dataphilic.io

Managed healthcare cloud

Healthcare Security

Best practices in cloud

Best Practices in Cloud

- Business Associate agreement
- Policies, governance and ownership
- Coverage for Security policy
- Establish cloud center of excellence
- Best practices in implementation
  - Accounts, network and security policy
- Automation
  - Infrastructure as a code
  - Evidence collection
- Choice of offerings

Who owns what?

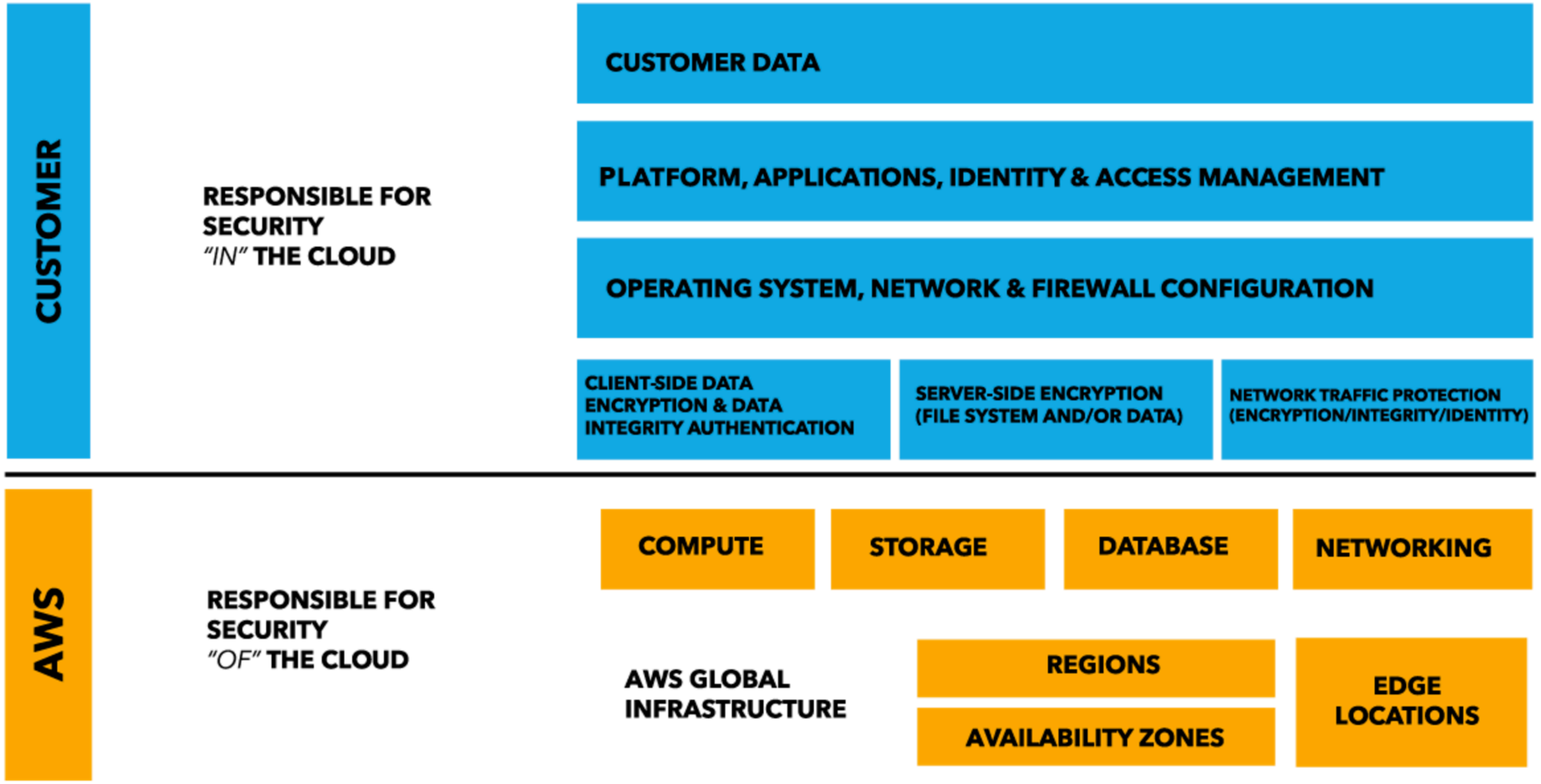
Customer

- Data
- Application
- Networking services
- Computing services
- Policies, Procedures, Awareness

Cloud service provider

- Internal Network
- Perimeter
- Physical

Map of shared responsibilities



CUSTOMER

RESPONSIBLE FOR SECURITY *"IN"* THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)

AWS

RESPONSIBLE FOR SECURITY *"OF"* THE CLOUD

COMPUTE

STORAGE

DATABASE

NETWORKING

AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Source: Amazon Web Services

BAA

Obtain Business Associate Agreement

- All good cloud service providers agree to BAA with customer

Service coverage for Cloud Security Policy

1. Confidentiality
    1. Encryption at rest
    2. Encryption in motion

2. Integrity
    1. IAM roles
    2. Groups and roles

3. Availability
    1. High availability zones
    2. Disaster recovery and business continuity

Cloud center of excellence

Team composition

- Cloud practice director
- Cloud solution architect
- Cloud DevOps engineers

Benefits

- Gain support from executive team
- Low cost experimentation to stay relevant
- Create hybrid organization

Accounts setup

Master-sub accounts benefits

- Separate accounts for development and production
- Consolidate billing, but charge back to individual departments made easier

Network setup

Multiple VPC and gateway

- Separate development from production
- Document access to separate network

Security group policy

Multiple security groups

- Isolate rules for access, keys, inbound and outbound connection
- Attach policies as a service
- Attach roles to groups and users

Automation for implementation

Benefits:

- Reduces human errors
- Improves consistency in adopting security policies.

