Cloud Security Architecture AWS
Project Design

A Resilient and Auditable Cloud Security Framework for Financial Services

Contents

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).

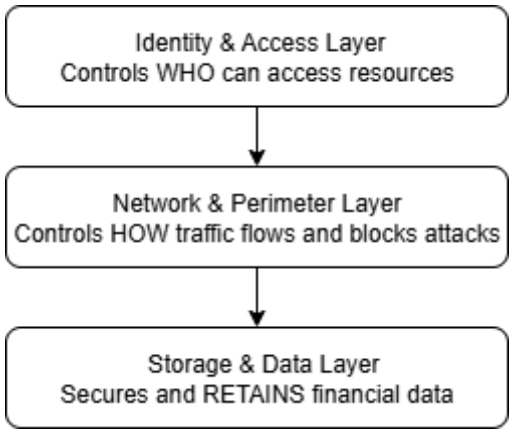


Figure 1. Integrated Security Architecture

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;

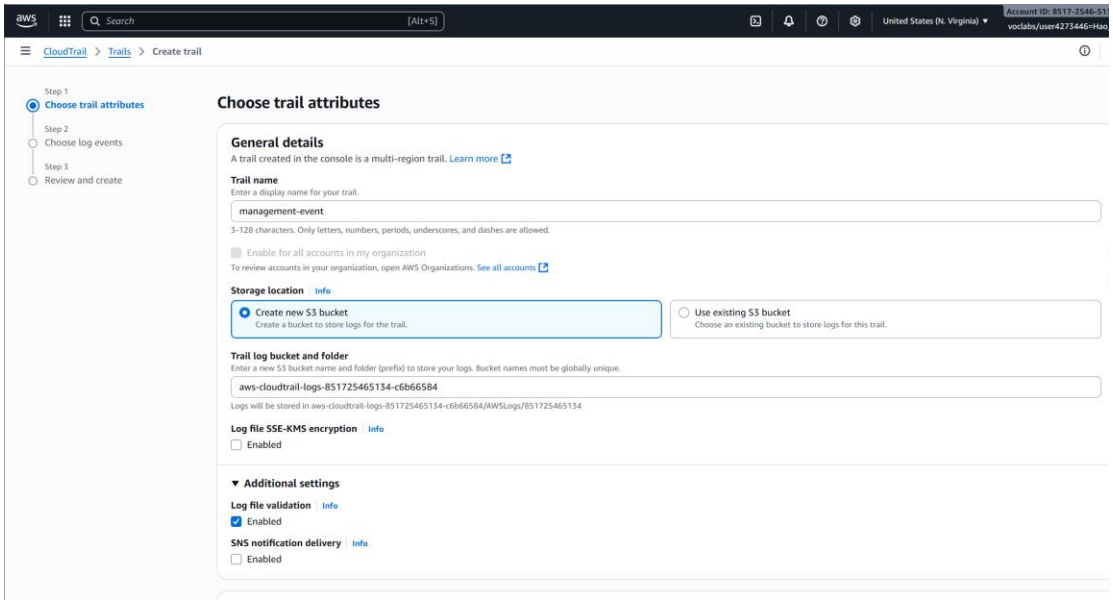
EventBridge→Lambda/SSM automatic isolation and rollback; Detective traceability afterwards.

3.1.1 AWS CloudTrail

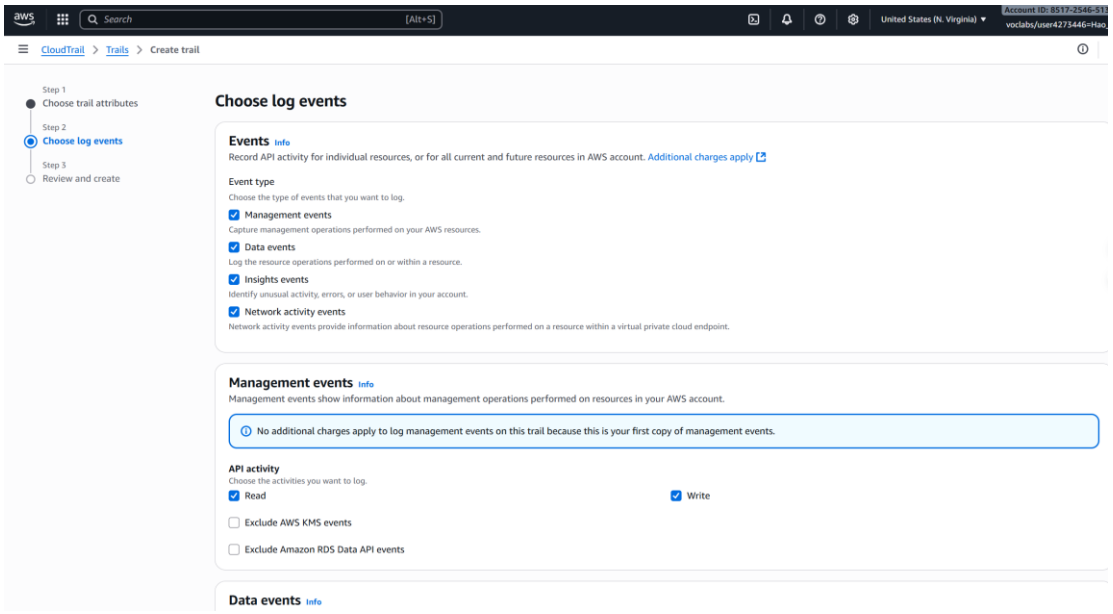
CloudTrail is used to record all management operation events in AWS accounts, and supports operation audit, risk monitoring and compliance requirements.

Steps:

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



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



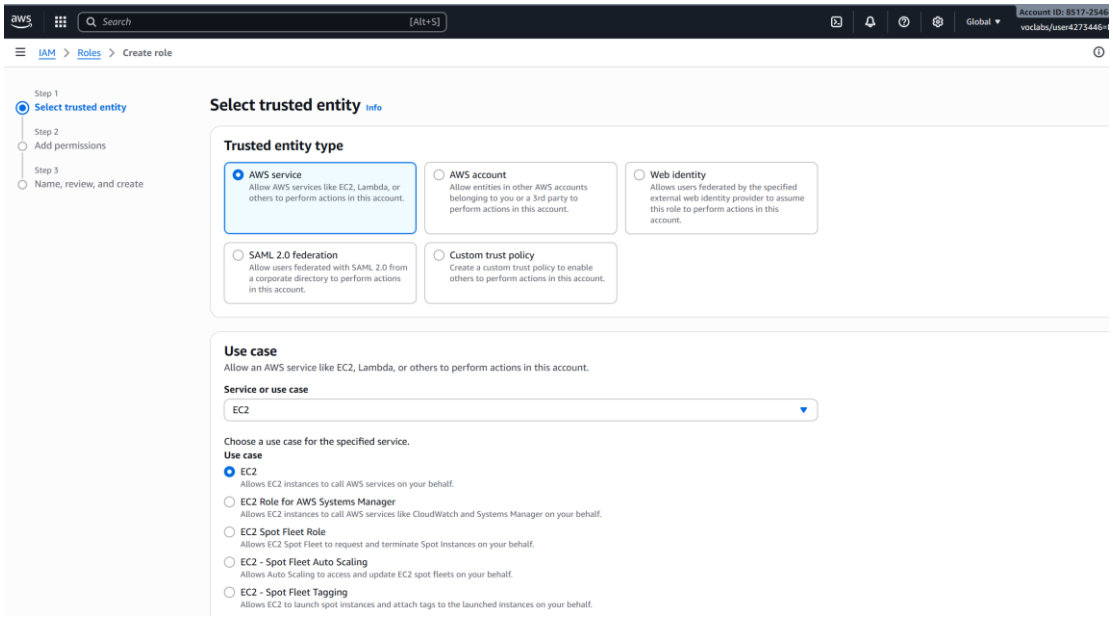
3.create.

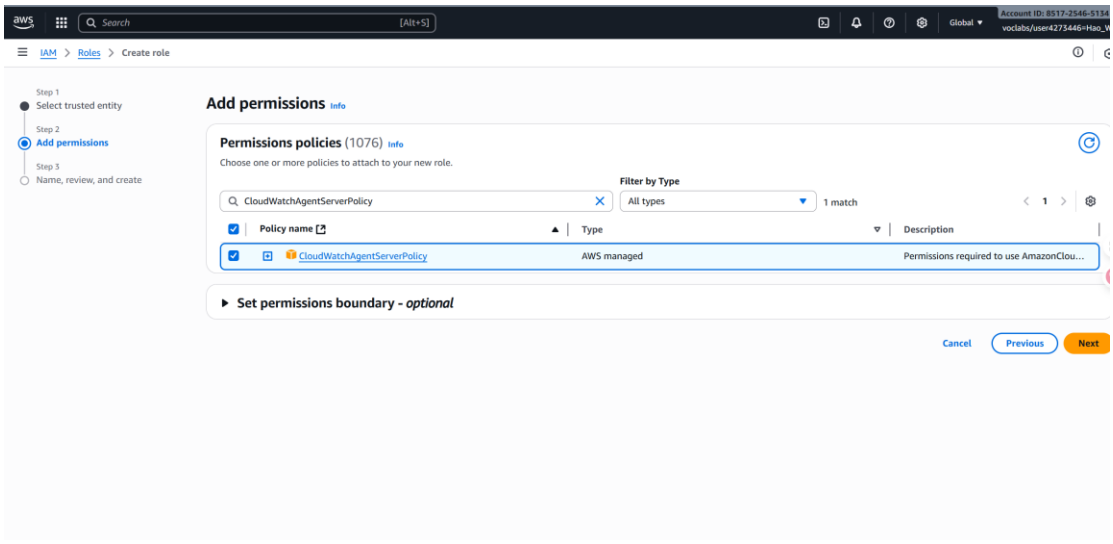
3.1.2 Amazon CloudWatch

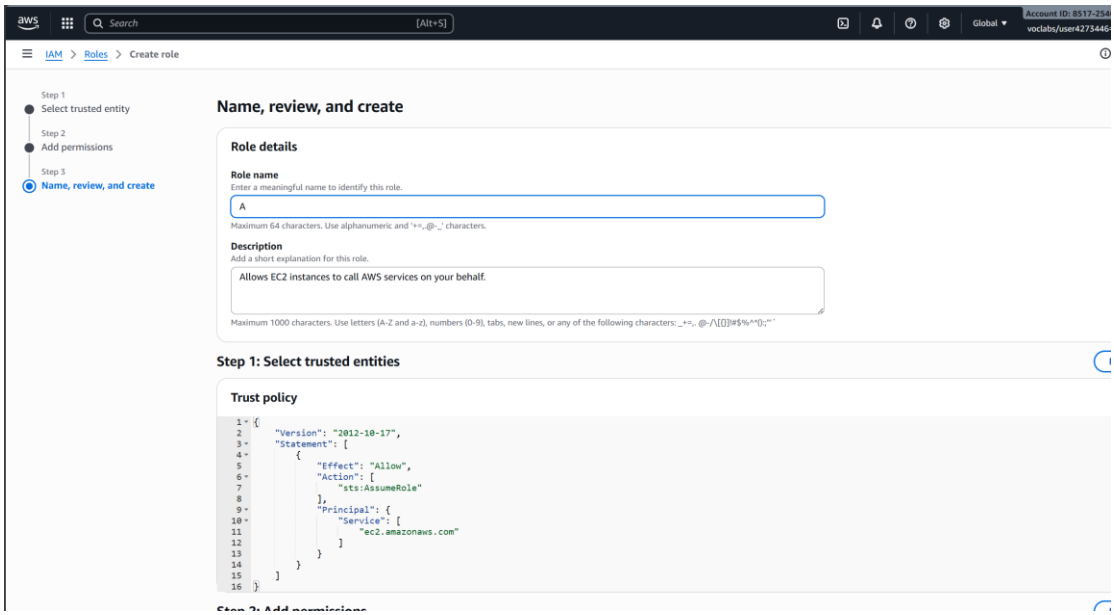
Responsible for real-time monitoring and alarm of resources and applications on the cloud, which is used for log analysis, indicator alarm and automatic response in the security architecture.

