ENPM665 – 0101

Midterm Group Project

Securing a Cloud-based Healthcare Application

Table of Contents

Vulnerability Assessment Report

Overview of the Report:

The report is an overall analysis of the vulnerabilities present in the cloud infrastructure for this Healthcare Application. This lists the identified vulnerabilities, their impact, and probable ways they can be secured. After successfully analyzing the infrastructure there are several risks associated, which are critical and need to be addressed with different possible ways for successful operations of infrastructure while maintaining accuracy. A detailed explanation for each security loophole is further provided under respective assessments below.

Identified Vulnerabilities and Recommendations:

1. Excessive permission for IAM roles:

The infrastructure can face a lot of issues due to excessive permissions provided the Administrator and Developer which grants the "*Allow*" effect and *"*"* action provides unrestricted access to all permissions to all the resources. Additionally, the Guest user has excessive access with "*s3:GetObject*" permission for all the objects in the S3 bucket, giving the unrestricted access. Any guest user can alter the data internally with these permissions.

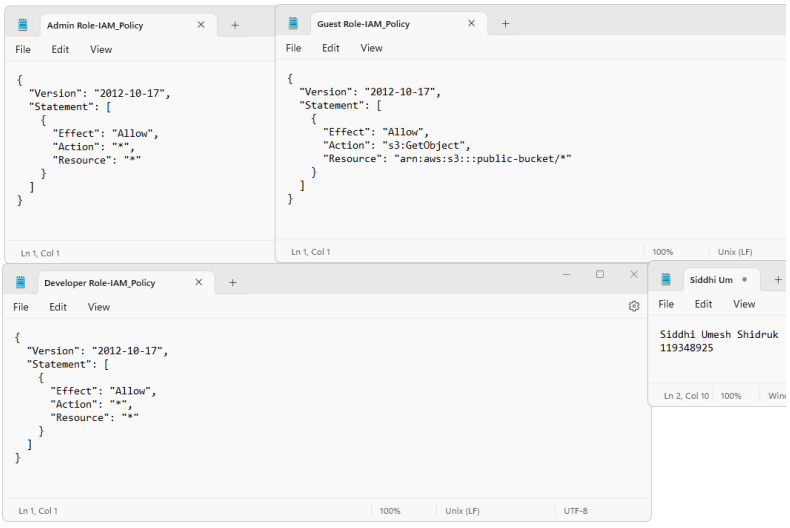
Severity: High

Impact:

As the IAM roles are provided with full access, there are risks associated with excessive permissions, which can lead to data loss, unauthorized access, insider threat, accidental data deletion, or modification. Some risks lead to compromise the AWS environments.

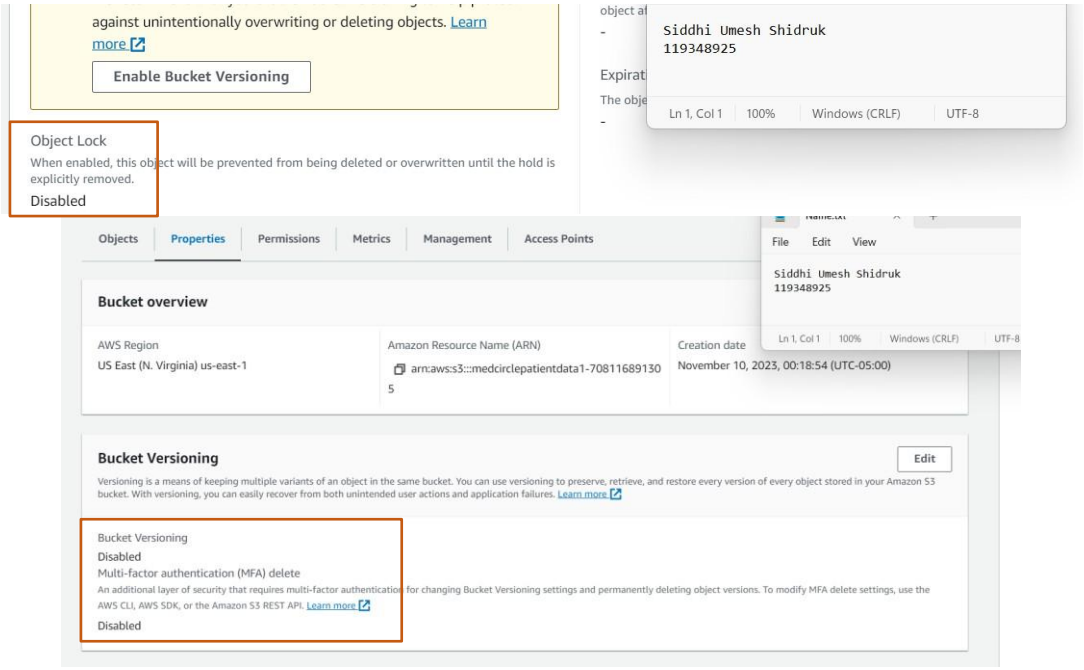
Potential ways for improvement

Recommendations for security improvements are, to follow the least privilege granting principle for authorized roles according to required tasks, implement strong access control to prevent harm to sensitive data, and to review permissions regularly.



2. *Misconfigurations in S3 Bucket*

S3 bucket is an important aspect of the infrastructure that stores data as the objects which exist in a bucket. If the S3 object lock is disabled, and the MFA delete is not configured, then this leads to security issues with S3 versioning.



Severity: High

Impact:

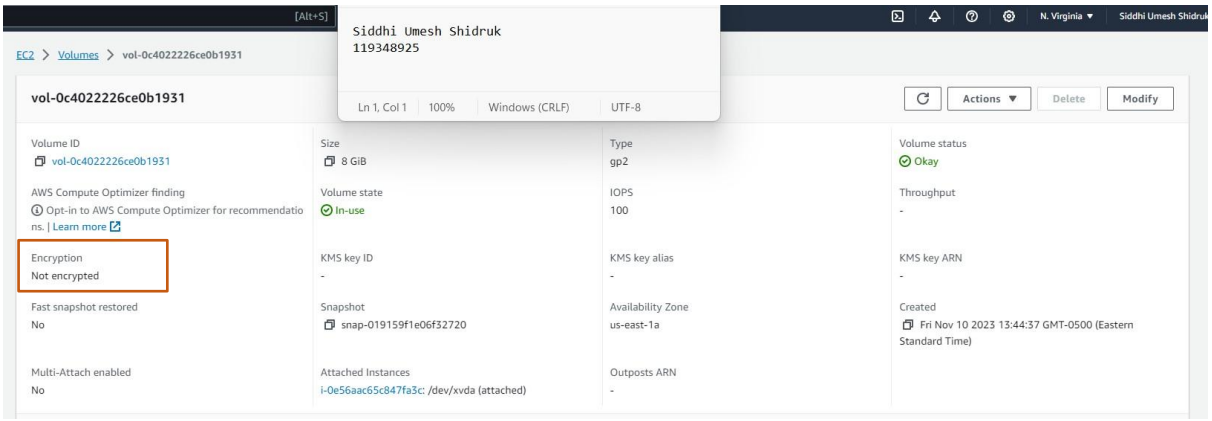
The misconfigurations can lead to several issues related to objects stored in the bucket. The object lock being disabled cannot prevent or provide recovery solutions for accidental modification or deletion of objects. There is no proper setting for accidental or intentional deletion of the bucket.

