
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

STP203-R

Security from day one: Establishing a baseline

Cole Calistra (he/him)

Principal Startup Solutions Architect
AWS

Anya Derbakova (she/her)

Senior Startup Solutions Architect
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

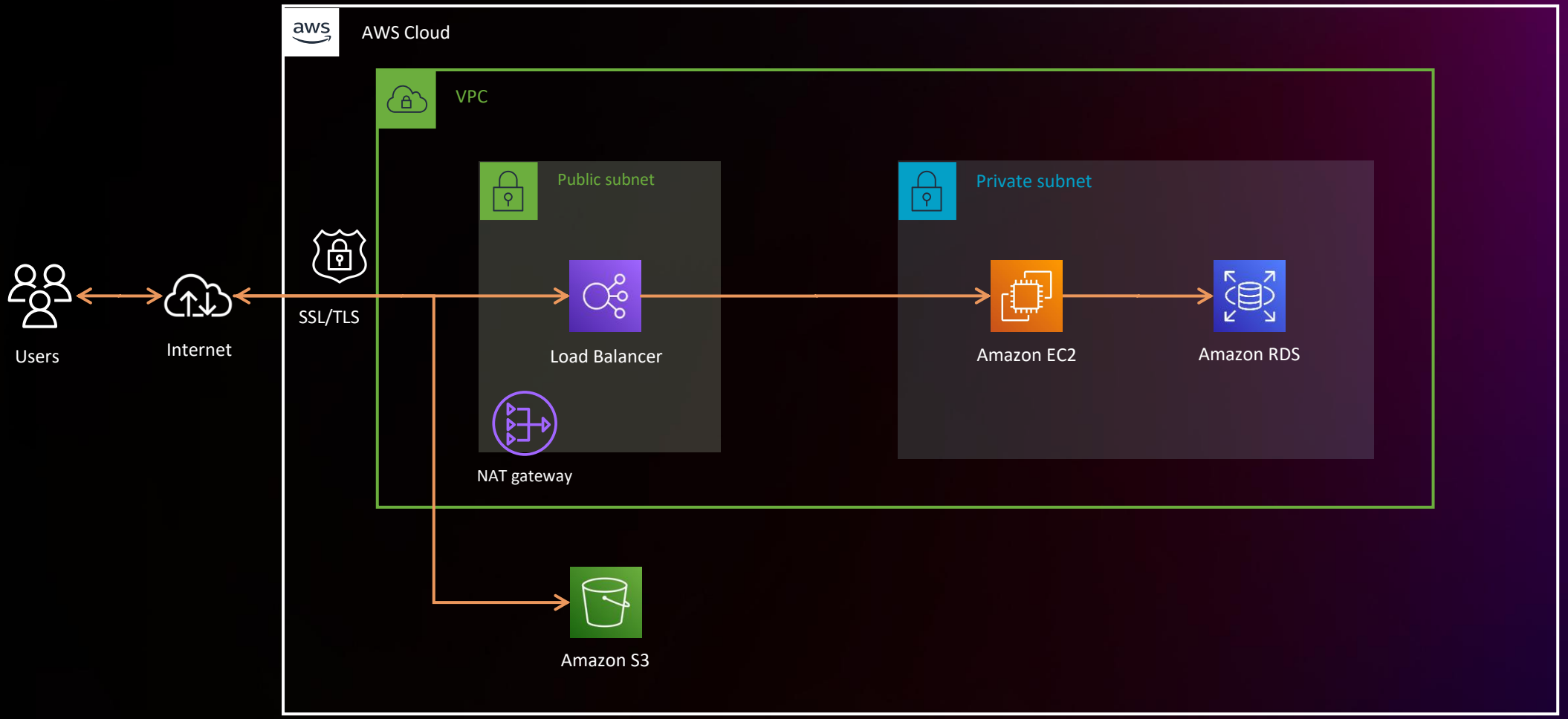
Congratulations!



We were all just hired as ExampleLabs’ new security engineering team!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecture diagram



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Startup Security Baseline

- Getting started on the right track
- Starting with a secure foundation
- Specially designed for early stage startups

SSB Guidance

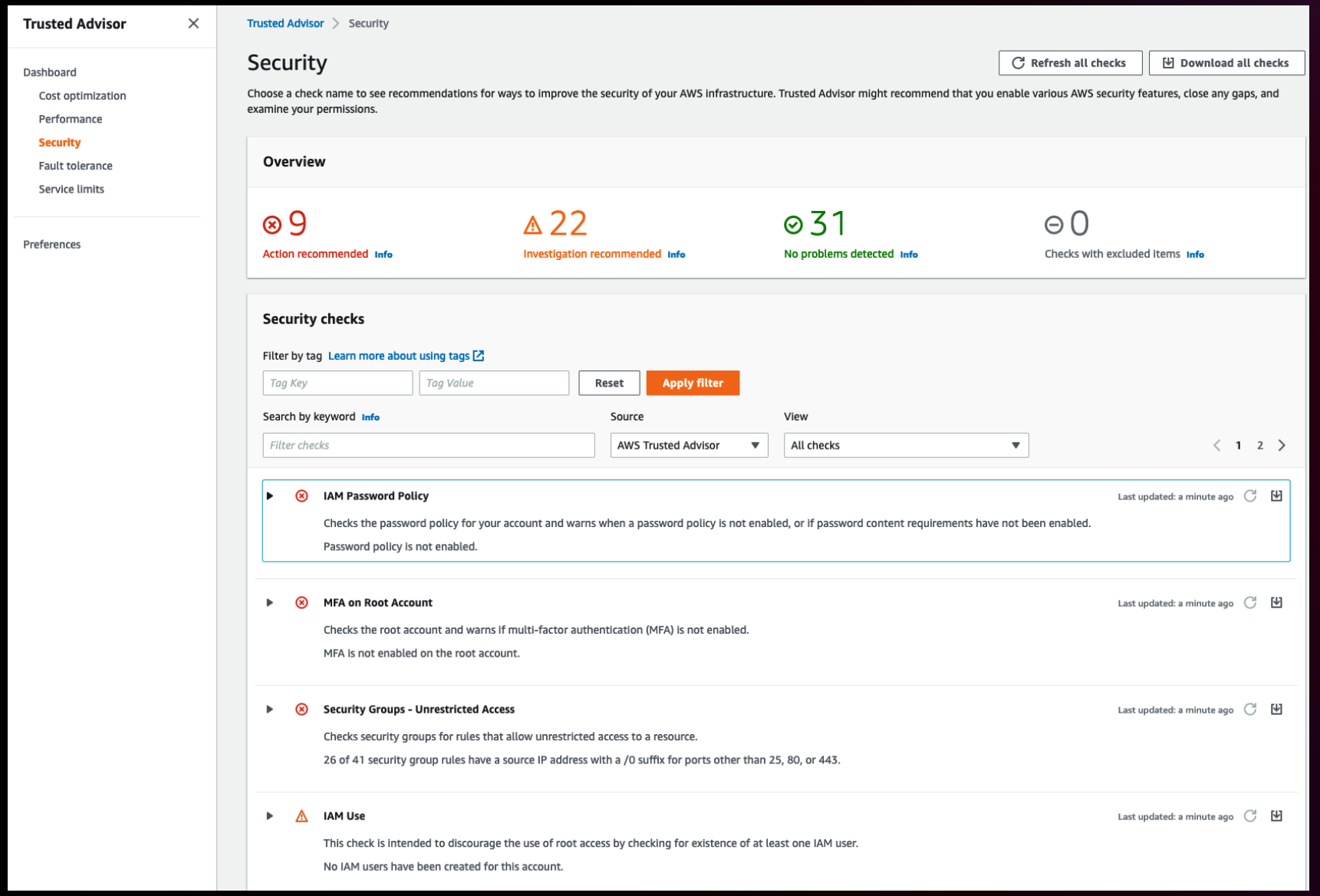
go.aws/3OlbbAY

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

First day

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

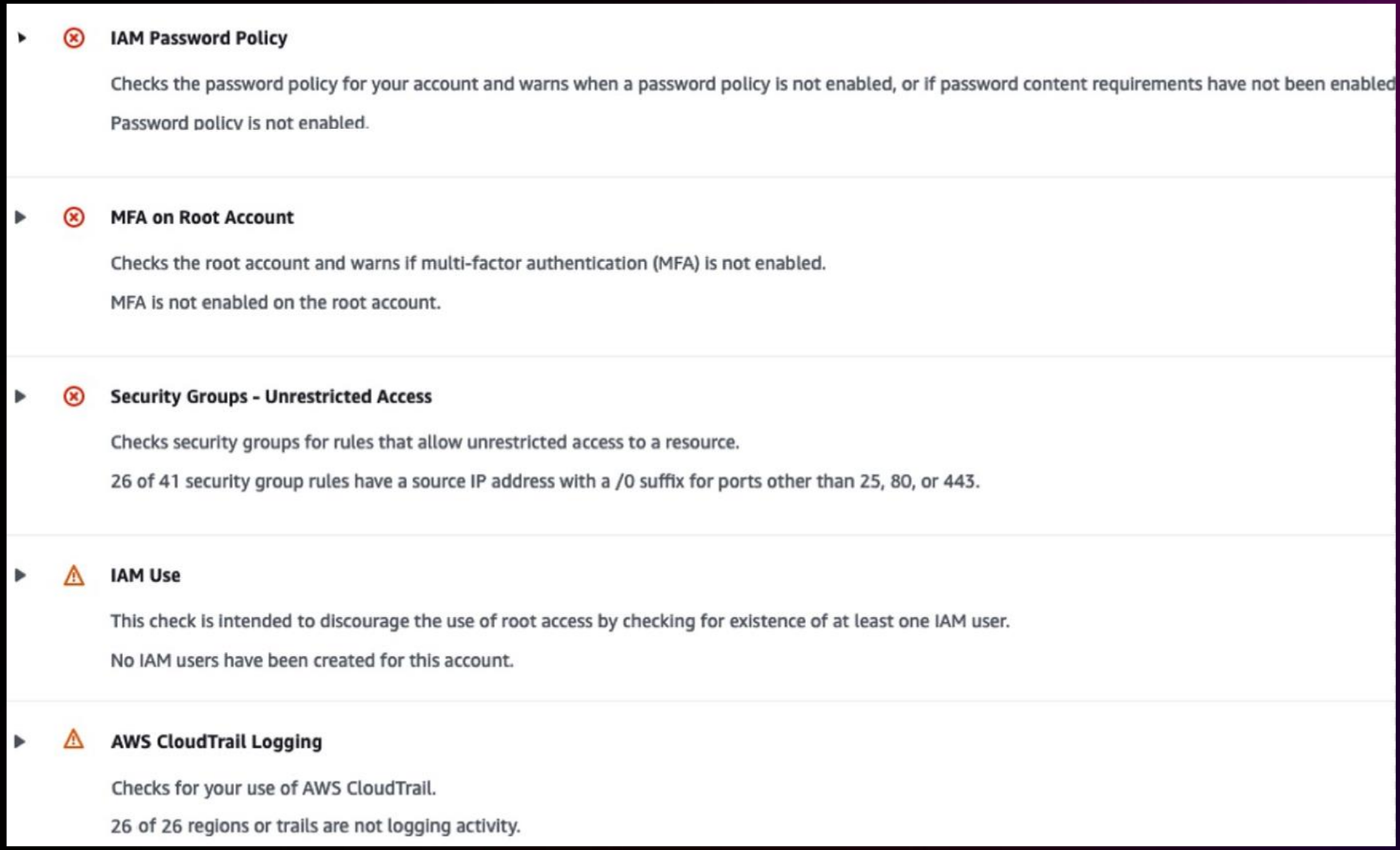
AWS Trusted Advisor





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Trusted Advisor Findings



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use of the root user

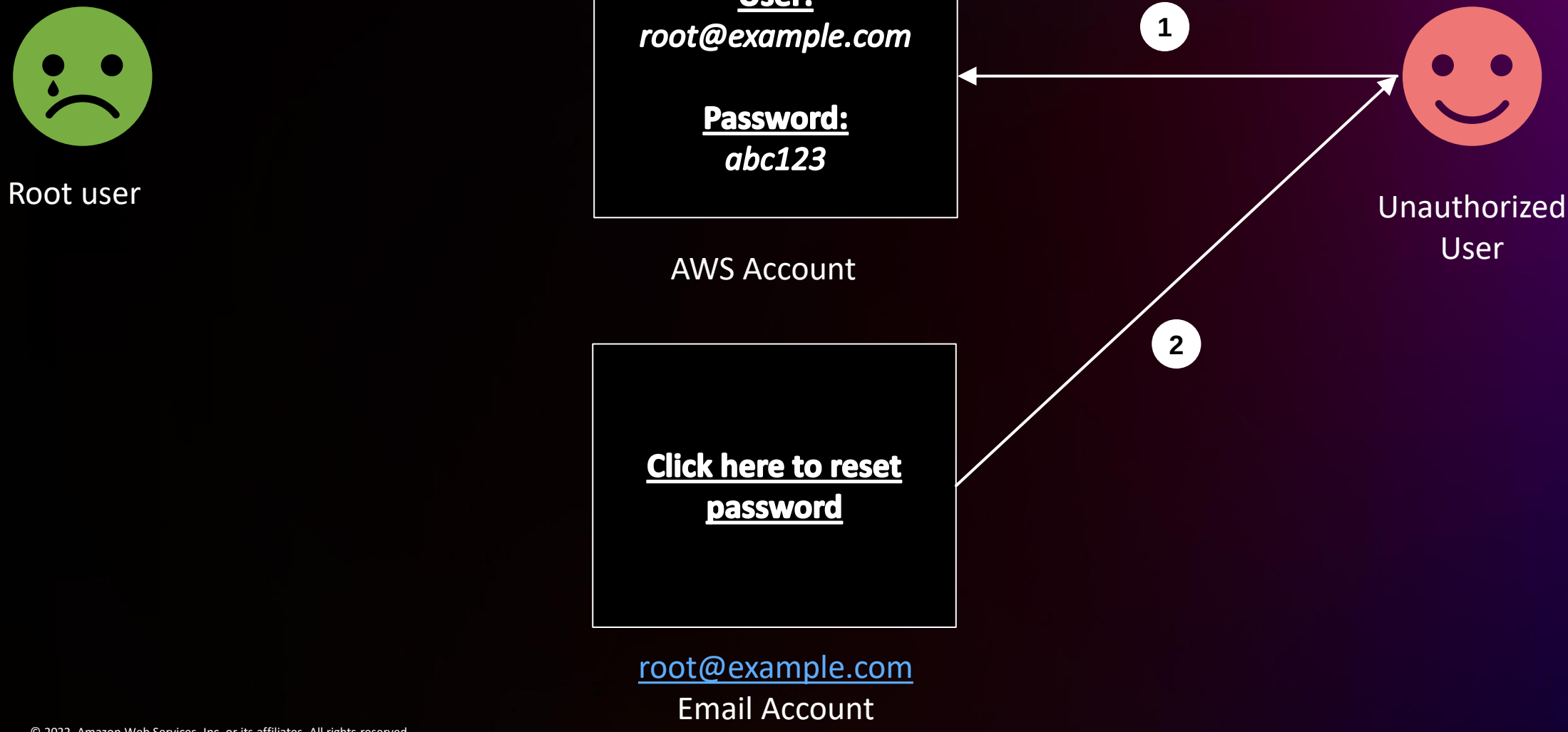
1. Secure it
    - Strong password
    - Multi-factor authentication (MFA)
    - Remove access keys

#root



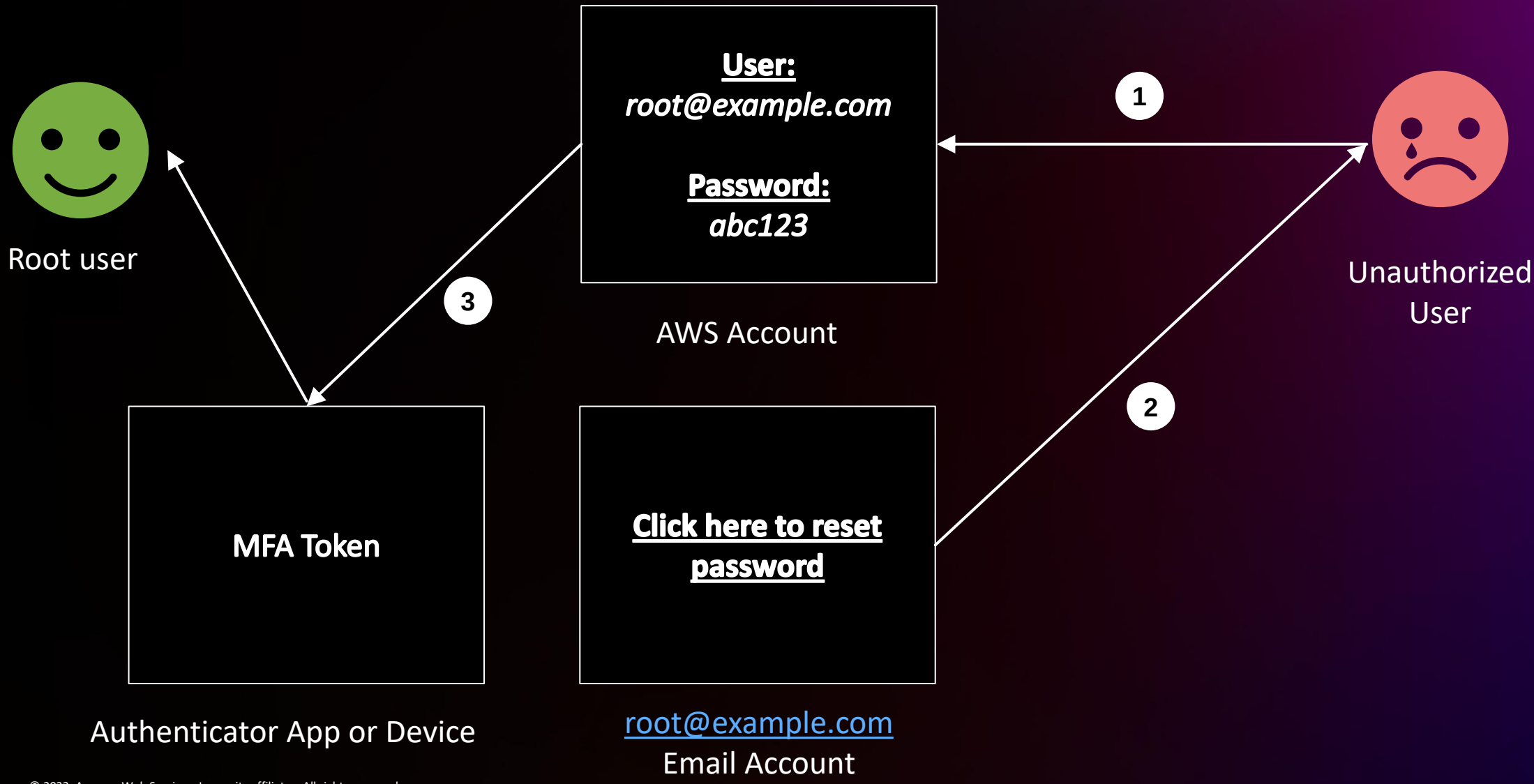
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How MFA protects



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How MFA protects



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tips

- Use/store multiple MFA devices for each account
- Use a password manager to create and store a strong password/MFA token for the root account

