# Free or Open Source Resources to Help with AWS Security



---

An annotated list of free resources and open source tools to assist with AWS security

> Unless otherwise noted, we have not used or evaluated evaluated these tools. As per usual with open source tools, be sure to evaluate tools before adopting them to ensure they are worthy of your trust.
>
> ✅ CIT Cloud Team has used the tool.

## IAM-Specific Tools

### Access Key Management

- ✅ awscli-login – Access Keys for AWS CLI Using Cornell Two-Step Login - Shibboleth
- 99designs/aws-vault – A vault for securely storing and accessing AWS credentials in development environments
- rapid7/awsaml – Awsaml is an application for providing automatically rotated temporary AWS credentials.
- RiotGames/key-conjurer – Temporary Credential Service
- aws-rotate-key – Easily rotate your AWS access key
- synfinatic/aws-sso-cli – Tool to make it easier to use AWS SSO for the CLI and web console.
- toshke/aws-keys-sectool – Tool that helps to lock down IAM access keys by adding IP-restrictions to IAM policies.
- aws/rolesanywhere-credential-helper – rolesanywhere-credential-helper implements the signing process for IAM Roles Anywhere's CreateSession API and returns temporary credentials in a standard JSON format that is compatible with the `credential_process` feature available across the language SDKs.
- tuladhar/cleanup-aws-access-keys – tool to search and clean up unused AWS access keys

### IAM/Resources Policy

- ✅ AWS Policy Generator – The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources.
- salesforce/policy_sentry – IAM Least Privilege Policy Generator
- duo-labs/cloudtracker – CloudTracker helps you find over-privileged IAM users and roles by comparing CloudTrail logs with current IAM policies.
- goldfiglabs/rpCheckup – rpCheckup is an AWS resource policy security checkup tool that identifies public, external account access, intra-org account access, and private resources
- iann0036/iamlive – Generate an IAM policy from AWS calls using client-side monitoring (CSM) or embedded proxy
- Netflix/repokid – Repokid removes permissions granting access to unused services from the inline policies of IAM roles in an AWS account
- aminohealth/wonk - tool that analyzes IAM policies and minimizes them to fit under IAM policy length limits
- ermetic/access-undenied-aws – parses AWS AccessDenied CloudTrail events, explains the reasons for them, and offers actionable remediation steps
- https://aws.permissions.cloud/ – comprehensive list of IAM actions, permissions, and API methods
- BishopFox/iam-vulnerable – Use Terraform to create your own vulnerable by design AWS IAM privilege escalation playground.
- PaloAltoNetworks/IAM-Deescalate – Helps mitigate privilege escalation risk in AWS identity and access management
- duo-labs/parliament – AWS IAM linting library to find malformed json, incorrect prefix and action names, incorrect resources or conditions for the actions provided, etc.
- flosell/iam-policy-json-to-terraform – Tool to convert an IAM Policy in JSON format into a Terraform aws_iam_policy_document

## Tools that Help Secure AWS Resources

### Multiple Resource Types

- ✅ asecure.cloud – Creates customized CloudFormation/Terraform templates to improve security of existing AWS resources, or deploy secured resources

- ✅ cloud-custodian/cloud-custodian – Rules engine for cloud security, cost optimization, and governance, DSL in yaml for policies to query, filter, and take actions on resources
- toniblyx/prowler – Prowler is a security tool to perform AWS security best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness
- aquasecurity/cloudsploit – Cloud Security Posture Management (CSPM)
- airbnb/streamalert – StreamAlert is a serverless, realtime data analysis framework which empowers you to ingest, analyze, and alert on data from any environment, using datasources and alerting logic you define
- RhinoSecurityLabs/pacu – The AWS exploitation framework, designed for testing the security of Amazon Web Services environments.
- RhinoSecurityLabs/cloudgoat – CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool
- Netflix/security_monkey – Security Monkey monitors AWS, GCP, OpenStack, and GitHub orgs for assets and their changes over time.
- RiotGames/cloud-inquisitor – Enforce ownership and data security within AWS
- tmobile/pacbot – Policy as Code Bot (PacBot) is a platform for continuous compliance monitoring, compliance reporting and security automation for the cloud.
- darkbitio/aws-recon – Multi-threaded AWS inventory collection tool with a focus on security-relevant resources and metadata.
- righteousgambitresearch/quiet-riot – Unauthenticated enumeration of services, roles, and users in an AWS account or in every AWS account in existence.
- fivexl/terraform-aws-cloudtrail-to-slack – Terraform module that deploys resources to parse AWS CloudTrail events and send alerts to Slack for events that match pre-configured rules
- ✅ cloudquery/cloudquery – Open-source cloud asset inventory powered by SQL. Can also perform Terraform drift checks.
- turbot/steampipe – Use SQL to instantly query your cloud services (AWS, Azure, GCP and more). Open source CLI. No DB required.
- simonw/s3-credentials – A tool for creating credentials for accessing S3 buckets. Helps generate tightly-scoped IAM policies limited to a single prefix within a single bucket.
- nccgroup/ScoutSuite – Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments.
- DataDog/stratus-red-team – Stratus Red Team is "Atomic Red Team™" for the cloud, allowing to emulate offensive attack techniques in a granular and self-contained manner.
- awslabs/aws-cloudsaga – Simulate security events in AWS
- awslabs/aws-automated-incident-response-and-forensics – The Automated Incident Response and Forensics aims to facilitate automated steps for incident response and forensics based on the AWS Incident Response White Paper
- awslabs/aws-security-assessment-solution – An AWS tool to help you create a point in time assessment of your AWS account using Prowler and Scout as well as optional AWS developed ransomware checks.
- jonrau1/ElectricEye – Continuously monitor your AWS attack surface and evaluate services for configurations that can lead to degradation of confidentiality, integrity or availability.
- ovotech/domain-protect – Protect against subdomain takeover by looking for dangling DNS (Route 53) records
- 9rnt/poro – Scan for publicly accessible assets on your AWS cloud environment
- aws-cloudformation/cloudformation-guard – Guard offers a policy-as-code domain-specific language (DSL) to write rules and validate JSON- and YAML-formatted data such as CloudFormation Templates, K8s configurations, and Terraform JSON plans/configurations against those rules.
- awslabs/assisted-log-enabler-for-aws – Assisted Log Enabler for AWS - Find AWS resources that are not logging, and turn them on. Can easily enable logging for S3 access, CloudTrail, load balancers, EKS, VPC flow logs, Route 53 resolver logs.
- BishopFox/cloudfox – Automating situational awareness for cloud penetration tests.
- flosell/trailscraper – CLI tool to get information out of AWS CloudTrail logs

