

Project Design

A Resilient and Auditable Cloud Security Framework for Financial Services

Contents

Executive Summary	1
1 Introduction.....	2
2 Overall Design Framework.....	3
2.1 Objectives and Purpose.....	3
2.2 Requirements Specification	3
2.3 Integrated Design	4
2.4 Cloud Security Lifecycle Mapping	4
2.5 Compliance and Continuous Assurance.....	5
3 Identity and Access Management (IAM + Security Hub)	6
3.1 Security	6
3.2 IAM identity and access management	12
4 Network and Perimeter Protection (VPC + WAF/Shield)	19
4.1 Objectives and Scope	19
4.2 Design and Configuration	19
4.3 Procedural Steps.....	20
4.4 Validation and Evidence	21
4.5 Implementation Plan and Risks	22
5 Storage and Data Protection (RDS, S3, DynamoDB, Glacier).....	24
5.1 Amazon S3 for Logs and Audit Data	24
5.2 Amazon RDS for Transaction Data.....	27
5.3 Amazon DynamoDB for High-Concurrency Events	31
5.4 Amazon S3 Glacier for Long-Term Archives	33
6.6 Compliance and Verification.....	34
6 Conclusion	36
Reference	37

Executive Summary

This report outlines a secure AWS architecture for financial services migrating from a data center. The goal is to ensure Confidentiality, Integrity, and Availability (CIA) while meeting PCI DSS, GDPR, and APRA CPS 234.

The design integrates three areas—Identity and Access Management, Network and Perimeter Protection, and Storage and Data Protection—each led by a stakeholder. Key measures include MFA, VPC segmentation, and encrypted multi-AZ storage. Mapped across the Cloud Security Lifecycle, they deliver compliance, monitoring, and recovery within a sustainable framework.

1 Introduction

The financial services industry is highly regulated and relies on secure handling of customer data. Migrating to AWS offers scalability but creates security and compliance challenges. Data leakage or downtime can cause serious damage.

This project designs a cloud architecture ensuring Confidentiality, Integrity, and Availability (CIA) while meeting PCI DSS (PCI Security Standards Council, 2024), GDPR (European Union, 2016), and APRA CPS 234 (APRA, 2019). It also follows AWS Well-Architected best practices (Amazon Web Services, 2024). The design covers three areas: Identity and Access Management, Network and Perimeter Protection, and Storage and Data Protection, forming a lifecycle-based framework across creation, use, storage, and disposal.

2 Overall Design Framework

2.1 Objectives and Purpose

The design secures financial workloads in AWS by ensuring CIA and meeting PCI DSS, GDPR, and APRA CPS 234. It follows AWS security guidelines and focuses on three areas, each led by a stakeholder (Table 1).

Table 1. Objectives and Stakeholder Responsibilities

Core Area	Purpose	Stakeholder
Identity and Access Management (IAM + Security Hub)	Centralized authentication, least-privilege enforcement, MFA, and security monitoring	Security Administrator
Network and Perimeter Protection (VPC + WAF/Shield)	Multi-AZ segmentation, limited exposure, and layered defense against external threats	Operations Engineer
Storage and Data Protection (RDS, S3, DynamoDB, Glacier)	Encryption, backup, recovery, and compliant data retention	Compliance Officer

2.2 Requirements Specification

To ensure the architecture is comprehensive and compliant, requirements follow cloud security best practices and financial regulations. Table 2 summarizes them with stakeholder responsibilities.

Table 2. Requirements Specification for Financial Cloud Security

Category	Key Requirement	Stakeholder Focus
Functional	IAM with MFA and centralized authentication	Security Administrator
	Continuous monitoring with CloudTrail/GuardDuty	Security Administrator

	Encrypted storage in RDS/S3/DynamoDB/Glacier	Compliance Officer
Non-Functional	Multi-AZ high availability and failover	Operations Engineer
	Auto Scaling and DynamoDB adaptive capacity	Operations Engineer
	Log retention ≥ 7 years with KMS encryption	Compliance Officer
Regulatory	PCI DSS – encryption and logging	Compliance Officer
	GDPR – data minimization and lifecycle expiration	Compliance Officer
	APRA CPS 234 – resilience, auditability, DR testing	All stakeholders

2.3 Integrated Design

The architecture integrates three layers: IAM defines access, VPC and perimeter security control traffic, and storage ensures data protection. Together, they form a unified framework that meets compliance and resilience goals (Figure 1).

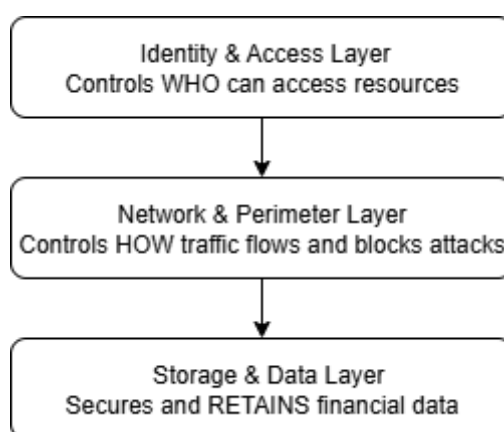


Figure 1. Integrated Security Architecture

2.4 Cloud Security Lifecycle Mapping

To ensure end-to-end protection, the security controls are aligned with the four phases of the Cloud Security Lifecycle. Table 3 summarizes the mapping.

Table 3. Cloud Security Lifecycle and Security Measures

Lifecycle Phase	Key Security Measures
Creation	IAM least-privilege policies, MFA, KMS encryption for new resources
Use	VPC Endpoints for private traffic, Security Groups/NACLs, CloudTrail monitoring, GuardDuty threat detection
Storage	RDS Multi-AZ deployment, S3 Versioning + Object Lock, DynamoDB PITR, KMS-encrypted backups
Disposal	S3 Lifecycle policies, Glacier archival with expiration, secure deletion of old logs and data

2.5 Compliance and Continuous Assurance

The design complies with PCI DSS, GDPR, and APRA CPS 234. Continuous assurance is guided by AWS Well-Architected practices and summarized in Table 4.

Table 4. Continuous Assurance Measures

Measure	Key Controls & Purpose
Automated Monitoring	CloudTrail, GuardDuty, and Security Hub provide real-time alerts and audit evidence
Immutable Logs	S3 Object Lock with KMS encryption ensures tamper-proof records for seven years
Disaster Recovery Drills	Multi-AZ deployment, replication, and failover testing maintain business continuity
Policy Audits	IAM Access Analyzer and AWS Config detect misconfigurations and enforce least privilege

3 Identity and Access Management (IAM + Security Hub) - Security

Administrator

3.1 Security

Objectives and scope:

Take Security Hub as the hub, and integrate Cloud Trail/Cloud Watch/Guard Duty/Detective/Config/Macie/Waf/Shield to form a closed loop of "detection → alarm classification → automatic disposal → evidence collection".

Overall logic:

Organization-level CloudTrail (including data events) centralizes S3(KMS+Object Lock) and connects with Cloud Watch Logs/Metric Filter+Alarms;

GuardDuty hosts threat detection, and Findings enters the Hub/ event bus;

WAF+Shield is blocked at the boundary, and the log is sent to Firehose/S3 for audit;

EventBridge→Lambda/SSM automatic isolation and rollback; Detective traceability afterwards.