Multiple MFA token announcement



go.aws/3TUsIkM

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use of the root user

#root



1. Secure it
   - Strong password
   - Multi-factor authentication (MFA)
   - Remove access keys

2. Avoid it
   - Set up IAM users and groups
   - Set up a password policy
   - Use MFA for IAM users

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tips

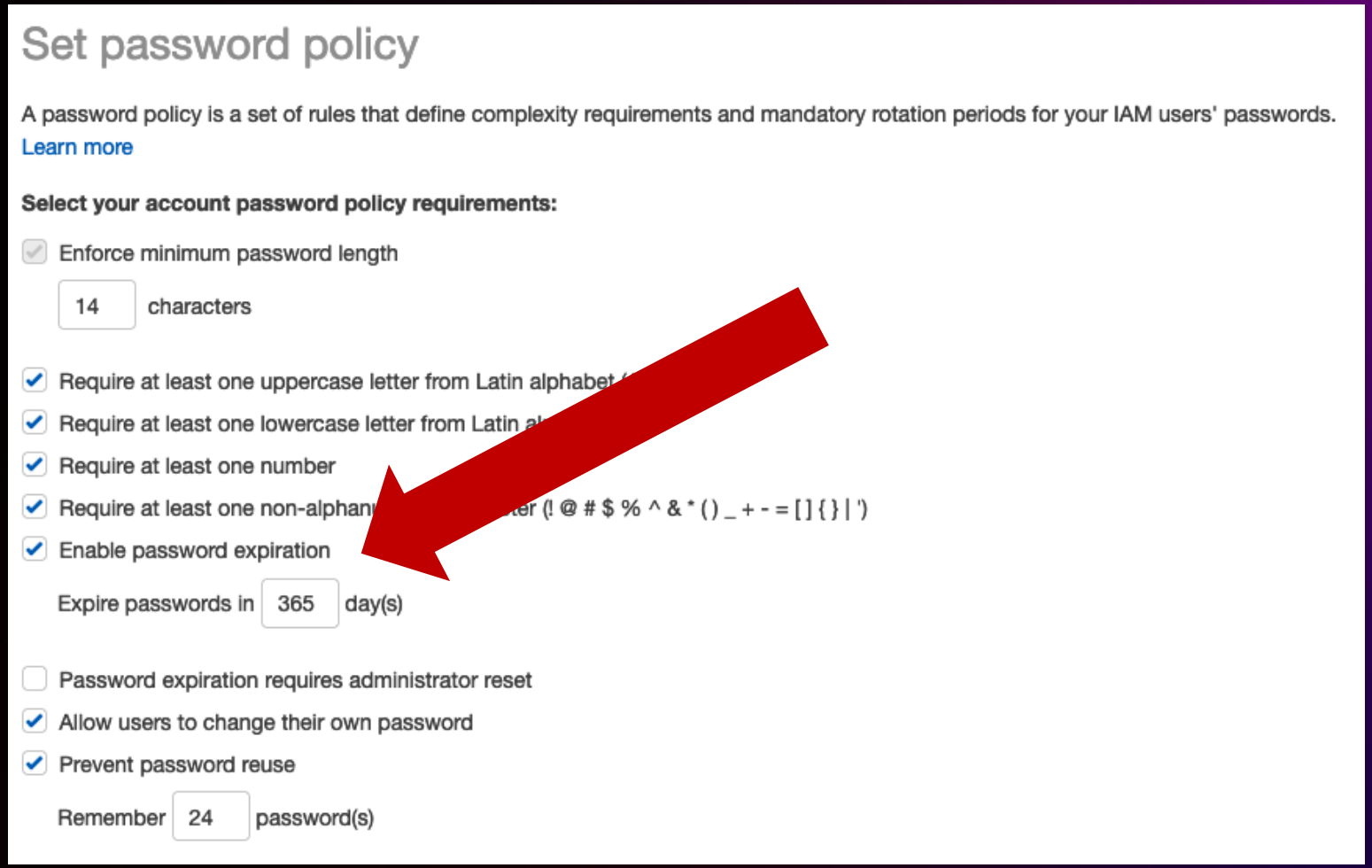
1. Use a company domain to register your accounts

2. Use email distribution lists for the account contacts

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enforce a password policy

1. Minimum length
2. Varied characters
3. Expiration

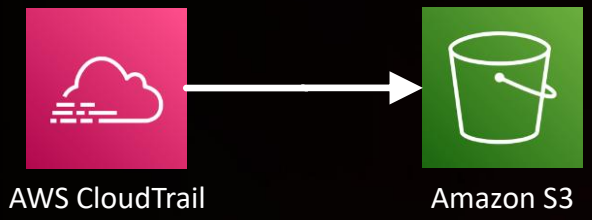


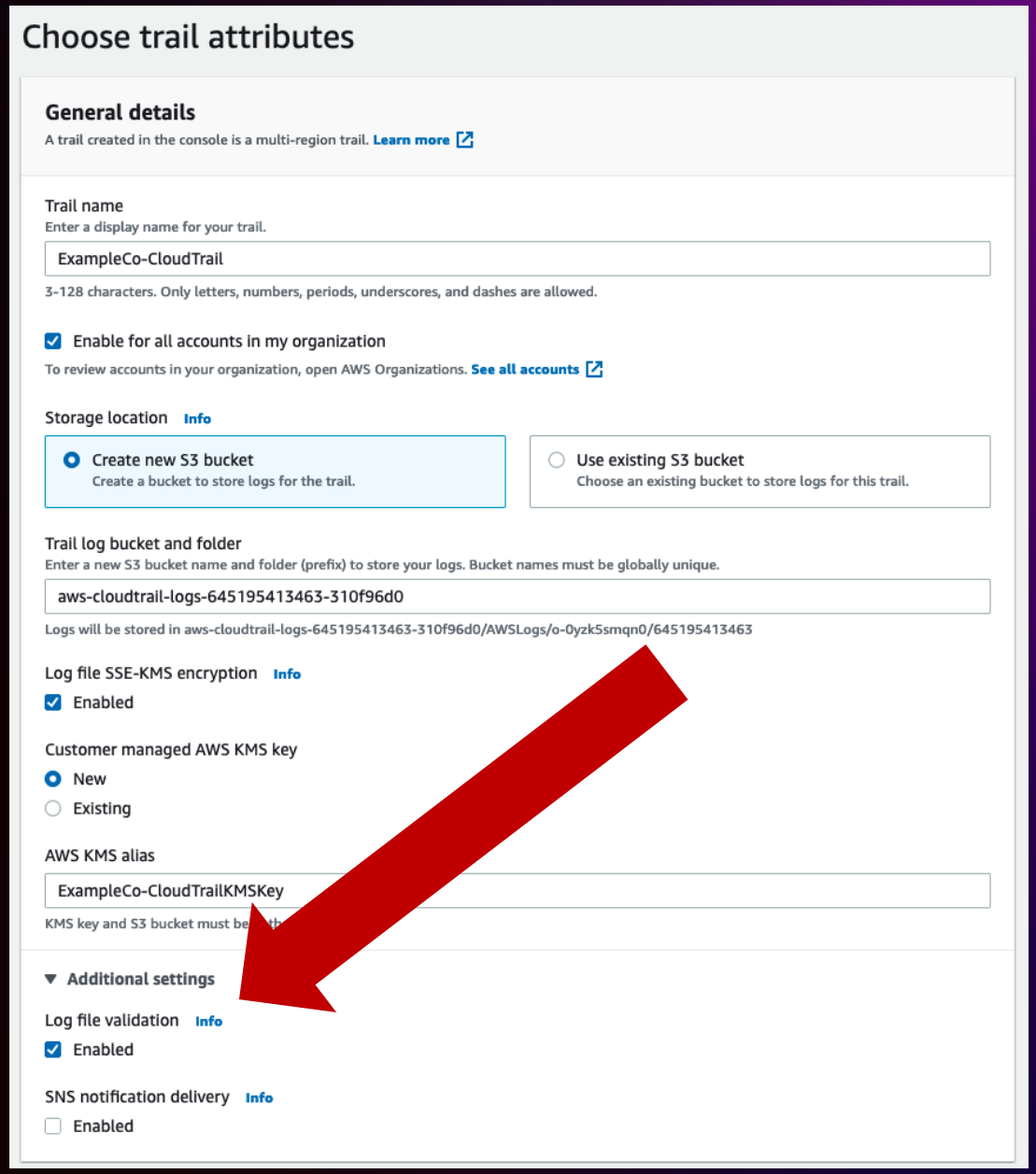
IAM Console → Account Settings → Password Policy → Change Password Policy

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logging events

1. Create a new AWS CloudTrail
2. Secure the Amazon S3 bucket

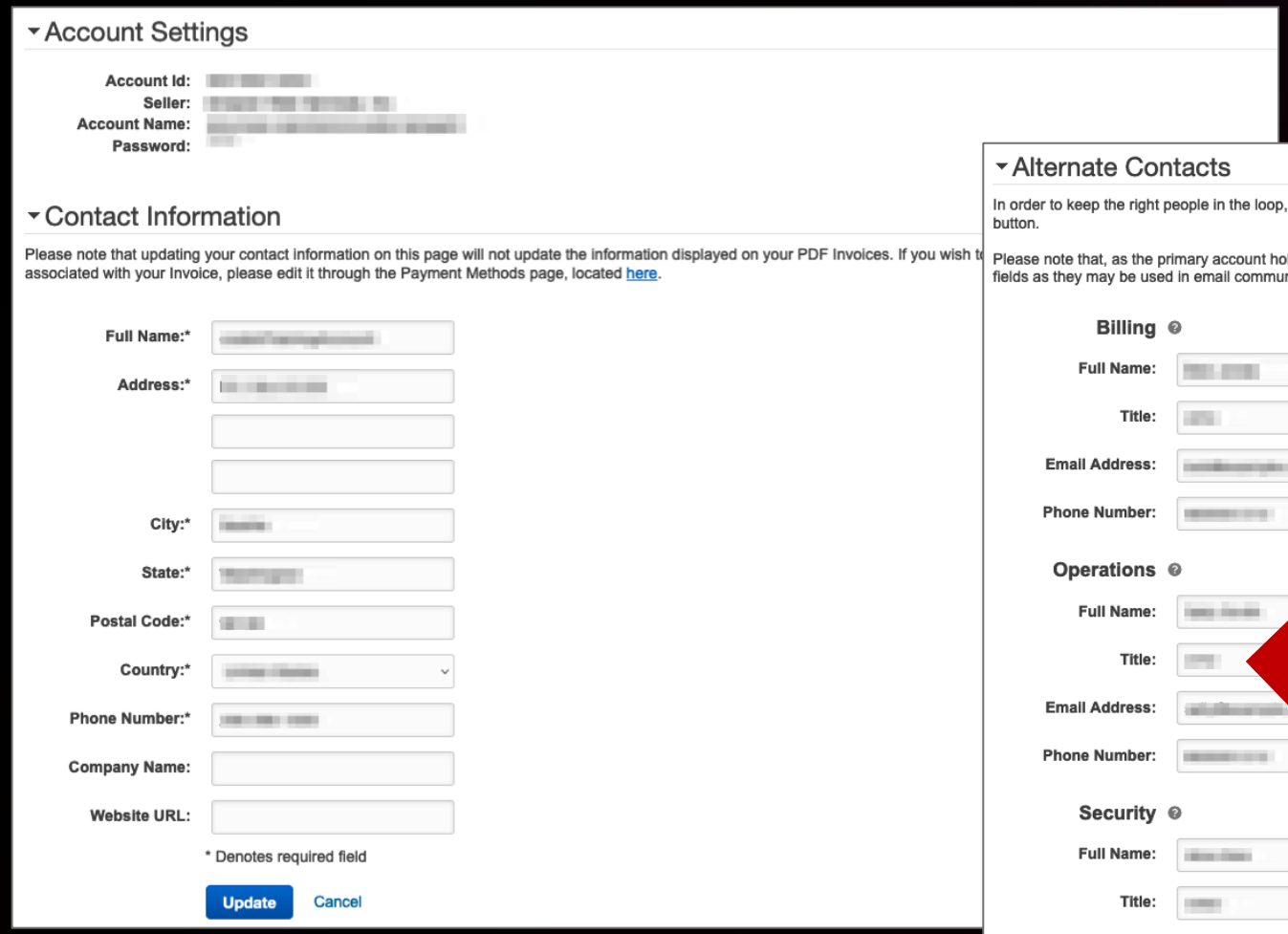


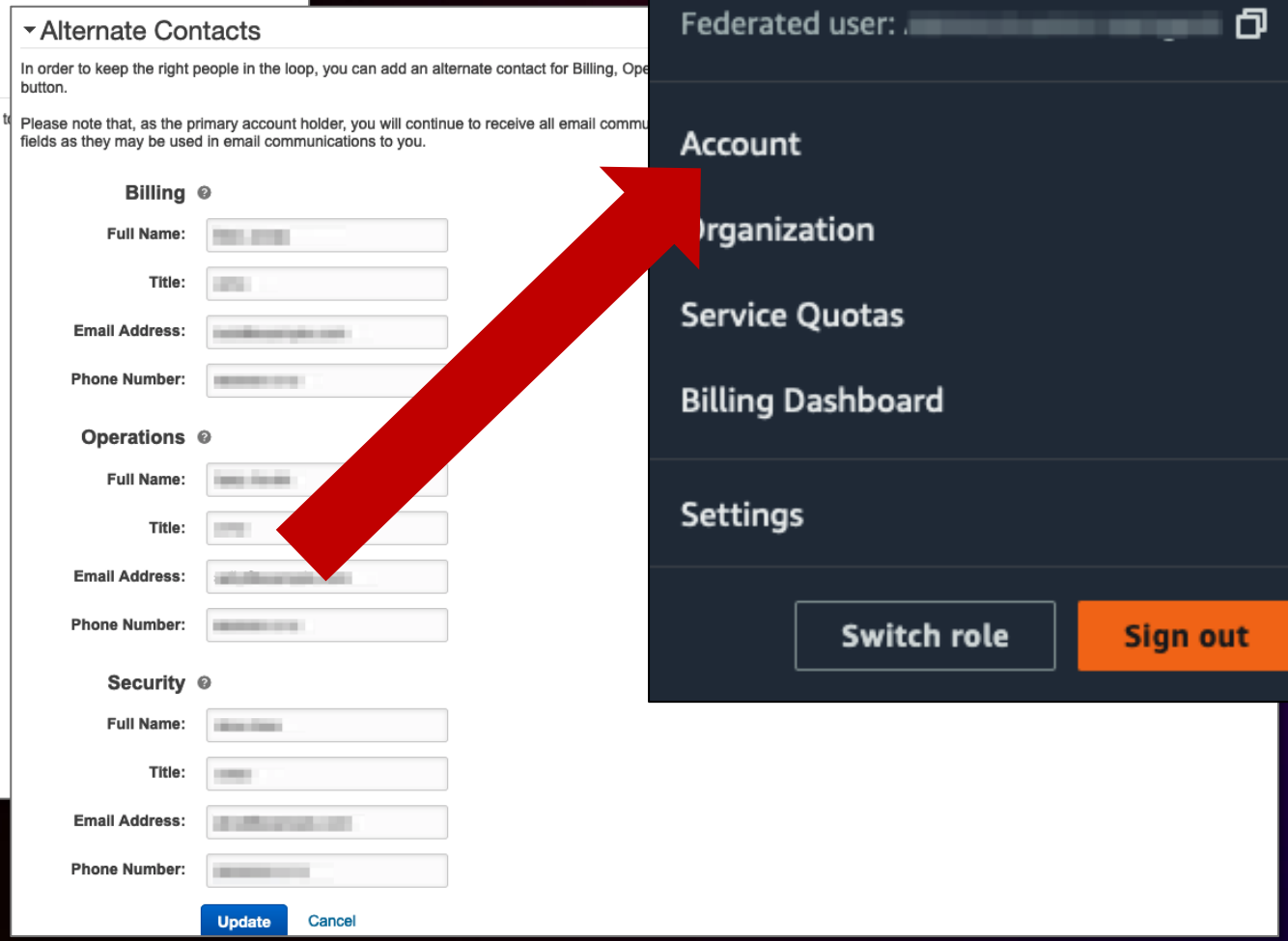


CloudTrail → Create Trail

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting account-level contacts

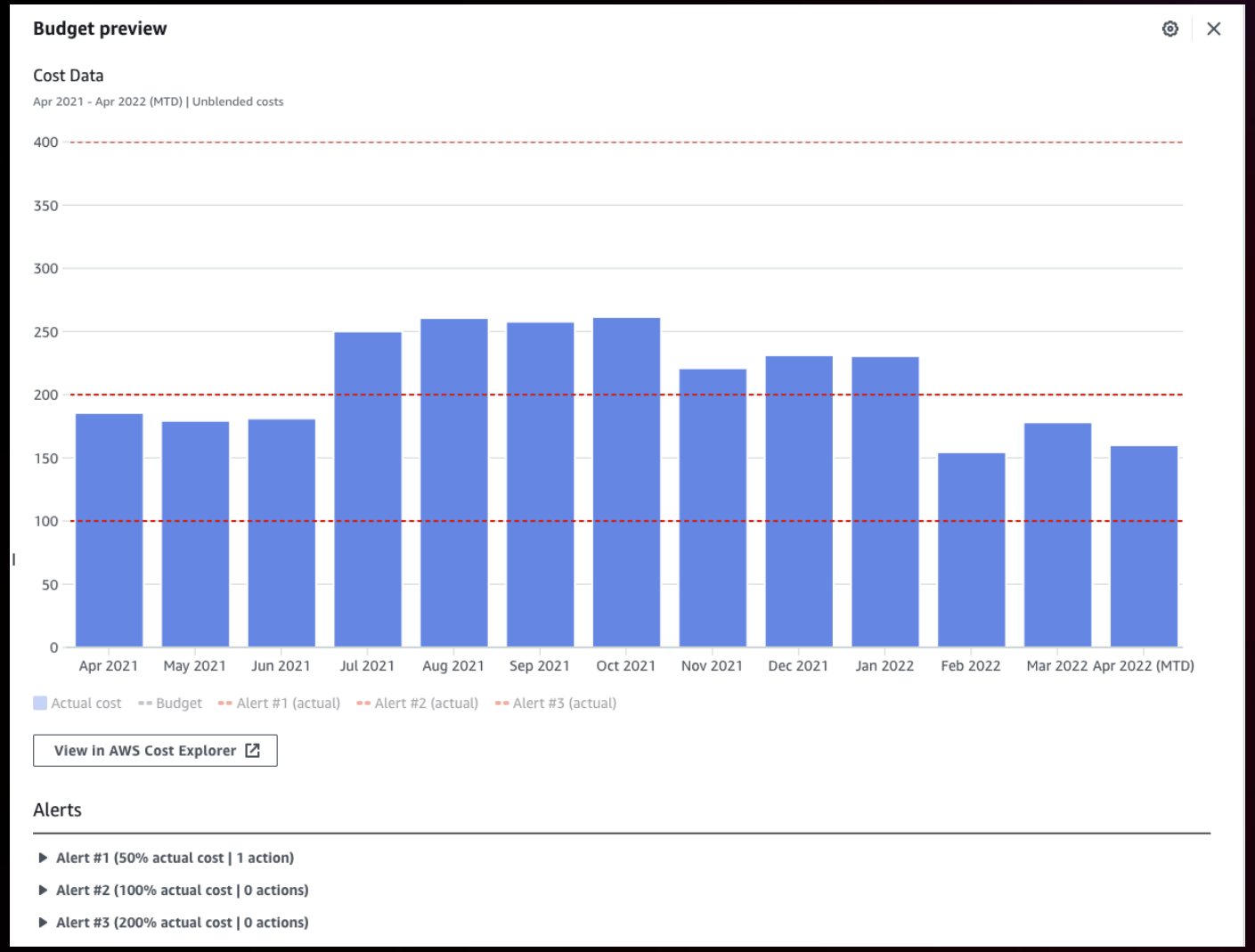




AWS Console → Account

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set up AWS Budgets



Billing → Budgets → Create a budget

AWS Budgets blog

go.aws/3AonVRK

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

First Day Recap/Takeaways

1. Setup MFA on the Root account
2. Start using IAM users
3. Turn on CloudTrail
4. Setup a budget and alerts

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Second Day

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Prevent public access to private S3 buckets

