1 Table of Contents

1.1 Revision History

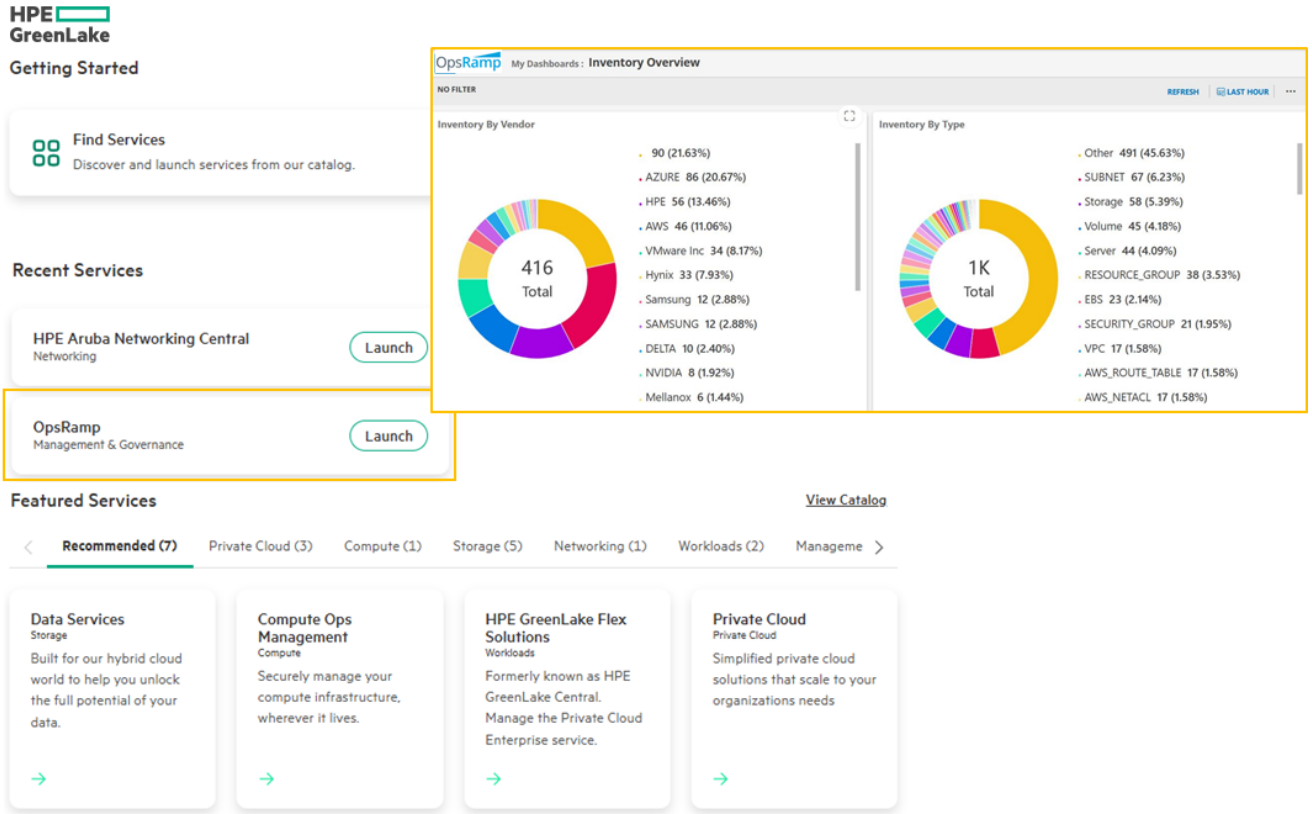
DATE	VERSION	EDITOR	CHANGES
08 Feb 2025	0.1	Ariya Parsamanesh	Initial creation
02 Mar 2025	0.2	Ariya Parsamanesh	Added the discovery workflow

2 OpsRamp Public Cloud Observability

2.1 Introduction

The increasing complexity of IT environments, especially with the addition of cloud services, can lead to chaos, inefficiencies, and uncontrolled "shadow IT." OpsRamp addresses these challenges with a comprehensive, cloud-based observability platform. By integrating logs, alerts, events, and network data, OpsRamp delivers AI-driven insights.

Essentially, OpsRamp is an AI-powered IT operations management platform that enables organisations to monitor, manage, and automate their entire IT infrastructure. A key strength is its extensive library of over 3,000 integrations for diverse infrastructure and applications. This provides a unified view of the organization's IT landscape, regardless of whether it's hybrid, on-premises, or cloud-based. OpsRamp offers health, performance, and availability dashboards, along with event management and automated remediation workflows.



The three components of OpsRamp are

- Discovery and Observability that automatically discovers every infrastructure resource in on-prem and 3rd party cloud environments. And then aggregating the metrics, events and logs from them in one dashboard.
- Event and Incident Management that automatically correlates, deduplicates and suppresses unnecessary alerts, to help reduce noise and focuses on root case of the issue.
- Intelligent Automation that improves efficiently through automating processes like routine maintenance tasks, remediation tasks in response to alerts, triggering tasks in 3rd party tools using APIs.

Benefits

- Simpler IT operation management, since instead of using multiple tools for each cloud infrastructure and environment, you get a consolidated on-premise, cloud and cloud-native observability.
- This enables you to respond to alert and security events more effectively
- Since you can co-relate various alerts, you can set your metrics and can automate the remediation, your service uptime will increase and results in better user and application experience.

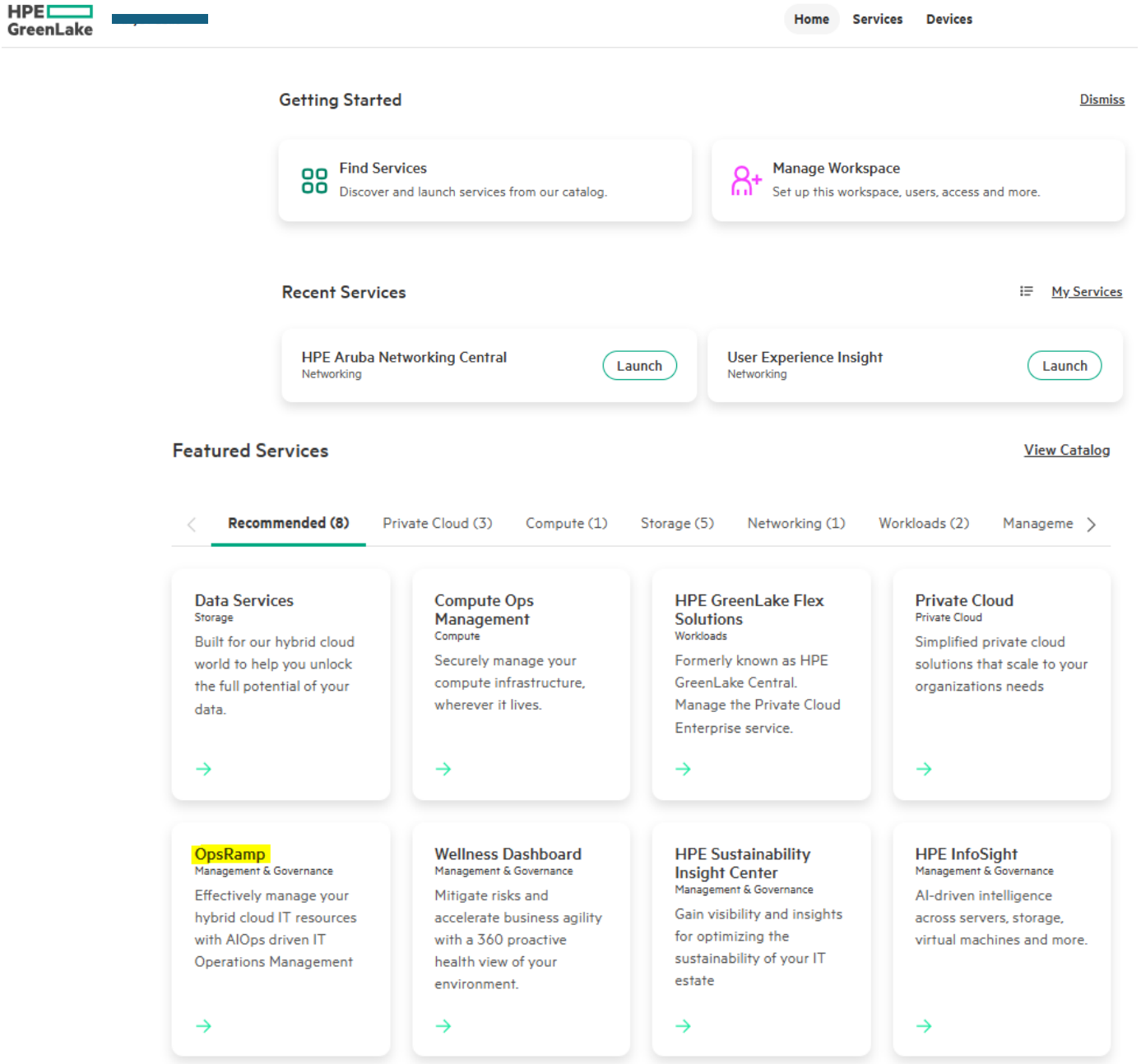
In this technote I'll cover the basic setup of OpsRamp and focus on its simplicity for adding observability of a cloud based environment.