3.1.1 AWS CloudTrail

CloudTrail is used to record all management operation events in AWS accounts, and supports operation audit, risk monitoring and compliance requirements.

Steps:

1.New regional Trail→ dedicated S3 log bucket (applicable to all regions, SSE-KMS, and public access).

The screenshot shows the AWS CloudTrail 'Create trail' console. The left sidebar indicates the current step is 'Step 1: Choose trail attributes'. The main content area is titled 'Choose trail attributes' and contains several sections:

- General details:** Includes a 'Trail name' field with the value 'management-event' and a note that it must be 3-128 characters.
- Storage location:** Offers two options: 'Create new S3 bucket' (selected) and 'Use existing S3 bucket'.
- Trail log bucket and folder:** Shows the bucket name 'aws-cloudtrail-logs-851725465134-c6b66584' and the folder path 'aws-logs-851725465134-1/2023/01/10/CloudTrail-851725465134-1'.
- Log file SSE-KMS encryption:** A checkbox labeled 'Enabled' is present.
- Additional settings:** Includes 'Log file validation' (checked 'Enabled') and 'SNS notification delivery' (unchecked 'Enabled').

2. Turn on the log file integrity verification; Turn on the data event (key S3 bucket/function).

The screenshot shows the AWS CloudTrail 'Create trail' console at 'Step 2: Choose log events'. The main content area is titled 'Choose log events' and contains several sections:

- Events:** A section with a note 'Record API activity for individual resources, or for all current and future resources in your AWS account. Additional charges apply.' It includes checkboxes for 'Management events', 'Data events', 'Insights events', and 'Network activity events', all of which are checked.
- Management events:** A section with a note 'Management events show information about management operations performed on resources in your AWS account.' It includes a message: 'No additional charges apply to log management events on this trail because this is your first copy of management events.'
- API activity:** A section with a note 'Choose the activities you want to log.' It includes checkboxes for 'Read' and 'Write', both of which are checked. There are also checkboxes for 'Exclude AWS KMS events' and 'Exclude Amazon RDS Data API events', both of which are unchecked.
- Data events:** A section with a note 'Data events show information about data plane operations performed on resources in your AWS account.'

3. create.

3.1.2 Amazon CloudWatch

Responsible for real-time monitoring and alarm of resources and applications on the cloud, which is used for log analysis, indicator alarm and automatic response in the security architecture.

Steps:

1. Trail settings → CloudWatch log integration → create a new log group, and give CloudTrail the IAM role of writing logs.

This screenshot shows the 'Select trusted entity' step of the AWS IAM 'Create role' wizard. The left sidebar indicates the current step is Step 1. The main content area is titled 'Select trusted entity' and includes an 'info' icon. Under 'Trusted entity type', there are five radio button options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. The 'AWS service' option is highlighted with a blue border. Below this, the 'Use case' section is titled 'Allow an AWS service like EC2, Lambda, or others to perform actions in this account.' It features a dropdown menu for 'Service or use case' with 'EC2' selected. A note says 'Choose a use case for the specified service.' Below this, there are several radio button options for 'Use case': 'EC2' (selected), 'EC2 Role for AWS Systems Manager', 'EC2 Spot Fleet Role', 'EC2 - Spot Fleet Auto Scaling', and 'EC2 - Spot Fleet Tagging'. Each option has a brief description of its function.

This screenshot shows the 'Add permissions' step of the AWS IAM 'Create role' wizard. The left sidebar indicates the current step is Step 2. The main content area is titled 'Add permissions' and includes an 'info' icon. It shows 'Permissions policies (1076)' and a search bar with 'CloudWatchAgentServerPolicy' entered, resulting in '1 match'. A table lists the policy with columns for 'Policy name', 'Type', and 'Description'. The 'CloudWatchAgentServerPolicy' is listed as 'AWS managed' with the description 'Permissions required to use AmazonCloudWatch'. Below the table, there is a link to 'Set permissions boundary - optional'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

This screenshot shows the 'Name, review, and create' step of the AWS IAM 'Create role' wizard. The left sidebar indicates the current step is Step 3. The main content area is titled 'Name, review, and create' and includes an 'info' icon. Under 'Role details', there is a 'Role name' field with 'A' entered and a 'Description' field with 'Allows EC2 instances to call AWS services on your behalf.' Below this, the 'Trust policy' section is titled 'Step 1: Select trusted entities' and shows a JSON snippet for the trust policy. The JSON defines a role that can assume the role of 'ec2.amazonaws.com'.

2. In the CloudWatch Alarms console, customize indicators to create alarms and set thresholds.

The screenshot displays the AWS CloudWatch console interface. The top navigation bar shows the AWS logo, a search bar, and the user's account information (United States (N. Virginia), Account ID: 81374254955, voclabs/user4273446-Hao-W). The main content area is divided into two sections: 'Create metric filter' and 'Create alarm'.

Create metric filter:

- Step 1: Define pattern** (selected)
- Step 2: Assign metric** (active)
- Step 3: Review and create**

Assign metric details:

- Create filter name:** Filter name: . Filter pattern: .
- Metric details:**
 - Metric namespace:** . ☒ Create new.
 - Metric name:** .
 - Metric value:** .

Create alarm:

- Step 1: Specify metric and conditions**
- Step 2: Configure actions** (active)
- Step 3: Add alarm details**
- Step 4: Preview and create**

Configure actions details:

- Notification:**
 - Alarm state trigger:** ☒ In alarm (The metric or expression is outside of the defined threshold.). ☐ OK (The metric or expression is within the defined threshold.). ☐ Insufficient data (The alarm has just started or not enough data is available.).
 - Send a notification to the following SNS topic:** ☒ Select an existing SNS topic. ☐ Create new topic. ☐ Use topic ARN to notify other accounts.
 - Send a notification to...** .
- Lambda action:**
- Auto Scaling action:**

3. EventBridge subscribes to key events → triggers Lambda isolation/tagging → SNS notification.

The first screenshot shows the 'Build event pattern' step in the AWS EventBridge console. The left sidebar indicates the current step is 'Build event pattern'. The main content area is titled 'Build event pattern' and includes sections for 'Events', 'Event source', and 'Sample event - optional'. The 'Event source' section has three radio buttons: 'AWS events or EventBridge partner events' (selected), 'Other', and 'All events'. The 'Sample event - optional' section has a 'Sample event type' section with three radio buttons: 'AWS events' (selected), 'EventBridge partner events', and 'Enter my own'. Below this is a 'Sample events' section with a search bar containing 'GuardDuty Finding' and a list of sample events. The second screenshot shows the 'Select target(s)' step. The left sidebar indicates the current step is 'Select target(s)'. The main content area is titled 'Select target(s)' and includes a 'Permissions' section, a 'Target 1' section, and a 'Permissions' section. The 'Target 1' section has a 'Target types' section with three radio buttons: 'EventBridge event bus', 'EventBridge API destination', and 'AWS service' (selected). Below this is a 'Select a target' section with a search bar containing 'Lambda function'. The 'Target location' section has two radio buttons: 'Target in this account' (selected) and 'Target in another AWS account'. Below this is a 'Function' section with a search bar containing 'Select or enter a Lambda function ARN'. The 'Permissions' section has two radio buttons: 'Use execution role (recommended)' (selected) and 'Use existing role'. Below this is an 'Execution role' section with two radio buttons: 'Create a new role for this specific resource' (selected) and 'Use existing role'. Below this is a 'Role name' section with a search bar.

