



AWS Cloud Configuration Review

For the attention of:

[Client SPOC Name]

[SPOC Designation]

Assessment Start Date:	XX/XX/202X
Assessment End Date:	XX/XX/202X
Report Issue Date:	XX/XX/202X
Document Version:	1.0
Score Type:	The vulnerability score of each issue in this report has been determined and ranked using the Krylo scoring scheme.

Contents

1	Your Assessment	3
1.1	Description	3
1.2	Scope and Objectives	3
1.3	Constraints	3
2	Executive Summary.....	4
3	Technical Summary.....	5
3.1	Risk Summary Graph	5
3.2	Summary of Vulnerabilities.....	6
4	Medium Risks	7
4.1	EC2: Secrets in Instance User Data	7
4.2	VPC: Overly Permissive Network Access Control List	8
5	Low Risks	9
5.1	EBS & S3: Resources Not Encrypted by Default	9
5.2	CloudTrail: Data Events Logging Never Configured.	11
5.3	S3: Bucket without Multi-Factor Authentication Delete.....	12
5.4	Non-compliance with CIS Benchmarks	13
6	Informational Risks	14
6.1	IAM: Unused Accounts not Disabled	14
6.2	IAM: Users Set without Multi-Factor Authentication	15
6.3	VPC: Subnets without Flow Logs	16
6.4	S3: Buckets without Versioning.....	17
7	Document Control.....	18

1 Your Assessment

1.1 Description

Your security assessment was carried out by **Team Krylo** between XX/XX/202X and XX/XX/202X. Throughout this engagement, the team made every effort to offer as much information as possible while adhering to the objectives, scope, and constraints outlined in the following sub-sections.

1.2 Scope and Objectives

The following Cloud Administration Panel was part of scope for this engagement:

- <https://client-name.signin.aws.amazon.com/console>

The following User account was provided:

- AssumeRole – ABC

1.3 Constraints

This engagement examined a snapshot in time of the AWS cloud infrastructure under consideration. Changes to the underlying configuration may result in the creation of new issues or a degraded security posture. Every day, new vulnerabilities and attack paths are identified, reinforcing the necessity for more security testing. Because project scope and time limits do not limit real-world attackers, more security flaws that could not reasonably be found during the engagement may exist and be exploited in the future.

2 Executive Summary

Krylo conducted an AWS Cloud configuration review against <Client>'s AWS cloud infrastructure as defined in **Section 1.2**. The cloud configuration review utilised a white-box approach where in the consultant received access to the AWS portal and consultation with <Client>'s technical staff.

The AWS cloud configuration review resulted in 10 vulnerabilities comprising of 2 Medium, 4 Low and 4 Informational findings.

A medium-risk vulnerability identified was regarding overly permissive network rules. These rules should be configured to limit access to the relevant areas of the network however when incorrectly set they may inadvertently allow access to all areas of the network providing an attacker with a much larger attack surface area. Another medium risk vulnerability was regarding secrets stored within instance data, these secrets contained SSH keys that could be used to gain remote access to another host, therefore if exposed an attacker could use the SSH key to gain access and potentially cause much further damage.

Low and informational risk issues regarded missing security options such as MFA not being required to delete potentially critical resources, insufficient logging of resources or networks, and unused user accounts not being de-activated or users using the same login credentials for a long period.

