Durex Documentation

Release 0.1.0

David Amrani Hernandez

Mar 04, 2019

Contents:

1 Test & Best practices **1**

1.1 ACM . . . 2
1.2 API Gateway . . . 3
1.3 AutoScaling . . . 3
1.4 CloudFront . . . 6
1.5 CloudTrail . . . 8
1.6 CloudWatch . . . 9
1.7 Config . . . 12
1.8 DynamoDB . . . 13
1.9 EBS . . . 14
1.10 EC2 . . . 16
1.11 ECR . . . 30
1.12 EFS . . . 31
1.13 ElasticSearch . . . 32
1.14 ELB . . . 34
1.15 EMR . . . 40
1.16 GuardDuty . . . 41
1.17 Health . . . 42
1.18 IAM . . . 42
1.19 Inspector . . . 49
1.20 KMS . . . 50
1.21 Lambda . . . 52
1.22 Organizations . . . 53
1.23 RDS . . . 54
1.24 ResourceGroup . . . 61
1.25 S3 . . . 61
1.26 SES . . . 66
1.27 Shield . . . 66
1.28 TrustedAdvisor . . . 67
1.29 VPC . . . 67
1.30 WAF . . . 71

2 Indices and tables **73**

CHAPTER 1

Test & Best practices

1. *ACM*
2. *API Gateway*
3. *AutoScaling*
4. *CloudFront*
5. *CloudTrail*
6. *CloudWatch*
7. *Config*
8. *DynamoDB*
9. *EBS*
10. *EC2*
11. *ECR*
12. *EFS*
13. *ElasticSearch*
14. *ELB*
15. *EMR*
16. *GuardDuty*
17. *Health*
18. *IAM*
19. *Inspector*
20. *KMS*
21. *Lambda*
22. *Organizations*

23. *RDS*
24. *ResourceGroup*
25. *S3*
26. *SES*
27. *Shield*
28. *TrustedAdvisor*
29. *VPC*
30. *WAF*

1.1 ACM

- *Expired ACM Certificates*
- *ACM Certificates Renewal*
- *ACM Certificates Validity*

1.1.1 Expired ACM Certificates

Risk: High
Description: Ensure that all expired SSL/TLS certificates in ACM service are removed.
Resolution: Delete any expired certificates.

1.1.2 ACM Certificates Renewal

Risk: Medium
Description: Ensure that SSL/TLS certificates in ACM are renewed 30 days before their validity period ends.
Resolution: Renew any SSL/TLS certificates that are about to expire using AWS Certificate Manager service.

1.1.3 ACM Certificates Validity

Risk: High
Description: Ensure that all the requests made during SSL/TLS certificate issue or renewal process are validated. These requests are managed in your account by ACM.
Resolution: Resend the domain validation email for any invalid SSL/TLS certificates using ACM console and API (CLI)

1.2 API Gateway

- *Enable CloudWatch Logs for APIs*
- *Enable Detailed CloudWatch Metrics for APIs*
- *API Gateway Private Endpoints*

1.2.1 Enable CloudWatch Logs for APIs

Risk: Medium
Description: Ensure that CloudWatch logs are enabled for all your APIs created with API Gateway service.
Resolution: Enable CloudWatch Logs for your API Gateway APIs

1.2.2 Enable Detailed CloudWatch Metrics for APIs

Risk: Medium
Description: Ensure that detailed CloudWatch metrics are enabled for all APIs created with API Gateway service.
Resolution: Enable detailed CloudWatch metrics for your API Gateway APIs stages

1.2.3 API Gateway Private Endpoints

Risk: Medium
Description: Ensure that API Gateway APIs are only accessible through private API endpoints and not visible to Internet.
Resolution: Change your API Gateway APIs endpoint type so these can be accessible only through private VPC endpoints

---

1.3 AutoScaling

- *ASG Cooldown Period*
- *Enable ASG Notifications*
- *App-Tier ASGs with Associated ELB*
- *CloudWatch Logs Agent for App-Tier ASG In Use*
- *IAM Roles for App-Tier ASG Launch Configurations*
- *Use Approved AMIs for App-Tier ASG Launch Configurations*
- *Auto Scaling Group Referencing Missing ELB*
- *Empty Auto Scaling Groups*
- *Launch Configuration Referencing Missing AMI*
- *Launch Configuration Referencing Missing Security Group*

- *Unused Launch Configuration Templates*
- *Multi-AZ Auto Scaling Groups*
- *Same ELB Availability Zones*
- *Suspended Auto Scaling Group Processes*
- *Web-Tier Auto Scaling Groups with Associated ELBs*
- *Use Approved AMIs for Web-Tier ASG Launch Configurations*

1.3.1 ASG Cooldown Period

Risk: High
Description: Ensure that ASGs are configured to use a cooldown period to temporarily suspend any scaling activities in order to allow the newly launched EC2 instance some time to start handling the application traffic.
Resolution: Implement an appropriate cooldown period for your Auto Scaling Groups.

1.3.2 Enable ASG Notifications

Risk: Low
Description: Ensure that Auto Scaling Groups are configured to send email notifications when a scaling event occurs, such as launching or terminating an EC2 instance. Once the ASG Notifications feature is enabled, the SNS topic associated will process and send ASG scaling events notifications to the email address that you specified during setup. **Resolution**: Configure your Auto Scaling Groups with the SNS service in order to send scaling events notifications via email.

1.3.3 App-Tier ASGs with Associated ELB

Risk: High
Description: Ensure that app-tier ASGs have associated ELBs in order to evenly distribute incoming traffic across all the EC2 instances available inside the ASG and help provide high availability for your applications.
Resolution: Create an ELB and associate it with your app-tier Auto Scaling Group (ASG)

1.3.4 CloudWatch Logs Agent for App-Tier ASG In Use

Risk: Medium
Description: Ensure that the EC2 instances launched in your app-tier ASG are using CloudWatch log agents to monitor, store and access log files (application or system data logs) from these instances. A CloudWatch Logs agent needs to be installed on the guest Operating System of the app-tier EC2 instance that you want to get logs from.
Resolution: - To install the Cloudwatch Logs agent on the EC2 instances in your app-tier ASG, you must re-create the ASG launch configuration and set it up with the necessary user data (i.e. agent installation script).

1.3.5 IAM Roles for App-Tier ASG Launch Configurations

Risk: Medium
Description: Ensure that app-tier ASG launch configurations are using IAM roles to delegate access to the applications running in your ASGs, applications that usually don't have access to AWS resources.

Resolution: To attach an IAM role to the EC2 instances launched in your app-tier ASG, you must re-create their launch configuration and configure it with a reference to a new IAM role.

1.3.6 Use Approved AMIs for App-Tier ASG Launch Configurations

Risk: High

Description: Ensure that app-tier ASG launch configurations are using approved AMIs to launch EC2 instances within the ASG.

Resolution: To launch EC2 instances inside your app-tier Auto Scaling Group from approved AMI, you must re-create the app-tier ASG launch configuration and configure it to support a golden AMI maintained and approved by your organization.

1.3.7 Auto Scaling Group Referencing Missing ELB

Risk: High

Description: Ensure that ASGs are referencing active ELBs in order to maintain the auto-scaling process healthy and the application load evenly distributed

Resolution: Update any ASGs that are missing load balancing capabilities due to inactive ELBs.

1.3.8 Empty Auto Scaling Groups

Risk: Recommendation

Description: Identify any empty Auto Scaling Groups available in your AWS account and delete them.

Resolution: Remove empty Auto Scaling Groups from your account.

1.3.9 Launch Configuration Referencing Missing AMI

Risk: High

Description: Ensure that ASGs launch configuration is referencing an active AMI.

Resolution: Fix any unhealthy Auto Scaling Groups by replacing their invalid launch configuration with a valid one.

1.3.10 Launch Configuration Referencing Missing Security Group

Risk: High

Description: Ensure that ASGs launch configuration is referencing one or more active Security Groups (SGs).

Resolution: Fix the unhealthy Auto Scaling Groups by replacing their invalid launch configuration.

1.3.11 Unused Launch Configuration Templates

Risk: Low

Description: Identify any Auto Scaling Launch Configuration templates that aren't used anymore by ASGs and delete them.

Resolution: Remove any unused Auto Scaling Launch Configuration templates.

1.3.12 Multi-AZ Auto Scaling Groups

Risk: Medium
Description: Ensure that ASGs span across multiple Availability Zones within an AWS region to expand the availability of your auto-scaled applications.
Resolution: Expand the availability of your auto-scaled web application by adding new Availability Zones to your existing Auto Scaling Groups configuration.

1.3.13 Same ELB Availability Zones

Risk: Medium
Description: Ensure that the ASGs and their associated ELBs are sharing the same Availability Zones in order to increase the performance of your auto scaling environments by allowing your applications to use AWS low-latency network links. **Resolution**: Configure your Auto Scaling Groups to share the same availability zones with their load balancers.

1.3.14 Suspended Auto Scaling Group Processes

Risk: Medium
Description: Ensure there are no ASGs with suspended processes, provisioned in your AWS account.
Resolution: Resume any auto scaling processes suspended in your ASGs after the application and/or environment remediation process is complete

1.3.15 Web-Tier Auto Scaling Groups with Associated ELBs

Risk: High
Description: Ensure that web-tier ASGs have associated ELBs to equally distribute incoming traffic across all EC2 instances available within the ASG and help provide high availability for your web applications.
Resolution: Create an ELB and associate it with your web-tier Auto Scaling Group (ASG)

1.3.16 Use Approved AMIs for Web-Tier ASG Launch Configurations

Risk: High
Description: - Ensure that web-tier ASG launch configurations are using approved (golden) AMIs to launch EC2 instances within the ASG.
Resolution: To launch EC2 instances in your web-tier ASG from golden/approved AMI, you must re-create the web-tier ASG launch configuration template with a reference to a well-defined AMI maintained and approved by your organization.

1.4 CloudFront

- *CloudFront CDN In Use*

- *CloudFront WAF Integration*
- *Enable Origin Access Identity for CloudFront Distributions with S3 Origin*
- *CloudFront Origin Insecure SSL Protocols*
- *CloudFront Security Policy*
- *Unencrypted CloudFront Traffic*
- *Use Cloudfront CDN*

1.4.1 CloudFront CDN In Use

Risk: Medium

Description: Ensure that CloudFront CDN service is used in your AWS account to secure and accelerate the delivery of your websites, media files or static resources (e.g., CSS files, JavaScript files, images) handled by your web applications. **Resolution**: In order to utilize Cloudfront as a CDN service to secure and accelerate the delivery of your websites, media files or other static resources, you must create and configure Cloudfront web distributions.

1.4.2 CloudFront WAF Integration

Risk: Medium

Description: Ensure that all your CloudFront distributions are integrated with the WAF.

Resolution: Integrate CloudFront with WAF you must create the required WAF Access Control List and associate it with the appropriate web distribution.

1.4.3 Enable Origin Access Identity for CloudFront Distributions with S3 Origin

Risk: Medium

Description: Ensure that the origin access identity feature is enabled for all your Cloudfront CDN distributions that utilize an S3 bucket as an origin in order to restrict any direct access to your objects through S3 URLs.

Resolution: Enable origin access identity for your Cloudfront CDN distribution and restrict the user access to the S3 bucket used as origin.

1.4.4 CloudFront Origin Insecure SSL Protocols

Risk: Medium

Description: Ensure that Cloudfront CDN distributions aren't using insecure SSL protocols (i.e. SSLv3) for HTTPS communication between CloudFront edge locations and your custom origins. We recommend using TLSv1.0 or later (ideally use only TLSv1.2 if your origins support it) and avoid using the SSLv3 protocol.

Resolution: To remove the deprecated SSLv3 protocol from your Cloudfront distributions origin.

1.4.5 CloudFront Security Policy

Risk: Medium

1.4.6 Unencrypted CloudFront Traffic

Risk: Medium
Description: Ensure that the communication between your CloudFront distributions and their custom origins is encrypted using HTTPS.
Resolution: Enable HTTPS for encrypting the traffic between your CloudFront distributions edge locations and their origins.

1.4.7 Use Cloudfront CDN

Risk: Medium
Description: Ensure that web application is using Cloudfront CDN to secure its content delivery (media files and static resource files such as .html, .css, .js).
Resolution: To use Cloudfront as a CDN to secure and accelerate the content delivery of your web application, you need to create and configure a Cloudfront web distribution.

1.5 CloudTrail

- *Enable access logging for CloudTrail buckets*
- *Enable MFA Delete for CloudTrail bucket*
- *CloudTrail insecure buckets*
- *Monitor CloudTrail Configuration Changes*
- *Enable CloudTrail integration with CloudWatch*
- *Enable CloudTrail log file integrity validation*
- *Enable CloudTrail log files encryption*
- *CloudTrail Log Files Delivery Failing*

1.5.1 Enable access logging for CloudTrail buckets

Risk: Medium
Description: Ensure that any S3 buckets used by CloudTrail have Server Access Logging feature enabled in order to track requests for accessing the buckets and necessary for security audits.
Resolution: To enable Server Access Logging for your CloudTrail bucket, you must be the bucket owner.

1.5.2 Enable MFA Delete for CloudTrail bucket

Risk: High
Description: Ensure that CloudTrail logging bucket use MFA Delete feature in order to prevent the deletion of any versioned log files.
Resolution: Enable MFA Delete protection for your CloudTrail logging bucket via AWS CLI.

1.5.3 CloudTrail insecure buckets

Risk: High
Description: Check for any CloudTrail logging buckets that are publicly accessible.
Resolution: To remove public access to your CloudTrail logging bucket.

1.5.4 Monitor CloudTrail Configuration Changes

Risk: High
Description: Monitor CloudTrail Configuration Changes.

1.5.5 Enable CloudTrail integration with CloudWatch

Risk: Medium
Description: Ensure CloudTrail events are being monitored with CloudWatch Logs for management and security purposes. This enables you to respond quickly to critical operational events detected with CloudTrail events and captured by CloudWatch logs.

1.5.6 Enable CloudTrail log file integrity validation

Risk: Medium
Description: Ensure that trails have file integrity validation feature enabled in order to check the log files and detect whether these were modified or deleted after CloudTrail agent delivered them to the S3 bucket.

1.5.7 Enable CloudTrail log files encryption

Risk: Medium
Description: Ensure that CloudTrail logs are encrypted at rest using server-side encryption provided by KMS Managed Keys (SSE-KMS) to enhance the security of your CloudTrail bucket and allow you to have better control over who can read the log files in your organization. **Resolution**: Enable SSE-KMS encryption for your CloudTrail log files.

1.5.8 CloudTrail Log Files Delivery Failing

Risk: Medium
Description: Ensure that the log files generated by your CloudTrail trails are delivered without any failures to designated recipients.

1.6 CloudWatch

- *Enable AWS Billing Alerts*
- *Enable CloudWatch Billing Alarm*

- *Exposed CloudWatch Event Bus*
- *CloudWatch Events In Use*
- *Alarm for Config Changes*
- *Alarm for Organizations Changes*
- *Alarm for multiple Sign-in Failures*
- *Monitor for AWS Console Sign-In Requests Without MFA*
- *Alarm for EC2 Instance Changes*
- *Alarm for EC2 Large Instance Changes*
- *Alarm for Root Account Usage*
- *Alarm for S3 Bucket Changes*

1.6.1 Enable AWS Billing Alerts

Risk: High
Description: Ensure that billing alerts are enabled in order to receive notifications when your AWS estimated charges exceed a threshold that you choose. These alerts are triggered by CloudWatch and sent to you using the SNS.

1.6.2 Enable CloudWatch Billing Alarm

Risk: High
Description: Set up a CloudWatch billing alarm to receive alerts when your AWS estimated charges exceed a threshold that you choose so you can decide whether to stop or reconfigure the AWS components that have reached the cost limit set. These alerts are triggered by CloudWatch and sent to you using the SNS.

1.6.3 Exposed CloudWatch Event Bus

Risk: High
Description: Ensure that CloudWatch default event bus is not configured to allow access to everyone (*) in order to prevent anonymous users from sharing their CloudWatch events.
Resolution: Update the access permissions defined for the CloudWatch default event bus in order authorize only specific AWS entities to send CloudWatch event data to your AWS account.

1.6.4 CloudWatch Events In Use

Risk: Medium
Description: Ensure that CloudWatch Events service is in use in order to enable you to react selectively and efficiently to system events that describe changes in your AWS resources.

1.6.5 Alarm for Config Changes

Risk: Medium
Description: Ensure there is a CloudWatch alarm created and configured in your AWS account to fire each time an AWS Config configuration change is made.

1.6.6 Alarm for Organizations Changes

Risk: Medium
Description: Ensure that there is a CloudWatch alarm implemented in your AWS Master account that is triggered each time an administrator-specific action occurs in your AWS Organizations.

1.6.7 Alarm for multiple Sign-in Failures

Risk: Medium
Description: Ensure there is a CloudWatch alarm created in your account that is triggered when there are three or more AWS Management Console sign-in failures during a 5 minutes period.

1.6.8 Monitor for AWS Console Sign-In Requests Without MFA

Risk: Medium
Description: Ensure CloudWatch monitors Management Console authentication requests that aren't protected by MFA.

1.6.9 Alarm for EC2 Instance Changes

Risk: Medium
Description: Ensure there is a CloudWatch alarm available in your AWS account that is triggered each time an EC2 instance configuration and status change is made. This CloudWatch alarm must fire every time an API call is performed to create, terminate, start, stop or reboot an EC2 instance.

1.6.10 Alarm for EC2 Large Instance Changes

Risk: Medium
Description: Ensure there is a CloudWatch alarm set up in your AWS account that is triggered each time an EC2 large instance is created. This CloudWatch alarm must fire and send email notifications every time an API call is made to provision a 4xlarge or 8xlarge EC2 instance.

1.6.11 Alarm for Root Account Usage

Risk: High
Description: Ensure there is a CloudWatch alarm created and configured in your AWS account to fire each time Root Account is used. This CloudWatch alarm must be triggered every time Root Account is used.

1.6.12 Alarm for S3 Bucket Changes

Risk: Medium
Description: Ensure there is a CloudWatch alarm created and configured in your AWS account to fire each time a S3 bucket configuration change is made.

1.7 Config

- *Monitor AWS Config configuration changes*
- *Enable AWS Config*
- *AWS Config Referencing Missing S3 Bucket*
- *AWS Config Referencing Missing SNS Topic*
- *AWS Config Log Files Delivery Failing*
- *Include Global Resources into AWS Config Settings*

1.7.1 Monitor AWS Config configuration changes

Risk: High
Description: Monitor AWS Config configuration changes.

1.7.2 Enable AWS Config

Risk: High
Description: Ensure that AWS Config service is enabled in all regions in order to have complete visibility over your AWS infrastructure configuration changes.
Resolution: Enable AWS Config in all regions available.

1.7.3 AWS Config Referencing Missing S3 Bucket

Risk: High
Description: Ensure that AWS Config service is referencing an active S3 bucket in order to save configuration information (history files and snapshots) for auditing purposes.
Resolution: Update AWS Config service configurations that reference missing S3 buckets.

1.7.4 AWS Config Referencing Missing SNS Topic

Risk: Medium
Description: Ensure that AWS Config service is referencing an active SNS topic in order to send configuration changes notifications to your SNS subscription endpoints for monitoring.
Resolution: Update AWS Config service configurations that reference missing SNS topics.

1.7.5 AWS Config Log Files Delivery Failing

Risk: Medium
Description: Ensure that the log files (history files and snapshots) generated by AWS Config are delivered without any failures to designated S3 bucket in order to store logging data for auditing purposes.

1.7.6 Include Global Resources into AWS Config Settings

Risk: Medium
Description: Ensure that AWS Config service is configured to include Global resources in order to have complete visibility over the configuration changes made in your AWS account.
Resolution: To include Global resources into AWS Config settings.

1.8 DynamoDB

- *Enable DynamoDB Auto Scaling*
- *DynamoDB Backup and Restore*
- *Enable DynamoDB Continuous Backups*
- *DynamoDB Server-Side Encryption*

1.8.1 Enable DynamoDB Auto Scaling

Risk: Medium
Description: Ensure that DynamoDB Auto Scaling feature is enabled to dynamically adjust provisioned throughput (read and write) capacity for your tables and global secondary indexes.
Resolution: Enable Application Auto Scaling for DynamoDB tables and indexes.

1.8.2 DynamoDB Backup and Restore

Risk: High
Description: Ensure that DynamoDB tables are using on-demand backup and restore functionality for data protection and archival purposes, helping you meet regulatory requirements in your organization.
Resolution: To make use of DynamoDB on-demand backup and restore functionality, you need to create full table backups and restore them when needed

1.8.3 Enable DynamoDB Continuous Backups

Risk: Medium
Description: Ensure that DynamoDB tables make use of Point-in-time Recovery (PITR) feature in order to automatically take continuous backups of your DynamoDB data.
Resolution: To make use of Point-in-time Recovery (PITR) feature and enable continuous backups for your DynamoDB tables

1.8.4 DynamoDB Server-Side Encryption

Risk: High

Description: Ensure that DynamoDB data at rest (tables, local secondary indexes, global secondary indexes and backups) is encrypted using Server-Side Encryption. The encryption process is using AWS-managed keys stored in KMS, adds no storage overhead and is completely transparent and you can insert, query, scan and delete items as before. **Resolution**: To make use of Server-Side Encryption feature for your new DynamoDB tables

---

1.9 EBS

- *Enable EBS Encryption*
- *Use KMS Customer Master Keys for EBS encryption*
- *EBS Volume Naming Conventions*
- *EBS Public Snapshots*
- *EBS volumes recent snapshots*
- *Remove EBS old snapshots*
- *Remove Unattached EC2 EBS volumes*
- *Enable EBS Snapshot Encryption*
- *EBS Volumes Attached to Stopped EC2 Instances*

1.9.1 Enable EBS Encryption

Risk: High
Description: With encryption enabled, your EBS volumes can hold very sensitive and critical data.
Resolution: To enable encryption on EBS volumes and snapshots, you need to re-create them.

1.9.2 Use KMS Customer Master Keys for EBS encryption

Risk: High
Description: Ensure that EBS volumes are using KMS CMK customer-managed keys instead of AWS managed-keys (default key used for volume encryption) in order to have more granular control over your data encryption and decryption process. **Resolution**: Use your own CMK key to encrypt an EBS volume.

1.9.3 EBS Volume Naming Conventions

Risk: Low
Description: Ensure that all your EBS volumes are using proper naming conventions for tagging in order to manage them more efficiently and adhere to AWS resource tagging best-practices.

1.9.4 EBS Public Snapshots

Risk: High
Description: Ensure that EBS volume snapshots aren't public (i.e. publicly shared with other AWS accounts) in order to avoid exposing personal and sensitive data.
Resolution: Change privacy property to private.

1.9.5 EBS volumes recent snapshots

Risk: Medium
Description: Ensure that EBS volumes have recent snapshots available for point-in-time recovery for a better, more reliable data backup strategy.
Resolution: Maintain your EBS backup stack up-to-date, you need to create new EBS snapshots.

1.9.6 Remove EBS old snapshots

Risk: Recommendation
Description: Check for any EBS snapshots older than 30 days available in your AWS account and remove them in order to lower the cost of your monthly bill.
Resolution: Safely delete any old and unneeded EBS volume snapshots from your AWS account.

1.9.7 Remove Unattached EC2 EBS volumes

Risk: Medium
Description: Identify any unattached (unused) EBS volumes available in your AWS account and remove them in order to lower the cost of your monthly AWS bill and reduce the risk of confidential/sensitive data leaving your premise.
Resolution: Remove any unused and unwanted EBS volumes from your AWS account.

1.9.8 Enable EBS Snapshot Encryption

Risk: Medium
Description: Ensure that the EBS volume snapshots that hold sensitive and critical data are encrypted to fulfill compliance requirements for data-at-rest encryption.
Resolution: To encrypt existing EBS volume snapshots available in your AWS account.

1.9.9 EBS Volumes Attached to Stopped EC2 Instances

Risk: Recommendation
Description: Identify any EBS volumes that are currently attached to stopped EC2 instances and remove them if the instances are no longer needed in order avoid unexpected charges on your AWS bill.
EC2

1.10 EC2

- *Approved/Golden AMI*
- *AWS Blacklisted AMI*
- *Enable AMI Encryption*
- *AMI Naming Conventions*
- *Check for AMI Age*
- *Unused AMI*
- *Unassociated Elastic IP Addresses*
- *Publicly Shared App-Tier AMIs*
- *App-Tier EC2 Instances Without Elastic or Public IP Addresses*
- *Check app-tier ELB subnet connectivity to Internet Gateway*
- *IAM Roles for App-Tier EC2 Instances*
- *Create and Configure App-Tier Security Group*
- *EC2 Instances Distribution Across Availability Zones*
- *EC2-Classic Elastic IP Address Limit*
- *Data-Tier Instances Without Elastic or Public IP Addresses*
- *Create and Configure Data-Tier Security Group*
- *Restrict data-tier subnet connectivity to VPC NAT Gateway*
- *Unrestricted Default Security Groups*
- *Default EC2 Security Groups In Use*
- *Detailed Monitoring for EC2 Instances*
- *EC2 Desired Instance Type*
- *Review EC2 Dedicated Instances*
- *EC2 Instance Not In Public Subnet*
- *Unused EC2 Reserved Instances*
- *Total Number of EC2 Instances*
- *EC2 Instance Type Generation*
- *Instance In Auto Scaling Group*
- *EC2 Platform*
- *EC2 Instance Limit*
- *EC2 Instance Naming Conventions*
- *EC2 Instances with Scheduled Events*
- *EC2 Instance Security Group Rules Count*
- *EC2 Instance Tenancy Type*
- *EC2 Instance Termination Protection*

- *EC2 Instance Age*
- *EC2 Instance IAM Roles*
- *Overutilized EC2 Instances*
- *Publicly Shared AMIs*
- *EC2 Reserved Instance Lease Expiration*
- *EC2 Security Groups Count*
- *EC2 Security Group Port Range*
- *Underutilized EC2 Instances*
- *EC2 Security Group Unrestricted Access*
- *Unrestricted CIFS Access*
- *Unrestricted DNS Access*
- *Unrestricted ElasticSearch Access*
- *Unrestricted FTP Access*
- *Unrestricted HTTP Access*
- *Unrestricted HTTPS Access*
- *Unrestricted ICMP Access*
- *Unrestricted Inbound Access on Uncommon Ports*
- *Unrestricted MongoDB Access*
- *Unrestricted MSSQL Database Access*
- *Unrestricted MySQL Database Access*
- *Unrestricted NetBIOS Access*
- *Unrestricted Oracle Database Access*
- *Unrestricted Outbound Access on All Ports*
- *Unrestricted PostgreSQL Database Access*
- *Unrestricted RDP Access*
- *Unrestricted RPC Access*
- *Unrestricted SMTP Access*
- *Unrestricted SSH Access*
- *Unrestricted Telnet Access*
- *Unused Elastic Network Interfaces*
- *Unused EC2 Key Pairs*
- *EC2-VPC Elastic IP Address Limit*
- *Publicly Shared Web-Tier AMIs*
- *Web-Tier EC2 Instances Without Elastic or Public IP Addresses*
- *Check web-tier ELB subnet connectivity to Internet Gateway*
- *Attach Policy to IAM Roles Associated with Web-Tier EC2 Instances*

- *IAM Roles for Web-Tier EC2 Instances*
- *Create and Configure Web-Tier Security Group*
- *Check web-tier subnet connectivity to VPC NAT Gateway*

1.10.1 Approved/Golden AMI

Risk: Medium
Description: Ensure that all the EC2 instances necessary for your application stack are launched from your approved base AMI (AMIs), known as golden AMIs in order to enforce consistency and save time when scaling your application.
Resolution: Create golden/approved machine images and enforce your AWS administrators to launch EC2 instances using only these images.

1.10.2 AWS Blacklisted AMI

Risk: Medium
Description: Ensure that all EC2 instances provisioned in your AWS account are launched from approved AMIs only and not from blacklisted AMIs in order to enforce security at application stack level.
Resolution: To relaunch an EC2 instance that was built from a blacklisted AMI

1.10.3 Enable AMI Encryption

Risk: High
Description: Ensure that AMIs are encrypted to fulfill compliance requirements for data-at-rest encryption. The AMI data encryption and decryption is handled transparently and doesn't require any additional action from your applications. **Resolution**: To encrypt any unencrypted AMI available in your AWS account, you need to create AMIs with encrypted snapshots from AMIs with unencrypted snapshots by copying them.

1.10.4 AMI Naming Conventions

Risk: Low
Description: Ensure that all your AMIs are using suitable naming conventions for tagging in order to manage them more efficiently and adhere to AWS resource tagging best-practices.

1.10.5 Check for AMI Age

Risk: Low
Description: Ensure that existing AMIs aren't older than 180 days in order to ensure their reliability and to meet security and compliance requirements.
Resolution: To re-create each outdated AMI with an up-to-date software stack.

1.10.6 Unused AMI

Risk: Recommendation

Description: Find any unused AMI available in your AWS account and remove them in order to lower the cost of your monthly AWS bill. The AMI removal/cleanup process consists of two steps: 1) deregister the unused image and 2) delete the snapshot associated with it. **Resolution**: To remove any unused AMIs available in your account, you need to deregister the image and then delete the associated snapshot.

1.10.7 Unassociated Elastic IP Addresses

Risk: Recommendation

Description: Check for any unattached Elastic IP addresses in your AWS account and release (remove) them in order to lower the cost of your monthly AWS bill.

Resolution: To release (remove) any unassociated Elastic IP addresses available in your AWS account.

1.10.8 Publicly Shared App-Tier AMIs

Risk: High

Description: Ensure that none of the AMIs created in your app tier are publicly shared with other AWS accounts in order to avoid exposing sensitive information, as these images can contain proprietary applications, personal data and configuration information that can be used to exploit or compromise running EC2 instances available in your app tier
Resolution: Make the publicly accessible app-tier AMIs private.

1.10.9 App-Tier EC2 Instances Without Elastic or Public IP Addresses

Risk: Medium

Description: Ensure that app-tier EC2 instances aren't associated with Elastic or Public IP addresses as these instances don't have to be publicly reachable

Resolution: To remove a Public IP address from an app-tier EC2 instance, you must re-launch the instance with the appropriate network configuration.