4. Create a security dashboard.

3.1.3 Amazon GuardDuty

Hosted threat detection, continuously monitoring malicious or unauthorized behaviors (account abuse, malicious traffic, suspicious DNS) of accounts and workloads, and improving the intrusion detection capability of cloud environment.

Steps:

1. GuardDuty service, which enables GuardDuty in each active area.
2. Update threat intelligence and white list: customize "trusted IP list" and "threat intelligence blacklist" (uploaded in JSON format).

3. Integrate alarm notification: import the GuardDuty discovery event into CloudWatch/EventBridge.

3.1.4 AWS WAF (linked with CloudFront/ALB)

Protect Web applications from common Web attacks, such as SQL injection, XSS cross-site scripts, malicious robot traffic, etc.

Steps:

1. create a Web ACL, and add managed rule groups and custom rules.
2. associate CloudFront or ALB.
3. Enable WAF log to Kinesis Firehose → S3/CloudWatch.

3.1.5 AWS Shield Standard

The basic protection services provided for distributed denial of service (DDoS) attacks are free for all AWS customers by default.

3.1.6 AWS Security service-roles and functions

Table 5. AWS Security service-roles and functions

Services/components	Role (position in security system)	Function
AWS CloudTrail	Audit and evidence base	Record the API/ console events in the account, and send them to S3(KMS encryption and integrity check) in a centralized way, and give an alarm in conjunction with CloudWatch/SNS, so as to meet the requirements of compliance and after-the-fact investigation.
Amazon CloudWatch	Monitoring and alarm center	Aggregate logs/indicators; Metric Filter+Alarm detects anomalies (such as unauthorized call and Root login); EventBridge triggers Lambda/SNS to realize automatic response and work order.

Amazon GuardDuty	Managed threat detection	Continuously detect account and workload anomalies (suspicious API, malicious traffic, etc.) based on CloudTrail/VPC Flow/DNS, and output Findings; ; Automatic isolation and notification of docking EventBridge/Lambda.
AWS WAF	Application layer firewall	Enable hosting+custom rules (SQLi/XSS/Geo/IP/rate limit, etc.) to intercept malicious requests at the edge; Generate detailed access/blocking logs for auditing and tuning.
AWS Shield Standard	DDoS basic protection	Automatically provide network layer and transport layer DDoS mitigation for CloudFront/ALB/Route 53 and other portals, improve usability, and cooperate with WAF to form layered defense.

3.2 IAM identity and access management

Objectives and scope:

Achieve unified identity (SSO), minimum authority (RBAC/ABAC+ authority boundary), strong authentication (MFA), zero trust condition (IP/Region/TLS), certificate governance and evidence traceability.

Overall logic:

Enterprise IdP → IAM Identity Center(SSO) unified into the cloud;

Issue permissions with Permission Sets;

All subjects who can create identities enforce permission boundaries.

3.2.1 IAM users

Represents an entity that needs direct access to AWS resources, and needs to create a unique identity for each administrator and business operator; It is forbidden to use Root every day, and at the same time force MFA to improve login security.

Steps:

1. Create IAM users and customize complex passwords.

The screenshot shows the 'Specify user details' step in the AWS IAM console. The 'User name' field is set to 'user1'. The 'Console password' section has 'Custom password' selected. A password is entered in the field, and a 'Show password' checkbox is visible. A note at the bottom states: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.' The left sidebar shows the progress: Step 1 (Specify user details) is active, followed by Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password).

2. Join the corresponding user groups (such as Admin group, Dev group, ReadOnly group, etc.).

The screenshot shows the 'Set permissions' step in the AWS IAM console. The 'Permissions options' section has 'Add user to group' selected. A note below states: 'Get started with groups: Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.' The left sidebar shows the progress: Step 1 (Specify user details) is completed, Step 2 (Set permissions) is active, Step 3 (Review and create) is next, and Step 4 (Retrieve password) is last. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

3. Enable MFA and select the "Virtual MFA" device.

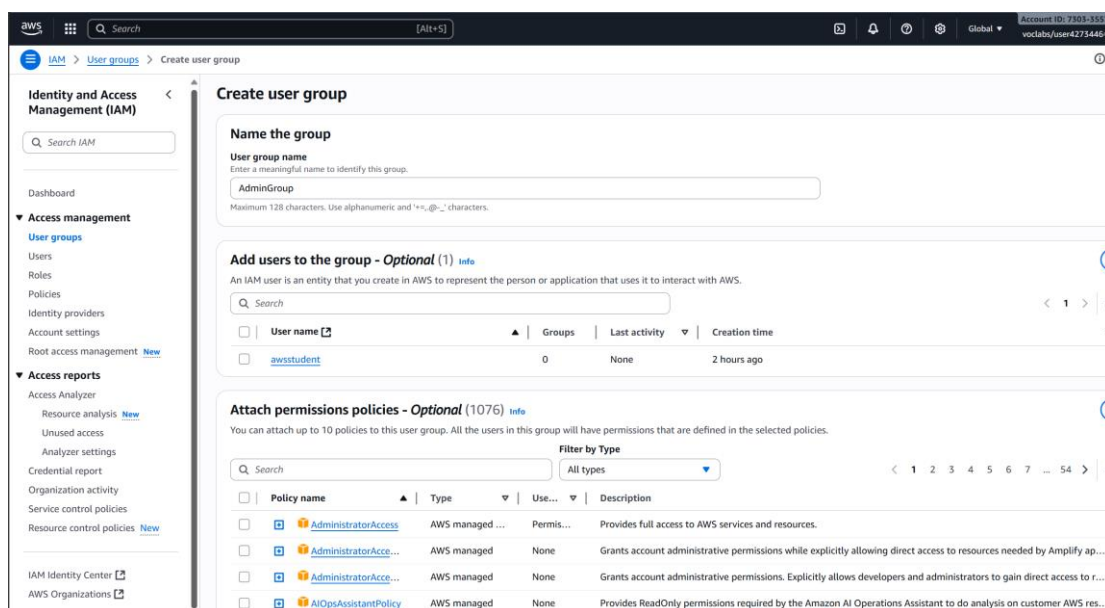
4. Check the user status with Credential Report/CloudTrail.

3.2.2 IAM user group

A collection of multiple IAM users, used to uniformly assign permissions. The goal of designing user groups is to realize role-based access control (RBAC), and to package permissions according to functional roles, so as to grant or reclaim permissions to people in batches, and it is necessary to implement responsibilities and minimum permissions.

Steps:

Define groups such as Admin/Dev/ReadOnly/SecOps, add users to the group, and attach customized fine policies.



3.2.3.IAM role

As an AWS identity, it has a set of permissions and can be temporarily played by the subject. The main goal of designing IAM role is to realize the relationship between temporary credentials and trust, avoid long-term exposure of credentials, improve security, and support access authorization between cross-account or AWS services.

