VULNERABILITY ASSESSMENT REPORT

-Group 26

EXECUTIVE SUMMARY

The study on Amazon Web Services (AWS) vulnerability assessment offers a thorough brief of the security stance in the company's AWS environment. The assessment aimed to identify any gaps, misconfigurations, and vulnerabilities that would jeopardize the integrity of the cloud infrastructure. Overall, the evaluation showed that strong network restrictions and properly configured security groups were in place, demonstrating a praiseworthy adherence to AWS security best practices.

Despite the largely strong security foundation, a few potential trouble spots were found. These include infrequent occurrences of unpatched systems and out-of-date software versions, which could provide possible entry points for bad actors. Furthermore, even with strong authentication procedures, sporadic instances of incorrectly configured access policies and permissions were found, highlighting the necessity of constant watchfulness.

By adopting these preventative measures, the company may strengthen the AWS environment's defenses against possible cyberattacks and protect the integrity, confidentiality, and availability of vital cloud-hosted assets and services.

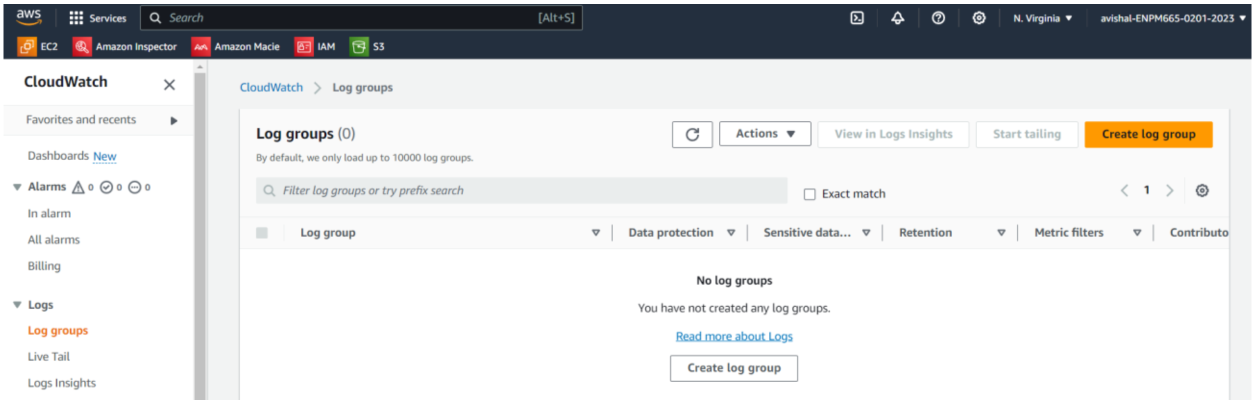
SUMMARY OF FINDINGS

Severity	Security Misconfiguration/Vulnerability
High	Overly Permissive IAM Policies. Users of groups with AdministratorAccess policy have MFA tokens disabled. DRS is not enabled for the region.
Medium	No security against Brute force attacks. No CloudWatch log groups found with metric filters or alarms associated. No Password policies are used to enforce password complexity requirement. EBS Default Encryption is not activated. Glue data catalog have disabled encrypt connection passwords and metadata encryption. Amazon GuardDuty is not enabled. Inspector2 is not enabled.
Low	IAM Access Analyzer is not enabled. SecurityAudit policy is not attached to any role.

No security against Brute force attacks. No CloudWatch log groups found with metric filters or alarms associated.

Description: No CloudWatch log groups have been found with associated metric filters or alarms for IAM policy changes.

