# Migration plan: Customer Name

This document will also form the basis of “As Built” documentation.

The purpose of this document is to outline the migration plan, provide build instructions for build engineers and provide information for the customer.

A lot of the documentation required is “infrastructure as code” in GIT repositories so the main purpose of this document is to outline the base configuration, High Level Stack, Code Repositories and Approach.

**High Level Activities**

*(Some of these may have already been completed as part of the initial discovery work prior to migration)*

|  |  |  |
| --- | --- | --- |
| **Task** | **Purpose** | **Responsibility** |
| Access to customer infrastructure, code and schemas. | Access provided to Teem to be able to review existing assets including code, technology and data schemas | Customer |
| Setup new environments | Create new environments to run customer applications and data in. | Teem |
| Security configuration | Ensure all environments meet AWS best practice / advisory requirements. | Teem |
| Deployment Setup | Ensure code can be deployed in a continuous integration model. | Teem |
| Data migration | Migrate data (different intervals during project including Smoke testing, dry runs and final migration). | Teem |
| Testing | Testing and validation of environment configuration in dev, prod (pre-go live) | Teem/Customer |
| Final Migration | Work together on final cutover of environment including DNS changes, final data migration. | Teem/Customer |

## Initial configuration

### Customer AWS accounts

The following AWS accounts will be created/used as part of the migration.

|  |  |  |
| --- | --- | --- |
| **Name** | **Account ID** | **Purpose** |
| Root-user |  | IAM User Authentication for Cross Account IAM Access to Sub Accounts.  Cloud Automation Tasks (Ansible etc…)  Route53 DNS Records |
| Dev/Test | TBD | Development, Test environments for Applications (OpenShift Docker etc…) |
| Prod |  | Production Apps and Data account |
| Ops | Not provisioned/required | For ops team/support including monitoring, VPC peering to other accounts for access via VPN/Bastion hosts etc. |

### Teem Ops AWS Accounts

The existing Teem Ops AWS Accounts are used by Teem Ops for the purposes of secure, 3rd party access for support, provisioning and operations management.

|  |  |  |
| --- | --- | --- |
| **Name** | **Account ID** | **Purpose** |
| Teem Ops Launch |  | IAM Authentication for cross account provisioning of apps, servers and databases. |
| Teem Ops Support |  | Teem Ops support and operations functions including maintenance, troubleshooting and VPN. |
| Teem Ops Billing | NA | Parent Billing Account for all “Managed/Billing” Customers only. |

### DNS

Public Route53 hosted zones will be in the Root AWS account.

Private Hosted zones will be in the Ops AWS Account

The Zones required are as follows:

|  |  |  |
| --- | --- | --- |
| **TLD** | **Used for** | **Public/Private** |
| <customer>.com | API endpoints  Public endpoints | Public (Root AWS Account) |
| <customer>.internal | Private DNS entries | Private (Ops AWS Account) |

### IAM Roles and Users

IAM Roles and users will be setup to allow access via cross account IAM / Assume Role.

***Roles***

These roles will be setup in the Dev/Test, Prod and Ops AWS Accounts.

* OrganizationAccountAccessRole: Default role
* CloudOpsRole: Used by cloud engineers for automation only. – existing cloud formation template provided by Teem Cloud Services
* TeemOpsRole: Used only by Teem Ops App – existing cloud formation template provided by Teem Ops
* ReadOnlyOpsRole: Used by Cyberfense and Teem for only

Teem Ops Role will require following rules.

* STS session token identifier must exist. (reduces risk of Account Takeover by compromised root account Teem Ops Users credentials).
* Only allow access from Trusted Teem Ops Launch account

***Groups***

The following group will be setup in root:

* CloudOps

This group will have only “STSAssumeRolePolicy” so they can access sub accounts via IAM Cross Account Role access.

***Users***

For each team member involved in the migration they will be setup as a user in the Root/IAM Account and added to the CloudOps group.

They will then have access to sub accounts which they can access by assuming the above “CloudOpsRole”.

MFA is to be enforced for all users.

Password rotation is for 90 days standard. Exceptions granted if required.

### KMS Keys

(For Enterprise Support customers a separate KMS AWS Account will be setup for key management).

KMS keys are setup to provide encryption of EBS/Root volumes and any other service, RDS Snapshots for example that can be encrypted at rest.

### EC2 Resources

These resources will need to be created prior to migration.

* EC2 Keypairs created – stored and managed by Secrets management tooling (in Teem Ops).

# Approach

Ansible will be used to automate the new infrastructure in the AWS accounts.

Based on the review, the preference for the Migration is to use these Ansible scripts so that the customer can also spin up additional AWS environments in separate accounts for dev or test in the future.

**Manual steps**

In addition to using Ansible some manual steps are required which are not part of the Ansible code.

This includes:

* OS/App Configuration for any VPN tooling
* VPC Connectivity to other VPCs or VPNs
* EC2 key pair management
* Any additional infrastructure that is not part of the Ansible playbooks.

## VPCs

The VPCs will be set up as part of Ansible. These are outlined as follows:

|  |  |  |
| --- | --- | --- |
| **VPC Name** | **Description** | **CIDR** |
| Ops (Ops Account) | Used for Monitoring, Bastion, VPN servers. | 10.X.0.0/16 |
| Prod (Prod Account) | Used for prod servers, RDS/Data, S3 Buckets, ELBS | 10.X.0.0/16 |
| Test (Dev Account) | Used for Test servers, RDS/Data, S3 Buckets, ELBS | 10.X.0.0/16 |
| Dev (Dev Account) | Used for Dev servers, RDS/Data, S3 Buckets, ELBS | 10.X.0.0/16 |

**Route53 Private Hosted Zone Configuration**

The Ops VPC requires the following to be configured as part of the build:

* enableDnsHostnames
* enableDnsSupport

Configured via the API or in Console:



# Ops Servers

|  |  |  |
| --- | --- | --- |
| **Server** | **Purpose** | **Comments** |
| OpenVPN | Connectivity from customer laptops/desktops | N/A |
| Bastion | Bastion host | N/A |

# Application

Document all applications here.

The application is made up of a…

## App Servers

The following App Servers will be configured and setup as part of the migration.

|  |  |  |
| --- | --- | --- |
| **Server** | **Purpose** | **Comments** |
| <Technology> | Run application | N/A |

## Code Repositories

There are a number of code repositories.

|  |  |
| --- | --- |
| **Repo** | **Purpose** |
| Customer REPO LINK | Core application code |

## Containers

|  |  |  |
| --- | --- | --- |
| Container Name | Purpose | Link |
| NA |  |  |

## Build and Deployment Process

The build process will use native AWS tooling for its underlying build tool and will require a mechanism for deployment.

The Build and Deployment process is made up of the following:

|  |  |
| --- | --- |
| **Component** | **Used for** |
| **AWS Code Build** | AWS Code build is used to build the artefacts. This is done using the above container and stores them in S3. |
| **Code Pipeline** | Code Pipeline takes the above artefacts from S3 and deploys them to dev environment. |
| **Prod Manual Process** | Currently the Production Deployment is a manual build, but with a view to automate based on “master” GIT branching strategy. |