Report for:

# AWS Security Assessment Sample Report

## ClientName

**March 24, 2021**

**Version: 1.0**


**Prepared by:** NCC Consultant

**Email:** n.consultant@nccgroup.com

**Telephone:** +44 (0)161 209 5200






NCC Group PLC - Security Testing Audit and Compliance

XYZ Building,
2 Hardman Boulevard,
Spinningfields,
Manchester,
M3 3AQ
https://www.nccgroup.com

# 1 Executive Summary

This report presents the findings of the AWS configuration security assessment conducted on behalf of Client Company Ltd (ClientName). The assessment was conducted between 15/03/2021 and 19/03/2021 and was authorised by ClientName.

## 1.1 Overview

The systems within scope require further work to ensure the security posture is appropriate to the assets which require protection. Two high risk issues were identified; these and other issues set out in this report should be addressed so that the organisation's security model maintains an appropriate defence in depth basis.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

| Component | Critical | High | Medium | Low | Total |
|---|---|---|---|---|---|
| Phase 2 –AWS Review | 0 | 2 | 3 | 5 | **10** |
| **Total** | **0** | **2** | **3** | **5** | **10** |

## 1.2 Assessment Summary

The most significant issue identified in the AWS configuration review was that IAM roles were assigned with excessive permissions. As a result, it was possible for a number of users to perform actions, such as executing arbitrary commands and accessing sensitive objects, for which they should not have sufficient permissions.

It was also of note that the network configuration was overly permissive. The account was configured in such a way that it was accessible from external addresses and the account had a high level of database connectivity. Consequently, it may be possible for external users to view the database and extract sensitive information, or information that may be helpful in developing further attacks. It is recommended that ClientName's resources are made only as accessible as necessary for normal business operation, in line with the principle of least privilege.

The remaining issues were all assessed to pose a lower risk or are reported for information only. Nevertheless, it is recommended that these are reviewed and addressed so as to bring the environment within scope into line with security best practice. It is important to recognise that even low risk issues can be exploited in combination with other issues as part of a wider attack which seeks to compromise an environment or application. In addition, resolving lower risk issues can have the dual benefit of reducing the attractiveness of systems to opportunistic attackers as well as enhancing the overall security posture.

More detailed information on each of the issues which were identified is included in the Technical Details section of this report.

## 1.3 Strategic Recommendations

The permissions assigned to the various IAM roles should be reviewed and amended such that all roles are only accorded the minimum permissions required to perform the required business functions. The inbuilt AWS IAM tools and functionality allow a considerable degree of control; however, these controls can only be effective when permissions are assigned to roles in accordance with the principle of least privilege.

Similarly, the AWS account should not be externally accessible from the wider Internet and the principle of least privilege should be applied to the resources which are accessible within the account. Alternatively, if external access is required, consideration should be given to restricting access to trusted IP addresses only.

It is acknowledged that operational business requirements may mean that a risk has to be accepted (or partly accepted) rather than mitigated. Where this is the case, it is recommended that this is appropriately documented within the relevant Risk Register to ensure that the organisation maintains full visibility of the risk to which it is exposed.

It is recommended that the issues set out in this report should be addressed by a structured programme of remedial actions which are prioritised in accordance with the perceived risk to the organisation.

# 2 Table of Contents

# 3 Technical Summary

NCC Group was contracted by ClientName to conduct a security assessment of the systems within scope in order to identify security issues that could negatively affect ClientName's business or reputation if they led to the compromise or abuse of systems.

## 3.1 Scope

The security assessment was carried out in the Production environment and included:

- AWS Review

The environment within the scope of this test is listed below:

- Client AWS Account `123456789012`

## 3.2 Caveats

Due to the nature of the environment, checks that would have a high probability of causing disruption to the named hosts were excluded. Denial of service attempts were excluded for the same reason.

## 3.3 Post Assessment Cleanup

Any test accounts which were created for the purpose of this assessment should be disabled or removed, as appropriate, together with any associated content. Delete the AWS account provisioned for this assessment.

