Best practice rules for Amazon Web Services

Amazon Web Services best practice rules

Trend Micro Cloud One™ – Conformity has over 750+ cloud infrastructure configuration best practices for your Amazon Web Services™, Microsoft® Azure, and Google Cloud™ environments. Here is our growing list of AWS security, configuration and compliance rules with clear instructions on how to perform the updates – made either through the AWS console or via the AWS Command Line Interface (CLI).

Conformity provides real-time monitoring and auto-remediation for the security, compliance and governance of your cloud infrastructure. Leaving you to grow and scale your business with confidence.

AWS Certificate Manager

ACM Certificate Expired

Ensure expired SSL/TLS certificates are removed from AWS Certificate Manager (ACM).

AWS ACM Certificates Renewal (30 days before expiration)

Ensure Amazon Certificate Manager (ACM) certificates are renewed before their expiration.

AWS ACM Certificates Renewal (45 days before expiration)

Ensure Amazon Certificate Manager (ACM) certificates are renewed before their expiration.

AWS ACM Certificates Renewal (7 days before expiration)

Ensure Amazon Certificate Manager (ACM) certificates are renewed before their expiration.

AWS ACM Certificates Validity

Ensure expired SSL/TLS certificates are removed from AWS Certificate Manager (ACM).

AWS ACM Certificates with Wildcard Domain Names

Ensure that wildcard certificates issued by Amazon Certificate Manager (ACM) or imported to ACM are not in use.

Amazon API Gateway

API Gateway Integrated With AWS WAF

Use AWS WAF to protect Amazon API Gateway APIs from common web exploits.

API Gateway Tracing Enabled

Ensure APIs created with Amazon API Gateway have active tracing support for AWS X-Ray enabled.

APIs CloudWatch Logs

Ensure APIs created with Amazon API Gateway have AWS CloudWatch logging enabled.

APIs Detailed CloudWatch Metrics

Ensure detailed CloudWatch metrics are enabled for Amazon API Gateway APIs stages.

Client Certificate

Use client-side SSL certificates for HTTP backend authentication within AWS API Gateway.

Content Encoding

Ensure APIs created with Amazon API Gateway have Content Encoding feature enabled.

Enable API Cache

Ensure that REST APIs created with Amazon API Gateway have response caching enabled.

Enable Encryption for API Cache

Ensure that stage-level cache encryption is enabled for your Amazon API Gateway APIs.

Private Endpoint

Ensure APIs created with Amazon API Gateway are only accessible via private endpoints.

Rotate Expiring SSL Client Certificates

Ensure that SSL certificates associated with API Gateway REST APIs are rotated periodically.

Amazon AppFlow

Enable Data Encryption with KMS Customer Master Keys

Ensure that Amazon AppFlow flows are encrypted with KMS Customer Master Keys (CMKs).

AWS App Mesh

Enable Access Logging for App Mesh Virtual Gateways

Ensure that Access Logging is enabled for your Amazon App Mesh virtual gateways.

Restrict External Traffic

Ensure that Amazon App Mesh proxies are only forwarding traffic between each other.

Amazon Athena

Enable Encryption for AWS Athena Query Results

Ensure that AWS Athena query results stored in Amazon S3 are encrypted at rest.

access security to your AWS resources.

AWS Auto Scaling

App-Tier Auto Scaling Group with associated Elastic Load Balancer

Ensure app-tier Auto Scaling Group has an associated Elastic Load Balancer.

Auto Scaling Group Cooldown Period

Ensure Amazon Auto Scaling Groups are utilizing cooldown periods.

Auto Scaling Group Health Check

Ensure AWS Auto Scaling Group is using the appropriate health check configuration to determine the health status of its instances.

Auto Scaling Group Notifications

Ensure AWS ASG Notifications feature is enabled within your Auto Scaling Groups settings.

Auto Scaling Group Referencing Missing ELB

Ensure Amazon Auto Scaling Groups are utilizing active Elastic Load Balancers.

Check for Auto Scaling Groups with integrated Elastic Load Balancers.

Ensure that each AWS Auto Scaling Group has an associated Elastic Load Balancer.

CloudWatch Logs Agent for App-Tier Auto Scaling Group In Use

Ensure an agent for AWS CloudWatch Logs is installed within Auto Scaling Group for app tier.

CloudWatch Logs Agent for Web-Tier Auto Scaling Group In Use

Ensure an agent for AWS CloudWatch Logs is installed within Auto Scaling Group for web tier.

Empty Auto Scaling Group

Identify and remove empty AWS Auto Scaling Groups (ASGs).

IAM Roles for App-Tier ASG Launch Configurations

Ensure Auto Scaling Group launch configuration for app tier is configured to use a customer created app-tier IAM role.

IAM Roles for Web-Tier ASG Launch Configurations

Ensure Auto Scaling Group launch configuration for web tier is configured to use a customer created web-tier IAM role.

Launch Configuration Referencing Missing AMI

Ensure AWS Launch Configurations are utilizing active Amazon Machine Images.

Launch Configuration Referencing Missing Security Groups

Ensure AWS Launch Configurations are utilizing active Security Groups.

Multi-AZ Auto Scaling Groups

Ensure AWS Auto Scaling Groups utilize multiple Availability Zones to improve environment reliability.

Same Availability Zones In ASG And ELB

Ensure AWS Availability Zones used for Auto Scaling Groups and for their Elastic Load Balancers are the same.

Suspended Auto Scaling Groups

Ensure there are no Amazon Auto Scaling Groups with suspended processes.

Unused Launch Configuration

Identify and remove unused AWS Auto Scaling Launch Configuration templates.

Use Approved AMIs for App-Tier ASG Launch Configurations

Ensure Auto Scaling Group launch configuration for app tier is configured to use an approved Amazon Machine Image.

Use Approved AMIs for Web-Tier ASG Launch Configurations

Ensure Auto Scaling Group launch configuration for web tier is configured to use an approved Amazon Machine Image.

Web-Tier Auto Scaling Group associated ELB

Ensure web-tier Auto Scaling Group has an associated Elastic Load Balancer.

AWS Backup

AWS Backup Service Lifecycle Configuration

Ensure Amazon Backup plans have a compliant lifecycle configuration enabled.

Check for Protected Amazon Backup Resource Types

Ensure that the appropriate resource types are protected by Amazon Backup within your AWS account.

Configure AWS Backup Vault Access Policy

Prevent deletion of backups using an Amazon Backup vault resource-based access policy.

AWS Budgets

Budget Overrun

Cost of '[Limit details eg Service: Lambda]' overruns the budget limit

Budget Overrun Forecast

Cost of '[Limit details eg Service: Lambda]' is estimated to overrun the budget limit.

Cost Fluctuation

Cost of '[Limit details eg Service: Lambda]' in the current period has fluctuated beyond the defined percentage limit of the previous period.

Cost Fluctuation Forecast

Cost of '[Limit details eg Service: Lambda]' in the current period is forecasted to fluctuate beyond the defined percentage limit of the previous period.

Current Contact Details

Ensure valid contact information for all your Amazon Web Services accounts.

Detailed billing

Ensure Detailed Billing is enabled for your Amazon Web Services account.

AWS CloudFormation

AWS CloudFormation Deletion Policy in Use

Ensure a deletion policy is used for your Amazon CloudFormation stacks.

AWS CloudFormation Drift Detection

Ensure that Amazon CloudFormation stacks have not been drifted.

AWS CloudFormation In Use

Ensure CloudFormation service is in use for defining your cloud architectures on Amazon Web Services

AWS CloudFormation Stack Failed Status

Ensure AWS CloudFormation stacks are not in Failed mode for more than 6 hours

AWS CloudFormation Stack Policy

Ensure CloudFormation stack policies are set to prevent accidental updates to stack resources.

CloudFormation Stack with IAM Role

Ensure that the IAM role associated with your AWS CloudFormation stack grants least privilege.

Enable AWS CloudFormation Stack Notifications

Ensure your AWS CloudFormation stacks are integrated with Simple Notification Service (SNS).

Enable AWS CloudFormation Stack Termination Protection

Ensure Termination Protection feature is enabled for your AWS CloudFormation stacks.

snapshots.

Use KMS Customer Master Keys for AWS Backup

Ensure that your backups are encrypted at rest using KMS Customer Master Keys (CMKs).

Amazon CloudFront

CloudFront Compress Objects Automatically

Ensure that AWS Cloudfront web distributions are configured to compress objects (files) automatically.

CloudFront Geo Restriction

Ensure geo restriction is enabled within CloudFront distribution.

CloudFront In Use

Ensure AWS CloudFront CDN service is in use for fast and secure web content delivery.

CloudFront Insecure Origin SSL Protocols

Ensure AWS CloudFront distributions origin(s) do not use insecure SSL protocols.

CloudFront Integrated With WAF

Ensure your Cloudfront CDN distributions are integrated with AWS WAF.

CloudFront Logging Enabled

Ensure AWS Cloudfront CDN distributions have access logging enabled.

CloudFront Security Policy

Ensure AWS CloudFront distributions are using improved security policies for HTTPS connections.

CloudFront Traffic To Origin Unencrypted

Ensure the traffic between the AWS CloudFront distributions and their origins is encrypted.

CloudFront Viewer Protocol Policy

Configure HTTP to HTTPS redirects for your CloudFront distribution viewer protocol policy.

Enable Origin Access Identity for CloudFront Distributions with S3 Origin

Ensure your AWS Cloudfront distributions are using an origin access identity for their origin S3 buckets.

Enable Origin Failover for CloudFront Distributions

Ensure that AWS CloudFront distributions are using Origin Failover feature to optimize their high availability.

FieldLevel Encryption

Ensure that Amazon CloudFront web distributions enforce field-level encryption.

Use Cloudfront Content Distribution Network

Use AWS Cloudfront Content Distribution Network for secure web content delivery.

