

HLD – Werk.nl\_database\_copy

Version: 1.3

Date: 09 May 2022

Confidentiality

This document has been prepared by DXC. The contents are confidential and must not be communicated in whole or in part to any other party without the prior written approval of DXC.

No copy or other reproduction, other than for the purpose of evaluation of this document, shall be made in whole or in part without the prior written permission of DXC.

The following notice applies to this document and shall be reproduced on any permitted copies

Copyright © 2021 DXC. All rights reserved

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](#_Toc102987261)

[1.1 Introduction 4](#_Toc102987262)

[1.2 Application use cases 4](#_Toc102987263)

[1.3 Out of Scope 4](#_Toc102987264)

[2 Architecture 5](#_Toc102987265)

[2.1 Conceptual 5](#_Toc102987266)

[2.2 System Context 6](#_Toc102987267)

[3 Functional Requirements 11](#_Toc102987268)

[4 Non-Functional Requirements 14](#_Toc102987269)

[4.1 Security & Compliance classifications 14](#_Toc102987270)

[4.2 Capacity and Performance (Volumetrics) 14](#_Toc102987271)

[4.3 Availability 15](#_Toc102987272)

[4.4 Security requirements 15](#_Toc102987273)

[4.5 System management 15](#_Toc102987274)

[4.6 Backup and Recovery 15](#_Toc102987275)

[4.7 Storage replication 15](#_Toc102987276)

[4.8 Scalability 15](#_Toc102987277)

[4.9 Disaster Recovery 15](#_Toc102987278)

[4.10 Technical Constraints 15](#_Toc102987279)

[4.11 DXC TAB requirements 16](#_Toc102987280)

[5 Solution 17](#_Toc102987281)

[5.1 Architectural Decisions 17](#_Toc102987282)

[5.2 Solution Overview 18](#_Toc102987283)

[5.3 System Diagram Production Environment 19](#_Toc102987284)

[5.4 System Diagram (OTA) 19](#_Toc102987285)

[5.5 SBB’s 19](#_Toc102987286)

[5.6 Load balancers 19](#_Toc102987287)

[5.7 Deviations from standards 20](#_Toc102987288)

[5.8 Licenses 20](#_Toc102987289)

[5.9 Service Management 20](#_Toc102987290)

[5.10 Security 20](#_Toc102987291)

[6 Potential future improvements 21](#_Toc102987292)

[Appendix A: Technology and Sizing 22](#_Toc102987293)

[Appendix B: Network Protocol Matrix 23](#_Toc102987294)

[Appendix C: Users and Groups 24](#_Toc102987295)

[Appendix D: Security 26](#_Toc102987296)

[Appendix E: Glossary 28](#_Toc102987297)

[Appendix F: Legenda System Diagram 29](#_Toc102987298)

[Appendix G: Control 30](#_Toc102987299)

# Application Overview

## Introduction

Werk.nl\_database\_copy is a solution that provides a copy of the Werk.nl operational Production data for the execution of queries. Having a query database avoids that the Werk.nl Online Transaction Processing (OLTP) database is impacted negatively in terms of performance, response times or stability. Potentially in the future multiple parties can access the Werk.nl information by querying the database\_copy without disturbing the operation.

The data in the WEDOK database will be kept up to date from the Werk.nl primary database (WEDO) by using Oracle DataGuard with only a short synchronization delay.

This design includes:

* an active Oracle database copy for Acceptance and Production environments
* data synchronization to the active database copy from the Werk.nl database for Acceptance and Production environments
* relocation of the interface to OBI (Oracle Business Intelligence) for Acceptance and Production environments from the primary Werk.nl database to the Werk.nl\_database\_copy (WEDOK) database, to allow OBI to run its queries against the database copy
* relocation of the DWH (Data Warehouse) interface from the primary Werk.nl database to the Werk.nl\_database\_copy (WEDOK) database.

## Application use cases

No use cases known to DXC.