Automation for evidences

Benefits:

- Reduces operational overhead
- Improves influence of CIO organization

What can be automated?

Infrastructure as a code

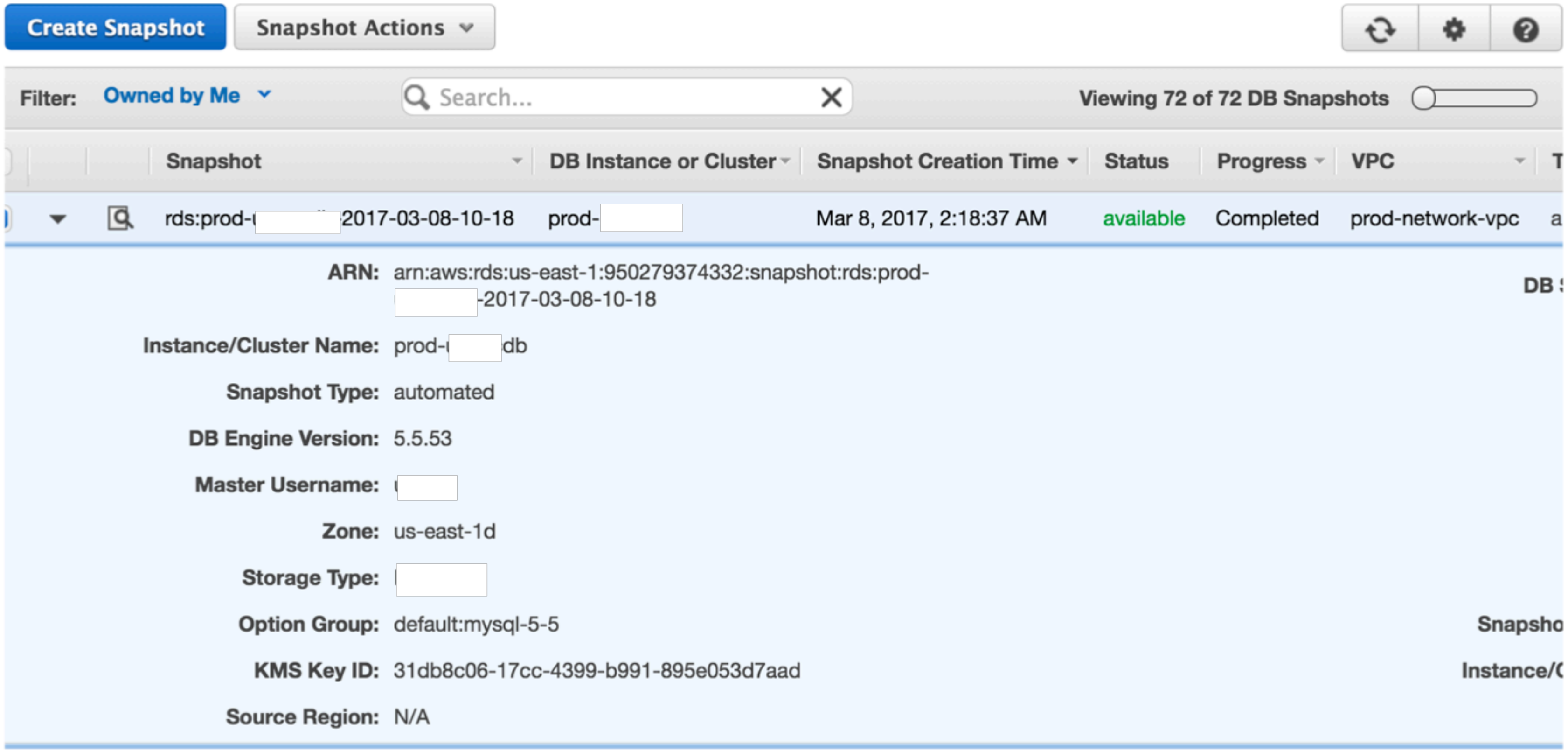
- Data encryption at rest
- Network traffic encryption
- Automated backups
- System monitoring and alerting
- VPC and security groups
- System access controls and logging
- Operating system: maintenance, management and patching
- Logging: Aggregation and archiving

dataphilic.io

Two best public cloud providers for healthcare

Offerings	AWS	Azure
Auto-scaling	Yes	Yes
Virtual machines (temporary and dedicated)	Yes	Yes
Durable and long term Storage	Yes	Yes
Security and access - HIPAA, PCI, ISO 27001, FEDRAMP, SSAE-16	Yes	Yes
Key management services	Yes	Yes
- Encryption at rest and in motion	Yes	Yes
- Identity and access management	Yes	Yes
SLAs, Support	Yes	Yes

Automated backups



Snapshot	DB Instance or Cluster	Snapshot Creation Time	Status	Progress	VPC	T
rds:prod-[redacted]2017-03-08-10-18	prod-[redacted]	Mar 8, 2017, 2:18:37 AM	available	Completed	prod-network-vpc	a

ARN: arn:aws:rds:us-east-1:950279374332:snapshot:rds:prod-[redacted]-2017-03-08-10-18

Instance/Cluster Name: prod-[redacted]db

Snapshot Type: automated

DB Engine Version: 5.5.53

Master Username: [redacted]