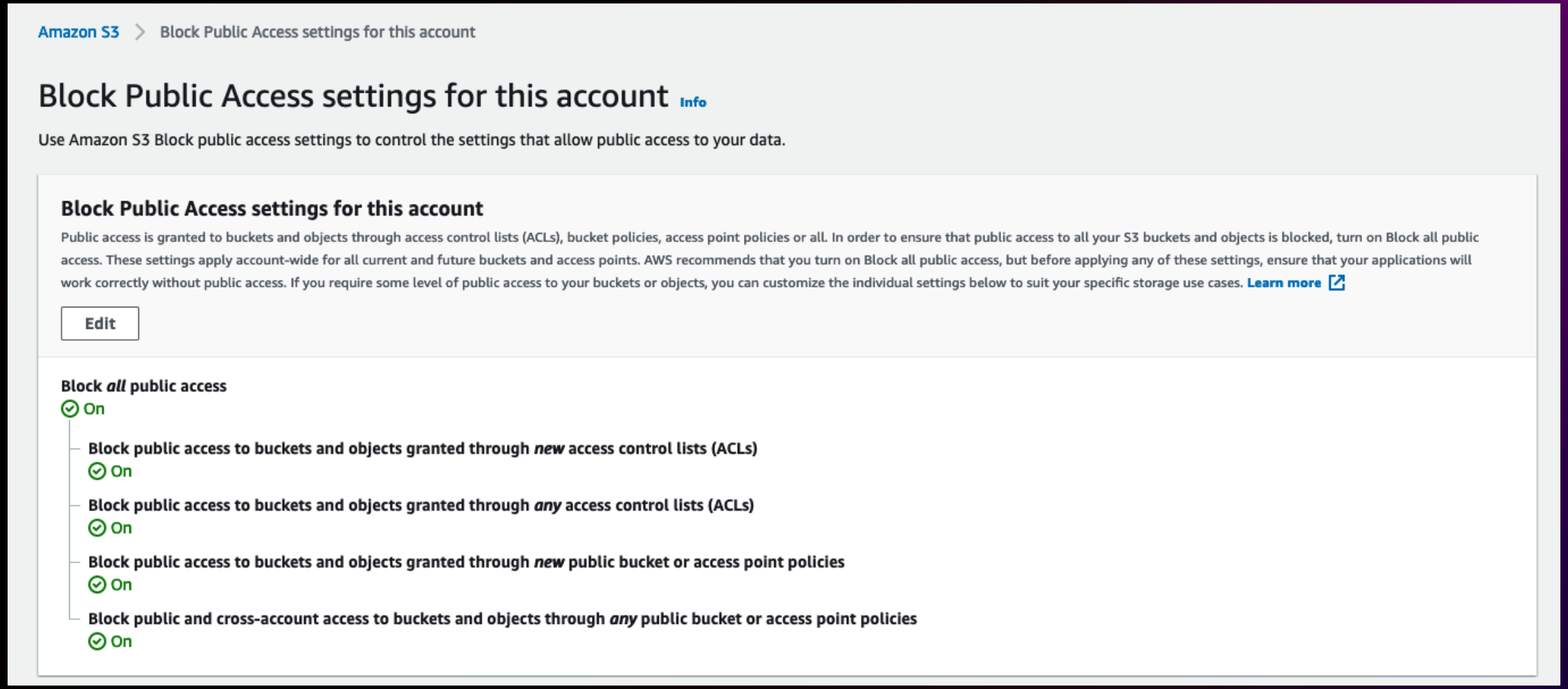




- Four security settings
- Applicable at the account level or on individual buckets

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Block public access to S3 buckets



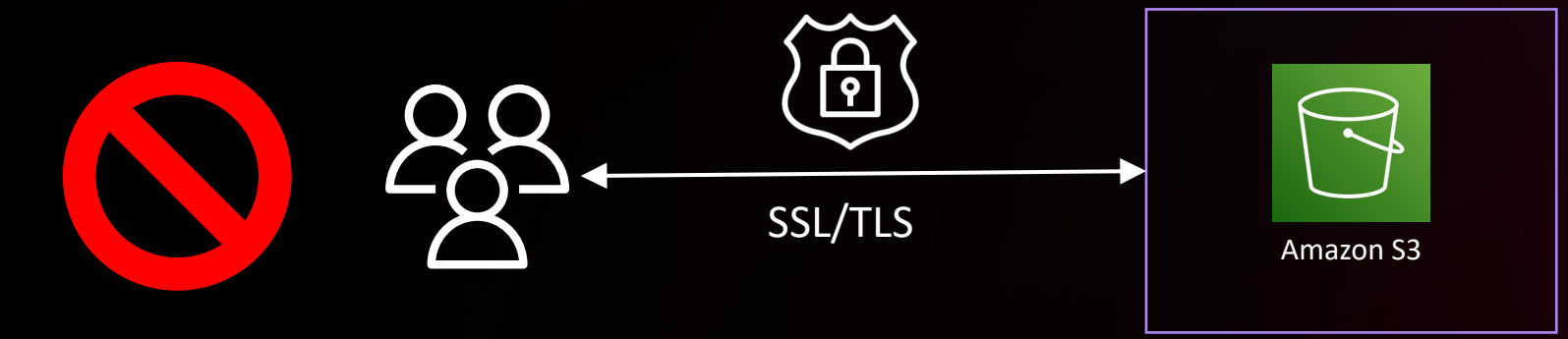
S3 → Block Public Access settings for this account → Edit

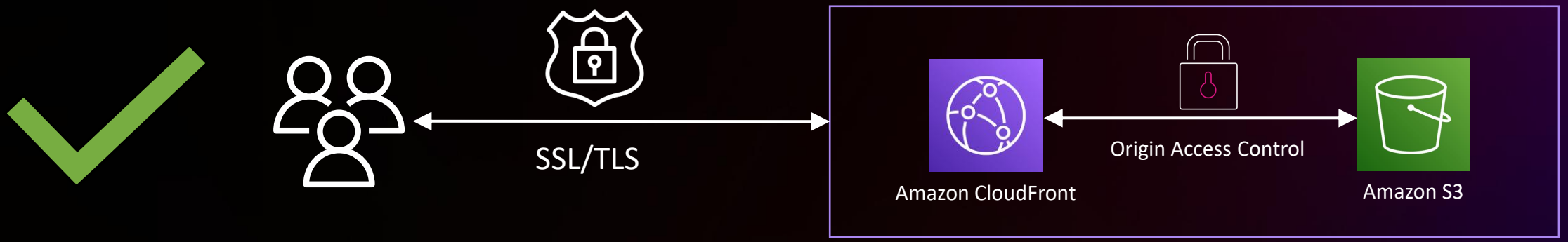
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3 → Amazon CloudFront

Enabling CloudFront for S3

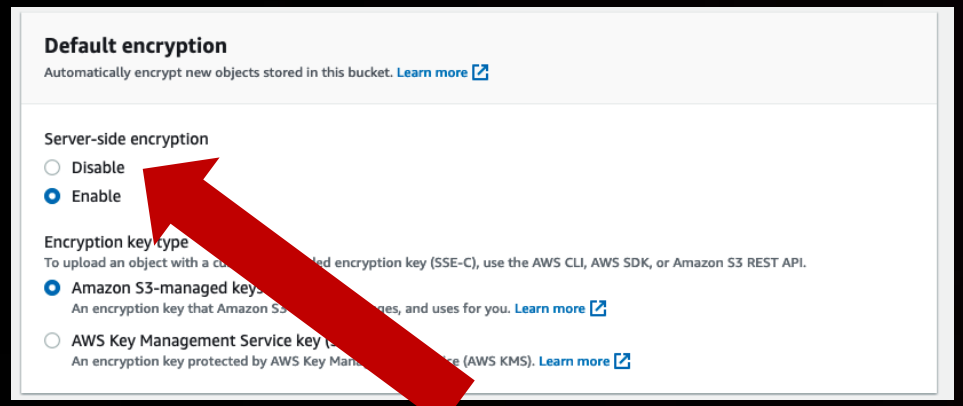
go.aws/3TQkEBJ



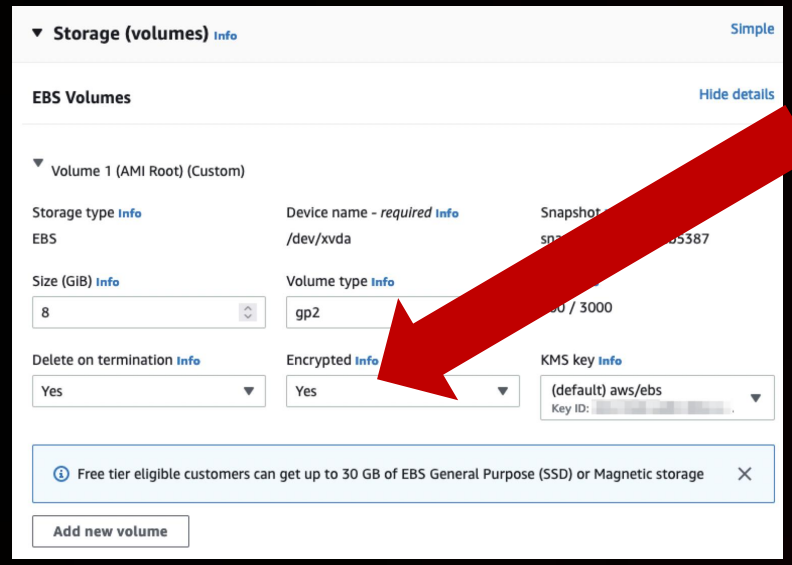


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

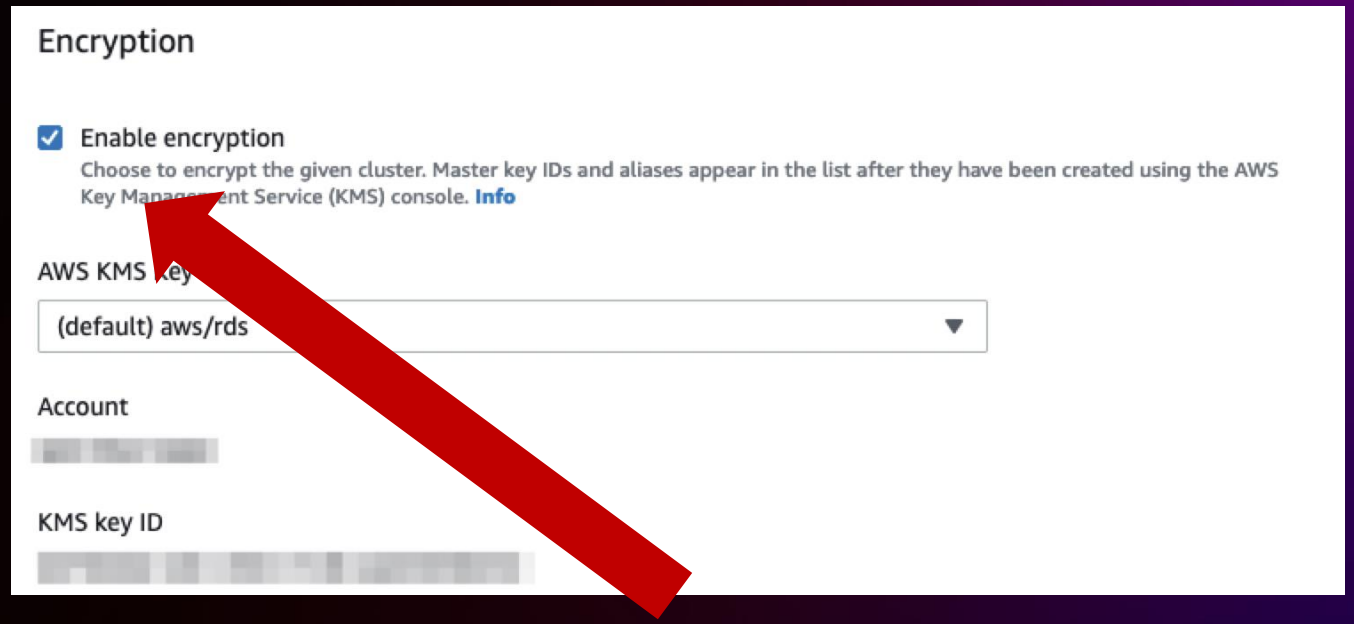
Encrypt storage at rest



Amazon S3 → Create bucket → Default encryption



EC2 → Launch instance → Storage (volumes) → Advanced



Amazon RDS → Create a database → Additional configuration

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EBS/Amazon RDS Public Snapshots

Amazon EBS Public Snapshots

Checks the permission settings for your Amazon Elastic Block Store (Amazon EBS) volume snapshots and alerts you if any snapshots are marked as public.

1 EBS snapshots are marked as public.

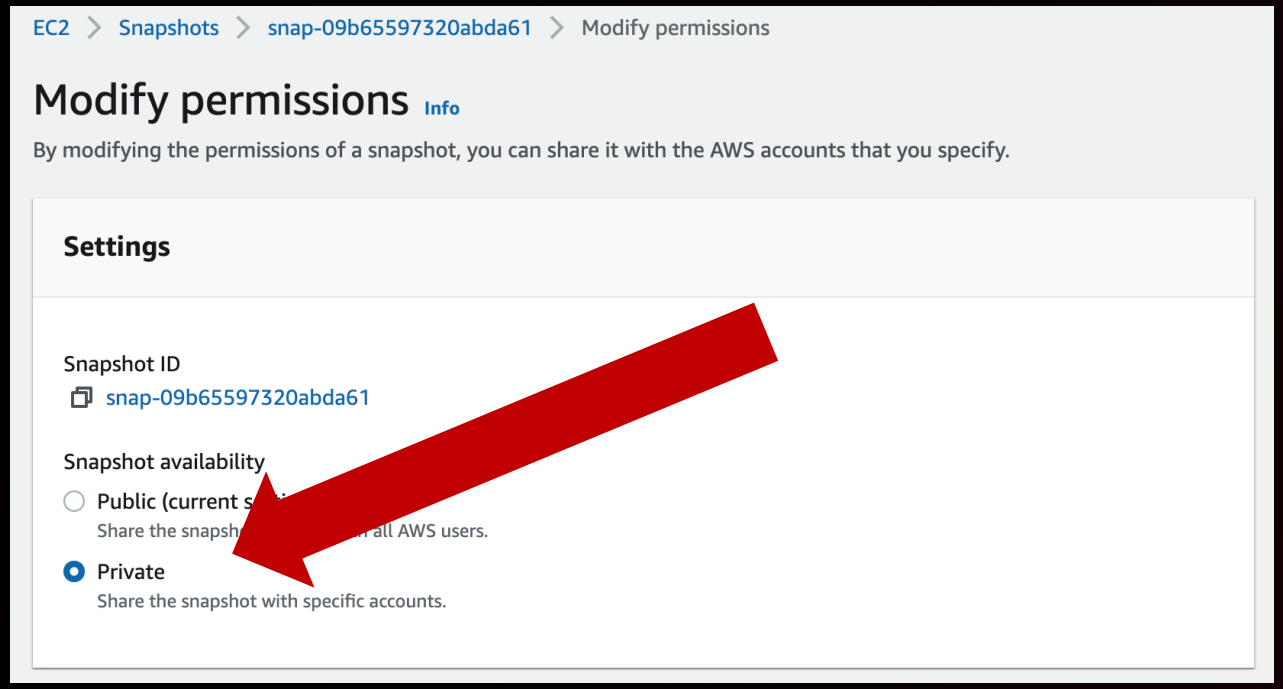
Amazon RDS Public Snapshots

Checks the permission settings for your Amazon Relational Database Service (Amazon RDS) DB snapshots and alerts you if any snapshots are marked as public.