## Out of Scope

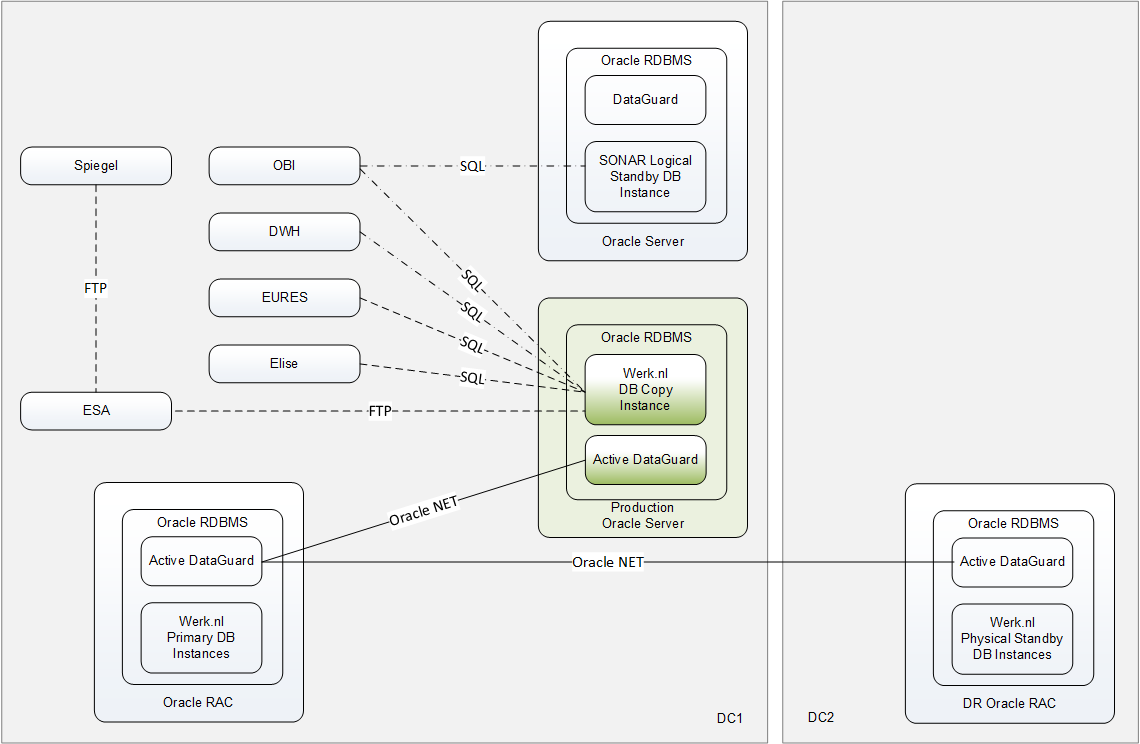
All components that belong to the UWV Office Infrastructure such as workstations, web browsers are out of scope.

Relocation of the Spiegel interface from Werk.nl primary database to the Werk.nl\_database\_copy (WEDOK) database.

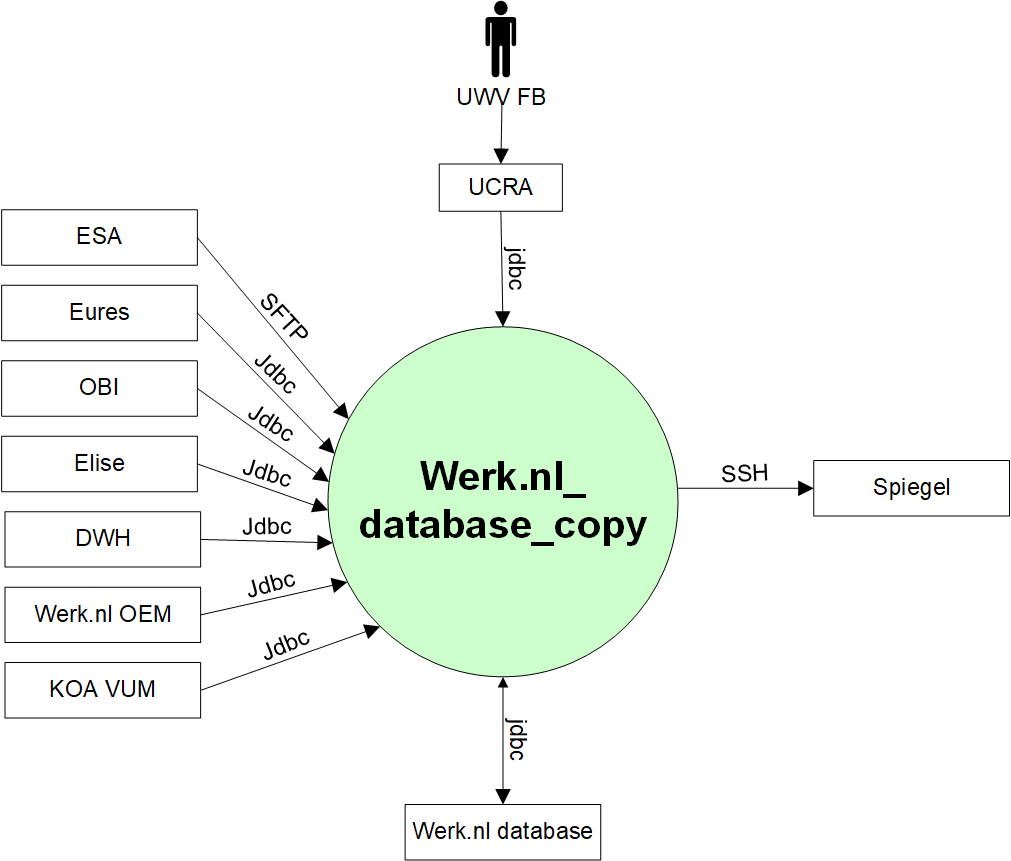
# Architecture

## Conceptual

The solution for Production environment outline is depicted below:



## System Context



### External Entities

#### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV FB, functional maintenance generates reports and manages the postcode data. |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal (UCRA -> Werk.nl\_database\_copy) |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Not specified |
| **Number of users** | 5 - 10 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Werk.nl database

|  |  |
| --- | --- |
| **Description** | Werk.nl Primary database (on the 3-node Oracle RAC cluster) |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming and outgoing |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Continuous updates to the database copy with a maximum delay of 15 minutes |
| **Volume of data** | WEDO instance has 1.7 TB // there are documents in the database that consume a lot of space |