Zone: us-east-1d

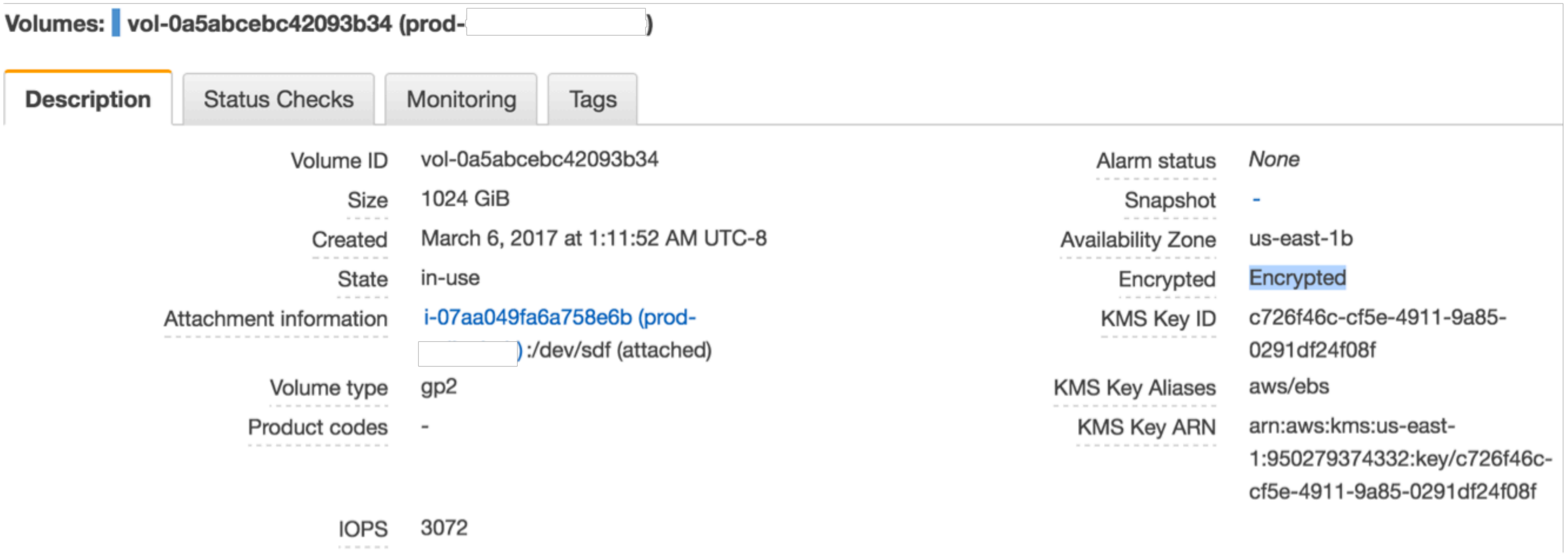
Storage Type: [redacted]

