stackArmor OpsAlert: Enabling a Well-Managed Cloud

stackArmor
July 2019

Table of Contents

1 About this document

stackArmor OpsAlert solution is for business managers and product owners to help organizations maximize cloud efficiency, maintain security and enable operational excellence, and reduce cloud costs by eliminating “idle” capacity. This document provides guidelines and recommendations to utilize **stackArmor OpsAlert** effectively.

Read more about OpsAlert at https://stackarmor.com/stackarmor-opsalert/

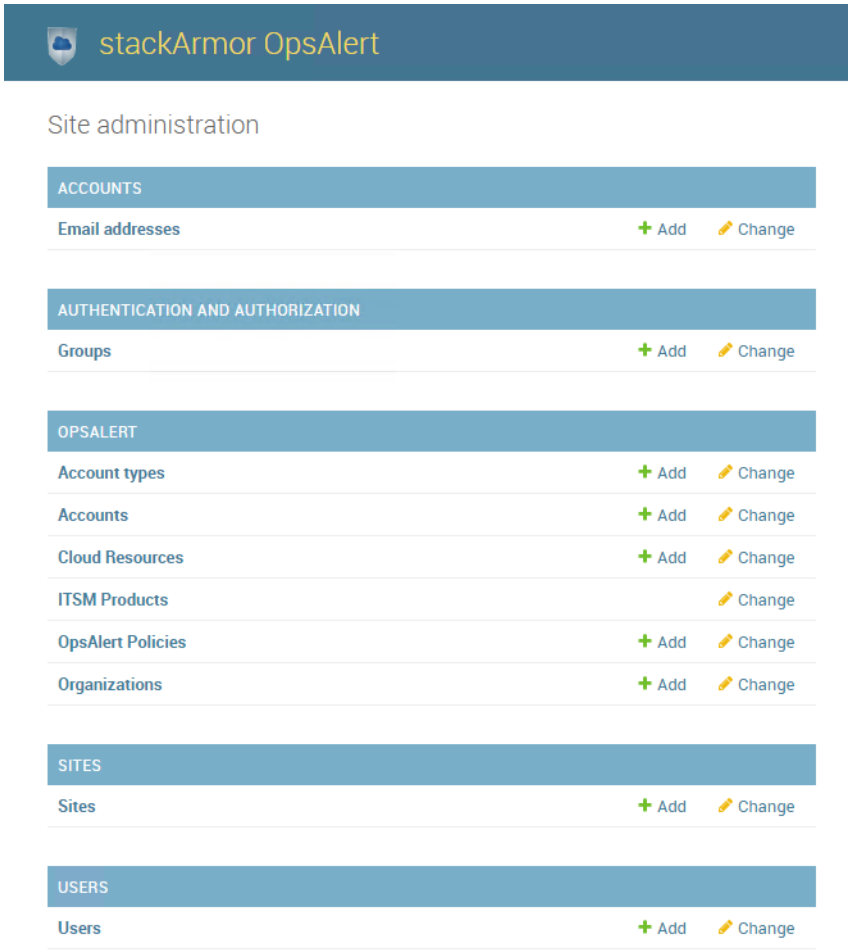
2. Adding Accounts to OpsAlert

Follow these steps on OpsAlert admin panel:

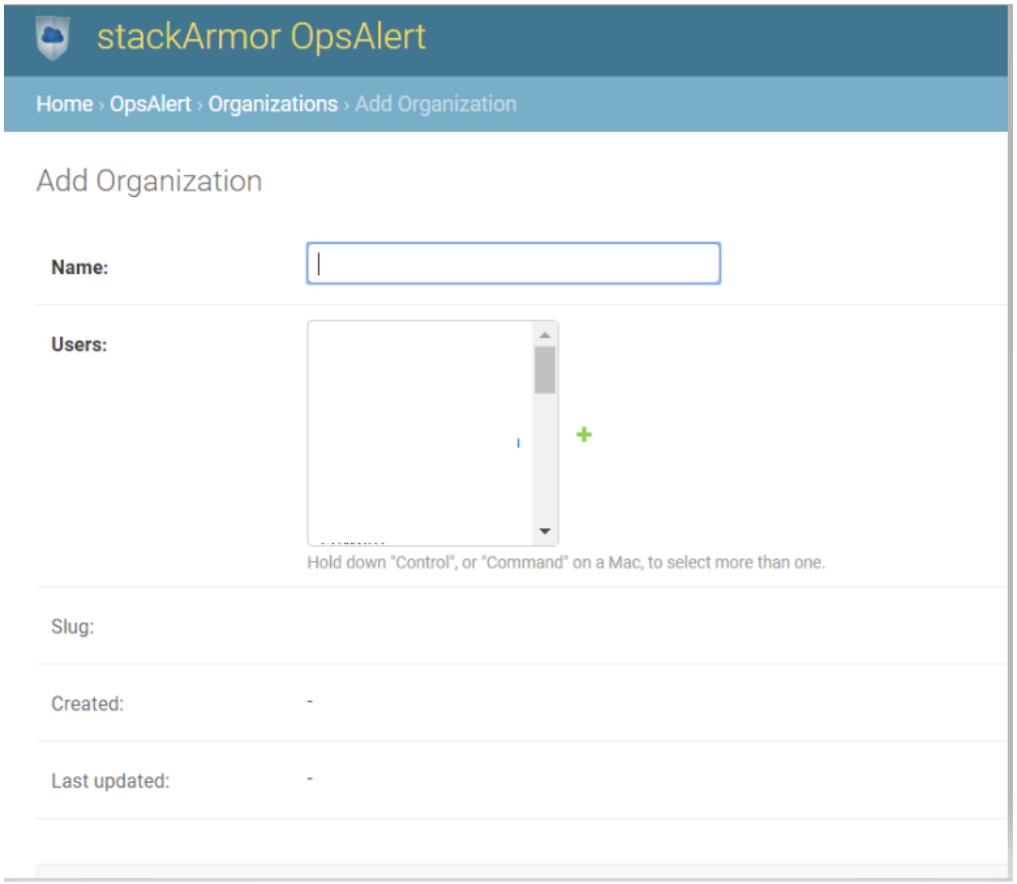
1) Login to Opsalert Admin Panel:

   - RDP into bastion (if applicable). Some projects may not require bastion server if VPN services are being used or are publicly available OA instances.
   - To access the admin portal, using Chrome go to http://xxx.xx.xxx/admin and sign in using admin user ID and password. You can create the additional user accounts on admin portal.

2) In Admin portal, select “Add” under **Account types**. Type “AWS” under the account type and save it.



3) Select **Organizations** and add the name of the organization and select which user should be a part of that organization.