1.10.10 Check app-tier ELB subnet connectivity to Internet Gateway

Risk: Medium

Description: - Ensure that the VPC route table associated with the app-tier ELB subnets has the default route set up to allow access to the Internet Gateway (IGW) in order to provide internet connectivity for the app-tier load balancer. A route table contains a set of rules that are used to determine where the network traffic is directed. The route table associated with the ELB subnets should contain a default route (i.e. 0.0.0.0/0) that points to an Internet Gateway.
Resolution: Create the required route (i.e. 0.0.0.0/0) with an IGW configured as gateway for the route table associated with the app-tier ELB subnets.

1.10.11 IAM Roles for App-Tier EC2 Instances

Risk: Medium

Description: Ensure that app-tier EC2 instances are using IAM roles to grant the necessary permissions (following the principle of least privilege) to the applications running on these instances.

Resolution: To attach IAM roles to your running app-tier EC2 instances, you need to re-launch those instances and associate them with the required IAM roles.

1.10.12 Create and Configure App-Tier Security Group

Risk: Medium
Description: Ensure there is an EC2 security group created and configured for the app tier to grant inbound access from the app-tier ELB security group for explicit ports, in order to secure the access to the EC2 instances running within the tier. **Resolution**: Create a compliant EC2 security group and configure it to allow inbound traffic from the app-tier ELB security group on explicit ports

1.10.13 EC2 Instances Distribution Across Availability Zones

Risk: Medium
Description: Ensure that EC2 instances are spread across all Availability Zones within an AWS region in order to maintain high reliability in the event of a service disruption
Resolution: To equally distribute your existing EC2 instances across the Availability Zones within the utilized AWS regions, you need to migrate these instances between Availability Zones.

1.10.14 EC2-Classic Elastic IP Address Limit

Risk: Medium
Description: Determine if the number of EC2-Classic Elastic IPs (EIPs) allocated per region is close to the limit number established by Amazon for accounts that support EC2-Classic platform and request limit increase in order to avoid encountering IP resource limitations on future EC2 provisioning sessions. As the IPv4 public IP addresses are a scarce resource nowadays, by default, all AWS accounts are limited to 5 (five) Elastic IP addresses per region.
Resolution: To request an increase for the EC2-Classic Elastic IP limit.

1.10.15 Data-Tier Instances Without Elastic or Public IP Addresses

Risk: Medium
Description: Ensure that data-tier instances aren't associated with Elastic or Public IP addresses as these database instances don't have to be publicly reachable and must be protected from exposure.
Resolution: To remove a Public IP address from a data-tier instance, you must re-launch the instance with the right network configuration.

1.10.16 Create and Configure Data-Tier Security Group

Risk: Medium
Description: Ensure there is an AWS security group created and configured for the data tier that grants inbound access from the app-tier security group on explicit TCP ports such as 3306 (MySQL, MariaDB and Aurora), 1433 (MSSQL), 1521 (Oracle SQL) and 5432 (PostgreSQL), to secure the access to your database instances. **Resolution**: To create a compliant Amazon data-tier security group and configure it to allow inbound traffic from the app-tier security group on explicit port (in this case TCP port 3306).

1.10.17 Restrict data-tier subnet connectivity to VPC NAT Gateway

Risk: Medium

Description: Ensure that the VPC route table associated with the data-tier subnets has no default route configured to allow access to an NAT Gateway in order to restrict Internet connectivity for the EC2 instances available within the data tier. A route table contains a set of rules (also known as routes) that are used to determine where the network traffic is directed. Each subnet deployed in your VPC must be associated with a route table to control the routing. The route table associated with the data-tier subnets should not have a default route (i.e. 0.0.0.0/0) that points to a NAT Gateway. **Resolution**: To remove the default route that has an NAT device configured as gateway for the route table associated with your data-tier subnets.

1.10.18 Unrestricted Default Security Groups

Risk: Medium
Description: Ensure that EC2 default security groups restrict all inbound public traffic in order to enforce AWS users (EC2 administrators, resource managers, etc) to create custom security groups that exercise the rule of least privilege instead of using the default security groups. **Resolution**: To restrict public inbound traffic to your default security groups and use custom security groups instead of default ones for your EC2 instances.

1.10.19 Default EC2 Security Groups In Use

Risk: Medium
Description: Ensure that the EC2 instances provisioned in your AWS account aren't associated with default security groups created alongside with your VPCs in order to enforce using custom and unique security groups that exercise the principle of least privilege. **Resolution**: To adhere to the principle of least privilege and replace the associated default security groups with custom security groups.

1.10.20 Detailed Monitoring for EC2 Instances

Risk: Low
Description: Ensure that detailed monitoring is enabled for your EC2 instances in order to have enough monitoring data to help you make better decisions on architecting and managing compute resources in your AWS account. By default, whenever an EC2 instance is launched, CloudWatch enables basic monitoring for that instance. The basic monitoring level collects monitoring data in 5 minute periods. To increase this level and make the monitoring data available at 1-minute periods, you must specifically enable it for your instance(s). **Resolution**: Enable detailed monitoring for your existing EC2 instances.

1.10.21 EC2 Desired Instance Type

Risk: Medium
Description: Determine if the EC2 instances provisioned in your AWS account have the desired instance type(s) established by your organization based on the workload deployed.
Resolution: To limit the EC2 instances that will be launched in your account to the desired instance type(s).

1.10.22 Review EC2 Dedicated Instances

Risk: Recommendation
Description: Ensure that all EC2 dedicated instances provisioned in your AWS account are regularly reviewed for cost optimization.

Resolution: Migrate your running EC2 dedicated instances to the default (shared) tenancy to reduce your monthly EC2 usage costs.

1.10.23 EC2 Instance Not In Public Subnet

Risk: High
Description: Ensure that no backend EC2 instances are provisioned in public subnets in order to protect them from exposure to the Internet. In this context, backend instances are EC2 instances that do not require direct access to the public internet such as database, API or caching servers. **Resolution**: To move your backend EC2 instances from public subnets to private subnets, you must re-launch these instances within the right subnets.

1.10.24 Unused EC2 Reserved Instances

Risk: Recommendation
Description: Ensure that all purchased EC2 Reserved Instances (RI) have corresponding instances running within the same account or within any linked AWS accounts available in an AWS Organization (if you are using one).
Resolution: Since EC2 Standard Reserved Instances cannot be canceled, the only way to remove the unneeded EC2 RIs and reclaim their cost is to sell them to other businesses and organizations on EC2 Reserved Instance Marketplace.

1.10.25 Total Number of EC2 Instances

Risk: Medium
Description: Determine if the number of EC2 instances provisioned in your AWS account has reached the limit quota established by your organization for the workload deployed.
Resolution: To raise an AWS support case to limit the number of provisioned EC2 instances based on your requirements.

1.10.26 EC2 Instance Type Generation

Risk: Medium
Description: Ensure that all servers available in your AWS account are using the latest generation of EC2 instances to get the best performance with lower costs.

1.10.27 Instance In Auto Scaling Group

Risk: Medium
Description: Orphaned EC2 Instances to make sure every instance is launched within an Auto Scaling Group in order to help improve the availability and scalability of your web applications during instance failures or denial-of-service attacks **Resolution**: To deploy a running EC2 instance into an AWS auto-scaling configuration using ASGs and ELBs for high reliability and security.

1.10.28 EC2 Platform

Risk: Medium
Description: Ensure that all your EC2 instances are deployed within the EC2-VPC platform instead of EC2-Classic platform for better flexibility and control over security, traffic routing and availability.
Resolution: To migrate your EC2-Classic instances to a VPC, you must recreate those instances in a VPC environment. To recreate the necessary instances.

1.10.29 EC2 Instance Limit

Risk: Medium
Description: Determine if the number of EC2 instances provisioned per region is close to the limit number established by EC2 Service Limit and request limit increase in order to avoid encountering resources limitations on future provisioning sessions. **Resolution**: To request an increase for EC2 instances limits based on your requirements.

1.10.30 EC2 Instance Naming Conventions

Risk: Low
Description: Ensure that all your EC2 instances are using suitable naming conventions for tagging in order to manage them more efficiently and adhere to AWS resource tagging best-practices. A naming convention is an established set of rules useful for choosing the name of an AWS resource.

1.10.31 EC2 Instances with Scheduled Events

Risk: High
Description: Determine if there are any EC2 instances scheduled for retirement and/or maintenance in your AWS account and take the necessary steps (reboot, restart or re-launch) to resolve them.
Resolution: To resolve EC2 instances scheduled for retirement/maintenance based on the event type (see Audit section to identify the event type(s) assigned to your instance(s)).

1.10.32 EC2 Instance Security Group Rules Count

Risk: Low
Description: Determine if there is a large number of security group rules assigned to an EC2 instance and reduce their number by removing any unnecessary or overlapping rules. To improve the instance network performance.
Resolution: To remove any unnecessary or overlapping inbound and outbound rules from the security group(s) associated with your EC2 instances.

1.10.33 EC2 Instance Tenancy Type

Risk: Medium
Description: Ensure that EC2 instances are using the appropriate tenancy model, i.e. Multi-Tenant Hardware (shared) or Single-Tenant Hardware (dedicated) in order to comply with your organization regulatory security requirements.
Resolution: To recreate/re-launch your running EC2 instances with the required tenancy.

1.10.34 EC2 Instance Termination Protection

Risk: Medium
Description: Ensure that the EC2 instances provisioned outside of the ASGs have Termination Protection safety feature enabled in order to protect your instances from being accidentally terminated.
Resolution: Enable Termination Protection for your EC2 instances launched manually using the AWS Management Console, API or CLI.

1.10.35 EC2 Instance Age

Risk: Low
Description: Identify and re-launch any running EC2 instances older than 180 days in order to ensure their reliability. An EC2 instance is not supposed to run indefinitely in the cloud and having too old instances in your AWS your account could increase the risk of potential issues. **Resolution**: To safely restart the old instances running inside your AWS account.

1.10.36 EC2 Instance IAM Roles

Risk: Medium
Description: Use IAM Roles/Instance Profiles instead of IAM Access Keys to appropriately grant access permissions to any application that perform API requests running on your EC2 instances. With IAM roles you can avoid sharing long-term credentials and protect your instances against unauthorized access. **Resolution**: To assign IAM roles to your running EC2 instances, you must re-launch those instances by creating images (AMIs) of the instances then launch new ones from images with the desired roles attached.

1.10.37 Overutilized EC2 Instances

Risk: High
Description: Identify any EC2 instances that appear to be overutilized and upgrade (resize) them in order to help your EC2-hosted applications to handle better the workload and improve the response time.
Resolution: Upgrade (upsize) the overused EC2 instances provisioned in your AWS account by adding more hardware resources (CPU and RAM memory) to the existing instances (vertical scaling).

1.10.38 Publicly Shared AMIs

Risk: Medium
Description: Ensure that AMIs aren't publicly shared with the other AWS accounts in order to avoid exposing sensitive data. **Resolution**: Share your images with specific AWS accounts without making them public.

1.10.39 EC2 Reserved Instance Lease Expiration

Risk: Recommendation
Description: Ensure that EC2 Reserved Instances are renewed before expiration in order to get a significant discount (up to 75% depending on the commitment term) on the hourly charges. The renewal process consists of purchasing another EC2 Reserved Instance so that Amazon can keep charging you based on the chosen reservation term.

Resolution: To renew the EC2 Reserved Instances before their reservation expire, you need to repurchase them using the same configuration attributes (region, instance type, OS platform, etc). To renew your existing EC2 RIs in order to avoid On-Demand rates charges when the current reservation expires.

1.10.40 EC2 Security Groups Count

Risk: Medium
Description: Determine if there is a large number of EC2 security groups available within each AWS regions and reduce their number by removing any unnecessary or obsolete security groups. To maintain optimal access security at the instance level, **Resolution**: To remove any unnecessary or obsolete EC2 security groups from an AWS region.

1.10.41 EC2 Security Group Port Range

Risk: Medium
Description: Ensure that security groups don't have range of ports opened for inbound traffic in order to protect your EC2 instances against denial-of-service (DoS) attacks or brute-force attacks.
Resolution: Implement specific ports instead of range of ports for your EC2 security groups.

1.10.42 Underutilized EC2 Instances

Risk: Recommendation
Description: Identify any EC2 instances that appear to be underutilized and downsize (resize) them to help lower the cost of your monthly AWS bill.
Resolution: Downsize (resize) the underused EC2 instances provisioned in your AWS account.

1.10.43 EC2 Security Group Unrestricted Access

Risk: Medium
Description: Check for EC2 security groups that allow total inbound and/or outbound access (0.0.0.0/0) on both common and uncommon ports (except 80 and 443 ports) in order to secure the access at the EC2 instance level.

1.10.44 Unrestricted CIFS Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 445 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict CIFS access to specific IPs.

1.10.45 Unrestricted DNS Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP and UDP port 53 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict DNS access to specific IPs.

1.10.46 Unrestricted ElasticSearch Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 9200 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict ElasticSearch access to specific IPs

1.10.47 Unrestricted FTP Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP ports 20 and 21 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict FTP access to specific IPs.

1.10.48 Unrestricted HTTP Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (i.e. 0.0.0.0/0) to TCP port 80 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict HTTP access to specific IPs.

1.10.49 Unrestricted HTTPS Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (i.e. 0.0.0.0/0) to TCP port 443 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict HTTPS access to specific IPs.

1.10.50 Unrestricted ICMP Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to any hosts using ICMP and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict ICMP access to specific IPs.

1.10.51 Unrestricted Inbound Access on Uncommon Ports

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to any uncommon TCP and UDP ports and restrict access to only those IP addresses that require it. A uncommon port can be any TCP/UDP port that is not included in the common services ports category, i.e. other than the commonly used ports such as 80 (HTTP), 443 (HTTPS), 20/21 (FTP), 22 (SSH), 23 (Telnet), 3389 (RDP), 1521 (Oracle), 3306 (MySQL), 5432 (PostgreSQL), 53 (DNS), 1433 (MSSQL) and 137/138/139/445 (SMB/CIFS). **Resolution**: Update EC2 security groups inbound configuration in order to restrict access to specific IPs.

1.10.52 Unrestricted MongoDB Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 27017 and restrict access to only those IP addresses that require it. TCP port 27017 is used by the MongoDB Database which is free and open-source cross-platform document-oriented NoSQL database **Resolution**: Update security groups inbound/ingress configuration in order to restrict Mongo Database access to specific IPs.

1.10.53 Unrestricted MSSQL Database Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 1433 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict MSSQL access to specific IPs.

1.10.54 Unrestricted MySQL Database Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 3306 and restrict access to only those IP addresses that require it. TCP port 3306 is used by the MySQL Server which is an open-source relational database management system (RDBMS) server. **Resolution**: Update security groups inbound/ingress configuration in order to restrict MySQL access to specific IPs.

1.10.55 Unrestricted NetBIOS Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 139 and UDP ports 137 and 138 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict NetBIOS access to specific IPs.

1.10.56 Unrestricted Oracle Database Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 1521 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict Oracle Database access to specific IPs.

1.10.57 Unrestricted Outbound Access on All Ports

Risk: Medium
Description: Check EC2 security groups for outbound rules that allow total access (0.0.0.0/0) to any TCP/UDP ports and restrict access to only those IP addresses that require it.
Resolution: Update EC2 security groups outbound configuration in order to restrict access to specific destinations.

1.10.58 Unrestricted PostgreSQL Database Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 5432 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict PostgreSQL Database access to specific IPs.

1.10.59 Unrestricted RDP Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 3389 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict RDP access to specific IPs.