Option Group: default:mysql-5-5

KMS Key ID: 31db8c06-17cc-4399-b991-895e053d7aad

Source Region: N/A

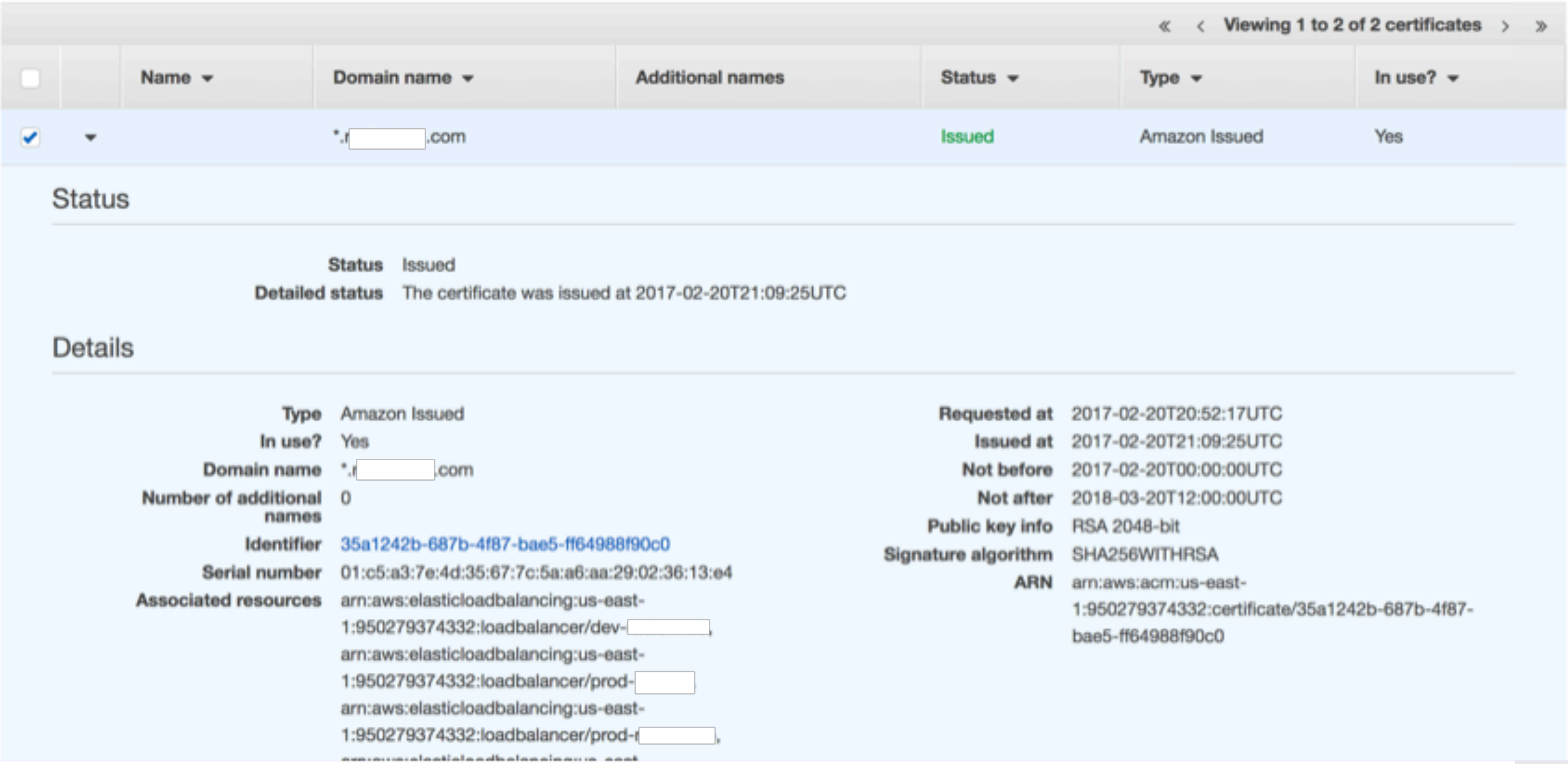
Encryption at rest



Volumes: vol-0a5abcebc42093b34 (prod-[redacted])

Volume ID	vol-0a5abcebc42093b34	Alarm status	*None*
Size	1024 GiB	Snapshot	-
Created	March 6, 2017 at 1:11:52 AM UTC-8	Availability Zone	us-east-1b
State	in-use	Encrypted	Encrypted
Attachment information	i-07aa049fa6a758e6b (prod-[redacted]):/dev/sdf (attached)	KMS Key ID	c726f46c-cf5e-4911-9a85-0291df24f08f
Volume type	gp2	KMS Key Aliases	aws/ebs
Product codes	-	KMS Key ARN	arn:aws:kms:us-east-1:950279374332:key/c726f46c-cf5e-4911-9a85-0291df24f08f
IOPS	3072		

Encryption in motion



« ‹ Viewing 1 to 2 of 2 certificates › »

□		Name	Domain name	Additional names	Status	Type	In use?
☑	▾		*.r[redacted].com		Issued	Amazon Issued	Yes

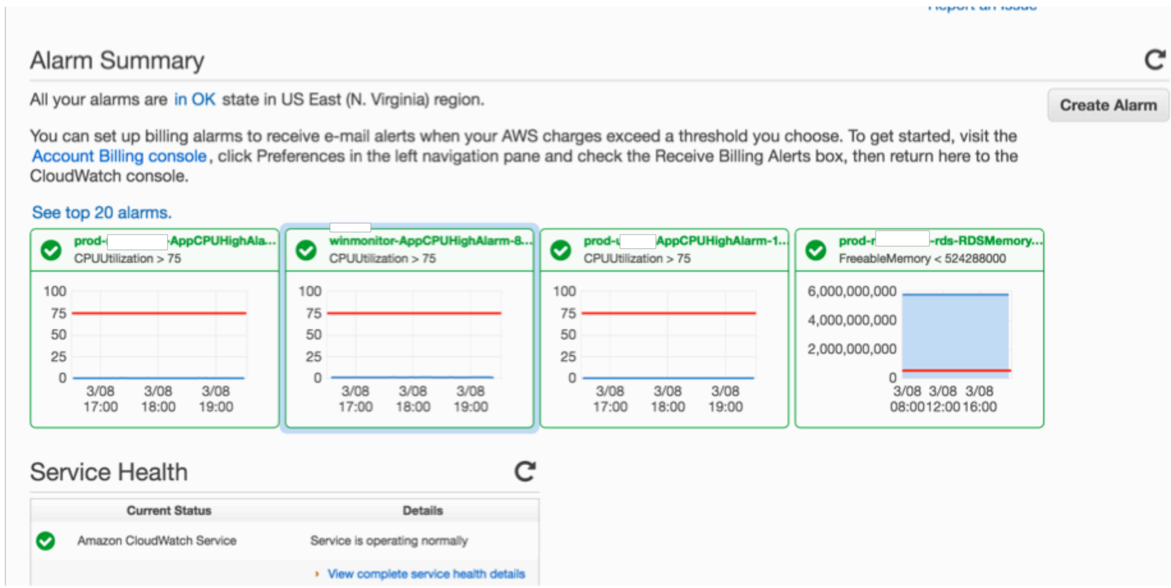
Status

Status	Issued
Detailed status	The certificate was issued at 2017-02-20T21:09:25UTC

Details

Type	Amazon Issued	**Requested at**	2017-02-20T20:52:17UTC
In use?	Yes	**Issued at**	2017-02-20T21:09:25UTC
Domain name	*.r[redacted].com	**Not before**	2017-02-20T00:00:00UTC
Number of additional names	0	**Not after**	2018-03-20T12:00:00UTC
Identifier	35a1242b-687b-4f87-bae5-ff64988f90c0	**Public key info**	RSA 2048-bit
Serial number	01:c5:a3:7e:4d:35:67:7c:5a:a6:aa:29:02:36:13:e4	**Signature algorithm**	SHA256WITHRSA
Associated resources	arn:aws:elasticloadbalancing:us-east-1:950279374332:loadbalancer/dev-[redacted], arn:aws:elasticloadbalancing:us-east-1:950279374332:loadbalancer/prod-[redacted] arn:aws:elasticloadbalancing:us-east-1:950279374332:loadbalancer/prod-r[redacted], arn:aws:elasticloadbalancing:us-east	**ARN**	arn:aws:acm:us-east-1:950279374332:certificate/35a1242b-687b-4f87-bae5-ff64988f90c0

System Monitoring and alerting



Report an issue

Alarm Summary

All your alarms are in OK state in US East (N. Virginia) region.

