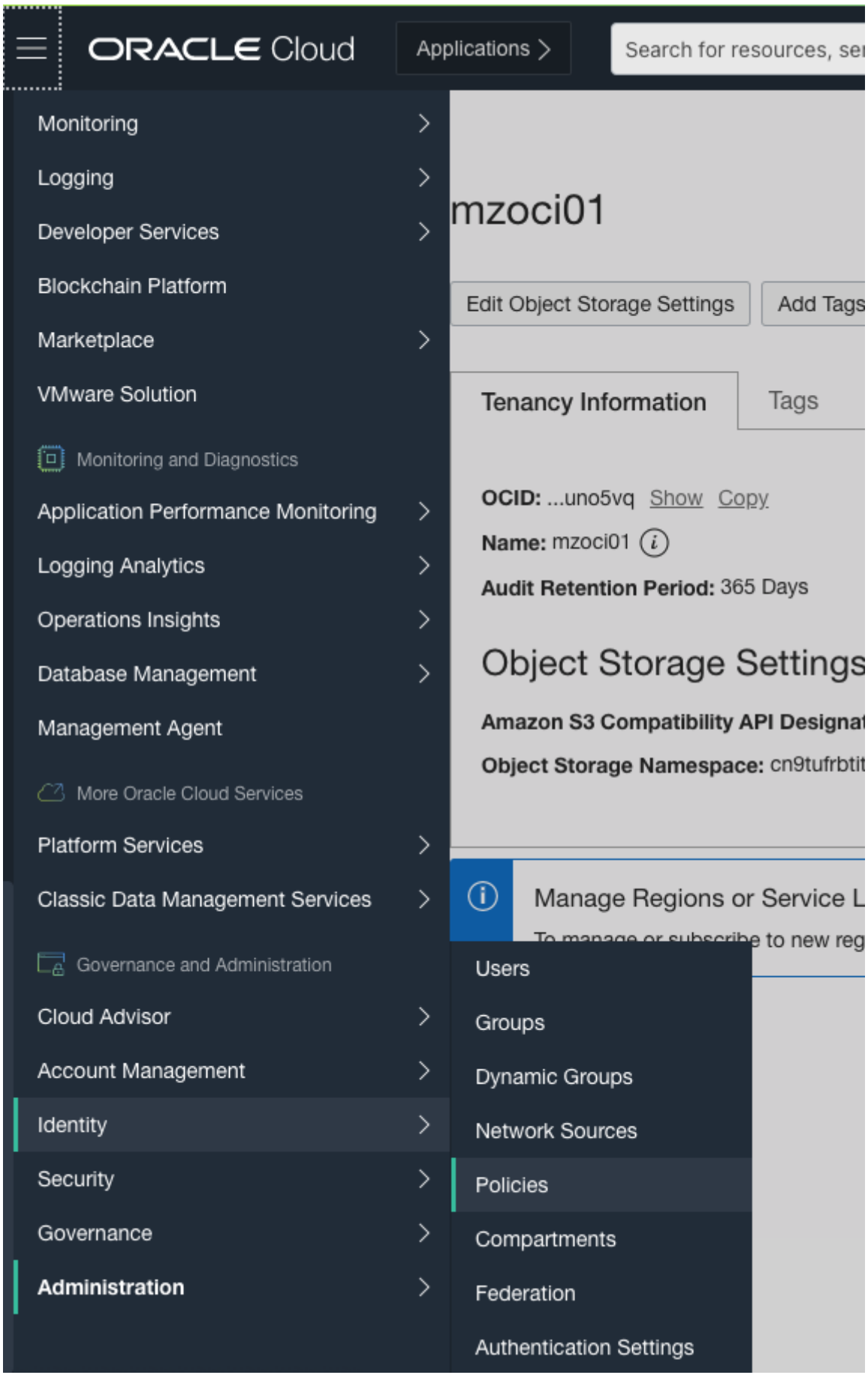
STEP 5. Add IAM User to Group

Go to Group that you made and Click `Add User to Group` Button and add IAM User.



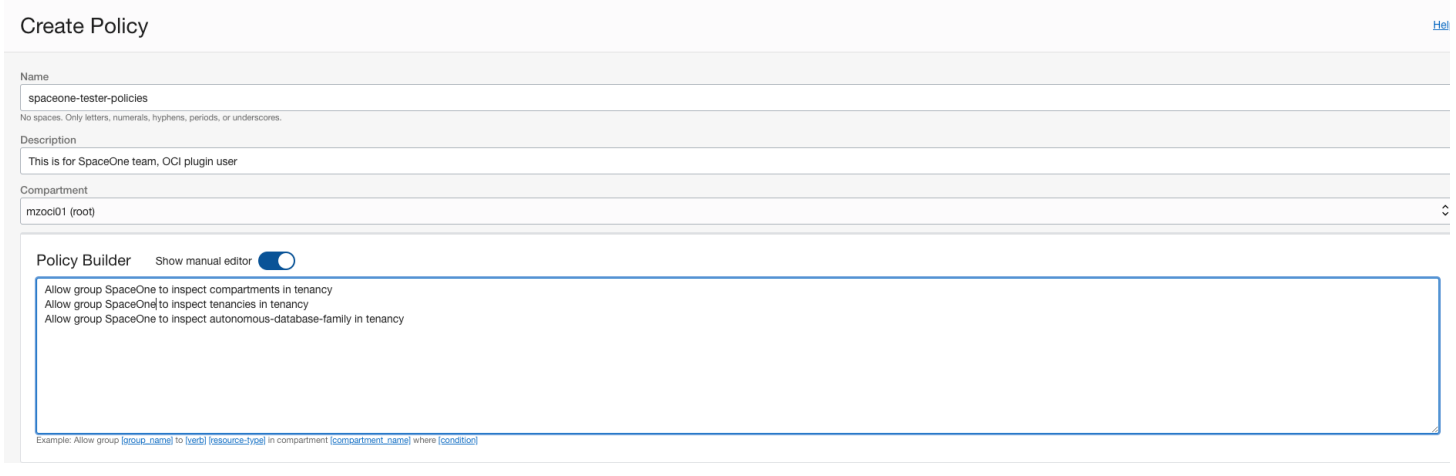
STEP 6. Set Policies to Group

Go to Identity > Policies and Click `Create Policy` Button.



Enter ***Name*** and ***Description*** and ***Policies*** by manually.
Entering statements directly in the text box, ensure that you follow the Policy Syntax rules.
When using General Collector, the **following two policies are required**:

```
Allow group {group_name} to inspect compartments in tenancy
Allow group {group_name} to inspect tenancies in tenancy
```



4.5 - (Alibaba Cloud) Service Account Policy Management

Details of API Security policy to use SpaceONE plugin

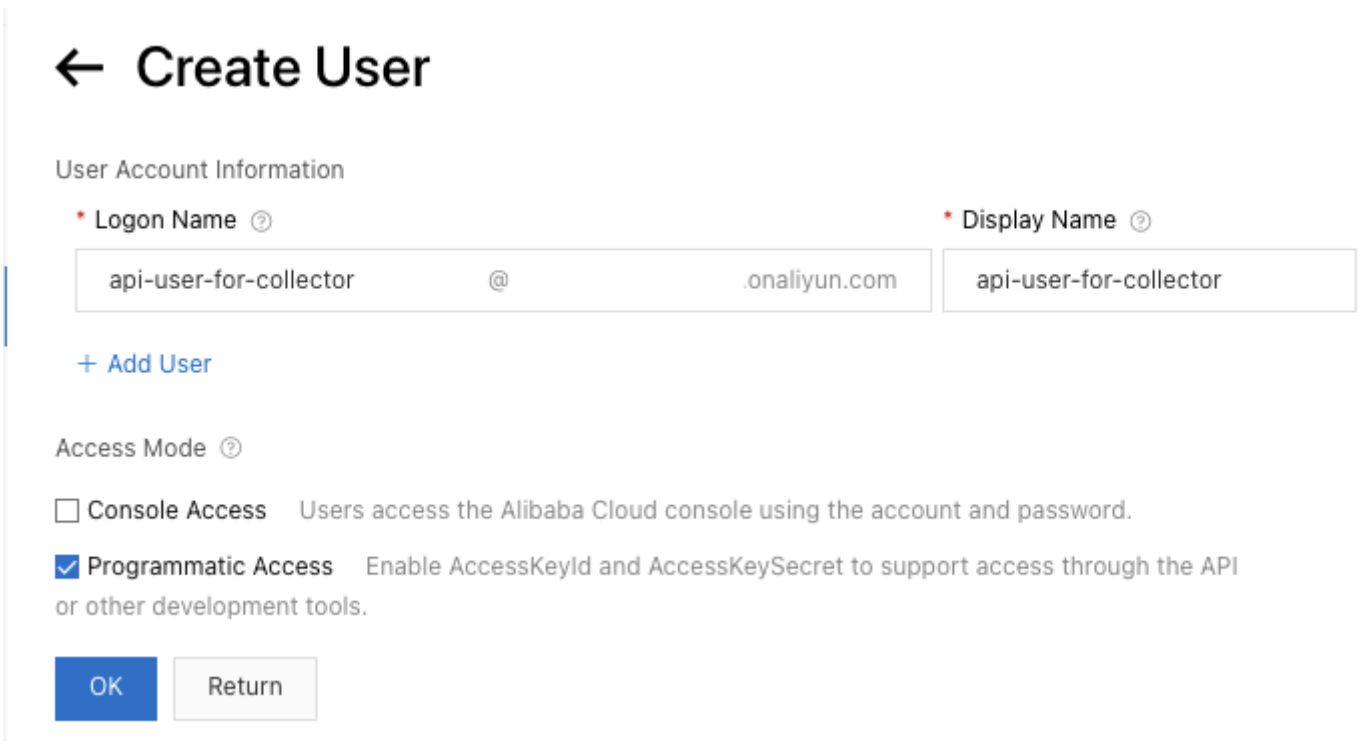
Service Account Policy

SpaceONE highly recommends to set appropriate permissions to **Service Account** for each purpose. Please, Set service account, To Create API for each use case:
General Collector

General Collector

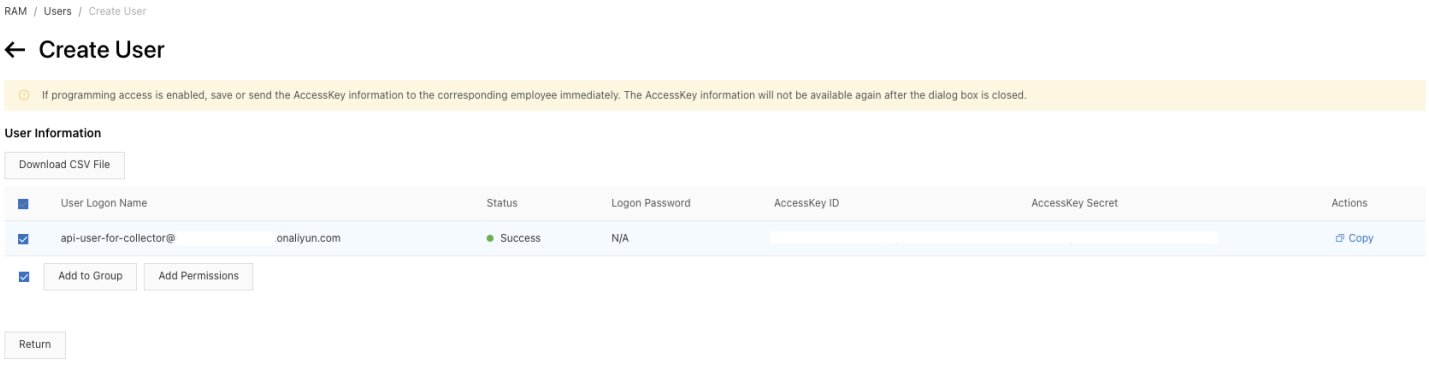
Collector requires appropriate authorities to collect cloud resources. We strongly recommend to limit collector's service account its permission to **read only access**.
Otherwise, you can add more restrictions per resources or actions. One of the useful example is to restrict its rights.

STEP 1. Create RAM users
Log on to the RAM console by using your Alibaba Cloud account.
In the left-side navigation pane, click `Users` under `Identities`.
Click `Create User`.
To create multiple RAM users at a time, click `Add User`.
Specify the ***Logon Name*** and ***Display Name*** parameters.
Click **OK** and return to *Create User screen*.



STEP 2. Create AccessKey pairs for RAM users
You need AccessKey pairs to enter Alibaba Cloud Credentials in the SpaceOne. If you have authorized a RAM user under your Alibaba Cloud account to manage their own AccessKey pairs, the RAM user can create an AccessKey pair in the RAM console.
In the left-side navigation pane, click `Users` under `Identities`.
In the User Logon Name/Display Name column, click the username of the ***target*** RAM user.
In the User AccessKey Pairs section, click `Create AccessKey`.
You must enter a verification code if you are creating an AccessKey pair for the first time.
Click `OK`.
The AccessKey Secret is displayed only once when you first create it. You cannot retrieve the AccessKey Secret if you forget it. We recommend that you save the AccessKey Secret for subsequent use.

If the AccessKey pair is disclosed or lost, you must create a new one. Currently, you can create a maximum of two AccessKey pairs.



STEP 3-1: Authorize RAM users to access data as read-only. (via console)

In the left-side navigation pane, click `Users` under `Identities`.

In the User Logon Name/Display Name column, click the username of the ***target*** RAM user.

Click `Add Permissions`. On the page that appears, the principal is automatically filled in.

In the Policy Name column, select `ReadOnlyAccess` policy for its ***System Policy***.

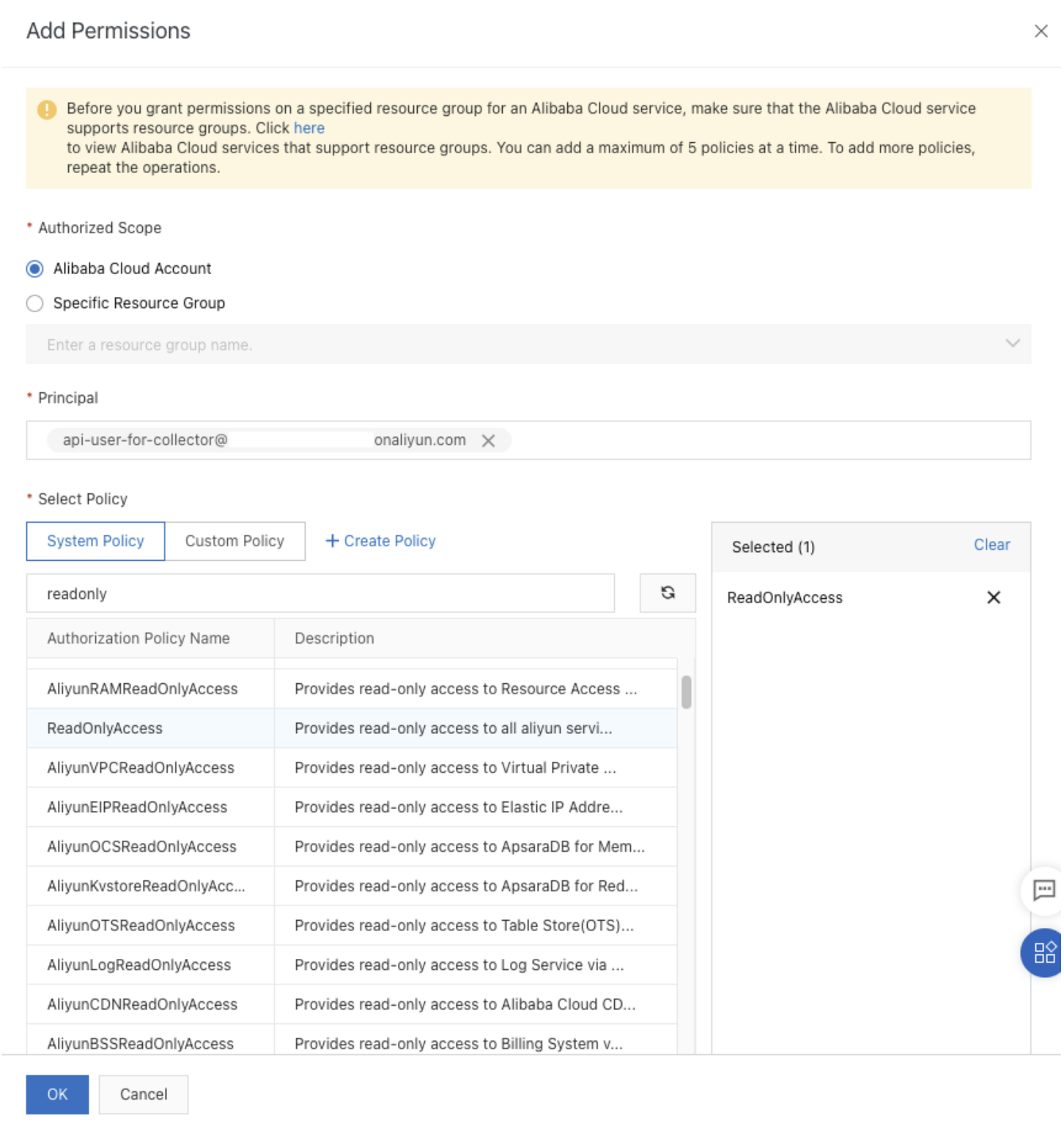
You can click X in the section on the right side of the page to delete the selected policy.

Click `OK`.

Click `Complete`.

You will return to *Create User screen*, and can check you ***AccessKey ID*** and ***AccessKey Secret***.

Alibaba Cloud generates AccessKey Pair by default when you create a user. Click **`Copy`** to copy your authentication information. Go to step 5 if you miss this step.



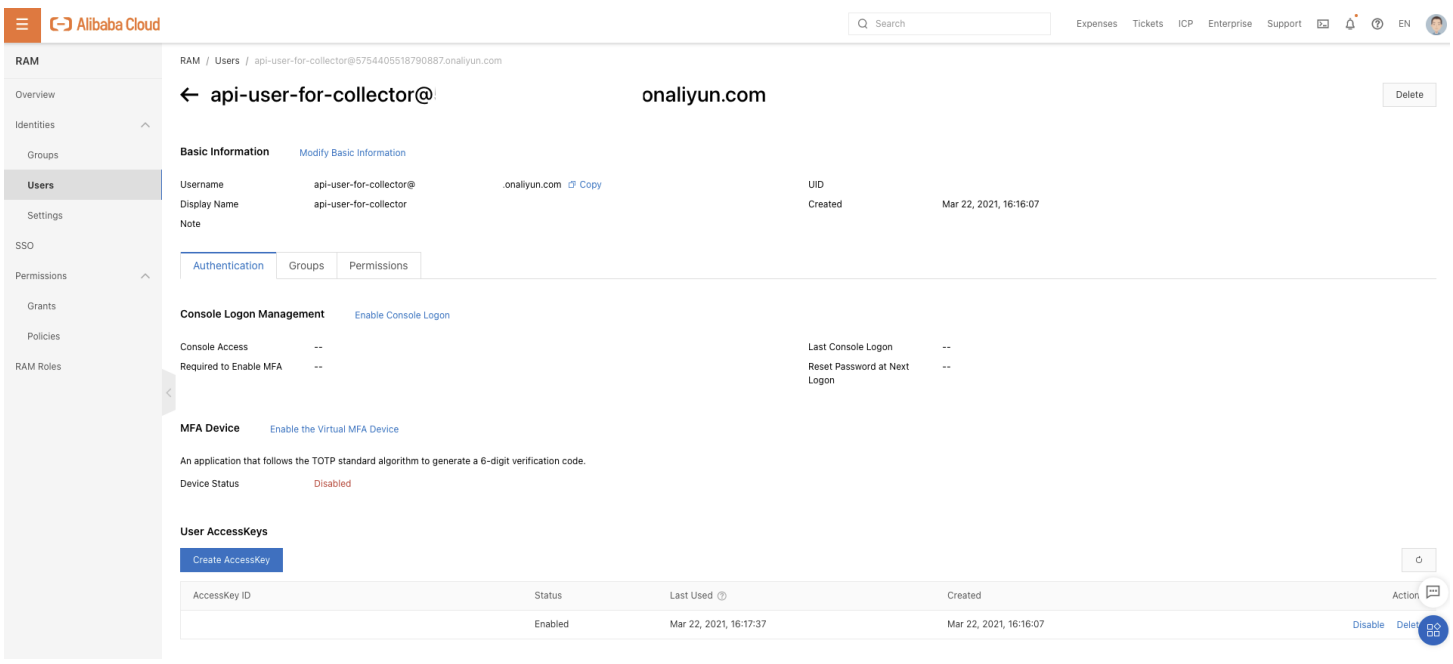
STEP 3-2: Authorize RAM users to access data as read-only. (via API call)

You can attach a policy to a RAM user by calling an AttachPolicyToUser API.

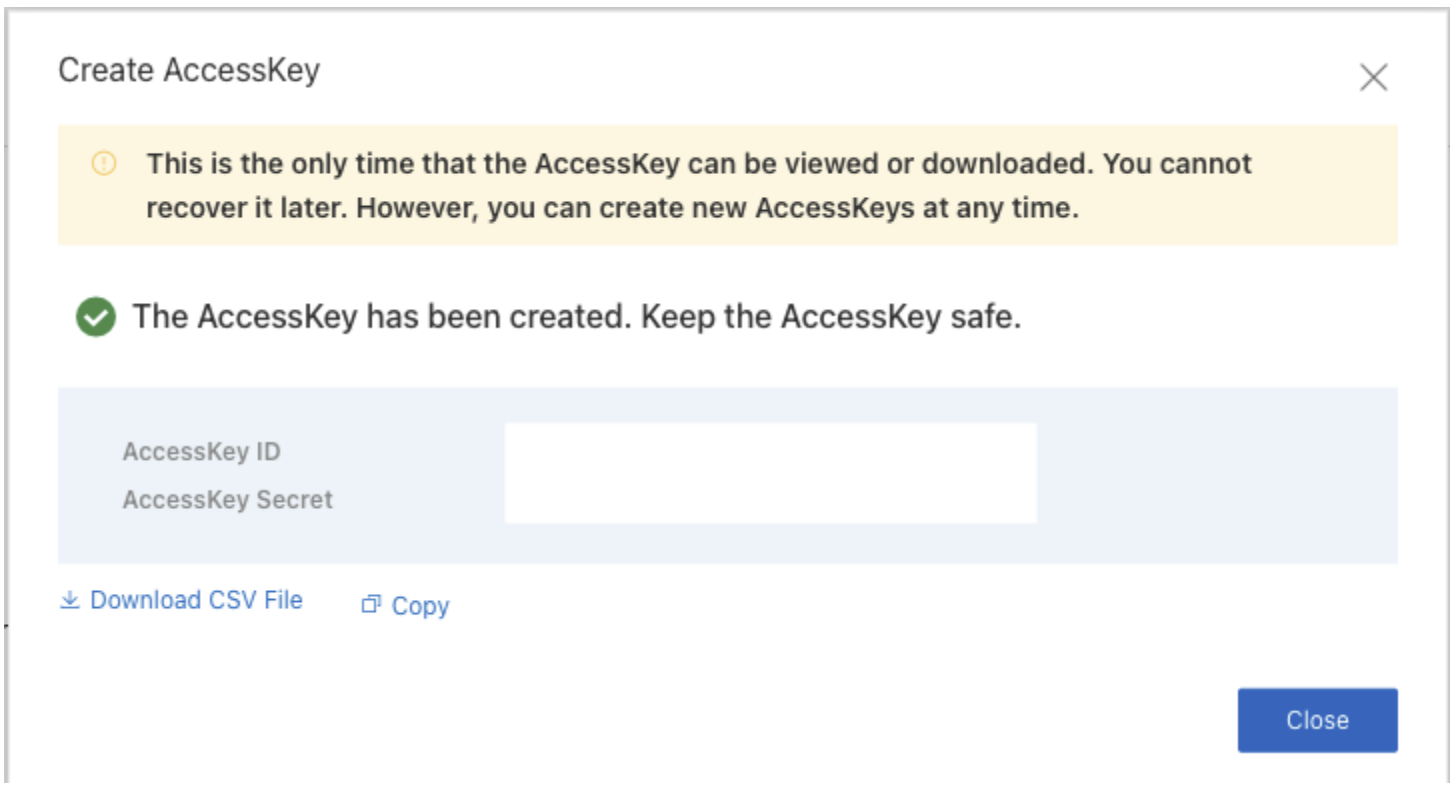
Action: AttachPolicyToUser
PolicyName: ReadOnlyAccess
PolicyType: System
UserName: the target RAM user name

STEP 4: Generate Your AccessKey Pair. (optional)

Go to RAM Console > Identities > Users > Choose the user you created for General Collector.
Click **`Create AccessKey`** in the *Authentication* tap.



You will receive *Create AccessKey popup*, and click **`Copy`** below the blue box to copy your ***AccessKey Pair*** information. Click **`Close`** to close the popup window.



5 - Inventory

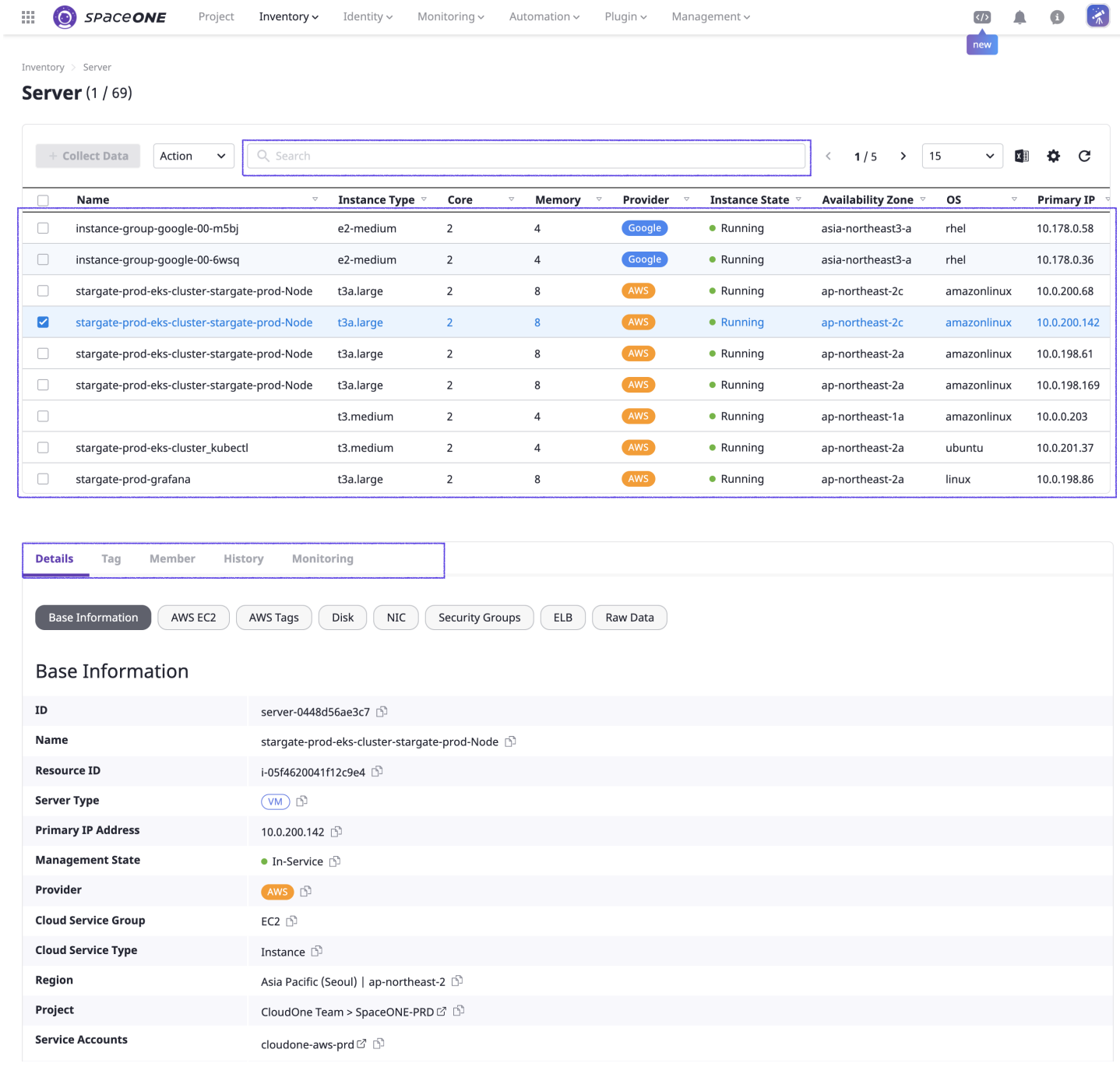
About Inventory

5.1 - Server

Managing server resources

Overview

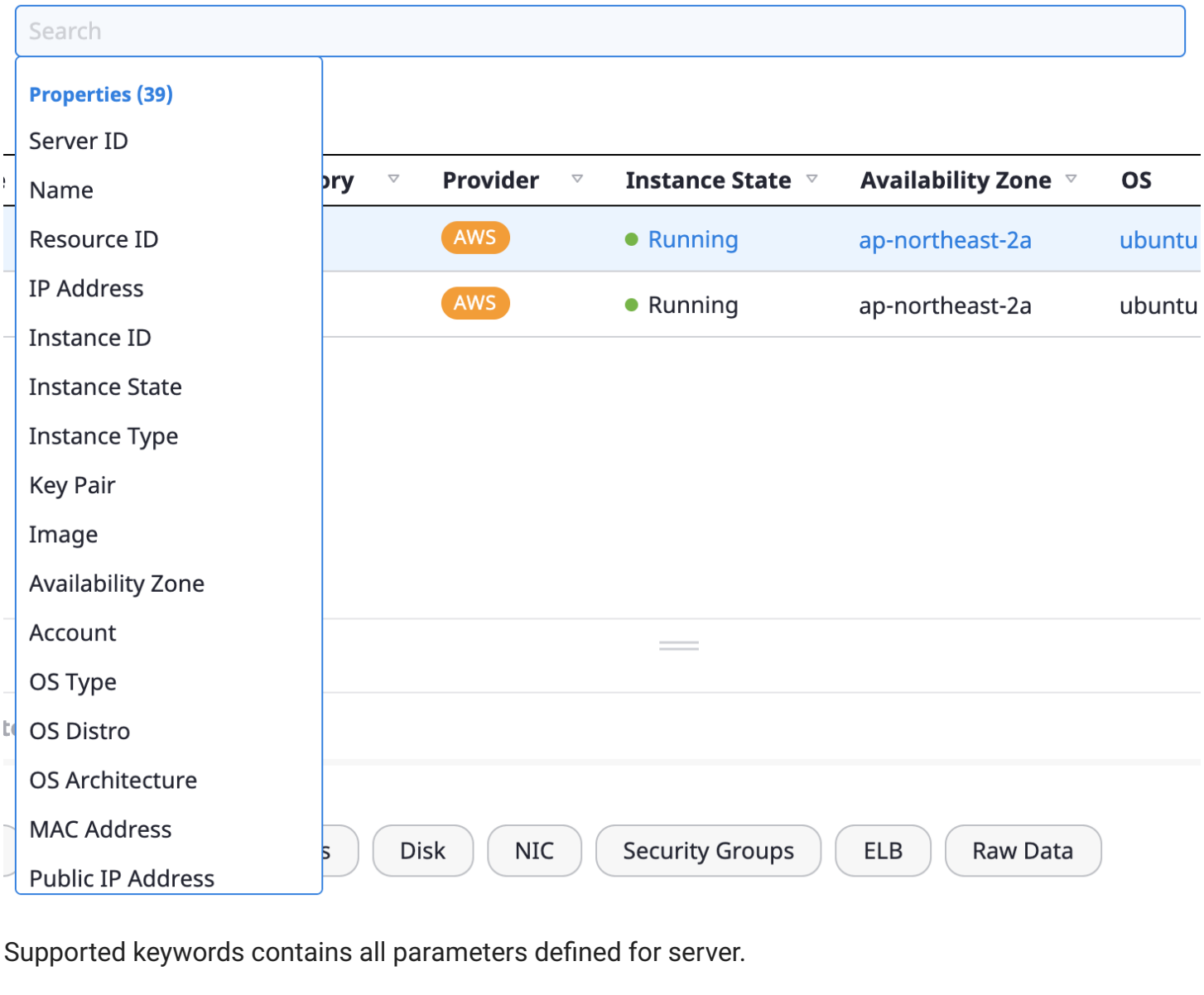
You can integrate server resources scattered by various regions or projects.
Through this page, Users can easily check detail status of servers without login to cloud console repeatedly nor connect to terminal.



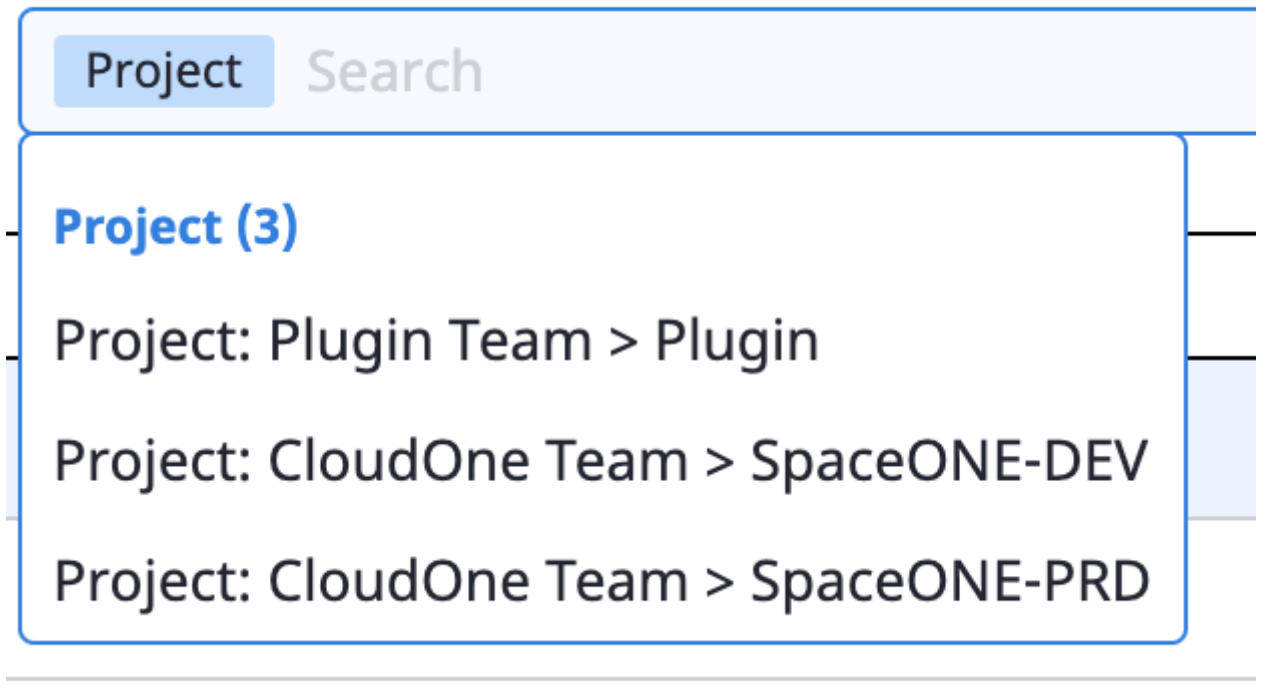
Server page is consist of several functions.
Search Bar : Easy to search servers by query.
Server List : Full list of servers that meet the conditions.
Detailed Status Tab : Checking detailed informations for each server.

Search Bar

User can query server easily by suggested keywords.
SpaceONE classify automatically based on major keywords. This allows users to conveniently search through the collected information.



Supported keywords contains all parameters defined for server.



Server list

Server information collected based on multi clouds.

Name	Instance Type	Core	Memory	Provider	Instance State	Availability Zone	OS	Primary IP	Public IP
windows-personal	t2.micro	1	1	AWS	Stopped	ap-northeast-2c	windows	172.31.47.107	3.36.6.28

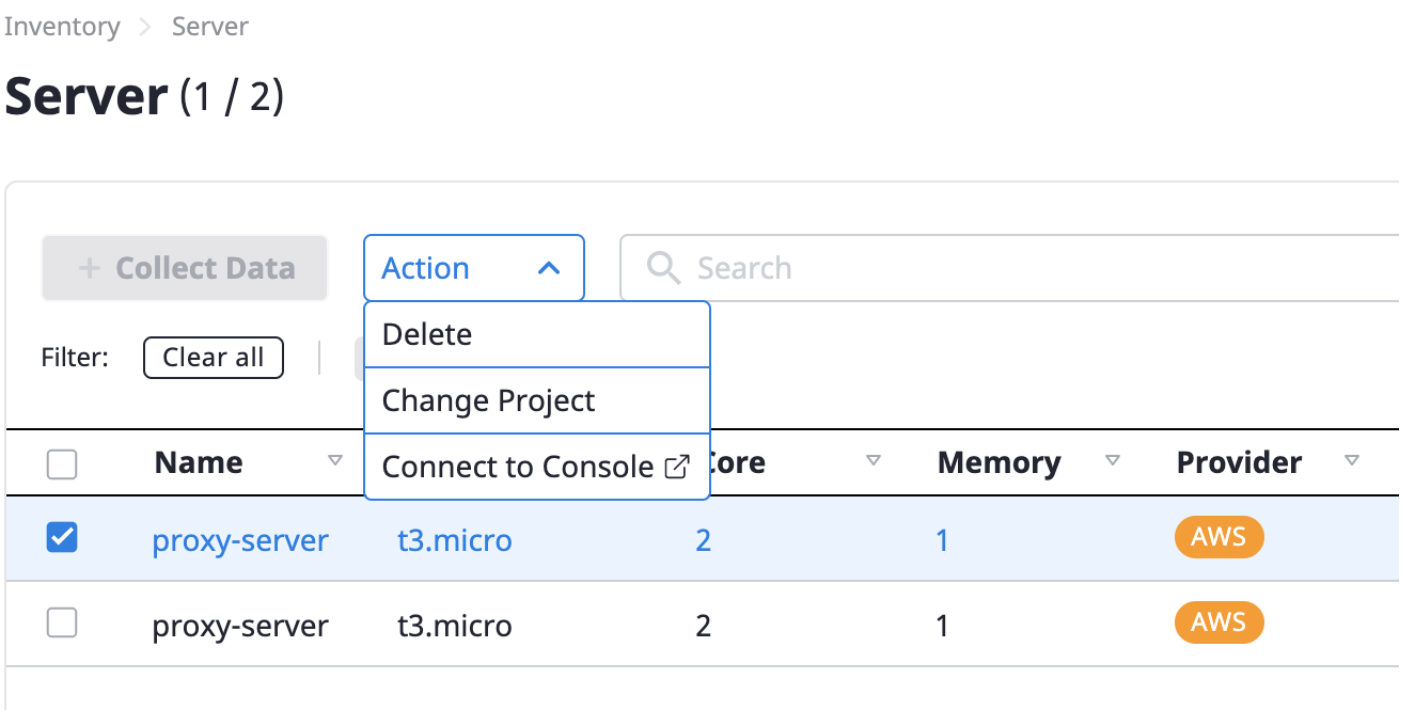
List of supported information is as follows.

Item	Description
Name	Name of server. This refer to name tag parameter supported by each cloud provider
Instance Type	Describes server specification. This refer to specific name provided each clouds compute services.
Core/Memory	Core/Memory(GB).
Provider	Cloud Provider (aws, azure, gcp, openstack, vmware, etc...)

Item	Description
Instance State	Power status of server. Each status refers to definitions of each cloud providers. (Running/ Stopped)
Availability Zone	Server region name
OS	Server OS type(ubuntu/amazonlinux/centos/win2018/etc..)
Primary IP	System used when it originates traffic to the default route
Public IP	Attached public ip to instance(AWS EIP).
Account ID	Root account id
Project	Name of project
Collection State	Collecting status by collectors(ACTIVE/DISCONNECTED). Indicates whether collecting information of target server is ok Disconnected status shows not available to collect. The persistence of 'Disconnected' is considered deletion of server(Delete from server list)
Last Collected	Latest timestamp of collectors

Action

By clicking ***Action*** button after selection of server, you can manage server status.



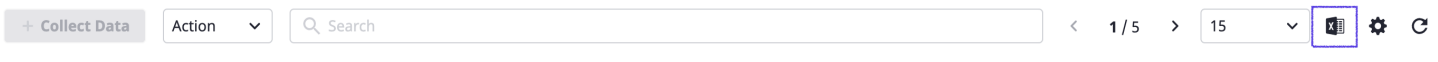
Delete : Remove from server list. Server will not be deleted physically. They will be added after re-collected by collectors.

Change Project : Change project which server is belong to.

Connect to Console : Link to AWS Console.

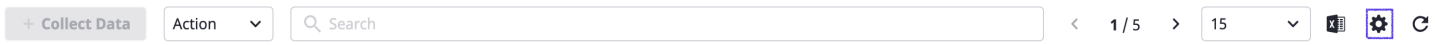
Export

All information within tables will be exported (Excel format).



Custom Table

You can personalize the fields that you want to display in the Resource List table.



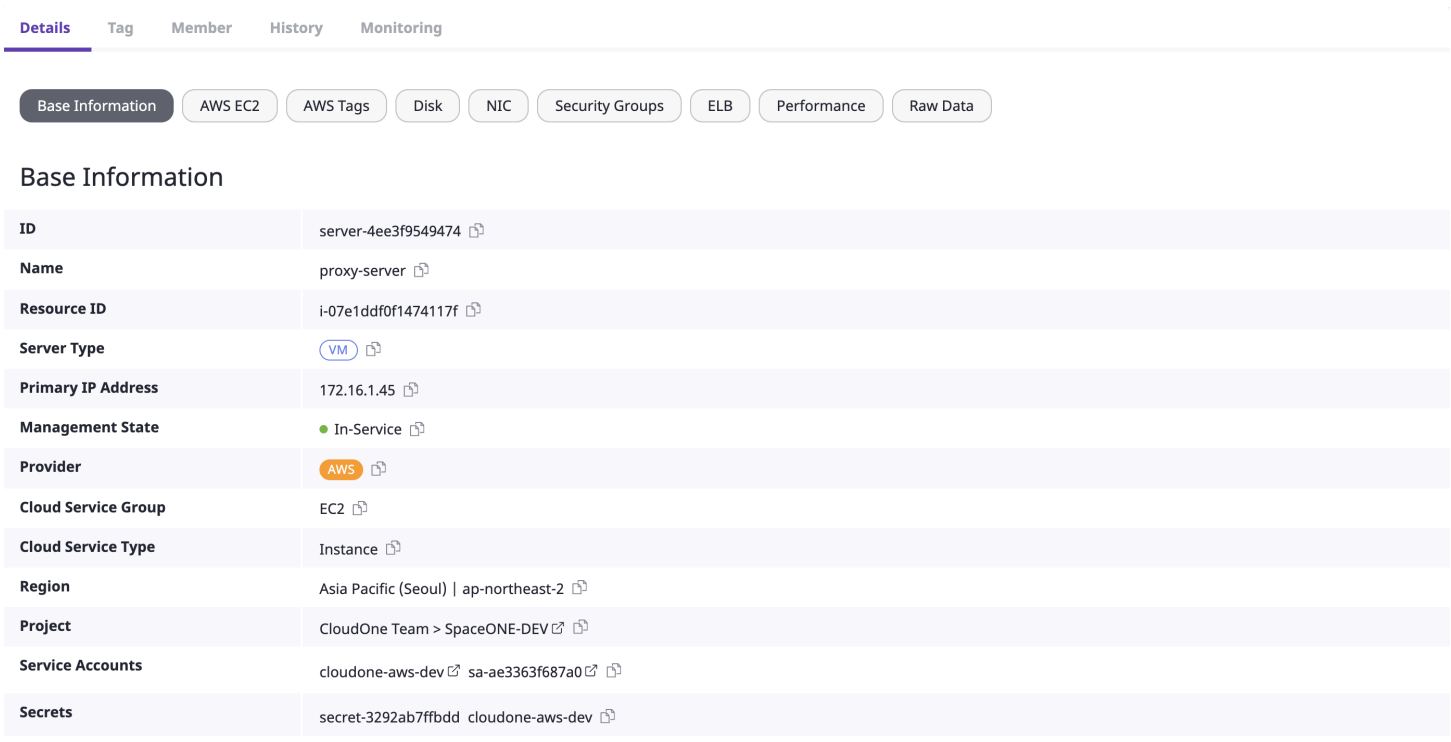
You can check details of Cumstom Table here. Custom Table Details.

Tab

Provides detailed information about the server. They are consists of tabs below.

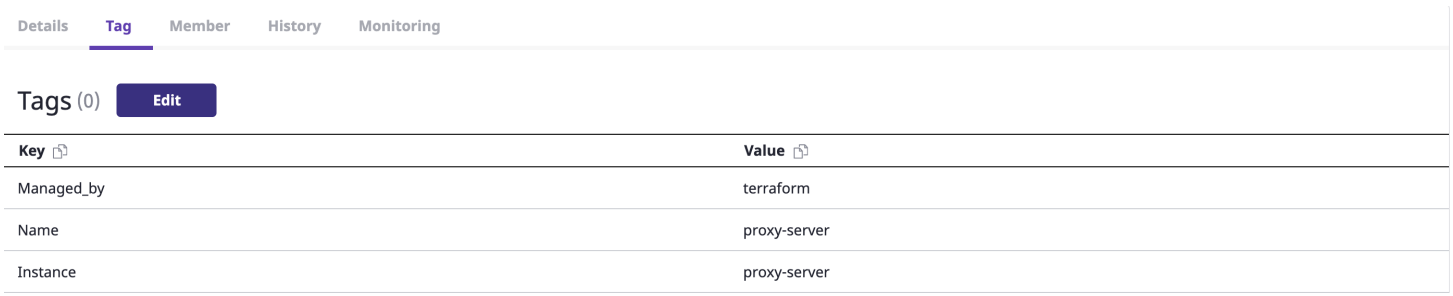
Details

Additional information provided(Machine image, Security group, etc..)



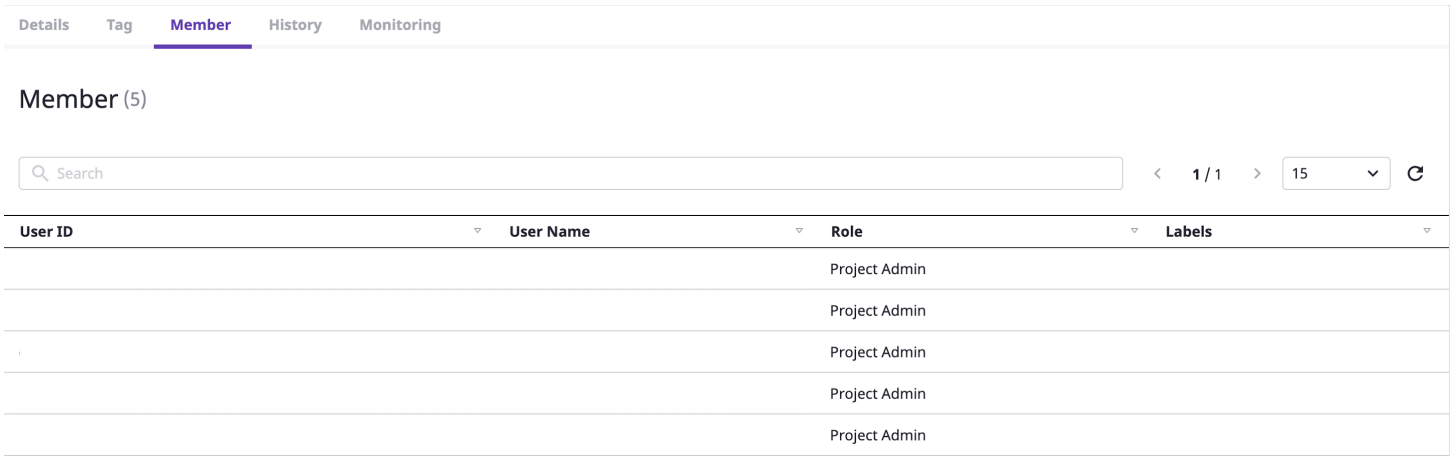
Tag

Grouping servers by tagging.



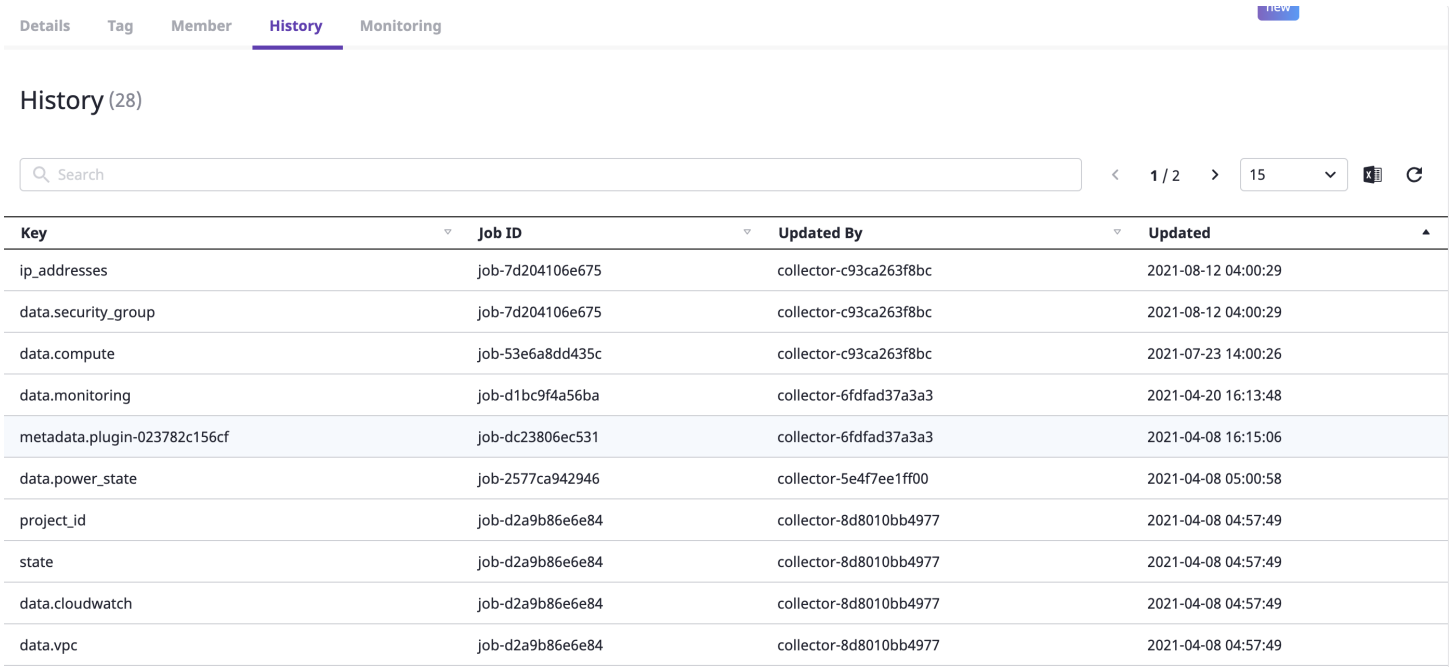
Member

List of server managers.



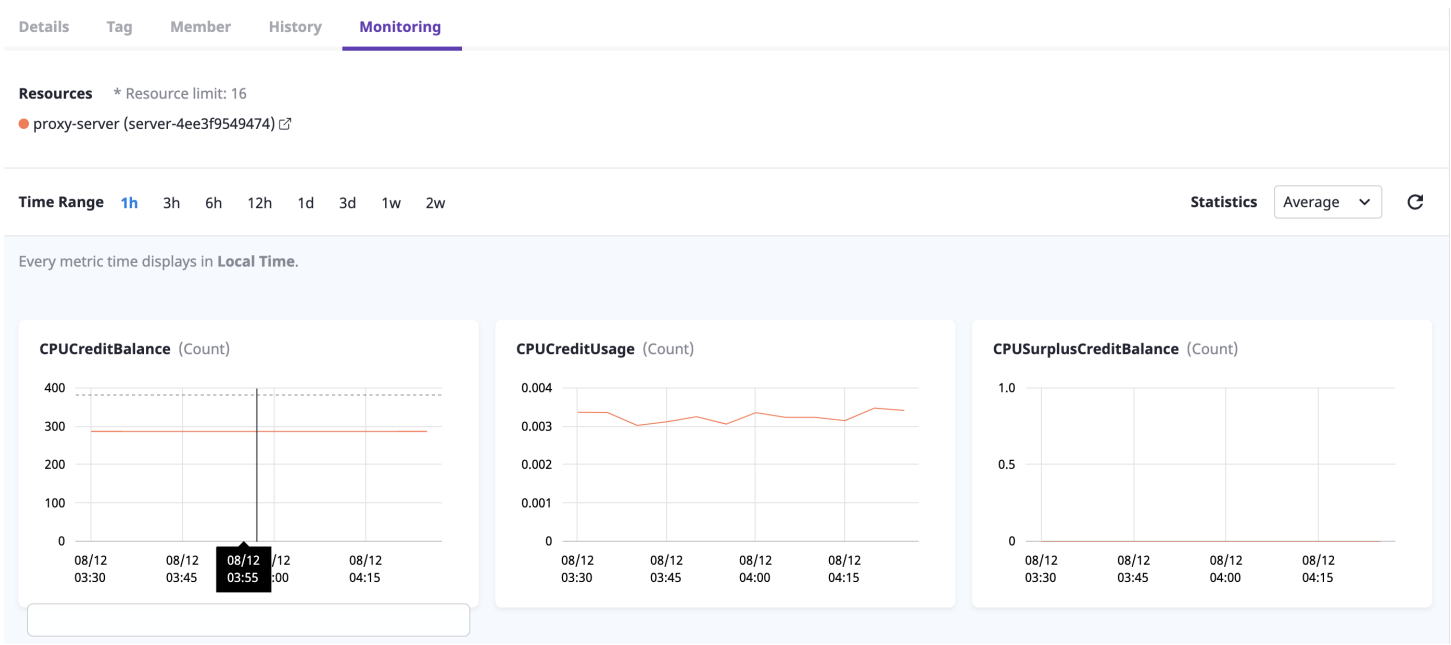
History

History of resources collected.



Monitoring

Monitoring metric informations provided by external monitoring sources(CloudWatch, Azure Monitor, StackDriver..).