Severity: Medium

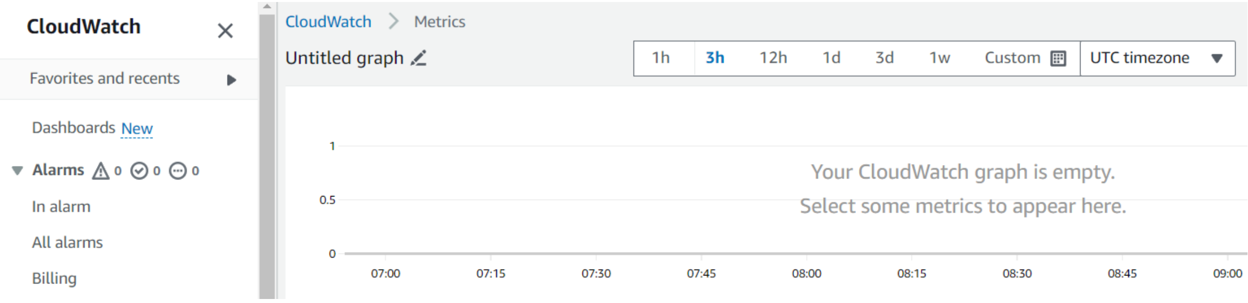


Log groups (0)

By default, we only load up to 10000 log groups.

No log groups

You have not created any log groups.



Your CloudWatch graph is empty.
Select some metrics to appear here.

Potential Impact:

A metric filter and alarm will be very useful for unauthorized requests and for IAM policy changes. Without them, the AWS account may not have a monitoring mechanism in place to detect and respond to changes in IAM policies in real-time.

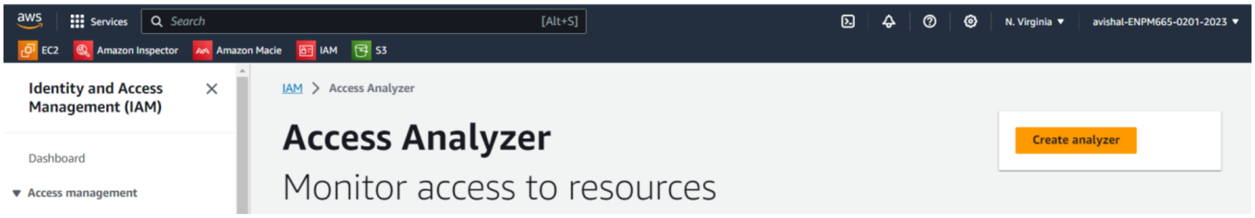
Remediation:

Set up CloudWatch log metric filters, configure alarms for robust monitoring and response mechanism for IAM policy changes in your AWS environment.

IAM Access Analyzer is not enabled.

Description: IAM Access Analyzer is not enabled.

Severity: Low



Access Analyzer

Monitor access to resources

Potential Impact:

AWS IAM Access Analyzer helps to identify unintended access to your resources and data, which is a security risk. Without IAM Access Analyzer, the account may not be utilizing a crucial tool for identifying and mitigating potential access risks within the AWS environment.

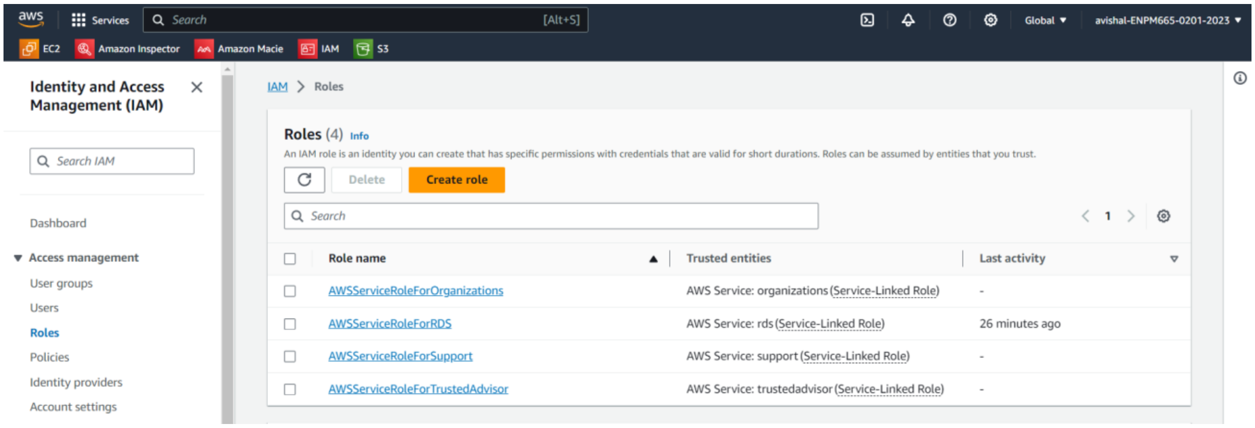
Remediation:

Enable IAM Access Analyzer to strengthen the security posture of the AWS resources.

SecurityAudit policy is not attached to any role.

Description: The SecurityAudit policy is not attached to any IAM role in the AWS account.

Severity: Low



Roles (4)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name ▲	Trusted entities	Last activity
□	AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	-
□	AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	26 minutes ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

Potential Impact:

Without the proper SecurityAudit policy attached to a role, there may be a lack of permissions necessary to conduct security audits effectively within the AWS environment.

Remediation:

Create a security audit role, attach the security audit policy, assign relevant users or groups to conduct security audits.

Overly Permissive IAM Policies.

Description: Granted broader permissions than necessary for a specific user, group, or role within AWS Identity and Access Management (IAM).

Severity: High

Potential Impact:

Overly permissive IAM policies increase security risks due to unnecessary access to resources, higher chances of accidental or intentional misuse, and potential non-compliance with security practices and regulatory requirements.

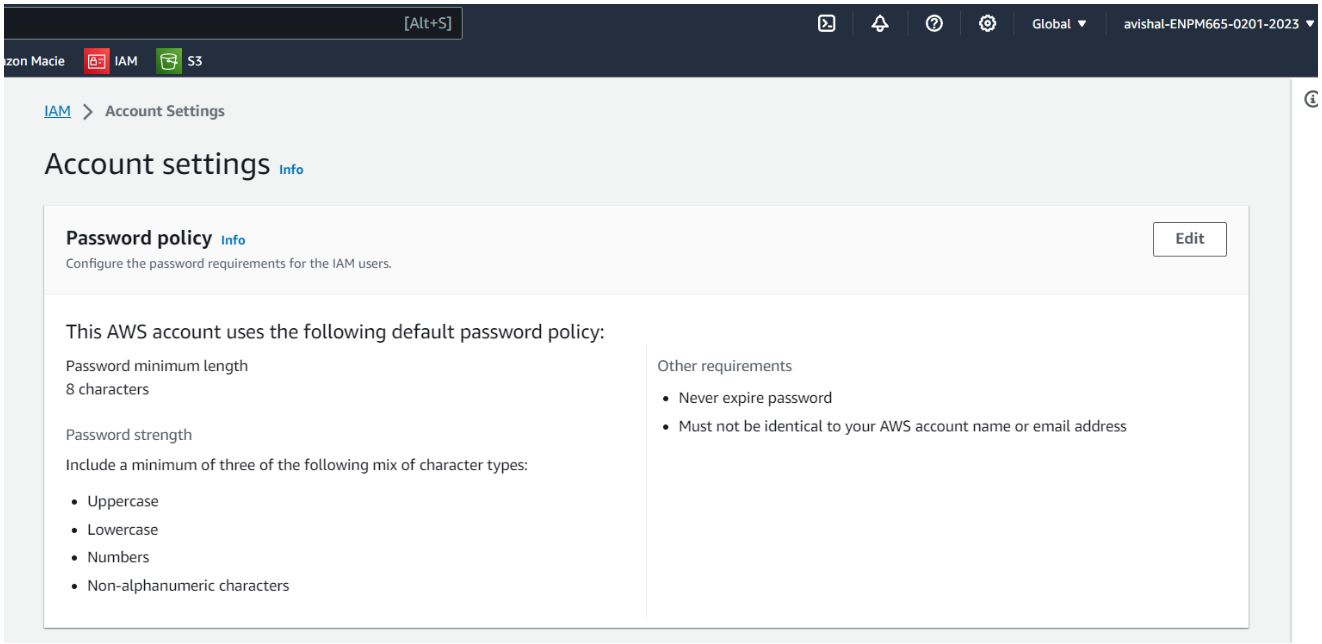
Remediation Recommendations:

It is recommended and considered standard security advice to grant least privilege. Granting only the permissions required to perform a task.