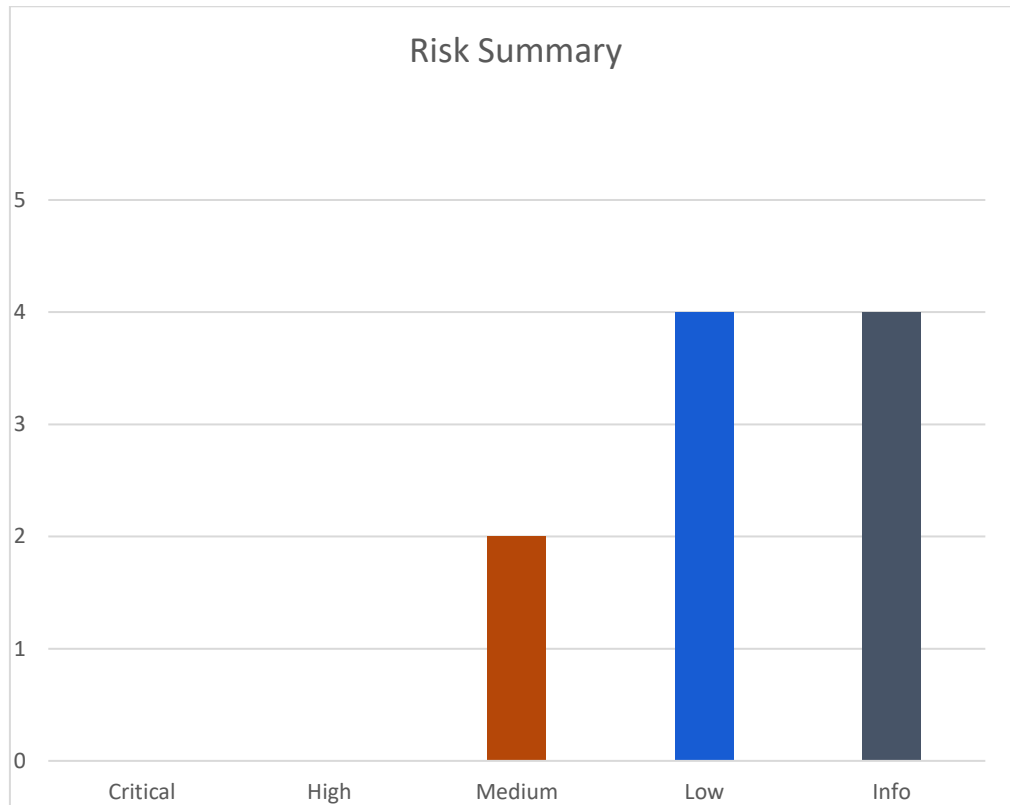
The informational findings are not considered an immediate threat but are considered security misconfigurations.

Overall, no immediate critical or high-risk vulnerabilities were identified within the AWS configuration that pose a serious risk to <Client>. Despite this, all medium-risk vulnerabilities should be resolved as a priority and low-risk vulnerabilities in a timely manner to best protect <Client> and its infrastructure.

3 Technical Summary

3.1 Risk Summary Graph

The following graph represents the distribution of the risks identified by vulnerability rating.



3.2 Summary of Vulnerabilities

SN	Description	Remediation	Risk
1	EC2: Secrets in Instance User Data	Avoid storing hard-coded credentials or authentication keys in plaintext in EC2.	Medium
2	VPC: Overly Permissive Network Access Control List	Reconfigure network ACLs to ensure that only required traffic is permitted.	Medium
3	EBS & S3: Resources Not Encrypted by Default	Ensure where available encryption is utilised and enforced.	Low
4	CloudTrail: Data Events Logging Never Configured	Enable CloudTrail in multi-region mode.	Low
5	S3: Bucket without Multi-Factor Authentication Delete	Implement MFA delete and versioning on critical buckets.	Low
6	Non-compliance with CIS benchmarks	Implement CIS Benchmark requirements.	Low
7	IAM: Unused Accounts not Disabled	Disable or remove accounts that are not required.	Informational
8	IAM: Users Set without Multi-Factor Authentication	Implement MFA.	Informational
9	VPC: Subnets without Flow Logs	Enable flow logs for subnets.	Informational
10	S3: Buckets without Versioning	Enable S3 bucket versioning.	Informational

4 Medium Risks

These are the concerns Krylo has recognized as posing a moderate but significant danger to [Client]. If an attacker exploited these vulnerabilities, the impact would be disruptive but unlikely to seriously interrupt typical corporate operations. It is prudent to examine and prepare for resolution of these difficulties, but only after more serious hazards have been handled. Krylo has supplied thorough details on how to duplicate each and the possible consequences of exploitation.

4.1 EC2: Secrets in Instance User Data

Risk: Medium

Description: User data is a metadata field of an EC2 instance that can be used to execute commands on hosts after the instances have been launched. This data is exposed to any entity with the most basic access to EC2, such as read only.

Impact: Instance User Data is useful in configuring resources without manual intervention. However, where the data contains sensitive information, such as authentication secrets, these may be at risk of compromise.

Instance(s): There were 3 instances of this issue identified at the following locations:

Instances
i-04XXXXXXXXXX
i-03XXXXXXXXXX
i-02XXXXXXXXXX

Proof of Concept:

The consultant discovered that the EC2 instance User-Data contains sensitive data, such as SSH key utilised for an authentication.

```
[...]  
owner: root:root  
path: /etc/eksctl/kubelet.yaml  
permissions: "0644"  
content: |  
-----BEGIN CERTIFICATE-----  
MIIC[...]qVd8=  
-----END CERTIFICATE-----
```

Recommendation: Avoid using EC2 instance metadata to transfer sensitive data, such as authentication credentials. Authentication credentials should be avoided when configuring resources to interact, and instead, roles should be attached to the resource.