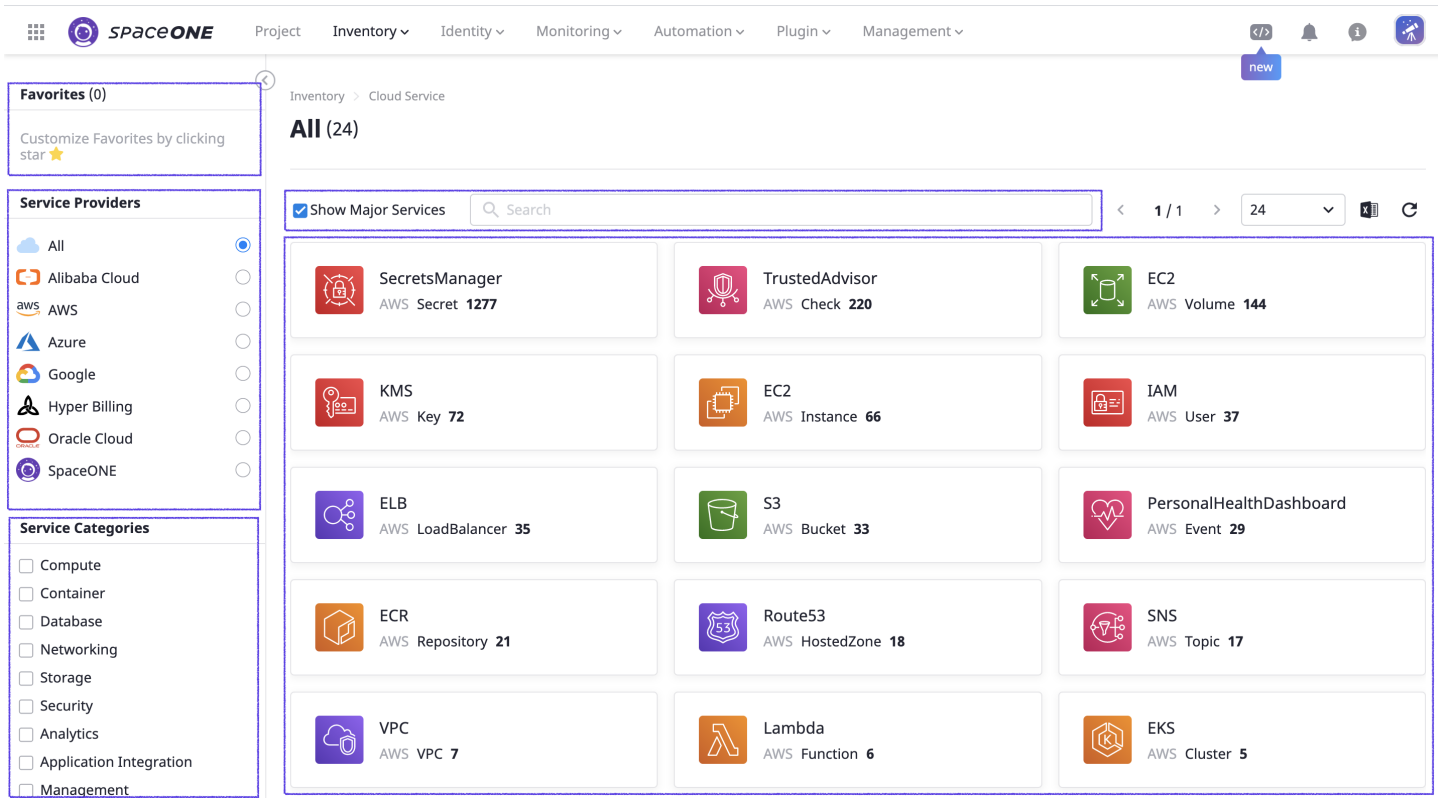


5.2 - CloudService

Overall cloud resources

Overview

Using various plugins in SpaceONE marketplace, Many cloud resources can be managed conveniently.



CloudService page is consist of several functions.
Favorites : Add Favorites for easy access.

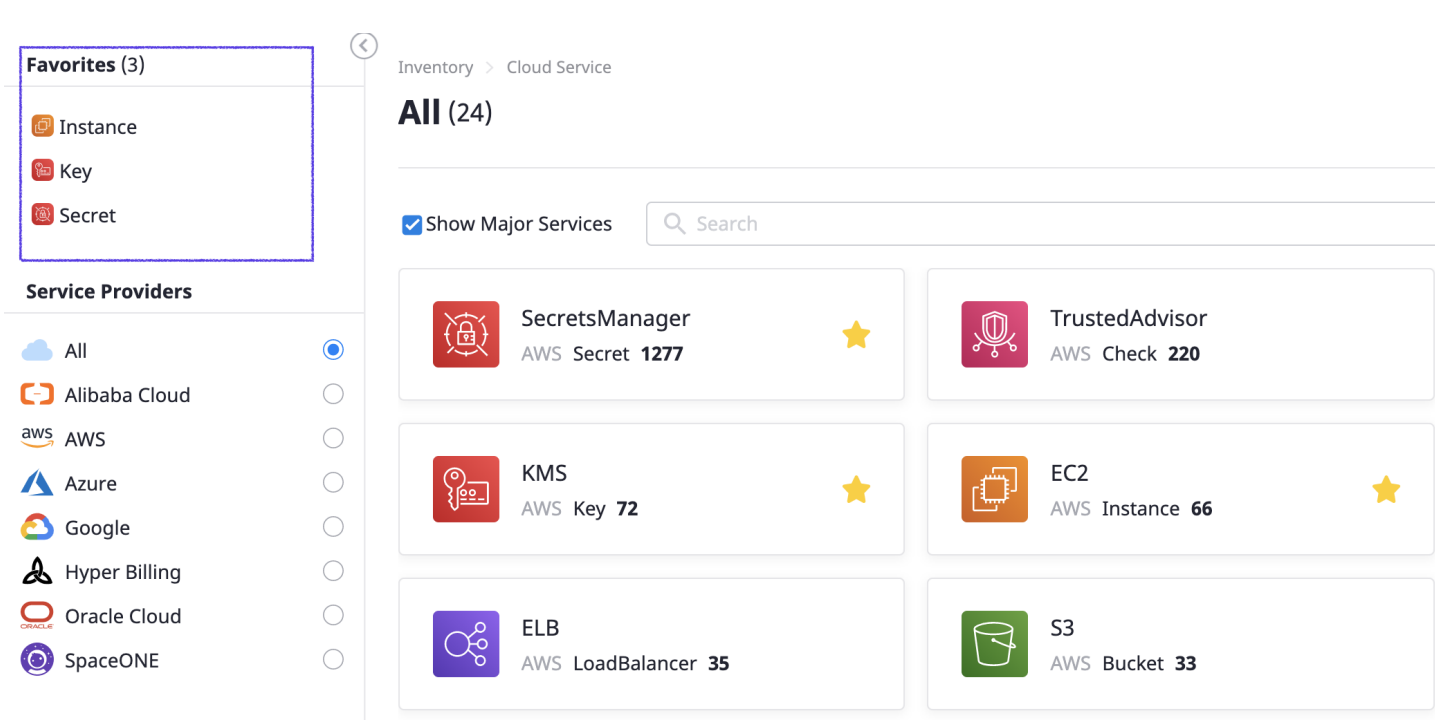
Filters : You can check the results through various filterings.

Search Bar : Search resources.

Cloud Resource list : You can check collected cloud resources.

Favorites

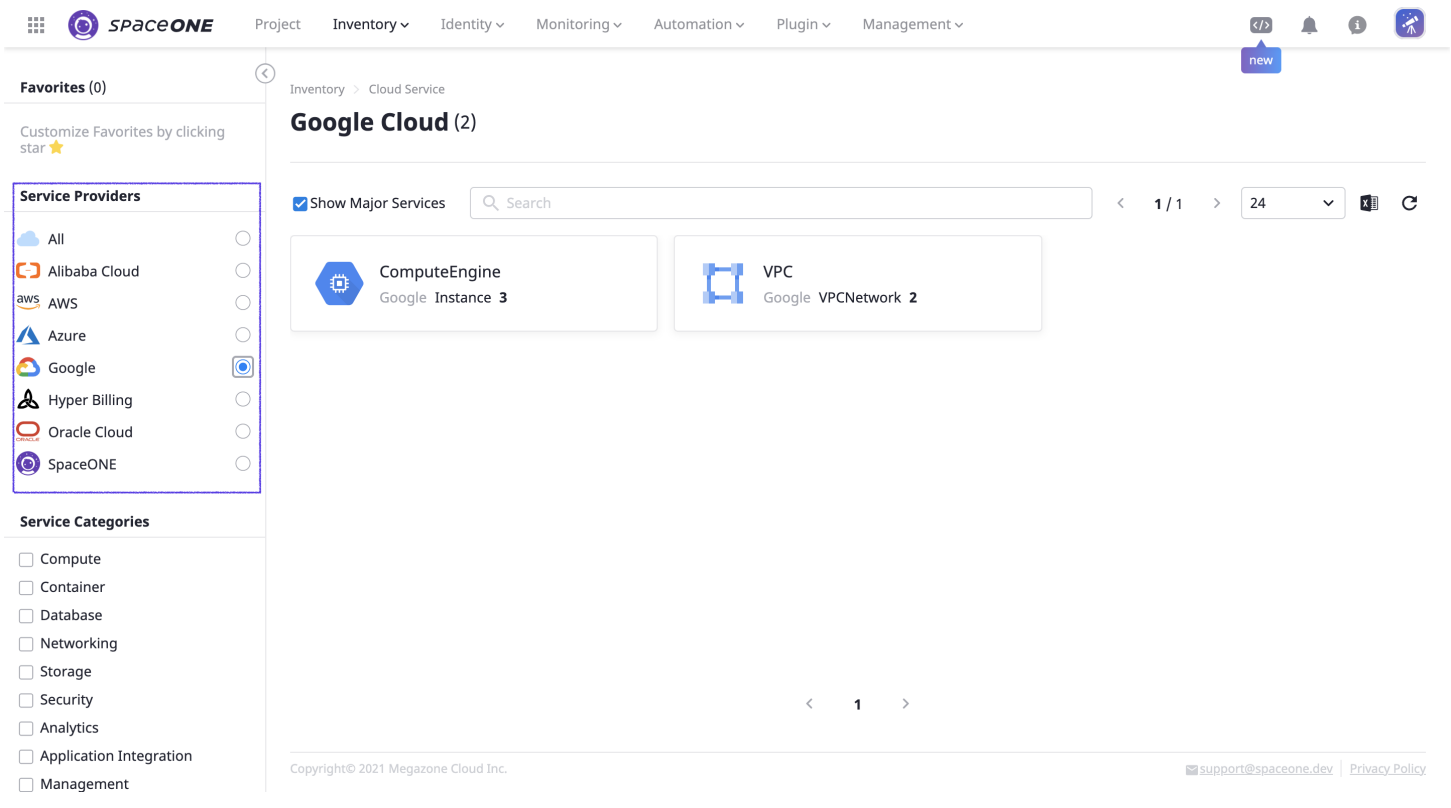
You can see favorite lists on the top left, and access it easily from the spaceONE main page.



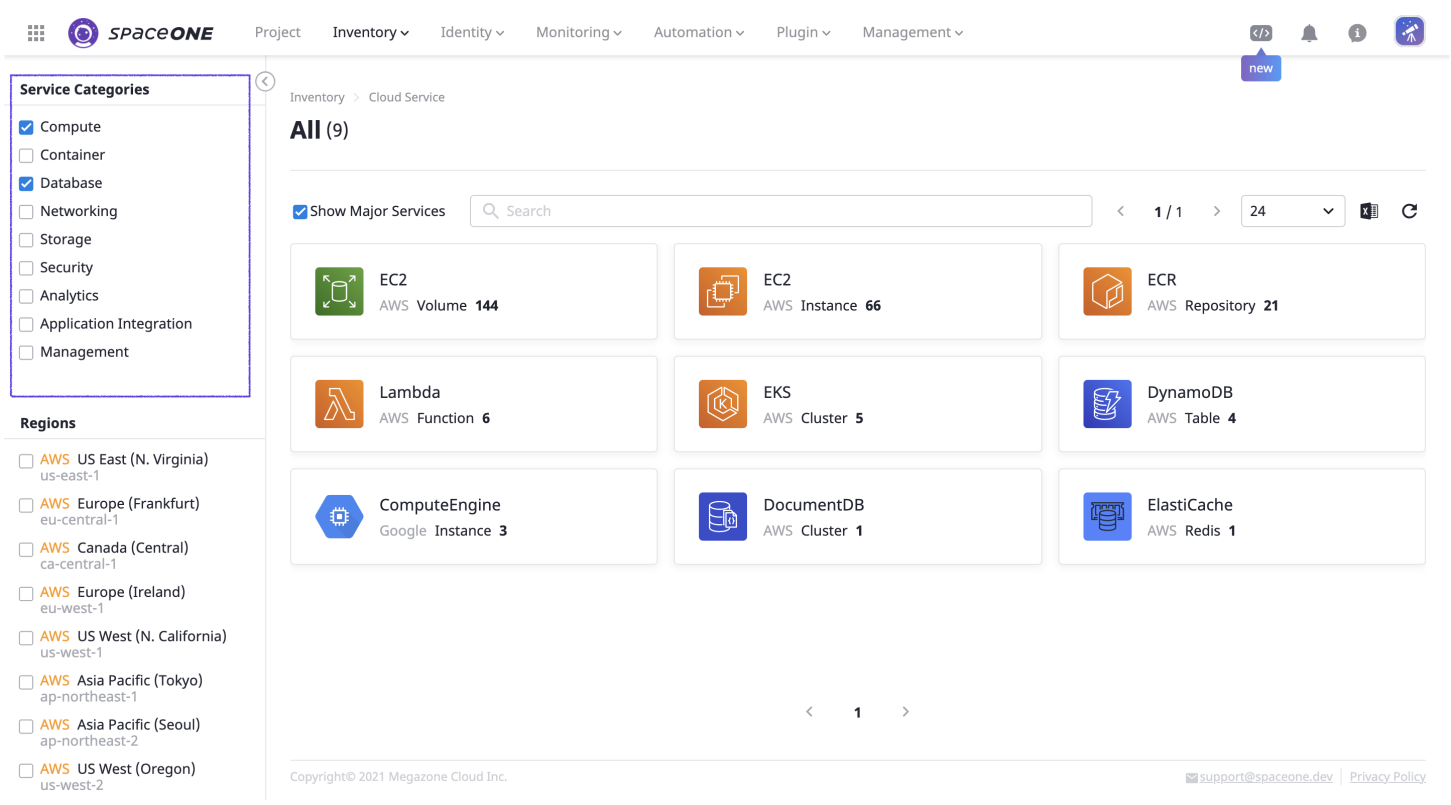
Filters

You can check the results through various filterings (Service Provider, Category , Region).

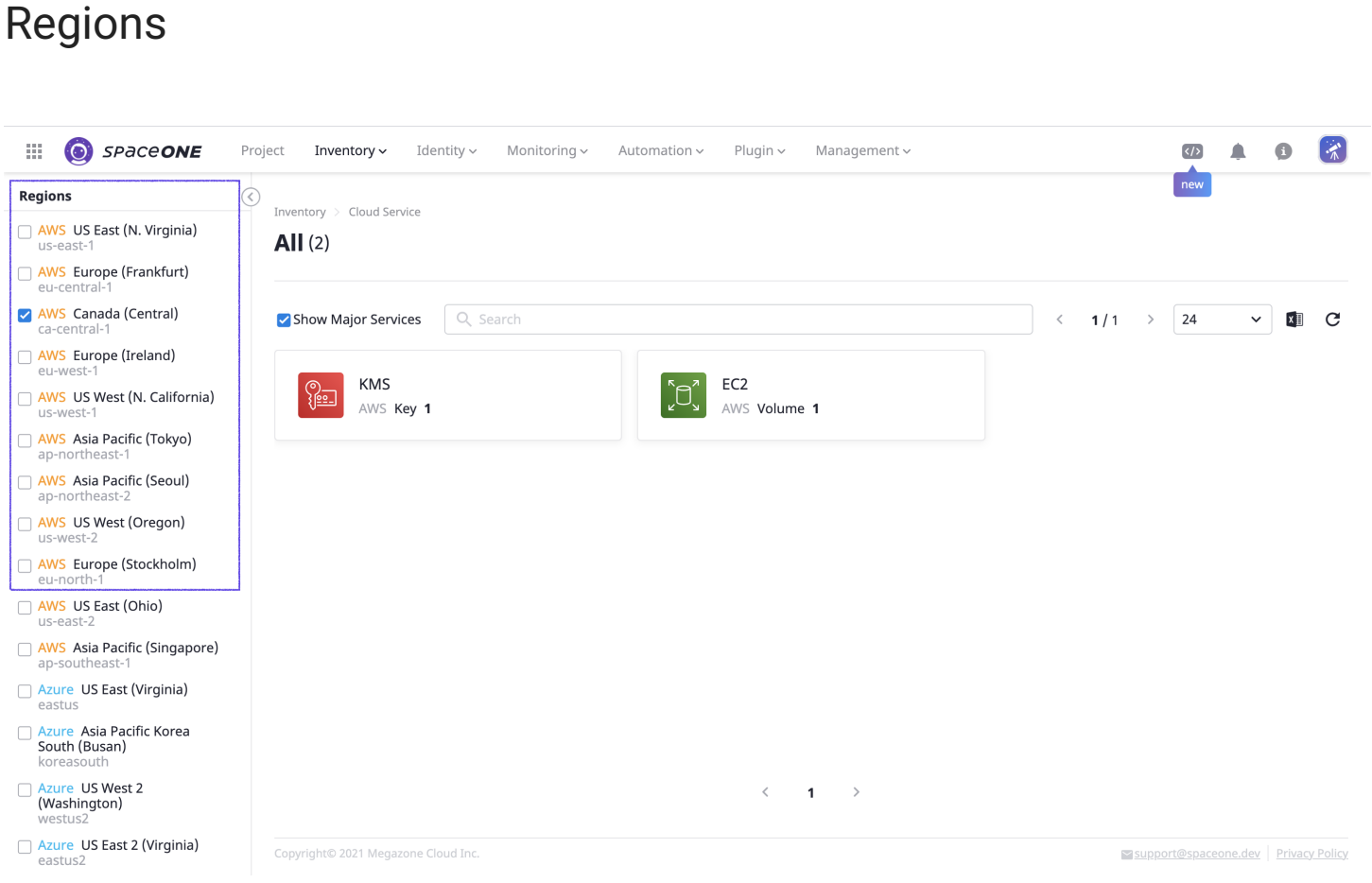
Service Providers



Service Categories

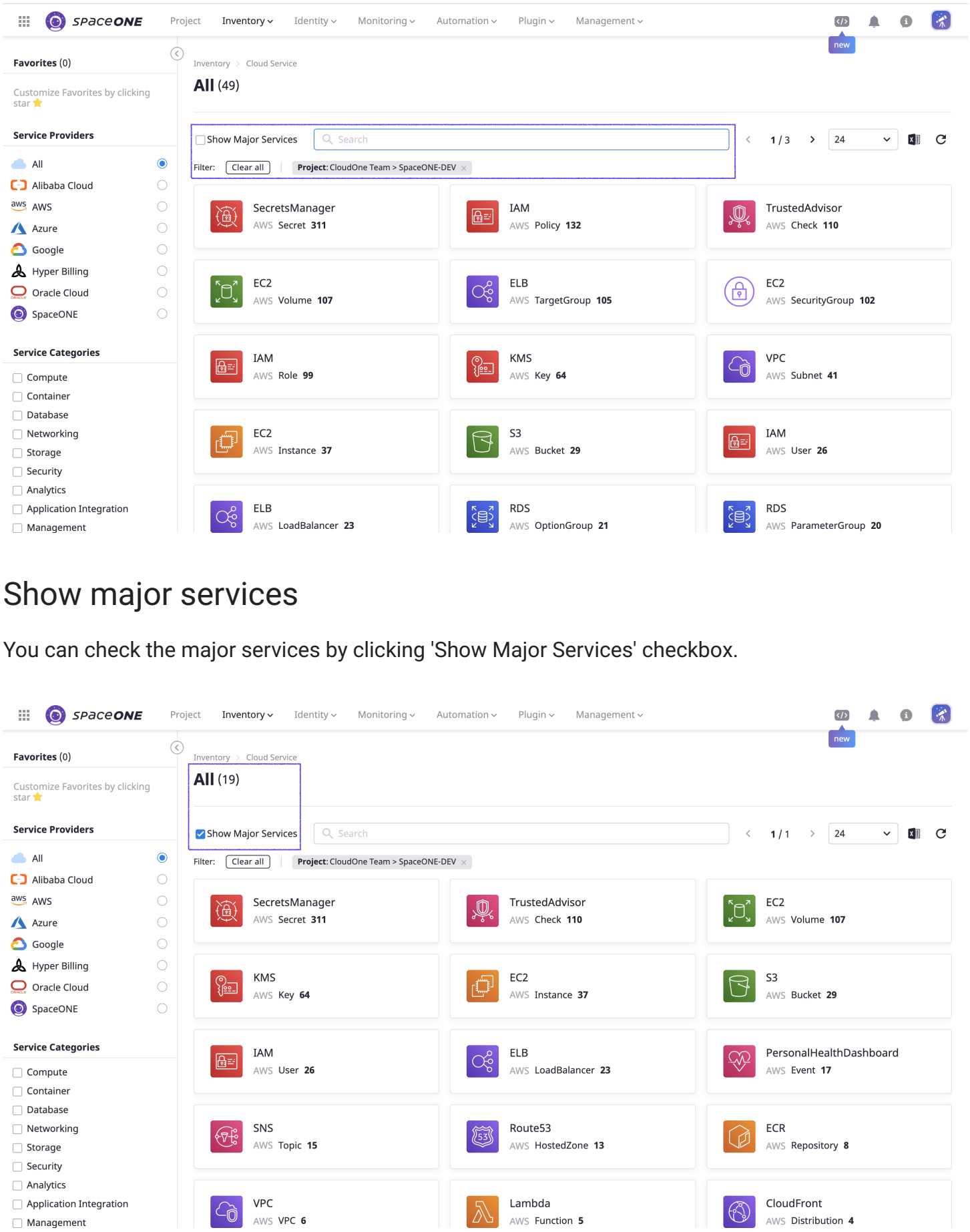


Regions



Search Bar

User can search resources they need using keywords.
By combination of keywords, resources can be searched by service type/group/projects/accounts/secret.

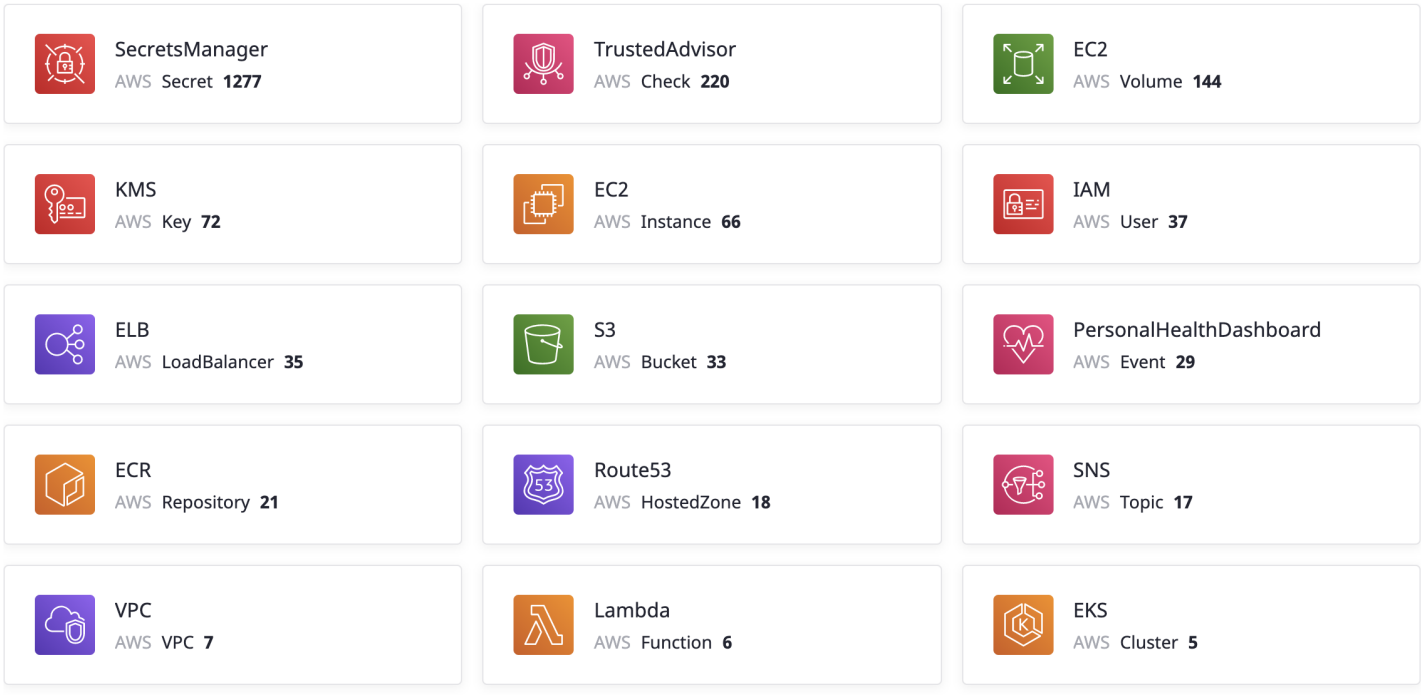


Show major services

You can check the major services by clicking 'Show Major Services' checkbox.

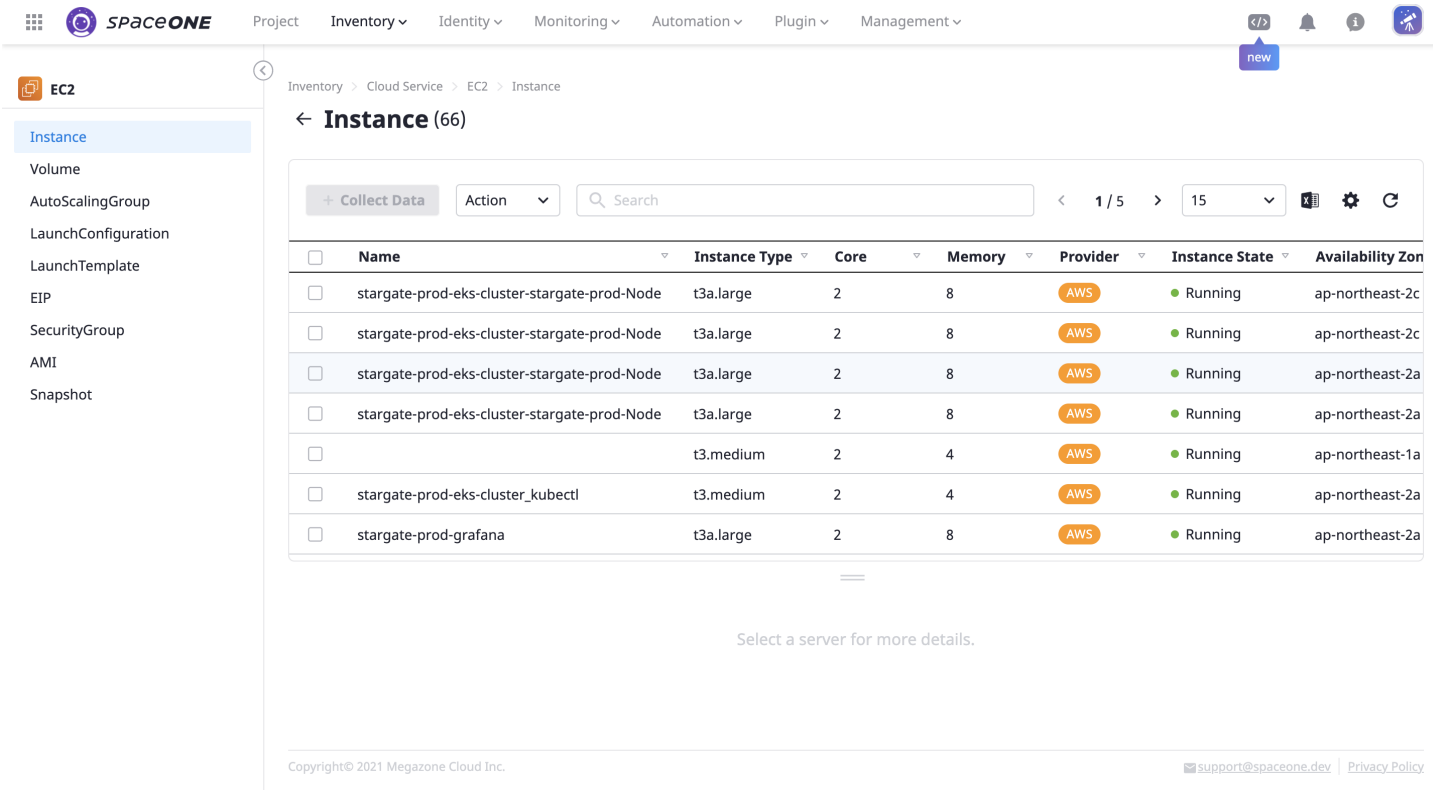
Cloud Resource List

Total list of collected cloud resources.
User can navigate to detailed page by clicking each cloud resources.



Detailed Status

User can check detailed informations of each cloud resource.
Relative information by each cloud resources can be viewed in one screen.

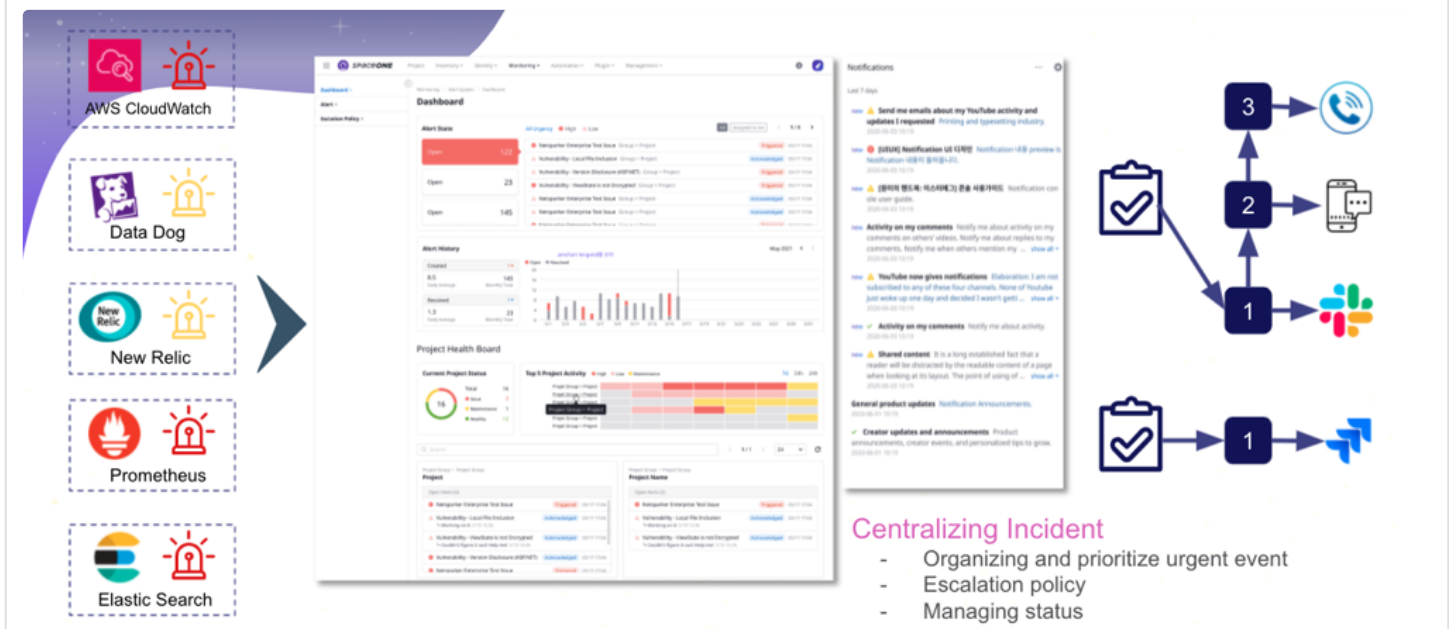


6 - Monitoring

SpaceONE Monitoring Service

About Alert Manager

SpaceONE의 Alert Manager는 다양한 모니터링 시스템에서 발생하는 다양한 패턴의 Event(혹은 Incident) 를 통합 관리할 수 있는 Tool 입니다.



Monitoring Webhook Plugin 에 의해 체계적으로 Filter된 Event message를 ***Alert*** 라고 합니다. Alert Manager를 통해 ***Alert*** 이 발생하여 종료되기까지의 모든 과정을 체계적으로 관리할 수 있습니다.

How It Works

용어 정의

Alert Manager에서 주로 사용하는 용어를 정리 합니다.

용어	설명
Event/Incident	외부의 모니터링 Tool(AWS SNS, Zabbix, DataDog 등..)에서 발생되는 다양한 패턴의 메시지 입니다. 인프라 및 어플리케이션에서 감지된 다양한 정보들을 포함 합니다.
Alert	SpaceONE의 다양한 Monitoring Webhook Plugin에 의해 필터링 되어 체계적으로 정리된 Event Message 입니다.
Alarm	SpaceONE의 Notification 서비스를 통해 발송되는 다양한 안내 메시지 입니다. 상세한 설명은 Notification 서비스 소개 를 참고해주세요.

6.1 - Alert Manager

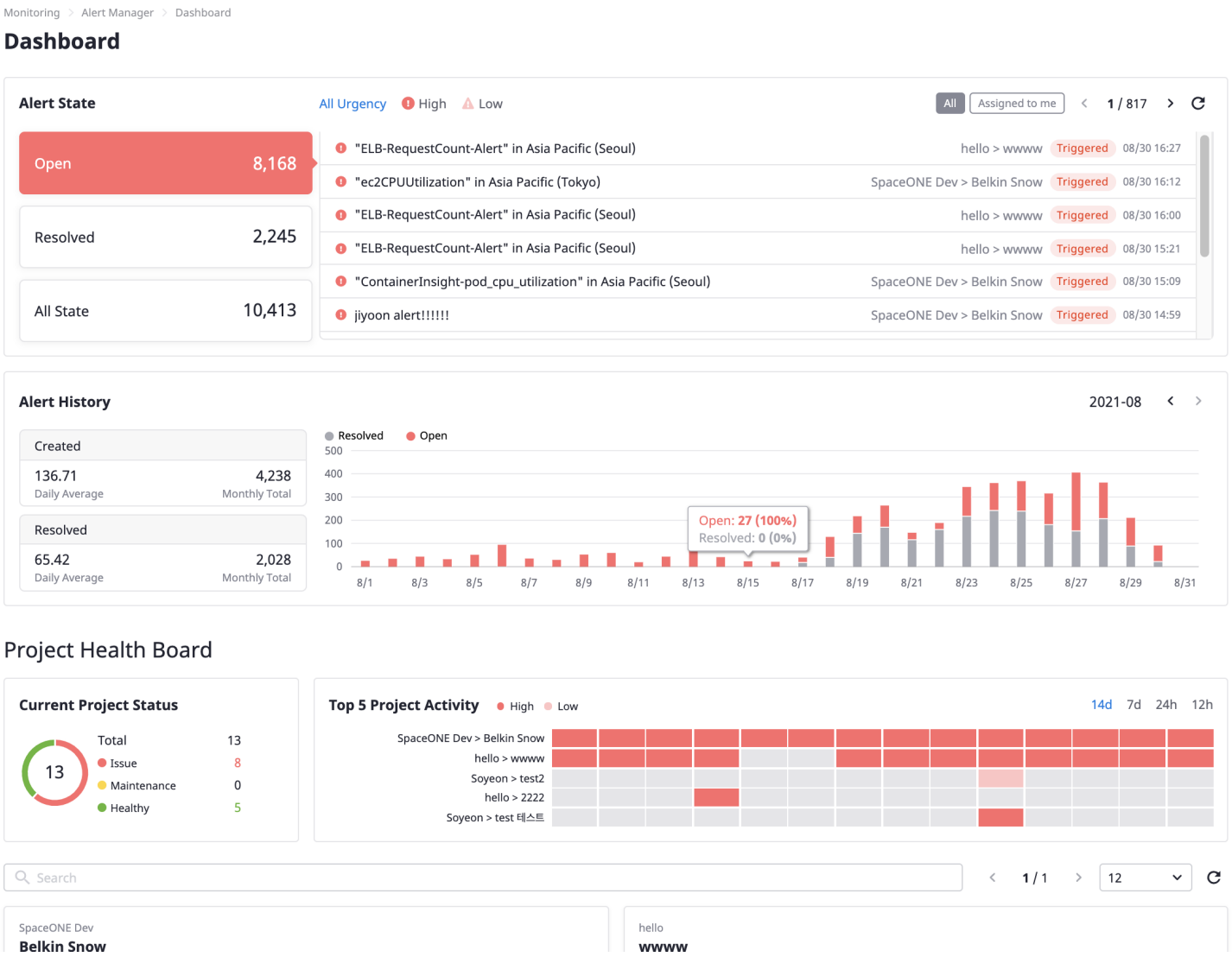
Monitoring Service

6.1.1 - Dashboard

Monitoring Service

Overview

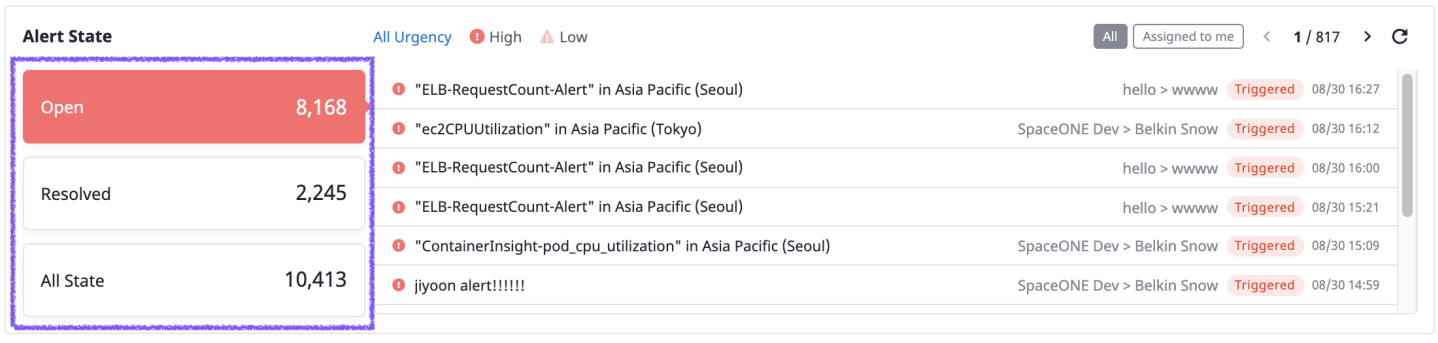
Alert Dashboard를 통해 수신된 모든 Alert의 현황을 한눈에 확인할 수 있습니다.



Dashboard

Alert State

전체 Alert 상태를 ***Open(Triggered, Acknowledge 포함)***, ***Resolved***, ***All State*** 로 구분하여 확인 가능 합니다.

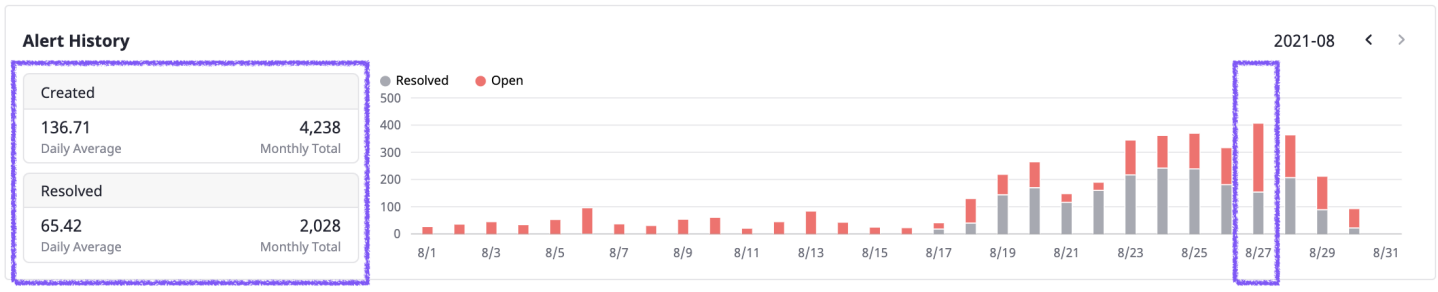


Urgency Type별로 Filter를 적용할 수 있습니다. 적용 가능한 Urgency Filter는 총 3가지(***`All, High, Low`***) 입니다.

Assigned to me 버튼을 클릭시 담당자가 **_나_**로 지정된 Alert만을 조회할 수 있습니다.

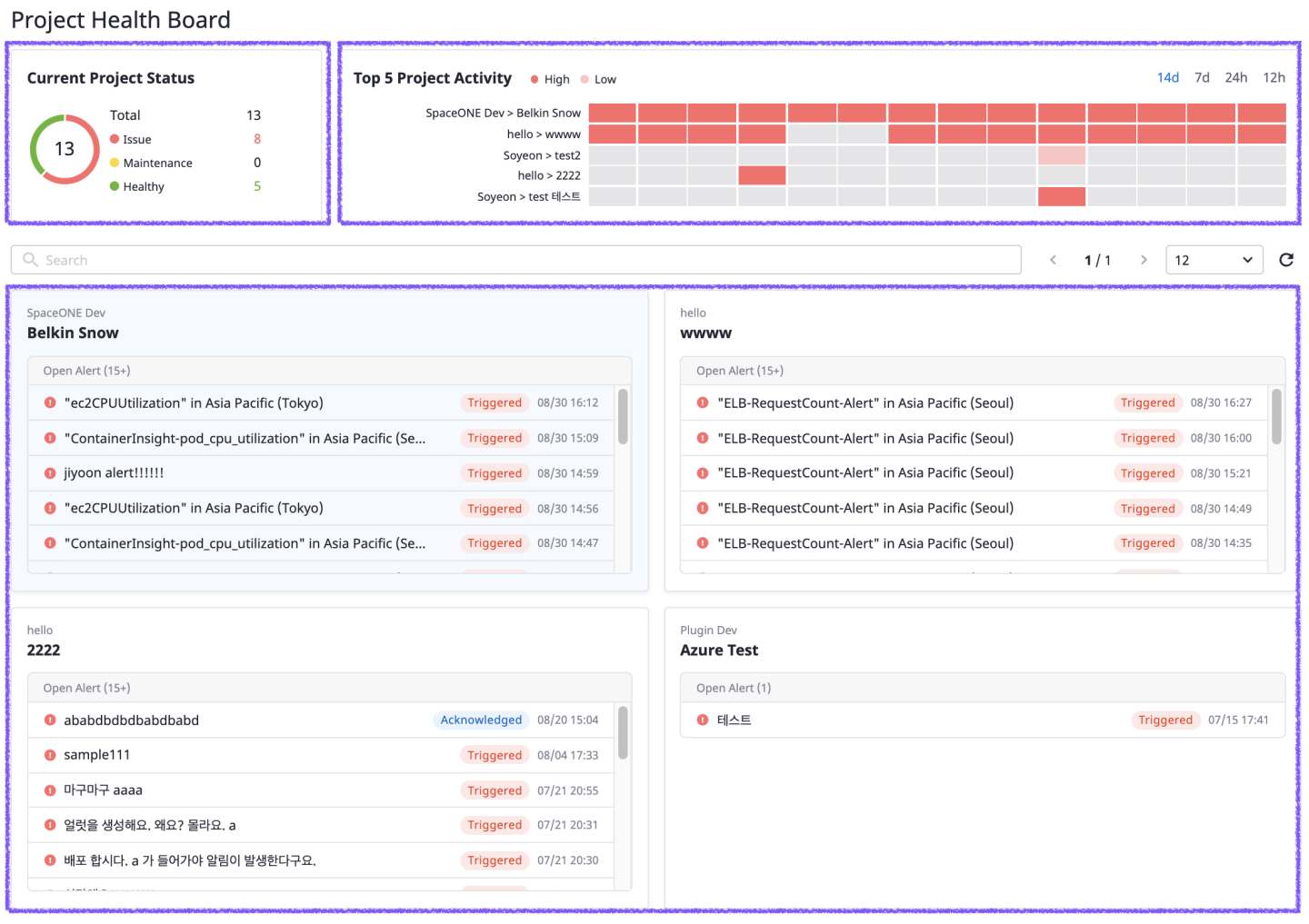
Alert History

전체 Alert 통계를 확인할 수 있습니다. 생성되고 완료된 Alert 통계와 일별 변화량을 확인할 수 있습니다.



Project Health Board

각 프로젝트별 현재 Alert 처리 현황을 확인할 수 있습니다. 전체 Project 중 Alert이 많이 발생한 Top 5 프로젝트를 확인할 수 있습니다. 전체 Project의 Alert를 편리하게 검색하고 상세 내용을 확인할 수 있습니다.

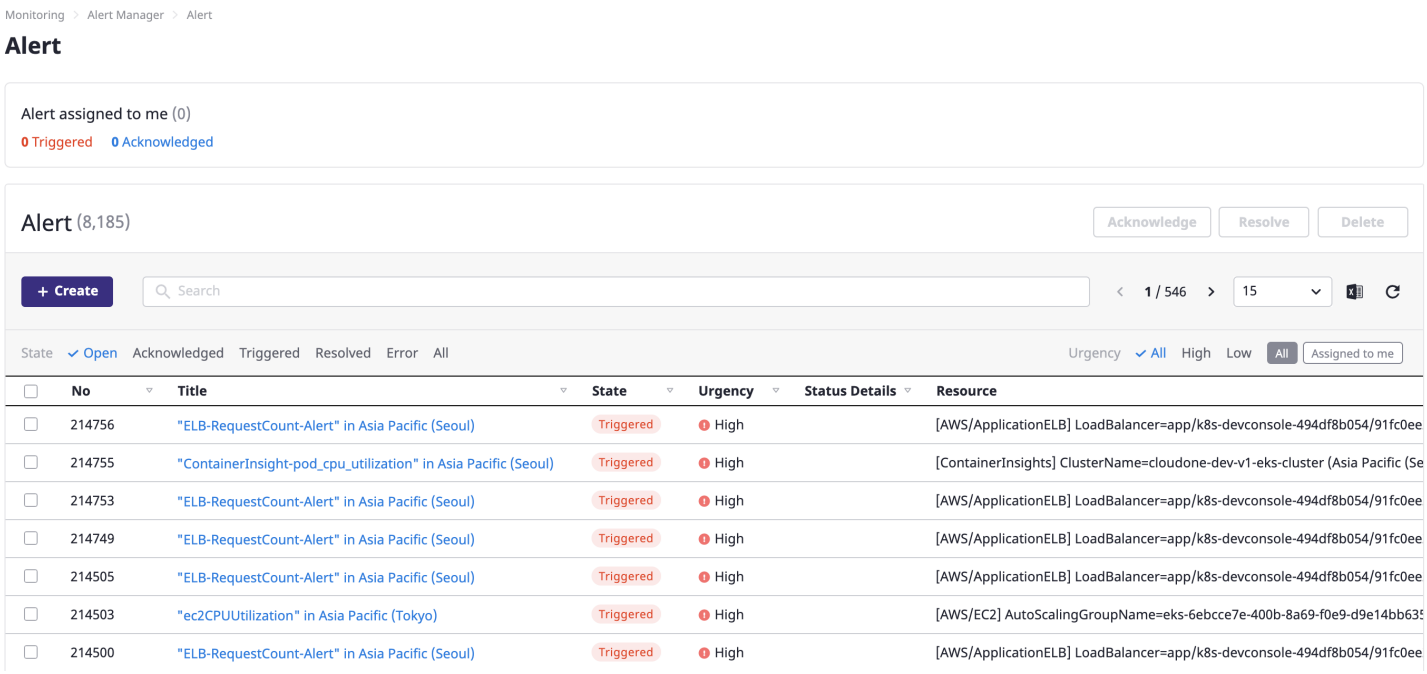


6.1.2 - Alert

Managing alert message for whole domain

Overview

수신된 모든 Alert을 관리할 수 있습니다. 각기 할당된 Role에 따라 관리 가능한 Alert이 구분됩니다. Project Admin Role인 경우, 소속된 Project에서 발생한 Alert List를 관리할 수 있습니다. Domain Admin 이상의 Role인 경우, 도메인 내에서 발생한 모든 Alert를 관리할 수 있습니다.

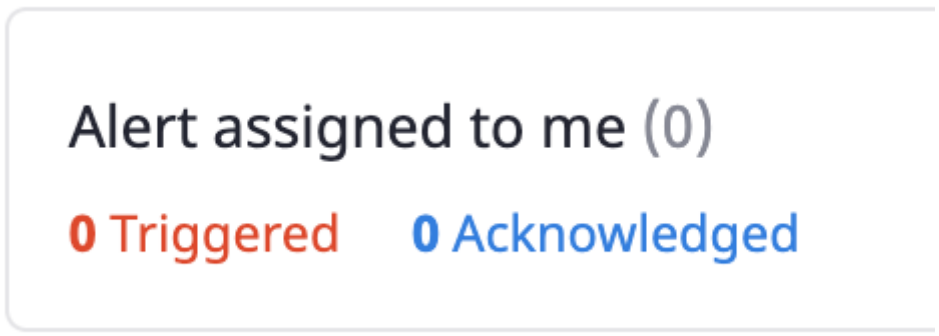


Alert List

Alert 리스트를 다양한 필터를 사용하여 조회할 수 있습니다.

Assigned to me

기본적으로 프로젝트에 수신된 모든 Alert List를 조회할 수 있습니다.
담당자가 ***나***로 직접 지정된 경우, 해당 Alert만 조회 할 수 있습니다.



Using Filters

Alert에 다양한 필터를 적용하여, 효율적인 조회가 가능 합니다.
설정가능한 Filter는 ***`State`*** ***`Urgency`*** 두 종류 입니다.

Alert State

State	설명

State	설명
Open	
Acknowledged	등록된 Alert에 담당자가 할당되어 처리중인 상태
Triggered	Alert이 최초 등록된 상태
Resolved	Alert 등록된 사항이 처리 완료된 상태
Error	Alert이 수신 되었으나, Param 오류 등으로 정상적으로 등록되지 않은 상태
All	모든 Alert 상태

Alert Urgency

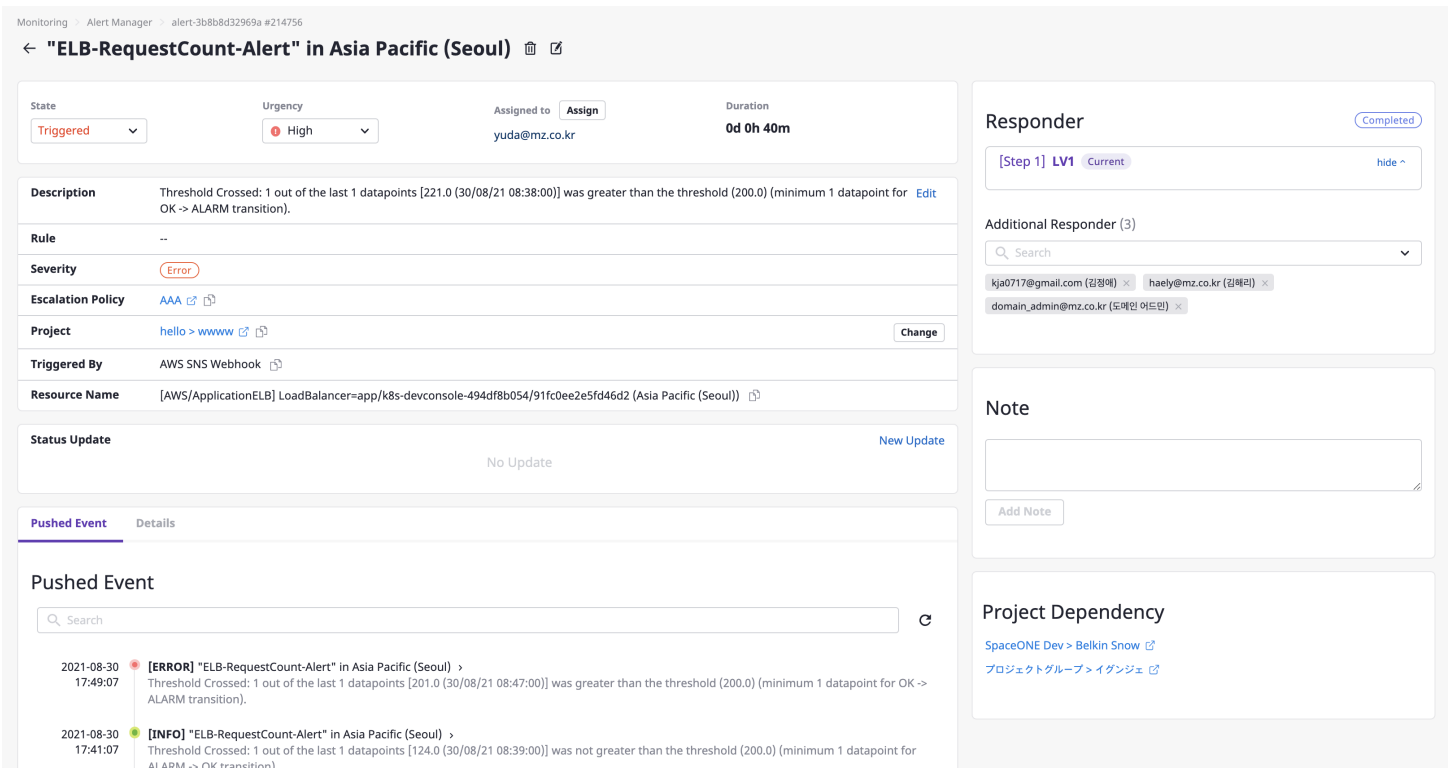
Urgency는 ***All***, ***High***, ***Low*** 로 구분 됩니다.

Export

조회 가능한 모든 Alert List를 ***`Excel Export`*** 가능합니다.

Alert Details

수신된 Alert의 상세 상태를 조회하고 처리 이력을 관리할 수 있습니다.



