Cloudwize compliance report

Thu Aug 05 2021 10:34:52 GMT+0000 (Coordinated Universal Time)

Cloud Accounts:

title	amount
total	382
passed	347
failed	35

Package name	Percentage
APRA	87%
MAS	87%
GDPR	95%
HIPAA	95%
NIST	89%
PCI DSS	91%
SOC2	75%
CIS	98%
ISO	100%
AWAF	100%

title	description	packages	severity	cloud	active patterns
Detect Underutilized EC2 Instance	To reduce the cost of your monthly AWS bill, detect any Amazon EC2 instances that appear to be underutilized and downsize (resize) them. By default, an EC2 instance is deemed "underutilized" when it matches the following criteria (to declare the instance "underutilized" both conditions must be met):	• APRA • MAS	High	aws	2
Enable Amazon Neptune Database Encryption	To meet regulatory requirements and prevent unauthorized users from accessing sensitive information, make sure to encrypt the data available on your Amazon Neptune database instances. Encrypting the data gives an additional layer of protection by securing your Neptune databases from unauthorized access to the underlying storage. Neptune is a fast, scalable, highly secure and fully-managed graph database service that facilitates building and running applications that work with deeply connected datasets.	• APRA • GDPR • HIPAA • MAS • NIST • PCI DSS	High	aws	2
Non-encrypted RDS Storage	To comply with compliance requirements for data-at-rest encryption, make sure your RDS database instances are encrypted . The RDS data encryption and decryption is managed transparently and does not require any additional action from you or your application.	• APRA • GDPR • HIPAA • MAS • NIST • PCI DSS • SOC2	High	aws	2
AWS RDS is Accessible to Public	To minimize security risks, detect any public facing RDS database instances provisioned in your AWS account and restrict unauthorized access. To restrict access to any RDS database instance acessible to the public, you must disable the database Publicly Accessible flag and update the VPC security group associated with the instance.	• APRA • GDPR • HIPAA • MAS • NIST • PCI DSS	High	aws	2
Idle EC2 Instance	Detect any Amazon EC2 instances that seem to be idle and stop or terminate them to help reduce the cost of your monthly AWS bill. By default, an EC2 instance is considered 'idle' when it meets the following criteria (to declare the instance 'idle' both conditions must be true): The total number of VolumeReadOps and VolumeWriteOps recorded per day for the last 7 days has been less than 1 (one) on average. This rule can help you work with the AWS Well-Architected Framework	• APRA • MAS	High	aws	1

title	description	packages	severity	cloud	active patterns
Full Administrative Privileges for IAM Policies	To advance 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, make sure there are no Amazon IAM policies (customer managed) that allow full administrative privileges in your AWS account. An IAM policy that allows full administrative permissions (such as access to all AWS actions and resources) is a policy that contains a statement with "Effect": "Allow" for "Action": "*" over "Resource": "*", i.e. "Statement": [{ "Effect": "Allow", "Action": "*", "Resource": "*" }].	• APRA • CIS • MAS • NIST	High	aws	1
Ensure RDS Automated Backups is Enabled	Make sure your RDS database instances have automated backups enabled for point-in-time recovery. To back up your database instances, AWS RDS automatically take a full daily snapshot of your data (with transactions logs) during the specified backup window and maintains the backups for a limited period of time (known as retention period) defined by the instance owner.	• NIST	High	aws	1
Detect Unrestricted Outbound Access on All Ports	To implement the principle of least privilege and reduce the possibility of a breach, check your EC2 security groups for outbound rules allowing unrestricted access (i.e. 0.0.0.0/0 or ::/0) to any TCP/UDP ports and restrict access to only those IP addresses that require it.	• APRA • HIPAA • MAS • NIST • PCI DSS	Medium	aws	18
Utilized KMS Customer Master Key (CMK)	Make sure you have KMS CMK customer-managed keys in use in your account instead of AWS managed-keys so that you 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.	• APRA • MAS • NIST	Medium	aws	16
Network ACL Outbound Traffic is unrestricted	Examine your AWS Network Access Control Lists (NACLs) for outbound rules that permit traffic from all ports and limit access to the required ports or port ranges. This is solely in order to implement the principle of least privilege and reduce the possibility of unauthorized access at the subnet level.	• APRA • MAS • NIST • PCI DSS	Medium	aws	16
Managed NAT Gateway is In Use	Make sure your AWS VPC network(s) use the highly available Managed NAT Gateway service, rather than an NAT instance, to enable EC2 instances sitting in a private subnet to connect to the internet, or with other AWS components.	• APRA • MAS • NIST	Medium	aws	16
Network ACL Inbound Traffic is unrestricted	Examine your AWS Network Access Control Lists (NACLs) for inbound rules that permit traffic from all ports and limit access to the required ports or port ranges. This is solely in order to implement the principle of least privilege and reduce the possibility of unauthorized access at the subnet level.	• APRA • MAS • NIST • PCI DSS	Medium	aws	16

