AWS Security Infrastructure Analysis Report

Analysis Date: 2025-10-01 19:00:28

Infrastructure Path: ..\infra

Total Findings: 28

HIGH SEVERITY (5 findings)

File	Line	Issue	Description
AwsIacSecurityStack.java	104	SSH Access from Anywhere	SSH port 22 is open to all IP addresses (0.0.0.0/0)
AwsIacSecurityStack.java	113	SSH Access from Anywhere	SSH port 22 is open to all IP addresses (0.0.0.0/0)
AwsIacSecurityStack.java	122	SSH Access from Anywhere	SSH port 22 is open to all IP addresses (0.0.0.0/0)
deploy.bat	75	Automatic Deployment Approval	CDK deployment without manual approval
deploy.sh	67	Automatic Deployment Approval	CDK deployment without manual approval

MEDIUM SEVERITY (9 findings)

File	Line	Issue	Description
AwsIacSecurityStack.java	104	HTTP Access from Anywhere	HTTP port 80 is open to all IP addresses
AwsIacSecurityStack.java	113	HTTP Access from Anywhere	HTTP port 80 is open to all IP addresses
AwsIacSecurityStack.java	122	HTTP Access from Anywhere	HTTP port 80 is open to all IP addresses
AwsIacSecurityStack.java	104	HTTPS Access from Anywhere	HTTPS port 443 is open to all IP addresses
AwsIacSecurityStack.java	113	HTTPS Access from Anywhere	HTTPS port 443 is open to all IP addresses

AwsIacSecurityStack.java	122	HTTPS Access from Anywhere	HTTPS port 443 is open to all IP addresses
AwsIacSecurityStack.java	92	Unrestricted Outbound Access	Security group allows all outbound traffic
AwsIacSecurityStack.java	67	Resources in Public Subnet	EC2 instance placed in public subnet
AwsIacSecurityStack.java	163	Resources in Public Subnet	EC2 instance placed in public subnet

LOW SEVERITY (8 findings)

File	Line	Issue	Description
AwsIacSecurityStack.java	134	EC2 Service Principal	EC2 instance has IAM role attached
AwsIacSecurityStack.java	18	Limited Monitoring	No explicit CloudWatch monitoring configuration
AwsIacSecurityStack.java	18	Limited Monitoring	No explicit CloudWatch monitoring configuration
AwsIacSecurityStack.java	145	Limited Monitoring	No explicit CloudWatch monitoring configuration
AwsIacSecurityStack.java	146	Limited Monitoring	No explicit CloudWatch monitoring configuration
AwsIacSecurityStack.java	147	Limited Monitoring	No explicit CloudWatch monitoring configuration
AwsIacSecurityStack.java	147	Limited Monitoring	No explicit CloudWatch monitoring configuration
AwsIacSecurityStack.java	149	Limited Monitoring	No explicit CloudWatch monitoring configuration

INFO SEVERITY (6 findings)

File	Line	Issue	Description
AwsIacSecurityStack.java	138	AWS Managed Policies	Using AWS managed policies
AwsIacSecurityStack.java	149	AWS Managed Policies	Using AWS managed policies
cdk.json	1	Secret usage checking enabled	CDK context setting: @aws-cdk/core:checkSecretUsage
cdk.json	1	IAM policy minimization enabled	CDK context setting: @aws-cdk/aws-iam:minimizePolicies
cdk.json	1	Default security group restriction enabled	CDK context setting: @aws-cdk/aws-ec2:restrictDefaultSecurityGroup
cdk.json	1	EFS anonymous access denied	CDK context setting: @aws-cdk/aws-efs:denyAnonymousAccess

Security Hardening Recommendations

• Network Security: Implement VPC Flow Logs, use private subnets, restrict SSH access

• Access Control: Implement least privilege IAM policies, enable MFA

• Monitoring: Enable CloudTrail, CloudWatch alarms, GuardDuty

• Data Protection: Enable encryption at rest, use AWS KMS

• Infrastructure: Use Systems Manager, implement security baselines