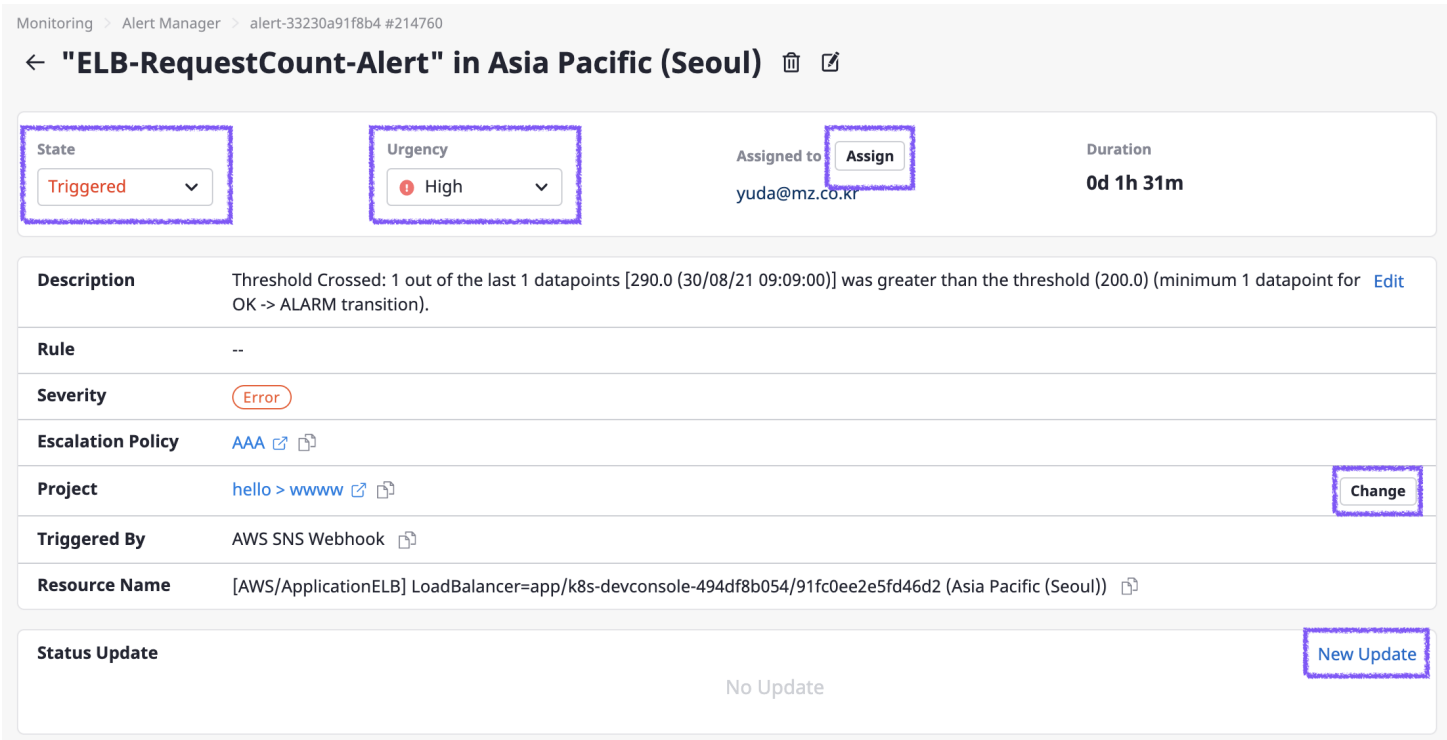
각 상세 항목에 대한 설명은 아래와 같습니다.

상세항목	설명
State	Alert의 진행 상황. ***Triggered***,***Acknowledged***,***Resolved*** 로 표시됩니다.
Urgency	Alert의 긴급도. ***High***, ***Low***
Assigned to	Alert의 담당자.
Duration	Alert이 지속된 시간.
Description	Alert의 기타설명.
Rule	Alert 발생 조건.
Severity	Alert의 심각도, Alert이 발생된 Data Source에서 측정된 기준 입니다.

상세항목	설명
Escalation Policy	적용된 Escalation Policy
Project	Alert이 발생된 Project
Triggered By	Alert를 전송한 모니터링 시스템
Resource Name	Alert 발생 대상

Changing Details

Alert의 담당자는 할당받은 Alert의 상태를 변경하고, 처리 이력을 정리할 수 있습니다.



State

Alert의 상태를 변경 합니다.

Urgency

Alert의 시급도를 변경 합니다.

Assigned to

Alert 처리 담당자를 지정합니다.

Project

Alert이 소속된 Project를 변경 합니다.

Status Update

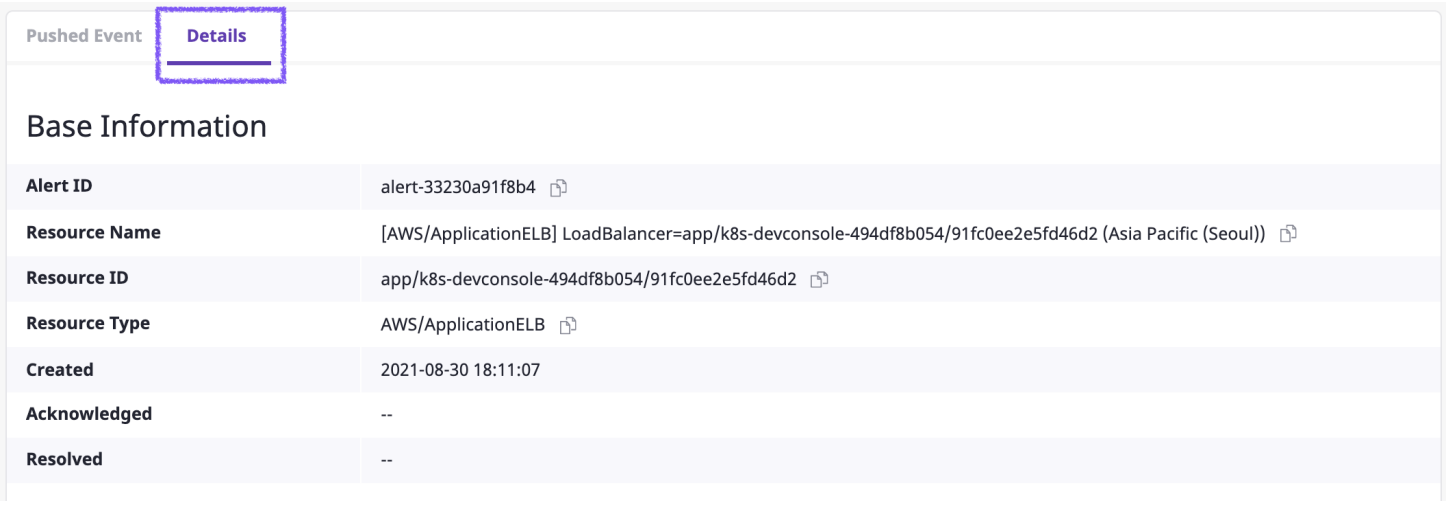
Alert 처리 단계별 진행상황 혹은 변화된 상태가 있는 경우 상세히 기록합니다.

Pushed Event

같은 Event가 중복으로 수신된 경우, Pushed Event에서 시간대별 상세 수신 이력을 확인할 수 있습니다.

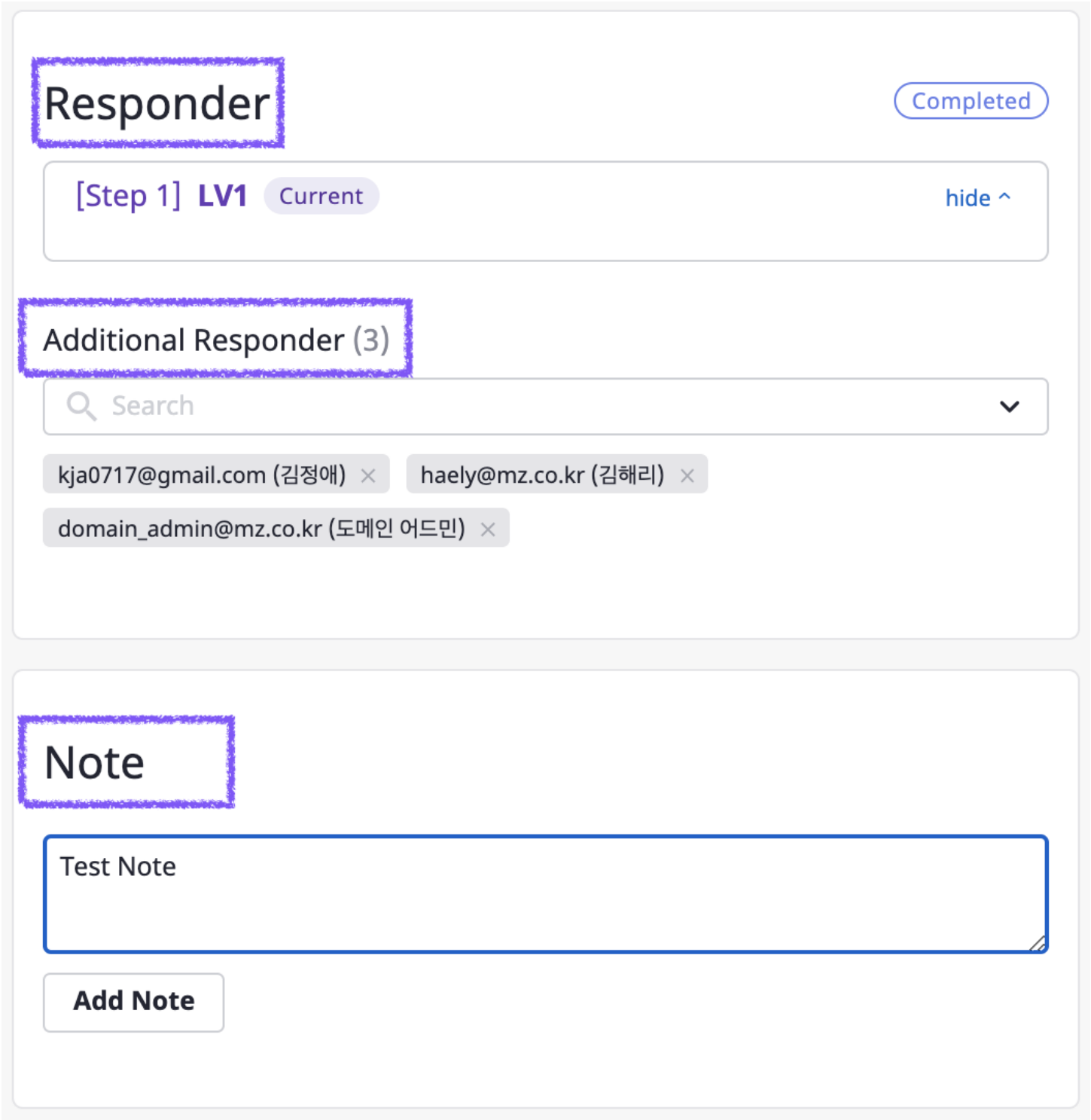
Details

수신된 Event의 원문을 확인할 수 있습니다.



Responder

Alarm을 수신받는 대상을 확인하고, 추가 대상자가 있는 경우 등록 합니다. 기본적으로 Project에 연결된 Escalation Policy에 정의된 Subscriber에게 전달 됩니다.



Additional Responder

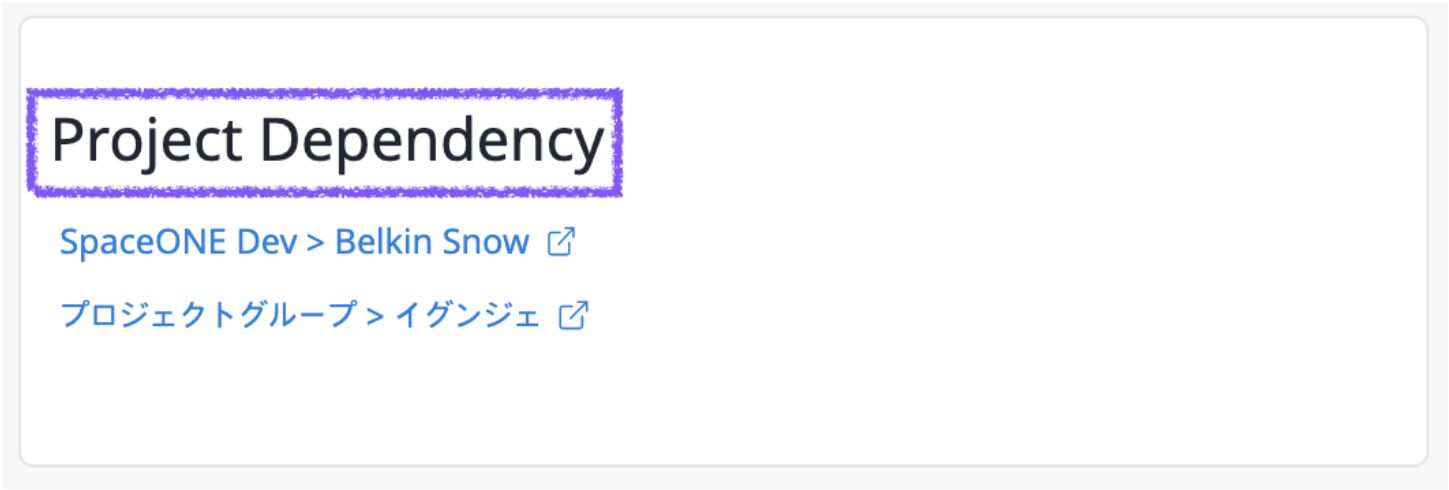
기본 등록된 Escalation Policy의 각 Level별 사용자 이외에 추가 사용자에게 Alert 전파가 필요할 경우 등록할 수 있습니다.

Note

Alert에 대해 구성원들이 Comment를 남겨 처리 중 문의사항과 이에 대한 답변을 등록할 수 있도록 합니다.

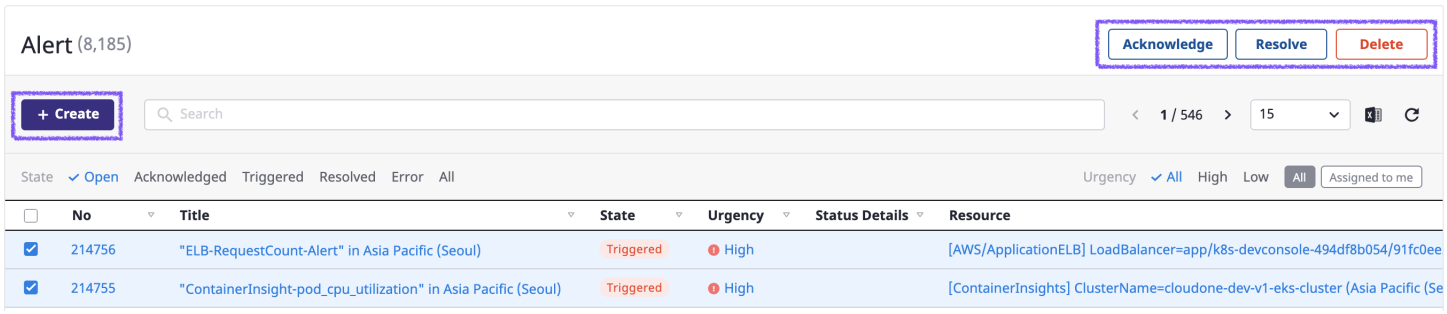
Project Dependency

수신된 Alert이 다른 Project에서도 관리되어야 할 필요가 있을 경우(ex. 장애가 다른 프로젝트에도 연관이 있는 경우) Project간 Dependency 설정이 가능합니다. 이러한 경우, Project A로 수신된 Alert를 다른 Project에서도 조회 및 처리가 가능합니다. Escalation Policy적용 되어 타 Project의 Member에도 알람이 전파 됩니다.



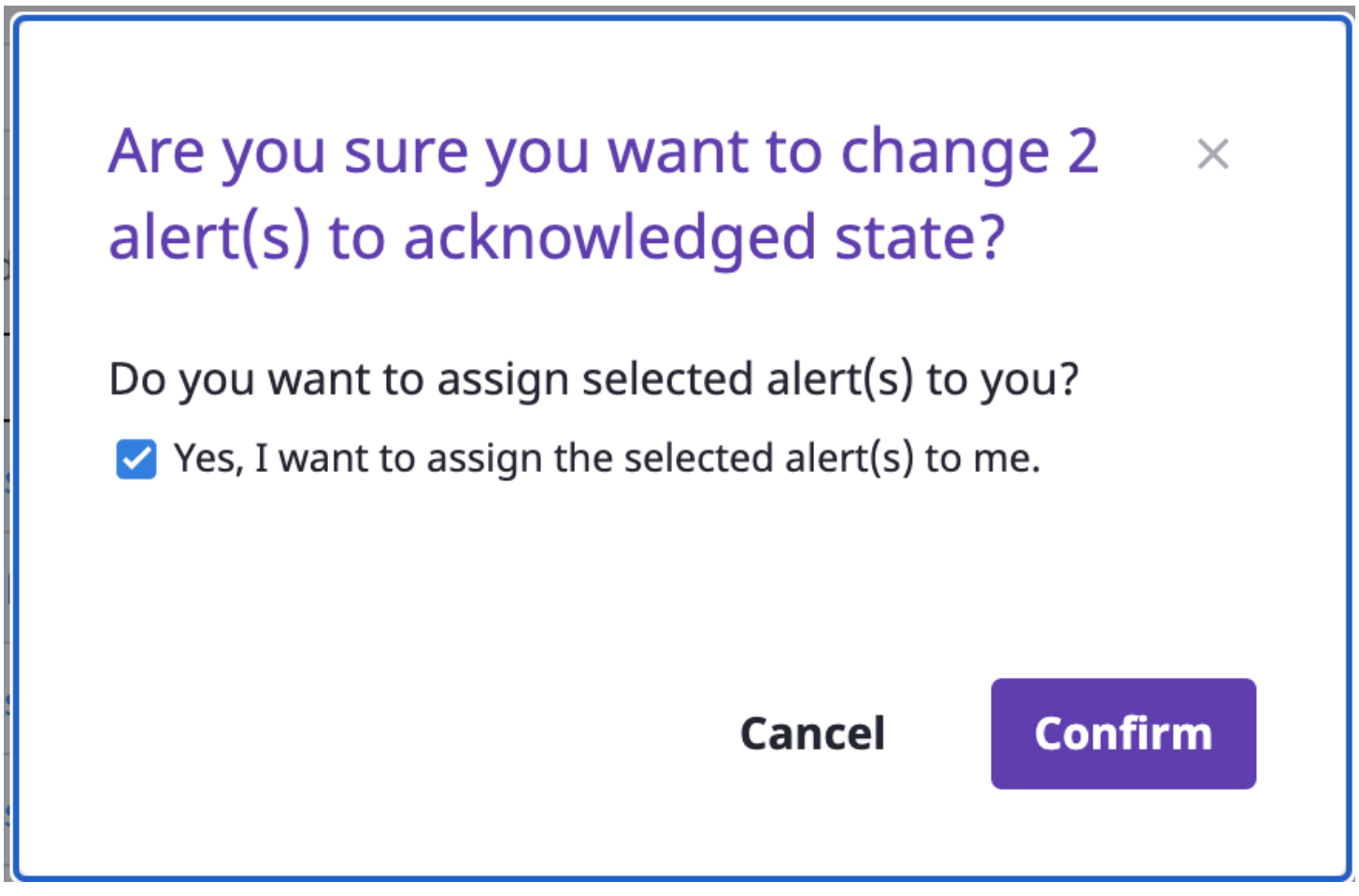
Alert Status Change

Alert Detail 을 통하지 않고 수신된 Alert의 상태를 간편하게 변경할 수 있습니다. 여러개의 Alert를 복수로 지정하여 한번에 상태 변경도 가능 합니다.



Acknowledge

복수의 선택된 Alert을 ***Acknowledge*** 상태로 전환할 수 있습니다. 상태 전환과 동시에 담당자를 지정할 수 있습니다.



Resolve

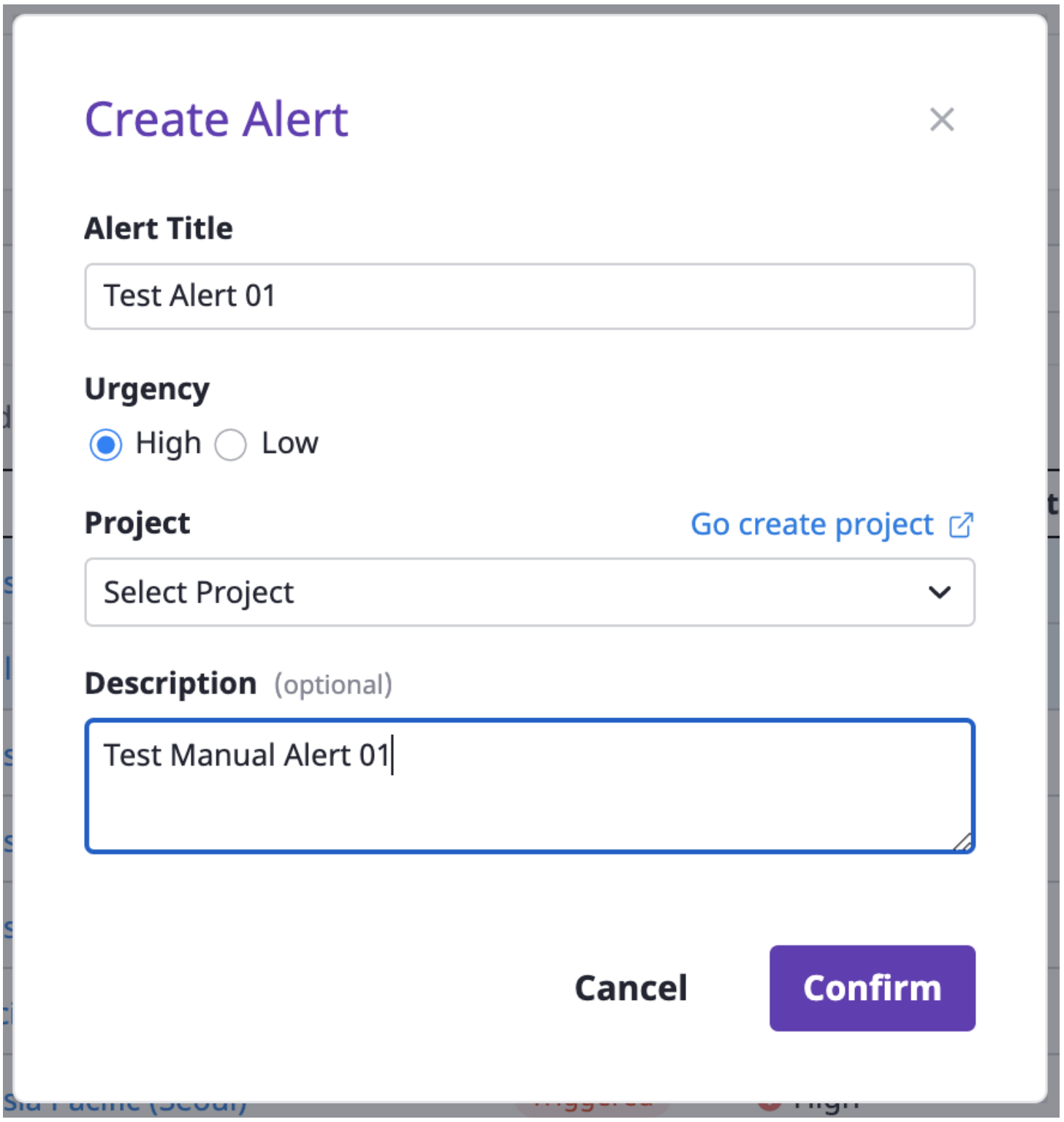
복수의 선택된 Alert을 ***Resolve*** 상태로 전환할 수 있습니다.

Delete

등록된 Alert를 삭제할 수 있습니다.

Manual Create Alert

시스템 외부에서 발생된 Alert 이외에 Console에서도 직접 Alert을 발생 시킬 수 있습니다. 관리자가 자체 기준에 의해 Alert를 등록하여 처리할 수 있도록 합니다.



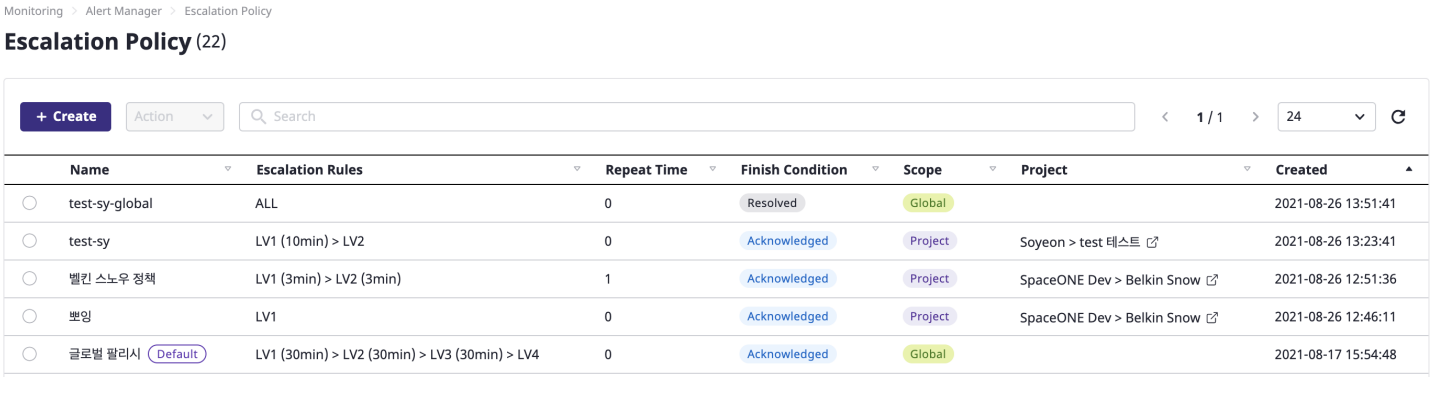
Item	Description
Alert Title	Alert의 이름을 수동으로 입력할 수 있습니다.
Urgency	Alert의 긴급도를 지정합니다.
Project	Alert이 등록될 Project를 지정합니다.
Description	Alert의 설명을 입력 합니다.

6.1.3 - Escalation Policy

Escalation policy to spread notification

Overview

수신된 Alert을 프로젝트의 구성원들에게 효과적으로 전달하기 위해, Escalation Policy를 생성,변경,삭제 합니다.



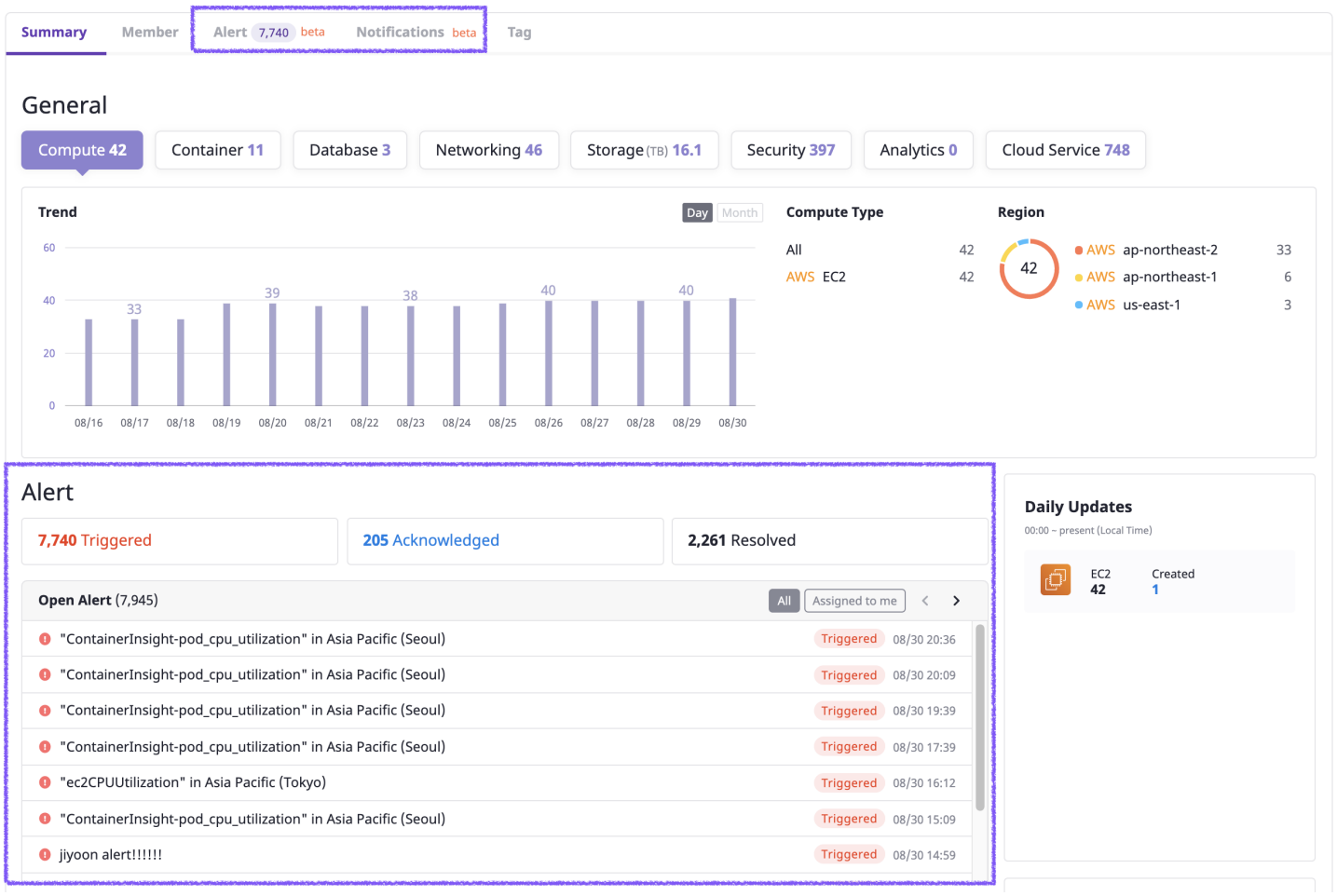
설정으로 상세 내용은 Admin Guide의 Escalation Policy 를 참고 하세요.

6.2 - Project Dashboard

Managing alert for each project.

Overview

각 Project 별로 Alert을 수신받기 위한 설정을 관리하고, 수신된 Alert 리스트를 확인할 수 있습니다.

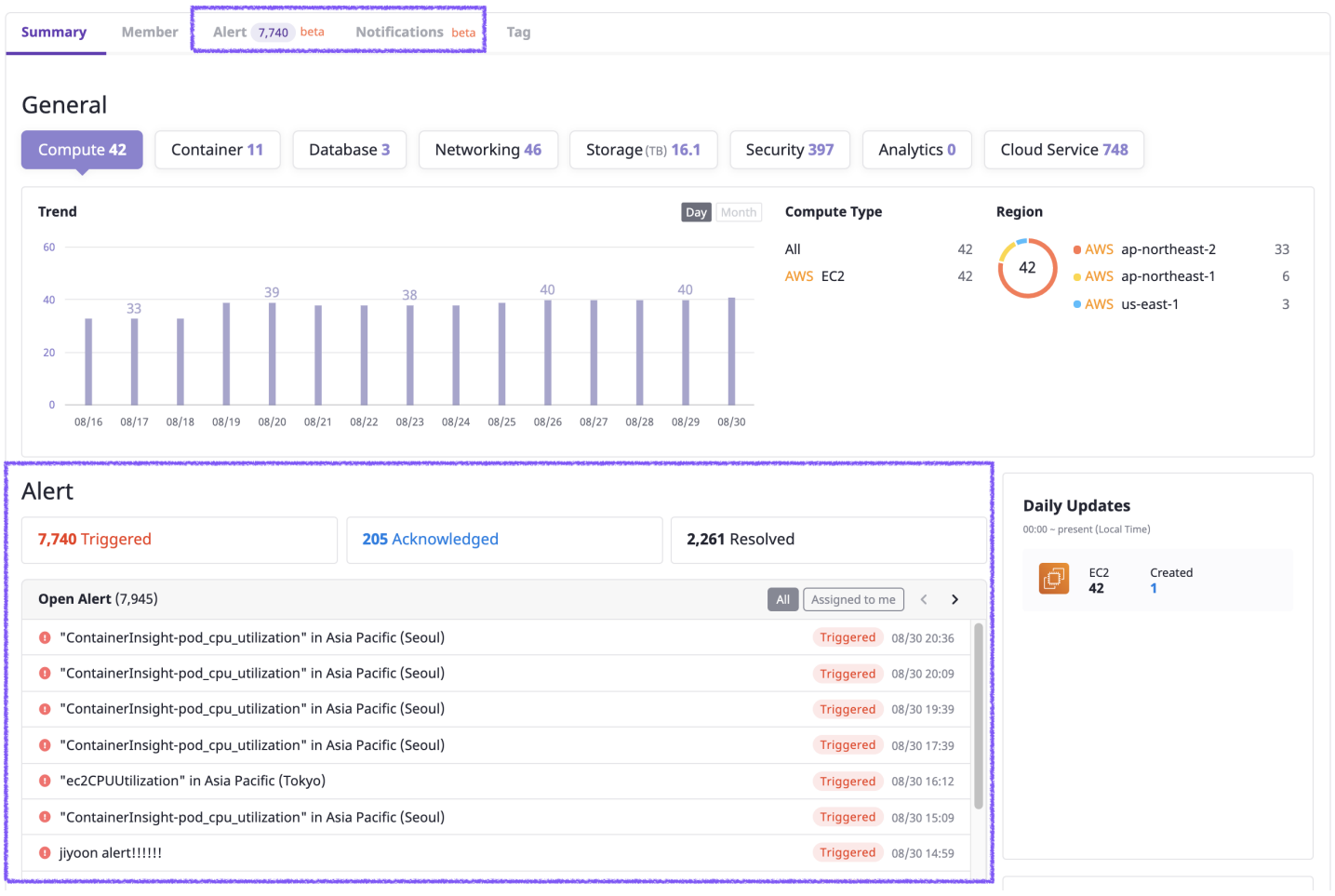


6.2.1 - Alert

Managing alert message for each project

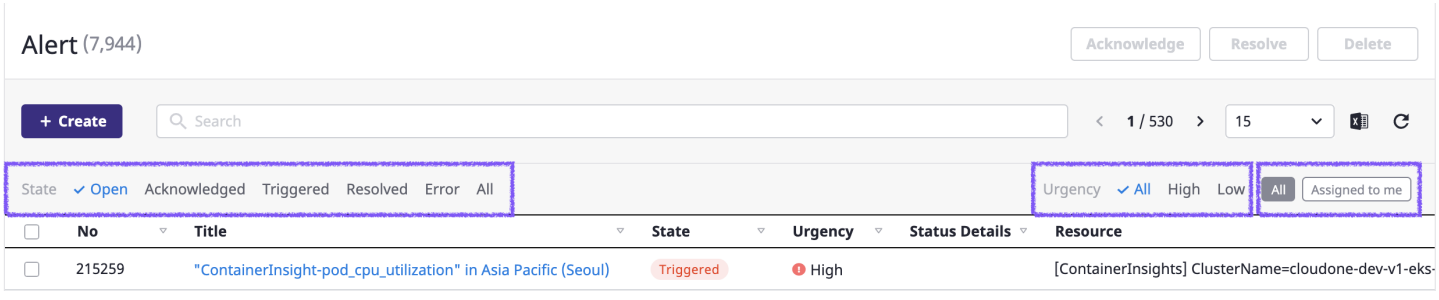
Overview

Project에 수신된 모든 Alert를 관리할 수 있습니다.



Alert List

Alert 리스트를 다양한 필터를 사용하여 조회할 수 있습니다.



Assigned to me

기본적으로 프로젝트에 수신된 모든 Alert List를 조회할 수 있습니다.
담당자가 ***나***로 직접 지정된 경우, 해당 Alert만 조회 할 수 있습니다.

Using Filters

Alert에 다양한 필터를 적용하여, 효율적인 조회가 가능 합니다.
설정가능한 Filter는 ***State*** ***Urgency*** 두 종류 입니다.

Alert State

State	설명
Open	
Acknowledged	등록된 Alert에 담당자가 할당되어 처리중인 상태
Triggered	Alert이 최초 등록된 상태
Resolved	Alert 등록된 사항이 처리 완료된 상태
Error	Alert이 수신 되었으나, Param 오류 등으로 정상적으로 등록되지 않은 상태
All	모든 Alert 상태

Alert Urgency

Urgency는 ***High***, ***Low*** 로 구분 됩니다.

Export

조회 가능한 모든 Alert List를 ***`Excel Export`*** 가능합니다.

Alert Details

수신된 Alert의 상세 상태를 조회하고 처리 이력을 관리할 수 있습니다. 상세 설명은 Alert Manager Alert Details 을 참고해 주세요.

Alert Status Change

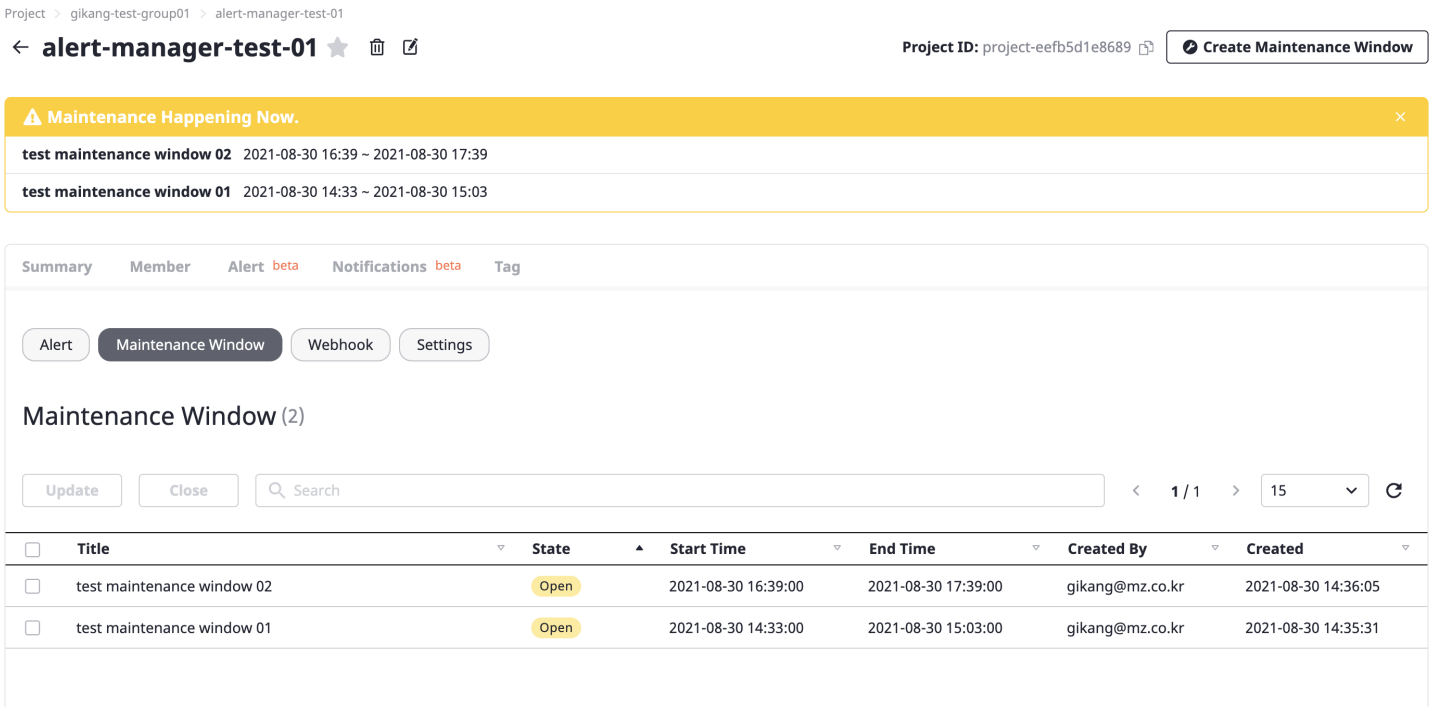
`Alert Detail` 을 통하지 않고 수신된 Alert의 상태를 간편하게 변경할 수 있습니다. 여러개의 Alert를 복수로 지정하여 한번에 상태 변경도 가능 합니다. Alert Status Change 를 참고해주세요.

6.2.2 - Maintenance Window

Register system maintenance window to avoid sending wrong notification

Overview

정기, 비정기적인 시스템 작업일정을 등록합니다. Project Dashboard를 통해 작업을 안내하고, 작업간 발생하는 알람이 Disable 됩니다.

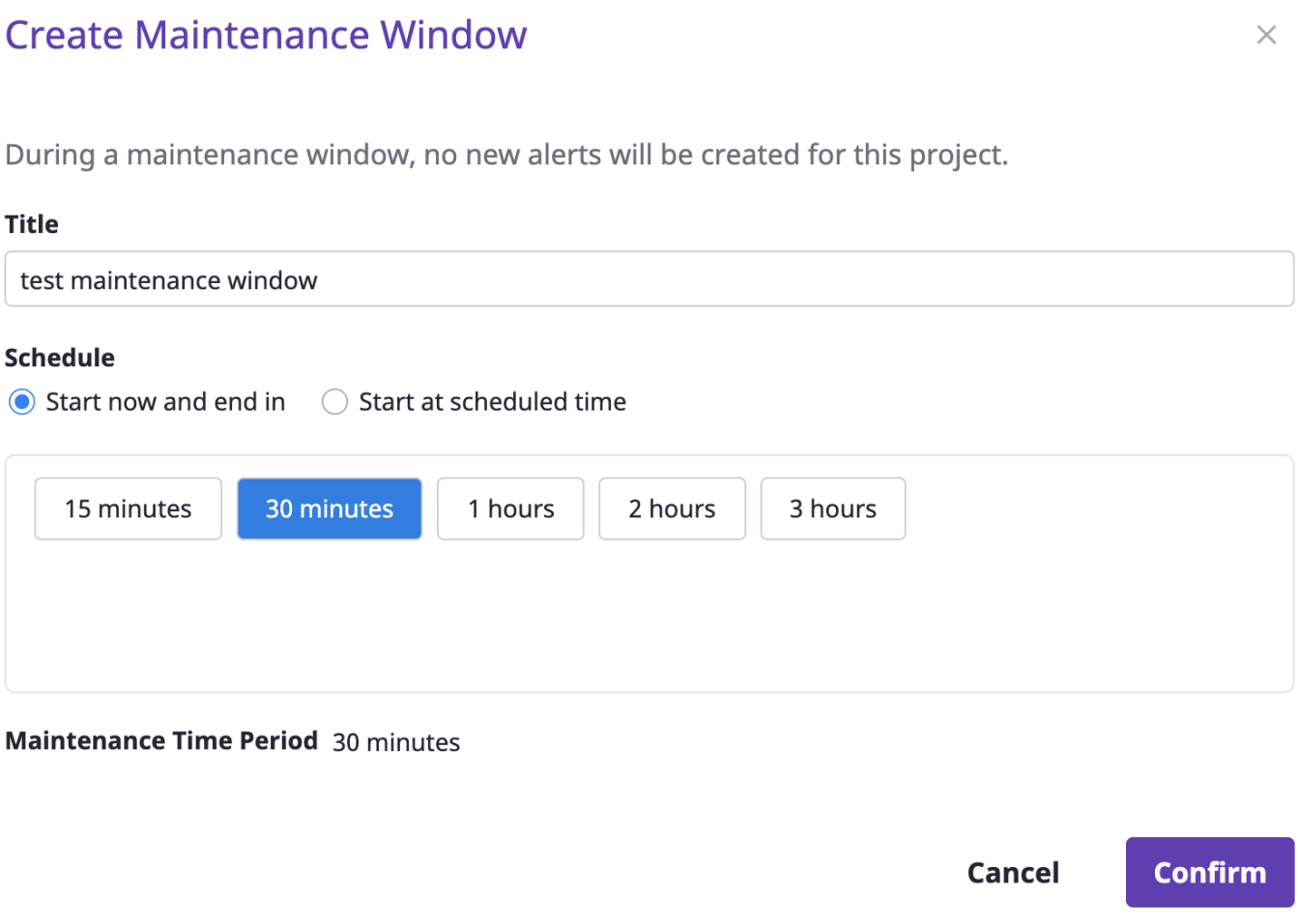


Managing Maintenance Window

작업 일정을 등록, 변경, 종료 할 수 있습니다.

Create Maintenance Window

작업 일정을 등록합니다. 작업명과 작업 일정을 등록합니다. 작업 일정에 대한 세부 옵션설명은 아래와 같습니다.

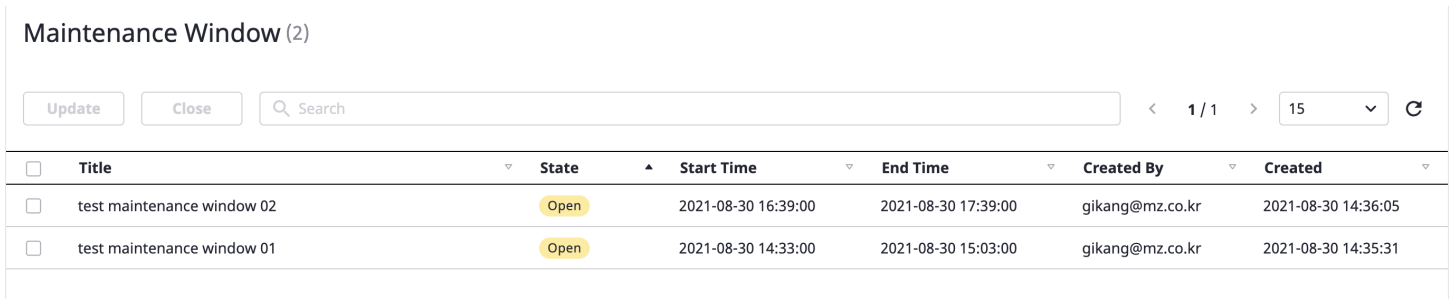


항목	설명

항목	설명
Start now and end in	지금 즉시 지정된 시간까지 작업 일정을 등록 합니다. 15분, 30분, 1시간, 2시간, 3시간 중 선택할 수 있습니다.
Start at scheduled time	향후 예정된 작업 일정을 예약할 수 있습니다. 시작시간과 종료 시간을 선택할 수 있습니다.

Maintenance Window List

작업 일정을 조회할 수 있습니다.



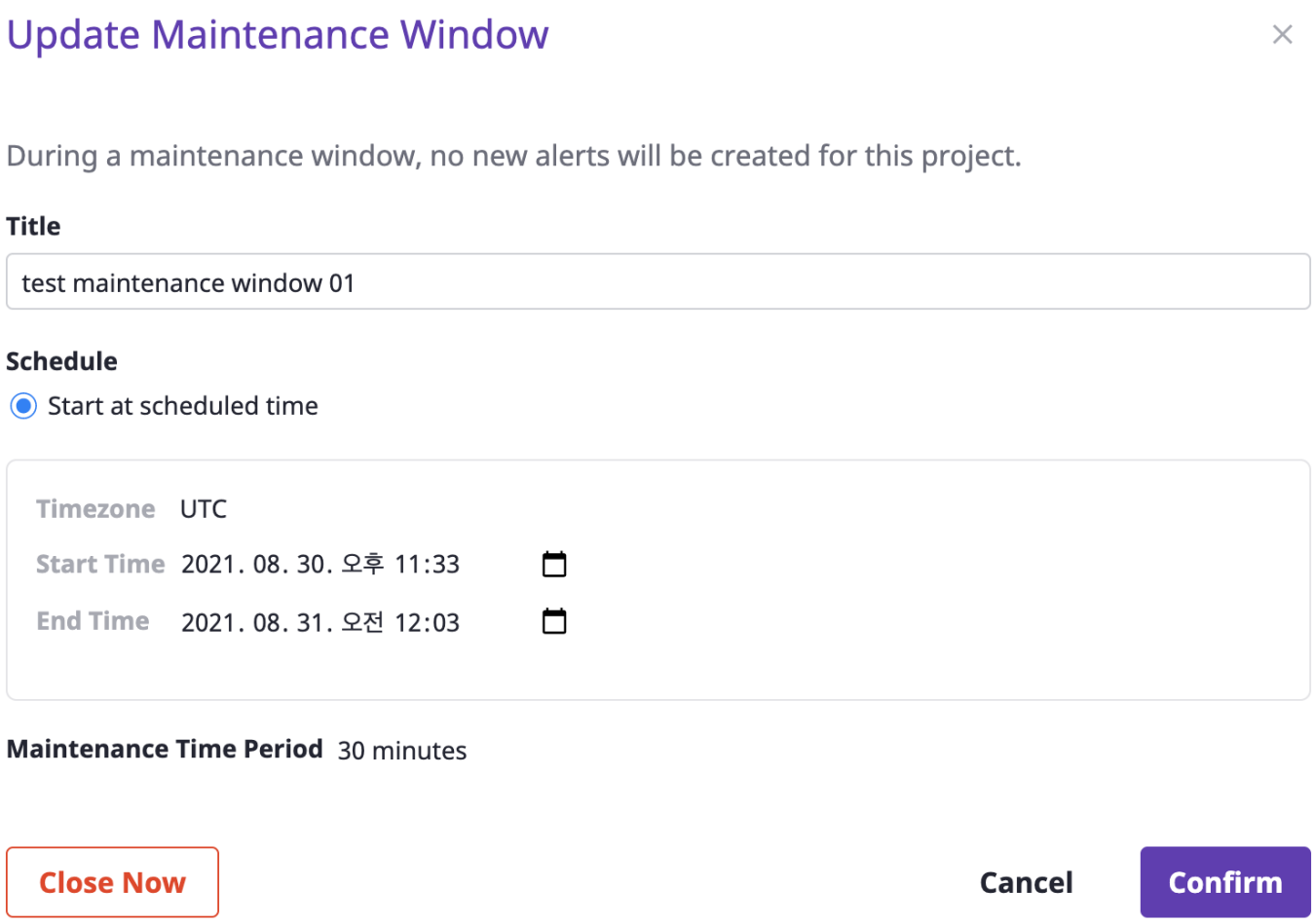
작업 일정의 각 Parameter에 대한 상세 설명은 아래와 같습니다.

항목	설명
Title	작업명
State	작업 진행 상태. 현재 작업 중인 경우 ***Open*** 작업이 완료된 경우 ***Closed***
Start Time, End Time	작업의 시작, 종료 시간
Create By	작업 일정을 등록한 사람
Created	작업 일정을 등록한 시간

검색 창을 통해 다양한 parameter 기반으로 작업 일정에 대한 조회가 가능합니다.

Update Maintenance Window

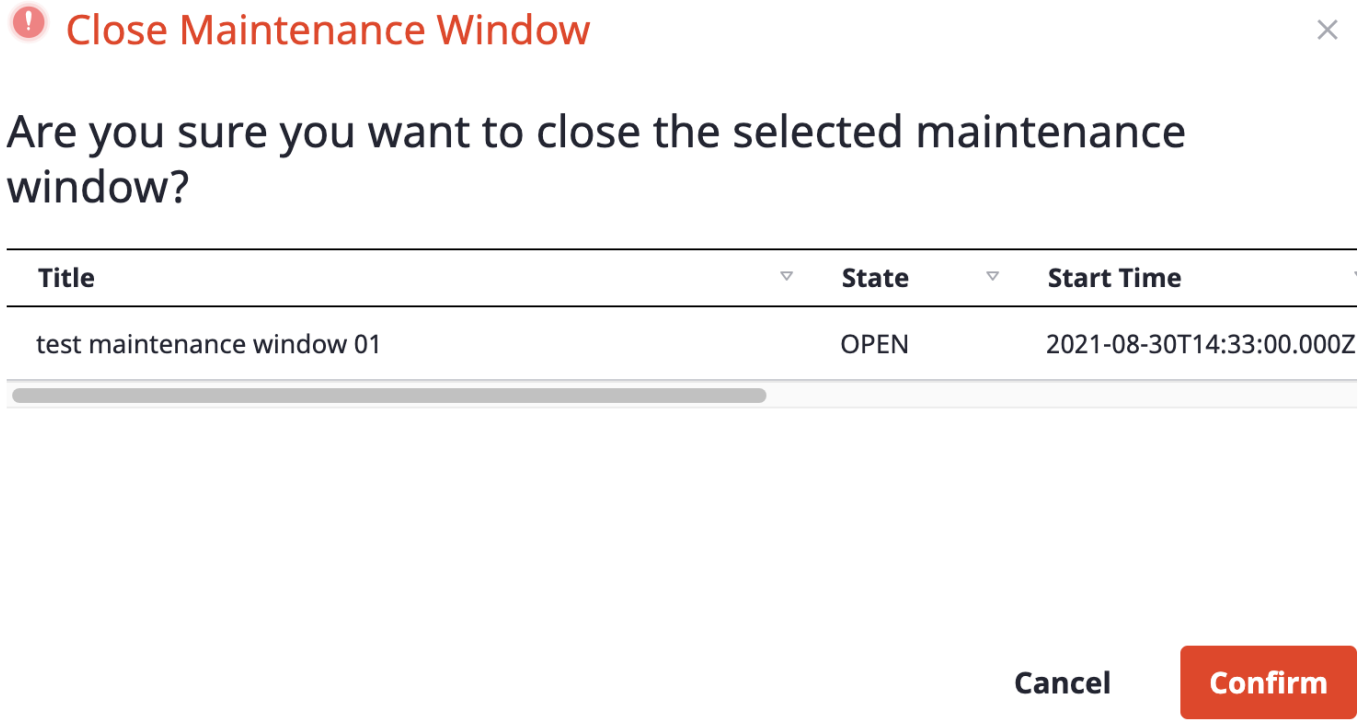
작업 일정을 변경할 수 있습니다.



> **Info**
>
> 예정된 작업의 내용을 변경할 수 있습니다. 작업 시간이 지나서 ***Closed*** 상태인 작업 일정은 변경할 수 없습니다.

Close Maintenance Window

진행중인 작업 일정을 강제로 종료할 수 있습니다.