1.10.60 Unrestricted RPC Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 135 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict RPC access to specific IPs.

1.10.61 Unrestricted SMTP Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 25 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict SMTP access to specific IPs.

1.10.62 Unrestricted SSH Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 22. Restrict access to only those IP addresses that require it,.
Resolution: Update security groups inbound/ingress configuration in order to restrict SSH access to specific IPs.

1.10.63 Unrestricted Telnet Access

Risk: Medium
Description: Check EC2 security groups for inbound rules that allow total access (0.0.0.0/0) to TCP port 23 and restrict access to only those IP addresses that require it.
Resolution: Update security groups inbound/ingress configuration in order to restrict Telnet access to specific IPs.

1.10.64 Unused Elastic Network Interfaces

Risk: Low
Description: Identify and delete any unused Elastic Network Interfaces in order to adhere to best-practices and to avoid reaching the service limit. An Elastic Network Interface (ENI) is pronounced unused when is not attached anymore to an EC2 instance. **Resolution**: To remove any unused Elastic Network Interfaces (ENIs) available in your AWS account.

1.10.65 Unused EC2 Key Pairs

Risk: Medium
Description: Identify and remove any unused EC2 key pairs in order to adhere to AWS security best-practices and protect against unapproved SSH access. An SSH key pair is evaluated as unused when is not associated with any of the EC2 instances available in the same AWS region. **Resolution**: To decommission (remove) any unused EC2 key pairs provisioned in your AWS account.

1.10.66 EC2-VPC Elastic IP Address Limit

Risk: Medium
Description: Determine if the number of EC2-VPC Elastic IPs (EIPs) allocated per region is close to the limit number established by AWS for accounts that support VPCs (VPCs) and request limit increase in order to avoid encountering IP resource limitations on future EC2 provisioning sessions. As the IPv4 public IP addresses are a scarce resource nowadays, all AWS accounts are limited to 5 (five) Elastic IP addresses per region. **Resolution**: To request an increase for the EC2-VPC Elastic IP limit.

1.10.67 Publicly Shared Web-Tier AMIs

Risk: High
Description: Ensure that none of the AMIs created in your web tier are publicly shared with other AWS accounts in order to avoid exposing sensitive information, as these images can contain proprietary web applications, personal data and configuration information that can be used to exploit or compromise running EC2 instances available in your web tier. **Resolution**: Make the publicly shared AMIs, available in your web tier.

1.10.68 Web-Tier EC2 Instances Without Elastic or Public IP Addresses

Risk: Medium
Description: Ensure that web-tier EC2 instances aren't associated with Elastic or Public IP addresses as these instances are usually deployed behind an internet-facing load balancer and don't have to be publicly reachable.
Resolution: To remove a Public IP address from a web-tier EC2 instance, you must re-launch the instance with the right network interface configuration.

1.10.69 Check web-tier ELB subnet connectivity to Internet Gateway

Risk: Medium
Description: Ensure that the VPC route table associated with the web-tier ELB subnets has the default route configured to allow access to an Internet Gateway (IGW) in order to provide internet connectivity for the web-tier load balancer. A VPC route table contains a set of rules (also known as routes) that are used to determine where the

network traffic is directed. The route table associated with the ELB subnets should contain a default route (i.e. 0.0.0.0/0) that points to an Internet Gateway. **Resolution**: To create the required route (i.e. 0.0.0.0/0) with an IGW configured as gateway for the route table associated with the web-tier ELB subnets

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

Risk: High
Description: Ensure that the IAM roles associated with your web-tier EC2 instances are using IAM policies to grant the necessary permissions to the web applications installed on these instances. The IAM policies must follow the principle of least privilege and provide the web-tier IAM roles the minimum level of access to the AWS services used by the applications. **Resolution**: To define and attach IAM policies to the IAM roles associated with your web-tier EC2 instances and implement the principle of least privilege (i.e. provide the minimal set of actions required to perform successfully the desired tasks)

1.10.71 IAM Roles for Web-Tier EC2 Instances

Risk: Medium
Description: Ensure that web-tier EC2 instances are using IAM roles to grant any necessary permissions to the web applications running on these instances as the applications can assume the role applied to their instances.
Resolution: To assign IAM roles to your running web-tier instances, you must re-launch those instances with the desired roles

1.10.72 Create and Configure Web-Tier Security Group

Risk: Medium
Description: Ensure there is an EC2 security group created and configured for the web tier to allow inbound traffic directly from the web-tier ELB security group for the required ports, in order to secure the access to the EC2 instances. **Resolution**: Create a compliant EC2 security group and configure it to allow inbound traffic from the web-tier ELB security group on explicit ports

1.10.73 Check web-tier subnet connectivity to VPC NAT Gateway

Risk: Medium
Description: Ensure that the VPC route table associated with the web-tier subnets has the default route configured to allow connectivity to the NAT Gateway deployed in the same VPC, in order to provide Internet access for the web-tier EC2 instances. **Resolution**: Create the necessary route with an NAT device configured as gateway for the route table associated with the web-tier subnets

---

1.11 ECR

- *ECR Unknown Cross Account Access*
- *Check for Exposed ECR Repositories*

1.11.1 ECR Unknown Cross Account Access

Risk: High
Description: Ensure that ECR repositories are configured to allow access only to trusted AWS accounts in order to protect against unauthorized cross account entities.
Resolution: Update the resource-based policies associated with your ECR repositories in order to allow cross account access only from trusted AWS entities

1.11.2 Check for Exposed ECR Repositories

Risk: High
Description: Identify any exposed ECR image repositories available in your AWS account and update their permissions in order to protect against unauthorized access.
Resolution: Update the resource-based policies associated with your ECR repositories in order to allow requests only from trusted entities

---

1.12 EFS

- *KMS Customer Master Keys for EFS Encryption*
- *Enable EFS Encryption*

1.12.1 KMS Customer Master Keys for EFS Encryption

Risk: High
Description: Ensure that EFS file systems are encrypted using KMS CMK customer-managed keys instead of AWS managed-keys (default keys used by the EFS service when there are no customer keys defined) in order to have more granular control over your data-at-rest encryption/decryption process. **Resolution**: To encrypt an existing EFS file system with your own KMS CMK customer-managed key you must copy the data from the existing file system onto the new one, that has the encryption feature enabled.

1.12.2 Enable EFS Encryption

Risk: High
Description: Ensure that EFS file systems are encrypted.
Resolution: To encrypt an existing EFS file system you must copy the data from the existing file system onto the new one, that has the encryption feature enabled.

1.13 ElasticSearch

- *ElasticSearch Cluster Status*
- *ElasticSearch Instance Type*
- *ElasticSearch Domain Encrypted with KMS CMKs*
- *ElasticSearch Unknown Cross Account Access*
- *ElasticSearch Exposed Domains*
- *ElasticSearch Domain IP-Based Access*
- *ElasticSearch General Purpose SSD Node Type*
- *ElasticSearch Version*
- *Enable ElasticSearch Zone Awareness*
- *Enable ElasticSearch Encryption At Rest*
- *ElasticSearch Free Storage Space*
- *Total Number of ElasticSearch Instances*
- *Enable ElasticSearch Node-to-Node Encryption*
- *Enable ElasticSearch Slow Logs*

1.13.1 ElasticSearch Cluster Status

Risk: High
Description: Ensure that ElasticSearch clusters are healthy.

1.13.2 ElasticSearch Instance Type

Risk: Medium
Description: Determine if the ElasticSearch instances provisioned have the desired instance type established by your organization based on the workload deployed.
Resolution: To limit the new ElasticSearch cluster instances to the desired type, create an AWS support case where you explain why you need this type of limitation.

1.13.3 ElasticSearch Domain Encrypted with KMS CMKs

Risk: High
Description: Ensure that ElasticSearch domains are encrypted with KMS Customer Master Keys (CMKs) instead of AWS managed-keys (default keys used by the ES service when there are no customer keys defined).
Resolution: To encrypt an existing ElasticSearch domain with your own KMS Customer Master Key, you must re-create the domain with the necessary encryption configuration.

1.13.4 ElasticSearch Unknown Cross Account Access

Risk: High

Description: Ensure that all your ElasticSearchclusters are configured to allow access only to trusted AWS users and accounts in order to protect against unauthorized cross account access.
Resolution: Update ElasticSearch clusters permissions in order to allow cross account access only from trusted entities.

1.13.5 ElasticSearch Exposed Domains

Risk: High
Description: Identify any publicly accessible ElasticSearch domains and update their access policy in order to stop any unsigned requests made to these resources (ES clusters).
Resolution: To block anonymous access to your ElasticSearch domains

1.13.6 ElasticSearch Domain IP-Based Access

Risk: High
Description: Ensure that the access to your ElasticSearchdomains is made based on whitelisted IP addresses only in order to protect them against unauthorized access.
Resolution: Implement an IP-based access policy for your ElasticSearch domains.

1.13.7 ElasticSearch General Purpose SSD Node Type

Risk: Recommendation
Description: Ensure that ElasticSearch clusters are using General Purpose SSD (gp2) data nodes instead of Provisioned IOPS SSD (io1) nodes for cost-effective storage that fits a broad range of workloads.
Resolution: To convert your ElasticSearch Provisioned IOPS SSD (io1) nodes to General Purpose SSD (gp2) nodes.

1.13.8 ElasticSearch Version

Risk: Medium
Description: Ensure that ElasticSearch clusters are using the latest version of ElasticSearch engine.
Resolution: To upgrade the ElasticSearch engine version for your ES domain, you must unload the existing data from the cluster to S3 then upload this data in a new ES cluster, created using the latest version of the ElasticSearch engine.

1.13.9 Enable ElasticSearch Zone Awareness

Risk: Medium
Description: Ensure that ElasticSearch cross-zone replication (Zone Awareness) is enabled to increase the availability of your ES clusters by allocating the nodes and replicate the data across two Availability Zones in the same region in order to prevent data loss and minimize downtime in the event of node or data center (AZ) failure.
Resolution: Enable cross-zone replication for your ElasticSearch clusters.

1.13.10 Enable ElasticSearch Encryption At Rest

Risk: High
Description: Ensure that ElasticSearch domains are encrypted.

Resolution: To enable at-rest encryption for your existing ElasticSearch domains, you must re-create them with the necessary encryption configuration.

1.13.11 ElasticSearch Free Storage Space

Risk: High
Description: Identify any ElasticSearch clusters that appear to run low on disk space and scale them up (add EBS-based storage) to help mitigate any issues triggered by insufficient disk space and improve their I/O performance.
Resolution: To expand the storage space for ElasticSearch clusters that run low on disk space, you can scale them up by adding storage to the existing data nodes volumes.

1.13.12 Total Number of ElasticSearch Instances

Risk: Medium
Description: Ensure that the number of ElasticSearch cluster instances (including dedicated master instances) provisioned in your AWS account has not reached the limit quota established by your organization for the ElasticSearch workload deployed. **Resolution**: To build an AWS support case to limit the number of provisioned ElasticSearch instances based on your requirements

1.13.13 Enable ElasticSearch Node-to-Node Encryption

Risk: High
Description: Ensure that node-to-node encryption feature is enabled for your ElasticSearch domains (clusters) in order to add an extra layer of data protection on top of the existing ES security features such as HTTPS client to cluster encryption and data-at-rest encryption and meet strict compliance requirements. **Resolution**: To enable node-to-node encryption for your existing ElasticSearch domains, you need to re-create them with the necessary configuration.

1.13.14 Enable ElasticSearch Slow Logs

Risk: Medium
Description: Ensure that ElasticSearch clusters have enabled the support for publishing slow logs to CloudWatch Logs.
Resolution: Enable ElasticSearch Slow Logs publishing to CloudWatch Logs.

1.14 ELB

- *Enable HTTPS/SSL Listener for App-Tier ELBs*
- *Enable Latest SSL Security Policy for App-Tier ELBs*
- *Add SSL/TLS Server Certificates to App-Tier ELBs*
- *App-Tier ELBs Health Check*

- *Enable ELB Access Logging*
- *AWS Classic Load Balancer*
- *Connection Draining Enabled*
- *Enable ELB Cross-Zone Load Balancing*
- *ELB insecure SSL ciphers*
- *ELB insecure SSL protocols*
- *ELB Listener Security*
- *ELB minimum number of EC2 instances*
- *ELB Security Group*
- *ELB Security Policy*
- *Remove unused ELBs*
- *ELB Instances Distribution Across Availability Zones*
- *Review AWS Internet Facing Load Balancers*
- *Enable HTTPS/SSL Listener for Web-Tier ELBs*
- *Enable Latest SSL Security Policy for Web-Tier ELBs*
- *Add SSL/TLS Server Certificates to Web-Tier ELBs*
- *Web-Tier ELBs Health Check*
- *Enable ALB (ELBv2)-Access-Logging*
- *Enable Elastic Load Balancing Deletion Protection*
- *ELBv2 Instances Distribution Across Availability Zones*
- *ALB (ELBv2)-Listener-Security*
- *Minimum Number of EC2 Target Instances*
- *ELBv2 Security Groups*
- *ALB (ELBv2)-Security-Policy*
- *Unused ELBs (ELBv2)*

1.14.1 Enable HTTPS/SSL Listener for App-Tier ELBs

Risk: High
Description: Ensure that app-tier ELB listeners are using the HTTPS/SSL protocol to encrypt the communication between your application clients and the load balancer.
Resolution: To secure the connection between the application clients and app-tier load balancer by using SSL encryption,

1.14.2 Enable Latest SSL Security Policy for App-Tier ELBs

Risk: High
Description: Ensure that app-tier ELBs listeners are using the latest AWS security policy for their SSL negotiation config.

Resolution: Enable the latest predefined SSL security policy for your app-tier ELBs

1.14.3 Add SSL/TLS Server Certificates to App-Tier ELBs

Risk: High
Description: Ensure that app-tier ELBs are using SSL/TLS certificates to encrypt the communication between your application users and the load balancer.
Resolution: To secure the traffic between your application users and the app-tier load balancer using SSL encryption, Update ELB configuration to attach an SSL/TLS server certificate.

1.14.4 App-Tier ELBs Health Check

Risk: High
Description: Ensure that app-tier ELBs are using the right health check configuration in order to monitor the availability of the EC2 instances registered to the ELBs through application layer.
Resolution: Update app-tier ELBs configuration in order to use application layer health checks instead of TCP health checks.

1.14.5 Enable ELB Access Logging

Risk: Medium
Description: Ensure that ELBs use access logging to analyze traffic patterns and identify and troubleshoot security issues.
Resolution: Enable access logging for your ELBs.

1.14.6 AWS Classic Load Balancer

Risk: Medium
Description: Ensure that HTTP/HTTPS applications (monolithic or containerized) are using the Application Load Balancer (ALB) instead of Classic Load Balancer (ELB) for enhanced incoming traffic distribution, better performance and lower costs. **Resolution**: Migrate your HTTP/HTTPS web application(s) from a Classic Load Balancer (ELB) to an Application Load Balancer (ALB) using the AWS Management Console and AWS CLI. To move your application(s) instances to the ALB, redirect the traffic and remove the ELB.

1.14.7 Connection Draining Enabled

Risk: Medium
Description: With Connection Draining feature enabled, if an EC2 backend instance fails health checks the ELB 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. **Resolution**: Enable Connection Draining.

1.14.8 Enable ELB Cross-Zone Load Balancing

Risk: Medium

Description: By using at least two subnets in different Availability Zones with the Cross-Zone Load Balancing feature enabled, your ELBs can distribute the traffic evenly across all backend instances.
Resolution: Enable Cross-Zone Load Balancing with at least two subnets in different Availability Zones.

1.14.9 ELB insecure SSL ciphers

Risk: Medium
Description: Check ELBs Secure Socket Layer (SSL) negotiation configuration (security policy) for any cipher suites that demonstrate vulnerabilities or have been rendered insecure by recent exploits.
Resolution: To remove any insecure cipher definitions from your ELB SSL negotiation settings.

1.14.10 ELB insecure SSL protocols

Risk: Medium
Description: Check ELBs SSL negotiation configuration for SSLv2, SSLv3, and TLSv1 insecure / deprecated SSL protocols
Resolution: To remove any insecure protocol definitions from your ELB SSL negotiation settings.

1.14.11 ELB Listener Security

Risk: High
Description: Check ELBs listener for secure configurations.
Resolution: To secure the connection between the client and the load balancer, update each ELB configuration to use listeners with HTTPS or SSL protocols (an X.509 SSL certificate is required).

1.14.12 ELB minimum number of EC2 instances

Risk: High
Description: Ensure that ELBs have at least two healthy EC2 backend instances assigned, in order to provide a better fault-tolerant load balancing configuration.
Resolution: To register additional healthy EC2 backend instances with your ELBs.

1.14.13 ELB Security Group

Risk: High
Description: Check ELB security layer for at least one valid security group that restrict access only to the ports defined in the load balancer listeners configuration.
Resolution: Update an insecure or invalid security group assigned to your load balancer.

1.14.14 ELB Security Policy

Risk: Medium
Description: Ensure that ELBs are using the latest AWS predefined security policies, ELBSecurityPolicy-2016-08 or ELBSecurityPolicy-TLS-1-2-2017-01 or ELBSecurityPolicy-TLS-1-1-2017-01, for their SSL negotiation configuration.

Resolution: Update ELB SSL negotiation configuration to use the latest AWS Predefined Security Policies.

1.14.15 Remove unused ELBs

Risk: Recommendation
Description: Identify unused ELBs, and delete them to help lower the cost of your monthly AWS bill.
Resolution: To remove any unused or inactive ELBs from your AWS account.

1.14.16 ELB Instances Distribution Across Availability Zones

Risk: Medium
Description: Ensure that the EC2 instances registered to your Elastic Load Balancing (ELB) are evenly distributed across all Availability Zones in order to improve the ELBs configuration reliability.
Resolution: To equally distribute your existing ELB backend instances across all Availability Zones within the selected AWS region, you need to add new Availability Zones to the ELB configuration and migrate the registered instances between these Availability Zones.

1.14.17 Review AWS Internet Facing Load Balancers

Risk: High
Description: Ensure that all Amazon internet-facing load balancers (Classic Load Balancers and Application Load Balancers) provisioned in your AWS account are regularly reviewed for security purposes.

1.14.18 Enable HTTPS/SSL Listener for Web-Tier ELBs

Risk: High
Description: Ensure that web-tier ELB listeners are using a secure protocol such as HTTPS/SSL to encrypt the communication between the web application clients and the load balancer.
Resolution: To secure the connection between the web clients and your web-tier load balancer by using SSL encryption, Update ELB configuration to use listeners with HTTPS or SSL protocols (an X.509 SSL certificate is required).

1.14.19 Enable Latest SSL Security Policy for Web-Tier ELBs

Risk: High
Description: Ensure that web-tier ELBs listeners are using the latest AWS security policy for their SSL negotiation configuration.
Resolution: Enable the latest predefined SSL security policy for your web-tier ELBs.

1.14.20 Add SSL/TLS Server Certificates to Web-Tier ELBs

Risk: High
Description: Ensure that web-tier ELBs are using SSL/TLS server certificates to encrypt the communication between the web application clients and the load balancer. When you use HTTPS/SSL (secure HTTP/TCP) for the ELB front-end listeners, you must deploy an SSL/TLS certificate on your load balancer. This SSL/TLS server

certificate is used by the web-tier ELB to terminate the connection and decrypt requests from clients before sending them to the EC2 instances behind the load balancer (also known as backend instances). **Resolution**: To secure the traffic between the web clients and your web-tier load balancer using SSL encryption, Update ELB configuration to attach an SSL/TLS server certificate (an X.509 certificate is required).

1.14.21 Web-Tier ELBs Health Check

Risk: High

Description: Ensure that web-tier ELBs are using the appropriate health check configuration in order to monitor the availability of the EC2 instances associated with the ELBs through application layer.

Resolution: Update web-tier ELBs configuration in order to use application layer health checks instead of TCP health checks.

ELBv2

1.14.22 Enable ALB (ELBv2) Access Logging

Risk: Medium

Description: Ensure that Application Load Balancers (ALBs) have Access Logging feature enabled for security, troubleshooting and statistical analysis purposes.

Resolution: Enable access logging for your Application Load Balancers (ALBs)

1.14.23 Enable Elastic Load Balancing Deletion Protection

Risk: Medium

Description: Ensure ELBv2 Load Balancers have Deletion Protection feature enabled in order to protect them from being accidentally deleted.

Resolution: Enable Deletion Protection safety feature for your Application Load Balancers and Network Load Balancers (ELBv2)

1.14.24 ELBv2 Instances Distribution Across Availability Zones

Risk: Medium

Description: Ensure that the EC2 instances (targets) registered to your Application Load Balancers (ALBs) and Network Load Balancers (NLBs) are evenly distributed across all Availability Zones in order to improve the reliability of your load balancers configuration. **Resolution**: To equally distribute your existing EC2 target instances across all Availability Zones within the selected AWS region, you need to add new Availability Zones to the ELBv2 load balancer configuration and migrate the registered instances between these Availability Zones.

1.14.25 ALB (ELBv2) Listener Security

Risk: High

Description: Check Application Load Balancer listeners for secure configurations.

Resolution: To secure the connection between your application clients and your load balancers, update ALBs listeners configuration to support the HTTPS protocol (an X.509 SSL certificate is required).

1.14.26 Minimum Number of EC2 Target Instances

Risk: High
Description: Ensure there are at least two healthy EC2 target instances registered to each Application Load Balancer (ALB) and Network Load Balancer (NLB) in order to provide a fault-tolerant load balancing configuration for your applications. **Resolution**: To register additional healthy EC2 instances to the target group(s) associated with your ELBv2 load balancers.

1.14.27 ELBv2 Security Groups

Risk: High
Description: Ensure that all Application Load Balancers (ALBs) available in your AWS account are associated with valid and secure security groups that restrict access only to the ports defined within the load balancers listeners configuration. **Resolution**: To replace any invalid/insecure security group associated with your ELBv2 load balancers.

1.14.28 ALB (ELBv2) Security Policy

Risk: Medium
Description: Ensure that ALBs are using the latest predefined security policy for their SSL negotiation configuration in order to follow security best-practices and protect their front-end connections against SSL/TLS vulnerabilities.
Resolution: Update Application Load Balancers listeners configuration to use the latest predefined security policies

1.14.29 Unused ELBs (ELBv2)

Risk: Recommendation
Description: Find any unused Application Load Balancers (ALBs) and Network Load Balancers (NLBs) and remove them in order to help lower the cost of your monthly AWS bill. An ELBv2 load balancer is considered "unused" when the associated target group has no EC2 target instance registered or when the registered target instances aren't healthy anymore. **Resolution**: Delete any unused ELB currently available in your AWS account

---

1.15 EMR

- *EMR Cluster In VPC*
- *EMR Desired Instance Type*
- *EMR Instance Type Generation*
- *Enable EMR In-Transit and At-Rest Encryption*
- *Total Number of EMR Instances*

1.15.1 EMR Cluster In VPC

Risk: Medium
Description: Ensure that EMR clusters are provisioned using the EC2-VPC platform instead of EC2-Classic platform (outdated from 2013.12.04) for better flexibility and control over security, better traffic routing and availability.
Resolution: To migrate your EMR clusters from EC2-Classic platform to EC2-VPC platform, you must re-create your clusters within a VPC. To relaunch and configure your EMR clusters in an VPC

1.15.2 EMR Desired Instance Type

Risk: Medium
Description: Determine if the EMR cluster instances (master and core instances) provisioned in your AWS account have the desired instance type established by your organization based on the workload deployed.
Resolution: To limit the new Elastic MapReduce cluster instances to the desired type, create an AWS support case where you explain why you need this type of limitation. For any existing EMR clusters launched without using the desired instance type, just clone the necessary clusters and re-create them using the desired instance type.

1.15.3 EMR Instance Type Generation

Risk: Medium
Description: Ensure that all EMR clusters provisioned in your AWS account are using the latest generation of instances in order to get better performance at lower cost.

1.15.4 Enable EMR In-Transit and At-Rest Encryption

Risk: High
Description: Ensure that EMR clusters are encrypted in order to meet security and compliance requirements. Data encryption helps prevent unauthorized users from reading sensitive data available on your EMR clusters and their associated data storage systems. This includes data saved to persistent media, known as data at-rest, and data that can be intercepted as it travels through the network, known as data in-transit. **Resolution**: To enable in-transit and at-rest encryption for your existing EMR clusters, you must define and configure an EMR security configuration then re-create these clusters with the new security configuration.

1.15.5 Total Number of EMR Instances

Risk: Medium
Description: Ensure that the number of Elastic MapReduce (EMR) cluster instances (master and core instances) provisioned in your AWS account has not reached the limit quota established by your organization for the EMR workload deployed. **Resolution**: To build an AWS support case in order to limit the number of provisioned Elastic MapReduce cluster instances based on your requirements

---

1.16 GuardDuty

- *GuardDuty Findings*

- *Monitor GuardDuty Configuration Changes*
- *GuardDuty In Use*

1.16.1 GuardDuty Findings

Risk: Medium
Description: Check for GuardDuty findings and resolve them step by step to ensure that AWS infrastructure is protected against security threats.

1.16.2 Monitor GuardDuty Configuration Changes

Risk: High
Description: Monitor GuardDuty Configuration Changes.
Resolution: Enable GuardDuty

1.16.3 GuardDuty In Use

Risk: Medium
Description: Ensure that GuardDuty service is currently enabled in order to protect your AWS environment and infrastructure (AWS accounts and resources, IAM credentials, guest operating systems, applications, etc) against security threats. **Resolution**: Enable GuardDuty

---

1.17 Health

- *AWS Health*

1.17.1 AWS Health

Risk: Medium
Description: Provides ongoing visibility into the health state of your AWS resources and services in order to keep you fully aware of what is happening in your AWS account from the availability and performance standpoint.

1.18 IAM

- *Unused IAM Access Keys*
- *IAM Access Keys Rotation*
- *Unnecessary IAM Access Keys*

- *Enable Security Challenge Questions for your Account*
- *Attach Policy to IAM Roles Associated with App-Tier EC2 Instances*
- *SSL/TLS Certificate Renewal*
- *Server Certificate Signature Algorithm*
- *IAM Server Certificate Size*
- *Deprecated AWS Managed Policies In Use*
- *IAM Users Unauthorized to Edit Access Policies*
- *IAM Users with Admin Privileges*
- *Detect IAM Configuration Changes*
- *IAM Group with Administrator Privileges In Use*
- *Unused IAM Groups*
- *Remove IAM Policies with Full Administrative Privileges*
- *IAM Customer Managed Policy with Administrative Permissions In Use*
- *IAM Role Policy Too Permissive*
- *IAM User Present*
- *Inactive IAM Users*
- *Unused IAM Users*
- *IAM Users with Password and Access Keys*
- *Valid IAM Identity Providers*
- *MFA Device Deactivated for IAM Users*
- *Enable MFA for IAM Users*
- *IAM Master and IAM Manager Roles*
- *IAM Password Expiry*
- *IAM Password Policy*
- *Root Account Access Keys*
- *Root Account Credentials Usage*
- *Root Account Active Signing Certificates*
- *Enable Hardware MFA for Root Account*
- *Enable MFA for Root Account*
- *IAM SSH Public Keys Rotation (90-Days)*
- *Unnecessary IAM SSH Public Keys*
- *IAM Support Role*

1.18.1 Unused IAM Access Keys

Risk: Medium
Description: Identify and remove any unused IAM access keys in order to protect your AWS resources against unapproved access. An IAM user access key pair is rendered as unused when is not being used for a specified period of time.
Resolution: To remove any unused (non-operational for more than 30 days) IAM access keys.

1.18.2 IAM Access Keys Rotation

Risk: High
Description: Ensure that all your IAM user access keys are rotated every month in order to decrease the likelihood of accidental exposures and protect your AWS resources against unauthorized access.
Resolution: To rotate (change) your outdated IAM access keys.

1.18.3 Unnecessary IAM Access Keys

Risk: Medium
Description: Identify and deactivate any unnecessary IAM access keys as a security best practice. AWS allows you to assign maximum two active access keys but this is recommended only during the key rotation process.
Resolution: To deactivate any unnecessary IAM access keys.

1.18.4 Enable Security Challenge Questions for your Account

Risk: Very High
Description: Ensure your account is configured to use security challenge questions so Amazon can use these questions to verify your identity in case your account become compromised or if you just need to contact their customer service for help. **Resolution**: To secure your AWS account identity by enabling and configuring security challenge questions.

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

Risk: High
Description: Ensure that the IAM roles associated with your app-tier EC2 instances are using IAM policies to assign necessary permissions to the applications installed on these instances.
Resolution: To define and attach access policies to the IAM roles associated with your app-tier EC2 instances and implement the principle of least privilege (i.e. provide the minimal set of actions required to perform successfully the desired tasks).

1.18.6 SSL/TLS Certificate Renewal

Risk: High
Description: Ensure that SSL/TLS certificates stored in IAM are renewed X days before their validity period ends.
Resolution: To renew (replace) the SSL/TLS certificates currently deployed on your ELBs.

1.18.7 Server Certificate Signature Algorithm

Risk: High
Description: - Ensure that all the SSL/TLS certificates stored within IAM aren't using the MD5/SHA-1 signature algorithm in order to adhere to AWS security best-practices and protect from Collision attacks (i.e. cryptographic hash collisions). **Resolution**: To replace any insecure/deprecated SSL/TLS certificates managed by IAM service.

1.18.8 IAM Server Certificate Size

Risk: Very High
Description: Ensure that all your SSL/TLS certificates, managed by IAM, have a strong key length of 2048 or 4096 bit.
Resolution: To replace any 1024-bit RSA SSL/TLS certificates currently available within IAM

1.18.9 Deprecated AWS Managed Policies In Use

Risk: Medium
Description: Ensure that deprecated IAM managed policies are replaced with new ones, approved by AWS.
Resolution: Change deprecated AWS managed policies with their replacement policies within IAM entities configuration

1.18.10 IAM Users Unauthorized to Edit Access Policies

Risk: High
Description: Identify any IAM users that aren't authorized to edit IAM policies and decommission them in order to protect against unapproved access.
Resolution: To decommission any unauthorized IAM users that have the permission to edit IAM access policies in your AWS account.

1.18.11 IAM Users with Admin Privileges

Risk: High
Description: Ensure that there are no IAM users with administrator permissions (i.e. privileged users) available in your AWS account in order to adhere to IAM security best-practices and implement the principle of least privilege (the practice of providing every user the minimal amount of access required to perform its tasks). **Resolution**: To adhere to security best-practices and implement the IAM Master and IAM Manager role policies for your privileged IAM user.

1.18.12 Detect IAM Configuration Changes

Risk: High
Description: To detect configuration changes made at the IAM service level, in your AWS account.

1.18.13 IAM Group with Administrator Privileges In Use

Risk: Medium
Description: Ensure there is an IAM group that has the types of permissions that administrators typically need, available in your AWS account.
Resolution: Create an IAM group that provides administrative permissions to the IAM users assigned to the group, required for administration purposes

1.18.14 Unused IAM Groups

Risk: Low
Description: Ensure that all the IAM groups in your AWS account are currently used and have at least one user attached. Otherwise, remove any orphaned (unused) IAM groups in order to prevent attaching unauthorized users.
Resolution: To remove all your unused IAM groups.

1.18.15 Remove IAM Policies with Full Administrative Privileges

Risk: High
Description: Ensure there are no IAM policies (inline and customer managed) that allow full administrative privileges available in your AWS account, in order to promote the principle of least privilege and provide the users, groups and roles that use these policies the minimal amount of access required to perform their tasks. **Resolution**: To detach IAM managed policies that provide full administrative privileges from IAM users, groups and roles

1.18.16 IAM Customer Managed Policy with Administrative Permissions In Use

Risk: Medium
Description: Ensure there is an IAM customer managed policy that allows administrative privileges for all AWS services and components, available in your AWS account.
Resolution: Create an IAM customer managed policy with administrative permissions, required for administration purposes

1.18.17 IAM Role Policy Too Permissive

Risk: Medium
Description: Ensure that the access policies attached to your IAM roles adhere to the principle of least privilege by giving the roles the minimal set of actions required to perform successfully their tasks

1.18.18 IAM User Present

Risk: Medium
Description: Ensure that the access to your AWS services and resources is made only through individual IAM users instead of the root account.
Resolution: Create IAM users necessary for everyday access to your AWS account.

1.18.19 Inactive IAM Users

Risk: Medium
Description: Identify any inactive IAM users, which aren't designed for API access, and disable their access as an extra security measure for protecting your AWS resources against unauthorized access.
Resolution: Disable the password-based access for any inactive IAM users and terminate their ability to access AWS resources through the Management Console.

1.18.20 Unused IAM Users

Risk: Medium
Description: Identify and remove any unused IAM users, which aren't designed for API access, as an extra security measure for protecting your AWS resources against unapproved access.
Resolution: Remove any unused IAM users from your AWS account.

1.18.21 IAM Users with Password and Access Keys

Risk: Medium
Description: Ensure that existing IAM users are either being used for API access or for console access in order to reduce the risk of unauthorized access in case their credentials (access keys or passwords) are compromised.

1.18.22 Valid IAM Identity Providers

Risk: Medium
Description: Ensure that the IAM Identity Providers (IdPs) utilized in your AWS account are valid in order to manage securely your user identities outside of AWS and give these external identities permissions to use AWS resources in your account. **Resolution**: To replace an invalid Identity Provider (IdP) available in your AWS account.For SAML Identity Providers:

1.18.23 MFA Device Deactivated for IAM Users

Risk: High
Description: MFA device deactivated for IAM users. When DeactivateMFADevice event is triggered, the system decommissions the specified MFA device and removes it from association with the IAM user name for which it was originally enabled, removing the extra layer of protection, set for the IAM user to achieve stronger authentication.

1.18.24 Enable MFA for IAM Users

Risk: High
Description: Ensure that all users with AWS Console access have MFA enabled in order to secure your AWS environment and adhere to IAM security best-practices.
Resolution: Enable MFA access protection for your IAM users.

1.18.25 IAM Master and IAM Manager Roles

Risk: High
Description: Ensure that the IAM administration and permission management in your AWS account is divided between two roles: IAM Master and IAM Manager. The IAM Master role duty is to create IAM users, groups and roles, while the IAM Manager role responsibility is to assign users and roles to groups. **Resolution**: Create the IAM Master and IAM Manager roles necessary for an efficient IAM administration and permission management in your AWS account.

1.18.26 IAM Password Expiry

Risk: Medium
Description: Identify the age of your IAM user passwords and ensure that these credentials are reset before their validity period ends in order to prevent password expiry.
Resolution: To reset any IAM user passwords that are about to expire soon.

1.18.27 IAM Password Policy

Risk: High
Description: Ensure that IAM users are using a strong password policy to define password requirements such as minimum length, expiration date, whether it requires a certain pattern, and so forth.
Resolution: Enable the IAM password policy for your AWS account.

1.18.28 Root Account Access Keys

Risk: High
Description: To secure your AWS environment and adhere to IAM best-practices ensure that the AWS account (root user) is not using access keys to perform API requests to access resources or billing information.
Resolution: To remove any active access keys created for your AWS root account.

1.18.29 Root Account Credentials Usage

Risk: High
Description: Ensure that the AWS root account credentials have not been used within the past 30 days (default threshold) to access your AWS account in order to keep the root account usage minimised.
Resolution: To restrict AWS root account usage implement the principle of least privilege by creating IAM users with minimal set of permissions necessary to access and manage just the required AWS resources and services.

1.18.30 Root Account Active Signing Certificates

Risk: High
Description: To secure your AWS account and adhere to security best-practices, ensure that AWS root user is not using X.509 certificates to perform SOAP-protocol requests to AWS services.
Resolution: To disable any active X.509 signing certificates created for your AWS root account

1.18.31 Enable Hardware MFA for Root Account

Risk: High
Description: Ensure that hardware MFA is enabled for your root account in order to secure the access to your AWS resources and adhere to Amazon security best-practices.
Resolution: Implement strong protection for your AWS root account using a MFA hardware device.

1.18.32 Enable MFA for Root Account

Risk: High
Description: Ensure that MFA is enabled for your root account in order to secure your AWS environment and adhere to IAM security best-practices.
Resolution: Enable MFA access protection for your AWS root account.

1.18.33 IAM SSH Public Keys Rotation (90 Days)

Risk: High
Description: Ensure that all your IAM SSH public keys are rotated every X days in order to decrease the likelihood of accidental exposures and protect your AWS CodeCommit repositories from unauthorized access.
Resolution: To rotate (change) your outdated IAM SSH public keys.

1.18.34 Unnecessary IAM SSH Public Keys

Risk: Medium
Description: Identify and deactivate any unnecessary IAM SSH public keys used to authenticate to AWS CodeCommit repositories. Amazon allows you to assign maximum two active SSH keys, however having two keys is recommended only during the key rotation process. As security best practice, **Resolution**: To deactivate any unnecessary IAM SSH public keys used for AWS CodeCommit repository access.

1.18.35 IAM Support Role

Risk: High
Description: Ensure there is an active IAM Support Role available in your AWS account. A Support Role is an IAM role configured to allow authorized users to manage incidents with AWS Support.
Resolution: Create an IAM Support Role and configure it to allow only authorized users to manage incidents with Support.

1.19 Inspector

- *AWS Inspector Findings*

1.19.1 AWS Inspector Findings

Risk: Medium
Description: Check for AWS Inspector Findings and resolve them step by step to ensure that systems are configured securely.
Resolution: To solve any Inspector Findings discovered for your EC2 resources provisioned in your AWS account.

1.20 KMS

- *App-Tier Customer Master Key In Use*
- *KMS Customer Master Key In Use*
- *Database Tier Customer Master Key In Use*
- *Default KMS Key Usage*
- *Disabled KMS keys*
- *Monitor KMS Configuration Changes*
- *KMS Unknown Cross Account Access*
- *KMS Exposed Keys*
- *Recover KMS Customer Master Keys*
- *Enable KMS Key Rotation*
- *Remove unused KMS keys*
- *Web-Tier Customer Master Key In Use*

1.20.1 App-Tier Customer Master Key In Use

Risk: High
Description: Ensure there is one KMS Customer Master Key created in your AWS account for the app tier in order to protect data that transits your AWS application stack, have full control over encryption process, and meet security and compliance requirements. **Resolution**: Create a dedicated KMS Customer Master Key to be used by AWS resources and services in your app stack.

1.20.2 KMS Customer Master Key In Use

Risk: Medium
Description: Ensure that you have KMS CMK customer-managed keys in use in your account instead of AWS managed-keys in order to have full control over your data encryption and decryption process. KMS CMK customer-managed keys can be used to encrypt and decrypt data for multiple AWS components such as S3, Redshift, EBS and RDS. **Resolution**: Use your own CMK customer-managed key instead of the default / AWS-managed key to encrypt an EBS vol.

1.20.3 Database Tier Customer Master Key In Use

Risk: High
Description: Ensure there is one KMS Customer Master Key created in your AWS account for the database tier in order to protect data-at-rest available in your AWS web stack, have full control over encryption/decryption process, and meet security and compliance requirements. **Resolution**: Create a dedicated KMS Customer Master Key to be used by AWS resources in your database tier

1.20.4 Default KMS Key Usage

Risk: Medium
Description: - Ensure that KMS Customer Master Keys (CMKs) are used by your AWS services and resources instead of default KMS keys, in order to have full control over data encryption/decryption process and meet compliance requirements **Resolution**: Use your own KMS Customer Master Key instead of the AWS default master key to encrypt an EBS volume

1.20.5 Disabled KMS keys

Risk: Recommendation
Description: Check for any disabled KMS keys available in your AWS account and remove them in order to lower the cost of your monthly bill.
Resolution: Schedule deletion for any disabled KMS Customer Master Keys available in your AWS account.

1.20.6 Monitor KMS Configuration Changes

Risk: High
Description: Monitor KMS Configuration Changes.

1.20.7 KMS Unknown Cross Account Access

Risk: High
Description: Ensure that all your KMS keys are configured to be accessed only by trusted AWS accounts in order to protect against unauthorized cross account access.
Resolution: Update KMS keys permissions in order to allow cross account access only to trusted entities.

1.20.8 KMS Exposed Keys

Risk: High
Description: Identify any publicly accessible KMS master keys and update their access policy in order to stop any unsigned requests made to these resources.
Resolution: To block anonymous access to your KMS master keys.

1.20.9 Recover KMS Customer Master Keys

Risk: Medium
Description: Identify any disabled KMS Customer Master Keys (CMK) that have been accidentally or intentionally scheduled for deletion in order to prevent losing any data encrypted with these keys.
Resolution: KMS allows a waiting period between 7 and 30 days before the key is completely deleted and unrecoverable. The deletion can be canceled any time before the selected waiting period expires. To cancel any KMS CMK scheduled for deletion.

1.20.10 Enable KMS Key Rotation

Risk: Medium
Description: Once enabled, the KMS Key Rotation will allow you to set an yearly rotation schedule for your CMK so when a customer master key is required to encrypt your new data, the KMS service can automatically use the latest version of the HSA backing key (AWS hardened security appliance key) to perform the encryption. **Resolution**: Enable KMS Key Rotation.

1.20.11 Remove unused KMS keys

Risk: Recommendation
Description: Check for any disabled KMS Customer Master Keys in your AWS account and remove them in order to lower the cost of your monthly AWS bill.
Resolution: KMS allows a waiting period between 7 and 30 days before the key is completely deleted and unrecoverable. The deletion can be canceled any time before the waiting period expires.

1.20.12 Web-Tier Customer Master Key In Use

Risk: High
Description: Ensure there is one KMS Customer Master Key created in your AWS account for the web tier in order to protect data that transits your AWS web stack, have full control over data encryption/decryption process, and meet compliance requirements. **Resolution**: Create a dedicated KMS Customer Master Key to be used by AWS resources provisioned in your web tier

---

1.21 Lambda

- *Exposed Lambda Functions*
- *Lambda Functions with Admin Privileges*
- *Lambda Unknown Cross Account Access*
- *Lambda Runtime Environment Version*
- *An IAM role for a Lambda Function*

1.21.1 Exposed Lambda Functions

Risk: High
Description: Identify any publicly accessible Lambda functions and update their access policy in order to protect against unauthorized users that are sending requests to invoke these functions.
Resolution: Update the access policies (also known as resource-based policies) associated with your Lambda functions in order to allow function invocation only from trusted AWS entities.

1.21.2 Lambda Functions with Admin Privileges

Risk: Medium
Description: Ensure that Lambda functions do not have administrative permissions (i.e. access to all AWS actions and resources) in order to promote the Principle of Least Privilege and provide your functions the minimal amount of access required to perform their tasks. **Resolution**: Implement the Principle of Least Privilege and provide your Lambda functions with the right set of permissions instead of full administrative permissions.

1.21.3 Lambda Unknown Cross Account Access

Risk: High
Description: Ensure that all your Lambda functions are configured to allow access only to trusted AWS accounts in order to protect against unauthorized cross account access (i.e. unknown function invocation requests
Resolution: Update the resource-based policies associated with your Lambda functions in order to allow function invocation only from trusted AWS accounts.

1.21.4 Lambda Runtime Environment Version

Risk: Medium
Description: Ensure that you always use the latest version of the execution environment for your Lambda functions in order to adhere to AWS best-practices and receive the newest software features, get the latest security patches and bug fixes, and benefit from better performance and reliability. **Resolution**: To upgrade the runtime environment version for your Lambda functions

1.21.5 An IAM role for a Lambda Function

Risk: High
Description: Ensure that Lambda functions do not share the same IAM execution role in order to promote the Principle of Least Privilege (POLP) by providing each individual function the minimal amount of access required to perform its tasks. **Resolution**: Create a separate IAM role (with the right set of permissions) for each individual Lambda function.

1.22 Organizations

- *Monitor AWS Org. Configuration Changes*

- *Enable All Features*
- *AWS Organizations In Use*

1.22.1 Monitor AWS Org. Configuration Changes

Risk: High
Description: Monitor AWS Organizations Configuration Changes.

1.22.2 Enable All Features

Risk: Medium
Description: Ensure that All Features is enabled in your Amazon Organizations to achieve full control over the use of AWS services and actions across multiple AWS accounts using Service Control Policies (SCPs).

1.22.3 AWS Organizations In Use

Risk: Medium
Description: Ensure that Amazon Organizations service is currently in use to gain central control over the use of AWS services across multiple AWS accounts (using Service Control Policies) in order to help you comply with the security and compliance policies in your company. **Resolution**: To make use of Amazon Organizations service and benefit from centralized control over the use of AWS services across multiple accounts you must create first an organization (with All features set enabled) using your current AWS account as the master account then invite other accounts to join your organization.

1.23 RDS

- *Aurora Database Instance Accessibility*
- *RDS Auto Minor Version Upgrade*
- *Enable RDS Automated Backups*
- *Enable RDS Deletion Protection*
- *Enable RDS Encryption*
- *RDS Free Storage Space*
- *Enable IAM Database Authentication*
- *Total Number of Provisioned RDS Instances*
- *RDS Multi-AZ*
- *Overutilized RDS Instances*
- *Publicly Accessible RDS Instances*
- *Use Data-Tier Security Group for RDS Databases*
- *RDS Database Default Port*

- *Use KMS Customer Master Keys for RDS encryption*
- *RDS General Purpose SSD Storage Type*
- *RDS Instance Not In Public Subnet*
- *RDS Database Master Username*
- *RDS Public Snapshots*
- *RDS Sufficient Backup Retention Period*
- *Enable RDS Transport Encryption*
- *Underutilized RDS Instances*
- *Unrestricted RDS DB Security Group*
- *Enable Route 53 Domain Auto Renew*
- *Create DNS Alias Record for Root Domain*
- *Remove Route 53 Dangling DNS Records*
- *Expired Route 53 Domain Names*
- *Route 53 Domain Name Renewal*
- *Enable Privacy Protection for Route 53 Domains*
- *Root Domain Alias Records that Point to ELB*
- *Monitor Route 53 Configuration Changes*
- *Route 53 DNS In Use*
- *Route 53 SPF DNS Records*
- *Enable Route 53 Domain Transfer Lock*
- *Monitor Route 53 Domains Configuration Changes*

1.23.1 Aurora Database Instance Accessibility

Risk: Medium
Description: Ensure that all the database instances in your Aurora clusters have the same accessibility (either public or private) in order to follow AWS best-practices.
Resolution: To ensure that the database instances in your Aurora clusters have the same accessibility (either public or private).

