AWS Security Checklist Report

AWS Security Checklist - Amazon Aurora

Item	Description
Encrypt data at rest	Encrypting your Aurora database at rest helps protect your data from unauthorized access or disclosure in the event of theft or loss of your storage devices.
Encrypt data in transit	Encrypting your Aurora database connections helps protect your data from unauthorized interception or disclosure during transmission.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to your Aurora database is limited to authorized users and applications.
Implement backup and disaster recovery plans	Implementing backup and disaster recovery plans helps ensure that your Aurora database is available and functional during a security breach or other disaster.
Monitor Aurora database activity	Monitoring Aurora database activity helps you identify potential security issues or anomalies in your Aurora environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Aurora resources are secure and compliant with your security policies.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.

AWS Security Checklist - Amazon EventBridge

Item	Description
Encrypt data in transit	Encrypting your EventBridge data in transit helps protect your data from unauthorized interception or disclosure during transmission.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to your EventBridge resources is limited to authorized users and applications.
Implement monitoring and logging	Implementing monitoring and logging helps you identify potential security issues or anomalies in your EventBridge environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your EventBridge resources are secure and compliant with your security policies.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.

AWS Security Checklist - Amazon Connect

Item	Description
Enable encryption for Amazon Connect data	Enabling encryption for Amazon Connect data at rest helps protect sensitive information from unauthorized access or disclosure.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to Amazon Connect is limited to authorized users and applications.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Amazon Connect resources are secure and compliant with your security policies.
Monitor Amazon Connect activity	Monitoring Amazon Connect activity helps you identify potential security issues or anomalies in your Amazon Connect environment.

AWS Security Checklist - Amazon MQ

Item	Description
Encrypt data in transit	Encrypting your MQ data in transit helps protect your data from unauthorized interception or disclosure during transmission.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to your MQ resources is limited to authorized users and applications.
Implement monitoring and logging	Implementing monitoring and logging helps you identify potential security issues or anomalies in your MQ environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your MQ resources are secure and compliant with your security policies.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.
Secure your MQ VPC	Securing your MQ Virtual Private Cloud (VPC) helps protect your MQ resources from unauthorized access and network-based attacks.
Implement backup and recovery	Implementing backup and recovery helps ensure that you can recover your MQ resources and data in the event of a disaster or data loss.
Implement message-level encryption	Implementing message-level encryption helps protect your MQ messages from unauthorized access or disclosure.
Implement message filtering and validation	Implementing message filtering and validation helps protect your MQ resources from malicious or invalid messages.

AWS Security Checklist - Amazon Redshift

Item	Description
Encrypt data at rest	Encrypting your Redshift data at rest helps protect your data from unauthorized access or disclosure in the event of theft or loss of your storage devices.
Encrypt data in transit	Encrypting your Redshift cluster connections helps protect your data from unauthorized interception or disclosure during transmission.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to your Redshift cluster is limited to authorized users and applications.
Implement backup and disaster recovery plans	Implementing backup and disaster recovery plans helps ensure that your Redshift cluster is available and functional during a security breach or other disaster.
Monitor Redshift cluster activity	Monitoring Redshift cluster activity helps you identify potential security issues or anomalies in your Redshift environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Redshift resources are secure and compliant with your security policies.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.
Secure your Redshift VPC	Securing your Redshift Virtual Private Cloud (VPC) helps protect your Redshift cluster from unauthorized access and network-based attacks.
Implement network security best practices	Implementing network security best practices helps ensure that your Redshift cluster is protected from network-based attacks and threats.

AWS Security Checklist - Amazon SQS

Item	Description
Encrypt data in transit	Encrypting your SQS data in transit helps protect your data from unauthorized interception or disclosure during transmission.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to your SQS resources is limited to authorized users and applications.
Implement monitoring and logging	Implementing monitoring and logging helps you identify potential security issues or anomalies in your SQS environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your SQS resources are secure and compliant with your security policies.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.
Secure your SQS VPC	Securing your SQS Virtual Private Cloud (VPC) helps protect your SQS resources from unauthorized access and network-based attacks.
Implement retention policies for your SQS messages	Implementing retention policies helps ensure that your SQS messages are stored securely and in compliance with your security policies.
Implement message-level encryption	Implementing message-level encryption helps protect your SQS messages from unauthorized access or disclosure.
Implement message filtering and validation	Implementing message filtering and validation helps protect your SQS resources from malicious or invalid messages.