No Password policies are used to enforce password complexity requirement.

Description: The AWS account does not have a password policy enforced. Specifically, passwords do not expire, and no password policies are in place to enforce complexity requirements.

Severity: Medium



Account settings Info

Password policy Info

Configure the password requirements for the IAM users.

This AWS account uses the following default password policy:

Password minimum length

8 characters

Password strength

Include a minimum of three of the following mix of character types:

- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

Potential Impact:

Includes increased security risks due to the absence of controls over password expiration and complexity.

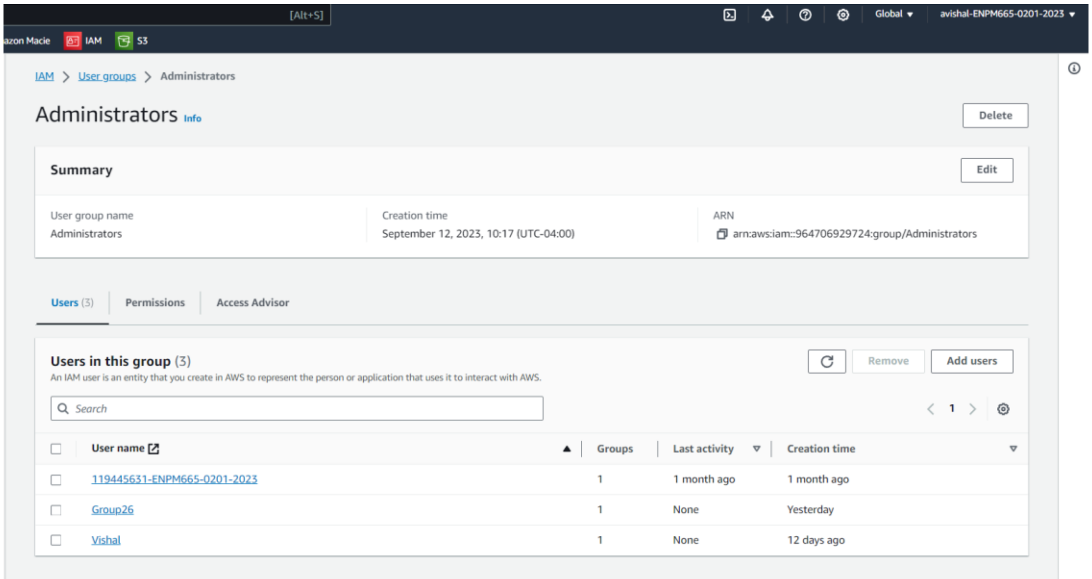
Remediation Recommendations:

Implement password policies, enforce password expiration, regularly review and update policies. Set the rules to enhance the complexity of the password.

Users of groups with AdministratorAccess policy have MFA tokens disabled.

Description: Group Administrators provides administrator access to users with MFA disabled.

Severity: High


[Alt+S]
Global ▾
avishal-ENPM665-0201-2023 ▾
azon Macie
IAM
S3
IAM > User groups > Administrators

Administrators Info

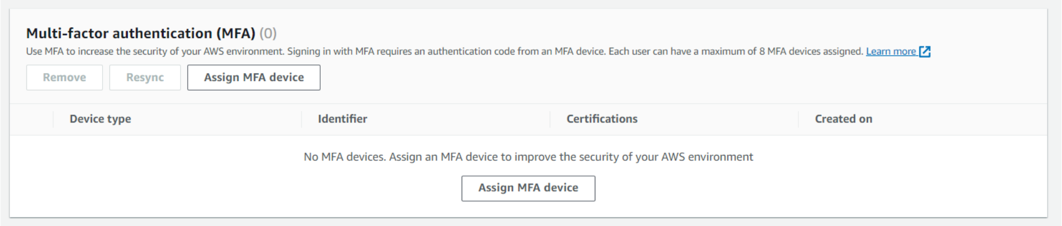
Summary

User group name	Creation time	ARN
Administrators	September 12, 2023, 10:17 (UTC-04:00)	arn:aws:iam::964706929724:group/Administrators

Users in this group (3)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

	User name	Groups	Last activity	Creation time
□	119445631-ENPM665-0201-2023	1	1 month ago	1 month ago
□	Group26	1	None	Yesterday
□	Vishal	1	None	12 days ago



Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Device type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Potential Impact:

This may allow anonymous users to perform actions and can lead to unauthorized access, higher vulnerability to credential-based attacks, and a higher risk of security breaches.

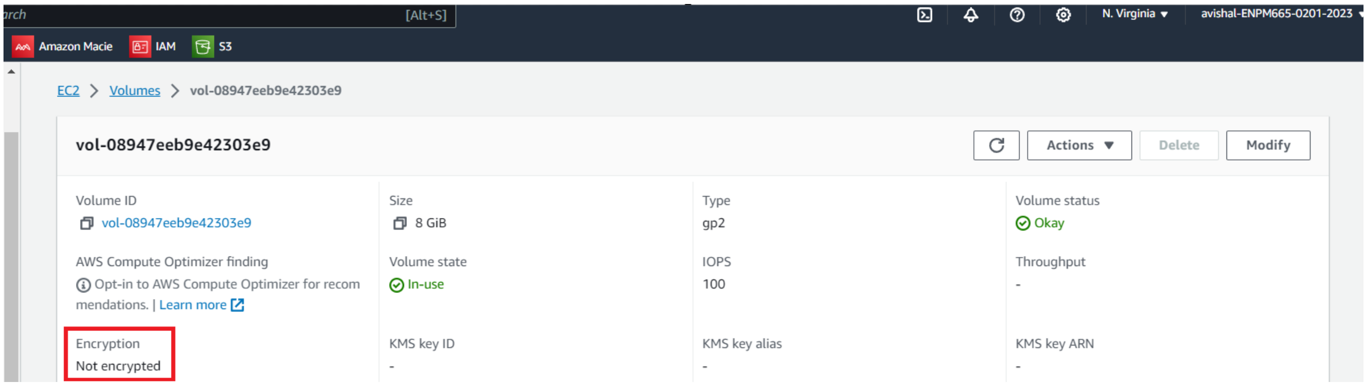
Remediation Recommendations:

Ensure users of groups with AdministratorAccess policy have MFA tokens enabled.

EBS Default Encryption is not activated.

Description: The default encryption for Amazon Elastic Block Store (EBS) volumes is not activated in the AWS account.

Severity: Medium


rch
[Alt+S]
N. Virginia ▾
avishal-ENPM665-0201-2023 ▾
Amazon Macie
IAM
S3
EC2 > Volumes > vol-08947eeb9e42303e9
Actions ▼
Delete
Modify

vol-08947eeb9e42303e9

Volume ID vol-08947eeb9e42303e9	Size 8 GiB	Type gp2	Volume status Okay
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more	Volume state In-use	IOPS 100	Throughput -
Encryption Not encrypted	KMS key ID -	KMS key alias -	KMS key ARN -

Potential Impact:

Higher risk of not protecting sensitive information which is at rest and could lead to compliance and security risks.