AWS CloudTrail

AWS CloudTrail Configuration Changes

CloudTrail configuration changes have been detected within your Amazon Web Services account.

Avoid Duplicate Entries in Amazon CloudTrail Logs

Ensure that AWS CloudTrail trails are not duplicating global service events in their aggregated log files."

CloudTrail Bucket MFA Delete Enabled

Ensure AWS CloudTrail logging bucket has MFA Delete feature enabled.

CloudTrail Bucket Publicly Accessible

Ensure CloudTrail trail logging buckets are not publicly accessible.

CloudTrail Data Events

Ensure Data events are included into Amazon CloudTrail trails configuration.

CloudTrail Delivery Failing

Ensure Amazon CloudTrail trail log files are delivered as expected.

CloudTrail Enabled

Ensure AWS CloudTrail trails are enabled for all AWS regions.

CloudTrail Global Services Enabled

Ensure AWS CloudTrail trails track API calls for global services such as IAM, STS and CloudFront.

CloudTrail Integrated With CloudWatch

Ensure CloudTrail event monitoring with CloudWatch is enabled.

CloudTrail Log File Integrity Validation

Ensure your AWS CloudTrail trails have log file integrity validation enabled.

CloudTrail Logs Encrypted

Ensure your AWS CloudTrail logs are encrypted using AWS KMS-Managed Keys (SSE-KMS).

CloudTrail Management Events

Ensure management events are included into AWS CloudTrail trails configuration.

CloudTrail S3 Bucket

Ensure that AWS CloudTrail trail uses the designated Amazon S3 bucket.

CloudTrail S3 Bucket Logging Enabled

Ensure AWS CloudTrail buckets have server access logging enabled.

Enable Object Lock for CloudTrail S3 Buckets

Ensure that AWS CloudTrail S3 buckets use Object Lock for data protection and regulatory compliance.

Amazon CloudWatch

Billing Alarm

Ensure your AWS costs are being monitored using a CloudWatch billing alarm.

Amazon CloudWatch Events

AWS CloudWatch Events In Use

Ensure CloudWatch Events is in use to help you respond to operational changes within your AWS resources.

Event Bus Exposed

Ensure that your AWS CloudWatch event bus is not exposed to everyone.

EventBus Cross Account Access

Ensure that AWS CloudWatch event buses do not allow unknown cross-account access for delivery of events.

Amazon CloudWatch Logs

AWS Config Changes Alarm

Ensure AWS Config configuration changes are being monitored using CloudWatch alarms.

AWS Console Sign In Without MFA

Monitor for AWS Console Sign-In Requests Without MFA

AWS Organizations Changes Alarm

Ensure Amazon Organizations changes are being monitored using AWS CloudWatch alarms.

Authorization Failures Alarm

Ensure any unauthorized API calls made within your AWS account are being monitored using CloudWatch alarms.

CMK Disabled or Scheduled for Deletion Alarm

Ensure AWS CMK configuration changes are being monitored using CloudWatch alarms.

CloudTrail Changes Alarm

Ensure all AWS CloudTrail configuration changes are being monitored using CloudWatch alarms.

Console Sign-in Failures Alarm

Ensure your AWS Console authentication process is being monitored using CloudWatch alarms.

Create CloudWatch Alarm for VPC Flow Logs Metric Filter

Ensure that a CloudWatch alarm is created for the VPC Flow Logs metric filter and an alarm action is configured.

EC2 Instance Changes Alarm

Ensure AWS EC2 instance changes are being monitored using CloudWatch alarms.

EC2 Large Instance Changes Alarm

Ensure AWS EC2 large instance changes are being monitored using CloudWatch alarms.

IAM Policy Changes Alarm

Ensure AWS IAM policy configuration changes are being monitored using CloudWatch alarms.

Internet Gateway Changes Alarm

Ensure AWS VPC Customer/Internet Gateway configuration changes are being monitored using CloudWatch alarms.

Metric Filter for VPC Flow Logs CloudWatch Log Group

Ensure that a log metric filter for the CloudWatch group assigned to the VPC Flow Logs is created.

Network ACL Changes Alarm

Ensure AWS Network ACLs configuration changes are being monitored using CloudWatch alarms.

Root Account Usage Alarm

Ensure Root Account Usage is being monitored using CloudWatch alarms.

Route Table Changes Alarm

Ensure AWS Route Tables configuration changes are being monitored using CloudWatch alarms.

S3 Bucket Changes Alarm

Ensure AWS S3 Buckets configuration changes are being monitored using CloudWatch alarms.

Security Group Changes Alarm

Ensure AWS security groups configuration changes are being monitored using CloudWatch alarms.

VPC Changes Alarm

Ensure AWS VPCs configuration changes are being monitored using CloudWatch alarms.

Amazon Comprehend

Enable Encryption for AWS Comprehend Analysis Job Results

Ensure that AWS Comprehend analysis job results stored in Amazon S3 are encrypted at rest.

AWS Compute Optimizer

Compute Optimizer Auto Scaling Group Findings

AWS Config

AWS Config Configuration Changes

AWS Config service configuration changes have been detected within your Amazon Web Services account.

AWS Config Enabled

Ensure AWS Config is enabled in all regions to get the optimal visibility of the activity on your account.

AWS Config Global Resources

Ensure Global resources are included into Amazon Config service configuration.

AWS Config Referencing Missing S3 Bucket

Ensure AWS Config service is using an active S3 bucket to store configuration changes files.

Config Delivery Failing

Ensure Amazon Config log files are delivered as expected.

AWS ConfigService

AWS Custom Rule

Ensure that all evaluation results returned for your AWS Config rules are compliant.

AWS Cost Explorer

Cost Anomaly Detection Findings

Ensure that unusual AWS spend is analyzed and mitigated using Amazon Cost Anomaly Detection.

Cost Anomaly Detection Monitor in Use

Ensure that a Cost Anomaly Detection monitor is running within your AWS cloud account.

Amazon DynamoDB Accelerator

Cluster Encryption

Ensure Amazon DynamoDB Accelerator (DAX) clusters enforce Server-Side Encryption (SSE).

Amazon Data Lifecycle Manager

Use AWS DLM to Automate EBS Snapshot Lifecycle

Use Amazon Data Lifecycle Manager (DLM) to automate EBS volume snapshots management.

AWS Database Migration Service

DMS Auto Minor Version Upgrade

Ensure that Amazon DMS replication instances have Auto Minor Version Upgrade feature enabled.

DMS Multi-AZ

Ensure that Amazon DMS replication instances have the Multi-AZ feature enabled

DMS Replication Instances Encrypted with KMS CMKs

Ensure that Amazon DMS replication instances are encrypted with KMS Customer Master Keys (CMKs).

Publicly Accessible DMS Replication Instances

Ensure that AWS DMS replication instances are not publicly accessible and prone to security risks.

Amazon DocumentDB

DocumentDB Clusters Encrypted with KMS CMKs

Ensure that Amazon DocumentDB clusters are encrypted with KMS Customer Master Keys (CMKs).

DocumentDB Encryption Enabled

Ensure that Amazon DocumentDB clusters data is encrypted at rest.

DocumentDB Sufficient Backup Retention Period

Ensure AWS DocumentDB clusters have a sufficient backup retention period set for compliance purposes.

Log Exports for DocumentDB

Ensure that your Amazon EC2 instances are optimized for better cost and performance.

Compute Optimizer Lambda Function Findings

Ensure that your Amazon Lambda functions are optimized for better performance and cost.

Amazon DynamoDB

AWS KMS Customer Master Keys for Table Encryption

Ensure that Amazon DynamoDB data is encrypted using AWS-managed Customer Master Keys.

DynamoDB Backup and Restore

Ensure on-demand backup and restore functionality is in use for AWS DynamoDB tables.

DynamoDB Continuous Backups

Ensure Amazon DynamoDB tables have continuous backups enabled.

Unused Table

Identify and remove any unused AWS DynamoDB tables to optimize AWS costs.

Amazon Elastic Block Store (EBS)

Amazon EBS Public Snapshots

Ensure that your Amazon EBS volume snapshots are not accessible to all AWS accounts.

App-Tier EBS Encrypted

Ensure all AWS EBS volumes for app tier are encrypted.

EBS Encrypted

Ensure that existing Elastic Block Store (EBS) attached volumes are encrypted to meet security and compliance requirements.

EBS Encrypted With KMS Customer Master Keys

Ensure EBS volumes are encrypted with KMS CMKs in order to have full control over data encryption and decryption.

EBS General Purpose SSD

Ensure EC2 instances are using General Purpose SSD (gp2) EBS volumes instead of Provisioned IOPS SSD (io1) volumes to optimize AWS EBS costs.

EBS Snapshot Encrypted

Ensure Amazon EBS snapshots are encrypted to meet security and compliance requirements.

EBS Volume Naming Conventions

Ensure EBS volumes are using proper naming conventions to follow AWS tagging best practices.

EBS Volumes Attached To Stopped EC2 Instances

Identify Amazon EBS volumes attached to stopped EC2 instances (i.e. unused EBS volumes).

EBS Volumes Recent Snapshots

Ensure AWS Elastic Block Store (EBS) volumes have recent snapshots available for point-in-time recovery.

EBS Volumes Too Old Snapshots

Identify and remove old AWS Elastic Block Store (EBS) volume snapshots for cost optimization.

Enable Encryption by Default for EBS Volumes

Ensure that your new Amazon EBS volumes are always encrypted in the specified AWS region.

Idle EBS Volume

Identify idle AWS EBS volumes and delete them in order to optimize your AWS costs.

Unused EBS Volumes

Identify and remove any unattached Elastic Block Store volumes to improve cost optimization and security.

Web-Tier EBS Encrypted

Ensure all AWS EBS volumes for web tier are encrypted.

Amazon EC2

AMI Naming Conventions

Ensure AWS AMIs are using proper naming conventions to follow AWS tagging best practices.

