

User Guide

User Guide of SpaceONE

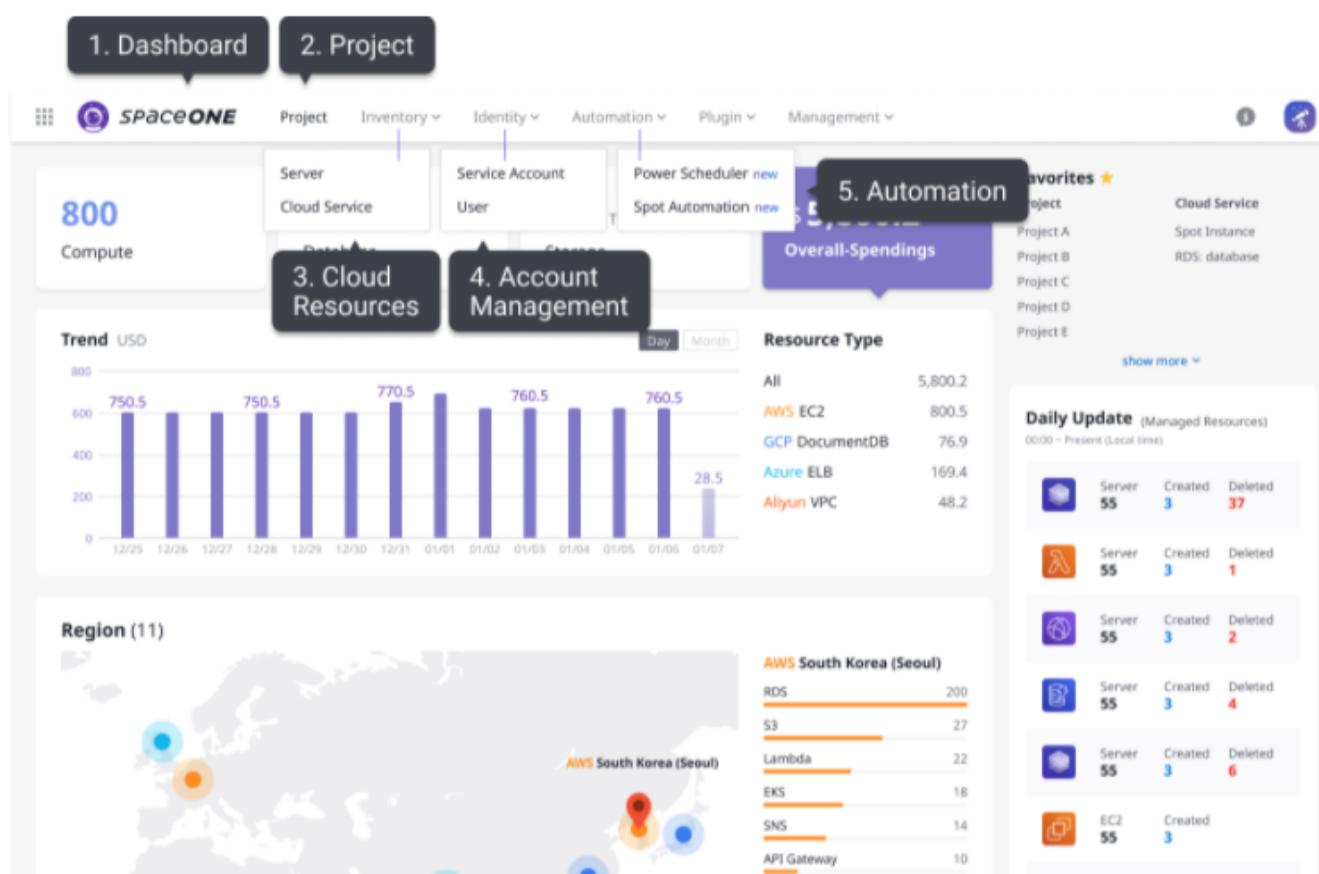
- 1: [Getting Started](#)
 - 1.1: [Basic Setup](#)
 - 1.2: [Power Scheduler Quick Start](#)
 - 1.3: [Alert Manager Quick Start](#)
- 2: [Dashboard](#)
 - 2.1: [Domain Dashboard](#)
- 3: [Project](#)
 - 3.1: [Project Group Management](#)
 - 3.2: [Project Management](#)
- 4: [Service Account](#)
 - 4.1: [\(AWS\) Service Account Policy Management](#)
 - 4.2: [\(Google Cloud\) Service Account Policy Management](#)
 - 4.3: [\(Azure\) Access Control \(IAM\) Policy Management](#)
 - 4.4: [\(Oracle Cloud Infrastructure\) Identity and Access Management\(IAM\) Policy Management](#)
 - 4.5: [\(Alibaba Cloud\) Service Account Policy Management](#)
- 5: [Inventory](#)
 - 5.1: [Server](#)
 - 5.2: [CloudService](#)
- 6: [Monitoring](#)
 - 6.1: [Alert Manager](#)
 - 6.1.1: [Dashboard](#)
 - 6.1.2: [Alert](#)
 - 6.1.3: [Escalation Policy](#)
 - 6.2: [Project Dashboard](#)
 - 6.2.1: [Alert](#)
 - 6.2.2: [Maintenance Window](#)
 - 6.2.3: [Webhook](#)
 - 6.2.4: [Settings](#)
 - 6.3: [Webhook Settings](#)
 - 6.3.1: [AWS SNS Webhook](#)
 - 6.3.2: [Grafana Webhook](#)
 - 6.3.3: [Zabbix Webhook](#)
- 7: [Notification](#)
 - 7.1: [Protocol Settings](#)
 - 7.1.1: [Voice Call Protocol](#)
 - 7.1.2: [SMS Protocol](#)
 - 7.1.3: [Email Protocol](#)
 - 7.1.4: [Slack Protocol](#)
 - 7.1.5: [Telegram Protocol](#)
- 8: [Automation](#)
 - 8.1: [Power Scheduler](#)
- 9: [My Account](#)
 - 9.1: [Account & Profile](#)
 - 9.2: [API Key](#)
 - 9.3: [Notifications](#)

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

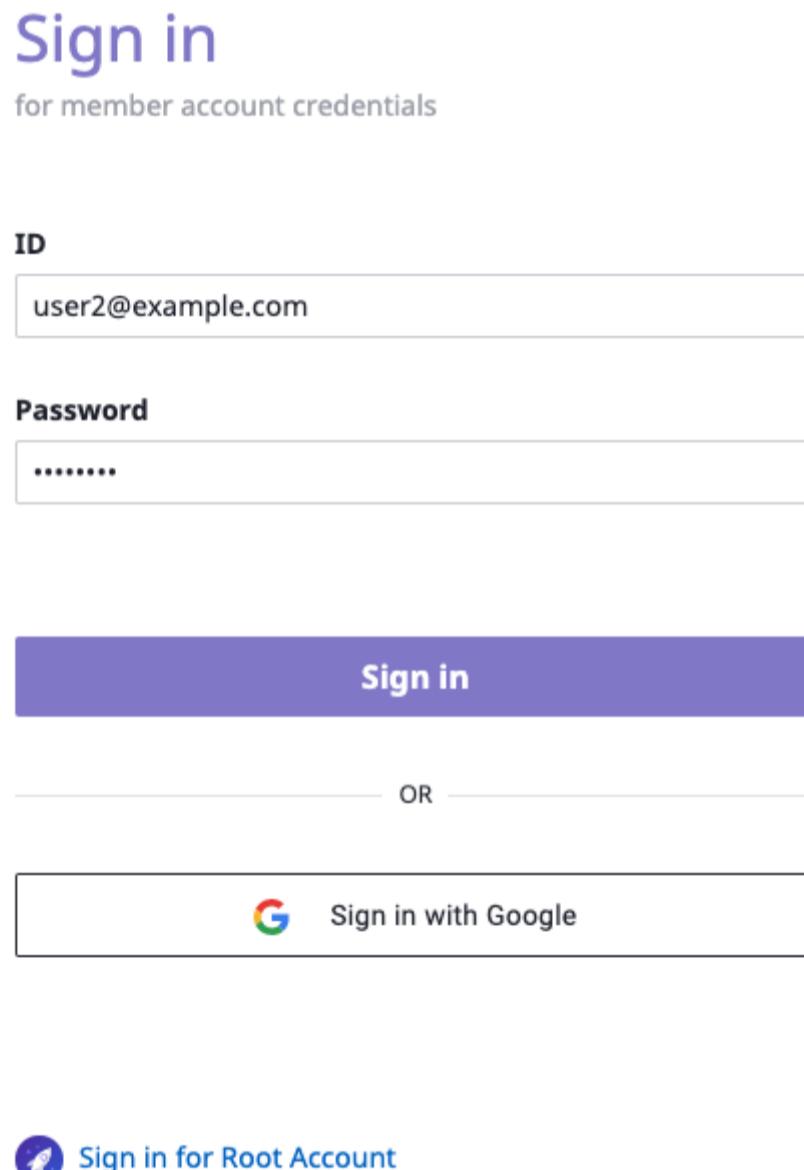
Step by Step Guide for Initial Setup

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.



The image shows a sign-in form for SpaceONE. It has fields for 'ID' (containing 'user2@example.com') and 'Password' (containing '*****'). There is a large purple 'Sign in' button. Below it, a horizontal line with 'OR' in the center separates it from a 'Sign in with Google' button, which includes the Google logo. At the bottom left, there is a link 'Sign in for Root Account' with a small rocket icon.

Sign in
for member account credentials

ID
user2@example.com

Password

Sign in

OR

Sign in with Google

Sign in for Root Account

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.

The screenshot shows the main navigation bar with 'Project' selected. Below it, the 'Favorites (0)' section is visible. The main content area is titled 'All Project (0)' with a sub-section 'Project > Services'. A search bar and a 'Create Group' button are present. At the bottom, there's a link '# All Project'.

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

This screenshot shows a 'Create Project Group' dialog box overlaid on the main project list. The 'Name' field contains 'SpaceONE'. The dialog includes 'Cancel' and 'Confirm' buttons.

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****)

This screenshot shows a 'Create Project' dialog box. The 'Name' field is filled with 'SpaceONE-DEV'. The dialog includes 'Cancel' and 'Confirm' buttons.

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**)

This screenshot shows a 'Create Project' dialog box. The 'Name' field is filled with 'SpaceONE-PRD'. The dialog includes 'Cancel' and 'Confirm' buttons.

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

The screenshot shows the SpaceONE Project management interface. The top navigation bar includes Project, Inventory, Identity, Automation, Plugin, and Management. On the left, there's a sidebar with Favorites (0), Search (SpaceONE Project), Project Groups (All Project, Business Support Systems, Landing Zone, Services, SpaceONE), and a Create Project button. The main content area displays the 'SpaceONE (2)' project group. It lists 'SpaceONE-DEV' and 'SpaceONE-PRD' with their respective server and cloud service counts (both 0). There are buttons to 'Add service account' for each. At the bottom, there's a copyright notice and a support link.

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.

The screenshot shows the SpaceONE Identity > Service Account interface. The top navigation bar includes Project, Inventory, Identity, Automation, Plugin, and Management. On the left, there's a sidebar with Service Providers (MEGAZONE, Google Cloud, SpaceONE, Hyper Billing, Microsoft Azure, AWS). The main content area shows the 'AWS Accounts' section with a '+ Add' button, an Action dropdown, and a search bar. A table header includes columns for Name, Account ID, Project, and Created. Below the table, it says 'No Items'. At the bottom, there's a note to select a service account for more details.

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 **Inventory** 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.

The screenshot shows the SpaceONE web interface with the following details:

- Collector List:** A table showing five collectors. The first one, "aws-cloud-services", is selected and highlighted in blue. It has a priority of 10 and is enabled. The plugin is "AWS Cloud Services collector" version 1.8. The last collected time is 2021-03-03 08:10:42.
- Collector Details View:** A modal window for the selected "aws-cloud-services" collector. It displays the "Base Information" tab, which includes fields like Name, State, Priority, Plugin Name, Version, Provider, Last Collected, and Created. Below this is a "Filter Format" section and a table with no items.

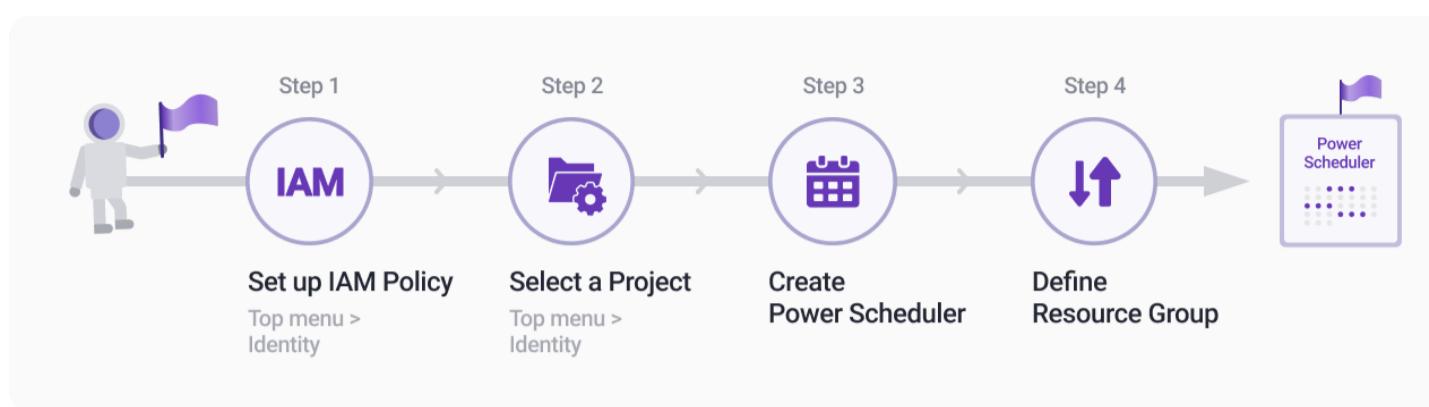
STEP 3: Click Confirm button on Collect Data pop-up window.

The screenshot shows the SpaceONE web interface with the following details:

- Collector List:** A table showing five collectors. The first one, "aws-cloud-services", is selected and highlighted in blue. It has a priority of 10 and is enabled. The plugin is "AWS Cloud Services collector" version 1.8. The last collected time is 2021-03-03 08:10:42.
- Collect Data Pop-up:** A modal window titled "Collect Data" for the "aws-cloud-services" collector. It displays the "AWS Cloud Services Collector" logo and collector ID information. It also shows "Collect Options" and "Credentials" sections, both currently set to "All". At the bottom are "Cancel" and "Confirm" buttons.
- Collector Details View:** A modal window for the selected "aws-cloud-services" collector, showing the "Base Information" tab with the same details as the list.

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](#)

[Set up Basic Scheduler Info](#)

[Configure Scheduler Runtime](#)

[Define Resource Group](#)

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.

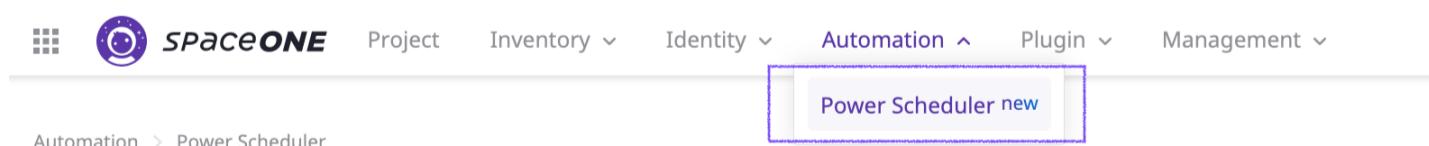
Please, assign corresponding access policies to SpaceONE from each provider's console as mentioned below, prior to create a Power Scheduler.

(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.

Project Group Name		Project Name		Project Group Name		Project Name		Project Group Name		Project Name	
적용된 자원 수 / 적용 가능한 자원 수 0/0	예상 절감 비용 \$ 7,200	적용된 자원 수 / 적용 가능한 자원 수 11/46	예상 절감 비용 \$ 2,921	적용된 자원 수 / 적용 가능한 자원 수 0/0	예상 절감 비용 \$ 5,528	적용된 자원 수 / 적용 가능한 자원 수 0/0	예상 절감 비용 \$ 366	적용된 자원 수 / 적용 가능한 자원 수 0/0	예상 절감 비용 \$ 8,873	적용된 자원 수 / 적용 가능한 자원 수 0/0	예상 절감 비용 \$ 9,986
스케줄 (3) ① [] ② [] ③ []	S M T W T F S [] [] [] [] [] []	스케줄 (+3) ① test2 ② test4	S M T W T F S [] [] [] [] [] []	스케줄 (+3) ①	S M T W T F S [] [] [] [] [] []	스케줄 (2) ① THANKYOUFORTHEMUSIC ② STARTUPSAREGOINGTOSANFRANCISCO-DES...	S M T W T F S [] [] [] [] [] []	스케줄 (1) ① schedule_new	S M T W T F S [] [] [] [] [] []	스케줄 (+3) ①	S M T W T F S [] [] [] [] [] []
+ 스케줄러 설정이 필요합니다.		+ 스케줄러 설정이 필요합니다.		+ 스케줄러 설정이 필요합니다.		+ 스케줄러 설정이 필요합니다.		+ 스케줄러 설정이 필요합니다.		+ 스케줄러 설정이 필요합니다.	
https://spaceone.console.doodle.spaceone.dev/automation/power-scheduler/project-e9bbe6e275f6											

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.

The screenshot shows the SpaceONE web interface with the 'Automation' menu selected. In the 'Power Scheduler' section, there is a list titled 'Scheduler List (0)' which displays the message 'There is no scheduler.' Below this, a form for creating a new scheduler is shown. The 'Scheduler Name' field is empty and has a placeholder 'Set the scheduler name. (no spaces)'. The 'New Scheduler' button is highlighted with a purple box.

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.

This screenshot shows the 'New Scheduler' creation form. The 'Scheduler Name' field is empty and has a blue border around it. The rest of the form includes the 'Automation > Power Scheduler > Electronics > 1' breadcrumb, a back arrow, a power icon, and a 'Scheduler Name' input field.

Configure scheduler runtime

This screenshot shows the 'Scheduler Time' configuration interface. It features a 24-hour grid for selecting a time range. A dashed blue box highlights the grid area where a user is performing a click-and-drag operation to set a time schedule. To the right of the grid, there are sections for 'Time Zone' (Asia/Tokyo), 'Repeat: Schedule' (with options for 'Repeat: Turn on' and 'Turn Off All'), and a 'This week' button.

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.

Scheduler Time Set the scheduler applying time.

02, 2021 < > This week

Time Zone: Asia/Tokyo

Repeat: Schedule

- Repeat: Turn on
- Turn Off All

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

Resource group Resource group to apply the scheduler

+ Add priority group

1 High Priority + Add resource group	2	3 High Priority Please, set group's priority	4	5 Low Priority
---	---	--	---	----------------

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

← Create a resource group

Base Information

Group Name*
Name must start with a maximum of 128 characters / letter and can contain only letters, numbers and hyphens. 16 characters display only on resource group card

Group Category

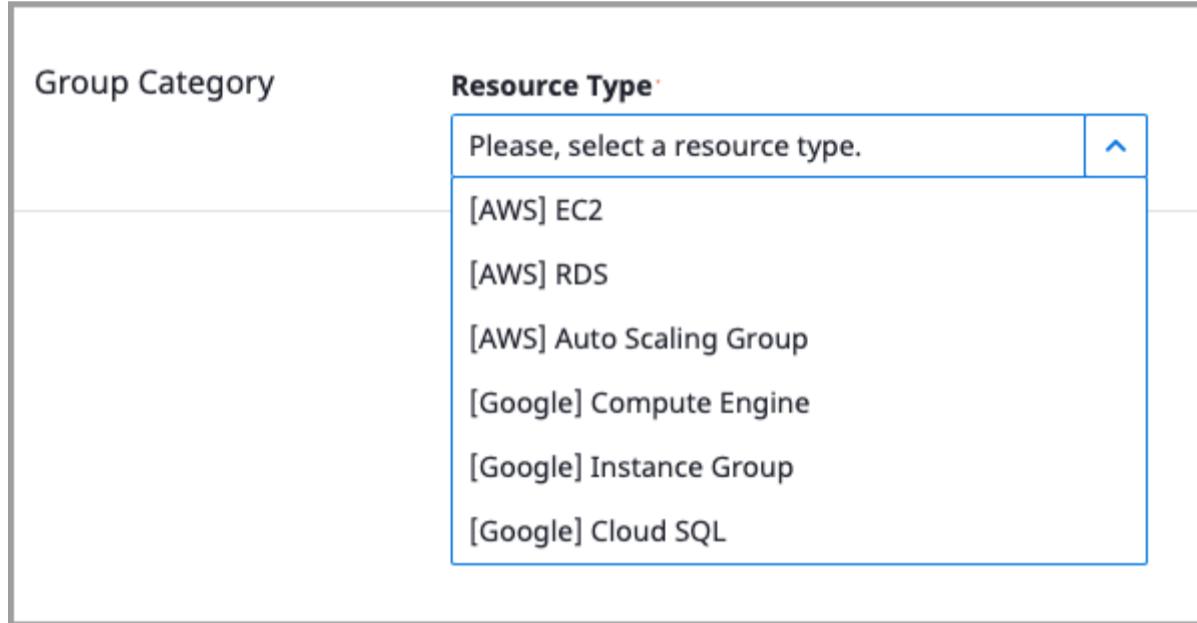
Resource Type
Please, select a resource type.

Cancel
Save

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.

← Create a resource group

Base Information

Group Name*
Name must start with a maximum of 128 characters / letter and can contain only letters, numbers and hyphens. 16 characters display only on resource group card

Group Category

Resource Type*
[AWS] EC2

1. Select resource type

Resource List (65)

Resource Search

Properties (39)								
Name	Instance Type	Core	Memory	Provider	Instance State	Availability Zone	OS	Port
song-windows	t2.medium	2	4	aws	● Running	us-east-1f	win2019	3.2
workernode	t3.medium	2	4	aws	● Running	us-west-1a	amazonlinux	
se2-ec2-02	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
se2-ec2-03	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
se2-ec2-04	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
se2-ec2-05	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
se2-ec2-01	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
se1-ec2-02	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1c	ubuntu	

2. click search bar

3. Select search filter

Cancel
Save

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

Resource List (5) Resource Search

Search Search filter

Filter: Clear all Name:case2 ×

ID	Name	Instance Type	Core	Memory	Provider	Instance State	Availability Zone	OS	Public IP
server-c22649e8e8f2	case2-ec2-02	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
server-95bda74ec29b	case2-ec2-03	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
server-58d6b8f3c859	case2-ec2-04	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
server-d44af70e19ca	case2-ec2-05	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	
server-19c7677bd92e	case2-ec2-01	t1.micro	1	0.61	aws	● Stopped	ap-northeast-1a	ubuntu	

Filtered resource

Enter all information, then click the save button below.



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

Confirm resource group list

X

Please confirm the resource group list. (5)

< 1 / 1 > 15 ⌂

ID	Name	Instance Type	Core	Memory	Provider
server-c22649e8e8f2	case2-ec2-02	t1.micro	1	0.61	aws
server-95bda74ec29b	case2-ec2-03	t1.micro	1	0.61	aws
server-58d6b8f3c859	case2-ec2-04	t1.micro	1	0.61	aws
server-d44af70e19ca	case2-ec2-05	t1.micro	1	0.61	aws
server-19c7677bd92e	case2-ec2-01	t1.micro	1	0.61	aws



✓ Create Power Scheduler success. X

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 Tool입니다. 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 설정입니다.

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.

Project > gikang-test-group01 > alert-manager-test-01

← alert-manager-test-01 ⚡ 🗑️ 🔍

Project ID: project-eefb5d1e8689 ⓘ Create Maintenance Window

Summary Member Alert beta Notifications beta Tag

Set an Alert of this Project

Click 'Activate Alert' to receive integrated external events or manage of this project.

Activate Alert

Configure Webhook Plugin

Project Dashboard > Alert > Webhook 탭을 클릭 합니다.

Add 버튼을 클릭합니다.

Project > gikang-test-group01 > alert-manager-test-01

← alert-manager-test-01 ⚡ 🗑️ 🔍

Project ID: project-eefb5d1e8689 ⓘ Create Maintenance Window

Summary Member Alert beta Notifications beta Tag

Alert Maintenance Window Webhook Settings

Webhook (0)

+ Add Action Search

Name	State	Type	Version	Webhook URL	Created
No Items					

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

Alert beta Notifications beta Tag

Add Webhook

Name
Webhook plugin test 01

Type

- AWS SNS Webhook
- AMOREPACIFIC Webhook
- Grafana Webhook**
- Zabbix Webhook

Version
1.0.1 (latest)

Cancel Confirm

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

Project > gikang-test-group01 > alert-manager-test-01
 ← alert-manager-test-01 ⭐ 🔍

Project ID: project-eefb5d1e8689 ⓘ

Create Maintenance Window

The screenshot shows the 'Alert' tab selected in the navigation bar. Below it, there are tabs for 'Maintenance Window', 'Webhook', and 'Settings'. A search bar and a table header are visible. The table has columns for Name, State, Type, Version, and Webhook URL. One entry is listed: 'Webhook plugin test 01' (Enabled), 'Grafana Webhook', version 1.0.1, with a placeholder URL.

Webhook Plugin Details

각 Tool 별로 설정을 위한 방법은 [Monitoring Tool Webhook Plugin Configuration Guide](#) 를 참고해주세요.

Alarm 수신 설정

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

Notifications Channel 설정

[Project Dashboard < Notifications](#)로 이동합니다.

추가하고자 하는 Channel을 선택 합니다.

Project > gikang-test-group01 > alert-manager-test-01

← alert-manager-test-01 ⭐ 🔍

Project ID: project-eefb5d1e8689 ⓘ

Create Maintenance Window

The screenshot shows the 'Notifications' tab selected in the navigation bar. Below it, there are tabs for 'Summary', 'Member', 'Alert', 'Notifications', and 'Tag'. A search bar and a table header are visible. The table has columns for icon, name, and 'Add' button. Options include Slack Protocol Channel, Megazone Voicecall Protocol Channel, Megazone SMS Protocol Channel, Email Protocol Channel, Telegram Protocol Channel, and SpaceONE User Channel. A note at the bottom states: 'SpaceOne User: Forward to the project members' personal notification channel'.

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

Base Information

Channel Name
Alert Manager Test Notification

Notifications Level
Level 1

Slack Channel
asdf

Slack Token
qwerqwefsdavasdwertzxcv

Schedule

Setting Mode
 All Time Custom

Topic

Setting Mode
 Receive all notifications Receive notifications based on selected topics

Cancel **Save**

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

Notifications Channel



[+ Add Slack Protocol Channel](#)



[+ Add Megazone Voicecall Protocol Channel](#)



[+ Add Megazone SMS Protocol Channel](#)



[+ Add Email Protocol Channel](#)



[+ Add Telegram Protocol Channel](#)



[+ Add SpaceONE User Channel](#)

SpaceOne User: Forward to the project members' personal notification channel

Slack Protocol	
Channel Name	Alert Manager Test Notification
Notifications Level	<input type="button" value="Lvl1"/>
Schedule	All Time
Topic	Receive all notifications

Notification Plugin Details

각 Plugin별 Channel 설정에 대한 상세한 방안은 [Notification Protocol Plugin 설정 가이드](#)를 참고 해주세요.

Escalation Policy 설정

*Project Dashboard > Alert > Settings*로 이동합니다.

Escalation Policy의 **Change** 버튼을 클릭 합니다.

Settings

Notification Policy
All Notifications

Auto Recovery
Do It Manually

Event Rule
0 Rules on This Project

Escalation Policy
Name Default
Finish Condition Acknowledged
Escalation Rules

STEP 1 Notification Level ALL
Repeat all 0 times

Create New Policy 버튼을 클릭 합니다.