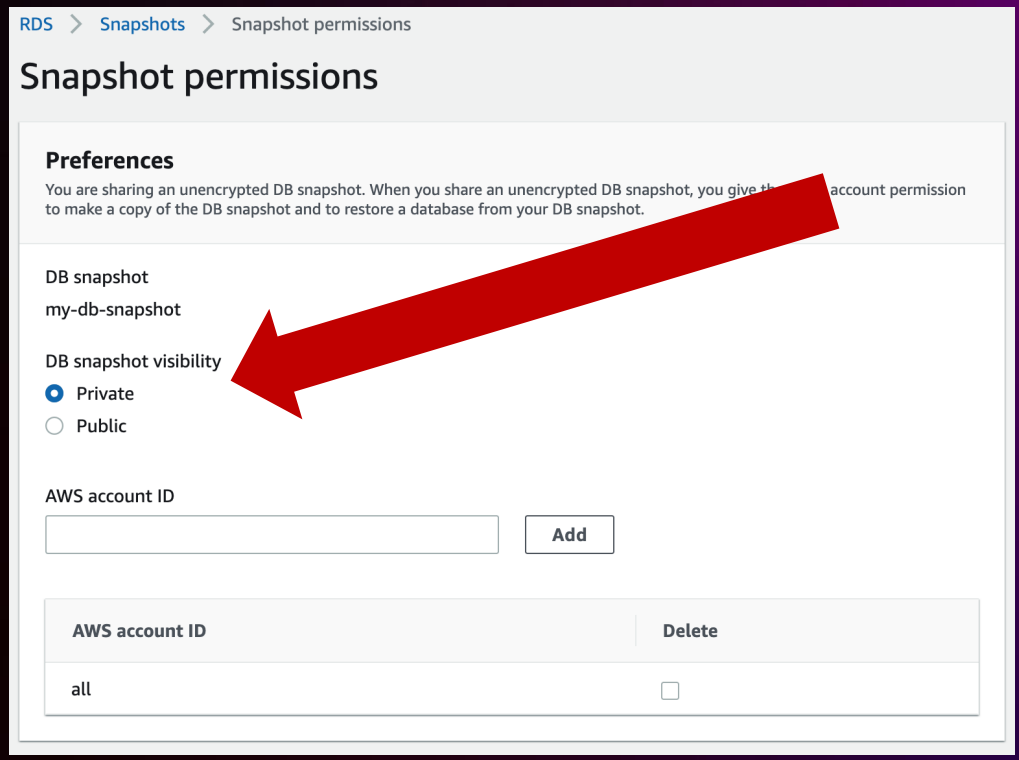
1 RDS snapshots are marked as public.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modify EBS & RDS snapshot permissions



Amazon EC2 → Snapshots → Select Snapshot → Permissions → Modify permissions



Amazon RDS → Snapshots → Select Snapshot → Actions → Share snapshot

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Second Day Recap/Takeaways

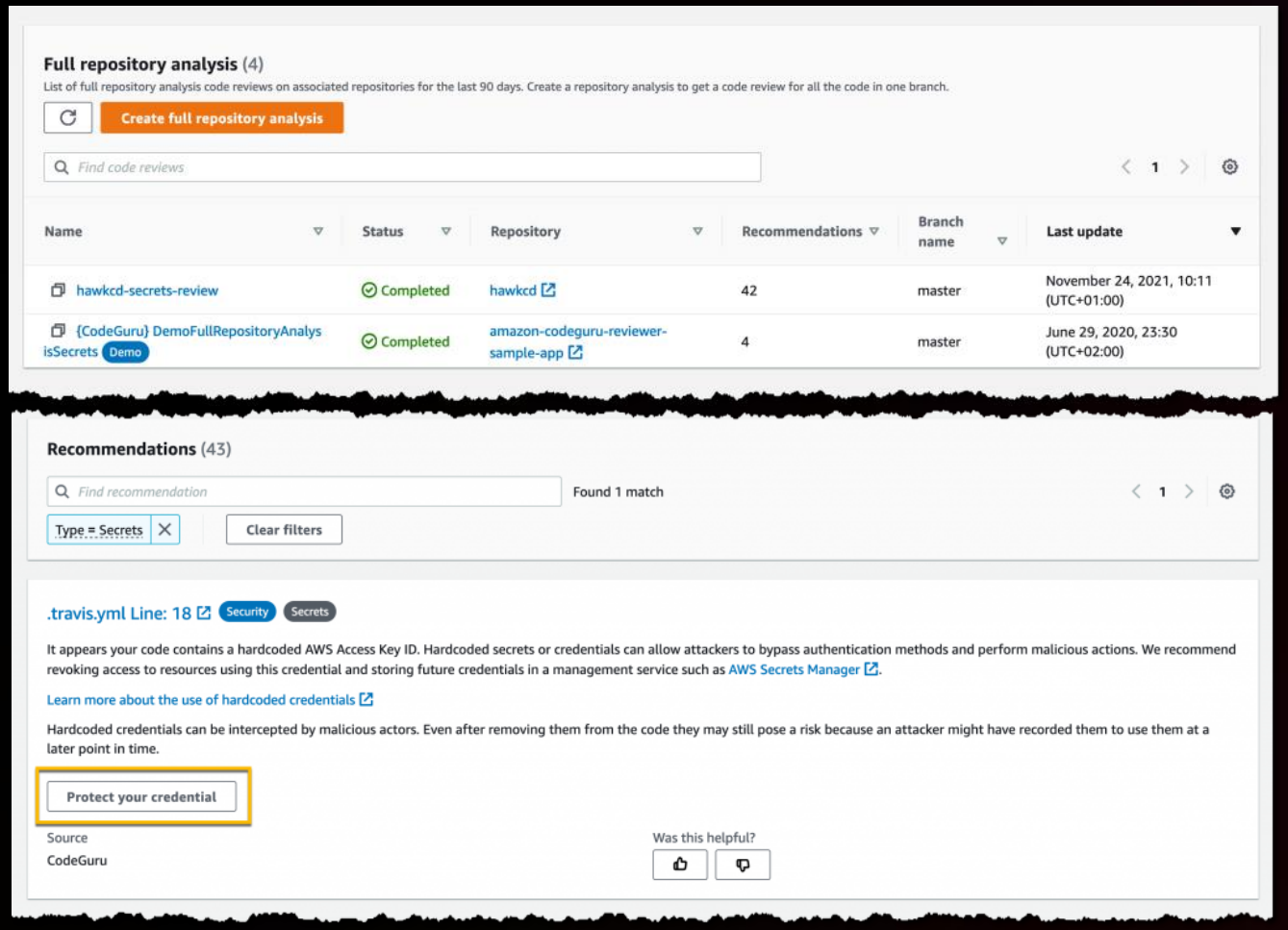
1. Prevent public access to private S3 buckets
2. Encrypt everything
3. Keep data snapshots private

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Third Day

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detect and remediate exposed secrets

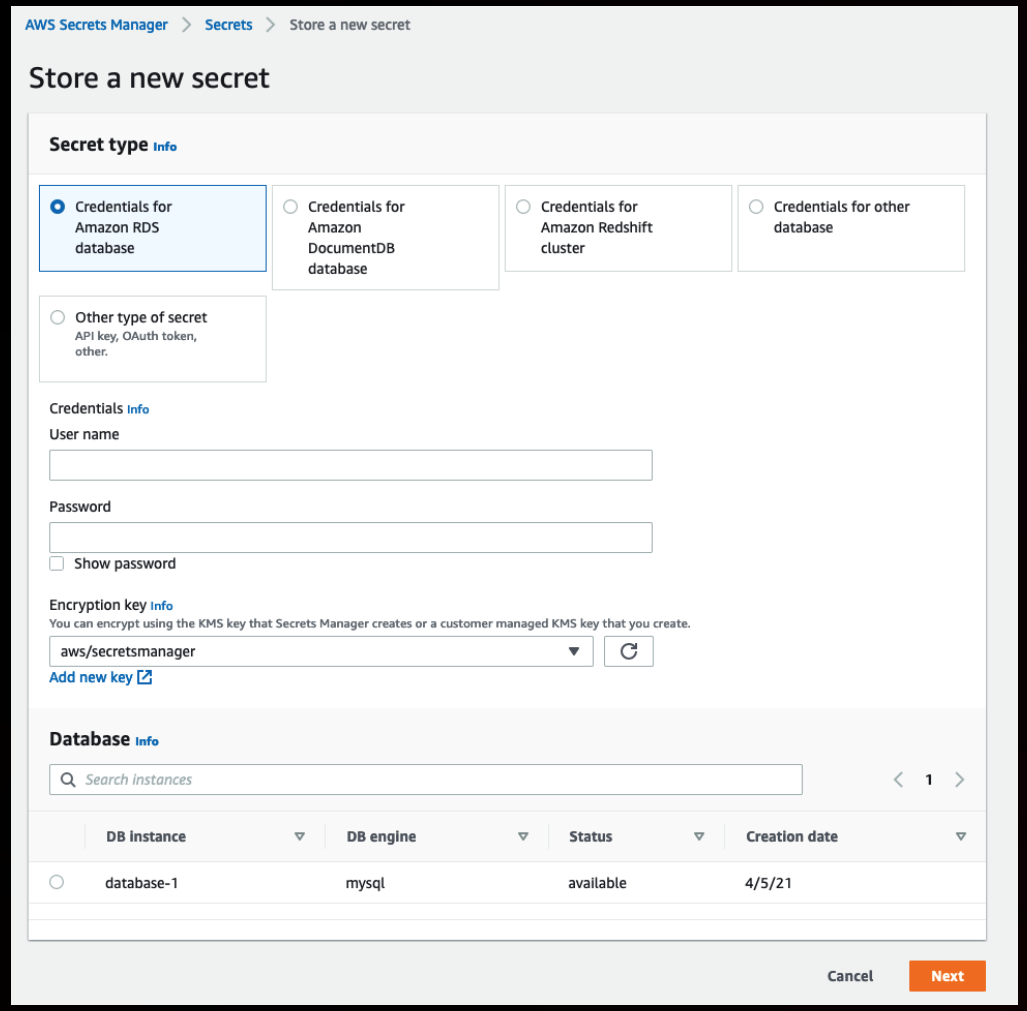


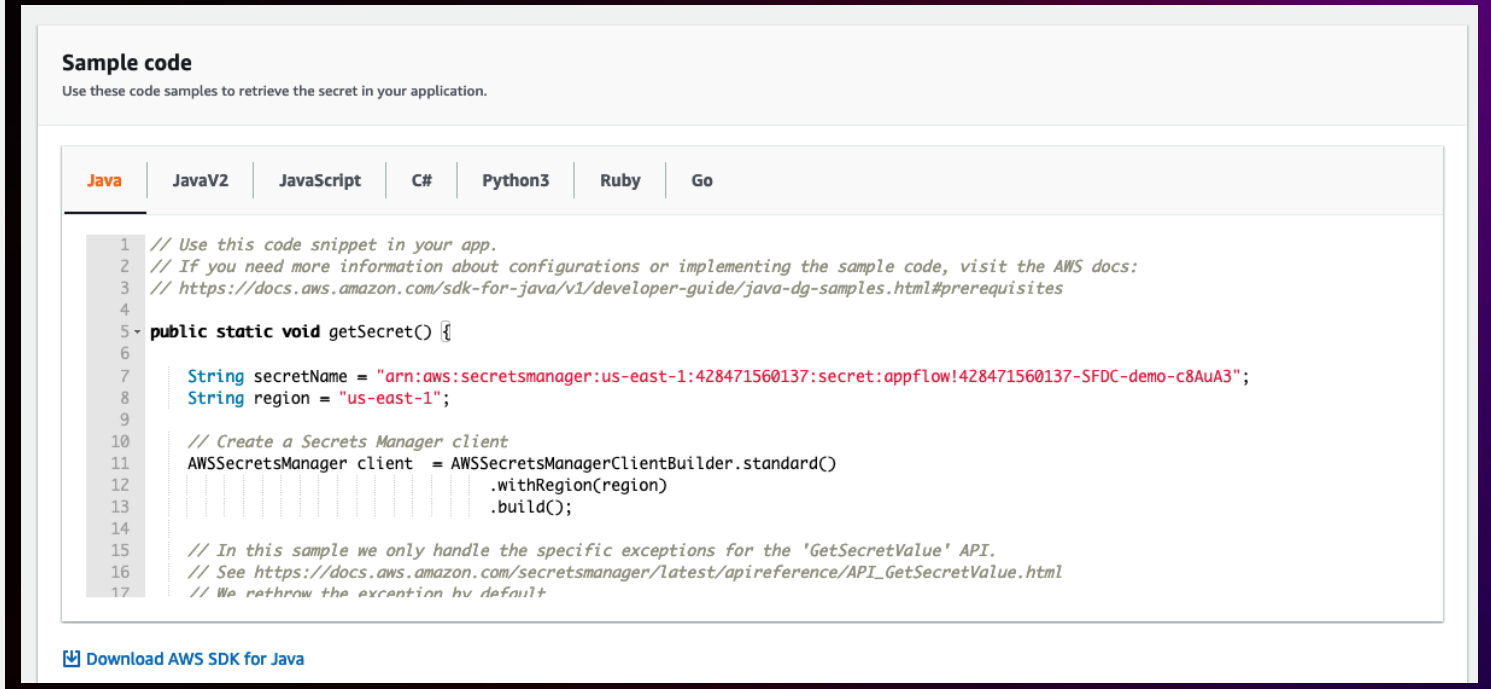

```
14  jdk:
15  - oraclejdk8
16  deploy:
17    provider: s3
18    access_key_id: AKIAIEBRQC6XJRYKOXHQ
19    secret_access_key:
20      secure: AEwlCQBuqwccLhHCbgof0pElzVHyD1vpKrIaDN5
21    bucket: drop-zone
22    skip_cleanup: true
```

Amazon CodeGuru → Associate repository and run analysis

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use ephemeral secrets





AWS Secrets Manager → Secrets → Store a new secret

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tip

Avoid committing secrets!

AWS Labs
git-secrets tool



bit.ly/3glsupd

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What else?

- Developer access to the infrastructure

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What else?

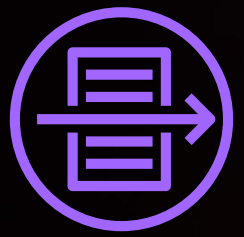
- Developer access to the infrastructure
- Threat detection

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty



Amazon Route 53
Resolver logs



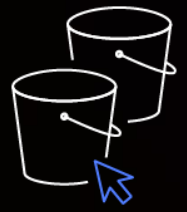
Amazon VPC
Flow Logs



AWS CloudTrail
events



Amazon GuardDuty



Amazon S3
data plane events



Amazon EKS control
plane logs

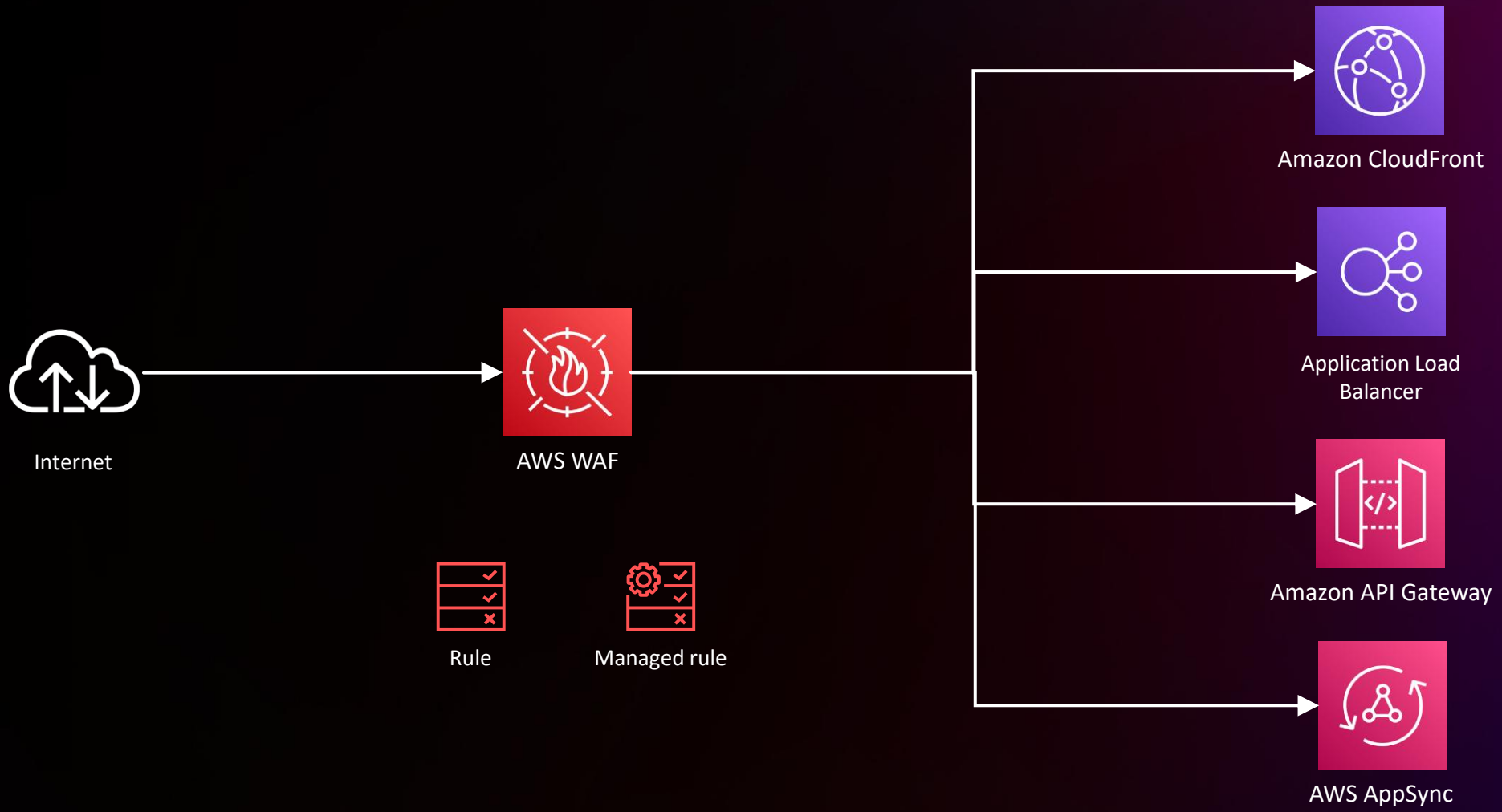
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What else?

- Developer access to the infrastructure
- Threat detection
- Edge protection

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use edge protection services



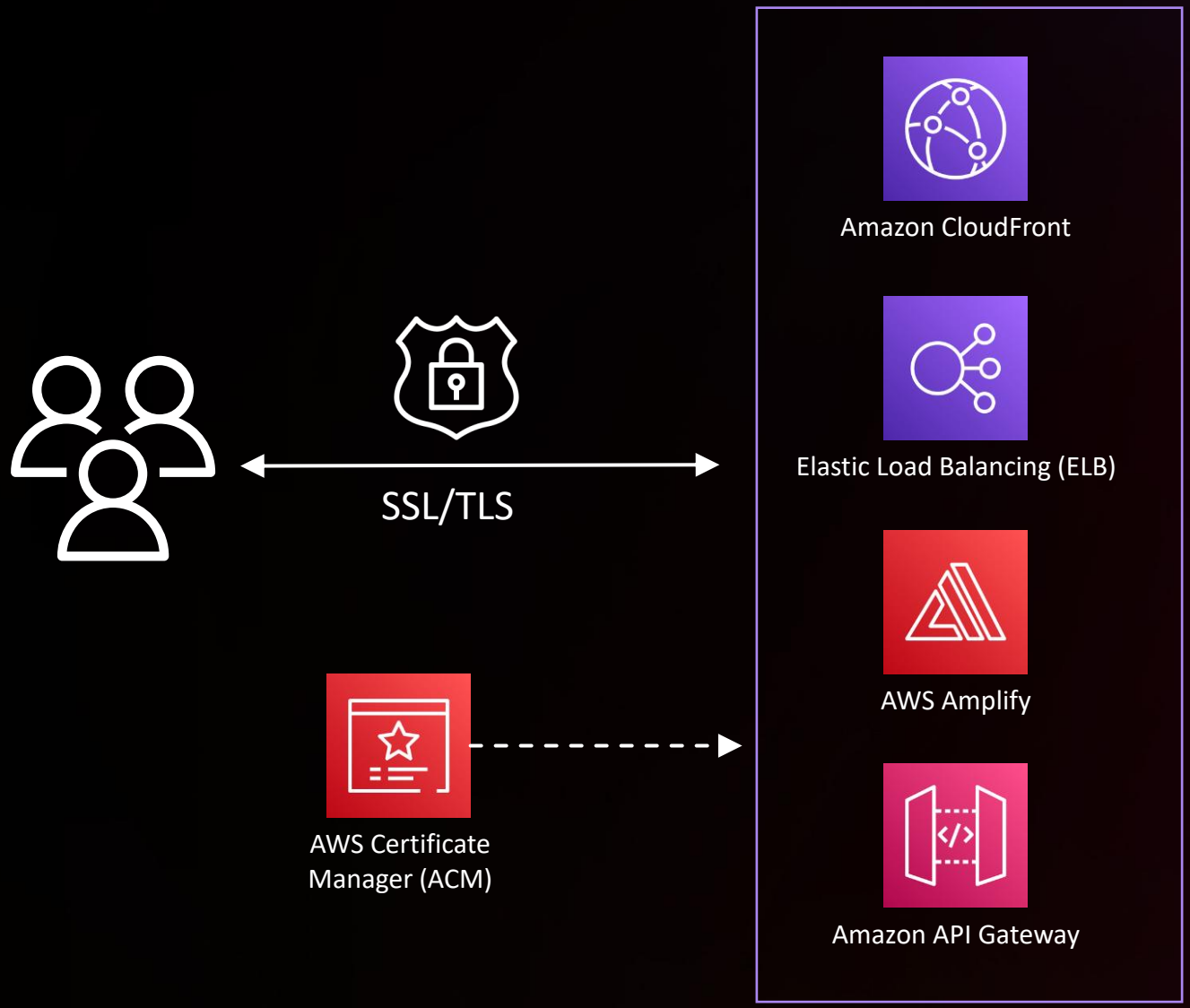
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What else?