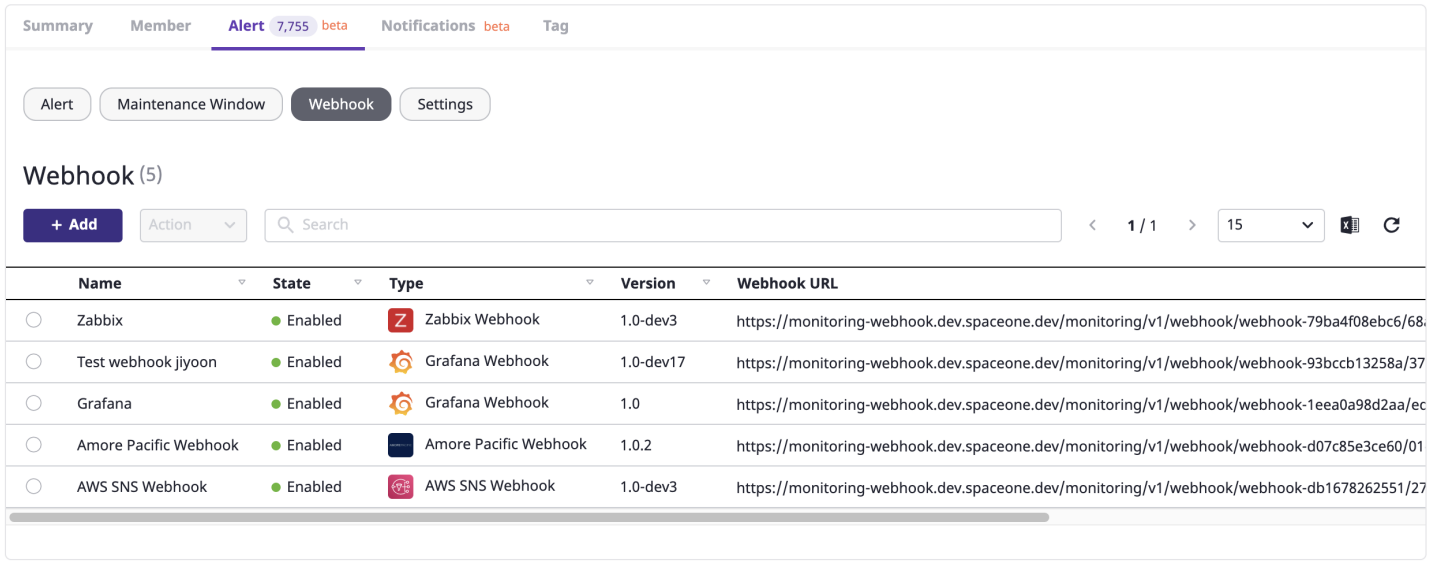


6.2.3 - Webhook

Install & configure monitoring webhook plugin to receive alert

Overview

SpaceONE의 Monitoring Service는 외부 시스템으로부터 Alert 수신시 Webhook 방식을 사용하고, 이를 지원하는 다양한 플러그인들을 가지고 있습니다. 다양한 플러그인들을 활용하여 Webhook URL을 생성하여 알람을 수신 받을 수 있습니다.



Webhook Plugin 리스트 조회시 각 항목에 대한 설명은 아래와 같습니다.

항목	설명
Name	Webhook의 수신 설정명
State	Webhook 가능 여부 ***Enabled*** 인 경우, ***Webhook URL*** 로부터 Alert이 수신 가능, ***Disabled*** 인 경우 수신되는 Alert이 무시됨
Type	Monitoring Webhook Plugin
Version	Monitoring Webhook Plugin의 Version
Webhook URL	Alert 수신을 위한 Endpoint, Webhook 추가시 자동으로 unique한 url 생성

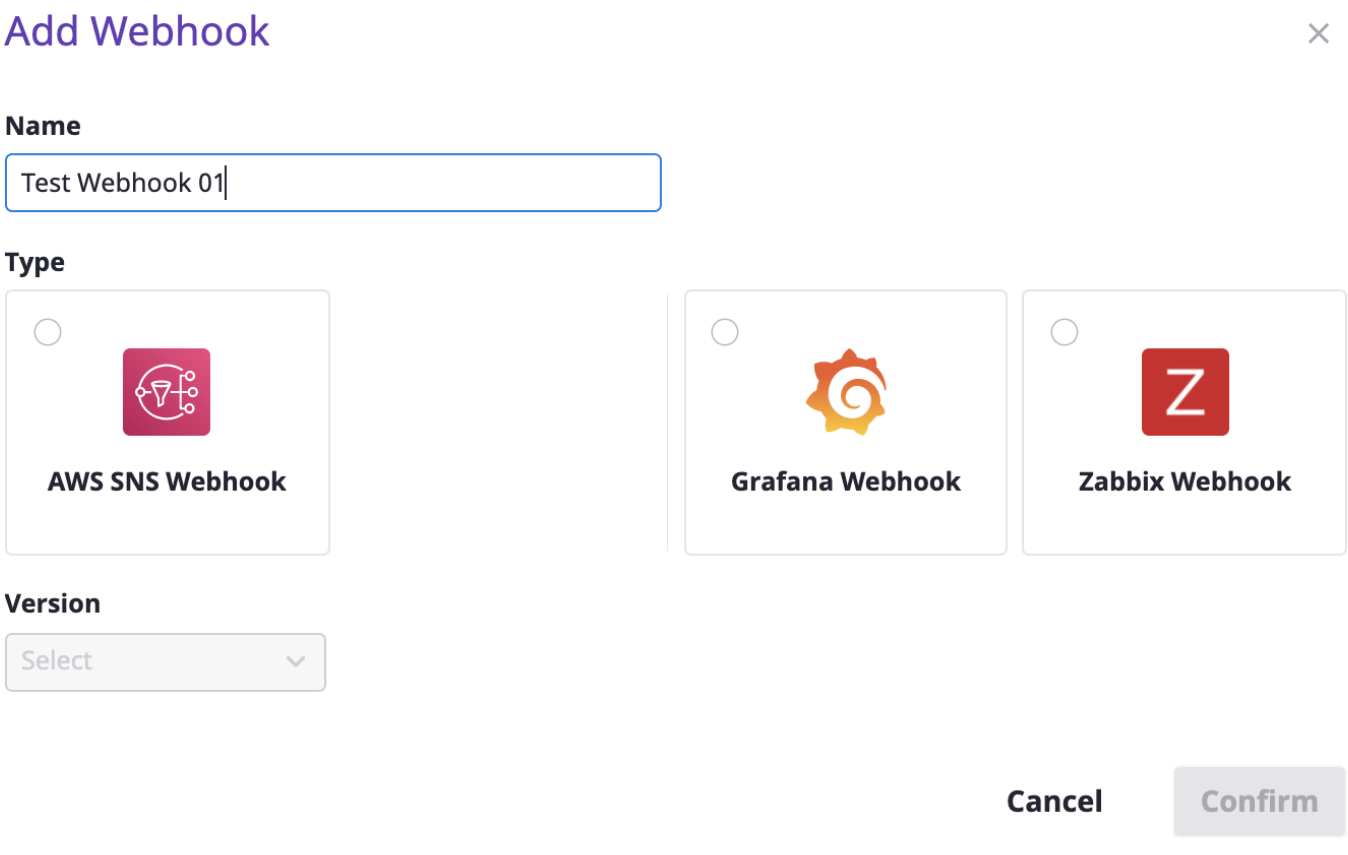
> **Info**
>
> Webhook URL을 외부의 모니터링 시스템과 연동하기 위한 가이드는
>
> Monitoring System 연결가이드 를 참조 해주세요.

Managing Webhook Plugin

Alert 를 수신받기 위한 다양한 종류의 ***Monitoring Webhook Plugin*** 을 추가,변경,삭제할 수 있습니다.

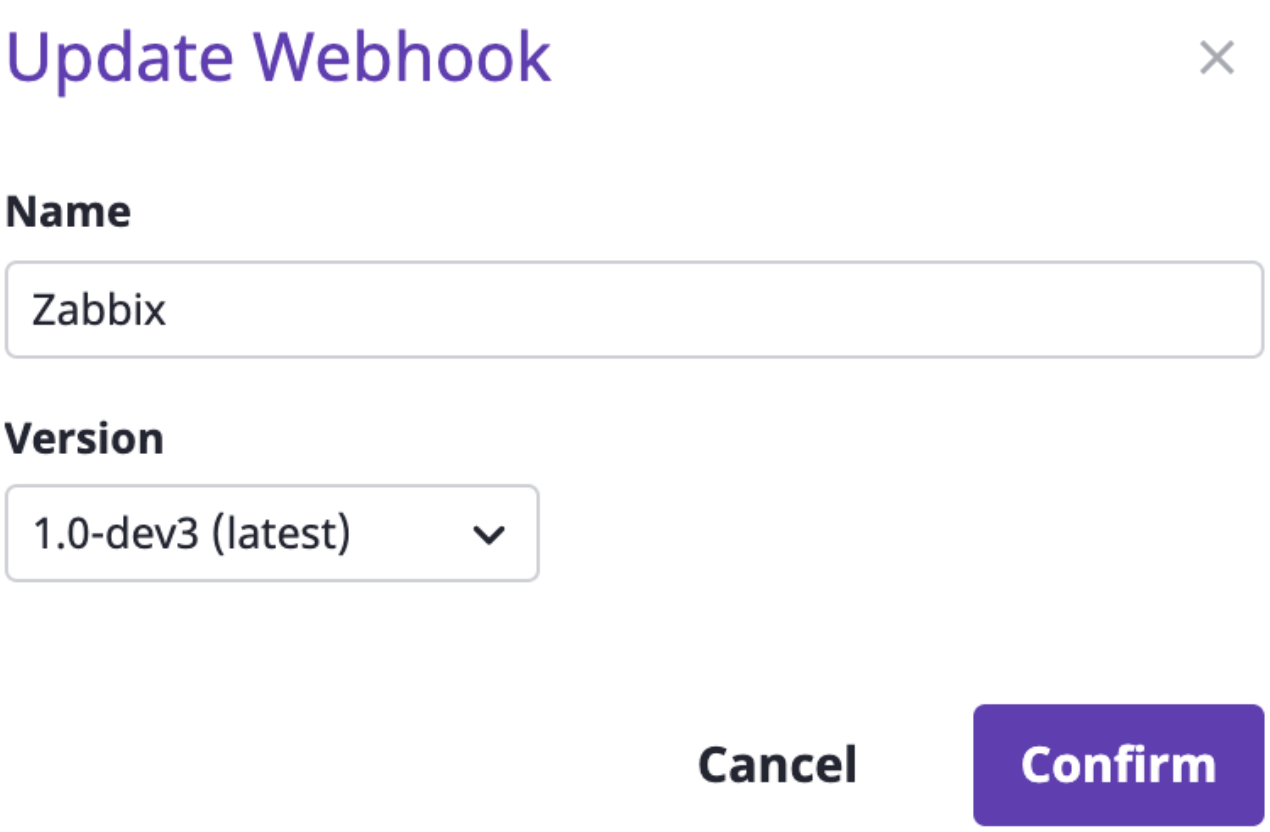
Add webhook plugin

MarketPlace 로부터 다양한 타입의 ***Monitoring Webhook Plugin*** 을 선택하여 설치합니다.



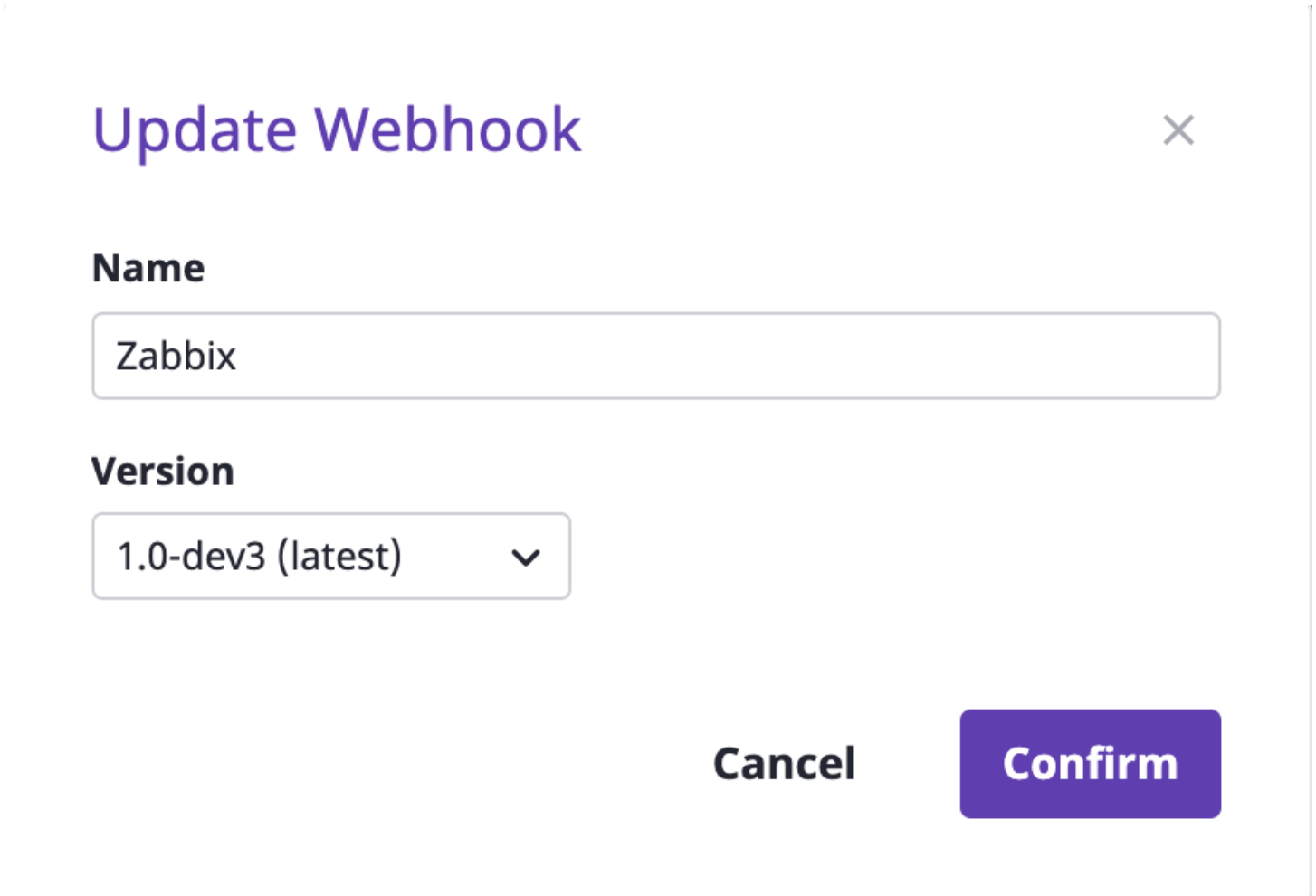
Update webhook plugin

Webhook의 이름과 사용되는 플러그인 버전을 변경할 수 있습니다.



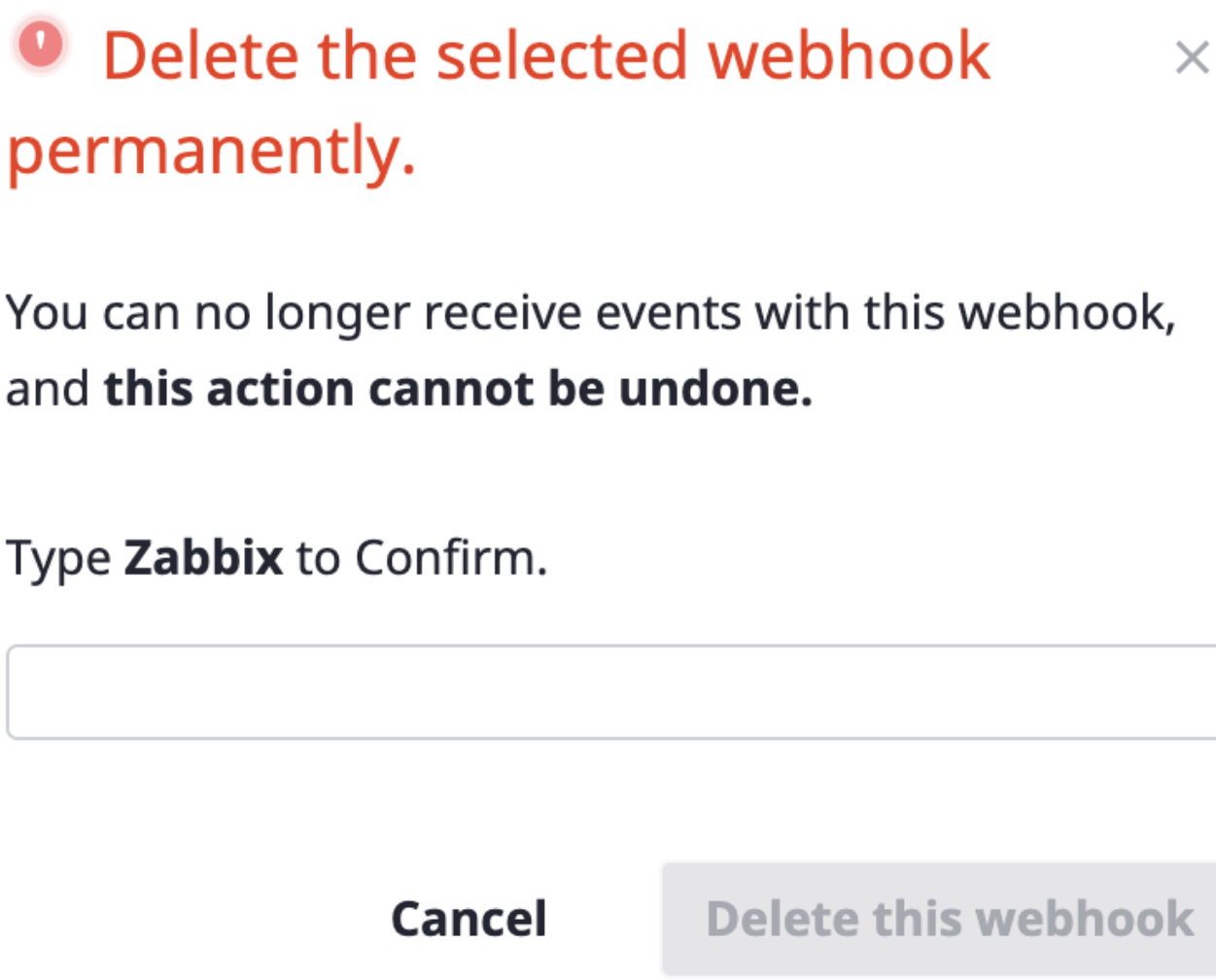
Disable webhook plugin

Webhook으로부터 수신되는 Alert이 무시 되도록 설정합니다.



Delete webhook plugin

Webhook을 삭제합니다.

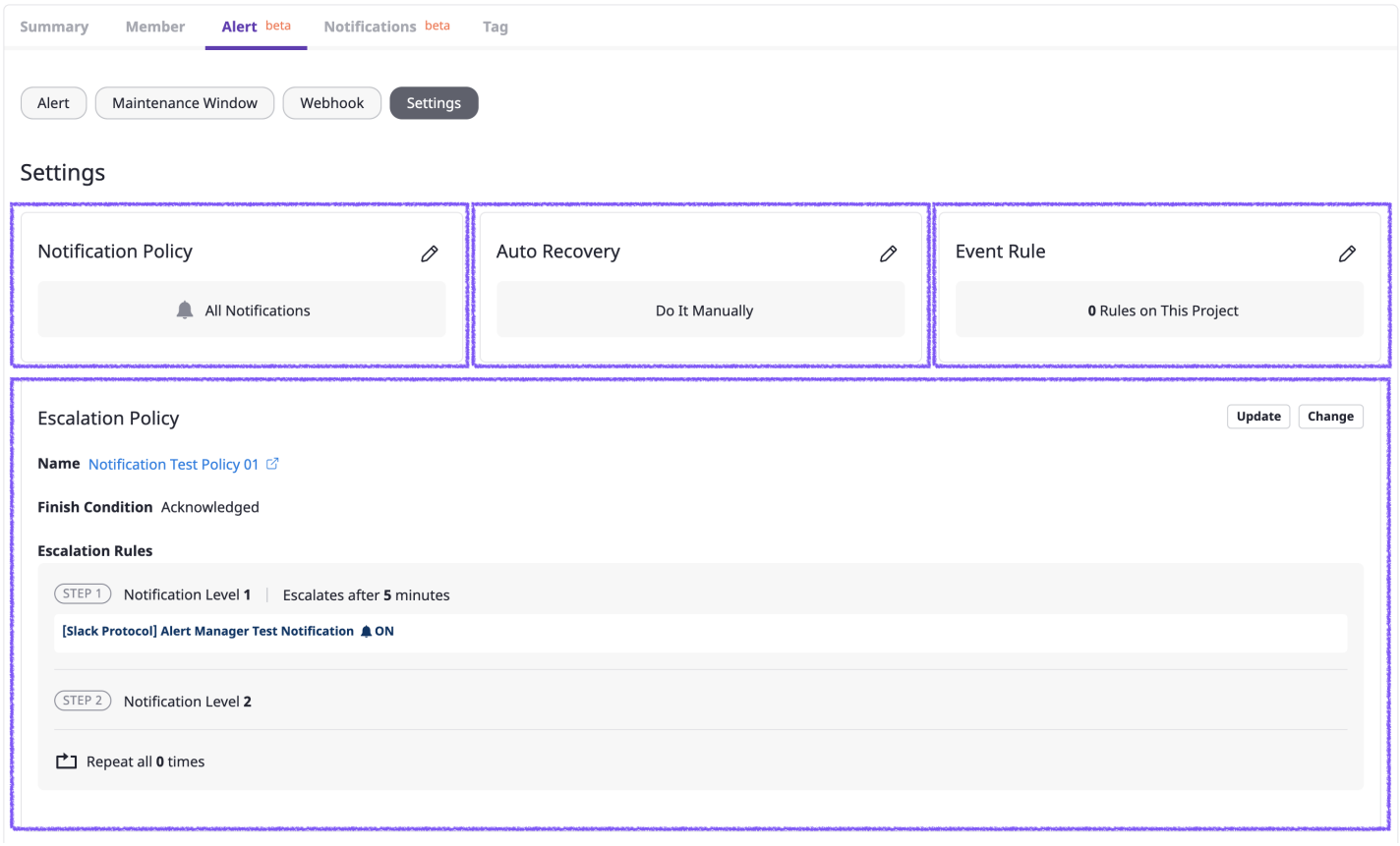


6.2.4 - Settings

Setting up detailed policy for managing alerts

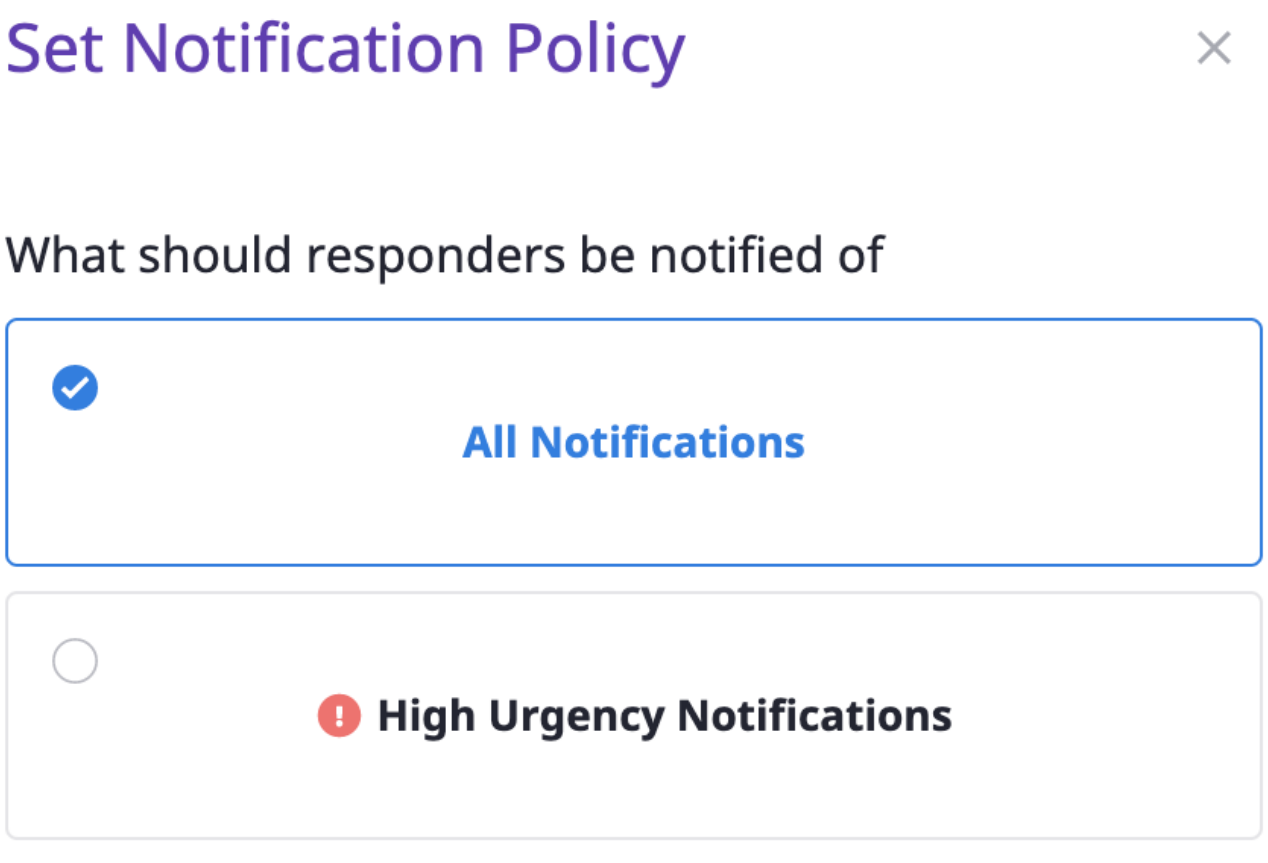
Overview

각 Project에 수신되는 Alert을 관리하기 위한 상세 옵션을 관리 합니다.



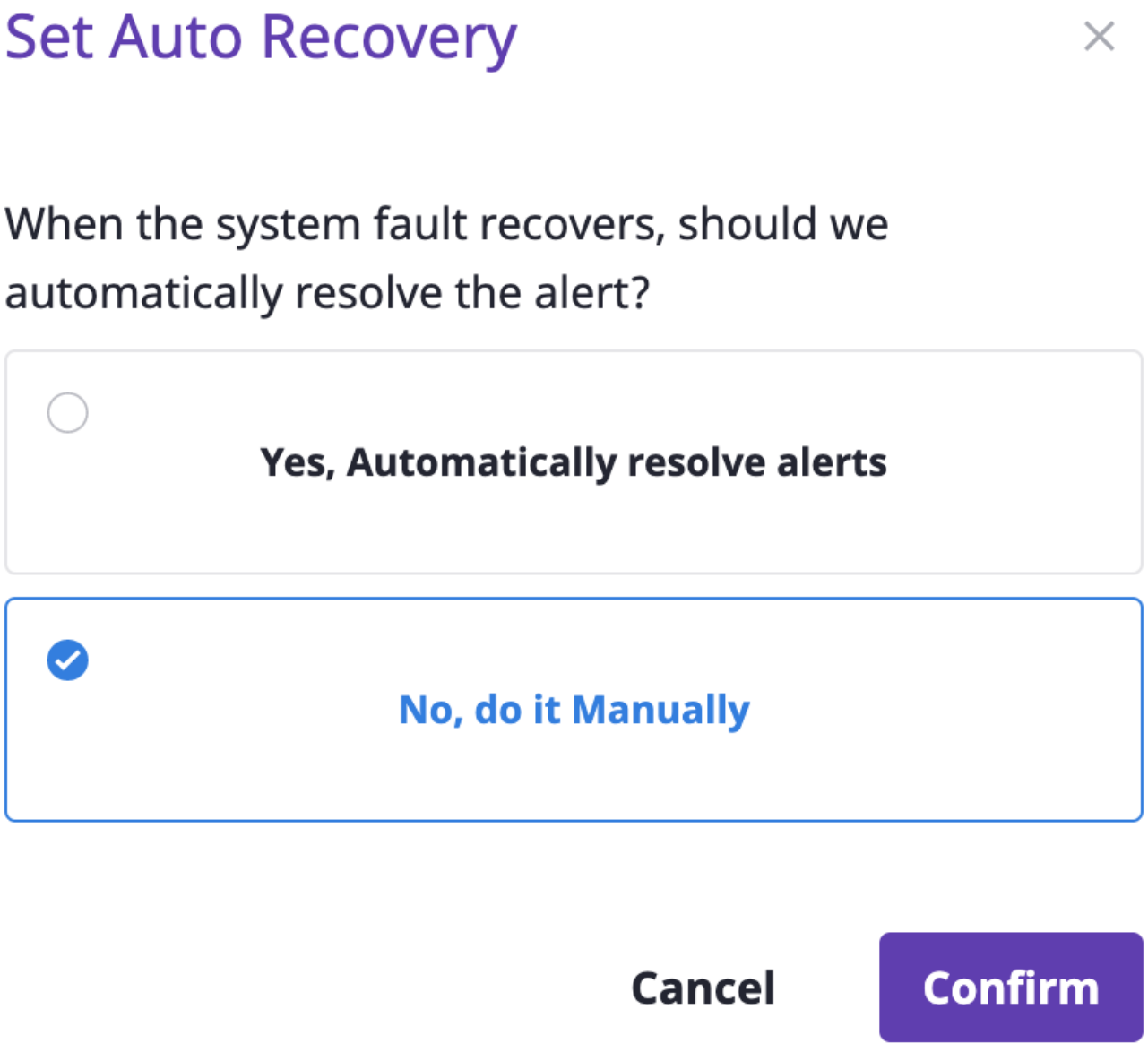
Notification Policy

알람의 민감도를 설정 합니다. ***All Notifications*** 인 경우 수신된 모든 Alert에 대해 알람을 발생합니다. ***High Urgency Notifications*** 인 경우 ***High*** 상태인 Alert에 대해서만 알람을 발생합니다.



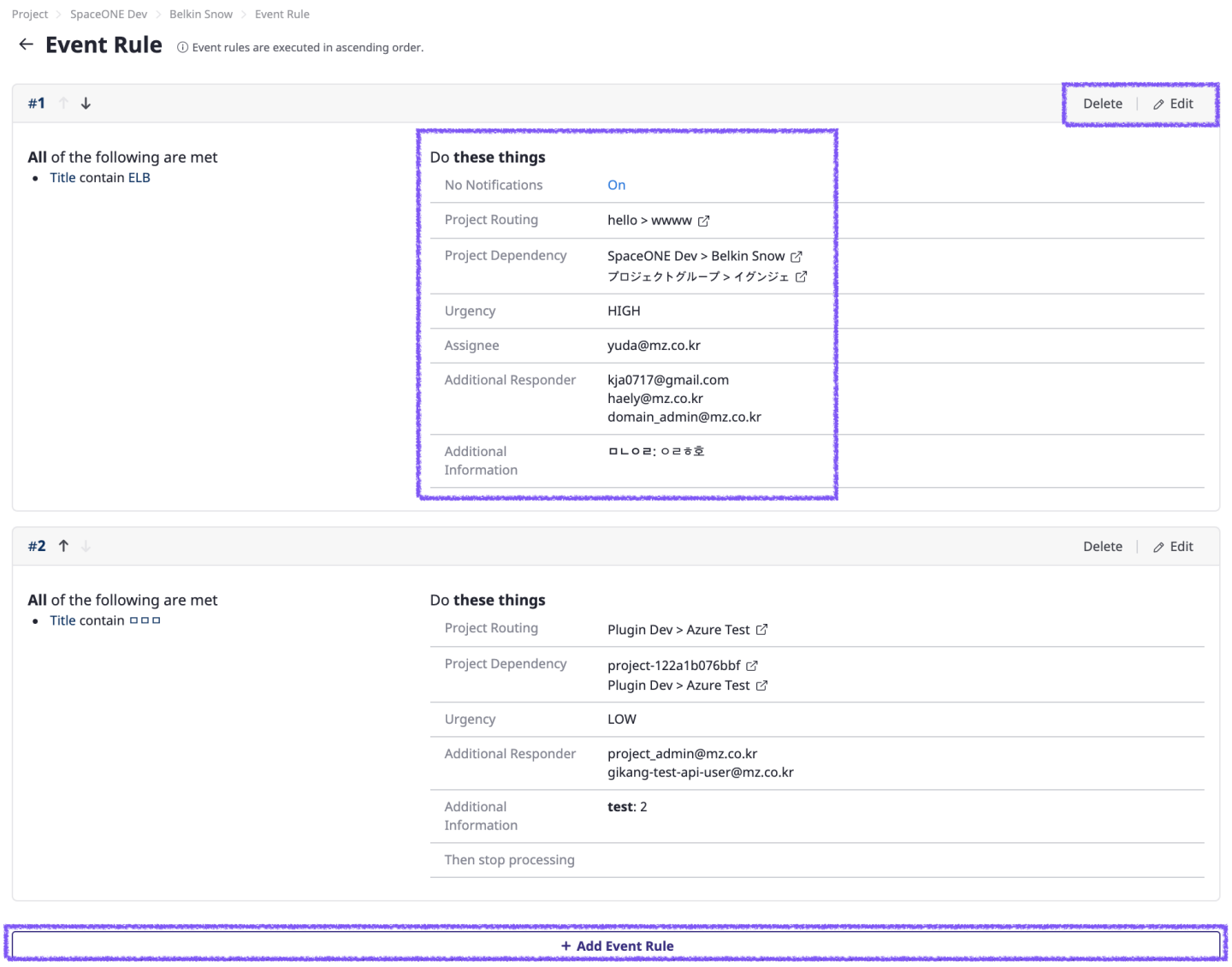
Auto Recovery

담당자가 매번 수동으로 Alert의 상태를 관리해 주지 않아도, 외부의 Monitoring System 으로부터 ***정상*** Alert를 수신한 경우 자동으로 ***Resolved*** 상태로 전환 됩니다.



Event Rule

수신된 Alert이 조건을 만족할 경우, 자동으로 지정된 동작을 수행할 수 있도록 정의 합니다. Alert Event를 수작업으로 관리해야 하는 어려움을 줄여줄 수 있습니다.

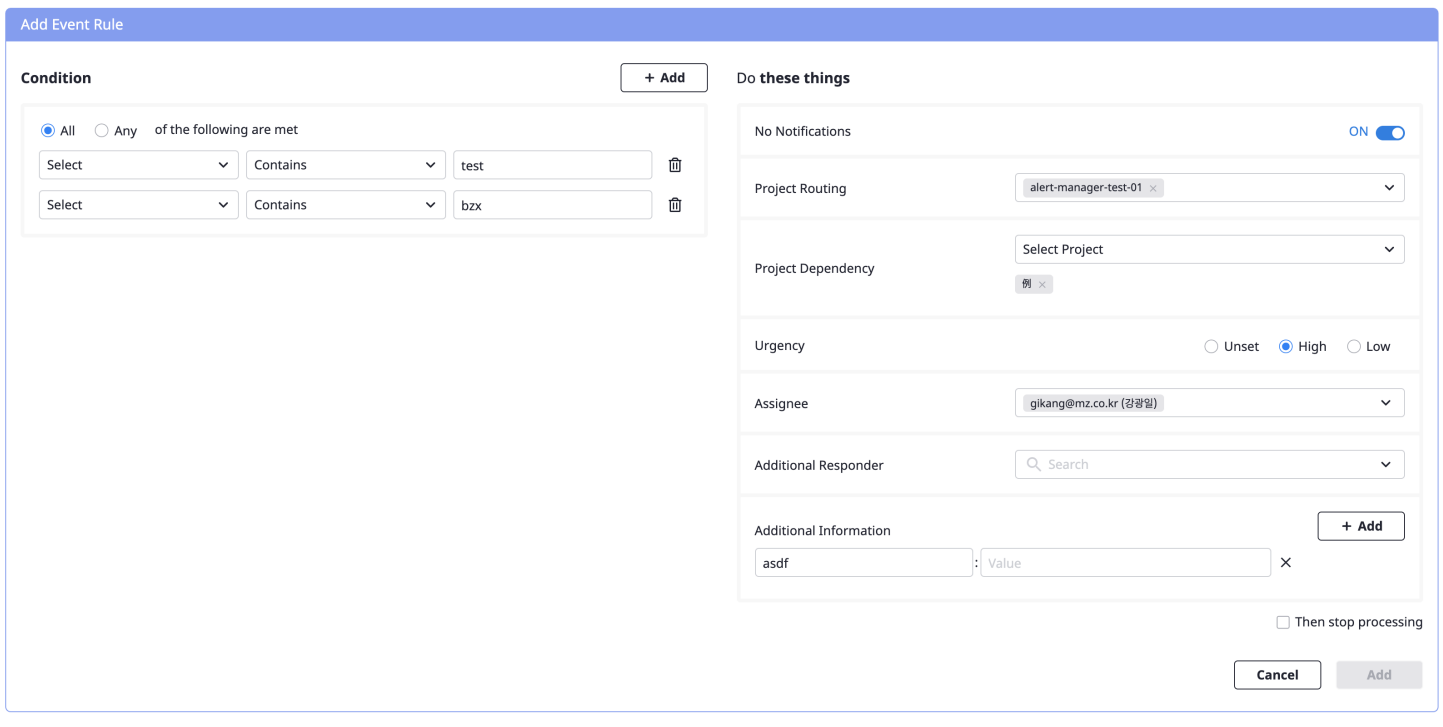


정의할 수 있는 항목은 아래와 같습니다.

항목	설명
No Notifications	Notification에서 제외 합니다. 해당 Alert 발생시 Notification이 발생하지 않습니다.
Project Routing	다른 Project Alert로 등록 합니다. 현재의 Project에는 등록되지 않습니다.
Project Dependency	자동으로 ***Project Dependency*** 설정을 추가 합니다. Alert 수신시 지정된 Project에도 전달됩니다.
Urgency	자동으로 Urgency가 지정 됩니다. ***low***, ***high*** 를 지정할 수 있습니다.
Additional Responder	자동으로 ***Additional Responder*** 에 지정된 사용자가 추가 됩니다.
Additional Information	입력된 Alert Event에 추가적인 정보를 입력 합니다.

Add Event Rule

Event Rule 편집 화면에서 화면 하단의 ***`Add Event Rule`*** 버튼을 클릭하여 Rule을 추가할 수 있습니다.



Edit Event Rule

Event Rule 편집 화면에서 각 Event Rule 우측의 ***Edit*** 버튼을 클릭하여 입력된 Rule을 변경할 수 있습니다.

Delete Event Rule

Event Rule 편집 화면에서 각 Event Rule 우측의 ***Delete*** 버튼을 클릭하여 입력된 Rule을 삭제할 수 있습니다.

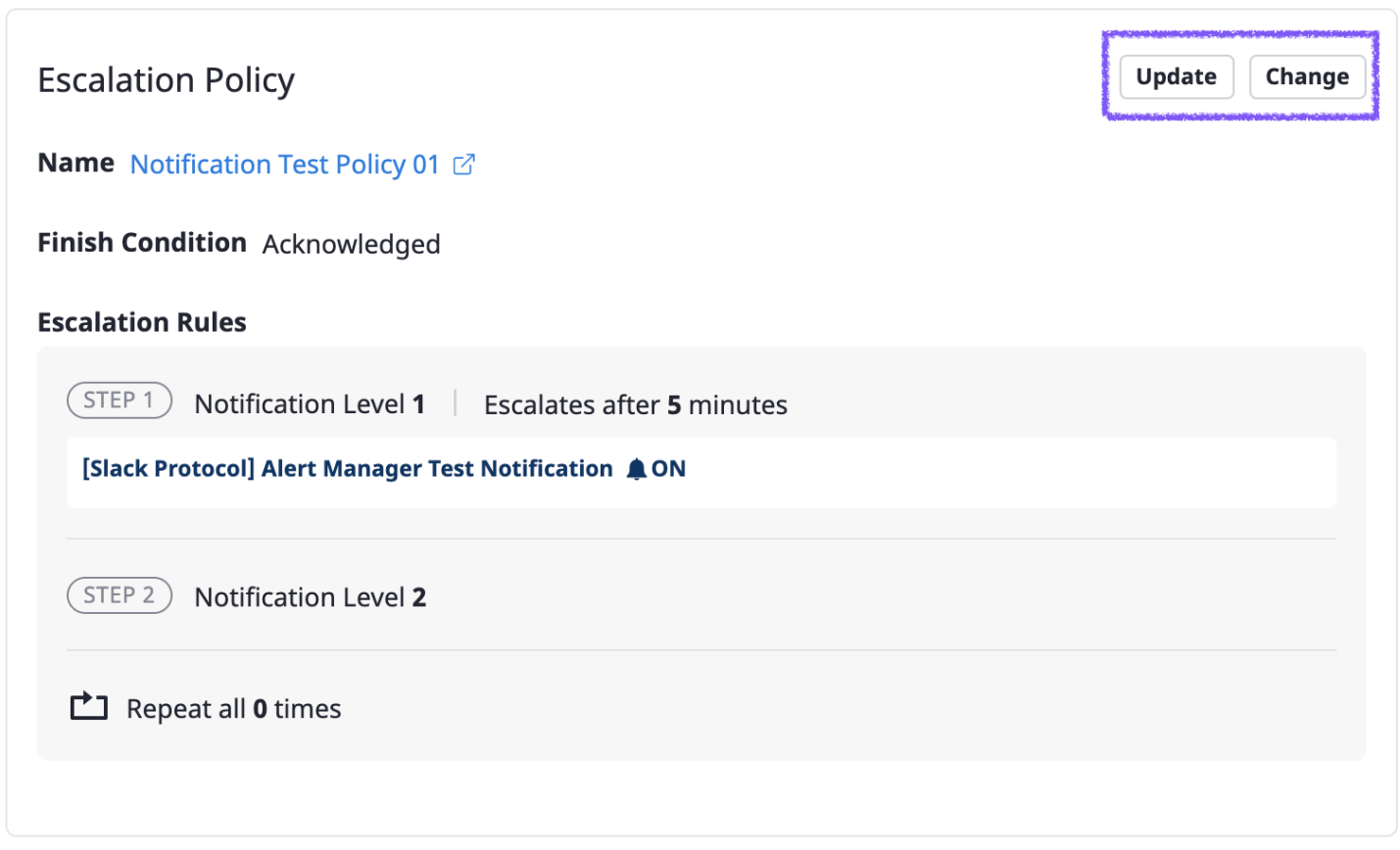
Escalation Policy

각 Project 별로 Notification 발생에 대한 세부 정책을 설정할 수 있습니다.

정책의 각 항목별 상세 설명은 Escalation Policy Admin Guide 를 참고 해주세요. Escalation Policy의 ***Name*** 의 링크를 클릭 했을 경우, 대상 ***Escalation Policy*** 관리 메인 화면으로 이동 합니다.

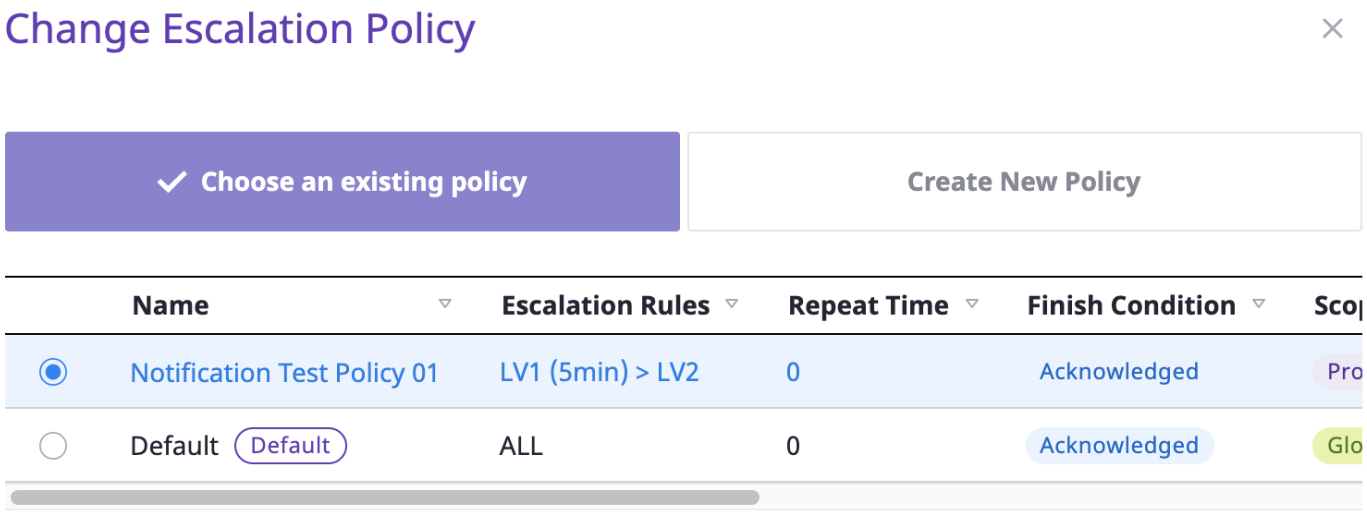
Update Existing Policy

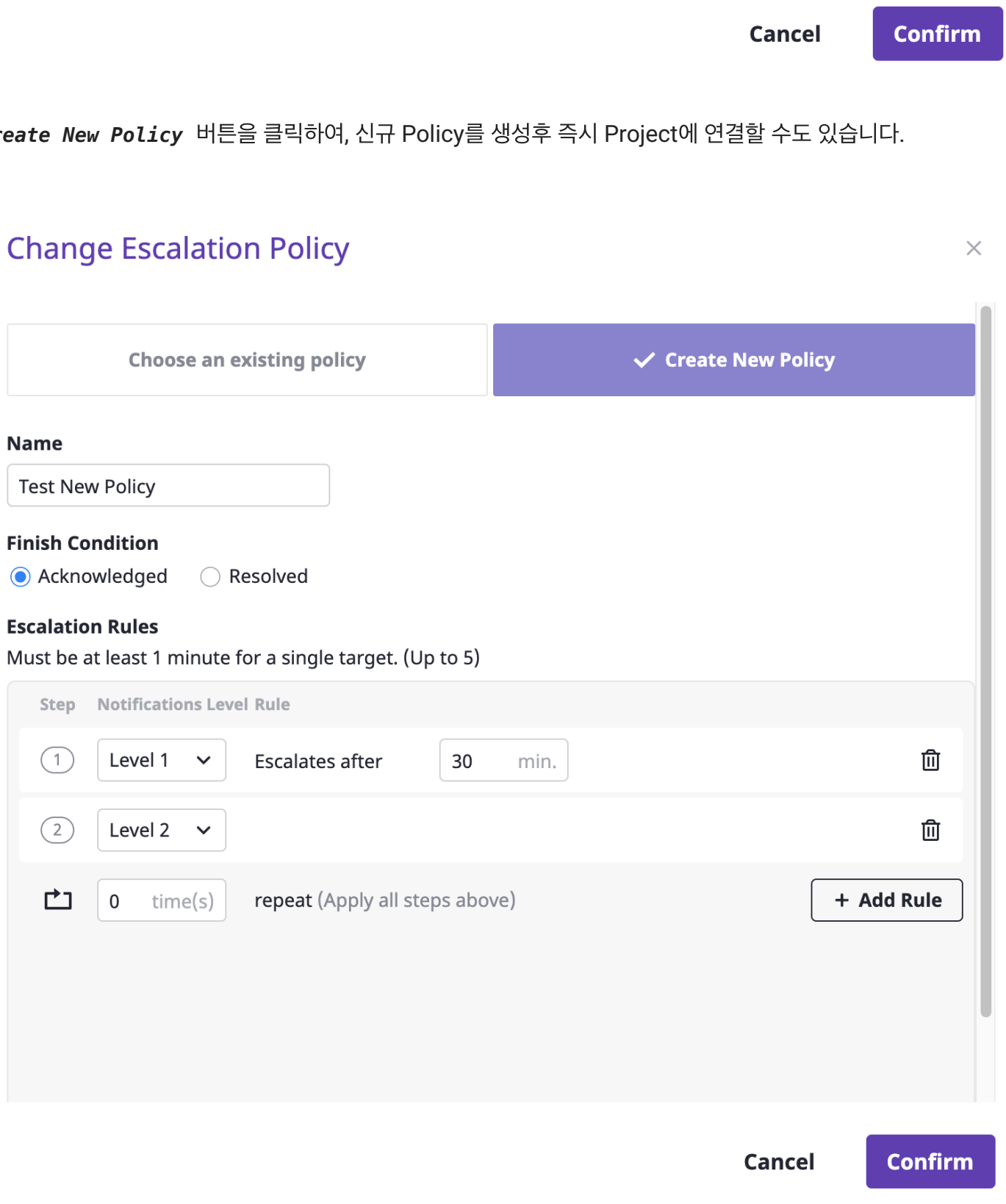
Update 버튼을 클릭하여 현재 지정된 Escalation Policy를 편리하게 편집할 수 있습니다. ***Monitoring > Alert Manager > Escalation Policy*** 내에서도 동일하게 변경이 가능합니다.



Change Existing Policy

Project에 연결된 Escalation Policy를 변경할 수 있습니다.





Create New Policy 버튼을 클릭하여, 신규 Policy를 생성후 즉시 Project에 연결할 수도 있습니다.

Escalation Policy 생성

새로운 Policy 생성에 대한 상세한 안내는 Creating New Escalation Policy를 참고 해주세요.