Any credentials, or sensitive data, stored in EC2 metadata should be removed.

Reference(s):

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

4.2 VPC: Overly Permissive Network Access Control List

Risk: Medium

Description: It was identified within the VPC configuration all traffic was permitted regardless of the host, or protocol. This applied to both ingress and egress network traffic.

Impact: Network Access Control Lists (ACLs) are used for an additional layer of security for network traffic. When rules are added to permit all network traffic, prior to deny rules, they are overwritten. This contradicts the ACL and prevents it from denying any traffic, leaving the network vulnerable to all kinds of network requests.

Instance(s): There were 5 instances of this issue identified at the following location:

Access Control Lists	
acL-0b8XXXXXXXXX	
acL-0acXXXXXXXXX	
acL-033XXXXXXXXX	
acL-09aXXXXXXXXX	
acL-6feXXXXXXXXX	

Proof of Concept:

Details Inbound Rules Outbound Rules Subnet associations Tags						
Edit inbound rules						
View All rules						
Rule #	Type	Protocol	Port Range	Source	Allow / Deny	
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW	
101	ALL Traffic	ALL	ALL	::/0	ALLOW	

Recommendation: Reconfigure network ACLs to ensure that only required traffic is permitted and set to deny all traffic that is not required.

Reference(s):

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.html>

5 Low Risks

These are the concerns Krylo has recognized as posing a low risk to [Client]. If an attacker exploited these vulnerabilities, the impact would be unlikely to seriously interrupt typical corporate operations. It is prudent to examine and prepare for resolution of these difficulties, but only after more serious hazards have been handled. Krylo has supplied thorough details on how to duplicate each and the possible consequences of exploitation.

5.1 EBS & S3: Resources Not Encrypted by Default

Risk: Low

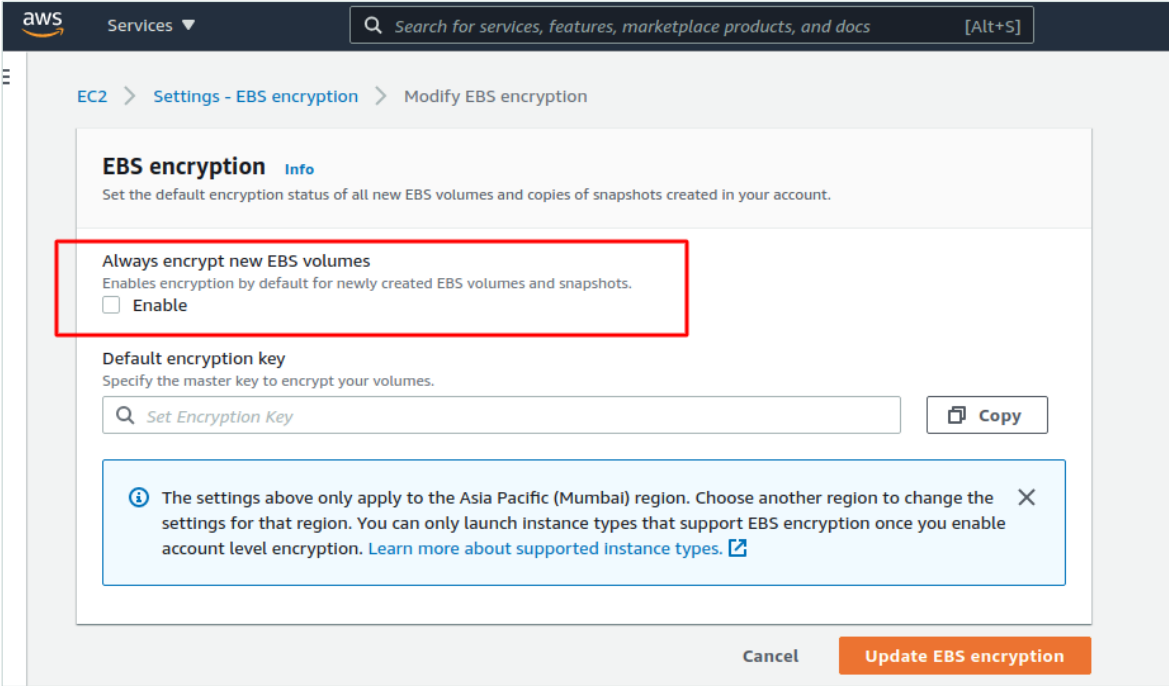
Description: It was identified that encryption for both “EBS Volumes” and “S3 Bucket” was not enabled.

