Datasource & Longview

Low Level Design

February 2022

|  |  |
| --- | --- |
| Application name | Datasource & Longview |
| Business purpose | Datasource - Quality Output server |
| Business criticality | Low |
| Service Owner | André Bieri |
| Cost code | 120036050 |
| Supported by | André Bieri |

In this document text in yellow color is to be considered as a placeholder (or sample data) and thus must be changed or removed as applicable.

In this document text in Grey color is to be considered as an explanation which information is expected in the relevant section and thus must be removed before the final document release.

**Important note**: For pure workload migrations of servers, there is no need to complete this document; a simple server request for a new server in Azure created via ITSM request will suffice. You’ll get a readily installed server with the operating system of your choice, but the application re-installation and data transfer remains your duty (e.g. local IT / the application owner).

We need to give an instruction what must be filled in in ITSM server request!

Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Changes / Approvals** | **Name** |
|  | 28/02 | Approved by security | Itay Peled |
|  |  |  |  |

Contents

[2 Application Overview 5](#_Toc81584748)

[2.1 Scope and Design Objectives 5](#_Toc81584749)

[2.2 General information 5](#_Toc81584750)

[3 Application Architecture Design 6](#_Toc81584751)

[3.1 High Level Design overview 6](#_Toc81584752)

[3.2 Low Level Design 7](#_Toc81584753)

[3.3 Azure infra components 8](#_Toc81584754)

[3.3.1 Compute services 9](#_Toc81584755)

[3.3.2 Storage Services and external fileshares 9](#_Toc81584756)

[3.3.3 Networking and Connectivity 10](#_Toc81584757)

[3.3.4 Service Interfaces List / FW Rules 10](#_Toc81584758)

[3.3.5 Azure Application Gateway / WAF / Azure FW 11](#_Toc81584759)

[3.3.6 Certificates 11](#_Toc81584760)

[3.3.7 Shared Infrastructure Sevices 12](#_Toc81584761)

[3.4 Requirements and Key Design Decisions 12](#_Toc81584762)

[4 Licensing, Assumptions and Dependencies 13](#_Toc81584763)

[4.1 Assumptions, Issues & Dependencies 13](#_Toc81584764)

[4.2 Service Life and Decommissioning 13](#_Toc81584765)

[4.3 Application Software Components 13](#_Toc81584766)

[4.4 Licenses 13](#_Toc81584767)

[5 Integration Architecture 14](#_Toc81584768)

[5.1 Interfaces List 14](#_Toc81584769)

[5.2 User connections 14](#_Toc81584770)

[5.3 Cloud to / from On-Prem Interfaces 14](#_Toc81584771)

[6 Security 15](#_Toc81584772)

[6.1 Security considerations 15](#_Toc81584773)

[6.2 Azure Asset Management (tags) 16](#_Toc81584774)

[7 Application migration planning 16](#_Toc81584775)

[7.1 On-premise application design 17](#_Toc81584776)

[7.1.1 Migration schedule / timeline 17](#_Toc81584777)

[7.1.2 On-premise servers used / required by the application 17](#_Toc81584778)

[7.1.3 Components linked to the application 17](#_Toc81584779)

[7.2 Lift & shift migration 18](#_Toc81584780)

[7.3 Database (DMS) migration 18](#_Toc81584781)

[7.4 Share Migration 18](#_Toc81584782)

[7.5 Internal application dependencies 18](#_Toc81584783)

[7.6 External application dependencies or application interfaces 19](#_Toc81584784)

[7.7 DNS names / Published websites / Third party connections 19](#_Toc81584785)

[7.8 DMZ / Firewall rules 19](#_Toc81584786)

[7.9 Performance / response times 19](#_Toc81584787)

[8 Configuration of target situation 20](#_Toc81584788)

[8.1 Database (DMS) migration Target server/database specification 20](#_Toc81584789)

[8.2 Share Migration 20](#_Toc81584790)

[9 Migration 21](#_Toc81584791)

[9.1 Move Group 21](#_Toc81584792)

[9.2 Target Architecture 22](#_Toc81584793)

[9.3 Dependency Map 23](#_Toc81584794)

[9.3.1 PROD Environment 24](#_Toc81584795)

[9.4 Pre-migration activities 24](#_Toc81584796)

[9.5 Test cases 25](#_Toc81584797)

[9.6 Post-migration activities 25](#_Toc81584798)

[9.7 Continue or fallback decision 26](#_Toc81584799)

[9.8 Reconfiguration after testing sign off 26](#_Toc81584800)

# Application Overview

## Scope and Design Objectives

This document details the Low-Level Design (LLD) for Datasource & Longview and the migration steps necessary to move the application from its current location to Azure.