AWS Security Checklist - API Gateway

Item	Description
Use HTTPS	Use HTTPS instead of HTTP for all API requests to encrypt data in transit and prevent man-in-the-middle attacks.
Enable API Gateway Logging	Enable logging to Amazon CloudWatch Logs to help with security analysis, change tracking, and compliance auditing.
Restrict Access with API Gateway Resource Policies	Define resource policies to restrict access to your APIs, based on IP address, Amazon VPC endpoint, or other attributes.
Use AWS WAF with API Gateway	Use AWS Web Application Firewall (WAF) with API Gateway to protect against common web exploits such as SQL injection and cross-site scripting (XSS).
Implement Authorization with API Gateway	Implement authorization with API Gateway to control who can access your APIs and what actions they can perform.
Protect Against Denial-of-Service (DoS) Attacks	Configure rate limiting, throttling, and caching to protect against DoS attacks and to ensure high availability and performance.
Use API Gateway Access Logging	Use access logging to track and monitor requests to your APIs, and to help with troubleshooting and compliance auditing.
Secure API Gateway Credentials	Use AWS Secrets Manager or AWS Key Management Service (KMS) to securely manage API Gateway credentials such as API keys and client certificates.

AWS Security Checklist - Athena

Item	Description
Limit access to Athena	Ensure that access to Athena is limited to only the necessary users and roles.
Use IAM policies to control access	Use IAM policies to control access to Athena resources.
Use encryption	Use encryption to protect sensitive data at rest and in transit.
Enable CloudTrail logging	Enable CloudTrail logging for Athena to track usage and changes to the service.
Enable VPC access	Enable VPC access for Athena to limit access to resources within your VPC.
Enable query result encryption	Enable query result encryption to protect sensitive data in query results.
Use AWS Glue to manage Athena data catalog	Use AWS Glue to manage the Athena data catalog and ensure that it is up-to-date and accurate.
Enable Amazon S3 server-side encryption	Enable Amazon S3 server-side encryption to protect data stored in S3 that is accessed by Athena.
Use parameterized queries	Use parameterized queries to protect against SQL injection attacks.

AWS Security Checklist - AWS Auto Scaling

Item	Description
Use IAM roles to control access to AWS Auto Scaling resources	Using IAM roles enables you to control which users and applications have access to AWS Auto Scaling resources and what actions they can perform.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit network access to AWS Auto Scaling resources	Limiting network access helps prevent unauthorized access and limits the impact of security breaches.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your Auto Scaling groups.
Regularly update your Auto Scaling groups and their components	Regularly updating your Auto Scaling groups and their components helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.

AWS Security Checklist - AWS Batch

Item	Description
Use IAM roles to control access to AWS Batch resources	Using IAM roles enables you to control which users and applications have access to AWS Batch resources and what actions they can perform.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit network access to AWS Batch resources	Limiting network access helps prevent unauthorized access and limits the impact of security breaches.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your AWS Batch environment.
Regularly update your AWS Batch environment and its components	Regularly updating your AWS Batch environment and its components helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.

AWS Security Checklist - CloudTrail

Item	Description
Enable CloudTrail logging	Enable AWS CloudTrail logging to track changes made to your AWS account and resources.
Encrypt CloudTrail logs	Use server-side encryption (SSE) or client-side encryption to encrypt CloudTrail logs at rest.
Restrict access to CloudTrail logs	Limit access to CloudTrail logs to only authorized personnel, using IAM policies or bucket policies.
Monitor CloudTrail logs	Monitor CloudTrail logs for unusual activity, using services like Amazon CloudWatch or Amazon Athena.
Enable multi-factor authentication (MFA) for CloudTrail logging	Enable MFA for CloudTrail logging to prevent unauthorized changes to CloudTrail configuration.
Regularly review CloudTrail logs	Regularly review CloudTrail logs to identify and investigate any security or compliance issues.
Protect CloudTrail credentials	Protect CloudTrail credentials, including access keys and secret access keys, using best practices like rotation and secure storage.

AWS Security Checklist - AWS Compute Optimizer

Item	Description
Enable encryption for Compute Optimizer data	Enabling encryption for Compute Optimizer data at rest helps protect sensitive information from unauthorized access or disclosure.
Enable AWS CloudTrail logging for Compute Optimizer	Enabling AWS CloudTrail logging for Compute Optimizer helps you monitor and audit changes to your Compute Optimizer resources.
Limit access to Compute Optimizer	Limiting access to Compute Optimizer helps prevent unauthorized access and limits the impact of security breaches.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Compute Optimizer resources are secure and compliant with your security policies.
Ensure data accuracy	Ensuring data accuracy helps Compute Optimizer provide accurate recommendations and avoid potential security issues.