6.3 - Webhook Settings

Monitoring Tool Configuration Guide for SpaceONE Monitoring Webhook Plugins

6.3.1 - AWS SNS Webhook

Set up a Topic and Subscription at AWS SNS Service

Set up a SNS topic and Subscription

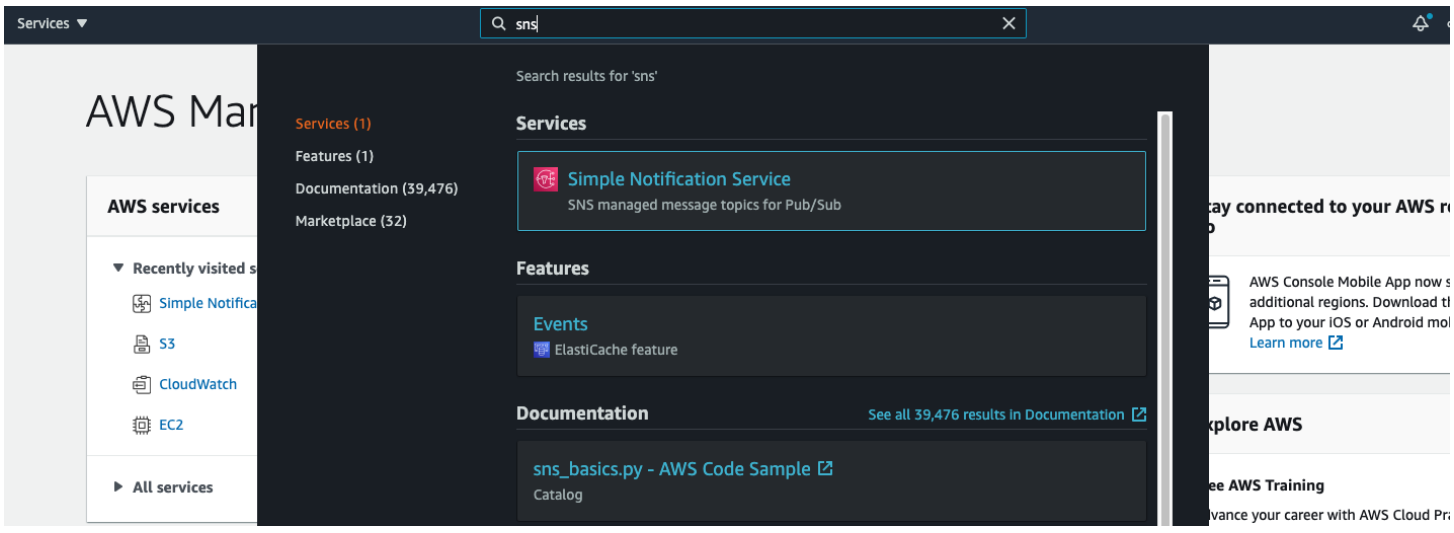
To ****Connect **SpaceONE's Alert Manager,** Set up AWS SNS's Topic and its Subscriptions
Please, Set SNS Topic and its Subscription for following Steps

Set up a Topic on AWS SNS

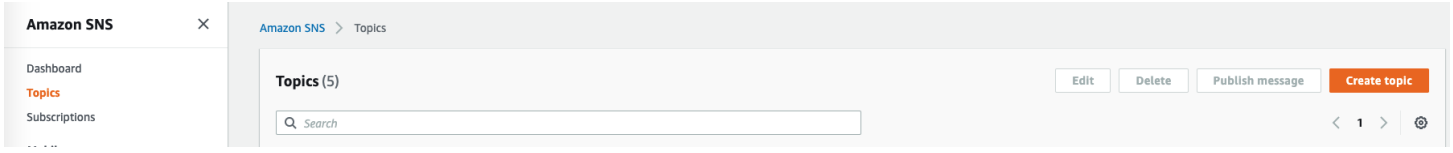
Set up a Subscription on AWS SNS

Set up a Topic on AWS SNS

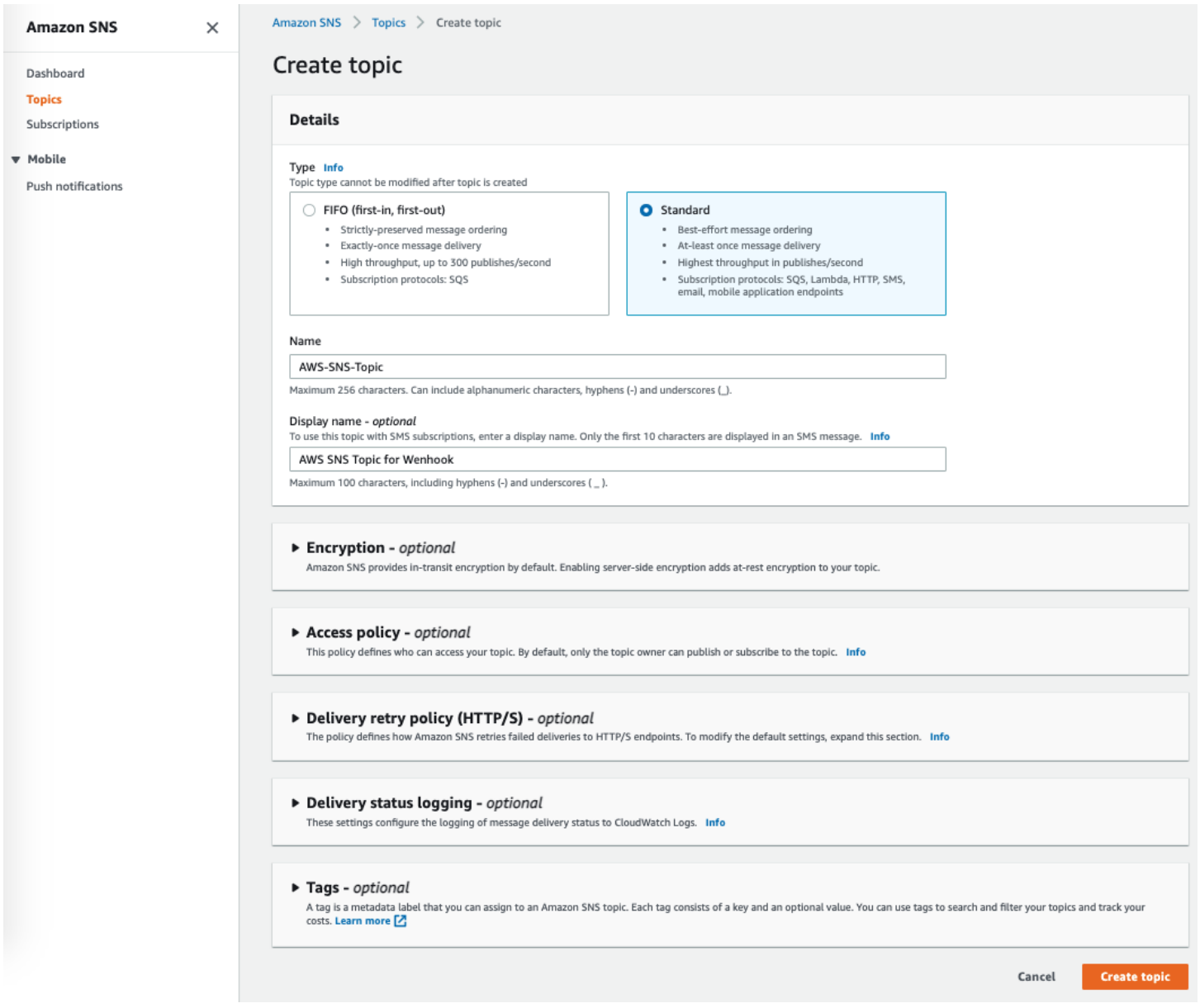
Step 1. Log in AWS Console > SNS > Topics



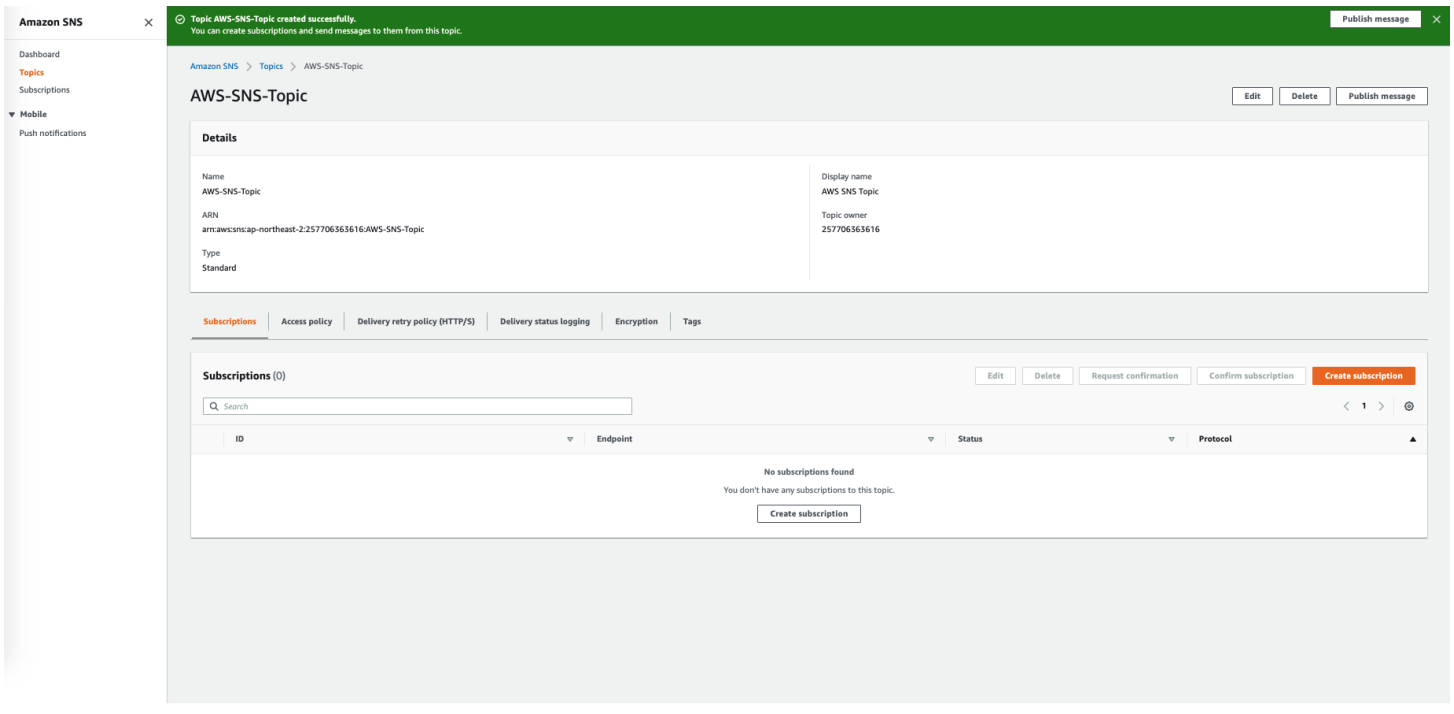
Step 2. Click `Create topic` Button



Step 3. Select `Standard` options and Give name for new topic as below



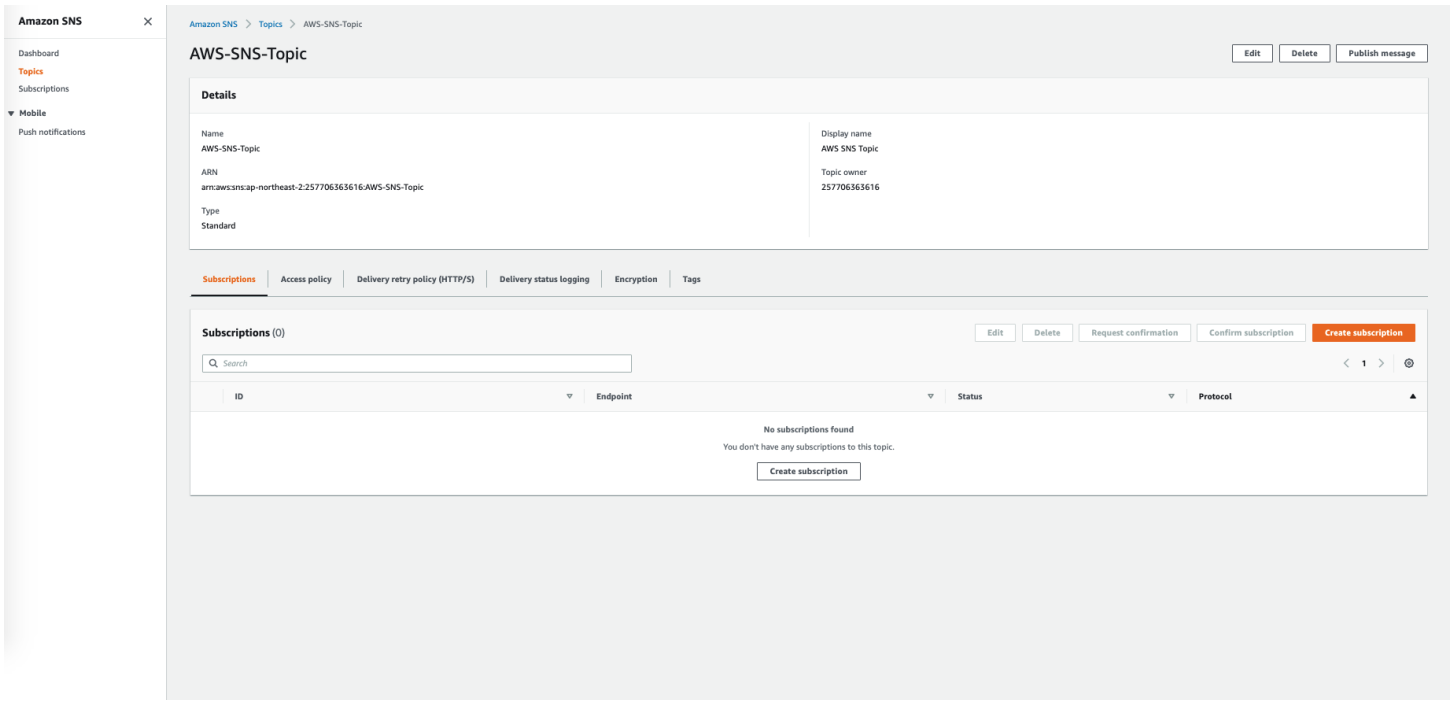
Step 4. Check Topic is created successfully.



Set up a Subscription on AWS SNS

Once Topic has created, as above. Please, set subscription.

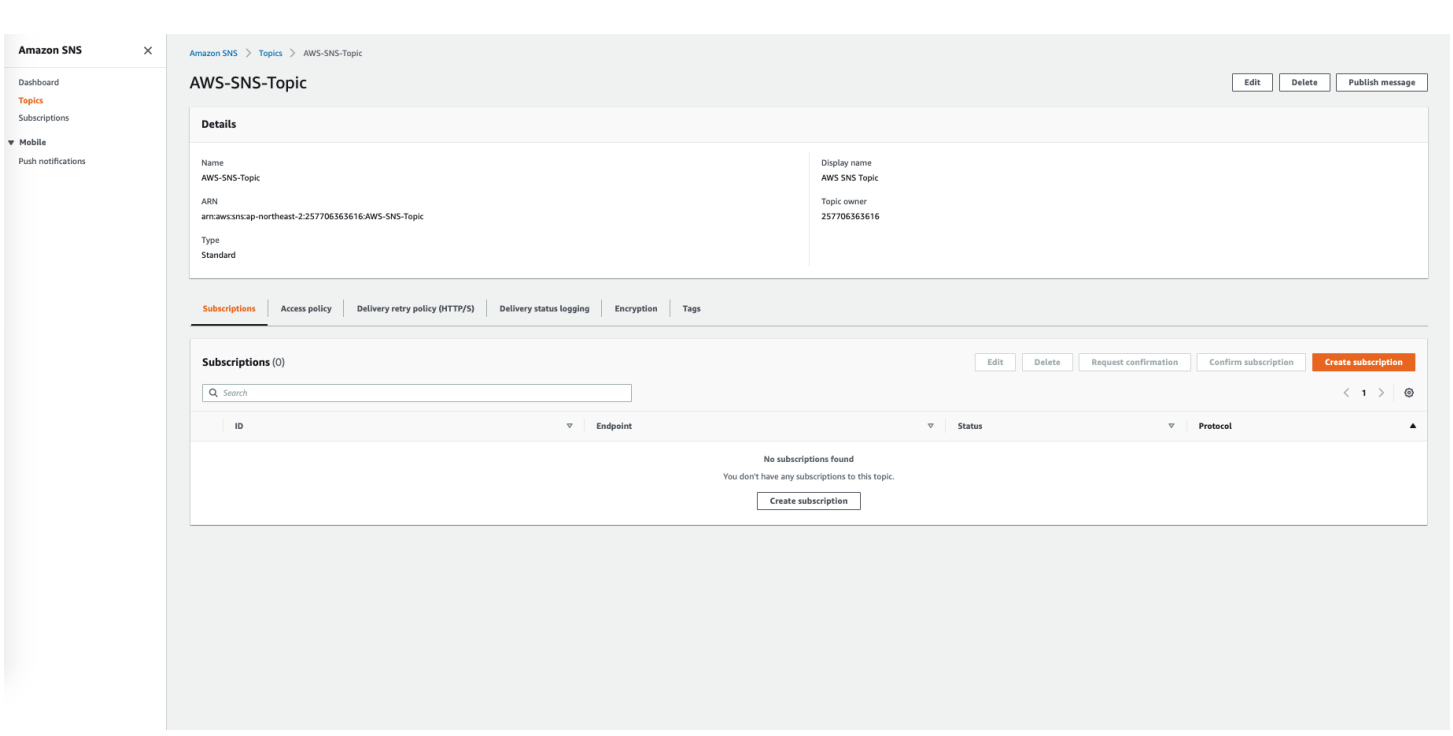
Step 1. Log in AWS Console > SNS > Topics > Select Topic that you would like to set up a subscription and then Click `Create subscription`



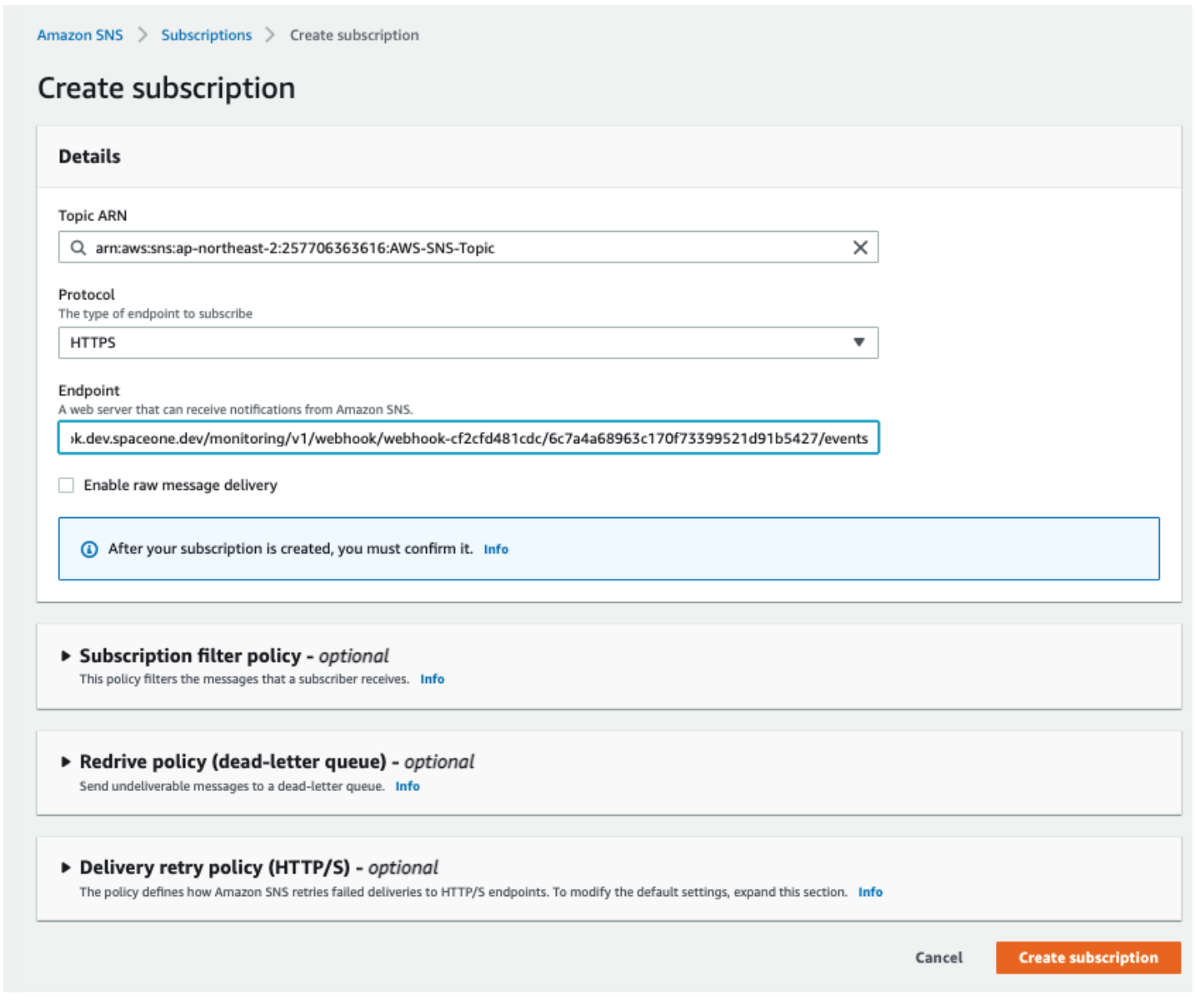
Step 2. Type or select each required fields and Click `Create subscription` button to Create subscription

Protocol : HTTPS

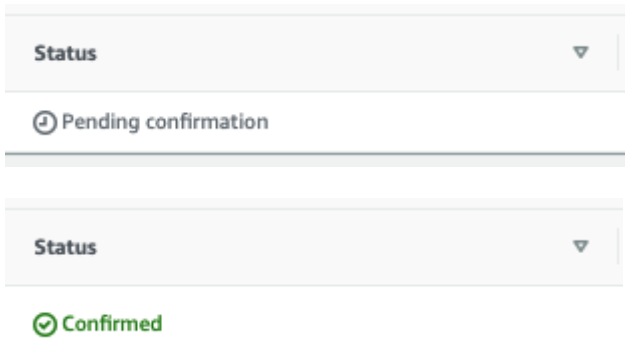
Endpoint : Webhook URL that you create from **SpaceONE******



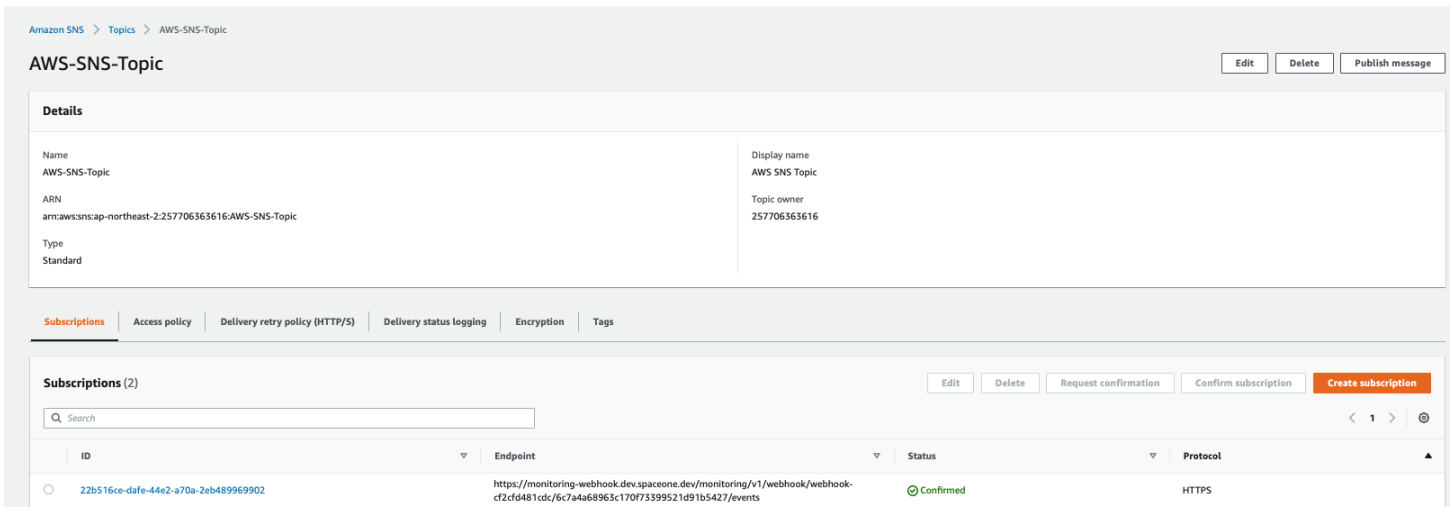
Step 3. Check created subscription under AWS Console > SNS > Topics > AWS-SNS (Created Topic)



Step 4. Check Status has changed after create a new subscription from `Pending confirmation` to `Confirmed` as below



Step 5. You are ready to get SNS message through Webhook once status updated as `Confirmed`



6.3.2 - Grafana Webhook

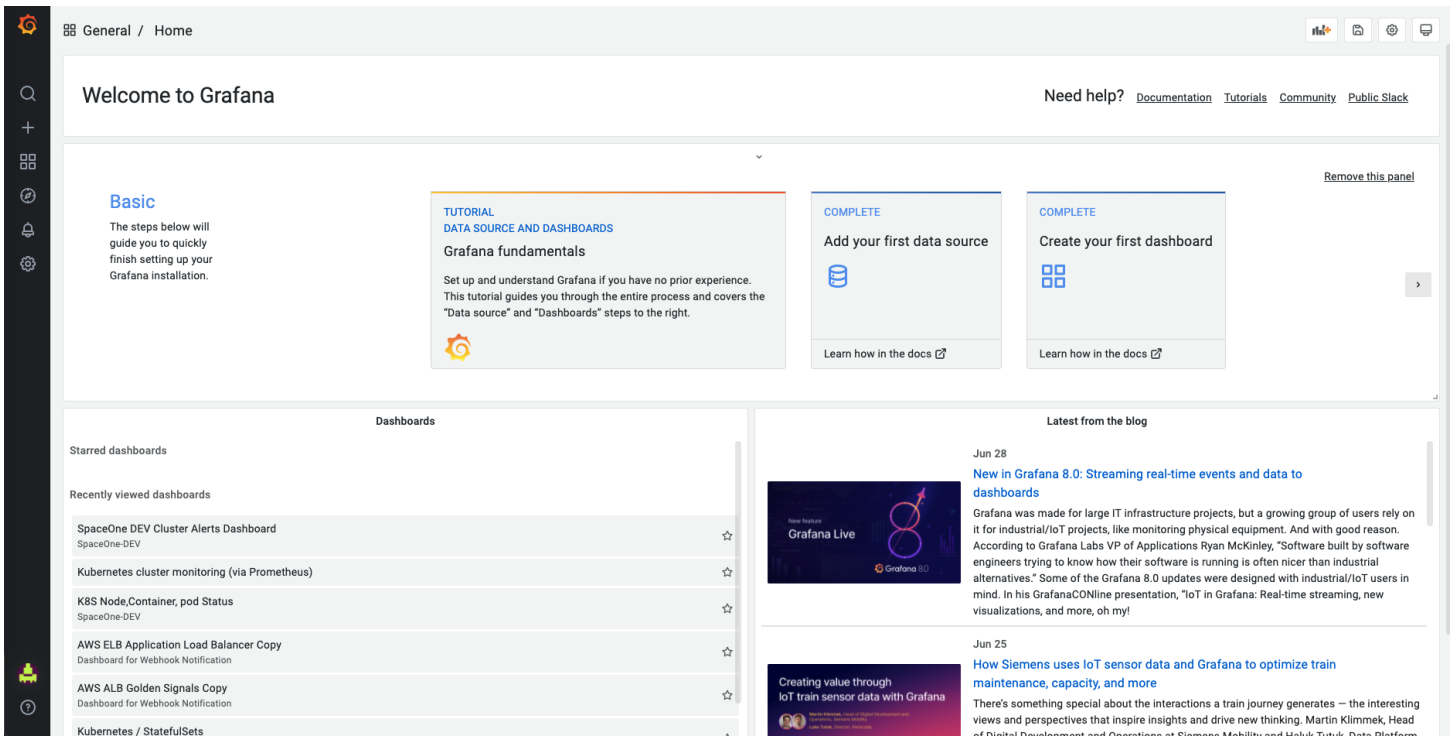
Monitoring Service

Set up a Webhook at Grafana

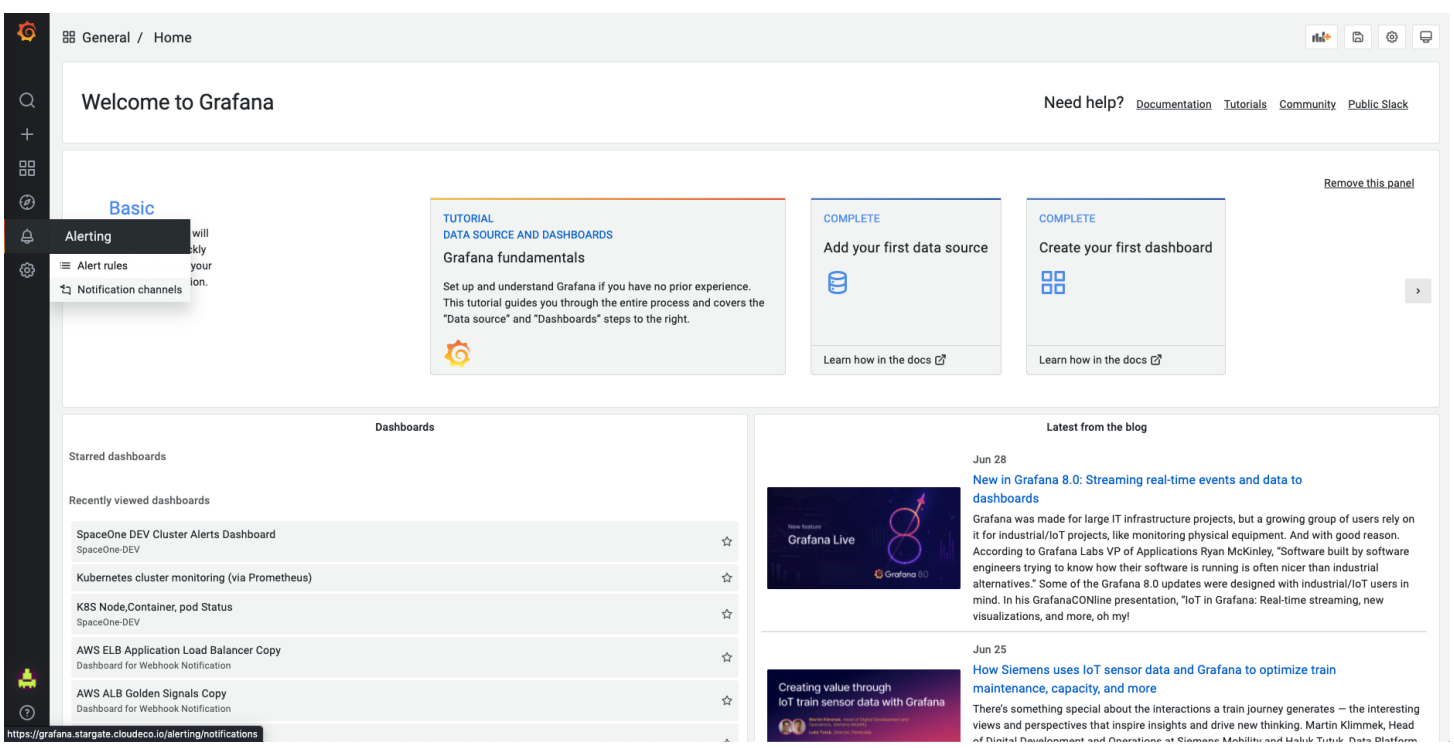
To Connect your Grafana with **SpaceONE's Alert Manager**, Set up Grafana's Notification Channels.
Please set the alerting channel with following steps
Set up a Notification Channel ****

Set up a Notification Channels

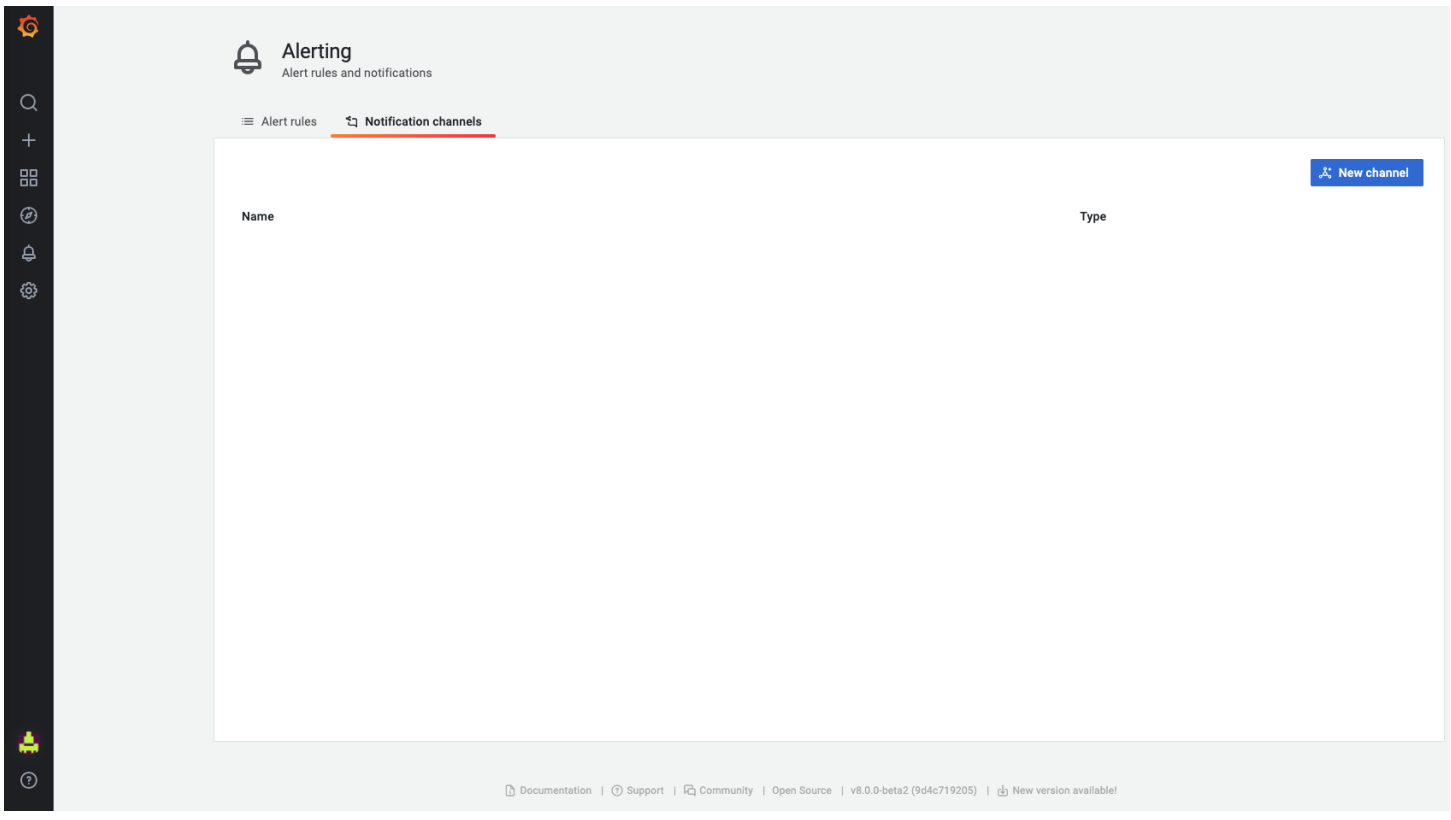
Step 1. Drive to Grafana on Browser



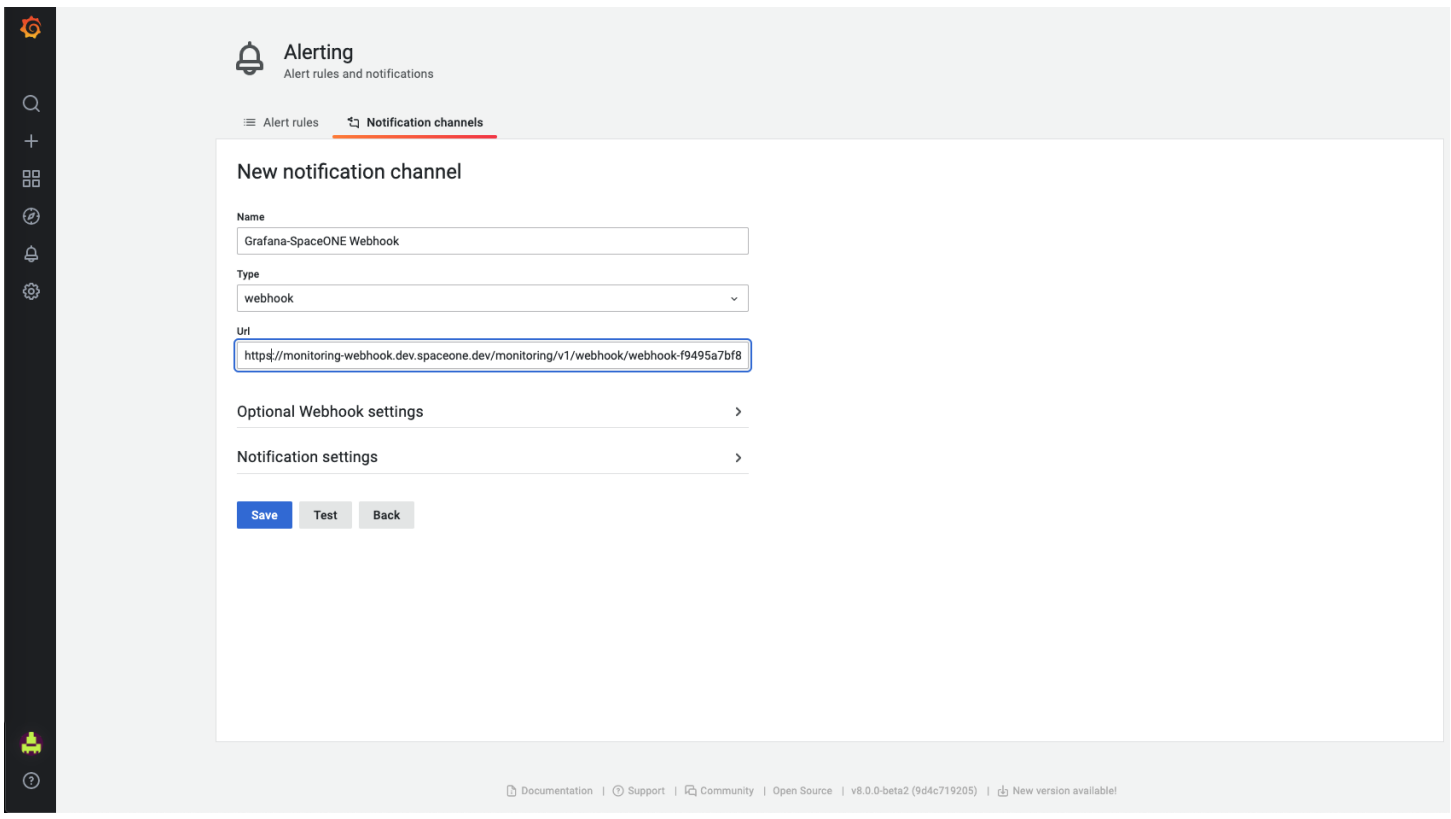
Step 2. Drive to Notification Channel on Browser



Step 3. Click `New Channel` button

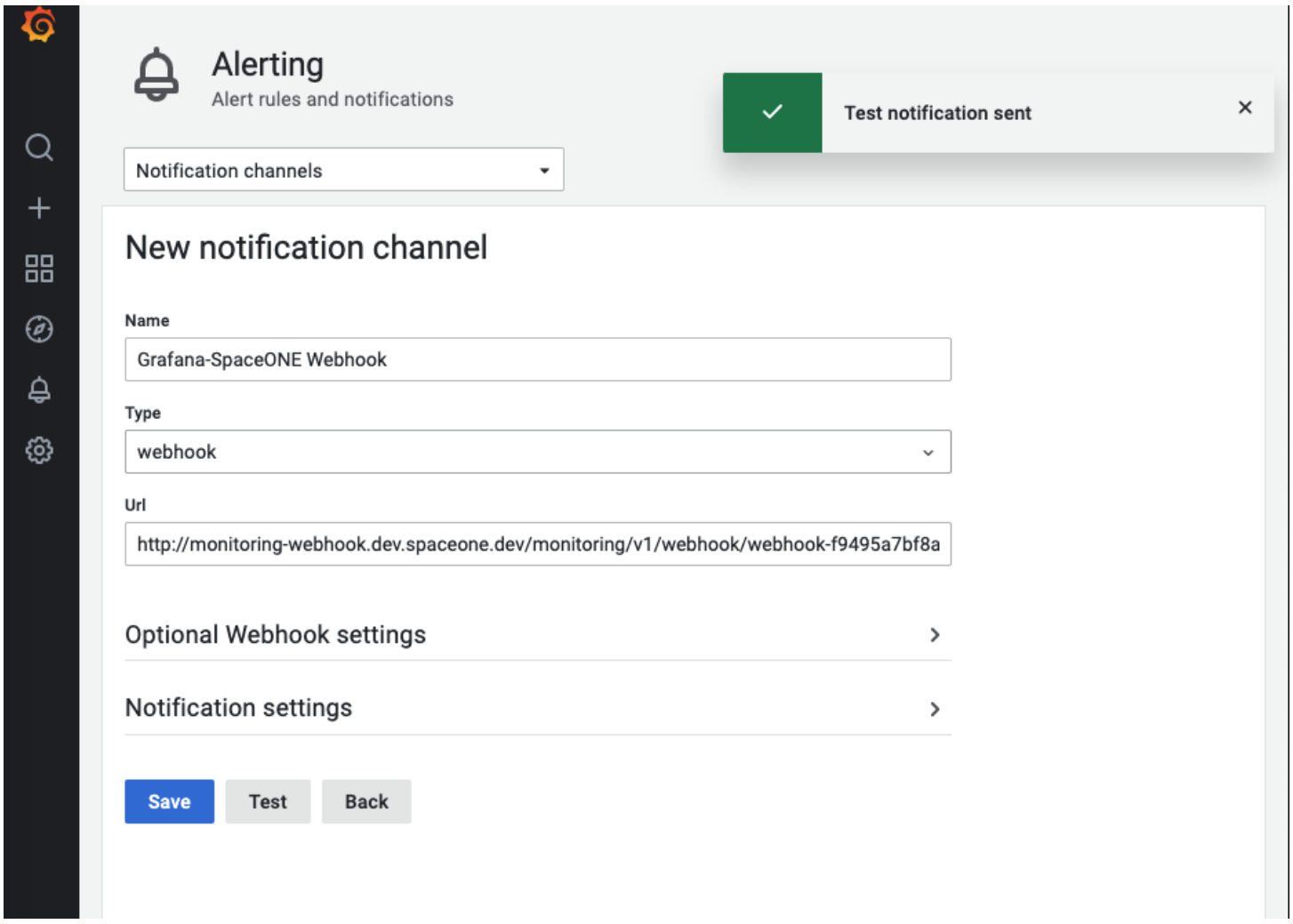


Step 4. Type name, [Webhook URL(from SpaceONE)] and Select Type of Channel as webhook

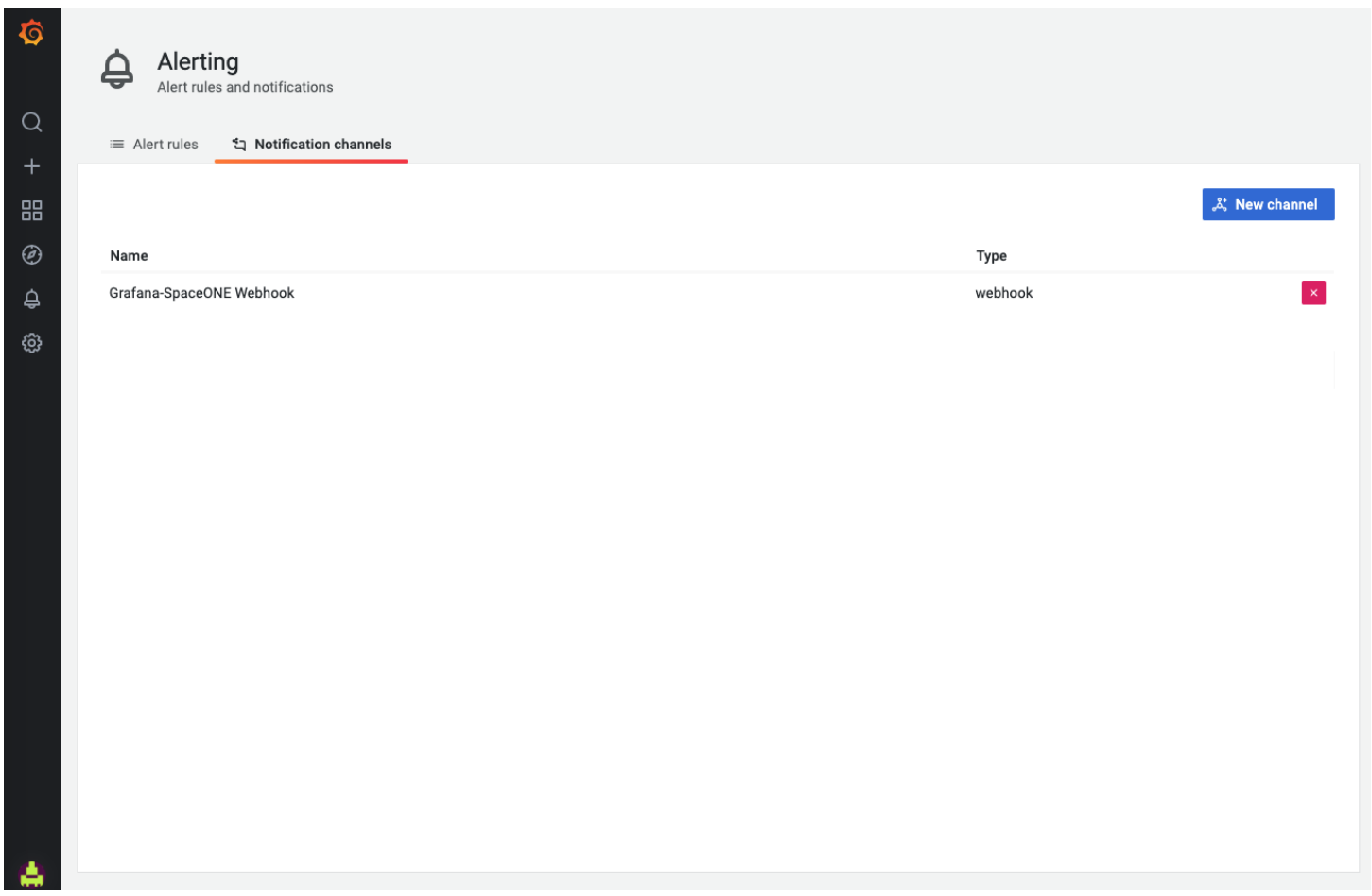


Grafana Webhook URL accepts only **HTTP** Protocol**.**
Created Webhook ****URL from **SpaceONE** is **HTTPS** but **HTTP** works as well**.
Please,** type ****URL ****as **HTTP like `http://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/...` **

Step 5. Please, Test URL by clicking Test button and then you will see pop up message that says Test Notification Sent.



Step 6. Click Save button and Check Notification Channel has successfully created.



6.3.3 - Zabbix Webhook

Monitoring service plugin zabbix webhook configuration guide

Set up a Webhook at Zabbix

To Connect **SpaceONE's Alert Manager,** Set up Zabbix's Webhook Media Type.
Please, Set Alerting Channel for following Steps

Set up a Zabbix Webhook Media

Step 1. Log in to Zabbix browser as Administrator
Step 2. Move to Media Type menu
Administration on Left menu -> `Media Types`
Step 3. Create New Media Type
Click on Create `media type` on the right-top.
Step 4. Fill out the Webhook information
Name: SpaceONE Webhook
Type: Webhook
Parameter: Add parameter information as a below

Name	Value
eventDate	{EVENT.DATE}
eventID	{EVENT.ID}
eventName	{EVENT.NAME}
eventSeverity	{EVENT.SEVERITY}
eventStatus	{EVENT.STATUS}
eventTime	{EVENT.TIME}
hostConn	{HOST.CONN}
hostID	{HOST.ID}
hostname	{HOST.HOST}
hostVisibleName	{HOST.NAME}
itemID	{ITEM.ID}
itemKey	{ITEM.KEY}
itemValue	{ITEM.VALUE}
message	{ALERT.MESSAGE}
title	{ALERT.SUBJECT}
to	{ALERT.SENDTO}
triggerID	{TRIGGER.ID}
triggerName	{TRIGGER.NAME}

Name	Value
triggerSeverity	{TRIGGER.SEVERITY}
triggerStatus	{TRIGGER.STATUS}
webhookURL	<<YOUR_ZABBIX_WEBHOOK_URL>>

Parameters

Name	Value	Action
eventDate	{EVENT.DATE}	Remove
eventID	{EVENT.ID}	Remove
eventName	{EVENT.NAME}	Remove
eventSeverity	{EVENT.SEVERITY}	Remove
eventStatus	{EVENT.STATUS}	Remove
eventTime	{EVENT.TIME}	Remove
hostConn	{HOST.CONN}	Remove
hostID	{HOST.ID}	Remove
hostname	{HOST.HOST}	Remove
hostVisibleName	{HOST.NAME}	Remove
itemID	{ITEM.ID}	Remove
itemKey	{ITEM.KEY}	Remove
itemValue	{ITEM.VALUE}	Remove
message	{ALERT.MESSAGE}	Remove
title	{ALERT.SUBJECT}	Remove
to	{ALERT.SENDTO}	Remove
triggerID	{TRIGGER.ID}	Remove
triggerName	{TRIGGER.NAME}	Remove
triggerSeverity	{TRIGGER.SEVERITY}	Remove
triggerStatus	{TRIGGER.STATUS}	Remove
webhookURL	https://monitoring-webhook.dev.sp	Remove

Add

You can check the WebhookURL in the project page -> webhook list on SpaceONE Console.

script: Copy and use the code below.

```
var params = JSON.parse(value),
req = new CurlHttpRequest(),
resp;
req.AddHeader('Content-Type: application/json');

var params = JSON.parse(value);
payload = {};
payload.title = params.title;
payload.message = params.message;
payload.to = params.to;

payload.event = {};
payload.event.id = params.eventID;
payload.event.name = params.eventName;
payload.event.date = params.eventDate;
payload.event.time = params.eventTime;
payload.event.status = params.eventStatus;
payload.event.severity = params.eventSeverity;

payload.item = {};
payload.item.id = params.itemID;
payload.item.key = params.itemKey;
payload.item.value = params.itemValue;

payload.trigger = {};
payload.trigger.id = params.triggerID;
payload.trigger.name = params.triggerName;
payload.trigger.severity = params.triggerSeverity;
payload.trigger.status = params.triggerStatus;

payload.host = {};
payload.host.id = params.hostID;
payload.host.connection_info = params.hostConn;
payload.host.name = params.hostname;
payload.host.visible_name = params.hostVisibleName;


resp = req.Post(params.webhookURL,
JSON.stringify(payload)
        );
return resp;
```

JavaScript

```
1  var params = JSON.parse(value),
2  req = new CurlHttpRequest(),
3  resp;
4  req.AddHeader('Content-Type: application/json');
5
6  var params = JSON.parse(value);
7  payload = {};
8  payload.title = params.title;
9  payload.message = params.message;
10 payload.to = params.to;
11
12 payload.event = {};
13 payload.event.id = params.eventID;
14 payload.event.name = params.eventName;
15 payload.event.date = params.eventDate;
16 payload.event.time = params.eventTime;
17 payload.event.status = params.eventStatus;
18 payload.event.severity = params.eventSeverity;
19
20 payload.item = {};
21 payload.item.id = params.itemID;
22 payload.item.key = params.itemKey;
23 payload.item.value = params.itemValue;
24
25 payload.trigger = {};
26 payload.trigger.id = params.triggerID;
27 payload.trigger.name = params.triggerName;
28 payload.trigger.severity = params.triggerSeverity;
29 payload.trigger.status = params.triggerStatus;
30
31 payload.host = {};
32 payload.host.id = params.hostID;
33 payload.host.connection_info = params.hostConn;
34 payload.host.name = params.hostname;
35 payload.host.visible_name = params.hostVisibleName;
36
37
```

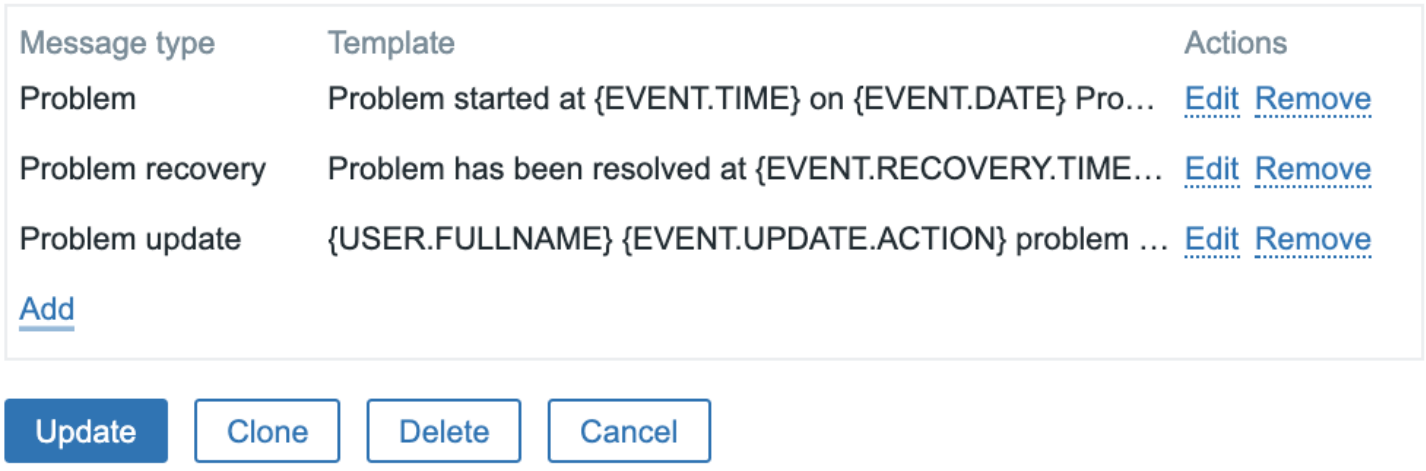
64424 symbols remaining

Apply Cancel

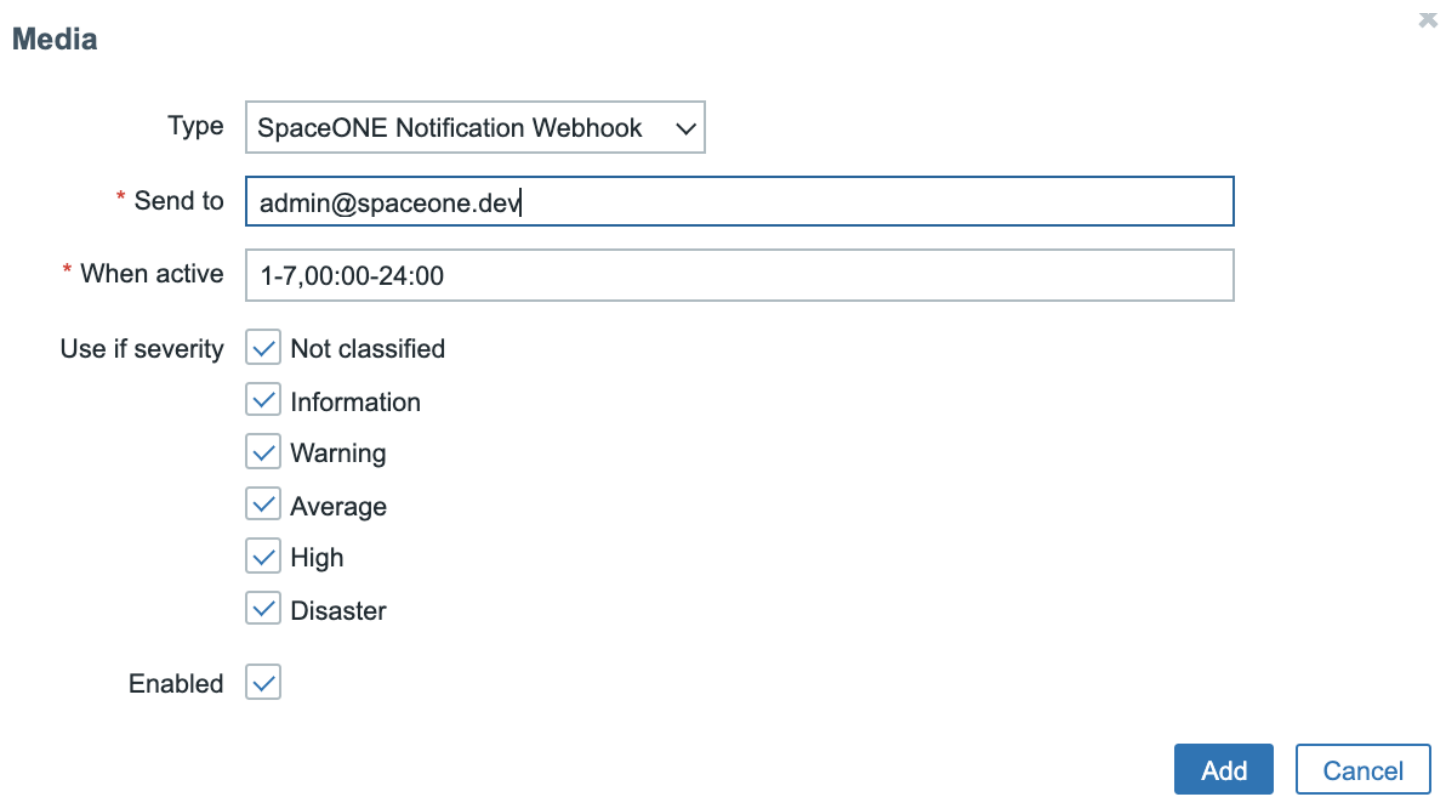
Step 5. Add the message templates
Move to Message templates tab and Click on Add button to add template.
Add 3 templates.

Message Type	Description
Problem	When a problem event occurs, it is send as a message in this format.
Problem recovery	When the problem event is resolved, it is sent as a message in this format.
Problem update	When the problem event is updated, it is sent as a message in this format.