2.2 Assumptions

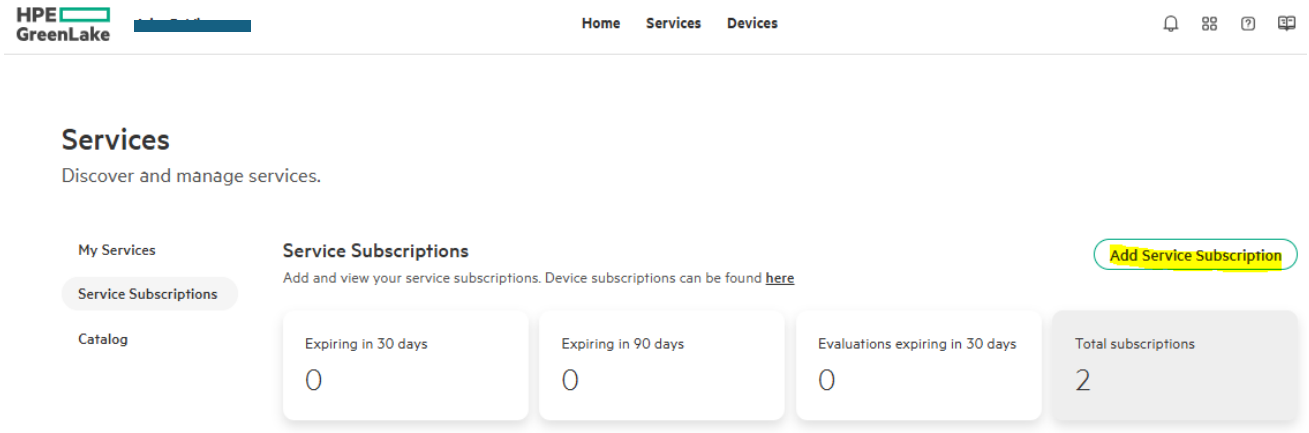
- You already have a valid GreenLake account
- Your OpsRamp subscription is added to your GreenLake account

2.3 GreenLake OpsRamp Access

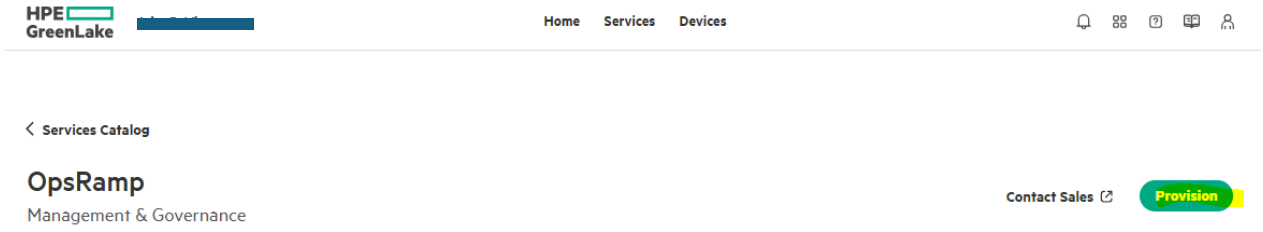
OpsRamp is a service app which is part of HPE GreenLake along with other apps that are available like Aruba Central and HPE Sustainability Insight Center just to mention a few. Here is my GreenLake account and it shows my recent services and also a service catalog.



OpsRamp is listed under Management and Governess Management tab of service catalog. But it also gets listed under recommended tab. You need to first add the OpsRamp subscription to your GreenLake service subscriptions.



And then go to the service catalog and provision OpsRamp app.



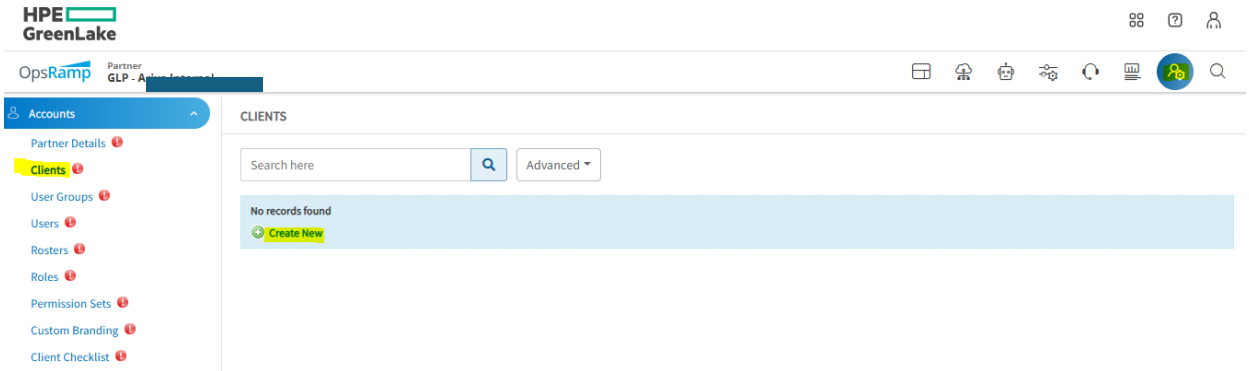
Once these are done you can launch the App and you'll be redirected to your OpsRamp dashboard.

2.4 OpsRamp Accounts

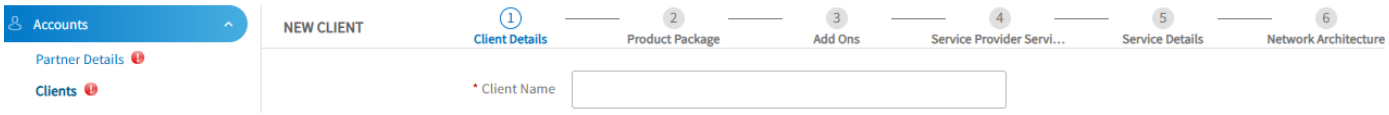
One thing to note about OpsRamp is that it uses multi-tenant architecture and hence it has different type of accounts. There is a "Partner" Account which is a top level account generally used by MSPs or large organisations. This account lets you create bunch of other accounts called "Client" accounts. These "Client" accounts could represent business units or branch offices, etc. With "Client" account you can then implement role base access control (RBAC), have different monitoring and visualisation specific to it, etc.