AWS Security Checklist - DynamoDB

Item	Description
Enable VPC Endpoints	Enable VPC endpoints to ensure that all traffic to and from your DynamoDB tables is restricted within your VPC and does not traverse the public internet.
Use IAM roles	Use IAM roles to control access to your DynamoDB tables and limit access to only the necessary permissions.
Enable encryption	Enable server-side encryption for your DynamoDB tables to protect against unauthorized access to your data.
Monitor access patterns	Monitor access patterns to your DynamoDB tables to detect anomalous behavior and potential security threats.
Enable audit logging	Enable audit logging for your DynamoDB tables to track access and changes to your data.
Enable automatic backups	Enable automatic backups for your DynamoDB tables to ensure that you can restore your data in the event of a disaster or data loss.
Use fine-grained access control	Use fine-grained access control to limit access to specific items or attributes within your DynamoDB tables.
Monitor network traffic	Monitor network traffic to and from your DynamoDB tables to detect and prevent unauthorized access or data exfiltration.

AWS Security Checklist - Amazon Elastic Block Store (EBS)

Item	Description
Encrypt data at rest	Encrypting your EBS volumes at rest helps protect your data from unauthorized access or disclosure in the event of theft or loss of your storage devices.
Use secure AWS Identity and Access Management (IAM) policies	Using secure IAM policies helps ensure that access to your EBS volumes is limited to authorized users and applications.
Implement backup and disaster recovery plans	Implementing backup and disaster recovery plans helps ensure that your EBS volumes are available and functional during a security breach or other disaster.
Monitor EBS volume activity	Monitoring EBS volume activity helps you identify potential security issues or anomalies in your EBS environment.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your EBS resources are secure and compliant with your security policies.

AWS Security Checklist - EC2

Item	Description
Use security groups	Create and configure security groups to control inbound and outbound traffic for your EC2 instances.
Enable monitoring	Enable CloudWatch monitoring to track the performance and status of your EC2 instances.
Create IAM roles	Create IAM roles to manage access to your EC2 instances and assign permissions for AWS resources and services.
Enable VPC Flow Logs	Enable VPC Flow Logs to monitor and capture information about IP traffic going to and from your EC2 instances in your VPC.
Implement Network ACLs	Use Network Access Control Lists (NACLs) to add an additional layer of security by controlling traffic at the subnet level.
Enable AWS Config	Enable AWS Config to continuously monitor and record your EC2 instances' configurations and evaluate them against best practices.
Encrypt EBS volumes	Enable encryption for your Elastic Block Store (EBS) volumes to protect your data at rest.
Enable instance metadata protection	Enable Instance Metadata Service Version 2 (IMDSv2) to protect against unauthorized access to the instance metadata.
Use dedicated tenancy	Use dedicated tenancy to launch EC2 instances on dedicated hardware for increased security and compliance.
Enable AWS Systems Manager	Use AWS Systems Manager to manage and automate tasks on your EC2 instances, such as patching and configuration management.
Regularly patch and update	Regularly apply security patches and updates to your EC2 instances and applications to reduce vulnerabilities.
Implement Amazon Inspector	Use Amazon Inspector to assess the security and compliance of your EC2 instances by identifying potential security issues.
Use Amazon GuardDuty	Enable Amazon GuardDuty to continuously monitor and detect threats to your EC2 instances and AWS accounts.
Enable Amazon Macie	Use Amazon Macie to discover, classify, and protect sensitive data stored in your EC2 instances.
Implement AWS WAF	Use AWS Web Application Firewall (WAF) to protect your web applications hosted on EC2 instances from common web exploits.
Enable AWS Shield	Enable AWS Shield to protect your EC2 instances from Distributed Denial of Service (DDoS) attacks.

AWS Security Checklist - ECR

Item	Description
Enable encryption	Enable encryption at rest for your ECR repositories to protect against unauthorized access to your data.
Use private repositories	Use private repositories to protect your container images from being accessed by unauthorized users.
Scan images for vulnerabilities	Use Amazon ECR image scanning to detect and remediate vulnerabilities in your container images.
Implement access control	Use IAM policies and resource-based permissions to control access to your ECR repositories and images.
Use VPC endpoints	Use VPC endpoints to securely access your ECR repositories without exposing them to the public internet.
Enable lifecycle policies	Use lifecycle policies to automatically clean up untagged or unused images, and to expire old images to reduce storage costs.
Audit trail	Enable AWS CloudTrail to log all API calls made to your ECR repositories for auditing and compliance purposes.