Potential ways for improvement:

AWS works in synchronization with S3, if there is a proper object lock setup, the information will be stored in the metadata for further consequences of retrieval, by simply adding a projection layer for objects from being modified. Moreover, configuring an MFA delete for S3 versioning can help prevent and ensure data in the bucket from being deleted accidentally, it can be configured in two ways hardware and virtual accordingly. Another useful way is to use *Amazon Macie* which analyses the sensitive data and automates protection policy against security risks.

3. *Unencrypted EBS Volume Associated with EC2 Instance:*

The EBS volume in the cloud environment lacks encryption, which is a crucial part of the infrastructure that stores sensitive information. The EC2 instance and EC2 volume are linked, allowing data storage and retrieval capabilities for efficient application operation which should be secured with encryption.



Severity: High

Impact:

When the volume lacks encryption, then it is a threat to the stored data for being vulnerable to potential breaches, unintentional data exposure, and security incidents associated with volume integrity.

Potential ways for improvement:

With the help of AWS EBS Encryption, the overall integrity of volume will be managed to provide confidentiality and integrity of stored information, as EBS serves as a primary block storage for EC2 instances. EBS encryption techniques use AWS KMS for creating an encrypting volume. It is a great solution for the encryption of the EBS volume associated with EC2 instances. AWS also provides a solution for encryption at default which needs to be configured.

4. *Lack of Recovery Plan:*

There is no comprehensive recovery plan available for any disaster, which can lead to different implications for the availability of data and services. Without a recovery plan, a cloud infrastructure can be vulnerable to various unforeseen events.

Severity: High

Impact:

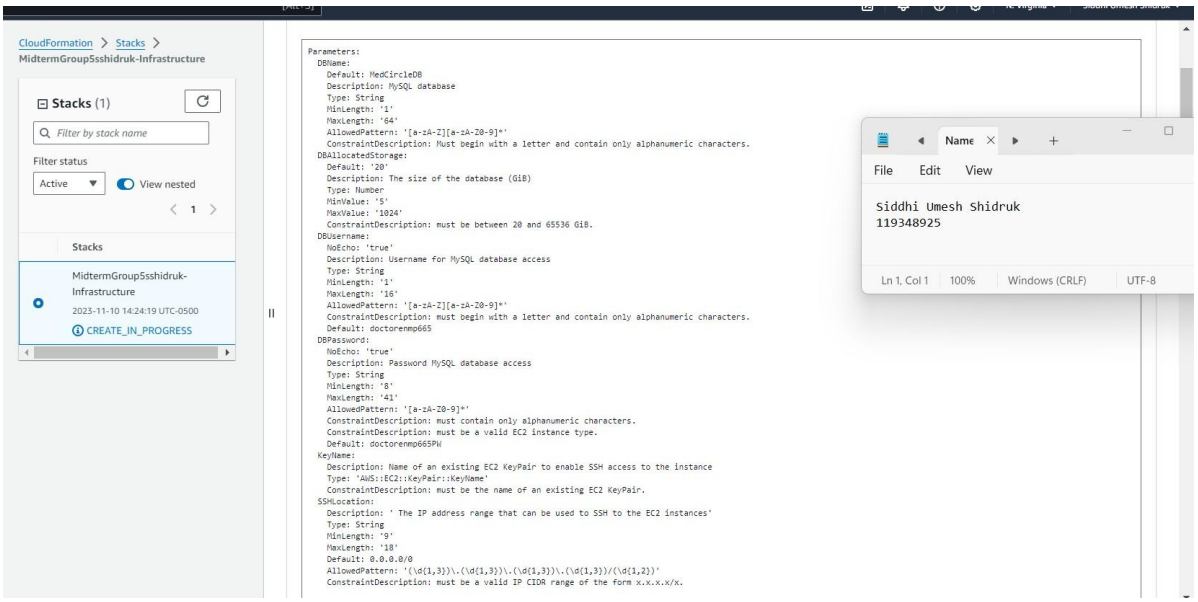
The absence of a recovery plan can expose organization to several risks, which can damage integrity and cloud environment disruption for any natural causes or technical failures. Without a recovery plan, the infrastructure can be caught off-guard by any challenges associated with accidental cloud security breaches.

Potential ways for improvement:

To mitigate future risks, the organization should conduct comprehensive risk assessments to identify vulnerabilities and establish a plan. A detailed disaster recovery plan can help secure this infrastructure. It is essential to implement a recovery plan by incorporating the AWS services for a cloud environment.

5. *Database credentials predetermined:*

Hardcoded credentials should not be abusable in database instances, that may leak sensitive data, if they are exploited by an attacker intentionally.



Severity: High

Impact:

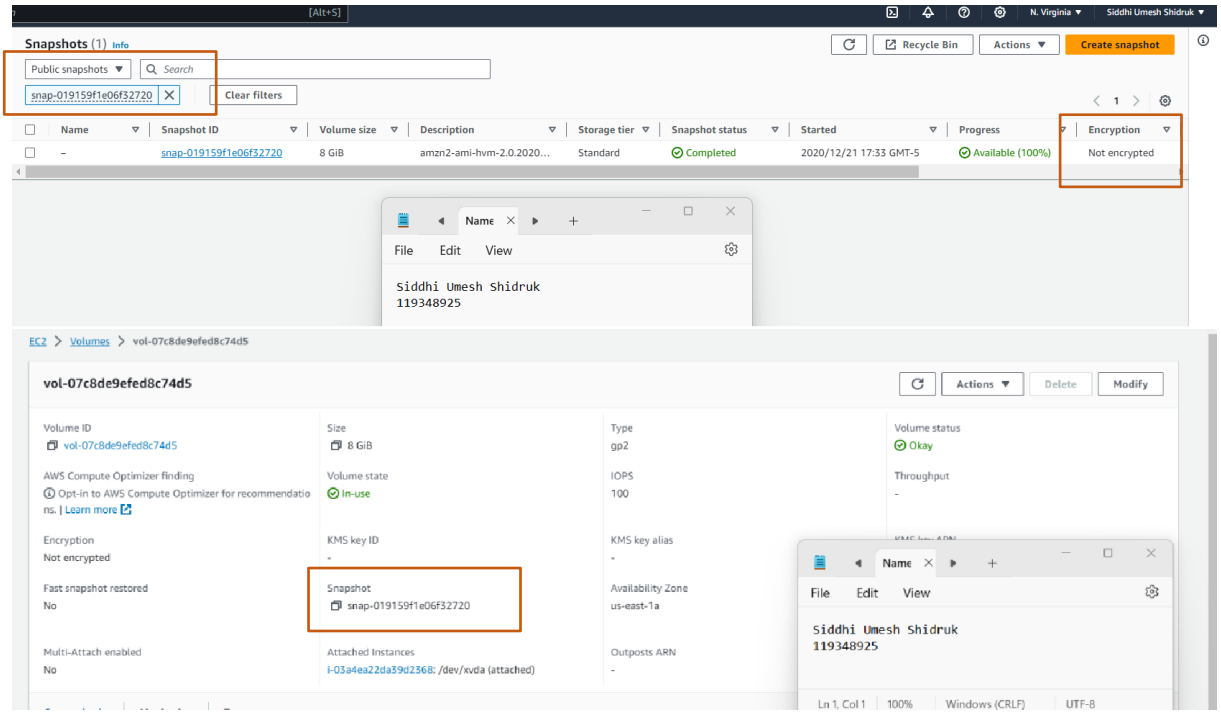
The impact of hardcoded credentials can create a potential entry for attackers to gain unauthorized access leading to data manipulation, stealing of sensitive resources for illegal purposes, posing potential risk to sensitive customer data, and exploitation of database integrity.