Steps:

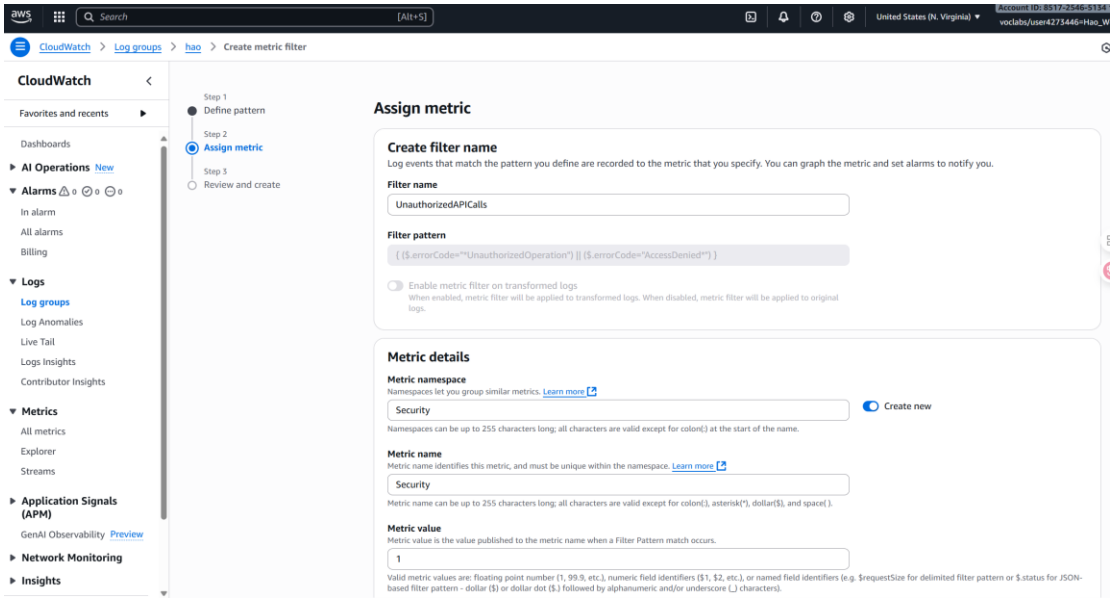
1.Trail settings →CloudWatch log integration → create a new log group, and give CloudTrail the IAM role of writing logs.

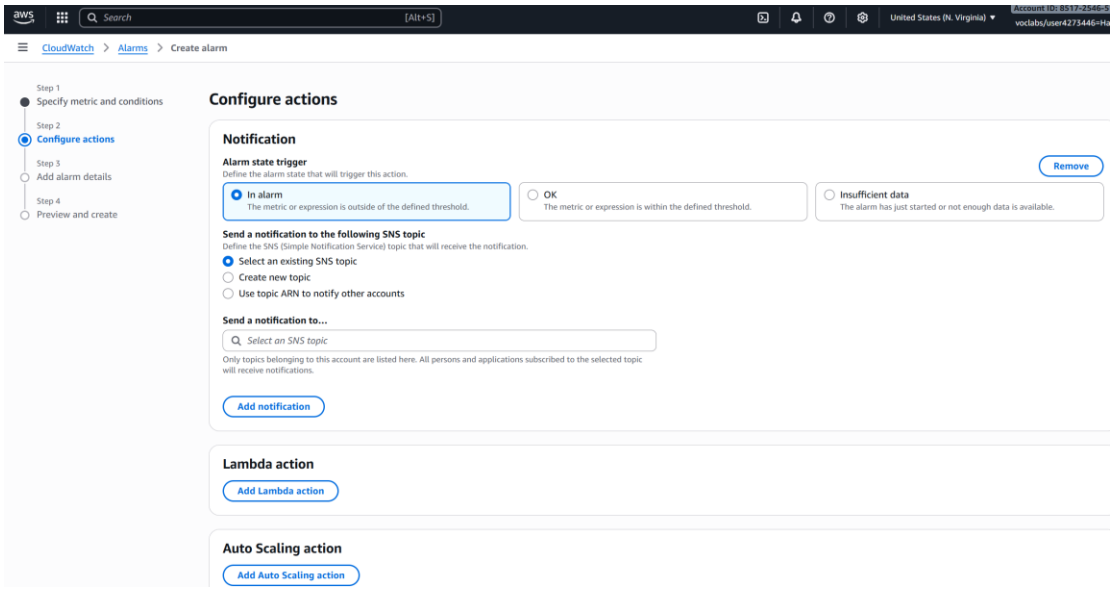

Search [Alt+S]
Global
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities 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.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.


Search [Alt+S]
Global
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1076) Info
Choose one or more policies to attach to your new role.
Filter by Type
CloudWatchAgentServerPolicy
All types
1 match
Policy name
Type
Description
CloudWatchAgentServerPolicy
AWS managed
Permissions required to use AmazonClou...
Set permissions boundary - optional
Cancel
Previous
Next

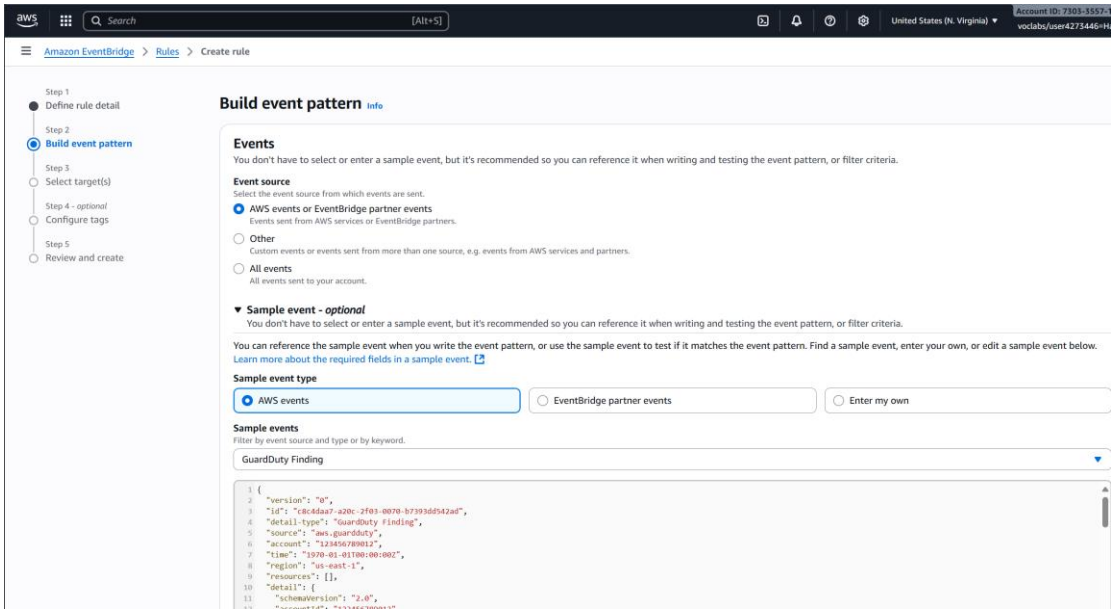

Search [Alt+S]
Global
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
A
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, .@-/\[{}]!#$%^*();:"'`
Step 1: Select trusted entities
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
}
}
]
}

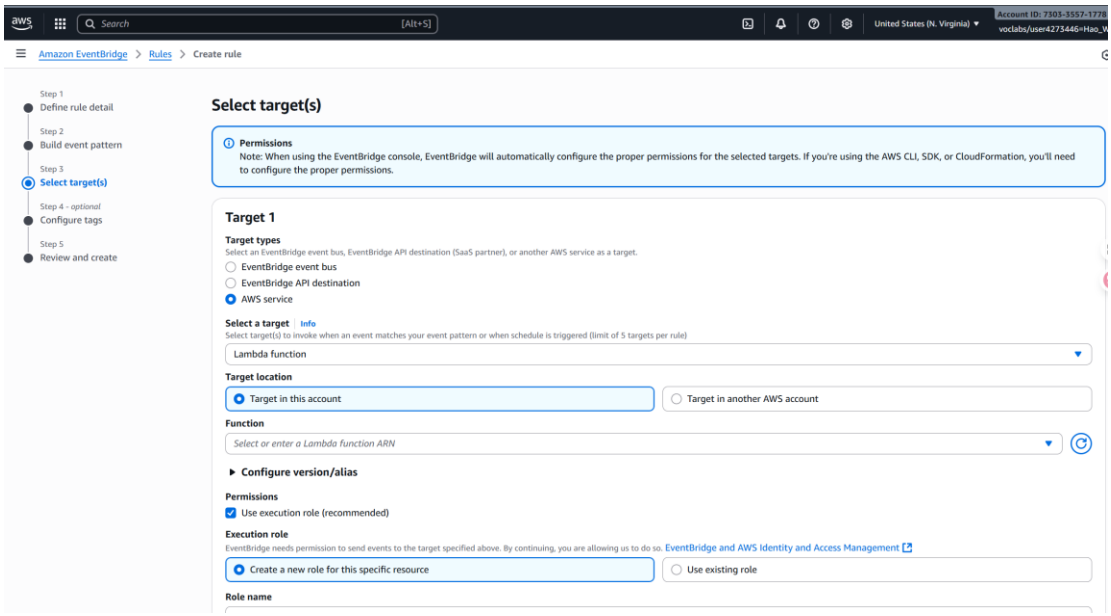
2.In the CloudWatch Alarms console, customize indicators to create alarms and set thresholds.