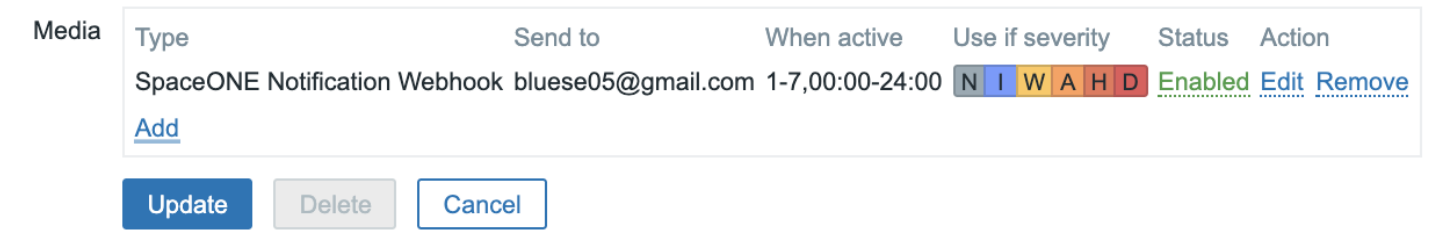
The subject and message can be used as they are in the given format or filled in after editing the content you want.



Step 6. Add media to Users
If webhook setting is completed in media type, add the webhook media to user.
Move to `Users` menu. `Administration` on Left menu -> `Users` . Select the user you want to set up and go to the Media tab.
Click on `Add` button to add a webhook media.
Step 7. Fill out the Media information
Type: Select the Webhook media type name created above.
Send to: Although it is a value that is not actually used, it is a required parameter, so you can use any information. (email or name)
When active: Use the given default value without modifying it (1-7,00:00-24:00). The actual schedule will be executed by `SpaceONE's Alert manager` .
Use if severity: Checked all
Enabled: Checked



When the setting is complete, click the `Add` button to complete the setting.



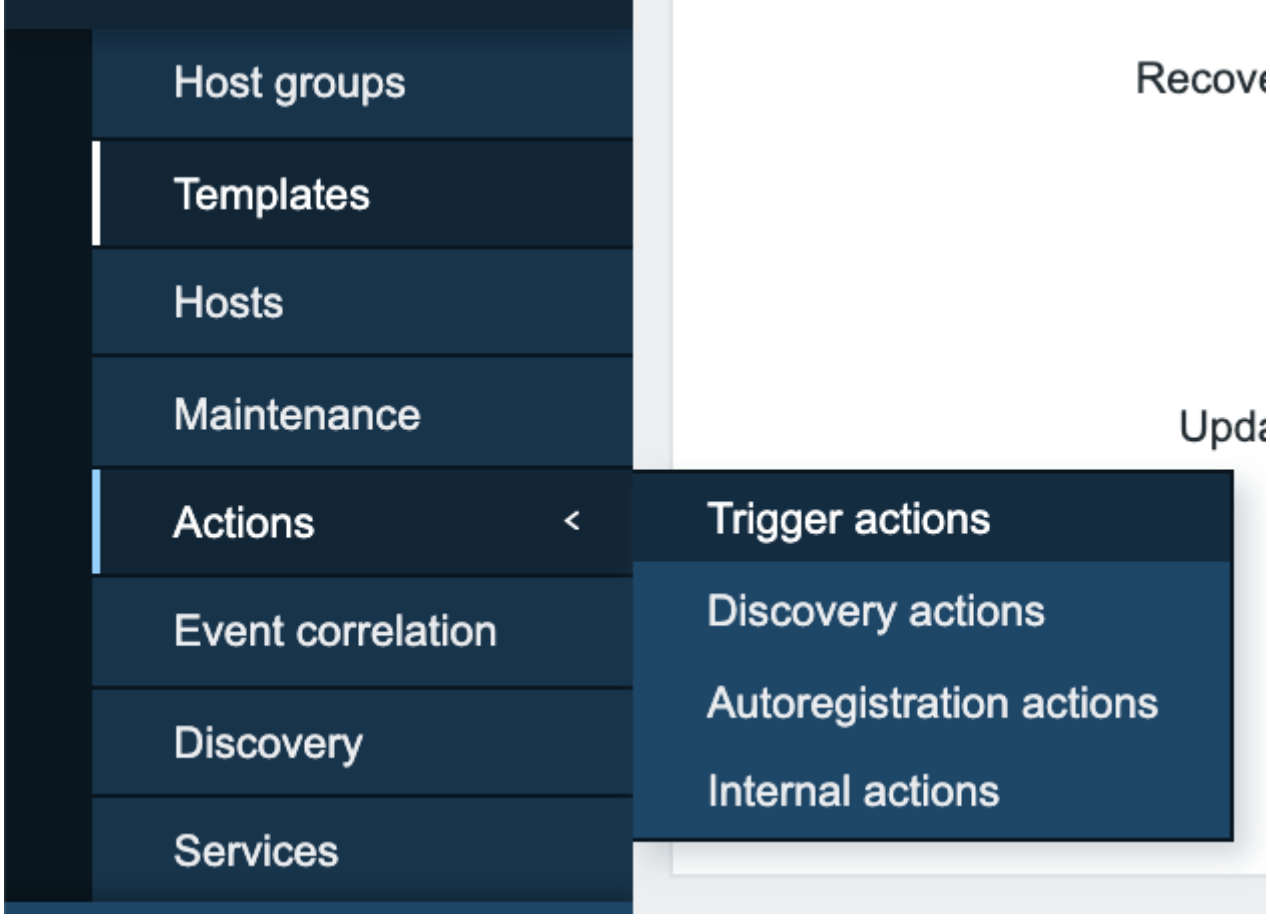
Finally, click the update button to finish.

Step 8. Add Trigger Action

Up to now, the settings for the webhook itself and the settings for the user who will use the webhook have been added.

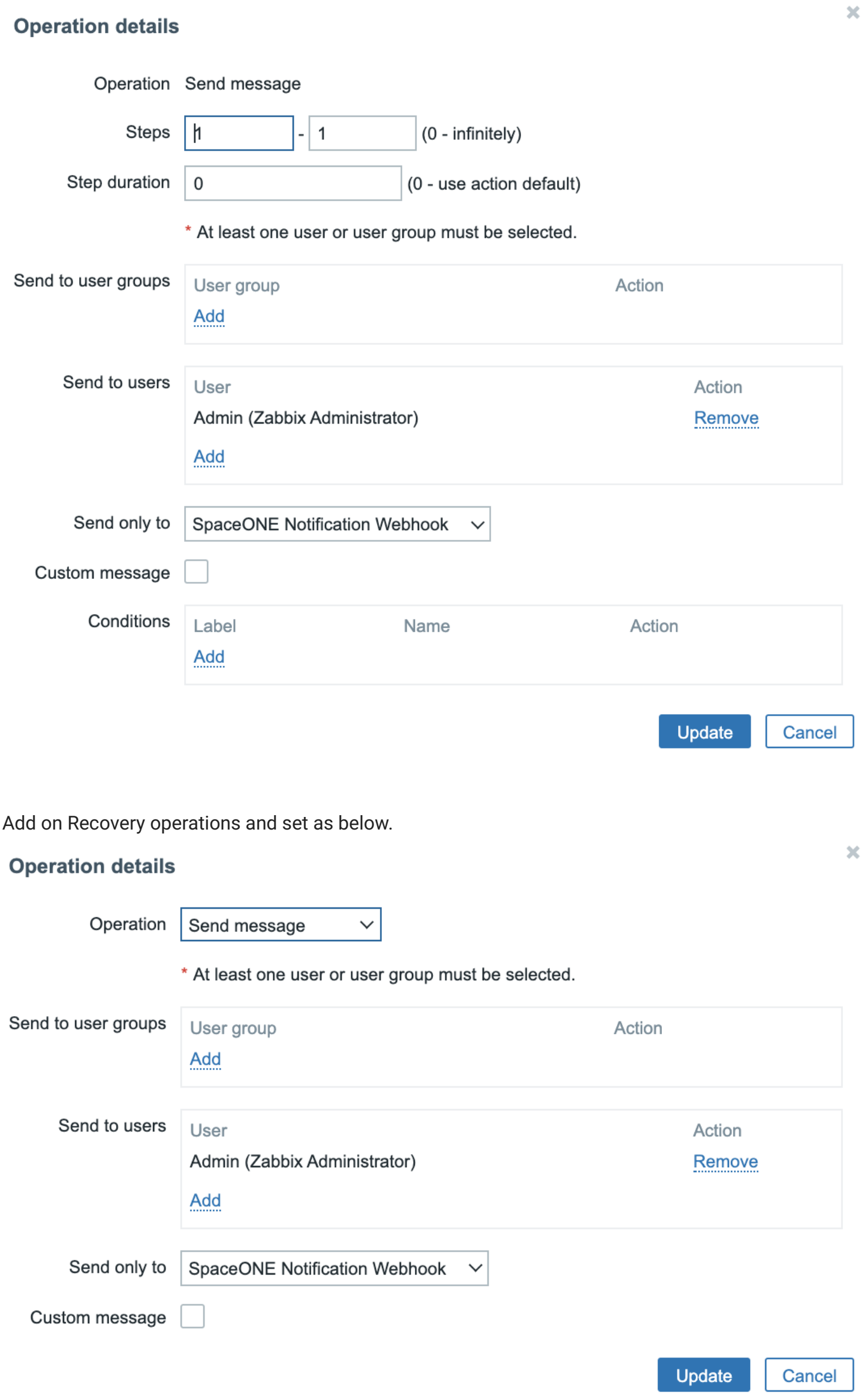
From now on, we will set up to send a message to the user who has set up a webhook when a specific event occurs.

Move to `Trigger actions` menu. `Configuration` on Left menu -> `Actions` -> `Trigger actions` .



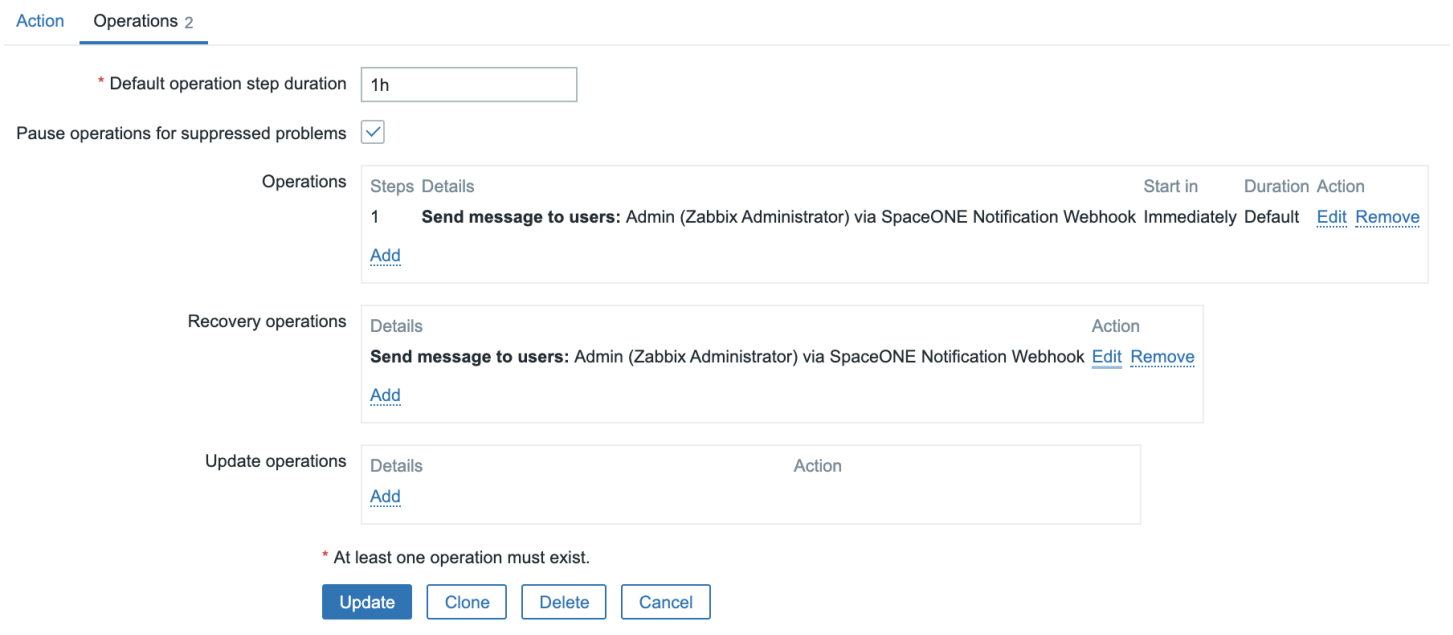
Click on `Create action` button on the right-top. Name: SpaceONE Webhook

Move to `Operations` tab. Add on `Operations` and set as below.



Add on Recovery operations and set as below.

Finally, the settings of the Operations tab.


Action
Operations 2
* Default operation step duration
1h
Pause operations for suppressed problems
Operations
Steps Details Start in Duration Action
1 Send message to users: Admin (Zabbix Administrator) via SpaceONE Notification Webhook Immediately Default Edit Remove
Add
Recovery operations
Details Action
Send message to users: Admin (Zabbix Administrator) via SpaceONE Notification Webhook Edit Remove
Add
Update operations
Details Action
Add
* At least one operation must exist.
Update
Clone
Delete
Cancel

7 - Notification

Notification Service & Plugins

About Notification

How It Works

용어 정의

용어	설명
Alarm	
Subscriber	
Channel	
Topic	

7.1 - Protocol Settings

Notification Protocol Plugin Setting Guide

7.1.1 - Voice Call Protocol

Notification Plugin Voice Call Protocol Configuration Guide

Overview

You can receive voice call ***alert*** message and return ***acknowledge*** via mobile.

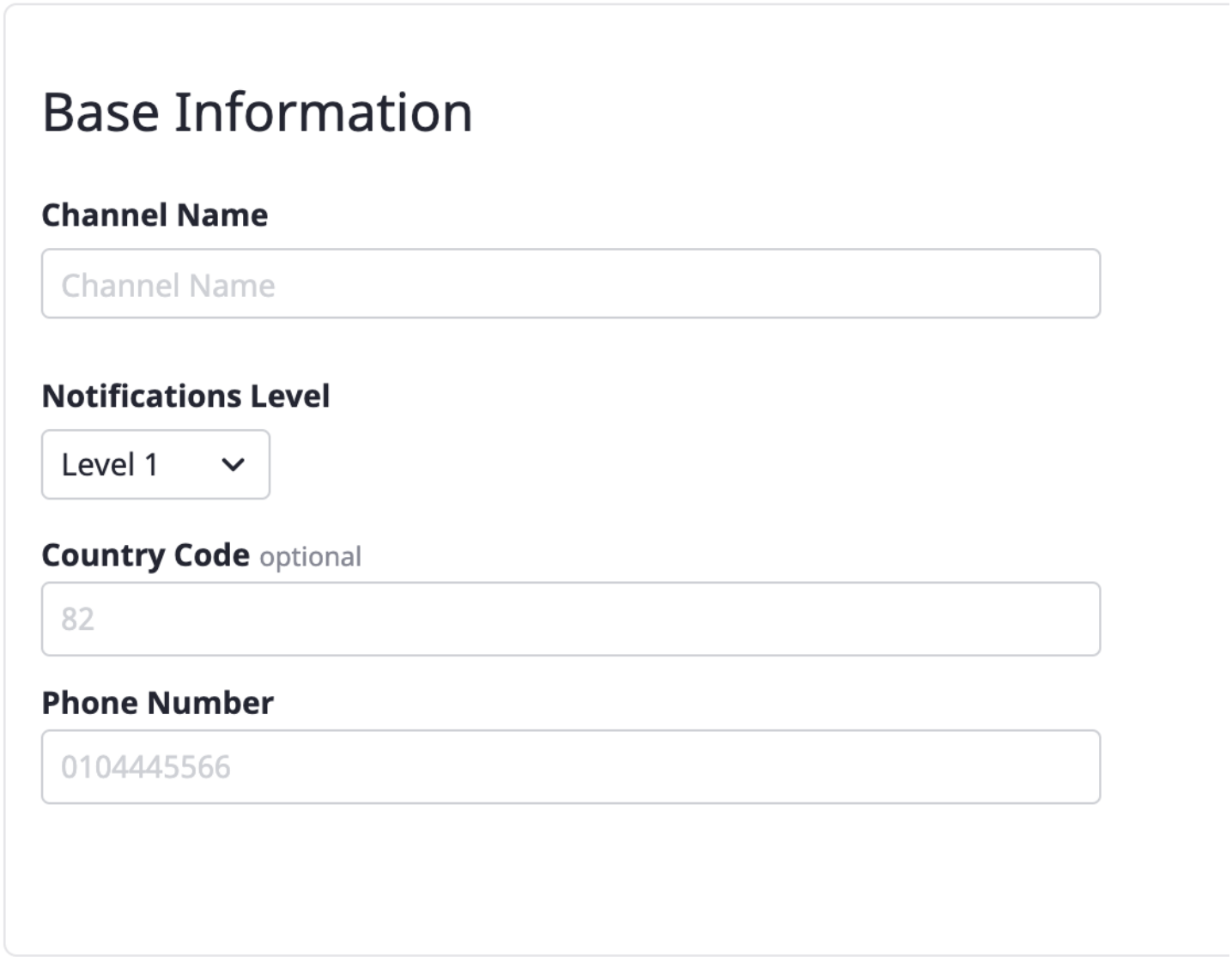
Prerequisites

There are not any requirements. Voice Call Protocol will be supported by ***AWS direct call*** in future release.

Add Voice Call Channel to your Project / User in SpaceONE

Go to ***`SpaceONE Console > Project > Notifications`*** which you want to get alerts.

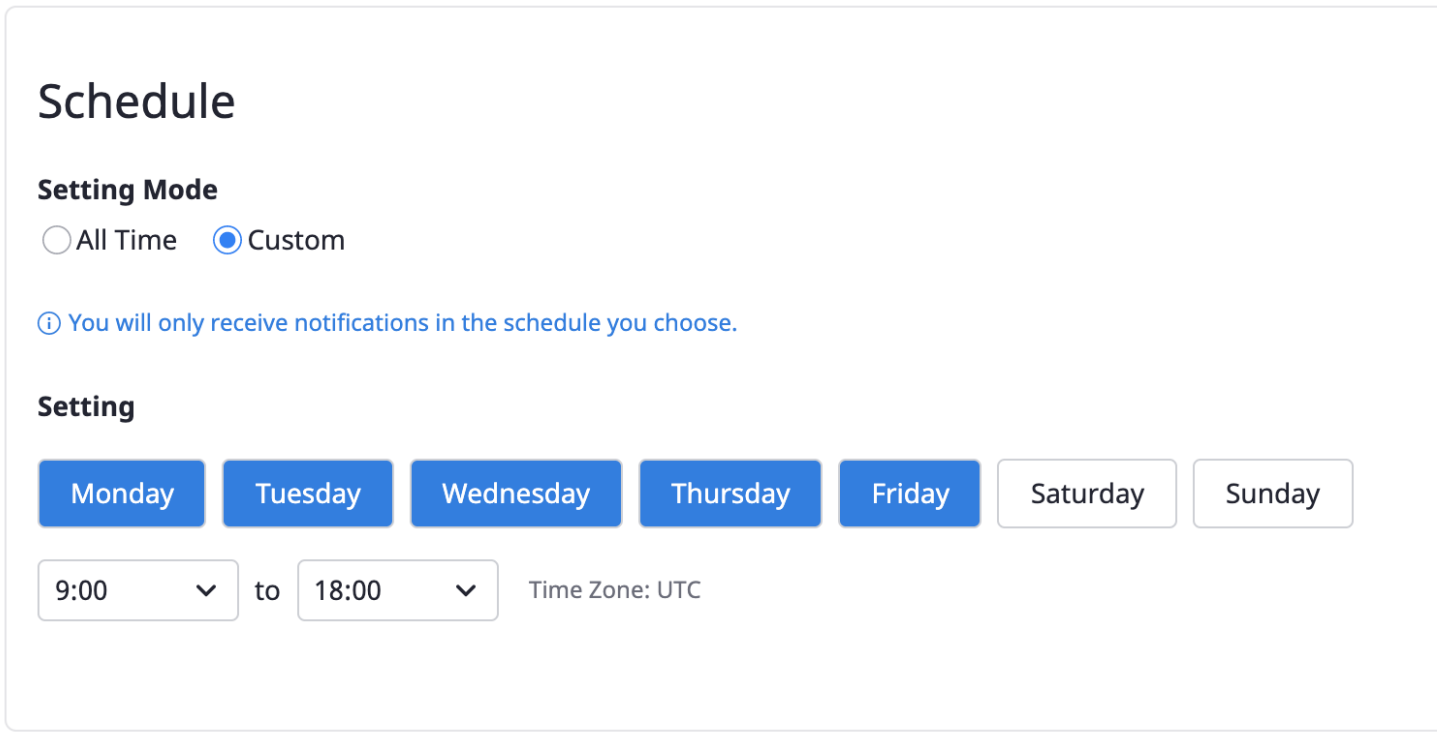
Basic Information



Item	Descriptions
Channel Name	Notification channel name
Notification Level	Which level to be placed in escalation policy, see Escalation Policy for details
Country Code	Region code for mobile phone(Default 82)
Phone Number	Mobile phone number

Notification Schedule

You can select when to receive alarm. There two options



Setting Mode	Descriptions
All Time	Receive alert notification any time
Custom	Receive alert notification within designated time period

Topic

Notification subscribes topics to check which alarm to send

About Notification Topics

Now only monitoring.Alert topics are available. Other topics will be created in future release.
Just pin ***Setting Mode*** to ***Receive all notifications***

Setting Mode	Descriptions
Receive all notifications	Allow notification channel to send all alert messages from ***any topics***
Receive notifications based on selected topics	Allow notification channel to send alert message from ***selected topics***

7.1.2 - SMS Protocol

Notification Plugin SMS Protocol Configuration Guide

Overview

You can receive SMS alert message and return acknowledge via mobile.

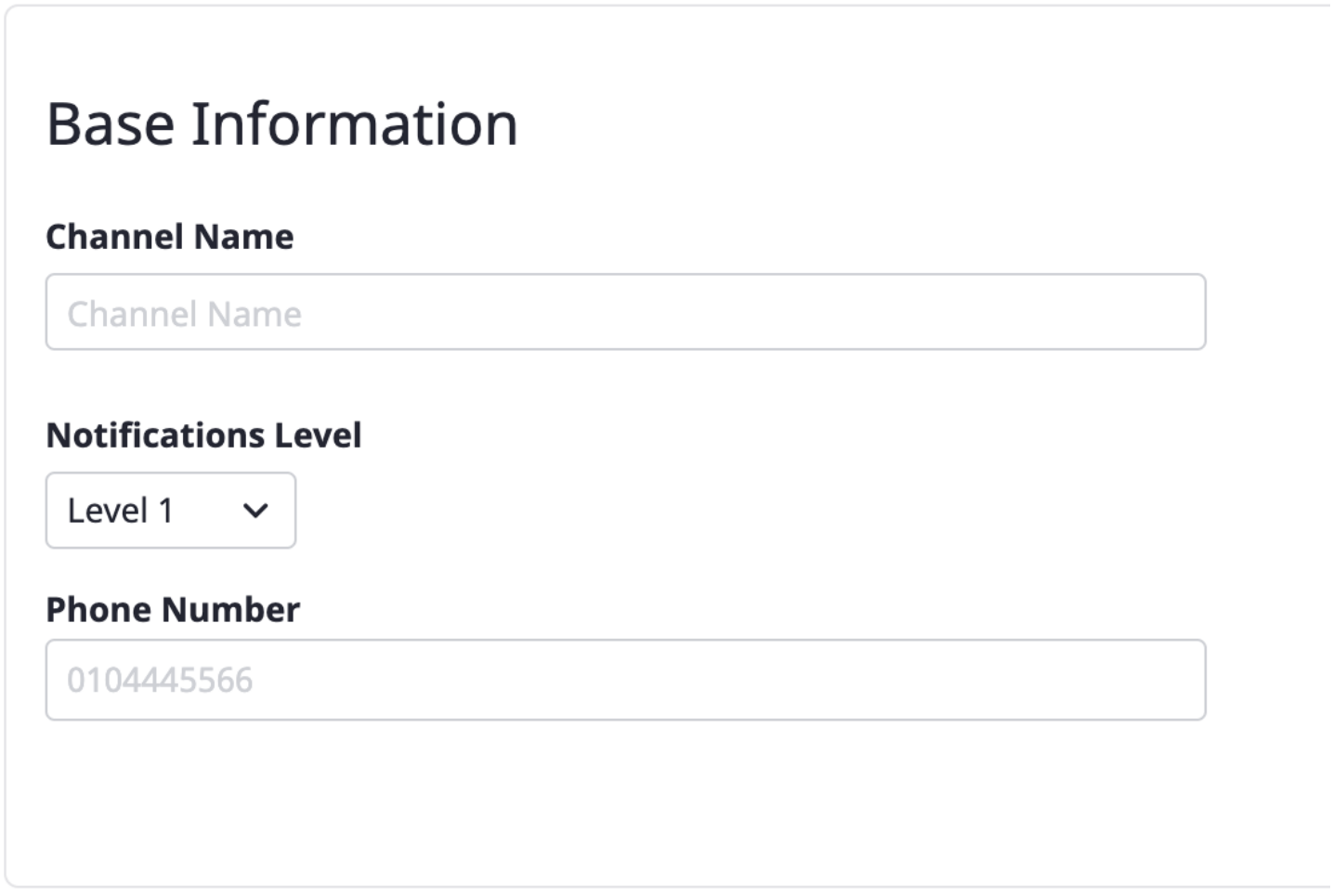
Prerequisites

There are not any requirements. SMS Protocol will be supported by AWS SNS in future release.

Add SMS Channel to your Project / User in SpaceONE

Go to ***SpaceONE Console > Project > Notifications*** which you want to get alerts.

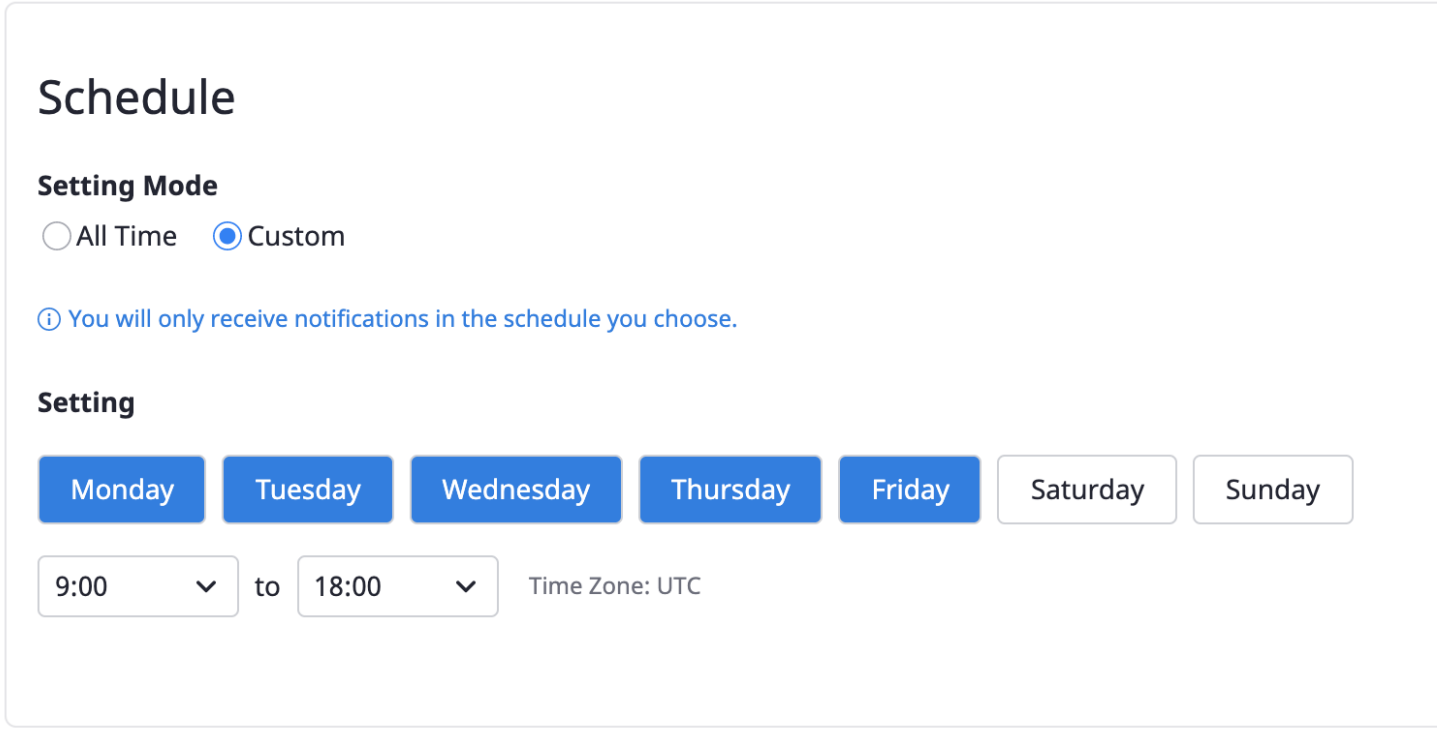
Basic Information



Item	Descriptions
Channel Name	Notification channel name
Notification Level	Which level to be placed in escalation policy, see Escalation Policy for details
Phone Number	Mobile phone number to receive sms message

Notification Schedule

You can select when to receive alarm. There two options



Setting Mode	Descriptions
All Time	Receive alert notification any time
Custom	Receive alert notification within designated time period

Topic

Notification subscribes topics to check which alarm to send

About Notification Topics

Now only monitoring.Alert topics are available. Other topics will be created in future release.
Just pin ***Setting Mode*** to ***Receive all notifications***

Setting Mode	Descriptions
Receive all notifications	Allow notification channel to send all alert messages from ***any topics***
Receive notifications based on selected topics	Allow notification channel to send alert message from ***selected topics***

7.1.3 - Email Protocol

Notification plugin Email protocol configuration guide

Overview

You can receive email ***alert*** message and return ***acknowledge*** .

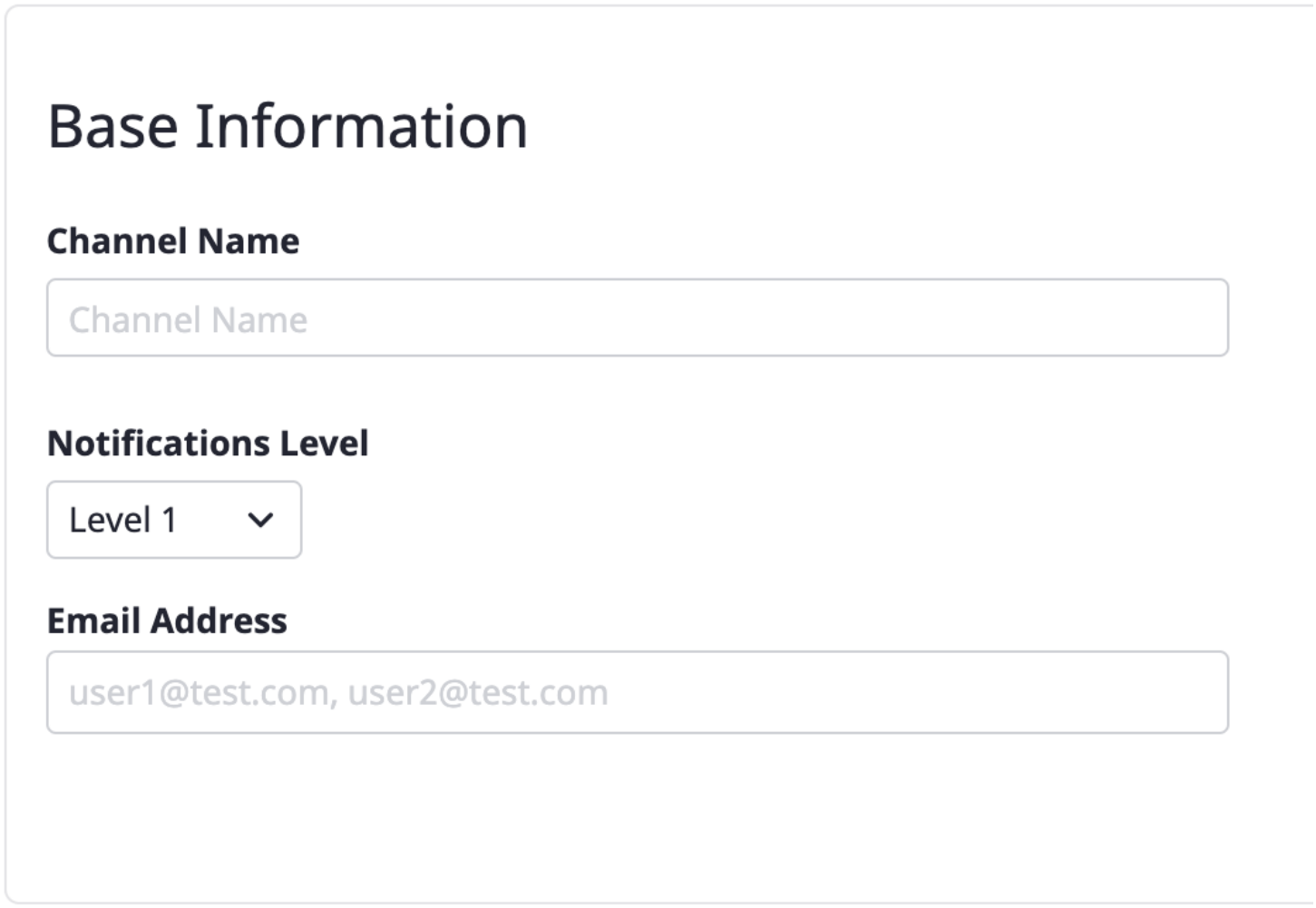
Prerequisites

There are not any requirements. Email Protocol will be supported by ***AWS SES*** in future release.

Add Email Channel to your Project / User in SpaceONE

Go to ***`SpaceONE Console > Project > Notifications`*** which you want to get alerts.

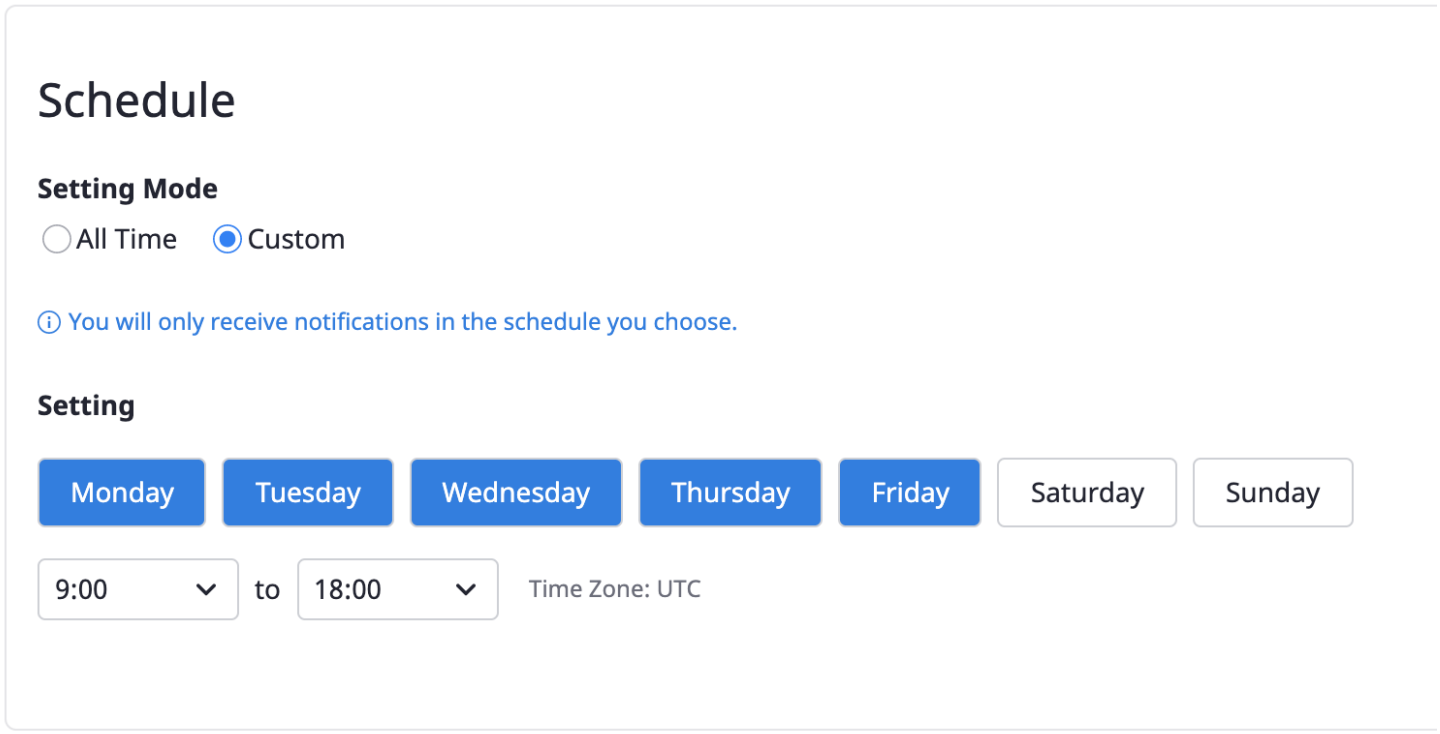
Basic Information



Item	Descriptions
Channel Name	Notification channel name
Notification Level	Which level to be placed in escalation policy, see Escalation Policy for details
Email Address	Email address to receive alert message. Multiple email address can be registered(ex. test1@test.com,test2@test.com)

Notification Schedule

You can select when to receive alarm. There two options



Setting Mode	Descriptions
All Time	Receive alert notification any time
Custom	Receive alert notification within designated time period

Topic

Notification subscribes topics to check which alarm to send

About Notification Topics

Now only monitoring.Alert topics are available. Other topics will be created in future release.
Just pin ***Setting Mode*** to ***Receive all notifications***

Setting Mode	Descriptions
Receive all notifications	Allow notification channel to send all alert messages from ***any topics***
Receive notifications based on selected topics	Allow notification channel to send alert message from ***selected topics***

7.1.4 - Slack Protocol

Notification Plugin Slack Protocol Configuration Guide

Overview

We can also add `Slack` to our list of `Notification` channels. There are few prerequisites to use Slack Bot on SpaceONE notification service, and the following will guide you to your **SpaceONE** notification journey with your `Slack` workspace.

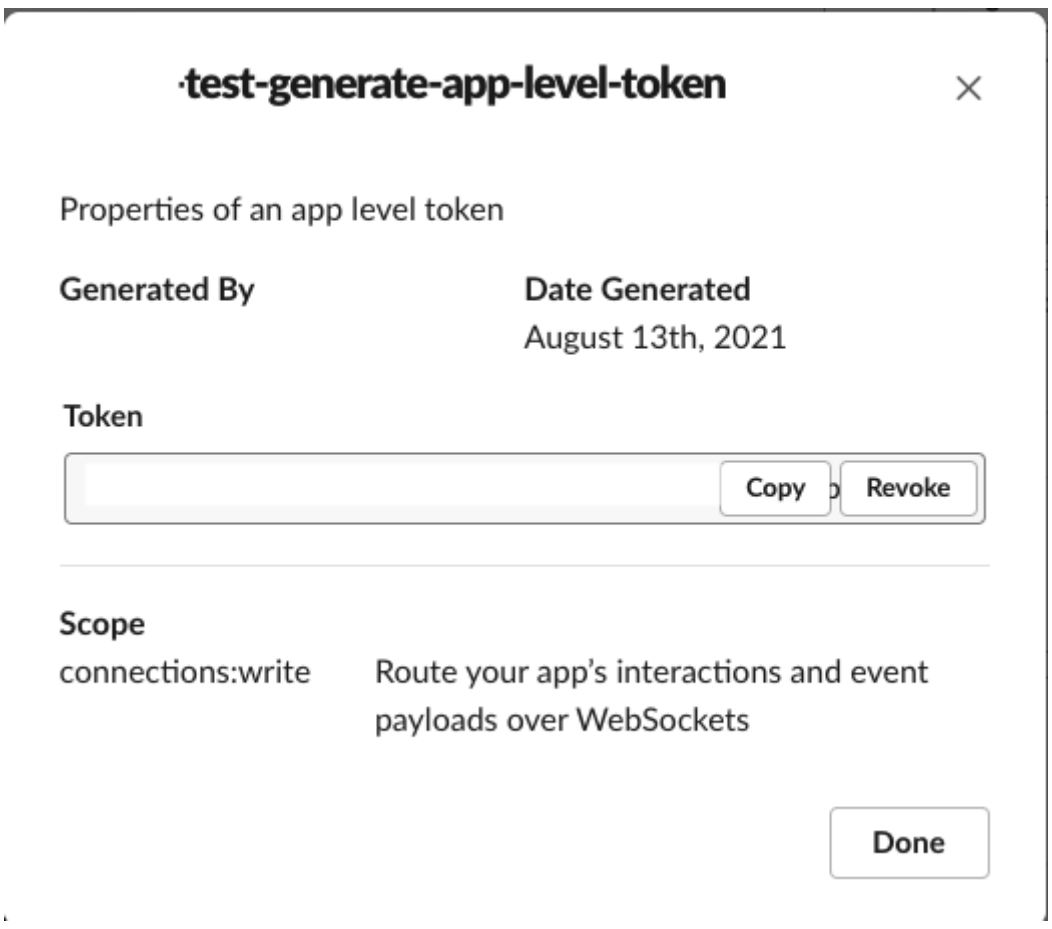
Prerequisites

Install the Slack app on your phone or PC. You will need a **OAuth Token** and **channel**.

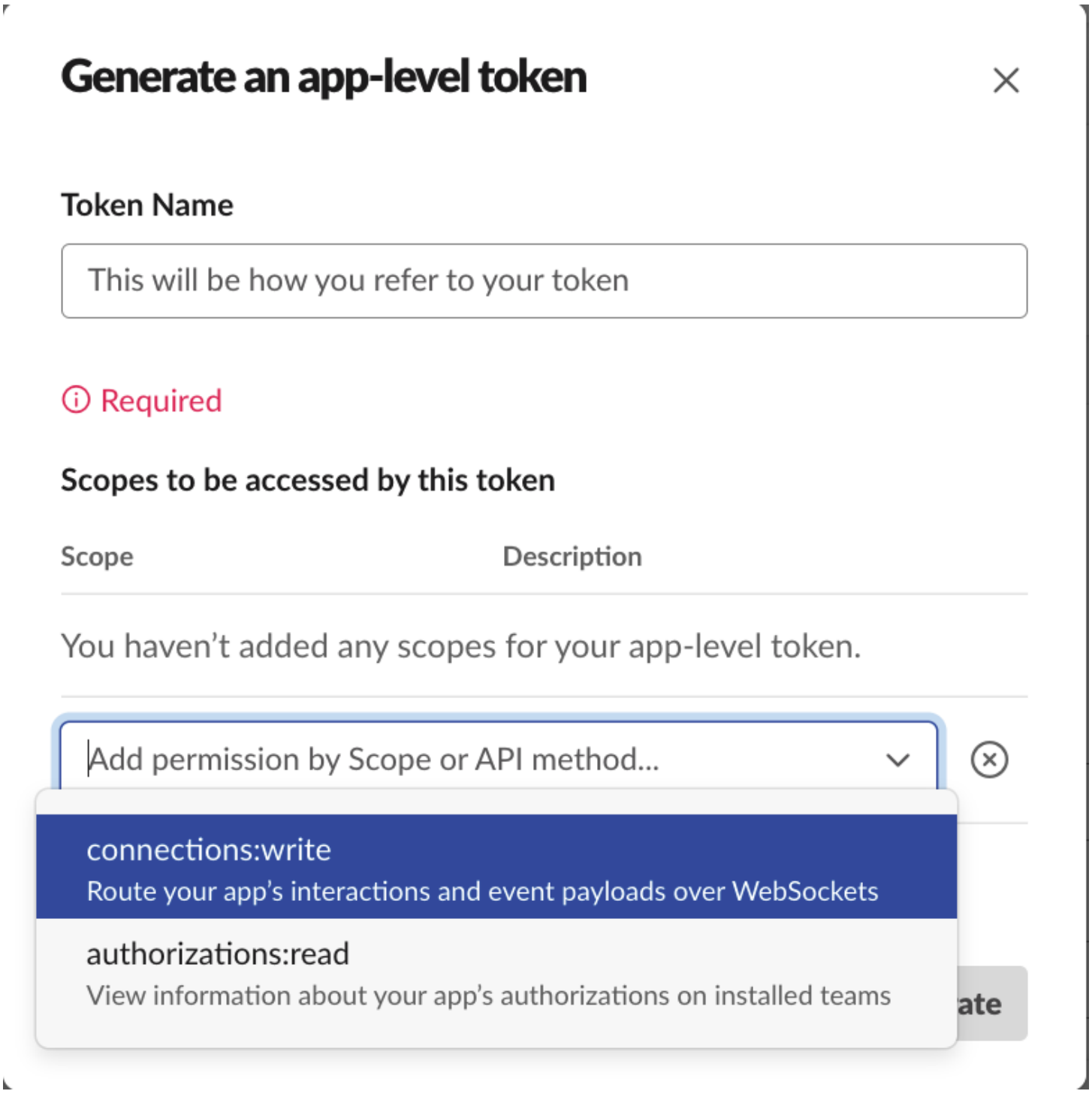
How to get Slack OAuth Token

Open the `Slack App Directory` of your Slack workspace. `Slack OAuth Token` is generated by creating a `slack app` and a `bot user`.
Slack OAuth token gives you the ability to handle things that relate to your app as a whole. To generate `Slack Access Token`, Follow the steps above:
Visit here and create a new slack app. Fill out your App Name and select the development workspace where you'll play around and build your app.

`OAuth & Permissions` section shows the information of tokens which allow your slack app to use features that apply to SpaceONE notification events. Copy the Token information in somewhere.



3. Go to `Scopes` section, you can add permission to access to slack channel. Click on 'Add an OAuth Scope' and select `chat:write` scope.



3. Go to `Basic Information` section, you can install your app by click on `Install to Workspace` button.

Token Information Alert

Token information need to be considered secure. Be sure not to share token

Display setting of SpaceONE Slackbot

Add Display settings to make your SpaceONE Slackbot even better.
Visit API Slack App and select your SpaceONE slack app.

Select the `Basic Information` in on the left menu and Find the `Display Information` section.

Fill out the App name and Short description.

Upload SpaceONE Slackbot icon on the `App icon & Preview` . Download the Bot image here.

How to generate Slack Bot users

Bot users are automated user accounts you can message with directly. You can eventually receive notification messages by inviting Bot User in your channel.
Go back to your slack workspace console.

Head to `Manage apps` page by click on `your_workspace_name` on the top-left corner > `Administration > Manage apps`

On the `Bot User` section, generate the Bot User and give it a name!

Go back to your slack workspace console again, and invite the bot by following steps:
Go to the channel

Click the channel's name, go to `Integrations` , and click `Add apps` .

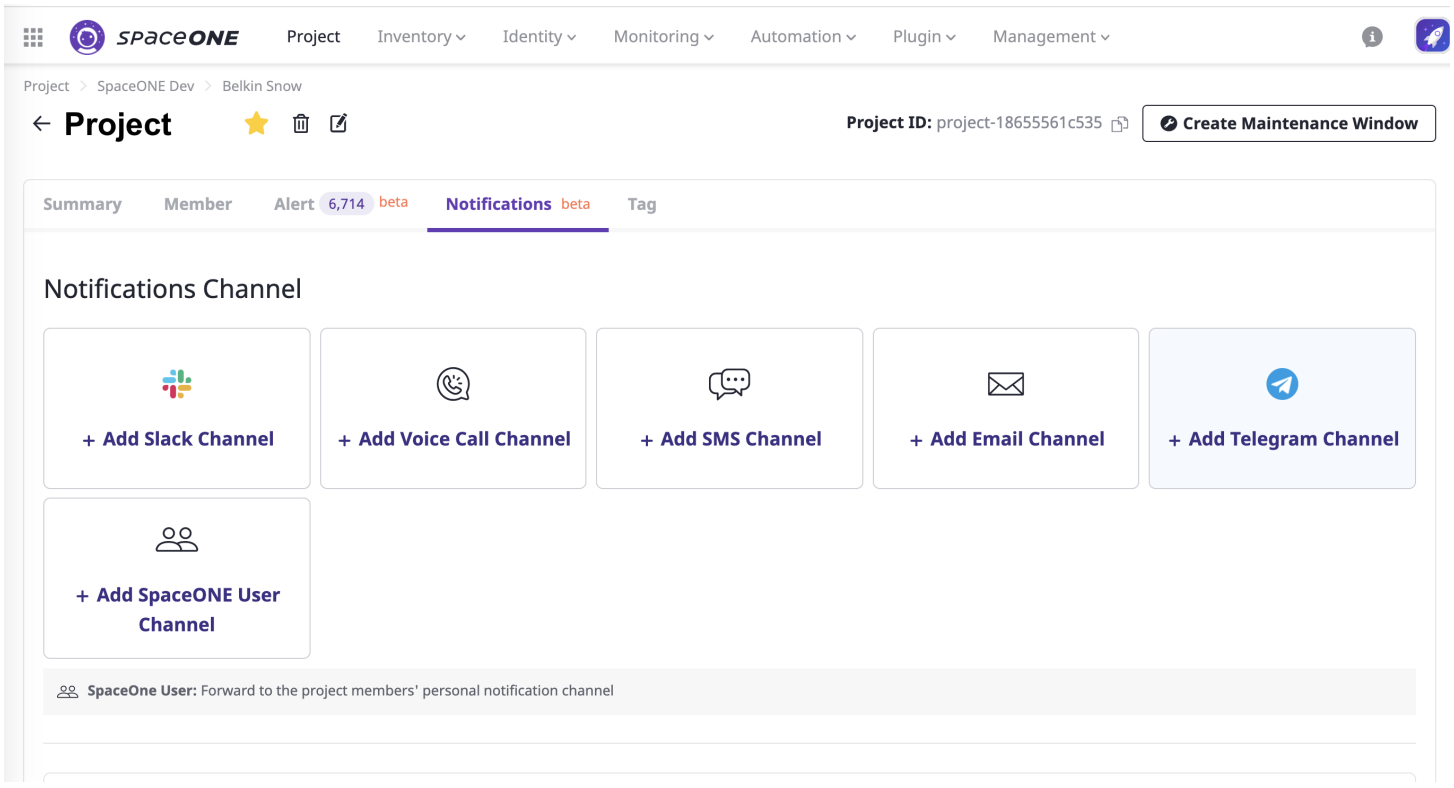
Find the apps we created right before, and add it.

Then, click `Add this app` button to a channel.

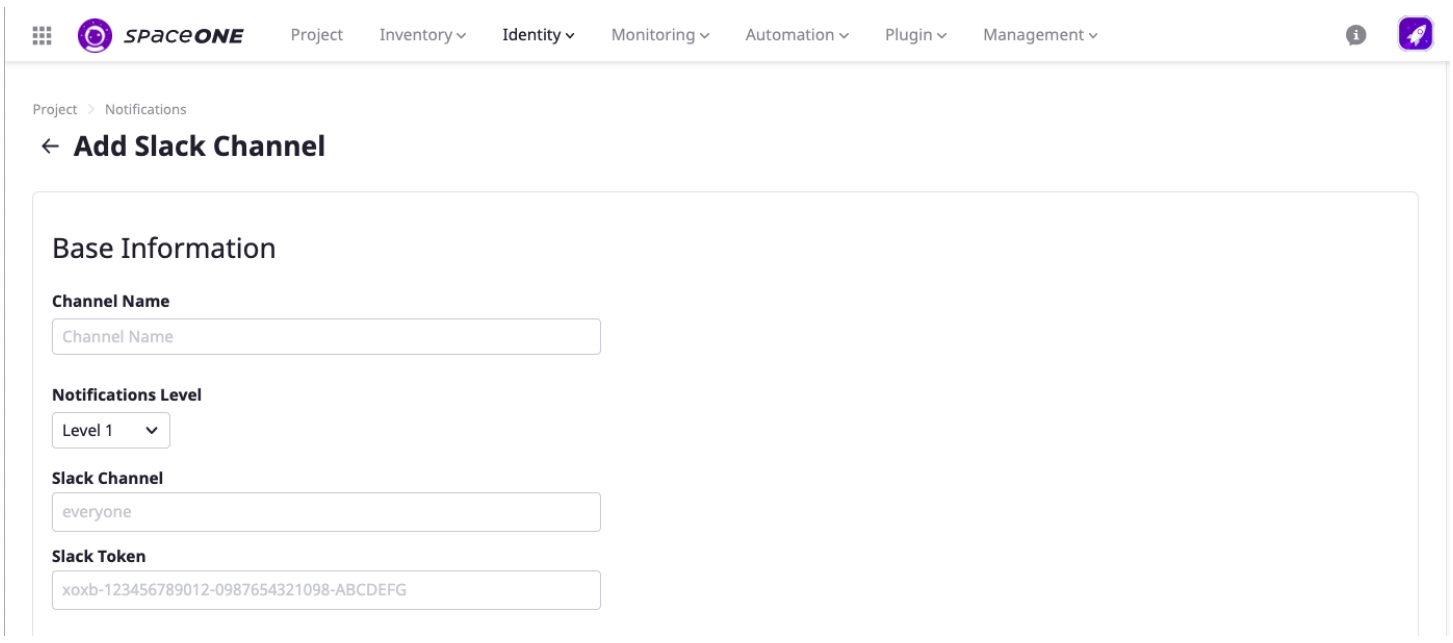
Add Slack Channel to your Project / User in SpaceONE

Go to `SpaceONE Console > Project` which you want to get alerts through Slack.

