INNOMED MIGRATION WORKSHEET – AWS SPECS BUILT FROM REQUIREMENTS

## Which Services Will You Use?

## To move InnoMed into the AWS cloud, they will need to leverage the following AWS Cloud Services: AutoScaling, Cloudtrail, EC2, ELB, IAM, RDS, S3, VPC

## Users, Groups, and Roles

List the name of the group in the Group box, then list any applicable users under each group.

|  |  |  |  |
| --- | --- | --- | --- |
| **Group: SysAdmin** | **Group: DBAdmin** | **Group: Monitoring** | **Role: EC2toS3** |
| sysadmin1 | dbadmin1 | monitoruser1 | web-tier service |
| Sysadmin2 | dbadmin2 | monitoruser2 |  |
|  |  | monitoruser3 |  |
|  |  | monitoruser4 |  |

|  |  |  |
| --- | --- | --- |
| **Group/Role#** | **Group/Role Name** | **Permissions** |
| **Group** | sysadmin | AdministratorAccess |
| **Group** | dbadmin | AmazonRDSFullAccess |
| **Group** | monitoring | AmazonEC2ReadOnlyAccess,  AmazonS3ReadOnlyAccess,  AmazonRDSReadOnlyAccess |
| **Role** | EC2toS3 | S3:Get\*, S3:List\*, S3:Put\* |

## Password Policy

|  |  |
| --- | --- |
| **Requirement** | **Solution** |
| **Should be at least 8 characters and**  **have 1 uppercase, 1 lowercase, 1**  **special character, and a number.** | Example: S1l3ntH1L! |
| **Change passwords every 90 days and**  **ensure that the previous three**  **passwords can’t be re-used.** | Utilize Amazon IAM services, In the *Account Settings* configure password policy. |
| **Administrator sign-in to the AWS**  **Management Console requires the**  **use of Virtual MFA.** | Implement a virtual MFA device. |
| **All administrators require**  **programmatic access** | Create access secret/key pairs for admin accounts. |

## VPC Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VPC** | **Region** | **Purpose** | **Subnets** | **AZs** | **CIDR Range** |
| **1** | Any region, must support RDS Multi-AZ w/ mirroring for SQL Server | Production | 8 | 2 | 10.0.0.0/16 |
| **2** | Same as VPC #1 (above) | Test & Dev | 8 | 2 | 10.0.0.0/16 |

## Production Subnet Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Subnet Name** | **VPC** | **Subnet Type (Public/Private)** | **AZ** | **Subnet Address** |
| Public1 | 1 | Public | a | 10.0.0.0/27 |
| Public2 | 1 | Public | b | 10.0.1.0/27 |
| WebPrivate1 | 1 | Private | a | 10.0.10.0/24 |
| WebPrivate2 | 1 | Private | b | 10.0.11.0/24 |
| AppPrivate1 | 1 | Private | a | 10.0.20.0/24 |
| AppPrivate2 | 1 | Private | b | 10.0.21.0/24 |
| DBPrivate1 | 1 | Private | a | 10.0.30.0/24 |
| DBPrivate2 | 1 | Private | b | 10.0.31.0/24 |

## Test/Dev Subnet Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Subnet Name** | **VPC** | **Subnet Type (Public/Private)** | **AZ** | **Subnet Address** |
| Public1 | 1 | Public | a | 10.0.0.0/27 |
| Public2 | 1 | Public | b | 10.0.1.0/27 |
| WebPrivate1 | 1 | Private | a | 10.0.10.0/24 |
| WebPrivate2 | 1 | Private | b | 10.0.11.0/24 |
| AppPrivate1 | 1 | Private | a | 10.0.20.0/24 |
| AppPrivate2 | 1 | Private | b | 10.0.21.0/24 |
| DBPrivate1 | 1 | Private | a | 10.0.30.0/24 |
| DBPrivate2 | 1 | Private | b | 10.0.31.0/24 |

## Instance Details

Describe the type, size, and justification for the instances you will use for each tier.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Tier** | **Tag** | **OS** | **Type** | **Size** | **Justification** | **# of instances** | **User data?** |
| **Web** | Key=Name  Value=web-tier | Windows Server 2016 Base | t2 | medium | Curently deployed 2 physical servers (2 cpus, 4gb memory) w/ MS Windows 2016 Base w/ IIS | 2 | yes |
| **App** | Key=Name  Value=app-tier | Windows Server 2016 Base | m4 | xlarge | Curently deployed 2 physical servers (4 cpus, 16gb memory) w/ MS Windows 2016 Base | 2 | yes |
| **DB** | Key=Name  Value=db-tier | RDS – SQL Server SE | db.m4 | 2xlarge | We want a Multi-Availabilty Zone deployment | N/a | N/a |

## Load Balancer and Instance Security Group Details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Load Balancer** | **Name** | **External/Internal** | **Subnets** | **SG Name** | **Rule** | **Source** |
| **Web Tier** | web-elb | external | Public01/Public02 | web-elb-sg | Allow Port 80 HTTP | All Traffic |
| **App Tier** | app-elb | internal | AppPrivate01/AppPrivate02 | app-elb-sg | Allow Port 8080 | web-tier-sg |

|  |  |  |  |
| --- | --- | --- | --- |
| **Instance Tier** | **SG Name** | **Rule** | **Source** |
| **Web Tier** | web-tier-sg | Allow port 80 | web-elb-sg |
| **App Tier** | app-tier-sg | Allow port 80 | app-elb-sg |
| **Database Tier** | db-tier-sg | Allow 1433 | app-tier-sg |

## Auto Scaling Launch Configuration

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tier** | **OS** | **Type** | **Size** | **Configuration Name** | **Role** | **Security Group** |
| **Web** | Windows Server 2016 Base | t2 | medium | WebTier | EC2toS3 | web-tier-sg |
| **App** | Windows Server 2016 Base | m4 | xlarge | AppTier | N/a | app-tier-sg |

## Auto Scaling Group

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Tier** | **Launch Configuration** | **Group Name** | **Group Size** | **VPC** | **Subnets** | **ELB** | **Tags** |
| **Web** | WebTier | WebTier | 2-4 | 1 | WebPrivate01, WebPrivate02 | web-elb | Key=Name  Value=web-tier |
| **App** | AppTier | AppTier | 2-4 | 1 | AppPrivate01, AppPrivate02 | app-elb | Key=Name  Value=app-tier |

## Auditing Questions

1. How do you configure an account to create an audit trail for all executed API calls?

AWS CloudTrail

1. Where do you save your logs?

AWS S3 Bucket

Joshua Lee [x@joshdlee.com](mailto:x@joshdlee.com) AWS-CSAA CCNA R&S