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





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;

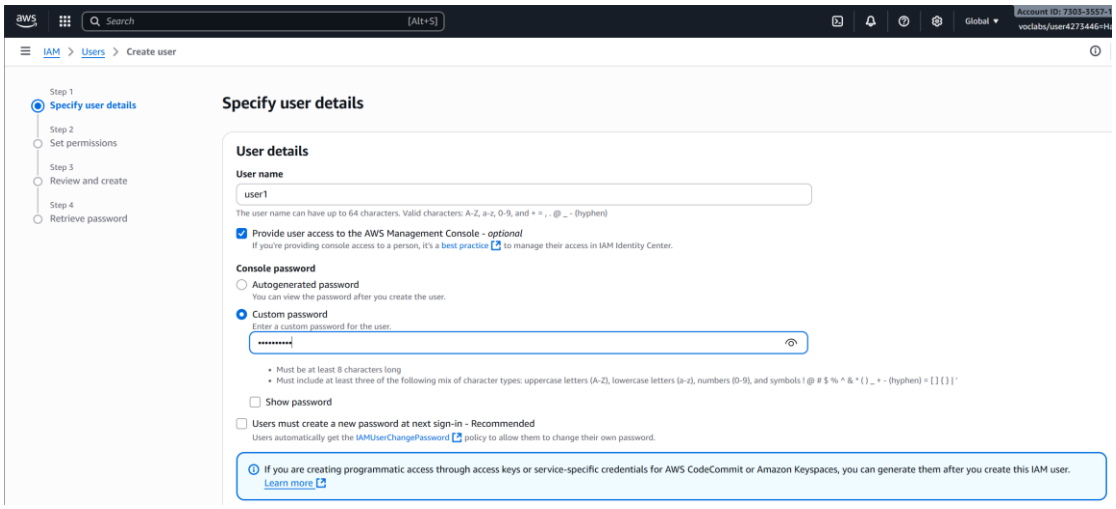
All subjects who can create identities enforce permission boundaries.

3.2.1 IAM users

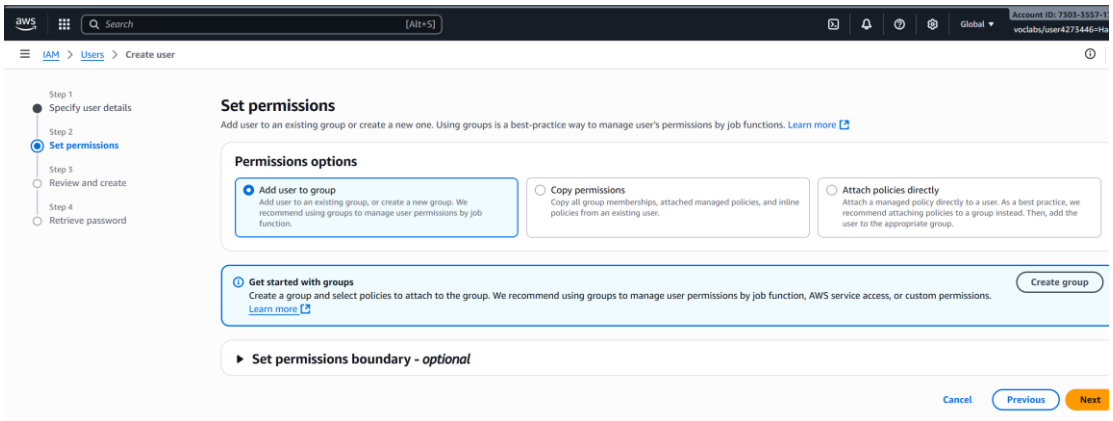
Represents an entity that needs direct access to AWS resources, and needs to create a unique identity for each administrator and business operator; It is forbidden to use Root every day, and at the same time force MFA to improve login security.

Steps:

1.Create IAM users and customize complex passwords.



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



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

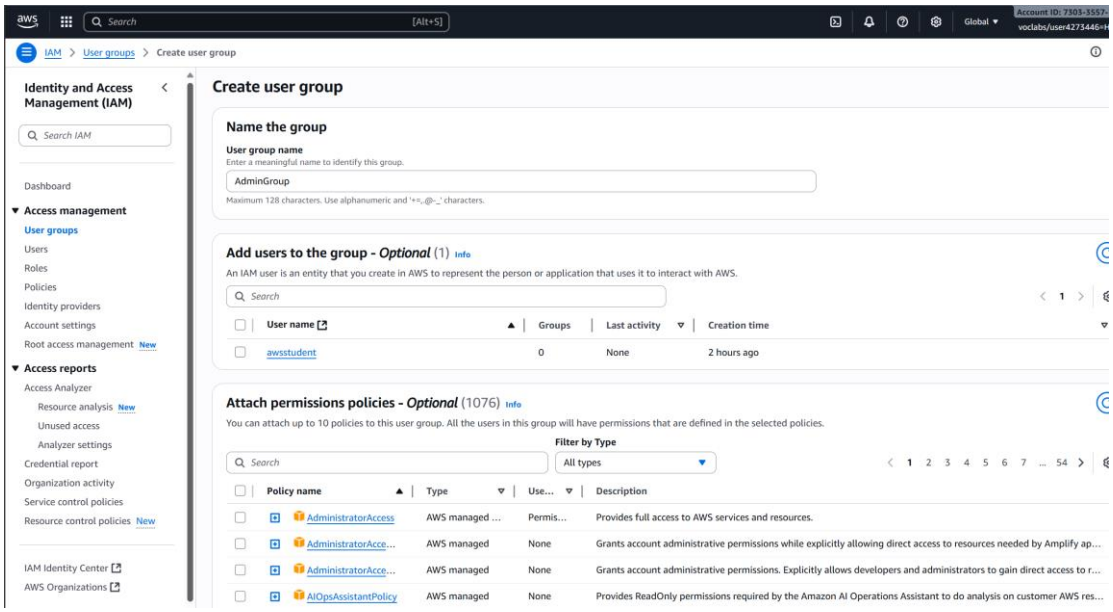
4.Check the user status with Credential Report/CloudTrail.

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.

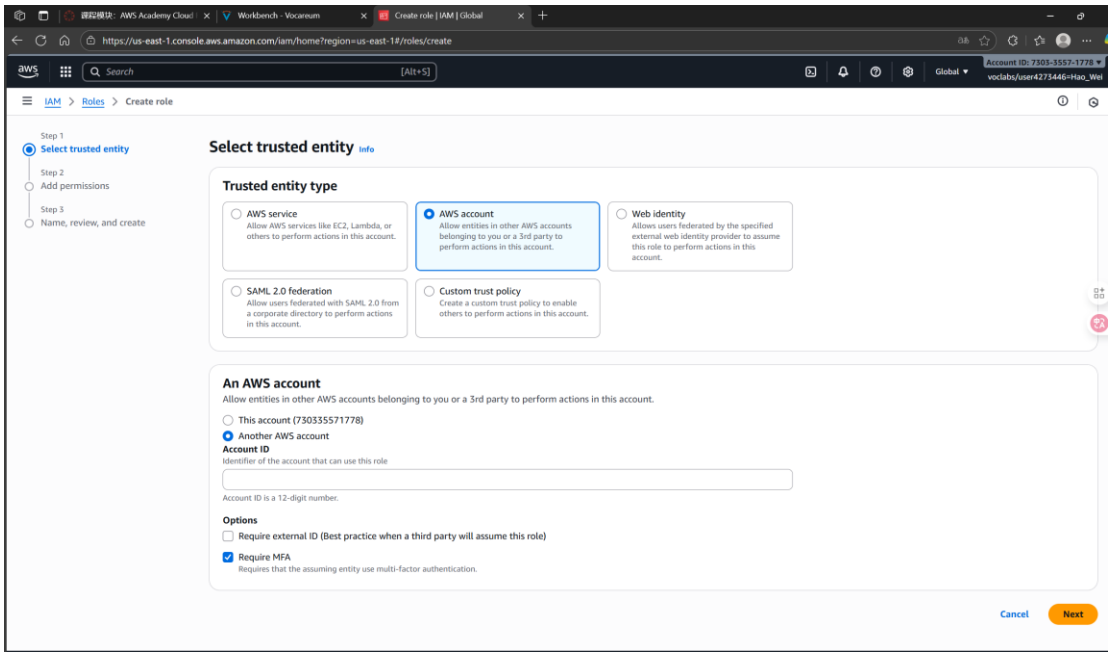


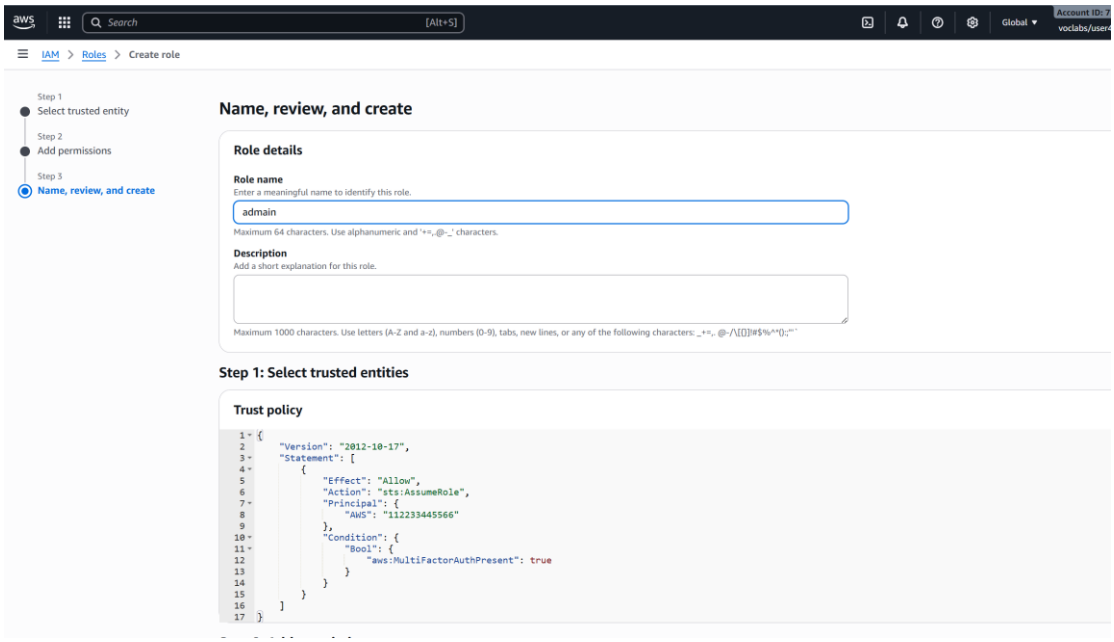
3.2.3.IAM role

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.