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

Change Escalation Policy

Choose an existing policy **✓ Create New Policy**

Name
Notification Test Policy 01

Finish Condition
 Acknowledged Resolved

Escalation Rules
Must be at least 1 minute for a single target. (Up to 5)

Step	Notifications Level	Rule
1	Level 1	Escalates after 5 min.
2	Level 2	
repeat (Apply all steps above)		+ Add Rule

Cancel **Confirm**

적용된 Policy를 확인 합니다.

Escalation Policy

Name [Notification Test Policy 01](#)

Finish Condition Acknowledged

Escalation Rules

STEP 1 Notification Level 1 | Escalates after 5 minutes

[Slack Protocol] Alert Manager Test Notification ON

STEP 2 Notification Level 2

Repeat all 0 times

Escalation Policy Details

Escalation Policy의 상세 설명은 [Escalation Policy 상세 설정 가이드](#)를 참고 해주세요.

2 - Dashboard

About Dash board

2.1 - Domain Dashboard

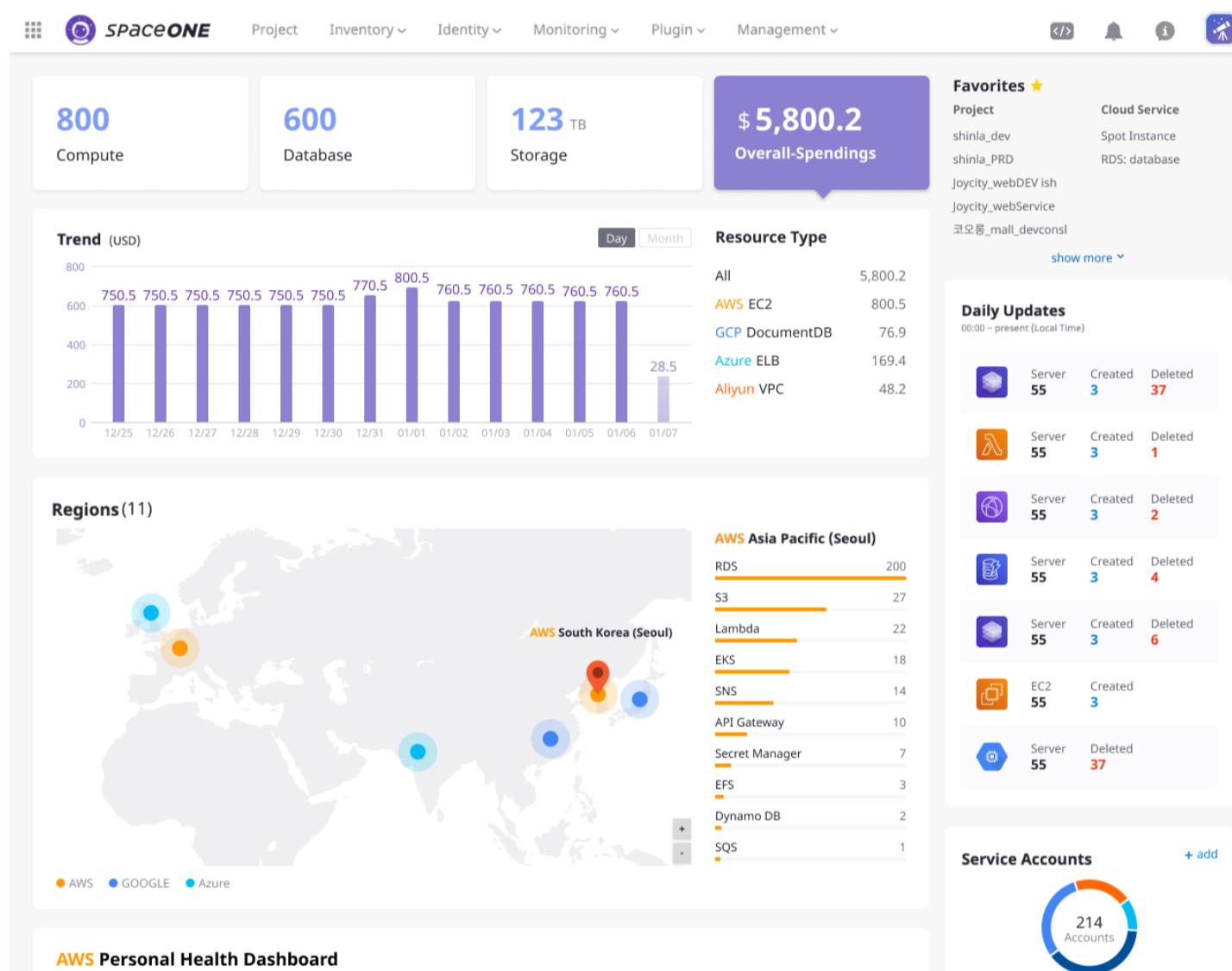
Domain Dashboard provides the full status of the Cloud Resources in your domain.

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.



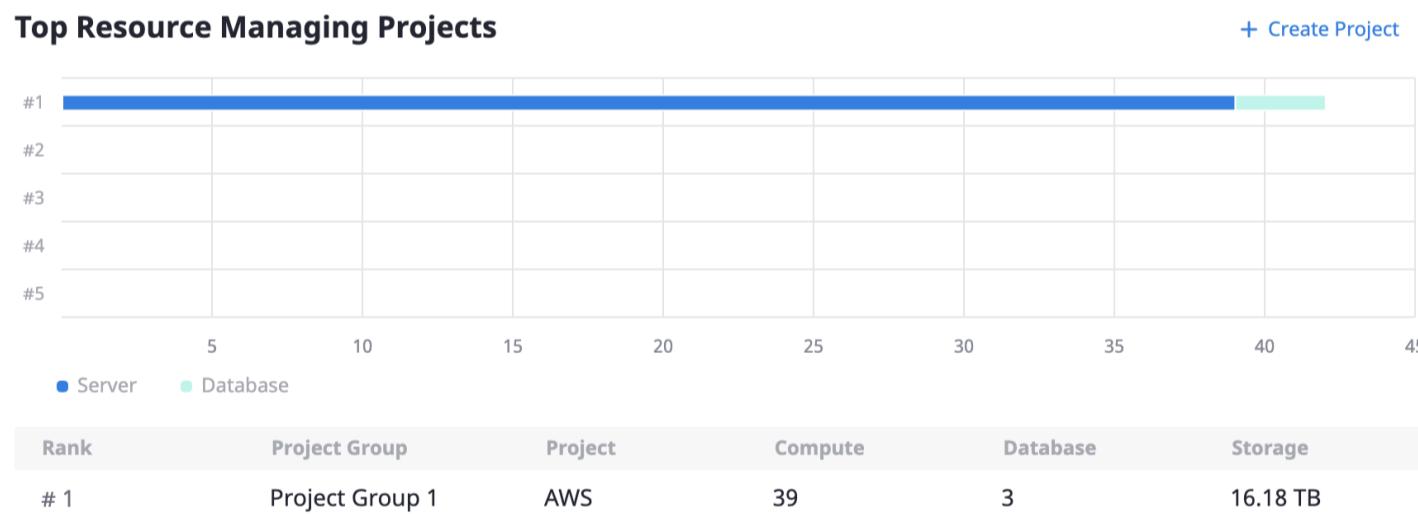
You can use the navigation bar at the top left corner of the screen to quickly navigate to each page.

The dashboard displays key metrics: 3 Database instances and 16.2 TB of Storage. A bar chart shows daily usage from July 22 to August 01, with values ranging from 224.5 to 234.1. A world map is visible at the bottom.

Date	Value
07/22	224.5
07/23	700
07/24	224.5
07/25	224.5
07/26	700
07/27	234.1
07/28	700
07/29	700
07/30	225.8
07/31	700

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.



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.

Service Accounts

[+ Add](#)

Provider	Account	Project
AWS	4	3
Azure	3	3
Google	3	3

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**.

Daily Updates ?

00:00 ~ present (Local time)

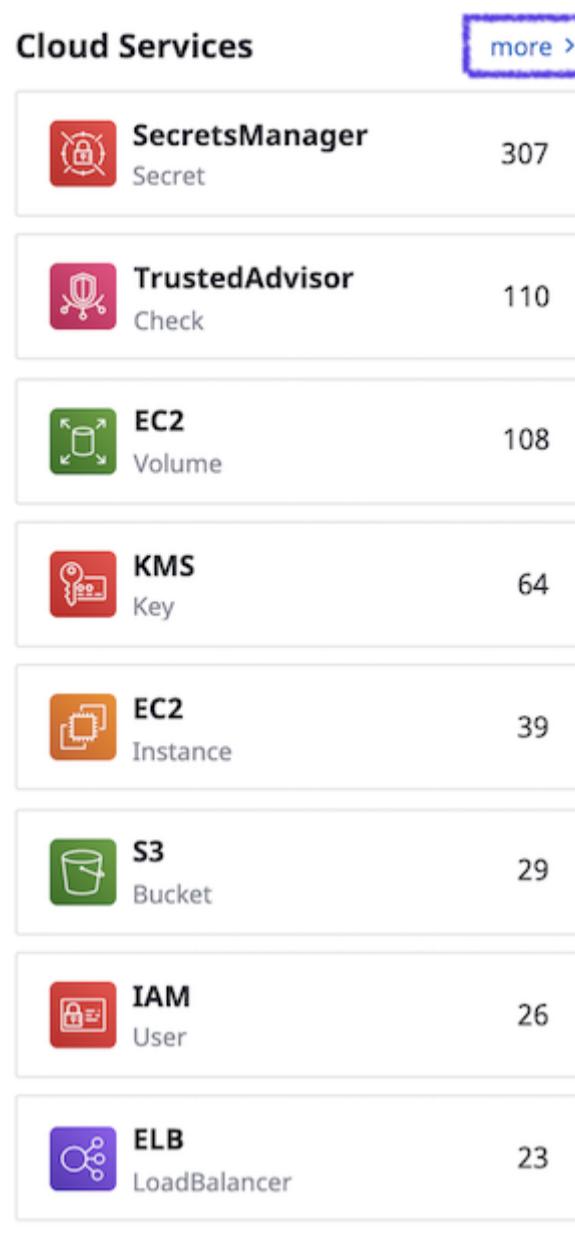


SecretsManager (247) Secret
Created 3

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

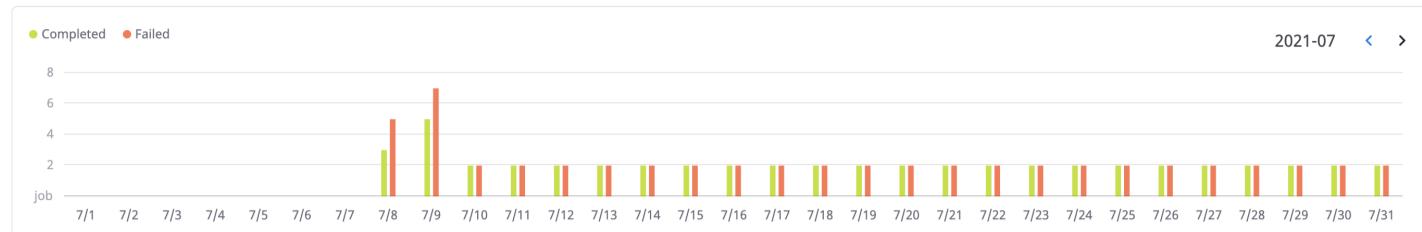
`Collecting jobs` shows jobs that are currently being collected.

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.

Collector History

Collecting Progress

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

Status: All In-Progress Completed Failed

Search: Filter: Clear all | Status: SUCCESS

1 / 4 | 15 | C

Job ID	Collector	Plugin	Status	Job Progress	Created	Duration
job-76fbfac10987	aws-cloud-service-collector-02	AWS Cloud Services collector	✓ Completed	<div style="width: 100%;">100%</div>	2021-08-03 13:48:53	4m 32s
job-a1669caab647	aws-cloud-service-collector	AWS Cloud Services collector	✓ Completed	<div style="width: 100%;">100%</div>	2021-08-03 13:00:01	5m 52s
job-426e73c3e506	google-cloud-service-collector	Google Cloud Services collector	✓ Completed	<div style="width: 100%;">100%</div>	2021-08-03 11:43:28	2m 16s
job-48e019e59328	azure-cloud-service-collector	Azure Cloud Service collector	✓ Completed	<div style="width: 100%;">100%</div>	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**.

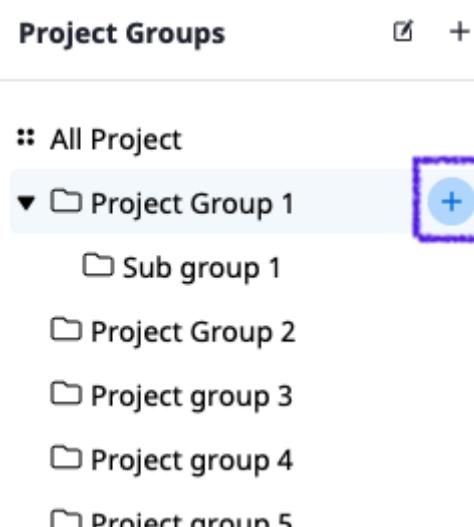
When you select a **Project group**, you can see all the projects that belong to the group at once.

Create Project Group

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

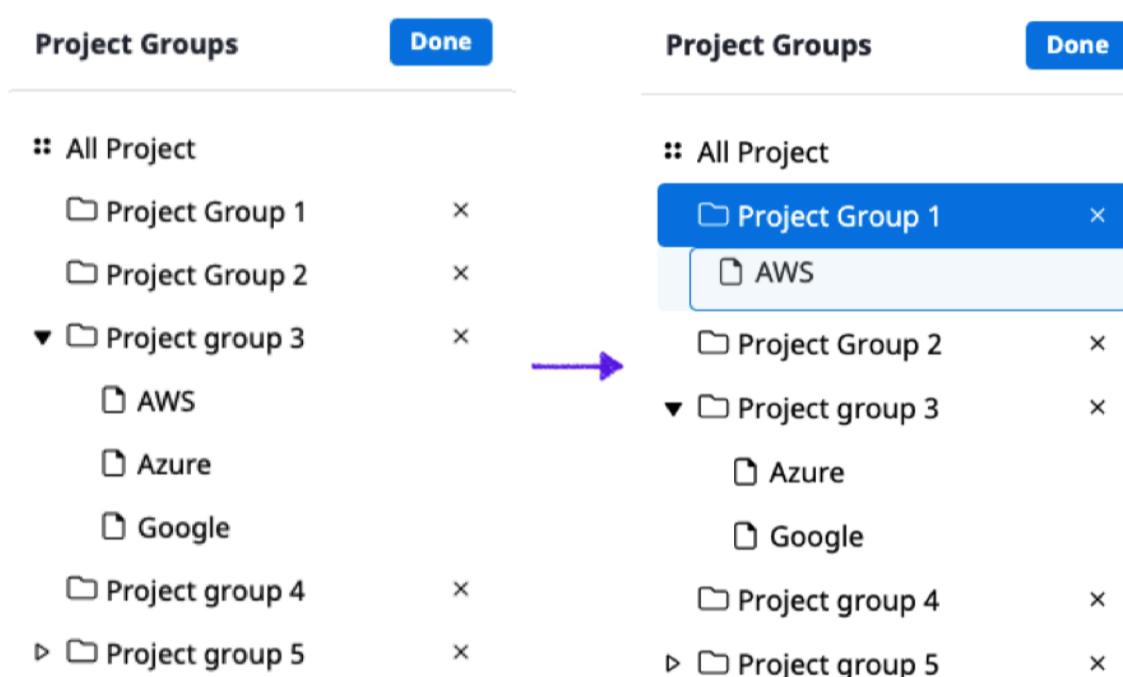
Project Groups can have hierarchical relationships.

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.

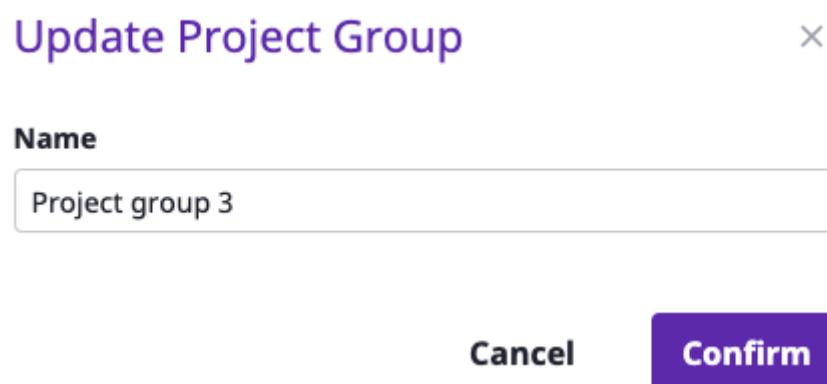
Project > Project group 3

Project group 3 (3) ★

+ Create Project

Edit group name
Delete selected group

Project group 3	AWS	Azure	Google
Servers 39 Cloud Services 178	Servers 0 Cloud Services 0	Servers 0 Cloud Services 0	Servers 0 Cloud Services 0
Service Accounts +	Service Accounts +	Service Accounts +	Service Accounts +



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.

The screenshot shows the SpaceONE web interface. On the left, there's a sidebar with "Favorites (0)", a search bar containing "Project group 3", and a list of "Project Groups" including "Project group 3" (selected), "Project group 1", "Project group 2", "Project group 4", and "Project group 5". The main area shows "Project group 3 (3) ★" with three sub-project cards: "Project group 3 AWS" (Servers 37 | Cloud Services 177), "Project group 3 Azure" (Servers 0 | Cloud Services 0), and "Project group 3 Google" (Servers 0 | Cloud Services 0). To the right, a "Manage Project Group Member" dialog is open, showing a table with one row: "User ID" (checkbox), "User Name" (dropdown), "Role" (dropdown), and "Labels" (dropdown). A "Manage Project Group Member" button is at the top of the dialog.

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

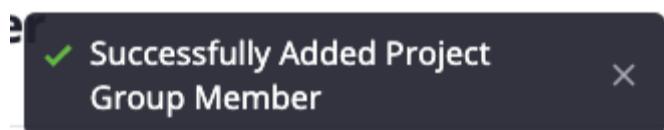
[← Manage Project Group Member](#)

A screenshot of the "Manage Project Group Member" dialog. The table header includes columns for "User ID" (checkbox), "User Name" (dropdown), "Role" (dropdown), and "Labels" (dropdown). There is one row with the status "No Items".

Add Member

The screenshot shows the 'Add Member' dialog box. At the top is a search bar with a placeholder 'Search' and a page indicator '1 / 1'. Below the search bar is a table with three columns: 'User ID', 'Name', and 'Email'. A single row is listed, showing 'example@mz.co.kr' in the 'User ID' column. At the bottom of the dialog are two buttons: 'Cancel' and 'Confirm', with 'Confirm' highlighted.

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 **Update** and **Delete** these Roles through the **Action** list menu.

← Manage Project Group Member

The screenshot shows the 'Manage Project Group Member' table. The table has a header row with columns: Action, User ID, User Name, Role, and Labels. The 'Action' column is expanded, showing 'Update' and 'Delete' options. A single row is listed, showing 'example@mz.co.kr' in the User ID column and 'Project Admin' in the Role column. The 'User ID' column is selected.

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**.

Project group 3 AWS	Project group 3 Azure	Project group 3 Google
Servers 39 Cloud Services 178	Servers 0 Cloud Services 0	Servers 0 Cloud Services 0
Service Accounts +	Service Accounts +	Service Accounts +

You can see a brief summary on how many **Servers** / **Cloud services** each project has.

You can also check your **Cloud Service Account Type**.

Project group 3
AWS

Servers **39** | Cloud Services **178**

Service Accounts +

Search Project Group

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

Search

Project group (6)

- Project Group 1
- Project Group 2
- Project group 3
- Project group 4
- Project group 5
- more

Project (4)

- AWS
- Azure
- Dev-new
- Google

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:

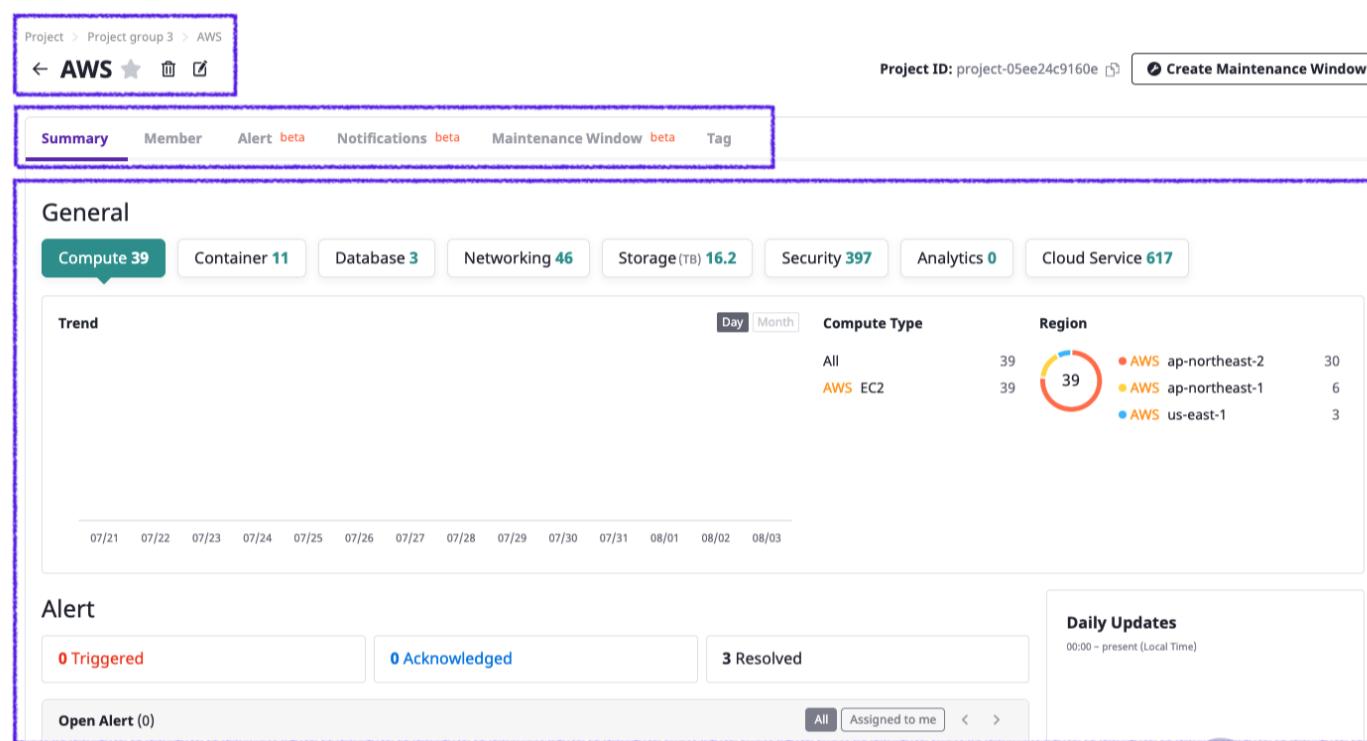
View and edit projects.

View project details

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

Project Dashboard

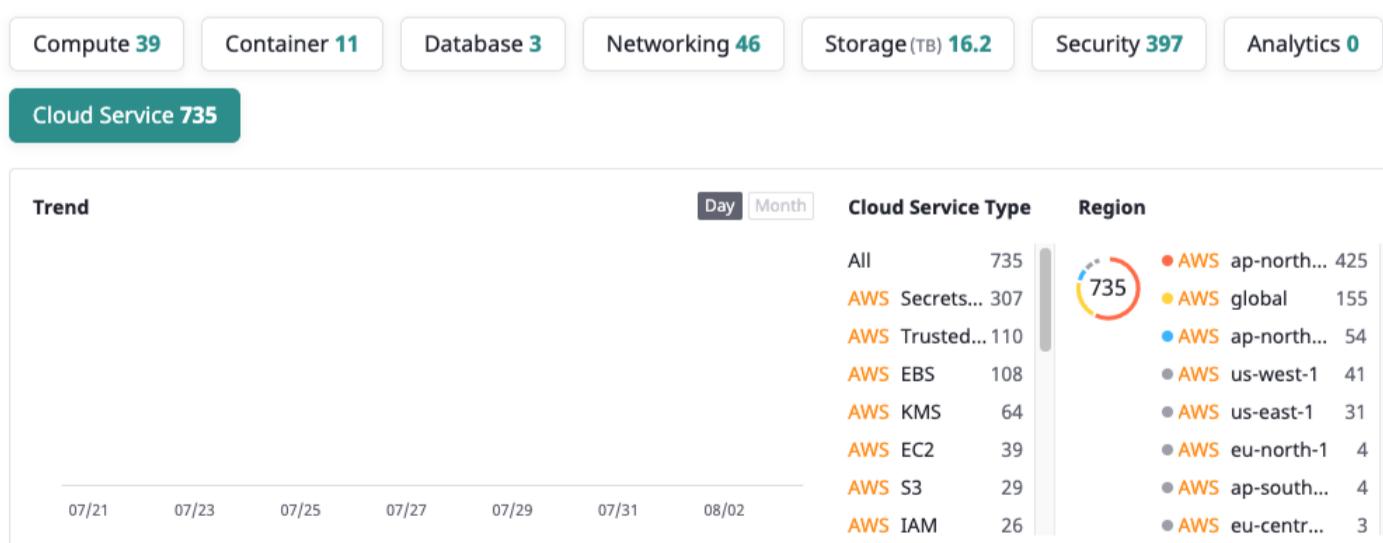
View overall usage of projects. Users can check usage by resource classifications. Click on each classification icon to see the detailed informations.



Summary

General

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



Alert

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

Alert

Open Alert (0)	All	Assigned to me

Billing

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

Billing



Personal Health Dashboard

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

AWS Personal Health Dashboard

0 Open Issues Past 7 days	0 Scheduled Changes Upcoming and Past 7 days	1 Other Notifications Past 7 days

Search

1 / 1

Event	Region	Start Time	Last Update Time	Affected Resources
Lambda Operational Notification ↗	global	2021-07-30 16:15:00	2021-07-30 21:40:43	Account ID :

Service Accounts

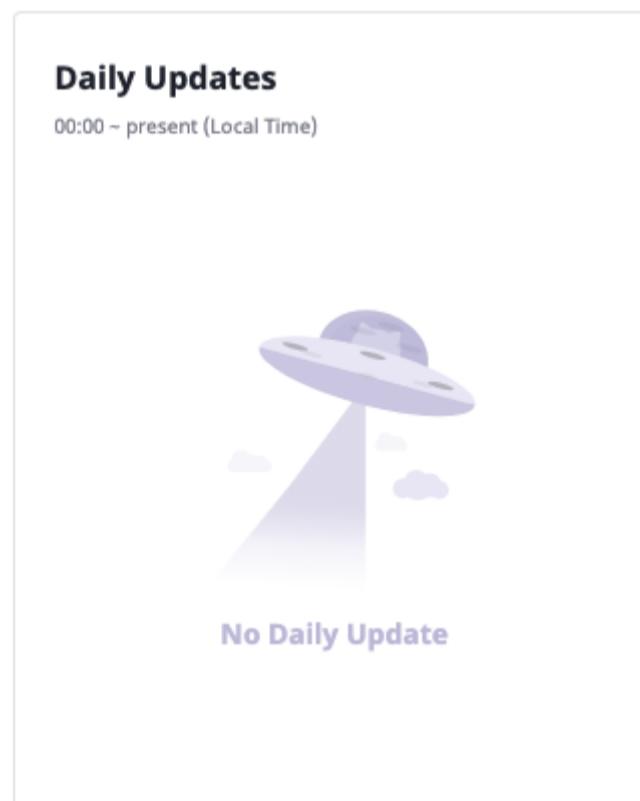
You can check resource usages from **Service Accounts** within the project. You can also check the amount of resources registered.