Revert any WAF/IDS/IPS/firewall changes which were made for the purposes of the assessment.

## 3.4 Risk Ratings

The table below gives a key to the icons and symbols used throughout this report to provide a clear and concise risk scoring system. It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

| Symbol | Risk Rating | CVSSv2 Score | Explanation |
|---|---|---|---|
|  | CRITICAL | 9.0 - 10 | A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible. |
|  | HIGH | 7.0 - 8.9 | A vulnerability was discovered that has been rated as high. This requires resolution in the short term. |
|  | MEDIUM | 4.0 - 6.9 | A vulnerability was discovered that has been rated as medium. This should be resolved as part of the ongoing security maintenance of the system. |
|  | LOW | 1.0 - 3.9 | A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks. |
|  | INFO | 0 - 0.9 | A discovery was made that is reported for information. This should be addressed in order to meet leading practice. |
|  | GOOD | N/A | Good security practices were being followed or an audit item was found to be present and correct. |

## 3.5 Findings Overview

All the issues identified during the assessment are listed below with a risk rating for each issue.

| Ref | Finding | Risk |
|---|---|---|
| SR-109-001 | **IAM Roles Assigned With Excessive Permissions** | High  |
| SR-109-002 | **Overly Permissive Network Configuration** | High  |
| SR-109-003 | **Unauthorised Access to S3 Buckets** | Medium  |
| SR-109-004 | **User Without MFA Enabled** | Medium  |
| SR-109-005 | **IAM Password Policy** | Medium  |
| SR-109-006 | **Automated Backups Not Enabled for RDS Instances** | Low  |
| SR-109-007 | **Single Availability Zone RDS Instance** | Low  |
| SR-109-008 | **Unused Security Groups** | Low  |
| SR-109-009 | **Subnets Using Default Network ACLs** | Low  |
| SR-109-010 | **CloudFormation Stack Without Termination Protection** | Low  |

# 4 Technical Details

| SR-109-001 | IAM Roles Assigned With Excessive Permissions | | |
|---|---|---|---|
| **Risk Rating** | High | **Status** | Open |

**Description:**
An analysis of the configured roles that were then assigned to running EC2 instances indicated that some of them would receive excessive permissions that could allow arbitrary commands to be launched across all the instances, read arbitrary S3 objects, etc.

As an example, the following role was present in the AWS configuration reviewed during this assessment:

```
[role name]
```

The following is a screenshot for this role listing the inline policies:

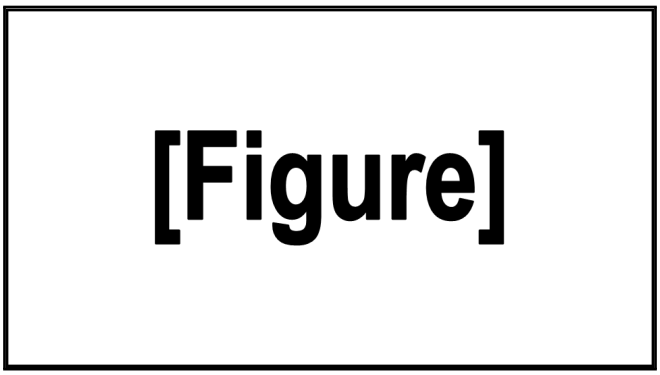


Figure 1: Sample role with inline policies attached

The "IAMFullAccess" inline policy was defined as follows:

```
{
    "Version": "2020-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*"
        }
    ]
}
```

The above policy gave administrative permissions to perform all actions in IAM, including managing passwords, access keys, MFA devices and user certificates.

This issue was rated as high risk in consideration of the security impact of unrestricted access to the IAM service.

**Recommendation:**
Create managed security policies following the least privileges security principle (i.e. including only the minimal set of API commands necessary for operations and listing the resources that would be affected by these commands) and attach these to the roles in use.[1,2,3,4]

**Affects:**

| AWS Account |
| --- |
| 123456789012 |

[1] **AWS Identity and Access Management (IAM)** https://aws.amazon.com/iam/
[2] **AWS Identity and Access Management Documentation** https://aws.amazon.com/documentation/iam/
[3] **AWS Documentation –IAM Best Practices: Use AWS Defined Policies to Assign Permissions Whenever Possible** https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#bp-use-aws-defined-policies
[4] **AWS Documentation – IAM Best Practices: Grant Least Privilege** https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

| SR-109-002 | Overly Permissive Network Configuration | | |
|---|---|---|---|
| **Risk Rating** | High | **Status** | Open |

**Description:**
Examination of the high level architecture diagram and configured firewall rules indicated that the network configuration was excessively permissive and a number of resources were publicly available.

The following high level figure illustrates the external addresses that were allowed a degree of access into the account:

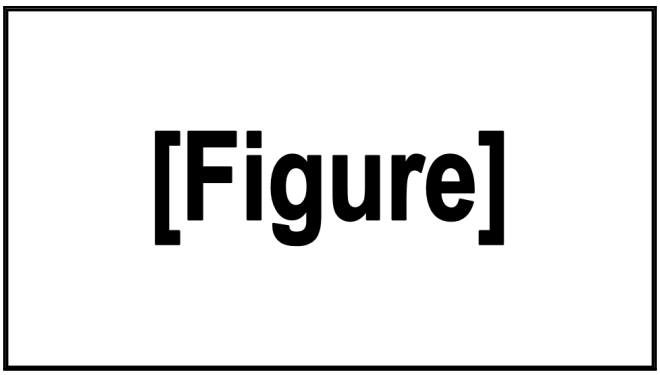


Figure 2: Global view of the AWS account

The following figure illustrates the high level database connectivity within the account:

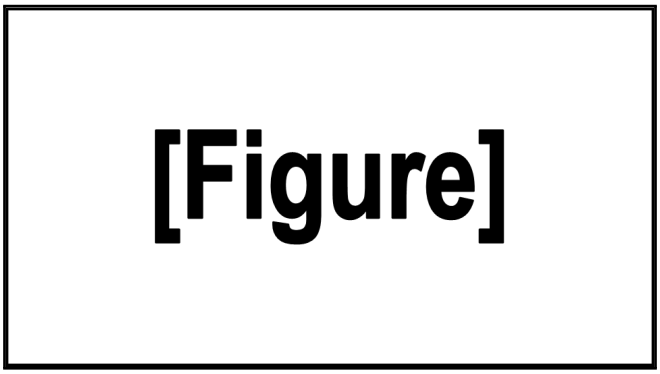


Figure 3: High level view of the database connectivity

The following figure illustrates the high level configuration of Virtual Private Networks (VPCs) within the account:

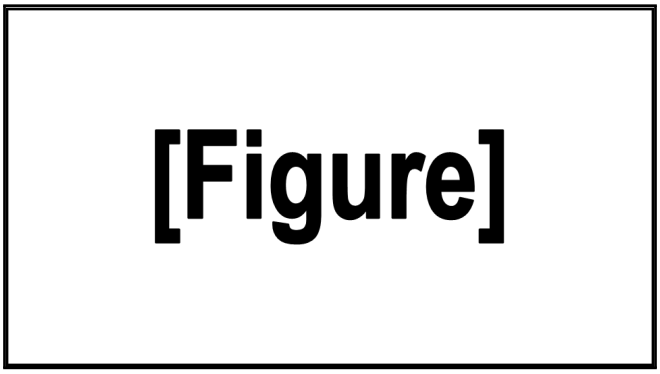


Figure 4: High level view of the VPC configuration

After review of the above, the following observations can be made:

- A large number of resources were publicly accessible. This presents an opportunity for abuse, especially in the case of sensitive or corporate resources.
- A permissive network configuration was observed, which allowed connections between resources in different sublets and VPCs. This poses a significant risk in the event that a host is compromised, as it would potentially enable attackers to move laterally within the AWS account.
- The AWS account held all of ClientName's assets, including corporate and production environments. This is considered contrary to security best practice.

**Recommendation:**
Unless necessary for normal business operation, ensure that the network is only accessible from internal addresses, or if not possible, consider creating a whitelist of external addresses which can access the network. Doing so will limit the resources that are accessible to an attacker. This could deny the individual access to information that may have been helpful in developing an attack, and it may deny a potential avenue into a achieving a foothold on the network.

ClientName should also limit the access privileges and general interconnectivity of the sublets, VPCs, and AWS account in line with the principle of least privilege. These privileges should be reduced to only what is necessary for normal operation of the business to as to limit an attacker's options in the event of a compromise.

**Affects:**

| AWS Account |
| --- |
| 123456789012 |

| SR-109-003 | Unauthorised Access to S3 Buckets | | |
|---|---|---|---|
| **Risk Rating** | Medium | **Status** | Open |

**Description:**
An S3 bucket was found to be configured with excessive permissions that could allow unauthorised access to the stored objects. This bucket included access to logs of the portal web application.

The following screenshot from the Management Console shows how full permissions to access the objects stored in the `BucketName` bucket were granted to any authenticated AWS user:

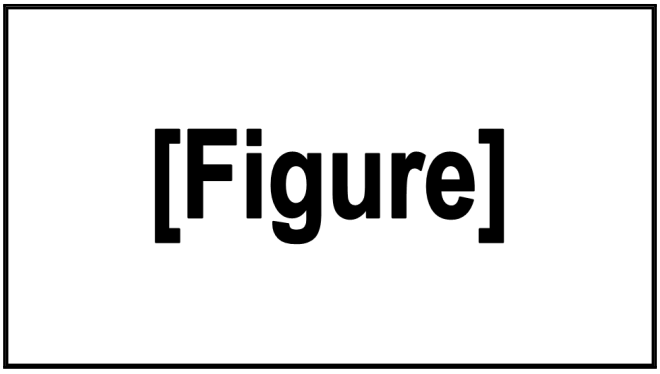


Figure 5: S3 bucket access

The "Any Authenticated AWS User" is a special group that will include any user having access to AWS and not only the users associated with the ClientName account. To demonstrate this problem, the following command was executed using API keys belonging to an NCC Group account:

```
$ aws --profile nccgroup s3 ls --recursive s3://[BucketName]

...
2021-01-25 09:45:04      765520 logs-01-25-2021.log
2021-01-26 11:22:01      801528 logs-01-26-2021.log
...
```

According to the permissions visible above, objects could have been downloaded and also deleted or otherwise edited. Additionally, new objects could be uploaded.

The following table includes all the S3 buckets affected by this issue and the type of permissions allowed to anonymous and any other AWS user (i.e. including AWS users not belonging to ClientName):

| S3 Bucket | User type | List | Upload/delete | View | Edit |
|---|---|---|---|---|---|
| BucketName | Any AWS user | Yes | Yes | Yes | Yes |

Technical details about this issue were transmitted to ClientName during testing and some actions were performed to mitigate the risk associated with this issue.

**Recommendation:**
Edit the permissions associated to the affected S3 buckets ensuring that no permissions are granted to the anonymous or "Any Authenticated AWS User" group. [5,6,7]

**Affects:**

| AWS Account |
| --- |
| 123456789012 |

[5] **Amazon S3** https://aws.amazon.com/s3/
[6] **Amazon Simple Storage Service Documentation** https://aws.amazon.com/documentation/s3/
[7] **AWS Documentation –Managing Access Permissions to Your Amazon S3 Resources** https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html

| SR-109-004 | User Without MFA Enabled | |  |
|---|---|---|---|
| **Risk Rating** | Medium | **Status** | Open |

**Description:**

Multiple accounts were identified which had password authentication enabled but did not have multi-factor authentication (MFA) enabled, contrary to security best practice. If MFA is not enabled, attackers could be able to access the AWS web console with just a username and password combination.

The following users had password-enabled access but were not configured to use multi-factor authentication:

```
<<List of users without MFA enabled>>
```

The users listed above were identified by running the following command from the AWS CLI:

```
aws iam get-credential-report --query 'Content' --output text | base64 -d | cut -d, -f1,4,8
```

The following was returned during testing in response to the above command:

```
[UserName], true, false
```

In this case, "true" after the username means that authentication via password was active. However, "false" returned in the third column means that MFA was not active.

**Recommendation:**

Implement MFA for the users with password authentication enabled.[8,9,10,11]

**Affects:**

| AWS Account |
|---|
| 123456789012 |

[8] **AWS Identity and Access Management (IAM)** https://aws.amazon.com/iam/
[9] **AWS Identity and Access Management Documentation** https://aws.amazon.com/documentation/iam/
[10] **AWS Documentation – Using Multi-Factor Authentication (MFA) in AWS** https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html
[11] **CIS Amazon Web Services Foundations** https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

| SR-109-005 | IAM Password Policy | | |
|---|---|---|---|
| **Risk Rating** | Medium | **Status** | Open |

**Description:**
No password policy was enabled in the IAM settings. This could result in the creation of weak user passwords.

The following screenshot illustrates the password policy settings that were observed:

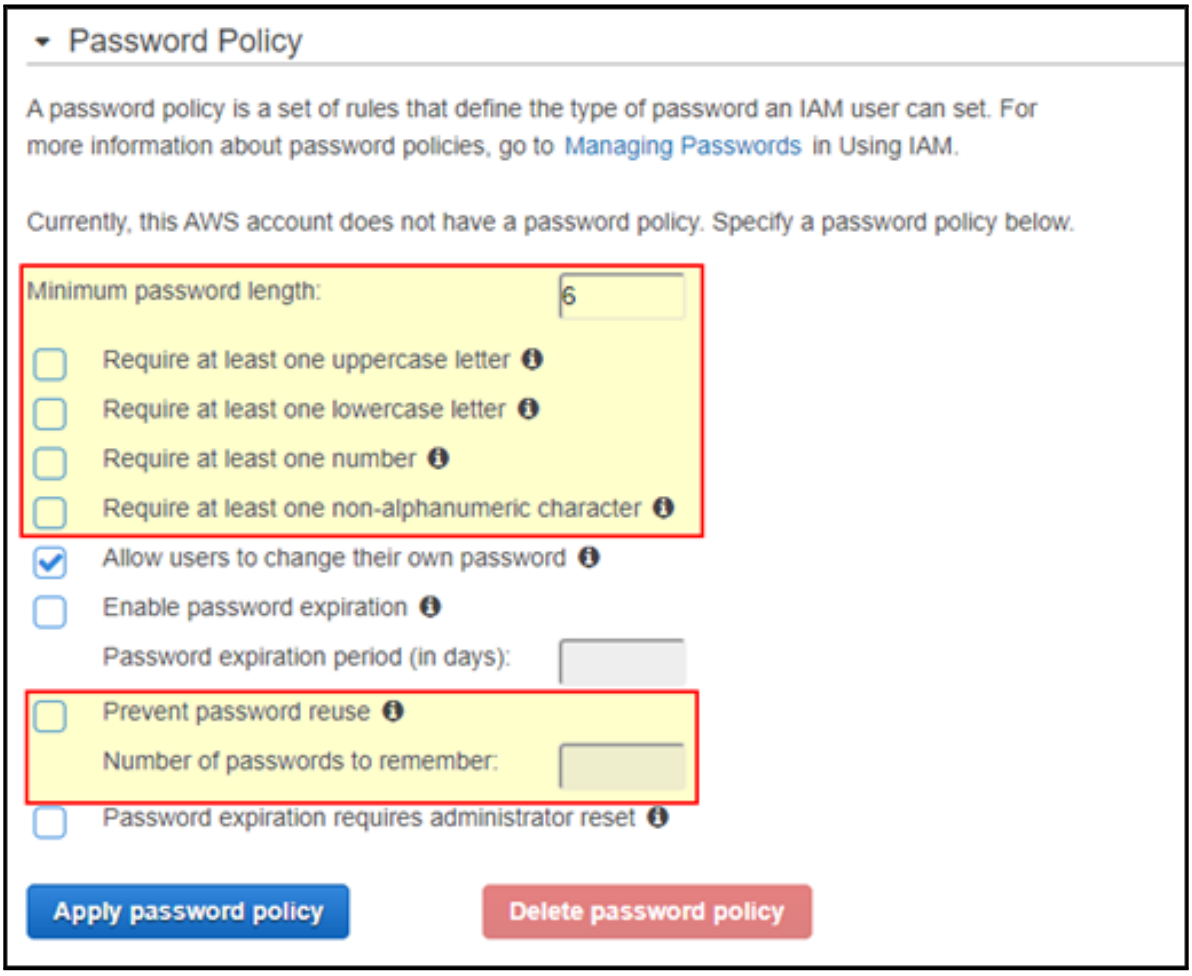


Figure 6: Password policy not enforced

**Recommendation:**

Ensure a strong password policy is in place. Specifically ensure that the following password policy is enforced:[12, 13, 14, 15]

- Passwords should use mixed case
- Passwords should include at least one number
- Passwords should include at least one symbol
- Passwords have a minimum length of 14 characters
- Passwords cannot be reused

**Affects:**

| AWS Account |
| --- |
| 123456789012 |

[12] **AWS Identity and Access Management (IAM)** https://aws.amazon.com/iam/