4) Under Accounts, click “Add”. Once “Add account” shows up, follow the steps below:

- Set account to Active
- Type Name of account (same as setup in command line)
- Select Account type as AWS from the drop-down
- Type the Account Identifier (It’s the AWS Account number)
- Type Email address where the notifications should be delivered. If multiple email addresses need to be added, use comma-separated format.
- Select Organization which you created in step above from the drop-down.
- Save the Account. This completes adding the account part.

Home › OpsAlert › Accounts › Add account

Add account

- [ ] Active
- [ ] Third party

Name:

Notes:

Account type: ---------

Identifier:

Email address:

Org: ---------

3. Create IAM role in AWS console.

Follow these steps on AWS console:

1) Create an IAM role called OpsAlert for the new AWS Account.
2) Assign the following policy to the IAM role created in previous step:

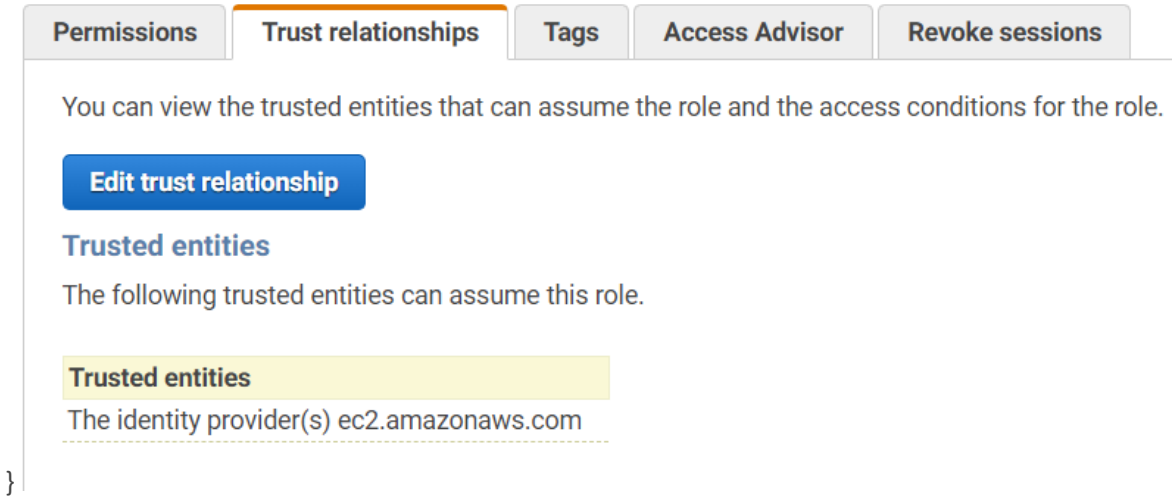
```
{
  "Statement": [
    {
      "Action": [
        "acm:Describe*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudFront:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:Lookup*",
        "cloudwatch:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "config:describe*",
        "directconnect:describe*",
        "dynamodb:List*",
        "dynamodb:Describe*",
        "elasticbeanstalk:Describe*",
        "ec2:Describe*",
        "ec2:Get*",
```

```
"elasticloadbalancing:Describe*",
"elasticache:Describe*",
"guardduty:List*",
"guardduty:Get*",
"iam:Get*",
"iam:List*",
"inspector:List*",
"inspector:Describe*",
"kinesis:Describe*",
"kinesis:List*",
"kms:List*",
"kms:Describe*",
"kms:Get*",
"lambda:List*",
"lambda:Get*",
"opsworks:Describe*",
"redshift:Describe*",
"rds:Describe*",
"rds:List*",
"route53:List*",
"route53:Get*",
"s3:List*",
"s3:Get*",
"s3:Head*",
"s3:PutObject",
"sdb:Get*",
"sdb:List*",
"sns:Check*",
"sns:Get*",
"sns:List*",
"sqs:Get*",
"sqs:List*",
```

```
                "tag:Get*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

3) Edit the trust relationship to be the following:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::XXXXXXXXXXXXXXX:role/<Opsalert-role-attached-to-instance>",
    "Service": "ec2.amazonaws.com"
   },
   "Action": "sts:AssumeRole"
  }
 ]
```



NOTE: - xxx = account number where the Opsalert instance is deployed in

Follow these steps on Instance:

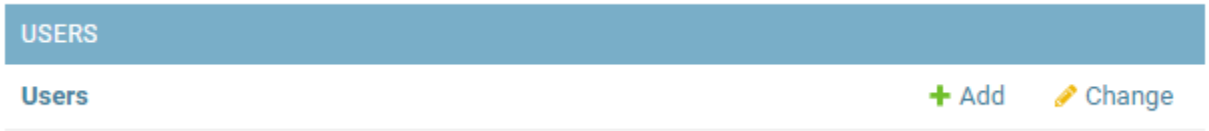
1) SSH in to OpsAlert instance.
2) Change directory to /opt/opsalert/opsalert-shell
3) Edit accounts.csv file and update the account information as per the example and remove unwanted lines.
   Use this line as an example:
   ▪ **ACCOUNT1,xxxxxxxxxxxxxxxx,arn:aws:iam:: xxxxxxxxxxxxxxx:role/stackarmor-opsalert**

   Where:
   ACCOUNT1 = Name of the account on OA admin Panel
   xxxxxxxxxxxxxxx = AWS Account number where the opsalert role is
   arn:aws:iam:: xxxxxxxxxxxxxxx:role/stackarmor-opsalert = Role ARN of above created OpsAert IAM Role