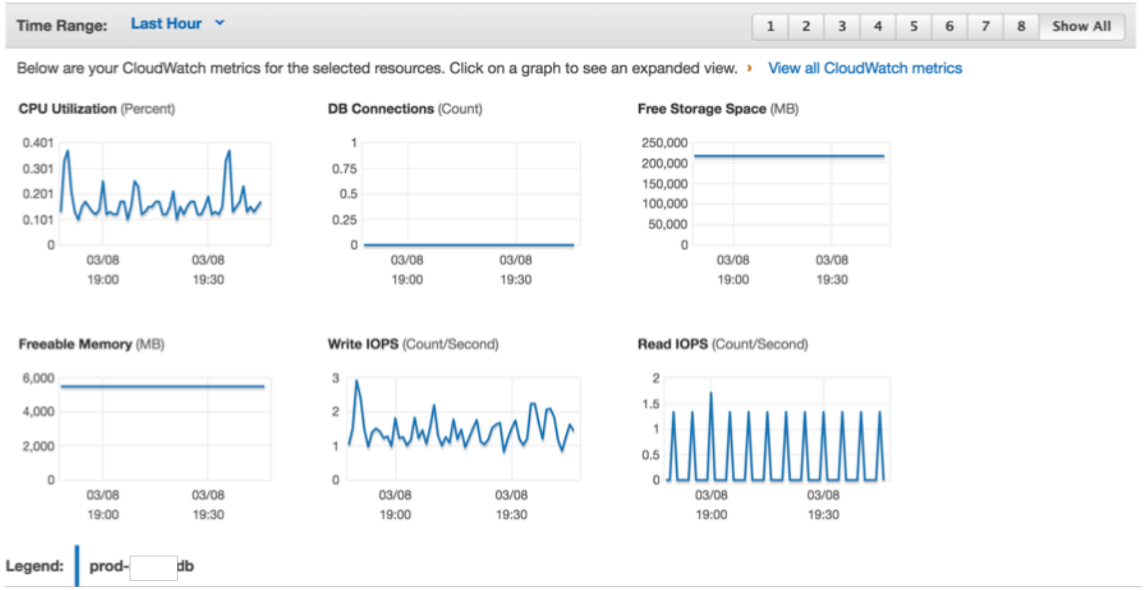
You can set up billing alarms to receive e-mail alerts when your AWS charges exceed a threshold you choose. To get started, visit the Account Billing console, click Preferences in the left navigation pane and check the Receive Billing Alerts box, then return here to the CloudWatch console.

See top 20 alarms.

