

HLD – Werkverkenner

Version: 1.1

Date: 17 january 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](#_Toc93322603)

[1.1 Introduction 4](#_Toc93322604)

[1.2 Application use cases 4](#_Toc93322605)

[1.3 Out of Scope 4](#_Toc93322606)

[2 Architecture 5](#_Toc93322607)

[2.1 Conceptual 5](#_Toc93322608)

[2.2 Context Diagram 6](#_Toc93322609)

[3 Functional Requirements 9](#_Toc93322610)

[4 Non-Functional Requirements 10](#_Toc93322611)

[4.1 Security & Compliance classifications 10](#_Toc93322612)

[4.2 Capacity and Performance (Volumetrics) 10](#_Toc93322613)

[4.3 Availability 11](#_Toc93322614)

[4.4 Security requirements 11](#_Toc93322615)

[4.5 System management 11](#_Toc93322616)

[4.6 Backup and Recovery 11](#_Toc93322617)

[4.7 Storage replication 11](#_Toc93322618)

[4.8 Scalability 11](#_Toc93322619)

[4.9 Disaster Recovery 12](#_Toc93322620)

[4.10 Technical Constraints 12](#_Toc93322621)

[4.11 DXC TAB requirements 12](#_Toc93322622)

[5 Solution 13](#_Toc93322623)

[5.1 Architectural Decisions 13](#_Toc93322624)

[5.2 Solution Overview 14](#_Toc93322625)

[5.3 System Diagram Production Environment 15](#_Toc93322626)

[5.4 System Diagram (OTA) 15](#_Toc93322627)

[5.5 SBB’s 15](#_Toc93322628)

[5.6 Load balancers 15](#_Toc93322629)

[5.7 Deviations from standards 15](#_Toc93322630)

[5.8 Licenses 16](#_Toc93322631)

[5.9 Service Management 16](#_Toc93322632)

[5.10 Security 16](#_Toc93322633)

[6 Potential future improvements 17](#_Toc93322634)

[Appendix B: Network Protocol Matrix 20](#_Toc93322635)

[Appendix C: Users and Groups 21](#_Toc93322636)

[Appendix D: Security 22](#_Toc93322637)

[Appendix E: Glossary 24](#_Toc93322638)

[Appendix F: Legenda System Diagram 26](#_Toc93322639)

[Appendix G: Control 27](#_Toc93322640)

# Application Overview

## Introduction

Werkverkenner 1.0 originates from 2011 and is currently deployed as integrated function within Werk.nl. In the period 2014-2015 several UWV clients have received additional questions which has led to an improved calculation model. This model has been further refined. Werkverkenner 2.0 backend is the implementation of this refined calculation model.

UWV clients receive a questionnaire from which a chance of the re-employability is calculated, and additional next steps will be proposed. The processing of the filled-in questionnaires and providing the output of the calculation is the main function of Werkverkenner 2.0 backend.

Werkverkenner 2.0 backend solution will be deployed on dedicated Application and database servers.

The Werkverkenner 2.0 Impact Assessment describes 4 Implementation phases.

1. Werkverkenner 2.0 backend zonder release Sonar.
2. Proces aanmaken taak werkverkenner 2.0 in Sonar (Release)
3. Sonar View op werkverkenner 2.0 resultaten (Release)
4. Uitfaseren Werkverkenner 1.0

Only phase 1 (Werkverkenner 2.0 zonder release Sonar) is included in this solution.

This design only covers the “backend” component of Werkverkenner 2.0.

## Application use cases

* Werkverkenner 2.0 is offered in the MyUWV environment.
* Via My Tasks the customer is offered a URL with which the questionnaire of Werkverkenner 2.0 can be opened.
* The availability of the questionnaire is guaranteed by K&S.
* Questionnaires are sent to the backend in the form of an XML message.
* Then disconnected from the customer interaction process with a Message Queue that can be processed at any other time.

## Out of Scope

* Implementation phases (slice) 2, 3 and 4 are not in scope of this document
* All components that belong to the UWV Office Infrastructure such as workstations, web browsers are explicitly out of scope for this design
* The application is developed in the UWV OTOD environment, the only environments in scope for this design are Acceptance and Production.