Impact: Within AWS, resources can be encrypted at rest or in transit to ensure confidentiality. If this encryption is not enabled then a well-positioned attacker may be able to recover cleartext information leading to a compromise in the confidentiality of the affected resources.

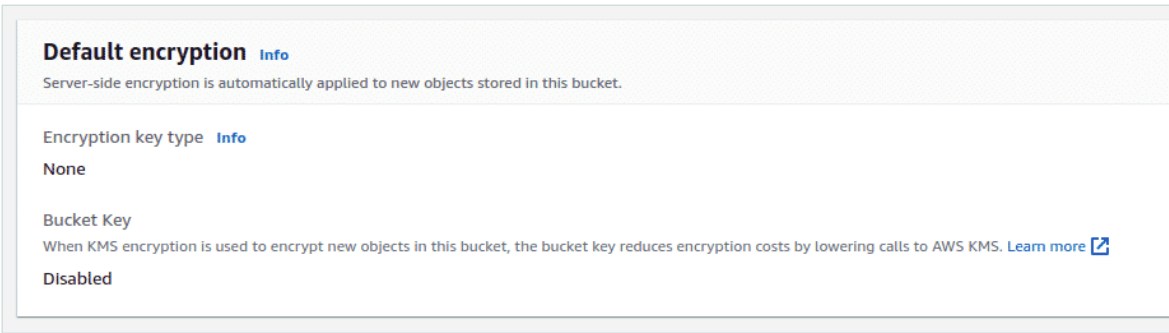
Instance(s): There were 5 instances of this issue identified at the following location:

Volumes/Bucket
vol-0b8XXXXXXXXX
vol-0acXXXXXXXXX
vol-033XXXXXXXXX
abc-test-versioning
pre-prod-abc-misc

Proof of Concept:



The screenshot shows the AWS Management Console interface for the 'Modify EBS encryption' page. The breadcrumb trail is 'EC2 > Settings - EBS encryption > Modify EBS encryption'. The main heading is 'EBS encryption' with an 'Info' link. Below it, a description states: 'Set the default encryption status of all new EBS volumes and copies of snapshots created in your account.' A red rectangular box highlights the 'Always encrypt new EBS volumes' section, which includes the text 'Enables encryption by default for newly created EBS volumes and snapshots.' and an unchecked 'Enable' checkbox. Below this is the 'Default encryption key' section, which says 'Specify the master key to encrypt your volumes.' and features a search bar with the placeholder 'Set Encryption Key' and a 'Copy' button. A blue information box at the bottom of the main content area contains a message: 'The settings above only apply to the Asia Pacific (Mumbai) region. Choose another region to change the settings for that region. You can only launch instance types that support EBS encryption once you enable account level encryption. [Learn more about supported instance types.](#)' At the bottom right of the page are 'Cancel' and 'Update EBS encryption' buttons.



The screenshot shows the 'Default encryption' page in the AWS Management Console. The heading is 'Default encryption' with an 'Info' link. The description reads: 'Server-side encryption is automatically applied to new objects stored in this bucket.' Under the 'Encryption key type' section (which has an 'Info' link), the value 'None' is displayed. Below this, the 'Bucket Key' section is shown as 'Disabled'. A note explains: 'When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)'.

Recommendation: Ensure where available encryption is utilised and enforced to provide confidentiality of data.

Reference(s):

<https://aws.amazon.com/blogs/security/importance-of-encryption-and-how-aws-can-help/>

5.2 CloudTrail: Data Events Logging Never Configured

Risk: Low

Description: The consultant found CloudTrail logging to be completely disabled in the environment.

Impact: CloudTrail logging can be used to determine what actions a particular user has taken during a specific period against AWS resources, by recording all related AWS API calls. This information can assist in the detection of malicious actions being performed, or during a suspected security breach when configured with CloudWatch monitoring and alerting capabilities.

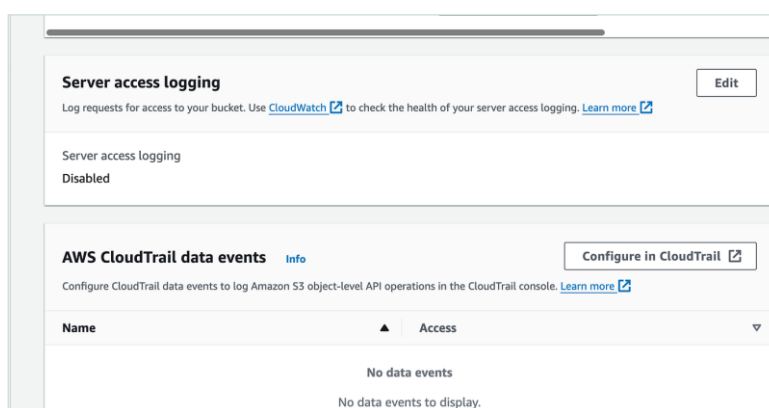
Trails should be configured in multi-region mode to highlight malicious or anomalous activity occurring within an AWS account in all regions, regardless of whether resources are provisioned in only one specific region. Recording events in a single region could allow malicious activity occurring in different regions go undetected.

Additionally, multi-region trails ensure that Global Service Logging is enabled for a trail by default, which allows the capture of events relating to global AWS services such as IAM. Failure to ensure that a trail is configured for Global Service Logging could allow events relating to such services to go unrecorded.

Instance(s): There was 1 instance of this issue identified at the following location:

Trail
all-users-all-actions

Proof of Concept:



Recommendation: Ensure CloudTrail is enabled, and that at least one trail is configured in multi-region mode. Within the AWS CloudTrail console, ensure that “Apply trail to all regions” option is set for the target trail.

Reference(s):

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html>

5.3 S3: Bucket without Multi-Factor Authentication Delete

Risk: Low

Description: The consultant identified that MFA delete was not configured.

Impact: MFA delete prevents objects from unauthorised or accidental deletion, without MFA delete an object can be deleted without any confirmation. This could result in a loss of data or downtime, preventing organisational users from accessing critical resources. It should be noted however that MFA delete can only be implemented on buckets that have versioning enabled.

Instance(s): There were 3 instances of this issue identified at the following locations:

Instances
storage-uploads-preproduction-s3-eu-west-1-v1
s3-access-logs
www-alb-logs-preproduction

Proof of Concept:

```
$aws s3api get-bucket-versioning --bucket storage-uploads-preproduction-s3-eu-west-1-v1
{
  "status": "Enabled"
}
```

Please note that “MFADelete” is missing from the above output.

Recommendation: Ensure versioning and MFA delete is enabled for all critical buckets to prevent accidental or unauthorised deletion.

Reference(s):

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html>

5.4 Non-compliance with CIS Benchmarks

Risk: Low

Description: The AWS service in use by <Client> was audited against the latest CIS benchmark for AWS. To ensure a granular overview of the tenant's security posture, both level 1 and level 2 checks were completed. Resource-specific checks were evaluated specifically against the resources which were part of the AWS solution.

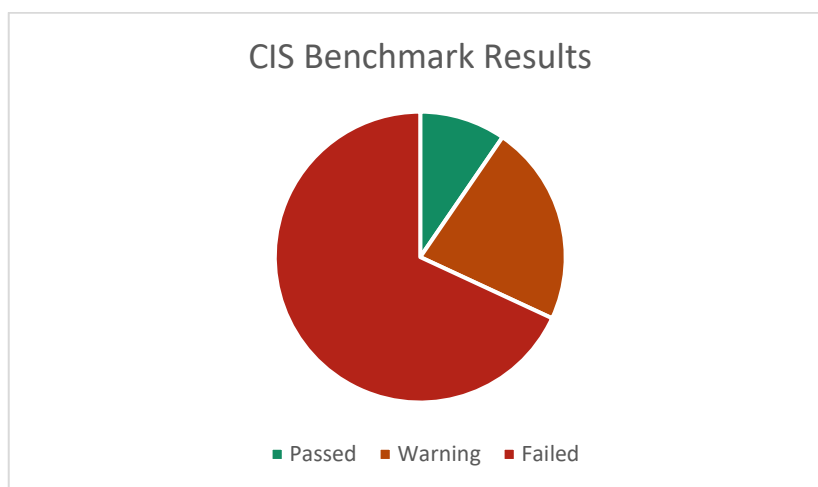
From the audit, it was identified that multiple settings were deemed as non-compliant by the standard.

Impact: The system's configuration failed to comply with recommended settings set by the Centre for Internet Security (CIS). While non-compliance with the CIS standard does not constitute a security risk, the settings it advocates harden the security stance of a system.