AWS AMI Encryption

Ensure that your existing AMIs are encrypted to meet security and compliance requirements.

Account Instance Limit

Ensure your AWS account does not reach the limit set by Amazon for the number of instances.

App-Tier EC2 Instance Using IAM Roles

Ensure an IAM Role for Amazon EC2 is created for app tier.

App-Tier Publicly Shared AMI

Ensure all customer owned Amazon Machine Images for app tier are not shared publicly.

Approved/Golden AMIs

Ensure all AWS EC2 instances are launched from approved AMIs.

Blocklisted AMIs

Ensure there are no AWS EC2 instances launched from blocklisted AMIs.

Check for EC2 Instances with Blocklisted Instance Types

Ensure there is no EC2 instance with the instance type blocklisted, available in your AWS account.

Check for Unrestricted Memcached Access

Ensure that no security group allows unrestricted inbound access on TCP/UDP port 11211 (Memcached).

Check for Unrestricted Redis Access

Ensure that no security group allows unrestricted inbound access on TCP port 6379 (Redis).

Check for vCPU-Based EC2 Instance Limit

Ensure that your EC2 instances do not reach the limit set by AWS for the number of vCPUs.

Default Security Group Unrestricted

Ensure default security groups restrict all public traffic to follow AWS security best practices.

Default Security Groups In Use

Ensure default EC2 security groups are not in use in order to follow AWS security best practices.

Descriptions for Security Group Rules

Ensure AWS EC2 security group rules have descriptive text for organization and documentation.

EC2 AMI Too Old

Check for any AMIs older than 180 days available within your AWS account.

EC2 Desired Instance Type

Ensure all your AWS EC2 instances are of a given instance type (e.g. m3.medium).

EC2 Instance Counts

Ensure your AWS account has not reached the limit set for the number of EC2 instances.

EC2 Instance Dedicated Tenancy

Ensure EC2 dedicated instances are regularly reviewed for cost optimization (informational).

EC2 Instance Detailed Monitoring

Ensure that detailed monitoring is enabled for the AWS EC2 instances that you need to monitor closely.

EC2 Instance Generation

Ensure your AWS servers are using the latest generation of EC2 instances for price-performance improvements.

EC2 Instance In VPC

Ensure EC2 instances are launched using the EC2-VPC platform instead of EC2-Classic outdated platform.

EC2 Instance Naming Conventions

Ensure EC2 Instances are using proper naming conventions to follow AWS tagging best practices.

EC2 Instance Not In Public Subnet

EC2 Instance Security Group Rules Counts

Ensure that the security group(s) associated with an EC2 instance does not have an excessive number of rules defined.

EC2 Instance Tenancy

Ensure EC2 instances have the required tenancy for security and regulatory compliance requirements.

EC2 Instance Termination Protection

Ensure Termination Protection feature is enabled for EC2 instances that are not part of ASGs.

EC2 Instance Too Old

Check for running AWS EC2 instances older than 180 days available within your AWS account.

EC2 Instance Using IAM Roles

Use Instance Profiles/IAM Roles to appropriately grant permissions to applications running on amazon EC2 instances

EC2 Reserved Instance Payment Failed

Ensure that none of your AWS EC2 Reserved Instance purchases have been failed.

EC2 Reserved Instance Payment Pending

Ensure that none of your AWS EC2 Reserved Instance purchases are pending.

EC2 Reserved Instance Recent Purchases

Ensure EC2 Reserved Instance purchases are regularly reviewed for cost optimization (informational).

EC2-Classic Elastic IP Address Limit Checkup

Ensure that your account does not reach the limit set by AWS for the number of allocated Elastic IPs.

EC2-VPC Elastic IP Address Limit Checkup

Ensure that your account does not reach the limit set by AWS for the number of Elastic IPs.

Enable AWS EC2 Hibernation

Ensure that Hibernation feature is enabled for EBS-backed EC2 instances to retain memory state across instance stop/start cycles.

Idle EC2 Instance

Identify idle AWS EC2 instances and stop or terminate them in order to optimize AWS costs.

Instance In Auto Scaling Group

Ensure every EC2 instance is launched inside an Auto Scaling Group (ASG) in order to follow AWS reliability and security best practices.

Overutilized AWS EC2 Instances

Identify overutilized EC2 instances and upgrade them to optimize application response time.

Publicly Shared AMI

Ensure your Amazon Machine Images (AMIs) are not accessible to all AWS accounts.

Reserved Instance Lease Expiration In The Next 30 Days

Ensure Amazon EC2 Reserved Instances (RI) are renewed before expiration.

Reserved Instance Lease Expiration In The Next 7 Days

Ensure Amazon EC2 Reserved Instances (RI) are renewed before expiration.

Security Group Excessive Counts

Ensure your AWS account does not have an excessive number of security groups per region.

Security Group Name Prefixed With 'launch-wizard'

Ensure EC2 security groups prefixed with "launch-wizard" are not in use in order to follow AWS security best practices.

Security Group Naming Conventions

Ensure security groups are using proper naming conventions to follow AWS tagging best practices.

Security Group Port Range

Ensure there are no EC2 security groups in your AWS account that open range of ports to allow incoming traffic.

Security Group Rules Counts

Ensure your EC2 security groups do not have an excessive number of rules defined.

SecurityGroup RFC 1918

Ensure no EC2 security group allows inbound traffic from RFC-1918 CIDRs in order to follow AWS security best practices.

Unassociated Elastic IP Addresses

Identify and remove any unassociated Elastic IP (EIP) addresses for cost optimization.

Underutilized EC2 Instance

Identify underutilized EC2 instances and downsize them in order to optimize your AWS costs.

Unrestricted CIFS Access

Unrestricted HTTP Access

Ensure no security group allows unrestricted inbound access to TCP port 80 (HTTP).

Unrestricted HTTPS Access

Ensure no security group allows unrestricted inbound access to TCP port 443 (HTTPS).

Unrestricted ICMP Access

Ensure no security group allows unrestricted inbound access using Internet Control Message Protocol (ICMP).

Unrestricted Inbound Access on Uncommon Ports

Ensure no EC2 security group allows unrestricted inbound access to any uncommon ports.

Unrestricted MongoDB Access

Ensure no security group allows unrestricted ingress access to MongoDB port 27017

Unrestricted MsSQL Access

Ensure no security group allows unrestricted inbound access to TCP port 1433 (MSSQL).

Unrestricted MySQL Access

Ensure no security group allows unrestricted inbound access to TCP port 3306 (MySQL).

Unrestricted NetBIOS Access

Ensure no AWS EC2 security group allows unrestricted inbound access to TCP port 139 and UDP ports 137 and 138 (NetBIOS).

Unrestricted Oracle Access

Ensure no security group allows unrestricted inbound access to TCP port 1521 (Oracle Database).

Unrestricted Outbound Access on All Ports

Ensure that your EC2 security groups do not allow unrestricted outbound/egress access.

Unrestricted PostgreSQL Access

Ensure no security group allows unrestricted inbound access to TCP port 5432 (PostgreSQL Database).

Unrestricted RDP Access

Ensure no AWS EC2 security group allows unrestricted inbound access to TCP port 3389 (RDP).

Unrestricted RPC Access

Ensure no security group allows unrestricted inbound access to TCP port 135 (RPC).

Unrestricted SMTP Access

- Ensure no AWS EC2 security group allows unrestricted inbound access to TCP port 25 (SMTP).

Unrestricted SSH Access

Ensure no AWS EC2 security group allows unrestricted inbound access to TCP port 22 (SSH).

Unrestricted Telnet Access

Ensure no AWS EC2 security group allows unrestricted inbound access to TCP port 23 (Telnet).

Unused AMI

Identify and remove any unused Amazon Machine Images (AMIs) to optimize AWS costs.

Unused AWS EC2 Key Pairs

Ensure unused AWS EC2 key pairs are decommissioned to follow AWS security best practices.

Unused EC2 Reserved Instances

Ensure that your Amazon EC2 Reserved Instances are being fully utilized.

Unused Elastic Network Interfaces

Ensure unused AWS Elastic Network Interfaces (ENIs) are removed to follow best practices.

Web-Tier EC2 Instance Using IAM Roles

Ensure an IAM Role for Amazon EC2 is created for web tier.

Web-Tier Publicly Shared AMI

Ensure all customer owned Amazon Machine Images for web tier are not shared publicly.

UDP port 53 (DNS).

Unrestricted Elasticsearch Access

Ensure no security group allows unrestricted inbound access to TCP port 9200 (Elasticsearch).

Unrestricted FTP Access

Ensure no EC2 security group allows unrestricted inbound access to TCP ports 20 and 21 (FTP).

Amazon Elastic Container Registry

ECR Repository Exposed

Ensure that AWS Elastic Container Registry (ECR) repositories are not exposed to everyone.

Enable Scan on Push for ECR Container Images

Ensure that each Amazon ECR container image is automatically scanned for vulnerabilities when pushed to a repository.

Lifecycle Policy in Use

Ensure that Amazon ECR image repositories are using lifecycle policies for cost optimization.

Repository Cross Account Access

Ensure that Amazon ECR repositories do not allow unknown cross account access.

Amazon Elastic Container Service (ECS)

Check for Amazon ECS Service Placement Strategy

Ensure that your Amazon ECS cluster services are using optimal placement strategies.

Check for ECS Container Instance Agent Version

Ensure that your Amazon ECS instances are using the latest ECS container agent version.

Check for Fargate Platform Version

Ensure that your Amazon ECS cluster services are using the latest Fargate platform version.

ECS Task Log Driver in Use

Ensure that a log driver has been defined for each active Amazon ECS task definition.

Enable CloudWatch Container Insights

Ensure that CloudWatch Container Insights feature is enabled for your AWS ECS clusters.

Monitor Amazon ECS Configuration Changes

Amazon Elastic Container Service (ECS) configuration changes have been detected in your AWS account.

Amazon Elastic File System (EFS)

AWS KMS Customer Master Keys for EFS Encryption

Ensure EFS file systems are encrypted with KMS Customer Master Keys (CMKs) in order to have full control over data encryption and decryption.

EFS Encryption Enabled

Ensure encryption is enabled for AWS EFS file systems to protect your data at rest.

Amazon Elastic Kubernetes Service (EKS)

EKS Security Groups

Ensure that AWS EKS security groups are configured to allow incoming traffic only on TCP port 443.

Enable Envelope Encryption for EKS Kubernetes Secrets

Ensure that envelope encryption of Kubernetes secrets using Amazon KMS is enabled.

Kubernetes Cluster Logging

Ensure that EKS control plane logging is enabled for your Amazon EKS clusters.

Kubernetes Cluster Version

Ensure that the latest version of Kubernetes is installed on your Amazon EKS clusters.

Monitor Amazon EKS Configuration Changes

Amazon EKS configuration changes have been detected within your Amazon Web Services account.

Publicly Accessible Cluster Endpoints

Ensure that AWS EKS cluster endpoint access is not public and prone to security risks.

Elastic Load Balancing

App-Tier ELB Listener Security

Ensure app tier ELB is using HTTPS/SSL listener.

App-Tier ELB Security Policy

Ensure app tier ELB have the latest SSL security policy configured.

App-Tier ELBs Health Check

Ensure app tier Elastic Load Balancer has application layer health check configured.

Classic Load Balancer

Ensure HTTP/HTTPS applications are using Application Load Balancer instead of Classic Load Balancer for cost and web traffic distribution optimization.

ELB Access Log

Ensure that your AWS Elastic Load Balancers use access logging to analyze traffic patterns and identify and troubleshoot security issues.

ELB Connection Draining Enabled

With Connection Draining feature enabled, if an EC2 backend instance fails health checks the Elastic Load Balancer will not send any new requests to the unhealthy instance. However, it will still allow existing (in-flight) requests to complete for the duration of the configured timeout.

ELB Cross-Zone Load Balancing Enabled

Ensure high availability for your ELBs by using Cross-Zone Load Balancing with multiple subnets in different AZs.

ELB Insecure SSL Ciphers

Ensure your ELBs do not use insecure or deprecated SSL ciphers.

ELB Insecure SSL Protocols

Ensure your ELBs do not use insecure SSL protocols.

ELB Instances Distribution Across AZs

Ensure even distribution of backend instances registered to an ELB across Availability Zones.

ELB Listener Security

Ensure that your AWS ELBs listeners are using a secure protocol (HTTPS or SSL).

ELB Minimum Number Of EC2 Instances

Ensure there is a minimum number of two healthy backend instances associated with each ELB.

ELB Security Group

Ensure there are valid security groups associated with your Elastic Load Balancer.

ELB Security Policy

Ensure AWS ELBs are using the latest predefined security policies.

Idle Elastic Load Balancer

Identify idle Elastic Load Balancers (ELBs) and terminate them in order to optimize AWS costs.

Internet Facing ELBs

Ensure Amazon internet-facing ELBs/ALBs are regularly reviewed for security purposes (informational).

Unused Elastic Load Balancers

Identify and remove any unused Elastic Load Balancers for cost optimization.

Web-Tier ELB Listener Security

Ensure web tier ELB is using HTTPS/SSL listener.

Web-Tier ELB Security Policy

Ensure web tier ELB have the latest SSL security policy configured.

Web-Tier ELBs Health Check

Ensure web tier Elastic Load Balancer has application layer health check configured.

Elastic Load Balancing V2

Configure Multiple Availability Zones for Gateway Load Balancers

Ensure that Amazon Gateway Load Balancers are using Multi-AZ configurations.

Drop Invalid Header Fields for Application Load Balancers

Ensure that Drop Invalid Header Fields feature is enabled for your Application Load Balancers to remove non-standard headers.

ELBv2 ALB Listener Security

Ensure that your Application Load Balancer (ALB) listeners are using a secure protocol such as HTTPS.

ELBv2 ALB Security Group

Ensure that your Amazon ELBv2 load balancers have secure and valid security groups.

ELBv2 ALB Security Policy

Ensure AWS Application Load Balancers (ALBs) are using the latest predefined security policy.

ELBv2 Access Log

Ensure access logging is enabled for your AWS ALBs to follow security best practices.

ELBv2 Elastic Load Balancing Deletion Protection

Ensure Deletion Protection feature is enabled for your AWS load balancers to follow security best practices.

ELBv2 Minimum Number of EC2 Target Instances

Ensure there is a minimum number of two healthy target instances associated with each AWS ELBv2 load balancer.

ELBv2 NLB Listener Security

Ensure that your AWS Network Load Balancer listeners are using a secure protocol such as TLS

Enable HTTP to HTTPS Redirect for Application Load Balancers

Ensure that your Application Load Balancers have a rule that redirects HTTP traffic to HTTPS.

Internet Facing ELBv2 Load Balancers

Ensure internet-facing ELBv2 load balancers are regularly reviewed for security reasons (informational).

Network Load Balancer Security Policy

Ensure that AWS Network Load Balancers are using the latest predefined security policy.

Unused ELBv2 Load Balancers

Identify unused Elastic Load Balancers (ELBv2) and delete them in order to reduce AWS costs.

Amazon EMR

AWS EMR Instance Type Generation

Ensure AWS EMR clusters are using the latest generation of instances for performance and cost optimization.

Cluster In VPC

Ensure AWS EMR clusters are launched in a Virtual Private Cloud (i.e. are using EC2-VPC platform).

EMR Cluster Logging

Ensure AWS Elastic MapReduce (EMR) clusters capture detailed log data to Amazon S3.

EMR Desired Instance Type

Ensure that all your Amazon EMR cluster instances are of given instance types.

EMR In-Transit and At-Rest Encryption

Ensure in-transit and at-rest encryption is enabled for Amazon EMR clusters.

EMR Instances Counts

Ensure fewer Amazon EMR cluster instances than the provided limit in your AWS account.

Amazon ElastiCache

ElastiCache Cluster Default Port

Ensure AWS ElastiCache clusters are not using the default ports set for Redis and Memcached cache engines.

ElastiCache Cluster In VPC

Ensure Amazon ElastiCache clusters are deployed into a Virtual Private Cloud (VPC)

ElastiCache Desired Node Type

Ensure that all your Amazon ElastiCache cluster cache nodes are of given types.

ElastiCache Engine Version

Ensure that the latest version of Redis/Memcached is used for your AWS ElastiCache clusters.

ElastiCache Instance Generation

Ensure ElastiCache clusters are using the latest generation of nodes for cost and performance improvements.

ElastiCache Nodes Counts

Ensure your AWS account has not reached the limit set for the number of ElastiCache cluster nodes.

ElastiCache Redis In-Transit and At-Rest Encryption

Ensure in-transit and at-rest encryption is enabled for Amazon ElastiCache Redis clusters.

ElastiCache Redis Multi-AZ

Ensure Amazon ElastiCache Redis clusters have the Multi-AZ feature enabled.

ElastiCache Reserved Cache Node Coverage

Ensure that your Amazon ElastiCache usage is covered by ElastiCache RI reservations.

ElastiCache Reserved Cache Node Lease Expiration In The Next 30 Days

Ensure Amazon ElastiCache Reserved Cache Nodes (RCN) are renewed before expiration.

ElastiCache Reserved Cache Node Lease Expiration In The Next 7 Days

Ensure Amazon ElastiCache Reserved Cache Nodes (RCN) are renewed before expiration.

ElastiCache Reserved Cache Node Payment Failed

Ensure AWS ElastiCache Reserved Node purchases have not failed.

ElastiCache Reserved Cache Node Payment Pending

Ensure AWS ElastiCache Reserved Node purchases are not pending.

ElastiCache Reserved Cache Node Recent Purchases

Ensure ElastiCache Reserved Cache Node purchases are regularly reviewed for cost optimization (informational).

Idle AWS ElastiCache Nodes

Identify any idle AWS ElastiCache nodes and terminate them in order to optimize your AWS costs.

Unused ElastiCache Reserved Cache Nodes

Ensure that your ElastiCache Reserved Cache Nodes are being utilized.

AWS Elastic Beanstalk

Elastic Beanstalk Enhanced Health Reporting

Ensure Enhanced Health Reporting is enabled for your AWS Elastic Beanstalk environment(s).

Elastic Beanstalk Managed Platform Updates

Ensure managed platform updates are enabled for your AWS Elastic Beanstalk environment(s).

Elastic Beanstalk Persistent Logs

Ensure persistent logs are enabled for your Amazon Elastic Beanstalk environment(s).

Enable Access Logs

Ensure that access logging is enabled for your Elastic Beanstalk environment load balancer.

Enable Elastic Beanstalk Environment Notifications

Enable alert notifications for important events triggered within your Amazon Elastic Beanstalk environment.

Amazon Elasticsearch Service

AWS Elasticsearch Slow Logs

Ensure that Slow Logs feature is enabled for your Amazon Elasticsearch (ES) clusters.

ElasticSearch ClusterStatus

Ensure that Amazon ElasticSearch (ES) clusters are healthy (Green).

ElasticSearch Domain Encrypted with KMS CMKs

Ensure AWS ElasticSearch domains are encrypted with KMS Customer Master Keys.

ElasticSearch Free Storage Space

Identify AWS ElasticSearch clusters with low free storage space and scale them to optimize their performance.

ElasticSearch Node To Node Encryption

Ensure node-to-node encryption is enabled for your Amazon ElasticSearch (ES) clusters.

Elasticsearch Accessible Only From Safelisted IP Addresses

Ensure only safelisted IP addresses can access your Amazon Elasticsearch domains.

Elasticsearch Cross Account Access

Ensure Amazon Elasticsearch clusters do not allow unknown cross account access.

Elasticsearch Dedicated Master Enabled

Ensure Amazon Elasticsearch clusters are using dedicated master nodes to increase the production environment stability.

Elasticsearch Desired Instance Type

Ensure that all your Amazon Elasticsearch cluster instances are of given instance types.

Elasticsearch Domain Exposed

Ensure Amazon Elasticsearch Service (ES) domains are not exposed to everyone.

Elasticsearch Domain In VPC

Ensure AWS Elasticsearch domains are accessible from a Virtual Private Cloud (VPC).

Elasticsearch General Purpose SSD

Ensure Elasticsearch nodes are using General Purpose SSD storage instead of Provisioned IOPS SSD storage to optimize the service costs.

Elasticsearch Instance Counts

Ensure fewer AWS Elasticsearch cluster instances than provided limit in your AWS account.

Elasticsearch Reserved Instance Lease Expiration In The Next 30 Days

Ensure Amazon Elasticsearch (ES) Reserved Instances are renewed before expiration.

Elasticsearch Reserved Instance Lease Expiration In The Next 7 Days

Ensure Amazon Elasticsearch (ES) Reserved Instances are renewed before expiration.

Elasticsearch Reserved Instance Payment Failed

Ensure AWS Elasticsearch Reserved Instance (RI) purchases have not failed.

Elasticsearch Reserved Instance Payment Pending

Ensure AWS Elasticsearch Reserved Instance (RI) purchases are not pending.

Elasticsearch Reserved Instance Recent Purchases

Ensure Elasticsearch Reserved Instance (RI) purchases are regularly reviewed (informational).

Elasticsearch Version

Ensure that you always use the latest version of Elasticsearch engine for your AWS Elasticsearch domains.

Elasticsearch Zone Awareness Enabled

Ensure high availability for your Amazon Elasticsearch clusters by enabling the Zone Awareness feature.

Encryption At Rest

Ensure at-rest encryption is enabled for your Amazon ElasticSearch domains.

Idle Elasticsearch Clusters

Identify any idle AWS Elasticsearch clusters and delete them in order to optimize your AWS costs.

Amazon FSx

Use KMS Customer Master Keys for FSx Windows File Server File Systems

Ensure AWS FSx for Windows File Server file systems data is encrypted using AWS

AWS Glue

CloudWatch Logs Encryption Mode

Ensure that at-rest encryption is enabled when writing Amazon Glue logs to CloudWatch Logs.

Glue Data Catalog Encrypted With KMS Customer Master Keys

Ensure that Amazon Glue Data Catalogs enforce data-at-rest encryption using KMS CMKs.

Glue Data Catalog Encryption At Rest

Ensure that Amazon Glue Data Catalog objects and connection passwords are encrypted.

Job Bookmark Encryption Mode

Ensure that encryption at rest is enabled for Amazon Glue job bookmarks.

S3 Encryption Mode

Ensure that at-rest encryption is enabled when writing AWS Glue data to Amazon S3.

Amazon GuardDuty

AWS GuardDuty Configuration Changes

GuardDuty configuration changes have been detected within your Amazon Web Services account.

GuardDuty Enabled

Ensure Amazon GuardDuty is enabled to help you protect your AWS accounts and workloads against security threats.

GuardDuty Findings

Ensure that Amazon GuardDuty findings are highlighted, audited and resolved.

AWS Health

Health Events

Provides real-time insights into the state of your AWS environment and infrastructure.

Firehose Delivery Stream Encryption

Ensure Amazon Kinesis Firehose delivery streams enforce Server-Side Encryption (SSE).

AWS Identity and Access Management (IAM)

AWS Account Root User Activity

Monitor AWS Account Root User Activity

AWS IAM Groups with Admin Privileges

Ensure there are no IAM groups with full administrator permissions within your AWS account.

AWS IAM Password Policy

Ensure AWS account has an IAM strong password policy in use

AWS IAM Server Certificate Size

Ensure that all your SSL/TLS certificates are using either 2048 or 4096 bit RSA keys instead of 1024-bit keys.

AWS IAM Users with Admin Privileges

Ensure there are no IAM users with full administrator permissions within your AWS account.

AWS Multi-Account Centralized Management

Set up, organize and manage your AWS accounts for optimal security and manageability.

Access Keys During Initial IAM User Setup

Ensure no access keys are created during IAM user initial setup with AWS Management Console.

Access Keys Rotated 30 Days

Ensure AWS IAM access keys are rotated on a periodic basis as a security best practice (30 Days).

Access Keys Rotated 45 Days

Ensure AWS IAM access keys are rotated on a periodic basis as a security best practice (45 Days).

Access Keys Rotated 90 Days

Ensure AWS IAM access keys are rotated on a periodic basis as a security best practice (90 Days).

Account Alternate Contacts

Ensure alternate contacts are set to improve the security of your AWS account.

Account Security Challenge Questions

Ensure security challenge questions are enabled and configured to improve the security of your AWS account.

Approved ECS Execute Command Access

Ensure that all access to the ECS Execute Command action is approved

Attach Policy to IAM Roles Associated with App-Tier EC2 Instances

Ensure IAM policy for EC2 IAM roles for app tier is configured.

Attach Policy to IAM Roles Associated with Web-Tier EC2 Instances

Ensure IAM policy for EC2 IAM roles for web tier is configured.

Canary Access Token

Detects when a canary token access key has been used

Check for IAM User Group Membership

Ensure that all Amazon IAM users have group memberships.

Check for Overly Permissive IAM Group Policies

Ensure that Amazon IAM policies attached to IAM groups are not too permissive.

Check for Unapproved IAM Users Existence

Ensure there are no unapproved Amazon IAM users available within your AWS cloud account.

Check for Untrusted Cross-Account IAM Roles

Ensure that AWS IAM roles cannot be used by untrusted accounts via cross-account access feature.

Credentials Last Used

Ensure that unused AWS IAM credentials are decommissioned to follow security best practices.

Cross-Account Access Lacks External ID and MFA

Ensure cross-account IAM roles use either MFA or external IDs to secure the access to AWS resources.

Expired SSL/TLS Certificate

Ensure expired SSL/TLS certificates are removed from AWS IAM.

Hardware MFA for AWS Root Account

IAM Group With Inline Policies

Ensure AWS IAM groups do not have inline policies attached.

IAM Master and IAM Manager Roles

Ensure that IAM Master and IAM Manager roles are active in your AWS cloud account.

IAM Policies With Full Administrative Privileges

Ensure IAM policies that allow full "*:*" administrative privileges are not created.

IAM Policies with Effect Allow and NotAction

Ensure AWS IAM policies do not use "Effect" : "Allow" in combination with "NotAction" element to follow security best practices.

IAM Role Policy Too Permissive

Ensure AWS IAM policies attached to IAM roles are not too permissive.

IAM User Password Expiry 30 Days

Ensure AWS Identity and Access Management (IAM) user passwords are reset before expiration (30 Days).

IAM User Password Expiry 45 Days

Ensure AWS Identity and Access Management (IAM) user passwords are reset before expiration (45 Days).

IAM User Password Expiry 7 Days

Ensure AWS Identity and Access Management (IAM) user passwords are reset before expiration (7 Days).

IAM User Policies

Ensure AWS IAM policies are attached to groups instead of users as an IAM best practice.

IAM User Present

Ensure there is at least one IAM user currently used to access your AWS account.

IAM User With Password And Access Keys

Ensure AWS IAM users have either API access or console access in order to follow IAM security best practices.

IAM Users Unauthorized to Edit Access Policies

Ensure AWS IAM users that are not authorized to edit IAM access policies are decommissioned..

Inactive IAM Console User

Ensure no AWS IAM users have been inactive for a long (specified) period of time.

MFA Device Deactivated

A Multi-Factor Authentication (MFA) device deactivation for an IAM user has been detected.

MFA For IAM Users With Console Password

Ensure Multi-Factor Authentication (MFA) is enabled for all AWS IAM users with AWS Console access.

Pre-Heartbleed Server Certificates

Ensure that your server certificates are not vulnerable to Heartbleed security bug.

Receive Permissions via IAM Groups Only

Ensure that IAM users receive permissions only through IAM groups.

Root Account Access Keys Present

Ensure that your AWS account (root) is not using access keys as a security best practice.

Root Account Active Signing Certificates

Ensure that your AWS root account user is not using X.509 certificates to validate API requests.

Root Account Usage

Ensure root account credentials have not been used recently to access your AWS account.

Root MFA Enabled

Ensure Multi-Factor Authentication (MFA) is enabled for the AWS root account.

SSH Public Keys Rotated 30 Days

Ensure AWS IAM SSH public keys are rotated on a periodic basis as a security best practice.

SSH Public Keys Rotated 45 Days

Ensure IAM SSH public keys are rotated on a periodic basis to adhere to AWS security best practices.

SSH Public Keys Rotated 90 Days

Ensure IAM SSH public keys are rotated on a periodic basis to adhere to AWS security

IAM Configuration Changes

AWS IAM configuration changes have been detected within your Amazon Web Services account.

IAM CreateLoginProfile detected

AWS IAM 'CreateLoginProfile' call has been detected within your Amazon Web Services account.

Support Role

Ensure there is an active Amazon IAM Support Role available within your AWS account.

Unapproved IAM Policy in Use

Ensure there are no unapproved AWS Identity and Access Management (IAM) policies in use.

Unnecessary Access Keys

Ensure there is a maximum of one active access keys available for any single IAM user.

Unnecessary SSH Public Keys

Ensure there is a maximum of one active SSH public keys assigned to any single IAM user.

Unused IAM Group

Ensure AWS IAM groups have at least one user attached as a security best practice.

Unused IAM User

Ensure unused IAM users are removed from AWS account to follow security best practice.

Valid IAM Identity Providers

Ensure valid IAM Identity Providers are used within your AWS account for secure user authentication and authorization.

Amazon Inspector

Amazon Inspector Findings

Ensure that Amazon Inspector Findings are analyzed and resolved.

Check for Amazon Inspector Exclusions

Ensure there are no exclusions found by Amazon Inspector assessment runs.

Days since last Amazon Inspector run

Ensure that Amazon Inspector runs occur every n days.

AWS Key Management Service

App-Tier KMS Customer Master Key (CMK) In Use

Ensure a customer created Customer Master Key (CMK) is created for the app tier.

Database-Tier KMS Customer Master Key (CMK) In Use

Ensure a customer created Customer Master Key (CMK) is created for the database tier.

Existence of Specific AWS KMS CMKs

Ensure that specific Amazon KMS CMKs are available for use in your AWS account.

KMS Cross Account Access

Ensure Amazon KMS master keys do not allow unknown cross account access.

KMS Customer Master Key (CMK) In Use

Ensure KMS Customer Master Keys (CMK) are in use to have full control over the encryption / decryption process.

KMS Customer Master Key Pending Deletion

Identify and recover any KMS Customer Master Keys (CMK) scheduled for deletion.

Key Exposed

Ensure Amazon KMS master keys are not exposed to everyone.

Key Rotation Enabled

Ensure KMS key rotation feature is enabled for all your Customer Master Keys (CMK).

Monitor AWS KMS Configuration Changes

Key Management Service (KMS) configuration changes have been detected within your AWS account.

Unused Customer Master Key

Identify and remove any disabled Customer Master Keys (CMK) to reduce AWS costs.

Web-Tier KMS Customer Master Key (CMK) In Use

Ensure a customer created Customer Master Key (CMK) is created for the web tier.

Amazon Kinesis

Kinesis Server Side Encryption

Ensure Amazon Kinesis streams enforce Server-Side Encryption (SSE).

Kinesis Stream Encrypted With CMK

Ensure AWS Kinesis streams are encrypted with KMS Customer Master Keys for

Ensure SSL/TLS certificates are renewed before their expiration.

SSL/TLS Certificate Expiry 7 Days

Ensure SSL/TLS certificates are renewed before their expiration.

Sign-In Events

AWS sign-in events for IAM and federated users have been detected.

AWS Lambda

Enable Active Tracing

Ensure that tracing (i.e. Lambda support for Amazon X-Ray service) is enabled for your Lambda functions.

Enable Code Signing

Ensure that Code Signing is enabled for Amazon Lambda functions.

Enable Dead Letter Queue for Lambda Functions

Ensure there is a Dead Letter Queue configured for each Lambda function available in your AWS account.

Enable Encryption at Rest for Environment Variables using Customer Master Keys

Ensure that Lambda environment variables are encrypted at rest with Customer Master Keys (CMKs) to gain full control over data encryption/decryption.

Enable Encryption in Transit for Environment Variables

Ensure that encryption in transit is enabled for the Lambda environment variables that store sensitive information.

Enable Enhanced Monitoring for Lambda Functions

Ensure that your Amazon Lambda functions are configured to use enhanced monitoring.

Function Exposed

Ensure that your Amazon Lambda functions are not exposed to everyone.

Lambda Function With Admin Privileges

Ensure no Lambda function available in your AWS account has admin privileges.

Lambda Runtime Environment Version

Ensure that the latest version of the runtime environment is used for your AWS Lambda functions.

Unknown Cross-Account Access

Ensure AWS Lambda functions do not allow unknown cross account access via permission policies.

Using An IAM Role For More Than One Lambda Function

Ensure that Lambda functions don't share the same IAM execution role.

VPC Access for AWS Lambda Functions

Ensure AWS Lambda functions are configured to access resources in a Virtual Private Cloud (VPC).

Amazon MQ

MQ Auto Minor Version Upgrade

Ensure AWS MQ brokers have the Auto Minor Version Upgrade feature enabled.

MQ Deployment Mode

Ensure that your Amazon MQ brokers are using the active/standby deployment mode.

MQ Desired Broker Instance Type

Ensure that all your Amazon MQ broker instances are of a given type.

MQ Engine Version

Ensure that the latest version of Apache ActiveMQ engine is used for your AWS MQ brokers.

MQ Log Exports

Ensure Log Exports feature is enabled for your Amazon MQ brokers.

MQ Network of Brokers

Ensure that Amazon MQ brokers are using the network of brokers configuration.

Publicly Accessible MQ Brokers

Ensure Amazon MQ brokers are not publicly accessible and prone to security risks.

Amazon Managed Streaming for Apache Kafka

Use KMS Customer Master Keys for AWS MSK Clusters

Ensure that your Amazon MSK data is encrypted using AWS KMS Customer Master Keys.

Amazon Macie

Amazon Macie In Use

AWS Macie v2

Amazon Macie Discovery Jobs

Ensure that Amazon Macie data discovery jobs are created and configured within each AWS region.

Amazon Macie Findings

Ensure that Amazon Macie security findings are highlighted, analyzed, and resolved.

Amazon Macie Sensitive Data Repository

Ensure that a data repository bucket is defined for Amazon Macie within each AWS region.

Compliance and Certifications

Amazon Neptune

IAM Database Authentication for Neptune

Ensure IAM Database Authentication feature is enabled for Amazon Neptune clusters.

Neptune Desired Instance Type

Ensure that all your Amazon Neptune database instances are of a given type.

Neptune Auto Minor Version Upgrade

Ensure Amazon Neptune instances have Auto Minor Version Upgrade feature enabled.

Neptune Database Backup Retention Period

Ensure AWS Neptune clusters have a sufficient backup retention period set for compliance purposes.

Neptune Database Encrypted With KMS Customer Master Keys

Ensure that AWS Neptune instances enforce data-at-rest encryption using KMS CMKs.

Neptune Database Encryption Enabled

Ensure that Amazon Neptune graph database instances are encrypted.

Neptune Multi-AZ

Ensure that Amazon Neptune database clusters have the Multi-AZ feature enabled.

AWS Network Firewall

AWS Network Firewall in Use

Ensure that your Amazon VPCs are using AWS Network Firewall.

Enable Deletion Protection for Network Firewalls

Ensure that Deletion Protection feature is enabled for your VPC network firewalls.

AWS Organizations

AWS Organizations Configuration Changes

AWS Organizations configuration changes have been detected within your Amazon Web Services account(s).

AWS Organizations In Use

Ensure Amazon Organizations is in use to consolidate all your AWS accounts into an organization.

Enable All Features

Ensure AWS Organizations All Features is enabled for fine-grained control over which services and actions the member accounts of an organization can access.

Amazon Relational Database Service

Amazon RDS Configuration Changes

Amazon Relational Database Service (RDS) configuration changes have been detected in your AWS account.

Amazon RDS Public Snapshots

Ensure that your Amazon RDS database snapshots are not accessible to all AWS accounts.

Aurora Database Instance Accessibility

Ensure that all database instances within an AWS Aurora cluster have the same accessibility.

Backtrack

Ensure that Amazon Aurora MySQL database clusters have backtracking enabled.

Cluster Deletion Protection

Ensure that Deletion Protection feature is enabled for your Aurora database clusters (provisioned and serverless).

DB Instance Generation

Ensure AWS RDS instances are using the latest generation of instance classes for cost and performance improvements.

Enable AWS RDS Transport Encryption

Ensure AWS RDS SQL Server instances have Transport Encryption feature enabled.

Enable Amazon RDS Storage AutoScaling

Ensure that RDS Storage AutoScaling feature is enabled to support unpredictable database workload.

Enable Aurora Cluster Copy Tags to Snapshots

Ensure that Amazon Aurora clusters have Copy Tags to Snapshots feature enabled.

Enable RDS Log Exports

Ensure Log Exports feature is enabled for your AWS RDS MySQL, Aurora and MariaDB database instances.

Enable RDS Snapshot Encryption

Ensure that AWS RDS snapshots are encrypted to meet security and compliance requirements.

Enable Serverless Log Exports

Ensure Log Exports feature is enabled for your Amazon Aurora Serverless databases.

IAM Database Authentication for RDS

Ensure IAM Database Authentication feature is enabled for your AWS RDS MySQL and PostgreSQL database instances.

Idle RDS Instance

Identify idle AWS RDS database instances and terminate them to optimize AWS costs.

Instance Deletion Protection

Ensure Deletion Protection feature is enabled for your AWS RDS database instances.

Instance Level Events Subscriptions

Ensure RDS event subscriptions are enabled for instance level events.

Overutilized AWS RDS Instances

Identify overutilized RDS instances and upgrade them in order to optimize database workload and response time.

Performance Insights

Ensure Performance Insights feature is enabled for your Amazon RDS database instances.

RDS Auto Minor Version Upgrade

Ensure AWS RDS instances have the Auto Minor Version Upgrade feature enabled.

RDS Automated Backups Enabled

Ensure AWS RDS instances have Automated Backups feature enabled.

RDS Copy Tags to Snapshots

Ensure that Amazon RDS instances have Copy Tags to Snapshots feature enabled.

RDS Default Port

Ensure Amazon RDS database instances are not using the default ports.

RDS Desired Instance Type

Ensure fewer Amazon RDS instances than the established limit in your AWS account.

RDS Encrypted With KMS Customer Master Keys

Ensure RDS instances are encrypted with KMS CMKs in order to have full control over data encryption and decryption.

Ensure event notifications are enabled for your Amazon Relational Database Service (RDS) resources.

RDS Free Storage Space

Identify RDS instances with low free storage space and scale them in order to optimize their performance.

RDS General Purpose SSD

Ensure RDS instances are using General Purpose SSD storage instead of Provisioned IOPS SSD storage to optimize the RDS service costs.

RDS Instance Counts

Ensure fewer Amazon RDS instances than the established limit in your AWS account.

RDS Instance Not In Public Subnet

Ensure no RDS database instances are running within AWS VPC public subnets.

