splunk> insights for AWS Cloud Monitoring

GETTING STARTED GUIDE

GETTING STARTED WITH SPLUNK INSIGHTS FOR AWS CLOUD MONITORING

Organizations of all sizes are moving their applications to the cloud to help them achieve their business and technology goals, while reducing both capital and operational costs. And for good reason too: cloud services provide compute power on an as-needed basis, with the ability to manage resources programmatically. The underlying hardware is managed by the cloud provider, reducing overhead and increasing speed to market.

The benefits of cloud services are huge, but they still present some challenges. While the hardware no longer requires active management, you still need to monitor resource utilization and troubleshoot the problems that come up. You may still have infrastructure in a datacenter, and you need to see all that data in a single place, rather than spread across multiple portals and tools. These hybrid environments add complexity to your infrastructure, and it can be hard to correlate data from the cloud with the data from the rest of your environment.

But for true cloud monitoring and troubleshooting, you need to be able to search and correlate the data from all your infrastructure. You need to get up and running quickly, and you want a proven solution that will scale as your business grows. Splunk Insights for AWS Cloud Monitoring can help with all of this—continue reading to learn how to use this solution to troubleshoot and monitor your AWS cloud infrastructure.

Getting Started

Getting started with Splunk Insights for AWS Cloud Monitoring is easy – just search for “Splunk” in the AWS Marketplace and choose the AMI. Some useful information on choosing an EC2 instance type and storage size can be found in Deploying Splunk Enterprise on Amazon Web Services. Once your instance is up and running, you can connect to it via the web interface on its public DNS using port 8000. Your default password will be the same as the instance ID.

When you log in to your instance, you’ll be taken directly to the Splunk App for AWS, but there will be no data until you configure roles and access to the required data sources.

Three options are available to configure the right IAM policies required for the data collection:

1. **EC2 Role (more secure):** attach an EC2 role to the AWS EC2 instance AMI – Splunk Insights for AWS Cloud Monitoring.
2. **IAM AssumeRole (more secure):** grant a primary AWS account access to collect data from multiple sub-accounts using AssumeRole API. (Learn more about configuration details.)
3. **IAM Access Key (less secure):** enter an AWS user Secret Key ID and Secret Key as a new account in Splunk AWS Add-on.

Learn more about available configurations.

DATA TYPE	WHAT IT CAN TELL YOU
Config	Configuration snapshots, historical configuration information and change notifications can show when changes were made—which can be valuable when troubleshooting
Config Rules	Config rules data give you information on status and compliance
Inspector	Data from the Amazon Inspector service can give you valuable security information about your AWS-hosted application
CloudTrail	The AWS CloudTrail service provides a record of management and change events
CloudWatch Logs	VPC logs available from the AWS CloudWatch Logs service capture IP traffic flow data for the network interfaces in your account
CloudWatch	Performance and billing metrics are available from the AWS CloudWatch service
Billing	Your configured billing reports, including historical bills and capacity planning information
S3	Log data that is sent to S3 from AWS services, access logs for S3, CloudFront and ELB services and CloudTrail data
Kinesis	Streaming data via AWS Kinesis
SQS	Message queues

Configure an EC2 Role

- This is the preferred option for organizations that have tight security controls and do not give out access keys.
- There is no direct access for IAM users or alternatively there is a disabled AssumeRole for IAM users.
- Credentials are managed by assigning them to instances via IAM AssumeRole.

Step-by-step process (all steps from the AWS Console):

1. Create a new AWS IAM Policy – Splunk Access IAM Policy
    a. From the AWS IAM service, click **Policies**
    b. Click **Create policy**
    c. Select the **JSON** tab
    d. Enter the required permissions (Learn more about configuring permissions.)
    e. Click **Review policy**
    f. Enter name (e.g., SplunkAccess)
    g. Click **Create policy**

2. Create a new EC2 role
    a. From the AWS IAM service, click **Roles**
    b. Click **Create role**
    c. Under AWS Service, select **EC2**
    d. Select **Next: Permissions**
    e. Search for the new policy name created in Step 1 (e.g., SplunkAccess)
    f. Select the policy
    g. Click **Next: Review**
    h. Enter a role name (e.g., splunkEC2role)
    i. Click **Create role**

3. Attach a new IAM role to an EC2 instance
    a. In your AWS Console, select the EC2 instance running Splunk Insights for AWS Cloud Monitoring
    b. Click **Actions → Instance Settings → Attach/Replace IAM Role**
    c. Select the EC2 role created in Step 2 above (e.g., splunkEC2role)

Result: The Splunk AWS Add-on will auto-discover this role and grant access to the AWS services.