Steps:

1. Create an executive role for EC2/Lambda, and the trusted entity type is AWS service. Select EC2.
2. Cross-account role: enter the target account ID; Grant only needed permissions.
3. Select permissions, attach hosting policies, and require MFA.

创建角色

创建角色 | IAM | 全局

← → ↻ 🏠 https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create

aws 🔍 Search [Alt+S]

iam Roles Create role

Account id: 7303-3557-1778
votahs/user4271446-Htao_W

Step 1
① Select trusted entity info
Step 2
○ Add permissions
Step 3
○ Name, review, and create

Select trusted entity info

Trusted entity type

- ☐ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☒ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- ☐ This account (730335571778)
- ☒ Another AWS account

Account ID
Identifier of the account that can use this role

Account ID is a 12-digit number.

Options

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☒ Require MFA
Requires that the assuming entity use multi-factor authentication.

Cancel Next

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and user account information. Below it, a breadcrumb trail reads "IAM > Roles > Create role". On the left sidebar, under the "Roles" section, three steps are listed: "Step 1: Select trusted entity", "Step 2: Add permissions", and "Step 3: Name, review, and create". Step 3 is currently selected.

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric + "+", "@", "-" characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _ , = , @ , / [] ! % * ' : ; ~ .

Trust policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "112233445566"
9       },
10      "Condition": {
11        "Bool": {
12          "aws:MultiFactorAuthPresent": true
13        }
14      }
15    }
16  ]
17 }
```

3.2.4. IAM strategy

Define the document with permission in JSON format to realize minimum permission and conditional control.

Steps:

1. Choose a strategy.
2. that lat role attached to the specify user.

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, a search bar, and the account ID. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, and Access reports. The main content area displays the 'Policies (1391)' page, which lists various AWS managed policies. A table of policies is shown with columns for Policy name, Type, Use..., and Description. The 'AmazonAppFlowFullAccess' policy is selected. Below the table, the 'Attach as a permissions policy' dialog is open, showing a list of IAM entities (users, groups, roles) to which the policy can be attached. The 'Attach policy' button is highlighted.

Policies (1391)
A policy is an object in AWS that defines permissions.

Filter by Type: All types

Policy name	Type	Use...	Description
AIOpsConsoleAdmi...	AWS managed	None	Grants full access to Amazon AI Operations service and its required permissions via AWS console. It also includes permisio...
AIOpsOperatorAcc...	AWS managed	None	Grants access to the Amazon AI Operations APIs for creating, updating, and deleting investigations, investigation events, a...
AIOpsReadOnlyAcc...	AWS managed	None	Grants ReadOnly permissions to the Amazon AI Operations service and its required resources.
AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaForBusiness services
AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessL...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessN...	AWS managed	None	-
AlexaForBusinessP...	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBusiness services
AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user's account.
AmazonAppFlow...	AWS managed	None	Provides full access to Amazon AppFlow and access to AWS services supported as flow source or destination (S3 and Redsh...
AmazonAppFlowR...	AWS managed	None	Provides read only access to Amazon Appflow flows

Attach as a permissions policy
To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (9)
Entities are IAM users, user groups and roles.

Filter by Entity type: All types

Entity name	Entity type
awsstudent	IAM Users
EC2InstanceRole	Roles
EMR_AutoScaling_DefaultRole	Roles
EMR_DefaultRole	Roles
EMR_EC2_DefaultRole	Roles
LabRole	Roles
vocareum	Roles
vocareum-eventbridge	Roles
voclabs	Roles

Buttons: Cancel, Attach policy

3.2.5 Multi-factor authentication (MFA)

When users log in or perform sensitive operations, additional dynamic verification codes are required to enhance account security. Prevent the disclosure and abuse of vouchers; Meet the requirements of compliance for strong certification.

Steps:

1. Enable MFA for Root and IAM users and enter the "Security Credentials" page.
2. Click "Assign MFA" in the "MFA Equipment" section.
3. Select the virtual MFA device.
4. Install the APP, scan the QR code and enter the MFA code.

3.2.6 AWS IAM-roles and functions

Table 6. AWS IAM-roles and functions

Services/components	Role (position in security system)	Function
AWS IAM	Identity and authorization control plane	Unified management of users, user groups, roles and policies; Implement minimum permissions and constraints (based on resources/labels /IP/MFA/ encrypted transmission, etc.).
IAM User	Unique person/service identity	Interactive or programmatic access subject; Get permission by joining a user group or attaching a policy; Daily use of Root is prohibited.
IAM User Group	RBAC aggregation unit	Grant/receive power in batches according to posts/responsibilities; Implement the separation of minimum authority and responsibility, and simplify the authority adjustment and audit when personnel change.
IAM Role	Temporary certificate and trust boundary	Obtain short-term vouchers by the trusted entity (person/service/cross-account) Assume; Used for service access, cross-account authorization and temporary right withdrawal (MFA can be enforced).
IAM Policy	Permission rule carrier	JSON defines Allow/Deny; ; Refine to operations/resources/conditions; The available permission boundary limits the maximum permission that can be granted; Explicitly Deny protects critical resources such as audit logs.
MFA	Strong authentication control	Root and high-power users are forced to enable; Sensitive operations can be constrained by aws:MultiFactorAuthPresent; Reduce the risk of unauthorized access caused by credential leakage.

IAM Access Analyzer	Access risk visualization	Discovering externally accessible resources/excessive trust and strategies; Based on the actual call, the thin policy is generated, and it continuously converges to the minimum permission.
Credential Report / CloudTrail	Identity compliance audit	Periodically export the user /MFA/ key status; Audit events such as Create/Attach/Assume in combination with CloudTrail to provide traceable evidence.

4 Network and Perimeter Protection (VPC + WAF/Shield) - Operations

Engineer

4.1 Objectives and Scope

The primary objective of this component is to design a multi-AZ private network architecture that ensures minimum exposure of financial workloads, enforces strong isolation between tiers, and provides centralized observability. The design considers the perspectives of different stakeholders—including compliance officers, security administrators, and operations engineers—ensuring that confidentiality, integrity, and availability requirements are fully addressed in the AWS environment.

4.2 Design and Configuration