The following list provides the reader with the scope for this project and service.

* Assessment of Datasource & Longview for Migration to Azure

## General information

Datasource & Longview is used for Datasource Quality Output server is used by users across Schindler

|  |  |
| --- | --- |
| Attribute | Description |
| Service Name | Datasource & Longview |
| Service Description | DataSOURCE - Quality Output server |
| Number of users and their location | Admin users and developers mainly; MAN/SIS Ebikon, Switzerland |
| Data classification (CIA) | Confidentiality – Confidential  Integrity – Normal  Availability – Important |
| Cost Center | 120011120 |
| KG | SHH |
| Service Owner | André Bieri |
| Technical Contact | André Bieri |

# Application Architecture Design

## High Level Design overview

Place Holder

* This is an application with prod & non-prod environment.
* The application is accessed from Internal Network.
* The Servers are in GDC Datacentres.

|  |  |  |
| --- | --- | --- |
| **Environment** | **PROD** | **NON-PROD** |
| WEB | 2 | 2 |
| APP |  |  |
| DB | 0 | 0 |
| **Grand Total** | **2** | **2** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Azure IP** | **Function** | **Environment** | **ITSM-Function** |
| MANWSR0028 | 10.10.158.12 | 10.37.10.83 | NON-PROD | FRONTEND WEB | Datasource Web Server Qual |
| SHHWSR1869 | 10.10.60.103 | 10.37.10.85 | NON-PROD | FRONTEND WEB | Longview Web Server Qual |
| SHHWSR1911 | 10.10.60.162 | 10.38.10.121 | PROD | FRONTEND WEB | Datasource Web Server Prod |
| SHHWSR1868 | 10.10.60.102 | 10.38.10.118 | PROD | FRONTEND WEB | Longview Web Server Prod |

Below is the list of Servers within the Datasource & Longview application.

**Red Color** servers are removed based on the list shared by Application owners.  
**Green Color** servers are New Servers added to the list based on the list shared by Application Owners.

## Low Level Design

This application is used for DataSOURCE Quality Output server

* DataSOURCE Quality Output server.
* The application is accessed from Internal Network.

**Production Environment**

**No Design document provided by AO**

Place Holder

## Azure infra components

Provide Azure resources top level configuration settings here.

* Regions
* Subscriptions
* Resource Groups

|  |  |  |  |
| --- | --- | --- | --- |
| Description | PROD | NON-PROD | Notes |
| Subscription | s-sis-eu-prod-01 | s-sis-eu-nonprod-01 |  |
| Azure Regions | EU North | EU North |  |
| Resource Group | rg-shh-prod-datasrclongvw-01 | rg-shh-qual-datasrclongvw-01 |  |

### Compute services

List all virtual servers here

#### Virtual Servers

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Server Name | Data Centre | Operating System | RAM (GB) | CPU Cores | Disk Size |
| MANWSR0028 | GDC | Win Server2019 | 4 | 2 | 963 |
| SHHWSR1869 | GDC | Win Server2019 | 4 | 4 | 799 |
| SHHWSR1911 | GDC | Win Server2019 | 8 | 2 | 846 |
| SHHWSR1868 | GDC | Win Server2019 | 16 | 6 | 964 |

#### DB Servers (MS SQL on IaaS)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Server Name | Data Centre | Operating System | SQL Version | RAM (GB) | CPU Cores | Disk Size GB |
| NA |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

There are DB Servers in this application Stack, but It has shared DB Server SHHWSR0975.global.schindler.com (NON-PROD), SHHWSR0974.global.schindler.com (PROD).

The DB team proposed to move the DataSource & LongView DB instances of SHHWSR0975(Non-Prod) to Shared IaaS VM “SHHWSR2234”. Respectively for the PROD, from SHHWSR0974 to Prod Shared IaaS VM “SHHWSR2232”.

### Storage Services and external fileshares

List all Azure Storage services instances used and external storage provider like NAS/NFS/iSCSI shares, etc.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Purpose | Type / Tier | Path |
| NA | NA | NA | NA |

### Networking and Connectivity

List Azure network services and/or FW configuration settings like FW rules

#### Azure Network Componets

|  |  |  |  |
| --- | --- | --- | --- |
| Component Name | PROD | NON-PROD | Reference ID |
| VNet | EU-PROD | EU-NONPROD | NA |
| Subnet | FrontEnd-IaaS-Subnet\_1  10.38.10.0/23 | FrontEnd-IaaS-Subnet\_1  10.37.10.0/23 | NA |

### Service Interfaces List / FW Rules

Firewall Rule-

<https://schindlerglobal.sharepoint.com/:x:/r/sites/SISCloudAdoption/Shared%20Documents/03%20Project%20Execution/06%20-%20Migration/GDC/GDC-MIG/Wave4/014%20DataSource%20%26%20longview/LLD/firewall%20rules_datasource%20%26%20longview.xlsx?d=wa1d6b6089fdb4961b2a67ce69a5061f5&csf=1&web=1&e=Ri9bye>

### Azure Application Gateway / WAF / Azure FW

**QUAL**

|  |  |
| --- | --- |
| Attribute | Value |
| Azure App Gateway Name | agw-prod-network-shhnag0003 |
| Backend Server | 10.37.10.83 |
| Backend Ports | 443 |
| Azure App Gateway Public Endpoint | dsinput-dev.global.schindler.com |

|  |  |
| --- | --- |
| Attribute | Value |
| Azure App Gateway Name | agw-prod-network-shhnag0003 |
| Backend Server | 10.37.10.85 |
| Backend Ports | 443 |
| Azure App Gateway Public Endpoint | dev-ds2output.global.schindler.com |

**PROD**

|  |  |
| --- | --- |
| Attribute | Value |
| Azure App Gateway Name | agw-prod-network-shhnag0003 |
| Backend Server | 10.38.10.121 |
| Backend Ports | 443 |
| Azure App Gateway Public Endpoint | dsinput.global.schindler.com |

|  |  |
| --- | --- |
| Attribute | Value |
| Azure App Gateway Name | agw-prod-network-shhnag0003 |
| Backend Server | 10.38.10.118 |
| Backend Ports | 443 |
| Azure App Gateway Public Endpoint | ds2output.global.schindler.com |

**Internet**

|  |  |  |  |
| --- | --- | --- | --- |
| Servers | Internet Required | URL to be Whitelist | Remarks |
| NA | NA | NA | NA |

### Certificates

|  |  |  |
| --- | --- | --- |
| **Internal URL** | **Issued to** | **Issuer** |
| \*.global.schindler.com | Schindler-issuing-GA-G01-01 | Wild Card Certificate |
|  |  |  |

### Shared Infrastructure Sevices

List Azure shared infrastructure services like backup, logging, monitoring, alerting, etc.

|  |  |  |  |
| --- | --- | --- | --- |
| Service Component Name | Service | Description | Reference ID |
| Identity | Active Directory Service |  | NA |
| DNS | DNS Service |  | NA |
| Monitoring | Azure Monitoring |  | NA |
| Backups | Azure Backup |  | NA |
| SIEM | NA |  | NA |
| Networking | NA |  | NA |

### Hostfile Details

No host files

## Requirements and Key Design Decisions

List of architecture Key Design Decisions (KDC) with relevant requirements is provided below:

|  |  |  |  |
| --- | --- | --- | --- |
| Ref. | Key Design Decision Area | Key Design Decision | Justification |
| 1 | Resilience & DR | Azure Locally Redundant Storage (LRS) will be used. | Requirement comes from data availability classification – Very Critical |
| 2 | Resilience & DR | Servers will be placed in Availability zone & Backup will also be available | In Case of Datacentre level failure, the other zone will be available & region level failure will be handled by restoring from Backup |
| 3 | Security/CMDB | Solution will use Azure tags for digital asset management. | ON 0-08100 standard requirement. |
| 4 | Connectivity | Solution will be securely published via internal FW/AppGateway/WAF | Azure LZ network design decision for internal exposed services. |
| 5 | Connectivity | Encryption for data in transit – TLS v.1.2 | ON 0-08100 standard requirements for data in transit over public networks. |
| 6 | Hosting Location | Azure Storage Account will be created in North Europe | Solution is deployed in the location closest to dependent Services |
| 7 | Hosting Type | Azure IaaS will be used | Aligned with requirements. |
| 8 | Hosting Type | Azure PaaS services will be used where possible. | Business requirement, LZ design decision. |
| 9 | Monitoring | All solution components must be connected to Azure monitoring services. | ON 0-08100 standard requirement. LZ networking design decision. |
| 10 | Access management | RBAC controlled access for admins and service owners. | The design is using standard LBE Azure infrastructure and patterns only. |
| 12 | Security | FW/WAF intrusion prevention capabilities like AV/IDS/IPS must be enabled. | ON 0-08100 standard requirement. LZ networking design decision. |
| 13 | Security | Azure Storage Encryption will be used for data at rest encryption. | ON 0-08100 standard requirement. Solution security requirement. |

# Licensing, Assumptions and Dependencies

## Assumptions, Issues & Dependencies

The following table provides the reader with an understanding of the **architecture items** only. Note. Project implementation and build RAID items should be captured in the project RAID log.

|  |  |
| --- | --- |
| Category | Description |
| Assumptions | NA |
| Issues | NA |
| Dependencies | There are DB Servers in this application Stack, but It’s having shared DB Server SHHWSR0975.global.schindler.com(NON-PROD),SHHWSR0974.global.schindler.com(PROD).  The DB team proposed to move the DataSource & LongView DB instances of SHHWSR0975(Non-Prod) to Shared IaaS VM “SHHWSR2234”. Respectively for the PROD, from SHHWSR0974 to Prod Shared IaaS VM “SHHWSR2232”. |

## Service Life and Decommissioning

The following table provides the reader with an understanding of the solutions service life and any decommissioning required.

|  |  |
| --- | --- |
| Category | Description |
| Service Life | Service will be deployed on a permanent basis. Will be reviewed every 2 years. |
| Decommissioning | Decommission as per the standard Azure services lifecycle. |

## Application Software Components

The following table provides the reader with the major application software components and versions to be implemented as part of this solution.

|  |  |
| --- | --- |
| Software Component Name | Software Component Version |
| NA | NA |

## Licenses

The following table provides the reader with the licenses required for the infrastructure deployment.

|  |  |
| --- | --- |
| Software License | Subscription License Qty |
| Windows | Azure PAYG / BYOL |

# Integration Architecture

## Interfaces List

The following table provides the reader with a view of the technical integration for the deployment.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Source | Broker System | Target | Batch (B) / Transactional (T) | Protocol / Port |
| 1 | NA | NA | NA | NA | NA |

## User connections

The following table provides the reader with a view of the technical integration for the deployment.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Source | Broker System | Target | Batch (B) / Transactional (T) | Protocol / Port |
| 1 | NA |  | NA | NA | NA |

## Cloud to / from On-Prem Interfaces

The following table provides the reader with a view of the impact to the Schindler on-premises networks for the deployment if applicable.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Ref From 4.1 | Peak(s) or Schedule Time(s) and Days | Firewall Rule? | Max # Per Hour | Max Size | Average Per Hour | Average Size |
|  | NA | NA | NA | NA | NA | NA |

# Security

The following section provides the reader with a view of the security considerations considered for the design.

## Security considerations

|  |  |
| --- | --- |
| Category | Description |
| Physical Location Security Considerations | Service is hosted in Azure cloud. According to shared responsibility model Microsoft is responsible for provisioning physical security controls. |
| Data access & governance (Authorization) | * Users are authenticated by LDAP * New admin user access will be provided in scope of the standard Schindler service request |
| Directory Services & Authentication | * Service use Active Directory for Authentication |
| Privileged access accounts and service/API user accounts | NA |
| Server security, perimeter security & changes to Schindler firewalls required? | * Azure Firewall will be used * WAF and Azure App Gateway will be used at stage 2 to secure end-users’ connections. * Azure Storage private endpoints will be used to route traffic via internal FW/WAF for additional security layer. * Direct access to Azure Storage public endpoints is disabled. |
| Legal & Regulatory Compliance | No |
| Information Security Considerations (including safeguard of sensitive and personal data) | Data protection controls must comply with Schindler ON 0-08100 Security Baseline. |
| If there is a PaaS (not Schindler Azure/AWS PaaS) or SaaS provider SHHolved in this solution, does the service provider meet targets specified in the CIA classification | No |
| Backup platform, type of backup & scheduling for servers and data | |  | | --- | | GL 01.2 - VM Snapshot Backup Standard, long term | | GL 03.4 - SQL PROD Backup, three months | |
| Patching schedule, service hours and maintenance windows | Maintenance Windows –  Non-Business Hours |
| Data archiving, cleansing & purging (life cycle management) | Service owner is responsible for data lifecycle management. |
| Data migration | Azure Migrate will be leverage for VM Replication to target Data will be migrated manually by copying files |
| Data and system audit & monitoring | All events will be monitored using Azure Log Analytics service.  This includes.   * Data changes auditing. * System access auditing. * Security monitoring. |

## Azure Asset Management (tags)

Following tags must be assigned to azure resources created in scope of this service deployment:

|  |  |
| --- | --- |
| Key | Value |
| Cost Center | 120011120 |
| Infra structure service | DataSOURCE Quality Output server |
| KG | SHH |
| Service owner | André Bierir |
| Technical contact | André Bierir |
| Confidentiality | Internal Use Only |
| Integrity | Normal |
| Availability | Important |
| Userbase | Unknown |

|  |  |
| --- | --- |
| **RG** | **rg-shh-prod-datasrclongvw-01** |
| **applicationowner** | André Bierir |
| **costcenter** | 120011120 |
| **infrastructureservice** | DataSOURCE Quality Output server |
| **kg** | SHH |
| **serviceowner** | André Bierir |
| **technicalcontact** | André Bierir |
|  |  |

|  |  |
| --- | --- |
| **RG** | **rg-shh-qual-datasrclongvw-01** |
| **applicationowner** | André Bierir |
| **costcenter** | 120011120 |
| **infrastructureservice** | DataSOURCE Quality Output server |
| **kg** | SHH |
| **serviceowner** | André Bierir |
| **technicalcontact** | André Bierir |
|  |  |

# Application migration planning

In the first chapter the business application’s setup is assessed. This includes scoping, initial planning, source server definition and description, including dependencies.

## On-premise application design

**Production Environment**

Place Holder

**No diagram for prod environment**

### Migration schedule / timeline

|  |  |
| --- | --- |
| Assessment completion deadline | 8thth February 2022 |
| Planning and Design completion deadline | 27th February 2022 |
| Pre-Migration Activities completion deadline | TBD |
| Migration Execution completion deadline | TBD |
| Post Migration activities completion deadline | TBD |

### On-premises servers used / required by the application

|  |  |  |  |
| --- | --- | --- | --- |
| **Server name** | **Shared server (yes/no)** | **Migration method** | **Server function/role** |
| NA | NA | NA | NA |

### Components linked to the application

* Application is Linked to LDAP for authentication

## Lift & shift migration

**Source Server Specification**

Servers will be rehosted to Azure using

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Function** | **Environment** | **Migration Method** |
| MANWSR0028 | 10.10.158.12 | FRONTEND WEB | NON-PROD | Rehost |
| SHHWSR1869 | 10.10.60.103 | FRONTEND WEB | NON-PROD | Rehost |
| SHHWSR1911 | 10.10.60.162 | FRONTEND WEB | PROD | Rehost |
| SHHWSR1868 | 10.10.60.102 | FRONTEND WEB | PROD | Rehost |

## Database (DMS) migration

There are DB Servers in this application Stack, but It has shared DB Server SHHWSR0975.global.schindler.com(NON-PROD),SHHWSR0974.global.schindler.com(PROD).

The DB team proposed to move the Datasoure & Longview DB instances of SHHWSR0975(Non-Prod) to Shared IaaS VM “SHHWSR2234”. Respectively for the PROD, from SHHWSR0974 to Prod Shared IaaS VM “SHHWSR2232”.

## Share Migration

Copy the below table **for each server or disc storage** to be migrated in this migration!

|  |  |
| --- | --- |
| **Source server** | **Configuration** |
| Host name | NA |
| Source IP address | NA |
| Domain | NA |
| Server or storage size | NA |
| Server OS | NA |

## Internal application dependencies

List and describe all dependencies internal to the application. In case the business application consists of multiple servers this list must also include all dependencies between these servers (related to the same application).

|  |  |
| --- | --- |
| **Dependency** | **Detailed Description** |
| NA | NA |

## External application dependencies or application interfaces

List and describe all dependencies external to the application. This includes all cases where the business application provides an interface towards other systems.

|  |  |
| --- | --- |
| **Interface** | **Detailed Description** |
| NA | NA |

## DNS names / Published websites / Third party connections

Internal DNS name for QA is hostname except arisqdb which will remain same after migration & would need no changes to be performed for these names. For Prod Internal DNS Names need to be changed to reflect the New IP.

|  |  |
| --- | --- |
| **Internal DNS names published** | shhwsr1911.global.schindler.com  dsinput.global.schindler.com  manwsr0028.global.schindler.com  dsinput-dev.global.schindler.com  shhwsr1869.global.schindler.com  dev-ds2output.global.schindler.com shhwsr1868.global.schindler.com  ds2output.global.schindler.com |
| **External DNS names** | NA |
| **SMTP relay usage** | NA |

## DMZ / Firewall rules

In case one or multiple of your servers SHH involved in this migration are sitting in a DMZ or have websites published on them please indicate this information in below table.

|  |  |
| --- | --- |
| List of current firewall rules if server is in a DMZ or generally behind firewall(s) | NA |

## Performance / response times

In case the Business Application has hard requirements with regards to application performance and or response times and these are critical to the end user’s acceptance of the cloud migration project, these performance / response time measurements must be made **prior** to the migration of the application and properly documented such that a valid baseline is created for later comparison. Please do note that **NO** performance complaints will be accepted post-migration in case no baseline has been provided prior to migration.

<Please include here any response time / performance requirements and measurements you have made prior to the application migration>  
  
**# No Performance / Response time available with the Application Team**

# Configuration of target situation

For each server to be lift & shifted in this migration  
Please refer the [**link**](https://schindlerglobal.sharepoint.com/sites/SISCloudAdoption/Shared%20Documents/03%20Project%20Execution/06%20-%20Migration/GDC/GDC-MIG/Wave2/042%20Printserver/01%20Survey%20Template/ServerDetails.xlsx) for server details & detailed SHH entry for Source & Target information

## Database (DMS) migration Target server/database specification

There are DB Servers in this application Stack, but It has shared DB Server SHHWSR0975.global.schindler.com(NON-PROD),SHHWSR0974.global.schindler.com(PROD).

The DB team proposed to move the Datasoure & LongView DB instances of SHHWSR0975(Non-Prod) to Shared IaaS VM “SHHWSR2234”. Respectively for the PROD, from SHHWSR0974 to Prod Shared IaaS VM “SHHWSR2232”.

## Share Migration

Copy the table below **for each server or disc storage** to be migrated in this migration!

|  |  |
| --- | --- |
| **Source server** | **Configuration** |
| Host name | NA |
| Source IP address | NA |
| Domain | NA |
| Server or storage size | NA |
| Server OS | NA |

