Splunk® App for AWS User Manual 5.1.0

Topology dashboard reference for the Splunk App for AWS

Generated: 2/09/2020 1:18 pm
Topography dashboard reference for the Splunk App for AWS

The Topology dashboard in the Splunk App for AWS displays the topology of your AWS resources and how they relate to each other. This dashboard relies on data from the AWS Config service, which is not available in GovCloud or China regions at this time.

**Note:** If your environment is complex, this dashboard may take several minutes to load.

**Use cases**

Use this dashboard to examine your resource usage to ensure you are following AWS best practices, maximizing efficiency, and minimizing cost. For example, this dashboard can help reveal:

- too many instances in a single VPC
- too many security groups
- security groups with few or no linked EC2 instances
- stopped instances with many attached EBS volumes
- whether EC2 instances are well secured in your private and public subnets
- whether autoscaling worked as expected
- CPU utilization and network traffic metrics layered over EC2 and EBS topology displays
- the relationships between your IAM users, groups, and policies

Toggle CPU Utilization, Network Traffic, Billing, and Amazon Inspector & Config Rules layers using the controls in the upper right corner of the dashboard to view these KPIs layered over your topology displays.

Review recommendations about security groups that you can delete or instances you should consider upgrading or downgrading based on usage. See Recommendations reference for the Splunk App for AWS.

Use the Topology Playback feature to review how your topology has changed over time.

You can also export the entire topology image to share offline.
**Data sources**

This dashboard relies on several data inputs and a saved search. In order to see your data, ask your admin to configure AWS Config, CloudTrail, CloudWatch, VPC Flow Logs, Billing, Amazon Inspector, and Config Rules inputs. When your inputs become active, the app automatically enables the Config: Topology Data Generator saved search, which supplies additional data specifically for this dashboard. The saved search is scheduled to run every twenty minutes, on the hour, twenty minutes past the hour, and forty minutes past the hour. Your admin can also trigger the saved search to run immediately from **Search > Reports** in the app.

In order to see data in the IAM layer, be sure to enable global resources for AWS Config in the AWS Management Console.

**Troubleshooting**

If you do not see the data that you expect in this dashboard, ask your admin to:

- check that the Config: Topology Data Generator saved search is enabled.
- trigger a new snapshot manually in the Configure tab, visible to admins.
- search for `sourcetype=aws:config` to ensure data is successfully reaching your Splunk platform

**Topology dashboard known behavior**

The number of EC2 instances may be different in other dashboards compared to the Topology dashboard. There are a few reasons this may occur:

1. The Topology dashboard uses the `aws:config` sourcetype to populate EC2 instances, and the Overview dashboards use the `aws:description` sourcetype. The `aws:config` sourcetype is region-specific, and provides events only when certain actions are performed on an EC2 instance. The `aws:description` sourcetype is region-independent, and provides the current status of an EC2 instance.

2. Dashboards that use the `aws:description` sourcetype track the status of EC2 instances, but it may not match EC2 instances in the Topology dashboard if the Config service or Config input in the Splunk Add-on for Amazon Web Services was disabled for a period of time.

3. If you start using the Splunk App for AWS, you do not receive events for previously-created EC2 instances with the `aws:config` sourcetype unless you perform any action in an EC2 instance from the AWS Management.
Console, whereas the `aws:description` sourcetype provides all the current EC2 instances you are running.