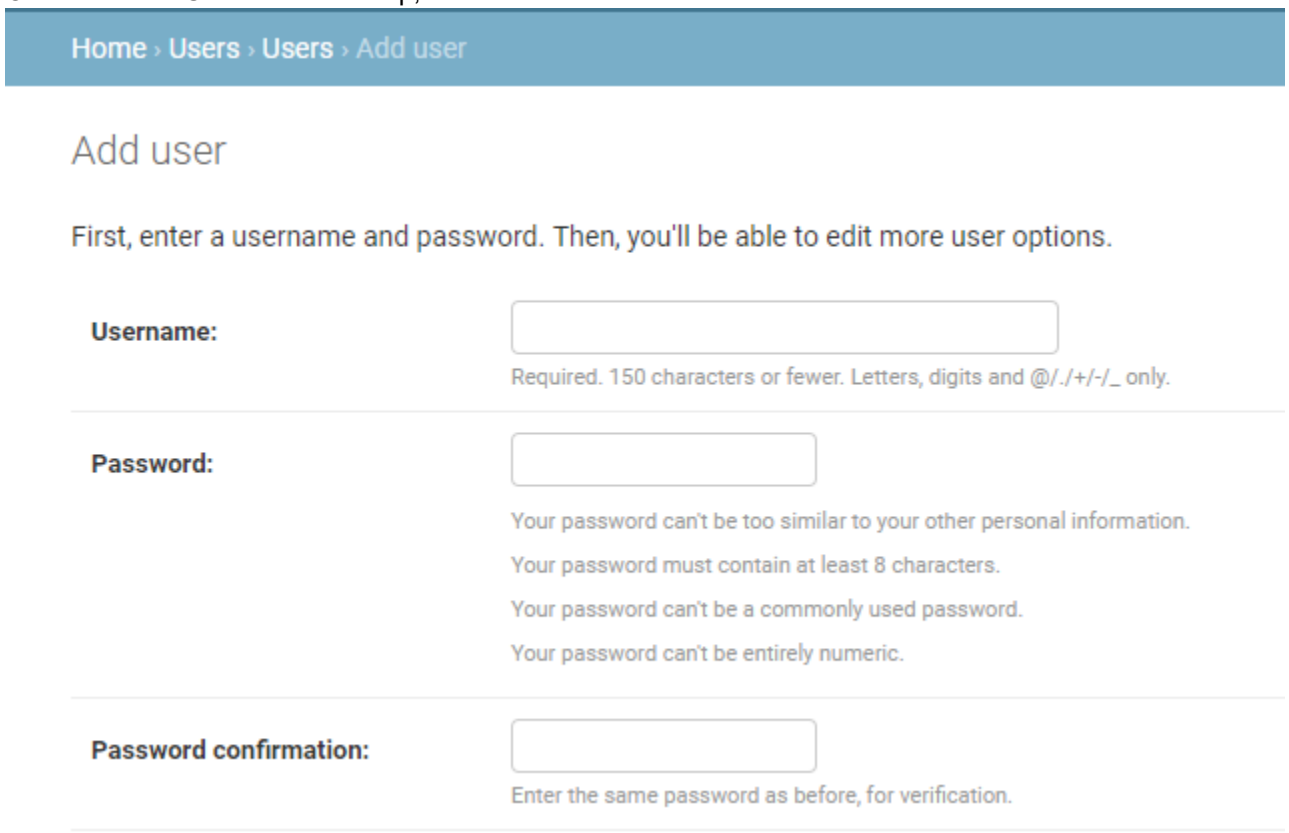
4 Adding Users to Opsalert

1) Log into Opsalert Admin Panel.

2) Under Site Administration, go to users and click on Add user.



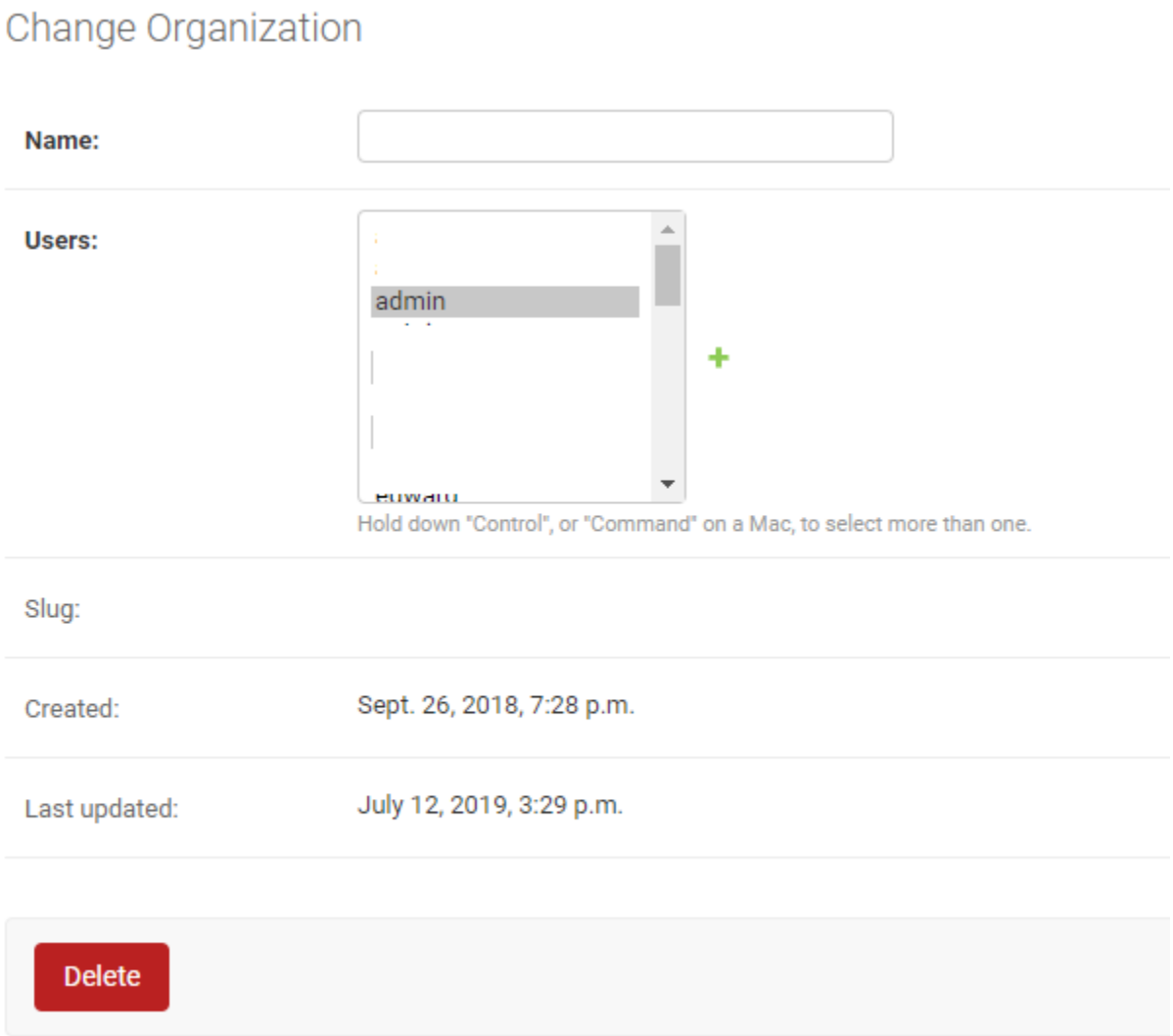
3) Once the “Add User” tab shows up, add the user information.



By default, new users don’t have any organization access. To give them the organization access. Follow these steps.