title	description	packages	severity	cloud	active patterns
Ensure RDS Snapshot Encryption is Enabled	To achieve compliance for data-at-rest encryption within your organization, make sure to encrypt your Amazon Relational Database Service (RDS) snapshots. The RDS snapshot encryption and decryption process is managed transparently and does not need any additional action from you or your application. The keys used for AWS RDS database snapshot encryption can be entirely handled and protected by the Amazon Web Services key management infrastructure or fully managed by the AWS customer through Customer Master Keys (CMKs).	• APRA • MAS • SOC2	Medium	aws	3
Ensure RDS Instance Deletion Protection is Enabled	To protect them from being accidentally deleted, make sure to enable the Deletion Protection feature for your Amazon Relational Database Service (RDS) instances.	• NIST	Medium	aws	2
AWS CloudFormation Stack Termination Protection Should Be Enabled	Amazon CloudFormation should have the Termination Protection feature enabled to protect them from being accidentally deleted. The safety feature can be enabled when you create the CloudFormation stack or existing stacks using the AWS API (UpdateTerminationProtection command). Once allowed, any attempt to delete an AWS CloudFormation stack with the feature enabled, the deletion fails.	• APRA • MAS	Medium	aws	2
Uisng AWS Default Security Groups	To enforce using custom and unique security groups that implement the principle of least privilege, ensure that the EC2 instances provisioned in your AWS account are not connected to default security groups created alongside your VPCs.	• APRA • MAS • NIST	Medium	aws	2
AWS CloudFormation Stack Policy	Make sure that your AWS CloudFormation stacks are configured to use policies as a in order to prevent accidental updates to stack resources.	• APRA • MAS • NIST	Medium	aws	2
AWS CloudFormation Stack configured to use SNS notifications	Make sure that all your AWS CloudFormation stacks are configured to use using Simple Notification Service to receive notifications when an event occurs.	• APRA • MAS • NIST	Medium	aws	2

title	description	packages	severity	cloud	active patterns
Disabled AWS IAM Db Authentication for RDS (MySql/Postgres databases)	Make sure to enable the IAM Database Authentication feature in order to use AWS Identity and Access Management (IAM) service to handle database access to your Amazon RDS MySQL and PostgreSQL instances. After enabling this feature, you do not have to enter a password when you connect to your MySQL/PostgreSQL database instances, and you enter an authentication token instead. An authentication token is a unique string of characters with a lifetime of 15 minutes that AWS RDS generates on your request. IAM Database Authentication removes the need of storing user credentials within the database configuration, because authentication is handled externally using AWS IAM.	• APRA • MAS • NIST	Medium	aws	2
RDS Minimum Backup Retention Period	To comply with the compliance requirements, make sure your RDS database instances have set a minimum backup retention period.	• NIST	Medium	aws	2
IAM Role Access Policy	Make sure the access policies connected to your IAM roles comply with the principle of least privilege by giving the roles the minimal set of actions required to perform their tasks successfully.	• APRA • MAS • NIST	Medium	aws	1
AWS CloudFront (CDN) Service Should be Considered on your Cloud Environments	Make Sure that AWS CloudFront Content Delivery Network (CDN) service is used within your AWS account to accelerate and secure the delivery of your websites. read more about the service on https://aws.amazon.com/cloudfront/	• HIPAA • NIST	Medium	aws	1
Detect Unrestricted SSH Access (ipv4)	To implement the principle of least privilege and reduce the possibility of a breach, check your EC2 security groups for inbound rules that allow unrestricted access (i.e. 0.0.0.0/0 or ::/0) to TCP port 22 nad restrict access to only those IP addresses that require it. TCP port 22 is used for secure remote login by connecting an SSH client application with an SSH server: https://en.wikipedia.org/wiki/Secure_Shell	• APRA • CIS • MAS • NIST • PCI DSS	Medium	aws	1
Detect Unrestricted HTTP Access	To implement the principle of least privilege and reduce the possibility of a breach, check your EC2 security groups for inbound rules allowing unrestricted access (i.e. 0.0.0.0/0) to TCP port 80 and restrict access to only those IP addresses that require it. TCP port 80 is used by HTTP.	• APRA • MAS • NIST • PCI DSS	Medium	aws	1

