**ProjectNAME**

<jeremy\_canale@Company.com>

**Effective Date: 04-04-2018**

**DOCUMENT APPROVAL**

**Meaning of Signatures**:

**“Approvers:”** Indicates completion of the document review and concurrence with the document content based on the individual team role and area of expertise. In addition, it serves as authorization to execute or close on execution as defined in the documentation.

|  |  |
| --- | --- |
| Approved By: |  |
| **Approved By:** |  |
| **Approved By:** |  |

CONTENTS

[1 INTRODUCTION 5](#_Toc508359791)

[1.1 OVERVIEW 5](#_Toc508359792)

[1.2 SCOPE 5](#_Toc508359793)

[2 APPLICATIONS & SYSTEMS 5](#_Toc508359794)

[2.1 OVERVIEW 5](#_Toc508359795)

[2.2 APPLICATION DIAGRAMS 5](#_Toc508359796)

[2.2.1 DEVELOPMENT ENVIRONMENT DESIGN 6](#_Toc508359797)

[2.2.2 TEST ENVIRONMENT DESIGN 7](#_Toc508359798)

[2.2.3 PRODUCTION ENVIRONMENT DESIGN 8](#_Toc508359799)

[2.3 SECURITY REQUIREMENTS 9](#_Toc508359800)

[2.3.1 APPLICATION NETWORKING TRAFFIC 9](#_Toc508359801)

[2.3.2 DATABASE TRAFFIC 9](#_Toc508359802)

[2.3.3 PIPELINE AND APPLICATION AUTOMATION 9](#_Toc508359803)

[2.3.4 HIGH AVAILABILITY 9](#_Toc508359804)

[2.3.5 BACKUP STRATEGY 9](#_Toc508359805)

[2.4 AWS CONSTRUCTS 9](#_Toc508359806)

[2.4.1 EC2 10](#_Toc508359807)

[2.4.2 TAGGING SPECIFICATION 10](#_Toc508359808)

[2.4.3 EBS 11](#_Toc508359809)

[2.4.4 KMS 12](#_Toc508359810)

[2.4.5 S3 13](#_Toc508359811)

[2.4.6 ELB 13](#_Toc508359812)

[2.5 WORK IN PROGESS 13](#_Toc508359813)

[3 CLOUDFORMATION STACKS 14](#_Toc508359814)

[4 AWS IAM POLICIES 15](#_Toc508359815)

[5 SECURITY GROUPS 16](#_Toc508359816)

[5.1 SUMMARY 16](#_Toc508359817)

[5.2 SECURITY GROUP LAYERS 16](#_Toc508359818)

[LAYER LIST 16](#_Toc508359819)

[5.3 SECURITY GROUP LAYER RULES 16](#_Toc508359820)

[OVERVIEW 16](#_Toc508359821)

[5.4 SECURITY GROUP NAMING 16](#_Toc508359822)

[EXAMPLES 16](#_Toc508359823)

[5.5 SECURITY GROUP APPROACH 17](#_Toc508359824)

[5.6 PROJECTNAME SECURITY GROUP DIAGRAM 18](#_Toc508359825)

[6 AWS Enterprise INFRASTRUCTURE 19](#_Toc508359826)

[6.1 ACCOUNTS 19](#_Toc508359827)

[6.1.1 CHART OF ACCOUNTS 19](#_Toc508359828)

[6.2 REGIONS 19](#_Toc508359829)

[6.2.1 OVERVIEW 19](#_Toc508359830)

[6.2.2 REGION LIST 19](#_Toc508359831)

[6.3 VIRTUAL PRIVATE CLOUD (VPC) 19](#_Toc508359832)

[6.3.1 OVERVIEW 19](#_Toc508359833)

[6.3.2 VPC LIST 20](#_Toc508359834)

[6.3.3 INTRA-VPC COMMUNICATION 20](#_Toc508359835)

[6.3.4 CLOUD INGRESS/EGRESS TO PREMISES 20](#_Toc508359836)

[6.3.5 CLOUD INGRESS/EGRESS TO INTERNET 20](#_Toc508359837)

[7 APPENDIX A: SOFTWARE INVENTORY 21](#_Toc508359838)

[7.1 WEB/APPLICATION SERVERS 21](#_Toc508359839)

[7.2 DATABASE SERVERS 21](#_Toc508359840)

# INTRODUCTION

This document outlines the specifications for the ProjectNAME application as it will be deployed into the Company AWS accounts as part of the Waterloo project that deploys the ProjectNAME application.

## OVERVIEW

This document, at a high-level, details the architecture of the ProjectNAME application in order to clarify the Amazon Web Services (AWS) constructs used and how they are instantiated.

## SCOPE

This document limits itself to the deployment plan for the ProjectNAME application as it relates to the AWS constructs and is not a comprehensive analysis of the application. Application details are discussed as to how they relate to the deployment as communicated to the Waterloo team.

# APPLICATIONS & SYSTEMS

## OVERVIEW

The focus of the migration is on moving the on-premise ProjectNAME application into AWS eu-central-1 Frankfurt across three environments:

* Development
* Test/QA
* Production

## APPLICATION DIAGRAMS

The following diagrams illustrate the conceptual elements of the application stacks as they exist inside of AWS

### 

### DEVELOPMENT ENVIRONMENT DESIGN

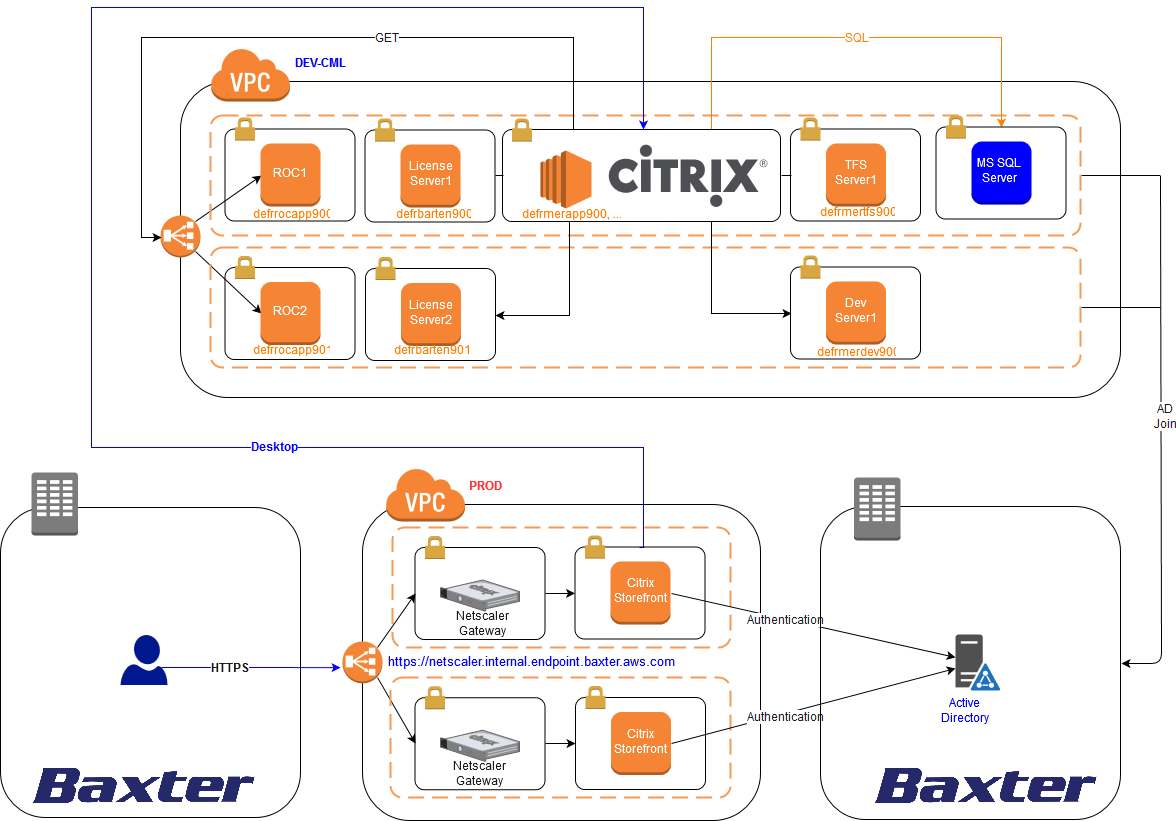


Figure 1 - DEVELOPMENT ENVIRONMENT DESIGN

## SECURITY REQUIREMENTS

### 2.3.1 APPLICATION NETWORKING TRAFFIC

Company requires encryption in transit for all AWS workloads.

The Company ProjectNAME team has confirmed that for data in transit, traditional SSL is supported with ROC ProjectNAME ressources but only the ELB will require an SSL Certificate.

The connection will be initialized through a Netscaler gateway endpoint from PROD environment which will allows users to connect to all Citrix nodes instances (DEV,TEST,PROD) after been authenticated with their own Active Directory credentials.

### 2.3.2 DATABASE TRAFFIC

1x MS SQL database for DEV environment.

2x MS SQL databases (HA) for TEST & PROD environment.

### 2.3.3 PIPELINE AND APPLICATION AUTOMATION

Certain prerequisites are installed and configured via the CloudFormation stack.

No pipeline currently exists to perform the deployment, and as such the ProjectNAME application will need to be revisited after the Enterprise DevOps Pipeline project begins.