Instance(s): All non-compliances and warnings have been included in Appendix X.x.

Proof of Concept:

An overview of the CIS benchmark result has been provided in the figure below:



Recommendation: Review the appropriate sections and create an action plan to enable and configure as many of the required settings. This can be achieved by following CIS benchmark standard documents to achieve lockdown compliance, as detailed in the following reference.

Reference(s):

https://www.cisecurity.org/benchmark/amazon_web_services

6 Informational Risks

These are the concerns found by Krylo as part of your evaluation that do not pose a direct or immediate danger to [Client]. These are frequently technical or operational realities that reflect a considerable variation from normal suggested practice but do not constitute a significant vulnerability or risk in and of themselves. These should be assessed and considered as part of your overall risk profile, and appropriately reduced once the more serious hazards have been addressed.

6.1 IAM: Unused Accounts not Disabled

Risk: Informational

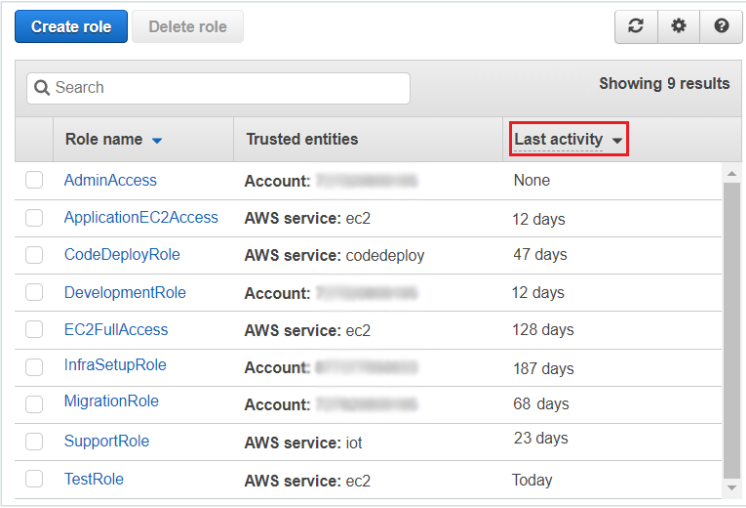
Description: The consultant discovered user accounts with more than 90 days since its last activity.

Impact: Once users leave the organisation or no longer need AWS access, the IAM user accounts should be removed. At least changing the password or deactivating the access keys is required so that former users do not have access. Not disabling old accounts increases the risk of account compromise or disgruntled ex-users logging in and causing damage.

Instance(s): There were 2 instances of this issue identified at the following location:

Users	
EC2FullAccess	
InfraSetupRole	

Proof of Concept:



Create role		Delete role		
Q Search		Showing 9 results		
Role name	Trusted entities	Last activity		
☐ AdminAccess	Account: [redacted]	None		
☐ ApplicationEC2Access	AWS service: ec2	12 days		
☐ CodeDeployRole	AWS service: codedeploy	47 days		
☐ DevelopmentRole	Account: [redacted]	12 days		
☐ EC2FullAccess	AWS service: ec2	128 days		
☐ InfraSetupRole	Account: [redacted]	187 days		
☐ MigrationRole	Account: [redacted]	68 days		
☐ SupportRole	AWS service: iot	23 days		
☐ TestRole	AWS service: ec2	Today		

Recommendation: Ensure that all credentials (including passwords and access keys) have been used and changed in the last 90 days.

Reference(s):

