Survey Administration Guide

Table of Contents

[Hosting Configuration 1](#_Toc473635202)

[AWS Basic Deployment Configuration 1](#_Toc473635203)

# Hosting Configuration

The back-end components for the Survey solution are deployed in AWS.

## AWS Configuration

Please complete the following steps to configure the Survey environment on AWS:

1. Log into the AWS administration console (AWS Account Number: 544253582050).
2. Switch to the correct AWS region (EU – Ireland).
3. Complete the following steps to create the **Survey** VPC:
   1. Select **Services > Networking > VPC** from the menu.
   2. Click on **Virtual Private Cloud > Your VPCs**.
   3. Click **Create VPC**.
   4. Enter the details for the new VPC:  
        
      Name tag: Survey   
      CIDR block: 10.0.0.0/16  
      Tenancy: Default
   5. Click **Yes, Create**.
4. Complete the following steps to create the **Survey** internet gateway:
   1. Select **Services > Networking > VPC** from the menu.
   2. Click on **Virtual Private Cloud > Internet Gateways**.
   3. Click **Create Internet Gateway**.
   4. Enter the details for the new internet gateway:  
        
      Name tag: Survey
   5. Click **Yes, Create**.
   6. Select the new internet gateway in the list and click **Attach to VPC**.
   7. Select the Survey VPC and click **Yes, Attach**.
5. Complete the following steps to create the **Survey - Public** network ACL:
   1. Select **Services > Networking > VPC** from the menu.
   2. Click **Security > Network ACLs**.
   3. Click **Create Network ACL**.
   4. Enter the details for the new network ACL:  
        
      Name tag: Survey - Public  
      VPC: Survey
   5. Click **Yes, Create**.
   6. Select the new network ACL in the list.
   7. Select the **Inbound Rules** tab and click **Edit**.
   8. Click **Add another rule** and enter the following details:  
        
      Rule #: 100  
      Type: Custom TCP Rule  
      Protocol: TCP  
      Port Range: 80  
      Source: 0.0.0.0/0  
      Allow / Deny: Allow
   9. Click **Add another rule** and enter the following details:  
        
      Rule #: 101  
      Type: Custom TCP Rule  
      Protocol: TCP  
      Port Range: 443  
      Source: 0.0.0.0/0  
      Allow / Deny: Allow
   10. Click **Add another rule** and enter the following details:  
         
       Rule #: 102  
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 22  
       Source: 0.0.0.0/0  
       Allow / Deny: Allow
   11. Click **Add another rule** and enter the following details:  
         
       Rule #: 103  
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 1024-65535  
       Source: 0.0.0.0/0  
       Allow / Deny: Allow
   12. Click **Save**.
   13. Select the **Outbound Rules** tab and click **Edit**.
   14. Click **Add another rule** and enter the following details:  
         
       Rule #: 100  
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 1024-65535  
       Destination: 0.0.0.0/0  
       Allow / Deny: Allow
   15. Click **Add another rule** and enter the following details:  
         
       Rule #: 101  
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 80  
       Destination: 0.0.0.0/0  
       Allow / Deny: Allow
   16. Click **Add another rule** and enter the following details:  
         
       Rule #: 102  
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 443  
       Destination: 0.0.0.0/0  
       Allow / Deny: Allow
   17. Click **Save**.
6. Complete the following steps to create the **Survey - Public** security group:
   1. Select **Services > Networking > VPC** from the menu.
   2. Click **Security > Security Groups**.
   3. Click **Create Security Group**.
   4. Enter the details for the security group:  
        
      Name tag: Survey - Public  
      Group name: Survey - Public  
      Description: Survey – Public  
      VPC: Survey
   5. Click **Yes, Create**.
   6. Select the Survey - Public security group in the list.
   7. Select the **Inbound Rules** tab and click **Edit**.
   8. Enter the details for the new inbound rule for TCP port 80:  
        
      Type: Custom TCP Rule  
      Protocol: TCP  
      Port Range: 80  
      Source: 0.0.0.0/0
   9. Click **Add another rule**.
   10. Enter the details for the new inbound rule for TCP port 443:  
         
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 443  
       Source: 0.0.0.0/0
   11. Click **Add another rule**.
   12. Enter the details for the new inbound rule for TCP port 22 (SSH):  
         
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 22  
       Source: 0.0.0.0/0
   13. Click **Save**.
7. Complete the following steps to create the **Survey - DB** network ACL:
   1. Select **Services > Networking > VPC** from the menu.
   2. Click **Security > Network ACLs**.
   3. Click **Create Network ACL**.
   4. Enter the details for the new network ACL:  
        
      Name tag: Survey - DB  
      VPC: Survey
   5. Click **Yes, Create**.
   6. Select the new network ACL in the list.
   7. Select the **Inbound Rules** tab and click **Edit**.
   8. Click **Add another rule** and enter the following details:  
        
      Rule #: 100  
      Type: Custom TCP Rule  
      Protocol: TCP  
      Port Range: 5432  
      Source: 10.0.0.0/24  
      Allow / Deny: Allow
   9. Click **Add another rule** and enter the following details:  
        
      Rule #: 101  
      Type: Custom TCP Rule  
      Protocol: TCP  
      Port Range: 1024-65535  
      Source: 10.0.0.0/24  
      Allow / Deny: Allow
   10. Click **Save**.
   11. Select the **Outbound Rules** tab and click **Edit**.
   12. Click **Add another rule** and enter the following details:  
         