Configure an IAM AssumeRole

1. Create a new AWS IAM AssumeRole from the sub-account
    a. From the AWS IAM service, click **Roles**
    b. Click **Create role**
    c. Select **Another AWS account**
    d. Enter the primary AWS account under the Account ID*
    e. Click **Next: Permissions**
    f. Select the SplunkAccess policy. (See Step 1 in section “Configure EC2 Role (more secure)” above).
    g. Click **Next: Review**
    h. Set the Role name (e.g., cross-account-splunk-access)
    i. Click Create role

2. Attach new IAM role to EC2 instance
    a. In your AWS Console, select the EC2 instance running Splunk Insights for AWS Cloud Monitoring
    b. Click **Actions → Instance Settings → Attach/Replace IAM Role**
    c. Select the AssumeRole created in Step 1 above (e.g., cross-account-splunk-access)

Result: The Splunk AWS Add-on will auto-discover this role and grant access to the AWS services.

Configure an IAM Access Key

1. From the Splunk App for AWS, click **Settings → Configure AWS Access** to be taken to the configuration screen.
2. Click the **Add** button to connect the app to your AWS account.
3. Create an IAM user on your AWS console that has sufficient permissions to access the data. Configure the logs (this means you may need to do some configuration of your AWS services to gather all of the data that you need – see the documentation for the Splunk App for AWS for details on these steps).
4. Enter an AWS Account Access Key ID and AWS Account Secret Access Key into the Add-on for AWS. If you have more than one account, you can add all of them so that you can see data from all of your accounts in Splunk.
5. Once you’ve set up at least one account, you can choose which data you want to bring into the Splunk platform.

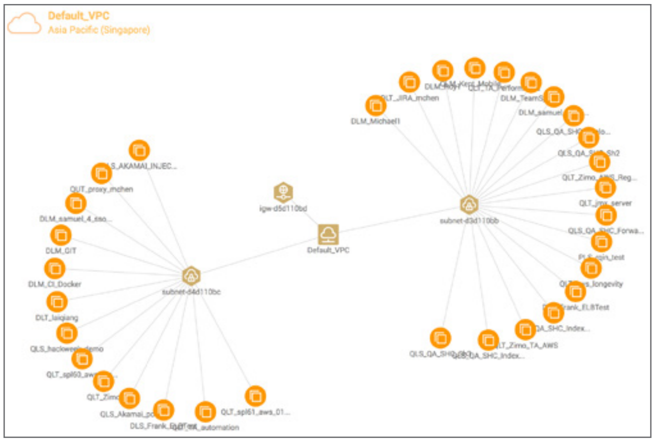


Figure 1: Topology Dashboard

The Secret Sauce Behind Splunk Insights: the Splunk App for AWS

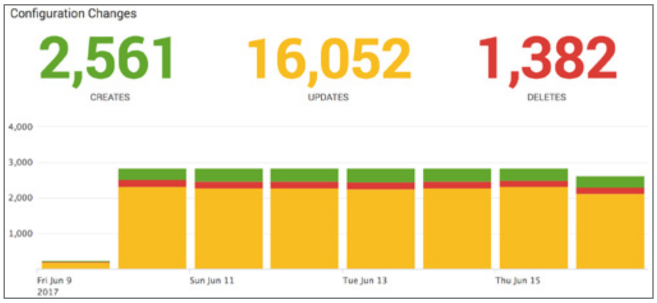
The Splunk App for AWS powers the insights behind Splunk Insights for AWS Cloud Monitoring and provides several dashboards to give you views into the performance, health, configuration, security and costs of your AWS environment. The Overview dashboards give you a high-level overview of your environment from different perspectives. The Topology view provides a dynamic map of your AWS resources and their relationships. The Timeline displays historical events chronologically. The Usage dashboards show your usage of various AWS services, including EC2 instances, EBS volumes, ELB instances, RDS and Lambda. There are also dashboards for capacity planning or viewing your existing reserved instances and a planner to see if you could save money by replacing some of your on-demand instances with reserved instances. The Security dashboards show activities and analyses that might be impacting the security of your AWS environment. Billing dashboards provide a budget planner, current and historical billing data and projections for future billing, helping you track the financial benefits of migrating your application to AWS.

Using Splunk for Cloud Monitoring

The saved searches from the application are available in the Splunk App for AWS documentation, but some sample searches using AWS data types are listed below as examples to help you start exploring your AWS data in Splunk searches. You can use the app's saved searches or searches that you create to build custom dashboards so you can see data from your AWS instances and your datacenters in one place. This gives you the ability to compare performance and availability in different environments.

