CSA

Low Level Design

March 2022

|  |  |
| --- | --- |
| Application name | CSA |
| Business purpose | Ivanti CSA is part of Ivanti Infrastructure and this sever is placed in DMZ. The client that are not connected through VPN, can commucicate to internal ivanti infrastructure through this server. It's acting like a bridge between outside and inside infrastructure. |
| Business criticality | Low |
| Service Owner | Jorge Blasco Torres |
| Cost code | 120032300 |
| Supported by | GIS |

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 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).

Gutha: we need to give an instruction what must be filled in in ITSM server request!

Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Changes / Approvals** | **Name** |
| 1.0 | 15/03 | Comments by security | Itay Peled |
|  |  |  |  |

Contents

[2 Application Overview 4](#_Toc73029610)

[2.1 Scope and Design Objectives 4](#_Toc73029611)

[2.2 General information 4](#_Toc73029612)

[3 Application Architecture Design 5](#_Toc73029613)

[3.1 High Level Design overview 5](#_Toc73029614)

[3.2 Low Level Design 7](#_Toc73029615)

[3.3 Azure infra components 9](#_Toc73029616)

[3.3.1 Compute services 10](#_Toc73029617)

[3.3.2 Database services 11](#_Toc73029618)

[3.3.3 Storage Services and external fileshares 11](#_Toc73029619)

[3.3.4 Networking and Connectivity 11](#_Toc73029620)

[3.3.5 Azure Application Gateway / WAF / Azure FW 12](#_Toc73029621)

[3.3.6 Certificates 12](#_Toc73029622)

[3.3.7 Shared Infrastructure Sevices 13](#_Toc73029623)

[3.4 Requirements and Key Design Decisions 14](#_Toc73029624)

[4 Licensing, Assumptions and Dependencies 15](#_Toc73029625)

[4.1 Assumptions, Issues & Dependencies 15](#_Toc73029626)

[4.2 Service Life and Decommissioning 15](#_Toc73029627)

[4.3 Application Software Components 15](#_Toc73029628)

[4.4 Licenses 16](#_Toc73029629)

[5 Integration Architecture 16](#_Toc73029630)

[5.1 Interfaces List 16](#_Toc73029631)

[5.2 User connections 16](#_Toc73029632)

[5.3 Cloud to / from On-Prem Interfaces 17](#_Toc73029633)

[6 Security 17](#_Toc73029634)

[6.1 Security considerations 17](#_Toc73029635)

[6.2 Azure Asset Management (tags) 18](#_Toc73029636)

[7 Application migration planning 19](#_Toc73029637)

[7.1 On-premise application design 19](#_Toc73029638)

[7.1.1 Migration schedule / timeline 20](#_Toc73029639)

[7.1.2 On-premise servers used / required by the application 21](#_Toc73029640)

[7.1.3 Components linked to the application 21](#_Toc73029641)

[7.2 Lift & shift (ASR) migration 21](#_Toc73029642)

[7.3 Database (DMS) migration 21](#_Toc73029643)

[7.4 Share Migration 22](#_Toc73029644)

[7.5 Internal application dependencies 22](#_Toc73029645)

[7.6 External application dependencies or application interfaces 22](#_Toc73029646)

[7.7 DNS names / Published websites / Third party connections 23](#_Toc73029647)

[7.8 DMZ / Firewall rules 23](#_Toc73029648)

[7.9 Performance / response times 23](#_Toc73029649)

[8 Configuration of target situation 24](#_Toc73029650)

[8.1 Database (DMS) migration 24](#_Toc73029651)

[8.2 Share Migration 24](#_Toc73029652)

[9 Migration 25](#_Toc73029653)

[9.1 Move Group 25](#_Toc73029654)

[9.2 Target Architecture 26](#_Toc73029655)

[9.3 Dependency Map 27](#_Toc73029656)

[9.3.1 QA Environment 27](#_Toc73029657)

[9.3.2 PROD Environment 27](#_Toc73029658)

