InfViz AWS Report
AuroraPinpointStack.template.json

Executive Summary

Introduction

This is a generated report for AWS cloudformation file
AuroraPinpointStack.template.json. Data used within this report was captured on
3/17/2023, 5:08:23 PM. The report's objective is to summarise the configuration.

Resources

Summary of the services being used are listed below

- Budgets
- IAM
- Config
- VPC
- NatGateway
- InternetGateway
- SecretsManager
- KMS
- S3
- RDS
- Serverless
- Pinpoint
- SNS
- CloudWatch
- CDK

Costing

Estimated monthly cost of the environment is $NaN USD

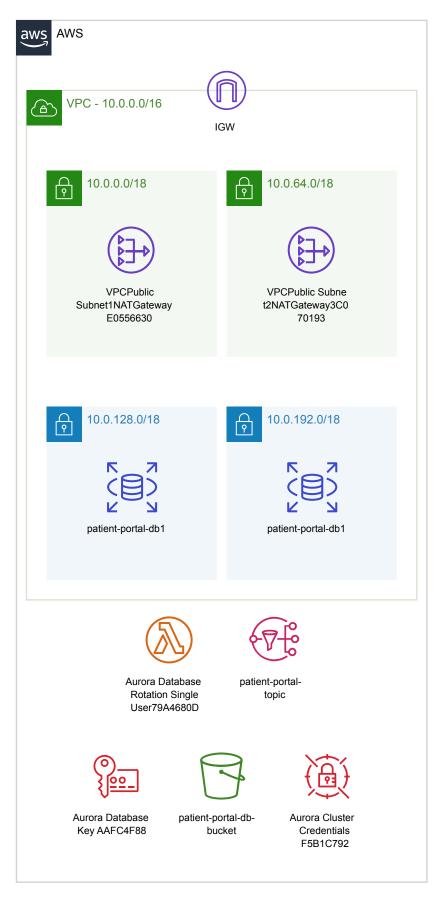| Service	Cost	%
NAT GW	$70.38	NaN%
S3	$0.23	NaN%

- Pricing is based on us-east-1
- Pricing is in USD
- This is an estimate only

Go to costing section to see detailed breakdown.

Hosting Diagram

AWS

VPC - 10.0.0.0/16

IGW

10.0.0.0/18

VPCPublic
Subnet1NATGateway
E0556630

10.0.64.0/18

VPCPublic Subne
t2NATGateway3C0
70193

10.0.128.0/18

patient-portal-db1

10.0.192.0/18

patient-portal-db1

Aurora Database
Rotation Single
User79A4680D

patient-portal-
topic

Aurora Database
Key AAFC4F88

patient-portal-db-
bucket

Aurora Cluster
Credentials
F5B1C792

rendered using InfViz v3.0

Nodes

Label	Type	Info
AuroraDatabaseKeyAAFC4F88	KMS-Key	No details
VPCPublicSubnet1NATGatewayE0556630	EC2-NatGateway	No details
VPCPublicSubnet2NATGateway3C070193	EC2-NatGateway	No details
patient-portal-db1	RDS-DBInstance	RDS DBInstanceClass : db.t3.small Engine : aurora-mysql EngineVersion : 5.7.12
patient-portal-db-bucket	S3-Bucket	S3 BucketEncryption: Yes
patient-portal-topic	SNS-Topic	SNS Subscriptions : 1 email
AuroraClusterCredentialsF5B1C792	SecretsManager-Secret	No details

Connectivity Table

Connections

From	To	Access
AuroraDatabaseRotationSingleUserSecurityGroup420EE692	Rds - AuroraDatabase5475D328	{'Fn::GetAtt': ['AuroraDatabase5475D328', 'Endpoint.Port']} tcp,
Rds - AuroraDatabase5475D328	Secret - AuroraClusterCredentialsF5B1C792	uses,

Network

VPC (VPCB9E5F0B4)

Key	Value
CidrBlock	10.0.0.0/16
EnableDnsHostnames	True
EnableDnsSupport	True
InstanceTenancy	default

Subnet 10.0.0.0/18 Routes (10.0.0.0/18)

Id	Destination Cidr Block	Via
VPCPublicSubnet1DefaultRoute91CEF279	0.0.0.0/0	VPCIGWB7E252D3

Subnet 10.0.64.0/18 Routes () (10.0.64.0/18)

Id	Destination Cidr Block	Via
VPCPublicSubnet2DefaultRouteB7481BBA	0.0.0.0/0	VPCIGWB7E252D3