Provider	Account Name	Compute	Database	Storage
AWS	aws-service-account-01	39	3	16.2 TB

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.

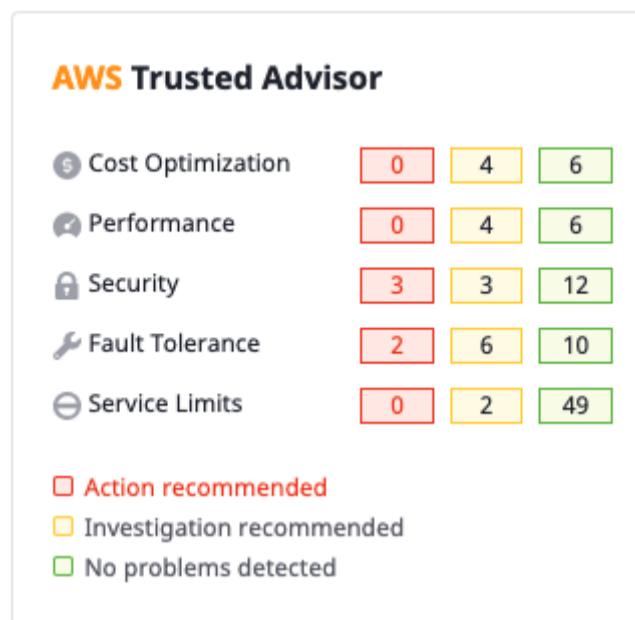
A screenshot of the Cloud Services section. It lists several services with their respective icons and counts:

- SecretsManager Secret: 307
- TrustedAdvisor Check: 110
- EC2 Volume: 108
- KMS Key: 64
- EC2 Instance: 39
- S3 Bucket: 29
- IAM User: 26

At the top right, there is a "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.

User ID	User Name	Role	Labels
stark@example.com		Project Admin	

Add member

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

Add Member

User ID	Name	Email
stark@example.com		
gikang@mz.co.kr	강광일	
claudia@mz.co.kr		

Add Member

Project Role: Select a Role

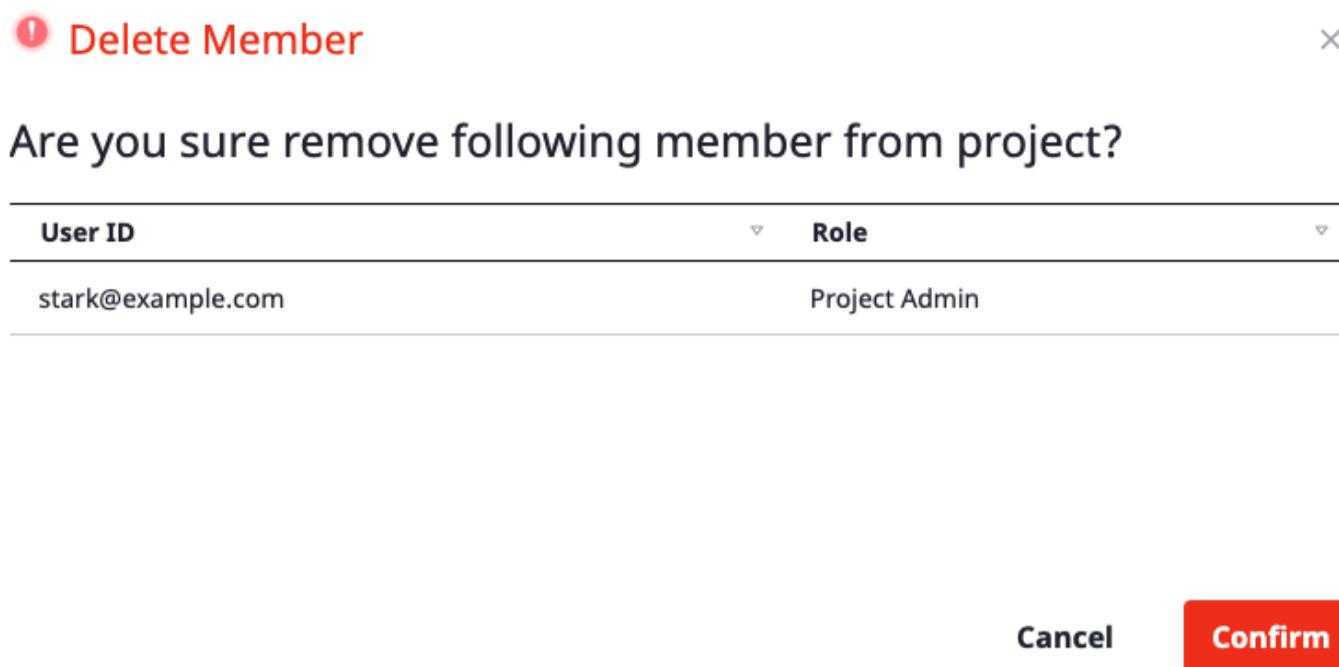
Labels: Up to 5 Labels

Ex. Developer +

Cancel Confirm

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**.

The interface shows the "Alert" tab selected. It includes buttons for "Alert", "Webhook", and "Settings". Below is a table header for "Alert (0)" with columns: No, Title, State, Urgency, Status Details, Resource, Created, Duration, Assigned to, and Triggered by. There are filters for State (Open), Urgency (All), and Assigned to me.

Notifications

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

The interface shows the "Notifications" tab selected. It displays a "Notifications Channel" section with four options: "Add Slack Protocol Channel" (Slack icon), "Add Megazone Voicecall Protocol Channel" (Megazone icon), "Add Megazone SMS Protocol Channel" (Megazone icon), and "Add SpaceONE User Channel" (User icon). A note at the bottom states: "SpaceOne User: Forward to the project members' personal notification 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.

Project > Project group 3 > AWS
 ← AWS ⚡ 📁 🖌

Project ID:



Create Maintenance Window

The screenshot shows the 'Maintenance Window' section of the AWS project. The table has the following columns: Title, State, Start Time, End Time, Created By, and Created. One row is present, titled 'Maintenance Example', which is currently 'Open'. The start time is 2021-08-03 14:52:00 and the end time is 2021-08-03 15:07:00. It was created by '@mz.co.kr' on 2021-08-03 14:52:45. There are buttons for 'Update' and 'Close' at the top left, and a search bar at the top right. The page number is 1/1, and there are 15 items per page.

Tag

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

The screenshot shows the 'Tag' section of the AWS project. The table has columns for Key and Value. There are no entries in the table.

← Tags

Add associated tags.
 The Key - Value pair is a required field. Only underscores (_), characters, and numbers are allowed. International characters are allowed.

+ Add Tags

Product Owner	:	Example	X
Region	:	Example	X

Cancel **Save**

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.

Base Information

ID	sa-99782cd6435d
Name	aws-service-account-03
Account ID	
Project	project-adeadf032dbb
Created	2021-08-03 02:39:00

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

Base Information

name

Account ID

Tags

Set [Test Service Account]'s tag.
The Key - Value pair is a required field. Only underscores (_), characters, and numbers are allowed. International characters are allowed.

[+ Add Tags](#)

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

Credentials

name

Secret Type

aws_access_key aws_assume_role

Input Form	Json Code
AWS Access Key <input type="text"/>	
AWS Secret Key <input type="text"/>	

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

Credentials

name

Secret Type

aws_access_key aws_assume_role

Input Form	Json Code
AWS Access Key <input type="text"/>	
AWS Secret Key <input type="text"/>	
Role ARN <input type="text"/>	

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.

The screenshot shows a user interface for selecting a project. At the top left is the word "Project". To its right is a button labeled "+ Create Project" with a blue border. Below this is a tree view of project groups:

- Project Group 1** (indicated by a downward arrow):
 - AWS
 - Azure
 - Google
 - Hyperbilling
- Project Group 2** (indicated by a rightward arrow):
 - Project Group 3

At the bottom of the list is the option " No project selected".

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**.

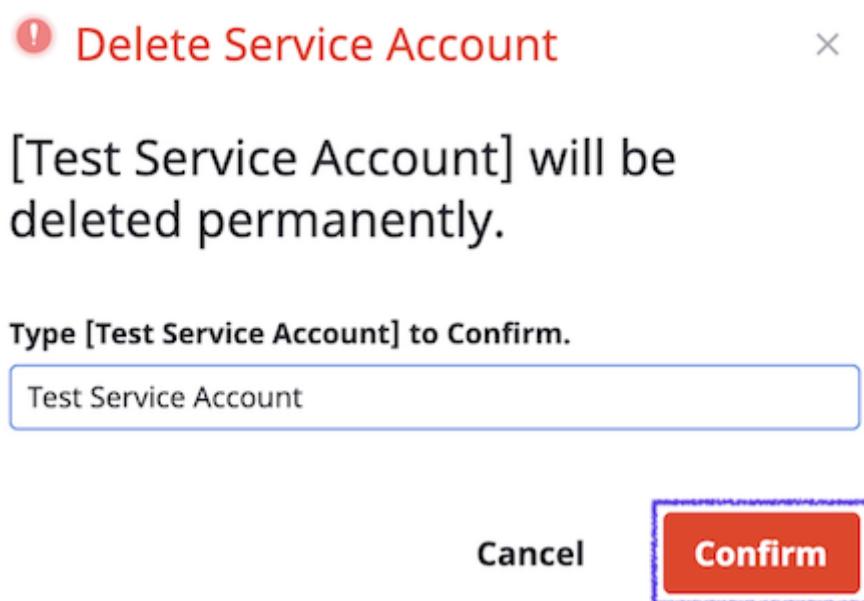
Select the target **Service Account**, then click **Action > Delete/Change Project**.

The screenshot shows a table listing service accounts. The columns are: Name, Account ID, Project, and Created. A search bar and pagination controls are at the top.

<input type="button" value="+ Add"/>	<input type="button" value="Action"/>	Search	<	1 / 1	>	15	▼	<input type="button"/>	<input type="button"/>	<input type="button"/>	C
		Delete									
<input type="checkbox"/>	Name	Change Project	Account ID	Project	Created						
<input checked="" type="checkbox"/>	Test Serv	Connect to Console	123456789001	Project Group 1 > AWS	2021-08-04 11:37:51						
<input type="checkbox"/>	aws-service-account-03	1233333		Project Group 2 > Canada	2021-08-03 11:39:00						
<input type="checkbox"/>	aws-service-account-02	123333		Project Group 2 > Japan	2021-08-03 11:36:48						
<input type="checkbox"/>	aws-service-account-01	257706363616		Project Group 1 > AWS	2021-07-08 16:06:49						

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**.

+ Add		Action	Search	<	1 / 1	>	15	▼	X	⚙	C
		Delete		Account ID	Project	Created					
Name											
Test Serv	<input checked="" type="checkbox"/>	Change Project	Connect to Console	123456789001	Project Group 1 > AWS	2021-08-04 11:37:51					
aws-service-account-03	<input type="checkbox"/>			1233333	Project Group 2 > Canada	2021-08-03 11:39:00					
aws-service-account-02	<input type="checkbox"/>			123333	Project Group 2 > Japan	2021-08-03 11:36:48					
aws-service-account-01	<input type="checkbox"/>			257706363616	Project Group 1 > AWS	2021-07-08 16:06:49					

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.

Details	Tag	Credentials	Member
Base Information			
ID	sa-353cd58dac69		
Name	Test Service Account		
Account ID	123456789001		
Project	project-7f0378dcd6ef		
Created	2021-08-04 02:37:51		

Tag

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

Details	Tag	Credentials	Member
Tags (0)			
Key		Value	
No Items			

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

Tags

Add associated tags.
The Key - Value pair is a required field. Only underscores (_), characters, and numbers are allowed. International characters are allowed.

Environment	:	Test	
-------------	---	------	--

Credentials

Credentials that contain key information can be added or deleted.

[Details](#) [Tag](#) [Credentials](#) [Member](#)

Credentials (1)

A screenshot of a web-based management interface. At the top, there are tabs labeled 'Details', 'Tag', 'Credentials' (which is highlighted with a purple border), and 'Member'. Below the tabs is a search bar with placeholder text 'Search' and a button with a magnifying glass icon. To the right of the search bar are navigation icons: a left arrow, '1 / 1', a right arrow, a page number '15', a down arrow, and a refresh/circular arrow icon. A horizontal line separates the header from the main content area. The main content area contains a table with four columns: 'Secret', 'Name', 'Schema', and 'Created'. There is one row in the table, representing a 'Test Service Account' with secret ID 'secret-9ecd059953e5', schema 'aws_access_key', and creation date '2021-08-04 11:37:51'.

Secret	Name	Schema	Created
secret-9ecd059953e5	Test Service Account	aws_access_key	2021-08-04 11:37:51

Member

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

[Details](#) [Tag](#) [Credentials](#) [Member](#)

Member (3)

A screenshot of a web-based management interface. At the top, there are tabs labeled 'Details', 'Tag', 'Credentials', and 'Member' (which is highlighted with a purple border). Below the tabs is a search bar with placeholder text 'Search' and a button with a magnifying glass icon. To the right of the search bar are navigation icons: a left arrow, '1 / 1', a right arrow, a page number '15', a down arrow, and a refresh/circular arrow icon. A horizontal line separates the header from the main content area. The main content area contains a table with four columns: 'User ID', 'User Name', 'Role', and 'Labels'. There are three rows in the table, each representing a user: Ray (User ID Ray@spaceone.co.kr, User Name Ray, Role Project Admin, Labels Developer), Ellen (User ID Ellen@spaceone.co.kr, User Name Ellen, Role Project Admin, Labels Developer), and Dylan (User ID Dylan@spaceone.co.kr, User Name Dylan, Role Project Admin, Labels Developer).

User ID	User Name	Role	Labels
Ray@spaceone.co.kr	Ray	Project Admin	Developer
Ellen@spaceone.co.kr	Ellen	Project Admin	Developer
Dylan@spaceone.co.kr	Dylan	Project Admin	Developer

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**.

Add user

1 2 3 4 5

Set user details

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

User name*	api-user-for-collector
+ Add another user	

Select AWS access type

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

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

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.

Add user

1 2 3 4 5

▼ Set permissions

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

Create policy
Filter policies
readonly
Showing 154 results

	Policy name	Type	Used as
<input type="checkbox"/>	IAMReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	NeptuneReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	None
<input checked="" type="checkbox"/>	ReadOnlyAccess	AWS managed	Permissions policy (5)
<input type="checkbox"/>	ResourceGroupsandTagEditorReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	ServiceQuotasReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	TranslateReadOnly	AWS managed	None
<input type="checkbox"/>	WellArchitectedConsoleReadOnlyAccess	AWS managed	None

▶ Set permissions boundary

Step 4. Add Tags

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

SpaceONE collectors are not related to tags in IAM.

Add user

1 2 3 4 5

Add tags (optional)

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

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

You can add 50 more tags.

Step 5. Review

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

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	api-user-for-collector
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

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

Type	Name
Managed policy	ReadOnlyAccess

Tags

No tags were added.

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).

Add user

1 2 3 4 5

Success

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

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

 Download .csv

	User	Access key ID	Secret access key
▶ <input checked="" type="checkbox"/>	api-user-for-collector		***** Show

PowerScheduler

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

Step 1. Create Policy

Go to IAM > Policies > Create policy.

The screenshot shows the 'Policy actions' section of the SpaceONE IAM interface. At the top, there are buttons for 'Create policy' and 'Policy actions'. Below this is a search bar and a filter dropdown labeled 'Filter policies'. A table lists several policies:

	Policy name	Type
<input type="radio"/>	▶	AWS managed
<input type="radio"/>	▶	Job function
<input type="radio"/>	▶	AWS managed
<input type="radio"/>	▶	AWS managed
<input type="radio"/>	▶	Customer managed

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**.

Create policy

1 2

Review policy

Name*	api-power-scheduler-policy																																
Use alphanumeric and '+,-,@-' characters. Maximum 128 characters.																																	
Description	api policy for spaceone power scheduler																																
Maximum 1000 characters. Use alphanumeric and '+,-,@-' characters.																																	
Summary	<table border="1"> <thead> <tr> <th colspan="4">Filter</th> </tr> <tr> <th>Service</th> <th>Access level</th> <th>Resource</th> <th>Request condition</th> </tr> </thead> <tbody> <tr> <td colspan="4">Allow (5 of 269 services) Show remaining 264</td> </tr> <tr> <td>DynamoDB</td> <td>Limited: Write, Tagging</td> <td>All resources</td> <td>None</td> </tr> <tr> <td>EC2</td> <td>Full: Tagging Limited: Write</td> <td>All resources</td> <td>None</td> </tr> <tr> <td>EC2 Auto Scaling</td> <td>Limited: Write, Tagging</td> <td>All resources</td> <td>None</td> </tr> <tr> <td>RDS</td> <td>Full: Tagging Limited: Write</td> <td>All resources</td> <td>None</td> </tr> <tr> <td>Support</td> <td>Limited: Read</td> <td>All resources</td> <td>None</td> </tr> </tbody> </table>	Filter				Service	Access level	Resource	Request condition	Allow (5 of 269 services) Show remaining 264				DynamoDB	Limited: Write, Tagging	All resources	None	EC2	Full: Tagging Limited: Write	All resources	None	EC2 Auto Scaling	Limited: Write, Tagging	All resources	None	RDS	Full: Tagging Limited: Write	All resources	None	Support	Limited: Read	All resources	None
Filter																																	
Service	Access level	Resource	Request condition																														
Allow (5 of 269 services) Show remaining 264																																	
DynamoDB	Limited: Write, Tagging	All resources	None																														
EC2	Full: Tagging Limited: Write	All resources	None																														
EC2 Auto Scaling	Limited: Write, Tagging	All resources	None																														
RDS	Full: Tagging Limited: Write	All resources	None																														
Support	Limited: Read	All resources	None																														

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**.

Add user

1 2 3 4 5

Set user details

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

User name*	api-user-for-collector
+ Add another user	

Select AWS access type

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

<input checked="" type="checkbox"/> Programmatic access	Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
<input type="checkbox"/> AWS Management Console access	Enables a password that allows users to sign-in to the AWS Management Console.

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

Add user

1 2 3 4 5

Set permissions

Policy name	Type	Used as
AutoScalingReadOnlyAccess	AWS managed	None

Step 7. Review

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

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	api-user-for-collector
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

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

Type	Name
Managed policy	AmazonDynamoDBReadOnlyAccess
Managed policy	AmazonEC2ReadOnlyAccess
Managed policy	AutoScalingReadOnlyAccess
Managed policy	AmazonRDSReadOnlyAccess
Managed policy	api-power-scheduler-policy

Tags

No tags were added.

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).

Add user

1 2 3 4 5

Success

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

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

Download .csv

	User	Access key ID	Secret access key
	api-user-for-collector		***** Show

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.

The screenshot shows the AWS IAM Policies page. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' at the top, followed by 'Dashboard', 'Access management' (with 'Groups', 'Users', and 'Roles' listed), 'Policies' (which is highlighted in orange), 'Identity providers', and 'Account settings'. At the top right, there are 'Create policy' and 'Policy actions' buttons. Below these are 'Filter policies' and a search bar. A table lists existing policies:

	Policy name	Type
<input type="radio"/>	▶	AWS managed
<input type="radio"/>	▶	Job function
<input type="radio"/>	▶	AWS managed
<input type="radio"/>	▶	AWS managed
<input type="radio"/>	▶	Customer managed

Step 2. Attach Policy Definitions

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

Create policy

1

2

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

The screenshot shows the 'Create policy' wizard. It has two tabs: 'Visual editor' (which is currently selected) and 'JSON'. There's also a 'Import managed policy' button. The JSON code area contains the following policy definition:

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "support:DescribeAttachment",
8                  "support:DescribeCaseAttributes",
9                  "support:DescribeCases",
10                 "support:DescribeCommunications",
11                 "support:DescribeIssueTypes",
12                 "support:DescribeServices",
13                 "support:DescribeSeverityLevels",
14                 "support:DescribeSupportLevel",
15                 "support:DescribeTrustedAdvisorCheckRefreshStatuses",
16                 "support:DescribeTrustedAdvisorCheckResult",
17                 "support:DescribeTrustedAdvisorChecks",
18                 "support:DescribeTrustedAdvisorCheckSummaries",
19                 "support:SearchForCases"
20             ],
21             "Resource": "*"
22         }
23     ]
24 }
  
```

The screenshot shows the 'Create policy' wizard with the JSON tab selected. The JSON code area contains the following partial policy definition:

```

{
    "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**.

Create policy

1 2

Review policy

Name*	api-healthdashboard-policy																
Use alphanumeric and '+=, @-_ ' characters. Maximum 128 characters.																	
Description																	
Maximum 1000 characters. Use alphanumeric and '+=, @-_ ' characters.																	
Summary <table border="1"> <thead> <tr> <th colspan="4">Filter</th> </tr> <tr> <th>Service</th> <th>Access level</th> <th>Resource</th> <th>Request condition</th> </tr> </thead> <tbody> <tr> <td>Allow (1 of 269 services) Show remaining 268</td> <td>Support</td> <td>Full: Read</td> <td>All resources</td> </tr> <tr> <td></td> <td></td> <td></td> <td>None</td> </tr> </tbody> </table>		Filter				Service	Access level	Resource	Request condition	Allow (1 of 269 services) Show remaining 268	Support	Full: Read	All resources				None
Filter																	
Service	Access level	Resource	Request condition														
Allow (1 of 269 services) Show remaining 268	Support	Full: Read	All resources														
			None														

Step 4. Log into AWS Console > IAM

Go to IAM > Users > Add user.

User name	Groups
user1	
user2	

Step 5. Set User Details

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

Add user

1 2 3 4 5

Set user details

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

User name*	api-user-for-collector
------------	------------------------

[+ Add another user](#)

Select AWS access type

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

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

Step 6. Set API Permission

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

Add user

1 2 3 4 5

Set permissions

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

[Create policy](#) [⟳](#)

Filter policies		Showing 1 result	
Policy name	Type	Used as	
<input checked="" type="checkbox"/> api-healthdashboard-policy	Customer managed	None	Edit

Step 7. Review

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

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	api-user-for-collector
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

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

Type	Name
Managed policy	AmazonDynamoDBReadOnlyAccess
Managed policy	AmazonEC2ReadOnlyAccess
Managed policy	AutoScalingReadOnlyAccess
Managed policy	AmazonRDSReadOnlyAccess
Managed policy	api-power-scheduler-policy

Tags

No tags were added.

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).

Add user

1 2 3 4 5

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

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

[Download .csv](#)

	User	Access key ID	Secret access key
	api-user-for-collector		***** Show

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",
        "sns:ListTopics"
      ]
    }
  ]
}
```

```
"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**.

The screenshot shows the Google Cloud Platform IAM & Admin Service Accounts creation interface. On the left, a sidebar lists various IAM management options like IAM, Identity & Organization, Policy Troubleshooter, etc., with 'Service Accounts' selected. The main area is titled 'Create service account'. Step 1, 'Service account details', is active, showing fields for 'Service account name' (set to 'api-service-account-for-collector'), 'Display name for this service account' (set to 'sample service account'), and 'Service account ID' (set to 'api-service-account-for-collec...@bluese-clodone-20200113.iam.gserviceaccount.com'). Step 2, 'Grant this service account access to project (optional)', and Step 3, 'Grant users access to this service account (optional)', are shown below. A 'CREATE' button is at the bottom of Step 1, and 'DONE' and 'CANCEL' buttons are at the bottom of the main form.

STEP 2. Set Service account details

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

The 'Create service account' dialog is shown with the following details filled in:

- Service account name:** api-service-account-for-collector
- Service account ID:** api-service-account-for-collec...@bluese-clodone-20200113.iam.gserviceaccount.com
- Service account description:** sample service account

Below the form, the steps for granting access are listed:

- Grant this service account access to project (optional)**
- Grant users access to this service account (optional)**

At the bottom are 'DONE' and 'CANCEL' buttons.

STEP 3: Grant Service account to Project

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

Create service account

Service account details

2 Grant this service account access to project (optional)

Grant this service account access to CloudOne DEV so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role	<input style="border: none; width: 100%; height: 100%;" type="button" value="Viewer"/>
------	--

Condition	<input style="border: none; width: 100%; height: 100%;" type="button" value="Add condition"/>
-----------	---



Read access to all resources.

[+ ADD ANOTHER ROLE](#)

[CONTINUE](#)

3 Grant users access to this service account (optional)

[DONE](#)

[CANCEL](#)

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.

Create service account

Service account details

Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role	<input style="border: none; width: 100%; height: 100%;" type="text" value="this_is_google_sample_user@gmail.com"/>	<input style="border: none; width: 100%; height: 100%;" type="button" value="?"/>
----------------------------	--	---

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role	<input style="border: none; width: 100%; height: 100%;" type="button" value="?"/>
-----------------------------	---

Grant users the permission to administer this service account

[DONE](#)

[CANCEL](#)

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.

The screenshot shows the Google Cloud Platform IAM & Admin Service Accounts page. A single service account, 'api-service-account-for-collector', is listed. The account has a green status icon, a name of 'api-service-account-for-collector', a description of 'sample service account', and a key ID of 'No keys'. The 'Actions' column for this account includes options for 'Edit', 'Disable', 'Create key', and 'Delete'.

Create private key for "api-service-account-for-collector"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

JSON

Recommended

P12

For backward compatibility with code using the P12 format

CANCEL CREATE

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.

Private key saved to your computer

bluese-cloudone-20200113-d118f2cfe059.json allows access to your cloud resources, so store it securely. [Learn more](#)

CLOSE

The screenshot shows the Google Cloud Platform IAM & Admin Service Accounts page. The same service account, 'api-service-account-for-collector', is now listed with a green status icon, a name of 'api-service-account-for-collector', a description of 'sample service account', and a key ID of 'No keys'. The 'Actions' column for this account includes options for 'Edit', 'Disable', 'Create key', and 'Delete'.

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
getlamPolicy

Bucket

list

get

getIamPolicy

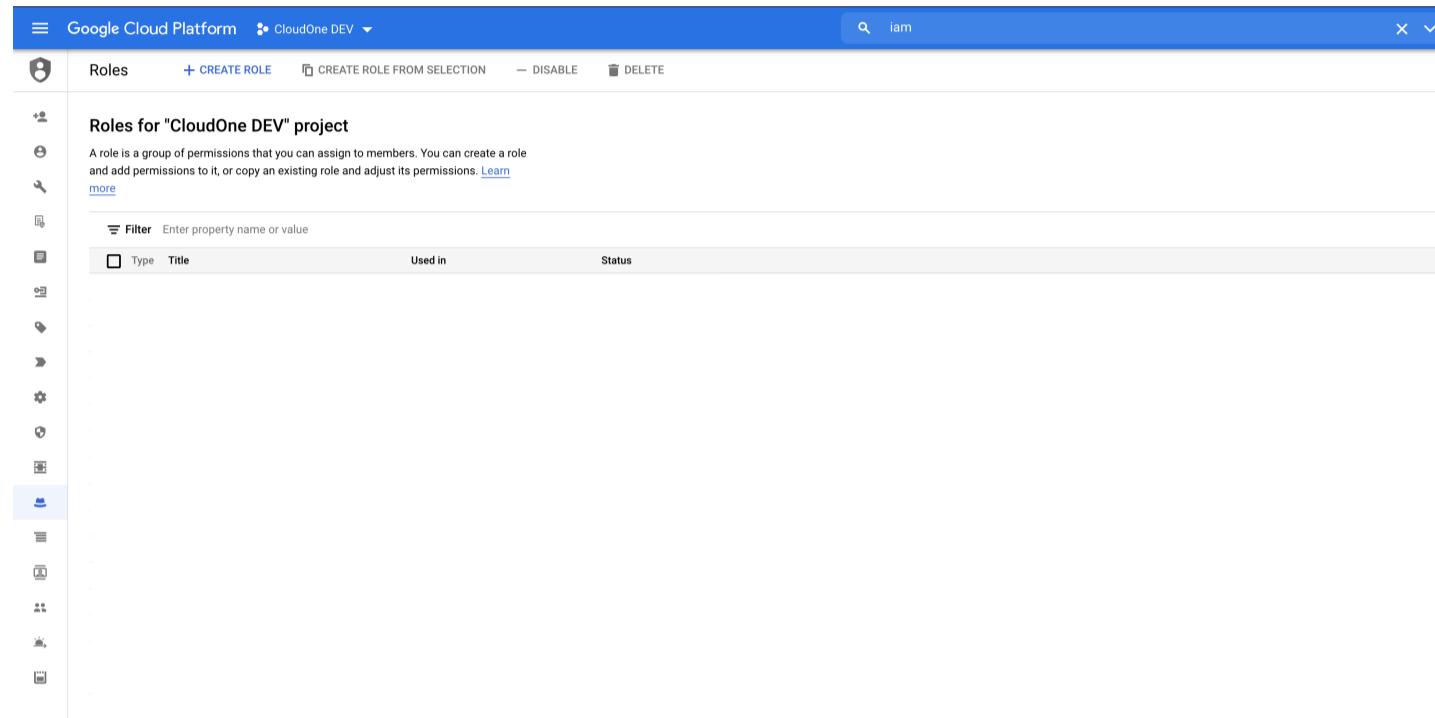
Big Query

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.