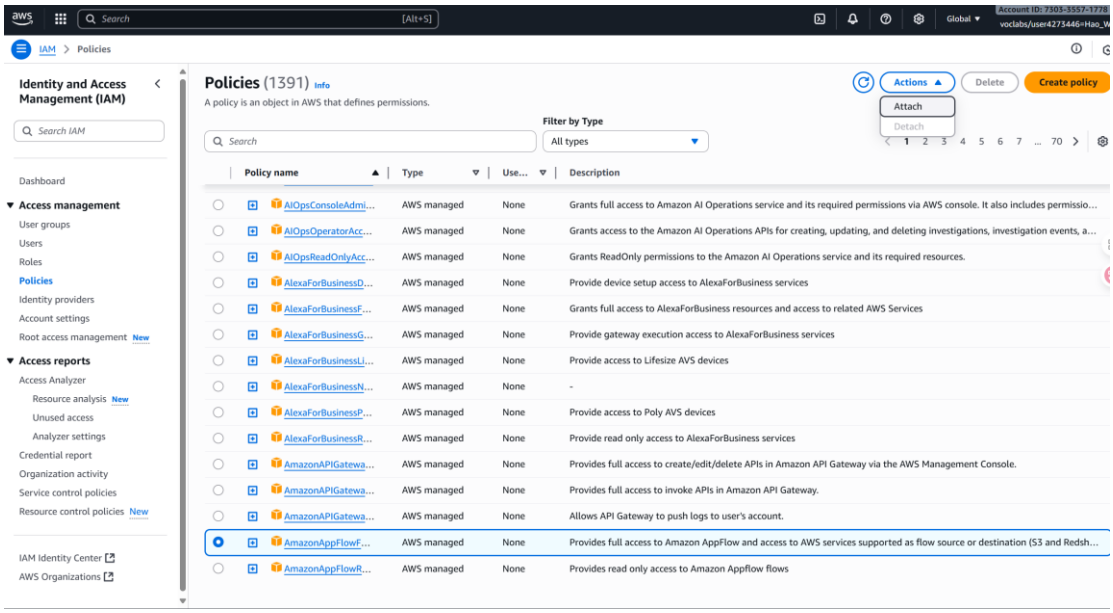


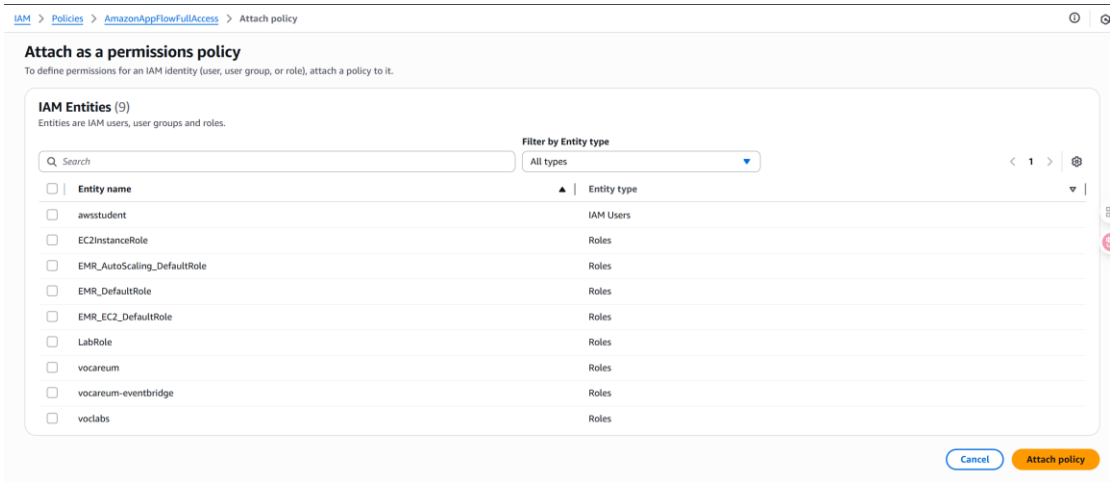
3.2.4. IAM strategy

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.





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).

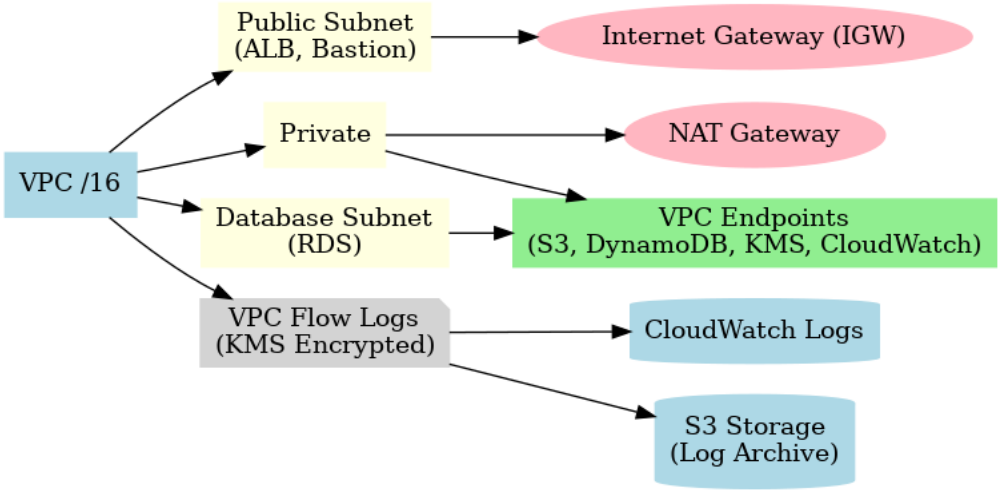
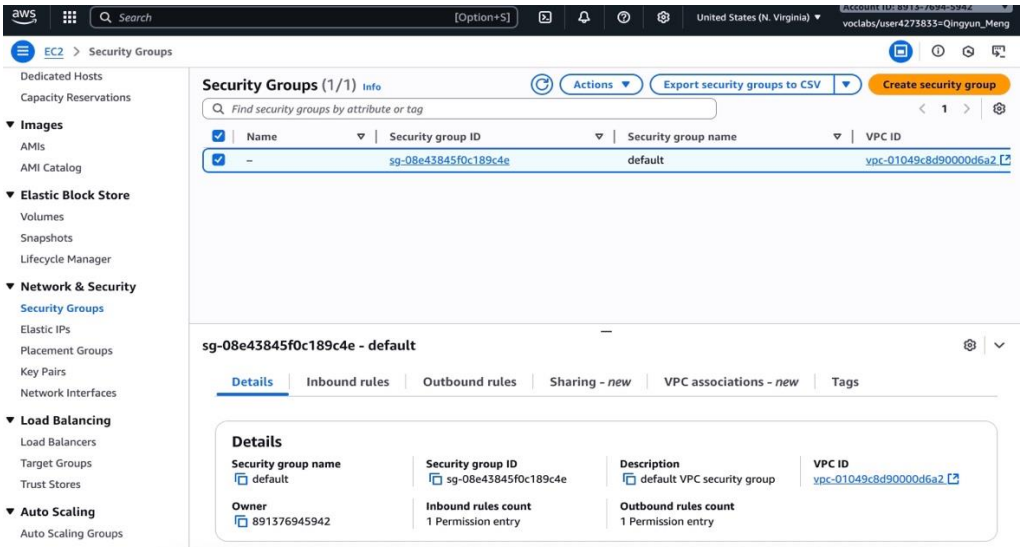


Figure 2: VPC Architecture Diagram.

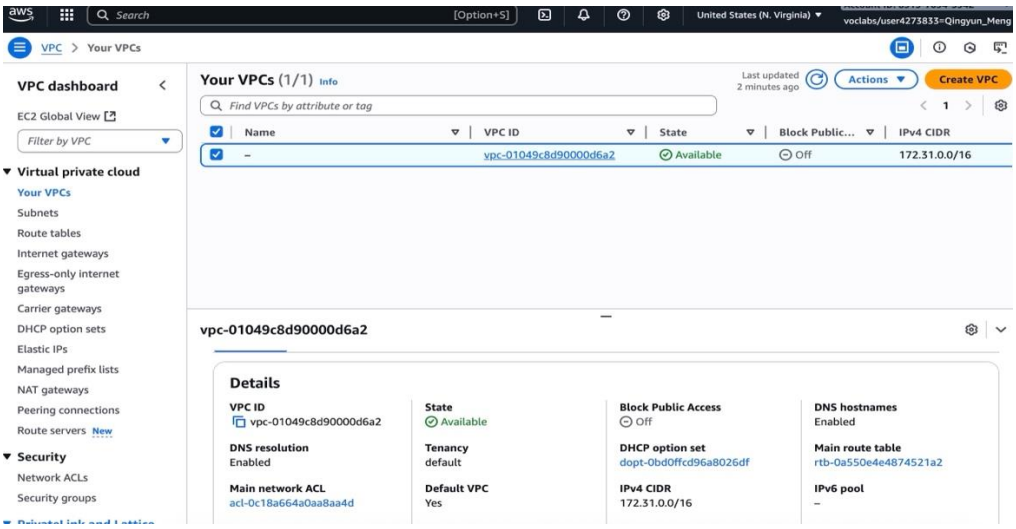
- Perimeter Protection: The Internet Gateway (IGW) is strictly limited to ALB and CloudFront exposure. Private EC2 instances are restricted to outbound traffic via highly available NAT gateways with allowlisted destinations.