Subnet 10.0.128.0/18 Routes (10.0.128.0/18)

Id	Destination Cidr Block	Via
VPCPrivateSubnet1DefaultRouteAE1D6490	0.0.0.0/0	VPCPublicSubnet1NATGatewayE0556630

Subnet 10.0.192.0/18 Routes () (10.0.192.0/18)

Id	Destination Cidr Block	Via
VPCPrivateSubnet2DefaultRouteF4F5CFD2	0.0.0.0/0	VPCPublicSubnet2NATGateway3C070193

RDS Databases

patient-portal-db1 (RDS-DBInstance)

Key	Value
DBClusterIdentifier	AuroraDatabase5475D328
DBInstanceClass	db.t3.small
DBInstanceIdentifier	patient-portal-db1
DBSubnetGroupName	AuroraDatabaseSubnets5EA8274A
DeleteAutomatedBackups	True
Engine	aurora-mysql

patient-portal-db (RDS-DBCluster)

Key	Value
AssociatedRoles	{'RoleArn': {'Fn::GetAtt': ['AuroraDatabaseS3ExportRoleF3D2F2DC', 'Arn']}},
BackupRetentionPeriod	35
CopyTagsToSnapshot	True
DatabaseName	patient-portal-db
DBClusterParameterGroupName	AuroraDatabaseClusterParameterGroup7A9ACBA0
DBSubnetGroupName	AuroraDatabaseSubnets5EA8274A
DeletionProtection	True
EnableCloudwatchLogsExports	error, general, audit,
EnableIAMDatabaseAuthentication	True
Engine	aurora-mysql
EngineVersion	8.0.mysql_aurora.3.03.0
KmsKeyId	AuroraDatabaseKeyAAFC4F88
MasterUsername	admin
MasterUserPassword	******
PreferredBackupWindow	01:00-02:00
PreferredMaintenanceWindow	sun:01:00-sun:02:00
StorageEncrypted	True

Key	Value
VpcSecurityGroupIds	DbSecurityGroupE9D701AD,

RDS-DBClusterParameterGroup

Id	Description	Family	Parameters
AuroraDatabase ClusterParameter Group7A9ACBA0	Cluster parameter group for aurora-mysql8.0	aurora-mysql8.0	{'aws_default_s3_role': {'Fn::GetAtt': ['AuroraDatabaseS3ExportRoleF3D2F2DC', 'Arn']}, 'Aws_default_ s3_role': {'Fn::GetAtt': ['AuroraDatabaseS3ExportRoleF3D2F2DC', 'Arn']}}

Messaging Services

patient-portal-topic (SNS-Topic)

Key	Value
DisplayName	patient-portal-topic
TopicName	patient-portal-topic

SNS-Subscription

Id	Protocol	Topic Arn	Endpoint
PinpointTopicfromemailcom37121691	email	PinpointTopic9A4D8BF5	from@email.com

SNS-TopicPolicy

Id	Policy Document	Topics
PinpointTopic PolicyA91BFE 2F	{'Statement': [{'Action': 'SNS:Publish', 'Effect': 'Allow', 'Principal': {'Service': 'pinpoint.amazo naws.com'}, 'Resource': {'Ref': 'PinpointTopic9A4D8BF5'}, 'Sid': '0'}], 'Version': '2012-10-17'}	PinpointTopic9 A4D8BF5,

Storage

patient-portal-db-bucket (S3-Bucket)

Key	Value
BucketEncryption	{'ServerSideEncryptionConfiguration': [{'ServerSideEncryptionByDefault': {'KMSMasterKeyID': {'Fn::GetAtt': ['AuroraDatabaseKeyAAFC4F88', 'Arn']}, 'SSEAlgorithm': 'aws:kms'}}]}
BucketName	patient-portal-db-bucket