# Architecture

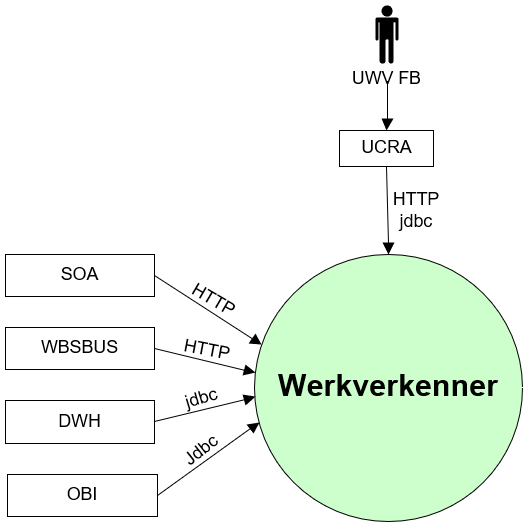
## Conceptual



**Key Concepts:**

* Werkverkenner 2.0 backend processes questionnaire and registration data from UWV clients and returns results in the form of scores for re-employability.
* ESB/SOA provides interface with various UWV applications and performs the actual calculations.
* The Werkverkenner 2.0 backend application communicates via the WBSBUS with all other applications.
* OBIEE retrieves the “Werkverkenner” results per customer and determines urgency and other follow-up actions for the customer and/or the employee of “Werkbedrijf”.
* DWH enables users with appropriate authorization on VIEWS to access “Results” and “Questionnaire/Answers”.
* Werkverkenner Beheer change/update application and business reference data, formulas and “Questionnaire: Practical Tips” in Werkverkenner 2.0.

## Context Diagram



### External entities

#### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV FB, Functionality to change/update Application and business reference data, formulas and “Vragenlijst: Praktische Tips” in Werkverkenner 2.0 |
| **Protocol and Port** | HTTP (8080), jdbc (1526) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### SOA

|  |  |
| --- | --- |
| **Description** | Provides two functions to Werkverkenner   * interfaces with various UWV applications * Performs the actual calculations (“rekenmodule”) on behalf of Werkverkenner |
| **Protocol and Port** | HTTP (8080) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | The connection from the SOA (Werk.nl) is protected by a system-to-system account. |
| **Number of users** | Not specified |
| **Number of transactions** | 350.000 questionnaires processed per year |
| **Frequency of transactions** | 1000 questionnaires processed per day |
| **Volume of data** | Not specified |

#### WBSBUS

|  |  |
| --- | --- |
| **Description** | DRL\_SCORES\_ Werkverkenner   * uwv.nl-drl-WBSBUS-WVK M-WVK BE |
| **Protocol and Port** | HTTP (8080) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | 350.000 questionnaires processed per year |
| **Frequency of transactions** | 1000 questionnaires processed per day |
| **Volume of data** | Not specified |

#### DWH

|  |  |
| --- | --- |
| **Description** | Enables users with appropriate authorization on VIEWS to access “Resultaten” and “Vragenlijst/Antwoorden” |
| **Protocol and Port** | jdbc (1526) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | This is considered as Applications links. Control done on the application |
| **Number of users** | Not specified |
| **Number of transactions** | 350.000 questionnaires processed per year |
| **Frequency of transactions** | 1000 questionnaires processed per day |
| **Volume of data** | Not specified |

#### OBI

|  |  |
| --- | --- |
| **Description** | OBI (Business analytical function) retrieves the “Werkverkenner” results per customer and determines urgency and other follow-up actions for the customer and/or the employee of “Werkbedrijf”. |
| **Protocol and Port** | jdbc (1526) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | This is considered as Applications links. Control done on the application |
| **Number of users** | Not specified |
| **Number of transactions** | 350.000 questionnaires processed per year |
| **Frequency of transactions** | 1000 questionnaires processed per day |
| **Volume of data** | Not specified |

# Functional Requirements

No functional requirements have been specified.

# Non-Functional Requirements

## Security & Compliance classifications

For the BIV Rating the following repostitory is used: “*2019 Risco Applicatie lijst V1.0*”

|  |  |
| --- | --- |
| **Application** | Werkverkenner |
| **Owner** | WB |
| **Availability (Beschikbaarheid)** | 3 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 2 |
| **Type of information /Data Classification** | Customer Personal data |
| **Direct or Indirect part of the primary information chain** | Direct |

Note: The BIV rating in the “*2020 UWV-brede Risico Applicatie Lijst v1.0*” differs (2, 2, 2+).