Firstly you need to setup a "Client" account then you might have a collector to discovers say network devices or an agent that is installed on resources that needs monitoring or a direct API integration.

To setup a client, you need to navigate to Setup icon >> Setup >> Client

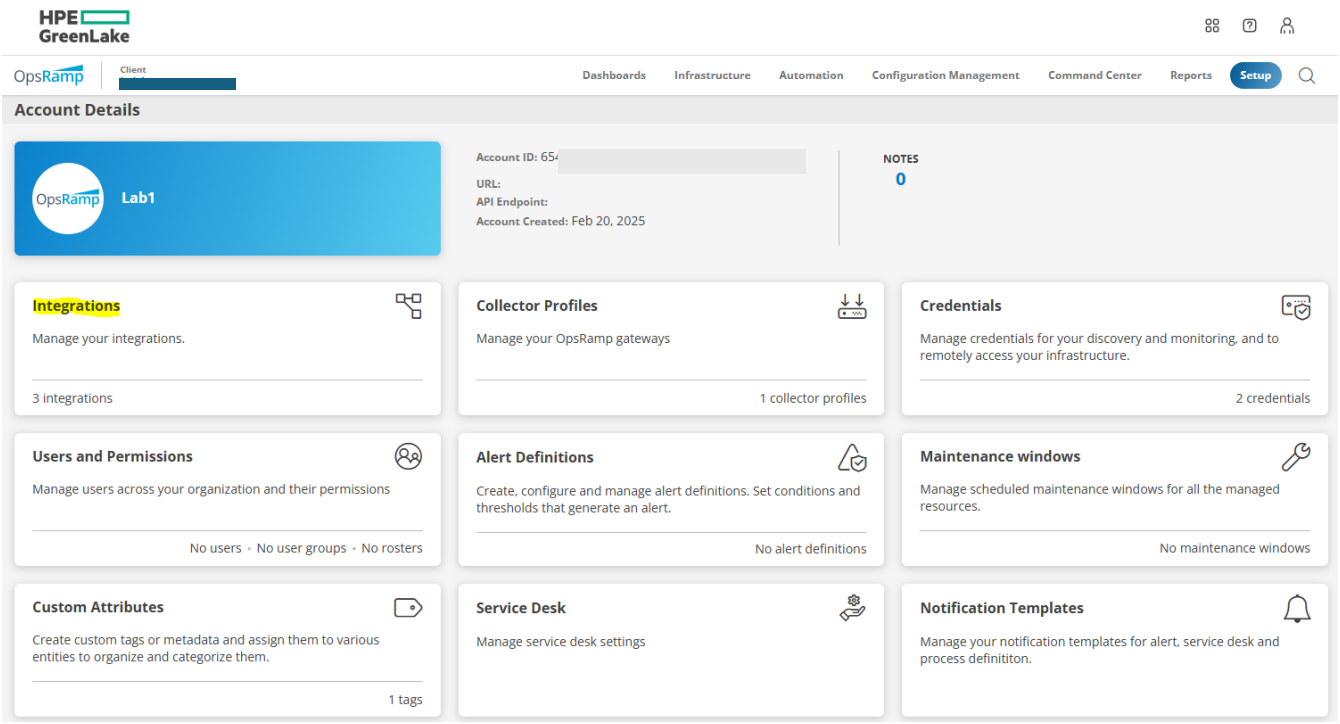


I won't go to the details of setting of a client as you can always refer to OpsRamp user guide, but as minimum you need to add the mandatory fields in Client detail part.



2.5 Public Cloud Discovery

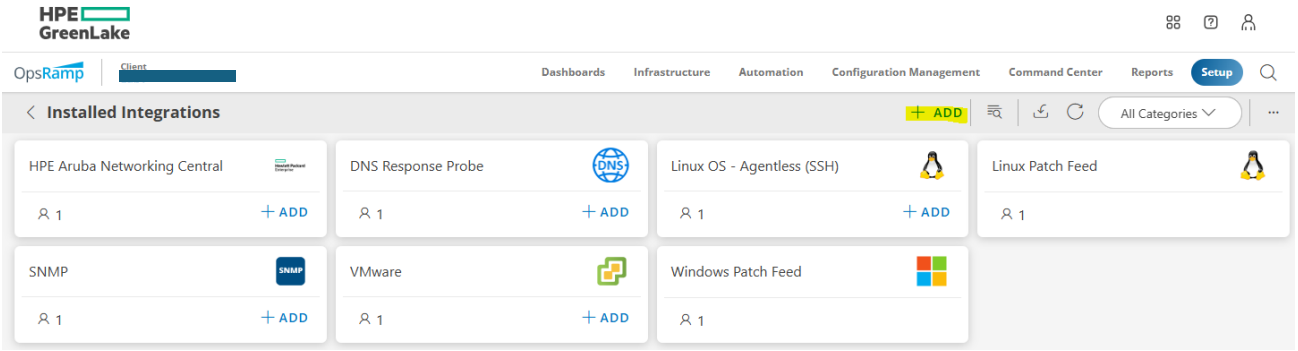
Now, to onboard public cloud resources, click on setup in the navigation bar and navigate to the account details page for the "client" that you just added.



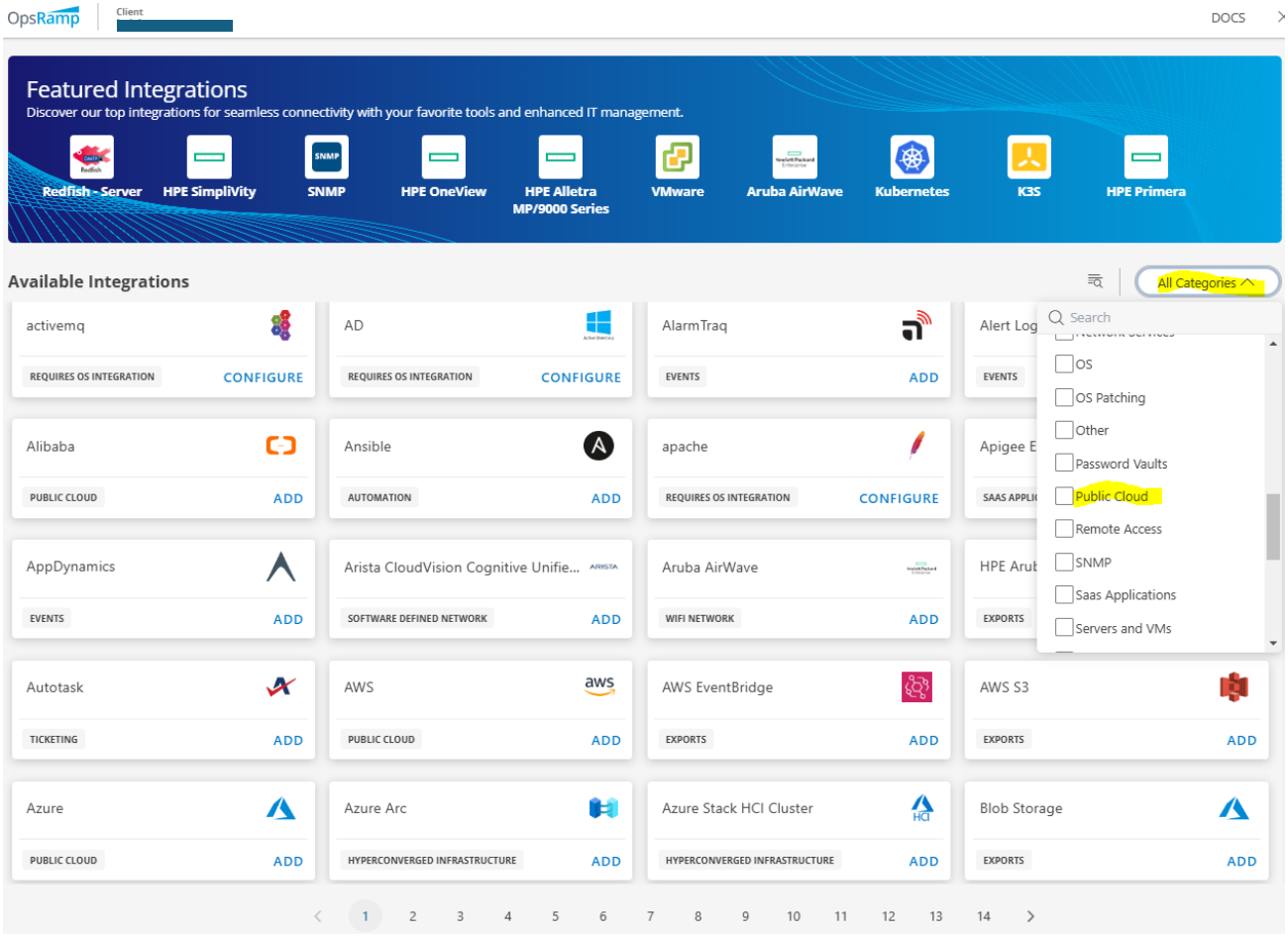
The account details page allows us to access the account details of our OpsRamp instance. Here there are a number of functional groups available like