#### Spiegel

|  |  |
| --- | --- |
| **Description** | Werk.nl\_datbase\_copy connection to Spiegel |
| **Protocol and Port** | SSH (22) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outgoing |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | 1-2 |
| **Number of transactions** | Several files |
| **Frequency of transactions** | Weekly |
| **Volume of data** | Medium, several 100MB |

#### ESA

|  |  |
| --- | --- |
| **Description** | ESA to Werk.nl\_database\_copy |
| **Protocol and Port** | SFTP (22) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Eures

|  |  |
| --- | --- |
| **Description** | Eures retrieves job vacancies and CVs from the copy database. |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | A scheduled extract once a day |
| **Volume of data** | Not specified |

#### OBI

|  |  |
| --- | --- |
| **Description** | Oracle Business Intelligence (OBI)  OBI implements the interface with a database link that is initiated from the OBI side and directly links into the WEDOK database. |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | A scheduled extract once a day |
| **Volume of data** | Not specified |

#### Elise

|  |  |
| --- | --- |
| **Description** | EDR failover connection for Elise to retrieve job vacancies, CVs, profession and education from the copy database |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### DWH

|  |  |
| --- | --- |
| **Description** | DataWarehouse wants to extract data from WEDOK on a weekly basis.  UWV Security (CISO Officer) and UWV Legal (Data Privacy Officer) have given permission to DWH to extract data from the following database schema: BSA\_OWNER, EIN\_DIGID, REG\_OWNER, SBI\_OWNER, SCA\_OWNER, SCV\_OWNER, SGO\_OWNER, SVG\_OWNER, SWP\_OWNER, SWR\_OWNER, SZT\_OWNER, VWS\_OWNER, SKB  For large tables these extracts will be incremental based on the date of last modification (if available). Small tables will be extracted as a whole (full).  DWH implements the interface with a database link that is initiated from the DWH side and directly links into the WEDOK database.  Note:the current Werk.nl-DWH interface is implemented with file transfers over SIP (System Integration Platform). The interface runs on Mondays at 05.00 hours. |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming |
| **Direct connection** | yes |
| **Security Controls** | the use of unencrypted communication is tolerated |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Once a week |
| **Volume of data** | Not specified |

#### Werk.nl OEM

|  |  |
| --- | --- |
| **Description** | Cloud Control solution for functional monitoring |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **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, resumes and profiles to exchange that with external parties. |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Incomming |
| **Direct connection** | Yes |
| **Security Controls** | Authorization method: Database account in the Werk.nl\_database\_copy |
| **Number of users** | 1 |
| **Number of transactions** | Daily scheduled retrieval of profiles |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not specified |

# Functional Requirements

**Werk.nl data must be made available for querying**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 01 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
| **Reach** | Local |  |  |
| **Requirement** | The copy database must be made available for querying. | | |
| **Description** | The copy database that is synchronized from the primary database must be opened for querying. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**Application queries must be scheduled**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 02 | **Necessity** | Optional |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
| **Reach** | Local |  |  |
| **Requirement** | UWV must manage all applications that run queries against the copy database to prevent multiple queries | | |
| **Description** | UWV must manage when what application runs which query to ensure that the environment has a predictable workload. Ad-hoc queries must be prevented. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**Applications have their own database account that gives read-only access**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 03 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
| **Reach** | Local |  |  |
| **Requirement** | Each application that wants to read data must have its own database account. | | |
| **Description** | Each application must be identifiable to support tracking & tracing of workload. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**All schemas of Werk.nl WEDO database must be accessible in read-only mode**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 04 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
| **Reach** | Local |  |  |
| **Requirement** | All schemas in the copy database must be accessible in read-only mode.  Note that access to all schemas depends on the security permission given to a specific WEDOK client. | | |
| **Description** | Clients must be able to read data from all schemas in the copy database. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**Changes to the primary Werk.nl database (like Create, Update, Delete tables) must automatically become available in the copy database**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 05 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
| **Reach** | Local |  |  |
| **Requirement** | The copy database must follow the primary database regarding changes in Data Definition Language (DDL) that are applied to the primary database. | | |
| **Description** | The changes (tables, views, and other database objects) that are applied on the primary database must also be applied to the copy database. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**Applications may access the WEDOK copy database via an Oracle DB-link**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 06 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Optional |
| **Reach** | Local |  |  |
| **Requirement** | Applications may use an Oracle database link as connection method between the application database and the copy database. | | |
| **Description** | Applications may use an Oracle database link to connect their database to the copy database. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**Applications may extract incremental data**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 07 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Optional |
| **Reach** | Local |  |  |
| **Requirement** | Applications may extract incremental data based on the date of last modification. The increments are daily. | | |
| **Description** | Applications may extract incremental data. The date of last modification (field in a table) will be used for this purpose. This may require changes to the source tables, as the copy database is a one-to-one copy of the source data. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**Maximum delay for data in copy database**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 08 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
| **Reach** | Local |  |  |
| **Requirement** | The maximum delay for data to become available in the copy database is set at 15 minutes. | | |
| **Description** | Applications require a pseudo online view on the WEDO operational data. Therefore, the copy copy must not be lagging more than this interval. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

**Applications may extract Full data**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 09 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
|  |  |  |  |
| **Reach** | Local |  |  |
| **Requirement** | Applications may extract all rows (full data).  Note that this may have impact on performance or response times as there are huge tables involved. | | |
| **Description** | An application may extract huge tables. | | |
| **Supporting SBBs** | Werk.nl\_database\_copy | | |