Sample Dashboard From the Splunk App for AWS

- **What?** Configuration Information and configuration change notifications
- **Why?** Tracking changes in your environment can be critical when troubleshooting
- **Sample Splunk Query:** sourcetype=”aws:config:notification” aws_account_id=”*” region=”*” | rename “configurationItemDiff.changeType” as “Change Type” | timechart count by “Change Type”


Configuration Changes

2,561 CREATES

16,052 UPDATES

1,382 DELETES

Figure 2: Configuration Change Panel of Overview Dashboard

Sample Dashboard From the Splunk App for AWS

- **What?** Metadata about your AWS environment
- **Why?** You can use this data to keep track of your environment
- **Sample Splunk Query:** sourcetype=”aws:description” aws_account_id=”*” region=”*” source=”*:ec2_instances” | dedup id | where state=”running” | stats count(id) by instance_type

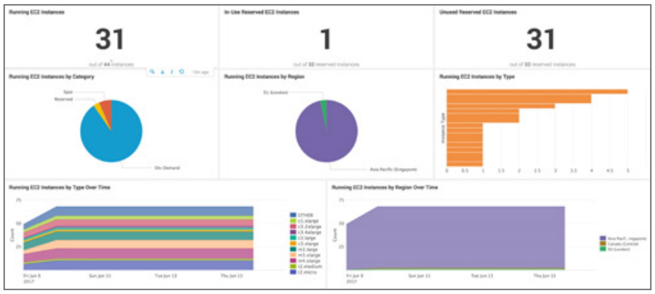


Figure 3: EC2 Instances Dashboard

Sample Dashboard from Splunk App for AWS

- **What?** CloudWatch performance metrics
- **Why?** To make sure that your resources are appropriately sized
- **Sample Splunk Query:** sourcetype=”aws:cloudwatch” eventtype=aws_cloudwatch_ec2_events aws_account_id=”*” region=”*” metric_name=CPUUtilization | timechart avg(Average) AS AverageCPU by InstanceId

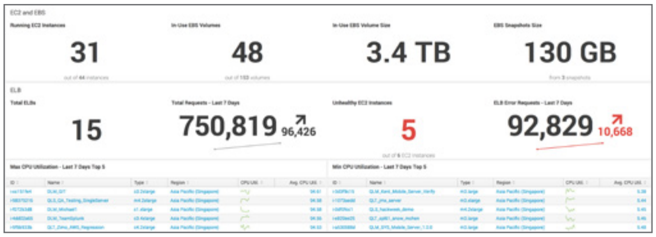


Figure 4: Usage Overview Dashboard

Sample Dashboard from Splunk App for AWS

- **What?** AWS billing data
- **Why?** To keep you on track with your cloud-related spending
- **Sample Splunk Query:** sourcetype=”aws:cloudwatch” source=”*:AWS/Billing” metric_dimensions=”*Currency=[USD]*” | dedup _time metric_dimensions aws_account_id | stats sum(Sum) as sum by _time aws_account_id metric_dimensions | rex field=metric_dimensions “ServiceName=\[(?<Service>.*?)\]” | eval day=strftime(‘_time’,”%Y/%m/%d”) | dedup day aws_account_id Service | timechart span=1d sum(sum) by aws_account_id

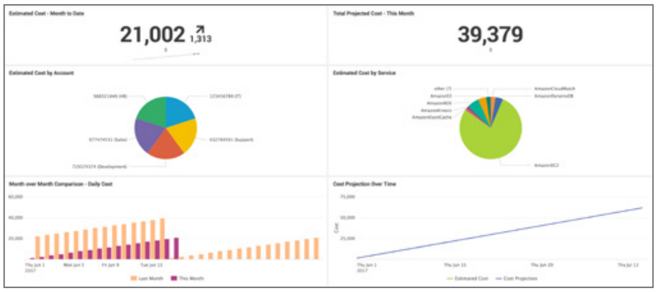

Estimated Cost - Month to Date
21,002
1,313
Total Projected Cost - This Month
39,379
Estimated Cost by Account
Estimated Cost by Service
AmazonCloudWatch
AmazonDynamoDB
AmazonEC2
Month over Month Comparison - Daily Cost
60,000
40,000
20,000
Last Month
This Month
Cost Projection Over Time
75,000
50,000
25,000
Cost
Estimated Cost
Cost Projection

Figure 5: Current Month Estimated Billing Dashboard

Summary

Splunk Insights for AWS Cloud Monitoring provides you with everything you need to get started monitoring your AWS environment quickly. Explore Splunkbase to find add-ons that you can use to bring other data into your Splunk instance. Build custom dashboards to help you correlate all your data in a single place, and gain insights into your whole environment, no matter where it lives.

Interested in trying Splunk Insights for AWS Cloud Monitoring for yourself?
Try a 15 Day Free Trial.

splunk> **Learn more:** www.splunk.com/asksales www.splunk.com