- Developer access to the infrastructure
- Threat detection
- Edge protection
- Securing network communications

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Require HTTPS for all public web endpoints



Step-by-step guidance on how to enable HTTPS on public endpoints

go.aws/3UNb2JI

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Third Day Recap/Takeaways

1. Protect your secrets
2. Secure your resources
3. Threat protection and edge protection

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Related sessions

Breakout sessions

STP207: Automating and evidencing key compliance security controls

STP306: Evolving your security capabilities through key growth stages

Chalk talks

STP212: Simple steps to prepare your environment for compliance

Startup Loft

STP308: How to manage risk with minimal disruption

Workshops

STP301: Startup security: Techniques to stay secure while building quickly

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Cole Calistra
ccalist@amazon.com

Anya Derbakova
annadrb@amazon.com



Please complete the session survey in the **mobile app**

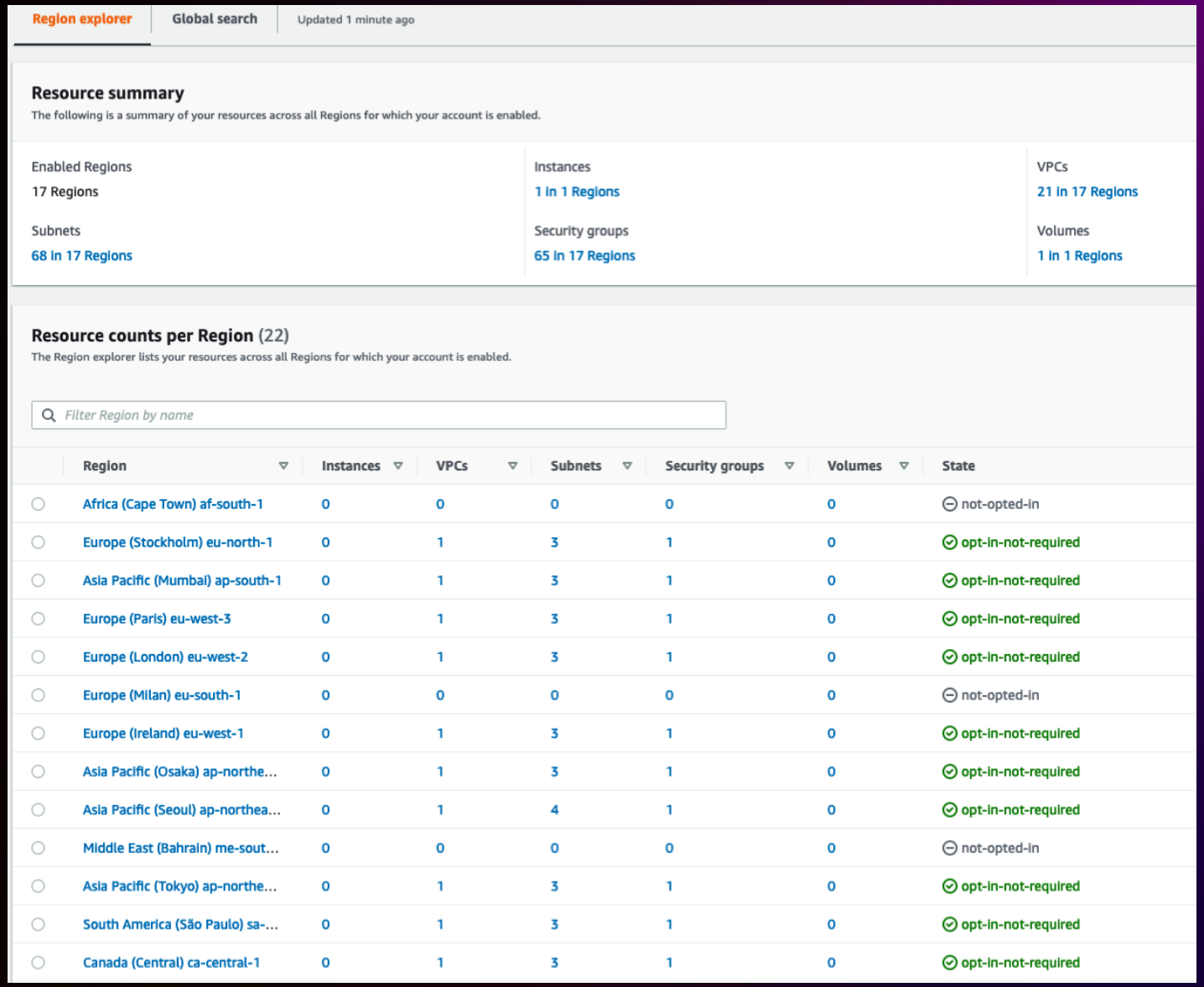
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

First Month and Beyond

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

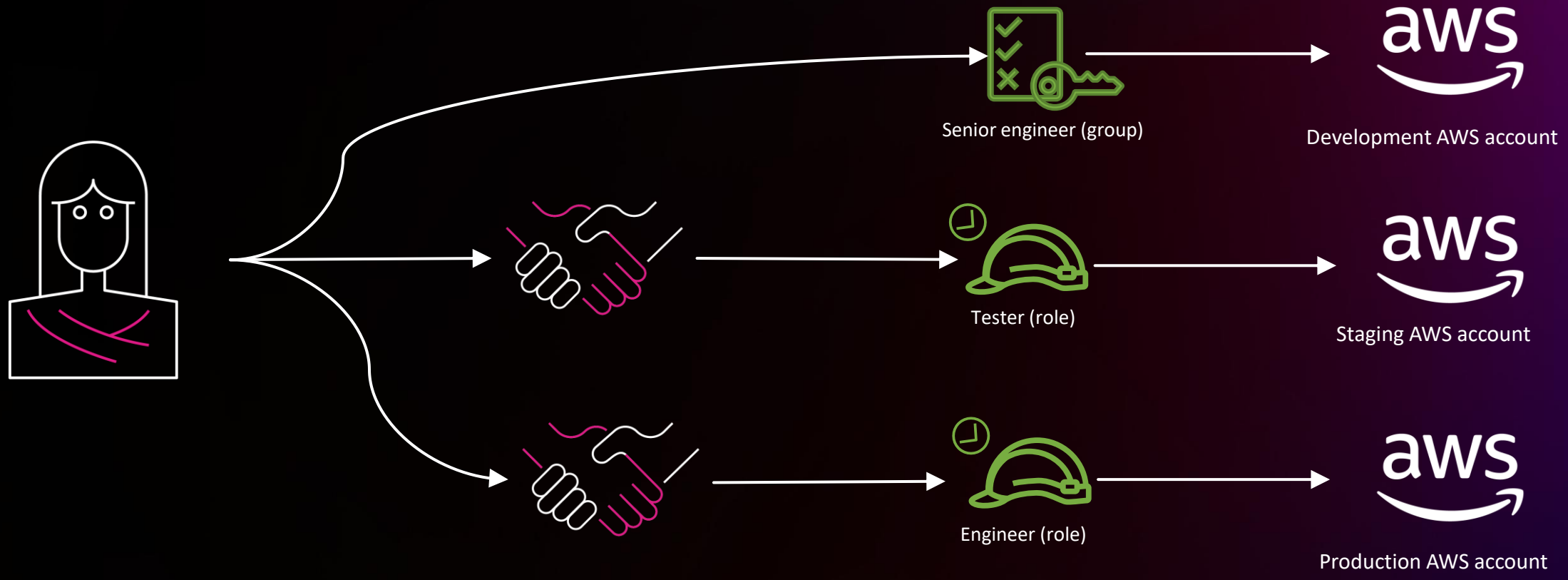
Delete unused resources

1. If you don’t need it, remove it
2. Avoid using the default VPC
3. Use EC2-Global View



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use separate accounts for separate environments



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tip

Transitioning to Multiple Accounts Prescriptive Guidance



go.aws/3OknrC7

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security as code (SaC)

Security services and tooling



Amazon GuardDuty



Amazon Inspector



Amazon Macie



AWS Firewall Manager



AWS Identity and Access Management (IAM)



AWS Security Hub

Infra as code (IaC) templates



AWS CloudFormation



AWS Cloud Development Kit (AWS CDK)

Deployment targets

Dev account

Staging account

Prod account

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

First Month and Beyond Recap/Takeaways

1. Clean up resources
2. Transition to multiple accounts
3. Implement security as code

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Related sessions

Breakout sessions

STP207: Automating and evidencing key compliance security controls

STP306: Evolving your security capabilities through key growth stages

Chalk talks

STP212: Simple steps to prepare your environment for compliance

Startup Loft

STP308: How to manage risk with minimal disruption

Workshops

STP301: Startup security: Techniques to stay secure while building quickly

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Cole Calistra
ccalist@amazon.com

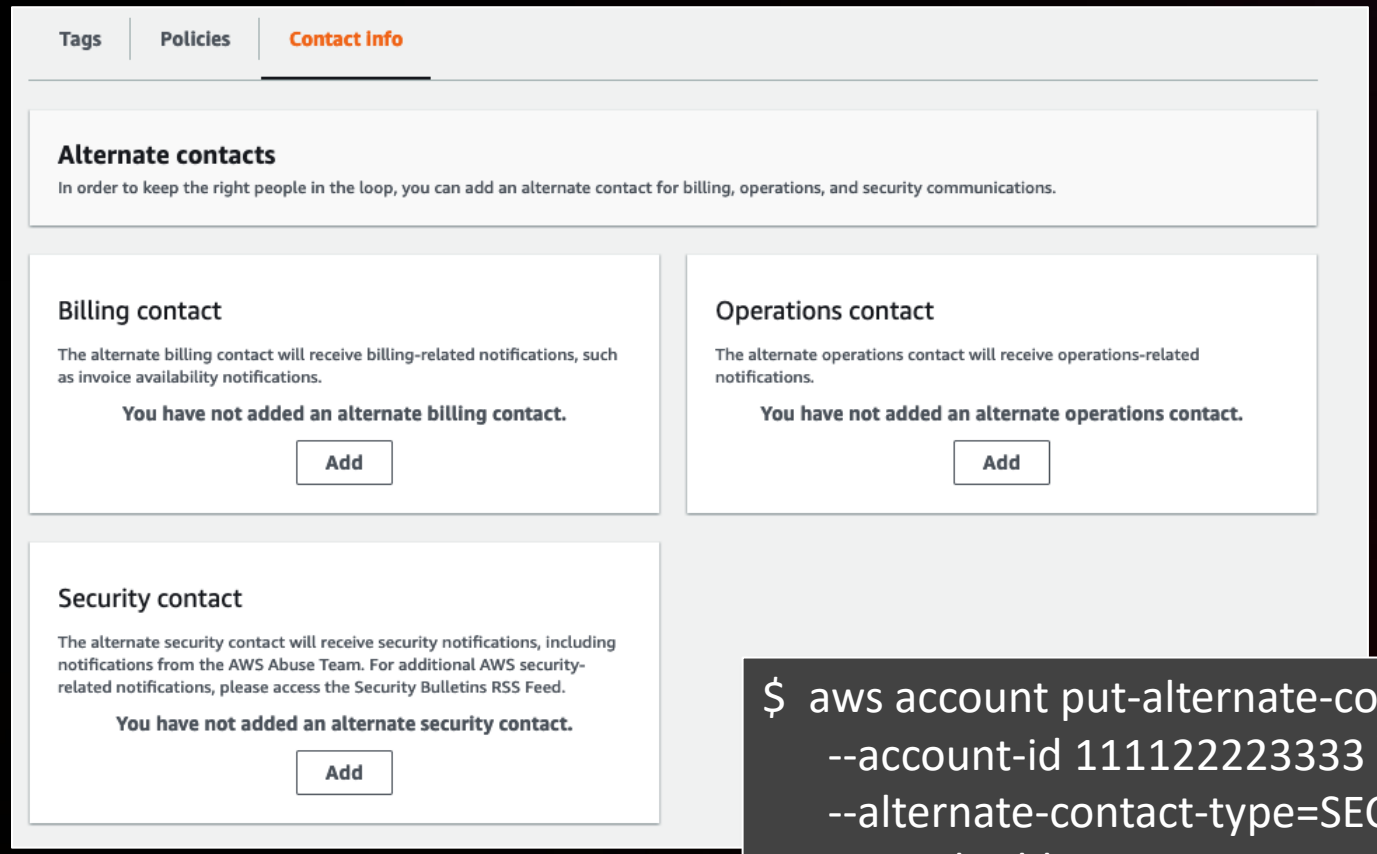
Anya Derbakova
annadrb@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting account-level contacts




```
$ aws account put-alternate-contact \
    --account-id 111122223333 \
    --alternate-contact-type=SECURITY \
    --email-address=security-contact@example.com \
    --phone-number="+1(555)555-5555" \
    --title="Security Contact" \
    --name="Mary Major"
```