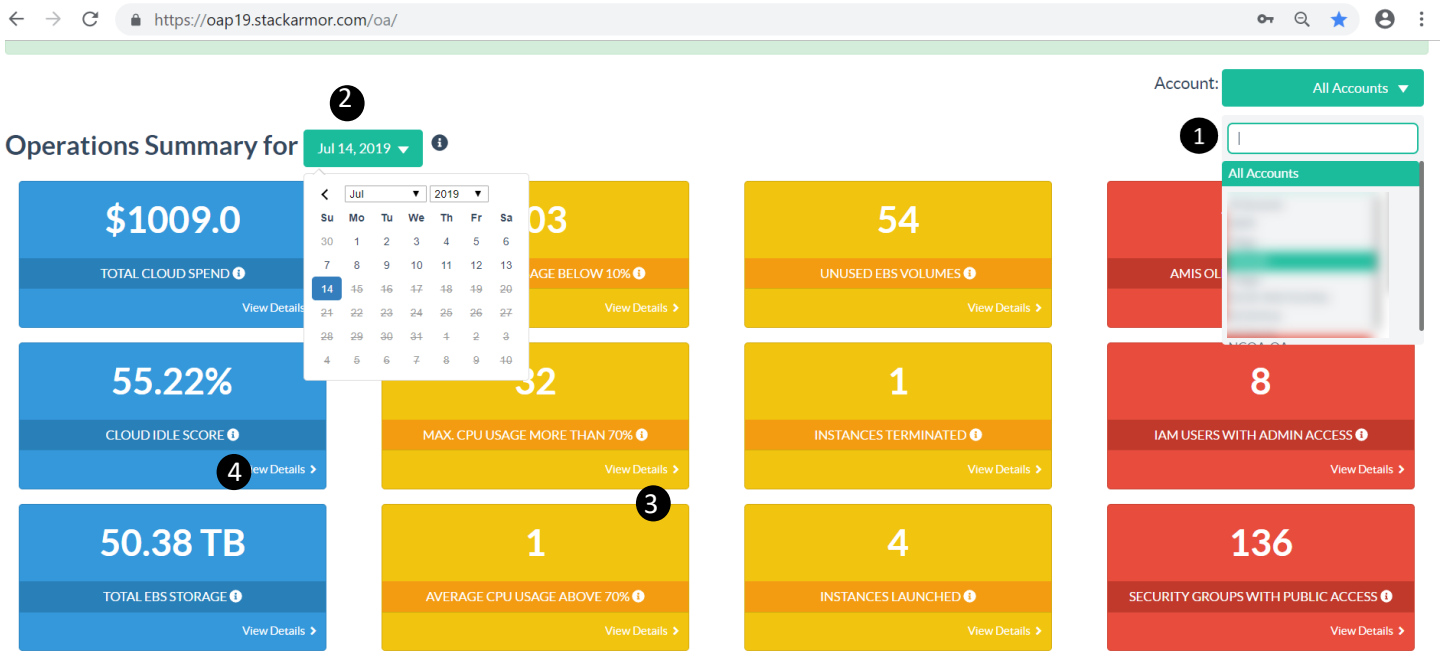
1) Click on “Organizations” under Site Administration.
2) Select the organizations from the list you want the new user to be a part off.

3) Once on “Change Organization” tab, select the user you created to give that user that specific organization access.



5 OpsAlert Dashboard

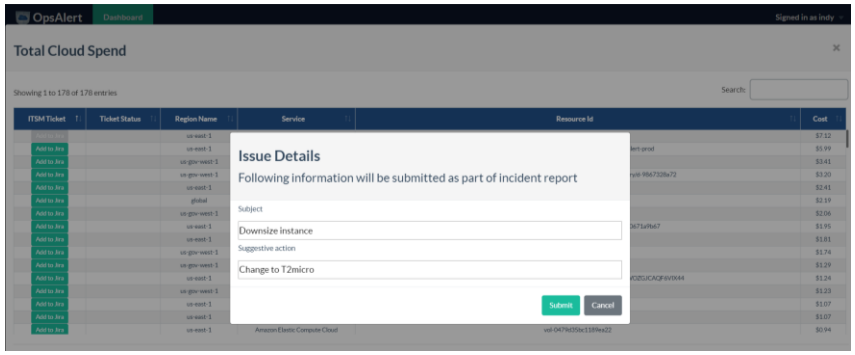
OpsAlert Dashboard provides an overview of key cloud operational data including cost, utilization and critical security systems information. It tracks 12 key business metrics that are essential for effective AWS cloud management. The dashboard provides the data for a selected date, or by default the data representative of past 24 hours.



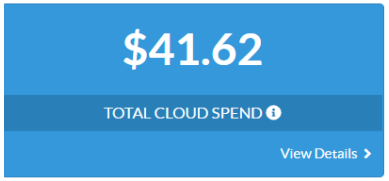
1. **Account** – Select an account from the dropdown. This is a multi-account dashboard and provides the ability to manage multiple accounts through a single login.

2. **Operations summary for** selected date – Select date from the calendar to view operational summary data for selected date and account.
3. **View Details** – Select **View Details** to find an in-depth tabular representation of the business metrics.
4. **Tooltip** – View ⓘ for metric description.

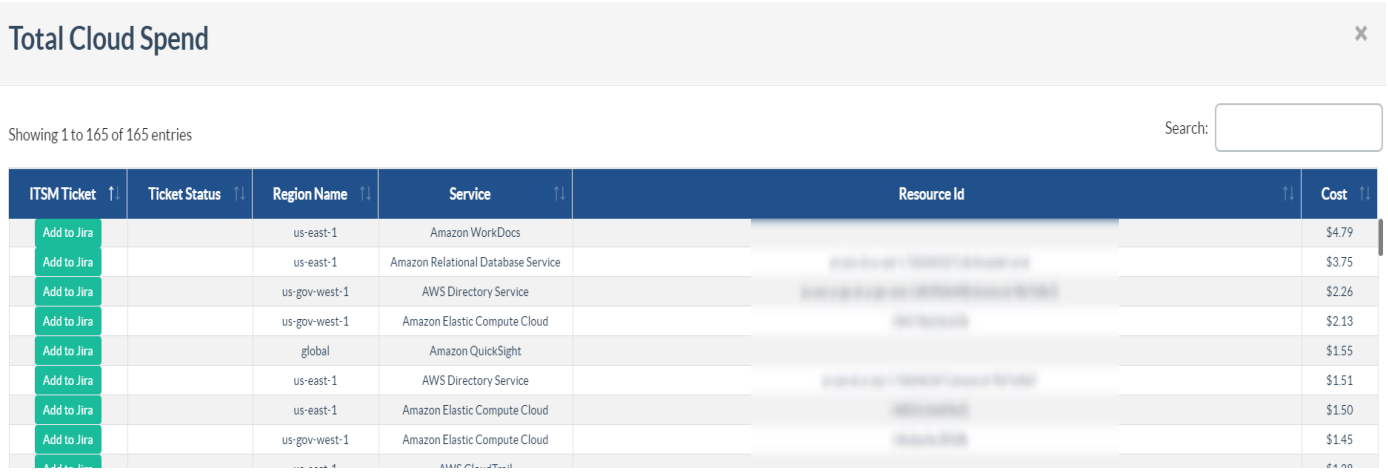
Note: Jira/ Service now integration – OpsAlert dashboard is integrated with Jira/ServiceNow for assigning tasks to the stackArmor IT Support Team and ensure quick remediation and drives accountability.