Service Health

Current Status	Details
✓ Amazon CloudWatch Service	Service is operating normally

› View complete service health details



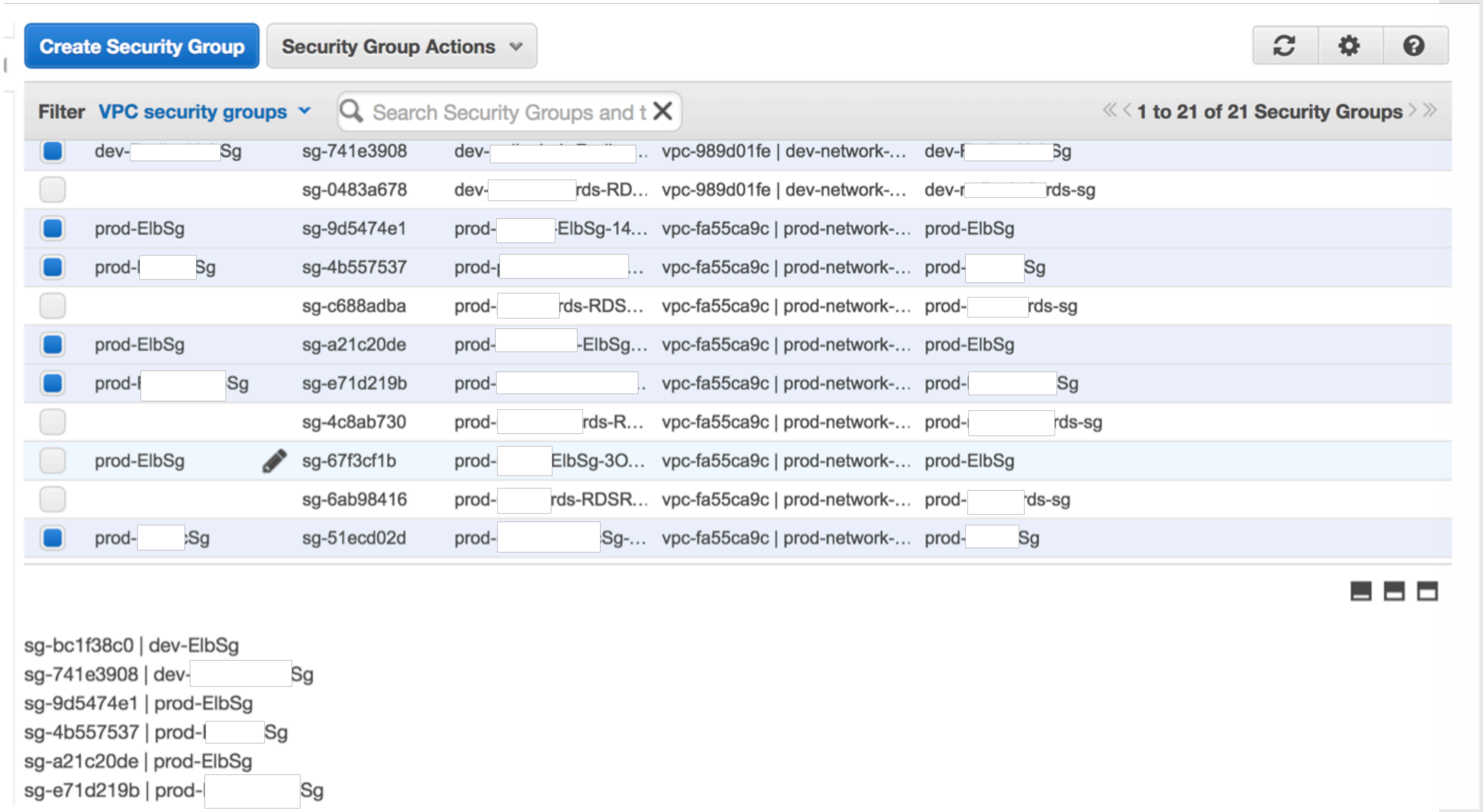
Time Range: Last Hour

Below are your CloudWatch metrics for the selected resources. Click on a graph to see an expanded view. › View all CloudWatch metrics

Legend: prod-[redacted]db

dataphilic.io

VPC and Security Groups



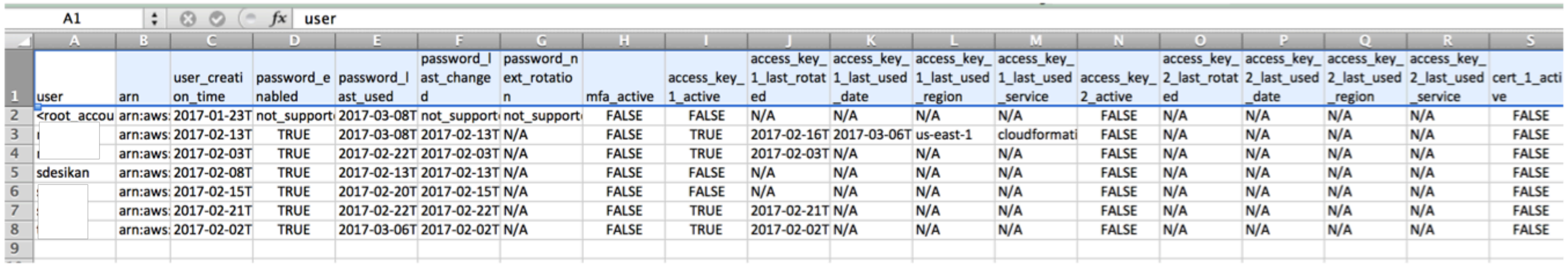
Create Security Group
Security Group Actions
Filter VPC security groups
Search Security Groups and t
1 to 21 of 21 Security Groups

■	dev-[redacted]Sg	sg-741e3908	dev-[redacted]..	vpc-989d01fe | dev-network-...	dev-[redacted]Sg
□		sg-0483a678	dev-[redacted]rds-RD...	vpc-989d01fe | dev-network-...	dev-r[redacted]rds-sg
■	prod-ElbSg	sg-9d5474e1	prod-[redacted]ElbSg-14...	vpc-fa55ca9c | prod-network-...	prod-ElbSg
■	prod-[redacted]Sg	sg-4b557537	prod-[redacted]...	vpc-fa55ca9c | prod-network-...	prod-[redacted]Sg
□		sg-c688adba	prod-[redacted]rds-RDS...	vpc-fa55ca9c | prod-network-...	prod-[redacted]rds-sg
■	prod-ElbSg	sg-a21c20de	prod-[redacted]-ElbSg...	vpc-fa55ca9c | prod-network-...	prod-ElbSg
■	prod-[redacted]Sg	sg-e71d219b	prod-[redacted].	vpc-fa55ca9c | prod-network-...	prod-[redacted]Sg
□		sg-4c8ab730	prod-[redacted]rds-R...	vpc-fa55ca9c | prod-network-...	prod-[redacted]rds-sg
□	prod-ElbSg	sg-67f3cf1b	prod-[redacted]ElbSg-3O...	vpc-fa55ca9c | prod-network-...	prod-ElbSg
□		sg-6ab98416	prod-[redacted]rds-RDSR...	vpc-fa55ca9c | prod-network-...	prod-[redacted]ds-sg
■	prod-[redacted]Sg	sg-51ecd02d	prod-[redacted]Sg-...	vpc-fa55ca9c | prod-network-...	prod-[redacted]Sg

sg-bc1f38c0 | dev-ElbSg
sg-741e3908 | dev-[redacted]Sg
sg-9d5474e1 | prod-ElbSg
sg-4b557537 | prod-[redacted]Sg
sg-a21c20de | prod-ElbSg
sg-e71d219b | prod-[redacted]Sg