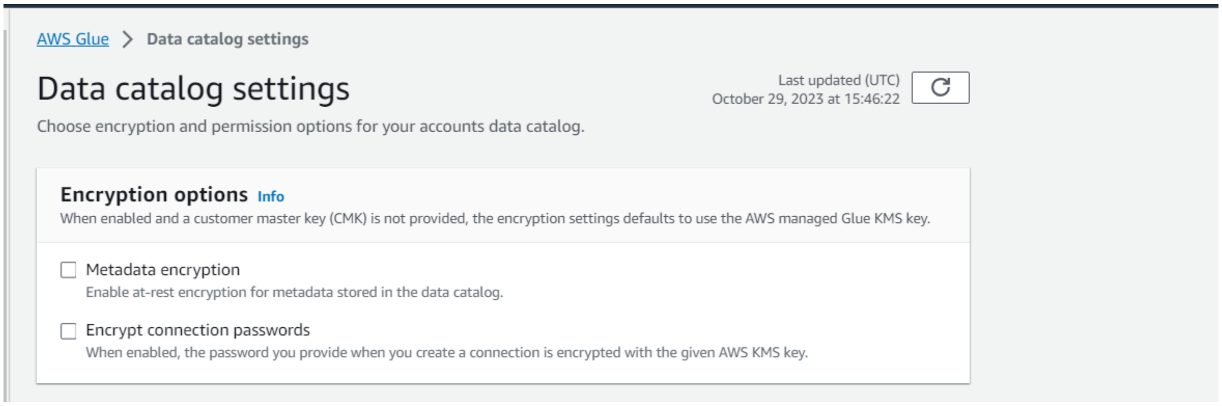
Remediation Recommendations:

Enable default encryption for EBS volumes in the AWS account. This will ensure that all new EBS volumes are encrypted by default.

Glue data catalog have disabled encrypt connection passwords and metadata encryption.

Description: Glue data catalog have disabled encrypt connection passwords and metadata encryption.

Severity: Medium



Data catalog settings

Choose encryption and permission options for your accounts data catalog.

Last updated (UTC)
October 29, 2023 at 15:46:22

Encryption options

When enabled and a customer master key (CMK) is not provided, the encryption settings defaults to use the AWS managed Glue KMS key.

☐ Metadata encryption
Enable at-rest encryption for metadata stored in the data catalog.

☐ Encrypt connection passwords
When enabled, the password you provide when you create a connection is encrypted with the given AWS KMS key.

Potential Impact:

Includes an increased risk of unauthorized access to sensitive information. This could potentially lead to data exposure, compliance issues, and security risks.

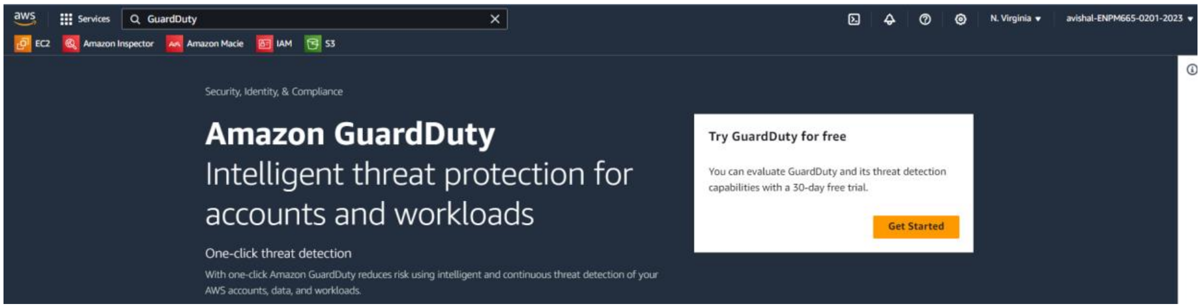
Remediation Recommendations:

Enable metadata encryption, enable encrypted connection passwords.

Amazon GuardDuty is not enabled.

Description: Amazon GuardDuty is not enabled in AWS account.

Severity: Medium



Security, Identity, & Compliance

Amazon GuardDuty

Intelligent threat protection for accounts and workloads

One-click threat detection

With one-click Amazon GuardDuty reduces risk using intelligent and continuous threat detection of your AWS accounts, data, and workloads.