RDS Master Username

Ensure AWS RDS instances are using secure and unique master usernames for their databases.

RDS Multi-AZ

Ensure AWS RDS clusters have the Multi-AZ feature enabled.

RDS Publicly Accessible

Ensure RDS database instances are not publicly accessible and prone to security risks.

RDS Reserved DB Instance Lease Expiration In The Next 30 Days

Ensure Amazon RDS Reserved Instances (RI) are renewed before expiration.

RDS Reserved DB Instance Lease Expiration In The Next 7 Days

Ensure Amazon RDS Reserved Instances (RI) are renewed before expiration.

RDS Reserved DB Instance Payment Failed

Ensure AWS RDS Reserved Instance purchases have not failed.

RDS Reserved DB Instance Payment Pending

Ensure Amazon RDS Reserved Instance purchases are not pending.

RDS Reserved DB Instance Recent Purchases

Ensure RDS Reserved Instance purchases are regularly reviewed for cost optimization (informational).

RDS Sufficient Backup Retention Period

Ensure AWS RDS instances have sufficient backup retention period for compliance purposes.

Security Groups Events Subscriptions

Ensure RDS event subscriptions are enabled for DB security groups.

Underutilized RDS Instance

Identify underutilized RDS instances and downsize them in order to optimize your AWS costs.

Unrestricted DB Security Group

Ensure there aren't any unrestricted DB security groups assigned to your RDS instances.

Unused RDS Reserved Instances

Ensure that your Amazon RDS Reserved Instances are being fully utilized.

Use AWS Backup Service in Use for Amazon RDS

Ensure that Amazon Backup service is used to manage AWS RDS database snapshots.

Conformity Real-Time Threat monitoring

AWS IAM User Created

An AWS Identity and Access Management (IAM) user creation event has been detected.

AWS IAM user has signed in without MFA

Amazon Web Services IAM user authentication without MFA has been detected.

AWS Root user has signed in without MFA

Conformity user authentication without MFA has been detected.

Network configuration change detected

Networking configuration changes have been detected within your Amazon Web Services account.

Root has signed in

Amazon Web Services account authentication using root credentials has been detected.

User activity in blocklisted regions

AWS User/API activity has been detected within blocklisted Amazon Web Services region(s).

User has failed signing in to AWS

Monitor AWS IAM user's failed signing attempts.

Amazon Redshift

Deferred Maintenance

Ensure Deferred Maintenance feature is enabled for your Amazon Redshift clusters.

Enable Redshift User Activity Logging

Ensure that user activity logging is enabled for your Amazon Redshift clusters.

Idle Redshift Cluster

Identify idle AWS Redshift clusters and terminate them in order to optimize AWS costs.

Redshift Automated Snapshot Retention Period

Ensure that retention period is enabled for Amazon Redshift automated snapshots.

Redshift Cluster Allow Version Upgrade

Ensure Version Upgrade is enabled for Redshift clusters to automatically receive upgrades during the maintenance window.

Redshift Cluster Audit Logging Enabled

Ensure audit logging is enabled for Redshift clusters for security and troubleshooting purposes.

Redshift Cluster Default Master Username

Ensure AWS Redshift database clusters are not using "awsuser" (default master user name) for database access.

Redshift Cluster Default Port

Ensure Amazon Redshift clusters are not using port 5439 (default port) for database access.

Redshift Cluster Encrypted

Ensure database encryption is enabled for AWS Redshift clusters to protect your data at rest.

Redshift Cluster Encrypted With KMS Customer Master Keys

Ensure Redshift clusters are encrypted with KMS customer master keys (CMKs) in order to have full control over data encryption and decryption.

Redshift Cluster In VPC

Ensure Amazon Redshift clusters are launched within a Virtual Private Cloud (VPC).

Redshift Cluster Publicly Accessible

Ensure Redshift clusters are not publicly accessible to minimise security risks.

Redshift Desired Node Type

Ensure that your AWS Redshift cluster nodes are of given types.

Redshift Disk Space Usage

Identify AWS Redshift clusters with high disk usage and scale them to increase their storage capacity.

Redshift Instance Generation

Ensure Redshift clusters are using the latest generation of nodes for performance improvements.

Redshift Nodes Counts

Ensure that your AWS account has not reached the limit set for the number of Redshift cluster nodes.

Redshift Parameter Group Require SSL

Ensure AWS Redshift non-default parameter groups require SSL to secure data in transit.

Redshift Reserved Node Coverage

Ensure that your Amazon Redshift usage is covered by RI reservations in order to optimize costs.

Redshift Reserved Node Lease Expiration In The Next 30 Days

Ensure Amazon Redshift Reserved Nodes (RN) are renewed before expiration.

Redshift Reserved Node Lease Expiration In The Next 7 Days

Ensure Amazon Redshift Reserved Nodes (RN) are renewed before expiration.

Redshift Reserved Node Payment Failed

Ensure that none of your AWS Redshift Reserved Node purchases have been failed.

Redshift Reserved Node Payment Pending

Ensure that none of your AWS Redshift Reserved Node (RN) purchases are pending.

Redshift Reserved Node Recent Purchases

Ensure Redshift Reserved Node purchases are regularly reviewed for cost optimization (informational).

Underutilized Redshift Cluster

Identify underutilized Redshift clusters and downsize them in order to optimize AWS

Amazon Web Services root/IAM user authentication from a non-approved country has been detected.

Amazon Route 53

Amazon Route 53 Configuration Changes

Route 53 configuration changes have been detected within your Amazon Web Services account.

Enable DNSSEC Signing for Route 53 Hosted Zones

Ensure that DNSSEC signing is enabled for your Amazon Route 53 Hosted Zones.

Privacy Protection

Ensure that Privacy Protection feature is enabled for your Amazon Route 53 domains.

Remove AWS Route 53 Dangling DNS Records

Ensure dangling DNS records are removed from your AWS Route 53 hosted zones to avoid domain/subdomain takeover.

Route 53 Domain Auto Renew

Ensure your domain names are automatically renewed by AWS Route 53 service.

Route 53 Domain Expired

Ensure expired AWS Route 53 domains names are restored.

Route 53 Domain Expiry 30 Days

Ensure AWS Route 53 domain names are renewed before their expiration.

Route 53 Domain Expiry 45 Days

Ensure AWS Route 53 domain names are renewed before their expiration (45 days before expiration).

Route 53 Domain Expiry 7 Days

Ensure AWS Route 53 domain names are renewed before their expiration.

Route 53 Domain Transfer Lock

Ensure your domain names have the Transfer Lock feature enabled in order to keep them secure.

Route 53 In Use

Ensure AWS Route 53 DNS service is in use for highly efficient DNS management.

Sender Policy Framework In Use

Ensure that Sender Policy Framework (SPF) is used to stop spammers from spoofing your AWS Route 53 domain.

Sender Policy Framework Record Present

Ensure there is an SPF record set for each MX DNS record in order to stop spammers from spoofing your domains.

Amazon Route 53 Domains

Amazon Route 53 Domains Configuration Changes

Route 53 Domains configuration changes have been detected within your Amazon Web Services account.

AWS Resource Groups

Tags

Ensure there is a tagging strategy in use for identifying and organizing AWS resources by name, purpose, environment, and other criteria.

Amazon S3

Amazon Macie Finding Statistics for S3

Capture summary statistics about Amazon Macie security findings on a per-S3 bucket basis.

DNS Compliant S3 Bucket Names

Ensure that your AWS S3 buckets are using DNS-compliant bucket names.

Enable Amazon S3 Bucket Keys

Ensure that Amazon S3 buckets are using S3 bucket keys to optimize service costs.

Enable S3 Block Public Access for AWS Accounts

Ensure that Amazon S3 public access is blocked at the AWS account level for data protection.

Enable S3 Block Public Access for S3 Buckets

Ensure that Amazon S3 public access is blocked at the S3 bucket level for data protection.

S3 Bucket Authenticated Users 'FULL_CONTROL' Access

Ensure S3 buckets do not allow FULL_CONTROL access to AWS authenticated users via S3 ACLs.

S3 Bucket Authenticated Users 'READ' Access

Ensure S3 buckets do not allow READ access to AWS authenticated users through ACLs.

S3 Bucket Authenticated Users 'READ_ACP' Access

Ensure AWS S3 buckets do not allow READ_ACP access to AWS authenticated users using ACLs.

S3 Bucket Authenticated Users 'WRITE' Access

Ensure S3 buckets do not allow WRITE access to AWS authenticated users through S3 ACLs.

S3 Bucket Authenticated Users 'WRITE_ACP' Access

Ensure S3 buckets do not allow WRITE_ACP access to AWS authenticated users using S3 ACLs.

S3 Bucket Default Encryption

Ensure Amazon S3 buckets have Default Encryption feature enabled.

S3 Bucket Logging Enabled

Ensure AWS S3 buckets have server access logging enabled to track access requests.

S3 Bucket MFA Delete Enabled

Ensure AWS S3 buckets have the MFA Delete feature enabled.

S3 Bucket Public 'FULL_CONTROL' Access

Ensure that your AWS S3 buckets are not publicly exposed to the Internet.

S3 Bucket Public 'READ' Access

Ensure AWS S3 buckets do not allow public READ access.

S3 Bucket Public 'READ_ACP' Access

Ensure that S3 buckets do not allow public READ_ACP access via Access Control Lists (ACLs).

S3 Bucket Public 'WRITE' ACL Access

Ensure AWS S3 buckets do not allow public WRITE ACL access.

S3 Bucket Public 'WRITE_ACP' Access

Ensure that S3 buckets do not allow public WRITE_ACP access via Access Control Lists (ACLs).

S3 Bucket Public Access Via Policy

Ensure AWS S3 buckets do not allow public access via bucket policies.

S3 Bucket Versioning Enabled

Ensure AWS S3 object versioning is enabled for an additional level of data protection.