### 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)

### – Server capacity

The initial capacity is based on the standard UWV Linux Application server deployment. Performance tests after setting up the server Acceptance environment should indicate whether the infrastructure must be up- or downscaled.

The application will be deployed on dedicated virtual server, the following server capacity is required:

* Production: 1 CPU with 4 GB memory
* Acceptance: 1 CPU with 4 GB memory

See Appendix A for details.

## Availability

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

## Security requirements

Access to the tooling must be restricted to authenticated and authorized users using the standard authentication and authorization mechanism.

### Access Management

Security with regards to interactive usage:

* The Werkverkenner 2.0 backend can/will only be triggered from authorized sessions in matter specific systems.
* The only exception to the rule above is the interactive execution of scripts to update/change the formulas and calculations of Werkverkenner 2.0. This requires role-based access to the application folders only and will be executed by DXC TAB.

Security with regards to usage of webservices-processing:

* No specific security requirements.

### Transactional traceability

Transactional traceability can only apply to the Werkverkenner indirectly:

* All external interfaces can be considered application/application links, which implies only derived authorizations can exist.
* Traceability of the scripts to update/change the Werkverkenner 2.0 formulas will need to be done through change management.

Detailed Security requirements are documented in Appendix D.

## System management

No specific system management requirements.

## Backup and Recovery

No specific backup requirements.

## Storage replication

|  |  |
| --- | --- |
| **Environment / System** | **Storage Replication** |
| Production | Yes |
| Acceptance | No |

## Scalability

The solution must be vertical scalable, Werkverkenner 2.0 BE application software determines how well the application scales.

## Disaster Recovery

No specific disaster recovery requirements.

## Technical Constraints

No technical constraints identified.

## DXC TAB requirements

|  |  |
| --- | --- |
| **Category** | **Description** |
| Deployment | * HTTP (8080) connection from Werk.nl TAB deployment to the Werkverkenner application server is required * jdbc (1526) connection from Werk.nl TAB deployment to the Werkverkenner database server is required * SSH (22) connection from XLdeploy to Werkverkenner application server is required |
| Other TAB applicable requirement | * HTTP (80, 8080) connection from Sitescope to the Werkverkenner application server is required for application monitoring |

# Solution

## Architectural Decisions

### Werkverkenner 2.0 application will be deployed on dedicated VM

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 1 | **Topic** | Deployment |
| **Status** | Approved | **Subject Area** | Platform |
| **Decision** | Werkverkenner 2.0 application will be deployed on dedicated VM | | |
| **Problem Statement** | On which platform will Werkverkenner 2.0 backend be deployed? | | |
| **Assumptions** |  | | |
| **Alternatives** |  | | |
| **Implications** | Application will no longer be hosted on an “Application Hotel” | | |

### Werkverkenner 2.0 database will be hosted on dedicated VM

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 2 | **Topic** | Deployment |
| **Status** | Approved | **Subject Area** | Database placement |
| **Decision** | Werkverkenner 2.0 databse will be hosted on dedicated VM | | |
| **Problem Statement** | Where will the database of Werkverkenner 2.0 backend be hosted? | | |
| **Assumptions** |  | | |
| **Alternatives** |  | | |
| **Justification** |  | | |
| **Implications** | Application will no longer be hosted on a “Database Hotel” | | |

### DXC TAB will execute the script to update Werkverkenner 2.0 formulas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | 3 | **Topic** | Security | |
| **Status** | Approved | **Subject Area** | Maintenance | |
| **Decision** | Execution of scripts to update/change the Werkverkenner 2.0 formulas will be done by DXC TAB as part of Change Management. | | | |
| **Problem Statement** | Who will execute the scripts to update/change the Werkverkenner 2.0 backend formulas? | | | |
| **Assumptions** | No Maintenance interface is available on Werkverkenner 2.0 backend. | | | |
| **Motivation** | Security requirements would prevent interactive access by UWV to shared application servers. | | | |
| **Justification** | Execution of the scripts to update/change the Werkverkenner 2.0 backend formulas require elevated privileges on the server. | | | |
| **Implications** | Execution of scripts to update/change the Werkverkenner 2.0 formulas will be done by DXC TAB as part of Change Management. | | |