[9.4 Pre-migration activities 28](#_Toc73029659)

[9.5 Test cases 28](#_Toc73029660)

[9.6 Post-migration activities 29](#_Toc73029661)

[9.7 Continue or fallback decision 29](#_Toc73029662)

[9.8 Reconfiguration after testing sign off 29](#_Toc73029663)

# Application Overview

## Scope and Design Objectives

This document details the Low-Level Design (LLD) for CSA appliance 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 CSA for migration to Azure

## General information

Please provide short business context here.

|  |  |
| --- | --- |
| **Attribute** | **Description** |
| Service Name | CSA |
| Service Description | The server is acting like a bridge between outside user and inside ivanti infrastructure. |
| Number of users and their location | 40k Computers Globally connected |
| Data classification (CIA) | Confidentiality – Internal User  Integrity – Normal  Availability – Important |
| Cost Center | 120032300 |
| KG | SHH |
| Service Owner | Jorge Blasco Torres <[jorge.blascotorres@schindler.com](mailto:jorge.blascotorres@schindler.com)> |
| Technical Contact | Jorge Blasco Torres <[jorge.blascotorres@schindler.com](mailto:jorge.blascotorres@schindler.com)> |

# Application Architecture Design

## High Level Design overview

Provide high level solution design overview here.

There is no design document provided by AO.

* This is a web application in Prod environment.
* The application is accessed only Internal and external users.
* The Servers are in GDC Datacentres.

Below is the list of servers that are part of CSA Application.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sever Name | IP Address | Azure IP | Function | Environment | ITSM-Function |
| shhxap0271 | 10.24.2.127 | 10.38.31.56 | DMZ-2 | Prod | CSA |

Below is the bifurcation based on environment & Tier

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **PROD** | **QA** | **DEV** |
| App | 0 | 0 | 0 |
| DB | 0 | 0 | 0 |
| WEB | 1 | 0 | 0 |
| Terminal Server | 0 | 0 | 0 |
| **Grand Total** | **1** | **0** | **0** |

## Low Level Design

Provide Low Level design description here. DO NOT add configuration settings here.

No design document was provided by AO

## Azure infra components

Provide Azure resources top level configuration settings here.

* Regions
* Subscriptions
* Resource Groups

|  |  |  |  |
| --- | --- | --- | --- |
| Description | PROD | QUAL | DEV |
| Subscription | s-sis-eu-prod-01 |  |  |
| Azure Regions | EU North |  |  |
| Resource Group | rg-shh-prod-csa-01 |  |  |

### Compute services

List all virtual servers here

#### Virtual Servers

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Server Name | Data Centre | Operating System | RAM (GB) | CPU Cores | Disk Size (GB) |
| shhxap0271 | GDC | CentOS Linux 7 | 8 | 4 | 50 |

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

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

Database services

### List all DB services and/or DB instances running on SQL Servers/SQL managed instances or Azure SQL PaaS

### 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 | Reference ID |
| NA | NA | NA | NA |

Place output of shared filesystem here if df -hT consists of cifs/nfs mounts

No CIFS/NFS shared Mounts points in this server.

### Networking and Connectivity

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

#### Azure Network Componets

|  |  |  |  |
| --- | --- | --- | --- |
| Component Name | PROD | NON PROD | Reference ID |
| VNet | EU-PROD |  |  |
| Subnet | sub-dmz2domain-01  10.38.31.0/24 |  |  |

### Network Interface details

Text

Description automatically generated

#### Service Interfaces List / FW Rules

[**Please find the link to the FW Rules**](https://schindlerglobal.sharepoint.com/:x:/r/sites/SISCloudAdoption/Shared%20Documents/03%20Project%20Execution/06%20-%20Migration/GDC/GDC-MIG/Wave4/040%20CSA/03%20CSA_FW/CSA_ap0271_FW.xlsx?d=w141670635f2c4e9a8b49ff76b26b26ca&csf=1&web=1&e=ReXP5I)

**//** Created the following public IP: pip-prod-shhxap0271-CSA-vip    -   20.223.16.179

We will not use the AppGW if they cannot create a CNAME for their service so please use this external IP.

**Internet**

|  |  |  |  |
| --- | --- | --- | --- |
| Servers | Internet Required | URL to be Whitelist | Remarks |
| All | Yes | \*.landesk.com | Vendor Sites ending with landesk.com needs to be accessible. |

### Azure Application Gateway / WAF / Azure FW

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

### 

### Certificates

|  |  |  |
| --- | --- | --- |
| **Internal URL** | **Issued to** | **Issuer** |
| shhxap0271.dmz2.schindler.com | shhxap0271.dmz2.schindler.com | DigiCert TLS RSA SHA256 2020 CA1 |

|  |  |  |
| --- | --- | --- |
| **External URL** | **Issued to** | **Issuer** |
| csa05.schindler.com | shhxap0271.dmz2.schindler.com | SSL-SG1-GINDE11 |

### 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 |

## 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 – 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. – Using NAT , Public IP got resolved with Internal IP |
| 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 | Migrating Server IP needs to be shared before the migration, They needs to configure the same in rest of the CSA appliances. |
| Certificate | 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 |
| Ivanti License | Third party – Software based License/ 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 |
|  |  |  |  |  |  |

## 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 taken into account 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 AD * New admin user access will be provided in scope of the standard Schindler service request |
| Directory Services & Authentication | * Service use Azure Active Directory to assign permissions to admin users |
| Privileged access accounts and service/API user accounts | Account name : Service |
| 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.   NAT configured to map public IP with its Internal IP for external users to access this web server. |
| 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. * The app is compliant to the Swiss Law |
| 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 99 - No Backup required |
| Patching schedule, service hours and maintenance windows | Maintenance Windows –  Week Day Business Hours. |
| Data archiving, cleansing & purging (life cycle management) | Service owner is responsible for data lifecycle management. |
| Data migration | Data will be migrated manually by copying files.  ASR will be leverage for VM Replication to target |
| 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 | 120032300 |
| Infra structure service | CSA |
| KG | SHH |
| Service owner | Jorge Blasco Torres <jorge.blascotorres@schindler.com> |
| Technical contact | Jorge Blasco Torres <jorge.blascotorres@schindler.com> |
| confidentiality | Internal use only |
| Integrity | Normal |
| availability | Important |
| Userbase | There are 40K computers connecting and 2 admin accounts |

|  |  |
| --- | --- |
| **RG** | **rg-shh-prod-csa-01** |
| **applicationowner** | Jorge Blasco Torres <jorge.blascotorres@schindler.com> |
| **costcenter** | 120032300 |
| **infrastructureservice** | infrastructure-server |
| **kg** | Shh |
| **serviceowner** | Jorge Blasco Torres <jorge.blascotorres@schindler.com> |
| **technicalcontact** | Jorge Blasco Torres <jorge.blascotorres@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

### Migration schedule / timeline

|  |  |
| --- | --- |
| Assessment completion deadline | 8th March, 2022 |
| Planning and Design completion deadline | 14th March, 2022 |
| Pre-Migration Activities completion deadline | NA |
| Migration Execution completion deadline | NA |
| Post Migration activities completion deadline | NA |

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

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

### Components linked to the application

Part of Ivanti Infrastructure

## Lift & shift (ASR) migration

Servers will be rehosted to Azure

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Function** | **Environment** | **Migration Method** |
| shhxap0271 | 10.24.2.127 | DMZ-2 | PROD | Rehost |

### Release and Kernel version

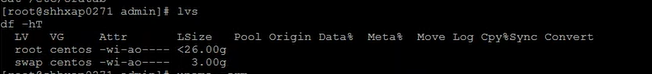
3.10.0-1160.53.1.e17.x86\_64



### Filesystem details

Graphical user interface

Description automatically generated with medium confidence



Note: If thin provision, then the Attribute section will be starting with a 't'. Thin provisioned logical volumes are not supported on Azure.

For each server to be lift & shifted in this migration  
Please refer the [link](https://schindlerglobal.sharepoint.com/:x:/r/sites/SISCloudAdoption/Shared%20Documents/03%20Project%20Execution/06%20-%20Migration/GDC/LTI/01-ServerList/GDC-AzureAdoption-MigrationDetailList_LTI.xlsx?d=w6a6199c213a742a4a34faf8c88c67459&csf=1&web=1&e=xfGE30) for server details & detailed inventory for Source & Target information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Function** | **Environment** | **Migration Method** |
| shhxap0271 | 10.24.2.127 | DMZ-2 | PROD | Rehost |

## Database (DMS) migration

No DB involved

## 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** |
| Other CSA Appliance | Migrating server New IP needs to be added in each CSA Appliance machines |

## 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 names published** | shhxap0271.dmz2.schindler.com |
| **External DNS names** | csa05.schindler.com |
| **SMTP relay usage** | Smtp.eu.schindler.com |

## 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) | Shhxap0271 |

## 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>

# Configuration of target situation

For each server to be lift & shifted in this migration  
Please refer the [**link**](https://schindlerglobal.sharepoint.com/:x:/r/sites/SISCloudAdoption/Shared%20Documents/03%20Project%20Execution/06%20-%20Migration/GDC/LTI/01-ServerList/GDC-AzureAdoption-MigrationDetailList_LTI.xlsx?d=w6a6199c213a742a4a34faf8c88c67459&csf=1&web=1&e=xfGE30) for server details & detailed inventory for Source & Target information

## Database (DMS) migration

Target server/database specification

No Database .

## 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

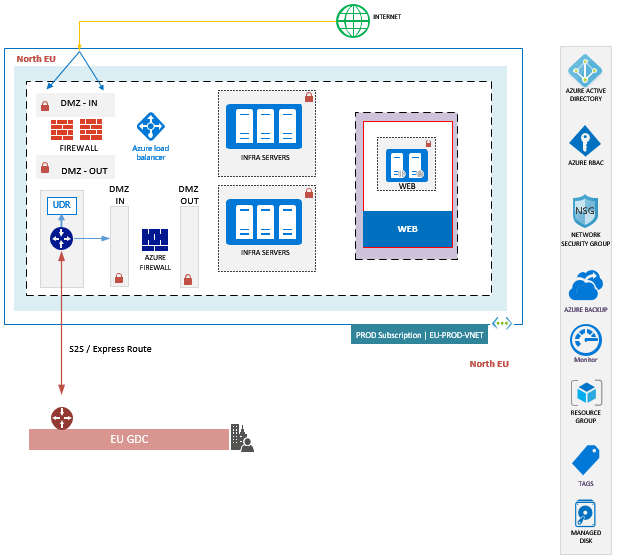
The third chapter describes the migration steps for the application server(s). This includes specific pre-migration activities, test case description, steps for conducting the actual migration and finally specific post migration activities.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Server Name** | **IP address** | **Function** | **Environment** | **Application** | **Move Group** | **Wave** |
| shhxap0271 | 10.24.2.127 | DMZ-2 | PROD | CSA |  | Wave4 |

## Move Group

## Target Architecture

The Servers will be placed in Prod & Non-Prod Subscription based on the Environment & Based on the Tier the Servers will be placed into the respective Subnet. Web Servers will be placed in the DMZ Zone as per the Source Architecture



## Dependency Map

### PROD Environment

## 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** | Needs to be blocked |
| **Boot order** | 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.

**To be detailed by application team**

|  |  |
| --- | --- |
| **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 | Jorge Blasco Torres <jorge.blascotorres@schindler.com> |
| Test acceptance sign off to be given by | Jorge Blasco Torres <jorge.blascotorres@schindler.com> |
| Planned test case execution window |  |

## Post-migration activities

Explain in detail all required post-migration activities to be completed after the migration.

|  |  |
| --- | --- |
| **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** | NA |
| **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.

|  |  |
| --- | --- |
| 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.