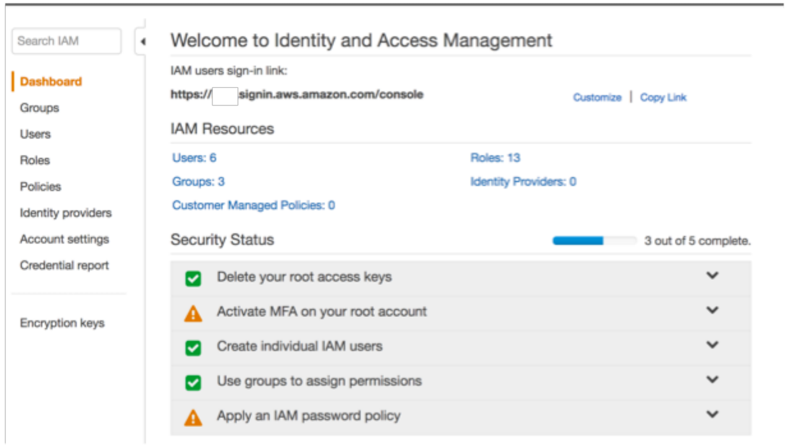
dataphilic.io

System access controls



A1 user

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	user	arn	user_creation_time	password_enabled	password_last_used	password_last_changed	password_next_rotation	mfa_active	access_key_1_active	access_key_1_last_rotated	access_key_1_last_used_date	access_key_1_last_used_region	access_key_1_last_used_service	access_key_2_active	access_key_2_last_rotated	access_key_2_last_used_date	access_key_2_last_used_region	access_key_2_last_used_service	cert_1_active
2	<root_accou	arn:aws:	2017-01-23T	not_support	2017-03-08T	not_support	not_support	FALSE	FALSE	N/A	N/A	N/A	N/A	FALSE	N/A	N/A	N/A	N/A	FALSE
3	[redacted]	arn:aws:	2017-02-13T	TRUE	2017-03-08T	2017-02-13T	N/A	FALSE	TRUE	2017-02-16T	2017-03-06T	us-east-1	cloudformati	FALSE	N/A	N/A	N/A	N/A	FALSE
4	[redacted]	arn:aws:	2017-02-03T	TRUE	2017-02-22T	2017-02-03T	N/A	FALSE	TRUE	2017-02-03T	N/A	N/A	N/A	FALSE	N/A	N/A	N/A	N/A	FALSE
5	sdesikan	arn:aws:	2017-02-08T	TRUE	2017-02-13T	2017-02-13T	N/A	FALSE	FALSE	N/A	N/A	N/A	N/A	FALSE	N/A	N/A	N/A	N/A	FALSE
6	[redacted]	arn:aws:	2017-02-15T	TRUE	2017-02-20T	2017-02-15T	N/A	FALSE	FALSE	N/A	N/A	N/A	N/A	FALSE	N/A	N/A	N/A	N/A	FALSE
7	[redacted]	arn:aws:	2017-02-21T	TRUE	2017-02-22T	2017-02-22T	N/A	FALSE	TRUE	2017-02-21T	N/A	N/A	N/A	FALSE	N/A	N/A	N/A	N/A	FALSE
8	[redacted]	arn:aws:	2017-02-02T	TRUE	2017-03-06T	2017-02-02T	N/A	FALSE	TRUE	2017-02-02T	N/A	N/A	N/A	FALSE	N/A	N/A	N/A	N/A	FALSE
9																			



Welcome to Identity and Access Management

IAM users sign-in link:

https://[redacted]signin.aws.amazon.com/console

IAM Resources

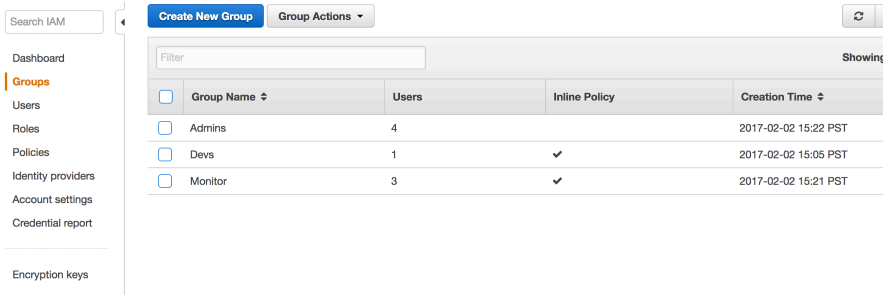
Users: 6 Roles: 13

Groups: 3 Identity Providers: 0

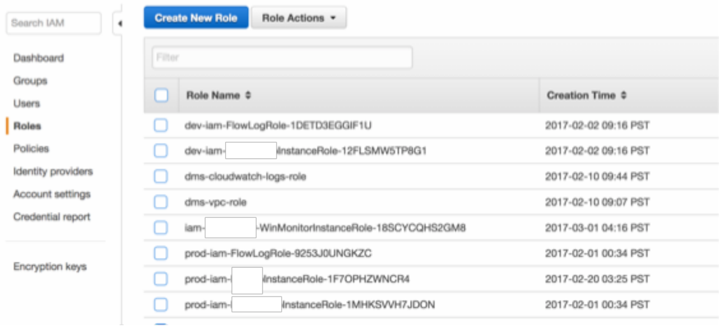
Customer Managed Policies: 0

Security Status 3 out of 5 complete.

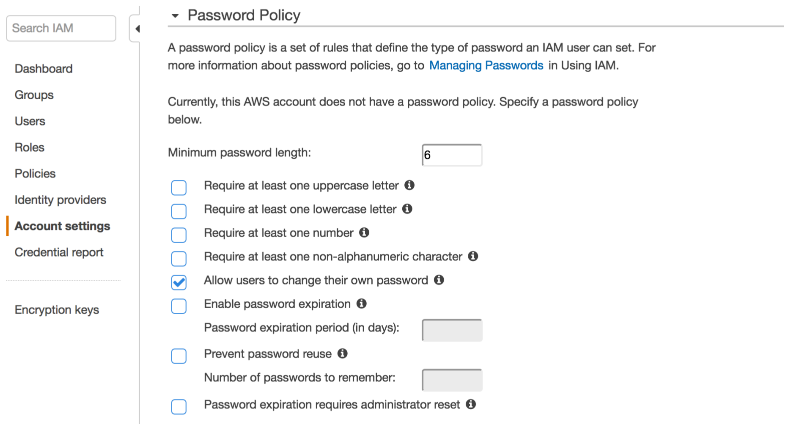
- ✓ Delete your root access keys
- ⚠ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ⚠ Apply an IAM password policy



□	Group Name	Users	Inline Policy	Creation Time
□	Admins	4		2017-02-02 15:22 PST
□	Devs	1	✓	2017-02-02 15:05 PST
□	Monitor	3	✓	2017-02-02 15:21 PST



