Esight(Network Management)

Low Level Design

december 2021

|  |  |
| --- | --- |
| Application name | Esight(Network Management) |
| Business purpose | Huawei wireless management – Used for managing the wireless infrastructure. |
| Business criticality | Low |
| Service Owner | Thangavel Mudaliar |
| Cost code | 120031500 |
| Supported by | Network Team  ([andrew.ballard@schindler.com](mailto:andrew.ballard@schindler.com),n[josef.prediger@schindler.com](mailto:josef.prediger@schindler.com))  DB -- (roland.faessler@schindler.com) |

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** |
|  |  |  |  |
|  |  |  |  |

Contents

[2 Application Overview 5](#_Toc81592648)

[2.1 Scope and Design Objectives 5](#_Toc81592649)

[2.2 General information 5](#_Toc81592650)

[3 Application Architecture Design 6](#_Toc81592651)

[3.1 High Level Design overview 6](#_Toc81592652)

[3.2 Low Level Design 7](#_Toc81592653)

[3.3 Azure infra components 8](#_Toc81592654)

[3.3.1 Compute services 9](#_Toc81592655)

[3.3.2 Storage Services and external fileshares 9](#_Toc81592656)

[3.3.3 Networking and Connectivity 9](#_Toc81592657)

[Internet 11](#_Toc81592658)

[3.3.4 Azure Application Gateway / WAF / Azure FW 11](#_Toc81592659)

[3.3.5 Shared Infrastructure Sevices 11](#_Toc81592660)

[3.3.6 Certificates 11](#_Toc81592661)

[3.4 Requirements and Key Design Decisions 12](#_Toc81592662)

[4 Licensing, Assumptions and Dependencies 13](#_Toc81592663)

[4.1 Assumptions, Issues & Dependencies 13](#_Toc81592664)

[4.2 Service Life and Decommissioning 13](#_Toc81592665)

[4.3 Application Software Components 13](#_Toc81592666)

[4.4 Licenses 13](#_Toc81592667)

[5 Integration Architecture 14](#_Toc81592668)

[5.1 Interfaces List 14](#_Toc81592669)

[5.2 User connections 14](#_Toc81592670)

[5.3 Cloud to / from On-Prem Interfaces 14](#_Toc81592671)

[6 Security 15](#_Toc81592672)

[6.1 Security considerations 15](#_Toc81592673)

[6.2 Azure Asset Management (tags) 16](#_Toc81592674)

[7 Application migration planning 17](#_Toc81592675)

[7.1 On-premise application design 17](#_Toc81592676)

[7.1.1 Migration schedule / timeline 18](#_Toc81592677)

[7.1.2 On-premise servers used / required by the application 18](#_Toc81592678)

[7.1.3 Components linked to the application 18](#_Toc81592679)

[7.2 Lift & shift (ASR) migration 18](#_Toc81592680)

[7.3 Database (DMS) migration 18](#_Toc81592681)

[7.4 Share Migration 19](#_Toc81592682)

[7.5 Internal application dependencies 19](#_Toc81592683)

[7.6 External application dependencies or application interfaces 19](#_Toc81592684)

[7.7 DNS names / Published websites / Third party connections 19](#_Toc81592685)

[7.8 DMZ / Firewall rules 21](#_Toc81592686)

[7.9 Performance / response times 21](#_Toc81592687)

[8 Configuration of target situation 22](#_Toc81592688)

[8.1 Database (DMS) migration Target server/database specification 22](#_Toc81592689)

[8.2 Share Migration 22](#_Toc81592690)

[9 Migration 23](#_Toc81592691)

[9.1 Move Group 23](#_Toc81592692)

[9.2 Target Architecture 23](#_Toc81592693)

[9.3 Dependency Map 24](#_Toc81592694)

[9.3.1 PROD Environment 24](#_Toc81592695)

[9.4 Pre-migration activities 25](#_Toc81592696)

[9.5 Test cases 26](#_Toc81592697)

[9.6 Post-migration activities 26](#_Toc81592698)

[9.7 Continue or fallback decision 27](#_Toc81592699)

[9.8 Reconfiguration after testing sign off 27](#_Toc81592700)