- 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

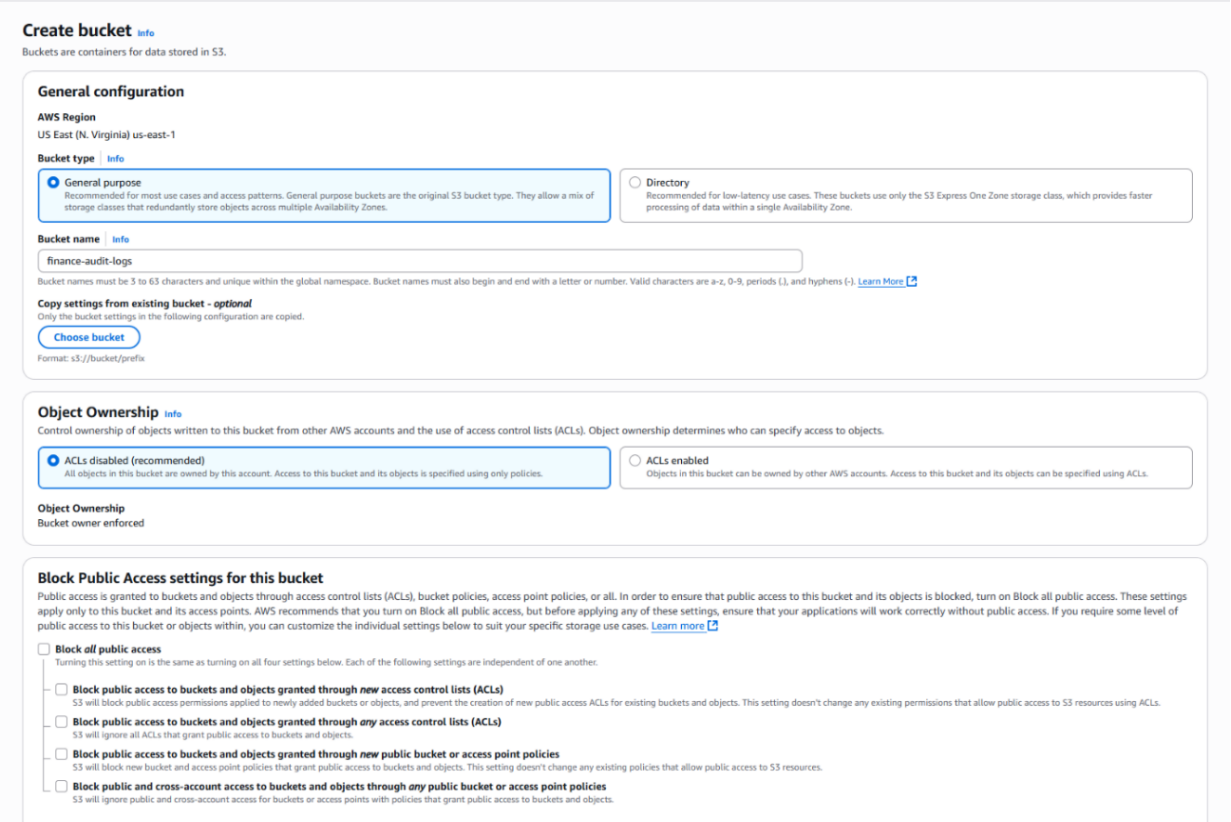
Data Category	AWS Service	Key Security Measures	Redundancy and Recovery Strategy
Transaction Data	Amazon RDS	SSE-KMS encryption; Secrets Manager for credentials; automated backups	Multi-AZ deployment; snapshot recovery
Logs and Audit Records	Amazon S3	Versioning; Object Lock; lifecycle policies	Cross-Region 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.

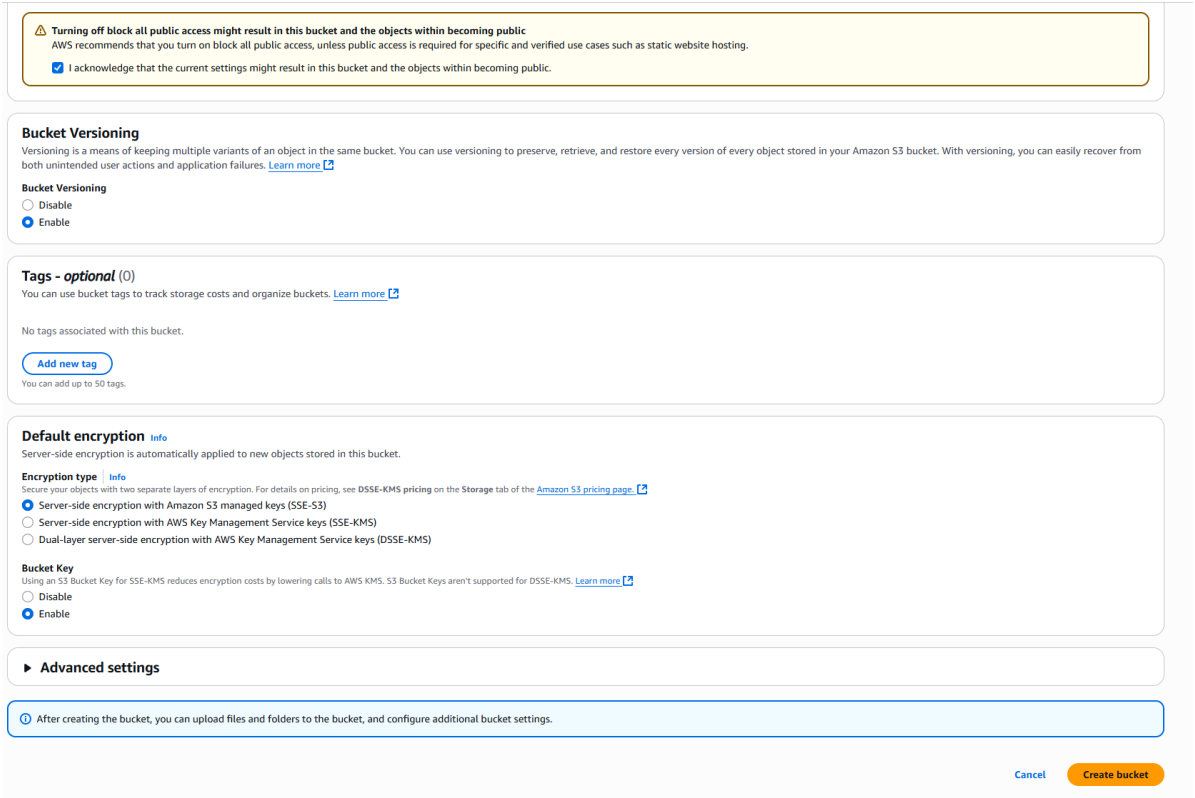
Implementation Steps：

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



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

Bucket → Properties → Default encryption

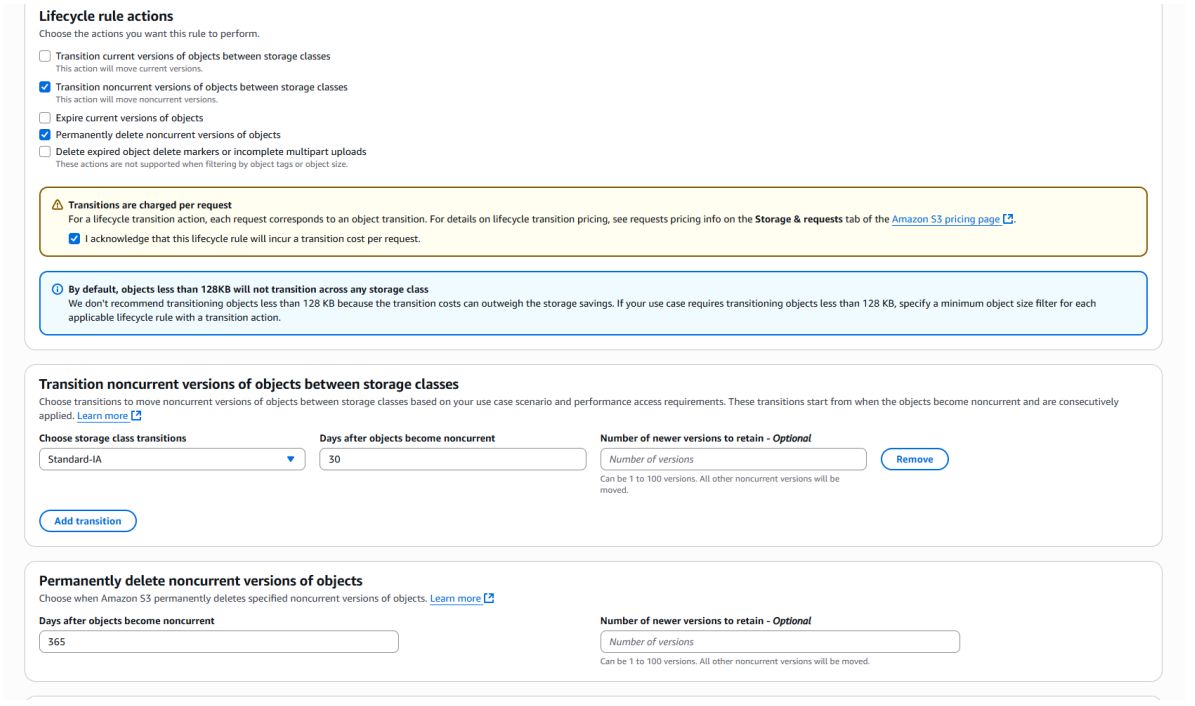


3. Enable Versioning to preserve all versions and prevent tampering.

Bucket → Properties

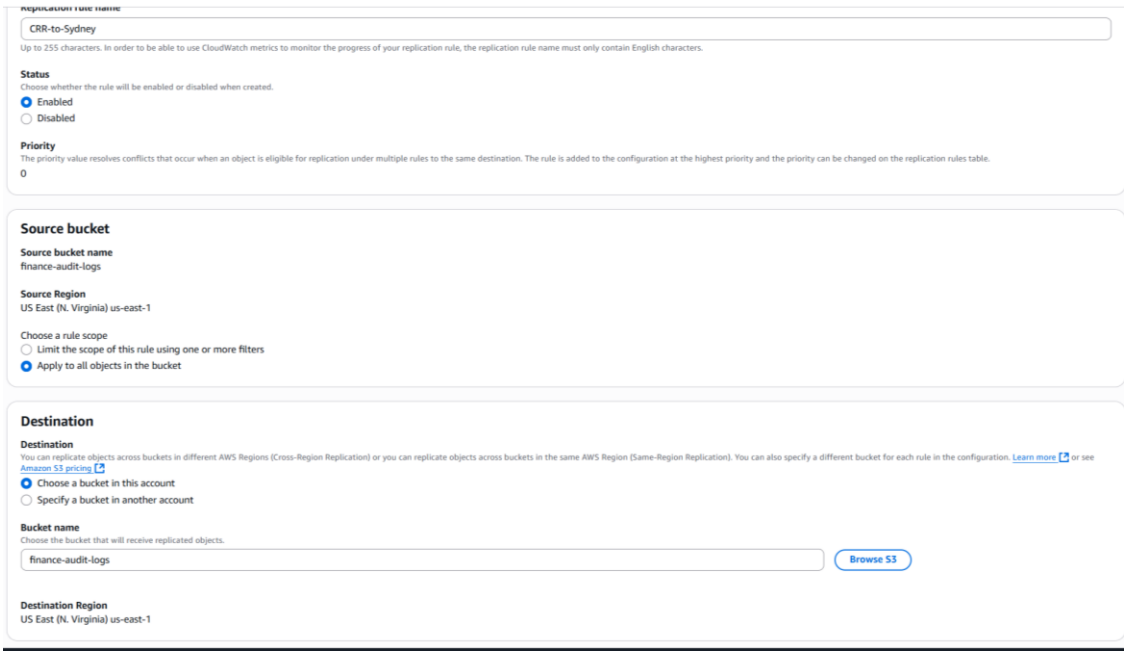
4. Configure lifecycle rules: transition noncurrent versions to S3-IA after 30 days, delete after 365 days.

