The Danger of Unused AWS Regions

By CloudSploit

Published: 2019-06-08 · Archived: 2026-04-05 18:41:26 UTC

Press enter or click to view image in full size

From: https://aws.amazon.com/about-aws/global-infrastructure/

I'll never forget one of the emails the we received in our support inbox at CloudSploit several months ago. An AWS user had emailed in desperation after finding over 50 EC2 instances running in the ap-northeast-1 region of his AWS account. He discovered these instances after his bill was thousands of dollars higher than the previous month. Based on the CPU utilization and some initial analysis, it appeared the instances were being used to mine Bitcoin 24/7.

While AWS ultimately refunded a large portion of his bill, the fact that someone had gained access to his account, deployed scores of resources, and racked up thousands of dollars in fees over the course of a month speaks strongly to the need for security monitoring in all AWS regions, not just the ones in active use. This is something CloudSploit stresses to its users when they ask if they can suppress our security scans in inactive regions.

Why Lock the Backdoor If You Never Use It?

If you have a security system for your home, would you only monitor the rooms you spend the most time in? Imagine not locking the back door because no one goes around that side of the house. If you've deployed security tools (even AWS's built-in tools like CloudTrail or ConfigService) only in the regions in which you have resources, you are failing to monitor perhaps the riskiest part of your infrastructure.

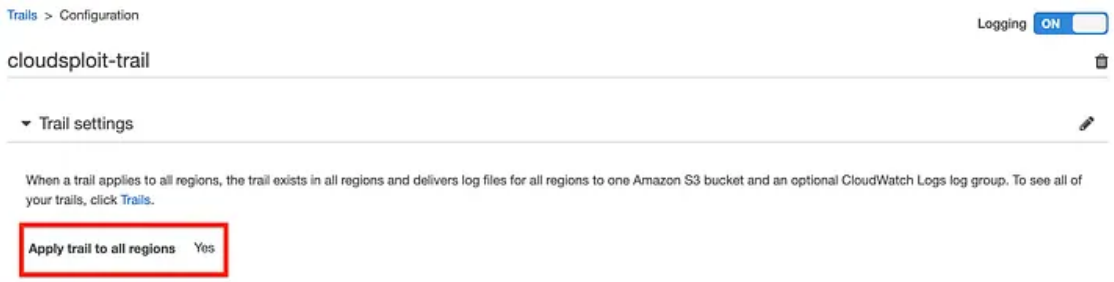
Get CloudSploit's stories in your inbox

This failure in security monitoring is something cloud attackers have been capitalizing on for years. If the goal is to remain undetected, what better way to do that than to deploy compromised resources in places where no one is looking? With a bit of careful capacity planning to avoid usage or billing spikes, an attacker could go undetected for months.

Monitoring Unused Regions with CloudTrail

Infrastructure and security teams have numerous ways to fight back. First and foremost, every security tool must be deployed in all regions, not just those that are in use. Fortunately, AWS provides easy configuration options to enable its built-in tools like CloudTrail to monitor all regions.