- Defining your various collectors that you might need to discover your endpoints/devices.
- Credentials that are needed to discover devices/servers/application in your network
- Defining the alerts for your environment
- Setting up your maintenance windows
- Using custom attribute for various integration like we do with New Aruba Central
- Define your notification templates that can be sent using email, SMS, or voice (needs to have your own subscribed add-on).
- and Integration group that provides app store for various integration with different application and infrastructure like public cloud.

Click on the integrations tile to access the OpsRamp integration app store. This page displays all the installed integration applications for this instance.



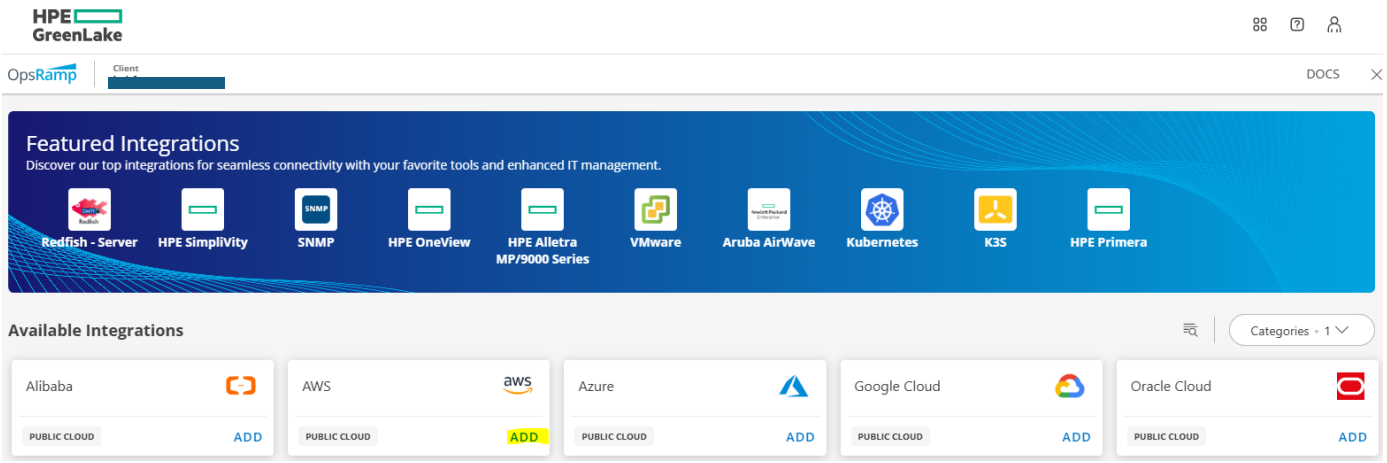
Next to integrate a new public cloud account we'll click on ADD which brings us to the next screen where we can choose the integration that we need. The list is in alphabetical order with the list of Featured integration at the top. OpsRamp provides the ability to discover and onboard resources or devices from any domain, vendor, or technology.



One of the important features of OpsRamp is its extensive integrations. The aim of the integrations is to connect OpsRamp to organisation's existing tools, platforms and ITSM solutions. Then based on these integrations OpsRamp can receive all the events, use its ML/AI to reduce the noise and correlate the alerts. Once we have the severity based Alerts then OpsRamp can provide automated remediation as well.

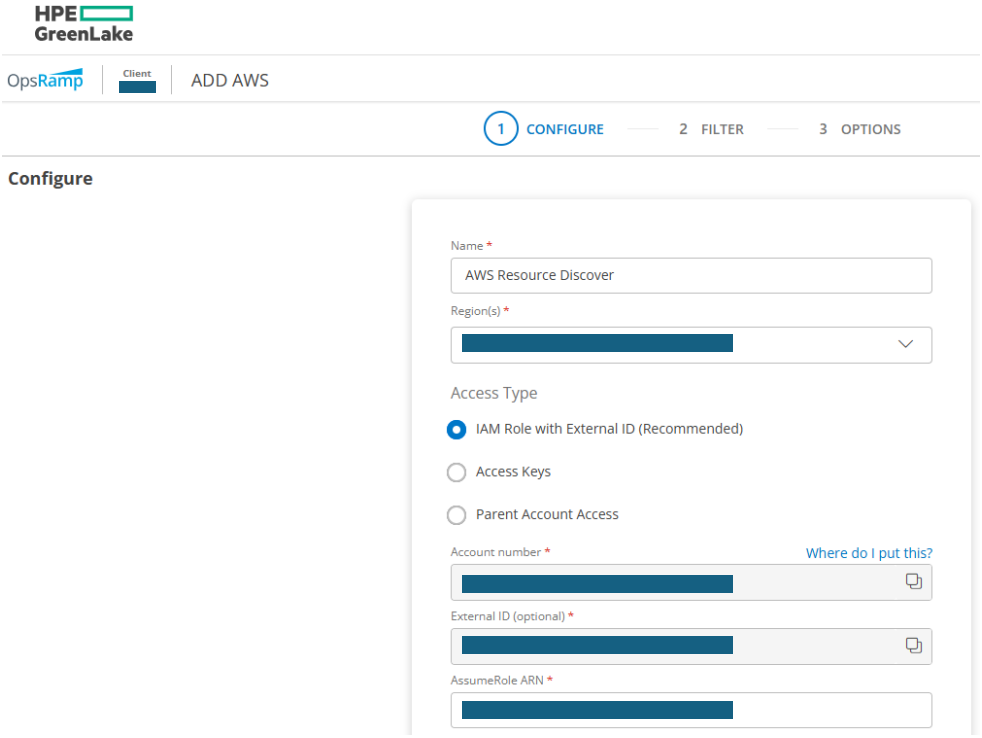
To filter the available integrations list, expand "all categories" filter at the top of the page and select public cloud as shown from the list. Now the page only shows the available Public Cloud Integration apps.

Here we'll choose to install the AWS app.