Other Services

CDKMetadata (CDK-Metadata) **Condition False - Not Deployed**

Key	Value
Condition	CDKMetadataAvailable
Analytics	v2:deflate64:H4sIAAAAAAAA/31TTW/bMAz9Lb0r2pICw3ZM0q0Iim2GE/Q60DLrqLElQR8NAsP/fZSU2EYL9GI+PIIi9Uiv+Lcf/OsdnN1C1KdFKyve7z2IEyPqqX1+FukHv+PZFbRJkEjrel7pFRlyyhW6luEQ3o4EJrV5kw3uitgkGC15qVaLQtkbLxkAZWhwYihXvn42I/HOxZUWo6KJ9qBQVJG5CpQ4eD1Dl8pmfuLVzWshUakyO4OeuiOYP+EfweIYLK6x8IzhdvFMeLeFbQu7k6q09KXLsUHm2RxGs9JdHq4NJPXxK7FRj0bmBORSWhOxAQYOWNE7+NT+ibA5gSeRZvTHhQ6TUPr10L45Yh9s83nElOh2swGlG75h8+e3cwE6d4/0TptRo1q0EF50E6B33vN8Eccq9ZzQwW9OpB/BQgcNtGxyJybK4oy4PmzlRgIUOKW0Wvx78JJJSdnXlelKDFcbSMsTdj6DF57i10VQ38V1Ai+htqiBmpjJbKX3OZZU9TuQRuZNi6D9J1kmrvUtxNWmttezX1a9laH+gxeHKME7lhpsHVqdHTWLdgui0hgGMaxRO5v8CYkNX+DoU6b+ZSuf0otcy2la+Sv7svb8jtfrvjy7tVJubBBedkhL7P9D/sA/mnTAwAA

AuroraClusterCredentialsF5B1C792 (SecretsManager-Secret)

Key	Value
Description	adminAuroraClusterCrendetials
GenerateSecretString	{'ExcludeCharacters': '"@/\ \", 'GenerateStringKey': 'password', 'PasswordLength': 30, 'SecretStringTemplate': '{"username":admin}'}
Name	adminAuroraClusterCredentials

DbSecurityGroupE9D701AD (EC2-SecurityGroup)

Key	Description	Ip Protocol	Obj	From Port	To Port
GroupName	patient-portal-db-sg				
groupDescription	Security Group for patient-portal-db				
Egress	Allow all outbound traffic by default	-1	0.0.0.0/0		
Ingress	from AuroraPinpointStackAuroraDatabaseRotationSingleUserSecurityGroupDF202B11:{IndirectPort}	tcp		AuroraDatabase5475D328	AuroraDatabase5475D328

AuroraDatabaseRotationSingleUserSecurityGroup420EE692 (EC2-SecurityGroup)

Key	Description	Ip Protocol	Obj
groupDescription	AuroraPinpointStack/AuroraDatabase/RotationSingleUser/SecurityGroup		
Egress	Allow all outbound traffic by default	-1	0.0.0.0/0

Budgets-Budget

Id	Budget	Notifications With Subscribers
Budget	{'BudgetLimit': {'Amount': 500, 'Unit': 'USD'}, 'BudgetName': 'patient-portal-db', 'BudgetType': 'CO ST', 'CostFilters': {'Service': ['AmazonRDS']}, 'TimeUnit': 'MONTHLY'}	{'Notification': {'ComparisonOperator': 'GREATER_THAN', 'NotificationType': 'ACTUAL', 'Threshold': 5 00, 'ThresholdType': 'PERCENTAGE'}, 'Subscribers': [{'Address': 'support@email.com', 'SubscriptionTy pe': 'EMAIL'}]},

CloudWatch-Alarm

Id	Comparison Operator	Evaluation Periods	Alarm Description	Dimensions	Metric Name	Namespace	Period	Statistic	Threshold
DashboardMyCpuUtilization Alarm 284DC6EF	GreaterThanOrEqualToThreshold	3	Alarm when CPU exceeds 90%	{'Name': 'DBClusterIdentifier', 'Value': {'Ref': 'AuroraDatabase5475D328'}},	CPUUtilization	AWS/RDS	300	Average	90

CloudWatch-Dashboard

Id	Dashboard Body	Dashboard Name
Dashboard7A714131	{"widgets":[{"type":"metric","width":6,"height":6,"x":0,"y":0,"properties":{"view":"timeSeries","title":"DB Connections","region":"AWS","metrics":[["AWS/RDS","DatabaseConnections","DBClusterIdentifier","AuroraDatabase5475D328"]],"yAxis":{}}},{"type":"metric","width":6,"height":6,"x":6,"y":0,"propert	patient-portal-dashboard

Config-ConfigRule

Id	Source	Config Rule Name	Description	Input Parameters	Maximum Execution Frequency	Scope

Id	Source	Config Rule Name	Description	Input Parameters	Maximum Execution Frequency	Scope
ConfigCompliance Soc2 Soc2Rule EC2Instance Security GroupIngr essRule s8F328 E52	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemCh angeNotification'}], 'SourceIdentifier': 'AWS_EC2_SECURI TY_GROUP_INGRE SS_RULES'}	Soc2Rule-EC2 Instance Security Group Ingress Rules	Checks that the security groups attached to EC2 instances allow only necessary ingress traffic	{'portNumber': 80, 'protocol': 'TCP', 'allowedCIDRs': '0.0.0.0/0', 'PortNumber': 80, 'Protocol': 'TC P', 'AllowedCIDRs': '0.0.0.0/0'}	TwentyFour_ Hours	{'ComplianceR esourceId': 'AWS::EC2::In stance', 'ComplianceR esourceTypes': ['AWS::EC2::In stance']}
ConfigC omplian ceSoc2 Soc2Ru leS3Buc ketPubli cAccess AE7C92 7A	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemCh angeNotification'}], 'SourceIdentifier': 'AWS_S3_BUCKET_ PUBLIC_ACCESS'}	Soc2Rule-S3 Bucket Public Access	Checks that S3 buckets do not allow public access	{'maxAccessKeyAge' : 60, 'MaxAccessKeyAge': 60}	TwentyFour_ Hours	{'ComplianceR esourceId': 'AWS::S3::Buc ket', 'ComplianceR esourceTypes': ['AWS::S3::Bu cket']}
ConfigC omplian ceSoc2 Soc2Ru leRDSS napshot Encrypti on4227 B974	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemCh angeNotification'}], 'SourceIdentifier': 'AWS_RDS_SNAPSH OT_ENCRYPTION'}	Soc2Rule-RDS Snapshot Encryption	Checks that RDS snapshots are encrypted	{'maxAccessKeyAge' : 60, 'MaxAccessKeyAge': 60}	TwentyFour_ Hours	{'ComplianceR esourceId': 'AWS::RDS::D BSnapshot', 'ComplianceR esourceTypes': ['AWS::RDS::D BSnapshot'] }
ConfigC omplian ceHipaa HipaaR uleEBS Volume Encrypti onD312 9E7A	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemCh angeNotification'}], 'SourceIdentifier': 'AWS_EBS_VOLUME _ENCRYPTION'}	HipaaRule -EBS Volume Encryption	Checks that EBS volumes attached to EC2 instances are encrypted	{}	TwentyFour_ Hours	{'ComplianceR esourceId': 'AWS::EC2::Vo lume', 'ComplianceR esourceTypes': ['AWS::EC2::V olume']}
ConfigC omplian ceHipaa HipaaR uleRDS Encrypti on3755 ADAB	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemCh angeNotification'}], 'SourceIdentifier': 'AWS_RDS_ENCRYP TION'}	HipaaRule -RDS Encryption	Checks that RDS instances are encrypted	{}	TwentyFour_ Hours	{'ComplianceR esourceId': 'AWS::RDS::D BInstance', 'ComplianceR esourceTypes': ['AWS::RDS::D BInstance'] }
ConfigC omplian ceHipaa HipaaR uleS3B ucketLo	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemCh	HipaaRule -S3 Bucket Logging	Checks that S3 buckets have logging enabled	{}	TwentyFour_ Hours	{'ComplianceR esourceId': 'AWS::S3::Buc ket', 'ComplianceR esourceTypes'

Id	Source	Config Rule Name	Description	Input Parameters	Maximum Execution Frequency	Scope
ggingBD10544C	angeNotification'}], 'SourceIdentifier': 'AWS_S3_BUCKET_LOGGING'}					: ['AWS::S3::Bucket']}
ConfigComplianceGdprMyGdprRuleEC2InstanceMetadataProtection2E5758A4	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemChangeNotification'}], 'SourceIdentifier': 'AWS_EC2_METADATA_PROTECTION'}	MyGdprRule-EC2Instance Metadata Protection	Checks that EC2 instances have metadata protection enabled	{'maxAccessKeyAge': 60, 'MaxAccessKeyAge': 60}	TwentyFour_Hours	{'ComplianceResourceId': 'AWS::EC2::Instance', 'ComplianceResourceTypes': ['AWS::EC2::Instance']}
ConfigComplianceGdprMyGdprRuleS3BucketEncryptionFAEC8B30	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemChangeNotification'}], 'SourceIdentifier': 'AWS_S3_BUCKET_ENCRYPTION'}	MyGdprRule-S3 Bucket Encryption	Checks that S3 buckets have server-side encryption enabled	{'maxAccessKeyAge': 60, 'MaxAccessKeyAge': 60}	TwentyFour_Hours	{'ComplianceResourceId': 'AWS::S3::Bucket', 'ComplianceResourceTypes': ['AWS::S3::Bucket']}
ConfigComplianceGdprMyGdprRuleLambdaFunctionLogging634BD72E	{'Owner': 'AWS', 'SourceDetails': [{'EventSource': 'aws.config', 'MessageType': 'ConfigurationItemChangeNotification'}], 'SourceIdentifier': 'AWS_LAMBDA_FUNCTION_LOGGING'}	MyGdprRule-LambdaFunction Logging	Checks that Lambda functions have logging enabled	{'maxAccessKeyAge': 60, 'MaxAccessKeyAge': 60}	TwentyFour_Hours	{'ComplianceResourceId': 'AWS::Lambda::Function', 'ComplianceResourceTypes': ['AWS::Lambda::Function ']}

Config-ConfigurationRecorder

Id	Role ARN	Name	Recording Group
ConfigComplianceSoc2ConfigCompliance11B85F4D	ConfigRoleF94F46B6	ConfigCompliance	{'AllSupported': True, 'IncludeGlobalResourceTypes': True}
ConfigComplianceHipaaConfigComplianceC5459902	ConfigRoleF94F46B6	ConfigCompliance	{'AllSupported': True, 'IncludeGlobalResourceTypes': True}
ConfigComplianceGdprConfigCompliance81C22DCD	ConfigRoleF94F46B6	ConfigCompliance	{'AllSupported': True, 'IncludeGlobalResourceTypes': True}

KMS-Alias

Id	Alias Name	Target Key Id

Id	Alias Name	Target Key Id
AuroraDatabaseKeyAliasF8206C67	alias/patient-portal-db	AuroraDatabaseKeyAAFC4F88

KMS-Key

Id	Key Policy	Enable Key Rotation
AuroraDatabaseKeyAAFC4F88	{'Statement': [{'Action': 'kms:*', 'Effect': 'Allow', 'Principal': {'AWS': {'Fn::Join': ['', ['arn:' , {'Ref': 'AWS::Partition'}, ':iam::', {'Ref': 'AWS::AccountId'}, ':root']]}}, 'Resource': '*'}], 'Version': '2012-10-17'}	True

Pinpoint-App

Id	Name
PinpointPinpointApp8202AE5C	patient-portal

SecretsManager-ResourcePolicy

Id	Resource Policy	Secret Id
AuroraClusterCredentialsPolicy231C664E	{'Statement': [{'Action': 'secretsmanager:DeleteSecret', 'Effect': 'Deny', 'Principal': {'AWS': {'Fn ::Join': ['', ['arn:', {'Ref': 'AWS::Partition'}, ':iam::', {'Ref': 'AWS::AccountId'}, ':root']]}}, 'Resource': '*'}], 'Version': '2012-10-17'}	AuroraClusterCredentialsF5B1C792

SecretsManager-RotationSchedule

Id	Secret Id	Rotation Lambda ARN	Rotation Rules
AuroraClusterCredentialsAttachmentRotationSchedule784F4B66	AuroraClusterCredentialsAttachment50AD3528	AuroraDatabaseRotationSingleUser79A4680D	{'AutomaticallyAfterDays': 30}

SecretsManager-SecretTargetAttachment

Id	Secret Id	Target Id	Target Type
AuroraClusterCredentialsAttachment50AD3528	AuroraClusterCredentialsF5B1C792	AuroraDatabase5475D328	AWS::RDS::DBCluster

Serverless-Application

Id	Location	Parameters

Id	Location	Parameters
AuroraD atabase Rotation SingleU ser79A4 680D	{'ApplicationId': {'Fn::FindInMap': ['AuroraDatabaseRotationSingleUserSARMapping2 AF3849D', {'Ref': ' AWS::Partition'}, 'applicationId']}, 'SemanticVersion': {'Fn::FindInMap': ['AuroraDatabaseRotationSi ngleUserSARMapping2AF3849D', {'Ref': 'AWS::Partition'}, 'semanticVersion']}}	{'endpoint': {'Fn::Join': ['', ['https://secretsmanager.', {'Ref': 'AWS::Region'}, '.', {'Ref': 'AWS ::URLSuffix'}]]}, 'functionName': 'AuroraPinpointStackAuroraDatabaseRotationSingleUse r202BDA1E', 'vp cSubnetIds': {'Fn::Join': ['', [{'Ref': 'VPCPrivateSubnet1Subnet8BCA10E0'}, ',', {'Ref': 'VPCPrivate