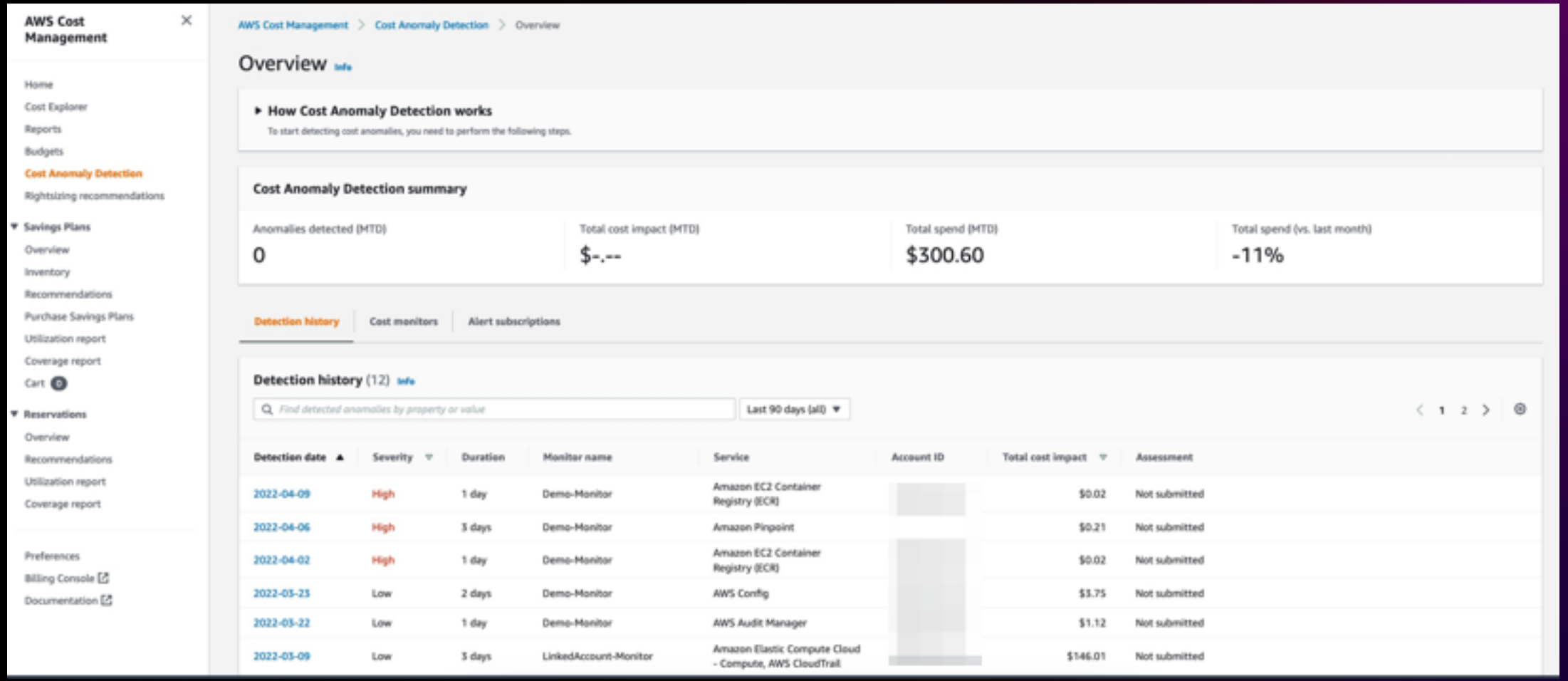
Script to manage contacts

go.aws/3tMvTQM

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tip

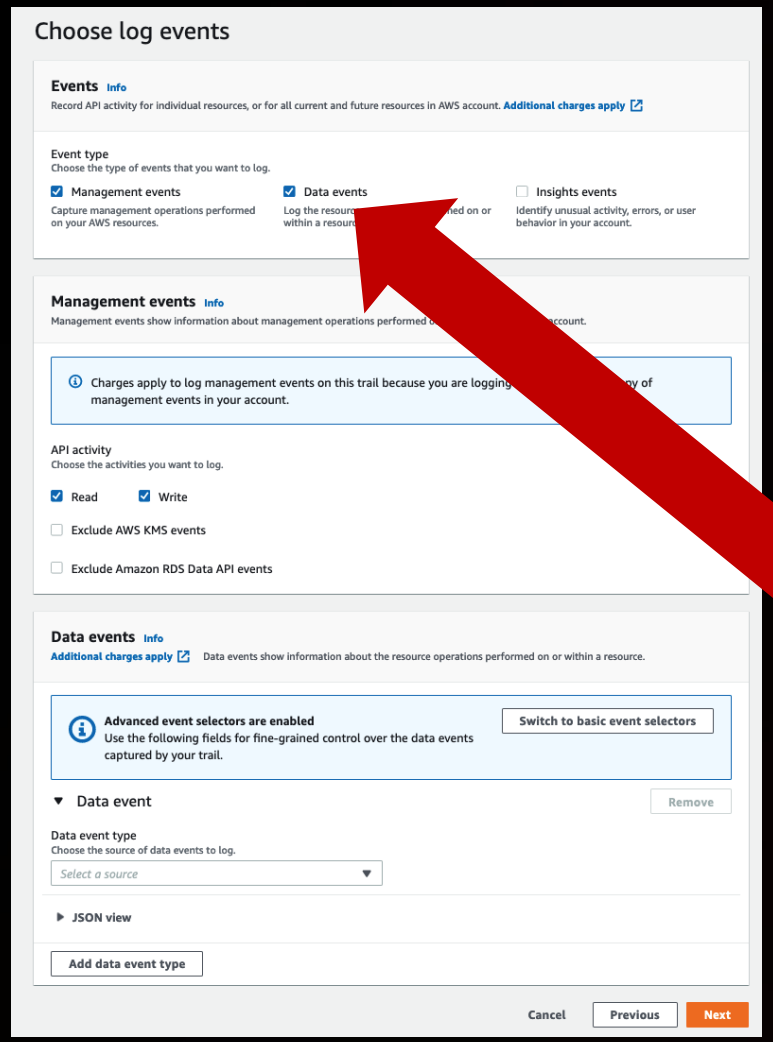
Turn on AWS Cost Anomaly Detection

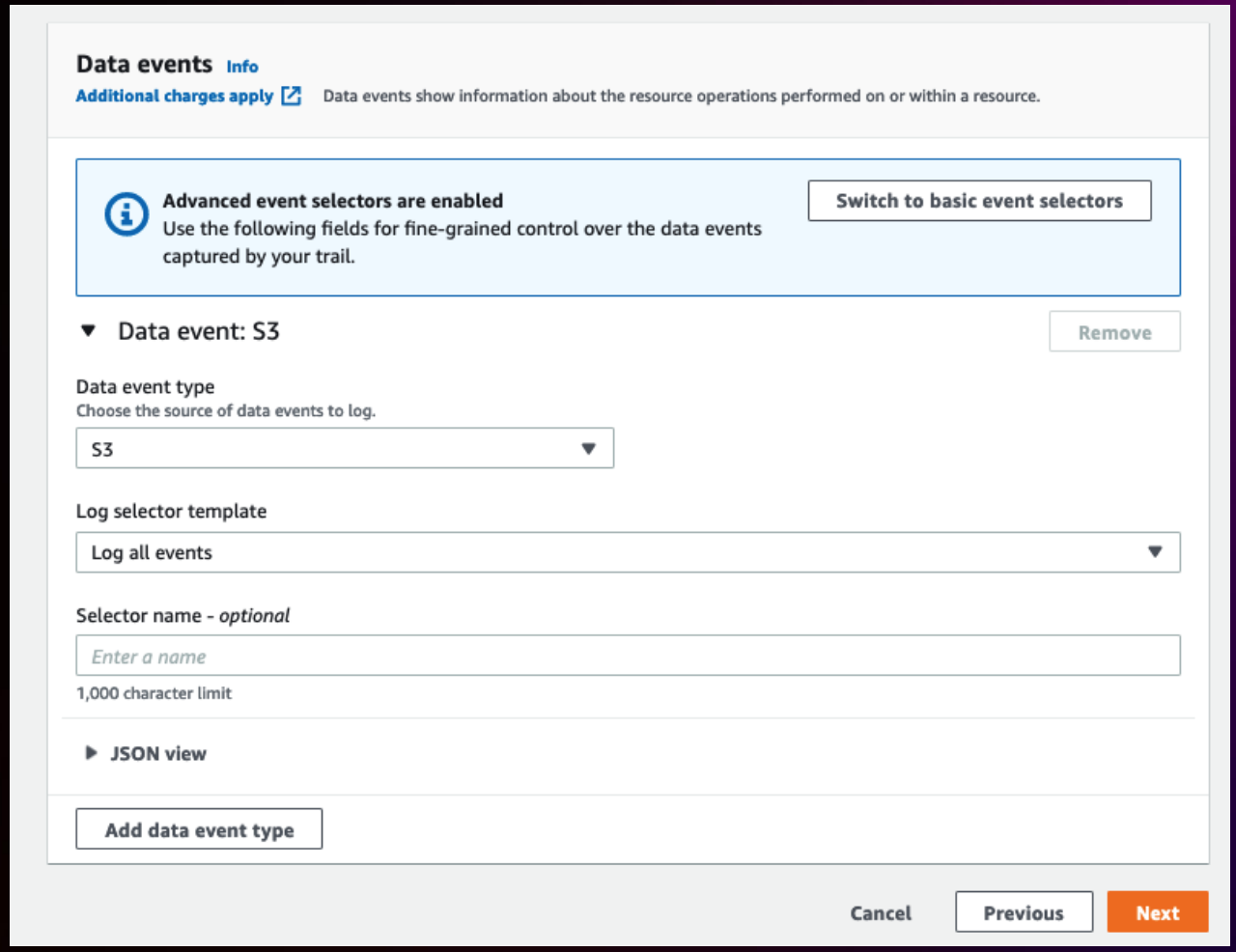


AWS Cost Explorer → Cost Anomaly Detection

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Log data events for Amazon S3 buckets

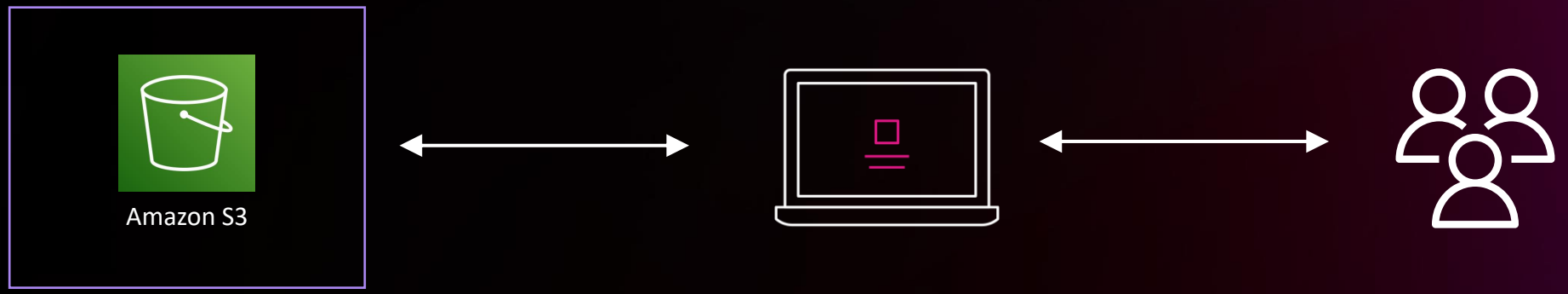




AWS CloudTrail → Trails → Create trail

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Accessing Amazon S3 From Web Browser