### 2.3.4 HIGH AVAILABILITY

High availability for the ProjectNAME application is facilitated by using multiple web/application worker instances spread across multiple AWS availability zones (AZ). User traffic transverses an ELB in order to allow a standard endpoint for users to connect regardless of the back-end servers.

Citrix nodes group will be also used across 2 AWS AZ.

In the case of a failure of a node, that node shall be re-instated from either the snapshot or replaced by running the CloudFormation and performing the manual steps necessary to configure the application.

### 2.3.5 BACKUP STRATEGY

Backups for the web workers will take the form of snapshots.

The snapshots shall occur daily and retained for keying off a tag and lambda function implemented by Onica Managed Services (MSP). The backups will be retained for 45 days for the Production environment.

## AWS CONSTRUCTS

The following AWS constructs are utilized or have been specifically noted as in scope in relation to the ProjectNAME application stack and shall be deployed via Cloud Formation templates. Cloud Formation templates shall be stored in a BitBucket ProjectNAME folder.

### 2.4.1 EC2

All application elements shall be run on specific EC2 instances. These EC2 instances shall be created from base Company golden images.

A mix of Windows 2016 and Citrix AMI will be provided to complete the ProjectNAME project.

All instances are Microsoft Windows Servers joined to the Company AWS domain via an automated process. As seen in the diagrams presented in this document, ProjectNAME is a fairly simple client/server two tier application with the following roles:

* .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Environment** | **Count** | **Company AMI ID (eu-central-1)** | **Minimum Specification** |
| Web/Application Server | Development | 1 | ami-f521aa9a + Citrix (Pending)  ami-f521aa9a + Citrix (Pending)  ami-f521aa9a + Citrix (Pending) | Company Windows 2016  Citrix (Pending) |
| Test | 1 |
| Production | 1 |
| Database Server  (JDE Turkey) | Development | 1 | TBD by DBA Team  TBD by DBA Team  TBD by DBA Team | MS SQL |
| Test | 1 |
| Production | 1 |

Auto Scaling has been activated and provides a multi-AZ ProjectNAME app cluster.

### 2.4.2 TAGGING SPECIFICATION

All EC2 instances and EBS volumes shall be tagged as per the instruction issued by Company in the tagging enforcement documentation. The tags are currently defined as in table below:

|  |  |
| --- | --- |
| **Keys** | **Values** |
| Name | [server hostnames] |
| Env | Dev, Test, Prod |
| Appname | ProjectNAME |
| Appid | Pending |
| Owner | andrew\_macnaughton\_jones@Company.com |
| CostCenter | 815960632 |

## 

### 2.4.3 EBS

All EC2 instances shall be EBS backed with standard SSD volumes. Both root and data volumes shall be encrypted using a KMS key generated specifically for the ProjectNAME Application.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Drive** | **Purpose** | **Drive Type** | **Drive Size (GB)** |
| Roc Server 1 & 2 | C:\ | Root | General Purpose SSD (GP2) | 100 |
| D:\ | Data | General Purpose SSD (GP2) | 100 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Drive** | **Purpose** | **Drive Type** | **Drive Size (GB)** |
| ProjectNAME Server 1 | C:\ | Root | General Purpose SSD (GP2) | 100 |
| D:\ | Data | General Purpose SSD (GP2) | 50 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Drive** | **Purpose** | **Drive Type** | **Drive Size (GB)** |
| TFS Server | C:\ | Root | General Purpose SSD (GP2) | 100 |
| D:\ | Data | General Purpose SSD (GP2) | 200 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Drive** | **Purpose** | **Drive Type** | **Drive Size (GB)** |
| Dev Server 1 | C:\ | Root | General Purpose SSD (GP2) | 100 |
| D:\ | Data | General Purpose SSD (GP2) | 200 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Drive** | **Purpose** | **Drive Type** | **Drive Size (GB)** |
| License Server 1 & 2 | C:\ | Root | General Purpose SSD (GP2) | 100 |
| D:\ | Data | General Purpose SSD (GP2) | 50 |

### 2.4.4 KMS

Company shall be generating a specific KMS key per application/region/account. The PROJECTNAME key shall be used to encrypt the EBS Root and Data volumes. This key is created in a specific CloudFormation script, which is executed by security personnel creating the key, an admin key IAM user policy/role, and a user key IAM policy/role.

As per Company standard, key rotation has been set at one year.

|  |  |  |
| --- | --- | --- |
| **Environment** | **KMS Key** | **Role** |
| Dev | bax-dev-ProjectNAME-encryptkey | **Dev Admin Role**  baxaws-dev-security-admin-role |
| **ProjectNAME Admin Role**  baxaws-dev-ProjectNAME-admin-role  **ProjectNAME Support Role**  baxaws-dev-ProjectNAME-support-role  **ProjectNAME Viewer Role**  baxaws-dev-ProjectNAME-viewer-role  **ProjectNAME Instance Role**  baxaws-dev-ProjectNAME-labelarchiveserver-ec2-role |
| Test | bax-test-ProjectNAME-encryptkey | **Test Admin Role**  baxaws-test-security-admin-role |
| **ProjectNAME Admin Role**  baxaws-test-ProjectNAME-admin-role  **ProjectNAME Support Role**  baxaws-test-ProjectNAME-support-role  **ProjectNAME Viewer Role**  baxaws-test-ProjectNAME-viewer-role  **ProjectNAME Instance Role**  baxaws-test-ProjectNAME-labelarchiveserver-ec2-role |
| Prod | bax-prod-ProjectNAME-encryptkey | **Prod Admin Role**  baxaws-prod-security-admin-role |
| **ProjectNAME Admin Role**  baxaws-prod-ProjectNAME-admin-role  **ProjectNAME Support Role**  baxaws-prod-ProjectNAME-support-role  **ProjectNAME Viewer Role**  baxaws-prod-ProjectNAME-viewer-role  **ProjectNAME Instance Role**  baxaws-prod-ProjectNAME-labelarchiveserver-ec2-role |

### 2.4.5 S3

S3 shall be used in the following two ways:

* Snapshots
  + Instance level snapshots shall be stored on S3
  + The ProjectNAME /Base/ packed AMI has been created using an S3 bucket in DEV environment to download the WAS middleware installation files used to setup ProjectNAME.