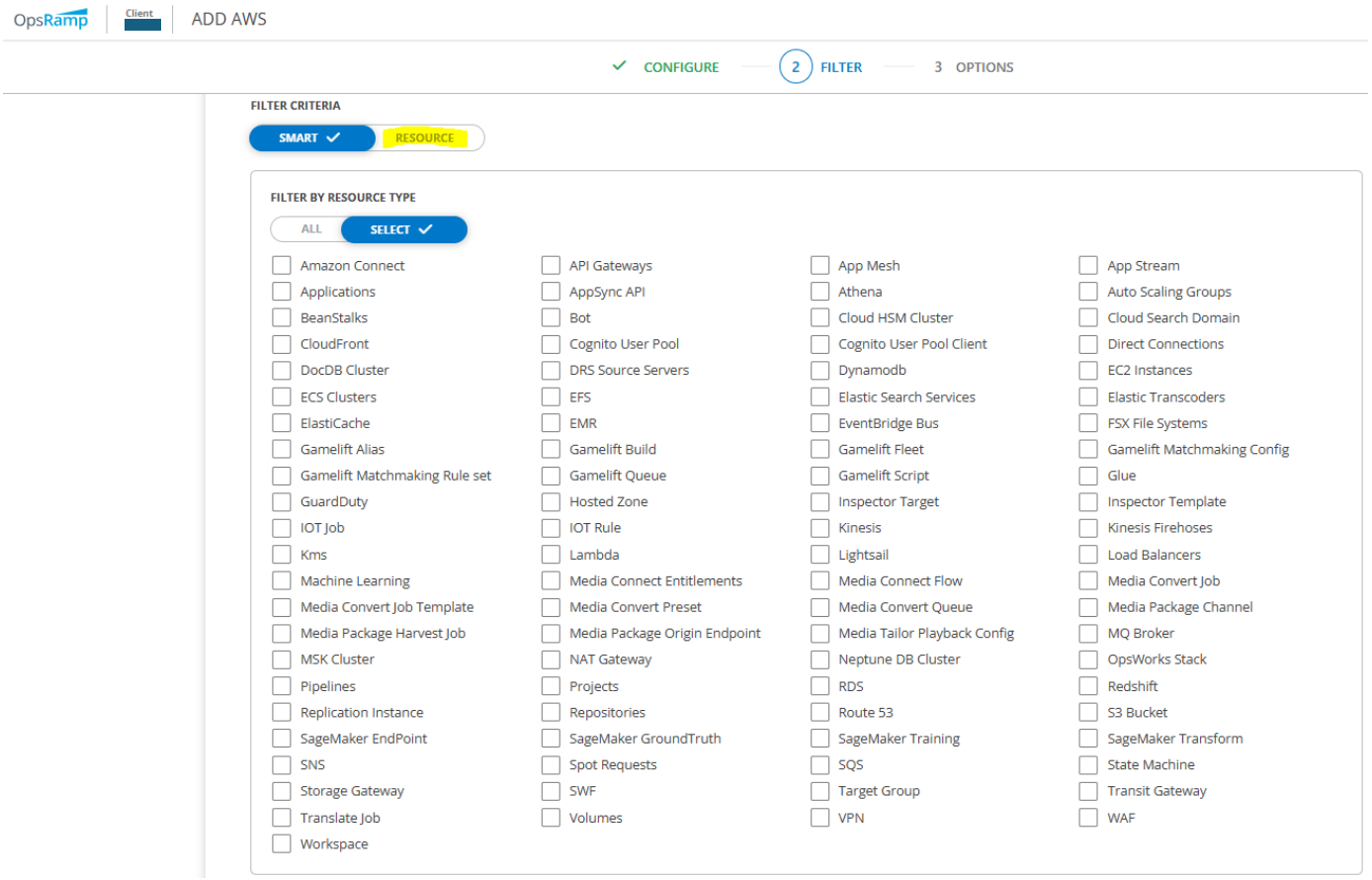


Next we get to the AWS configuration page to begin the process of discovering and onboarding resources. It is assumed that you have authorised access to AWS account and you have IAM with AssumeRole External ID.

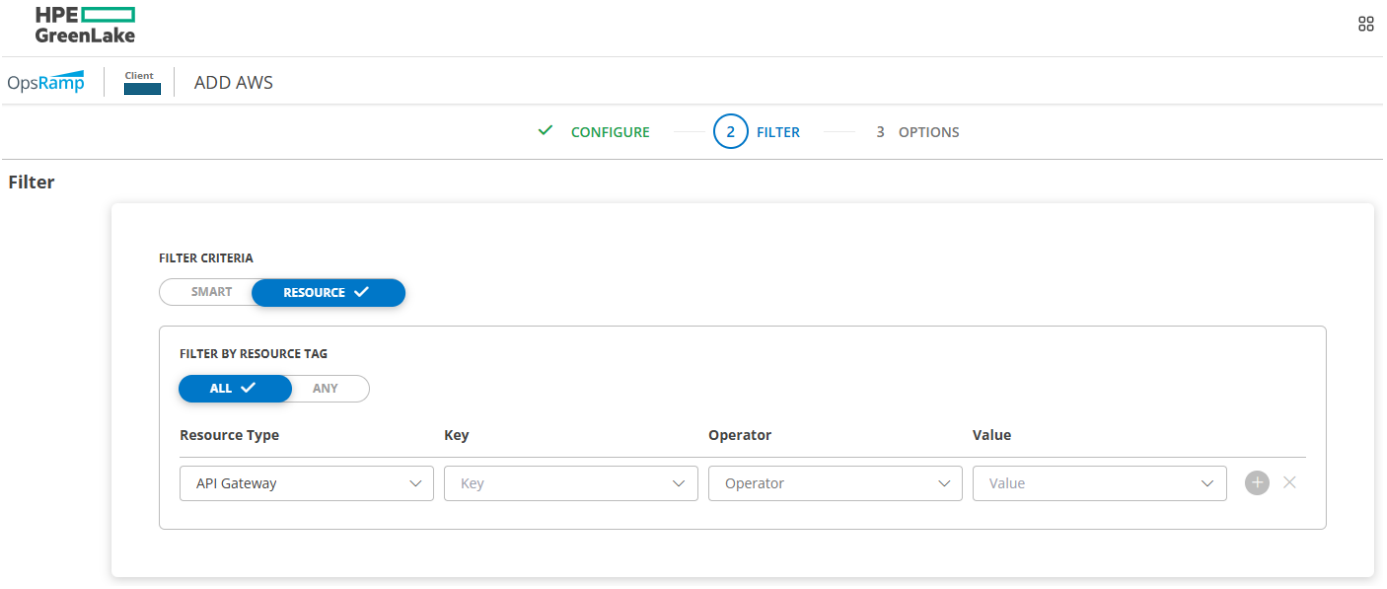
OpsRamp recommends that the AWS integration uses the External ID method as it adds an additional layer of security to the integration, for details of it please refer to OpsRamp user guide.