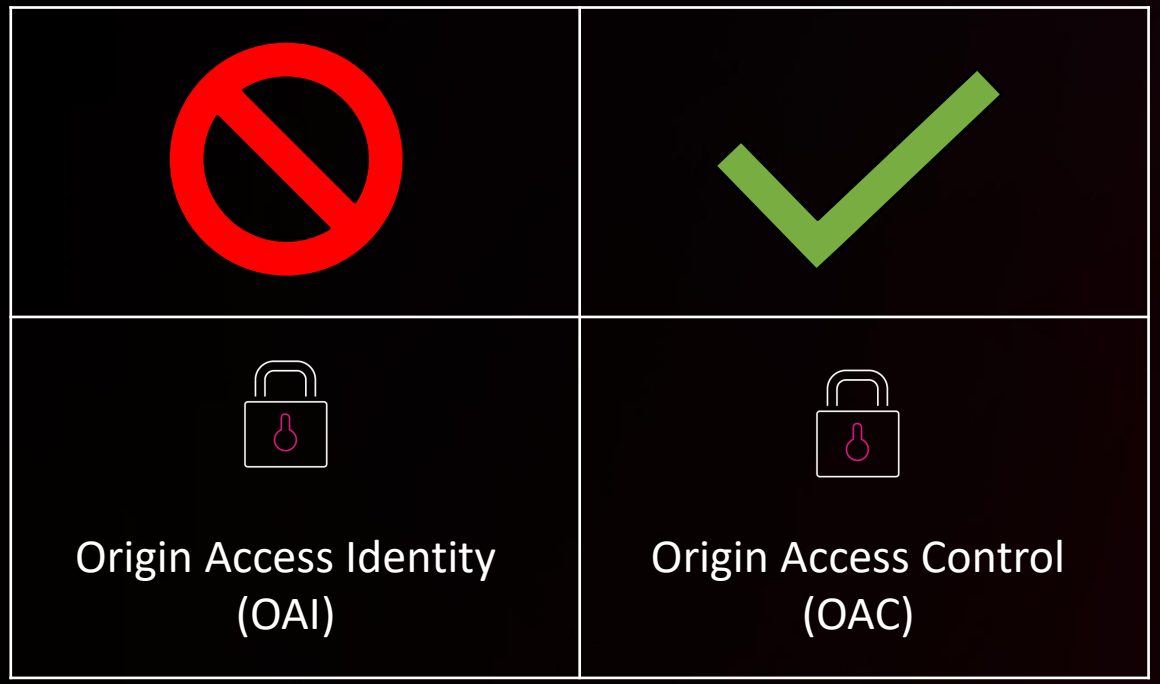


https://bucket-name.s3.region-code.amazonaws.com/key-name

https://s3.region-code.amazonaws.com/bucket-name/key-name

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront OAC vs. OAI

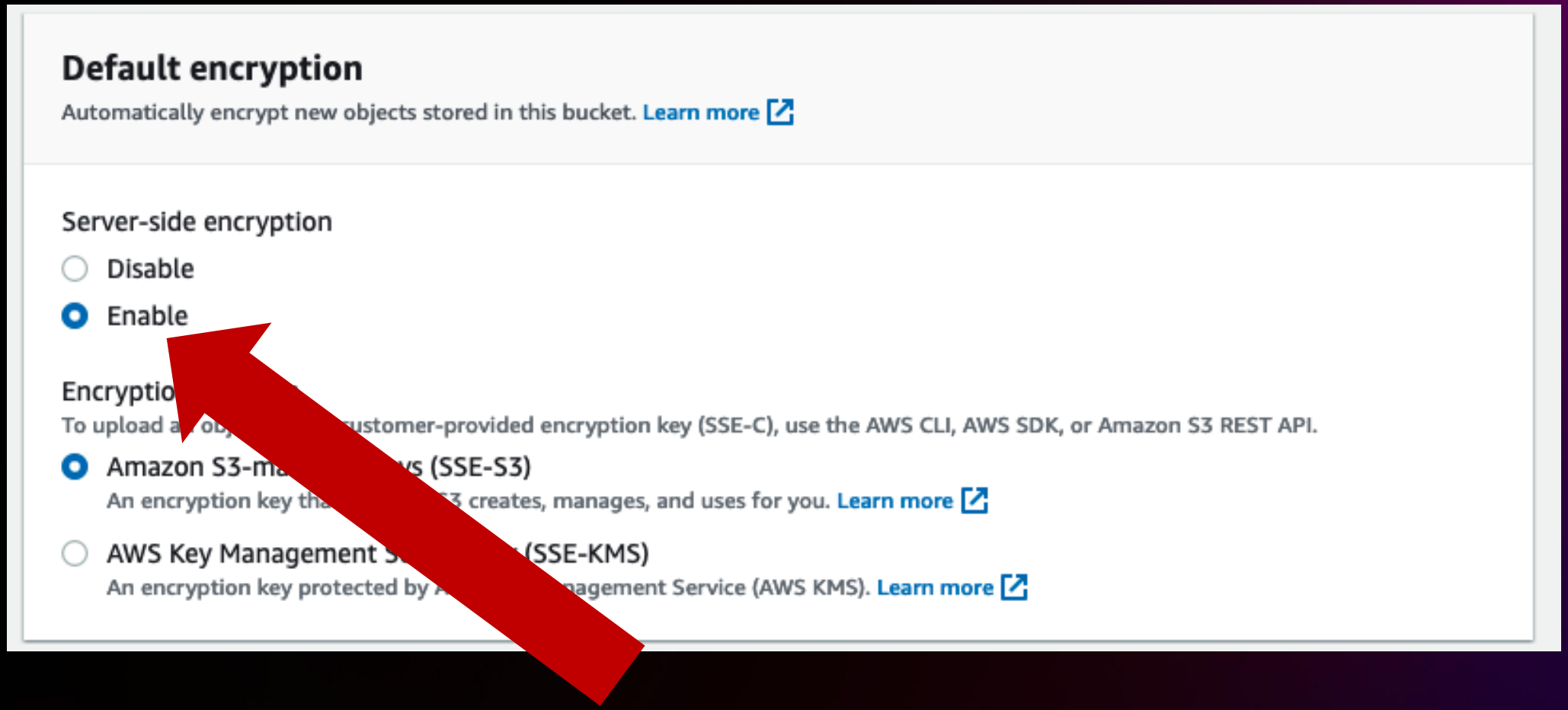


Step-by-step guidance
on how to migrate to
Origin Access Control

go.aws/3ArieT4

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

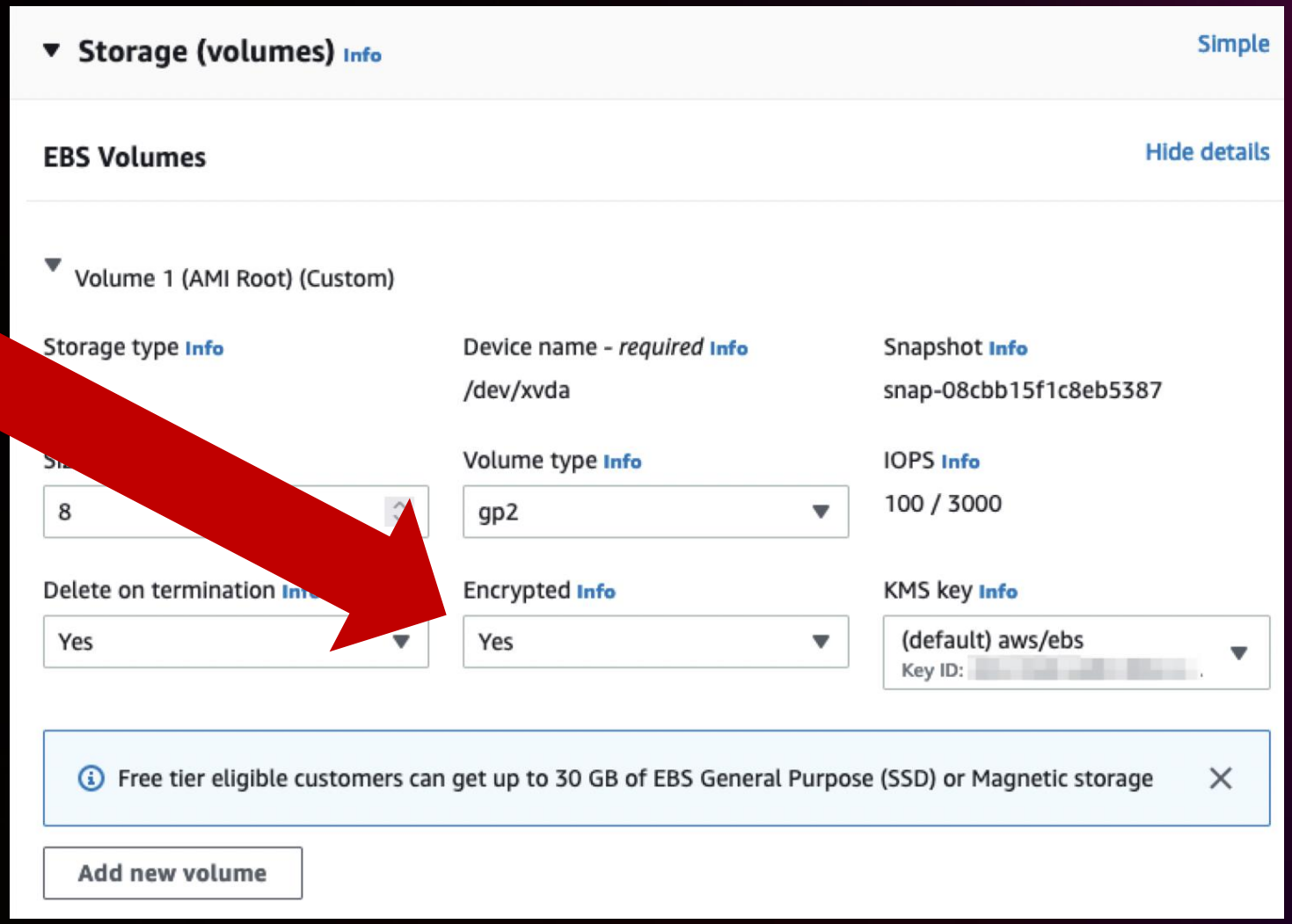
Encrypt Amazon S3 buckets



Amazon S3 → Create bucket → Default encryption

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

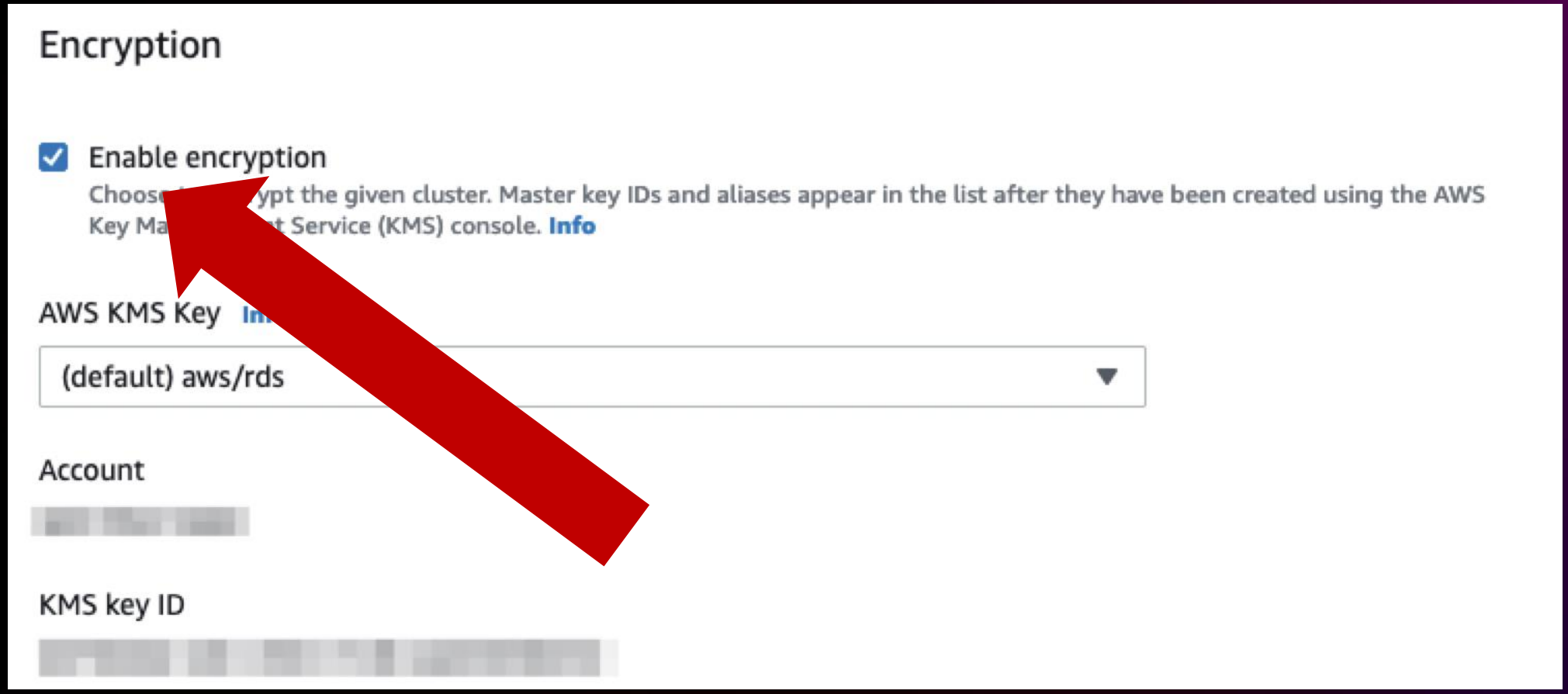
Encrypt Amazon EBS volumes



Amazon EC2 → Launch instance → Storage (volumes) → Advanced

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

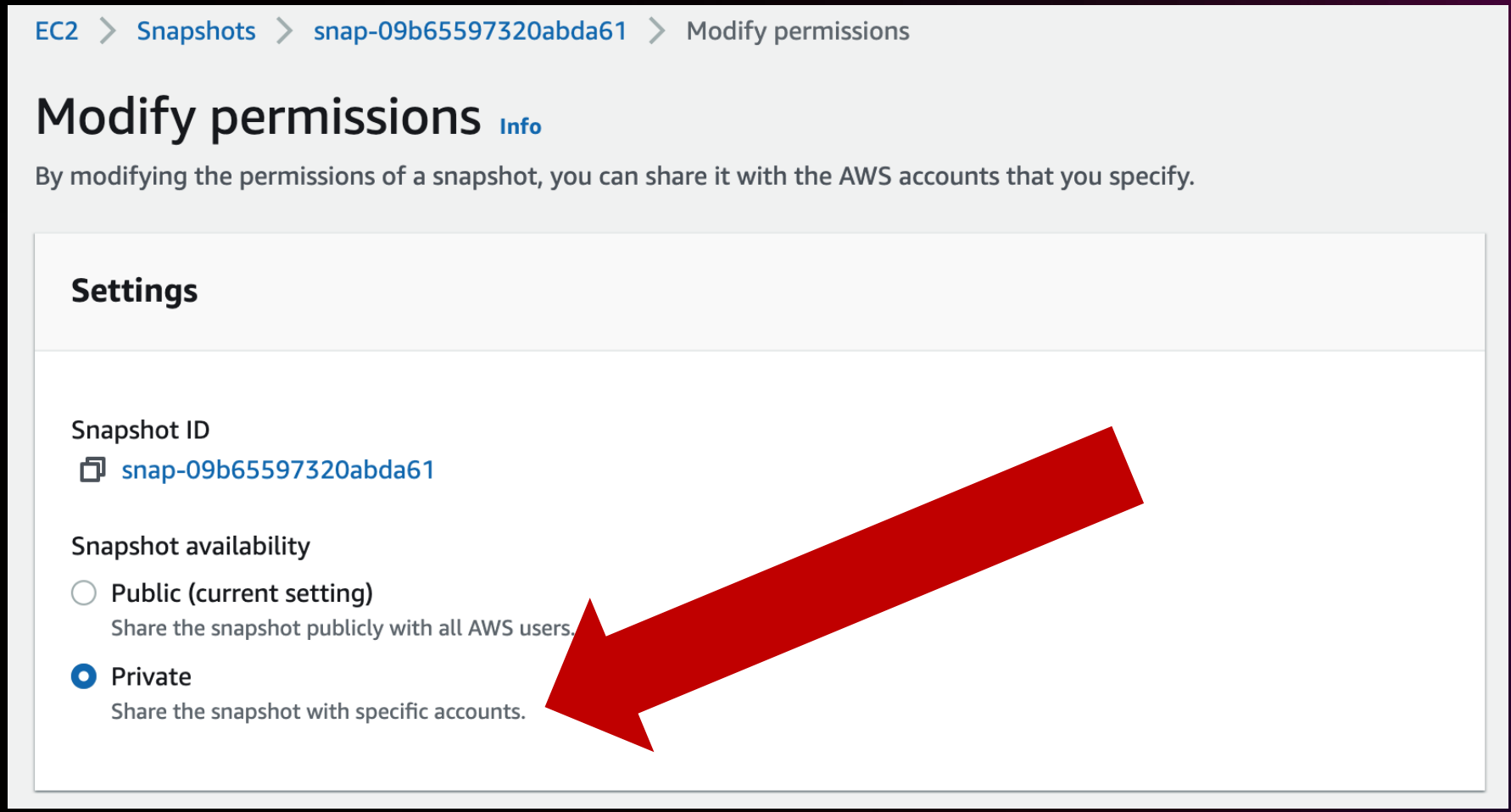
Encrypt Amazon RDS databases



Amazon RDS → Create a database → Additional configuration

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

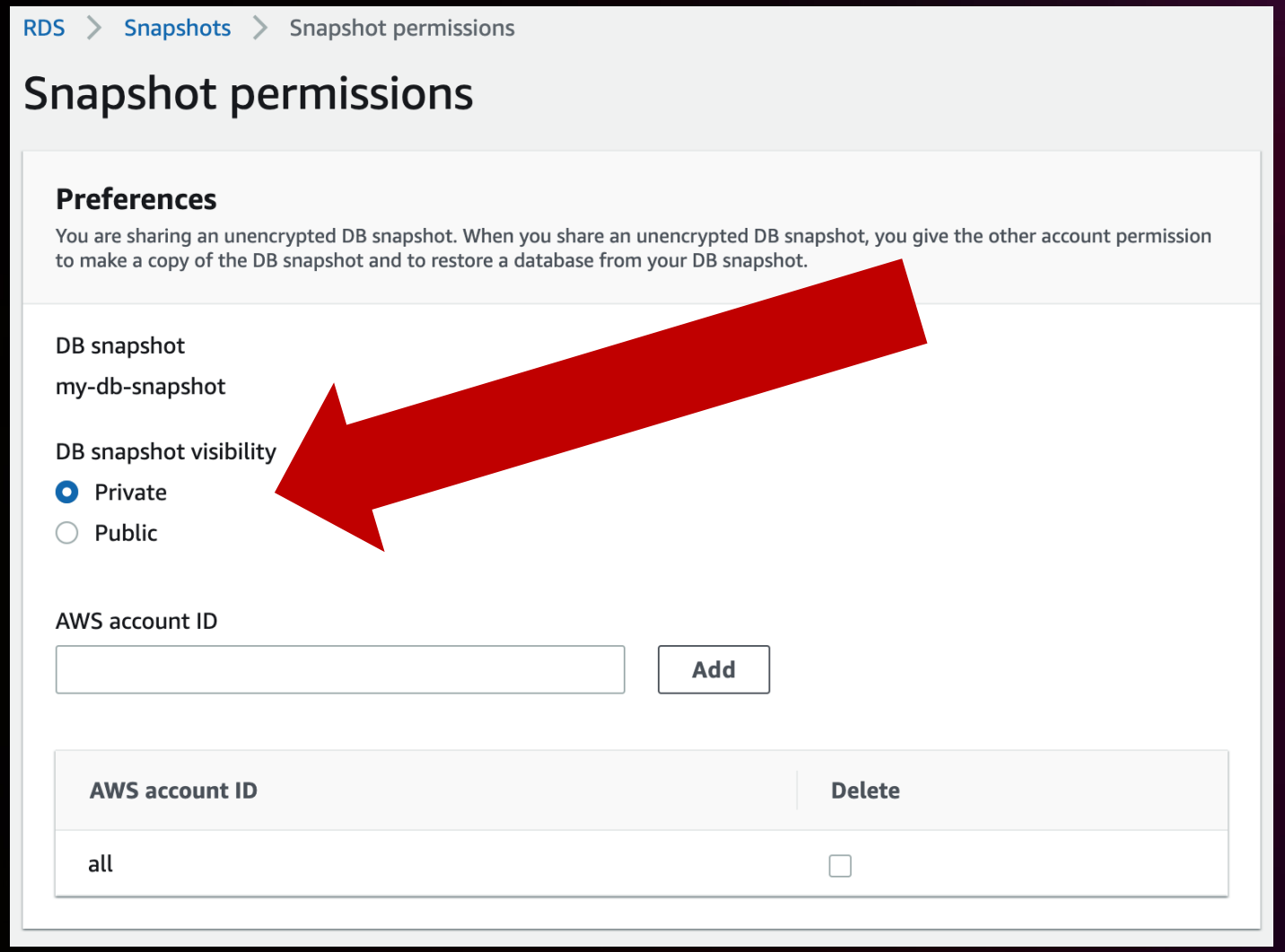
Modify Amazon EBS Snapshot Permissions



Amazon EC2 → Snapshots → Select Snapshot → Permissions → Modify permissions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

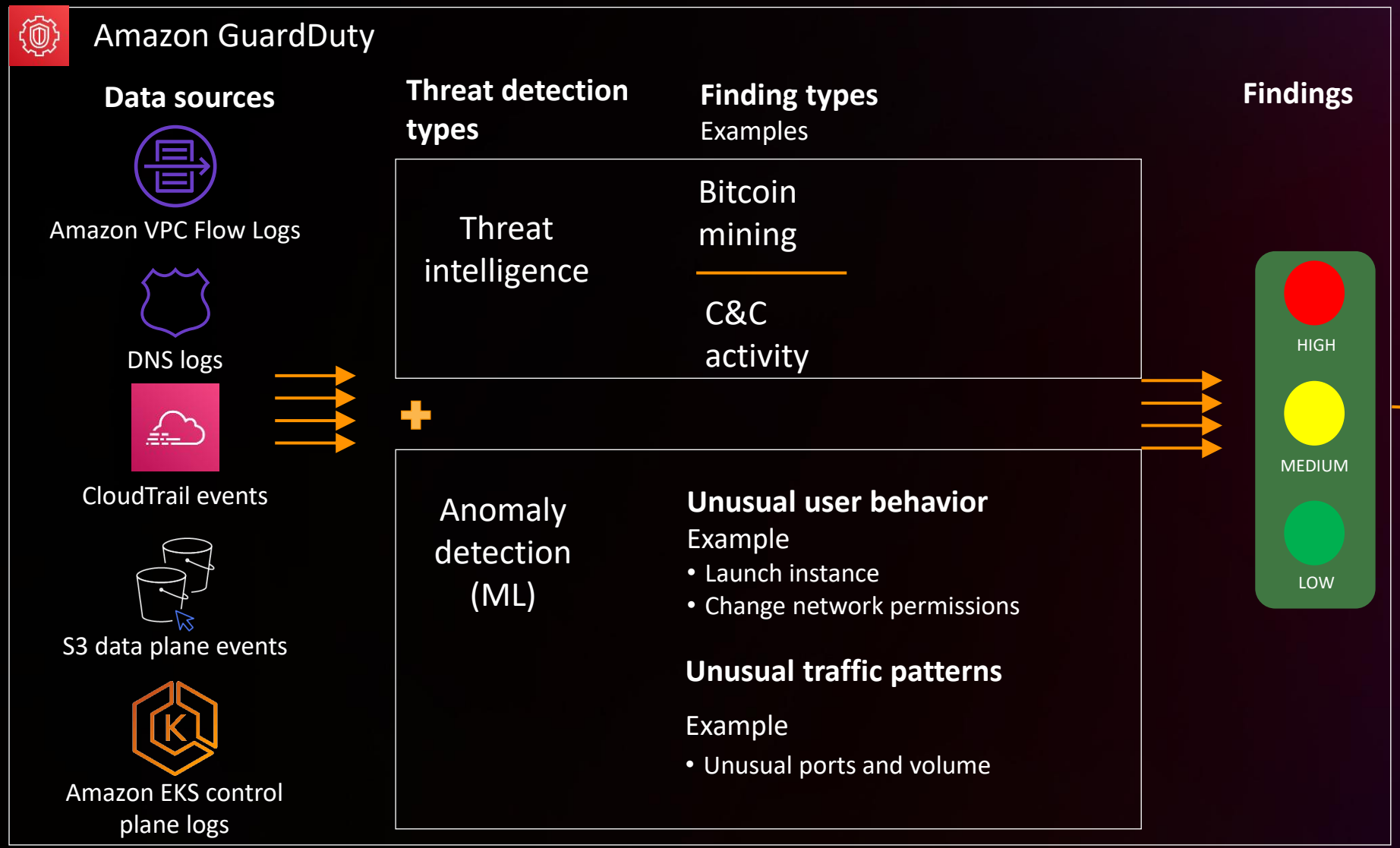
Modify Amazon RDS Snapshot Permissions



Amazon RDS → Snapshots → Select Snapshot → Actions → Share snapshot

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does Amazon GuardDuty work?



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tips

1. Turn on GuardDuty in all the AWS Regions
2. Turn on protection for Amazon S3 and Amazon EKS

Script to turn on GuardDuty in all the Regions



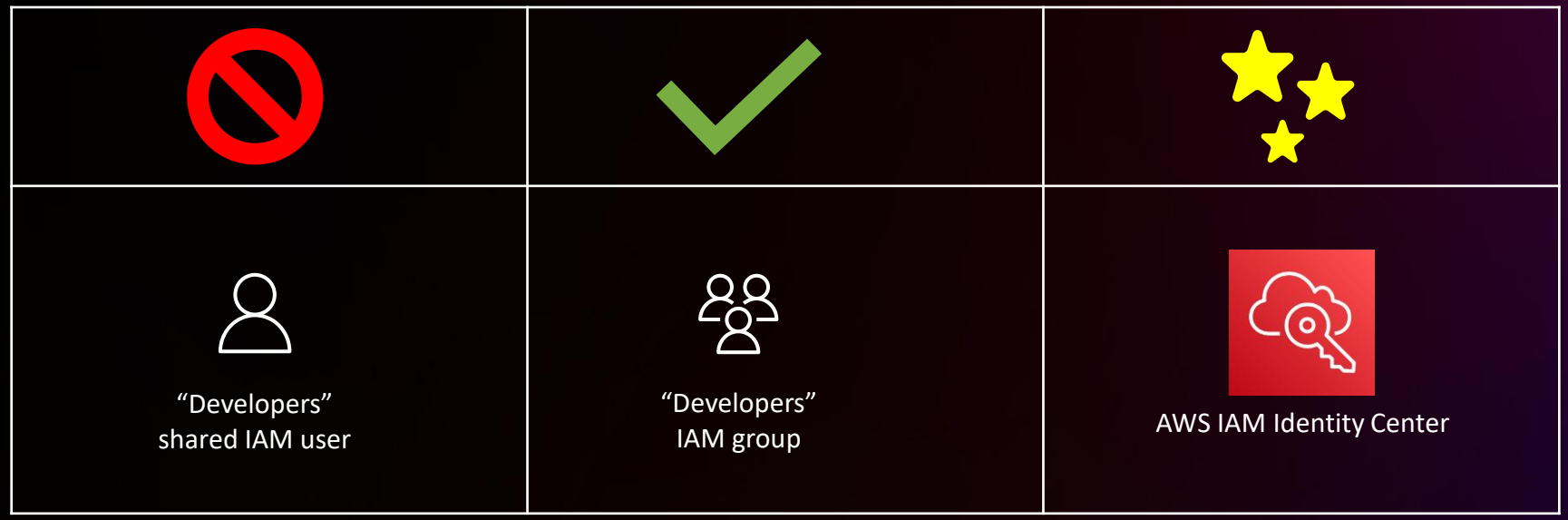
bit.ly/3V3J0Zu

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

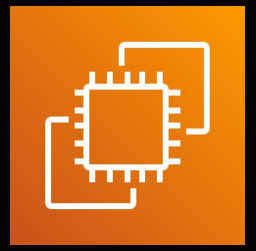
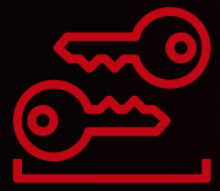
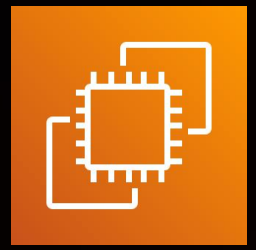
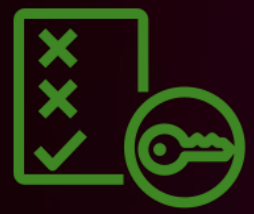
Configure console access

1. Have an IAM user for each human that accesses AWS
2. Don’t share credentials
3. Require MFA for all
4. Grant access to IAM groups, not users



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

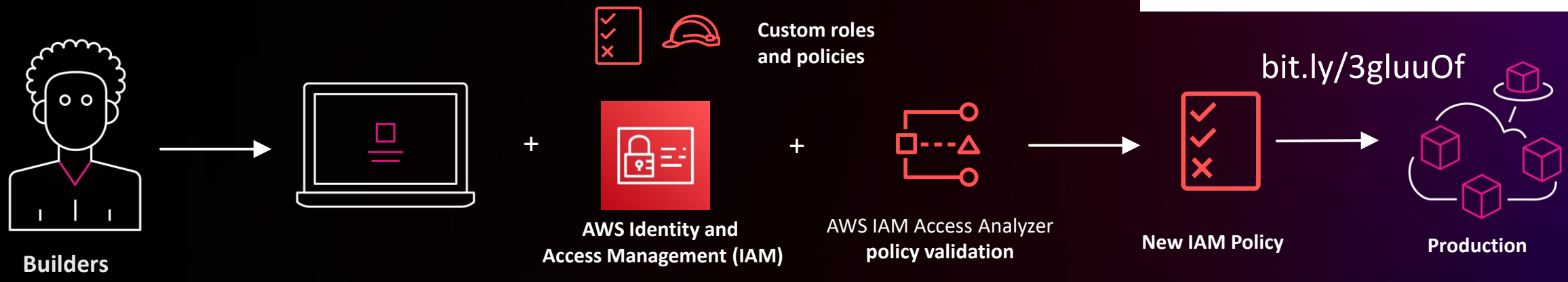
Use IAM roles for permissions

	 Amazon EC2	 Long-term security credential	 User policy	 Amazon S3
	 Amazon EC2	 Temporary security credential	 Amazon S3 policy	 Amazon S3