### 2.4.6 ELB

DEV, TEST & PROD will use a classic load balancer for the ROC part of ProjectNAME.

These ELBs shall be used to abstract the servers from the user to provide high availability, as well as the ability to replace the instances without impacting the user’s endpoint.

## WORK IN PROGESS

* Citrix Architecture

This information will be implemented and qualified prior to deployment in production.

# CLOUDFORMATION STACKS

Per Company’s requests, the ProjectNAME Application stack has been broken up into the following CloudFormation Documents:

|  |  |  |
| --- | --- | --- |
| **Purpose** | **Environment** | **Bitbucket Location** |
| Application KMS Key | Dev | TBD by Security Team |
| Test/QA | TBD by Security Team |
| Production | TBD by Security Team |
| IAM Policies | Dev | Pending new architecture with Citrix |
| Test/QA | Pending new architecture with Citrix |
| Production | Pending new architecture with Citrix |
| Security Groups | Dev | Pending |
| Test/QA | Pending |
| Production | Pending |
| Application Stack | Dev | Pending |
| Test/QA | Pending |
| Production | Pending |

# AWS IAM POLICIES

As a result of the ProjectNAME IAM policy CloudFormation the following roles and policies are created or utilized.

|  |  |  |
| --- | --- | --- |
| **Environment** | **Role** | **Policies** |
| Dev | ProjectNAME Admin Role  baxaws-dev-ProjectNAME-admin-role | -bax-dev-cloudtrail-read-policy  -bax-dev-ProjectNAME-admin-policy  -bax-dev-kms-usage-policy  -bax-dev-deny-policy  -bax-dev-ProjectNAME-readonly-policy |
| ProjectNAME Support Role  baxaws-dev-ProjectNAME-support-role | -bax-dev-support-management-policy  -bax-dev-ProjectNAME-support-policy  -bax-dev-cloudtrail-read-policy  -bax-dev-deny-policy  -bax-dev-ProjectNAME-readonly-policy |
| Test | ProjectNAME Admin Role  baxaws-test-ProjectNAME-admin-role | -bax-test-cloudtrail-read-policy  -bax-test-deny-policy  -bax-test-kms-usage-policy  -bax-test-ProjectNAME-readonly-policy  -bax-test-ProjectNAME-admin-policy |
| ProjectNAME Support Role  baxaws-test-ProjectNAME-support-role | -bax-test-cloudtrail-read-policy  -bax-test-deny-policy  -bax-test-ProjectNAME-support-policy  -bax-test-support-management-policy  -bax-test-ProjectNAME-readonly-policy |
| Prod | ProjectNAME Admin Role  baxaws-dev-ProjectNAME-admin-role | -bax-prod-cloudtrail-read-policy  -bax-prod-ProjectNAME-admin-policy  -bax-prod-kms-usage-policy  -bax-prod-deny-policy  -bax-prod-ProjectNAME-readonly-policy |
| ProjectNAME Support Role  baxaws-dev-ProjectNAME-support-role | -bax-prod-cloudtrail-read-policy  -bax-prod-deny-policy  -bax-prod-ProjectNAME-support-policy  -bax-prod-support-management-policy  -bax-prod-ProjectNAME-readonly-policy |

# SECURITY GROUPS

## SUMMARY

Security Groups shall be used to facilitate network security at the instance level. Standard best practices will be observed for all communication to the ProjectNAME EC2 instances to other AWS resources.

## SECURITY GROUP LAYERS

**OVERVIEW**

Security Groups shall be organized into conceptual layers, relevant to how they apply and control traffic to the instance target.