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_finding-unused.html

6.2 IAM: Users Set without Multi-Factor Authentication

Risk: Informational

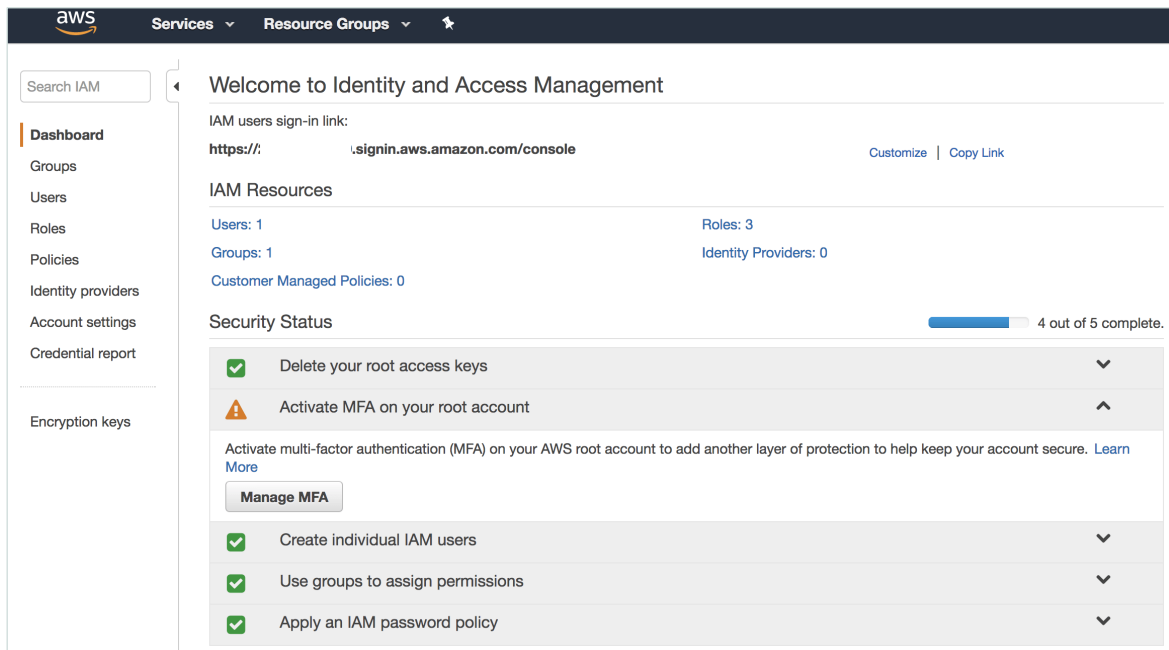
Description: Users were identified to be configured without MFA.

Impact: Multi-Factor Authentication (MFA) provides an additional layer of security for user credentials. When enabled an additional authentication check will be performed when the user logs in rather than just relying on a password and username. When not enabled this raises the risk of user accounts being compromised by an attacker who has correctly guessed the user's password.

Instance(s): There were 2 instances of this issue identified at the following location:

URL(s)
Root
John Doe

Proof of Concept:



The screenshot shows the AWS IAM console dashboard. The left sidebar contains navigation links: Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Welcome to Identity and Access Management' and includes a search bar. Below the welcome message, there are links for IAM users sign-in and IAM Resources. The 'Security Status' section shows a progress bar at 4 out of 5 complete. The steps listed are: Delete your root access keys (completed), Activate MFA on your root account (in progress, highlighted with a warning icon and a 'Manage MFA' button), Create individual IAM users (completed), Use groups to assign permissions (completed), and Apply an IAM password policy (completed).

Recommendation: Implement MFA for user accounts to provide an additional layer of security for user credentials. MFA should also be implemented on all administrator accounts.

Reference(s):

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

6.3 VPC: Subnets without Flow Logs

Risk: Informational

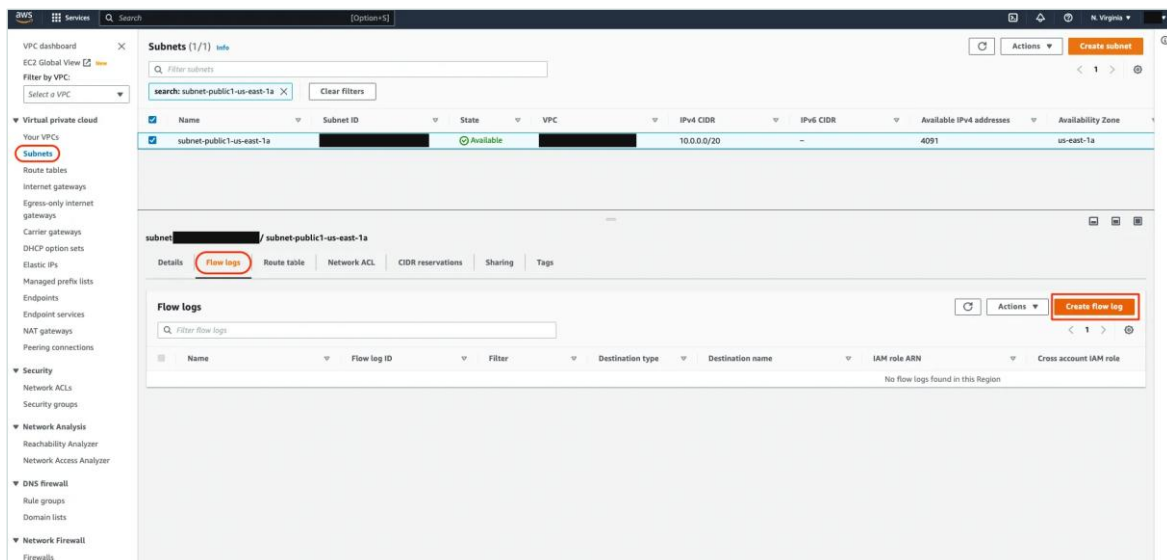
Description: The consultant identified flow logs were disabled for subnets.

