Managing an Amazon Web Services environment

To reduce the expenses of buying, owning, and maintaining physical data centers and servers, your organization has converted most of its infrastructure to cloud infrastructure on Amazon Web Services. This means you have whole new data types to secure and monitor. You need to learn the new services and the metrics that help you run your applications in the AWS cloud efficiently. You want to use Splunk software to manage all the different components of Amazon Web Services, including elastic cloud compute instances, elastic load balancer instances, virtual private clouds, and elastic block store volumes. You also plan to monitor user behavior on these systems.

Data required

- AWS EC2 data
- AWS description data
- VPC Flow
- Cloudtrail

How to use Splunk software for this use case

You can run many searches with Splunk software to maintain your AWS environment. Depending on what information you have available, you might find it useful to identify some or all of the following.

Elastic Cloud Compute (EC2)

- Current AWS elastic compute cloud instances
- CPU utilization of Elastic Compute Cloud (EC2) instances
- Unused Elastic IPs with no attached instances
- AWS Elastic Compute Cloud (EC2) monitoring using Splunk Infrastructure Monitoring

Elastic Load Balancers

- Current AWS elastic load balancer instances
- Health of AWS elastic load balancers

Elastic Block Store (EBS)

- Current AWS elastic block store volumes
- Unattached AWS elastic block store volumes
- AWS EBS volumes without a current snapshot

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Simple Storage Service (S3)

- Public S3 bucket identification
- Geographic access to AWS S3 Buckets

Lambda

- Critical AWS Lambda metrics
- Logging output from AWS Lambda functions

Infrastructure

- Current AWS virtual private cloud infrastructure
- Changes made to AWS cloud infrastructure
- Health of critical AWS infrastructure from CloudWatch metrics

Additional

- Users who haven’t accessed AWS for an extended time
- Resources with non-compliant AWS configuration rules
- Logging output from AWS Cloudwatch
- Disabled AWS CloudTrail logging
- Missing AWS resource tags
- Common AWS resource tags and tag values

Next steps

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Number of deprovisioned resources that are found to be idle
- Cost savings from deprovisioning and optimization
- Mean time to problem resolution

You may also want to look at the following processes in your organization that commonly impact success with this use case:

- Capacity planning and resource optimization to keep operating expenses as low as possible
- Provisioning and automation groups using orchestrators such as Kubernetes, Ansible, Puppet, and AWS CloudFormation
- Security and compliance will consume and compliment data within this use case.

This use case is also included in the IT Essentials Work app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand
and implement this use case:

- Blog: [Six top metrics to monitor in AWS EBS](#)
- Blog: [12 top things to monitor in Amazon EC2](#)
- Conf Talk: [Capacity planning and cost containment with AWS](#)
- Conf Talk: [How to save money monitoring, managing, and securing your cloud using the Splunk App for AWS](#)
- White Paper: [Getting Data Into (GDI) Splunk from AWS](#)
- Tool: [Splunk AWS Project Trumpet](#)
- App: [Splunk App for AWS](#)