- VPC Setup: A /16 VPC is segmented into public and private subnets across multiple AZs, supported by nine route tables (ingress, public, private, databases, operations, and VPC endpoints).

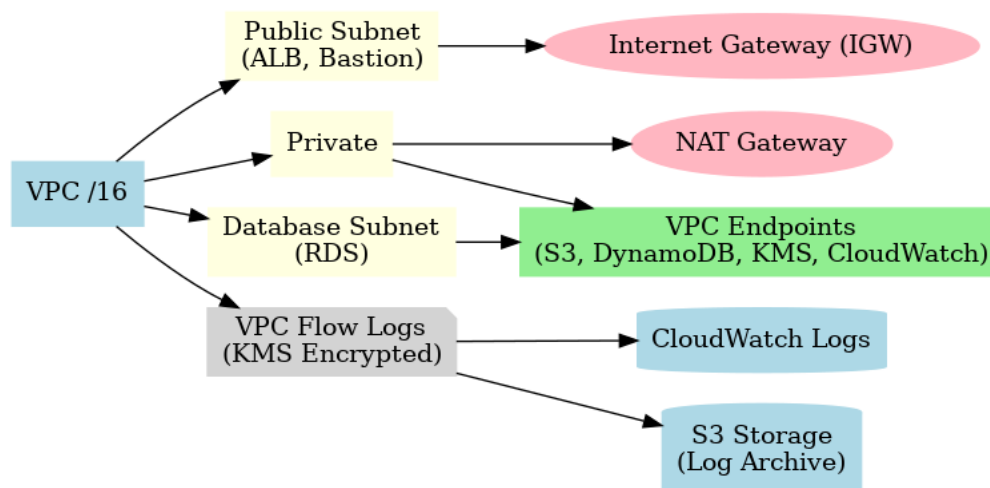
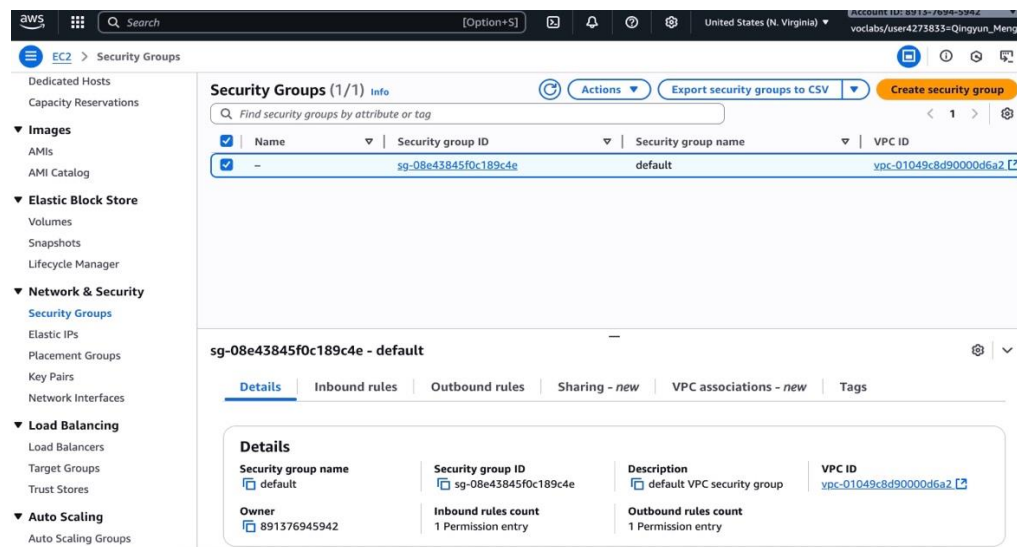


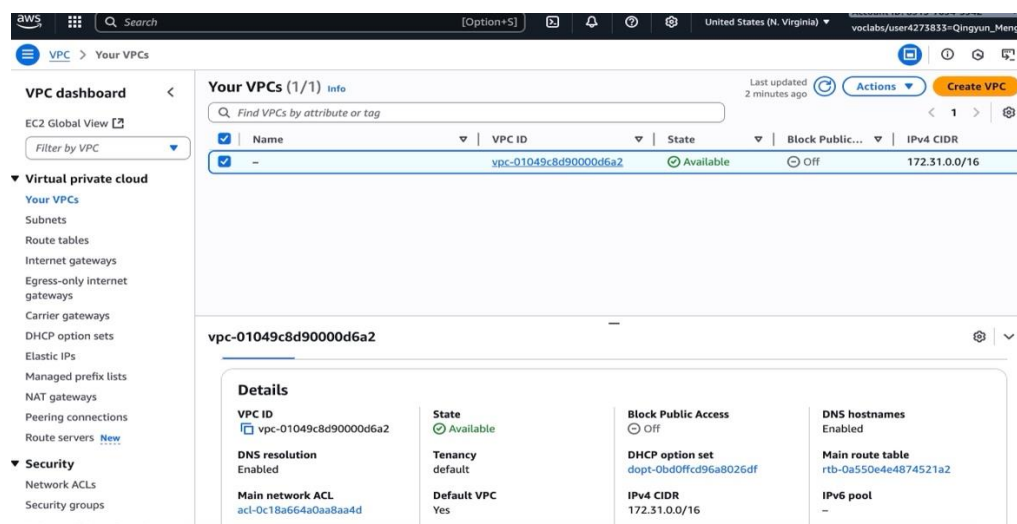
Figure 2: VPC Architecture Diagram.

- Perimeter Protection: The Internet Gateway (IGW) is strictly limited to ALB and CloudFront exposure. Private EC2 instances are restricted to outbound traffic via highly available NAT gateways with allowlisted destinations.
- Access Control: Security Groups (SG) adopt a default-deny posture, opening only

essential application ports. Network ACLs (NACL) add horizontal segmentation, preventing unauthorized lateral movement between subnets.



- Private Endpoints: VPC Endpoints are provisioned for S3, DynamoDB, KMS, and CloudWatch Logs, ensuring sensitive traffic remains within the private network without traversing the public Internet.
- Logging and Monitoring: VPC Flow Logs are enabled and directed to CloudWatch and S3, encrypted with KMS. These logs provide visibility for anomaly detection, compliance evidence, and forensic analysis.



4.3 Procedural Steps

1. **Define Subnets and Route Tables** – Create public, private, and database subnets in multiple AZs and map them to dedicated route tables. *This ensures redundancy and isolation, and will be validated by connectivity tests to confirm only the public subnet is exposed externally. It supports APRA CPS 234 by enforcing segmentation of critical financial workloads.*
2. **Configure IGW and NAT Gateways** – Allow inbound traffic only via the IGW for ALB/CloudFront, and restrict private subnet egress through NAT gateways with allowlisting. *This reduces the attack surface and will be validated through penetration testing to confirm unauthorized traffic is blocked. It meets PCI DSS by preventing uncontrolled internet exposure of cardholder data systems.*
3. **Deploy Security Groups and NACLs** – Apply a default-deny posture, allowing only required ports (e.g., 443) in SGs and restricting lateral movement with NACLs. *Validation includes testing rejected traffic attempts, while compliance is demonstrated by least-privilege controls required under ISO/IEC 27001 for financial data environments.*
4. **Provision VPC Endpoints** – Enable private connectivity to AWS services (S3, DynamoDB, KMS, CloudWatch). *This will be validated by ensuring sensitive traffic does not route through the public internet, and compliance alignment is achieved by protecting regulated data flows in accordance with APRA and PCI DSS.*
5. **Enable VPC Flow Logs** – Configure Flow Logs with KMS encryption and export them to CloudWatch and S3. *Validation involves reviewing captured logs of both allowed and denied traffic, while compliance requirements are addressed by maintaining immutable audit records for seven years as required by financial regulators.*

4.4 Validation and Evidence

- Use Cases
 - Public subnets accessible only through ALB endpoints, confirming perimeter control.

- Private instances unreachable from the internet, validating isolation of financial systems.
- Unauthorized outbound traffic blocked by SG/NACL rules, confirming least privilege enforcement.
- VPC Endpoints accessible only within the VPC, proving private routing for sensitive workloads.

Evidence

- Connectivity Testing Reports – Documented test results verifying that only approved ingress/egress is functional. *This demonstrates regulatory compliance with APRA CPS 234 on system resilience.*
- VPC Flow Logs – Logs capturing both allowed and denied traffic patterns. *These serve as auditable records for PCI DSS Requirement 10 (logging and monitoring of access to financial systems).*
- Routing, SG, and NACL Configuration Exports – Evidence of a default-deny security posture. *These provide auditors with proof of network-level least privilege, aligning with ISO/IEC 27001 controls.*
- Compliance Alignment – Collected logs and configuration evidence ensure adherence to Australian financial regulations, supporting the organization's obligations to regulators and customers.

4.5 Implementation Plan and Risks

- Milestones
 - D5: Provision VPC, Subnets, and Route Tables.
 - D9: Deploy IGW and NAT gateways with outbound allowlists.
 - D12: Enforce Security Groups and NACL baselines.
 - D15: Configure VPC Endpoints.
 - D18: Enable and validate VPC Flow Logs.
- Risks and Mitigations

- Route Misconfiguration: May expose resources or disrupt traffic. → Mitigated by peer reviews and AWS Config drift detection.
- Excessive Exposure: Overly permissive SG/NACL rules increase attack surface. → Mitigated by baseline templates and automated testing.
- Policy Conflicts: ACL/Security Group overlaps may cause access issues. → Mitigated by regression testing and monitoring.
- Integration and Value

This component integrates with Identity and Access Management by ensuring secure entry points, and with Storage and Data Protection by securing private connectivity to S3 and DynamoDB. Together, these controls deliver a consistent architecture that balances confidentiality, integrity, and availability. The plan demonstrates clear objectives, precise functions, and stakeholder-driven design, fulfilling both technical and compliance requirements.

5 Storage and Data Protection (RDS, S3, DynamoDB, Glacier) -

Compliance Officer

In financial services, data is the core asset, and any leakage, loss, or tampering poses serious risks. The goal of this component is to build a secure, compliant, and recoverable storage architecture on AWS, ensuring confidentiality, integrity, and availability in line with the Well-Architected Framework and regulations such as PCI DSS and GDPR.

The solution adopts a layered design, assigning each data type to the most suitable service and retention policy, as summarized in Table 7.

Table 7. Overall Storage Security Design

Data Category	AWS Service	Key Security Measures	Redundancy and Recovery Strategy
Transaction Data	Amazon RDS	SSE-KMS encryption; Secrets Manager for credentials; automated backups	Multi-AZ deployment; snapshot recovery
Logs and Audit Records	Amazon S3	Versioning; Object Lock; lifecycle policies	Cross-Region Replication (CRR); transition to S3-IA; expiration of old versions
High-Concurrency Events	Amazon DynamoDB	SSE-KMS encryption; VPC Endpoint access restriction	Point-in-Time Recovery (PITR, 35 days)
Long-Term Archives	Amazon S3 Glacier	Vault Lock (immutability); compliance retention policies	Multi-Region redundancy; 7–10 years archival

5.1 Amazon S3 for Logs and Audit Data

A dedicated S3 bucket (finance-audit-logs) is created in us-east-1, with access restricted to a VPC Endpoint. The objective is to ensure encryption, immutability, and disaster recovery.

Implementation Steps:

1. Create S3 bucket in us-east-1 with ACLs disabled and Block Public Access enabled.

Create bucket [info](#)
Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [info](#)
finance-audit-logs

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Object Ownership [info](#)
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

2. Enable SSE-KMS and enforce TLS for encryption in transit and at rest.

Bucket → Properties → Default encryption

Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add new tag](#)