# Application Overview

## Scope and Design Objectives

This document details the Low-Level Design (LLD) for Esight (Network Management) 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 Esight (Network Management) Application for Cloud Compatibility

## General information

Esight(Network Management) is used to Used for managing the wireless infrastructure.

|  |  |
| --- | --- |
| Attribute | Description |
| Service Name | Esight(Network Management) |
| Service Description | Huawei wireless management - Used for managing the wireless infrastructure. |
| Number of users and their location | 15 |
| Data classification (CIA) | Confidentiality – Internal use only  Integrity – Normal  Availability – Important |
| Cost Centre | 120031500 |
| KG | SHH |
| Service Owner | Thangavel Mudaliar |
| Technical Contact | Network Team  ([andrew.ballard@schindler.com](mailto:andrew.ballard@schindler.com),n[josef.prediger@schindler.com](mailto:josef.prediger@schindler.com), Thangavel)  DB -- (roland.faessler@schindler.com) |

# Application Architecture Design

## High Level Design overview

Esight (Network Management) is Used for managing the wireless infrastructure.

Place Holder

Below bifurcation of servers into respective environments and tiers

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **PROD** | **QA** | **Total** |
| Web | 1 | 0 | 1 |
| **Grand Total** | **1** | **0** | **1** |

This Application has DB which is hosted on same server SHHWSR1492.

Below is the list of Servers within the Esight(Network Management) Application Stack.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Server Name | IP address | Azure IP | Function | Environment | ITSM-Function |
| SHHWSR1491 | 10.10.100.200 | 10.38.14.114 | INFRA | PROD | Network Management |

## Low Level Design

* This is a Single-tier application with Prod environment.
* The application is accessed from Internal Network.

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 | NA |  |
| Azure Regions | EU North | NA |  |
| Resource Group | rg-shh-prod-esightnwmgnt-01 | NA |  |

### Compute services

List all virtual servers here

#### Virtual Servers

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server Name** | **Data Centre** | **Operating System** | RAM (GB) | **CPU Cores** | **Disk Size (GB)** |
| SHHWSR1492 | SHH | WinServer2012 | 16 | 2 | 120 |

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

DB lies within the same server SHHWSR1492.

### 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 | NA | NA |
| Subnet | Infrastructure-IaaS-Subnet\_1 App – 10.38.14.0/23 | NA | NA |

#### Service Interfaces List / FW Rules

Since the hit count is Zero and firewall policy comes under gGRP-SRV-GAS\_AB\_WEB\_SERVERS, gGRP-SRV-GAS\_AB\_SQL\_SERVERS, We haven’t added firewall Rules

### AO provided these protocols and Ports for this server

### Https:443,https:31943,https:31942

### Internet

|  |  |  |  |
| --- | --- | --- | --- |
| Servers | Internet Required | URL to be Whitelist | Remarks |
| NA | NO | NA | NA |

### Azure Application Gateway / WAF / Azure FW

// Since the server functionality is Infra , we can bypass Application Gateway

|  |  |
| --- | --- |
| Attribute | Value |
| Azure App Gateway Name | NA |
| Backend Server | NA |
| Backend Ports | NA |
| Azure App Gateway Public Endpoint | NA |

### Shared Infrastructure Sevices

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

|  |  |  |  |
| --- | --- | --- | --- |
| Service Component Name | Service | Description | Ref ID |
| Identity | Active Directory Service |  | NA |
| DNS | DNS Service |  | NA |
| Monitoring | NA | Infra and APP monitoring respectively | NA |
| Backups | Azure Backup |  | NA |
| SIEM | NA |  | NA |
| Networking | NA |  | NA |

### Certificates

|  |  |  |
| --- | --- | --- |
| **External URL** | **Issued to** | **Issuer** |
| |  | | --- | | NA | | NA | |  | | --- | | NA | |
| **Internal URL** | **Issued to** | **Issuer** |
| NA | |  | | --- | | NA | | |  | | --- | | NA | |

## 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 Geo Redundant Storage (GRS) will be used. | Requirement comes from data availability classification – Important |
| 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 | Disk space issue, need to clean the logs time to time |
| Dependencies | NA |

