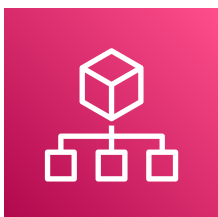


Securing AWS

A Getting Started Checklist

Account Management

It's important to start with a clear, and secure account structure. Ensuring each account adheres to a documented standard is an important first step.



- ☐ Enable AWS Organizations for centralized account management
- ☐ Enable multi-factor authentication (MFA) for the root account
- ☐ Enable MFA for all IAM users
- ☐ Regularly rotate access keys and passwords
- ☐ Implement a strong password policy
- ☐ Remove unused or inactive IAM users and access keys

Identity and Access Management (IAM)

Controlling who (or what) has access to your AWS account is a key part of securing your AWS environment.

- ☐ Use Identity Federation where possible, and avoid creating permanent credentials in AWS
- ☐ Follow the principle of least privilege for IAM users, roles, and policies
- ☐ Consider using customer-managed identity-policies for fine-grain control
- ☐ Regularly review and update identity-based policies and permissions



Monitoring and Logging

Without adequate monitoring in place, you cannot be sure of the actions occurring in your AWS environment and who (or what) is taking those actions.



- ☐ Make sure AWS CloudTrail is retaining log data by configuring S3 and/or CloudWatch Logs
- ☐ Use AWS Config to discover resources and monitor for changes and compliance
- ☐ Enable AWS Security Hub for security alerts and compliance reporting
- ☐ Configure Amazon GuardDuty for continuous threat detection
- ☐ Set up AWS CloudWatch for monitoring and alerting
- ☐ Regularly review and analyze security logs

Networking and Firewall

Proper deployment and configuration of networks and access control is the foundation of building secure, highly-available workloads on AWS.

- ☐ Deploy Virtual Private Clouds (VPC) according to AWS best practice
- ☐ Use security groups and network ACLs to restrict both inbound and outbound traffic
- ☐ Enable VPC Flow Logs for network traffic analysis
- ☐ Use VPC private endpoints for secure access to AWS services



Data Protection

Protecting your data at rest and while it is in transit is a critical part of building solutions on AWS.



- ☐ Encrypt data at rest using AWS Key Management Service (KMS)
- ☐ Ensure data is encrypted in transit using HTTPS/TLS
- ☐ Regularly back up data using Amazon Simple Storage Service (S3), Amazon Relational Database Snapshots (RDS), or AWS Backup
- ☐ Protect data from accidental deletion by limiting access to only those entities who require it

Security Auditing and Compliance

Ensuring the security of your AWS environments is an on-going process. Just because your solution was secure on day one, doesn't mean that is still is.

- ☐ Conduct regular security audits using the AWS Well-Architected Framework
- ☐ Use the AWS Trusted Advisor to identify and address non-compliance resources
- ☐ Use AWS Config Rules to monitor (and remediate) non-compliant resources
- ☐ Implement and regularly update a security incident response plan



Common Misconfigurations

Over the years, we've reviewed many AWS accounts. Here are remedies for some of the most common oversights we see in customer accounts.



- ☐ Ensure no S3 buckets allow for public access and that proper resource policies are implemented
- ☐ Avoid overly permissive security group rules and open ports
- ☐ Avoid overly broad IAM policies and permissions
- ☐ Regularly update and patch software to reduce vulnerabilities
- ☐ Avoid making resources accessible from the public Internet

Are you ready to improve the security of your AWS accounts?

Since 2016, we've [helped customers](#) build, design and operate secure, highly available workloads on AWS.

Key Activities

- Data Collection:** using a combination of automated scripts and manual data collection, we'll build a snapshot of the current state of your AWS environment.
- Interviews:** where appropriate we'll schedule follow-up sessions with your team to collect any additional information required to complete the account review.
- Analysis:** Our team of certified AWS experts will review the collected data and interview feedback and provide insight and guidance on the current state of your AWS deployment.

Deliverables

- Analysis Review:** Our team will review the findings with you and your team and answer any questions about the analysis.
- Session Recording:** The analysis review session will be recorded and provided to you and your team.
- Audit Document:** A detailed review of your AWS environment organized by account and identifying areas of possible improvement. You can use this document to improve the security of your AWS account.



- AWS WAF Delivery
- AWS Lambda Delivery
- AWS Config Delivery
- Amazon DynamoDB Delivery

- AWS CloudFormation Delivery
- Amazon EC2 for Windows Server Delivery