Potential ways for improvement:

Using *AWS Secret Manager* solves the problem of managing hardcoded credentials. AWS Secret manager will rotate and store database credentials and improve security measures, avoiding potential compromised activities. It helps store and retrieve credentials with appropriate protection and ease of access.

6. *EBS Snapshot not Encrypted:*

Elastic Block Store (EBS) snapshot helps as copies to the EBS volumes, providing necessary backup strategies for information on volume at the time of some recovery plans. Without encryption, it is open such that it can be easily compromised and critical data is always at the risk of exposure, which in turn doesn't fulfil the requirements for data-at-rest.



Severity: High

Impact:

If the EBS snapshots are not encrypted it is easy to access the server and use the unencrypted snapshot to gain sensitive information. Unencrypted snapshots can go public when they are not encrypted with proper encryption techniques, making it possible with easy access for exploiting vulnerabilities on the server.

Potential ways for improvement

It is a good practice for security concerns to configure encryption for EBS snapshots via the EC2 dashboard, if the snapshot is encrypted then replicating the same one can be difficult. Snapshot encryption will also help to keep the infrastructure information secure. The EBS encryption uses strong encryption which is, managed by AWS Key Management infrastructure through AWS Key Management Service (KMS).

Data Security Assessment Report

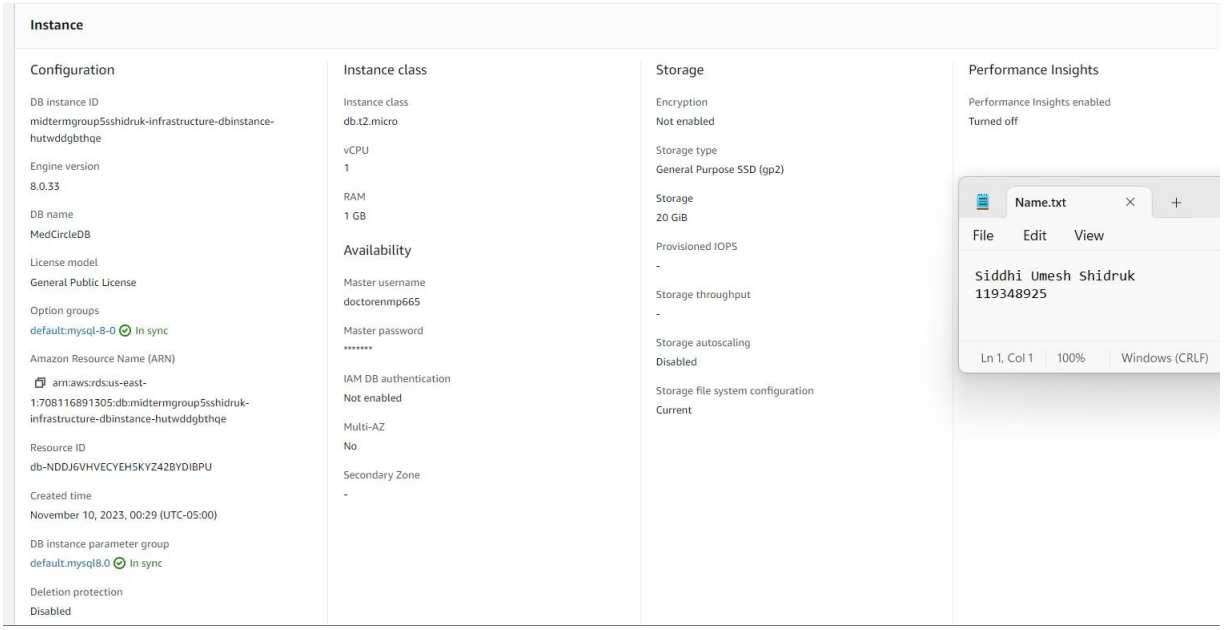
Overview of the Report:

The Data Security Assessment provides a detailed documentation of the risk analysis associated with the given cloud infrastructure. It typically includes strategies and areas for improvements with the help of AWS services for different types of data security threats.

Identified Vulnerabilities and Recommendations:

1. No proper authentication for the database:

Proper authentication of the database should always be maintained otherwise, a critical vulnerability may arise, posing the threat of unauthorized access control, poor credentials in S3 or encryption keys, and even compromised system infrastructure or virtual machines.



Impact:

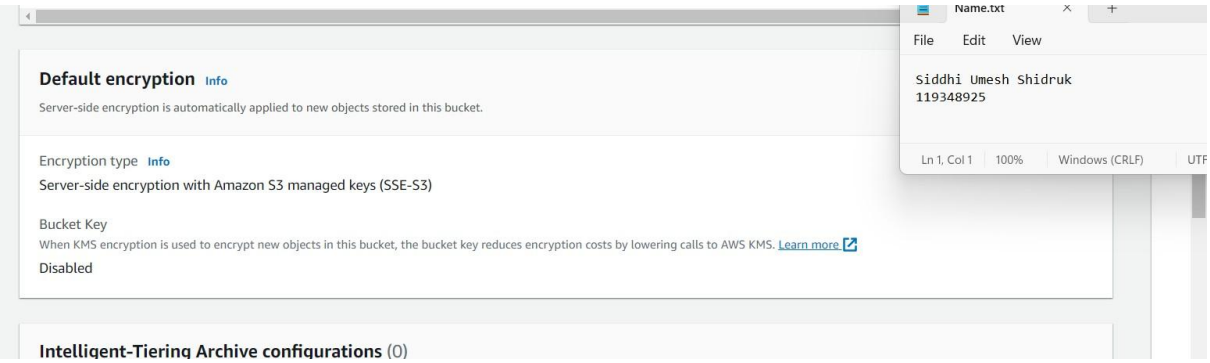
If databases rely on weak infrastructure measures, then inadequate authentication increases the vulnerability of unauthorized access, which exploits the sensitivity of high-priority data and resources. Privilege escalation also depends on authentication measures, such that a user with extensive permission might exploit the machine easily.