Bucket → Management → Lifecycle rules



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

Bucket → Management → Replication rules



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

AWS Console → CloudTrail → Event history

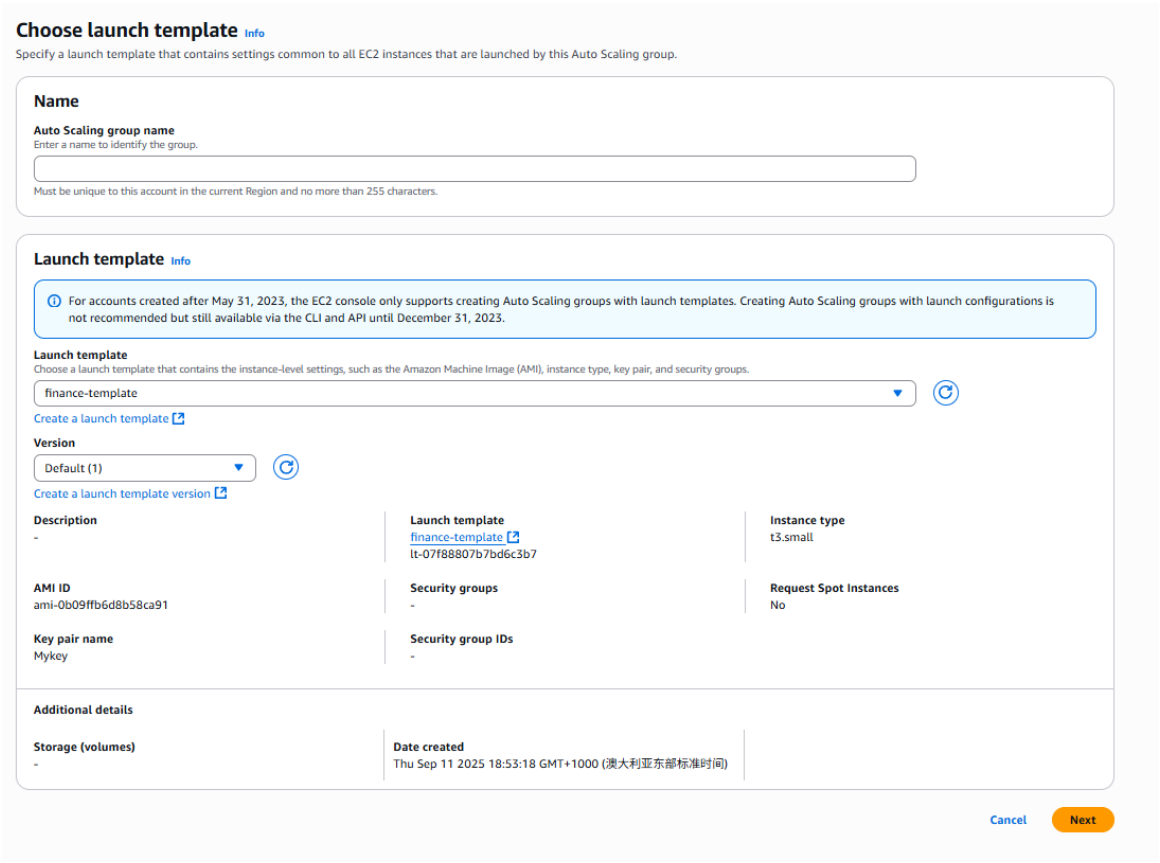
5.2 Amazon RDS for Transaction Data

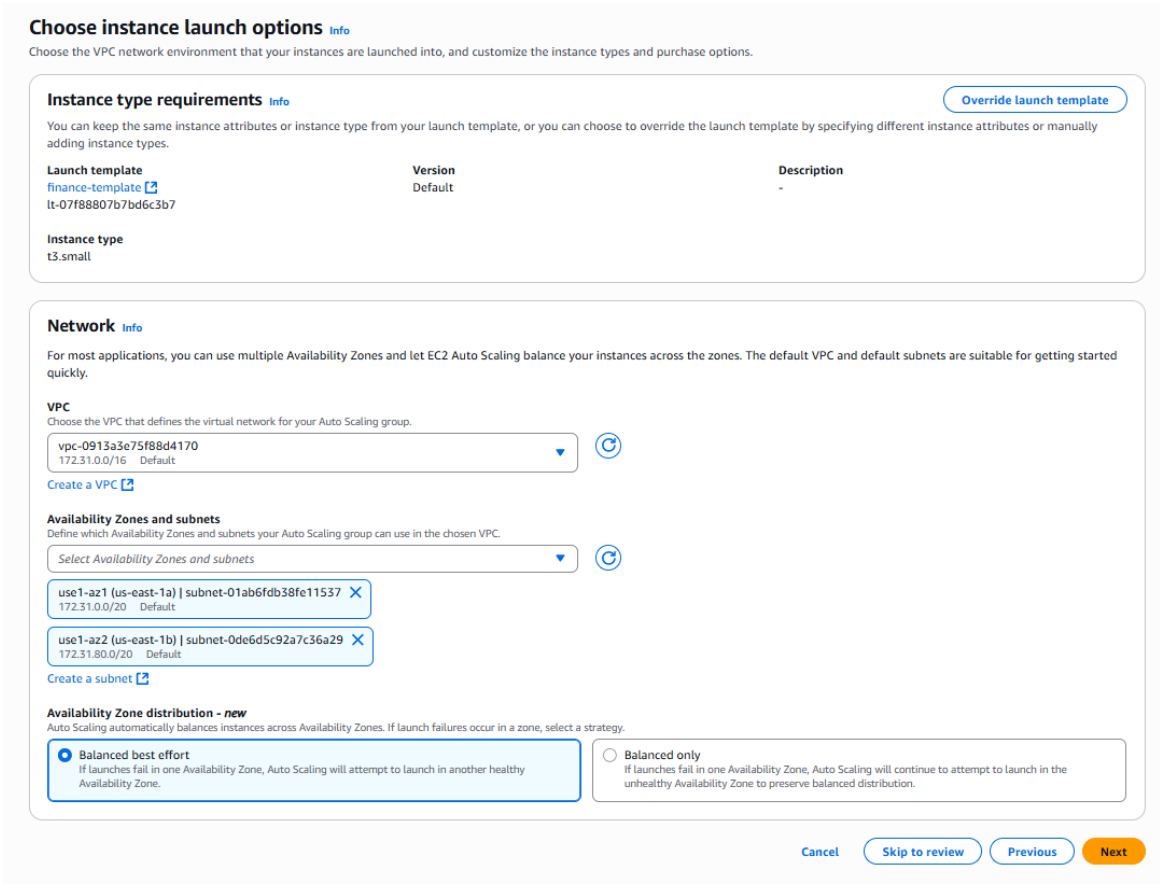
To guarantee continuous availability of financial applications, the compute layer is designed with Auto Scaling and multi-AZ deployment. The objective is to ensure resilience, scalability, and business continuity.

Implementation Steps：

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

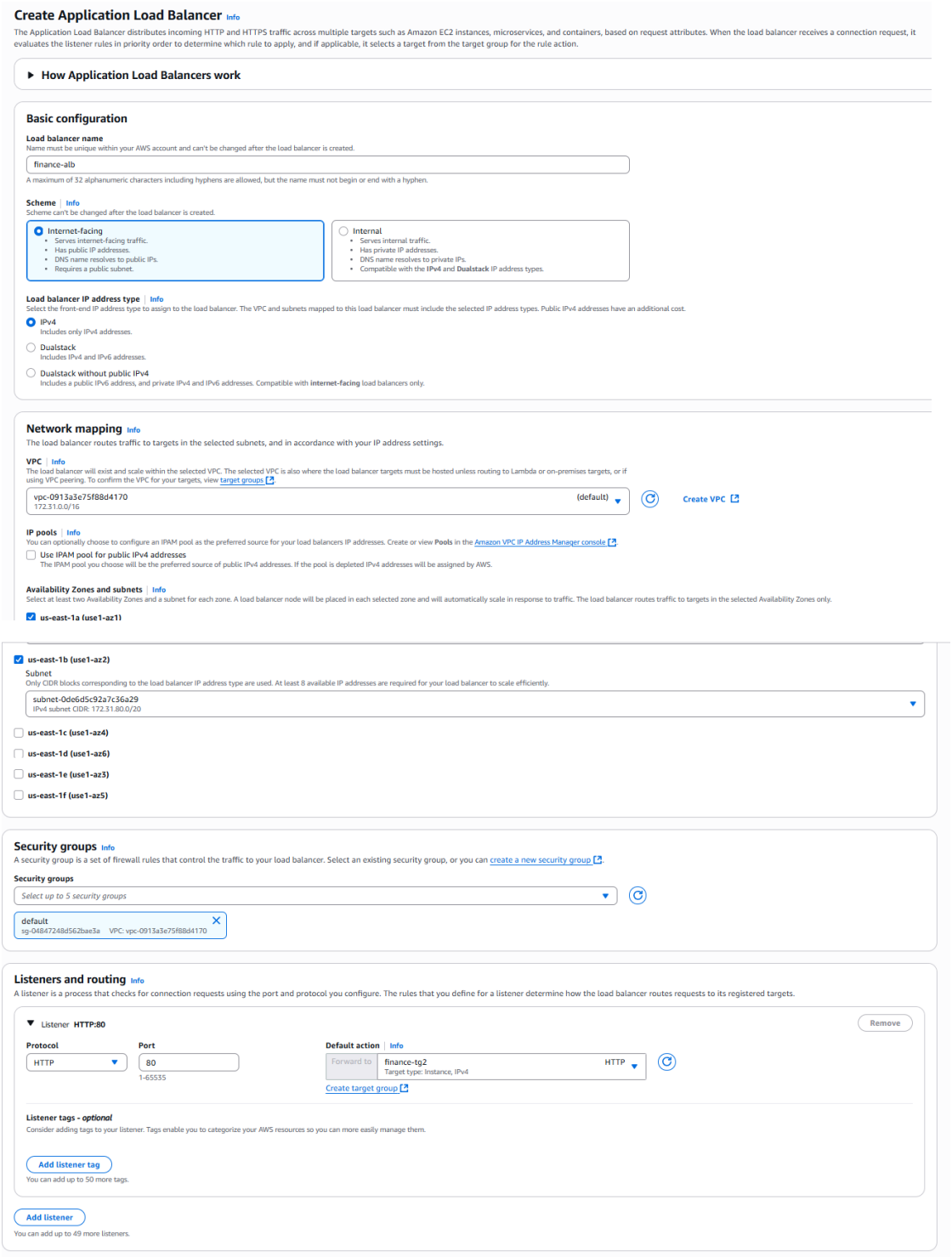
EC2 → Auto Scaling Groups → Create group