### CloudFormation

- cfripper – Library and CLI tool for analyzing CloudFormation templates and check them for security compliance
- stelligent/cfn_nag – The cfn-nag tool looks for patterns in CloudFormation templates that may indicate insecure infrastructure.
- bridgecrewio/checkov – Prevent cloud misconfigurations and find vulnerabilities during build-time in infrastructure as code, container images and open source packages with Checkov by Bridgecrew.

### Keys and Secrets

- awslabs/git-secrets – Prevents you from committing secrets and credentials into git repositories
- exec-with-secrets – Handle secrets in Docker using AWS KMS, SSM parameter store, Secrets Manager, or Azure Key Vault
- dxa4481/truffleHog – Searches through git repositories for high entropy strings and secrets, digging deep into commit history
- zricethezav/gitleaks – Scan git repos (or files) for secrets using regex and entropy

### S3

- sa7mon/S3Scanner – Scan for open AWS S3 buckets and dump the contents

## Log Querying

- https://github.com/Permiso-io-tools/CloudGrappler –A purpose-built tool designed for effortless querying of high-fidelity and single-event detections related to well-known threat actors in popular cloud environments such as AWS and Azure
- https://github.com/Permiso-io-tools/CloudConsoleCartographer – A framework for condensing groupings of cloud events (e.g. CloudTrail logs) and mapping them to the original user input actions in the management console UI for simplified analysis and explainability

## Monitoring

- zoph-io/aws-security-survival-kit – Bare minimum AWS Security Alerting

# Useful Articles

- 27 Aug 2022 Incident Response in AWS
- Lesser Known Techniques for Attacking AWS Environments – This post discusses lesser known attack techniques that bad actors can use in attacking AWS accounts, and how to defend against them.
- 21 Nov 2021 Github Actions & AWS OIDC
- 27 Oct 2022 GitHub Actions: Secure cloud deployments with OpenID Connect – GitHub Actions now supports OpenID Connect (OIDC) for secure deployments to cloud, which uses short-lived tokens that are automatically rotated for each deployment.
- 05 Oct 2021 AWS Access Keys - A Reference — This post outlines how to identify the different types of keys, where you're likely to find them across the different services, and the order of access precedence for the different SDKs and tools.
- 23 Sep 2021 IAM Vulnerable - Assessing the AWS Assessment Tools
- 15 Sep 2021 AWS federation comes to GitHub Actions
- 23 Aug 2021 Cloud Security Orienteering - How to Rapidly Understand and Secure an AWS Cloud Environment (and corresponding checklist)

# Training and Tutorials

- AWS Security Workshops – A collection of the latest AWS Security workshops from AWS
- Serverless Security Workshop – In this workshop, you will learn techniques to secure a serverless application built with AWS Lambda, Amazon API Gateway and RDS Aurora. From AWS
- flAWS 2 Challenge – Teaches you AWS (Amazon Web Services) security concepts. The challenges are focused on AWS specific issues, so no buffer overflows, XSS, etc. Able to be attacker or defender for challenges.
- CI/CDon't – An active learning exercise where you plan the bad guy where your goal is to gain access to administrative credentials for an AWS account.
- https://github.com/avishayil/cdk-goat – Vulnerable by Design AWS Cloud Development Kit (CDK) Infrastructure
- https://github.com/BishopFox/cloudfoxable – Create your own vulnerable by design AWS penetration testing playground

# Other Compilations of Security Resources

- puresec/awesome-serverless-security – A curated list of serverless security resources such as (e)books, articles, whitepapers, blogs and research papers.
- toniblyx/my-arsenal-of-aws-security-tools – List of open source tools for AWS security: defensive, offensive, auditing, DFIR, etc.
- ramimac/aws-customer-security-incidents - A repository of breaches of AWS customers
- hackingthe.cloud - An encyclopedia for offensive and defensive security knowledge in cloud native technologies (repo / website)