5.1 Total Cloud Spend



Total Cloud Spend is calculated from AWS cost and usage reports in the last 24 hours. This data is open to change till final invoice is created. In the table below, view the breakdown of the Cloud Spend per **Service**, **Region** and **Resource ID** and sort to the highlight the cost and get a quick overview of the services cost across region.



Total Cloud Spend

Showing 1 to 165 of 165 entries

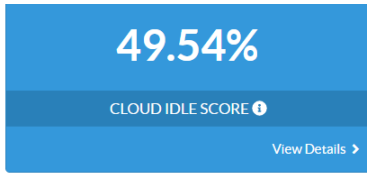
Search:

ITSM Ticket	Ticket Status	Region Name	Service	Resource Id	Cost
Add to Jira		us-east-1	Amazon WorkDocs		$4.79
Add to Jira		us-east-1	Amazon Relational Database Service		$3.75
Add to Jira		us-gov-west-1	AWS Directory Service		$2.26
Add to Jira		us-gov-west-1	Amazon Elastic Compute Cloud		$2.13
Add to Jira		global	Amazon QuickSight		$1.55
Add to Jira		us-east-1	AWS Directory Service		$1.51
Add to Jira		us-east-1	Amazon Elastic Compute Cloud		$1.50
Add to Jira		us-gov-west-1	Amazon Elastic Compute Cloud		$1.45

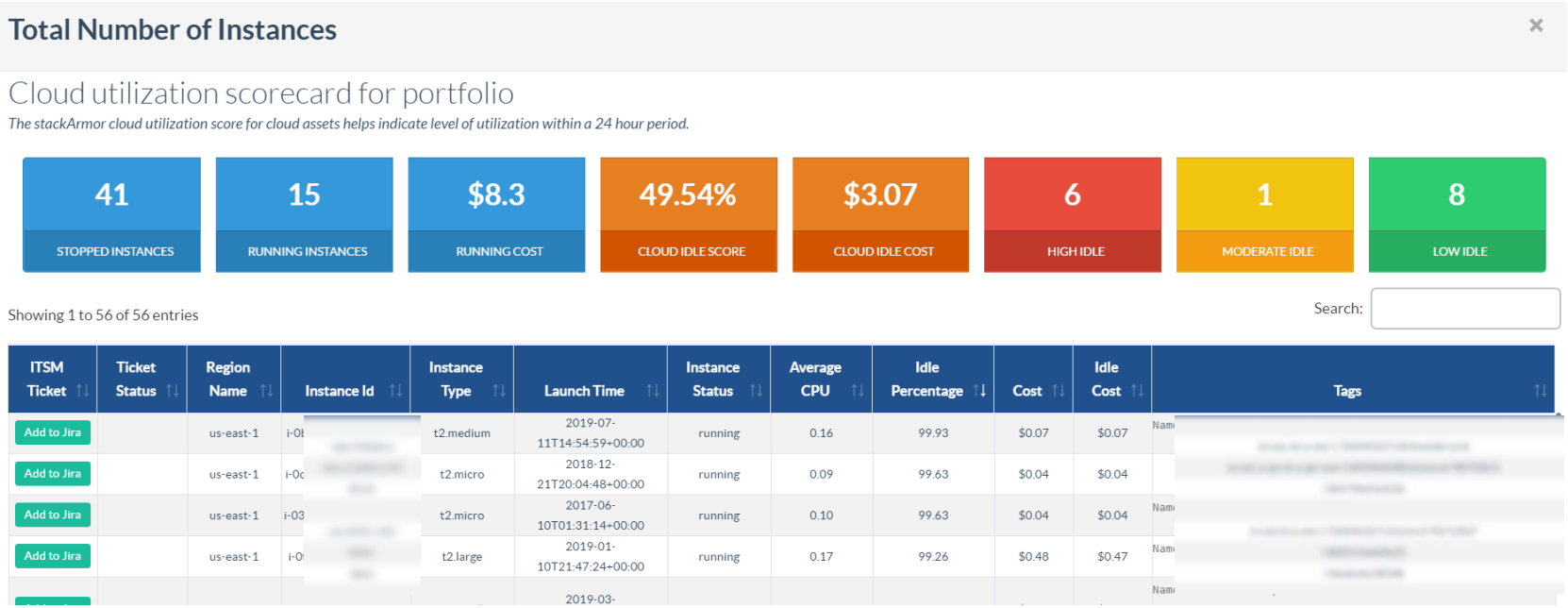
Recommendations:

- Monitor sudden jump in **Total Cloud Spend**. Sort for services that were added recently contributing to the increase.
- Sort to identify resources that are not being utilized and contributing to cost. For e.g. If Amazon WorkDocs is not being used, replace with S3 bucket for storage and cost optimization.
- Leverage customized reporting suggestions provided by stackArmor IT Support Team.
- Raise a ticket for recommendations from stackArmor IT Support staff.

5.2 Cloud Idle Score



1. **Cloud Utilization scorecard** for portfolio – Helps indicate level of cloud utilization in a 24-hour period.
2. **Total number of instances** – Provides list of all instances along with **Instance ID**, **Type**, **Launch Time**, **Status** running in the selected account for the specified date along with cost.



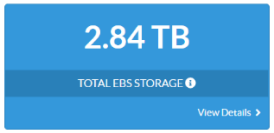
Cloud utilization scorecard for portfolio:

- **Running cost** – Total cost of running the instances.
- **Cloud Idle Score** – It is the overall average idle score of all instances. Represents cloud idle capacity that is being paid for but not utilized. This is calculated by averaging the computed idle score of each of the EC2 and RDS instances.
- **Cloud Idle Cost** – Cumulative idle cost of each of the EC2 and RDS instances. Idle cost of instance = instance idle score *instance usage cost.
- **High Idle** denotes the instances that are idle 90% of the time.
- **Moderate Idle** applies to instances idling between 70-90% of the time
- **Low Idle** instances are idle less than 70 % of the time or being utilized 70% of the time.