The screenshot shows the 'Create Role' page in the Google Cloud Platform IAM & Admin section. A modal window titled 'Add permissions' is displayed, listing various storage bucket permissions. The 'storage.bucket' filter is applied, and the list includes actions like 'storage.buckets.get', 'storage.buckets.list', and 'storage.objects.get'. The 'Status' column indicates all are 'Supported'.

STEP 3: Review Permissions

Review the permissions once you've created a role.

The screenshot shows the 'plugin-collector-role-special-svc' role details page. It displays the role's name, ID (projects/bluese-cloudone-20200113/roles/CustomRole), and launch stage (Alpha). The 'Description' section notes it was created on 2021-04-07. The '6 assigned permissions' section lists the same set of storage bucket permissions as the creation screen.

STEP 4: Set Created Role into the Service Account

Move to menu **IAM > IAM**.

The screenshot shows the 'Permissions' tab for the 'CloudOne DEV' project. It lists the service account 'api-service-account-for-collector' with the 'Viewer' role assigned. The table shows the member, role, analyzed permissions, and inheritance status.

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

The screenshot shows the Google Cloud Platform IAM Permissions page for the "CloudOne DEV" project. On the left, there's a sidebar with various icons. The main area has tabs for "PERMISSIONS" and "RECOMMENDATIONS HISTORY". Under "PERMISSIONS", it says "Permissions for project 'CloudOne DEV'". It lists two service accounts with highly privileged roles: "Owner / Editor" and "Viewer". Below this, there's a section for "View By" (MEMBERS or ROLES) and a "Filter" bar. A table lists members with their names and roles. On the right, the "Edit permissions" panel is open. It shows a "Member" section with "api-service-account-for-collec@bluese-cloudone-20200113.iam.gserviceaccount.com" and a "Project" section for "CloudOne DEV". There are three roles listed: "Sample SpaceONE Power ...", "Viewer", and "plugin-collector-role-spec...". Each role has a "Condition" section with a "Add condition" link. At the bottom of the panel are "SAVE", "SIMULATE", and "CANCEL" buttons.

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.

This screenshot is similar to the one above, showing the "Edit permissions" panel for the "CloudOne DEV" project. The "Member" section now includes a new role: "BigQuery Resource Viewer". Its description is "View all BigQuery resources but cannot make changes or purchasing decisions." Another role, "BigQuery Data Viewer", is also listed with its description "Access to view datasets and all of their contents". The "Condition" sections for these roles also have "Add condition" links. The "SAVE", "SIMULATE", and "CANCEL" buttons are at the bottom.

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**.

The screenshot shows the Google Cloud Platform IAM & Admin interface. The left sidebar lists various administrative tools: IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Labels, Settings, Privacy & Security, Identity-Aware Proxy, Roles (which is selected and highlighted in blue), Audit Logs, Essential Contacts, Groups, Early Access Center, and Quotas. The main content area is titled "Roles for 'CloudOne DEV' project". It includes a brief description of what a role is, a "Learn more" link, and a "Filter" button. A table displays columns for Type, Title, Used in, and Status, but no data is present.

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

The screenshot shows the Google Cloud Platform (GCP) IAM & Admin interface. On the left sidebar, under the 'Roles' section, the 'Create Role' button is highlighted. The main content area displays the 'Create Role' form. The 'Title' field is set to 'Sample SpaceONE Power Scheduler'. The 'Description' field notes the creation date as 'Created on: 2021-02-10'. The 'ID' field is set to 'PowerScheduler'. The 'Role launch stage' is set to 'General Availability'. Below the form is a 'No assigned permissions' section, which includes a 'Filter' table and a note about third-party service permissions. A modal window titled 'Add permissions' is open, listing various Compute Engine permissions with checkboxes. The 'compute.instances.start' and 'compute.instances.stop' checkboxes are checked. The bottom right of the modal has 'CANCEL' and 'ADD' buttons.

Custom roles let you group permissions and assign them to members of your organization. You can manually select permissions or import permission sets. [Learn more](#)

Title *
Sample SpaceONE Power Scheduler

Description
Created on: 2021-02-10

ID *
PowerScheduler

Role launch stage
General Availability

+ ADD PERMISSIONS

No assigned permissions

Filter table

Permission ↑ Status

compute.instances.setScheduling Supported

compute.instances.setServiceAccount Supported

compute.instances.setShieldedInstanceIntegrityPolicy Supported

compute.instances.setShieldedVmIntegrityPolicy Supported

compute.instances.setTags Supported

compute.instances.start Supported

compute.instances.startWithEncryptionKey Supported

compute.instances.stop Supported

compute.instances.suspend Supported

compute.instances.update Supported

111 – 120 of 260 < >

Some permissions might be associated with and checked by third-party services. These permissions contain the third party's service and do not have a permission prefix.

CREATE CANCEL

Add permissions

Filter permissions by role
Compute Instance Admin (v1)

Filter table

Permission ↑ Status

compute.instances.setScheduling Supported

compute.instances.setServiceAccount Supported

compute.instances.setShieldedInstanceIntegrityPolicy Supported

compute.instances.setShieldedVmIntegrityPolicy Supported

compute.instances.setTags Supported

compute.instances.start Supported

compute.instances.startWithEncryptionKey Supported

compute.instances.stop Supported

compute.instances.suspend Supported

compute.instances.update Supported

CANCEL ADD

STEP 3: Review Permission

Review the permissions in the role you've created.

Sample SpaceONE Power Scheduler + EDIT ROLE CREATE FROM ROLE

ID: projects/bluese-cloudone-20200113/roles/PowerScheduler
Role launch stage: General Availability

Description
Created on: 2021-02-10

11 assigned permissions

```
cloudsql.databases.update
cloudsql.instances.restart
cloudsql.instances.startReplica
cloudsql.instances.stopReplica
cloudsql.instances.update
compute.accounts.update
compute.accountsManagers.update
compute.instanceGroupManagers.update
compute.instanceGroups.update
compute.instances.reset
compute.instances.start
compute.instances.stop
```

Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.

STEP 4: Set Created Role into the Service Account

Drive to menu IAM > IAM.

IAM & Admin IAM + ADD - REMOVE

PERMISSIONS RECOMMENDATIONS HISTORY

Permissions for project "CloudOne DEV"

These permissions affect this project and all of its resources. [Learn more](#)

View By: MEMBERS ROLES

Name: api-service-account-for-collector

Type	Member ↑	Name	Role	Analyzed permissions (excess/total)	Inheritance
✉	api-service-account-for-collec@bluese-cloudone-20200113.iam.gserviceaccount.com	api-service-account-for-collector	Viewer	0/0	DEV

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.

CloudOne DEV Search products and resources

IAM + ADD - REMOVE

PERMISSIONS RECOMMENDATIONS HISTORY

Permissions for project "CloudOne DEV"

These permissions affect this project and all of its resources. [Learn more](#)

View By: MEMBERS ROLES

Name: api-service-account-for-collector

Role: Viewer Condition: Add condition

Member: api-service-account-for-collec@bluese-cloudone-20200113.iam.gserviceaccount.com Project: CloudOne DEV

Role: sample Condition: Add condition

Sample SpaceONE Power Scheduler
Created on: 2021-02-10

MANAGE ROLES

CloudOne DEV Search products and resources

IAM + ADD - REMOVE

PERMISSIONS RECOMMENDATIONS HISTORY

Permissions for project "CloudOne DEV"

These permissions affect this project and all of its resources. [Learn more](#)

View By: MEMBERS ROLES

Name: api-service-account-for-collector

Role: Sample SpaceONE Power ... Condition: Add condition

Member: api-service-account-for-collec@bluese-cloudone-20200113.iam.gserviceaccount.com Project: CloudOne DEV

Role: Condition: Add condition

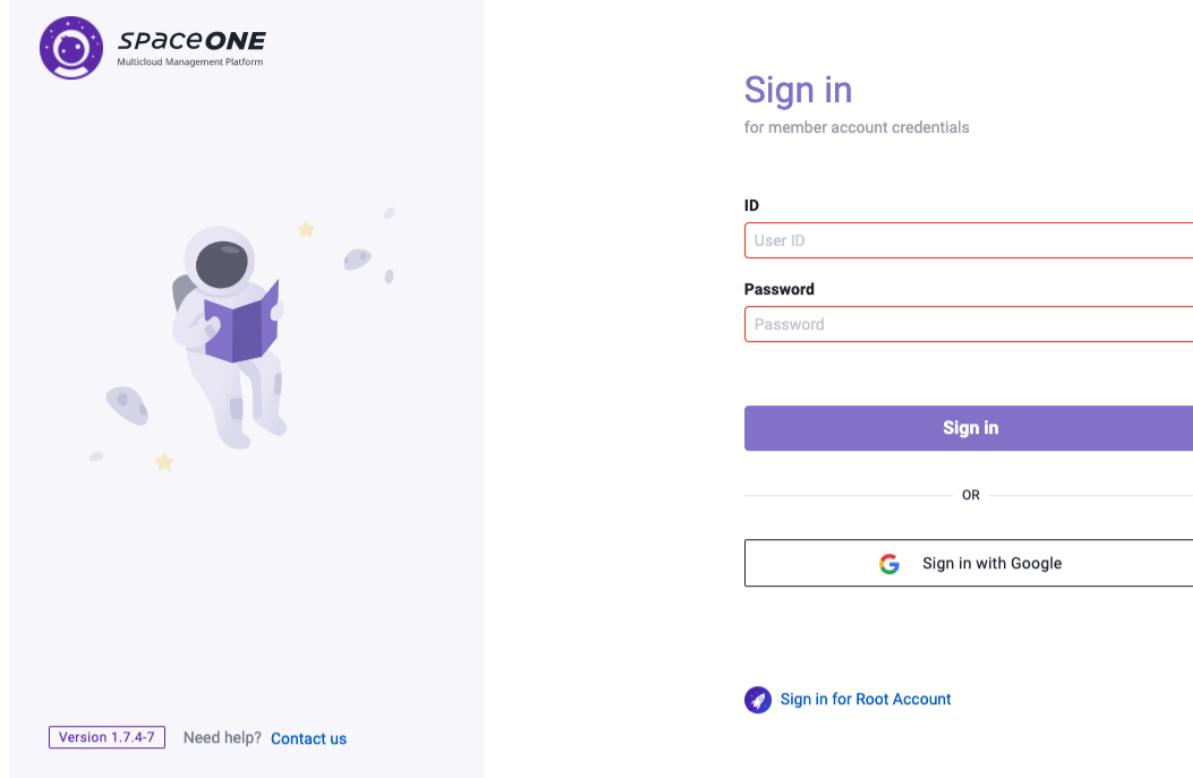
Created on: 2021-02-10

+ ADD ANOTHER ROLE

SAVE CANCEL

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.

The screenshot shows the 'Add Service Account' page. On the left, there are sections for 'Base Information' (name: Google Cloud test-service Account on SpaceOne, project ID: api-service-account-for-collector) and 'Credentials' (name: Google Cloud test-service Account on SpaceOne). On the right, a code editor displays a JSON configuration:

```

1  {
2    "type": "service_account",
3    "project_id": "api-service-account-for-collector",
4    "private_key_id": "",
5    "private_key": "-----",
6    "client_email": "",
7    "client_id": "1d"
8
9
10 }
11

```

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.

The screenshot shows a modal dialog titled 'Project (optional)' with a '+ Create Project' button. It displays a list of projects under the heading 'The [asdfasdf] is/ are in [googles].'. The 'googles' project is selected. Other projects listed include MAKEmake, Premium Support, Project Group Test, SpaceONE, SpaceONE_project1, Test Group, jhpjhp, jiyoon-pg, jongmon-pg, and localhost. At the bottom, there is an 'No project selected' option. Below the dialog are 'Cancel' and 'Save' buttons.

Step 6: Confirm your Registration

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

The screenshot shows the 'Google Accounts' list page. The table has columns: Name, Project ID, Project, and Created. One account is listed: Google Cloud test-Service Account on SpaceOne (Project ID: api-service-account-for-collector, Project: Google cloud Test > google test, Created: 2021-04-16 07:14:10).

Name	Project ID	Project	Created
Google Cloud test-Service Account on SpaceOne	api-service-account-for-collector	Google cloud Test > google test	2021-04-16 07:14:10

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.

The screenshot shows the Microsoft Azure Resource groups page. At the top, there are navigation links for 'Home' and 'Resource groups'. Below the header, there are several action buttons: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Feedback'. A search bar says 'Search resources, services, and docs (G+/-)'. There are also filter options for 'Subscription == all', 'Location == all', and 'Add filter'. The main area displays a table with 5 records, showing columns for 'Name', 'Subscription', and 'Location'. The table includes a header row and a footer row indicating 'Showing 1 to 5 of 5 records.' and 'No grouping'.

Name	Subscription	Location
[Icon]	Azure subscription 1	Southeast Asia
[Icon]	Azure subscription 1	East US
[Icon] Resource group name	Azure subscription 1	East US
[Icon]	Azure subscription 1	East US
[Icon]	Azure subscription 1	Korea Central

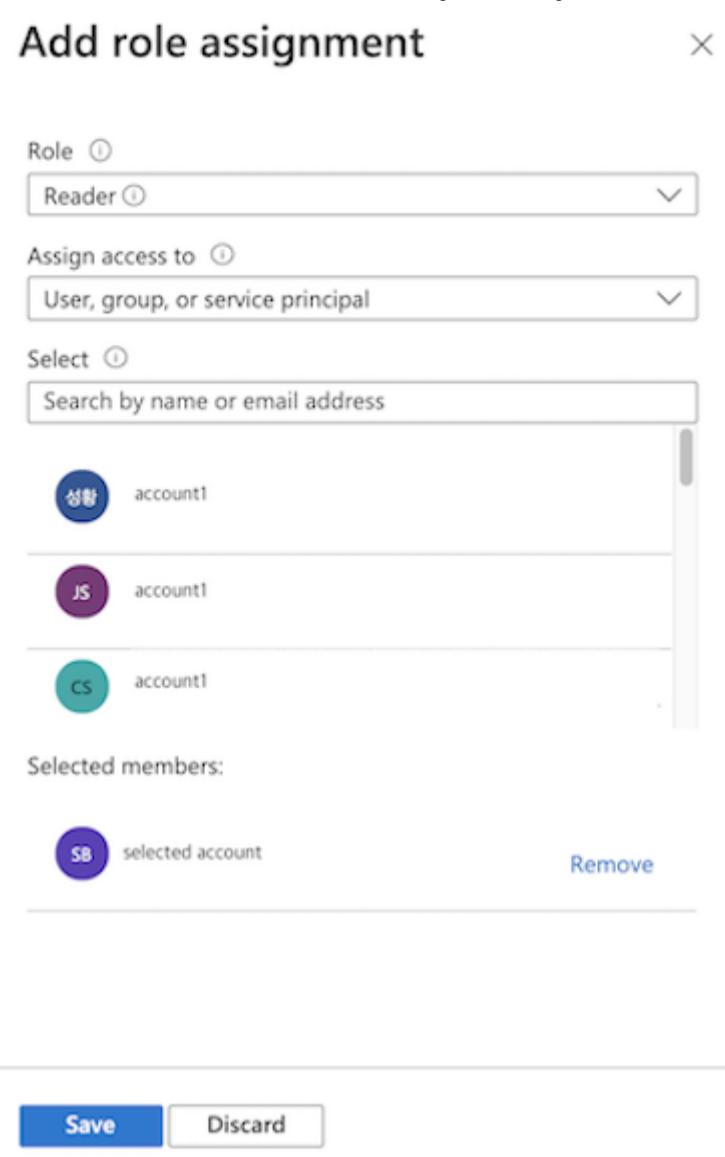
STEP 2. Add Access Control (IAM)

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

The screenshot shows the Microsoft Azure Access control (IAM) page for a specific resource group. The left sidebar lists various management tabs: Overview, Activity log, Access control (IAM), Tags, Events, Settings (Deployments, Security, Policies, Properties, Locks), and Cost Management (Cost analysis, Cost alerts (preview)). The 'Access control (IAM)' tab is selected. The main content area has a title '| Access control (IAM) ...'. It includes a search bar, a toolbar with '+ Add', 'Download role assignments', 'Edit columns', 'Refresh', 'Remove', and 'Got feedback?', and a 'Check access' menu with 'Role assignments', 'Roles', 'Deny assignments', and 'Classic administrators'. Below this, there are two main sections: 'My access' (View my level of access to this resource) and 'Grant access to this resource' (Grant access to resources by assigning a role). Both sections include a 'View' button and a 'Learn more' link.

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

The screenshot shows the Microsoft Azure home page. At the top, there's a search bar and a navigation bar with icons for Home, Notifications, and Help. Below the search bar, there's a section titled 'Azure services' with icons for 'Create a resource', 'Subscriptions', 'Virtual machine scale sets', 'Virtual machines', 'Resource groups', 'API Management...', 'API Connections', 'Monitor', 'Automation Accounts', and 'More services'. A purple box highlights the 'Subscriptions' icon. Below this, there's a 'Recent resources' table with one item: 'Azure subscription 1' (Subscription type, last viewed 13 minutes ago). At the bottom, there are sections for 'Navigate' (Subscriptions, Resource groups, All resources, Dashboard) and 'Tools'.

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

The screenshot shows the 'Subscriptions' page in Microsoft Azure. It lists one subscription: 'Azure subscription 1'. The table columns include 'Subscription name', 'Subscription ID', 'My role', 'Current cost', and 'Status'. The 'Subscription name' column has a purple box around it. There are filters at the top for 'Subscription name', 'Subscription ID', 'My role', 'Current cost', and 'Status'. Buttons for 'Apply' and 'Search' are also present.

STEP 3: Click the +Add role assignment button.

The screenshot shows the 'Azure subscription 1 | Access control (IAM)' page. On the left, there's a sidebar with links like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Security', 'Events', 'Cost Management', 'Billing', and 'Settings'. The 'Access control (IAM)' link is highlighted with a purple box. The main area has a table with columns for 'Add role assignment (disabled)', 'Add co-administrator (disabled)', 'Add custom role (disabled)', and 'View my access'. There are buttons for 'Download role assignments', 'Edit columns', 'Refresh', 'Remove', and 'Got feedback'. A large purple box highlights the '+Add' button in the top-left corner of the main content area.

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**

Azure subscription 1 | Access control (IAM)

Add role assignment (disabled)

Add co administrator (disabled)

Add custom role (disabled)

View my level of access to this resource.

Grant access to this resource

Grant access to resources by assigning

Check access

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

Find: User, group, or service principal

View my access

View access to this resource

View

View deny assignments

Note

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

Add role assignment

Role: Reader

Assign access to: User, group, or service principal

Select: cludone

CloudONE

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

Learn more about RBAC

Save Discard

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

	Name	Status	Email	Federated	Created	Last Sign In
<input type="checkbox"/>	spaceone-tester	Active	-	No	Wed, Mar 24, 2021, 09:13:10 UTC	-
<input type="checkbox"/>	oracleidentity.cloudservice/bluese@mz.co.kr	Active	-	Yes	Wed, Jan 20, 2021, 01:08:44 UTC	-
<input type="checkbox"/>	oracleidentity.cloudservice/ahnhj@mz.co.kr	Active	-	Yes	Wed, Jan 20, 2021, 01:07:10 UTC	-
<input type="checkbox"/>	oracleidentity.cloudservice/inhu@mz.co.kr	Active	-	Yes	Wed, Jan 20, 2021, 01:04:40 UTC	-
<input type="checkbox"/>	oracleidentity.cloudservice/orch@mz.co.kr	Active	-	Yes	Wed, Jan 20, 2021, 01:03:55 UTC	-

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.

The screenshot shows the 'Identity > Groups > Group Details' page. On the left, there's a large green circular icon with a white 'G' and the word 'ACTIVE' below it. The main area has a title 'SpaceOne' and a sub-section 'Group Information' with an OCID and creation date. A central modal window is titled 'Add User to Group' with a dropdown menu for selecting a user. Below the modal, a table lists the 'Group Members' with one entry: 'spaceone-tester'.

STEP 6. Set Policies to Group

Go to Identity > Policies and Click Create Policy Button.

The screenshot shows the Oracle Cloud Identity service. The sidebar on the left lists various services such as Monitoring, Logging, Developer Services, Blockchain Platform, Marketplace, VMware Solution, Monitoring and Diagnostics, Application Performance Monitoring, Logging Analytics, Operations Insights, Database Management, Management Agent, More Oracle Cloud Services, Platform Services, Classic Data Management Services, Governance and Administration, Cloud Advisor, Account Management, Identity, Security, Governance, and Administration. The 'Identity' service is currently selected. A sub-menu for 'Identity' is displayed on the right, listing 'Manage Regions or Service Links', 'Users', 'Groups', 'Dynamic Groups', 'Network Sources', 'Policies', 'Compartments', 'Federation', and 'Authentication Settings'. The 'Policies' option is highlighted with a blue background.

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
```

Create Policy

Name
spaceone-tester-policies
No spaces. Only letters, numerals, hyphens, periods, or underscores.

Description
This is for SpaceOne team, OCI plugin user

Compartment
mzoclo1 (root)

Policy Builder Show manual editor