You can add up to 50 tags.

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable

☒ Enable

► **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

3. Enable Versioning to preserve all versions and prevent tampering.

Bucket → Properties

4. Configure lifecycle rules: transition noncurrent versions to S3-IA after 30 days, delete after 365 days.

Bucket → Management → Lifecycle rules

Lifecycle rule actions

Choose the actions you want this rule to perform.

☐ Transition current versions of objects between storage classes
This action will move current versions.

☒ Transition noncurrent versions of objects between storage classes
This action will move noncurrent versions.

☐ Expire current versions of objects

☒ Permanently delete noncurrent versions of objects

☐ Delete expired object delete markers or incomplete multipart uploads
These actions are not supported when filtering by object tags or object size.

Transitions are charged per request

For a lifecycle transition action, each request corresponds to an object transition. For details on lifecycle transition pricing, see requests pricing info on the [Storage & requests](#) tab of the [Amazon S3 pricing page](#).

☒ I acknowledge that this lifecycle rule will incur a transition cost per request.

By default, objects less than 128KB will not transition across any storage class

We don't recommend transitioning objects less than 128 KB because the transition costs can outweigh the storage savings. If your use case requires transitioning objects less than 128 KB, specify a minimum object size filter for each applicable lifecycle rule with a transition action.

Transition noncurrent versions of objects between storage classes

Choose transitions to move noncurrent versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects become noncurrent and are consecutively applied. [Learn more](#)

Choose storage class transitions Days after objects become noncurrent Number of newer versions to retain - Optional

Standard-IA 30 Number of versions [Remove](#)

Can be 1 to 100 versions. All other noncurrent versions will be moved.

[Add transition](#)

Permanently delete noncurrent versions of objects

Choose when Amazon S3 permanently deletes specified noncurrent versions of objects. [Learn more](#)

Days after objects become noncurrent Number of newer versions to retain - Optional

365 Number of versions

Can be 1 to 100 versions. All other noncurrent versions will be moved.

5. Set up Cross-Region Replication with versioning and IAM role for DR.

Bucket → Management → Replication rules

The screenshot shows the AWS S3 Replication Rules configuration page. The rule name is 'CRR-to-Sydney'. The status is 'Enabled'. The priority is '0'. The source bucket is 'finance-audit-logs' in the 'US East (N. Virginia) us-east-1' region. The rule scope is set to 'Apply to all objects in the bucket'. The destination is set to 'Choose a bucket in this account', and the bucket name is 'finance-audit-logs' in the 'US East (N. Virginia) us-east-1' region. A 'Browse S3' button is visible next to the bucket name field.

Replication rule name
CRR-to-Sydney
Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status
Choose whether the rule will be enabled or disabled when created.
☒ Enabled
☐ Disabled

Priority
The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.
0

Source bucket
Source bucket name
finance-audit-logs
Source Region
US East (N. Virginia) us-east-1
Choose a rule scope
☐ Limit the scope of this rule using one or more filters
☒ Apply to all objects in the bucket

Destination
Destination
You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. [Learn more](#) or see [Amazon S3 pricing](#).
☒ Choose a bucket in this account
☐ Specify a bucket in another account
Bucket name
Choose the bucket that will receive replicated objects.
finance-audit-logs [Browse S3](#)
Destination Region
US East (N. Virginia) us-east-1

6. Verify CloudTrail logs for S3 Put/Delete events to confirm auditability.

AWS Console → CloudTrail → Event history

5.2 Amazon RDS for Transaction Data

To guarantee continuous availability of financial applications, the compute layer is designed with Auto Scaling and multi-AZ deployment. The objective is to ensure resilience, scalability, and business continuity.

Implementation Steps:

1. Deploy Auto Scaling group with ≥ 2 EC2 instances across AZs for HA.

EC2 → Auto Scaling Groups → Create group

Choose launch template

Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name

Enter a name to identify the group.

Must be unique to this account in the current Region and no more than 255 characters.

Launch template

Info

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

finance-template

Create a launch template

Version

Default (1)

Create a launch template version

Description

-

Launch template

finance-template

lt-07f8807b7bd6c3b7

Instance type

t3.small

AMI ID

ami-0b09ffb6d8b58ca91

Security groups

-

Request Spot Instances

No

Key pair name

Mykey

Security group IDs

-

Additional details

Storage (volumes)

-

Date created

Thu Sep 11 2025 18:53:18 GMT+1000 (澳大利亚东部标准时间)

Cancel

Next

Choose instance launch options

Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Instance type requirements

Info

Override launch template

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template

finance-template

lt-07f8807b7bd6c3b7

Version

Default

Description

-

Instance type

t3.small

Network

Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0913a3e75f88d4170

172.31.0.0/16

Default

Create a VPC

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

use1-az1 (us-east-1a) | subnet-01ab6fdb38fe11537

172.31.0.0/20

Default

use1-az2 (us-east-1b) | subnet-0de6d5c92a7c36a29

172.31.80.0/20

Default

Create a subnet

Availability Zone distribution - new

Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

Balanced best effort

If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

Balanced only

If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

Cancel

Skip to review

Previous

Next

2. Configure ALB to distribute traffic evenly across instances.

EC2 → Load Balancers → Create ALB

Create Application Load Balancer [Info](#)

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

► How Application Load Balancers work

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

finance-a1b

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme [Info](#)

Scheme can't be changed after the load balancer is created.

☒ Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

☐ Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type [Info](#)

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ IPv4

Includes only IPv4 addresses.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

☐ Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with internet-facing load balancers only.

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#).

vpc-0913a3e75f88d4170

172.31.0.0/16

(default)



[Create VPC](#)

IP pools [Info](#)

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view [Pools](#) in the [Amazon VPC IP Address Manager console](#).

☐ Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets [Info](#)

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☒ us-east-1a (use1-az1)