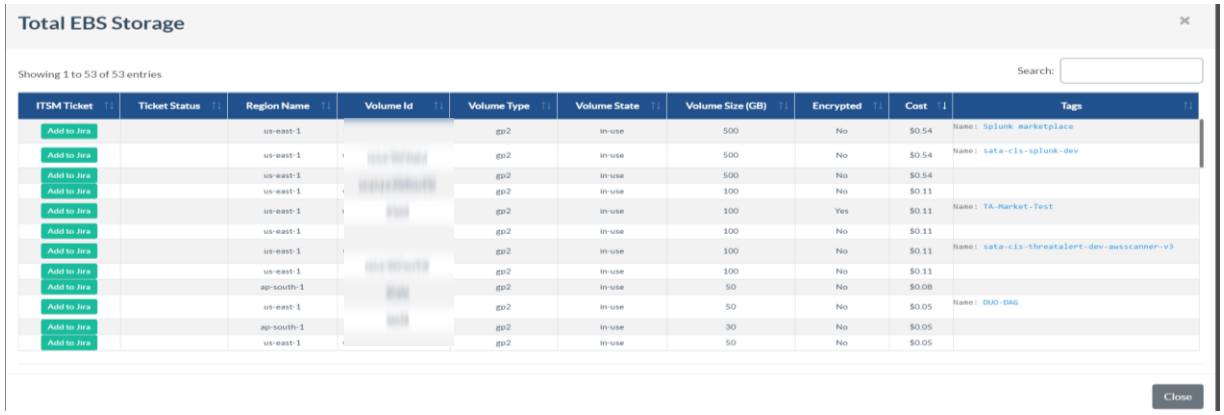
Recommendations:

- Identify idle instances and detect cost wastage. Determine need of the instance based on tagging and utilization and take informed decision towards a cost effective, better utilized cloud. E.g. As per the screenshot review the 6 instances that are High Idle, their utilization and costs incurred. Based on the review, you can either downsize or stop the instances.
- Ensure operational efficiency by tagging the instances. Use **Search** to identify **Test** instances that are not being used but incurring costs.
- Raise a ticket for recommendations from stackArmor IT Support staff.

5.3 Total EBS Storage



Total EBS storage allocated to all AWS resources. See the breakdown of the EBS Volume by **Volume ID**, **Type**, **State**, **Size** and **Encryption** status. You can sort to identify the highest spend by Volume.



Total EBS Storage

Showing 1 to 53 of 53 entries

Search:

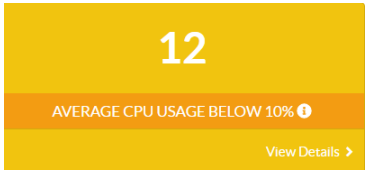
ITSM Ticket	Ticket Status	Region Name	Volume Id	Volume Type	Volume State	Volume Size (GB)	Encrypted	Cost	Tags
Add to Jira		us-east-1	[redacted]	gp2	in-use	500	No	$0.54	Name: Splunk marketplace
Add to Jira		us-east-1	[redacted]	gp2	in-use	500	No	$0.54	Name: sata-cis-splunk-dev
Add to Jira		us-east-1	[redacted]	gp2	in-use	500	No	$0.54	
Add to Jira		us-east-1	[redacted]	gp2	in-use	100	No	$0.11	
Add to Jira		us-east-1	[redacted]	gp2	in-use	100	Yes	$0.11	Name: TA-Market-Test
Add to Jira		us-east-1	[redacted]	gp2	in-use	100	No	$0.11	
Add to Jira		us-east-1	[redacted]	gp2	in-use	100	No	$0.11	Name: sata-cis-threatalert-dev-awsscanner-v3
Add to Jira		us-east-1	[redacted]	gp2	in-use	100	No	$0.11	
Add to Jira		ap-south-1	[redacted]	gp2	in-use	50	No	$0.08	
Add to Jira		us-east-1	[redacted]	gp2	in-use	50	No	$0.05	Name: DUO-DAG
Add to Jira		ap-south-1	[redacted]	gp2	in-use	30	No	$0.05	
Add to Jira		us-east-1	[redacted]	gp2	in-use	50	No	$0.05	

Close

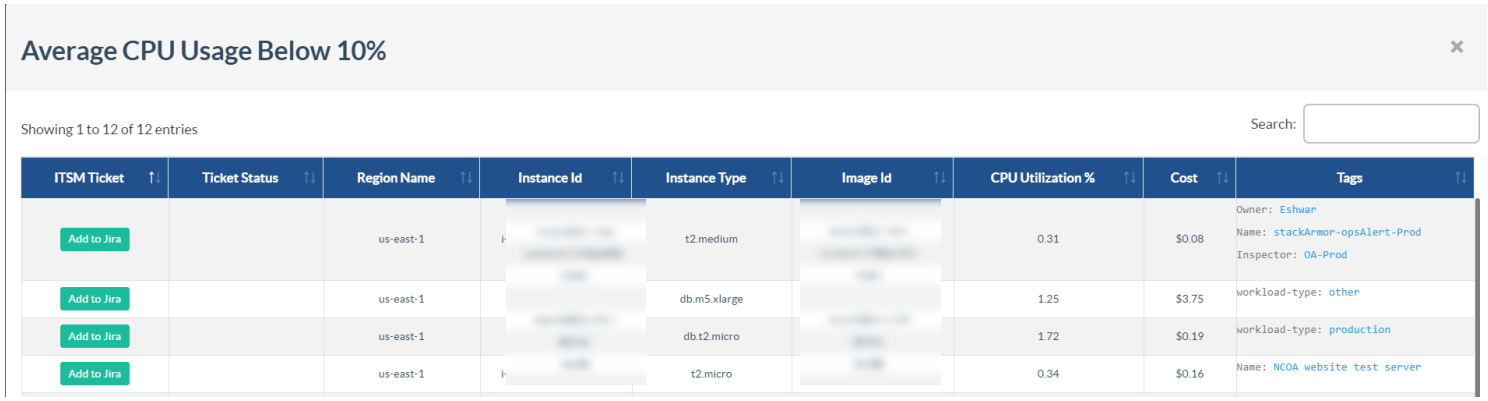
Recommendations:

- If any of the production instances are not encrypted, it raises a security concern. Raise a Jira Ticket to address this.
- Tag untagged EBS volumes for operational efficiency and enable easier management oversight.
- If the Volume Status = available, it indicates that the EBS volume is not being utilized and incurring extra costs. (stackArmor also tracks Unused EBS Volumes which is discussed later in the document)
- Raise a Ticket for recommendations from stackArmor IT Support staff.