Potential ways for improvement:

Implementation of secure authentication mechanisms will directly reduce the risk of database exploitation. *AWS IAM Access Analyzer* can be used for improving configurations and enforcing the least privilege principle. Regularly managing the IAM credentials will improve IAM authentication for the database.

2. Absence of KMS keys for S3 bucket:

The absence of AWS Key Management Service for the S3 bucket security is a configuration error, leading to data loss and security breaches in cloud infrastructure. The risks associated with the absence of KMS are limited key management control, non-compliance, and unencrypted data at rest.



Impact:

Without KMS, the S3 bucket will be open to being accidentally modified by any user or exploited by an attacker. Lack of data confidentiality and violations of standard compliance with poor encryption methods will also account for the impact of security breaches.

Potential ways for improvement:

Centralized management of encrypted keys provides a secure mechanism for controlling and reducing encryption risks. Enabling the use of the KMS service will keep the data in S3 buckets encrypted and, hence, reduce vulnerabilities, and compliance levels will also be maintained. Documentation of encryption policies will not only make the system more likely to work against vulnerabilities but will also establish a regular auditing practice.

3. Unencrypted Protected Health Information (PHI):

Data breaches of patients' highly sensitive and Protected Health Information (PHI) can occur due to various vulnerability exploitations, and having a cloud infrastructure with unencrypted data makes it easier for the attacker to get access.

Impact

The implications of unencrypted PHI in cloud infrastructure leads to data exposure, legal consequences such as non-adherence to compliance, and data integrity risks. Organizations' reputations also come at stake for severe data breaches, and patient trust in healthcare firms will have a negative impact.

Potential ways for improvement

Use of encryption in databases when it is at rest and implementation of proper network segments with TLS and SSL protocols to secure communication channels. Key management helps in securely managing the encryption keys, and AWS S3 can be used for the protection of data as it provides server-side encryption.

4. Compliance Issues:

The infrastructure being a healthcare application, there are some rules and regulations that must be followed to comply with industry standards for providing a safe, secure, and trustworthy environment. The storage of unencrypted patient sensitive data can breach the privacy of patient records.

Impact:

When there is non-compliance build-up, there can be security concerns impacting the patient's sensitive data, which can lead to high penalties and legal actions against the organization for violating the privacy of consumers. Along with organizations' reputation, individuals can be affected by different forms of data breaches, which may lead to customers entrusting the organization.

Potential ways for improvement:

To meet compliance requirements for healthcare organizations, the infrastructure should be up-to-date with their policies and standards, which can be done with HIPAA (Healthcare Insurance Portability and Accountability Act). HIPAA is an act for protecting sensitive data and managing data disclosure policies with the customer's consent. The infrastructure should be under the security rule for HIPAA, as it follows all the guidelines for CIA triad. Use of *AWS Security Hub* will be helpful to check if the requirements are as per the standards and control, and mapping these requirements by performing audits.

Network Security Assessment Report

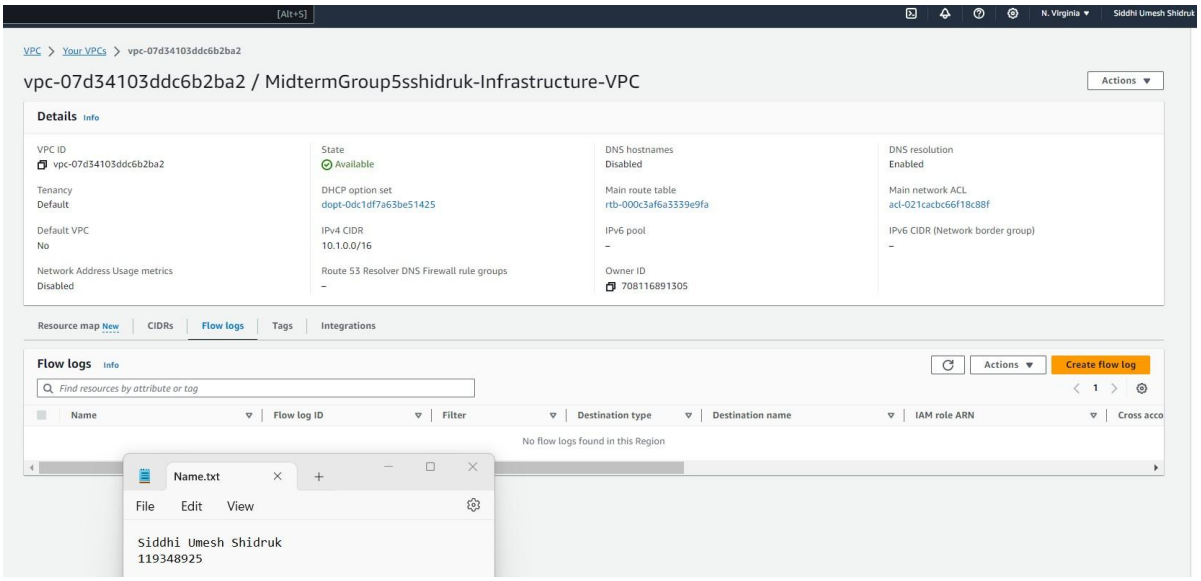
Overview of Report:

The report contains output for the assessment of network risks associated with the healthcare application. The report aims to provide detailed feedback on what the network risks are for the cloud infrastructure and various ways to provide a secure environment using AWS services

Identified Vulnerabilities and Recommendations:

1. No Logging for VPC flow logs:

There is an absence of VPC flow log monitoring for network traffic received and sent from the VM for this infrastructure. It is important to have access to monitor inbound and outbound network traffic to identify any malicious activities.



Impact:

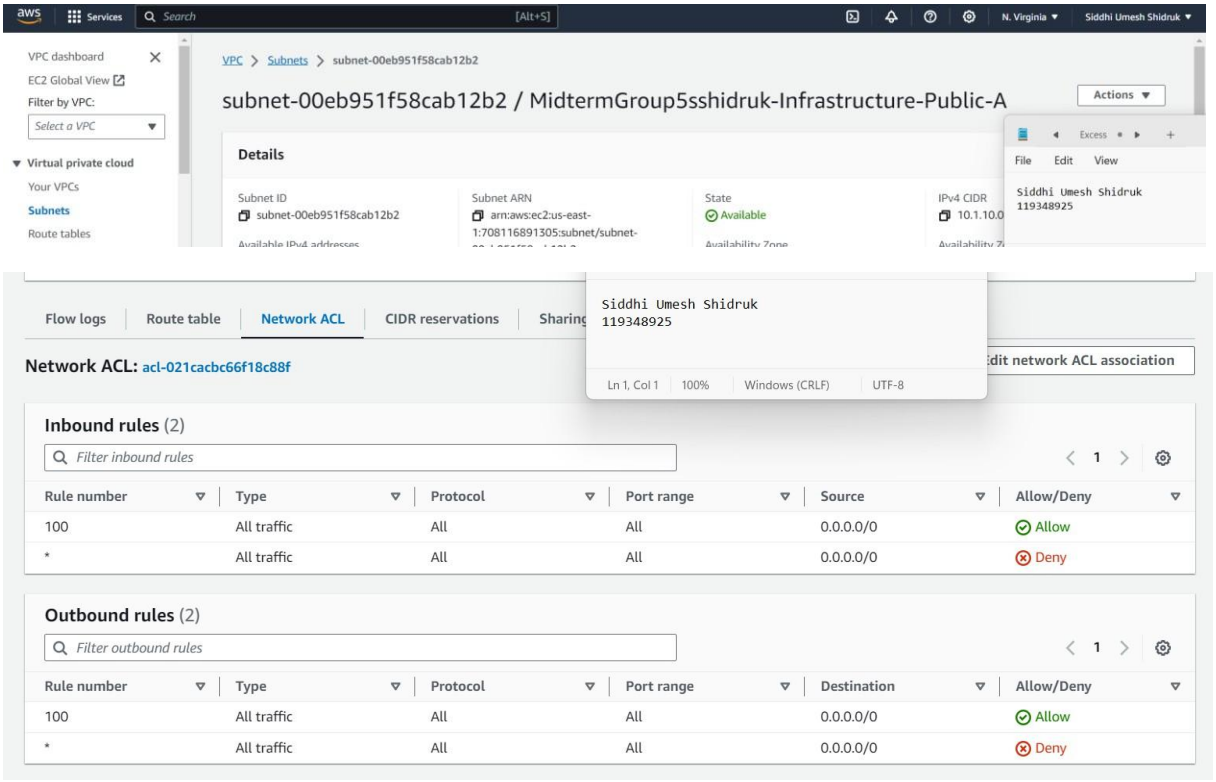
The unavailability of logging data can result in the scarcity of network communication history, which is a crucial part of security such that it requires to troubleshoot and identify threats, which can lead to hindering incident detection abilities for any incidents. VPC flow logs are also part of logging and monitoring, which can lead to non-compliance with default standards for the organization.

Potential Ways for Improvement:

Enabling the VPC logs with *AWS VPC flow logs* in integration with *AWS CloudWatch* is a necessity to improve network visibility along with increased detection for troubleshooting and security purposes. Also, by configuring CloudWatch, it is easy to store and search logs for proactive monitoring of unusual network activity alerts.

2. Network Access Control List (NACL) is in open state:

The Network Access Control List (NACL) in the infrastructure is open to network traffic from default IPs and ports, which are vital for security purposes. By default, the NACL permits default IP addresses and ports without configuration of network traffic rules.



Impact:

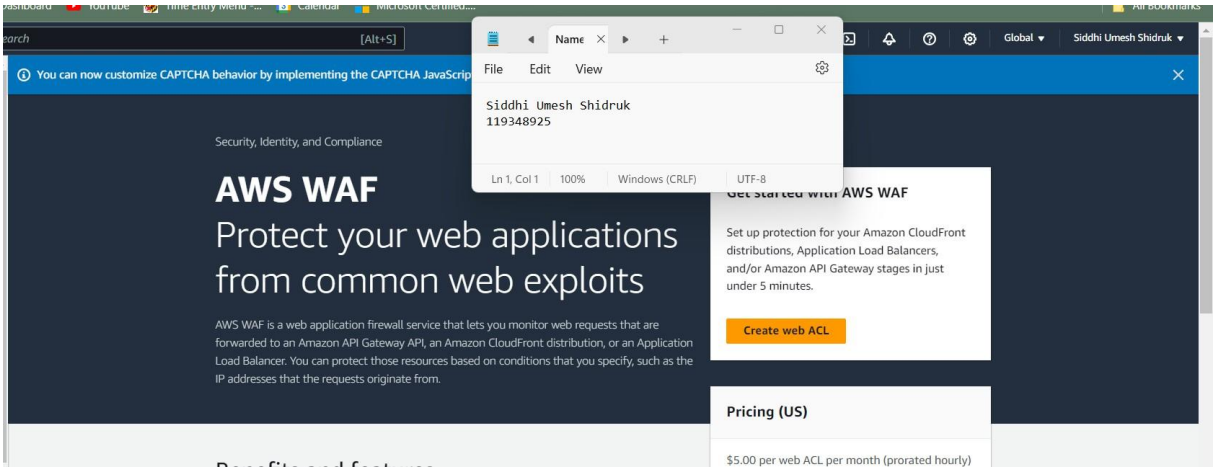
The infrastructure being in an open state provides illegal access through sensitive ports, which can let the attacker or insider threats to access the AWS environments, which can lead to the modifications and extraction of sensitive information.

Potential Ways for Improvement:

The easiest solution to provide security is to configure rules for default NACL or create custom rules for ACL for the VPC, which can add an additional layer of security. The NACL allows and denies inbound and outbound traffic according to the configuration rules, allowing it to reject unwanted traffic at the subnet level.

3. No Web Application Firewall (WAF) configuration

There needs to be an effective network rule management strategy in place that decides what kind of traffic should be allowed and rejected via the network. Also, data from third-party applications is blindly trusted and allowed into the network.



Impact:

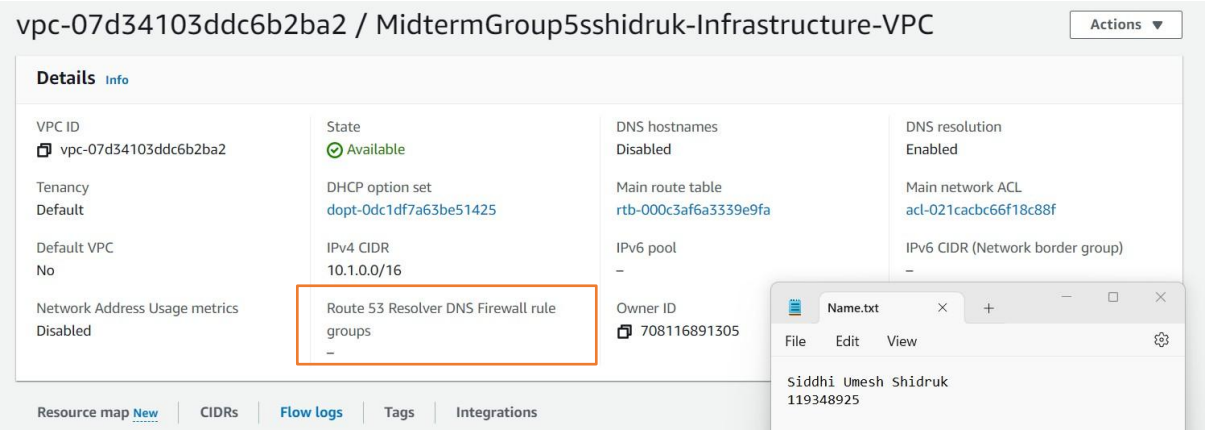
Firewalls serve as the initial barrier against unauthorized entry and malicious network traffic. Incorrect configuration or excessive rules can lead to unwanted access, data breaches, service outages, malware infiltrations, data exfiltration, and violations of compliance.