☒ us-east-1b (use1-az2)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0de6d5c92a7c36a29

IPv4 subnet CIDR: 172.31.80.0/20

☐ us-east-1c (use1-az4)☐ us-east-1d (use1-az6)☐ us-east-1e (use1-az3)☐ us-east-1f (use1-az5)Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

default

sg-04847248d562bae3a VPC: vpc-0913a3e75f88d4170

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP-80

Remove

Protocol

HTTP

Port

80

1-65535

Default action [Info](#)

Forward to

finance-tg2

Target type: instance, IPv4

HTTP

[Create target group](#)

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

[Add listener](#)

You can add up to 49 more listeners.

3. Add scaling policy (scale out if CPU >70%) for elasticity and cost optimization.

Auto Scaling Groups → Scaling policies

Configure group size and scaling - optional [Info](#)

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances)

Desired capacity

Specify your group size.

2

Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

6

Equal or greater than desired capacity

Automatic scaling - optional

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

☐ No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

☒ Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Target Tracking Policy

Metric type [Info](#)

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization

Target value

70

Instance warmup [Info](#)

300

seconds

4. Integrate Route 53 health checks + failover routing for DNS-level redundancy.

Route 53 → Health checks / Failover routing

Create health check [Info](#)

Create a new health check to monitor the health of a specified resource.

Configuration

Configuration options have cost implications. Pricing will vary based on the selected resource type. Advanced configurations have an additional cost. [View pricing](#).

Name - optional

A friendly name that lets you easily find a health check in the dashboard.

finance-primary-hc

The name must have 1-256 characters. Valid characters: A-Z, a-z, 0-9, -, (hyphen), and _ (underscore).

Resource

☒ Endpoint

Establish a connection with the resource to determine its health status.

☐ Calculated health check

The status of the health check is based on the status of the other health checks.

☐ CloudWatch alarm

The status of the health check is based on the state of a specified CloudWatch alarm.

Specify endpoint by

☒ IP address

☐ Domain name

IP address

The path can be any value for which your endpoint will return an HTTP status code of 2xx or 3xx when the endpoint is healthy.

HTTP

finance-atlb-1323587285-us-east-1.elb.amazonaws.com

Advanced configuration**Request interval**

In this time interval you will receive one request per health checker.

☒ Standard (30 seconds)

☐ Fast (10 seconds)

Failure threshold

The number of consecutive health check failures that is considered unhealthy.

3

☐ String matching - optional

Search the response body for a specified search string. The endpoint is considered healthy if the entire value appears within the first 5120 bytes of the response body.

☐ Latency graphs - optional

Display latency graphs on the health checks details page, can not be edited after creation.

☐ Invert health check status

Causes Route 53 to invert the status of a health check, for example, a health check that is healthy, is considered unhealthy.

☐ Disable health check

Causes Route 53 to stop monitoring health of the specified endpoint, CloudWatch alarm, or other health checks. You can force a failover by inverting the health check status.

Health checker Regions

Check the endpoint from a minimum of three selected Regions.

5. Enable CloudWatch alarms (CPU/utilization/5XX) for proactive monitoring and incident response.

CloudWatch → Alarms → Create alarm

5.3 Amazon DynamoDB for High-Concurrency Events

Amazon DynamoDB is deployed to handle high-frequency financial transactions and audit events, ensuring low-latency writes, scalability under concurrent workloads, and data integrity.

Implementation Steps:

1. Create table finance-events with partition key eventID and sort key timestamp.

DynamoDB → Create table

Create table

Table details [Info](#)
DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.

Table name
This will be used to identify your table.

Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.).

Partition key
The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.

1 to 255 characters and case sensitive.

Sort key - optional
You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among all items sharing the same partition key.

1 to 255 characters and case sensitive.

2. Enable Auto Scaling on RCUs/WCUs to handle concurrency.

Table → Capacity → Auto Scaling

Edit read/write capacity

Capacity mode [Info](#)

☐ On-demand
Simplify billing by paying for the actual reads and writes your application performs.

☒ Provisioned
Manage and optimize your costs by allocating read/write capacity in advance.

► Capacity calculator [Info](#)

Table capacity

Read capacity

Auto scaling [Info](#)
Dynamically adjusts provisioned throughput capacity on your behalf in response to actual traffic patterns.

☒ On
☐ Off

Minimum capacity units
2

Maximum capacity units
10

Target utilization (%)
70

Initial provisioned units [Info](#)
5

Write capacity

Auto scaling [Info](#)
Dynamically adjusts provisioned throughput capacity on your behalf in response to actual traffic patterns.

☒ On
☐ Off

Minimum capacity units
2

Maximum capacity units
10

Target utilization (%)
70

Initial provisioned units [Info](#)
5

[To avoid throttling, make sure your read and write provisioned capacity units are high enough to handle your traffic.](#)

3. Enable PITR for 35-day full recovery window.

DynamoDB → Backups → Enable PITR

Create on-demand backup

Create a one-time snapshot backup of your table. Schedule automatic backups of your table in [AWS Backup](#).

Source table [Info](#)

Source table
finance-events

Backup settings [Info](#)

A backup name will be created automatically.

☒ Default settings
Create a backup that stays in warm storage.

☐ Customize settings
Create a backup that can transition to cold storage and be deleted as it ages.

Backup window
Start in 1 hour

Retention period
Always

Backup management
AWS Backup

Backup vault
Default

Transition to cold storage
Never

IAM Role
AWSBackupDefaultServiceRole

Tags - optional

AWS Backup copies tags from the DynamoDB table to the recovery point upon creation. You can specify additional tags to add to the recovery point.

No tags are associated with the resource.

[Add new tag](#)
You can add 50 more tags.

[Cancel](#) [Create backup](#)

4. Enable DynamoDB Streams + integrate with Lambda for real-time audit pipelines.

DynamoDB → Tables → Streams

Turn on DynamoDB stream

DynamoDB stream details

Capture item-level changes in your table, and push the changes to a DynamoDB stream. You then can access the change information through the DynamoDB Streams API.

View type

Choose which versions of the changed items you would like to push to the DynamoDB stream.

☒ New and old images
Both the new and old images of the changed item.

☐ Key attributes only
Only the key attributes of the changed item.

☐ New image
The entire item as it appears after it was changed.

☐ Old image
The entire item as it appears before it was changed.

[Cancel](#) [Turn on stream](#)

5. Encrypt with SSE-KMS and enforce TLS for compliance (PCI DSS).

Table → Properties → Encryption

Manage encryption [info](#)

All data stored in Amazon DynamoDB is fully encrypted at rest. By default, DynamoDB manages the encryption key, and you are not charged any fee for using it.

Encryption at rest**Encryption key management**

- ☐ **AWS owned key**
The key is owned and managed by DynamoDB. You are not charged additional fees for using this key.
- ☒ **AWS managed key**
The key is stored in your account and managed by AWS Key Management Service (KMS). AWS KMS charges apply.
- ☐ **Customer managed key**
The key is stored in your account and managed by you. AWS KMS charges apply.

[Cancel](#)[Save changes](#)

5.4 Amazon S3 Glacier for Long-Term Archives

Amazon S3 Glacier is used to archive audit logs and historical compliance data. It provides secure, durable, and low-cost storage for infrequently accessed data, ensuring financial records remain available for investigation without burdening primary storage.

Implementation Steps:

1. Create finance-archives bucket in us-east-1 with Block Public Access enabled.

S3 → Create bucket

Create bucket [info](#)

Buckets are containers for data stored in S3.

General configuration**AWS Region**

US East (N. Virginia) us-east-1

Bucket type [info](#)

- ☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
- ☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [info](#)

finance-archives

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership [info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

- ☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ☐ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☒ **Block public access to buckets and objects granted through any access control lists (ACLs)**

2. Enable SSE-KMS (CMK) for all archived objects.

Bucket → Properties → Default encryption

Edit default encryption info

Default encryption
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type info
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).
☐ Server-side encryption with Amazon S3 managed keys (SSE-S3)
☒ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

AWS KMS key info
☒ Choose from your AWS KMS keys
☐ Enter AWS KMS key ARN

Available AWS KMS keys
 arnaws:kms:us-east-1:65465432034:alias/aws/s3 ⊕ [Create a KMS key](#)

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)
☐ Disable
☒ Enable

⚠ Changing the default encryption settings might cause in-progress replication and Batch Replication jobs to fail. These jobs might fail because of missing AWS KMS permissions on the IAM role that's specified in the replication configuration. If you change the default encryption settings, make sure that this IAM role has the necessary AWS KMS permissions. [Learn more](#)

[Cancel](#) [Save changes](#)

3. Configure lifecycle rule: move objects >90 days to Glacier.

4. Define expiration: delete after 7 years (financial compliance).

Bucket → Management → Lifecycle rules

Lifecycle rule actions
Choose the actions you want this rule to perform.

☒ Transition current versions of objects between storage classes
This action will move current versions.

☐ Transition noncurrent versions of objects between storage classes
This action will move noncurrent versions.

☒ Expire current versions of objects
☐ Permanently delete noncurrent versions of objects
☐ Delete expired object delete markers or incomplete multipart uploads
These actions are not supported when filtering by object tags or object size.

⚠ Transitions are charged per request
For a lifecycle transition action, each request corresponds to an object transition. For details on lifecycle transition pricing, see requests pricing info on the **Storage & requests** tab of the [Amazon S3 pricing page](#).

☒ I acknowledge that this lifecycle rule will incur a transition cost per request.

ⓘ By default, objects less than 128KB will not transition across any storage class
We don't recommend transitioning objects less than 128 KB because the transition costs can outweigh the storage savings. If your use case requires transitioning objects less than 128 KB, specify a minimum object size filter for each applicable lifecycle rule with a transition action.

Transition current versions of objects between storage classes
Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. [Learn more](#)

Choose storage class transitions	Days after object creation	
Standard-IA	30	Remove
Glacier Deep Archive	90	Remove

[Add transition](#)

Expire current versions of objects
For version-enabled buckets, Amazon S3 adds a delete marker and the current version of an object is retained as a noncurrent version. For non-versioned buckets, Amazon S3 permanently removes the object. [Learn more](#)

Days after object creation
2555

5. Enable Object Lock (compliance mode) for WORM retention if required.

Bucket → Properties → Object Lock

6.6 Compliance and Verification

Integration with IAM-managed KMS, CloudTrail, and VPC Endpoints ensures least-privilege enforcement and unified auditing across components.

The storage and data protection design aligns with PCI DSS, GDPR, and APRA CPS 234. Compliance is enforced through encryption, immutability, auditability, and retention policies across all services. Sensitive data is encrypted with KMS keys and transmitted over TLS, logs are retained for at least seven years, and recovery strategies are verified through regular drills.

Across the Cloud Security Lifecycle, data is secured at creation (SSE-KMS, TLS), during use (IAM, VPC Endpoints, Auto Scaling), in storage (RDS Multi-AZ, S3 Versioning, DynamoDB PITR, CRR), and at disposal (lifecycle expiration rules). Table 8 summarizes the mapping of regulatory requirements to AWS controls, ensuring the framework is auditable and resilient.

Table 8. Mapping Regulatory Requirements to AWS Security Configurations

Regulation	Requirement	AWS Implementation
PCI DSS	Encrypt sensitive financial data	SSE-KMS with CMK + TLS in transit
GDPR	Right to erasure / data minimization	Lifecycle rules + expiration after 7 years
APRA CPS 234	Auditability and data resilience	CloudTrail + Cross-Region Replication

6 Conclusion

This report has presented a secure cloud architecture tailored for financial services migrating to AWS. By integrating identity and access management, network and perimeter protection, and storage and data security, the design ensures a layered defense that reduces risks of data leakage, unauthorized access, and service disruption. The framework aligns with PCI DSS, GDPR, and APRA CPS 234, embedding compliance into technical and operational controls. Mapped across the cloud security lifecycle, the solution provides encryption, monitoring, recovery, and secure disposal of data.

Reference

Amazon Web Services. (2024). AWS well-architected framework: Security pillar.
Amazon Web Services.

Australian Prudential Regulation Authority. (2019). CPS 234 information security.
APRA Prudential Standard.

European Union. (2016). General data protection regulation (GDPR): Regulation
(EU) 2016/679. Official Journal of the European Union.

PCI Security Standards Council. (2024). Payment card industry data security standard
(PCI DSS) version 4.0.1. PCI Security Standards Council.