5.4 Average CPU Usage below 10%



Average CPU Usage below 10% gives the count of instances with average CPU Utilization below 10%. Review the list to see if these instances can be downsized to save costs. Sort to track the Highest spend and take necessary action.



Average CPU Usage Below 10%

Showing 1 to 12 of 12 entries

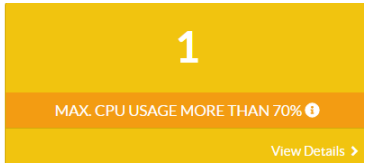
Search:

ITSM Ticket	Ticket Status	Region Name	Instance Id	Instance Type	Image Id	CPU Utilization %	Cost	Tags
Add to Jira		us-east-1		t2.medium		0.31	$0.08	Owner: Eshwar Name: stackArmor-opsAlert-Prod Inspector: OA-Prod
Add to Jira		us-east-1		db.m5.xlarge		1.25	$3.75	workload-type: other
Add to Jira		us-east-1		db.t2.micro		1.72	$0.19	workload-type: production
Add to Jira		us-east-1		t2.micro		0.34	$0.16	Name: NCOA website test server

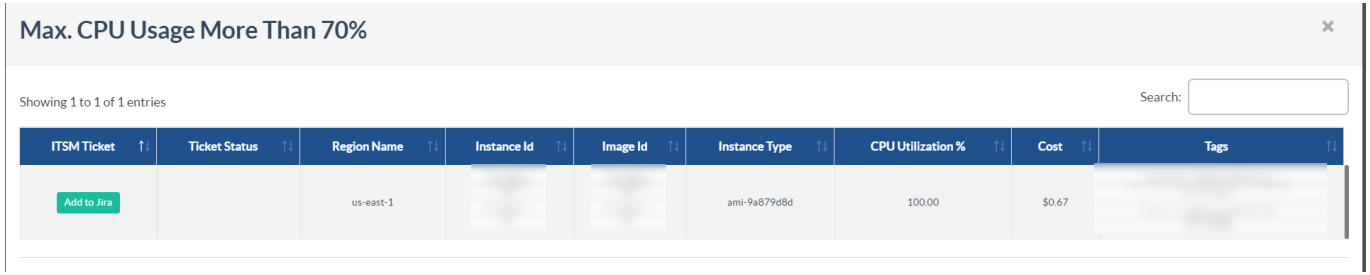
Recommendations:

- Review instance type, tags and establish the need for the instance
- Downsize or stop the instance based on utilization
- Raise a Ticket for recommendations from stackArmor IT Support staff.

5.5 Max CPU Usage above 70%



Count of instance with maximum CPU utilization above 70%. Highlights the instance that is overutilized and the need to investigate further.



Recommendations:

- Review to see whether more instances need to be allocated for load balancing
- Probe for any unusual activity. Ascertain whether any service is running in the background without your knowledge.
- Upsize Instance.
- If the CPU Utilization percentage reaches 100% then the system might become unresponsive.

5.6 Avg CPU Usage above 70%

Average CPU Usage above 70% provides the count of instances with average CPU Utilization above 70%.

Recommendations:

- Review to see whether more instances need to be allocated for load balancing or upsize instance.
- Probe for any unusual activity.

5.7 Unused EBS Volumes

EBS storage allocated but not attached to any AWS resources.

Showing 1 to 3 of 3 entries

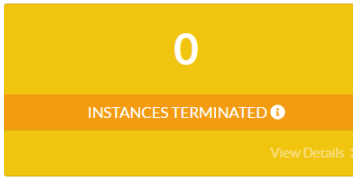
Search:

ITSM Ticket	Ticket Status	Region Name	Volume Id	Volume Type	Volume Size (GB)	Encrypted	Tags
—		us-east-1	[redacted]	gp2	available	Yes	
—		us-east-1	[redacted]	gp2	available	Yes	
—		us-east-1	[redacted]	gp2	available	Yes	

Recommendations:

- Delete Unused EBS Volumes. Review the list as part of regular cleanup operations and reduce unwanted costs.

5.8 Instances Terminated



Provides list of all instances terminated in the last 24 hours for the selected date.

Showing 1 to 1 of 1 entries

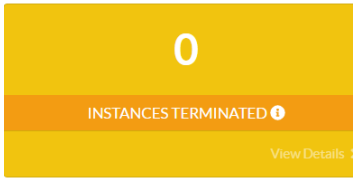
Search:

ITSM Ticket	Ticket Status	Region Name	Instance Id	Image Id	Launch Time	Termination Reason	Cost	Tags
[redacted]		us-east-1	i-0[redacted]	ami-[redacted]0	Jul 15, 2019, 4:51 PM	User initiated (2019-07-15 21:49:31 GMT)	-	Name: Indiggo_Outlook_Build_Slave Purpose: Jenkins

Recommendations:

- From a security standpoint ensure that instances were not terminated by mistake.

5.9 Instances Launched



Provides list of all instances (ID, Region Name, Instance Type, Image ID, Launch Time, security groups, tags) launched in the last 24 hours of the selected date along with the associated costs.

Recommendations:

- Corelate jump in cost to new instances launched.
- Monitor security groups to ensure data security.

5.10 AMIs Older Than 30 days

Provides the count of AMIS discovered on AWS created older than 30 days from the selected date. This helps to keep up with the organizations DLP policy. This helps to reduce storage cost by deleting outdated backups. This number should be less, as it ads to the billing expenses.

AMIs Older Than 30 Days

Showing 1 to 26 of 26 entries

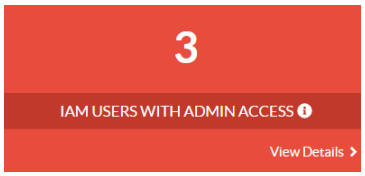
Search:

ITSM Ticket	Ticket Status	Region Name	Image Id	Platform	Description	Architecture	Creation Date	Tags
Add to Jira		us-west-1			FedoraOpenShift	x86_64	2/11/2017, 11:18 PM	
Add to Jira		ap-southeast-2			tesy	x86_64	7/4/2018, 5:17 AM	
Add to Jira		us-east-1	a		Backup prior to upgrade	x86_64	8/24/2018, 8:50 AM	
Add to Jira		us-east-1	a		threatalert-27thAug	x86_64	8/27/2018, 9:06 AM	
Add to Jira		us-east-1	a		threatalert-dev-msa-awsscanner-test-3.1	x86_64	9/12/2018, 2:24 PM	
Add to Jira		us-east-1	a		sata-cis-splunk-dev	x86_64	9/12/2018, 2:25 PM	
Add to Jira		us-east-1	a		Secondry Node 0 for west	x86_64	9/21/2018, 2:39 PM	