Impact: Flow logs aid investigations into incidents such as unauthorized network traffic. Without flow logs enabled, performing these investigations to identify the cause of downtime, or malicious network traffic would be much harder to accomplish.

Instance(s): There was 1 instance of this issue identified at the following location:

Subnet
Subnet-public1-us-east-1a

Proof of Concept:



Recommendation: Ensure flow logs are configured for subnets to maintain an audit of network traffic and help investigate unauthorized access or downtime.

Reference(s):

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

6.4 S3: Buckets without Versioning

Risk: Informational

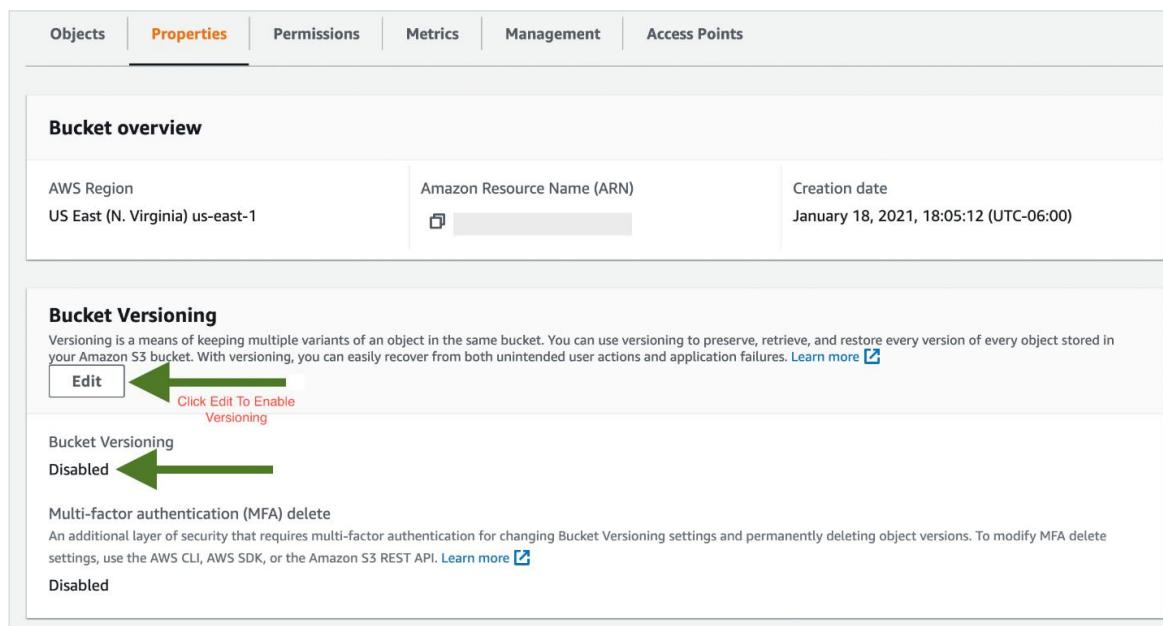
Description: The consultant discovered S3 bucket versioning was disabled on multiple buckets.

Impact: Versioning is a feature which can be used to keep multiple variants of an object within the same object. This can be used to preserve, retrieve, and restore every version of objects stored in a bucket. Versioning is also used as data protection and retention against unintended user actions and application failures, such as accidental or intentional deletion of objects.

Instance(s): There was 1 instance of this issue identified at the following location:

Bucket
Example-bucket

Proof of Concept:



Objects Properties Permissions Metrics Management Access Points

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::example-bucket	Creation date January 18, 2021, 18:05:12 (UTC-06:00)
---	---	---

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Edit

Click Edit To Enable Versioning

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Recommendation: Administrators should enable Versioning protection on S3 buckets.

Reference(s):

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>

7 Document Control

Name	Date	Version	Comment
[Tester 1]	XX/XX/202X	0.1	Initial Draft
[Tester 2]	XX/XX/202X	0.2	Technical QA (Final)
[Tester 1]	XX/XX/202X	1.0	Final Release