```
Allow group SpaceOne to inspect compartments in tenancy
Allow group SpaceOne to inspect tenancies in tenancy
Allow group SpaceOne to inspect autonomous-database-family in tenancy
```

Example: Allow group [group_name] to [verb] [resource-type] in compartment [compartment_name] where [condition]

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.

← Create User

User Account Information

* Logon Name ②

api-user-for-collector

* Display Name ②

.onaliyun.com

api-user-for-collector

+ Add User

Access Mode ②

Console Access Users access the Alibaba Cloud console using the account and password.

Programmatic Access Enable AccessKeyId and AccessKeySecret to support access through the API or other development tools.

OK **Return**

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* tab.

The screenshot shows the Alibaba Cloud RAM User details page. The left sidebar has 'RAM' selected under 'Identity'. The main area shows a user named 'api-user-for-collector@onaliyun.com'. Under the 'Authentication' tab, there is a prominent blue button labeled 'Create AccessKey'. Below it, a table lists an existing access key: 'AccessKey ID' (redacted), 'Status' (Enabled), 'Last Used' (Mar 22, 2021, 16:17:37), and 'Created' (Mar 22, 2021, 16:16:07). There are 'Disable' and 'Delete' buttons next to the table.

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.

The screenshot shows the 'Create AccessKey' modal. At the top, it says 'Create AccessKey' and has a close button. A yellow warning box contains the text: 'This is the only time that the AccessKey can be viewed or downloaded. You cannot recover it later. However, you can create new AccessKeys at any time.' Below this, a green checkmark icon and the text 'The AccessKey has been created. Keep the AccessKey safe.' are displayed. The modal includes fields for 'AccessKey ID' and 'AccessKey Secret', both of which are redacted. At the bottom, there are buttons for 'Download CSV File' (with a CSV icon), 'Copy' (with a copy icon), and a large blue 'Close' button.

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.

The screenshot shows the SpaceONE web interface for managing servers. At the top, there is a navigation bar with links for Project, Inventory (selected), Identity, Monitoring, Automation, Plugin, and Management. Below the navigation bar is a search bar and a table header with columns: Name, Instance Type, Core, Memory, Provider, Instance State, Availability Zone, OS, and Primary IP. The table lists several servers, including some from Google and AWS providers. One specific server, "stargate-prod-eks-cluster-stargate-prod-Node", is selected and highlighted with a blue border. In the bottom half of the interface, there is a "Details" tab selected, showing detailed information for the selected server. This includes fields like ID, Name, Resource ID, Server Type, Primary IP Address, Management State, Provider, Cloud Service Group, Cloud Service Type, Region, Project, and Service Accounts. Each field has a corresponding value and a small icon.

Name	Instance Type	Core	Memory	Provider	Instance State	Availability Zone	OS	Primary IP
instance-group-google-00-m5bj	e2-medium	2	4	Google	Running	asia-northeast3-a	rhel	10.178.0.58
instance-group-google-00-6wsq	e2-medium	2	4	Google	Running	asia-northeast3-a	rhel	10.178.0.36
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2c	amazonlinux	10.0.200.68
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2c	amazonlinux	10.0.200.142
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2a	amazonlinux	10.0.198.61
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2a	amazonlinux	10.0.198.169
	t3.medium	2	4	AWS	Running	ap-northeast-1a	amazonlinux	10.0.0.203
stargate-prod-eks-cluster_kubectl	t3.medium	2	4	AWS	Running	ap-northeast-2a	ubuntu	10.0.201.37
stargate-prod-grafana	t3a.large	2	8	AWS	Running	ap-northeast-2a	linux	10.0.198.86

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.

Search

Properties (39)					
Server ID	Category	Provider	Instance State	Availability Zone	OS
Name		AWS	● Running	ap-northeast-2a	ubuntu
Resource ID		AWS	● Running	ap-northeast-2a	ubuntu
IP Address					
Instance ID					
Instance State					
Instance Type					
Key Pair					
Image					
Availability Zone					
Account					
OS Type					
OS Distro					
OS Architecture					
MAC Address		Disk	NIC	Security Groups	ELB
Public IP Address					Raw Data

Supported keywords contains all parameters defined for server.

Project Search

Project (3)

- Project: Plugin Team > Plugin
- Project: CloudOne Team > SpaceONE-DEV
- Project: CloudOne Team > SpaceONE-PRD

Server list

Server information collected based on multi clouds.

<input checked="" type="checkbox"/>	Name	Instance Type	Core	Memory	Provider	Instance State	Availability Zone	OS	Primary IP	Public IP
<input checked="" type="checkbox"/>	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.

Inventory > Server

Server (1 / 2)

The screenshot shows a table of servers with two entries. The first entry is selected, indicated by a checked checkbox. The second entry has an unchecked checkbox. The columns are Name, Core, Memory, and Provider. The first entry has values proxy-server, t3.micro, 2, 1, and AWS. The second entry has values proxy-server, t3.micro, 2, 1, and AWS. Above the table, there is a 'Filter:' input field with a 'Clear all' button. To the right of the table, there is a search bar and a 'Search' button. A dropdown menu labeled 'Action' is open, showing three options: 'Delete', 'Change Project', and 'Connect to Console'. The 'Delete' option is highlighted with a blue background.

Name	Core	Memory	Provider
proxy-server	2	1	AWS
proxy-server	2	1	AWS

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..)

ID	server-4ee3f9549474
Name	proxy-server
Resource ID	i-07e1dd0f1474117f
Server Type	VM
Primary IP Address	172.16.1.45
Management State	In-Service
Provider	AWS
Cloud Service Group	EC2
Cloud Service Type	Instance
Region	Asia Pacific (Seoul) ap-northeast-2
Project	CloudOne Team > SpaceONE-DEV
Service Accounts	cloudone-aws-dev
Secrets	secret-3292ab7ffbdd

Tag

Grouping servers by tagging.

Key	Value
Managed_by	terraform
Name	proxy-server
Instance	proxy-server

Member

List of server managers.

User ID	User Name	Role	Labels
		Project Admin	

History

History of resources collected.

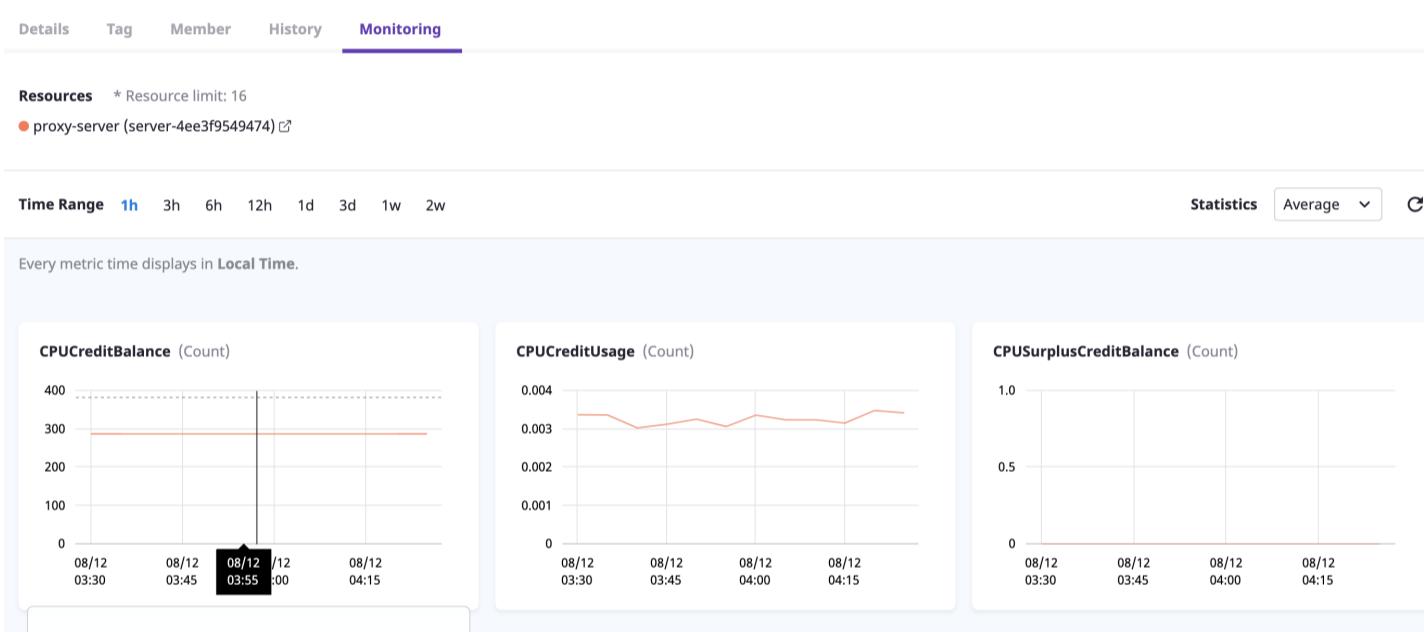
History (28)

Search: 1 / 2 15

Key	Job ID	Updated By	Updated
ip_addresses	job-7d204106e675	collector-c93ca263f8bc	2021-08-12 04:00:29
data.security_group	job-7d204106e675	collector-c93ca263f8bc	2021-08-12 04:00:29
data.compute	job-53e6a8dd435c	collector-c93ca263f8bc	2021-07-23 14:00:26
data.monitoring	job-d1bc9f4a56ba	collector-6fdfad37a3a3	2021-04-20 16:13:48
metadata.plugin-023782c156cf	job-dc23806ec531	collector-6fdfad37a3a3	2021-04-08 16:15:06
data.power_state	job-2577ca942946	collector-5e4f7ee1ff00	2021-04-08 05:00:58
project_id	job-d2a9b86e6e84	collector-8d8010bb4977	2021-04-08 04:57:49
state	job-d2a9b86e6e84	collector-8d8010bb4977	2021-04-08 04:57:49
data.cloudwatch	job-d2a9b86e6e84	collector-8d8010bb4977	2021-04-08 04:57:49
data.vpc	job-d2a9b86e6e84	collector-8d8010bb4977	2021-04-08 04:57:49

Monitoring

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



5.2 - CloudService

The screenshot shows the SpaceONE CloudService interface. At the top left is a box labeled "Overall cloud resources". The main area displays a grid of 12 service cards, each with an icon, service name, and count. The services listed are: SecretsManager (AWS Secret 1277), TrustedAdvisor (AWS Check 220), EC2 (AWS Volume 144), KMS (AWS Key 72), EC2 (AWS Instance 66), IAM (AWS User 37), ELB (AWS LoadBalancer 35), S3 (AWS Bucket 33), PersonalHealthDashboard (AWS Event 29), ECR (AWS Repository 21), Route53 (AWS HostedZone 18), SNS (AWS Topic 17), VPC (AWS VPC 7), Lambda (AWS Function 6), and EKS (AWS Cluster 5). On the left sidebar, there are sections for "Favorites (0)" (with a note to "Customize Favorites by clicking star"), "Service Providers" (listing All, Alibaba Cloud, AWS, Azure, Google, Hyper Billing, Oracle Cloud, and SpaceONE), and "Service Categories" (listing Compute, Container, Database, Networking, Storage, Security, Analytics, Application Integration, and Management).

Overview

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

The screenshot shows the SpaceONE CloudService interface. The main area displays a grid of 12 service cards, each with an icon, service name, and count. The services listed are: SecretsManager (AWS Secret 1277), TrustedAdvisor (AWS Check 220), EC2 (AWS Volume 144), KMS (AWS Key 72), EC2 (AWS Instance 66), IAM (AWS User 37), ELB (AWS LoadBalancer 35), S3 (AWS Bucket 33), PersonalHealthDashboard (AWS Event 29), ECR (AWS Repository 21), Route53 (AWS HostedZone 18), SNS (AWS Topic 17), VPC (AWS VPC 7), Lambda (AWS Function 6), and EKS (AWS Cluster 5). On the left sidebar, there are sections for "Favorites (0)" (with a note to "Customize Favorites by clicking star"), "Service Providers" (listing All, Alibaba Cloud, AWS, Azure, Google, Hyper Billing, Oracle Cloud, and SpaceONE), and "Service Categories" (listing Compute, Container, Database, Networking, Storage, Security, Analytics, Application Integration, and Management).

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.

The screenshot shows the SpaceONE CloudService interface. The main area displays a grid of 12 service cards, each with an icon, service name, and count. The services listed are: SecretsManager (AWS Secret 1277), TrustedAdvisor (AWS Check 220), EC2 (AWS Volume 144), KMS (AWS Key 72), EC2 (AWS Instance 66), IAM (AWS User 37), ELB (AWS LoadBalancer 35), S3 (AWS Bucket 33), PersonalHealthDashboard (AWS Event 29), ECR (AWS Repository 21), Route53 (AWS HostedZone 18), SNS (AWS Topic 17), VPC (AWS VPC 7), Lambda (AWS Function 6), and EKS (AWS Cluster 5). On the left sidebar, there are sections for "Favorites (3)" (listing Instance, Key, and Secret), "Service Providers" (listing All, Alibaba Cloud, AWS, Azure, Google, Hyper Billing, Oracle Cloud, and SpaceONE), and "Service Categories" (listing Compute, Container, Database, Networking, Storage, Security, Analytics, Application Integration, and Management).

Filters

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

Service Providers

The screenshot shows the SpaceONE interface for managing service providers. On the left, there's a sidebar with sections for 'Favorites (0)' and 'Service Providers'. Under 'Service Providers', a list includes All, Alibaba Cloud, AWS, Azure, Google, Hyper Billing, Oracle Cloud, and SpaceONE. Below this is a section for 'Service Categories' with checkboxes for Compute, Container, Database, Networking, Storage, Security, Analytics, Application Integration, and Management. The main content area is titled 'Google Cloud (2)' and shows two services: ComputeEngine (3 instances) and VPC (2 VPCNetworks). A navigation bar at the top includes Project, Inventory, Identity, Monitoring, Automation, Plugin, Management, and a 'new' button. The bottom of the screen has copyright information and support links.

Service Categories

This screenshot shows the SpaceONE interface for service categories. The sidebar includes sections for 'Service Categories' (with checkboxes for Compute, Container, Database, Networking, Storage, Security, Analytics, Application Integration, and Management), 'Regions' (listing various AWS regions like us-east-1, eu-central-1, ca-central-1, etc.), and 'AWS' (listing regions like us-east-1, eu-central-1, ca-central-1, etc.). The main content area is titled 'All (9)' and lists nine AWS services: EC2 (Volume 144), ECR (Repository 21), Lambda (Function 6), EKS (Cluster 5), DynamoDB (Table 4), ComputeEngine (Instance 3), DocumentDB (Cluster 1), and ElastiCache (Redis 1). The interface is similar to the previous one, with a navigation bar and footer links.

Regions

The screenshot shows the SpaceONE interface for regions. The sidebar includes sections for 'Regions' (listing AWS regions like us-east-1, eu-central-1, ca-central-1, etc.) and 'Azure' (listing regions like us-east-2, ap-southeast-1, etc.). The main content area is titled 'All (2)' and lists two services: KMS (Key 1) and EC2 (Volume 1). The interface follows the same layout with a navigation bar and footer links.

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.

The screenshot shows the SpaceONE Cloud Service Inventory interface. At the top, there is a navigation bar with links for Project, Inventory, Identity, Monitoring, Automation, Plugin, and Management. Below the navigation bar is a search bar with a placeholder 'Search' and a checkbox labeled 'Show Major Services'. A filter section shows 'Project: CloudOne Team > SpaceONE-DEV'. The main area displays a grid of 12 resource cards, each with an icon, service name, and count. The resources include SecretsManager (AWS Secret 311), IAM (AWS Policy 132), TrustedAdvisor (AWS Check 110), EC2 (AWS Volume 107), ELB (AWS TargetGroup 105), EC2 (AWS SecurityGroup 102), IAM (AWS Role 99), KMS (AWS Key 64), VPC (AWS Subnet 41), EC2 (AWS Instance 37), S3 (AWS Bucket 29), IAM (AWS User 26), ELB (AWS LoadBalancer 23), RDS (AWS OptionGroup 21), and RDS (AWS ParameterGroup 20).

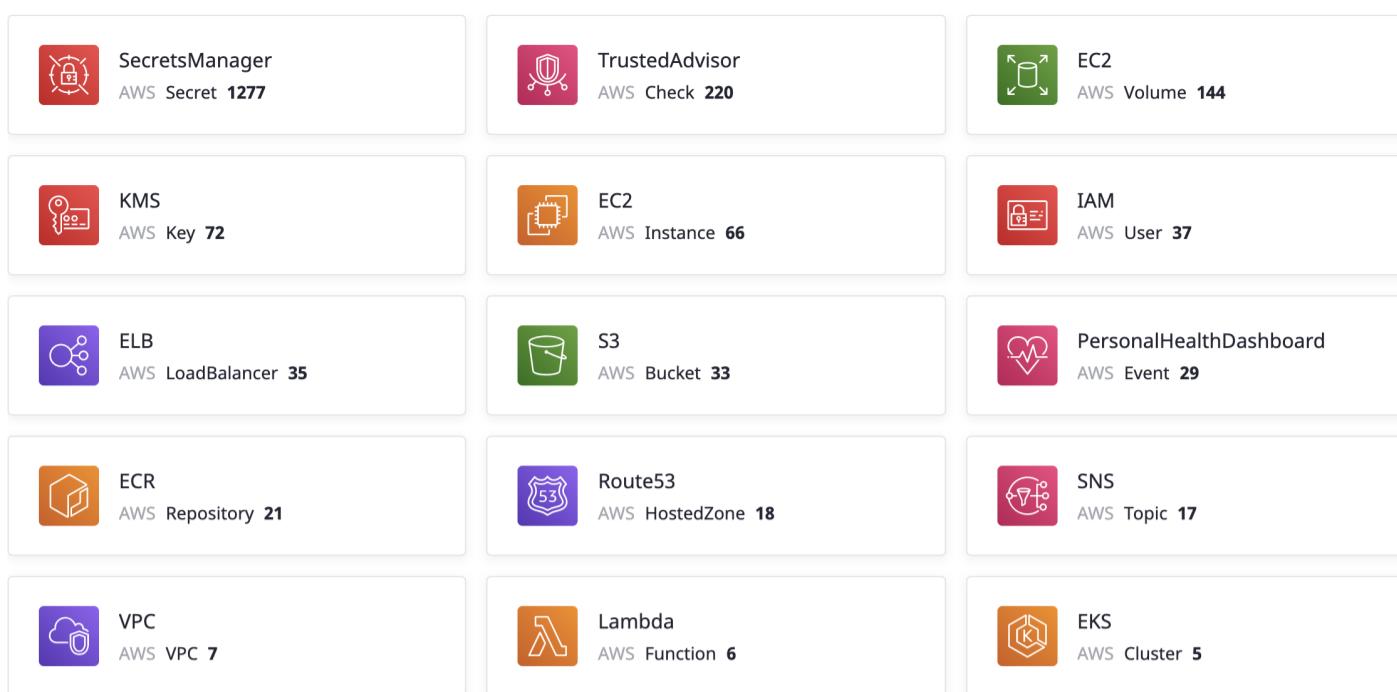
Show major services

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

This screenshot is similar to the previous one, but the 'Show Major Services' checkbox is checked, which filters the results to show only 19 major services. The grid now includes additional services like PersonalHealthDashboard, ECR, Lambda, and CloudFront, while others like VPC and RDS are no longer visible.

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.

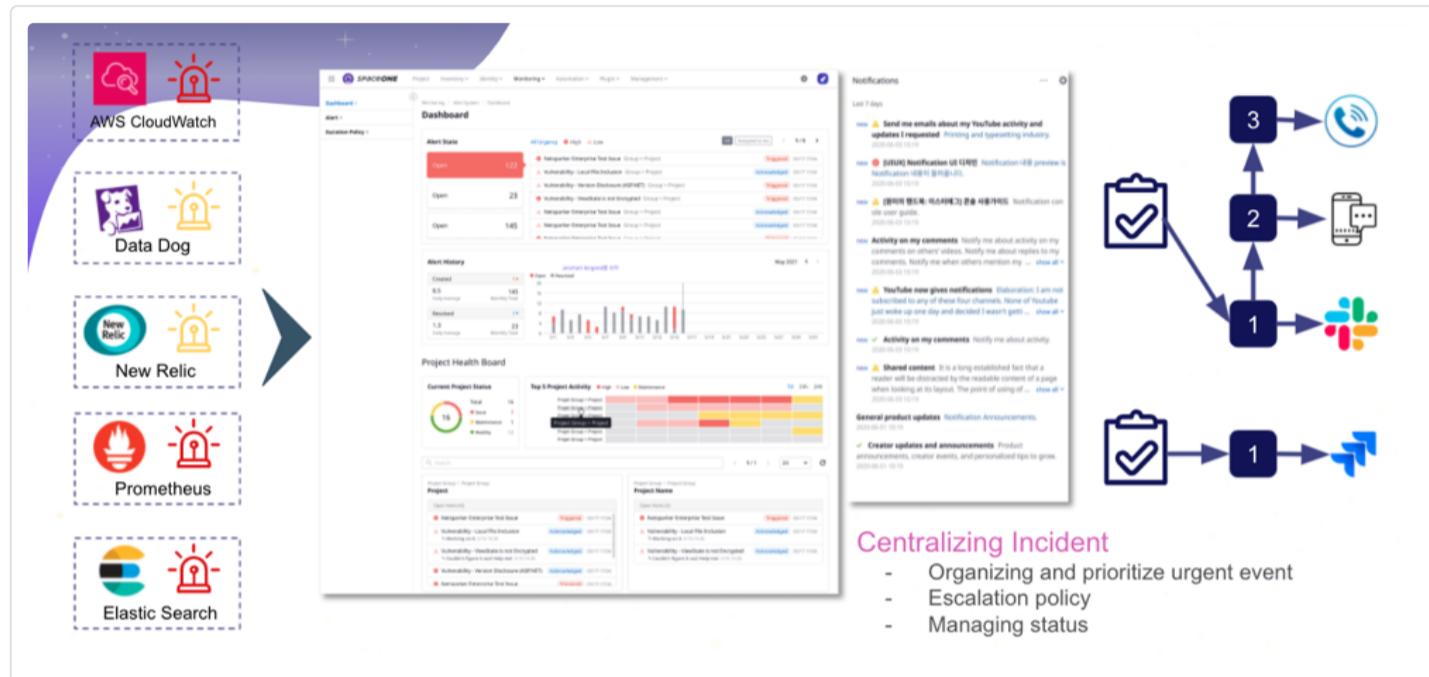
Name	Instance Type	Core	Memory	Provider	Instance State	Availability Zone
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2c
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2c
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2a
stargate-prod-eks-cluster-stargate-prod-Node	t3a.large	2	8	AWS	Running	ap-northeast-2a
	t3.medium	2	4	AWS	Running	ap-northeast-1a
stargate-prod-eks-cluster_kubectl	t3.medium	2	4	AWS	Running	ap-northeast-2a
stargate-prod-grafana	t3a.large	2	8	AWS	Running	ap-northeast-2a

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 Tool입니다.



Monitoring Webhook Plugin에 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 메시지입니다. 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 메시지입니다. 상세한 설명은 Notification 서비스 소개 를 참고해주세요.

6.1 - Alert Manager

Monitoring Service

6.1.1 - Dashboard

Monitoring Service

Overview

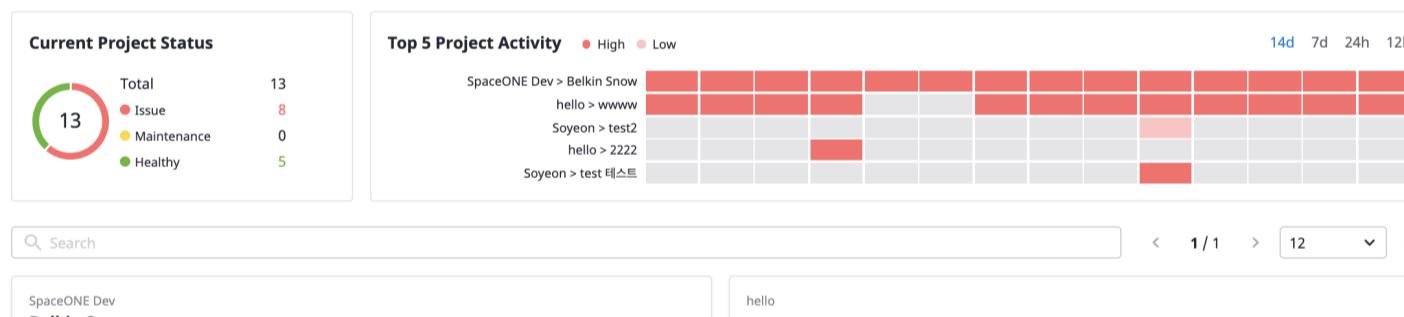
Alert Dashboard를 통해 수신된 모든 Alert의 현황을 한눈에 확인할 수 있습니다.

Monitoring > Alert Manager > Dashboard

Dashboard



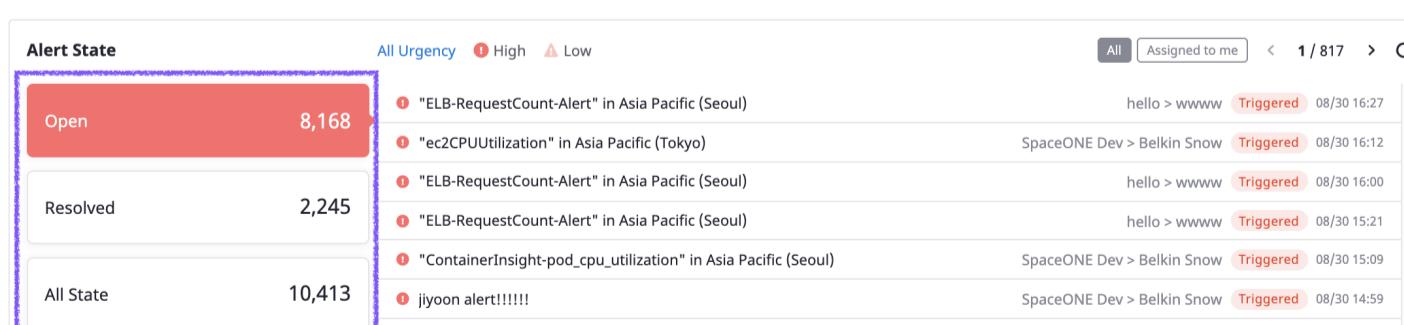
Project Health Board



Dashboard

Alert State

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

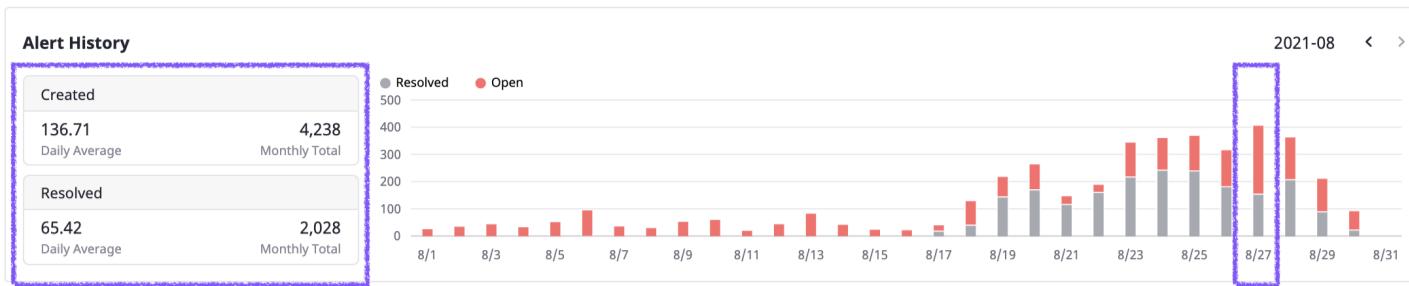


Urgency Type별로 Filter를 적용할 수 있습니다. 적용 가능한 Urgency Filter는 총 3가지(**All**, **High**, **Low**)입니다.

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.

Project Health Board

Current Project Status

Total	Issue	Maintenance	Healthy
13	8	0	5

Top 5 Project Activity

14d 7d 24h 12h

SpaceONE Dev > Belkin Snow
hello > wwwww
Soyeon > test2
hello > 2222
Soyeon > test 테스트

Search

SpaceONE Dev Belkin Snow

Open Alert (15+)

- "ec2CPUUtilization" in Asia Pacific (Tokyo) Triggered 08/30 16:12
- "ContainerInsight-pod_cpu_utilization" in Asia Pacific (Se... Triggered 08/30 15:09
- jiyoon alert!!!!!! Triggered 08/30 14:59
- "ec2CPUUtilization" in Asia Pacific (Tokyo) Triggered 08/30 14:56
- "ContainerInsight-pod_cpu_utilization" in Asia Pacific (Se... Triggered 08/30 14:47

hello wwwww

Open Alert (15+)

- "ELB-RequestCount-Alert" in Asia Pacific (Seoul) Triggered 08/30 16:27
- "ELB-RequestCount-Alert" in Asia Pacific (Seoul) Triggered 08/30 16:00
- "ELB-RequestCount-Alert" in Asia Pacific (Seoul) Triggered 08/30 15:21
- "ELB-RequestCount-Alert" in Asia Pacific (Seoul) Triggered 08/30 14:49
- "ELB-RequestCount-Alert" in Asia Pacific (Seoul) Triggered 08/30 14:35

2222

Open Alert (15+)

- ababdbbdbabdabd Acknowledged 08/20 15:04
- sample111 Triggered 08/04 17:33
- 마구마구 aaaa Triggered 07/21 20:55
- 알럿을 생성해요. 왜요? 몰라요. a Triggered 07/21 20:31
- 배포 합시다. a 가 들어가야 알림이 발생한다구요. Triggered 07/21 20:30

Plugin Dev Azure Test

Open Alert (1)

- 테스트 Triggered 07/15 17:41

Detailed description: This dashboard provides an overview of project health. It includes a summary of current issues per project, a heatmap of recent alert activity across projects, and detailed lists of open alerts for three specific projects: Belkin Snow, hello wwwww, and 2222. The Belkin Snow and hello wwwww sections show multiple triggered alerts, while the 2222 section shows acknowledged alerts. The Azure Test project has one open alert labeled '테스트'.

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.

Monitoring > Alert Manager > Alert

Alert

The screenshot shows the 'Alert' section of the SpaceONE interface. At the top, it displays 'Alert assigned to me (0)' with '0 Triggered' and '0 Acknowledged' counts. Below this is a table header with columns: No, Title, State, Urgency, Status Details, and Resource. The table lists 8,185 alerts, all of which are currently triggered and have a high urgency level. Each alert entry includes a checkbox, the alert ID, the title, its state (Triggered), urgency (High), status details (e.g., [AWS/ApplicationELB] LoadBalancer=app/k8s-devconsole-494df8b054/91fc0ee), and resource information (e.g., ClusterName=cloudone-dev-v1-eks-cluster). Buttons for 'Acknowledge', 'Resolve', and 'Delete' are located at the top right of the alert list.

Alert List

Alert 리스트를 다양한 필터를 사용하여 조회할 수 있습니다.

Assigned to me

기본적으로 프로젝트에 수신된 모든 Alert List를 조회할 수 있습니다.

담당자가 나로 직접 지정된 경우, 해당 Alert만 조회 할 수 있습니다.

Alert assigned to me (0)

0 Triggered 0 Acknowledged

Using Filters

Alert에 다양한 필터를 적용하여, 효율적인 조회가 가능 합니다.

설정 가능한 Filter는 **State Urgency** 두 종류입니다.

The screenshot shows the 'Alert' section of the SpaceONE interface. At the top, it displays 'Alert (8,185)' with buttons for 'Acknowledge', 'Resolve', and 'Delete'. Below this is a table header with columns: No, Title, State, Urgency, Status Details, and Resource. The table lists 8,185 alerts. A blue box highlights the 'State' and 'Urgency' filter dropdowns at the bottom of the table. The 'State' dropdown is set to 'Open' and the 'Urgency' dropdown is set to 'All'. Other filter options like 'Acknowledged', 'Triggered', 'Resolved', 'Error', and 'All' are also visible.

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 UrgencyUrgency는 **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.

Monitoring > Alert Manager > alert-3b8b8d32969a #214756

← "ELB-RequestCount-Alert" in Asia Pacific (Seoul) ⌂ ⌂

State	Triggered	Urgency	High	Assigned to	yuda@mz.co.kr	Duration	0d 0h 40m
Description	Threshold Crossed: 1 out of the last 1 datapoints [221.0 (30/08/21 08:38:00)] was greater than the threshold (200.0) (minimum 1 datapoint for OK -> ALARM transition).						
Rule	--						
Severity	Error						
Escalation Policy	AAA ⌂ ⌂						
Project	hello > www ⌂ ⌂						
Triggered By	AWS SNS Webhook ⌂						
Resource Name	[AWS/ApplicationELB] LoadBalancer=app/k8s-devconsole-494df8b054/91fc0ee2e5fd46d2 (Asia Pacific (Seoul)) ⌂						
Status Update	New Update						
Pushed Event		Details					
Pushed Event		<p>Search</p> <p>2021-08-30 17:49:07 [ERROR] "ELB-RequestCount-Alert" in Asia Pacific (Seoul) > Threshold Crossed: 1 out of the last 1 datapoints [201.0 (30/08/21 08:47:00)] was greater than the threshold (200.0) (minimum 1 datapoint for OK -> ALARM transition).</p> <p>2021-08-30 17:41:07 [INFO] "ELB-RequestCount-Alert" in Asia Pacific (Seoul) > Threshold Crossed: 1 out of the last 1 datapoints [124.0 (30/08/21 08:39:00)] was not greater than the threshold (200.0) (minimum 1 datapoint for OK -> OK transition)</p>					

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 기준입니다.

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.

The screenshot shows the 'Pushed Event' details page. At the top, there are tabs for 'Pushed Event' and 'Details'. Below the tabs is a search bar and a clear button. The main area displays two event entries:

- 2021-08-30 18:12:07** [INFO] "ELB-RequestCount-Alert" in Asia Pacific (Seoul) > Threshold Crossed: 1 out of the last 1 datapoints [108.0 (30/08/21 09:10:00)] was not greater than the threshold (200.0) (minimum 1 datapoint for ALARM -> OK transition).
- 2021-08-30 18:11:07** [ERROR] "ELB-RequestCount-Alert" in Asia Pacific (Seoul) > Threshold Crossed: 1 out of the last 1 datapoints [290.0 (30/08/21 09:09:00)] was greater than the threshold (200.0) (minimum 1 datapoint for OK -> ALARM transition).

Details

수신된 Event의 원문을 확인할 수 있습니다.

The screenshot shows the 'Details' tab selected on the SpaceONE Pushed Event page. Below it is a table titled 'Base Information' containing the following data:

Alert ID	alert-33230a91f8b4
Resource Name	[AWS/ApplicationELB] LoadBalancer=app/k8s-devconsole-494df8b054/91fc0ee2e5fd46d2 (Asia Pacific (Seoul))
Resource ID	app/k8s-devconsole-494df8b054/91fc0ee2e5fd46d2
Resource Type	AWS/ApplicationELB
Created	2021-08-30 18:11:07
Acknowledged	--
Resolved	--

Responder

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

The screenshot shows the SpaceONE Alert configuration interface. At the top, there is a header with the title "Responder" and a status indicator "Completed". Below the header, there is a section titled "[Step 1] LV1 Current" with a "hide ^" button. The main content area is divided into two sections: "Additional Responder (3)" and "Note". The "Additional Responder" section contains three entries: "kja0717@gmail.com (김정애) ×", "haely@mz.co.kr (김해리) ×", and "domain_admin@mz.co.kr (도메인 어드민) ×". Below this is a search bar with the placeholder "Search". The "Note" section contains a single note entry: "Test Note" with an "Add Note" button below it.

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 Policy 적용 되어 타 Project의 Member에도 알람이 전파 됩니다.

The screenshot shows the SpaceONE Alert configuration interface. The main content area is titled "Project Dependency". It contains two entries: "SpaceONE Dev > Belkin Snow" and "プロジェクトグループ > イグンジェ".

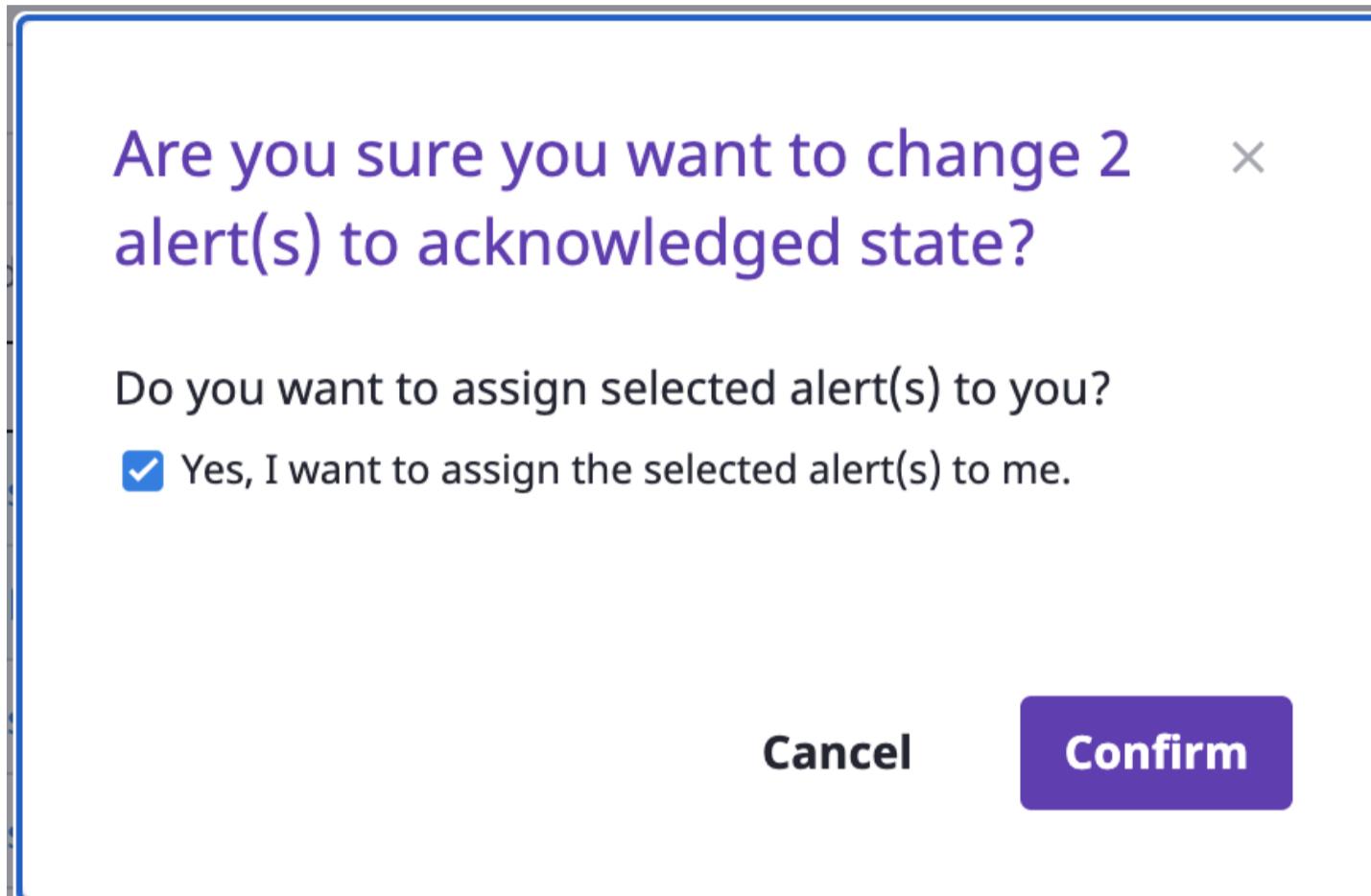
Alert Status Change

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

The screenshot shows a list of alerts with two items selected. The first alert is titled "ELB-RequestCount-Alert" and the second is "ContainerInsight-pod_cpu_utilization". Both are in the "Triggered" state and have "High" urgency. The "Acknowledge" button is highlighted with a blue border.

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 Alert를 발생 시킬 수 있습니다. 관리자가 자체 기준에 의해 Alert를 등록하여 처리할 수 있도록 합니다.

Create Alert

Alert Title

Test Alert 01

Urgency

High Low

Project

Go create project ↗
Select Project ▾

Description (optional)

Test Manual Alert 01

Cancel **Confirm**

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.

Monitoring > Alert Manager > Escalation Policy

Escalation Policy (22)

+ Create Action Search							1 / 1	24	C
Name	Escalation Rules	Repeat Time	Finish Condition	Scope	Project	Created			
test-sy-global	ALL	0	Resolved	Global		2021-08-26 13:51:41			
test-sy	LV1 (10min) > LV2	0	Acknowledged	Project	Soyeon > test 테스트	2021-08-26 13:23:41			
밸킨 스노우 정책	LV1 (3min) > LV2 (3min)	1	Acknowledged	Project	SpaceONE Dev > Belkin Snow	2021-08-26 12:51:36			
뽀잉	LV1	0	Acknowledged	Project	SpaceONE Dev > Belkin Snow	2021-08-26 12:46:11			
글로벌 팔리시	(Default)	LV1 (30min) > LV2 (30min) > LV3 (30min) > LV4	0	Acknowledged	Global	2021-08-17 15:54:48			

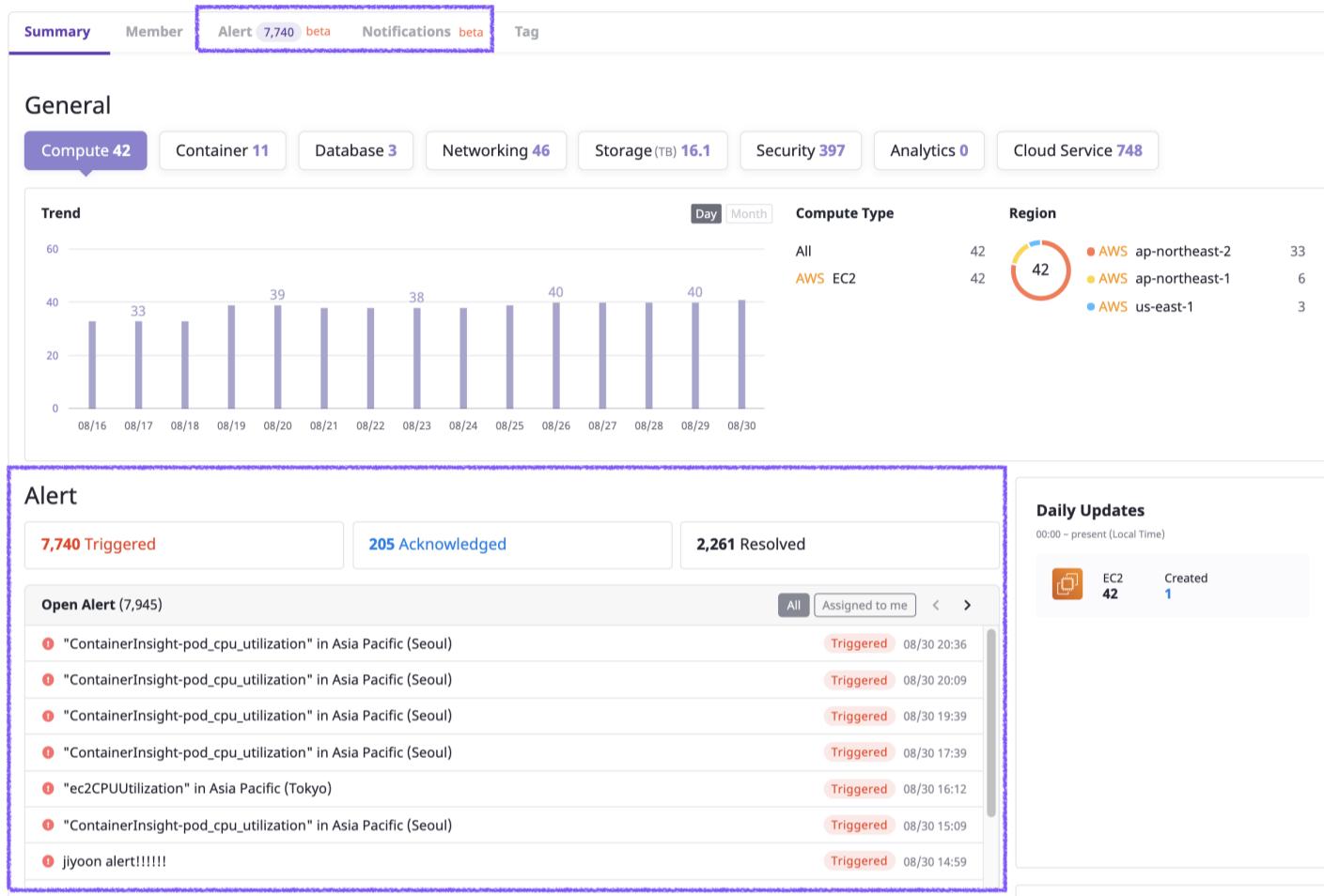
설정으로 상세 내용은 Admin Guide의 [Escalation Policy](#)를 참고 하세요.

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

7,740 Triggered | 205 Acknowledged | 2,261 Resolved

Open Alert (7,945)

- ContainerInsight-pod_cpu_utilization in Asia Pacific (Seoul) Triggered 08/30 20:36
- ContainerInsight-pod_cpu_utilization in Asia Pacific (Seoul) Triggered 08/30 20:09
- ContainerInsight-pod_cpu_utilization in Asia Pacific (Seoul) Triggered 08/30 19:39
- ContainerInsight-pod_cpu_utilization in Asia Pacific (Seoul) Triggered 08/30 17:39
- ec2CPUUtilization in Asia Pacific (Tokyo) Triggered 08/30 16:12
- ContainerInsight-pod_cpu_utilization in Asia Pacific (Seoul) Triggered 08/30 15:09
- jyoon alert!!!!!! Triggered 08/30 14:59

Daily Updates
00:00 ~ present (Local Time)

EC2 42 | Created 1

Alert List

Alert 리스트를 다양한 필터를 사용하여 조회할 수 있습니다.

Alert (7,944)

+ Create | Search | Acknowledge | Resolve | Delete

< 1 / 530 > 15 | C

State	Open	Acknowledged	Triggered	Resolved	Error	All	Urgency	All	High	Low	All	Assigned to me
<input type="checkbox"/>	No	Title	<input type="checkbox"/>	State	<input type="checkbox"/>	Urgency	<input type="checkbox"/>	Status Details	<input type="checkbox"/>	Resource		
<input type="checkbox"/>	215259	"ContainerInsight-pod_cpu_utilization" in Asia Pacific (Seoul)	<input type="checkbox"/> Triggered	<input type="checkbox"/> High	[ContainerInsights] ClusterName=cloudone-dev-v1-eks-							

Assigned to me

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

Using Filters

Alert에 다양한 필터를 적용하여, 효율적인 조회가 가능 합니다.

설정 가능한 Filter는 **State** **Urgency** 두 종류입니다.

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 통하여 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.

The screenshot shows the Project Dashboard for 'alert-manager-test-01'. At the top, there's a yellow banner indicating 'Maintenance Happening Now' with two entries: 'test maintenance window 02' (2021-08-30 16:39 ~ 2021-08-30 17:39) and 'test maintenance window 01' (2021-08-30 14:33 ~ 2021-08-30 15:03). Below this, the 'Maintenance Window' tab is selected in the navigation bar. The main area displays a table of maintenance windows with columns: Title, State, Start Time, End Time, Created By, and Created. The table shows two entries: 'test maintenance window 02' (Open, 2021-08-30 16:39:00, 2021-08-30 17:39:00, gikang@mz.co.kr, 2021-08-30 14:36:05) and 'test maintenance window 01' (Open, 2021-08-30 14:33:00, 2021-08-30 15:03:00, gikang@mz.co.kr, 2021-08-30 14:35:31).

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.

Create Maintenance Window

During a maintenance window, no new alerts will be created for this project.

Title

test maintenance window

Schedule

Start now and end in Start at scheduled time

15 minutes 30 minutes 1 hours 2 hours 3 hours

Maintenance Time Period 30 minutes

Cancel

Confirm

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.

Maintenance Window (2)						
		Update	Close	Search	1 / 1	15
□	Title	State	Start Time	End Time	Created By	Created
□	test maintenance window 02	Open	2021-08-30 16:39:00	2021-08-30 17:39:00	gikang@mz.co.kr	2021-08-30 14:36:05
□	test maintenance window 01	Open	2021-08-30 14:33:00	2021-08-30 15:03:00	gikang@mz.co.kr	2021-08-30 14:35:31

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.

Update Maintenance Window

×

During a maintenance window, no new alerts will be created for this project.

Title

test maintenance window 01

Schedule

Start at scheduled time

Timezone UTC

Start Time 2021. 08. 30. 오후 11:33



End Time 2021. 08. 31. 오전 12:03

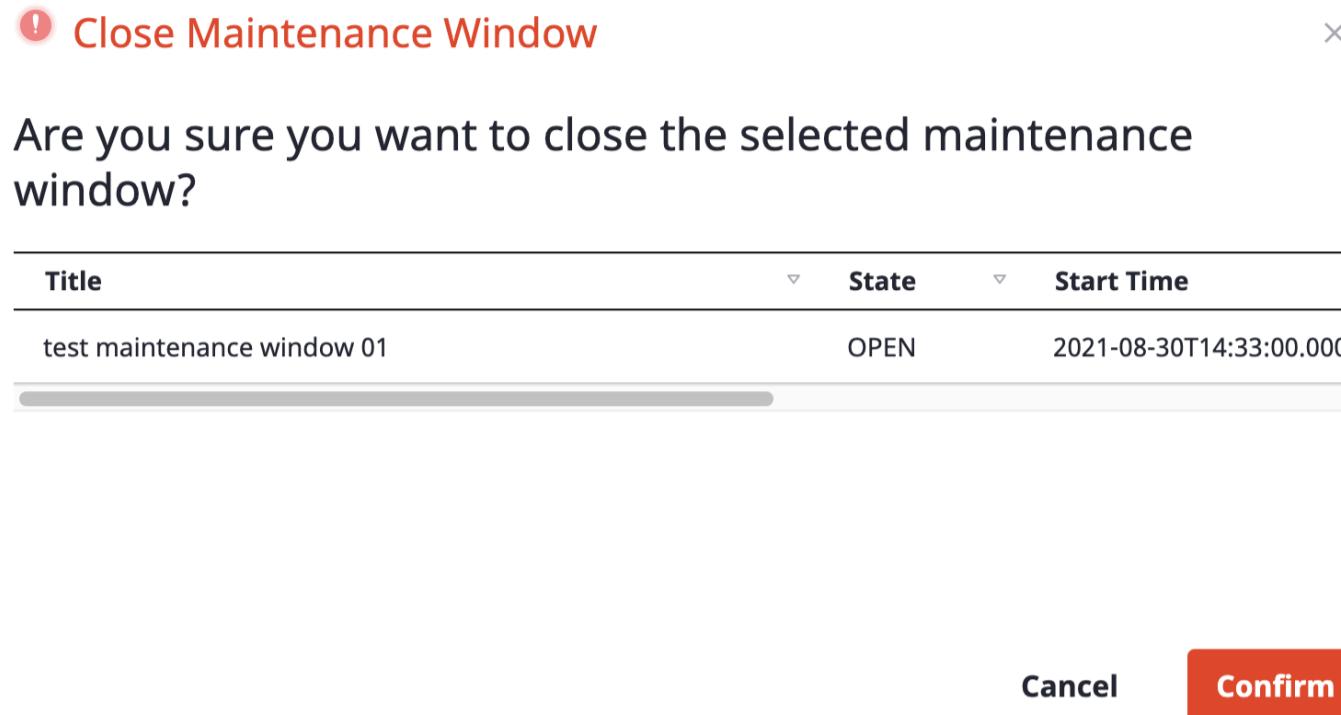
**Maintenance Time Period** 30 minutes**Close Now****Cancel****Confirm**

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.

Name	State	Type	Version	Webhook URL
Zabbix	Enabled	Zabbix Webhook	1.0-dev3	https://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-79ba4f08ebc6/68
Test webhook jyoon	Enabled	Grafana Webhook	1.0-dev17	https://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-93bccb13258a/37
Grafana	Enabled	Grafana Webhook	1.0	https://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-1eea0a98d2aa/ec
Amore Pacific Webhook	Enabled	Amore Pacific Webhook	1.0.2	https://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-d07c85e3ce60/01
AWS SNS Webhook	Enabled	AWS SNS Webhook	1.0-dev3	https://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-db1678262551/27

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

MarketPlace로부터 다양한 타입의 **Monitoring Webhook Plugin** 을 선택하여 설치합니다.

Add Webhook

Name

Test Webhook 01

Type

AWS SNS Webhook



Grafana Webhook



Zabbix Webhook

Version

Select

Cancel

Confirm

Update webhook plugin

Webhook의 이름과 사용되는 플러그인 버전을 변경할 수 있습니다.

Update Webhook

Name

Zabbix

Version

1.0-dev3 (latest)

Cancel

Confirm

Disable webhook plugin

Webhook으로부터 수신되는 Alert이 무시 되도록 설정합니다.

Update Webhook

X

Name

Zabbix

Version

1.0-dev3 (latest)

Cancel **Confirm**

Delete webhook plugin

Webhook을 삭제합니다.

⚠ Delete the selected webhook
permanently.

X

You can no longer receive events with this webhook,
and **this action cannot be undone**.

Type **Zabbix** to Confirm.

Cancel**Delete this webhook**

6.2.4 - Settings

Setting up detailed policy for managing alerts

Overview

각 Project에 수신되는 Alert을 관리하기 위한 상세 옵션을 관리 합니다.

The screenshot shows the 'Alert' tab selected in the top navigation bar. Below it, there are tabs for 'Maintenance Window', 'Webhook', and 'Settings'. The 'Settings' tab is active. The main area is titled 'Settings' and contains three sections: 'Notification Policy' (with a sub-section for 'All Notifications'), 'Auto Recovery' (set to 'Do It Manually'), and 'Event Rule' (showing '0 Rules on This Project'). Below these is the 'Escalation Policy' section, which includes a 'Name' field set to 'Notification Test Policy 01', a 'Finish Condition' of 'Acknowledged', and an 'Escalation Rules' section. The 'Escalation Rules' section shows two steps: 'STEP 1' (Notification Level 1, Escalates after 5 minutes, Slack Protocol Alert Manager Test Notification ON) and 'STEP 2' (Notification Level 2, Repeat all 0 times). There are 'Update' and 'Change' buttons at the top right of the escalation policy section.

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.

Set Notification Policy

X

What should responders be notified of



All Notifications



! High Urgency Notifications

Cancel

Confirm

Auto Recovery

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

Set Auto Recovery

X

When the system fault recovers, should we automatically resolve the alert?



Yes, Automatically resolve alerts



No, do it Manually

Cancel

Confirm

Event Rule

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

Project > SpaceONE Dev > Belkin Snow > Event Rule
[← Event Rule](#) ⓘ Event rules are executed in ascending order.

The screenshot shows the 'Event Rule' configuration page with two rules listed:

- Rule #1:**
 - All of the following are met:
 - Title contain ELB
 - Do these things:
 - No Notifications: On
 - Project Routing: hello > wwwwww ↗
 - Project Dependency: SpaceONE Dev > Belkin Snow ↗
プロジェクトグループ > イグンジェ ↗
 - Urgency: HIGH
 - Assignee: yuda@mz.co.kr
 - Additional Responder: kja0717@gmail.com, haely@mz.co.kr, domain_admin@mz.co.kr
 - Additional Information: ロゴ: オレンジ
- Rule #2:**
 - All of the following are met:
 - Title contain テスト
 - Do these things:
 - Project Routing: Plugin Dev > Azure Test ↗
 - Project Dependency: project-122a1b076bbf ↗
Plugin Dev > Azure Test ↗
 - Urgency: LOW
 - Additional Responder: project_admin@mz.co.kr, gikang-test-api-user@mz.co.kr
 - Additional Information: test: 2
 - Then stop processing

[+ Add Event Rule](#)

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.

← Event Rule ⓘ Event rules are executed in ascending order.

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.

Change Escalation Policy

X

✓ Choose an existing policy
Create New Policy

Name	Escalation Rules	Repeat Time	Finish Condition	Scope
<input checked="" type="radio"/> Notification Test Policy 01	LV1 (5min) > LV2	0	Acknowledged	Project
<input type="radio"/> Default	Default	ALL	Acknowledged	Global

Cancel
Confirm

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

Change Escalation Policy

X

Choose an existing policy
✓ Create New Policy

Name

Finish Condition

Acknowledged Resolved

Escalation Rules

Must be at least 1 minute for a single target. (Up to 5)

Step Notifications Level Rule

1	Level 1	Escalates after	30 min.	Delete	
2	Level 2				Delete
repeat (Apply all steps above)		+ Add Rule			

Cancel
Confirm

Escalation Policy 생성

새로운 Policy 생성에 대한 상세한 안내는 [Creating New Escalation Policy](#)를 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

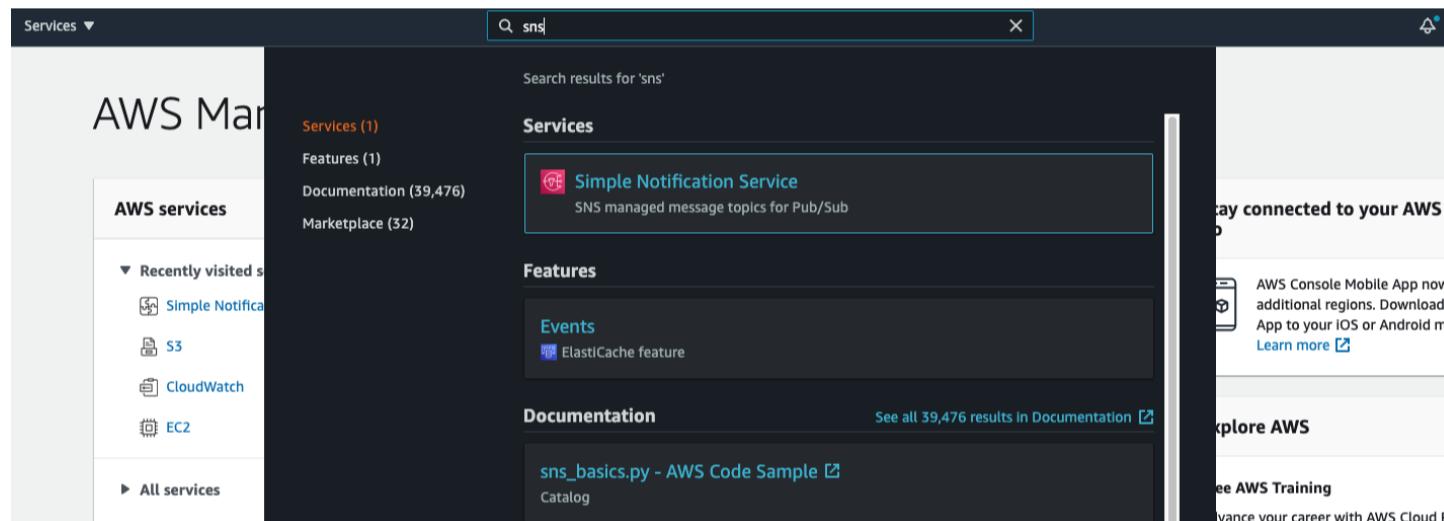
Please, Set SNS Topic and its Subscription for following Steps

[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

Create topic

Details

Type [Info](#)
Topic type cannot be modified after topic is created

FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name
Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - *optional* [Info](#)
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

AWS SNS Topic for Webhook
Maximum 100 characters, including hyphens (-) and underscores (_).

Encryption - optional
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

Access policy - optional
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. [Info](#)

Delivery retry policy (HTTP/S) - optional
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section. [Info](#)

Delivery status logging - optional
These settings configure the logging of message delivery status to CloudWatch Logs. [Info](#)

Tags - optional
A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. [Learn more](#)

[Cancel](#) [Create topic](#)

Step 4. Check Topic is created successfully.

AWS-SNS-Topic

Details

Name AWS-SNS-Topic	Display name AWS SNS Topic
ARN arn:aws:sns:ap-northeast-2:257706363616:AWS-SNS-Topic	Topic owner 257706363616
Type Standard	

[Edit](#) [Delete](#) [Publish message](#)

[Subscriptions](#) [Access policy](#) [Delivery retry policy \(HTTP/S\)](#) [Delivery status logging](#) [Encryption](#) [Tags](#)

Subscriptions (0)

ID	Endpoint	Status	Protocol
No subscriptions found You don't have any subscriptions to this topic. Create subscription			

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

AWS-SNS-Topic

Details

Name: AWS-SNS-Topic	Display name: AWS SNS Topic
ARN: arn:aws:sns:ap-northeast-2:257706363616:AWS-SNS-Topic	Topic owner: 257706363616
Type: Standard	

Subscriptions (0)

ID	Endpoint	Status	Protocol
No subscriptions found. You don't have any subscriptions to this topic.			

Actions: Edit | Delete | Request confirmation | Confirm subscription | **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](#)****

AWS-SNS-Topic

Details

Name: AWS-SNS-Topic	Display name: AWS SNS Topic
ARN: arn:aws:sns:ap-northeast-2:257706363616:AWS-SNS-Topic	Topic owner: 257706363616
Type: Standard	

Subscriptions (0)

ID	Endpoint	Status	Protocol
No subscriptions found. You don't have any subscriptions to this topic.			

Actions: Edit | Delete | Request confirmation | Confirm subscription | **Create subscription**

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

Create subscription

Details

Topic ARN
arn:aws:sns:ap-northeast-2:257706363616:AWS-SNS-Topic

Protocol
The type of endpoint to subscribe
HTTPS

Endpoint
A web server that can receive notifications from Amazon SNS.
ik.dev.spaceone.dev/monitoring/v1/webhook/webhook-cf2cf481cdc/6c7a4a68963c170f73399521d91b5427/events

Enable raw message delivery

After your subscription is created, you must confirm it. [Info](#)

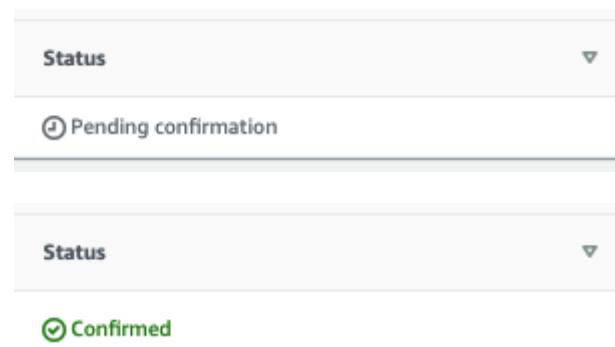
Subscription filter policy - optional
This policy filters the messages that a subscriber receives. [Info](#)

Redrive policy (dead-letter queue) - optional
Send undeliverable messages to a dead-letter queue. [Info](#)

Delivery retry policy (HTTP/S) - optional
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section. [Info](#)

Actions: Cancel | **Create subscription**

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

ID	Endpoint	Status	Protocol
22b516ce-dafe-44e2-a70a-2eb489969902	https://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-cf2cf481cd;6c7a4a68963c170f73399521d91b5427/events	Confirmed	HTTPS

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

The screenshot shows the Grafana Home page. On the left, there is a sidebar with icons for search, add, dashboard, alerting, notifications, and documentation. The main area has a "Welcome to Grafana" header and a "Basic" section with a "TUTORIAL DATA SOURCE AND DASHBOARDS" card about Grafana fundamentals. Below this are three "COMPLETE" cards: "Add your first data source" (with a database icon), "Create your first dashboard" (with a grid icon), and "Learn how in the docs". To the left of these cards is a "Dashboards" sidebar listing several dashboards like "SpaceOne DEV Cluster Alerts Dashboard" and "AWS ALB Application Load Balancer Copy". To the right is a "Latest from the blog" sidebar with two posts: "New in Grafana 8.0: Streaming real-time events and data to dashboards" (published Jun 28) and "How Siemens uses IoT sensor data and Grafana to optimize train maintenance, capacity, and more" (published Jun 25).

Step 2. Drive to Notification Channel on Browser

This screenshot is identical to the previous one, but the "Alerting" tab is highlighted in the sidebar. This indicates that the user has navigated to the Grafana Alerting configuration screen.

Step 3. Click New Channel button

The screenshot shows the 'Alerting' section of the SpaceONE interface. The 'Notification channels' tab is selected. At the top right, there is a blue button labeled 'New channel'. The main area is currently empty, showing columns for 'Name' and 'Type'.

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

The screenshot shows the 'New notification channel' creation form. The 'Name' field is filled with 'Grafana-SpaceONE Webhook'. The 'Type' dropdown is set to 'webhook'. The 'Url' field contains the value 'https://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-f9495a7bf8'. Below the form, there are 'Optional Webhook settings' and 'Notification settings' sections, each with a 'Save' button. At the bottom, there are 'Save', 'Test', and 'Back' buttons.

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.

The screenshot shows the SpaceONE Alerting interface. On the left is a dark sidebar with various icons. The main area has a header "Alerting" with a bell icon and "Alert rules and notifications". A sub-header "Notification channels" is visible. A modal window titled "New notification channel" is open. It contains fields for "Name" (Grafana-SpaceONE Webhook), "Type" (webhook), and "Url" (http://monitoring-webhook.dev.spaceone.dev/monitoring/v1/webhook/webhook-f9495a7bf8a). Below these are sections for "Optional Webhook settings" and "Notification settings", each with a right-pointing arrow. At the bottom are three buttons: "Save" (blue), "Test" (grey), and "Back" (grey). A green success message "Test notification sent" is displayed in the top right corner of the modal.

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

The screenshot shows the SpaceONE Alerting interface with the "Notification channels" tab selected. The sidebar is visible on the left. The main area displays a table with one row. The row contains "Name" (Grafana-SpaceONE Webhook), "Type" (webhook), and a red "X" button for deletion. A blue "New channel" button is located at the top right of the list area.

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 var params = JSON.parse(value);
6 payload = {};
7 payload.title = params.title;
8 payload.message = params.message;
9 payload.to = params.to;
10
11 payload.event = {};
12 payload.event.id = params.eventID;
13 payload.event.name = params.eventName;
14 payload.event.date = params.eventDate;
15 payload.event.time = params.eventTime;
16 payload.event.status = params.eventStatus;
17 payload.event.severity = params.eventSeverity;
18
19 payload.item = {};
20 payload.item.id = params.itemID;
21 payload.item.key = params.itemKey;
22 payload.item.value = params.itemValue;
23
24 payload.trigger = {};
25 payload.trigger.id = params.triggerID;
26 payload.trigger.name = params.triggerName;
27 payload.trigger.severity = params.triggerSeverity;
28 payload.trigger.status = params.triggerStatus;
29
30 payload.host = {};
31 payload.host.id = params.hostID;
32 payload.host.connection_info = params.hostConn;
33 payload.host.name = params.hostname;
34 payload.host.visible_name = params.hostVisibleName;
35
36
37

```

64424 symbols remaining

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.

Message type	Template	Actions
Problem	Problem started at {EVENT.TIME} on {EVENT.DATE} Pro...	Edit Remove
Problem recovery	Problem has been resolved at {EVENT.RECOVERY.TIME}...	Edit Remove
Problem update	{USER.FULLNAME} {EVENT.UPDATE.ACTION} problem ...	Edit Remove
Add		

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

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

Media

Type	SpaceONE Notification Webhook
* Send to	admin@spaceone.dev
* When active	1-7,00:00-24:00
Use if severity	<input checked="" type="checkbox"/> Not classified <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Average <input checked="" type="checkbox"/> High <input checked="" type="checkbox"/> Disaster
Enabled	<input checked="" type="checkbox"/>
Add Cancel	

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

Media

Type	Send to	When active	Use if severity	Status	Action
SpaceONE Notification Webhook	bluese05@gmail.com	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove
Add					

[Update](#) [Delete](#) [Cancel](#)

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.

Operation details

Operation Send message

Steps - (0 - infinitely)

Step duration (0 - use action default)

* At least one user or user group must be selected.

Send to user groups

User group	Action
Add	

Send to users

User	Action
Admin (Zabbix Administrator)	Remove
Add	

Send only to

Custom message

Conditions

Label	Name	Action
Add		

[Update](#)

[Cancel](#)

Add on Recovery operations and set as below.

Operation details

Operation

* At least one user or user group must be selected.

Send to user groups

User group	Action
Add	

Send to users

User	Action
Admin (Zabbix Administrator)	Remove
Add	

Send only to

Custom message

[Update](#)

[Cancel](#)

Finally, the settings of the Operations tab.

[Action](#) [Operations 2](#)

* Default operation step duration

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

Base Information

Channel Name

Notifications Level

▼

Country Code optional

Phone Number

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

Schedule

Setting Mode

All Time Custom

(i) You will only receive notifications in the schedule you choose.

Setting

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
--------	---------	-----------	----------	--------	----------	--------

9:00	▼	to	18:00	▼	Time Zone: UTC
------	---	----	-------	---	----------------

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

Base Information

Channel Name

Notifications Level

Phone Number

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

Schedule

Setting Mode

All Time Custom

(i) You will only receive notifications in the schedule you choose.

Setting

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

9:00

▼

to

18:00

▼

Time Zone: UTC

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

Base Information

Channel Name

Notifications Level

Email Address

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

Schedule

Setting Mode

All Time Custom

(i) You will only receive notifications in the schedule you choose.

Setting

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

9:00

▼

to 18:00

▼

Time Zone: UTC

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**.

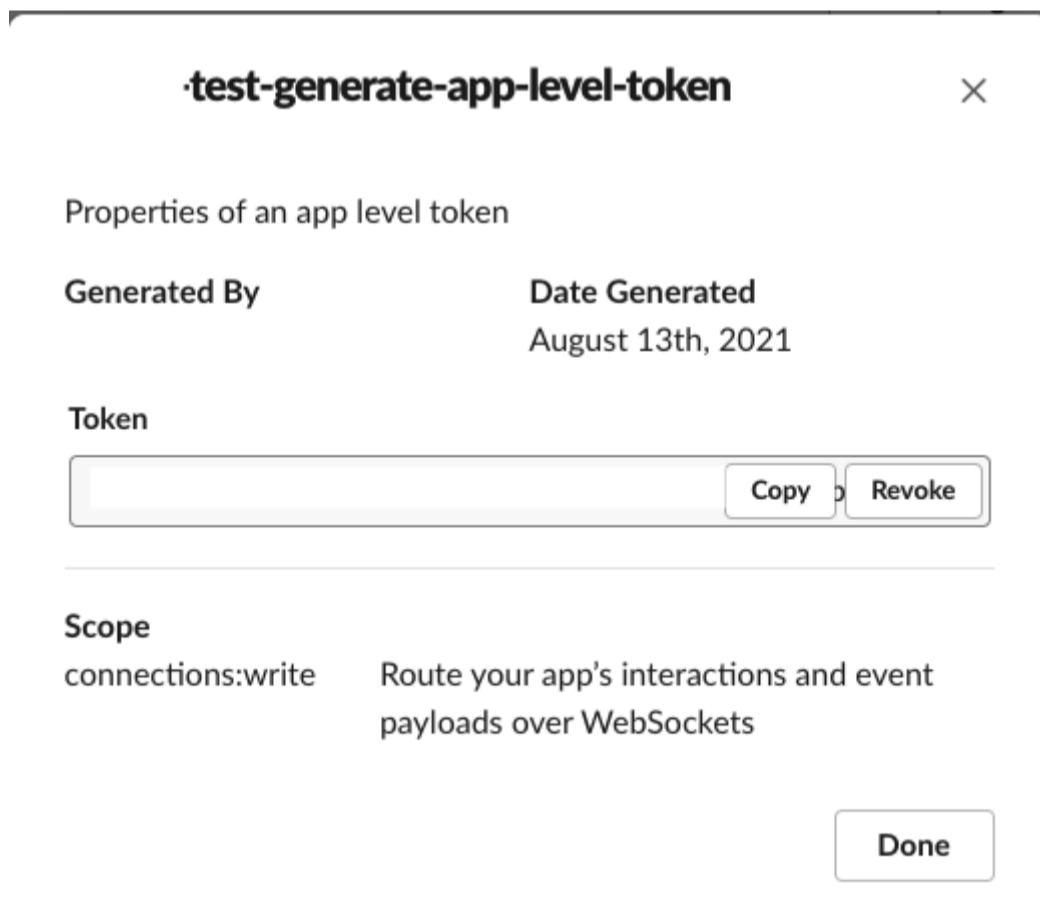
How to get Slack OAuth Token

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.

Generate an app-level token

Token Name

This will be how you refer to your token

i Required

Scopes to be accessed by this token

Scope	Description
You haven't added any scopes for your app-level token.	
Add permission by Scope or API method...	
connections:write Route your app's interactions and event payloads over WebSockets	
authorizations:read View information about your app's authorizations on installed teams	Create

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 .

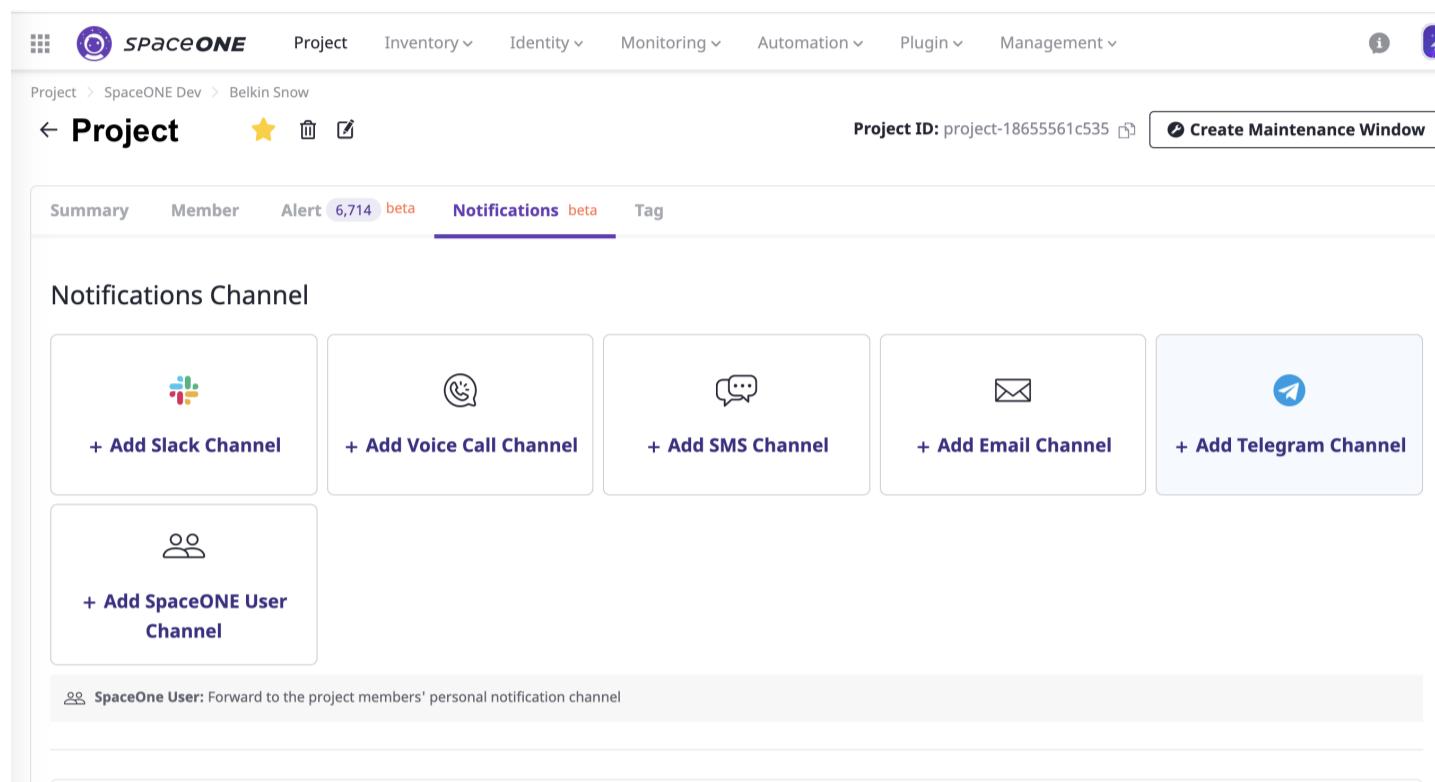
Find the apps we created right before, and add it.

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.

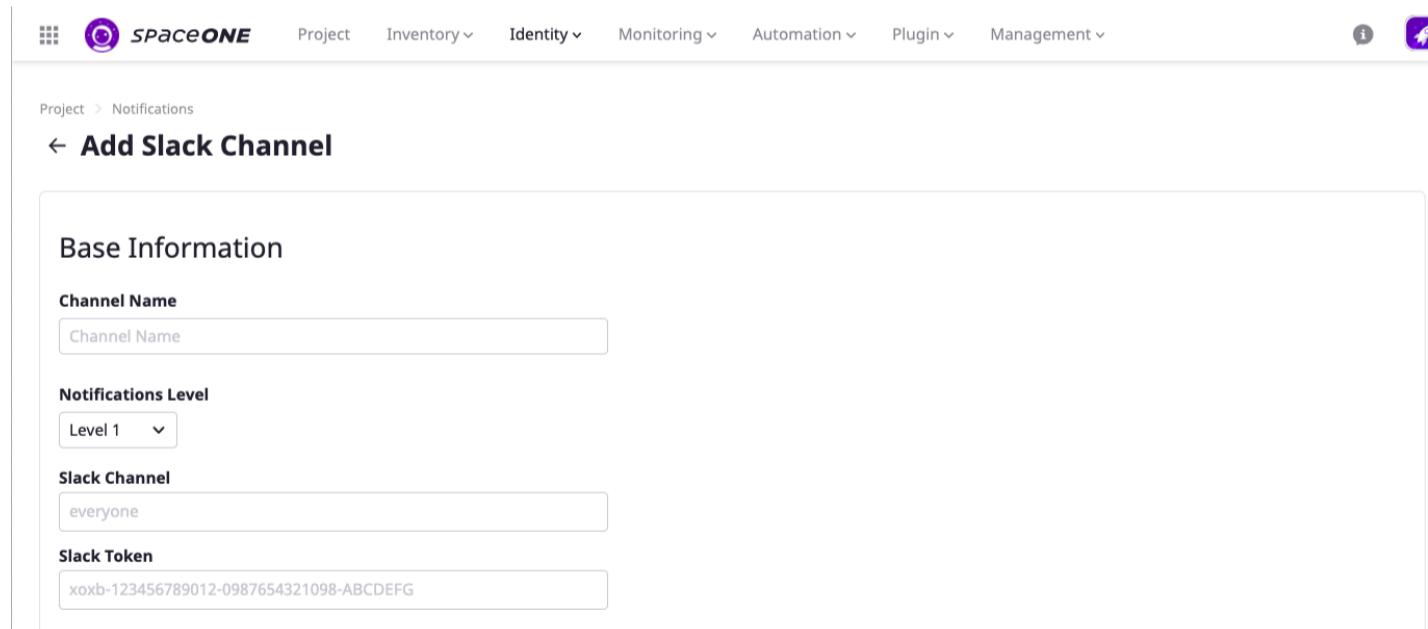
Basic Information



The screenshot shows the SpaceONE Project page with the Notifications tab selected. There are five buttons for adding different channels: Slack Channel, Voice Call Channel, SMS Channel, Email Channel, and Telegram Channel. Below these buttons is a button for adding a SpaceONE User channel. A note at the bottom states: "SpaceOne User: Forward to the project members' personal notification channel".

Set information above.

These items below are descriptions for plugins



The screenshot shows the 'Add Slack Channel' configuration page. It includes fields for Channel Name, Notifications Level (Level 1), Slack Channel (everyone), and Slack Token (xoxb-123456789012-0987654321098-ABCDEFG).

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

Schedule

Setting Mode

All Time Custom

(i) You will only receive notifications in the schedule you choose.

Setting

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

9:00

▼

to 18:00

▼

Time Zone: UTC

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

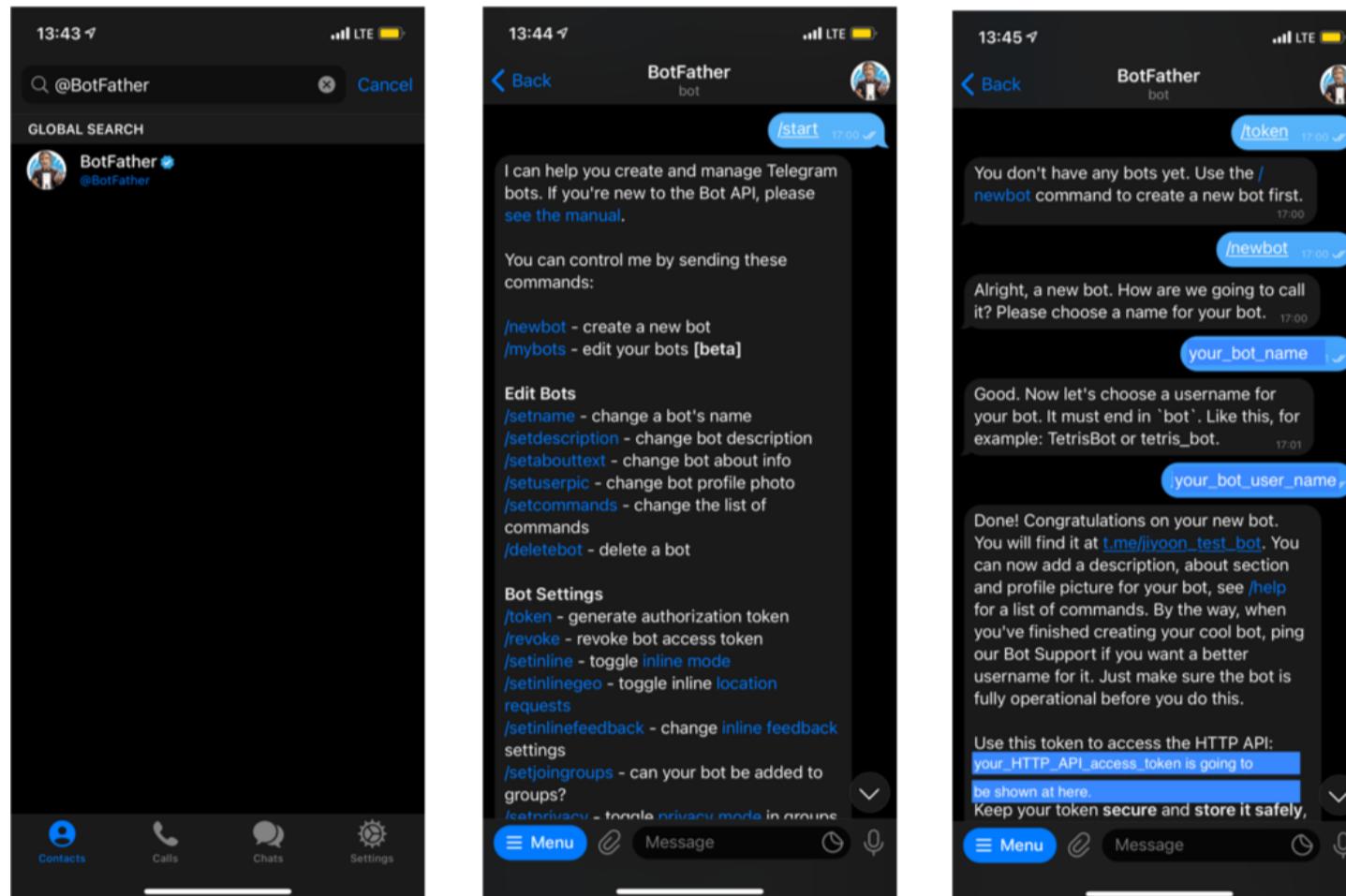
We can also add **Telegram** to our list of **Notification** channels. There are few prerequisites to use **Telegram Bot** on SpaceONE notification service, and the following will guide you to your **SpaceONE** notification journey.

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:

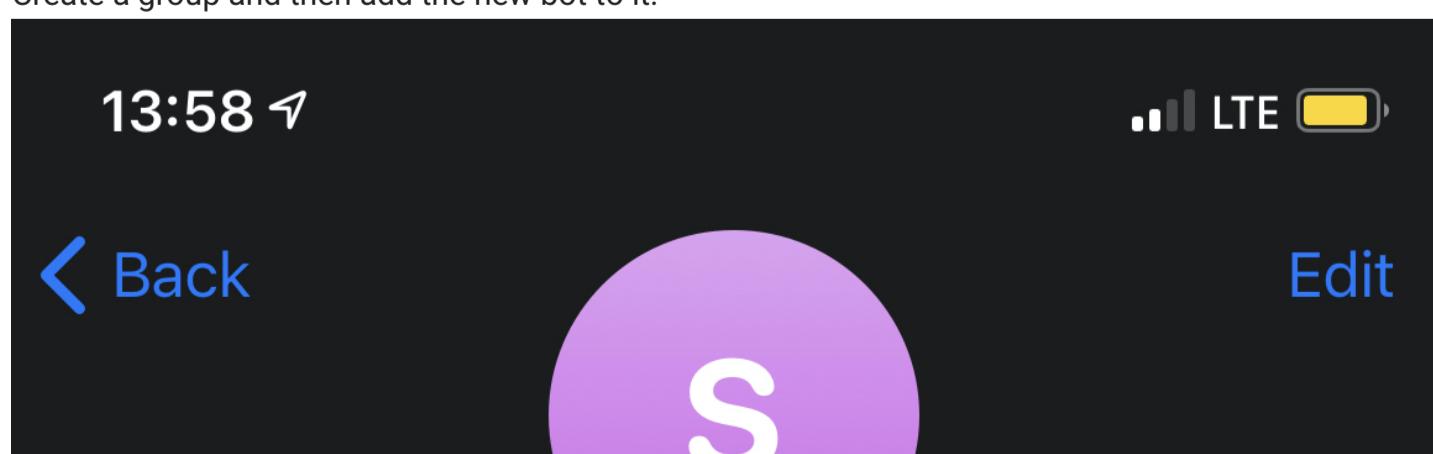


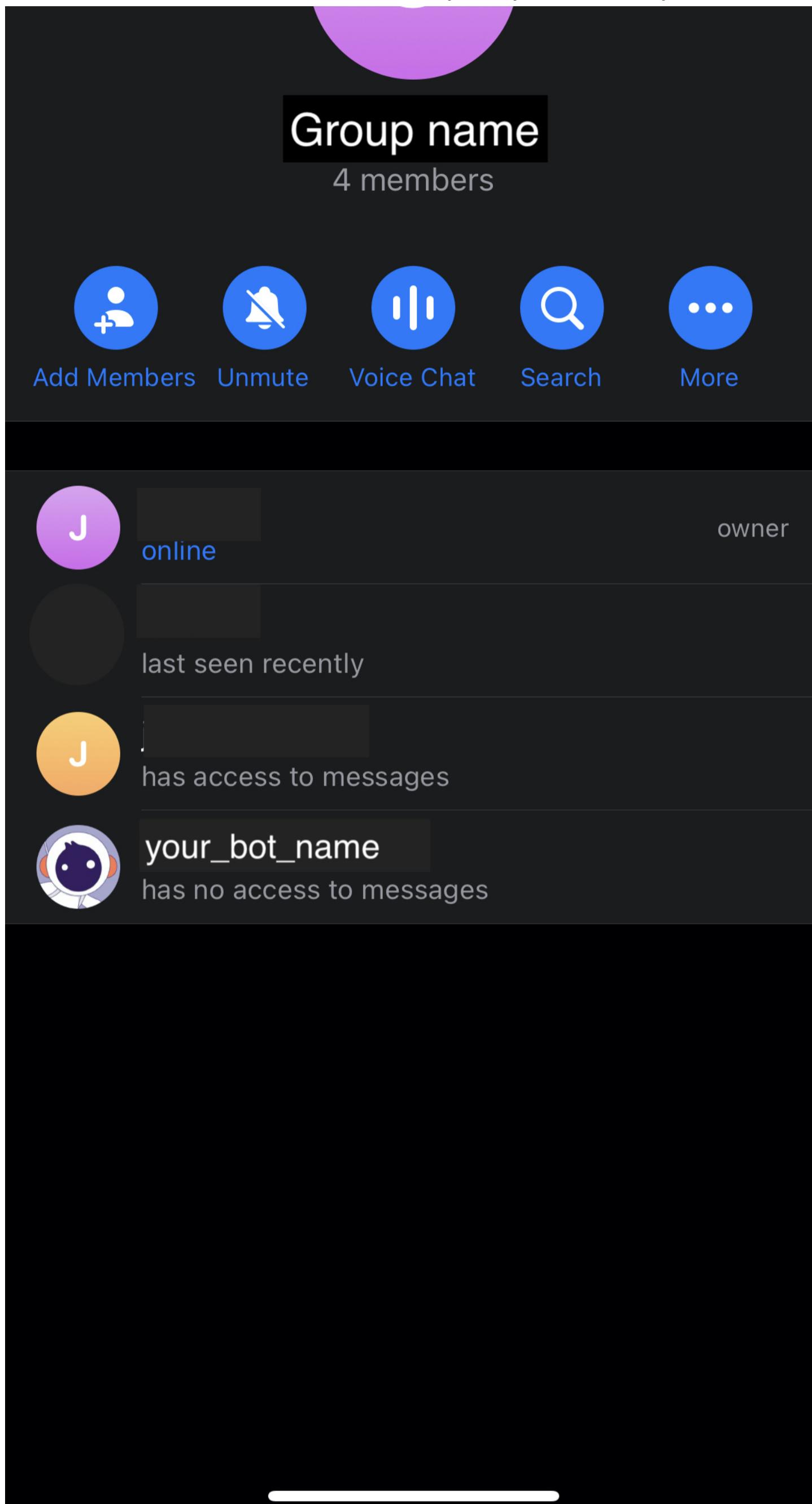
Do not forget that the username must end in `bot` and must be unique. You will get given a **HTTP API token** which is your **BOT API Token** to be used in SpaceONE. It will be in the form **XXXXXXXXXX:YYYYYYYYYYYYYYYYYYYYYYYY**.

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 find it

Add Telegram Channel to your Project / User in SpaceONE

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

Basic Information

The screenshot shows the SpaceONE Project management interface. The top navigation bar includes links for Project, Inventory, Identity, Monitoring, Automation, Plugin, and Management. Below the navigation is a breadcrumb trail: Project > SpaceONE Dev > Belkin Snow. A back arrow labeled '← Project' is present. On the right, there's a 'Project ID: project-18655561c535' and a 'Create Maintenance Window' button. The main content area has tabs for Summary, Member, Alert (6,714 beta), Notifications (beta), and Tag. The Notifications tab is active. Below the tabs, a section titled 'Notifications Channel' contains five buttons: '+ Add Slack Channel', '+ Add Voice Call Channel', '+ Add SMS Channel', '+ Add Email Channel', and '+ Add Telegram Channel'. There is also a separate button for '+ Add SpaceONE User Channel'. A note at the bottom states: 'SpaceOne User: Forward to the project members' personal notification channel'.

Set information above.

The screenshot shows the 'Add Telegram Channel' configuration page. The top navigation bar is identical to the previous screenshot. The main content area has a title '← Add Telegram Channel'. Below it is a 'Base Information' section with four input fields: 'Channel Name' (with a placeholder 'Channel Name'), 'Notifications Level' (set to 'Level 1'), 'Chat ID' (containing '-514081686'), and 'BOT API Token' (containing 'XXXXXXXX:YYYYYYYYYYYYYYYYYYYYYYYY').

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, see How To get Bot API Token to get information

Notification Schedule

You can select when to receive alarm. There two options

Schedule

Setting Mode

All Time Custom

(i) You will only receive notifications in the schedule you choose.

Setting

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

9:00

▼

to 18:00

▼

Time Zone: UTC

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 to the group,

then send a message to the group again,

then try the `getUpdates` url again.

Visit [Telegram API Bot](#) for an additional understanding 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

The screenshot shows the SpaceONE Power Scheduler dashboard with three project cards:

- Collector-Plugin:** Shows 0/16 resources, estimated cost savings \$ N/A, and a weekly schedule heatmap with no scheduled tasks.
- SpaceONE-DEV:** Shows 10/65 resources, estimated cost savings \$ N/A, and a weekly schedule heatmap with three scheduled tasks: tokyo-ec2-dev, seoul-ec2-dev, and us-west-ec2-dev.
- SpaceONE-PRD:** Shows 0/13 resources, estimated cost savings \$ N/A, and a weekly schedule heatmap with a note: "Please register a schedule."

Annotations on the screenshot highlight the **Search Bar**, **Schedule widget**, and **Schedule Heatmap**.

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.

Power Scheduler

Search Bar

Repeat schedule setting time: Unset, Less than 12 hours, Over 12 hours

Project Name	Applied resources / Number of applicable resources	Estimated cost savings approx.
Collector-Plugin	0/16	\$ N/A
SpaceONE-DEV	10/65	\$ N/A
SpaceONE-PRD	0/13	\$ N/A

Schedule (1) test-scheduler-01

Schedule (3) tokyo-ec2-dev, seoul-ec2-dev, us-west-ec2-dev

Schedule Heatmap

Please register a schedule.

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

Automation > Power Scheduler > CloudOne Team > SpaceONE-DEV

← tokyo-ec2-dev On

Scheduler Time Set the scheduler applying time. 02, 2021 < > This week

	SUN 21	MON 22	TODAY 23	WED 24	THR 25	FRI 26	SAT 27
00							
01							
02							
03							
04							
05							
06							
07							
08							
09							
10							
11:14							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							

Time Zone
Asia/Seoul

Repeat: Schedule
 Repeat: Turn on Edit
 Turn Off

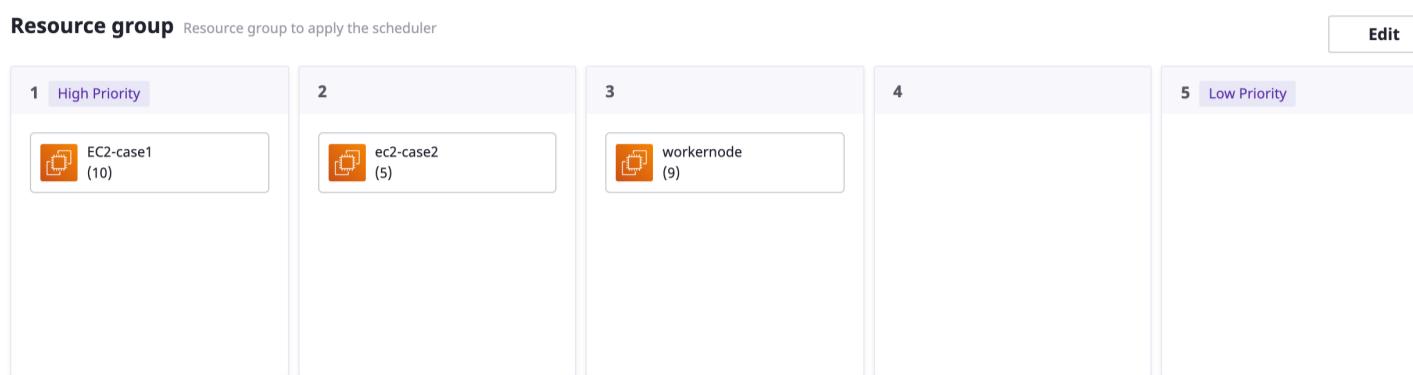
One time schedule
 Turn On Edit
 Turn Off Edit

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

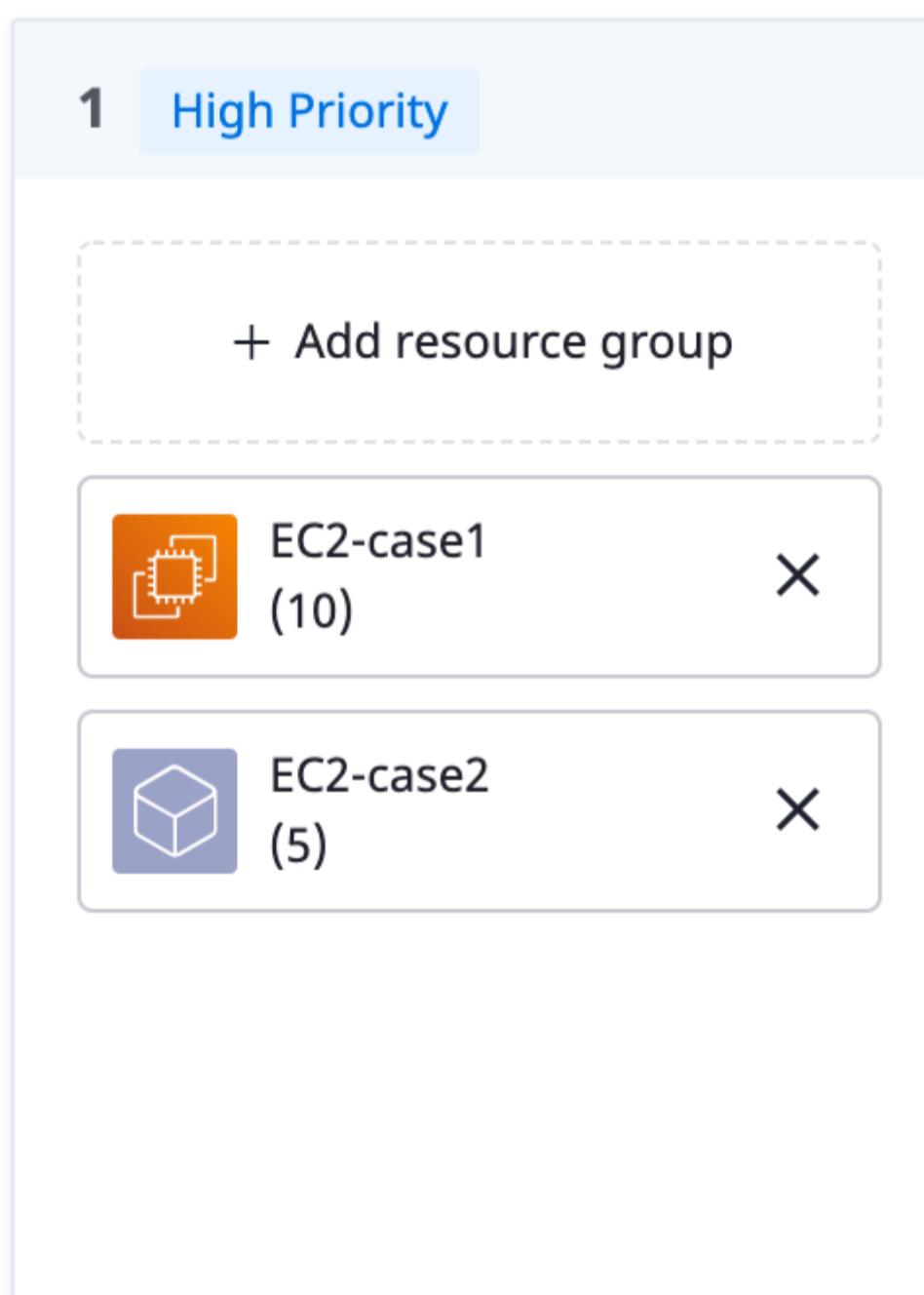
• Priority by Resource Group



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

[← Create a resource group](#)

Base Information

Group Name*
Name must start with a maximum of 128 characters / letter and can contain only letters, numbers and hyphens. 16 characters display only on resource group card

Group Category

Resource Type*

[AWS] EC2

Resource List (65)

Resource Search

ID	Name	Instance Type	Core	Memory	Provider	Instance State	Availability Zone	OS	Pt
server-14ae40ebb7d8	jhsong-windows	t2.medium	2	4	AWS	● Running	us-east-1f	win2019	3.2
server-f7f5436ba603	workernode	t3.medium	2	4	AWS	● Running	us-west-1a	amazonlinux	
server-c22649e8e8f2	case2-ec2-02	t1.micro	1	0.61	AWS	● Stopped	ap-northeast-1a	ubuntu	
server-95bda74ec29b	case2-ec2-03	t1.micro	1	0.61	AWS	● Stopped	ap-northeast-1a	ubuntu	
server-58d6b8f3c859	case2-ec2-04	t1.micro	1	0.61	AWS	● Stopped	ap-northeast-1a	ubuntu	
server-d44af70e19ca	case2-ec2-05	t1.micro	1	0.61	AWS	● Stopped	ap-northeast-1a	ubuntu	
server-19c7677bd92e	case2-ec2-01	t1.micro	1	0.61	AWS	● Stopped	ap-northeast-1a	ubuntu	
server-ce8e95e27f8c	case1-ec2-02	t1.micro	1	0.61	AWS	● Stopped	ap-northeast-1c	ubuntu	

1 / 5 15 ⌂

Cancel
Save

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

Automation > Power Scheduler > CloudOne Team > SpaceONE-DEV

New Scheduler On

Target power state(on/off)

Name of scheduler

Scheduler Name Set the scheduler name. (no spaces)*

Scheduler Time Set the scheduler applying time. → **Scheduler timetable edit**

02, 2021 < > This week

	SUN 21	MON 22	TODAY 23	WED 24	THR 25	FRI 26	SAT 27
00							
01							
02							
03							
04							
05							
06							
07							
08							
09							
10							
11:17							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							

Set the time schedule by click-drag.

*note: All resources are inactive without setting.

Resource group Resource group to apply the scheduler

Resource group edit

+ Add priority group

1 High Priority	2	3	4	5 Low Priority
+ Add resource group				

Cancel
Save

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 character, 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.

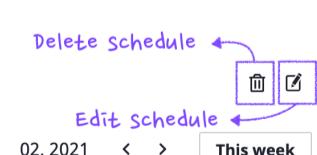
Confirm the input information, then click **save** button.

Schedule Deletion

Automation > Power Scheduler > CloudOne Team > SpaceONE-DEV

← tokyo-ec2-dev 

Scheduler Time Set the scheduler applying time.



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

Scheduler Edit

← tokyo-ec2-dev **Scheduler Time** Set the scheduler applying time.**Resource group** Resource group to apply the scheduler

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.

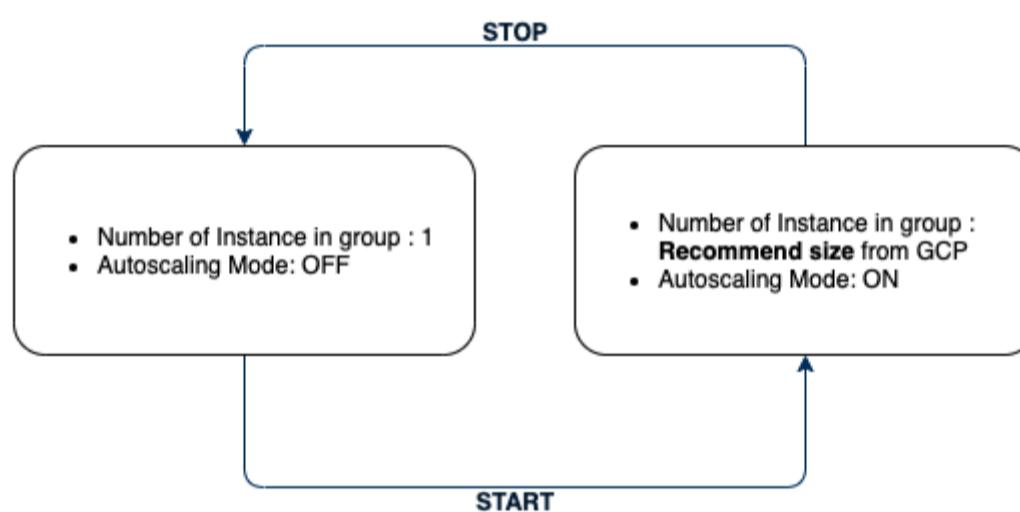
Results on Action:

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

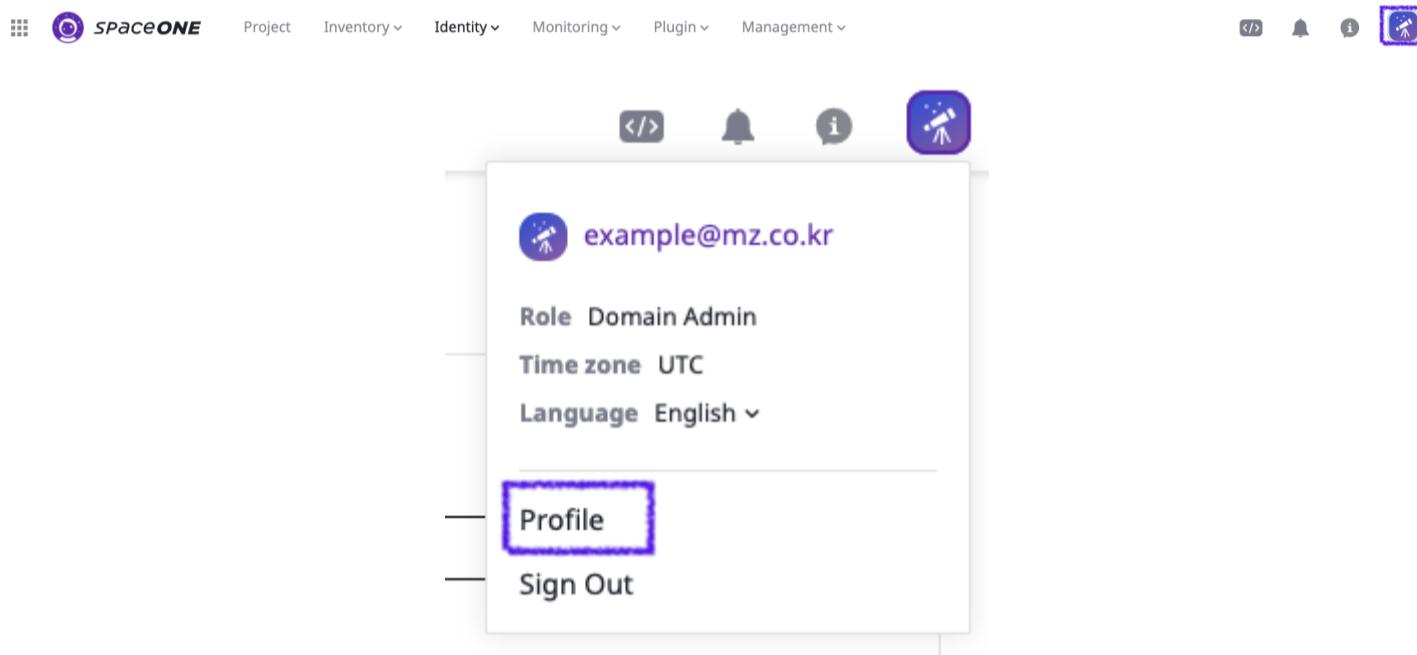
9.1 - Account & Profile

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.

Account & Profile

Base Information

ID	example@mz.co.kr
Role	Domain Admin
E-mail	
Time Zone	UTC x
Language	English (default) ▼

Save Changes

Change Password

Password	
Password Check	

Save Changes

Users can change all information, except **ID** and **Role**.

After changing any information, click **Save Changes**.

A Success message will appear to confirm.

✓ Successfully Updated User

9.2 - API Key

Creating and Managing API Keys

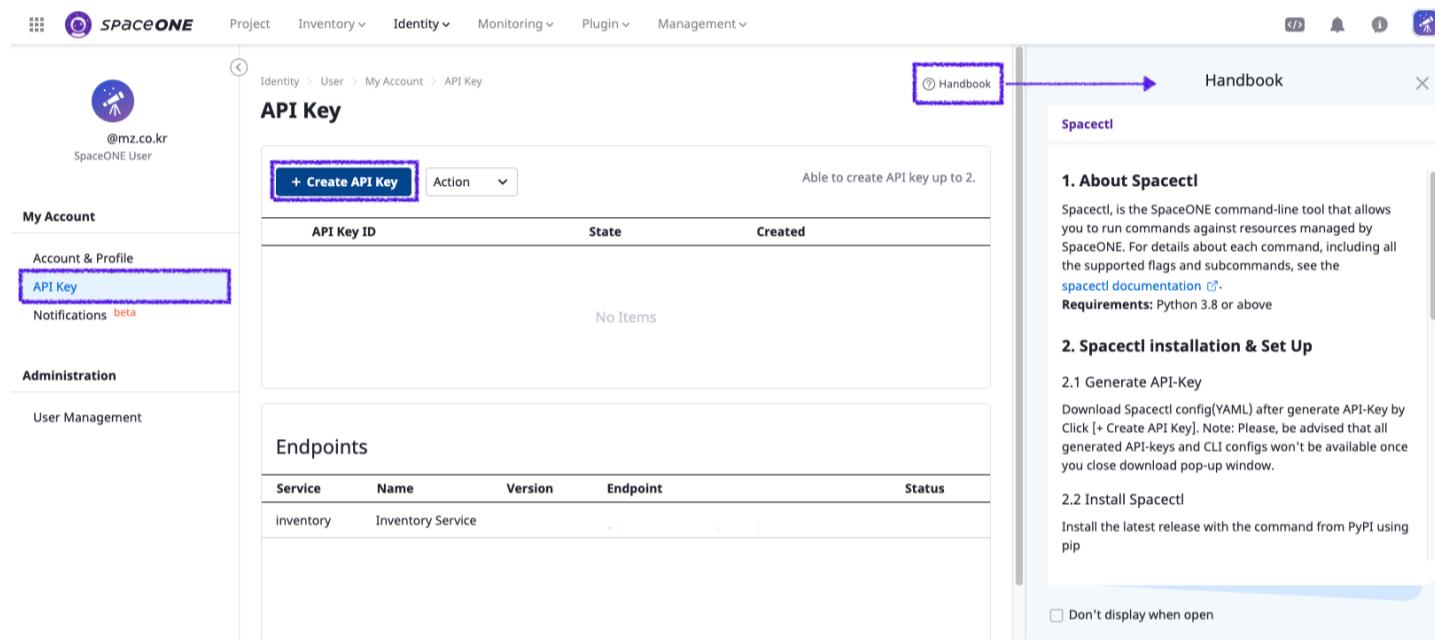
Creating API Keys

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.



Successfully created API Key!

⚠ You have to download the JSON or Config file before you continue. You will not be able to download the file again after close this.

API Key ID

api-key-ae8001220cf5 [show ▾](#)

[Download JSON](#)

Spacectl (CLI)

ⓘ The SpaceONE command-line tool, spacectl, allows you to run commands against resources managed by SpaceONE. [view more ↗](#)

spacectl configuration [show ▾](#)

[Download YAML](#)

[Confirm](#)

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](#).

Identity > User > My Account > API Key

[Handbook](#)

API Key

Able to create API key up to 2.		
API Key ID	State	Created
<input checked="" type="radio"/> api-key-ae8001220cf5	Enabled	2021-08-12 11:06:06
<input type="radio"/> api-key-ffc5be03f251	Enabled	2021-08-12 11:07:19

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**.

API Key

		Action	Able to create API key up to 2.	
API Key ID		Enable	State	Created
api-key-ae800122	<input checked="" type="radio"/>	Delete	● Enabled	2021-08-12 11:06:06
api-key-ffc5be03f251	<input type="radio"/>		● Enabled	2021-08-12 11:07:19

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

Endpoints

Service	Name	Version	Endpoint	Status
inventory	Inventory Service			

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 receive 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**.

Base Information

Channel Name

SpaceONE Channel - 01

Phone Number

010

Schedule

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

Schedule

Setting Mode

All Time Custom

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

Schedule

Setting Mode

All Time Custom

① You will only receive notifications in the schedule you choose.

Setting

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
9:00	to	18:00				

Time Zone: Asia/Seoul

Topic

You can choose to receive all notifications regardless of topics.

Topic

Setting Mode

Receive all notifications Receive notifications based on selected topics

Or you can receive notifications based on selected topics only.

Topic

Setting Mode

Receive all notifications Receive notifications based on selected topics

Setting

monitoring.Alert

Save

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

[← Add Megazone SMS Protocol Channel](#)

Base Information

Channel Name
SpaceONE Channel - 01

Phone Number
010

Schedule

Setting Mode
 All Time Custom

Topic

Setting Mode
 Receive all notifications Receive notifications based on selected topics

Voicecall Protocol Channel

You can add **Megazone voicecall protocol channel** and receive notifications for them.

If you create a voicecall protocol channel, you will be notified by voice calls.

Click **+ Add Megazone Voicecall Protocol Channel**.

Identity > User > My Account > Notifications

Notifications

Notifications Channel

- [+ Add Megazone SMS Protocol Channel](#)
- [+ Add Megazone Voicecall Protocol Channel](#)
- [+ Add Slack Protocol Channel](#)

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

[← Add Megazone Voicecall Protocol Channel](#)

Base Information

Channel Name: SpaceONE Channe - 02

Country Code (optional): 82

Phone Number: 010

Schedule

Setting Mode: All Time Custom

Topic

Setting Mode: Receive all notifications Receive notifications based on selected topics

[Cancel](#) [Save](#)

Slack Protocol Channel

You can add **Slack protocol channel** and receive notifications for them.

If you create a Slack protocol channel, you will be notified from the corresponding Slack channel.

Click **+ Add Slack Protocol Channel**.

Identity > User > My Account > Notifications

Notifications

Notifications Channel

- [+ Add Megazone SMS Protocol Channel](#)
- [+ Add Megazone Voicecall Protocol Channel](#)
- [+ Add Slack Protocol Channel](#)

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

[← Add Slack Protocol Channel](#)

Base Information

Channel Name: SpaceONE Channel - 03

Slack Channel: Test_channel

Slack Token: xxxx

Schedule

Setting Mode: All Time Custom

Topic

Setting Mode: Receive all notifications Receive notifications based on selected topics

[Cancel](#) [Save](#)

Edit/Delete Channel

Edit

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

The screenshot shows a form for editing a channel named "SpaceONE Channel - 01". The form includes fields for Channel Name (SpaceONE Channel - 01), Phone Number (010), Schedule (All Time), and Topic (Receive all notifications). On the right side, there are four "Edit" buttons, each preceded by a small icon and the word "Edit". A blue rectangular box highlights these four "Edit" buttons.

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

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

The screenshot shows the same edit form as above, but with a purple rectangular box highlighting the "Save Changes" button at the top right of the form area.

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

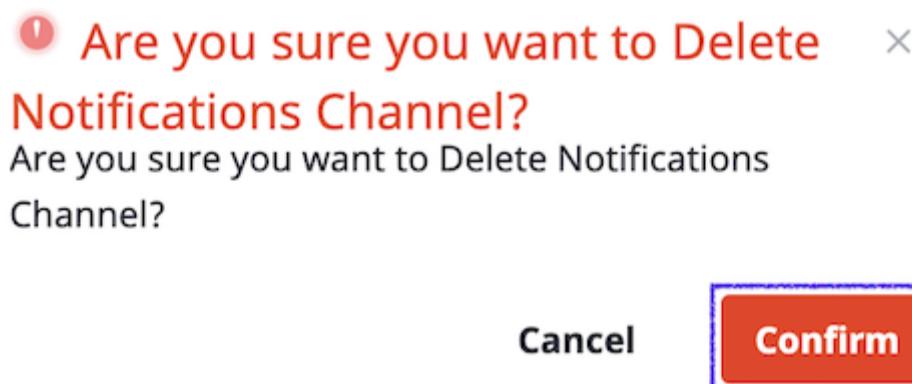
Delete

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

The screenshot shows the edit form again, with a blue rectangular box highlighting the trash can icon located at the top right of the form area.

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

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.

The screenshot shows the edit form once more, focusing on the toggle switch button for "Megazone SMS Protocol". The switch is currently in the "on" position, indicated by a blue outline around the switch icon.

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

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