# Non-Functional Requirements

## Security & Compliance classifications

Not available in list “2019 Risico Applicatie Lijst v1.1” or “2020 UWV-brede Risico Applicatie Lijst v1.0”.

|  |  |
| --- | --- |
| **Application** | WEDOK (Werk.nl\_database\_copy) |
| **Owner** | WB |
| **Availability (Beschikbaarheid)** | Not specified |
| **Integrity (Integriteit)** | Not specified |
| **Confidentiality (Vertrouwelijkheid)** | 2+ |
| **Type of information /Data Classification** | Not specified |
| **Direct or Indirect part of the primary information chain** | Not specified |

The following assumption is made and agreed with UWV PM: Data is a copy for the Werk.nl DB, so the same confidentiality classification (2+) is used as for the original data.

### Risk Analysis UWV

No risk analysis provided by UWV.

### Applicable security and compliance frameworks

|  |  |
| --- | --- |
| Security & Compliance Framework | Applicable |
| BIR 2017 | Yes |
| AVG / GDPR | Yes |
| DIGID | No |
| SUWI | No |
| Additional frameworks | Not specified |

## Capacity and Performance (Volumetrics)

**Storage size must be identical with WEDO size**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 01 | **Necessity** | Essential |
| **Status (Input)** | Approved | **Status (Output)** | Satisfied |
| **Reach** | Local |  |  |
| **Requirement** | As WEDOK must have a storage size that is identical to the Werk.nl WEDO database because it is a physical copy database. | | |
| **Description** | All information from the WEDO database will be synchronized to the physical copy database. | | |
| **Supporting SBBs** | SBB-WEDOK-01 | | |

## Availability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Environment** | **Application Target** | **Application Service Hours** | **Infra Target** | **Infra Service Hours** |
| Production | 98% | 5 x 12 (Mo-Fr, 7-19h) | 99.5% | 7 x 24 |
| Acceptance | 98% | 5 x 12 (Mo-Fr, 7-19h) | 98% | 5 x 12 (Mo-Fr, 7-19h) |

## Security requirements

User accounts must be created on the primary server and will be propagated to the copy database. Some users will have access to the primary database and will also automatically get access to the copy database.

Some WEDOK applications are only allowed to have read access to the copy database. WEDOK applications must have a user account on the copy database. Some users that have access to the copy database must not be able to logon on the primary database.

User and application access to WEDOK must be approved by UWV Security.

Database access is only allowed for DXC Database Administrators (DXC DBA). UWV FB may use Oracle SQLDeveloper or other tools to access the WEDOK copy database.

Detailed security requirements are documented in Appendix D

## System management

No specific system management requirements are applicable

## Backup and Recovery

No database backup is required, restore must be done by recreating the copy database from the Werk.nl primary database using Oracle Data Guard.

## Storage replication

|  |  |
| --- | --- |
| **Environment** | **Storage type** |
| Production | Replicated |
| Acceptance | Not replicated |

## Scalability

To support the application growth the system must be vertical scalable

## Disaster Recovery

No specific disaster recovery requirements are applicable.

## Technical Constraints

No technical contrains.

## DXC TAB requirements

|  |  |
| --- | --- |
| **Category** | **Description** |
| Deployment | * jdbc (1521) connection from Werk.nl TAB deployment to the Werk.nl\_database\_copy is required |
| Other TAB applicable requirement | * jdbc (1521) connection from Werk.nl OEM to the Werk.nl\_database\_copy is required |

# Solution

## Architectural Decisions

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 01 | **Topic** | Infrastructure |
| **Status** | Approved | **Subject Area** | Servers |
| **Decision** | The system will be deployed on virtual servers for Production and Acceptance | | |
| **Problem Statement** |  | | |
| **Assumptions** | Oracle databases with ‘single RDBMS installations’ and ‘Oracle databases with active Data Guard’ will have the Private Cloud Oracle Database as landing zone | | |
| **Motivation** |  | | |
| **Alternatives** |  | | |
| **Justification** |  | | |
| **Implications** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 02 | **Topic** | Infrastructure |
| **Status** | Approved | **Subject Area** | Servers |
| **Decision** | The virtual servers will run on Oracle RDBMS cluster | | |
| **Problem Statement** | The servers run on virtual servers (see 01). | | |
| **Assumptions** | The capacity of the Oracle RDBMS cluster fit the WEDOK requirements. | | |
| **Motivation** | The servers need a VMWare host Server to run on. | | |
| **Alternatives** |  | | |
| **Justification** | It is expected that the available Oracle RDBMS cluster have sufficient capacity. | | |
| **Implications** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 03 | **Topic** | Availability |
| **Status** | Approved | **Subject Area** | Data Guard protection mode |
| **Decision** | Data Guard in maximum performance protection mode | | |
| **Problem Statement** | The selected Data Guard Mode has a direct relation to Recovery Point Objectives (RPO) and performance. | | |
| **Assumptions** |  | | |
| **Motivation** | Multiple Data Guard modes exist | | |
| **Alternatives** |  | | |
| **Justification** | WEDOK is positioned as a query database. It is therefore best to use maximum performance mode. | | |
| **Implications** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 04 | **Topic** | Application configuration |
| **Status** | Approved | **Subject Area** | Implementation techniques (IT) |
| **Decision** | UWV FB use UCRA for their administrative tasks | | |
| **Problem Statement** |  | | |
| **Assumptions** |  | | |
| **Motivation** | UCRA is the standard method for UWV FB to access the application in case this is required | | |
| **Alternatives** |  | | |
| **Justification** | Use the standard solutions as much as possible | | |
| **Implications** | Access to the UCRA environment through UWV WPOL AD group  Access to the DB is possible only via personal accounts | | |