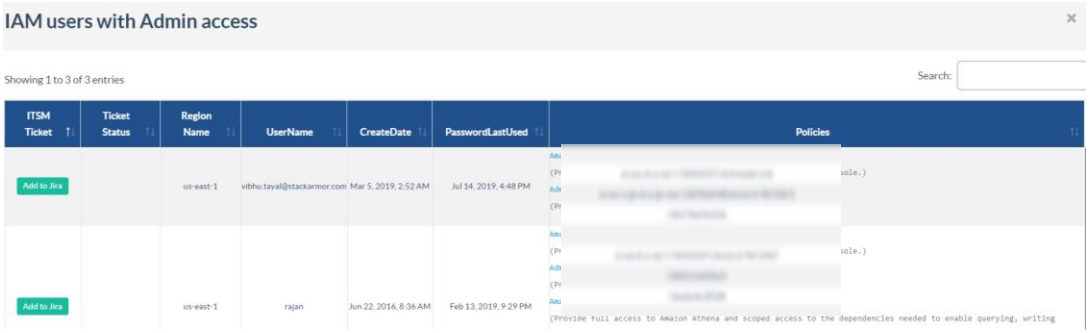
Recommendations:

- Reduce storage costs by deleting outdated backups.
- Raise a ticket with stackArmor IT support to ensure this periodical clean up activity and take a step ahead to better managed AWS cloud.

5.11 IAM users with admin access



Provides a list of IAM users with admin privileges.



Recommendations:

- From a security standpoint ensure that the right set of people have admin access. If the user count increases, probe the user credentials further.

5.12 Security groups with public access

Provides list of publicly accessible security groups with high risk configurations.

Recommendations:

- This helps protect your AWS account from a security perspective. Review the list and the security port details to ensure that only groups that should have public access are listed.
- Raise a ticket to with stackArmor IT support if you see a discrepancy.

6 Cost and Idle Trends

The trends above help provide a quick overview of cloud health from a cost, operational efficiency and utilization perspective. A time frame such as a quarter can be selected to understand the trend in Cloud Spend, Idle Score, Total instance count and Total EBS storage. A spike or dip should be backed up by an informed rationale, for e.g. new instances launched, instances terminated, new services launched.

6.1 Total Cloud Spend

In the screenshot there is spike for the selected time period, a spike can be seen in Total Cloud Spend in the beginning of the month for both June and July. In turn probe the reason for the spike and ascertain whether those cloud costs can be minimized. In this scenario the cloud cost was contributed by the onetime payment for reserved instances, workspace, business support, service catalogue, tax etc.

6.2 Overall Cloud Idle score

It is generally a good practice to have a Cloud Idle Score between 20- 30%. If this shoots up to 50 or more, monitor the change in the environment to ensure optimum cloud utilization and eliminate cost wastage.

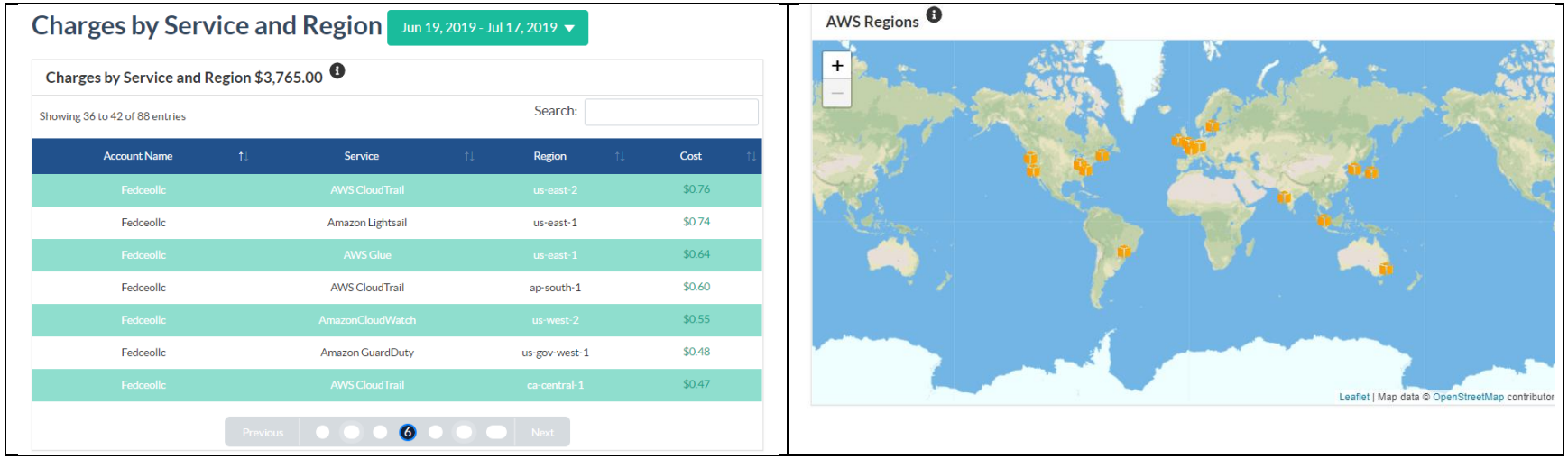
6.3 Total Instance Count

The Total Instance Count trend in most cases has a correlation with the cloud spend with exceptions. Monitor sudden dip or spike in instances and be informed for the reason. If instances were spun up by mistake, take the required actions to shut them to avoid extra costs.

6.4 Total EBS Storage

Investigate the reason for the spike in EBS Storage. In the scenario above, the spikes are representative of a one-off anomaly in the data it represents. The spike did not contribute to additional costs.

7 Charges by Service and Region



Account Name	Service	Region	Cost
Fedceollc	AWS CloudTrail	us-east-2	$0.76
Fedceollc	Amazon Lightsail	us-east-1	$0.74
Fedceollc	AWS Glue	us-east-1	$0.64
Fedceollc	AWS CloudTrail	ap-south-1	$0.60
Fedceollc	AmazonCloudWatch	us-west-2	$0.55
Fedceollc	Amazon GuardDuty	us-gov-west-1	$0.48
Fedceollc	AWS CloudTrail	ca-central-1	$0.47

The table above is very helpful for reporting purposes. Both the visualizations complement each other, as one provides data and the other provides a visual overview of services spun up in regions contributing towards over all costs. Monitoring this is also important from an operational and security standpoint.

- The total cost by service and region for the period selected is $3765
- Provides the summary of AWS charges by service and region.
- Click on the cost to see the breakup of the cost by usage.
- The geographical visualization provides a quick overview of services across regions. Hover over the region icon to display top 5 contributing services for the region.

Please reach out to solutions@stackarmor.com for any queries.