

Discontinuation notice: GorillaStack will be discontinued. [Please visit our SoftwareOne website](#)



Key CloudTrail Events To Monitor for Security in AWS

By | ⌚ 30 Oct 2017



CloudTrail is an amazing source of data, rich with API call history, allowing us to monitor who is attempting to do what within our AWS accounts.

However, it isn't all sunshine and rainbows. As every call is logged (including assumption of role, switching of roles, and even creation of a log stream), we end up with a lot of logging to digest.

Since we released our [Slack bot for CloudTrail events](#), in the over 400 Million CloudTrail events we have monitored, we have determined that users only want to be notified of 1 in 25,000 CloudTrail events. That is a really high signal to noise ratio!

We use cookies to improve your website experience. To find out more about the cookies we use, see our [Privacy Policy](#).

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.



ConsoleLogin

We’re starting with something basic here, but there is a reason for it. Almost every AWS user has an account where they don’t anticipate frequent login activity (production for example). Getting notified of access attempts to such black boxes can be advantageous.

StopLogging

StopLogging is an event type that comes from CloudTrail itself. Monitoring this event type can help you catch anyone deactivating CloudTrail logging, be that maliciously or otherwise.

CreateNetworkAclEntry, CreateRoute

These two VPC changes are worth monitoring. New ACL entries and routes in your route tables can expose new attack vectors to your infrastructure and are handy for your SecOps team to monitor.

AuthorizeSecurityGroupEgress, AuthorizeSecurityGroupIngress, RevokeSecurityGroupEgress, RevokeSecurityGroupIngress

Monitoring changes to Security Group ingress and egress settings is a powerful capability and is worth listening out for.

ApplySecurityGroupsToLoadBalancer, SetSecurityGroups

These are Elastic Load Balancers that are specific security group events and worth listening out for too. Here we monitor changes in which security groups are selected.

AuthorizeDBSecurityGroupIngress, CreateDBSecurityGroup, DeleteDBSecurityGroup, RevokeDBSecurityGroupIngress

These are the same as above, but of the RDS flavor and still worth monitoring, especially for internet facing RDS instances.

Don’t forget you can track all these events in Slack using our free [CloudTrail for Slack bot](#).

Next, we’ll dive deep into which [IAM CloudTrail events](#) SecOps teams should consider listening out for. You can also check out our [comprehensive list of CloudTrail events](#) to monitor.

If you’ll like to let us know what you think, reach out to us at [Slack](#).

Share [f](#) [t](#) [in](#) [p](#)

We use cookies to improve your website experience. To find out more about the cookies we use, see our [Privacy Policy](#).

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Cookies settings

Accept

Decline

Automate DevOps

- Cloud Optimization
- Real Time Events
- Backup and Disaster Recovery
- Book a Demo
- Try for Free

Support

- Documentation
- Changelog
- Open Source
- System Status
- Submit a Ticket

Resources

- Customer Stories
- Blog
- Templates
- Use Cases
- Join us on Slack

About GorillaStack

- Why GorillaStack?
- Press Releases
- Find Us at GitHub
- Partner with Us
- Contact Us



Advanced
Technology
Partner

Cloud Management
Tools Competency

Public Sector Partner

SaaS Partner



We use cookies to improve your website experience. To find out more about the cookies we use, see our [Privacy Policy](#).

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

[Cookies settings](#)

Accept

Decline