# Migration

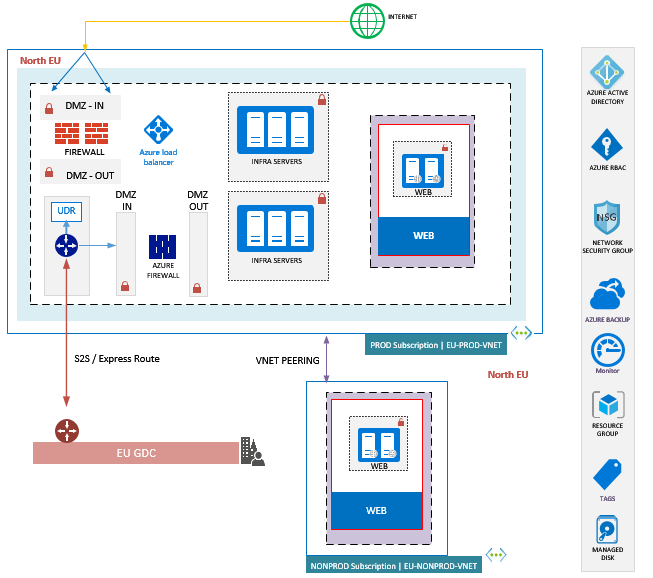
The third chapter describes the migration steps for the application server(s). This includes specific pre-migration activities, test case description, steps for conducting the actual migration and finally specific post migration activities.

## Move Group

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Function** | **Environment** | **App Stack** | **Move Group** | **Wave** |
| MANWSR0028 | 10.10.158.12 | FRONTEND WEB | NON-PROD | Datasource & Longview |  | wave 4 |
| SHHWSR1869 | 10.10.60.103 | FRONTEND WEB | NON-PROD | Datasource & Longview |  | Wave 4 |
| SHHWSR1911 | 10.10.60.162 | FRONTEND WEB | PROD | Datasource & Longview |  | Wave 4 |
| SHHWSR1868 | 10.10.60.102 | FRONTEND WEB | PROD | Datasource & Longview |  | Wave 4 |

## Target Architecture

* The Servers will be placed in Non-Prod and Prod Subscription based on the Environment.
* Based on the Tier the Servers will be placed into the respective Subnet.
* Shared services like monitoring, IDAM, backup will be leveraged from the existing shared infrastructure.
* 4 Web servers will be migrated to Non-Prod and Prod Subscription



## Dependency Map

Place Holder

### PROD Environment

No Design document provided by AO

Place Holder

## Pre-migration activities

Explain in detail all required pre-migration activities to be completed prior to the migration. If certain steps are time sensitive, please do indicate this!

|  |  |
| --- | --- |
| **Application stops** | Manual – Service Stop by the Application Owners |
| **Application start** | Manual – Service Start by the Application Owners |
| **Block user traffic** | NA |
| **Boot order** | DB , Web |

## Test cases

Detailed description of the test cases that need to be completed after the failover to Azure but during the migration slot. Please note that the test case execution must be done by local IT and or the application responsible.   
  
# Application Team must fill in the detail’s prior migration

|  |  |
| --- | --- |
| **Test case name** | **Detailed test case description** |
|  |  |
|  |  |
|  |  |

Overall test coordination lies with the application owner, the migration Team will NOT organize / orchestrate / conduct testing during the outage window!

|  |  |
| --- | --- |
| Overall test effort estimation during outage |  |
| Name of test users and their function | André Bieri |
| Test acceptances sign off to be given by | André Bieri |
| Planned test case execution window |  |

## Post-migration activities

Below listed activities shall be carried out once the migration is completed

|  |  |
| --- | --- |
| **DNS** | DNS listed in [Section 7.7](#_DNS_names_/) needs to be changed to point to New IP in Azure |
| **Load Balancer** | NA |
| **DB Configuration** | Applications needs to be configured to connect to New IP of the DB Server if it is configured with an IP Address |
| **Firewall** | Firewall changes to be performed as per [Section 3.4](#_Service_Interfaces_List) |
| **Monitoring** | Configure Zabbix on Cloud for the New Instance IP as per [Section 6.1](#_Security_considerations) |
| **Backup** | Configure Backup as per [Section 6.1](#_Security_considerations) |

## Continue or fallback decision

After test case execution, the final go / no-go decision must be taken. Please include a detailed description of the specific conditions in which a rollback / fallback will be conducted.

# To be filled in post migration

|  |  |
| --- | --- |
| Decision taker for approved fallback to on premise |  |
| Fall back to on premise servers |  |
| Individuals to be informed of fallback decisions |  |

## Reconfiguration after testing sign off

Please list in detail all steps that need to be executed after the test cases have been executed and sign off for has been provided.

# To be filled in post migration