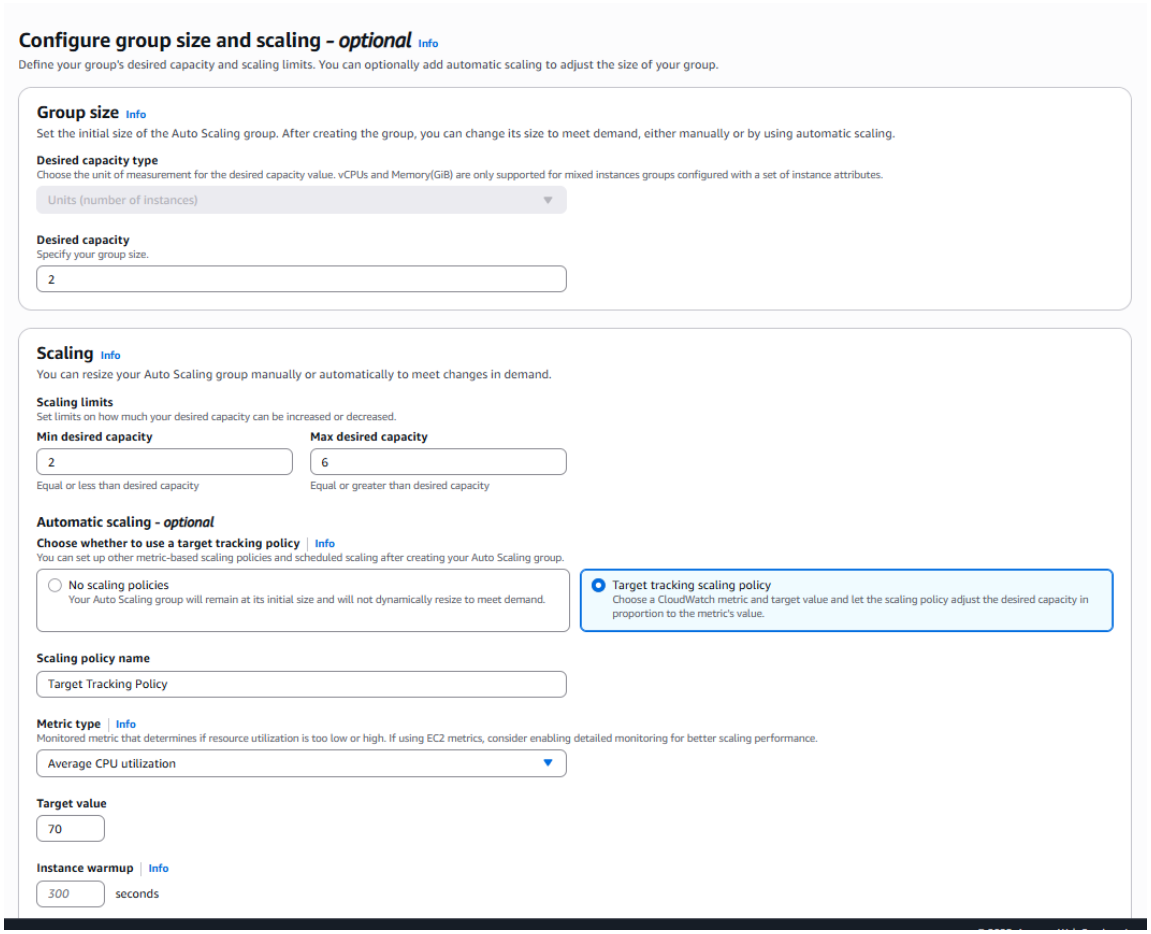
2. Configure ALB to distribute traffic evenly across instances.

EC2 → Load Balancers → Create ALB



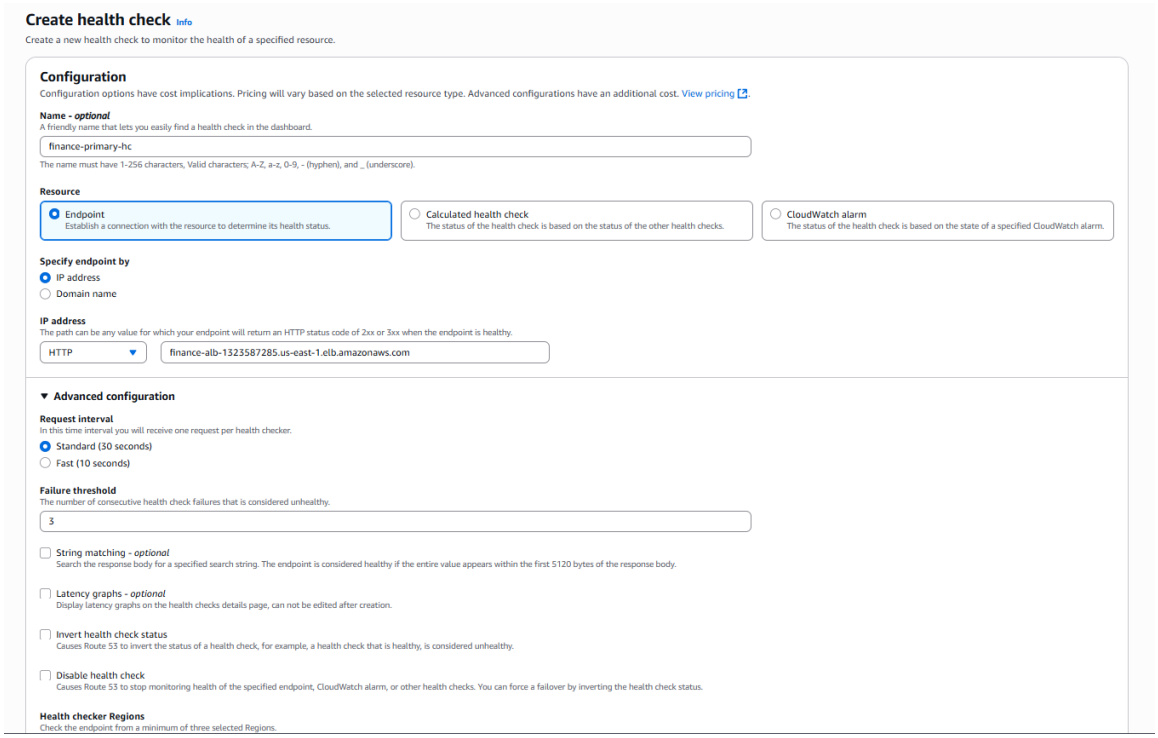
3. Add scaling policy (scale out if CPU >70%) for elasticity and cost optimization.

Auto Scaling Groups → Scaling policies



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

Route 53 → Health checks / Failover routing



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

CloudWatch → Alarms → Create alarm

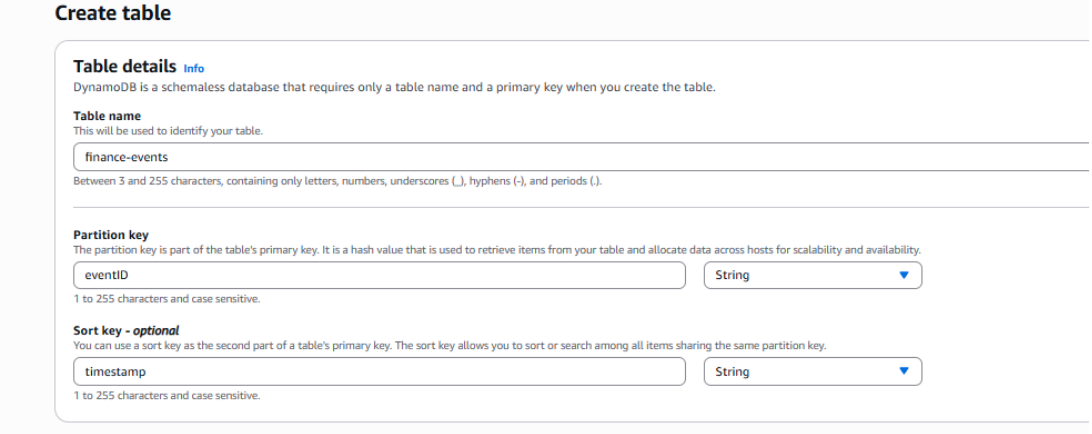
5.3 Amazon DynamoDB for High-Concurrency Events

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:

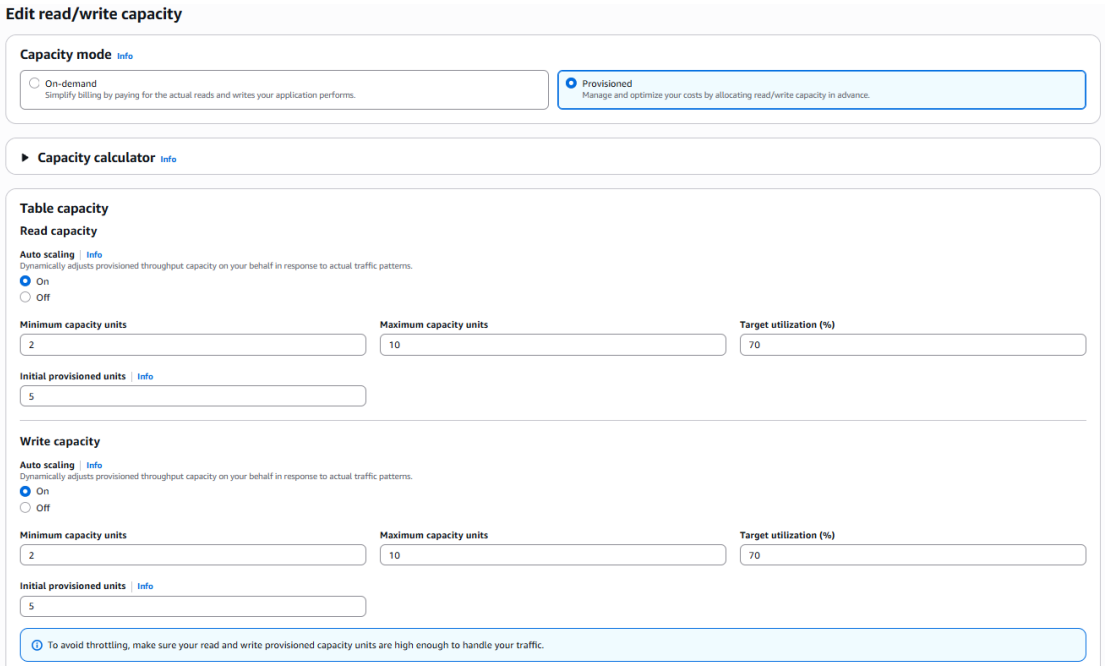
1. Create table finance-events with partition key eventID and sort key timestamp.