Basic Information



Set information above.
These items below are descriptions for plugins

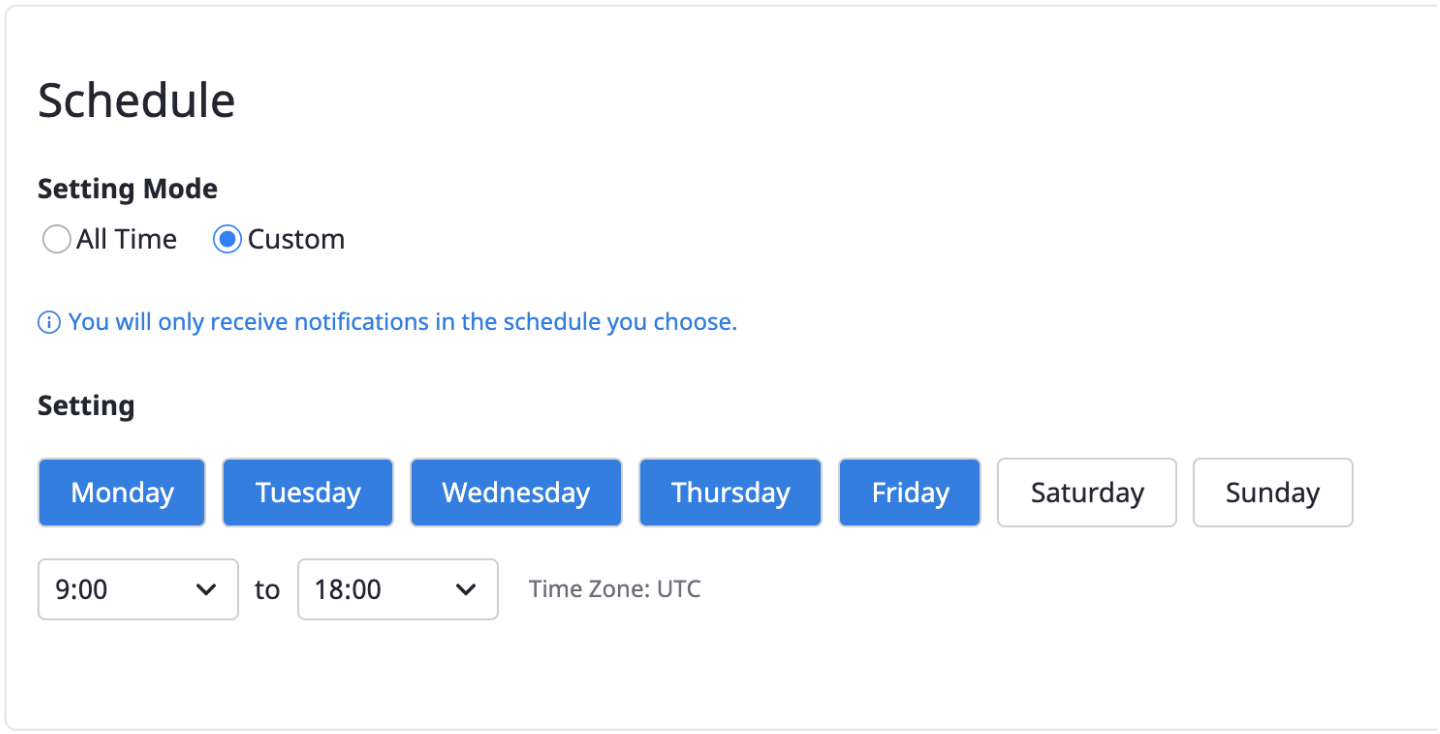


Item	Descriptions
Channel Name	Notification channel name
Notifications Level	Which level to be placed in escalation policy, see Escalation Policy for details
Slack Channel	Name of the slack channel to publish message. No need # in front of channel name
Slack Token	Token of slack app

Save and Test, now you are ready for SpaceONE Journey with Slack notification channel.

Notification Schedule

You can select when to receive alarm. There two options



Setting Mode	Descriptions
All Time	Receive alert notification any time
Custom	Receive alert notification within designated time period

Topic

Notification subscribes topics to check which alarm to send

About Notification Topics

Now only monitoring.Alert topics are available. Other topics will be created in future release.
Just pin ***Setting Mode*** to ***Receive all notifications***

Setting Mode	Descriptions
Receive all notifications	Allow notification channel to send all alert messages from ***any topics***
Receive notifications based on selected topics	Allow notification channel to send alert message from ***selected topics***

Troubleshooting

Visit Slack Basic App Setup for an additional explains of new Slack app.

```
Happy SpaceONE-ing with Slack notification channel!
```

7.1.5 - Telegram Protocol

Notification Plugin Telegram Protocol Configuration Guide

Overview

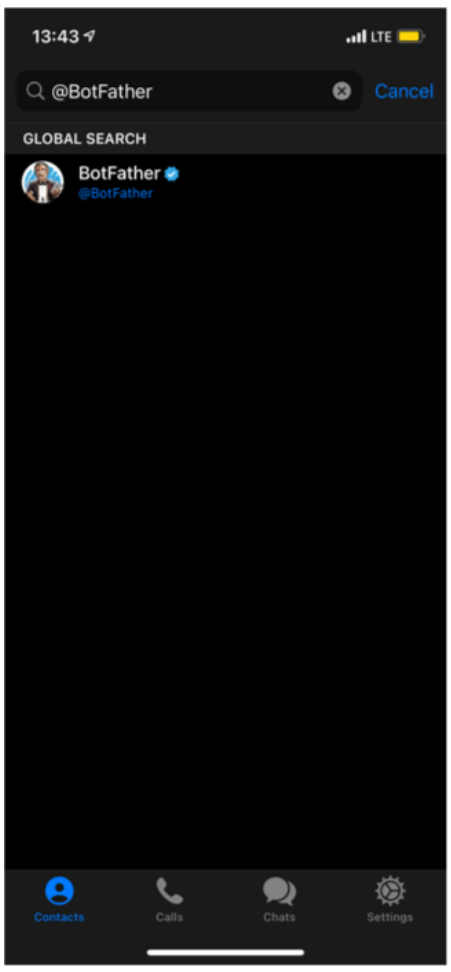
We can also add **`Telegram`** to our list of `Notification` channels. There are few prerequisites to use Telegram Bot on SpaceONE notification service, and the following will guide you to your **SpaceONE** notification journey.

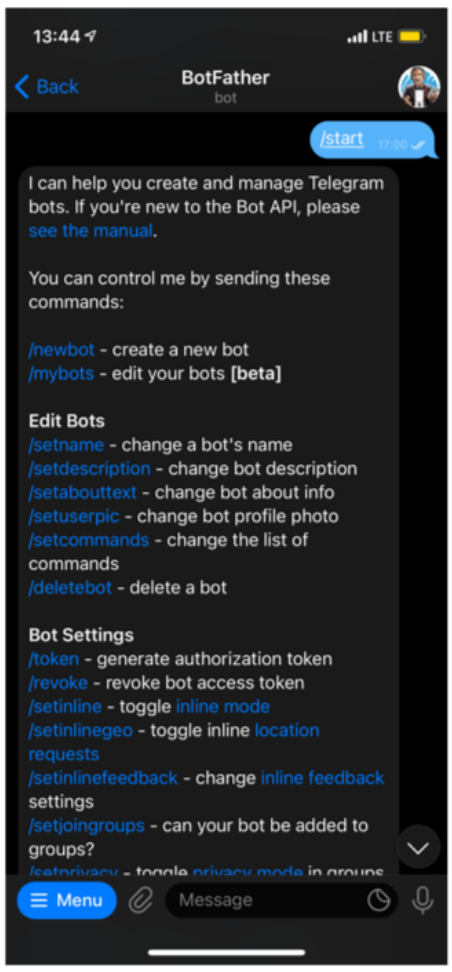
Prerequisites

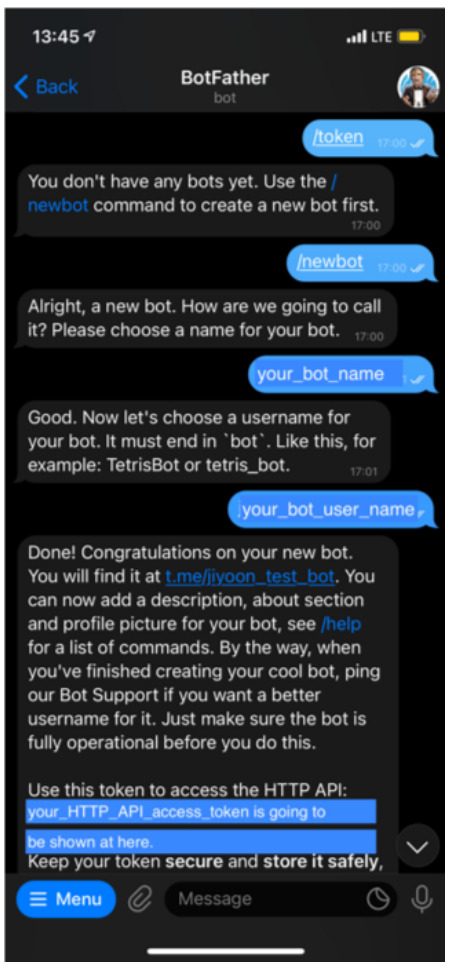
Install the Telegram app on your phone or PC. You will need a **BOT API TOKEN** and **CHAT ID**.

How to get BOT API Token

Open `Telegram`, and create a new Bot by searching for `@BotFather` and then typing `/start`, `/token`, and `/newbot` by turns. Your interaction with BotFather will be similar as following:



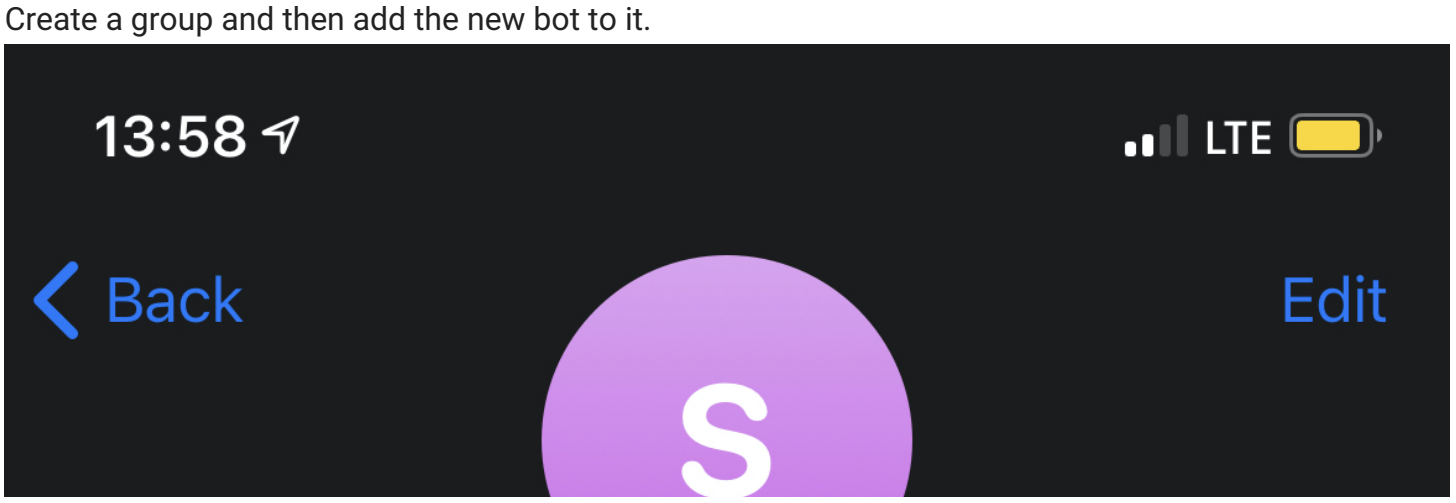


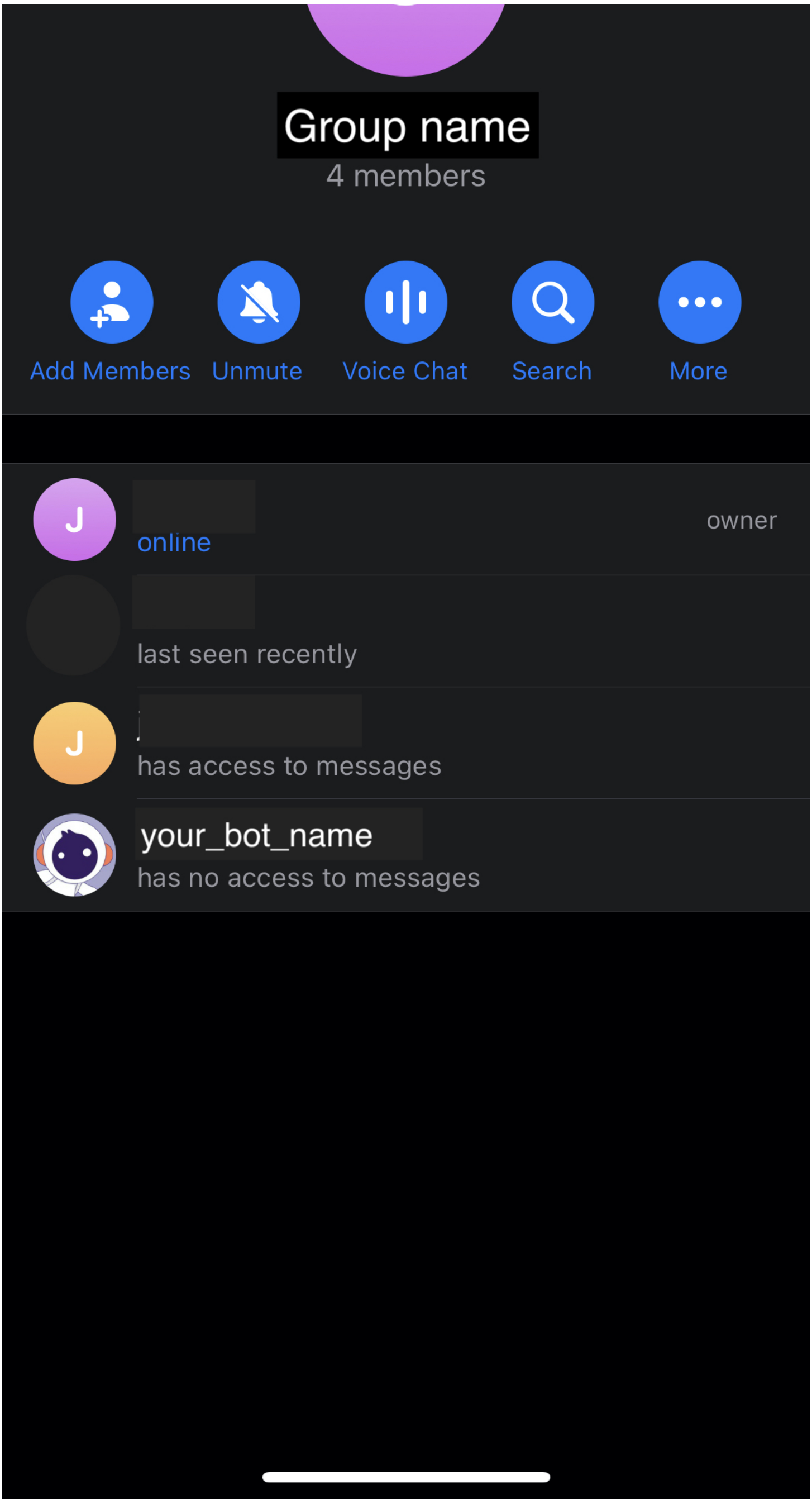


Do not forget that the username must end in bot and must be unique. You will get given a HTTP API token which is your BOT API Token to be used in SpaceONE. It will be in the form **`XXXXXXXXX:YYYYYYYYYYYYYYYYYYYYYYYYYYYYY`**.

How to get Chat ID

You then need the **Chat ID**. To get this, following will help you to get the Chat ID.
Create a group and then add the new bot to it.





send a message to the group, so that the group has at least 1 message.

Go to your browser, visit the url https://api.telegram.org/botXXX:YYY/getUpdates (replace the XXX:YYY with the **BOT API token** you just got from Telegram)

In the JSON Response, you should see a node with a message that has the type=group, This node will also have an ID. Copy this into CHAT ID field in SpaceONE. The CHAT ID will most likely be a negative number in the form of -#########.

Precautions

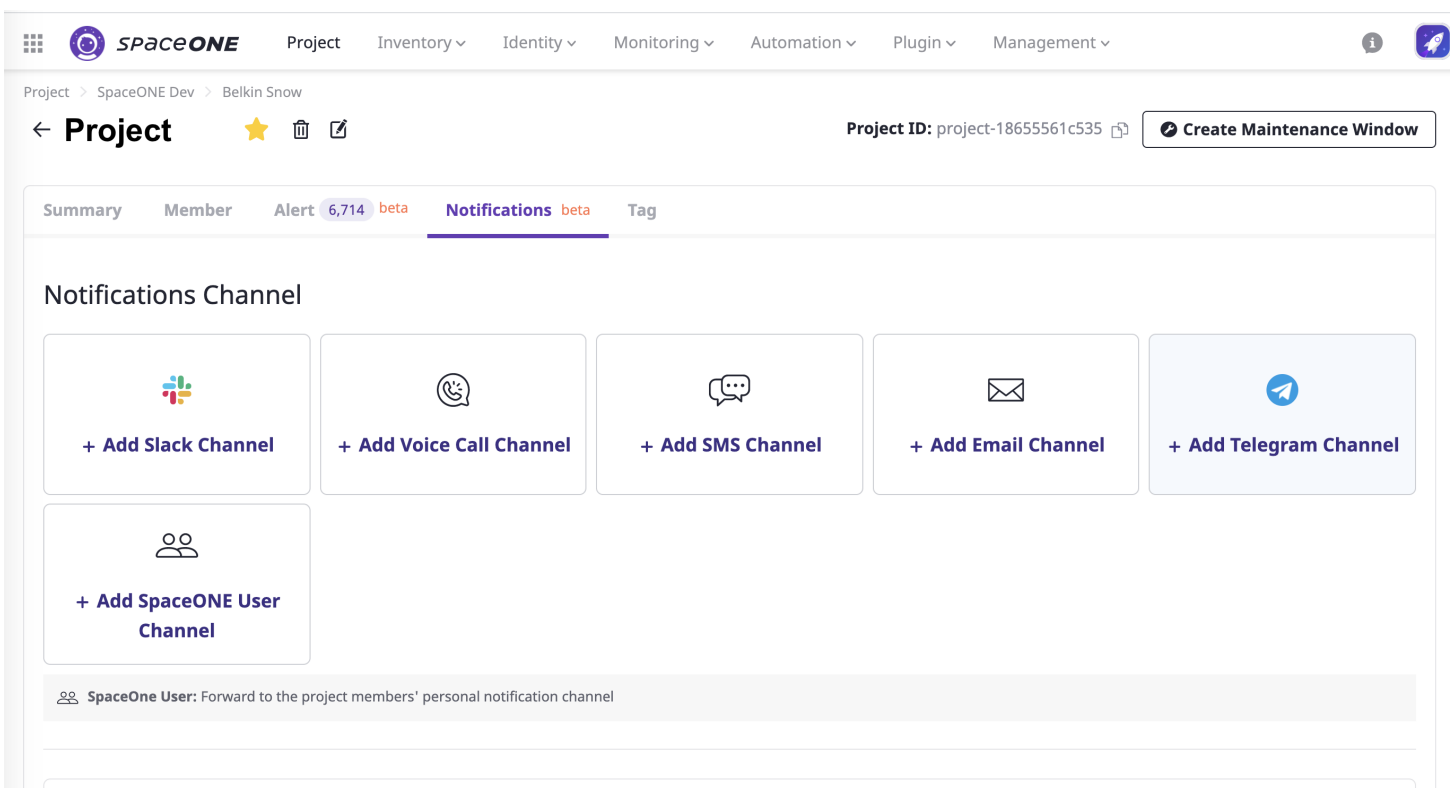
The chat id is likely to be a negative number, so make sure you copy the negative symbol as well when setting the chat id in the script.

```
Eg, If chat id = -123456789, occasionally quickly copying and pasting you may f
```

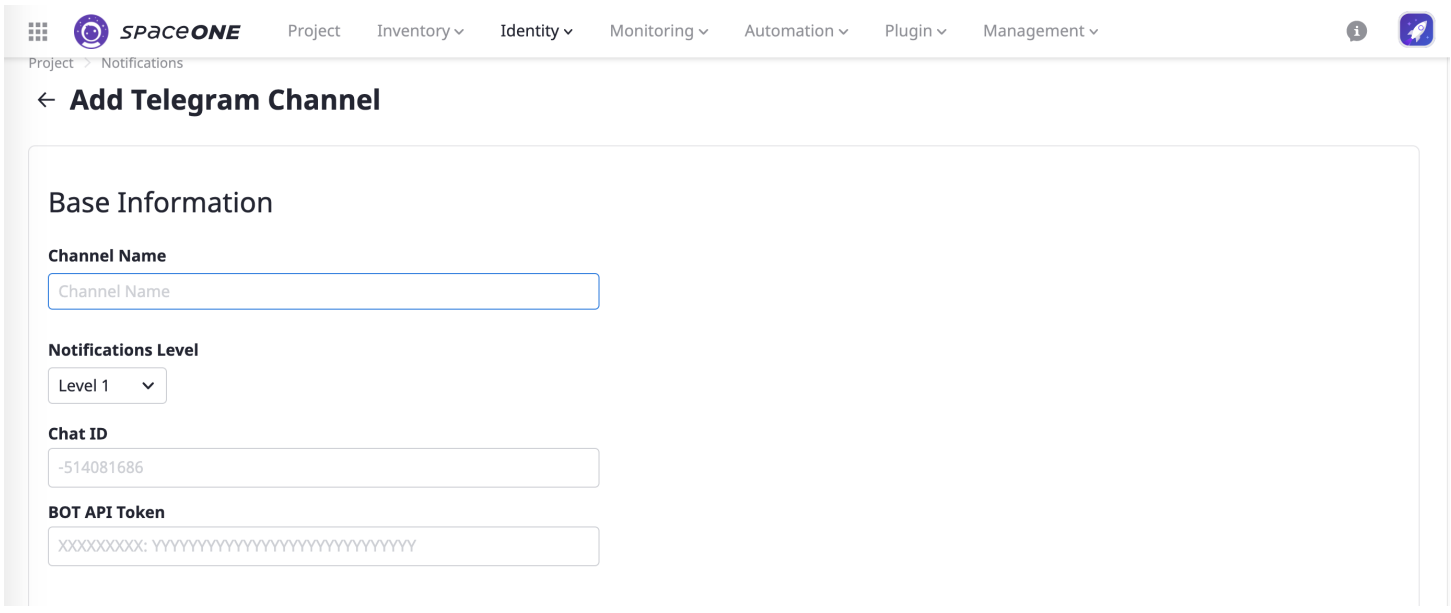
Add Telegram Channel to your Project / User in SpaceONE

Go to `SpaceONE Console > Project` which you want to get alerts through `Telegram` .

Basic Information



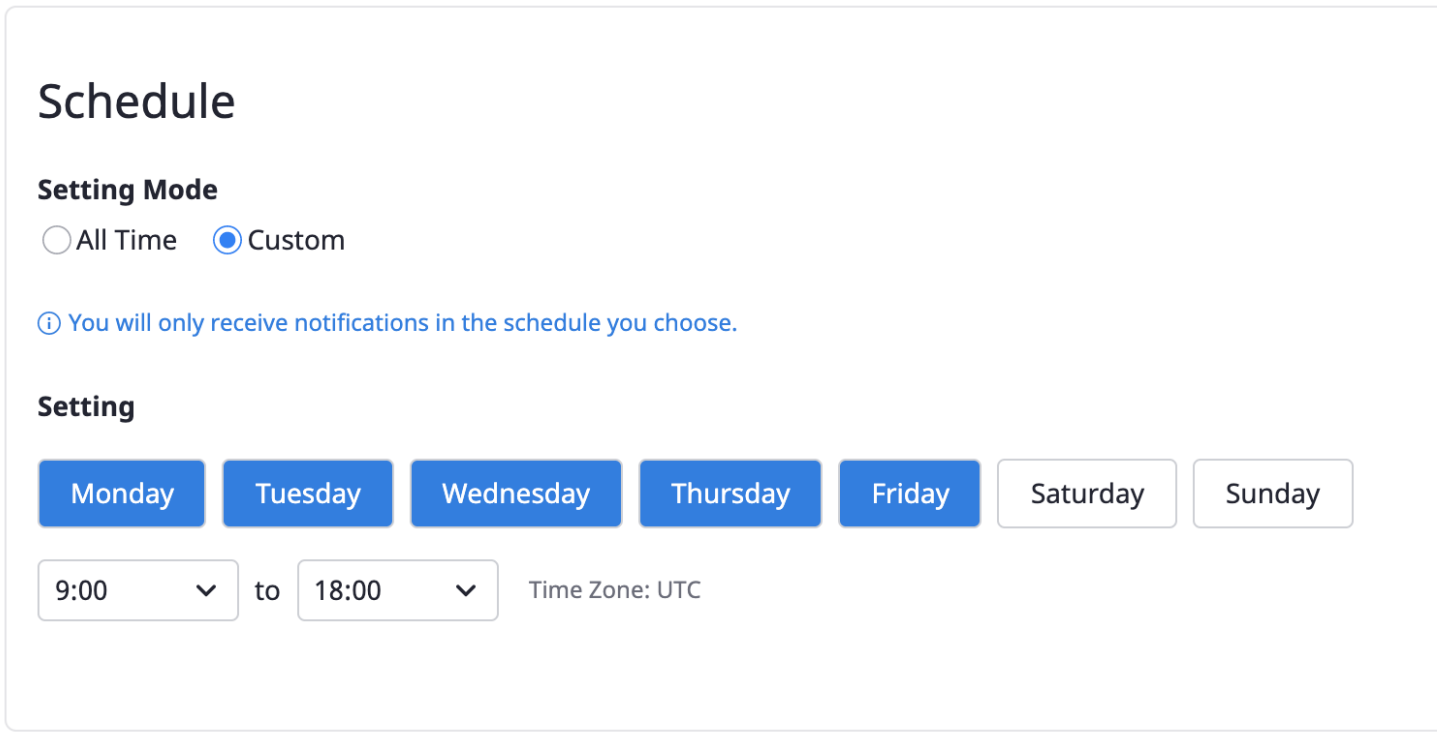
Set information above.



Item	Descriptions
Channel Name	Notification channel name
Notification Level	Which level to be placed in escalation policy, see Escalation Policy for details
Chat ID	Telegram chatting room ID, see How To get Chat ID to get information
BOT API Token	Telegram bot api token, seeHow To get Bot API Token to get information

Notification Schedule

You can select when to receive alarm. There two options



Setting Mode	Descriptions
All Time	Receive alert notification any time
Custom	Receive alert notification within designated time period

Topic

Notification subscribes topics to check which alarm to send

About Notification Topics

Now only monitoring.Alert topics are available. Other topics will be created in future release.
Just pin ***Setting Mode*** to ***Receive all notifications***

Setting Mode	Descriptions
Receive all notifications	Allow notification channel to send all alert messages from ***any topics***
Receive notifications based on selected topics	Allow notification channel to send alert message from ***selected topics***

Save and Test, now you are ready for SpaceONE Journey with Telegram notification channel.

```
Happy SpaceONE-ing with Telegram notification!
```

Troubleshooting

If the `getUpdates` url doesn't return a node containing a group with an id, then
Remove your bot from the group,

and then re add your bot the the group,

then send a message to the group again,

then try the getUpdates url again.

Visit Telegram API Bot for an additional understading of Telegram API Bot services.

8 - Automation

About automation.

8.1 - Power Scheduler

Managing Power Status of Cloud Resources in projects

Overall

In Power Scheduler page, User can schedule power status of target cloud resources.
Power Scheduler page offers listing scheduler information, add/update/delete scheduler.

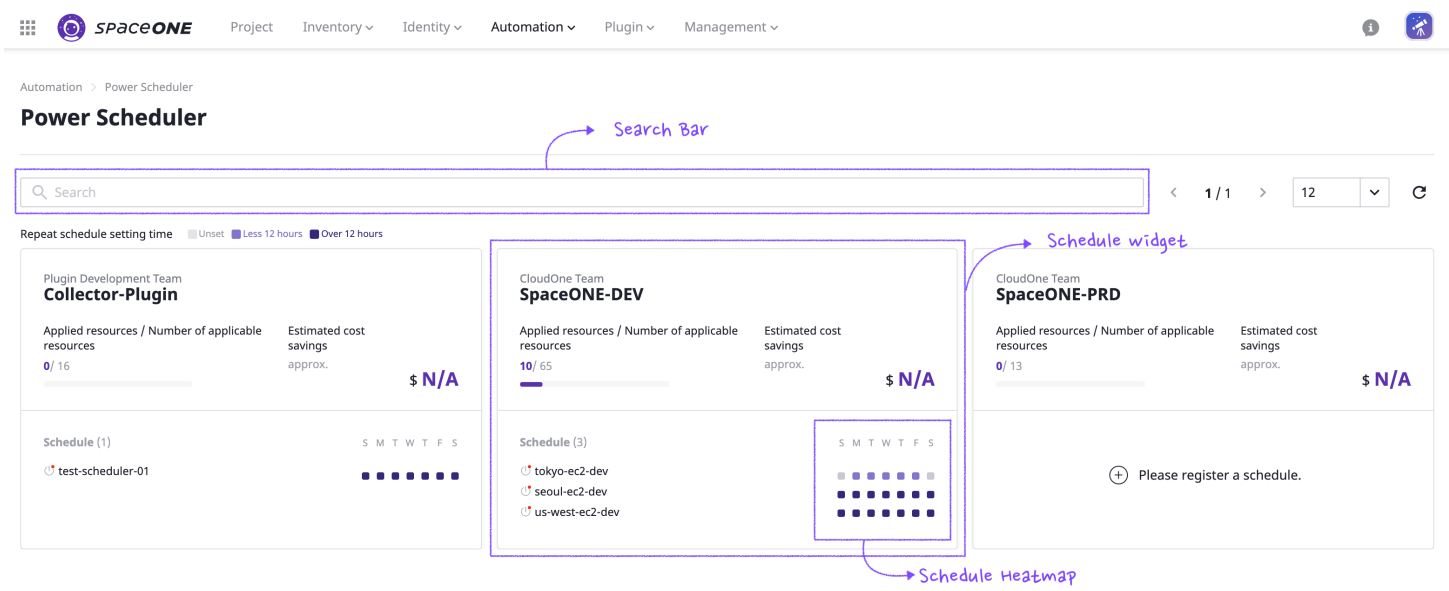
Prerequisites

User need to define security policy(IAM) before setup power scheduler.
Before creating Power Scheduler modify your existing policy, For detailed process refer to link below.

(AWS) Service Account Policy Management

(Google Cloud) Service Account Policy Management

Power Scheduler Dashboard



Scheduler list by Projects

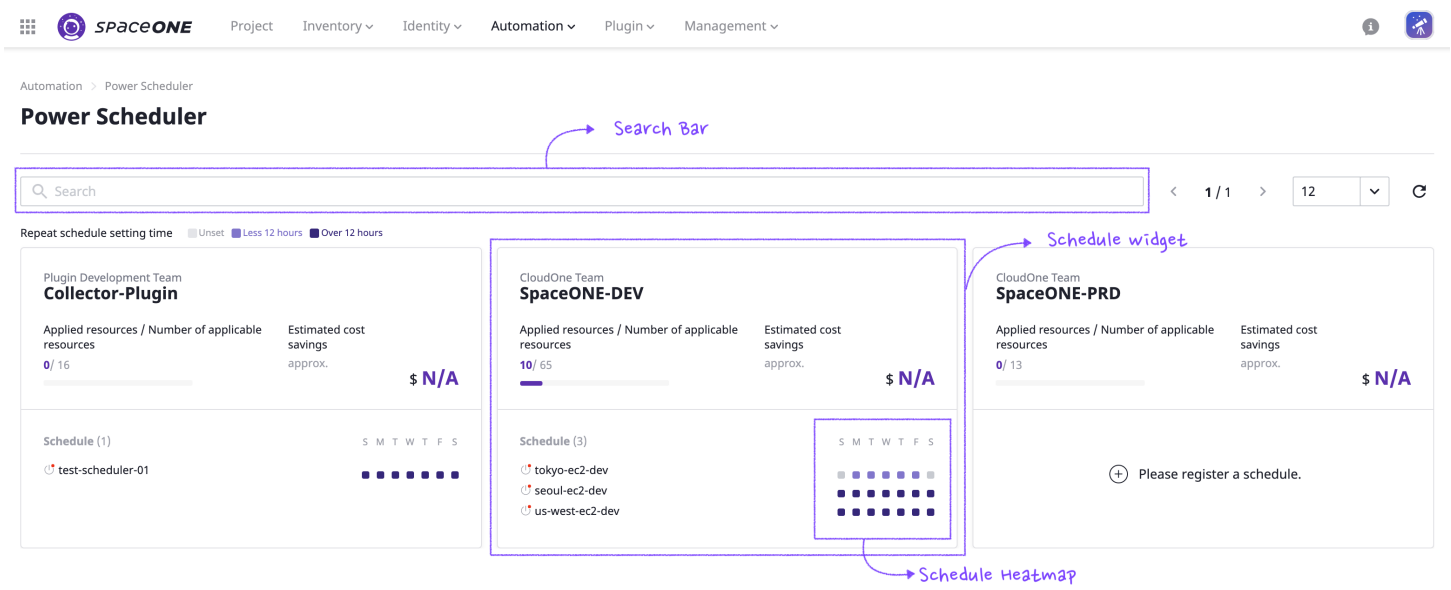
User can see Overall status of power scheduling

Search Bar

User can search status of power scheduling by project name.

Scheduling Widget

Items of power scheduler information for each projects are below.



Item	Description
Project Name	Name of projects which is linked to power scheduler
Number of Resource	Number of resources : Number of resources that are controlled by power scheduler. Number of resources available : Total number of resources can be scheduled by power scheduler (Server, RDS, Auto Scaling Group).
Schedule	List of running schedule(Up to 3 items)
Estimated Reduced Cost	Reduced cost by power scheduler in last 1 months(US dollar).
Scheduled Job	Length of each schedule

Scheduling Meat Map
The color of scheduling head map has 2 steps. The color shows how long is scheduled job. Each color means below
Scheduled time is between 0 ~ 12 hours Scheduled time is between 12~24 hours

Scheduler Management

Scheduler Calendar

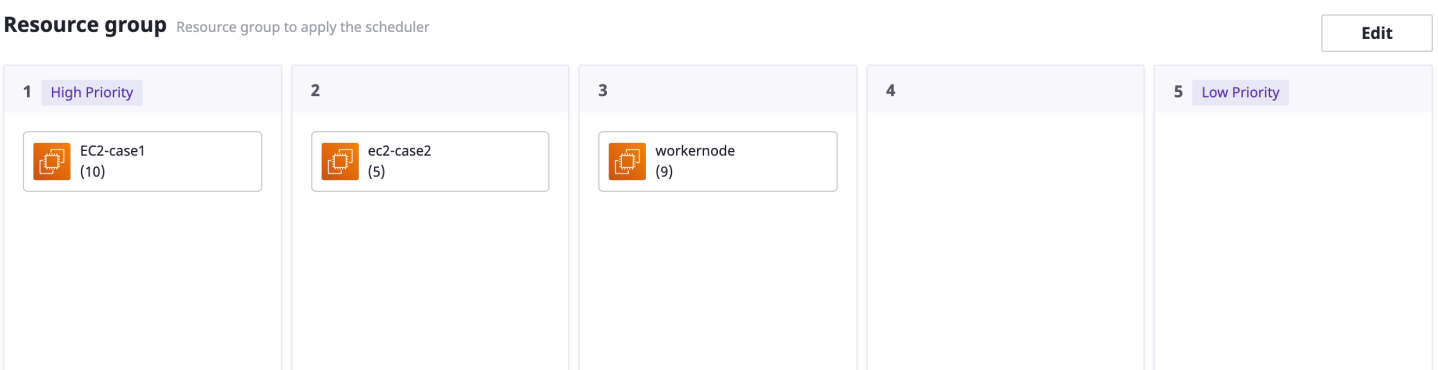
In scheduler Calendar, User can manage this functions

Scheduling Time

User can see scheduler timetable. x-axis is date, y-axis is time to be controlled. By clicking ***This weeks*** jump to power scheduling plan for this weeks.
Move to next/previous weeks by < > buttons right upper side of table.

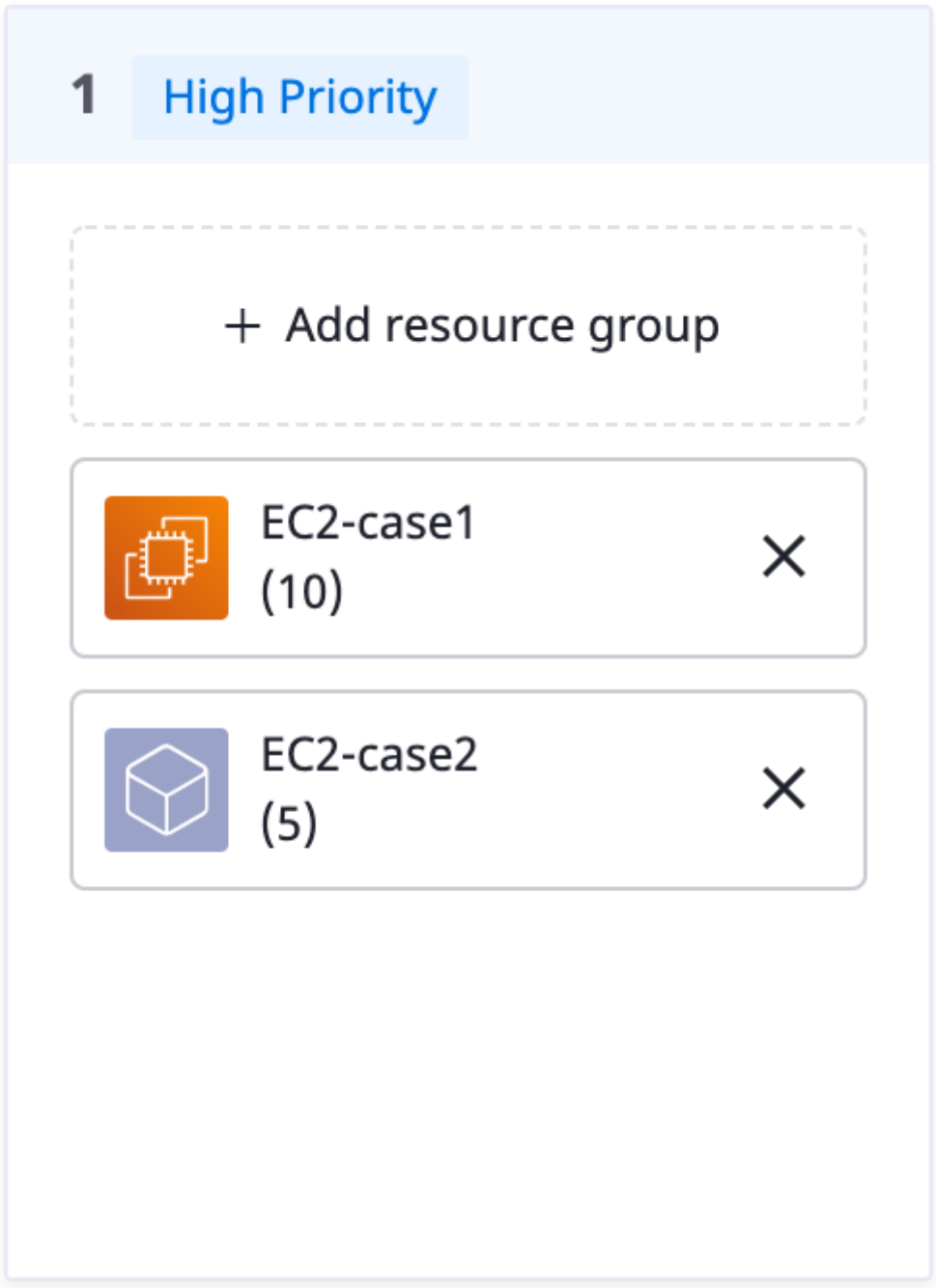
Resource Group

• Priority by Resource Group

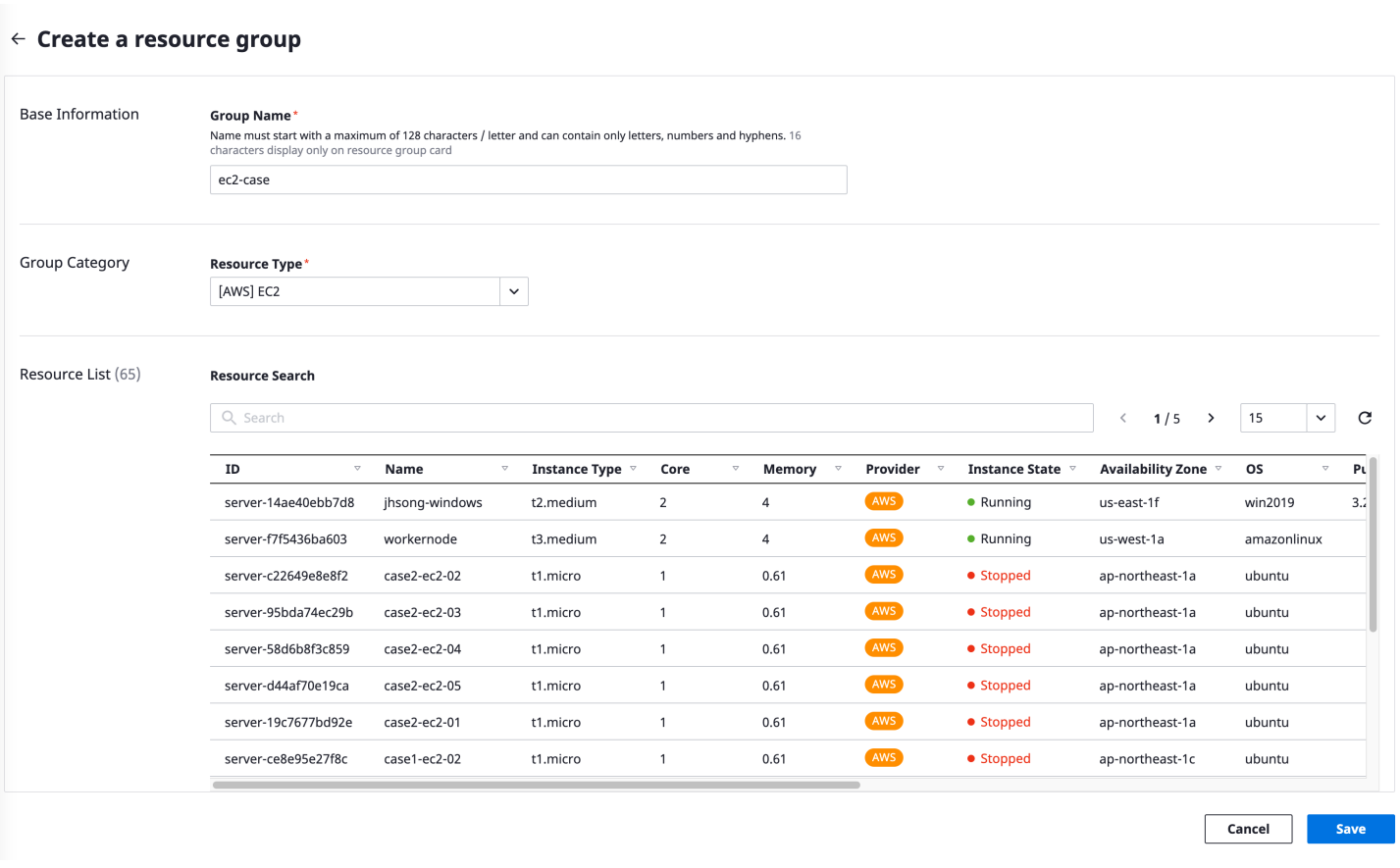


Scheduler is consist of several resource group. Each resource group has step defined by priority.
The lower number gets higher priority. The status change of higher priority finishes first. If the target status is ***ON***, higher priority ***Resource Group*** start first.
Create/Deleting ***Resource Group*** is done by clicking ***Edit button > + Add Group***.

Resource Groups In Same Priority



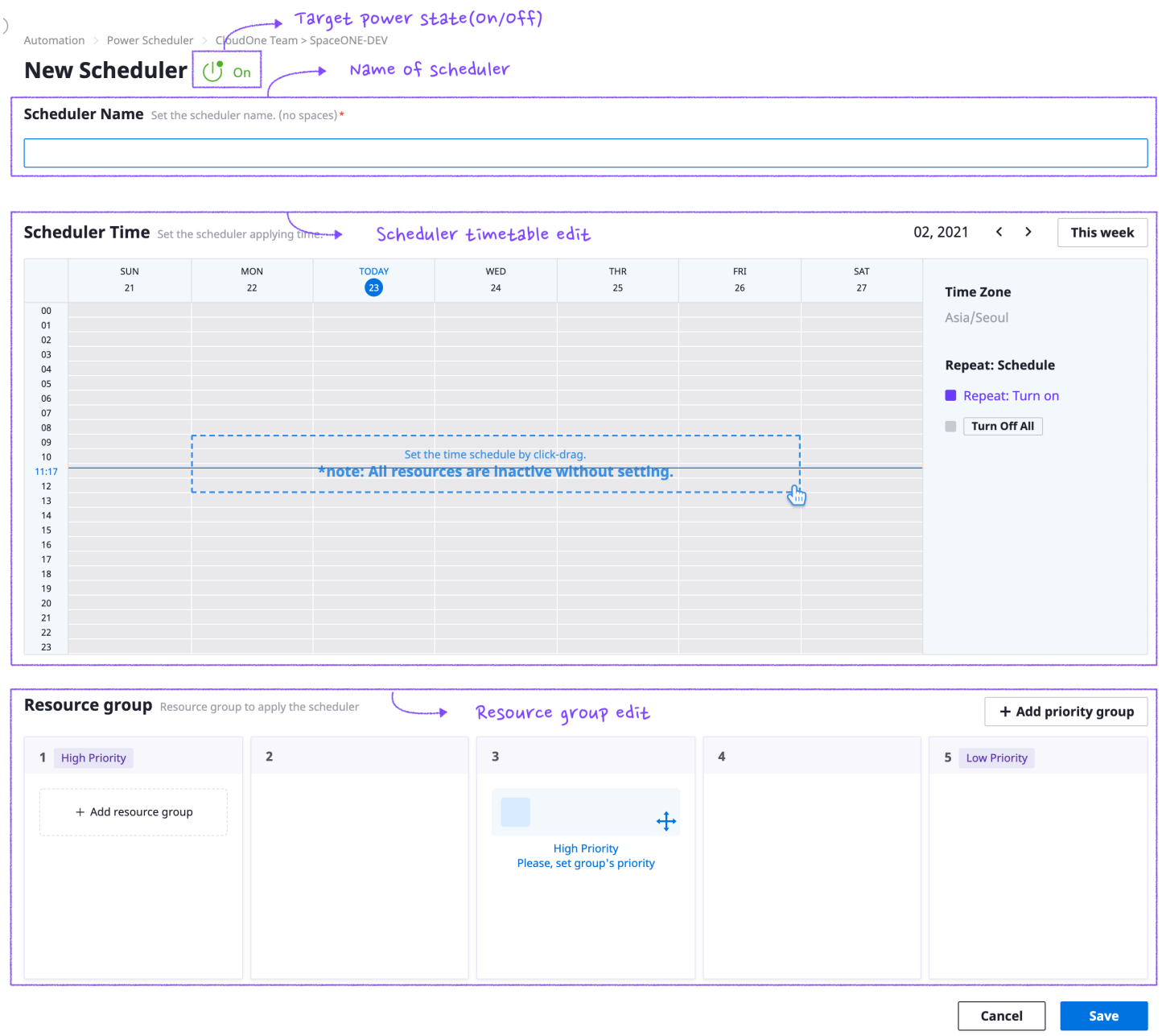
There is sequence of changing status between resource groups in same priority.
Upper position resource group changes first, and Lower position goes second.
Details of Resource Group



Detailed status resource group is done by clicking ***Name of Resource Group.***

Item	Description
Name	Name of Resource Group
Resource Type	Type of Resource Group(Instance, RDS, Autoscaling)
Target List	List of Cloud Resources to be controlled

Creating New Scheduler



By Clicking ***Creating New Scheduler*** button, New scheduler editing screen appears.
If there is no existed scheduler, Creation screen is auto generated.

To create schedule, fill out several items required.

Name

Name of Schedule.
Combination of String, Number, '-' is valid. escape character is not available.

Timestamp

Specifying time for scheduler, x-axis is date, y-axis is detailed time.
Selecting range of times done by click & drag in calendar.
Schedule has two mode.

Scheduled mode	State	Description	color
Repeated Schedule		Repeated by every weeks. Within selected area, Resources are On, Otherwise(Non selected) resources became Off.	drawing
One time	ON	Event time for specific date. At the selected area, resources became on.	drawing
One time	OFF	Event time for specific date. At the selected area, resources became off.	drawing

Resource Group

Creating resource groups to control.
By ***Creating Resource Group*** button, ***Creating Resource Group Page*** Pops up.
Informations to be specified are belows

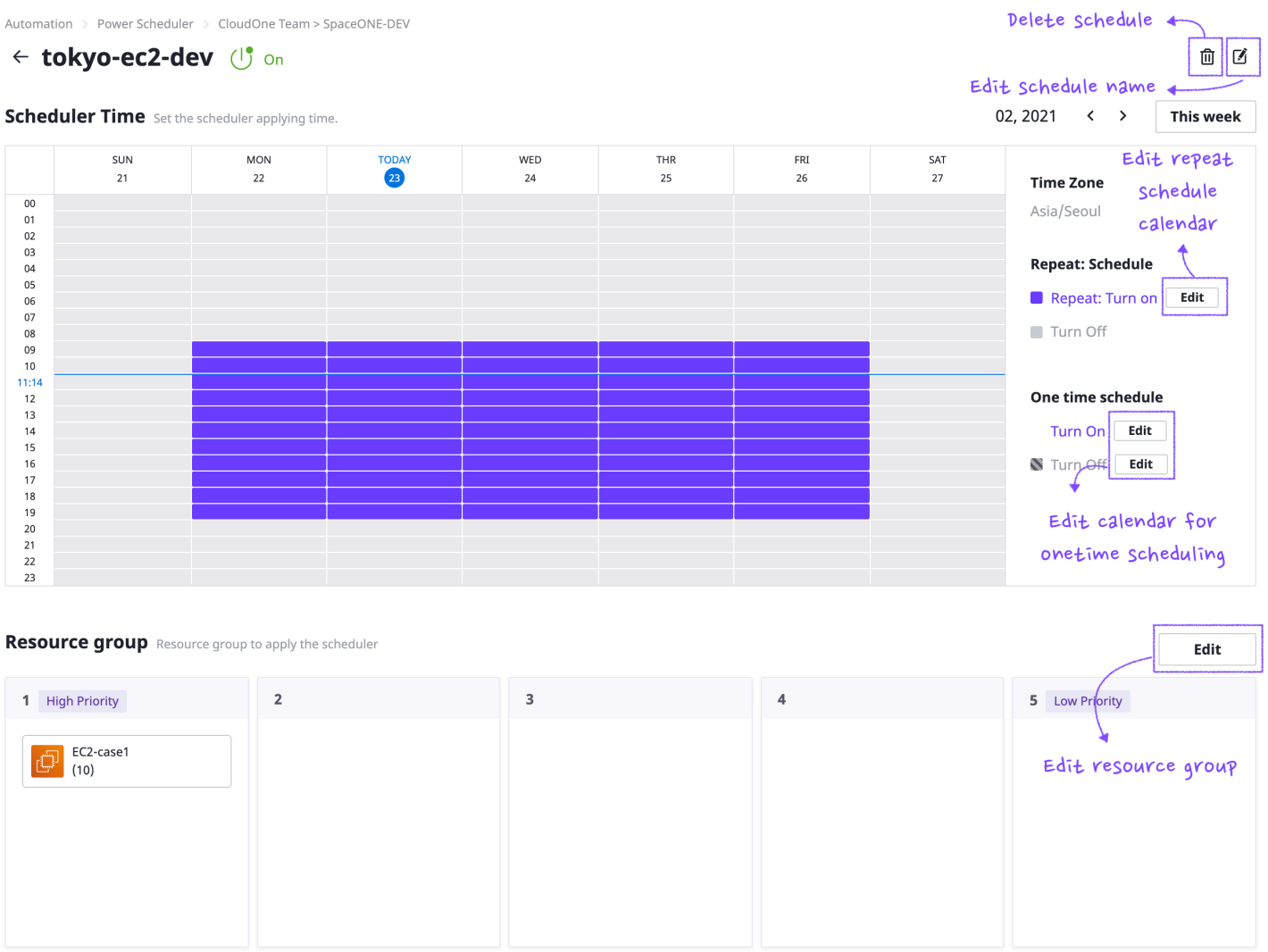
Item	Description
Name	Enter ***Resource Group*** name. Total 128 character is available. Name should start with character(not number). Name can be a combination of charcter, number, '-'
Resource Type	Select resource type. Available list of resource group is belows. [AWS] EC2 [AWS] RDS [AWS] Auto Scaling Group [Google] Compute Engine [Google] Instance Group [Google] Cloud SQL
Resource List	Target Cloud Resources to be controlled. Selected by search filter.

Confirm the input information, then click ***save*** button.

Schedule Deletion

By clicking ***Trash Can*** button, Scheduler can be deleted.

Scheduler Edit



item	Description
Scheduler Name	By Clicking ***Scheduler Edit*** button right upper of page. Scheduler name can be edited.
Scheduler Calendar	By clicking Edit button in calendar. One time schedule, Repeated time scheduled can be edited.
Resource Group	***Resource Group*** can be edited ***edit*** button below.

Limitation & Restrictions

Some limitations for power scheduler service are existed, Most of them are inherited from functionality of each cloud providers.

AWS

Cloud resources which has conditions below can not managed by power scheduler service
AutoScalingGroup
ASG controlled by ***EKS managed group***

RDS Instance
Instance that member of ***replication***

SQL Server DB using ***Multi-AZ***

RDS Aurora Instance
Member of ***Aurora global database***

Cluster that using ***parallel query feature***

Reference
AWS DB instance limitation

Google Cloud

Cloud resources has a such a condition that does not support within power scheduler Service
Compute Engine
Compute Engine resources may **NOT** turn on/off if selected compute engines are instance of **Instance group**.

Categorizing **Instance group**'s compute engine and normal compute engine on the view will be available soon.