Potential ways for improvement:

The required protection for this risk can be provided by using the *AWS WAF*, which will allow monitoring of web requests, and also the firewall will restrict the number of unsecured open ports for better security.

4. *DNS firewall not configured:*

The Route 53 resolver DNS firewall protects outbound DNS requests from VPC, which prevents DNS exfiltration of data. The DNS firewall works as a shield to protect malicious DNS requests and different types of attacks. The infrastructure can face several unknown DNS requests that needs to be filtered for any unofficial communication.



Impact:

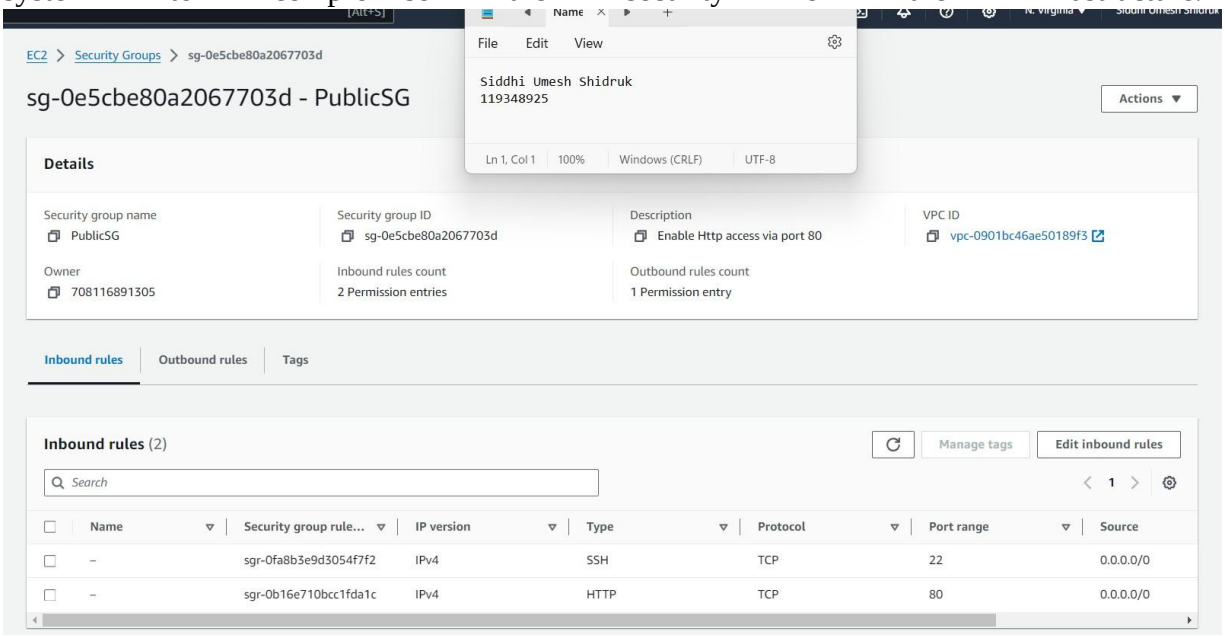
The attacker may try to steal sensitive information via DNS attack, as there are no queried rules associated, this will let the attacker exploit the weakness via DNS. A lack of DNS firewall configuration will be a potential aspect, that will result into downtime if not properly configured.

Potential ways for improvement**:**

The best way to overcome this problem is by enabling and configuring rules for the Route 53 DNS firewall. The DNS firewall will filter queries with certain rules and restrict the traffic to provide the required security solution from different types of DNS attacks. Along with that, using *AWS CloudWatch* to monitor the different number of DNS queries to be filtered by Route 53 resolver.

5. Security group with unrestricted access:

The security groups are configured with unrestricted access concerning ports for default IPs associated with instances. This is a highly vulnerable risk to incoming traffic reaching the network with any resource with unrestricted access, exposing a way for new attacks on the system to compromise the security of the infrastructure.



Impact:

Allowing unrestricted access to critical ports can lead to resource access, data breach, exposure, and theft with unauthorized access. This can be a potential reason for different types of attacks such as brute force, privilege escalation and exploitation of vulnerabilities.

Potential ways for improvement:

The easiest recommendation for this security threat is to create restricted access to the security groups with specific permission sets and monitoring techniques for unauthorized network communication via available ports.

Virtual Machine Vulnerabilities Assessment Report

Overview of Report:

This report consists of a detailed analysis done for the security aspects of the virtual machines hosted on AWS. Virtual Machines are the instances and most of them are part of the EC2 service of AWS. Based on the evaluation for healthcare, the major vulnerabilities discovered along with potential ways to prevent them are listed below.

Identified Vulnerabilities and Recommendations:

1. Patching Issues:

Process of identifying, deploying, and updating security flaws and software patches to have the system up and running with heuristic analysis against security vulnerabilities in a cloud-based environment. This is critical and if not configured properly integrity of cloud-based systems can be adversely affected.

Impact:

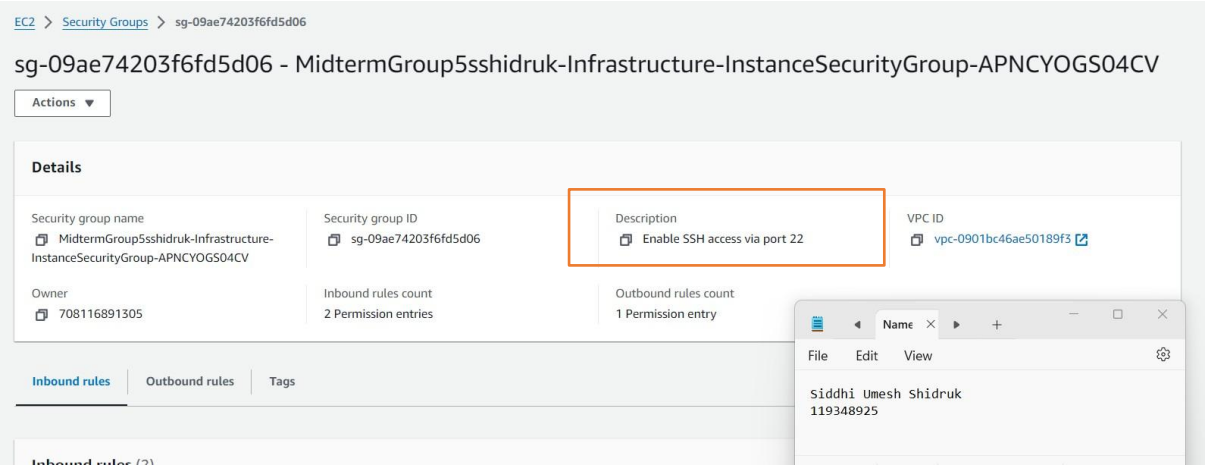
Failing to keep the VMs updated with the latest trend of security patches may affect the organizations' compliance level and data protection standards leading to legal consequences. Unpatched virtual environments open one more layer of attack which potentially might affect the whole infrastructure, resulting in the common error of "Security Patch Missing" in AWS.