[13] **AWS Identity and Access Management Documentation** https://aws.amazon.com/documentation/iam/
[14] **AWS Documentation –Managing Passwords** https://docs.aws.amazon.com/IAM/latest/UserGuide/Credentials-ManagingPasswords.html
[15] **CIS Amazon Web Services Foundations** https://www.cisecurity.org/benchmark/amazon_web_services/

| SR-109-006 | Automated Backups Not Enabled for RDS Instances | | |
|---|---|---|---|
| **Risk Rating** | Low | **Status** | Open |

**Description:**

Automated backups had not been enabled for a number of Relational Database Service (RDS) instances. This feature facilitates the creation of periodic RDS instance snapshots, which in turn ensure that data restoration is possible in the event of an incident affecting the source database.

The following screenshot from the Management Console shows that the `production-data` and `development-db` RDS instances had automated backups disabled:

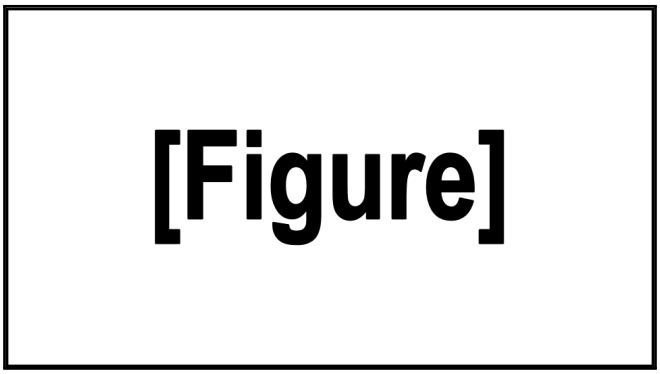


Figure 7: RDS Instance with automated backups disabled

**Recommendation:**

Ensure that all RDS database instances that host sensitive data have automated backups enabled for point-in-time recovery. [16, 17, 18]

**Affects:**

| AWS Account |
|---|
| 123456789012 |

[16] **Amazon Relational Database Service (RDS)** https://aws.amazon.com/rds/
[17] **Amazon Relational Database Service Documentation** https://aws.amazon.com/documentation/rds/
[18] **AWS Documentation –Backing Up and Restoring Amazon RDS DB Instances** https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_CommonTasks.BackupRestore.html

| SR-109-007 | Single Availability Zone RDS Instance | | |
|---|---|---|---|
| **Risk Rating** | Low | **Status** | Open |

**Description:**

A number of Relational Database Service (RDS) instances were configured without the Multi-Availability Zone (Multi-AZ) enabled. Without this, should an availability zone specific database failure occur, then Amazon RDS cannot automatically fail over to the standby availability zone so that database operations can resume quickly without administrative intervention.