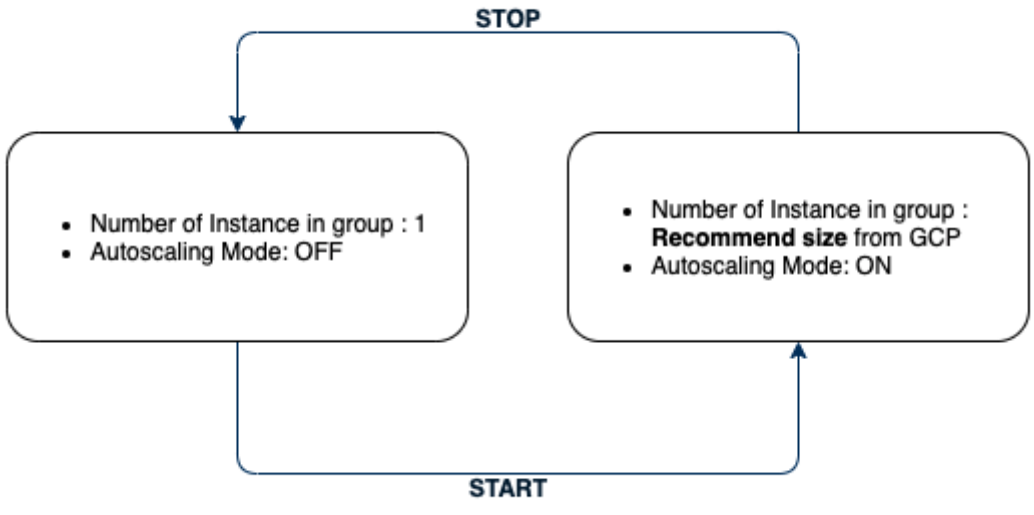
Instance Group

Only **Stateless** type in Instance Group is valid to turn on/off in power scheduler service because Google Cloud supports autoscaling on **Stateless** type only in Instance Group. (Refer to google.compute.instance_group)

Minimum number of Instance in Instance group is 1 when instance group scales in(autoscaling) except certain type (Unmanaged Instance Group).

> ## Please, be advised that Instance Group is working for action Start/Stop as followings
>
> **Valid type:**
>
> **Stateless** (**Managed**) as mentioned above.
>
> **Results on Action:**
>
> Recommend size is given by Google Cloud from their own statistic
>
> **ON :** Scale up to recommend size(count) of Instance group and autoscaling mode is on (Keep scale in/out itself by recommend size if autoscaling mode is on).
>
> **OFF :** No matter autoscaling mode is on or off, diminish Instance Group to 1 Instance and autoscaling mode is off.

Action Cycle & status



9 - My Account

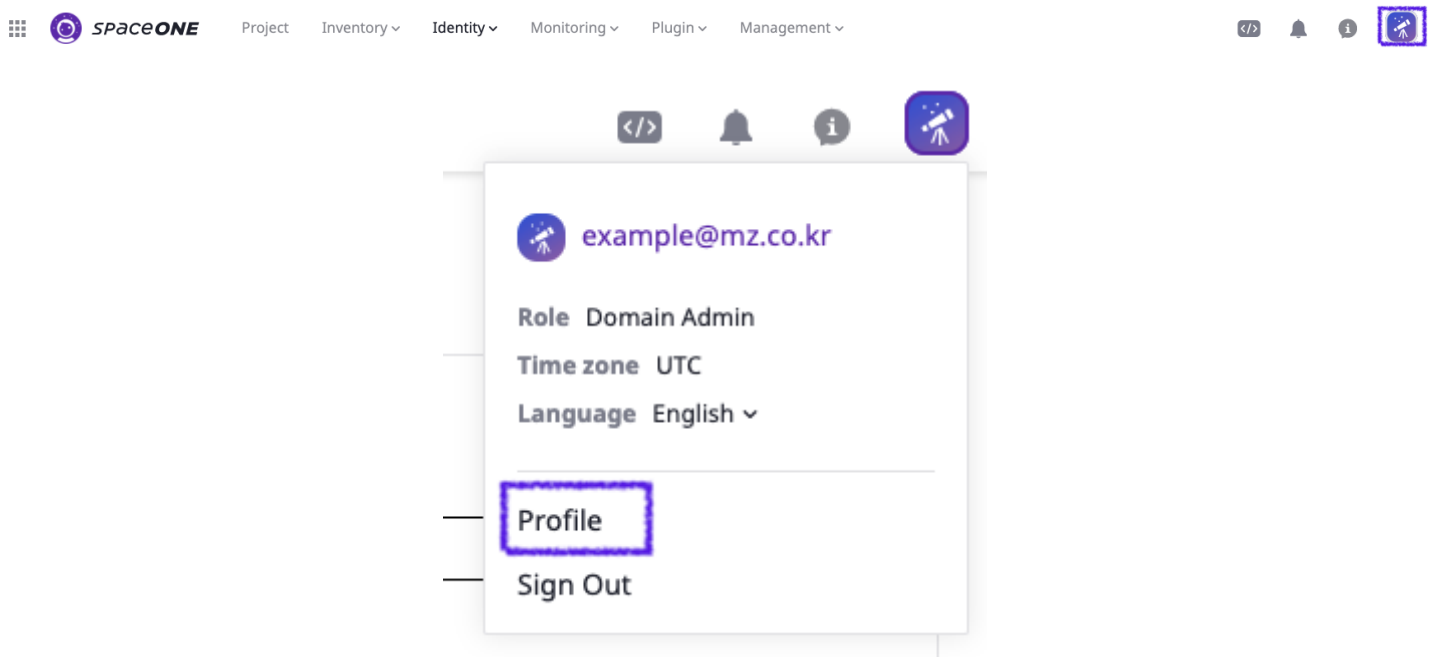
User Profile & Settings

9.1 - Account & Profile

User Information

User Profile

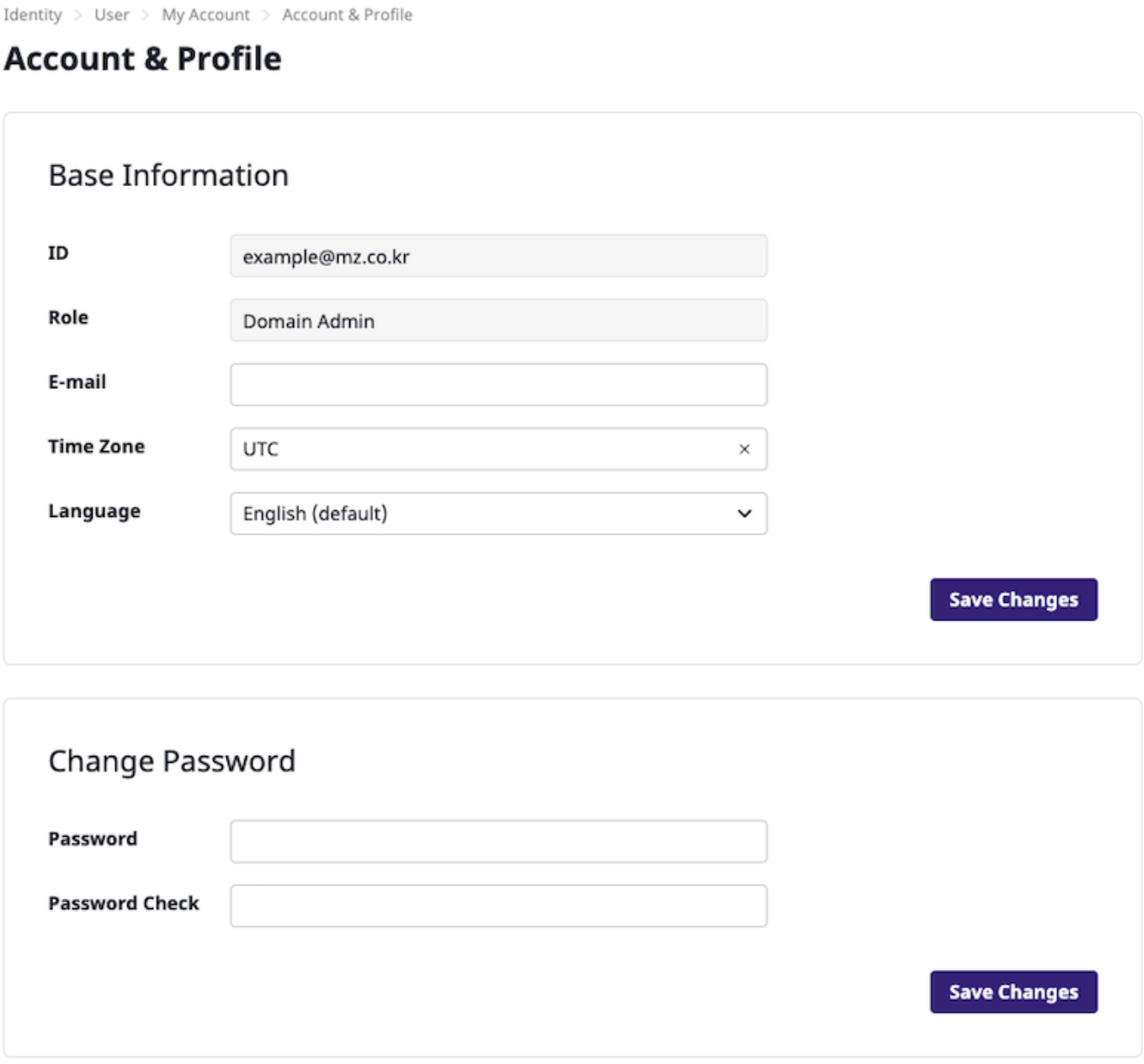
Users can view and modify their profile information through the **`Profile`** menu.
You can reach this menu by clicking on the Profile Icon on the top right corner of the console.



Role : User role (Domain Admin/Project Admin).
Time Zone : User time zone (UTC/Seoul/Tokyo).
Language : User Language options (English/Korean/Japanese).
Profile : Modify User Information.
Log Out : Log out and return to the console login page.

Editing Profile

By clicking the **`Profile`** menu, you can move to the User information window.



Users can change all information, except ***ID*** and ***Role***.
After changing any information, click **`Save Changes`** .
A Success message will appear to confirm.

9.2 - API Key

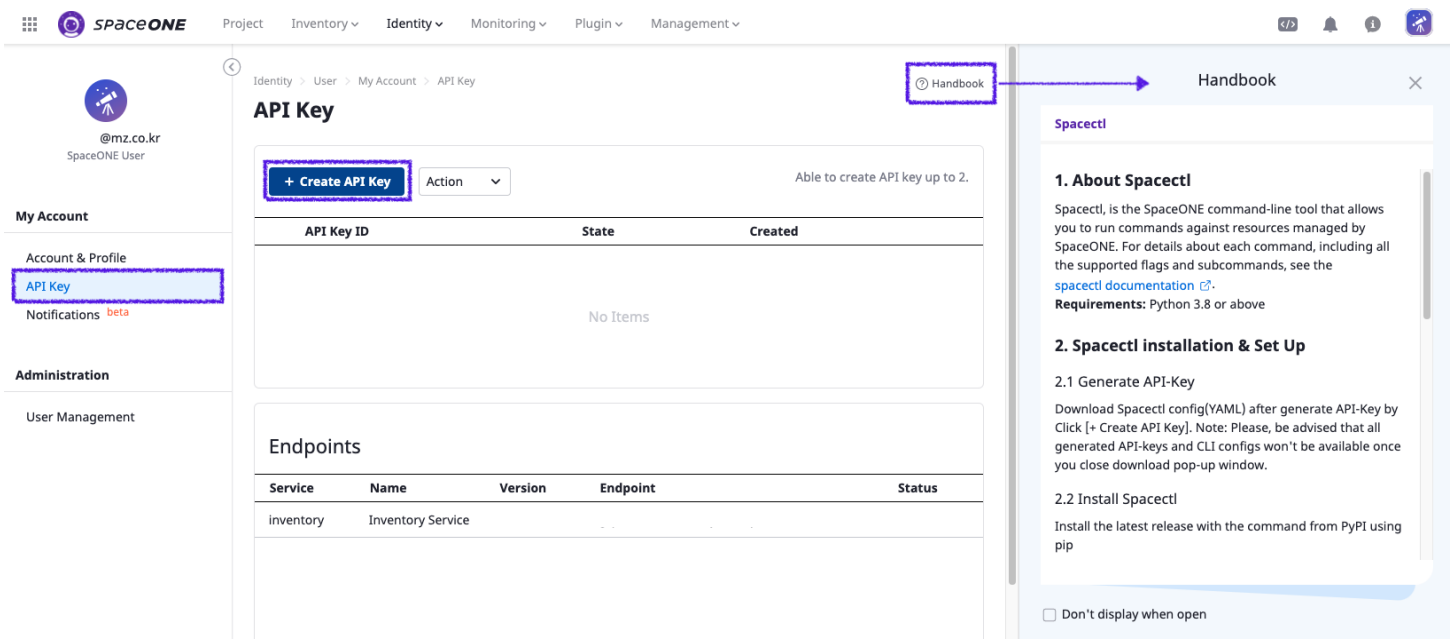
Creating and Managing API Keys

Creating API Keys

Users can create and manage **API Keys** from the `My Account` side bar > `API Keys` .
To create an API Key simply click `+ Create API Key` .

> **Users are only allowed to create 2 API Keys maximum.**

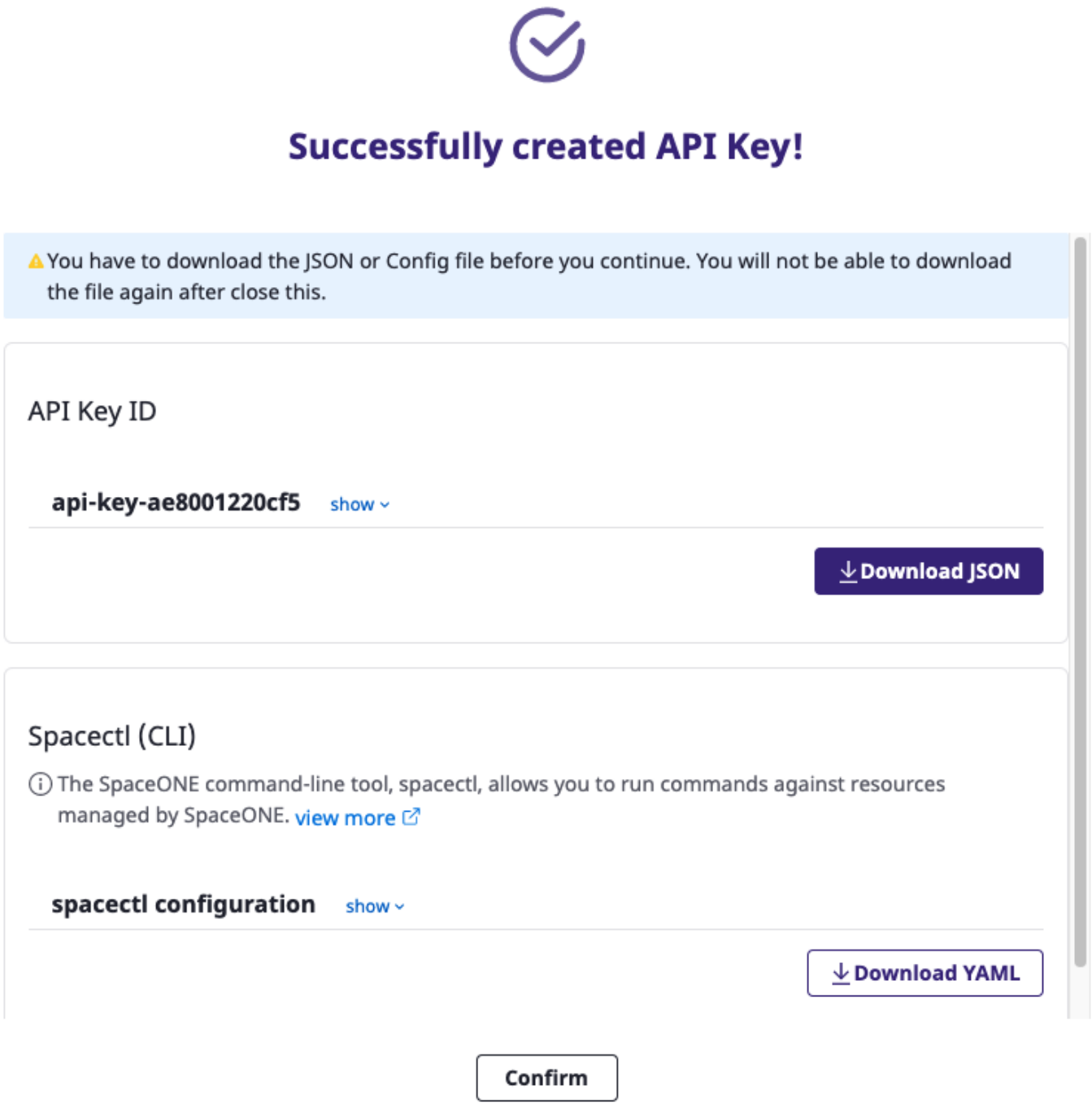
For further information you can read the *Handbook* SpaceONE provides at the top right corner of the page.



Downloading API Keys

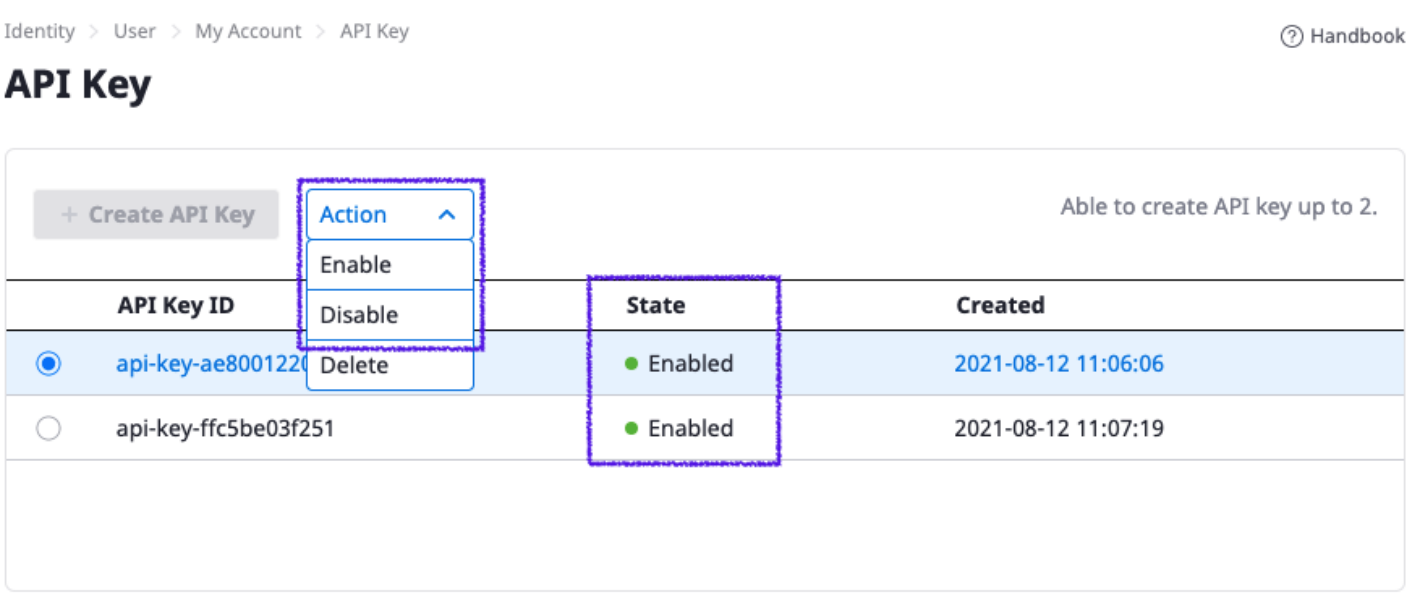
When clicking the `+ Create API Key` , an API Key Creation Success message will appear.
From this window you can `Download JSON` or `Download YAML` .

> **It's essential that users *Download their JSON / Config files* before they move on. Once you confirm and close this window(pop-up) you will NOT be able to download the same files again.**



Enable / Disable API Keys

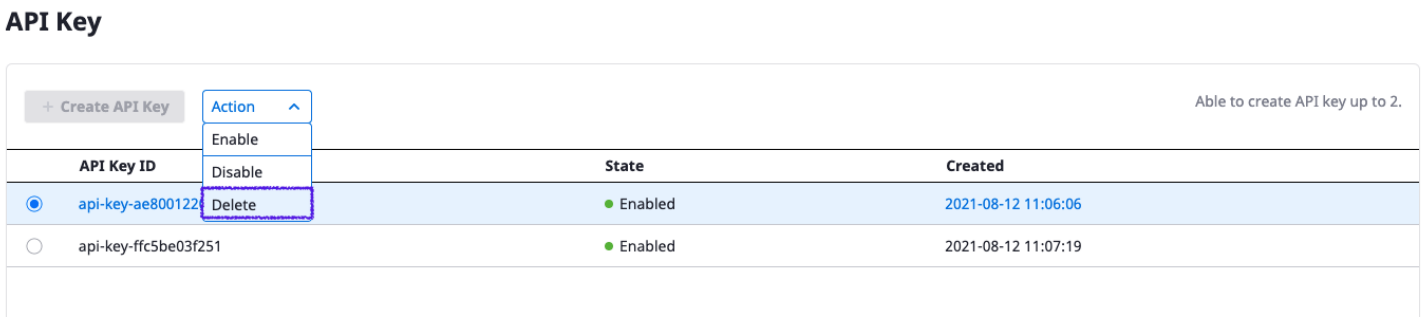
Once you've created API Keys they will appear on the **`API Key`** list.
To Enable or Disable keys, users can select and then use the **`Action`** list menu > **`Enable / Disable`** .
Change of status will be shown on the column **`State`** .



> **Enabling, Disabling, and Deleting API Keys can take up to approximately 10 minutes to actually be applied.**

Delete API Keys

To delete API Keys select and use the **`Action`** list menu > **`Delete`** .



> **Enabling, Disabling, and Deleting API Keys can take up to approximately 10 minutes to actually be applied.**

Endpoints

Users can also check the EndPoints for the API Keys.
Currently SpaceONE provides Endpoints of the following features:

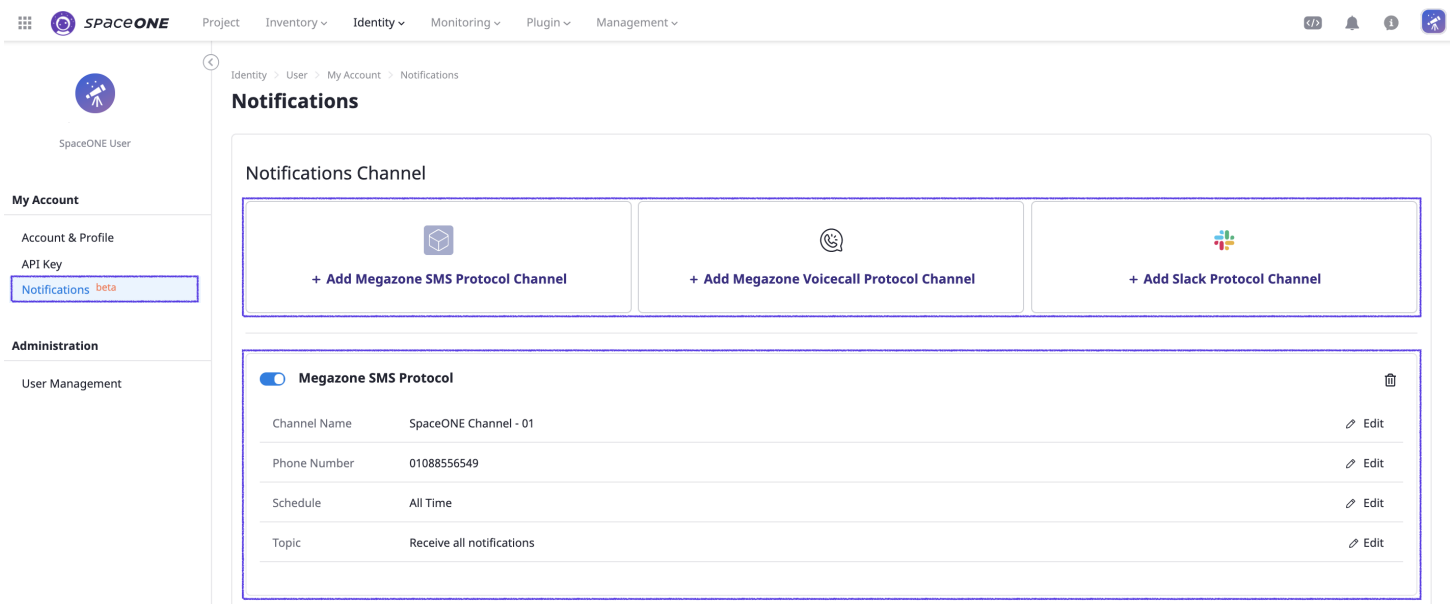
Cloud Services
Cloud Service Types
Collectors
Jobs
Job Tasks
Regions
Resource Groups
Servers

9.3 - Notifications

Managing Notifications

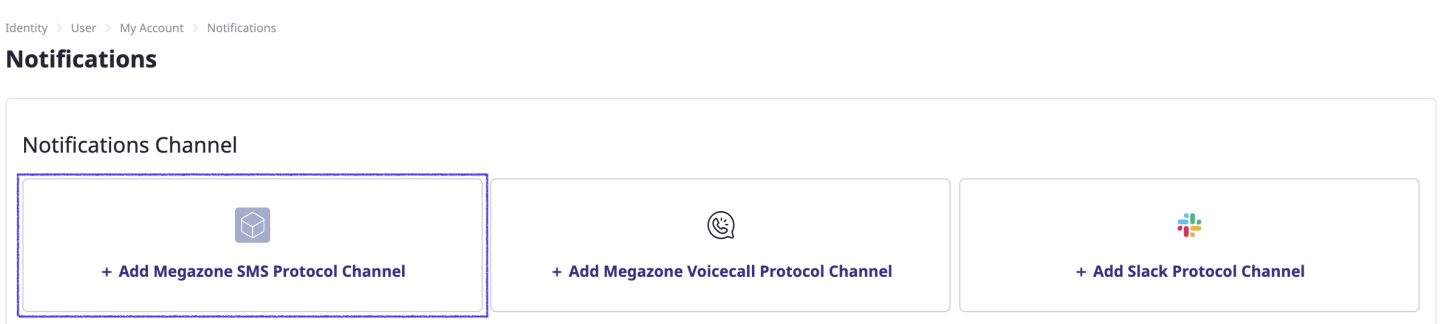
Overview

On the notification page, you can easily manage notification settings for SMS, voicecall, and Slack protocol channels.



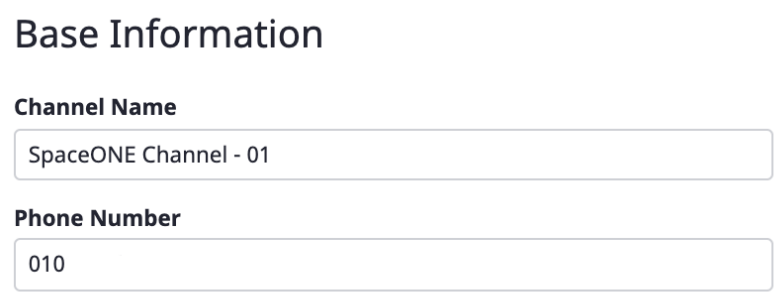
SMS Protocol Channel

You can add **Megazone SMS protocol channels** and recevice notifications for them.
If you create an SMS protocol channel, you will be notified by text messages.
Click **+ Add Megazone SMS Protocol Channel**.



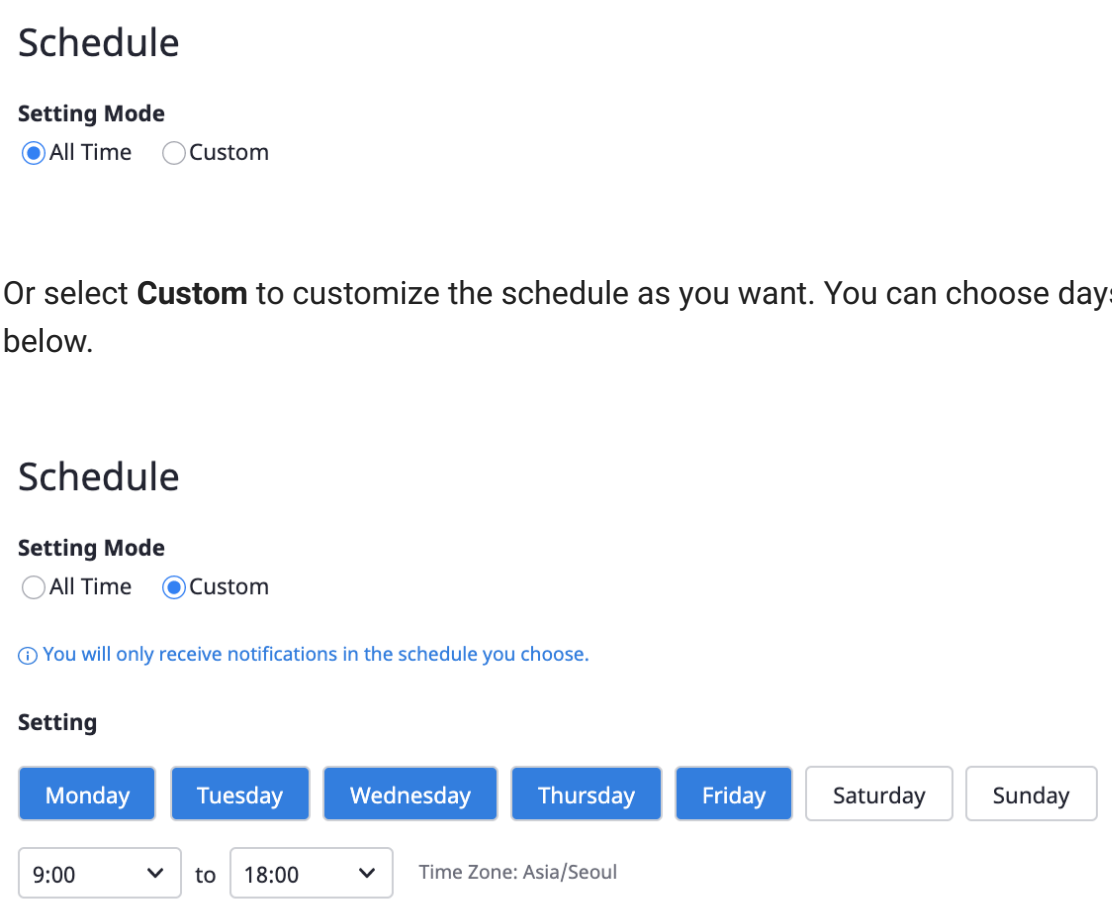
Base Information

Enter an SMS protocol **channel name** and your **phone number**.



Schedule

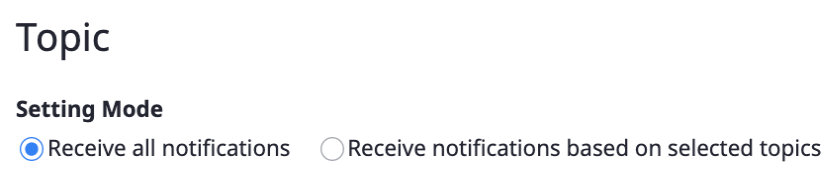
You can set the schedule to **All Time**.



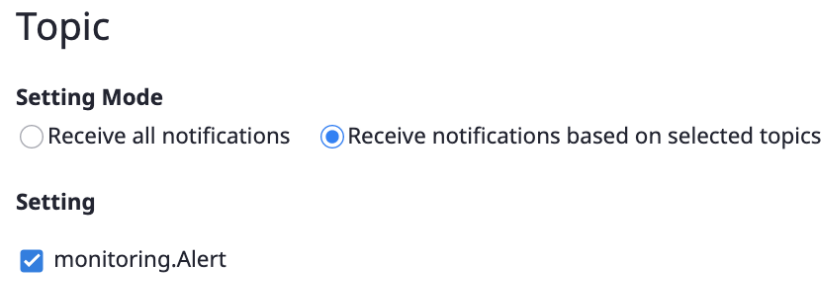
Or select **Custom** to customize the schedule as you want. You can choose days and time as shown below.

Topic

You can choose to receive all notifications regardless of topics.

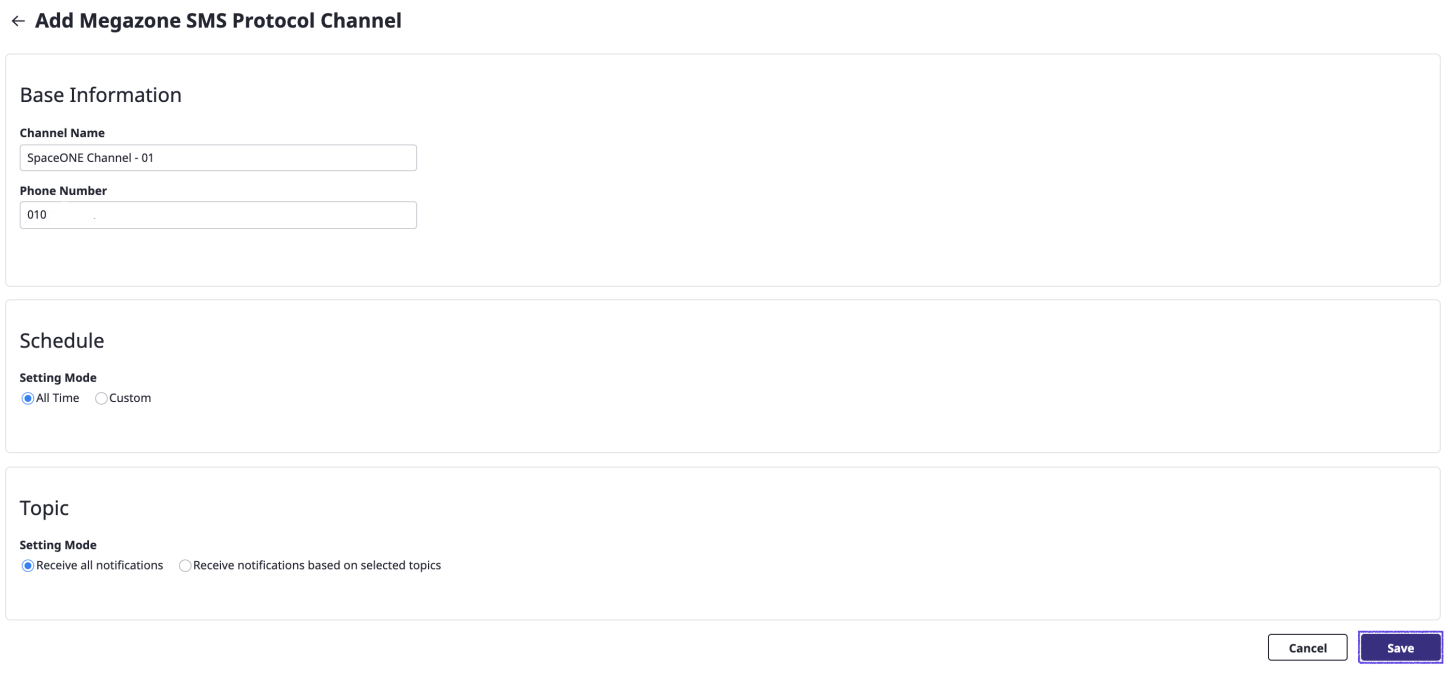


Or you can receive notifications based on selected topics only.



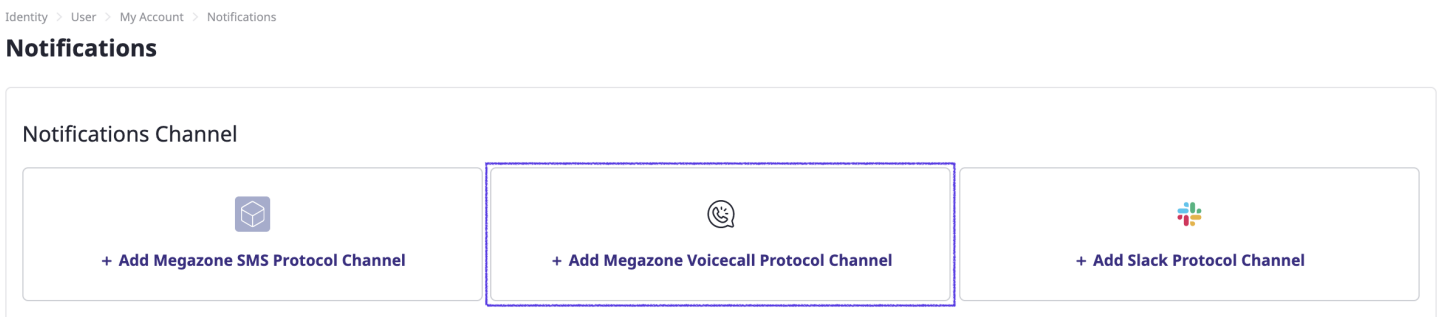
Save

Click the **save** button at the bottom right corner.

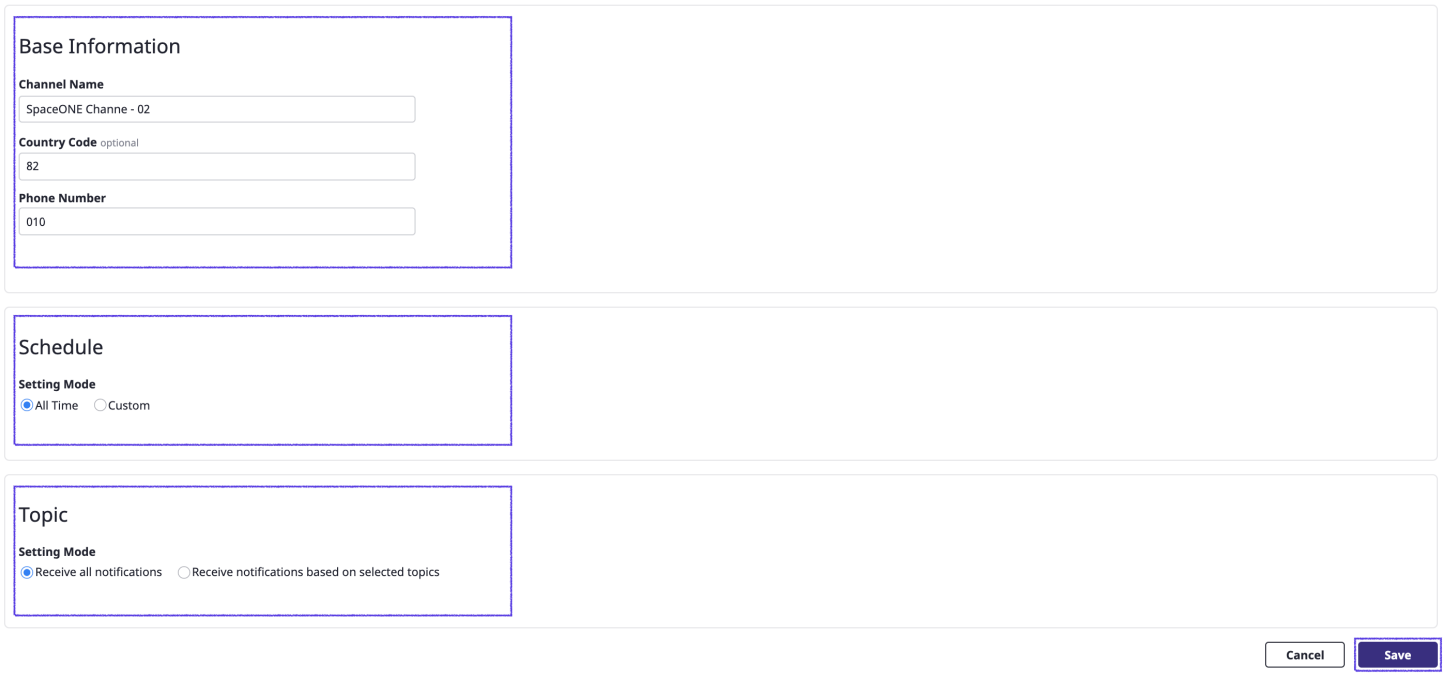


Voicecall Protocol Channel

You can add **Megazone voicecall protocol channel** and recevice notifications for them.
If you create a voicecall protocol channel, you will be notified by voice calls.
Click **+ Add Megazone Voicecall Protocol Channel**.

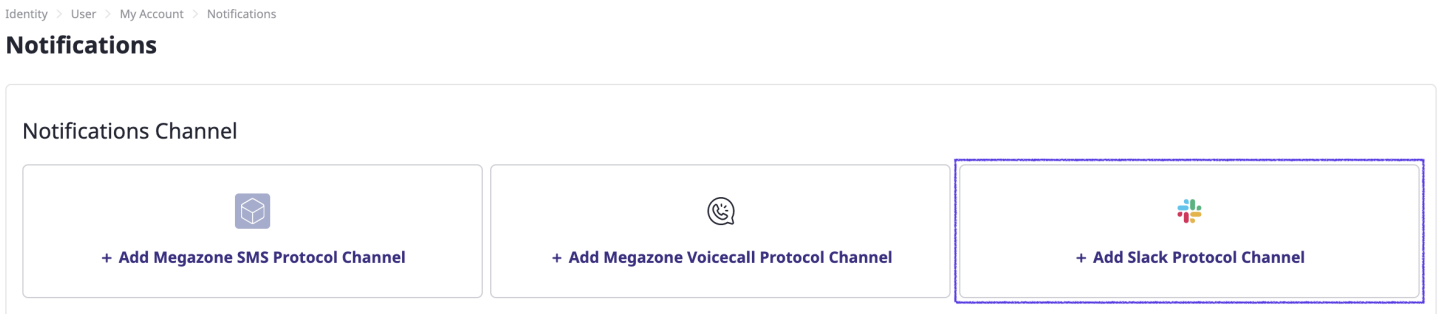


Fill in base information and select schedule and topic setting modes. Then, click the save button.

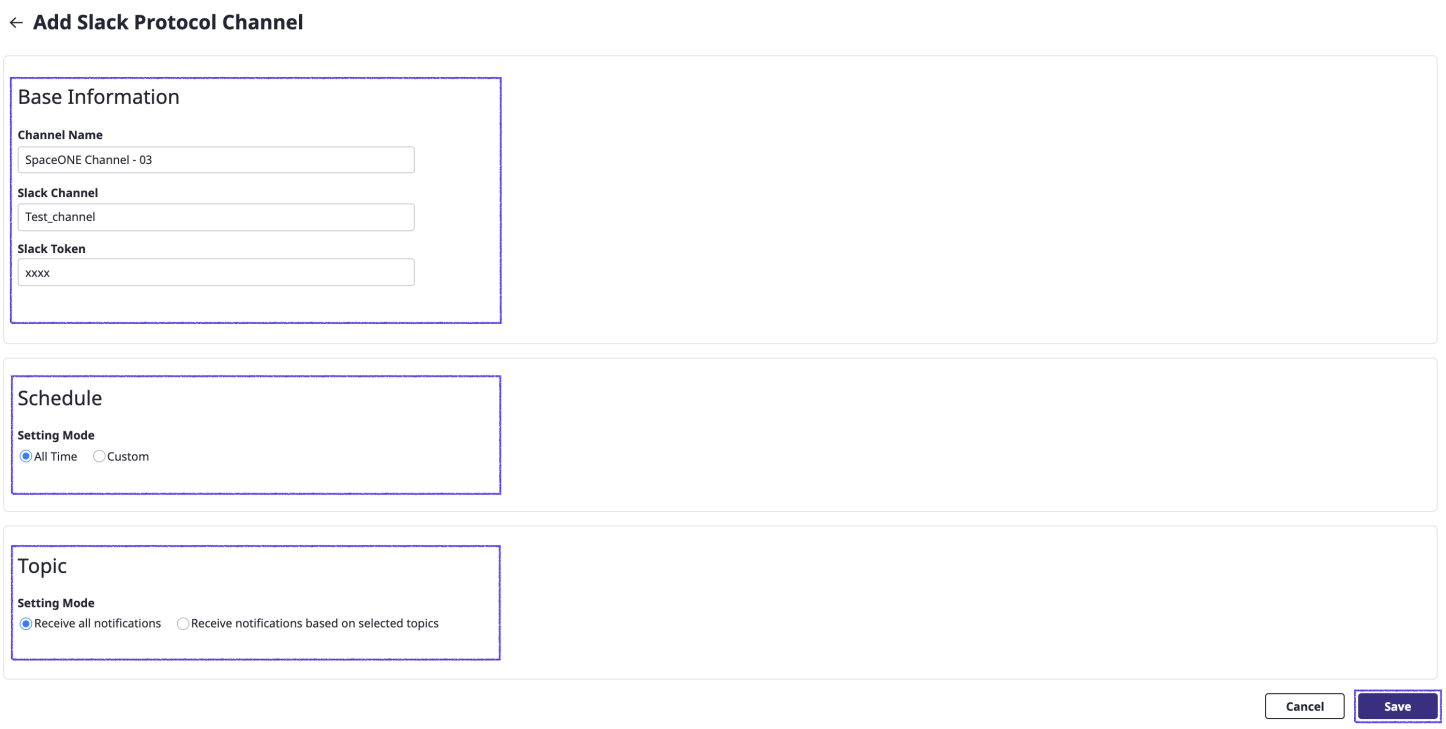


Slack Protocol Channel

You can add **Slack protocol channel** and recevice notifications for them.
If you create a Slack protocol channel, you will be notified from the corresponding Slack channel.
Click **+ Add Slack Protocol Channel**.



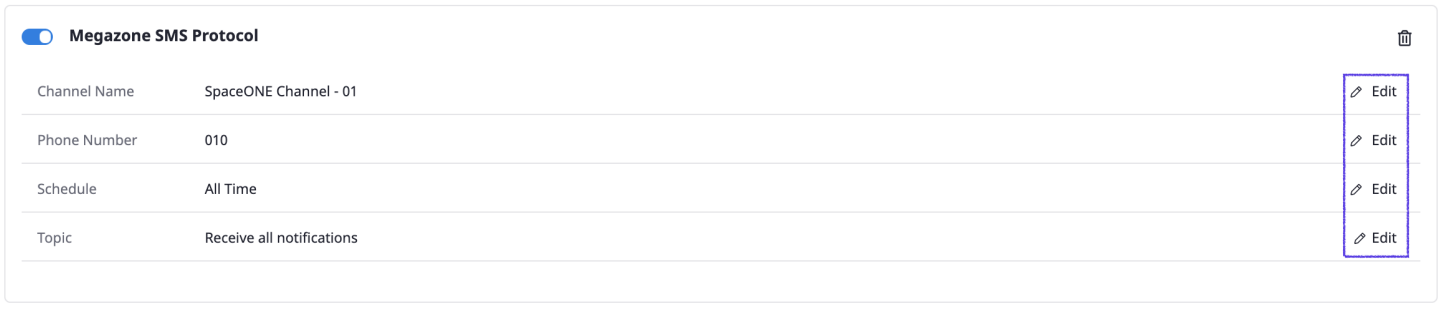
Fill in base information and select schedule and topic setting modes. Then, click the save button.



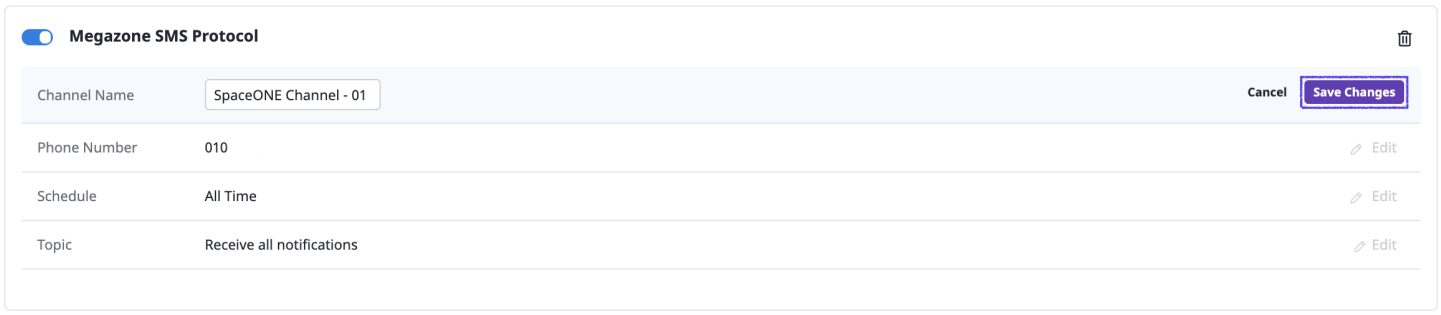
Edit/Delete Channel

Edit

To edit a channel, click the **Edit** button on the right.

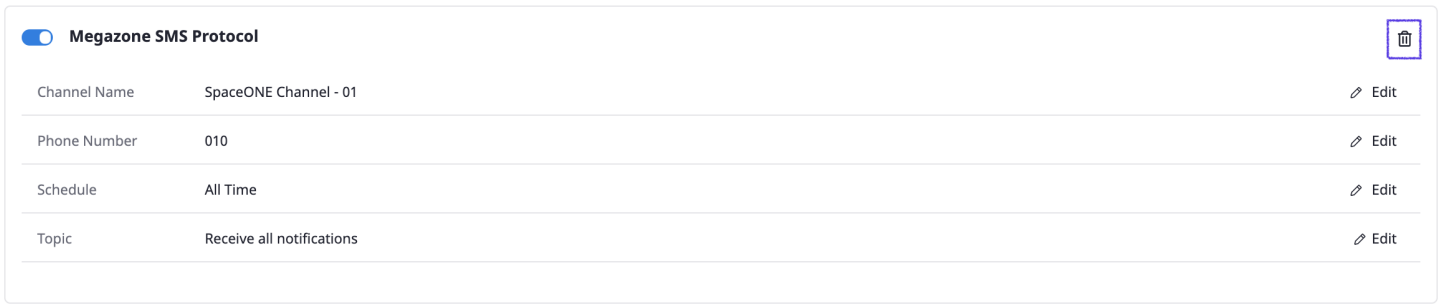


Make changes you want and click the **Save Changes** button.

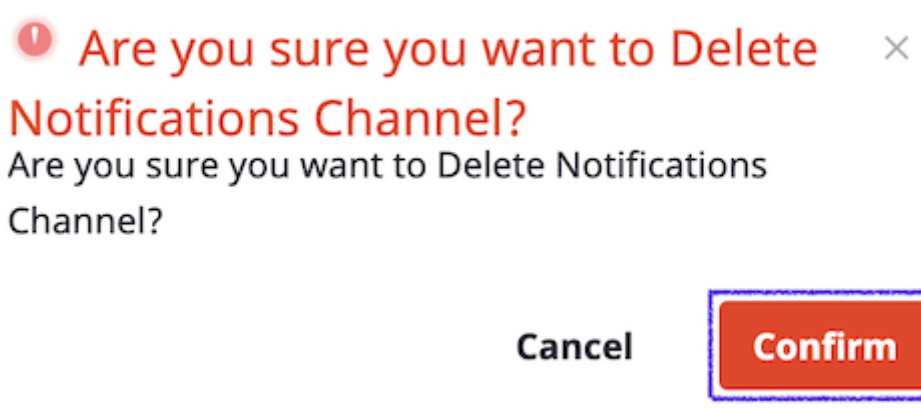


Delete

To delete a channel, click the **trash can icon** on the right.

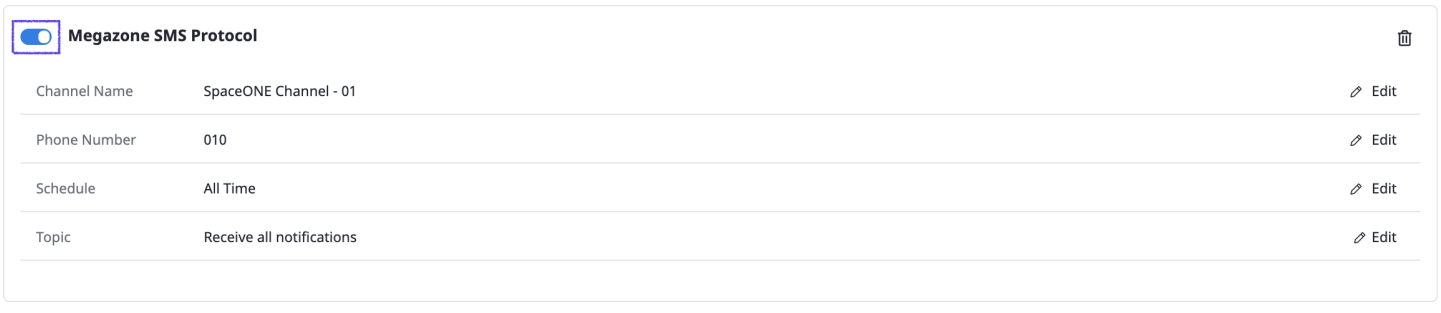


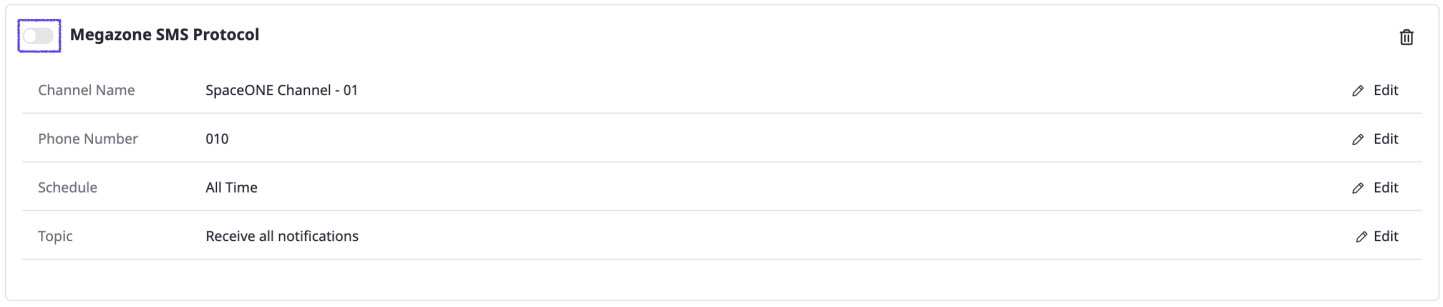
Then the delete confirmation message will pop up as shown below. Click the **Confirm** button.



Enable/Disable Channel

To enable or disable a channel, simply flip the toggle switch button.




Megazone SMS Protocol
Channel Name
SpaceONE Channel - 01
Edit
Phone Number
010
Edit
Schedule
All Time
Edit
Topic
Receive all notifications
Edit