

Federal Home Loan Bank of San Francisco

Benefits Summary



Enhanced Security and Compliance



Increased Scalability



Automation and Efficiency



Optimized Resource Management

Industry

Banking, Financial Services

Location

United States

Challenge

The need to centralize security assessments for regular AWS audits across multiple accounts

Featured Services

AWS IAM, AWS Organizations, AWS Config, AWS Lambda, AWS S3, AWS KMS, Terraform

FHLBank San Francisco

About the Company

The Federal Home Loan Bank of San Francisco provides banking services to various financial institutions while ensuring compliance with regulatory standards.

CHALLENGE

The bank faced the challenge of centralizing security assessments to enable regular audits of AWS Resources across multiple AWS Accounts.

SOLUTION

nClouds proposed a solution utilizing Terraform to automate the deployment and configuration of AWS conformance packs, which contain Managed Rules for standard audits and Custom Rules for resources outside the Managed Rules' scope. In addition to using Terraform to automate infrastructure provisioning and manage configurations efficiently, the company leverages the following Amazon services:

AWS IAM: To manage access and permissions securely across AWS services

AWS Organizations: To centrally manage billing, control access, compliance, and security across AWS accounts

AWS Config: To enable detailed assessment, auditing, and evaluation of configurations of AWS resources

AWS Lambda: To run code in response to triggers such as changes in data or system state, which supports custom rule execution

AWS S3: To store audit results securely in an encrypted format using AWS KMS for enhanced data protection

AWS KMS: To provide centralized control over cryptographic keys used to encrypt stored audit results

RESULTS

From April 2020 to August 2022, nClouds implemented Terraform-driven security audits for the Federal Home Loan Bank of San Francisco. The firm set up three conformance packs based on CIS 1.4 Level 1, Security Best Practices, and Operational Best Practices, alongside a custom AWS Config rule for SSL policy audits on load balancers. All audit data was securely stored in a KMS-encrypted, customer-managed S3 bucket, ensuring compliance and enhancing data security management.

BENEFITS

There are many useful resources for creating the conformance pack containing Managed Rules. AWS various templates for reference so the conformance packs can be tailored to the client's specific needs. In addition, templating a Custom Rule as a Terraform module enabled the company to expand this structure for generating additional Custom Rules later.





AWS Account
FHLBSF-Master

Security Best Practices
Operational Best Practices
CIS 1.4

AWS Config > Conformance packs

Conformance packs

A conformance pack is a collection of AWS Config rules and remediation actions that can be deployed and monitored as a single entity in your AWS account. Learn more

Conformance packs

Filter rules by name or compliance status

OrgConformsPack-fhlbsf-aws-con...	OrgConformsPack-fhlbsf-aws-con...	OrgConformsPack-fhlbsf-aws-con...
Deployment status: Completed	Deployment status: Completed	Deployment status: Completed
91% Compliance score	7% Compliance score	89% Compliance score



AWS Account
FHLBSF-Master

Required Encryption
EC2 / EBS / ELB
Required Tags

Identity and Access Management (IAM)

Search IAM

Service control policies (SCPs)

Choose the name of an SCP to view a report of the services that member accounts can access. You can use this information to edit the SCP in the AWS Organizations console to deny access to services that you don't need. Learn more

Policy name	Attached to entities
FullAWSAccess	20+
aws-guardrails-rfctx	1
aws-guardrails-kuzHuo	1
aws-guardrails-TXQ6m	1
aws-guardrails-RFxtu	-
fhlbsf-org-sandbox-required-tags	1
aws-guardrails-eBauV	1
aws-guardrails-LaRoix	1
fhlbsf-org-sandbox-required-encryption	1
fhlbsf-org-sandbox-required-tags-elb	1
aws-managed-policy-for-iam-users	1



AWS Account
Config Rules: FHLBSF-Master
IAM Role: FHLBSF-ALL*

AWS Config Enabled
Outdated TLS/SSL Policies
SQS Encrypted

AWS Config > Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
fhlbsf-cis-1-13-iam-user-single-access-key-conformance-pack-ckpdy1hd	Not set	Process check	DETECTIVE	-
fhlbsf-cis-1-19-iam-expired-certificates-conformance-pack-ckpdy1hd	Not set	Process check	DETECTIVE	-
fhlbsf-cis-1-16-iam-policy-no-statements-with-admin-access-conformance-pack-ckpdy1hd	Not set	AWS managed	DETECTIVE	Compliant
fhlbsf-cis-1-12-iam-user-unused-credentials-check-conformance-pack-ckpdy1hd	Not set	AWS managed	DETECTIVE	Compliant
fhlbsf-cis-1-17-iam-policy-in-use-conformance-pack-ckpdy1hd	Not set	AWS managed	DETECTIVE	Compliant
OrgConfigRule-fhlbsf-custom-scp-lazy-balancing-outdated-tls-ssl-policies-ke3z9rgh	Not set	Custom Lambda	DETECTIVE	-
AWSControlTower_AWS-GR_EBS_OPTIMIZED_INSTANCE	Not set	AWS managed	DETECTIVE	-
AWSControlTower_AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	Not set	AWS managed	DETECTIVE	-
OrgConfigRule-fhlbsf-custom-scp-s3-buckets-required-tags-check-ghtmryzj	Not set	Custom Lambda	DETECTIVE	-
AWSControlTower_AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	Not set	AWS managed	DETECTIVE	-