### LAYER LIST

|  |  |
| --- | --- |
| **Layer** | **Definition** |
| User Application traffic | Traffic allowed to ELB from Users |
| Server Application traffic | Traffic allowed to application servers from ELB |
| Database traffic | Traffic allowed to Database servers from application servers |
| Standard Company Windows traffic | Standard Traffic allowed to windows servers |

## SECURITY GROUP LAYER RULES

### OVERVIEW

In addition to the layers, security groups will follow the following ruleset:

## SECURITY GROUP NAMING

The following naming scheme should be used for ProjectNAME Security Groups:

bax-<Environment>-<application>--role-sg

### EXAMPLES

Bax-dev-ProjectNAME-adcontroller-sg

## SECURITY GROUP APPROACH

Security Groups should be analyzed and added as servers come online. The following process should be followed for each new server:

1. Ask the following questions of each instance
   1. What core services does this system need? (Each can have multiple rules, but most systems get the same MGMT set)
   2. What Tier is the server in? (Should have only 1 rule)
   3. What Application is this server a part of. (Should have only a single rule)
      1. If Protected, does this system require any outbound internet access (1 rule to grant if yes)
   4. Does this server need to communicate with any servers in Shared Services (If so, add the respective tier rule to the instance)?
   5. Does this server need to communicate with any other servers in other tiers?
2. For each answer, see if a security group already exists that solves the need. If so, use it.
3. If the rule does not exist, create one following the rules and the naming convention.

This solution can be applied to all servers that come online, regardless of timeframe. Additionally, these rules should be audited via the API and each instance checked for compliance.

## PROJECTNAME SECURITY GROUP DIAGRAM

Pending (Waiting Ports Access)

Figure 3 - PROJECTNAME SECURITY GROUP DIAGRAM

# AWS Enterprise INFRASTRUCTURE

## ACCOUNTS

### 6.1.1 CHART OF ACCOUNTS

|  |  |  |
| --- | --- | --- |
| **Account** | **Account Name or Purpose** | **Account ID** |
| baxaws-dev-cml | Development | 148411111111 |
| baxaws-test-cml | Test/QA | 699022222222 |
| baxaws-prod-cml | Production | 687133333333 |

## REGIONS

### 6.2.1 OVERVIEW

A single AWS region will be utilized as ProjectNAME is by design a single instance implementation used by end users geographically dispersed across the Company Corporate WAN.

### 6.2.2 REGION LIST

|  |  |  |
| --- | --- | --- |
| **Name** | **Purpose** | **AWS Region** |
| PRIMARY | All instantiations for ProjectNAME | eu-central-1 (Frankfurt) |

## VIRTUAL PRIVATE CLOUD (VPC)

### 6.3.1 OVERVIEW

Each occurrence of the ProjectNAME environments is instantiated into specific VPCs expressly delegated by account and environment role.

### 6.3.2 VPC LIST

|  |  |  |
| --- | --- | --- |
| **VPC** | **Usage** | **VPC Name** |
| PROD | All systems related to production workloads, processing of production data, or servicing revenue-producing systems or customers | bax-prod-cml-eu-central-1-vpc |
| TEST/QA | Isolated QA systems used for verification of new software and support platforms to support software development | bax-test-cml-eu-central-1-vpc |
| DEV | Systems and workloads related to the ongoing development of technology platforms and software | bax-dev-cml-eu-central-1-vpc |

### 6.3.3 INTRA-VPC COMMUNICATION

Any needs for the ProjectNAME application stack to access other VPCs in the same region is handled via VPC peering. While not identified as a need, Company’s current strategy used to route to VPCs in other AWS regions is for the traffic to be routed through the Company network.

### 6.3.4 CLOUD INGRESS/EGRESS TO PREMISES

All Company VPCs inside eu-central-1 currently connect back to on premise resources via AWS VPN constructs.

### 6.3.5 CLOUD INGRESS/EGRESS TO INTERNET

N/A

# APPENDIX A: SOFTWARE INVENTORY

## WEB/APPLICATION SERVERS

* IBM Websphere 8.0

## DATABASE SERVERS

* Oracle

Change History

| Document Version | Change(s) and Reason for Change(s) | Effective Date |
| --- | --- | --- |
| 1 | Initial document Creation as per CRQxxxxxxxxxxxxxxxxx | See Stamp |