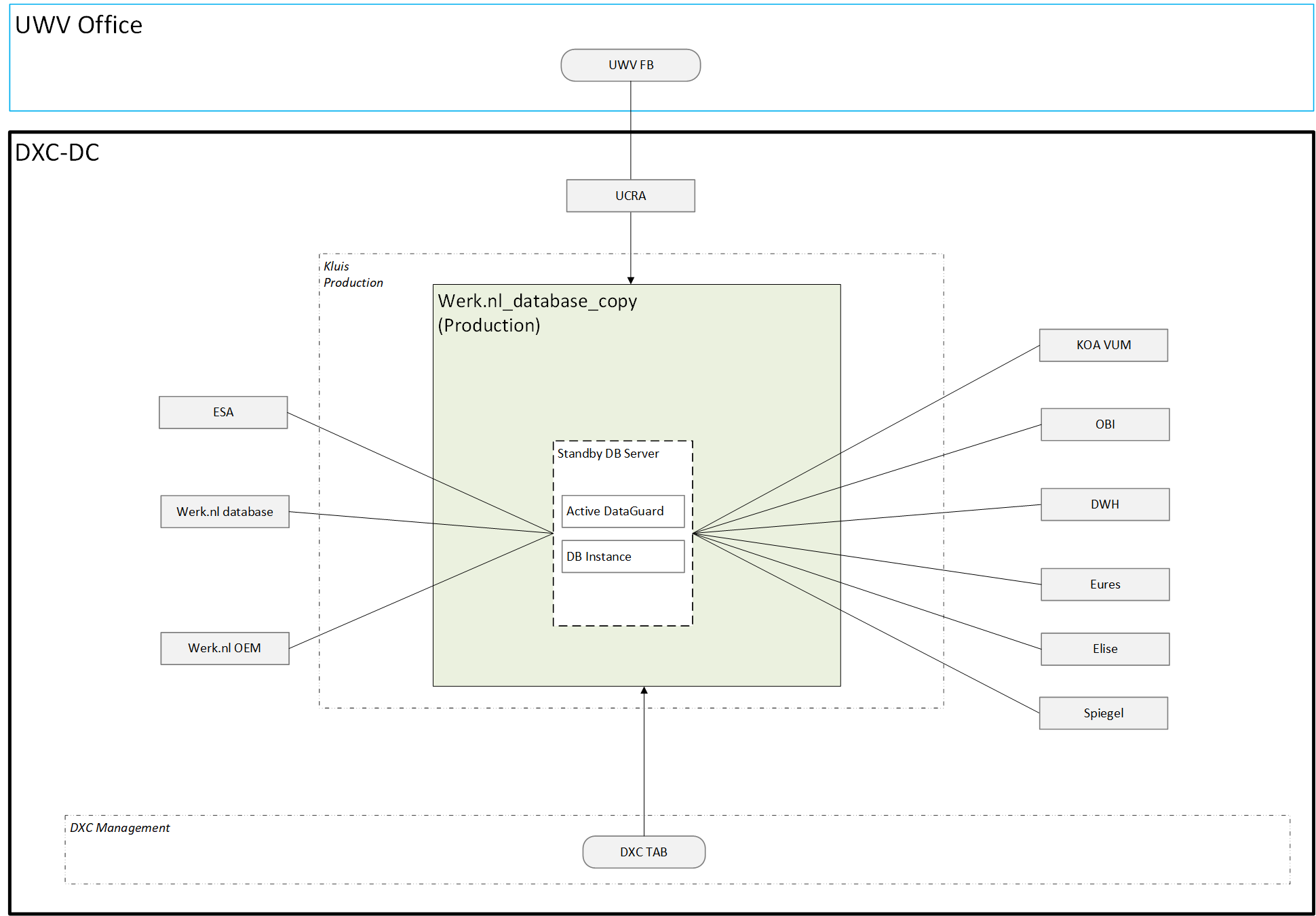
|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 05 | **Topic** | Network |
| **Status** | Approved | **Subject Area** | Security Zone |
| **Decision** | Werk.nl\_database\_copy will be placed in the kluis security zone | | |
| **Problem Statement** |  | | |
| **Assumptions** | The BIV rating was not found in the UWV provided classification sheet. We assumed that the confidentiality classification for the database copy is the same as for the original database which is 2+ | | |
| **Motivation** | According the agreed security baseline the data for applications with confidentiality classification 2+ or higher must go to the kluis security zone | | |
| **Alternatives** |  | | |
| **Justification** |  | | |
| **Implications** | The kluis uses micro segmentation this means that all connections from and to the system must be approved | | |

## Solution Overview

See chapter 2.1

## System Diagram Production Environment

System Diagram of the Production environment and node descriptions.



### Node descriptions and zone-projections

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Zone** | **Environment** | **Node** | **Infra Service Level** |
| Kluis | Production | Database Server 1 | Silver |
| Kluis | Acceptance | Database Server 1 | Bronze |

### DNS

The customer facing DNS name for this application is: **WEDOK.\*-dc.ba.uwv.nl**

Production: **WEDOK.P-dc.ba.uwv.nl**

Acceptance: **WEDOK.A-dc.ba.uwv.nl**

## System Diagram (OTA)

System diagram for Acceptance is the same as for Production, therefore no separate diagram is provided.

## SBB’s

IaaS Plus - VM- DXC Managed

PaaS - Virtual Oracle database - DXC Managed

## Load balancers

No load balancers are used.

## Deviations from standards

The solution does not deviate from the DXC and UWV agreed standards

### Risk Acceptance Letter / Exception to Policy

| **Nr** | **Short description of the deviation** | **Name of the Risk Letter document** |
| --- | --- | --- |
| 1 | UCRA (FrontOffice) connection to Database server (Kluis) | 20210616-001 |

## Licenses

Oracle Database EE 12.2.0.1

Oracle Active Data Guard 12c

Oracle Grid control agent 13.4.0.0

## 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”.

### Authentication and Authorization

For UCRA:

Standard (LDAP - UWV AD group nested in DXC AD group - using the trust): User Authentication and Authorization will be performed against the UWV AD using nested groups, as per standard design.

For database access:

Deviation3 (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.

### 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.

* No firewalls reside in between nodes in the same network security zone.
* Connections, like interfaces, coming from outside the network security zone do cross one or more firewalls.

Copy DB server will be placed in Production Kluis zone (eventually Acceptance Kluis zone). All connections to that zone require access throught firewall.

For firewall requests and details see Appendix B.

# Potential future improvements

* UWV to identify the owner of the Werk.nl\_database\_copy and set clear privileges for all parties, who requires to the access data

# Appendix A: Technology and Sizing

***Nodes:***

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **Location** | **Environment Zone** | **Node Description** | **vCPU** | **RAM (GB)** | **OS** | **SBB Type /SLA** | **Storage Replication** |
| Private Cloud Oracle DB | Kluis | AM3 | Production | Database Server 1 UWVA3VLPORA0001 | 2 | 32 | RHEL 7.9 | VM IaaS+ Silver | Yes |
| Private Cloud Oracle DB | Kluis | AM2 | Acceptance | Database Server 2 UWVA2VLAORA0002 | 2 | 32 | RHEL 7.9 | VM IaaS+ Bronze | Yes |

***Storage:***

*Oracle Database server(s)*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Server / 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** |
| Database Server 1 / P UWVA3VLPORA0001 | 100 GB | 100 GB | 100 GB | 1,1TB  (2x500 + 100GB) | 1,1TB  (2x500 + 100GB) | 250 GB | 250 GB |
| Database Server 2/ A UWVA2VLAORA0002 | 100 GB | 100 GB | 100 GB | 1,1TB  (2x500 + 100GB) | 1,1TB  (2x500 + 100GB) | 250 GB | 250 GB |

***Software:***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported by vendor** | **Support contract** | **Latest version (N, N-1)** |
| Server-name | 1-OS | RHEL | 7.9 | Y | detials | Y |
| Server-name | 3-Database | Oracle database server | 12.2.0.1.0 | Y | details | Y |
| Server-name | 4-Middleware | Oracle Automatic Storage Manager ASM | 19 | Y | details | Y |
| Server-name | 4-Middleware | Oracle Clusterware CRS | 19 | Y | details | Y |
| Server-name | 4-Middleware | Oracle Data Guard | 12 | Y | details | Y |
| Server-name | 5-Application | Oracle Grid control agent | 13.4.0.0 | Y | details | Y |

***Load Balancers:***

N/A

# Appendix B: Network Protocol Matrix

*The DXC firewall is used to protect access to the WEDOK.*

*The following ports must be opened in the Firewall to allow access using the database link:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DWH | WEDOK servers | DB link | 1521 |  |
| OBI | WEDOK servers | DB link | 1521 |  |
| EURES | WEDOK servers | DB link | 1521 |  |
| Elise | WEDOK server | DB link | 1521 |  |
| ESA File server | WEDOK servers | SCP SSH | 22 |  |
| Oracle RAC servers | WEDOK servers | DB link | 1521 |  |
| KOA VUM | WEDOK server | DB link | 1521 |  |

Connectivity sheet 1.3



# Appendix C: Users and Groups



**User accounts to UCRA**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **UWV** | | **DXC** | |  |
| **Environment** | **Domain** | **Group** | **Domain** | **Group** | **Description** |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-WEDOK | P-dc.ba.uwv.nl | L-RG-UWV-P-WEDOK | Access from UCRA to WEDOK |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-WEDOK | A-dc.ba.uwv.nl | L-RG-UWV-A-WEDOK | Access from UCRA to WEDOK |

**Local user accounts**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **User role** | **User permissions** | **ABS Role** | **Application /Server** | **DXC Solution Group** | **Description** |
| DB user | Read access to WEDOK | Read access to WEDOK | WEDOK DB (A, P) | DXC TAB | UWV FB Database access to WEDOK |

***Service Accounts:***

|  |  |  |  |
| --- | --- | --- | --- |
| **Account** | **Domain** | **Permissions** | **Description** |
| svc\_dblink\_dwh | P-dc.ba.uwv.nl | Establish read-only DB connection to WEDOK | DB user for DWH access to WEDOK |
| svc\_dblink\_obi | P-dc.ba.uwv.nl | Establish read-only DB connection to WEDOK | DB user for OBI access to WEDOK |
| svc\_dblink\_eures | P-dc.ba.uwv.nl | Establish read-only DB connection to WEDOK | DB user for EURES access to WEDOK |
| svc\_koavum\_wnlcopy\_P | P-dc.ba.uwv.nl | Establish read-only DB connection and VUM views to WEDOK | DB user for KOA VUM access to WEDOK |
| svc\_dblink\_dwh | A-dc.ba.uwv.nl | Establish read-only DB connection to WEDOK | DB user for DWH access to WEDOK |
| svc\_dblink\_obi | A-dc.ba.uwv.nl | Establish read-only DB connection to WEDOK | DB user for OBI access to WEDOK |
| svc\_dblink\_eures | A-dc.ba.uwv.nl | Establish read-only DB connection to WEDOK | DB user for EURES access to WEDOK |
| svc\_koavum\_wnlcopy\_A | A-dc.ba.uwv.nl | Establish read-only DB connection and VUM views to WEDOK | DB user for KOA VUM access to WEDOK |

# Appendix D: Security

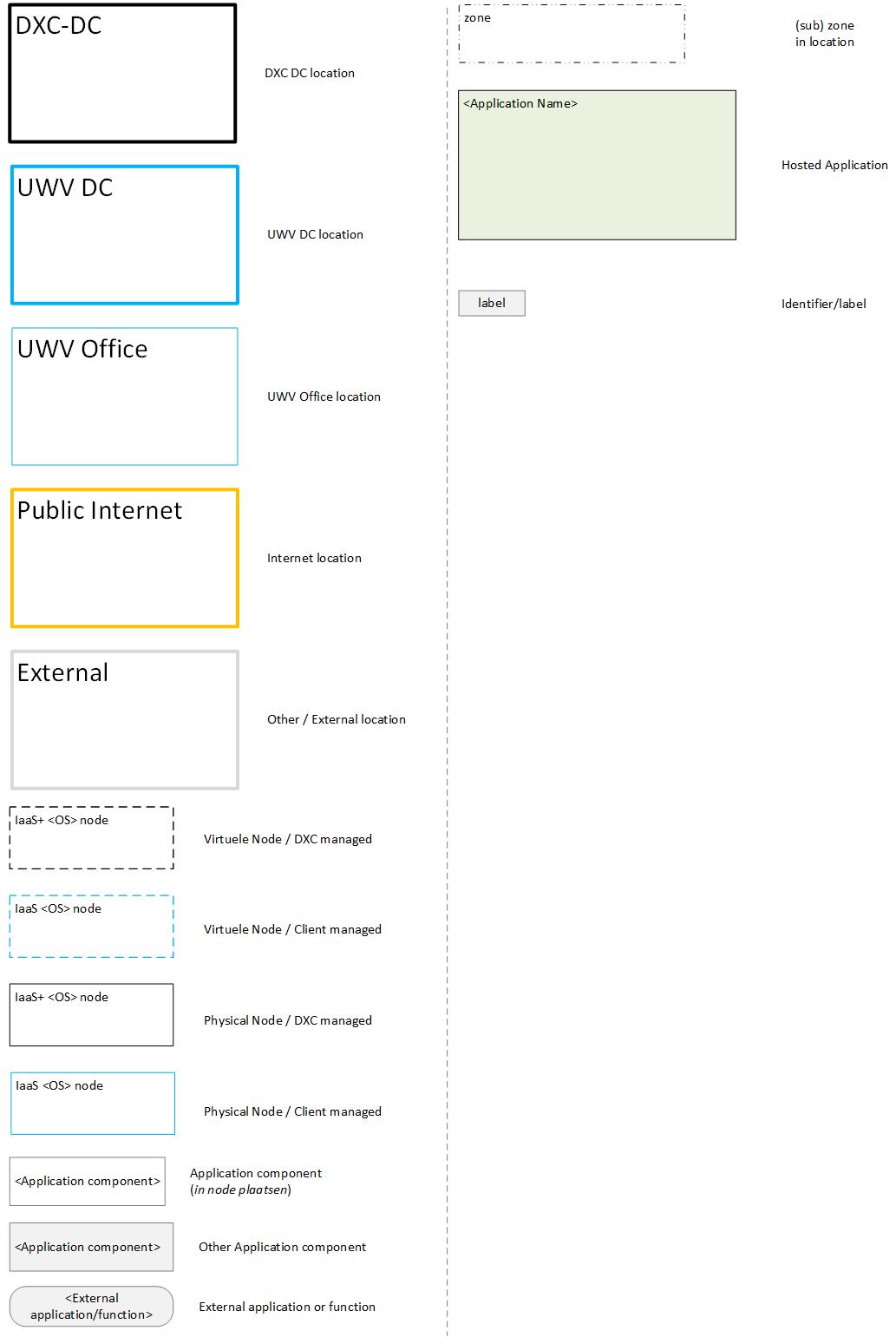
| Security & Compliance requirement | Deviations from the standard | Implementation of the requirements |
| --- | --- | --- |
| Authorization | Applicable | See Chapter 5.10.1 and Appendix C |
| OS hardening | No deviations required | N/A |
| Additional Middleware / database security configuration settings | No deviations required | N/A |
| Firewall ports (GRIP SSD-1) | Applicable | See Chapter 5.10.2 and Appendix B |
| UWV Admin / console interface  (GRIP SSD-17) | Applicable | Admin console available: Yes |
| Limit HTTP header information  (GRIP SSD-24) | Not applicable | N/A |
| Limit HTTP methods  (GRIP SSD-26) | Not applicable | N/A |
| Disable Directory Listing  (GRIP SSD-29) | N/A | N/A |
| TLS/SSL Certificates | No TLS/SSL is used | N/A |
| Session Encryption - HTTPS  (GRIP SSD-4) | No HTTPs is used | N/A |
| Session Encryption – SFTP  (GRIP SSD-4) | SFTP | N/A |
| Session Encryption – TLS version (GRIP SSD-4) | No TLS/SSL is used | N/A |
| Security of Data in Transit External | N/A | N/A |
| Security of Data in Transit Internal | No deviations | N/A |
| Segregation in security zones for Production | No deviations | See Appendix A |
| Segregation of Development, Test, Acceptance and Production environment | No deviations | See Appendix A |
| All software used must be supported by the vendor | No deviations | See Appendix A |
| Malware protection | No deviations | N/A |
| Security Logging and -Monitoring | No deviations | 1 year |

# Appendix E: Glossary

Glossary of terms used in this HLD.

|  |  | **Notes** |
| --- | --- | --- |
| **ASO** | Account Security Officer |  |
| **CMO** | Current Mode of Operation refers to the old situation at IBM |  |
| **DXC managed systems** | All systems in the datacenters where DXC is responsible for |  |
| **EoS** | End of Support |  |
| **MSS** | DXC’s portfolio of Managed Security Services |  |
| **SBB** | Solution Building Block |  |
| **PDXC** | Platform DXC |  |
| **CVA** | Customer Virtual Appliance |  |
| **GRC** | Governance risk and compliance |  |
| **SPCM** | Server policy and compliance monitoring |  |
| **TCM** | Technical compliance monitoring |  |
| **SECMON** | Security monitoring |  |
| **MEP** | Managed Endpoint Protection |  |
| **PAM** | Privilege Account Management |  |
| **IBP** | Informatie Beveiligings Plan |  |
| **ASP** | Account Security Plan |  |
| **ISMS** | Information Security management System |  |
| **WEC** | Windows Event Collector |  |
| **DXC management REALM** | Management network of DXC dedicated for UWV in Amsterdam DC’s |  |
| **CI** | Configuration Item |  |
| **CIs** | Configuration Items |  |
| **SME** | Subject matter expert |  |
| **TCM** | Technology compliance management |  |
| **IBP** | Informatie beveiligings plan |  |
| **SIEM** | Security Incidents and Event management |  |
| **(s)FTP** | Secure File Transfer Protocol - SSH |  |
| **FTPs** | File Transfer Protocol - SSL |  |

# Appendix F: Legenda System Diagram



# Appendix G: Control

**DOCUMENT AUTHORISATION**

| Name | Role | Date |
| --- | --- | --- |
| Cora Kuijper | DXC Technical Transformation Lead (verification) | 13-04-2021 |
| Andre Koppenol | UWV Lead Architect (verification) |  |
| Joep Pelle (delegated to Hans Kreisel) | DXC Account Delivery Lead (acceptance) | 16-04-2021 |

**DOCUMENT DISTRIBUTION**

| Name | Role | Date |
| --- | --- | --- |
| As per agreed PMO process |  |  |
| UWV Design Office | Design authority |  |

**CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Summary of Changes |
| SharePoint version 0.2 | 25-08-2020 | DXC architecture team | First iteration of the HLD |
| SharePoint version 0.3 | 28-01-2021 | DXC architecture team | Second iteration of the HLD VI  Updated all pictures, connections |
| SharePoint version 0.5 | 11-02-2021 | DXC architecture team | Ready for first UWV review |
| SharePoint version 0.7 | 31-03-2021 | DXC architecture team | Updates after first UWV review |
| Verification version 0.8 | 13-04-2021 | DXC architecture team | Third iteration of the HLD |
| Verification version 0.9 | 16-04-2021 | DXC architecture team | Design Office verification |
| Version 1.0 | 21-04-2021 | DXC architecture team | Positive verified HLD |
| Version 1.1 | 17-01-2022 | DXC architecture team | Post implementation HLD   * Updated Context diagram according connectivity sheet * Added DXc TAB requirements (4.11) * System diagram updated (according contect diagram) * Connectivity sheet added to Appendix B |
| Version 1.1.1 | 02-03-2022 | DXC architecture team | Updated Appendix A with servernames |
| Version 1.2 | 18-03-2022 | DXC architecture team | Finalized |
| Version 1.3 | 09-05-2022 | DXC architecture team | Updates for change CHG0049063. Connectivity KOA VUM and WEDOK.  Update 1 – Include connection with VUM KOA in chapter 2.2, 5.3, Appendix B and Appendix C |