1.23.2 RDS Auto Minor Version Upgrade

Risk: Medium
Description: Ensure that RDS database instances have the Auto Minor Version Upgrade flag enabled in order to receive automatically minor engine upgrades during the specified maintenance window. Each version upgrade is available only after is tested and approved by AWS. **Resolution**: Update RDS instances configuration and enable Auto Minor Version Upgrade.

1.23.3 Enable RDS Automated Backups

Risk: High
Description: Ensure that RDS database instances have automated backups enabled for point-in-time recovery. To back up your database instances, RDS take automatically a full daily snapshot of your data (with transactions logs) during the specified backup window and keeps the backups for a limited period of time (known as retention period) defined by the instance owner. **Resolution**: Update RDS instances configuration and enable automated backups.

1.23.4 Enable RDS Deletion Protection

Risk: Medium
Description: Ensure that Relational Database Service (RDS) instances have Deletion Protection feature enabled in order to protect them from being accidentally deleted. Deletion protection is supported by all RDS engines as well as the Aurora MySQL and Aurora PostgreSQL database engines. **Resolution**: Enable Deletion Protection feature for your existing RDS database instances

1.23.5 Enable RDS Encryption

Risk: High
Description: Ensure that RDS database instances are encrypted to fulfill compliance requirements for data-at-rest encryption. The RDS data encryption and decryption is handled transparently and doesn't require any additional action from you or your application. **Resolution**: Enable data encryption for your existing RDS instances you need to re-create (back-up and restore) them with encryption flag enabled.

1.23.6 RDS Free Storage Space

Risk: High
Description: Identify any RDS database instances that appear to run low on disk space and scale them up to alleviate any problems triggered by insufficient disk space and improve their I/O performance.
Resolution: To scale up (expand) the storage space for any RDS database instances that run low on disk space

1.23.7 Enable IAM Database Authentication

Risk: Medium
Description: Ensure IAM Database Authentication feature is enabled in order to use IAM service to manage database access to your RDS MySQL and PostgreSQL instances. With this feature enabled, you don't have to use a password when you connect to your MySQL/PostgreSQL database instances, instead you use an authentication token. **Resolution**: Enable IAM Database Authentication feature for your existing RDS database instances in order to manage your MySQL/PostgreSQL database user credentials through IAM users and roles

1.23.8 Total Number of Provisioned RDS Instances

Risk: Medium
Description: Ensure that the number of RDS database instances provisioned in your AWS account has not reached the limit quota established by your organization for the RDS workload deployed.

Resolution: To build an AWS support case in order to limit the number of provisioned RDS database instances based on your requirements

1.23.9 RDS Multi-AZ

Risk: Medium

Description: Ensure that RDS clusters are using Multi-AZ deployment configurations for high availability and automatic failover support fully managed by AWS.

Resolution: Update RDS clusters configuration and enable Multi-AZ deployment.

1.23.10 Overutilized RDS Instances

Risk: High

Description: Identify any RDS database instances that appear to be overutilized and upgrade (upsize) them to help handle better the database workload and improve the response time.

Resolution: Upgrade (resize) the overused RDS database instances provisioned in your AWS account. To resize an overutilized RDS instance.

1.23.11 Publicly Accessible RDS Instances

Risk: High

Description: Check for any public facing RDS database instances provisioned in your AWS account and restrict unauthorized access in order to minimise security risks. To restrict access to any publicly accessible RDS database instance, you must disable the database Publicly Accessible flag and update the VPC security group associated with the instance. **Resolution**: Update RDS instances connection configuration in order to restrict access.

1.23.12 Use Data-Tier Security Group for RDS Databases

Risk: Medium

Description: Ensure that RDS instances are using the dedicated data-tier security group in order to control and secure the access to their databases.

Resolution: To reconfigure your RDS database instances in order to use the data-tier security group

1.23.13 RDS Database Default Port

Risk: Low

Description: Ensure that RDS databases instances aren't using their default endpoint ports (i.e. MySQL/Aurora port 3306, SQL Server port 1433, PostgreSQL port 5432, etc) in order to promote port obfuscation as an additional layer of defense against non-targeted attacks. **Resolution**: To change the default port number for your existing RDS database instances.

1.23.14 Use KMS Customer Master Keys for RDS encryption

Risk: High

Description: Ensure that RDS database instances are using KMS CMK customer-managed keys rather than AWS managed-keys (default keys used by RDS when there are no customer keys available), in order to have more granular control over your data-at-rest encryption/decryption process. **Resolution**: Since RDS encryption is an immutable setting that must be turned on at the creation time, to migrate a database from unencrypted to encrypted, the database must be backed up and restored onto a new one with the encryption flag enabled.

1.23.15 RDS General Purpose SSD Storage Type

Risk: Recommendation

Description: Ensure that RDS instances are using General Purpose SSDs instead of Provisioned IOPS SSDs for cost-effective storage that fits a broad range of database workloads. Unless you are running mission-critical applications that require more than 10000 IOPS or 160 MiB/s of throughput per database, we recommende converting your Provisioned IOPS RDS instances to General Purpose instances in order to lower the cost of your monthly AWS bill while keeping the same I/O performance. **Resolution**: To convert your Provisioned IOPS SSD based RDS instances to General Purpose SSD based instances, you need to modify your instances storage type configuration.

1.23.16 RDS Instance Not In Public Subnet

Risk: High

Description: Ensure that no RDS database instances are provisioned inside VPC public subnets in order to protect them from direct exposure to the Internet. Since database instances aren't Internet-facing and their management (running software updates, implementing security patches, etc) is done by Amazon, these instances should run only in private subnets. **Resolution**: To move your RDS database instances from public subnets to private subnets, you must replace their current subnet groups with the ones that contain VPC private subnets.

1.23.17 RDS Database Master Username

Risk: Medium

Description: Ensure that RDS production databases aren't using 'awsuser' as master username, regardless of the RDS database engine type used, instead a unique alphanumeric string must be defined as the login ID for the master user.

Resolution: Change the master username for your RDS database instances you need to re-create them and migrate the existing data to the new instances.

1.23.18 RDS Public Snapshots

Risk: High

Description: Ensure that Relational Database Service (RDS) database snapshots aren't publicly accessible (i.e. shared with all AWS accounts and users) in order to avoid exposing your private data.

Resolution: Restrict completely the public access to your RDS database snapshots and make them private

1.23.19 RDS Sufficient Backup Retention Period

Risk: Medium

Description: Ensure that RDS database instances have set a minimum backup retention period in order to achieve the compliance requirements. Recommended a minimum (default) retention period of 7 (seven) days but you can adjust

the minimumRetentionPeriod parameter value to narrow or extend the default retention period. **Resolution**: Update RDS instances automated backups configuration and extend the retention period.

1.23.20 Enable RDS Transport Encryption

Risk: High

Description: Ensure that Microsoft SQL Server instances provisioned with RDS have Transport Encryption feature enabled in order to meet security and compliance requirements.

Resolution: To enable the Transport Encryption feature for your Microsoft SQL Server database instances, you need to update the necessary RDS parameter group and change the rds.force_ssl parameter value to 1.

1.23.21 Underutilized RDS Instances

Risk: Recommendation

Description: Identify any RDS database instances that appear to be underutilized and downsize (resize) them to help lower the cost of your monthly AWS bill.

Resolution: Downsize (resize) the underused RDS instances provisioned in your AWS account.

1.23.22 Unrestricted RDS DB Security Group

Risk: Medium

Description: Ensure that RDS DB security groups do not allow access from 0.0.0.0/0 (i.e. anywhere, every machine that has the ability to establish a connection) in order to reduce the risk of unauthorized access.

Resolution: Update RDS DB security groups configuration in order to restrict access.

Route53

1.23.23 Enable Route 53 Domain Auto Renew

Risk: High

Description: Ensure that Route 53 Auto Renew feature is enabled to automatically renew your domain names as the expiration date approaches. The automatic renewal registration fee will be charged to your AWS account and you will get an email with the renewal confirmation once the registration is processed. **Resolution**: Update Route 53 domains configuration and enable the Auto Renew feature.

1.23.24 Create DNS Alias Record for Root Domain

Risk: Medium

Description: Ensure that a DNS alias record for the root domain name is created in your Route 53 hosted zone.

Resolution: Create and configure a Route 53 DNS alias record for your root domain name.

1.23.25 Remove Route 53 Dangling DNS Records

Risk: Medium

Description: Ensure that any dangling DNS records are deleted from your Route 53 public hosted zones in order to maintain the integrity and authenticity of your domains/subdomains and to protect against domain hijacking attacks.

Resolution: To adhere to DNS security best-practices and remove any dangling DNS records available in your Route 53 hosted zones.

1.23.26 Expired Route 53 Domain Names

Risk: High
Description: Identify and restore any expired domain names registered with Route 53. The restoration fee will be charged to your AWS account and you will get a confirmation email once the registration process is completed.
Resolution: To restore any expired domain names registered with Route 53.

1.23.27 Route 53 Domain Name Renewal

Risk: High
Description: Ensure that all the domain names registered with Route 53 or transferred to Route 53 are renewed X days before their validity period ends.
Resolution: Route 53 doesn't provide a manual method to renew domain names that are about to expire, therefore to make sure your domains aren't suspended once their expiration date is reached, you must enable Route 53 automatic renewal. To Update Route 53 domain names configuration and enable automatic renewal.

1.23.28 Enable Privacy Protection for Route 53 Domains

Risk: Low
Description: Ensure that Route 53 domains have Privacy Protection feature enabled in order to hide all their contact information from WHOIS queries and reduce the amount of spam received. The feature allows you to conceal your personal phone number, email and physical address for the domain names registered and/or transferred to Route 53 service. **Resolution**: Enable Privacy Protection for your Route 53 domains in order to hide all their contact information from WHOIS queries and reduce spam

1.23.29 Root Domain Alias Records that Point to ELB

Risk: Medium
Description: Ensure that the root domain alias record points to the ELB associated with your web-server layer.
Resolution: Update Route 53 domains configuration and enable the Auto Renew feature.

1.23.30 Monitor Route 53 Configuration Changes

Risk: High
Description: Monitor Route 53 configuration changes.

1.23.31 Route 53 DNS In Use

Risk: High
Description: Ensure that Route 53 Domain Name System (DNS) service is used in your AWS account to manage DNS zones for your domains. Route 53 is an authoritative Domain Name System service built on top of AWS highly

available, scalable and reliable infrastructure. **Resolution**: In order to utilize Route 53 as DNS service for your domain names, you must create and configure Route 53 hosted zones.

1.23.32 Route 53 SPF DNS Records

Risk: Medium
Description: Ensure your Route 53 hosted zones have a TXT DNS record that contains a corresponding Sender Policy Framework (SPF) value set for each MX record available. The SPF record enables your Route 53 registered domains to publicly state which mail servers are authorized to send emails on its behalf. **Resolution**: Create SPF record sets for the corresponding MX records in your Route 53 DNS hosted zones.

1.23.33 Enable Route 53 Domain Transfer Lock

Risk: High
Description: Ensure that Route 53 registered domains are locked to prevent any unauthorized transfers to another domain name registrar. Your domains must have the Transfer Lock feature enabled.
Resolution: Update Route 53 domain names configuration and enable transfer locking.
Route53Domains

1.23.34 Monitor Route 53 Domains Configuration Changes

Risk: High
Description: Monitor Route 53 Domains configuration changes.

1.24 ResourceGroup

- *Use tags to organize AWS resources*

1.24.1 Use tags to organize AWS resources

Risk: Low
Description: Ensure that user-defined tags (metadata) are being used for labeling, collecting and organizing resources available in your AWS environment.

1.25 S3

- *S3 Bucket Authenticated 'FULL_CONTROL' Access*
- *S3 Bucket Authenticated 'READ' Access*

- *S3 Bucket Authenticated 'READ_ACP' Access*
- *S3 Bucket Authenticated 'WRITE' Access*
- *S3 Bucket Authenticated 'WRITE_ACP' Access*
- *Enable S3 Bucket Default Encryption*
- *Enable Access Logging for S3 Buckets*
- *Enable MFA Delete for S3 Buckets*
- *S3 Bucket Public Access Via Policy*
- *Publicly Accessible S3 Buckets*
- *S3 Bucket Public 'READ' Access*
- *S3 Bucket Public 'READ_ACP' Access*
- *S3 Bucket Public 'WRITE' Access*
- *S3 Bucket Public 'WRITE_ACP' Access*
- *Enable Versioning for S3 Buckets*
- *Review S3 Buckets with Website Configuration Enabled*
- *Detect S3 Configuration Changes*
- *S3 Unknown Cross Account Access*
- *Secure Transport*
- *Server-Side Encryption*
- *Limit S3 Bucket Access by IP Address*

1.25.1 S3 Bucket Authenticated 'FULL_CONTROL' Access

Risk: Very High
Description: Ensure that S3 buckets aren't granting FULL_CONTROL access to authenticated users (i.e. signed AWS accounts or IAM users) in order to prevent unauthorized access. An S3 bucket that allows full control access to authenticated users will give any AWS account or IAM user the ability to LIST (READ) objects, UPLOAD/DELETE (WRITE) objects, VIEW (READ_ACP) objects permissions and EDIT (WRITE_ACP) permissions for the objects within the bucket. **Resolution**: To remove authenticated FULL_CONTROL access for your S3 buckets.

1.25.2 S3 Bucket Authenticated 'READ' Access

Risk: Very High
Description: Ensure that S3 buckets content cannot be listed by AWS authenticated accounts or IAM users in order to protect your S3 data against unauthorized access. An S3 bucket that allows READ (LIST) access to authenticated users will provide AWS accounts or IAM users the ability to list the objects within the bucket and use the information acquired to find objects with misconfigured ACL permissions and exploit them. **Resolution**: To remove authenticated READ access to your S3 buckets.

1.25.3 S3 Bucket Authenticated 'READ_ACP' Access

Risk: Very High

Description: Ensure that S3 buckets content permissions cannot be viewed by AWS authenticated accounts or IAM users in order to protect against unauthorized access. An S3 bucket that grants READ_ACP (VIEW PERMISSIONS) access to AWS signed users can allow them to examine your S3 Access Control Lists (ACLs) configuration details and find permission vulnerabilities. **Resolution**: To remove authenticated READ_ACP access for your S3 buckets ACL configuration.

1.25.4 S3 Bucket Authenticated 'WRITE' Access

Risk: Very High

Description: Ensure that S3 buckets cannot be accessed for WRITE actions by AWS authenticated accounts or IAM users in order to protect your S3 data from unauthorized access. An S3 bucket that allows WRITE (UPLOAD/DELETE) access to any AWS authenticated users can provide them the capability to add, delete and replace objects within the bucket without restrictions. **Resolution**: To remove authenticated WRITE access for your S3 buckets.

1.25.5 S3 Bucket Authenticated 'WRITE_ACP' Access

Risk: Very High

Description: Ensure that S3 buckets do not allow authenticated AWS accounts or IAM users to modify access control permissions to protect your S3 data from unauthorized access. An S3 bucket that allows WRITE_ACP access to AWS authenticated users can give these the capability to edit permissions and gain full access to the resource. Allowing this type of access is dangerous and can lead to data loss or unexpectedly high S3 charges on your AWS bill as a result of economic denial-of-service attacks. **Resolution**: To remove authenticated WRITE_ACP access for your S3 buckets.

1.25.6 Enable S3 Bucket Default Encryption

Risk: High

Description: Ensure that default encryption is enabled at the bucket level to automatically encrypt all objects when stored in S3. The S3 objects are encrypted during the upload process using Server-Side Encryption with either S3-managed keys (SSE-S3) or KMS-managed keys (SSE-KMS). **Resolution**: Enable default encryption for your existing S3 buckets.

1.25.7 Enable Access Logging for S3 Buckets

Risk: Medium

Description: Ensure that S3 Server Access Logging feature is enabled in order to record access requests useful for security audits. By default, server access logging is not enabled for S3 buckets.

Resolution: To enable Server Access Logging for an S3 bucket, you must be logged in as the bucket owner.

1.25.8 Enable MFA Delete for S3 Buckets

Risk: Low

Description: Ensure your buckets are using MFA Delete feature in order to prevent the deletion of any versioned S3 objects.

Resolution: Enable MFA Delete protection for your S3 buckets via AWS CLI (not supported via AWS Management Console).

1.25.9 S3 Bucket Public Access Via Policy

Risk: Very High
Description: Ensure that S3 buckets aren't publicly accessible via bucket policies in order to protect against unauthorized access.
Resolution: To restrict access to your publicly accessible S3 buckets via bucket policies.

1.25.10 Publicly Accessible S3 Buckets

Risk: Very High
Description: Ensure there aren't any publicly accessible S3 buckets available in your AWS account in order to protect your S3 data from loss and unauthorized access.
Resolution: To remove public (FULL_CONTROL) access for your S3 buckets.

1.25.11 S3 Bucket Public 'READ' Access

Risk: Very High
Description: Ensure that S3 buckets content cannot be publicly listed in order to protect against unauthorized access.
Resolution: To remove public READ access from your S3 buckets.

1.25.12 S3 Bucket Public 'READ_ACP' Access

Risk: Very High
Description: Ensure that S3 buckets content permissions details cannot be viewed by anonymous users in order to protect against unauthorized access.
Resolution: To remove public access to your S3 buckets ACL config information (ACL permissions).

1.25.13 S3 Bucket Public 'WRITE' Access

Risk: Very High
Description: Ensure that S3 buckets cannot be publicly accessed for WRITE actions in order to protect your S3 data from unauthorized users.
Resolution: To remove public WRITE access for your S3 buckets.

1.25.14 S3 Bucket Public 'WRITE_ACP' Access

Risk: Very High
Description: Ensure that S3 buckets do not allow anonymous users to modify their access control permissions to protect your S3 data from unauthorized access.
Resolution: To remove public WRITE_ACP access for your S3 buckets.

1.25.15 Enable Versioning for S3 Buckets

Risk: Low

Description: Ensure that S3 buckets have the versioning flag enabled in order to preserve and recover overwritten and deleted S3 objects as an extra layer of data protection and/or data retention.
Resolution: Enable object versioning for your existing S3 buckets.

1.25.16 Review S3 Buckets with Website Configuration Enabled

Risk: Medium
Description: Ensure that S3 buckets with website configuration enabled are regularly reviewed for security purposes.
Resolution: When you disable S3 website hosting, S3 service removes the website configuration from your buckets so that these buckets are no longer accessible from the website endpoint.

1.25.17 Detect S3 Configuration Changes

Risk: Very High
Description: To detect configuration changes performed at the S3 service and resources level, in your AWS account.

1.25.18 S3 Unknown Cross Account Access

Risk: High
Description: Ensure that all your S3 buckets are configured to allow access only to trusted AWS accounts in order to protect against unauthorized cross account access.
Resolution: Update S3 buckets policy in order to allow cross account access only from trusted entities.

1.25.19 Secure Transport

Risk: Medium
Description: Ensure that S3 buckets enforce encryption of data over the network (as it travels to and from S3) using SSL
Resolution: To enforce SSL-only access to your S3 buckets via access policies

1.25.20 Server-Side Encryption

Risk: Medium
Description: Ensure that S3 buckets are protecting their sensitive data at rest by enforcing Server-Side Encryption
Resolution: Enable Server-Side Encryption for your S3 buckets via access policies.

1.25.21 Limit S3 Bucket Access by IP Address

Risk: Medium
Description: Ensure that S3 buckets are configured using policies to allow access only to specific (trusted) IP addresses in order to protect against unauthorized access
Resolution: Update S3 buckets policy in order to grant access only to specific (trusted) IP addresses.

1.26 SES

- *Enable DKIM for SES*
- *Unknown Cross-Account Access*
- *Exposed SES Identities*
- *SES Identity Verification Status*

1.26.1 Enable DKIM for SES

Risk: Low
Description: Ensure DKIM feature is enabled in your SES settings to protect both email senders and receivers against phishing attacks by using DKIM-signature headers to make sure that each message sent is authentic.
Resolution: Enable DKIM signing for your existing SES registered identities (domains and email addresses).

1.26.2 Unknown Cross-Account Access

Risk: High
Description: Ensure that all your SES identities are configured to allow access only to trusted (friendly) AWS accounts in order to prevent unauthorized users from sending emails on your behalf.
Resolution: Update the sending authorization policies associated with your SES identities in order to allow sender requests only from trusted AWS entities (delegate senders)

1.26.3 Exposed SES Identities

Risk: High
Description: Identify any exposed SES identities and update their sending authorization policy in order to stop unauthorized users from sending emails from domains or addresses owned by your SES account.
Resolution: Update the sending authorization policies associated with your SES identities in order to allow sender requests only from trusted AWS entities (delegate senders)

1.26.4 SES Identity Verification Status

Risk: Low
Description: Ensure SES identities are verified in order to prove their ownership and to prevent others from using them. Before you can use SES to send emails, you must verify each email address (or the email address domain) that you will use as a "From", "Source", "Sender" or "Return-Path" address, to confirm that you own it. **Resolution**: To verify any SES identities in order to prove their ownership.

1.27 Shield

- *AWS Shield In Use*

1.27.1 AWS Shield In Use

Risk: Medium
Description: Ensure that Shield service is currently in use in order to protect your AWS-powered web applications from Distributed Denial of Service (DDoS) attacks that can affect the application's availability and response time by overwhelming (flooding) them with traffic from multiple sources. **Resolution**: - To enable AWS Shield Advanced tier for your AWS account

---

1.28 TrustedAdvisor

- *Trusted Advisor Checks*
- *Exposed IAM Access Keys*

1.28.1 Trusted Advisor Checks

Risk: Medium
Description: Ensure that all Trusted Advisor checks found in your AWS account are inspected and resolved.
Resolution: To fix the issue highlighted by the selected Trusted Advisor check (i.e. enable MFAfor the AWS root account)

1.28.2 Exposed IAM Access Keys

Risk: Extreme
Description: Identify and invalidate (disable) any exposed IAM access keys in order to protect your AWS resources against unapproved access.
Resolution: Disable exposed IAM access keys so that these credentials can no longer be used to access to AWS.

1.29 VPC

- *Allocate Elastic IPs for NAT Gateways*
- *Create App-Tier VPC Subnets*
- *Create Data-Tier VPC Subnets*
- *Default VPC In Use*
- *Unused VPC Internet Gateways*
- *Use Managed NAT Gateway for VPC*
- *Create NAT Gateways in at Least Two Availability Zones*
- *Ineffective Network ACL DENY Rules*

- *Unrestricted Network ACL Inbound Traffic*
- *Unrestricted Network ACL Outbound Traffic*
- *Create Route Table for Private Subnets*
- *Create Route Table for Public Subnets*
- *Enable Flow Logs for VPC Subnets*
- *VPC Endpoint Unknown Cross Account Access*
- *VPC Exposed Endpoints*
- *VPC Endpoints In Use*
- *Enable VPC Flow Logs*
- *VPC Naming Conventions*
- *VPC Peering Connection Configuration*
- *Unused Virtual Private Gateways*
- *Create Web-Tier ELB Subnets*
- *Create Web-Tier VPC Subnets*

1.29.1 Allocate Elastic IPs for NAT Gateways

Risk: Medium
Description: Ensure that an Elastic IP is allocated for each NAT gateway that you want to deploy in your AWS account.
Resolution: To allocate an Elastic IP for each NAT gateway that you want to deploy in your VPC

1.29.2 Create App-Tier VPC Subnets

Risk: Medium
Description: Ensure that at least two subnets in two different Availability Zones are created for your app tier. Each app-tier subnet must reside entirely within one Availability Zone and cannot span multiple zones.
Resolution: Create VPC subnets for your web tier (at least two subnets in different Availability Zones)

1.29.3 Create Data-Tier VPC Subnets

Risk: Medium
Description: Ensure that at least two subnets in two different Availability Zones are created for your data tier. Each data-tier subnet must be located entirely in one Availability Zone and cannot span multiple zones.
Resolution: Create VPC subnets for your data tier (at least two subnets in different Availability Zones)

1.29.4 Default VPC In Use

Risk: Medium
Description: Ensure that AWS application is not deployed within the default VPC in order to follow security best-practices.
Resolution: Create a non-default VPC and migrate your custom AWS applications to it

1.29.5 Unused VPC Internet Gateways

Risk: Low
Description: Identify and remove any unused VPC Internet Gateways (IGWs) and VPC Egress-Only Internet Gateways (EIGWs) in order to adhere to best-practices and to avoid approaching the service limit (by default, you are limited to 5 IGWs and 5 EIGWs per AWS region). **Resolution**: To remove any unused IGWs and EIGWs available in your VPC

1.29.6 Use Managed NAT Gateway for VPC

Risk: Medium
Description: Ensure that VPC network(s) use the highly available Managed NAT Gateway service instead of an NAT instance in order to enable EC2 instances sitting in a private subnet to connect to the internet or with other AWS components. **Resolution**: Enable the Managed NAT Gateway service for your VPC network(s).

1.29.7 Create NAT Gateways in at Least Two Availability Zones

Risk: Medium
Description: Ensure that NAT gateways are deployed in at least two Availability Zones in order to enable EC2 instances available within private subnets to connect to the Internet or to other AWS services but prevent the Internet from initiating a connection with those instances. **Resolution**: To deploy your NAT gateways in at least two Availability Zones

1.29.8 Ineffective Network ACL DENY Rules

Risk: High
Description: Ensure that NACLs do not have ineffective or misconfigured DENY rules that promotes overly-permissive access to your VPC.
Resolution: To reconfigure any ineffective NACL DENY rules in order to block the traffic to the necessary port.

1.29.9 Unrestricted Network ACL Inbound Traffic

Risk: Medium
Description: Check NACLs for inbound rules that allow traffic from all ports and limit access to the required ports or port ranges only.
Resolution: Update NACL inbound rules configuration in order to allow traffic from specific source port or source port range only.

1.29.10 Unrestricted Network ACL Outbound Traffic

Risk: Medium
Description: Check NACLs for outbound rules that allow traffic from all ports and limit access to the required ports or port ranges only.
Resolution: Update NACL outbound rules configuration in order to allow traffic to specific destination port or port range only.

1.29.11 Create Route Table for Private Subnets

Risk: Medium
Description: Ensure that a custom route table is created and associated with your private subnets.
Resolution: Create a custom route table and associate it with your web/app/data private subnets.

1.29.12 Create Route Table for Public Subnets

Risk: Medium
Description: Ensure that a custom route table is created and associated with your VPC public subnets.
Resolution: Create a custom route table and associate it with your public subnets

1.29.13 Enable Flow Logs for VPC Subnets

Risk: Low
Description: Ensure that flow logs are enabled for your VPC subnets. Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces associated with your subnets.
Resolution: Enable flow logs for your VPC subnets

1.29.14 VPC Endpoint Unknown Cross Account Access

Risk: Medium
Description: Ensure that all your VPC endpoints are configured to allow access only to trusted AWS accounts in order to protect against unauthorized cross account access
Resolution: Update VPC endpoints policy in order to allow cross account access only from trusted entities.

1.29.15 VPC Exposed Endpoints

Risk: Medium
Description: Identify any fully accessible VPC endpoints and update their access policy in order to stop any unsigned requests made to the supported services and resources.
Resolution: To restrict access to your VPC endpoints.

1.29.16 VPC Endpoints In Use

Risk: Medium
Description: Ensure that VPC endpoints are being used to allow you to securely connect your VPC to other AWS services and VPC endpoint services without the need of an Internet Gateway (IGW), NAT device, VPN connection or an AWS Direct Connect connection. **Resolution**: A VPC endpoint enables you to connect with particular AWS services that are outside your VPC network through a private link. To deploy and configure a VPC endpoint in your AWS account

1.29.17 Enable VPC Flow Logs

Risk: Medium

Description: Once enabled, the Flow Logs feature will start collecting network traffic data to and from your VPC, data that can be useful to detect and troubleshoot security issues and make sure that the network access rules aren't overly permissive. **Resolution**: Enable Flow Logs for your VPC, you need to create first an IAM role that will grant permissions to publish flow log streams to the specified log group in CloudWatch Logs

1.29.18 VPC Naming Conventions

Risk: Low
Description: Ensure that VPCs (VPCs) are using appropriate naming conventions for tagging in order to manage them more efficiently and adhere to AWS resource tagging best-practices.

1.29.19 VPC Peering Connection Configuration

Risk: Medium
Description: Review the routing tables of your peered VPCs to determine if the existing peering connection configuration is compliant with the desired routing policy.
Resolution: Implement the compliant routing policy for the selected VPC peering connection.

1.29.20 Unused Virtual Private Gateways

Risk: Low
Description: Identify and delete any unused VGWs.
Resolution: To remove any unused Virtual Private Gateways provisioned in your AWS account.

1.29.21 Create Web-Tier ELB Subnets

Risk: Medium
Description: Ensure that subnets for the web-tier ELBs are created. Each web-tier ELB subnet must reside entirely in one Availability Zone and cannot span zones.
Resolution: Create web-tier subnets (at least two subnets in different AZs) and associate them with your web-tier ELB

1.29.22 Create Web-Tier VPC Subnets

Risk: Medium
Description: Ensure that at least two subnets in two different Availability Zones are created for your web tier. Each web-tier subnet must reside entirely within one Availability Zone and cannot span zones.
Resolution: Create VPC subnets for your web tier (at least two subnets in different Availability Zones)

1.30 WAF

- *AWS Web Application Firewall In Use*

1.30.1 AWS Web Application Firewall In Use

Risk: Medium

Description: Ensure that WAF service is currently in use.

Resolution: In order to enable WAF as the web firewall service to protect your AWS-powered web applications from security exploits, you must create one or more web ACLs, each ACL containing rules and actions to perform when a rule is satisfied.

CHAPTER 2

Indices and tables

- genindex
- modindex
- search