Potential ways for improvements:

Keeping the rules up-to-date for unpatched vulnerabilities, testing and validating patches, and OS updates. Use of *AWS RDS* and *AWS Aurora* service will auto-enable the database patching. *AWS Inspector* service can be used to find the EC2 vulnerabilities. Based on the results, unpatched segments can be fixed on priority. Another simpler approach is to use *Patch Manager* as a service under *AWS Systems Manager* for automating the patch management.

2. *Remote Code Execution Default SSH access:*

RCE in cloud security is a vulnerability of high severity, its CVSS score depends on the attack vector, complexity, and CIA triad might be considerably high. VM segment of the exploit may include the use of default SSH access, which in turn compromises the whole machine as the attacker can arbitrarily run code and gain access to the cloud through weak secure shell configurations (SSH).



Impact:

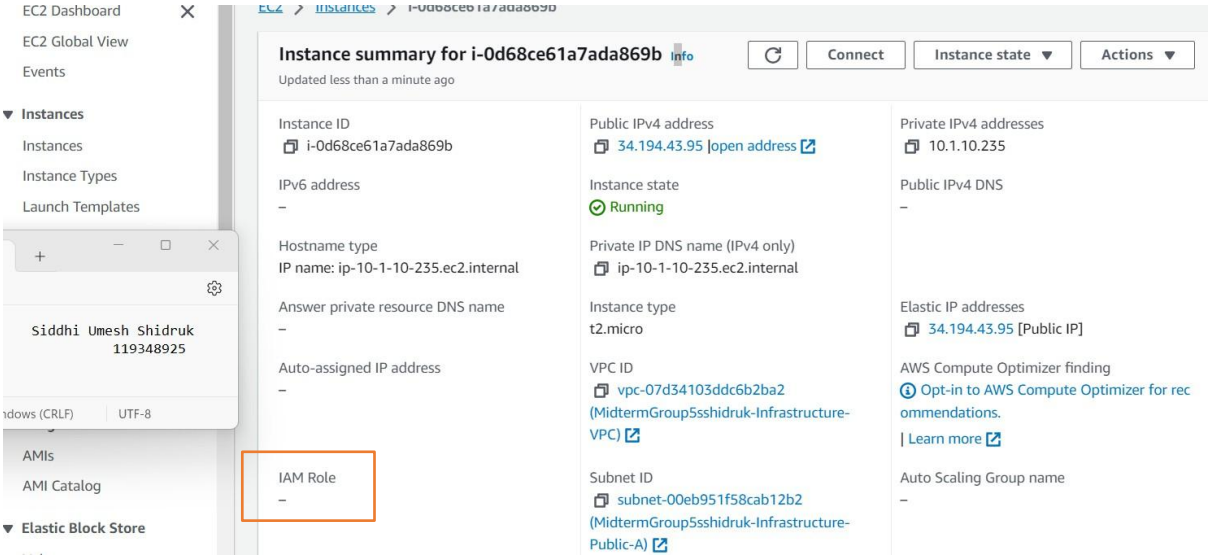
Cloud-based healthcare infrastructure with default SSH configuration will be vulnerable to RCE and if exploited by the attackers, the overall potential impact will lead to various security breaches and risks such as the availability of sensitive patient healthcare data with no confidentiality and integrity.

Potential ways for improvements:

Mitigation of the risks associated with RCE will lead to the implementation of strong passwords and the changing of default credentials. *AWS VPC* service protects RCE and allows us to prevent DoS and brute force attacks. *AWS Config* is suitable for SSH because it assesses monitoring compliance with security policies, which ensures that the default credentials are not used repeatedly.

3. IAM role not present for EC2 instance:

IAM roles under EC2 instances possess some risks, as they are a crucial security feature. Excessive permission, insecure IAM policies, unprotected access keys, and unrestricted access to EC2 metadata service are the vulnerabilities that create a loophole for security breaches.



Impact:

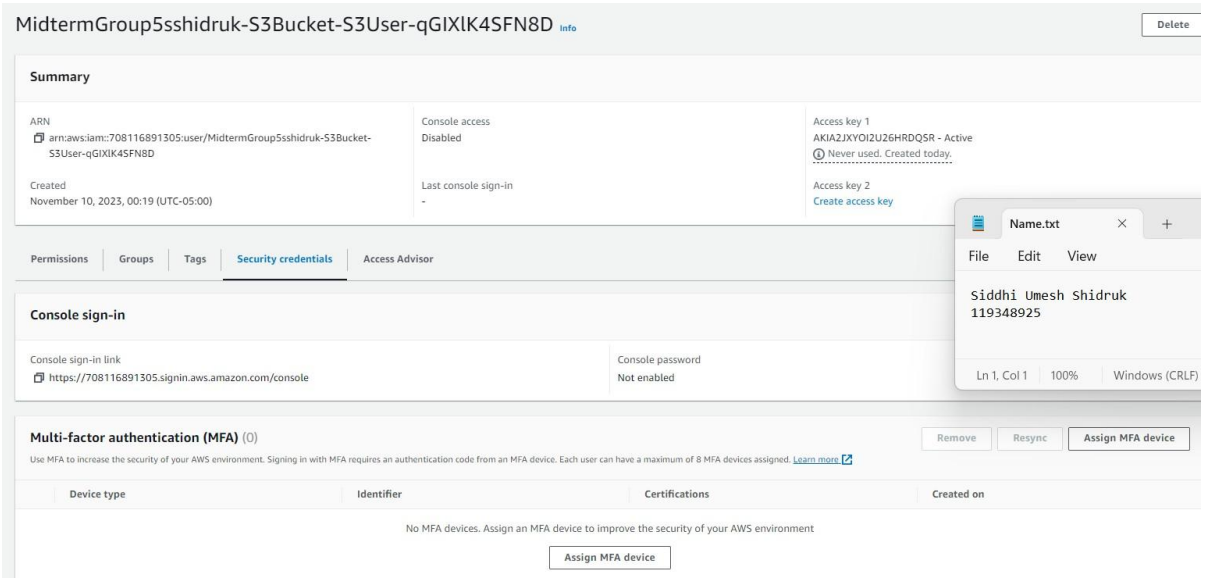
The impact of excessive permission and insecure IAM policies can allow the attacker to expose sensitive data because of the permissions associated with the EC2 stating to allow for all access keys stored on EC2 through "*", leading to compromised control over the system with inadequate logging and monitoring.

Potential ways for improvements:

Restricting the access of EC2 metadata along with deploying secure permission will improve the security loopholes. Avoiding hard-coded credentials and the use of IAM roles with temporary credentials will allow to enhance the security dynamically by following IAM policies.