AWS Account
Insights: FHLBSF-ALL*

FHLBSF CIS Benchmarks
FHLBSF Operational Best Practices
FHLBSF Organization Config Custom Rules
FHLBSF Security Best Practices
fhlbsf-cis-1-1
fhlbsf-cis-1-2

Security Hub > Insights

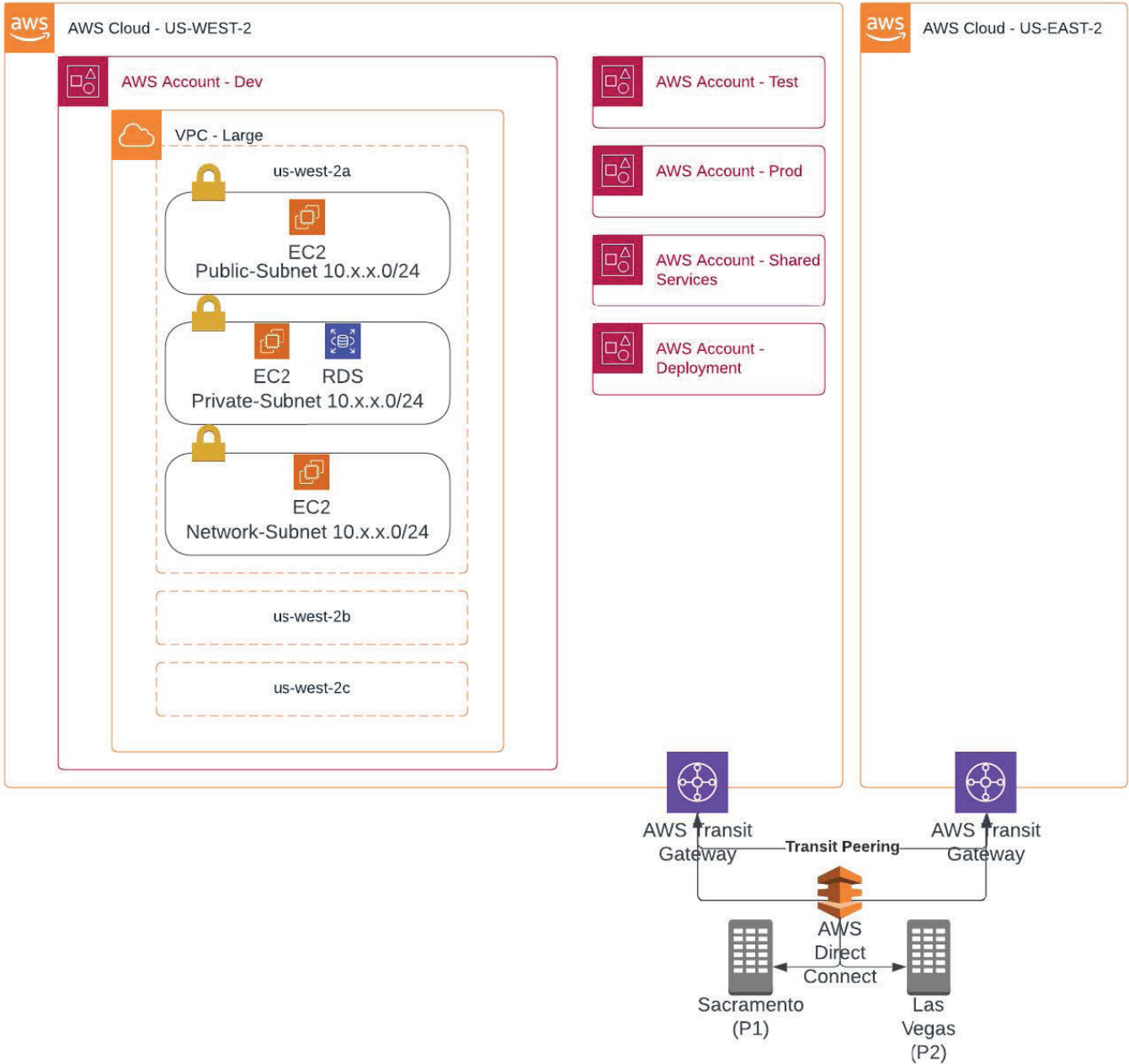
Manage all of your findings from a single Region. With finding aggregation, you can use a single aggregation Region to view and update findings from multiple linked Regions. Administrator accounts configure the aggregation. Security Hub replicates findings and finding updates for all of the member accounts in the linked Regions.

Security Hub > Insights

Insights (31)

Filter Insights: Custom insights 31 matches

FHLBSF CIS Benchmarks Custom insight 0-day Finding trend	FHLBSF Operational Best Practices Custom insight 0-day Finding trend	FHLBSF Organization Config Custom Rules Custom insight 0-day Finding trend
FHLBSF Security Best Practices Custom insight 0-day Finding trend	fhlbsf-cis-1-1 Custom insight 0-day Finding trend	fhlbsf-cis-1-2 Custom insight 0-day Finding trend



About nClouds

nClouds is a certified, award-winning provider of AWS and DevOps consulting and implementation services. We partner with our customers as extensions of their teams to build and manage modern infrastructure solutions that deliver innovation faster. We leap beyond the status quo.

Copyright © 2024 nClouds, Inc. All rights reserved