Security Checklist - General

Click on each item to learn more

1 **Protect you root account.**
Protect your access keys the same way you protect your private banking access.

2 **Protect your CloudTrail and your Billing S3 Bucket.**
Limit access to users and roles on a “need-to-know” basis.

3 **Activate region based CloudTrail.**
Ensure visibility and traceability of all your AWS account activities.

4 **Create administration roles with limited privileges.**
Use IAM policies to limit access only to services needed.

5 **Familiarize yourself with AWS Security Token Service (STS) and roles.**
AWS STS is a service that enables you to request temporary, limited-privilege credentials.

6 **Familiarize yourself with AWS Detailed Billing and monitor your monthly usage regularly.**
AWS Detailed Billing provides you with a “by-the-hour” insight of resources used and costs incurred.

Security Checklist – EC2/VPC/EBS

amazon web services

Click on each item to learn more

1 **Only use encrypted EBS volumes.**
Encrypt your data, snapshots, and disk I/O using the customary AES-256 algorithm.

2 **Activate your VPC Flow Logs.**
Collect IP traffic from and to the network interfaces in your VPCs for further analysis.

3 **Protect your EC2 Key Pairs.**
Follow our best practices for managing your access keys.

4 **Leverage IAM roles for EC2.**
Limit access only to required resources using IAM policies and roles.

5 **Control inbound and outbound traffic to your EC2 Instances with clearly structured Security Groups.**
A Security Group is a virtual, easy-to-use firewall for each EC2 instance controlling inbound and outbound traffic.

Security Checklist – S3

Click on each item to learn more

1 **Don’t create any public access S3 buckets.**
Control access to your S3 buckets using IAM or S3 Bucket Policies.

2 **Encrypt sensitive data in S3 using Server Side Encryption (SSE).**
Enforce encryption using the appropriate bucket policy.

3 **Encrypt inbound and outbound S3 data traffic.**
Use S3 SSL endpoints to safely transfer data via HTTPS.

4 **Familiarize yourself with S3 Versioning and S3 Lifecycle Policies.**
Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket.
Automate the lifecycle of your S3 objects with rule based actions.

5 **Activate S3 Access Logging and analyze logs regularly.**
The analysis of access logs will help you during security audits, provide detailed insight into user behavior, and help you better understand your S3 usage bills.