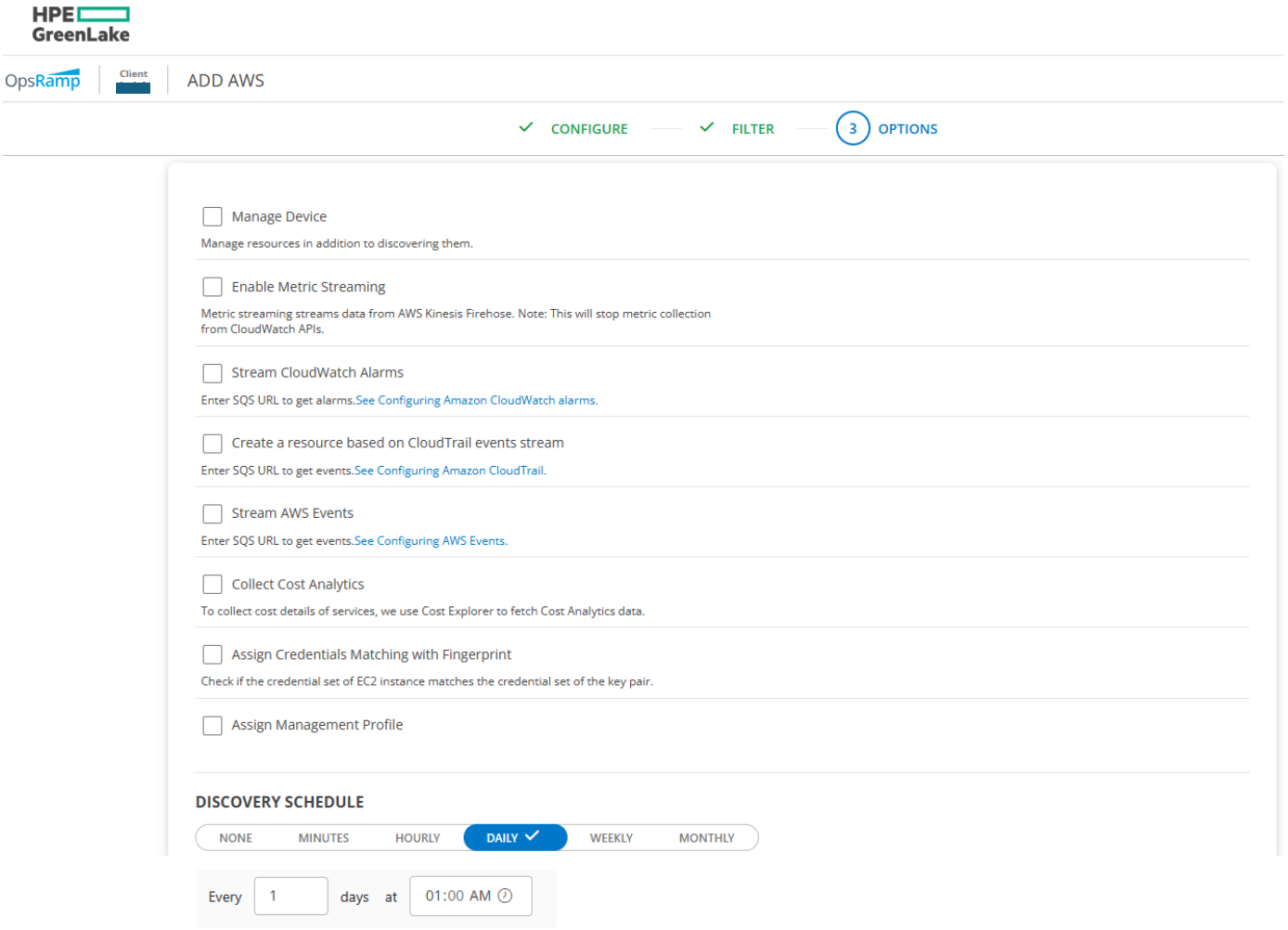
Once all the information has been entered, click next to proceed. Now we are brought to the filter page where Few can toggle between the available filter options and specify the type of AWS resources we want to onboard to our OpsRamp instance.



We can choose to discover and onboard all the resources in the AWS account, or they can choose to only discover specific resource types.

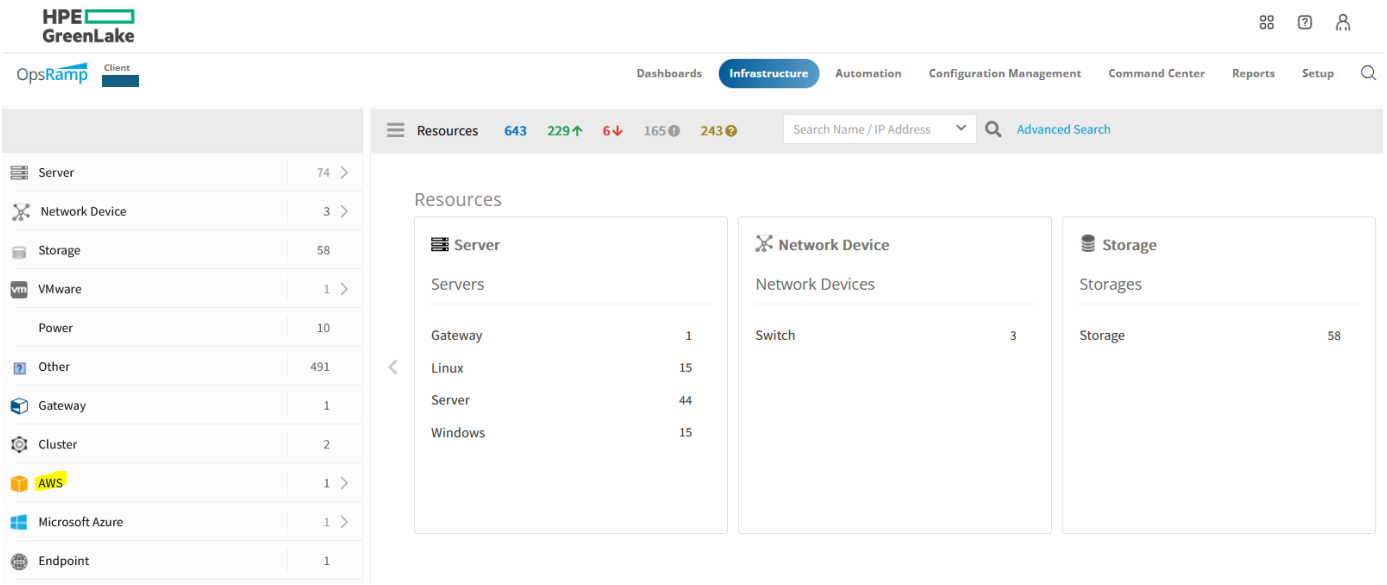


The last page of the public cloud discovery process provides flexible options to manage AWS resources while onboarding onto the OpsRamp instance.