AWS Security Checklist - Amazon EKS

Item	Description
Enable VPC Flow Logs	Enabling VPC Flow Logs allows you to capture information about the IP traffic going to and from your EKS cluster, which can be useful for troubleshooting and security analysis.
Use RBAC (Role-Based Access Control) to control access to the Kubernetes API	RBAC enables you to define granular access controls to the Kubernetes API, which helps prevent unauthorized access and privilege escalation.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Use network policies to control traffic flow	Network policies enable you to control the flow of traffic to and from your Kubernetes pods, which can help prevent unauthorized access and limit the impact of security breaches.
Regularly update your EKS cluster and its components	Regularly updating your EKS cluster and its components helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your EKS cluster.

AWS Security Checklist - AWS Elastic Beanstalk

Item	Description
Use IAM roles to control access to AWS Elastic Beanstalk resources	Using IAM roles enables you to control which users and applications have access to AWS Elastic Beanstalk resources and what actions they can perform.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit network access to Elastic Beanstalk resources	Limiting network access helps prevent unauthorized access and limits the impact of security breaches.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your Elastic Beanstalk environments.
Regularly update your Elastic Beanstalk environments and their components	Regularly updating your Elastic Beanstalk environments and their components helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.
Implement function-level access control	Use AWS Identity and Access Management (IAM) policies to control access to your Elastic Beanstalk environments. Restrict access to only the actions and resources that are necessary for the environment to perform its intended actions.
Implement secure deployment practices	Implementing secure deployment practices helps ensure that your Elastic Beanstalk environments are deployed securely and that your applications are not vulnerable to security breaches.
Use WAF to protect against web-based attacks	AWS WAF (Web Application Firewall) can be used to protect against common web-based attacks such as SQL injection and cross-site scripting.
Implement access and authentication controls for applications	Implementing access and authentication controls for your applications helps ensure that only authorized users can access sensitive information or perform privileged actions.
Implement data protection controls for applications	Implementing data protection controls for your applications helps ensure that sensitive information is protected from unauthorized access or disclosure.

AWS Security Checklist - Fargate

Item	Description
Use task roles	Assign a task role to your Fargate tasks to ensure that they have only the necessary permissions to perform their specific functions.
Use VPC	Deploy Fargate tasks in a VPC to control network access and to restrict public access to your resources.
Use security groups	Define security groups to control inbound and outbound traffic for your Fargate tasks and to restrict access to only necessary ports.
Use IAM roles for service accounts (IRSA)	Use IAM roles for service accounts (IRSA) to enable your pods to communicate securely with other AWS services using IAM credentials.
Encrypt data at rest	Use encryption to protect sensitive data stored in volumes attached to Fargate tasks.
Encrypt data in transit	Use encryption to protect data in transit between Fargate tasks and other AWS services or external endpoints.
Monitor container images	Regularly scan and monitor container images for vulnerabilities and keep them up to date to reduce the risk of exploits.
Enable logging	Enable logging for your Fargate tasks to monitor and audit activity within your containers.
Use AWS Secrets Manager	Use AWS Secrets Manager to securely store and manage sensitive data such as passwords, API keys, and other credentials used by your Fargate tasks.

AWS Security Checklist - Lambda

Item	Description
Use AWS Secrets Manager or AWS Systems Manager Parameter Store to store sensitive information	To prevent accidental exposure of sensitive information, use AWS Secrets Manager or AWS Systems Manager Parameter Store to store sensitive information such as passwords, API keys, and database connection strings.
Implement function-level access control	Use AWS Identity and Access Management (IAM) policies to control access to your Lambda functions. Restrict access to only the actions and resources that are necessary for the function to perform its intended actions.
Enable VPC access for your Lambda functions	Use Amazon Virtual Private Cloud (VPC) to isolate your Lambda functions from the public internet and to access resources in your own VPC.
Enable AWS X-Ray tracing	Enable AWS X-Ray tracing to monitor and troubleshoot your serverless application. X-Ray provides end-to-end tracing of requests and helps you identify performance bottlenecks and errors.
Use AWS Key Management Service to encrypt data in transit and at rest	Use AWS Key Management Service (KMS) to create and manage encryption keys that protect your data. Encrypt data in transit and at rest using KMS-managed keys.
Monitor and log function invocations	Use Amazon CloudWatch to monitor and log function invocations. Use CloudWatch Logs to store and analyze logs generated by your Lambda functions.
Use AWS Config to monitor resource configurations and compliance	Use AWS Config to monitor the configurations of your Lambda functions and their associated resources. Use Config rules to define compliance rules for your resources and to get notifications when they change.
Implement least privilege permissions for your Lambda functions	Use the principle of least privilege to assign permissions to your Lambda functions. Assign only the necessary permissions to access the required resources and actions.
Use environment variables to configure your Lambda functions	Use environment variables to pass configuration information to your Lambda functions. Store sensitive configuration information in AWS Secrets Manager or AWS Systems Manager Parameter Store.
Implement automated deployments for your Lambda functions	Use AWS CodeDeploy to automate the deployment of your Lambda functions. CodeDeploy can help you perform rolling deployments and automate the testing of your functions.
Test and monitor your Lambda functions	Use AWS Lambda built-in monitoring capabilities to monitor the health of your Lambda functions. Use AWS Lambda Test Events to test your functions in different scenarios.

AWS Security Checklist - AWS Local Zones

Item	Description
Use VPCs to isolate resources in Local Zones	Using VPCs helps to isolate your resources within AWS Local Zones and prevent unauthorized access to your resources.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit access to Local Zones resources	Limiting access to Local Zones resources helps prevent unauthorized access and limits the impact of security breaches.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your Local Zones resources.
Regularly update your Local Zones resources	Regularly updating your Local Zones resources helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.
Implement function-level access control	Use AWS Identity and Access Management (IAM) policies to control access to your Local Zones resources. Restrict access to only the actions and resources that are necessary for the resource to perform its intended actions.
Implement secure deployment practices	Implementing secure deployment practices helps ensure that your Local Zones resources are deployed securely and that your applications are not vulnerable to security breaches.
Implement backup and disaster recovery plans	Implementing backup and disaster recovery plans helps ensure that your Local Zones resources are available and functional during a security breach or other disaster.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.
Implement security controls for data at rest	Implementing security controls for data at rest helps ensure that sensitive information is protected from unauthorized access or disclosure.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Local Zones resources are secure and compliant with your security policies.

AWS Security Checklist - S3

Item	Description
Enable versioning	Enable versioning for your S3 buckets to protect against accidental deletion or overwrite.
Enable encryption in S3	Enable encryption for your S3 buckets to protect against unauthorized access to your data at rest.
Create IAM policies	Use IAM policies to control access to your S3 buckets and objects.
Enable object lock	Enable object lock to prevent objects from being deleted or overwritten for a defined retention period.
Enable bucket logging	Enable access logging on your S3 buckets to monitor and analyze access patterns and identify potential security risks.
Enable CloudTrail integration	Integrate your S3 buckets with AWS CloudTrail to capture and store data events for auditing and compliance purposes.
Enable AWS Config	Enable AWS Config to continuously monitor and record your S3 bucket configurations and evaluate them against best practices.
Set up S3 event notifications	Configure S3 event notifications to send messages when specific events occur in your S3 buckets, such as object creation or deletion.
Implement bucket policies	Use S3 bucket policies to manage permissions at the bucket level, controlling access to all objects within a bucket.
Set up CORS configurations	Configure Cross-Origin Resource Sharing (CORS) to control which origins can access your S3 buckets and objects.
Enable MFA Delete	Enable Multi-Factor Authentication (MFA) Delete to require additional authentication when deleting objects or changing bucket versioning settings.
Enable transfer acceleration	Enable S3 Transfer Acceleration to improve data transfer speed and reduce latency for your S3 buckets.
Implement bucket tagging	Use bucket tagging to organize and manage your S3 buckets and enable cost allocation tracking.
Configure lifecycle policies	Set up lifecycle policies to automate the management of objects in your S3 buckets, such as transitioning objects to different storage classes or deleting objects.
Implement public access blocking	Use S3 Block Public Access settings to prevent public access to your S3 buckets and objects.
Use VPC endpoints	Create VPC endpoints for Amazon S3 to securely access your buckets over a private network connection.

AWS Security Checklist - SNS

Item	Description
Enable access logging	Enable access logs for SNS to monitor access and provide audit trails.
Enable server-side encryption	Enable server-side encryption for SNS to protect against unauthorized access to your data.
Use IAM policies to control access	Use IAM policies to control access to your SNS topics and prevent unauthorized access.
Enable VPC Endpoints	Use VPC Endpoints for SNS to allow your applications to send messages to SNS over a private network.
Enable SNS message filtering	Use SNS message filtering to ensure that subscribers receive only the messages they are interested in.
Rotate access keys regularly	Rotate SNS access keys regularly to reduce the risk of unauthorized access.
Enable CloudTrail logging	Enable CloudTrail logging for SNS to monitor and audit API calls and detect suspicious activity.

AWS Security Checklist - VPC

Item	Description
Create a VPC with multiple subnets	Design your VPC with multiple subnets spread across multiple Availability Zones to ensure high availability and fault tolerance.
Use Security Groups and Network ACLs	Use Security Groups and Network ACLs to define inbound and outbound traffic rules for your VPC resources, ensuring that only necessary traffic is allowed.
Implement Private and Public Subnets	Segregate resources within your VPC into private and public subnets based on their exposure to the internet. Keep critical resources in private subnets with no direct internet access.
Use NAT Gateways for outbound traffic	Use NAT Gateways to allow instances in private subnets to access the internet while still preventing inbound traffic from the internet.
Use VPC Flow Logs	Enable VPC Flow Logs to capture information about the IP traffic going to and from network interfaces in your VPC for monitoring and auditing purposes.
Use VPC endpoints for AWS services	Use VPC endpoints to privately connect your VPC to supported AWS services, ensuring that traffic between your VPC and these services does not traverse the public internet.
Implement proper routing	Configure routing tables for each subnet in your VPC, ensuring that traffic is routed only to intended destinations.
Use VPN or Direct Connect for hybrid environments	If connecting your VPC to on-premises environments, use AWS VPN or Direct Connect for secure and reliable connectivity.
Periodically review Security Groups and Network ACLs	Regularly review and update your Security Groups and Network ACLs to ensure that they continue to meet your security requirements and follow the principle of least privilege.
Encrypt sensitive data	Encrypt sensitive data in transit and at rest when transmitted between your VPC and other networks, or stored within your VPC.
Implement proper IAM policies	Use IAM policies to control access to VPC resources and actions, ensuring that users and applications have only the necessary permissions.

AWS Security Checklist - Amazon Lightsail

Item	Description
Use strong passwords and multi-factor authentication (MFA)	Using strong passwords and MFA helps prevent unauthorized access to your Lightsail resources and data.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit network access to Lightsail resources	Limiting network access helps prevent unauthorized access and limits the impact of security breaches.
Enable backups and snapshots	Backups and snapshots enable you to recover your data and restore your instances to a previous state in case of data loss or security incidents.
Regularly update your Lightsail instances and their software	Regularly updating your Lightsail instances and their software helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your Lightsail instances.

AWS Security Checklist - AWS Outposts

Item	Description
Isolate resources in VPCs	Isolating your resources in Virtual Private Clouds (VPCs) helps to prevent unauthorized access to your AWS Outposts resources.
Encrypt data in transit and at rest	Encrypting data in transit and at rest helps protect sensitive information from interception and unauthorized access.
Limit access to Outposts resources	Limiting access to your AWS Outposts resources helps prevent unauthorized access and limits the impact of security breaches.
Enable logging and monitoring	Logging and monitoring enable you to detect and respond to security incidents and other issues affecting your AWS Outposts environment.
Regularly update your Outposts resources	Regularly updating your Outposts resources helps ensure that security vulnerabilities are addressed and that you are using the latest features and functionality.
Implement function-level access control	Use AWS Identity and Access Management (IAM) policies to control access to your Outposts resources. Restrict access to only the actions and resources that are necessary for the resource to perform its intended actions.
Implement secure deployment practices	Implementing secure deployment practices helps ensure that your Outposts resources are deployed securely and that your applications are not vulnerable to security breaches.
Implement backup and disaster recovery plans	Implementing backup and disaster recovery plans helps ensure that your Outposts resources are available and functional during a security breach or other disaster.
Implement least privilege access	Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions.
Implement security controls for data at rest	Implementing security controls for data at rest helps ensure that sensitive information is protected from unauthorized access or disclosure.
Regularly review and audit security controls	Regularly reviewing and auditing security controls helps ensure that your Outposts resources are secure and compliant with your security policies.