Press enter or click to view image in full size

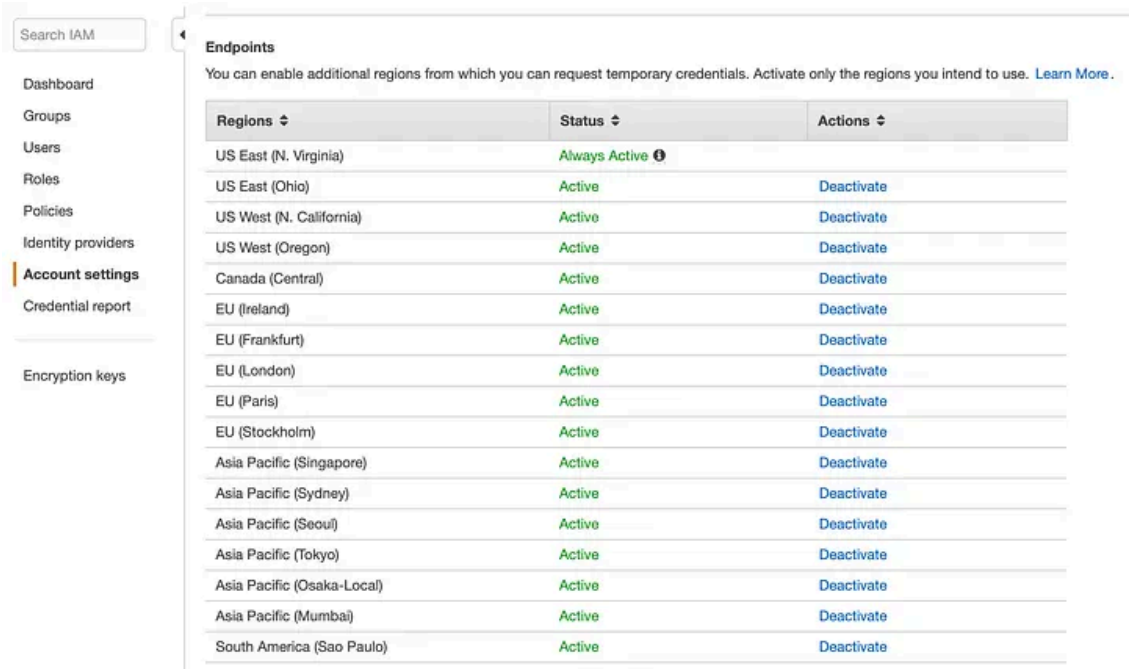


Enable CloudTrail in All AWS Regions

Deactivate Unused Region Endpoints

It’s a little-known and little-used setting, but AWS allows you to disable the ability for users to generate STS credentials in unused regions. This page is accessible from the IAM console.

Press enter or click to view image in full size

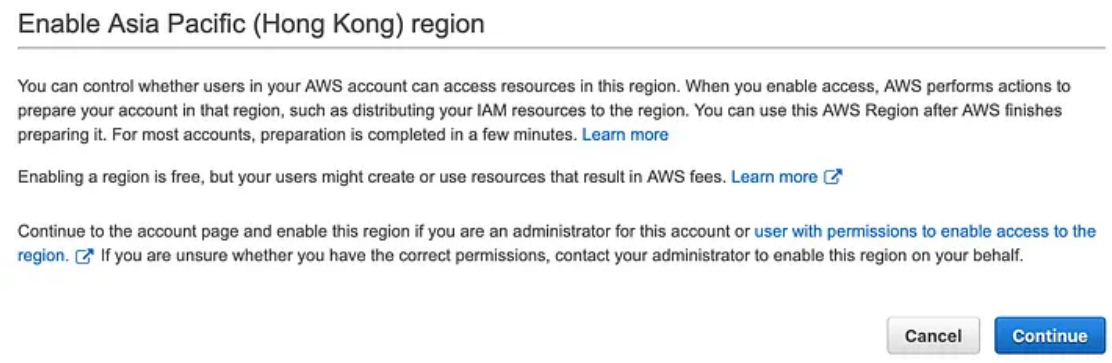


Deactivate STS Endpoints in Unused Regions

Don’t Enable New Regions Unless Required

AWS appears to have noticed the issue presented by unused regions and, beginning with the new ap-east-1 (Hong Kong) region, have disabled the region by default. If you attempt to create resources in it, you’ll be asked to enable the region.

Press enter or click to view image in full size



Avoid Enabling Regions Unless You Plan to Use Them

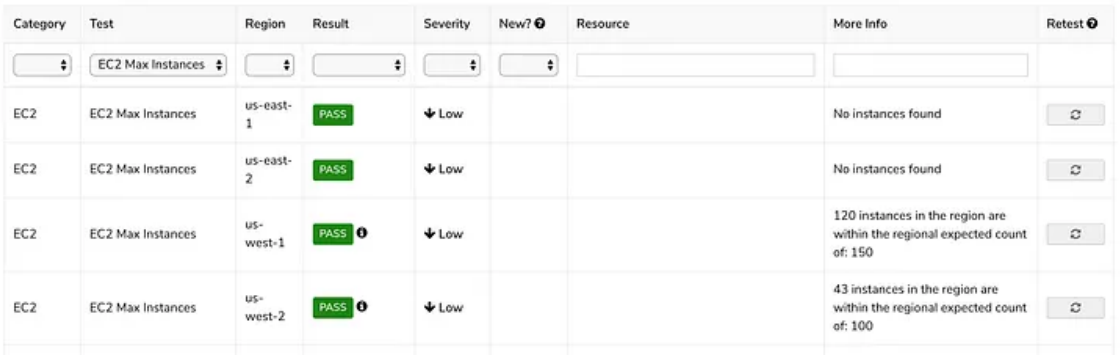
Monitor for Regional Activity

It’s paramount that any activity in unused regions is quickly detected. There are many tools, such as Splunk, that can ingest CloudTrail logs and alert based on region. Additionally, CloudSploit has added a number of features that help detect this activity.

In our open-source scans, we have a plugin called “EC2 Max Count” which counts the number of running instances in a region and alerts if it exceeds a configurable threshold. In unused regions, this threshold can be set

to “0.”

Press enter or click to view image in full size

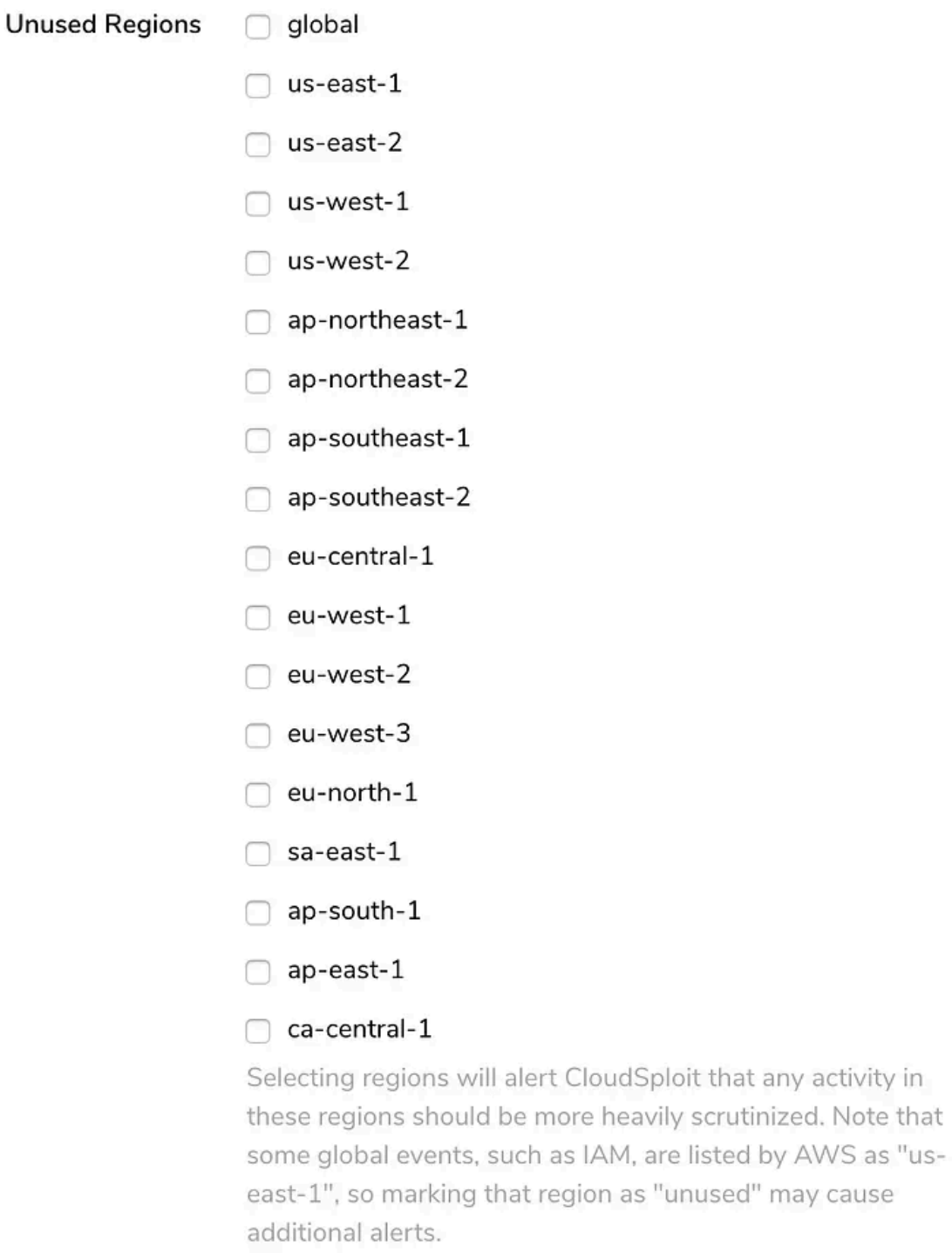


Category	Test	Region	Result	Severity	New?	Resource	More Info	Retest
	EC2 Max Instances							
EC2	EC2 Max Instances	us-east-1	PASS	Low			No instances found	
EC2	EC2 Max Instances	us-east-2	PASS	Low			No instances found	
EC2	EC2 Max Instances	us-west-1	PASS	Low			120 instances in the region are within the regional expected count of: 150	
EC2	EC2 Max Instances	us-west-2	PASS	Low			43 instances in the region are within the regional expected count of: 100	

CloudSploit’s Scans Detect Instance Counts in All Regions

Our Real-Time Events service also allows you to define unused regions and receive alerts within seconds of activity being detected.

Press enter or click to view image in full size



Conclusion

AWS's growing global footprint means that account operators and security teams need to be more vigilant than ever when it comes to monitoring accounts for potential malicious activity. With a few configuration tweaks and monitoring tools, detecting activity in these regions is quite simple and can greatly improve the account security posture.

CloudSploit is a provider of open source, free, and paid hosted SaaS solutions for cloud security monitoring.