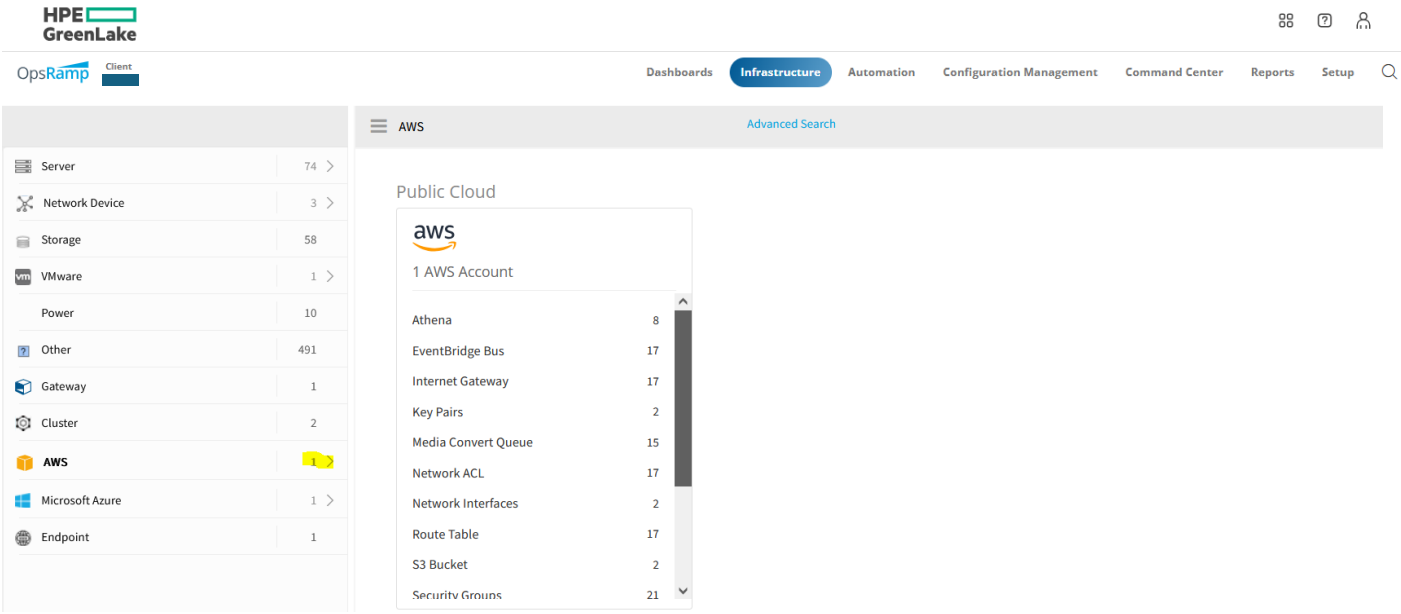


We can define a discovery schedule to ensure that all resource statuses are in sync between OpsRamp and AWS Infrastructure. Now click finish to complete the installation and initiate the resource discovery. Once the AWS resource discovery is completed by OpsRamp, the resources will be arranged by resource type.

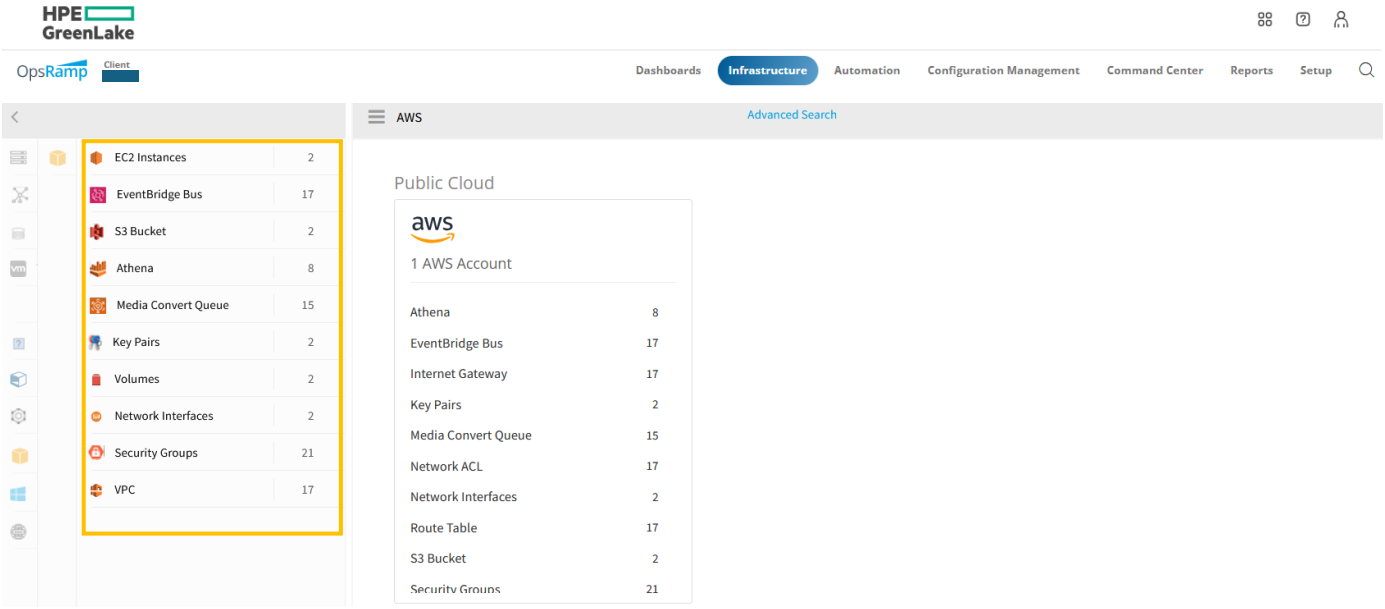
To view the newly discovered public cloud resources, we'll navigate to "Infrastructure >>Resources" and then by clicking on AWS.

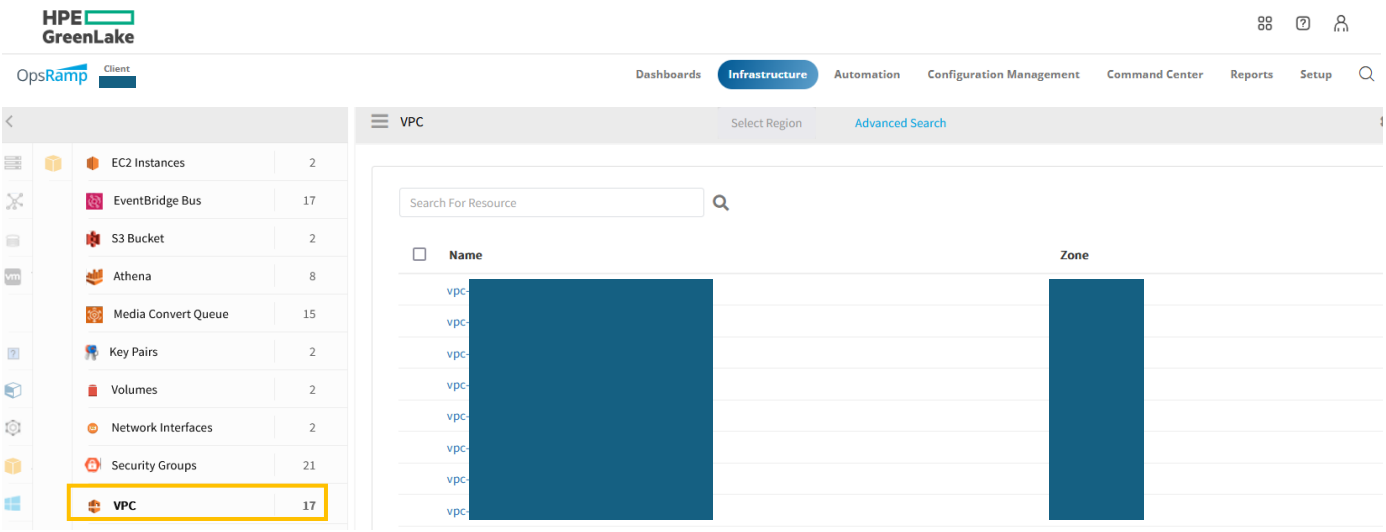


The AWS infrastructure resource page shows the list of AWS resources that were discovered and onboarded to OpsRamp.

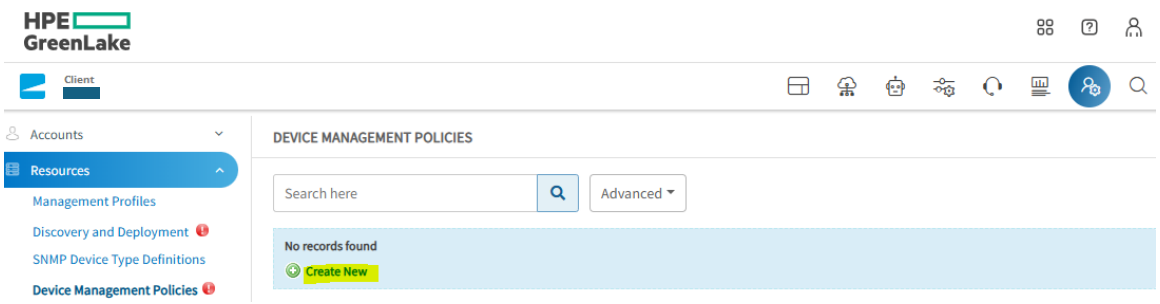


Then you can click on the highlighted area to get the details of each resource.