title	description	packages	severity	cloud	active patterns
Lambda Runtime Environment Latest Version	Make sure you always utilize the latest version of the execution environment for your Amazon Lambda functions in order to comply with AWS best practices and get the newest software features, and receive the latest security patches and bug fixes, and benefit from better performance and reliability. An AWS Lambda runtime (execution) environment is a container build based on the configuration settings you gave when you made your Lambda function. Amazon Lambda serverless architecture supports several runtime environments such as Node.js, Edge Node.js, Java, Python and .NET Core (C#) which you can utilize when performing your functions.	• APRA • MAS • NIST • PCI DSS	Medium	aws	1
Enable Lambda Tracing Feature	To gain visibility into the functions execution and performance, make sure to enable tracing for your AWS Lambda functions. When enabling the tracing feature, Amazon activates Lambda support for AWS X-Ray, a service that collects data about requests that your functions perform, and also gives tools you can use to view, filter and gather insights into the collected data to detect issues and opportunities for optimization.	• NIST	Medium	aws	1
Ensure AWS Lambda functions have access to VPC networks	Make sure your Amazon Lambda functions have access to VPC-only resources, such as AWS Redshift data warehouses, AWS ElastiCache clusters, AWS RDS database instances, and service endpoints that can be acessed only from within a particular Virtual Private Cloud (VPC).	• APRA • MAS • PCI DSS	Medium	aws	1
Route 53 iin Use	Make sure to use AWS Route 53 Domain Name System (DNS) service within your AWS account to manage DNS zones for your domains. AWS Route 53 is an authoritative Domain Name System service that is highly available, scalable and reliable infrastructure built on top of AWS.	• NIST	Medium	aws	1

title	description	packages	severity	cloud	active patterns
AWS Web Application Firewall is In Use	Make sure Amazon Web Application Firewall (WAF) service is currently in use. Its goal is to protect your AWS-powered web applications from security exploits that could affect their availability and overall security, or consume excessive resources (resource starvation attacks). Amazon WAF is a web application firewall service that lets you monitor any HTTP(S) requests that are forwarded to AWS CloudFront or AWS ELB. To enable AWS WAF protection, simply create web Access Control Lists (ACLs), define the ACLs rules, which reference one or more conditions, and the actions to take when each rule is followed. The newly created WAF ACLs can then be attached, for example, to the Amazon CloudFront CDN distribution used by your web applications. To get a quick start with AWS WAF, you can also use AWS Pre-configured Protections, an automated solution that consists of a pre-configured AWS WAF template that includes a set of predefined ACL rules, which can be customized to optimize your requirements. These are designed to block common web-based attacks such as bad bots, Cross-Site Scripting, and SQL Injection.	• APRA • MAS • NIST	Medium	aws	1
Naming Conventions for Security Groups	Make sure that all your EC2 security groups are using suitable naming conventions for tagging to manage them more efficiently and adhere to AWS tagging best practices. A naming convention is a defined set of rules useful for selecting the name of an AWS resource.	• APRA • MAS	Low	aws	18
Ensure RDS Log Exports is Enabled	To publish database log events directly to AWS CloudWatch Logs, make sure your Amazon RDS database instances have enabled the Log Exports feature. By publishing database logs to Amazon CloudWatch, you can create better and more seamless interactions with your database instance logs using AWS services.	• APRA • MAS	Low	aws	2
Ensure RDS Copy Tags to Snapshots is Enabled	To allow tags set on your database instances to be copied automatically to any automated or manual RDS snapshots created from these instances, make sure your Amazon Relational Database (RDS) instances use the Copy Tags to Snapshots feature. After enabling the feature, tags can be copied to all future copies of an AWS RDS snapshot, including cross-region snapshots.	• APRA • MAS	Low	aws	2
Identify EC2 instances older than 180 days	To ensure reliability, identify and re-launch any running AWS EC2 instances that are older than 180 days. An EC2 instance should not run indefinitely in the cloud; having old instances within your AWS account increases the risk of potential issues.	• APRA • MAS	Low	aws	2

title	description	packages	severity	cloud	active patterns
AWS RDS Default Port is being utilized	To promote port obfuscation as an additional layer of defense against non-targeted attacks, make sure your Amazon RDS databases instances are not using their default endpoint ports (i.e. MySQL/Aurora port 3306, SQL Server port 1433, PostgreSQL port 5432, etc).	• APRA • NIST • PCI DSS	Low	aws	2
Enable RDS Event Notifications	Make sure your AWS RDS resources have enabled the event notifications in order to be informed when an event occurs for a given database instance, database snapshot, database security group or database parameter group. The RDS service groups these events into categories that you can subscribe to allowing you to be notified via AWS SNS when an event in that category occurs. For example, if you subscribe to the Backup category for a given RDS database instance, you will be notified whenever a backup-related event occurs for the specified database instance.	• NIST	Low	aws	2