4. Multifactor authentication for root account

Multi-factor Authentication for the root account is not enabled, it is easy to access the server files without any authorization.



Impact:

If the root user and the IAM user are granted the same access, this could lead to a security lapse. If the MFA in the root account is disabled, then an attacker can easily manage to get unauthorized access resulting into privilege escalation, data breaches, and credential theft. There could be a severe system outage and disruption of services.

Potential ways for improvements:

The exploits of data breaches and system outages along with unauthorized access can be controlled by the AWS services. *AWS CloudTrail* will record all the API calls and audit trails for easy monitoring of third-party logs. For compliance, IAM Policy Simulations can be used to test whether the MFA requirements are up-to-date.

Disaster Recovery Assessment Report

Overview of Report:

The recovery options for any disaster occurrences and risk management precautions utilizing AWS services will be covered in the assessment report. The lack of a recovery plan for the Healthcare infrastructure raises the possibility of data loss. The main objective of the report is to offer risk management strategies for unexpected system failures by insufficient backup methods.

Issues and Risk Management Strategies:

1. Security breaches or Database corruption:

Recommendation:
There are possibilities of data breach within the infrastructure, using *AWS Backup* these can be mitigated by managing resources across regions by implementing cross-regions and cross-account backups, this can increase availability by making backups in multiple regions. Due to any disruptions in the default region, data services can be made available from cross-regions using this service.

Also, a setup of *AWS Relational Database Service (RDS) Multi-AZs* service, which replicates original database instances in different availability zones making it available for recovery plans. Moreover, it is crucial to protect the replicated backup using some cryptographic algorithm and encryption keys. This can be done by utilizing the AWS Key Management Service (KMS) keys to encrypt the backup.

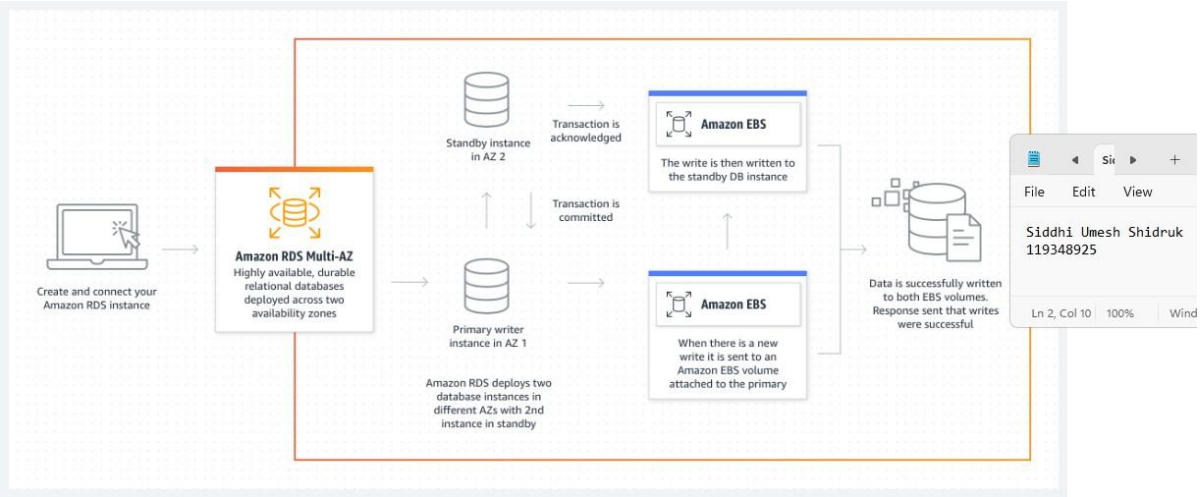
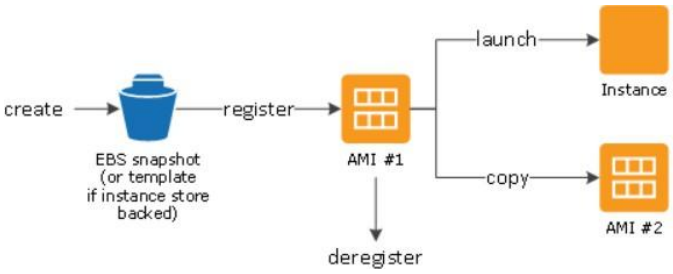


Image taken from: https://aws.amazon.com/rds/features/multi-az/

2. *Virtual Machine Crash:*

Recommendation:
There are certain unexpected events such as virtual machine breakdown, which should be considered a priority, and a solid backup plan should be available to overcome such situations. For that reason, *AWS Amazon Machine Image* (AMI) service can be useful for VM issues. AWS AMI is a fully configured image of the operating system of the user's choice.

Additionally, AWS EC2's snapshot service can be used to take snapshots of the default volume to utilize as a strategy in the case of EC2 instances breakdowns. Like the previous point, to protect the EBS volumes, *AWS Key Management Service (KMS)* keys can be employed which ensures the security of the volume's data and file system.



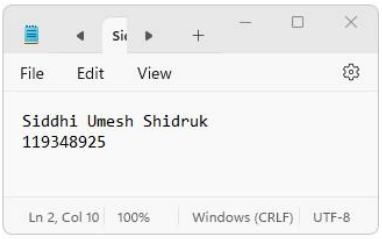


Image taken from: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

3. *Instance Termination protection disabled:*

Recommendation:
By default, instance termination is disabled, but the termination protection, for instance, should be enabled. The reason is that accidental deletion of instances can lead to various issues such as operation downtime, reconfiguration issues, and critical data loss. The best practice is to enable the protection using *AWS CLI or AWS Management Console*, which will help safeguard against accidental deletion, ensuring secure measures for any future consequences.

4. *Absence of logging and monitoring activities:*

Recommendation:
Without logging and monitoring it is difficult to detect incident responses for new vulnerabilities. The failure of an effective plan for monitoring malicious incidents can result in an overall impact on the system and a failure to prevent any consequences that can be detected.

Using the *AWS CloudWatch* and *AWS CloudTrail*, it will be easy to monitor and log activities in the infrastructure such as monitoring network traffic and data flow for unusual events. AWS CloudTrail can provide a plan to monitor captured events and track unauthorized actions.

References:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

https://docs.aws.amazon.com/whitepapers/latest/architecting-hipaa-security-and-compliance-on-aws/encryption-and-protection-of-phi-in-aws.html

https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

https://docs.aws.amazon.com/codeguru/detector-library/python/hardcoded-credentials/

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/monitoring-resolver-dns-firewall-with-cloudwatch.html

https://www.trendmicro.com/cloudoneconformity-staging/knowledge-base/aws/EBS/snapshot-encrypted.html

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html

https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards.html

https://www.awscoach.net/aws-nacl-vs-security-groups/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

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

https://www.intelligentdiscovery.io/controls/ebs/aws-ebs-encrypted-snapshots

https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#default-network-acl

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_testing-policies.html