       Rule #: 100  
       Type: Custom TCP Rule  
       Protocol: TCP  
       Port Range: 1024-65535  
       Destination: 10.0.0.0/24  
       Allow / Deny: Allow
   13. Click **Save**.
8. Complete the following steps to create the **Survey - DB** security group:
   1. Select **Services > Networking > VPC** from the menu.
   2. Click **Security > Security Groups**.
   3. Click **Create Security Group**.
   4. Enter the details for the security group:  
        
      Name tag: Survey - DB  
      Group name: Survey - DB  
      Description: Survey – DB  
      VPC: Survey
   5. Click **Yes, Create**.
   6. Select the Survey - DB security group in the list.
   7. Select the **Inbound Rules** tab and click **Edit**.
   8. Enter the details for the new inbound rule for TCP port 80:  
        
      Type: Custom TCP Rule  
      Protocol: TCP  
      Port Range: 5432  
      Source: 10.0.0.0/24
   9. Click **Save**.
9. Complete the following steps to create the **Survey - Public - A** subnet:
   1. Select **Services > Networking > VPC** from the menu.
   2. Click **Virtual Private Cloud > Subnets**.
   3. Click **Create Subnet**.
   4. Enter the details for the new subnet:  
        
      Name tag: Survey - Public - A  
      VPC: Survey  
      Availability Zone: eu-west-1a  
      CIDR block: 10.0.0.0/25
   5. Click **Yes, Create**.
   6. Select the Survey - Public - A subnet in the list.
   7. Select the **Network ACL** tab and click **Edit**.
   8. Select the **Survey - Public** network ACL from the list.
   9. Click **Save**.
10. Complete the following steps to create the **Survey - Public - B** subnet:
    1. Select **Services > Networking > VPC** from the menu.
    2. Click **Virtual Private Cloud > Subnets**.
    3. Click **Create Subnet**.
    4. Enter the details for the new subnet:  
         
       Name tag: Survey - Public - B  
       VPC: Survey  
       Availability Zone: eu-west-1b  
       CIDR block: 10.0.0.128/25
    5. Click **Yes, Create**.
    6. Select the Survey - Public - B subnet in the list.
    7. Select the **Network ACL** tab and click **Edit**.
    8. Select the **Survey - Public** network ACL from the list.
    9. Click **Save**.
11. Complete the following steps to create the **Survey - Public** route table:
    1. Select **Services > Networking > VPC** from the menu.
    2. Click **Virtual Private Cloud > Route Tables**.
    3. Click **Create Route Table**.
    4. Enter the details for the new route table:  
         
       Name tag: Survey - Public  
       VPC: Survey
    5. Click **Yes, Create**.
    6. Select the new route table in the list.
    7. Select the **Routes** tab and click **Edit**.
    8. Click **Add another route**.
    9. Enter the details for the new route:  
         
       Destination: 0.0.0.0/0  
       Target: Select the Survey Internet Gateway
    10. Click **Save**.
    11. Select the **Subnet Associations** tab and click **Edit**.
    12. Select the Survey - Public - A and Survey - Public - B subnets in the list and click **Save**.
12. Complete the following steps to create the Survey RDS instance:
    1. Select **Services > Database > RDS** from the menu.
    2. Click **RDS Dashboard > Instances**.
    3. Click **Launch DB Instance**.
    4. Select **PostgreSQL** and click **Select**.
    5. Select **Dev / Test** and click **Next Step**.
    6. Enter the details for the new RDS instance:  
         
       DB Engine Version: 9.6.1  
       DB Instance Class: db.t2.small  
       Multi-AZ Deployment: Yes  
       Storage Type: General Purpose (SSD)  
       Allocated Storage: 100GB  
       DB Instance Identifier: survey   
       Master Username: postgres  
       Master Password: GSPQzQ3EL95JCnaz  
       Confirm Password: GSPQzQ3EL95JCnaz
    7. Click **Next Step**.
    8. Enter the advanced settings for the RDS instance:  
         
       VPC: Survey  
       Subnet Group: The default subnet group for the Survey VPC  
       Publicly Accessible: No  
       Availability Zone: No preference  
       VPC Security Group(s): Survey – DB (VPC)  
         
       Database Name: survey  
       Database Port: 5432  
       DB Parameter Group: default.postgres9.6  
         
       Backup Retention Period: 7 days  
       Backup Window: No Preference  
         
       Enable Enhanced Monitoring: No  
         
       Auto Minor Version Upgrade: Yes  
       Maintenance Window: No Preference
    9. Click **Launch DB Instance**.
13. Complete the following steps to create the Survey – App – 1instance:
    1. Select **Services > Compute > EC2** from the menu.
    2. Click **Instances > Instances**.
    3. Click **Launch Instance**.
    4. Select **Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type**.
    5. Select the **t2.large** instance type.
    6. Click **Next: Configure Instance Details**.
    7. Enter the details for the new instance:  
         
       Number of instances: 1  
       Network: Survey  
       Subnet: Survey – Public - A  
       Auto-assign Public IP: Enable  
       IAM role: None  
       Shutdown behavior: Stop  
       Enable termination protection: Protect against accidental termination  
       Monitoring: None  
       Tenancy: Shared – Run a shared hardware instance  
         
       Network interfaces: Leave default options
    8. Click **Next: Add Storage**.
    9. Enter **100 GiB** as the size of the **Root** volume with the **General Purpose SSD (GP2)** volume type.
    10. Click **Next: Add Tags**.
    11. Add the tag **Name** with the value **Survey – App - 1**.
    12. Click **Next: Configure Security Group**.
    13. Select the **Survey - Public** existing security group.
    14. Click **Review and Launch**.
    15. Click **Launch**.
    16. Ensure you select the correct key to use to login to the instance.

## AWS Instances

The following instances have been configured for the solution: