

HLD – WBS

(Werk Bemiddeling Service)

Version: 2.3

Date: 26.01.2023

Document purpose

This High-Level Design (HLD) is used to:

* Validate the Application solution from a technical perspective through architectural review
* Plan and execute implementation of the solution
* Support Technical Application Management

The document outlines:

* An overview of the application and its architecture
* Functional and non-functional requirements
* Solution description
  + By default, the solution will use standard services from the DXC catalog for UWV. Where applicable required variances will be described.

Relation to Reference Architecture, ABB’s, HLD VI, SBB’s and SAD

The UWV Reference Architecture provides the context for the HLD VI. The HLD VI is focused on the architectures enabling the datacentre hosting services, its building blocks and the integrations.

* **Architectures Building Blocks (ABB)**, maintained by UWV, are built up from a collections of solution building blocks (SBB’s), so most building blocks will interoperate with other building blocks (integrations).
* **Solution Building Blocks (SBBs),** maintained by DXC, represent components that will be used to implement the required capability for the datacenter hosting service;

This HLD leverages the ABB’s and SBB’s as a foundation for the solution.

The following documents may be relevant as context to this HLD:

* The Software Architecture Document
* Technisch Beheer Handboek (TBH – technical management handbook)
* Technisch Koppelvlak Document (TKD – technical interface document)
* Procedure HandBoek (PHB – procedure handbook – part 1 = standard, 2 – exceptions)

Structure of the document

High level flow: first the application overview and architecture are described followed by the functional and non-functional requirements that ‘drive’ the solution as described in the final chapter. The appendices include any additional details or specifics for the application described in this HLD. See table of contents on next page for further details.

Content of the document

DXC has prepared this document in good faith and is partly based on the information made available to it by UWV and IBM (e.g. HLD document). The statements and content in this document should be qualified accordingly. For the same reason some references in this document might be ‘outdated’ (i.e. not in this document anymore nor in other related documents).

Table of Contents

[1 Application Overview 4](#_Toc119414572)

[1.1 Introduction 4](#_Toc119414573)

[1.2 Application use cases 4](#_Toc119414574)

[1.3 Out of Scope 4](#_Toc119414575)

[2 Architecture 5](#_Toc119414576)

[2.1 Conceptual 5](#_Toc119414577)

[2.2 Context diagram 6](#_Toc119414578)

[3 Functional Requirements 16](#_Toc119414579)

[4 Non-Functional Requirements 17](#_Toc119414580)

[4.1 Security & Compliance classifications 17](#_Toc119414581)

[4.2 System and Software requirements 17](#_Toc119414582)

[4.3 Availability 18](#_Toc119414583)

[4.4 Security requirements 18](#_Toc119414584)

[4.5 System management 18](#_Toc119414585)

[4.6 Backup and Recovery 18](#_Toc119414586)

[4.7 Storage replication 19](#_Toc119414587)

[4.8 Scalability 19](#_Toc119414588)

[4.9 Disaster Recovery 19](#_Toc119414589)

[4.10 Infrastructure Technical Constraints 19](#_Toc119414590)

[4.11 DXC TAB requirements 19](#_Toc119414591)

[5 Solution 21](#_Toc119414592)

[5.1 Architectural Decisions 21](#_Toc119414593)

[5.2 Node descriptions and zone-projections 21](#_Toc119414594)

[5.3 System diagram – Production 22](#_Toc119414595)

[5.4 System diagram Non-Production 22](#_Toc119414596)

[5.5 SBB’s 23](#_Toc119414597)

[5.6 Load balancers 23](#_Toc119414598)

[5.7 Deviations from standards (RAL / EtP) 24](#_Toc119414599)

[5.8 Service Management 24](#_Toc119414600)

[5.9 Security 24](#_Toc119414601)

[6 Potential future improvements 26](#_Toc119414602)

[Version Control 27](#_Toc119414603)

[Appendix A: Technology and Sizing (at design verification) 30](#_Toc119414604)

[*Node details* 30](#_Toc119414605)

[*Storage* 31](#_Toc119414606)

[*Software* 32](#_Toc119414607)

[*Load Balancers* 33](#_Toc119414608)

[Appendix B: Network Protocol Matrix 34](#_Toc119414609)

[Appendix C: Users and Groups 35](#_Toc119414610)

[Appendix E: Glossary 36](#_Toc119414611)

[Appendix F: Legenda 37](#_Toc119414612)

[Legenda Context Diagram 37](#_Toc119414613)

[Legenda System Diagram 37](#_Toc119414614)

# Application Overview

## Introduction

WBS stands for “Werk Bemiddeling Service” and is used by the UWV (CWI) advisors for the mediation of job seekers.

## Application use cases

WBS is an application in which job vacancies are administered. It is used by work coaches to mediate between job seekers and employers. WBS also delivers web services to application like SONAR (not directly, all through WBSBUS) and changes to job vacancy information are placed on the service bus. It uses ELISE as a matching service and the EURES-BACKEND has a database link to the WBS database for sharing vacancies to Brussels.

Besides the application interfaces, WBS depends on scheduled jobs to exchange WBS data with different national municipalities, business reporting systems within UWV (DWH) and user management departments within UWV. The references to these jobs are:

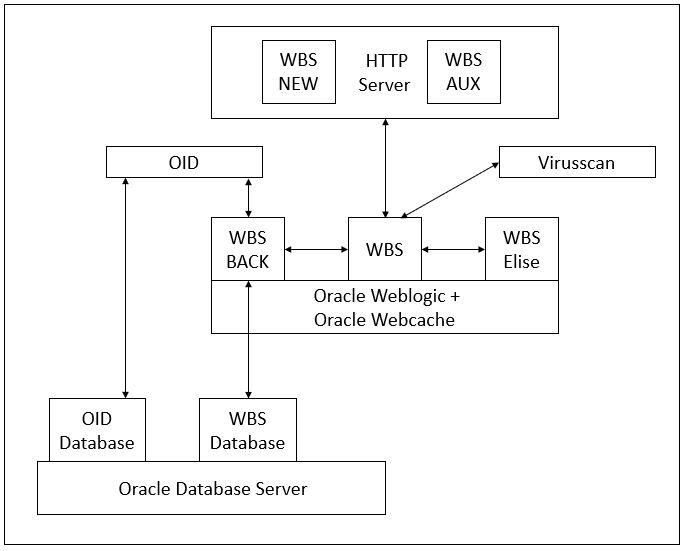
* DWI job – Gathers information from the WBS database in csv-files and send these files to a list of e-mail recipients.
* DWH job – Gathers information from the WBS database in text-files and send these files with FTP to the SI-FT system and collection by DWH.
* User Privileges - Gathers information from the WBS database and WBS OID and creates a csv file. The csv file is emailed as an attachment to a list of recipients.

## Out of Scope

* The development and test environment are not managed by DXC and are out of scope of this HLD
* All components that belong to the UWV Office Infrastructure such as workstations, web browsers are out of scope.

# Architecture

## Conceptual



**Key concepts:**

* Three environments: One in the Production domain and 2 in Acceptance domain (WATO and KATO)
* 3-tier setup, Web Frontend, Application Backend and database tier.
* There will be 2 webservers in a load balanced configuration (both in production and acceptance). KATO will not be loadbalanced and will only have 1 frontend en 1 backend server.
* Weblogic systems run on RHEL.
* Application backend will be deployed in Weblogic containers. There will be separate containers for WBS, WBS Back and WBS Elise connector.
* The Web Frontend is split into two parts WBS-New and WBS-Aux: two separate Web applications
* WBS web applications use a Windows Virus scanning server for scanning uploaded documents,
* The databases will run on Oracle database server on RHEL.
* WBS OID is considered as part of the WBS application and runs on a separate server, also on RHEL

**KATO**

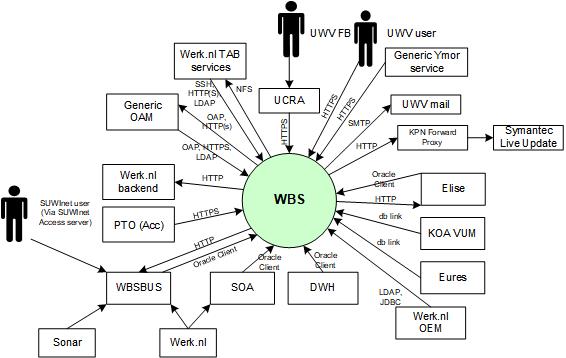
Next to Production and Acceptance (WATO) there is also a KATO environment. The KATO (Kanban Acceptatie Test Omgeving) environment was formerly known as the TST environment.

KATO is a 'light version' of the official acceptance environment of Werkbedrijf. Acceptance tests are performed on this environment without a load and performance test. In Werkbedrijf KATO chain traceable personal data is used, because only then a correct test can be done. The AVG laws and regulations requires the KATO environment to be placed under a stricter regime and therefore it is now hosted in the acceptance domain, and it is managed by DXC.

To summarize there is 1 production environment and 2 acceptance environments:

* WATO - official acceptance
* KATO - light version of acceptance

## Context diagram



### External entities

#### UWV FB

|  |  |
| --- | --- |
| **Description** | System adminstrator of the WBS-system accessing the Adminstrations functions of the system. These administration functions exist on the application web interface |
| **Protocol and Port** | HTTPS:443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No: via UCRA |
| **Security Controls** | Authorisation method or authentication method: WBS OID  Authorisation method or authentication method: OAM  Use certificates: Yes (Entrust)  Service account: No  Other: <(only mention if applicable) other applicable security control related configuration> |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### UWV user

|  |  |
| --- | --- |
| **Description** | Workcoaches (from UWV Werkplek and SUWI portaal) using the WBS -system to collect information, support workseekers and mediate between them and employers. |
| **Protocol and Port** | HTTPS: 443 |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound: communication is initiated by the entity |
| **Direct connection** | Yes: direct connection between application and entity |
| **Security Controls** | Authorisation method or authentication method: WBS OID  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### SUWInet user

|  |  |
| --- | --- |
| **Description** | SUWInet user (including SBR) is a user that is using SUWI Inkijk to get information from WBS. |
| **Protocol and Port** | HTTP: 80 |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound: communication is initiated by the entity |
| **Direct connection** | No: via SUWnet access server and WBSBUS |
| **Security Controls** | Authorisation method or authentication method: SUWI  Use certificates: No  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Generic Ymor service

|  |  |
| --- | --- |
| **Description** | Werkbedrijf service to be able to perform end-user performance measurements (in production only) of the WBS application. |
| **Protocol and Port** | HTTPS: 443 |
| DC (Datacenter) connection | External |
| **Direction** | Inbound: communication is initiated by the entity |
| **Direct connection** | Yes: direct connection between application and entity |
| **Security Controls** | Authorisation method or authentication method: None required  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### UWV mail

|  |  |
| --- | --- |
| **Description** | Used to route e-mails for automatic notifications.  The acceptance environment uses the “Werkbedrijf” Generieke services mail relay. Production uses the KPN/UWV Mail relay. |
| **Protocol and Port** | SMTP: 25 |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound - Communication is initiated by the application |
| **Direct connection** | Yes: direct connection between application and entity |
| **Security Controls** | Authorisation method or authentication method: None required  Use certificates: No  Service account: No  Other: WBS server must be whitelisted at Mail Relay |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Symantec Live Update

|  |  |
| --- | --- |
| **Description** | Symantec’s sytems to update the AntiVirus software within the WBS-system. |
| **Protocol and Port** | HTTP: 3128 (proxy.voorzieningen.uwv.nl) |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound: communication is initiated by the application |
| **Direct connection** | No: via KPN forward proxy. |
| **Security Controls** | Authorisation method or authentication method: None required  Use certificates: No  Service account: No  Other: Required communication added to the browse profile for the system at the KPN forward Proxy |
| **Number of users** | 1 antivirus host in acceptance and 1 antivirus host in production. |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Elise

|  |  |
| --- | --- |
| **Description** | Elise WBS is an application specialised in accurately matching vacancies with CVs of candidates.   1. Elise Data replicator 2. Retrieve Matching information |
| **Protocol and Port** | 1. Oracle client:1526 2. HTTP: 80, 2800, 2801 |
| **DC (Datacenter) connection** | 1. Internal 2. Internal |
| **Direction** | 1. Inbound: communication is initiated by the entity 2. Outbound: communication is initiated by the application |
| **Direct connection** | 1. Yes: direct connection 2. Yes: direct connection |
| **Security Controls** | Connection 1:  Authorisation method or authentication method: WBS db account  Use certificates: No  Service account: No  Connection 2:  Authorisation method or authentication method: None required  Use certificates: No  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### KOA VUM

|  |  |
| --- | --- |
| **Description** | A KOA application combining data of job vacancies and resumes to exchange that with external parties. |
| **Protocol and Port** | DB link:1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound: communication is initiated by the entity |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: WBS db account  Use certificates: No  Service account: No |
| **Number of users** | 1 |
| **Number of transactions** | Daily scheduled retrieval updated vacancies |
| **Frequency of transactions** | Daily |
| **Volume of data** | Low/Medium |

#### Eures

|  |  |
| --- | --- |
| **Description** | Eures is a portal accessible for people looking for a job in Europe. UWV provides vacancies (vacatures) infromation from WBS to this portal. |
| **Protocol and Port** | DB link:1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound: communication is initiated by the entity |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: WBS db account  Use certificates: No  Service account: No |
| **Number of users** | 1 |
| **Number of transactions** | Daily scheduled retrieval of ± 3.000 updated vacancies |
| **Frequency of transactions** | Daily |
| **Volume of data** | 3.000 x 10 kB ~ 30 MB1 |

#### Werk.nl

|  |  |
| --- | --- |
| **Description** | 1. Werk.nl environment with different application components interacting with WBS. 2. Vacancies updates from WBS to Elise WBS via Werk.nl servicebus (SOA) |
| **Protocol and Port** | 1. Oracle client: 1526 2. Oracle client: 1526 |
| **DC (Datacenter) connection** | 1. Internal 2. Internal |
| **Direction** | 1. Inbound 2. Inbound |
| **Direct connection** | 1. No, via WBSBUS 2. No, via SOA |
| **Security Controls** | Connection 1:  Authorisation method or authentication method: WBS db account  Use certificates: No  Service account: No  Connection 2:  Authorisation method or authentication method: WBS db account  Use certificates: No  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Sonar

|  |  |
| --- | --- |
| **Description** | Sonar requests information from WBS to support business processes within Sonar. |
| **Protocol and Port** | HTTP: 80 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No, via WBSBUS |
| **Security Controls** | Authorisation method or authentication method: none required  Use certificates: No  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Werk.nl backend

|  |  |
| --- | --- |
| **Description** | Werkbedrijf Enterprise Java applications: Werk.nl backend application, VWS, BO&C en CDK. WBS uses VWS and BO&C |
| **Protocol and Port** | HTTP: 80 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound: communication is initiated by the application |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: None required  Use certificates: No  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Generic OAM

|  |  |
| --- | --- |
| **Description** | Generic Oracle Access Manager (OAM) enables the use of Windows AD as the single source for the authentication for Single Sign On (SSO) for the UWV users. |
| **Protocol and Port** | HTTP: 80, HTTPS: 443 , LDAP: 389, OAP: 5575 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Both: communication is initiated by the application and the entity |
| **Direct connection** | Yes: direct connection between application and entity |
| **Security Controls** | Authorisation method or authentication method: None required  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Werk.nl TAB services

|  |  |
| --- | --- |
| **Description** | The Werk.nl TAB services contain several services to support TAB, these services include:   1. TAB Deployment server: used to support configuration and deployment of the Werkbedrijf applications and middleware. 2. TAB NFS: This NFS server is used as shared storage for Werkbedrijf middleware or applications supported by TAB. |
| **Protocol and Port** | 1. For protocol and port details see chapter 4.11 2. NFS: 111, 2049 |
| **DC (Datacenter) connection** | 1. Internal 2. Internal |
| **Direction** | 1. Inbound: communication is initiated by the entity 2. Outbound: communication is initiated by the application |
| **Direct connection** | 1. Yes 2. Yes |
| **Security Controls** | Connection 1:  Authorisation method or authentication method: None required  Use certificates: No  Service account: No  Connection 2:  Authorisation method or authentication method: None required  Use certificates: No  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### PTO (Acc)

|  |  |
| --- | --- |
| **Description** | Performance Tests only on WATO environment, accessing LB & Webservers. |
| **Protocol and Port** | HTTPS: 443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: WBS OID  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Werk.nl OEM

|  |  |
| --- | --- |
| **Description** | Werk.nl OEM Cloud Control has connection with the WBS database and Identity provider to gather WBS data for the scheduled jobs. |
| **Protocol and Port** | JDBC (1526). LDAP (389) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound: communication is initiated by the entity |
| **Direct connection** | Yes: direct connection between application and entity |
| **Security Controls** | Jdbc Connection:  Authorisation method or authentication method: None required  Use certificates: No  Service account: Yes  LDAP Connection:  Authorisation method or authentication method: None required  Use certificates: No  Service account: Yes |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | **DWI Job**  Acceptance: Once every day on workdays at noon  Production: Every hour on workdays between 7:00 – 19:00  **DWH Job**  Acceptance: Once every Wednesday at 18:30  Production: Every Friday at 18:30  **User Privileges**  Acceptance: Once every third Monday of the month at 3:00  Production: Once every third Monday of the month at 3:00 |
| **Volume of data** | **DWI Job**  7 queries resulting in csv-files.  **DWH Job**  37 queries resulting in text-files.  **User Privileges**  1 query resulting in csv-files. |

#### DWH

|  |  |
| --- | --- |
| **Description** | Data Warehouse DB connection |
| **Protocol and Port** | HTTPS: 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: None required  Use certificates: No  Service account: Yes |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

# Functional Requirements

No functional requirements specified.

# Non-Functional Requirements

## Security & Compliance classifications

For the BIV Rating the following repository is used: “2022 UWV-brede Risico Applicatie Lijst v1.0”

|  |  |
| --- | --- |
| **Application** | WBS |
| **Owner** | WB |
| **Availability (Beschikbaarheid)** | 2 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 2+ |
| **Type of information /Data Classification** | Personal data of clients |

### Risk analysis UWV

No risk analysis provided by UWV

### Applicable security and compliance frameworks

|  |  |
| --- | --- |
| Security & Compliance Framework | Applicable |
| BIO | Yes |
| AVG / GDPR | Yes |
| DIGID | No |
| SUWI | Yes |
| Additional frameworks | Not applicable |

## System and Software requirements

### System (Operating system (OS))

| **Operating System** | **Version** |
| --- | --- |
| Windows (virusscan server) | 2019 |
| RHEL (remaining servers) | 7.9 |

### Software (Licenses)

| **Software product / component** | **Version** |
| --- | --- |
| Oracle Database server | 19c |
| Oracle OID | 12.2.1.4 |
| Oracle Weblogic Server | 12.2.1.4 |
| Oracle HTTP server (includes Webgate) | 12.2.1.4 |
| Symantec Endpoint Protection | 14.3 |
| Symantec Protection Engine | 8.2 |
| Extended support for Java | 8 |

### Capacity and performance

The web servers should be responsive even during peak loads, the design should allow for upscaling of resources in order to improve performance.

No numbers provided by UWV on the required response times therefore current sizing is considered as enough. Vertical scaling is possible in case needed.

## Availability

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Application Target** | **Application Service Hours** | **Infra Target** |
| Production | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 99,5% |
| Acceptance | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% |

## Security requirements

No specific security requirements are applicable

### System logging

No specific system logging requirements are applicable

## System management

No specific system management requirements are applicable.

### Additional application related infra requirements

|  |  |
| --- | --- |
| **Requirements** | **Status** |
| Use STARTTLS option for UWV mail | No |
| Is Microsoft DTC used for inflight transactions | Not applicable |
| Is HTTPS cookie stickiness required on the load balancer | No |

## Backup and Recovery

|  |  |  |
| --- | --- | --- |
|  | **Default** | **Deviation (when applicable)** |
| Backup | standard backup | Not applicable |
| Restore | no specific restore order | Not applicable |
| Dependency | no dependencies | Not applicable |

## Storage replication

|  |  |
| --- | --- |
| **Environment** | **Storage Replication\*** |
| Production | Replicated storage |
| Acceptance | Replicated storage |
| Acceptance (KATO) | Non-replicated storage |

\* Storage replication is available for all Private Cloud systems (with SLA Gold, Silver and Bronze) and Legacy (AIX) systems with SLA Gold and Silver. Storage replication is not available for Legacy (AIX) systems with SLA Bronze, in this case only Backup / Restore is available

## Scalability

The design should allow for upscaling of resources to improve performance. The initial systems setup will be vertically and horizontally scalable.

Scalability limitations from the application are not defined, not applicable, or unknown to DXC.

## Disaster Recovery

No specific disaster recovery requirements applicable.

## Infrastructure Technical Constraints

No infrastructure technical constraints.

## DXC TAB requirements

|  |  |
| --- | --- |
| **Category** | **Description** |
| Deployment (TAB Deployment server) | * TCP (22, 80, 443) connection from Werk.nl TAB deployment to WBS Web * TCP (22, 7001, 8003, 8005, 8007) connection from Werk.nl TAB deployment to WBS App * TCP (22, 7001, 389, 80, 3060) connection from Werk.nl TAB deployment to WBS OID * TCP (7001, 389, 80, 3060) connection from Werk.nl TAB deployment to WBS OID on AIX (or “the old” WBS OID system) for data export purposes. * TCP (1526) connection from Werk.nl TAB deployment to WBS DB * X11-forwarding enabled for MobaXterm on Linux web-, application- and OID/IDM servers. |
| Deployment (XL Deploy) | * XL Deploy connection (SSH (22)) required to WBS Servers   + WBS web servers   WBS application servers |
| Shared Storage (TAB NFS server) | * NFS (111, 2049) connection from the WBS servers to the TAB NFS server is required |
| Application monitoring (Sitescope) | Below ports and interfaces are relevant Sitescope to WBS application monitoring:   * TCP (7001,389) for OID server, * TCP (5556, 8003, 8005, 8007, 7001) for app servers, * TCP (80, 443) for web servers, * HTTPS (443) for load balancer, |

# Solution

## Architectural Decisions

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Decision** | **Comments** | **Status** |
| 1 | A 3-tier architecture will be used: A separate presentation from application tier and data tier. | redesign is needed for the WBS application to seperate the presentation and the application tier onto 2 virtual machines | Approved |
| 2 | Single sign on and authentication will be arranged via Generic OAM | a dedicated authentication server will not be required anymore. | Approved |
| 3 | Production will have 4 equally sized web and application servers | Load can be handled by 2 web servers and 2 application servers.  To avoid single point of failure in 1 DC, there will be 2 application servers and 2 Web Servers | Approved |
| 4 | KATO environment will consist of a web/application server and a dedicated database server | The web/application server in the pre-GO kanban environment also contains a database. This was not according to design. | Approved |
| 5 | Performance tests will be done in the WATO environment. | This was decided by UWV, because of possible performance issues. | Approved |

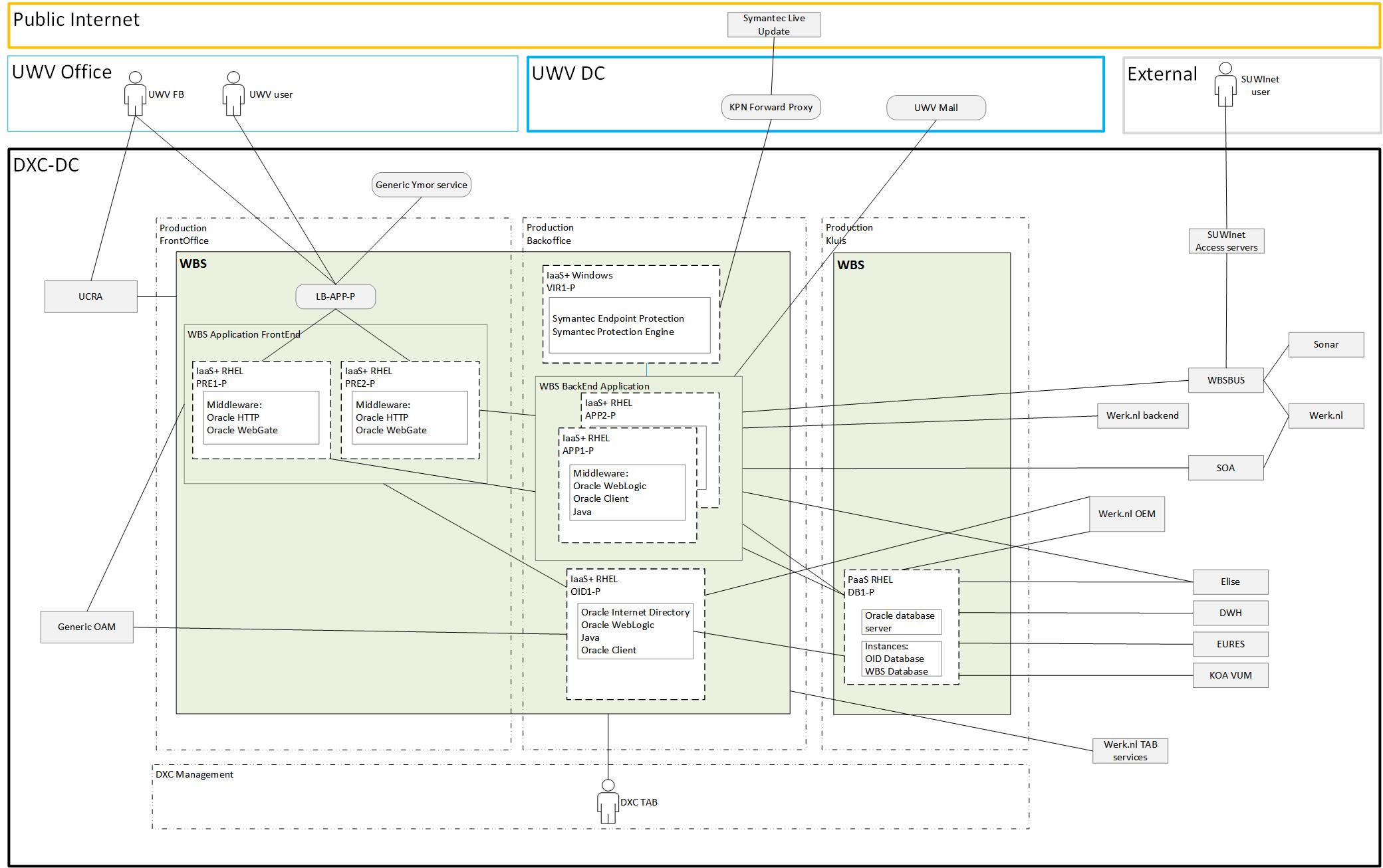
## Node descriptions and zone-projections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Zone** | **Domain** | **Server Type** | **Node ID** | **Infra Service Level** |
| FrontOffice | Production | Presentation Server 1 | PRE1-P | Silver |
| FrontOffice | Production | Presentation Server 2 | PRE2-P | Silver |
| BackOffice | Production | Application Server 1 | APP1-P | Silver |
| BackOffice | Production | Application Server 2 | APP2-P | Silver |
| BackOffice | Production | OID Server | OID1-P | Silver |
| Kluis | Production | Database Server | DB1-P | Silver |
| BackOffice | Production | Virusscan Server | VIR1-P | Silver |
| FrontOffice | Acceptance | Presentation Server 1 | PRE1-A | Bronze |
| FrontOffice | Acceptance | Presentation Server 2 | PRE1-A | Bronze |
| BackOffice | Acceptance | Application Server 1 | APP1-A | Bronze |
| BackOffice | Acceptance | Application Server 2 | APP2-A | Bronze |
| BackOffice | Acceptance | OID Server | OID1-A | Bronze |
| Kluis | Acceptance | Database Server | DB1-A | Bronze |
| BackOffice | Acceptance | Virusscan Server | VIR1-A | Bronze |
| FrontOffice | Acceptance | Presentation Server (Kato) | PRE1-K | Bronze |
| BackOffice | Acceptance | Application Server (Kato) | APP1-K | Bronze |
| Kluis | Acceptance | Database Server (Kato) | DB1-K | Bronze |
| BackOffice | Acceptance | OID Server (Kato) | OID1-K | Bronze |

### DNS (customer facing name)

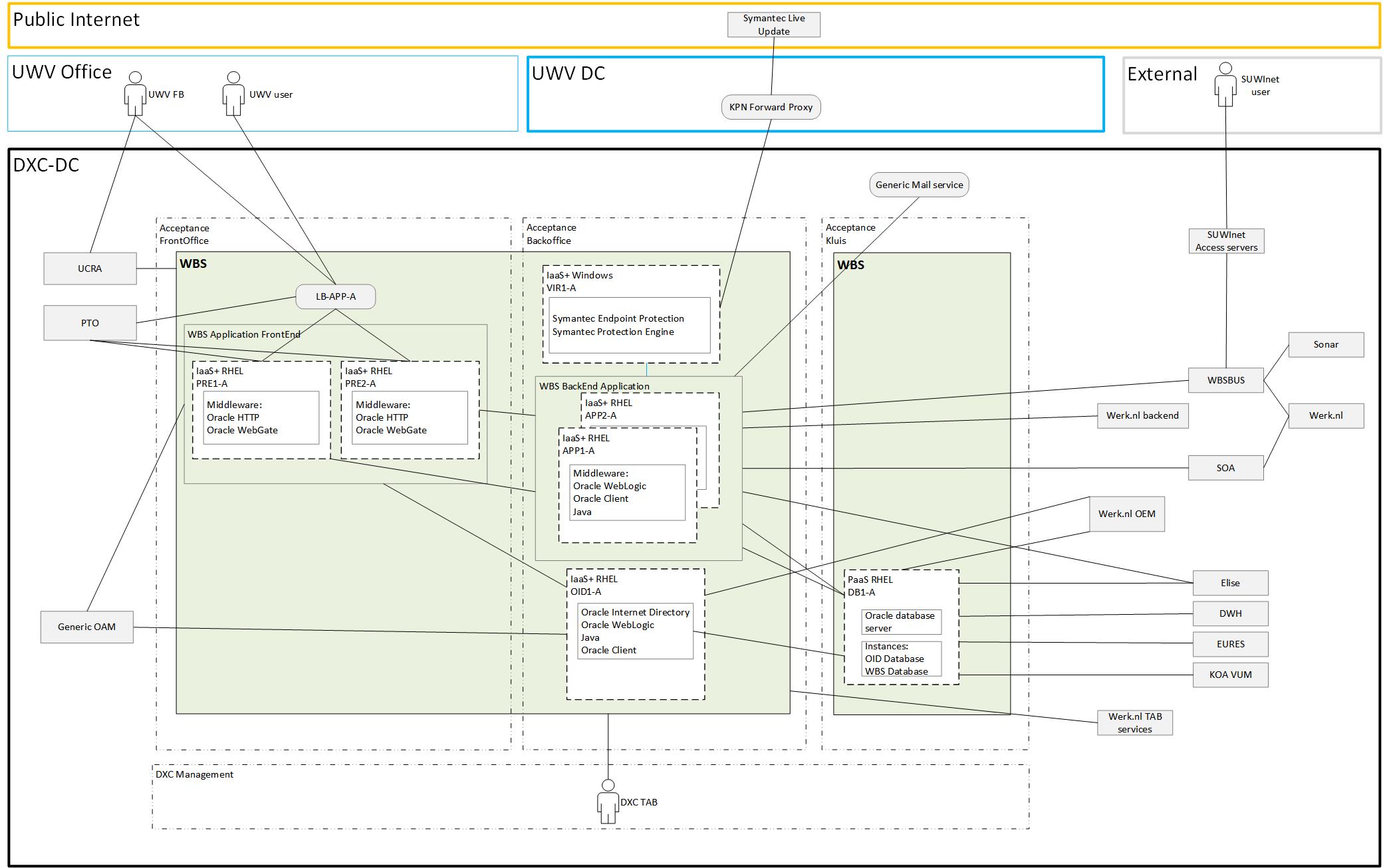
|  |  |  |
| --- | --- | --- |
| **Domain** | **Customer facing name** | **DNS suffix** |
| Production | WBS | P-dc.ba.uwv.nl |
| Acceptance | WBS | A-dc.ba.uwv.nl |
| Acceptance | WBS-KATO | A-dc.ba.uwv.nl |

## System diagram – Production

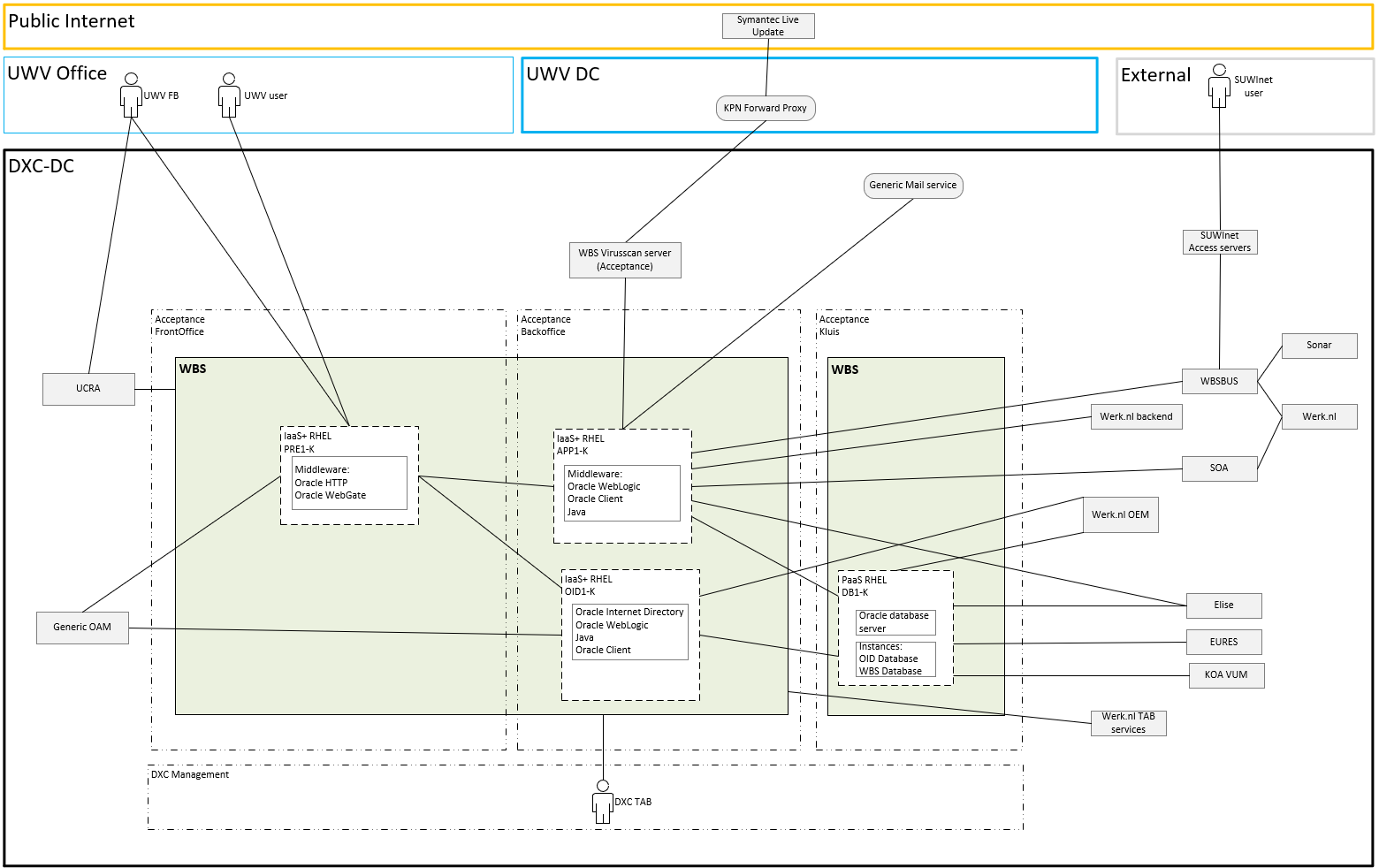


## System diagram Non-Production

### Acceptance (WATO)



### Acceptance (KATO)



## SBB’s

|  |
| --- |
| **Standard Building Block Type** |
| IaaS+ - VM- DXC Managed |
| PaaS - Virtual Oracle database - DXC Managed |

## Load balancers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Load balancer** | **Load balancer type** | **LB ID** | **Description** |
| Production | Yes | Private Cloud | LB-APP-P | LB for WBS Oracle HTTP |
| Acceptance | Yes | Private Cloud | LB-APP-A | LB for WBS Oracle HTTP |

Details can be found in Appendix A – Load balancers

## Deviations from standards (RAL / EtP)

RAL (Risk Acceptance Letter) / EtP (Exception to Policy)

| **Nr** | **Short description of the deviation** | **RAL / EtP required** | **Risk ID** |
| --- | --- | --- | --- |
| 1 | Java Version 8 is going to be used due to compatibility issues with WebLogic 12c, this version is marked as Restricted because of EOS Q3 2021 – EoES is till 2030  (Additional licenses for support are required) | Yes | 20220627-003 |
| 2 | Connections required between different systems in FrontOffice and WBS database in Kluis. Includes systems: WBSBUS | Yes | 20220307-001 |
| 3 | No Encryption: sending emails through KPN mailrelay (outside DXC DC) without STARTTLS | Yes | 20220627-001 |
| 4 | Patching not done: log4j 1.x library with vuln. Unwilling to patch or delete files. RTPA requirements not met. | Yes | 20221004-001-B |

## Service Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Infra Hosting** | **Database / Middleware Management** | **Technical Application Management** |
| Production | Silver | TAB Basis | TAB Basis |
| Acceptance | Bronze | TAB Basis | TAB Basis |

## Security

Security details can be found in Appendix D, any deviations are document in chapter ‘Deviations from standards’.

### User Authentication and Authorization

**UWV FB user with database access**

Variation 4 (Local - local login using local account): User Authentication and Authorization will be performed localy using a local user account, Middleware or AIX access for UWV users requested through the ABS IAM system and changes in PDXC.

**WBS end users**

Other variation:

User Authentication and Authorization will be performed against WBS OID and Generic OAM.

Details are specified in Appendix C

### Firewalls

The data center network offers multiple logical network compartments and has security zones and OTAP domains within it kept separate through a combination of dedicated physical firewall clusters and distributed software defined firewall functions.

* Connections, like interfaces, coming from outside the network security zone do cross one or more firewalls.
* Node to node communication inside the FrontOffice security zone and the same domain do not need to cross a firewall
  + Exception: Node to loadbalancer communication (inside the FrontOffice security zone and the same domain) do need to cross a firewall
* Node to node communication inside the BackOffice security zone and the same domain do not not need to cross a firewall
  + Exception: Node to loadbalancer communication (inside the BackOffice security zone and the same domain) do do need to cross a firewall

For the application we distinguish the following connection categories:

* *Internal:* Connection within the application. For example, ODBC connection between the application- and the database server, if they are in different security zones a firewall is required and the Internal connection is document in the table below
* *External (inside DXC):* Connection external for the application but inside the DXC data center. For example, FTP connection between Application server and SI-File Transfer. To determine if these connections require a Firewall request the security zones must be known, this level of detail is not available in the HLD. The external (inside DXC) connections are not documented in the HLD but can be found in the application connectivity overview sheet.
* *External (outside DXC):* Connection external for the application and outside the DXC data center. For example, HTTP connection between Application server and the UWV Citrix KA farm. All external (outside DXC) connections are documented in the table below

For WBS the following is applicable:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Connection Type** | **Between (component 1)** | **And (component 2)** |
| Internal | HTTP | WBS Presentation servers | WBS Application servers |
| Internal | JDBC | WBS Application servers | WBS Database server |
| Internal | HTTP | WBS Presentation servers | WBS OID server |
| Internal | TCP | WBS Virus | WBS Application servers |
| Internal | HTTP | WBS OID server | WBS Database server |
| External (outside DXC) | HTTPS | UWV Werkplek | WBS Loadbalancer |
| External (outside DXC) | HTTP | WBS Virus | KPN Forward proxy |
| External (outside DXC) | SMTP | WBS Application servers | UWV Mail |

For details see Appendix B

# Potential future improvements

|  |  |  |
| --- | --- | --- |
| **ID** | **Proposed improvement** | **Reason** |
| 1 | Move WBS OID from the WBS application | Move to a central OID is only possible after transition of Sonar to DXC. This transition is in progress. |
| 2 | Update Java and Weblogic middleware | Current versions of Java and Weblogic middleware are stated in project I-AT. Existing WBS software is prepared for this stack of Java and Weblogic. |

# Version Control

**USED TEMPLATE**

|  |
| --- |
| Based on HLD Template: UWV HLD - TEMPLATE 1.86.docx |

**DOCUMENT AUTHORISATION**

| Name | Role | Date |
| --- | --- | --- |
| Hans Kreisel | DXC Account Architect (verification) |  |
| Raymond Groenewoud | UWV Lead Architect (verification) |  |
| Rick van Diemen, delegated to Hans Kreisel | DXC Account Delivery Lead (acceptance) |  |

**DOCUMENT DISTRIBUTION**

| Name | Role | Date |
| --- | --- | --- |
| As per agreed PMO process |  |  |
| UWV TDA (Technical Design Authority) | Design authority |  |

**CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Summary of Changes |
| Verification version 0.7 | 12-10-2020 | DXC architecture team | Updated version after update IBM HLD and updated connectivity information |
| Verification version 0.8 | 30-10-2020 | DXC architecture team | Third iteration of the HLD |
| Verification version 0.9 | 30-10-2020 | DXC architecture team | Design Office verification |
| Version 1.0 | 25-11-2020 | DXC architecture team | Positive verified HLD |
| Version 1.1 | 27-11-2020 | DXC architecture team | Post implementation HLD |
| Version 1.1.1 | 18-03-2022 | DXC architecture team | Updates for change CHG0046772.  Update 1 – Include connection with VUM KOA in chapter 2.2, 5.3 & 5.4  Update 2 – WBS is set up with HTTPS, changes in chapters 5.7.1, Appendix D |
| Version 1.2 | 7-15-2021 | DXC architecture team | First Draft WBS-GOH Redesign WBS.   * NORA Zones, Database in Vault, 3-tier design, upgrade software components. |
| Version 1.3 | 7-20-2021 | DXC architecture team | Update – Java 11 becomes Java 8 due to compatibility with WebLogic 12r2 |
| Version 1.3.1 | 9-2-2021 | DXC architecture team | Newer version based on Review of 1.3   * Update to HLD template version 1.81 |
| Version 1.4 | 25-1-2022 | DXC architecture team | HLD prepared for WBS GOH. |
| Version 1.8 | 03-02-2022 | DXC architecture team | HLD version for account review.  Changes are described in below PDF: |
| Version 1.9 | 08-02-2022 | DXC architecture team | TDA verification |
| Version 2.0 | 09-02-2022 | DXC architecture team | TDA fasttrack approved version |
| Version 2.1 |  | DXC architecture team | Post implementation HLD  Update 1: Align context diagram and entity descriptions with existing connections.  Update 2: Added TAB requirements related deployment and monitoring.  Update 3: Werk.nl OEM Cloud Control for management of WBS jobs.  5-10-2022:   * Accepted all tracked changes and removed comments * Updated to latest template version (1.86)   + Removed Appendix A – certificates (not part of the template, must be specified in the TMM * Added KATO description in 2.1 * Adjusted storage replication for acceptance (non‑replicated to replicated and non‑replicated for KATO) * Updated the context and system diagrams * Updated 5.9.2 with external connection for UWV mail and UWV Werkplek * Updated Appendix A – Node details, correct landing zone, SBB and node ID   10-10-2022:   * Added deviation #4: RAL for log4j 1.x library vulnerability   19-10-2022:   * Deleted TAB requirement : *TCP (22, 111, 2049) connection from Werk.nl TAB deployment to TAB NFS required*. This requirement belongs to the Werk.nl HLD and can be found there.   20-10-2022:   * Added PTO to the HLD. Changed Context diagram, added External entity and Arch. Decision. * Added internal connection for Virus scanner to application servers   27-10-2022   * Added DWH to context diagram and System diagrams for Prod & Acc. After Go-live the fact showed up that these connections were not available.   28-10-2022   * Changed various sizes for several systems, because they didn’t match the reported values: APP1-A, APP2-A, OID1-K, DB1-K |
| Version 2.2 | 17-11-2020 | DXC architecture team | 01-12-2022   * Updated Risk ID of ETP #4 because of KATO inclusion after RTPA. 20221004-001-A became 20221004-001-B. |
| Version 2.3 | 26-01-2023 | D. van den Brink | 26-01-2022  Reduced storage for KATO DB1-K as per actual usage |

# Appendix A: Technology and Sizing (at design verification)

## *Node details*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **Location** | **Domain** | **Node ID** | **vCPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Repl** |
| Private Cloud Oracle MW | FrontOffice | AM2 | Production | PRE1-P | 2 | 16 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Silver | IaaS+ | yes |
| Private Cloud Oracle MW | FrontOffice | AM3 | Production | PRE2-P | 2 | 16 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Silver | IaaS+ | yes |
| Private Cloud Oracle MW | BackOffice | AM2 | Production | APP1-P | 2 | 24 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Silver | IaaS+ | yes |
| Private Cloud Oracle MW | BackOffice | AM3 | Production | APP2-P | 2 | 24 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Silver | IaaS+ | yes |
| Private Cloud Oracle MW | BackOffice | AM2 | Production | OID1-P | 2 | 6 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Silver | IaaS+ | yes |
| Private Cloud Oracle DB | Kluis | AM2 | Production | DB1-P | 4 | 24 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Silver | PaaS | yes |
| Private Cloud | BackOffice | AM2 | Production | VIR1-P | 1 | 4 | |  |  | | --- | --- | | Windows 2019 | Select | | Silver | IaaS+ | yes |
| Private Cloud Oracle MW | FrontOffice | AM3 | Acceptance | PRE1-A | 2 | 16 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | yes |
| Private Cloud Oracle MW | FrontOffice | AM2 | Acceptance | PRE2-A | 2 | 16 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | yes |
| Private Cloud Oracle MW | BackOffice | AM3 | Acceptance | APP1-A | 2 | 24 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | yes |
| Private Cloud Oracle MW | BackOffice | AM2 | Acceptance | APP2-A | 2 | 24 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | yes |
| Private Cloud Oracle MW | BackOffice | AM3 | Acceptance | OID1-A | 2 | 6 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | yes |
| Private Cloud Oracle DB | Kluis | AM3 | Acceptance | DB1-A | 4 | 24 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | PaaS | yes |
| Private Cloud | BackOffice | AM3 | Acceptance | VIR1-A | 1 | 4 | |  |  | | --- | --- | | Windows 2019 | Select | | Bronze | IaaS+ | yes |
| Private Cloud Oracle MW | FrontOffice | AM3 | Acceptance | PRE1-K | 2 | 16 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | no |
| Private Cloud Oracle MW | BackOffice | AM3 | Acceptance | APP1-K | 2 | 24 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | no |
| Private Cloud Oracle MW | BackOffice | AM3 | Acceptance | OID1-K | 2 | 6 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | IaaS+ | no |
| Private Cloud Oracle DB | Kluis | AM3 | Acceptance | DB1-K | 4 | 16 | |  |  | | --- | --- | | RHEL 7.9 | Select | | Bronze | PaaS | no |

## *Storage*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **C-drive OS (Fixed)** | **D-drive App (mandatory)** | **E-drive (optional)** | **F-drive (optional)** | **…-drive (optional)** |
| VIR1-P | Production | 100 GB | 50 GB | n/a | n/a | n/a |
| VIR1-A | Acceptance | 100 GB | 50 GB | n/a | n/a | n/a |

*Windows Application server(s)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App (mandatory)** | **Disk 1 – Mountpoint 2 (optional)** | **Disk 1 – Mountpoint 3 (optional)** | **Disk 2 – Mountpoint 1 (optional)** |
| PRE1-P | Production | 100 GB | 500 GB | n/a | n/a | n/a |
| PRE2-P | Production | 100 GB | 500 GB | n/a | n/a | n/a |
| APP1-P | Production | 100 GB | 500 GB | n/a | n/a | n/a |
| APP2-P | Production | 100 GB | 500 GB | n/a | n/a | n/a |
| OID1-P | Production | 100 GB | 100 GB | n/a | n/a | n/a |
| PRE1-A | Acceptance | 100 GB | 250 GB | n/a | n/a | n/a |
| PRE2-A | Acceptance | 100 GB | 250 GB | n/a | n/a | n/a |
| APP1-A | Acceptance | 100 GB | 500 GB | n/a | n/a | n/a |
| APP2-A | Acceptance | 100 GB | 500 GB | n/a | n/a | n/a |
| OID1-A | Acceptance | 100 GB | 150 GB | n/a | n/a | n/a |
| PRE1-K | Acceptance | 100 GB | 100 GB | n/a | n/a | n/a |
| APP1-K | Acceptance | 100 GB | 100 GB | n/a | n/a | n/a |
| OID1-K | Acceptance | 100 GB | 150 GB | n/a | n/a | n/a |

*Linux Application server(s)*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk0 OS (Fixed)** | **Disk1 Oracle Binaries (Fixed)** | **Disk2 ASM Binaries (Fixed)** | **ASM DATA1 DiskGroup1 Data Files, Control Files** | **ASM DATA2 DiskGroup1 Data Files, Control Files** | **ASM FRA1 DiskGroup2 Archive and Flashback Logs** | **ASM FRA2 DiskGroup2 Archive and Flashback Logs** |
| DB1-P | Production | 100 GB | 100 GB | 100 GB | 150 GB | 150 GB | 50 GB | 50 GB |
| DB1-A | Acceptance | 100 GB | 100 GB | 100 GB | 100 GB | 100 GB | 50 GB | 50 GB |
| DB1-K | Acceptance | 100 GB | 100 GB | 100 GB | 100 GB | 100 GB | 50 GB | 50 GB |

*Oracle Database server(s)*

## *Software*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported by vendor** |
| PRE1-P, PRE2-P, PRE1-A, PRE2-A, PRE1-K | 1-OS | RHEL | 7.9 | Y |
| PRE1-P, PRE2-P, PRE1-A, PRE2-A, PRE1-K | 2-Library | Oracle Java | 8 | Y |
| PRE1-P, PRE2-P, PRE1-A, PRE2-A, PRE1-K | 4-Middleware | Oracle HTTP server | 12.2.1.4 | Y |
| PRE1-P, PRE2-P, PRE1-A, PRE2-A, PRE1-K | 4-Middleware | Oracle Webgate (is installed together with Oracle HTTP Server, no separate software ) | 12.2.1.4 | Y |
| APP1-P, APP2-P, APP1-A, APP2-A, APP1-K | 1-OS | RHEL | 7.9 | Y |
| APP1-P, APP2-P, APP1-A, APP2-A, APP1-K | 2-Library | Oracle Java | 8 | Y |
| APP1-P, APP2-P, APP1-A, APP2-A, APP1-K | 4-Middleware | Oracle Weblogic server (Fusion Middleware Infrastructure) | 12.2.1.4 | Y |
| APP1-P, APP2-P, APP1-A, APP2-A, APP1-K | 4-Middleware | Oracle client | 19.14.0.0.0 | Y |
| OID1-P, OID1-A, OID1-K | 1-OS | RHEL | 7.9 | Y |
| OID1-P, OID1-A, OID1-K | 2-Library | Oracle Java | 8 | Y |
| OID1-P, OID1-A, OID1-K | 4-Middleware | Oracle Weblogic server (Fusion Middleware Infrastructure) | 12.2.1.4 | Y |
| OID1-P, OID1-A, OID1-K | 4-Middleware | Oracle OID | 12.2.1.4 | Y |
| OID1-P, OID1-A, OID1-K | 4-Middleware | Oracle client | 19.14.0.0.0 | Y |
| DB1-P, DB1-A, DB1-K | 1-OS | RHEL | 7.9 | Y |
| DB1-P, DB1-A, DB1-K | 3-Database | Oracle database server | 19.14.0.0.0 | Y |
| VIR1-P, VIR1-A | 1-OS | Windows | 2019 | Y |
| VIR1-P, VIR1-A | 4-Middleware | Symantec Endpoint Protection | 14.3 | Y |
| VIR1-P, VIR1-A | 4-Middleware | Symantec Protection Engine | 8.2 | Y |

## *Load Balancers*

***Private Cloud / Legacy***

|  |  |  |
| --- | --- | --- |
| **Application Shortname** | WBS | WBS |
| **FQDN** | p-wbs-fo-lb-avi.p-dc.ba.uwv.nl | a-wbs-fo-lb-avi.a-dc.ba.uwv.nl |
| **FQDN alias** | WBS.p-dc.ba.uwv.nl | WBS.a-dc.ba.uwv.nl |
| **FROM: Security zone**  **(client side)** | Outside datacentre | Outside datacentre |
| **TO: Security zone**  **(load balancer server side)** | FrontOffice | FrontOffice |
| **Domain** | Production | Acceptance |
| **Pool Members (Node ID)** | PRE1-P  PRE2-P | PRE1-A  PRE2-A |
| **Application Layer Protocol** | HTTP (L7) | Select |
| **Application Port(s)** | 80 |  |
| **Expected concurrent connections** | <1000 | <1000 |
| **Load balancing Algorithm** | Round-Robin | Round-Robin |
| **Stickiness/Persistance** | System-Persistence-Client-IP | System-Persistence-Client-IP |
| **Health monitor type** | System-HTTP | System-HTTP |
| **Port / Ports for use with Health Monitor** | 80, 443 | 80, 443 |
| **HTTP Get request (optional)** |  |  |
| **HTTP Response string / code (optional)** |  |  |
| **Additional Comments** |  |  |

# Appendix B: Network Protocol Matrix

*The following ports must be allowed on the firewalls (Only Internal and External (outside DXC) connections are mentioned, External (inside DXC) are specified in the connectivity sheet).*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UWV Office   * KA systems | DXC DC   * Production: Load Balancer   Acceptance: Load Balancer | TCP | 443 | HTTPS |

**Workcoach to Load Balancer**

*The following ports must be allowed on the firewalls between Workcoach and Application Server (Kato)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UWV Office   * KA systems | DXC DC  Acceptance: Application server (Kato) | TCP | 443 | HTTPS |

**Workcoach to Application Server (Kato)**

*The following ports must be allowed on the firewalls between Application server and UWV Mail*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DXC DC   * Production: Application Servers * Acceptance: Application Servers   Acceptance: Application server (Kato) | UWV DC  UWV Mail | TCP | 25 | SMTP |

**Application Server to UWV Mail**

*The following ports must be allowed on the firewalls between Virusscan server and Internet Proxy KPN*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DXC DC   * Production: Virusscan Server * Acceptance: Virusscan Server | UWV DC   * Internet Proxy KPN | TCP | 3128 | Symantec Live Update |

# Appendix C: Users and Groups

***User Authentication and Authorisation managed by DXC:***

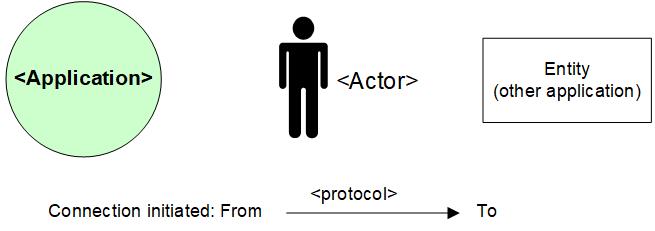
DXC Managed Users and groups are documented by DXC TAB in the TBH / TMM (Technisch Beheer Handboek / Technical Maintenance Manual) or by the Lead Engineer during the realization phase

# Appendix E: Glossary

| **Acronym** | **Description** | **Notes** |
| --- | --- | --- |
| **ABS** | “Authorisatie Beheers Systeem” | Authorization Management System |
| **AOAG** | MS SQL Always On Availability Group | Db Architecture |
| **ASO** | Account Security Officer |  |
| **ASP** | Account Security Plan |  |
| **BAD** | “Basis Applicatie Diensten” | Basic Application Services |
| **CI** | Configuration Item |  |
| **CIs** | Configuration Items |  |
| **CMO** | Current Mode of Operation refers to mode of operation of the old supplier. | See FMO |
| **CVA** | Customer Virtual Appliance |  |
| **DXC managed systems** | All systems in the datacenters where DXC is responsible for |  |
| **DXC management REALM** | Management network of DXC dedicated for UWV in Amsterdam DC’s |  |
| **EoS** | End of Support |  |
| **FMO** | Future Mode of Operation refers to mode of operation of the new supplier. |  |
| **FTP(s)** | File Transfer Protocol - SSL | See (s)FTP |
| **(s)FTP** | Secure File Transfer Protocol | See FTP(s) |
| **GRC** | Governance risk and compliance |  |
| **IBP** | Informatie Beveiligings Plan |  |
| **ISMS** | Information Security management System |  |
| **MEP** | Managed Endpoint Protection |  |
| **MSS** | DXC’s portfolio of Managed Security Services |  |
| **PAM** | Privilege Account Management |  |
| **PDXC** | Platform DXC | Hardware Platform |
| **SBB** | Solution Building Block |  |
| **SECMON** | Security monitoring |  |
| **SIEM** | Security Incidents and Event management |  |
| **SIP AMG** | Systeem Integratie API Management Gateway” |  |
| **SME** | Subject matter expert |  |
| **SPCM** | Server policy and compliance monitoring |  |
| **TCM** | Technology compliance management |  |
| **WEC** | Windows Event Collector |  |

# Appendix F: Legenda

## Legenda Context Diagram



## Legenda System Diagram