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

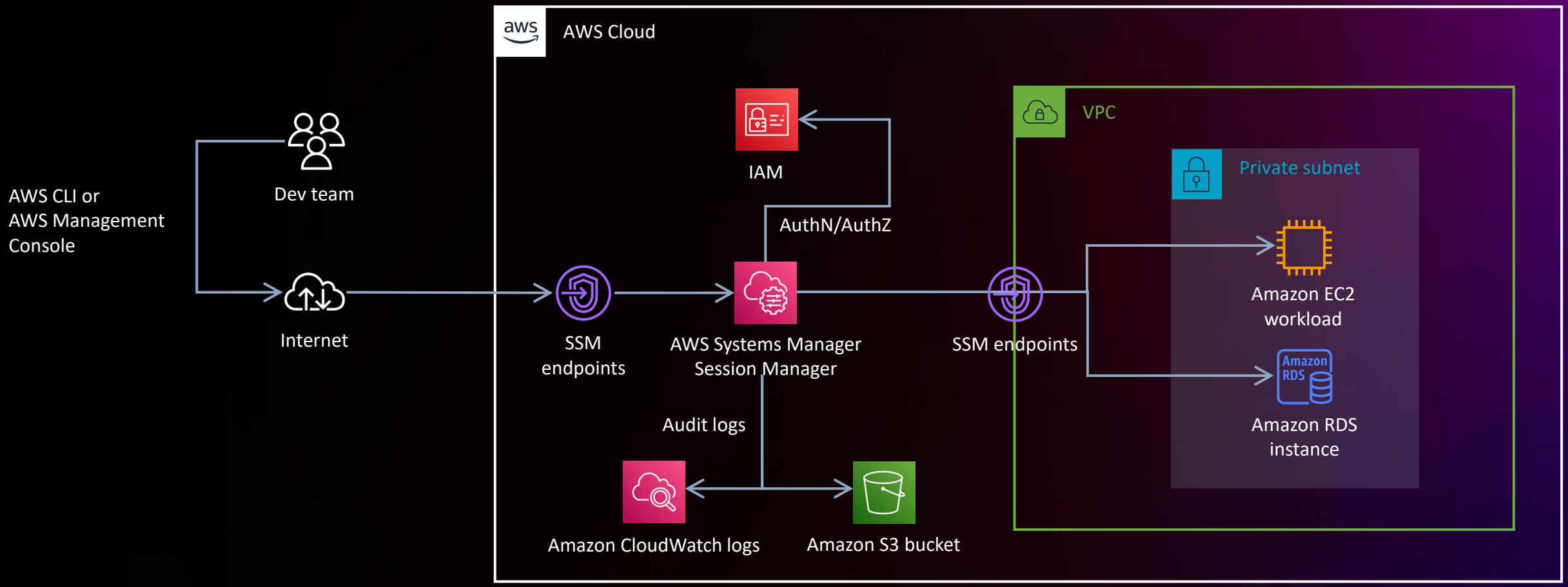
Pro tip

Get to least privilege with IAM Access Analyzer



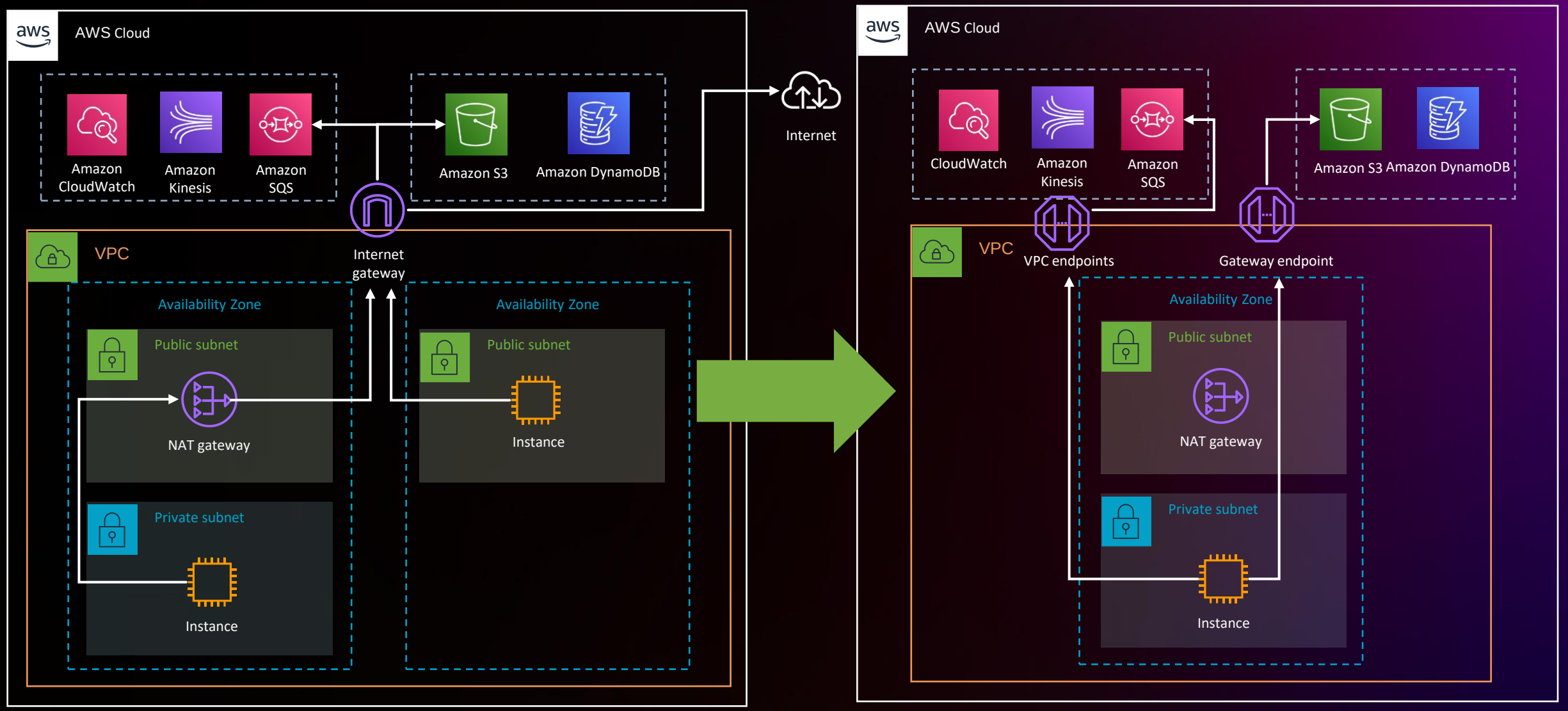
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use AWS Systems Manager instead of SSH or RDP



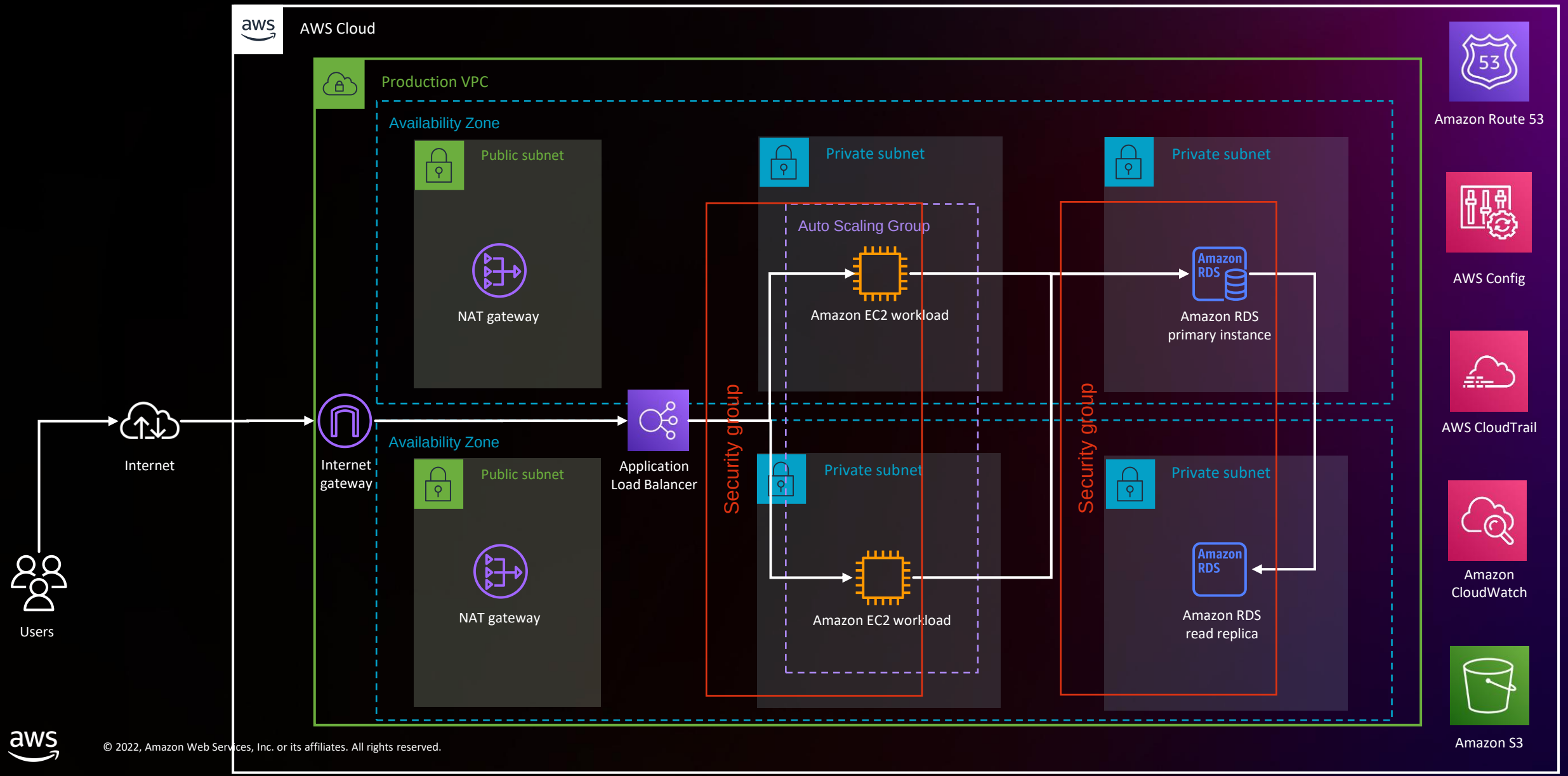
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use VPC endpoints to access services



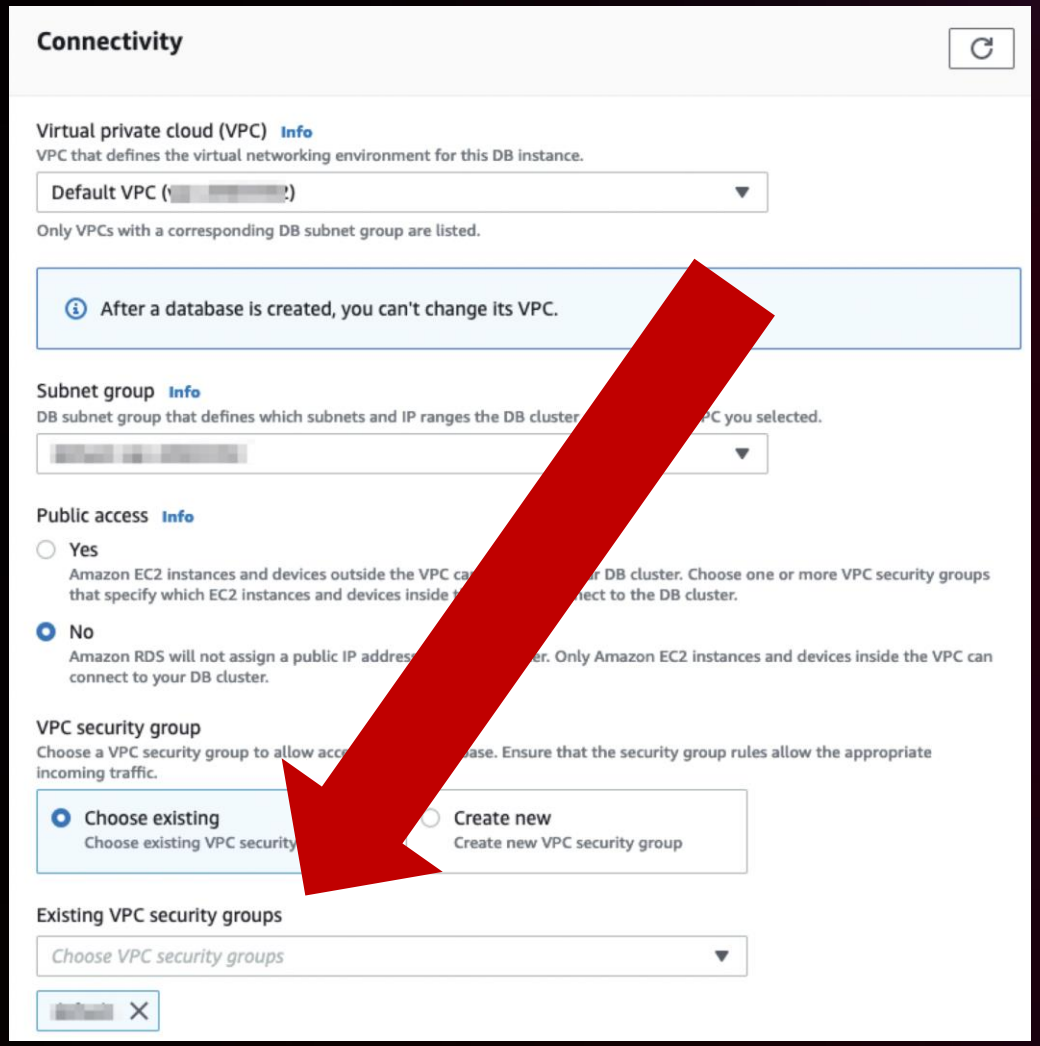
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deploy private resources in private subnets



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

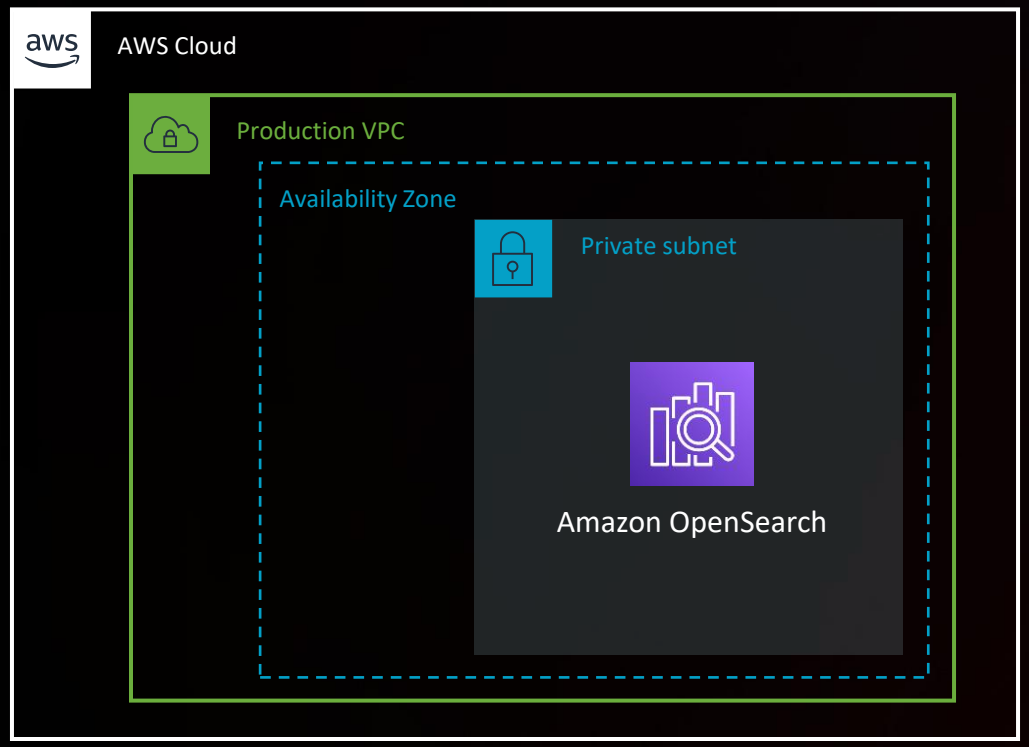
Use security groups to restrict access



Amazon EC2 → Launch instance

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deploy OpenSearch Domains Within a VPC



Creating index snapshots
in Amazon OpenSearch Service

go.aws/3TN8cCD

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing OpenSearch Service

- Deploy in a VPC
- Access control
- Encryption at rest
- Encryption in transit

Best practices for securing
Amazon OpenSearch Service



go.aws/3geIWrp

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security growth model

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS foundational and layered security services


AWS Organizations


AWS Security Hub


AWS Shield


AWS Certificate Manager


AWS KMS


AWS Network Firewall


AWS WAF


AWS Firewall Manager


AWS CloudHSM


AWS Secrets Manager


Amazon GuardDuty


Amazon Macie


Amazon Inspector


AWS Security Hub


Amazon CloudWatch


AWS Step Functions


AWS Systems Manager


AWS Lambda


AWS CDK


AWS CloudFormation

Identify → Protect → Detect → Automate / Respond / Investigate → Recover


AWS Config


AWS Trusted Advisor


AWS Systems Manager


AWS Control Tower


Amazon Cloud Directory


IAM

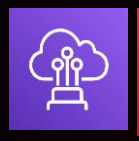

AWS Transit Gateway


Amazon VPC


AWS IAM Identity Center


AWS Directory Service


Amazon VPC PrivateLink


AWS Direct Connect


Amazon Cognito


Amazon Detective


Amazon CloudWatch


AWS CloudTrail


Amazon S3 Glacier


AWS Elastic Disaster Recovery


Snapshot

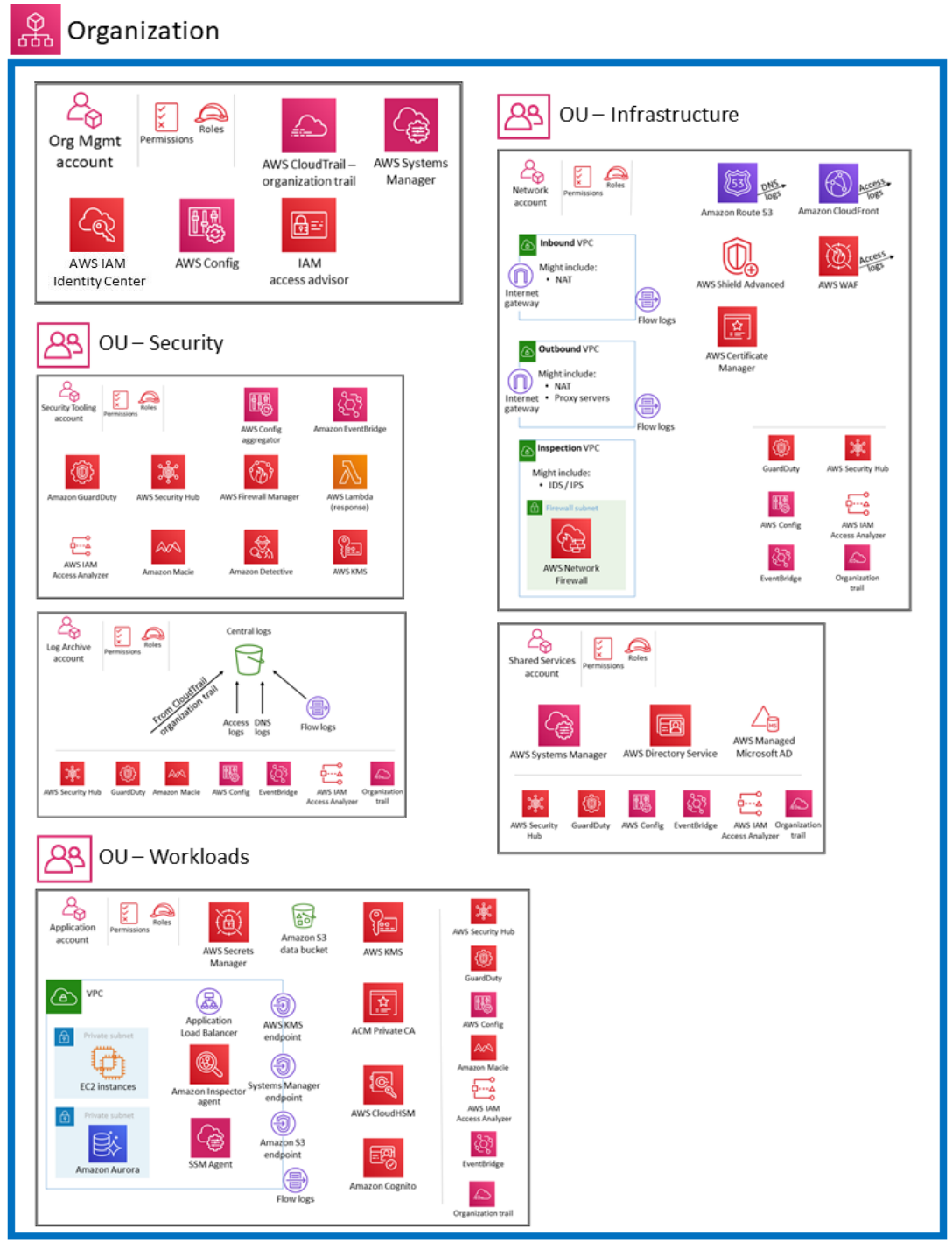

Archive

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS SRA

AWS SRA whitepaper

go.aws/3hS0cmA



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.