## 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 |
| MS SQL Server | Azure PAYG / BYOL |
| 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 | 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 | NA |
| 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 involved 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 | Service owner will maintain a backup copy of the files  GL 03.2 - SQL PROD Backup |
| Patching schedule, service hours and maintenance windows | Maintenance Windows –  19th January 2022 9 AM CEST |
| 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.   Application is running in IIS and monitored using Zabbix |

## Azure Asset Management (tags)

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

|  |  |
| --- | --- |
| Key | Value |
| Cost Centre | 120031500 |
| Infra structure service | Esight (Network Management) |
| KG | SHH |
| Service owner | Thangavel Mudaliar |
| Technical contact | NetworkTeam([andrew.ballard@schindler.com](mailto:andrew.ballard@schindler.com),n[josef.prediger@schindler.com](mailto:josef.prediger@schindler.com), Thangavel)  DB -- (roland.faessler@schindler.com) |
| Confidentiality | Internal Use only |
| Integrity | Normal |
| Availability | Important |
| Userbase | Internal, Accessed only by the Network team. CET |

|  |  |
| --- | --- |
| **RG** | **rg-shh-prod-esightnwmgnt-01** |
| **applicationowner** | Thangavel Mudaliar |
| **costcenter** | 120031500 |
| **infrastructureservice** | infrastructure-server |
| **kg** | SHH |
| **serviceowner** | Thangavel Mudaliar |
| **technicalcontact** | NetworkTeam([andrew.ballard@schindler.com](mailto:andrew.ballard@schindler.com),n[josef.prediger@schindler.com](mailto:josef.prediger@schindler.com), Thangavel)  DB -- (roland.faessler@schindler.com) |

# 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 Design document provided by AO

### Migration schedule / timeline

|  |  |
| --- | --- |
| Assessment completion deadline | 7th December 2021 |
| Planning and Design completion deadline | 10th December 2021 |
| Pre-Migration Activities completion deadline | TBD |
| Migration Execution completion deadline | TBD |
| Post Migration activities completion deadline | TBD |

### On-premise 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 (ASR) migration

Source server specification

Servers will be rehosted to Azure using Azure Migrate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Function** | **Environment** | **Migration Method** |
| SHHWSR1492 | 10.10.100.200 | INFRA | PROD | Rehost |

## Database (DMS) migration

Source server/database specification

Database lies in the same Server “SHHWSR1492”.

## 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 and External DNS Names need to be changed to reflect the New IP.

|  |  |
| --- | --- |
| **Internal DNS names published** | https://esight:31943/portal/index.html |
| **External DNS names** | NA |
| **SMTP relay usage** | NA |

## DMZ / Firewall rules

In case one or multiple of your servers 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/Wave2/051%20WSUS/01%20Survey%20Template/ServerDetails.xlsx) for server details & detailed inventory for Source & Target information

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

Database lies within the Same server and planned for Lift & Shift. Involving the DB Server team during Migration.

## 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 |

# 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

esight is divided into 1 move groups based on the Environment & falls under 1 different migration waves

This is a proposed Move Group & Wave Group and may change based on the migration timelines

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Function** | **Environment** | **App Stack** | **Move Group** | **Wave** |
| SHHWSR1492 | 10.10.100.200 | INFRA | PROD | esight |  | Wave2 |
|  |  |  |  |  |  |  |

## Target Architecture

* The Servers will be placed in 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.
* 1 Web Server will be migrated to the Prod Subscription

## Dependency Map

Incoming communication to WSUS is limited to internal stack communication whereas outbound connection is seen for Web, SQL & LDAP

### PROD Environment

Incoming communication to WSUS is for Web Protocol whereas outbound connection is seen for Web & LDAP

## 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 stop** | Manual – Service Stop by the Application Owners |
| **Application start** | Manual – Service Start by the Application Owners |
| **Block user traffic** | NA |
| **Boot order** | APP |

## 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 | Network team(Valere Seignoux,Josef prediger, Andrew Ballard) |
| Test acceptance sign off to be given by | Thangavel Mudaliar |
| 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 3.3.3.2](#_Service_Interfaces_List_1) |
| **Monitoring** | Configure Zabbix on Cloud for the New Instance IP 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 decision |  |

## 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