S3 Buckets Encrypted with Customer-Provided CMKs

Ensure that Amazon S3 buckets are encrypted with customer-provided AWS KMS CMKs.

S3 Buckets Lifecycle Configuration

Ensure Amazon S3 buckets have lifecycle configuration enabled for security and cost optimization purposes.

S3 Buckets with Website Configuration Enabled

Ensure S3 buckets with website configuration enabled are regularly reviewed (informational).

S3 Configuration Changes

AWS S3 configuration changes have been detected within your Amazon Web

S3 Object Lock

Ensure that AWS S3 buckets use Object Lock for data protection and/or regulatory compliance.

S3 Transfer Acceleration

Ensure that Amazon S3 buckets use Transfer Acceleration feature for faster data transfers.

Secure Transport

Ensure AWS S3 buckets enforce SSL to secure data in transit

Server Side Encryption

Ensure AWS S3 buckets enforce Server-Side Encryption (SSE)

Amazon Simple Email Service

DKIM Enabled

Ensure DKIM signing is enabled in AWS SES to protect email senders and receivers against phishing.

Exposed SES Identities

Ensure that your AWS SES identities (domains and/or email addresses) are not exposed to everyone.

Identify Cross-Account Access

Ensure that AWS SES identities (domains and/or email addresses) do not allow unknown cross-account access via authorization policies.

Identity Verification Status

Ensure AWS SES identities (email addresses and/or domains) are verified.

Amazon Simple Notification Service (SNS)

AWS SNS Appropriate Subscribers

Ensure appropriate subscribers to all your AWS Simple Notification Service (SNS) topics.

Enable Server-Side Encryption for AWS SNS Topics

Ensure that Amazon SNS topics enforce Server-Side Encryption (SSE).

SNS Cross Account Access

Ensure Amazon SNS topics do not allow unknown cross account access.

SNS Topic Accessible For Publishing

Ensure SNS topics do not allow "Everyone" to publish.

SNS Topic Accessible For Subscription

Ensure SNS topics do not allow "Everyone" to subscribe.

SNS Topic Encrypted With KMS Customer Master Keys

Ensure that Amazon SNS topics are encrypted with KMS Customer Master Keys (CMKs).

SNS Topic Exposed

Ensure that AWS Simple Notification Service (SNS) topics are not exposed to everyone.

Amazon Simple Queue Service

Queue Server Side Encryption

Ensure Amazon SQS queues enforce Server-Side Encryption (SSE).

Queue Unprocessed Messages

Ensure AWS SQS queues do not retain a high number of unprocessed messages.

SQS Cross Account Access

Ensure AWS Simple Queue Service (SQS) queues do not allow unknown cross account access.

SQS Dead Letter Queue

Ensure there is a Dead Letter Queue configured for each Amazon SQS queue.

SQS Encrypted With KMS Customer Master Keys

Ensure SQS queues are encrypted with KMS CMKs to gain full control over data encryption and decryption.

SQS Queue Exposed

Ensure that AWS Simple Queue Service (SQS) queues are not exposed to everyone.

AWS Systems Manager

Check for SSM Managed Instances

Ensure that all EC2 instances are managed by AWS Systems Manager (SSM) service.

SSM Parameter Encryption

Ensure that Amazon SSM parameters that hold sensitive configuration data are encrypted.

SSM Session Length

Ensure that all active sessions in the Session manager do not exceed a set period of

Amazon SageMaker

Amazon SageMaker Notebook Instance In VPC

Ensure Amazon SageMaker notebook instances are running inside a Virtual Private Cloud (VPC).

Notebook Data Encrypted

Ensure that data available on Amazon SageMaker notebook instances is encrypted.

Notebook Data Encrypted With KMS Customer Master Keys

Ensure Amazon SageMaker notebook instances enforce data-at-rest encryption using KMS CMKs.

Notebook Direct Internet Access

Ensure Notebook instance is not publicly available

AWS Secrets Manager

Secret Encrypted With KMS Customer Master Keys

Ensure that AWS Secrets Manager service enforces data-at-rest encryption using KMS CMKs.

Secret Rotation Enabled

Ensure that automatic rotation is enabled for your Amazon Secrets Manager secrets.

Secret Rotation Interval

Ensure that Amazon Secrets Manager automatic rotation interval is properly configured.

Secrets Manager In Use

Ensure that AWS Secrets Manager is in use for secure and efficient credentials management.

AWS Security Hub

AWS Security Hub Findings

Ensure that Amazon Security Hub findings are analyzed and resolved.

AWS Security Hub Insights

Ensure that Amazon Security Hub insights are regularly reviewed (informational).

Detect AWS Security Hub Configuration Changes

Security Hub service configuration changes have been detected within your Amazon Web Services account.

Review Enabled Security Hub Standards

Ensure that enabled Amazon Security Hub standards are reviewed (informational).

AWS Shield

Shield Advanced In Use

Use AWS Shield Advanced to protect your web applications against DDoS attacks.

AWS Storage Gateway

Use KMS Customer Master Keys for AWS Storage Gateway File Shares

Ensure that your Amazon Storage Gateway file share data is encrypted using KMS Customer Master Keys (CMKs).

Use KMS Customer Master Keys for AWS Storage Gateway Tapes

Ensure that your Amazon Storage Gateway virtual tapes are encrypted using KMS Customer Master Keys.

Use KMS Customer Master Keys for AWS Storage Gateway Volumes

Ensure that your Amazon Storage Gateway volumes data is encrypted using KMS Customer Master Keys (CMKs).

AWS Support

Support Plan

Ensure appropriate support level is enabled for necessary AWS accounts (e.g. production accounts).

AWS Transfer

Enable AWS Transfer for SFTP Logging Activity

Ensure that AWS CloudWatch logging is enabled for Amazon Transfer for SFTP user activity.

AWS Trusted Advisor

Exposed IAM Access Keys

Ensure exposed IAM access keys are invalidated to protect your AWS resources from unauthorized access.

Trusted Advisor Checks

Ensure that Amazon Trusted Advisor checks are examined and resolved..

Trusted Advisor Service Limits

Monitor AWS Service Limits to ensure that the allocation of resources is not reaching the limit.

Amazon Virtual Private Cloud (VPC)

AWS VPC Peering Connections Route Tables Access

Ensure that the Amazon VPC peering connection configuration is compliant with the desired routing policy.

AWS VPN Tunnel State

Ensure the state of your AWS Virtual Private Network (VPN) tunnels is UP

Ineffective DENY Rules for Network ACLs

Ensure that Network ACL DENY rules are effective within your VPC network configuration.

Managed NAT Gateway In Use

Ensure AWS VPC Managed NAT (Network Address Translation) Gateway service is enabled for high availability (HA).

Specific Gateway Attached To Specific VPC

Ensure that a specific Internet/NAT gateway is attached to a specific VPC.

Unrestricted Inbound Traffic on Remote Server Administration Ports

Ensure that no Network ACL (NACL) allows unrestricted inbound traffic on TCP ports 22 and 3389.

Unrestricted Network ACL Inbound Traffic

Ensure no Amazon Network ACL allows inbound/ingress traffic from all ports.

Unrestricted Network ACL Outbound Traffic

Ensure no Amazon Network ACL allows outbound/egress traffic to all ports.

Unused VPC Internet Gateways

Ensure unused VPC Internet Gateways and Egress-Only Internet Gateways are removed to follow best practices.

Unused Virtual Private Gateways

Ensure unused Virtual Private Gateways (VGWs) are removed to follow best practices.

VPC Endpoint Cross Account Access

Ensure Amazon VPC endpoints do not allow unknown cross account access.

VPC Endpoint Exposed

Ensure Amazon VPC endpoints are not exposed to everyone.

VPC Endpoints In Use

Ensure VPC endpoints are being used to connect your VPC to another AWS service.

VPC Flow Logs Enabled

Ensure Virtual Private Cloud (VPC) Flow Logs feature is enabled in all applicable AWS regions.

VPC Naming Conventions

Ensure AWS VPCs are using proper naming conventions to follow AWS tagging best practices.

VPC Peering Connections To Accounts Outside AWS Organization

Ensure VPC peering communication is only between AWS accounts, members of the same AWS Organization.

VPN Tunnel Redundancy

Ensure AWS VPNs have always two tunnels active in order to enable redundancy.

AWS WAF - Web Application Firewall

AWS Web Application Firewall In Use

Ensure AWS WAF is in use to protect your web applications from common web exploits.

Enable Logging for Web Access Control Lists

Ensure that logging is enabled for Amazon WAF Web Access Control Lists.

AWS Well-Architected

AWS Well-Architected Tool Findings

Ensure that the high and medium risk issues identified in a workload by the AWS Well-Architected Tool are highlighted, audited, and resolved.

AWS Well-Architected Tool in Use

Ensure AWS Well-Architected Tool is in use to help you build and maintain secure, efficient, high-performing and resilient cloud application architectures.

AWS WorkDocs

Enable MFA for AD Connector Directories

Ensure that Multi-Factor Authentication (MFA) is enabled for AD Connector directories in Amazon WorkDocs.

Amazon WorkSpaces

Unused WorkSpaces

Ensure that your Amazon WorkSpaces service instances are being utilized.

WorkSpaces Desired Bundle Type

Ensure your AWS account has not reached the limit set for the number of WorkSpaces instances.

WorkSpaces Instances Counts

Ensure your AWS account has not reached the limit set for the number of WorkSpaces instances.

WorkSpaces Operation State

Ensure security and Amazon WorkSpaces instances are healthy.

WorkSpaces Storage Encryption

Ensure encryption is enabled for AWS WorkSpaces storage volumes to protect your data at rest.

AWS X-Ray

X-Ray Data Encrypted With KMS Customer Master Keys

Ensure Amazon X-Ray encrypts traces and related data at rest using KMS CMKs.