The following database instances (based on the aurora engine) were configured with Multi-AZ disabled:

- preproduction-data
- test-data
- development-db

The following screenshot shows that Multi-AZ was disabled for one of the instances listed above:

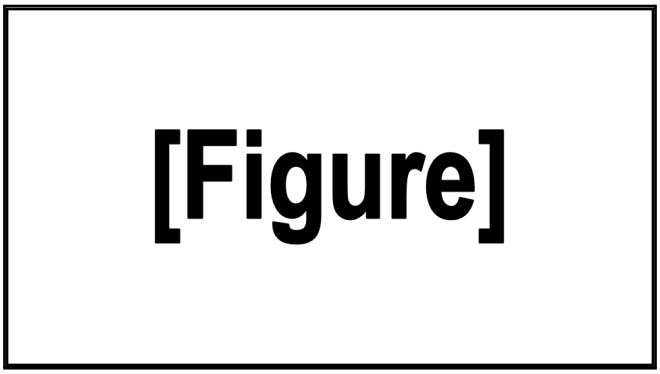


Figure 8: RDS Availability Zone

**Recommendation:**

Consideration should be given to modifying the configuration of the database instances to enable Multi-AZ. This is especially important if the applications using the databases require high availability.[19,20,21]

**Affects:**

| AWS Account |
|---|
| 123456789012 |

[19] **Amazon Relational Database Service (RDS)** https://aws.amazon.com/rds/
[20] **Amazon Relational Database Service Documentation** https://aws.amazon.com/documentation/rds/
[21] **AWS Documentation –High Availability (Multi-AZ)** https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

| SR-109-008 | Unused Security Groups | |  |
|---|---|---|---|
| **Risk Rating** | Low | **Status** | Open |

**Description:**

A number of security groups were defined which were unused and may not be required. This being the case, their existence in the configuration increases the risk that they may be inappropriately assigned.

The following security groups were found to be unused:

- `SecurityGroupName1` (security group ID `sg-123456789`)
- `SecurityGroupName2` (security group ID `sg-123456789`)
- `SecurityGroupName3` (security group ID `sg-123456789`)

**Recommendation:**

The unused security groups should be reviewed and removed if no longer required.[22,23,24]

**Affects:**

| AWS Account |
|---|
| 123456789012 |

[22] **Amazon Virtual Private Cloud** https://aws.amazon.com/vpc/
[23] **Amazon Virtual Private Cloud Documentation** https://aws.amazon.com/documentation/vpc/
[24] **CIS Amazon Web Services Foundations** https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

| SR-109-009 | Subnets Using Default Network ACLs | | |
|---|---|---|---|
| **Risk Rating** | Low | **Status** | Open |

**Description:**
A number of subnets were identified to be using the default Network Access Control List (NACL), allowing all incoming and outgoing network traffic. In this configuration, the affected NACLs do not provide the secondary layer of security defence that they are supposed to.

The following network ACLs were affected by this issue in the `us-east-1` region:

- «NACL name» (NACL ID `acl-123456789`)
- «NACL name» (NACL ID `acl-123456789`)
- «NACL name» (NACL ID `acl-123456789`)

The following screenshot was taken from the AWS Management Console and shows the inbound rules available for the first of the NACLs listed above:

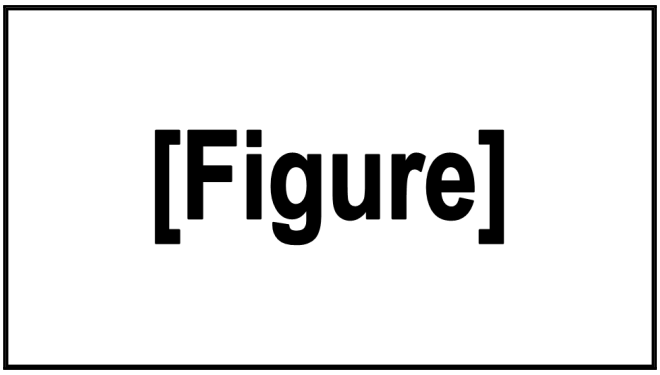


Figure 9: Default network ACL in use

The outbound rules were similar, allowing all outgoing traffic.