□	Role Name	Creation Time
□	dev-iam-FlowLogRole-1DETD3EGGIF1U	2017-02-02 09:16 PST
□	dev-iam-[redacted]InstanceRole-12FLSMW5TP8G1	2017-02-02 09:16 PST
□	dms-cloudwatch-logs-role	2017-02-10 09:44 PST
□	dms-vpc-role	2017-02-10 09:07 PST
□	iam-[redacted]-WinMonitorInstanceRole-18SCYCQHS2GM8	2017-03-01 04:16 PST
□	prod-iam-FlowLogRole-9253J0UNGKZC	2017-02-01 00:34 PST
□	prod-iam-[redacted]InstanceRole-1F7OPHZWNCR4	2017-02-20 03:25 PST
□	prod-iam-[redacted]InstanceRole-1MHKSVVH7JDON	2017-02-01 00:34 PST



Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to Managing Passwords in Using IAM.

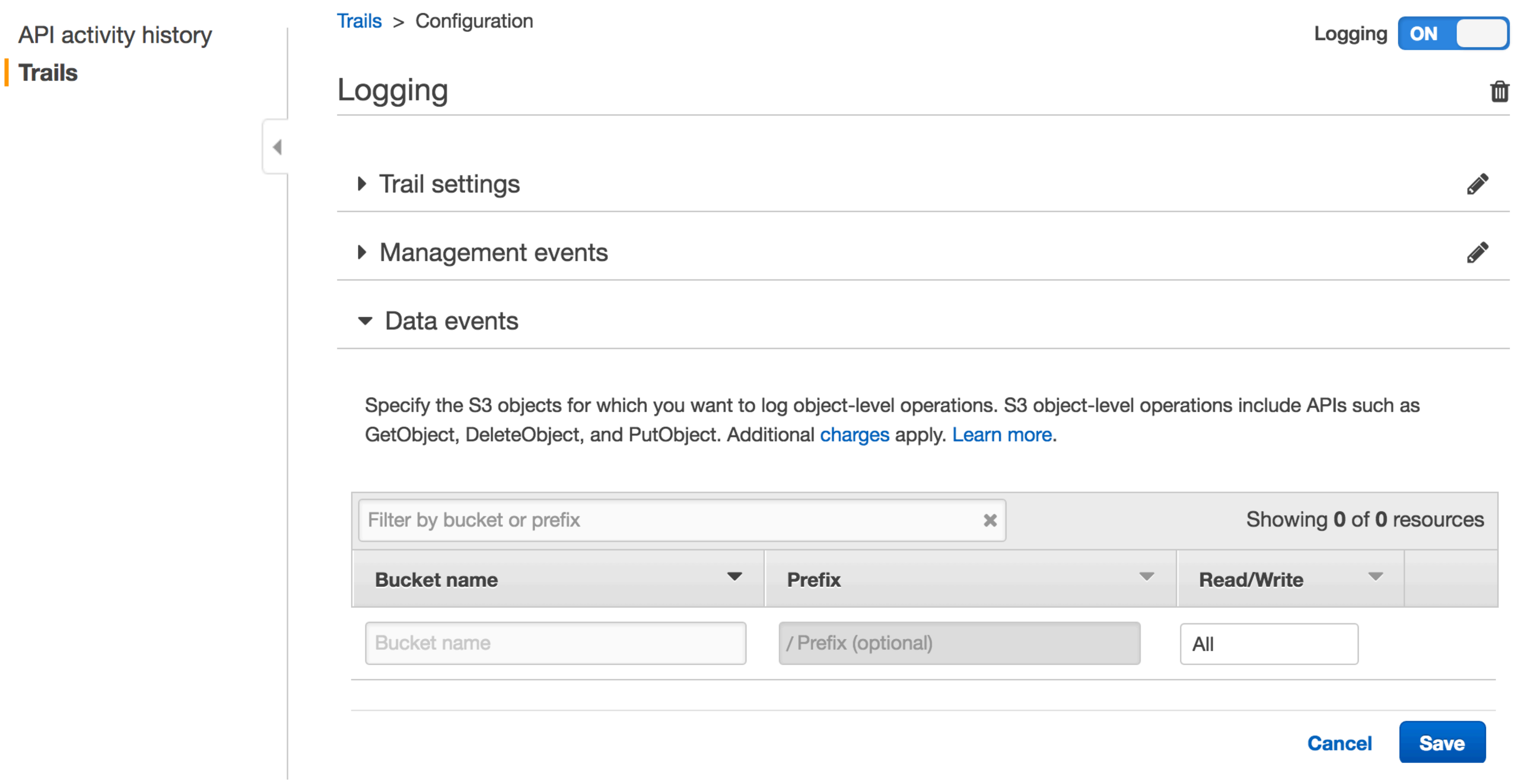
Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length: 6

- □ Require at least one uppercase letter
- □ Require at least one lowercase letter
- □ Require at least one number
- □ Require at least one non-alphanumeric character
- ☑ Allow users to change their own password
- □ Enable password expiration
  - Password expiration period (in days):
- □ Prevent password reuse
  - Number of passwords to remember:
- □ Password expiration requires administrator reset

dataphilic.io

Logging and audit trails



Logging

- Trail settings
- Management events
- Data events

Specify the S3 objects for which you want to log object-level operations. S3 object-level operations include APIs such as GetObject, DeleteObject, and PutObject. Additional charges apply. Learn more.

Filter by bucket or prefix — Showing **0** of **0** resources

Bucket name	Prefix	Read/Write
Bucket name	/ Prefix (optional)	All

Thank you

Contact:
Shreehari Desikan
sdesikan@dataphilic.io
408-786-8830