Try GuardDuty for free

You can evaluate GuardDuty and its threat detection capabilities with a 30-day free trial.

Potential impact:

Higher risk of not identifying and responding to security threats and suspicious activities within the AWS environment and could lead to delayed or missed alerts about potential security incidents which impacts the organization.

Remediation Recommendations:

Enable amazon GuardDuty, review and customize GuardDuty settings to align with specific security requirements.

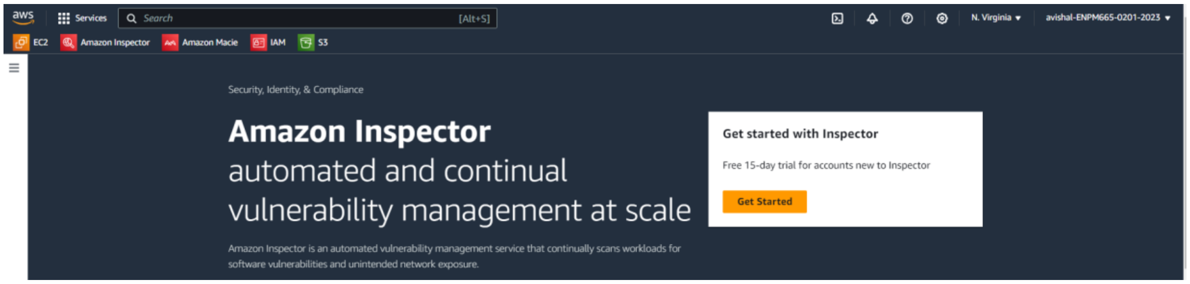
Inspector2 is not enabled.

Description: Amazon Inspector 2 is not enabled in the AWS account.

Severity: Medium

Potential Impact:

Without using AWS Inspector, we may not be aware of all the security vulnerabilities in your AWS resources, which could lead to unauthorized access, data breaches, or other security incidents.



Security, Identity, & Compliance

Amazon Inspector

automated and continual vulnerability management at scale

Amazon Inspector is an automated vulnerability management service that continually scans workloads for software vulnerabilities and unintended network exposure.

Get started with Inspector

Free 15-day trial for accounts new to Inspector

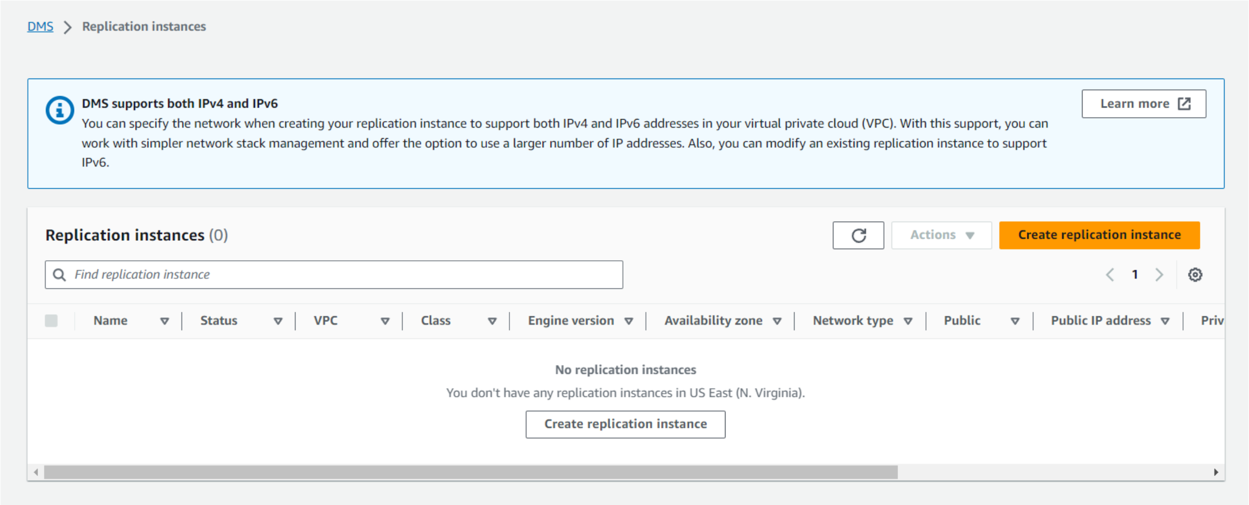
Remediation Recommendation:

Enable Amazon Inspector 2, set up and configure Inspector 2 assessments to scan EC2 instances and other resources for security vulnerabilities and compliance issues.

DRS is not enabled for the region.

Description: AWS Database Replication Service (DRS) is not enabled for the specified region

Severity: High



DMS supports both IPv4 and IPv6

You can specify the network when creating your replication instance to support both IPv4 and IPv6 addresses in your virtual private cloud (VPC). With this support, you can work with simpler network stack management and offer the option to use a larger number of IP addresses. Also, you can modify an existing replication instance to support IPv6.

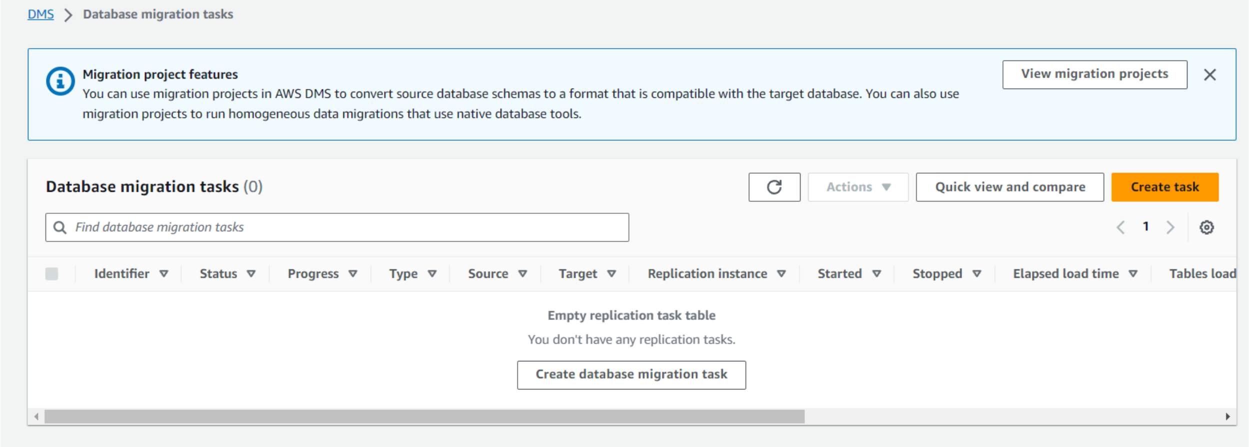
Replication instances (0)

□	Name	Status	VPC	Class	Engine version	Availability zone	Network type	Public	Public IP address	Priv

No replication instances

You don't have any replication instances in US East (N. Virginia).

Create replication instance



DMS > Database migration tasks

Migration project features

You can use migration projects in AWS DMS to convert source database schemas to a format that is compatible with the target database. You can also use migration projects to run homogeneous data migrations that use native database tools.

View migration projects
Actions ▾
Quick view and compare
Create task

Database migration tasks (0)

Find database migration tasks
1

□	Identifier	Status	Progress	Type	Source	Target	Replication instance	Started	Stopped	Elapsed load time	Tables load

Empty replication task table

You don't have any replication tasks.

Potential Impact:

If DRS is not enabled with jobs, then it may not be able to recover from a disaster. This implies that DRS's data synchronization, redundancy, and automatic database failover features won't work, which could result in more downtime and less availability in the event of a database failure.

Remediation Recommendations:

Enable Database Replication Service (DRS), configure the source and target databases, replication instances, and replication groups in accordance with your unique database needs.