It should be noted that default NACLs were also available across the remaining AWS regions/VPC.

**Recommendation:**
Network ACLs should be considered as the secondary layer of security defence against unwanted traffic. Consequently, consideration should be given to implementing NACLs that only allow the necessary inbound and outbound traffic to the associated VPC subnets.[25,26,27,28,29]

**Affects:**

| AWS Account |
|---|
| 123456789012 |

[25] **Amazon Virtual Private Cloud** https://aws.amazon.com/vpc/
[26] **Amazon Virtual Private Cloud Documentation** https://aws.amazon.com/documentation/vpc/
[27] **AWS Documentation –VPC Security** https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html
[28] **AWS Documentation –Network ACLs** https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html7
[29] **AWS Documentation –Recommended Network ACL Rules for Your VPC** https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_NACLs.html

| SR-109-010 | CloudFormation Stack Without Termination Protection | |  |
|---|---|---|---|
| **Risk Rating** | Low | **Status** | Open |

**Description:**

The Termination Protection setting available for the CloudFormation service was not found to be enabled for one stack. When this feature is enabled for a stack, deletion attempts will fail and the stack (including its current status), will remain unchanged. Security best practice for CloudFormation management recommends enabling this feature for production environments.

The following command was run for the `StackName` stack:

```
$ aws cloudformation describe-stacks --region eu-west-1 --stack-name [StackName] --
 ➜  query 'Stacks[*].EnableTerminationProtection'
 ➜
[
    false
]
```

As can be seen above, the `describe-stacks` command returned `false`, indicating that the Termination Protection safety feature was not enabled for the selected stack.

It should be noted that CloudFormation stack policies may also be used to prevent stack resources from being unintentionally updated or deleted during a stack update process. However, stack policies cannot protect stacks from being terminated, as IAM users who have the permission to delete a stack may still delete it.

**Recommendation:**

Ensure that Amazon CloudFormation stacks have Termination Protection enabled in order to protect them from being accidentally deleted.[30,31,32]

**Affects:**

| AWS Account |
|---|
| 123456789012 |

[30] **AWS CloudFormation** https://aws.amazon.com/cloudformation/
[31] **AWS CloudFormation Documentation** https://aws.amazon.com/documentation/cloudformation/
[32] **AWS Documentation –Protecting a Stack From Being Deleted** https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-protect-stacks.html

# 5 Document Control

## Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

## Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Client Company Ltd (ClientName).

NCC Group gives permission to copy this report for the purposes of disseminating information within your organisation or any regulatory agency.

## 5.1 Document Data

| | |
|---|---|
| **Data Classification** | Client Confidential |
| **Client Name** | ClientName |
| **Project Reference** | 99999 |
| **Document Title** | AWS Security Assessment Sample Report |
| **Author** | NCC Consultant |

## 5.2 Document History

| Issue No. | Issue Date | Issued by | Change Description |
|---|---|---|---|
| 0.1 | 2021-03-22 | NCC Consultant | Draft for NCC Group internal review only |
| 0.2 | 2021-03-23 | A. Reviewer | Revised QA |
| 1.0 | 2021-03-24 | NCC Consultant | Released to client |

## 5.3 Document Distribution List

| Name | Role |
|---|---|
| A. Sponsor | Project Sponsor, ClientName |
| NCC Consultant | Consultant, NCC Group |
| A. Manager | Account Manager, NCC Group |

# 6 Assessment Team

The following members of staff were assigned to this assessment:

| Name | Job Title | Comments |
|---|---|---|
| NCC Consultant | Senior Security Consultant, NCC Group | CREST Registered Tester (CRT), Offensive Security Certified Professional (OSCP) |