DynamoDB → Create table



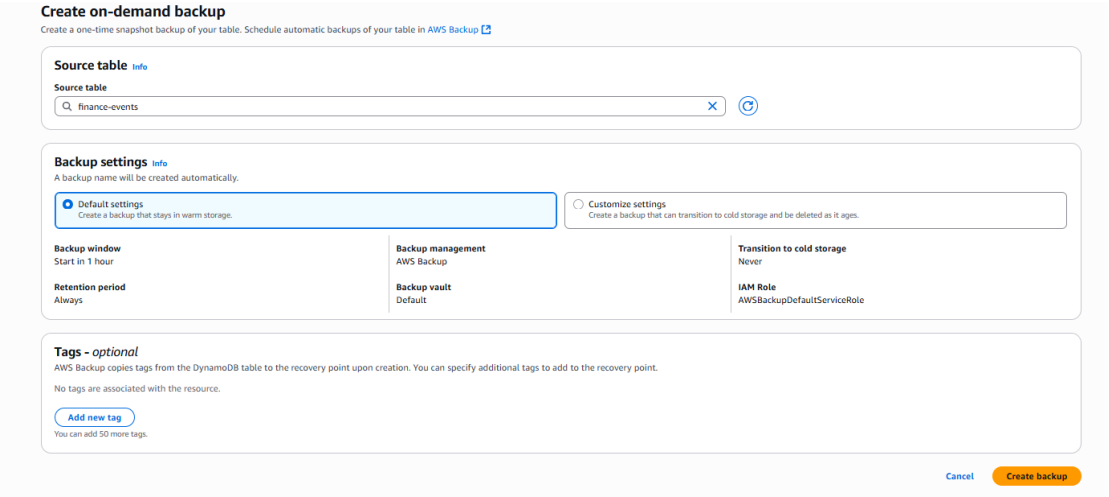
2. Enable Auto Scaling on RCUs/WCUs to handle concurrency.

Table → Capacity → Auto Scaling



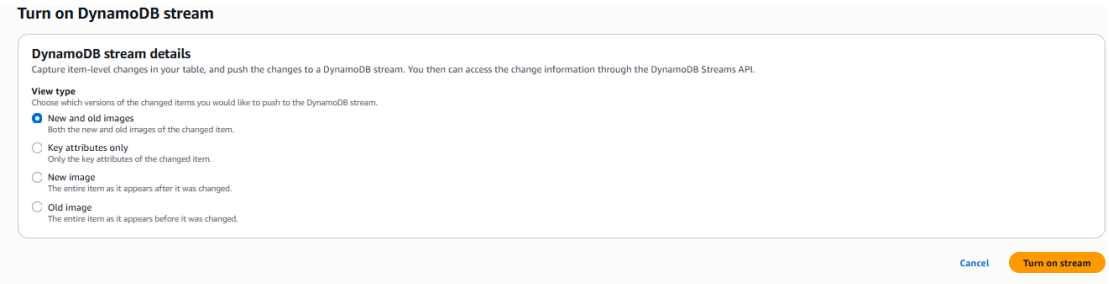
3. Enable PITR for 35-day full recovery window.

DynamoDB → Backups → Enable PITR



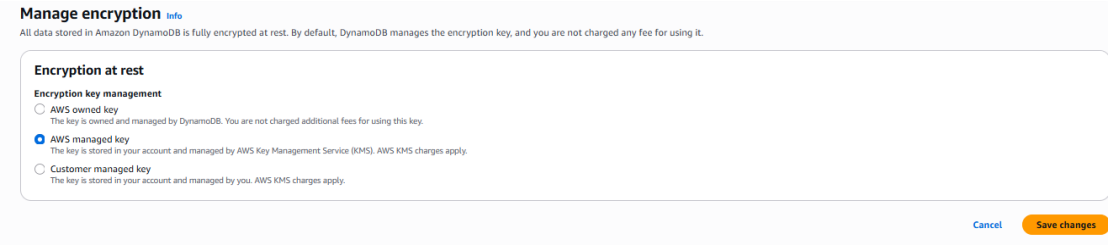
4. Enable DynamoDB Streams + integrate with Lambda for real-time audit pipelines.

DynamoDB → Tables → Streams



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

Table → Properties → Encryption



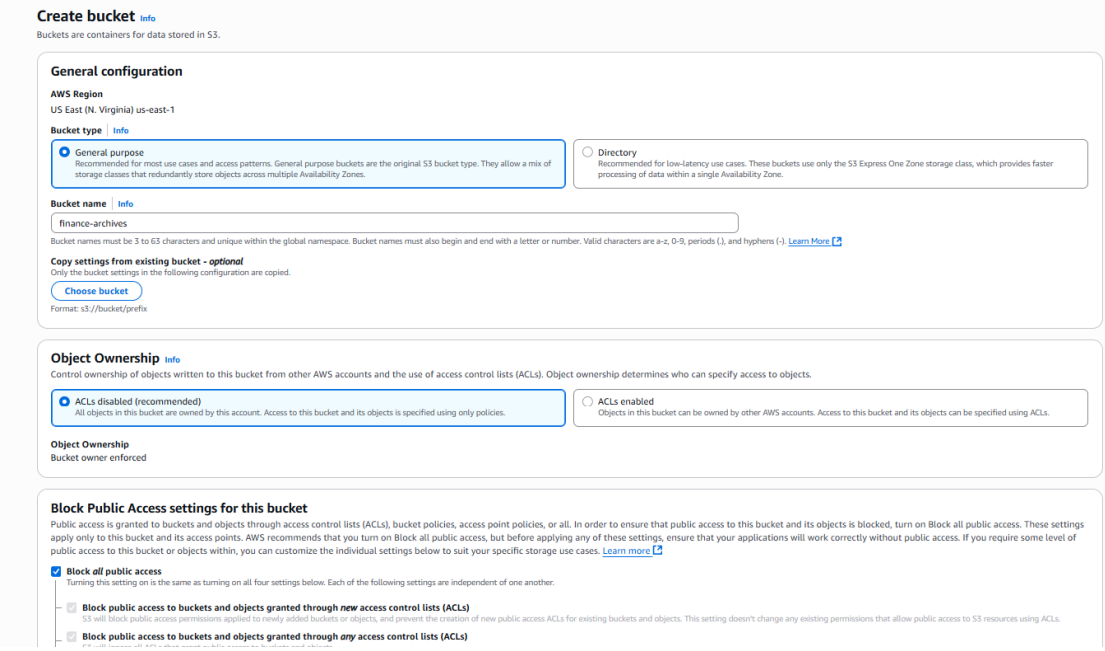
5.4 Amazon S3 Glacier for Long-Term Archives

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:

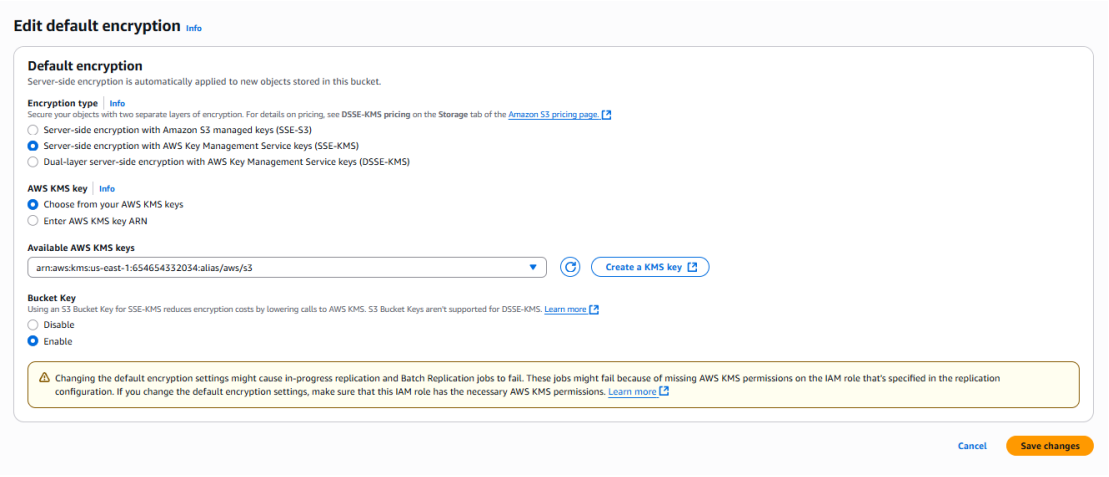
1. Create finance-archives bucket in us-east-1 with Block Public Access enabled.

   S3 → Create bucket



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

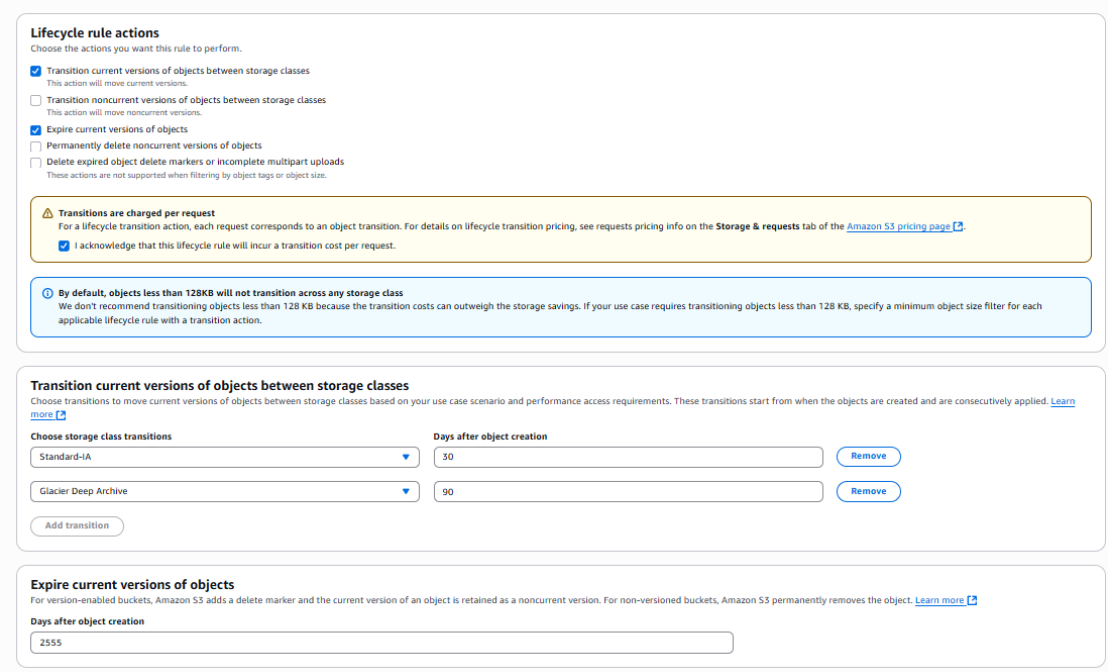
   Bucket → Properties → Default encryption



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

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

Bucket → Management → Lifecycle rules



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.