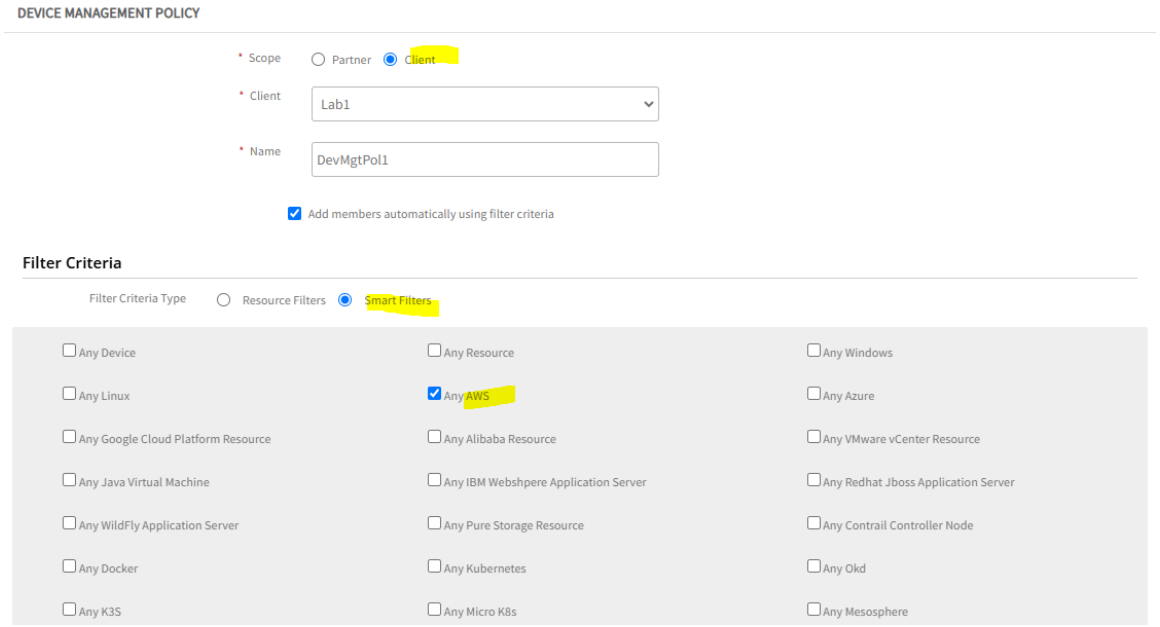




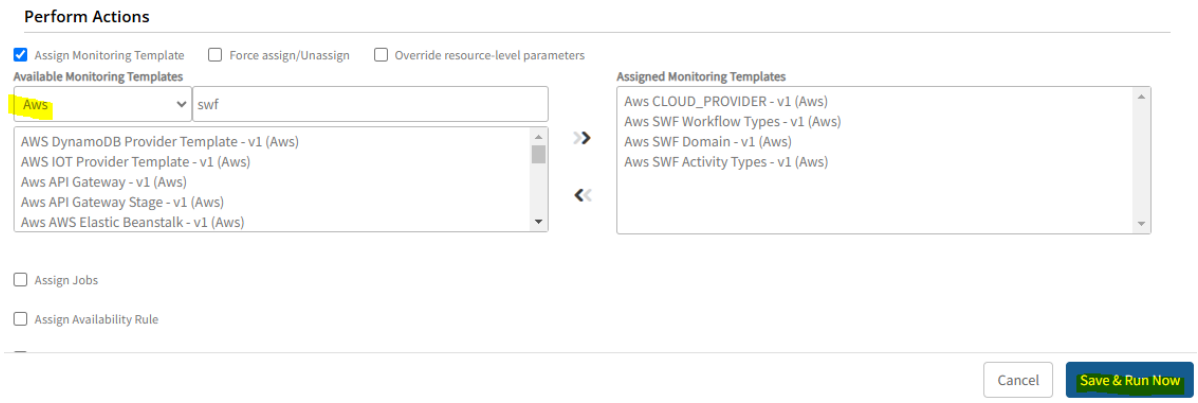
It is important to collect metrics for monitoring and managing resources. The easiest way to collect metrics is to create device management policy to obtain metrics from all your discovered resources and any future ones automatically. We need to go to Setup >> Resources >> Device Management Policies.



Select the Smart filters to be able to choose from the categories.

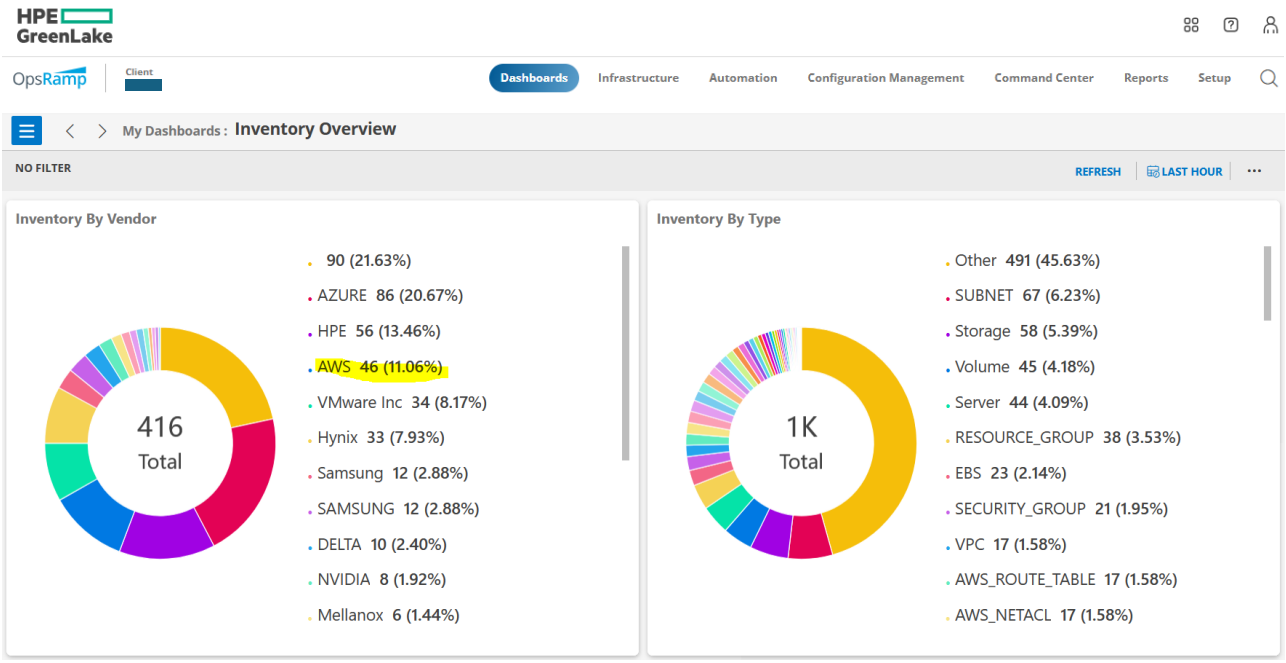


Now scroll down and select check the check box for “Assign Monitoring Template”. Then select AWS as a filter and choose relevant templates for your test or even all the available templates.



OpsRamp inlcudes a vast number of Monitoring templates that can be applied to the resouce types and then based on that you can see the perfornace, availability of the resouce in the customise dashboad. For more details about Monitoring templates please refer to the OpsRamp user guide.

Now when we go back to our dashboard, we should see all the resources that are disvoverd and assigned.



Lastly you can have a number of customised dashboards at different levels. Partner administrator, a Client administrator, or a user with Manage Dashboard permission can create dashboards.