### Infra service level for production is Bronze

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 4 | **Topic** | Security & compliance classification |
| **Status** | Approved | **Subject Area** | Availability |
| Decision | Infra service level for Production is Bronze (same as CMO) | | |
| Issue or Problem Statement | The BIV rating (availability=3) and the existing infrastructure service level (bronze) are not in line with eachother, however the availability requirement only requests 98%. The availability classification 3 seems to contradict with the infra availability requirement of 98%. | | |
| Alternatives |  | | |
| Justification | Werkverkenner is considered as an AS-IS migration, no change is made to the existing Service Level, but is will be added to the future improvements as something that requires investigation | | |
| Implications | Infra availability for Production is 98%. | | |

### Werkverkenner 2.0 backend Application and database servers will be hosted in the BackOffice security zone.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 5 | **Topic** | Zoning |
| **Status** | Approved | **Subject Area** | Security |
| Decision | WVK 2.0 BE Application and database servers will be hosted in the BackOffice security zone. | | |
| Issue or Problem Statement | Determine the appropriate placement of infrastructure services. | | |
| Alternatives |  | | |
| Justification | The WVK 2.0 BE is an application that performs backend processing. | | |
| Implications | No FW request required for connection between application and database | | |

## Solution Overview

See chapter 2.2 Sytem context for the functional overview of the solution.

## System Diagram Production Environment



### Node descriptions and zone-projections

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Zone** | **Environment** | **Node** | **Infra Service Level** |
| BackOffice | Production | Application Server | Bronze |
| BackOffice | Production | Database Server | Bronze |
| BackOffice | Acceptance | Application Server | Bronze |
| BackOffice | Acceptance | Database Server | Bronze |

### DNS

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

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

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

## System Diagram (OTA)

Acceptance is the same as in Production. O and T do not exist (not in scope).

## SBB’s

IaaS Plus - VM- DXC Managed

PaaS - Virtual Oracle database - DXC Managed

## Load balancers

No load balancers are used in the Werkverkenner 2.0 BE application.

## Deviations from standards

No deviations.

### Risk Acceptance Letter / Exception to Policy

| **Nr** | **Short description of the deviation** | **Name of the Risk Letter document** |
| --- | --- | --- |
| 1 | Apache version 9.037 | 20211214-004 |

## Licenses

Oracle Database 12.2

## Service Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Infra Hosting** | **Database / Middleware Management** | **Technical Application Management** |
| Production | Bronze | 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

User Authentication and Authorization will be performed localy using a user account in the DXC resource domain, this standard for Linux OS access for UWV users requested through the ABS IAM system and changes in PDXC, for details see 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.

* 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.

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 Werkverkenner 2.0 the following is applicable: no internal or external (outside DXC) connections are applicable, for details see Appendix B

# Potential future improvements

* UWV to investigate if the authentication and authorization with OBI and DWH applications can be improved
* UWV to investigate the current BIV rating and if needed align the infrastructure solution (security zones and availability).

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

***Nodes:***

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **Location** | **Environment Zone** | **Node Description** | **vCPU** | **RAM (GB)** | **OS** | **SBB Type /SLA** | **Storage**  **Replication** |
| Private Cloud | Backoffice | AM2 | Production | Werkverkenner Application Server\_P | 1 | 4 | RHEL 7.9 | VM IaaS+/ bronze | Yes |
| Private Cloud - Oracle | Backoffice | AM2 | Production | Werkverkenner Database Server\_P | 2 | 8 | RHEL 7.9 | VM IaaS+/ bronze | Yes |
| Private Cloud | Backoffice | AM3 | Acceptance | Werkverkenner Application Server\_A | 1 | 4 | RHEL 7.9 | VM IaaS+/ bronze | No |
| Private Cloud - Oracle | Backoffice | AM3 | Acceptance | Werkverkenner Database Server\_A | 2 | 8 | RHEL 7.9 | VM IaaS+/ bronze | No |

***Storage:***

*Linux / AIX Application server(s):*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server** | **Disk 0 – Mountpoint 1 OS (mandatory)** | **Disk 1 – Mountpoint 1 App (mandatory)** | **Disk 1 – Mountpoint 2 (optional)** | **Disk 1 – Mountpoint 3 (optional)** | **Disk 2 – Mountpoint 1 (optional)** |
| Werkverkenner Application Server\_P | 100 GB | 50 GB |  |  |  |
| Werkverkenner Application Server\_A | 100 GB | 50 GB |  |  |  |

*Oracle Database server(s):*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Server** | **Disk0 OS (mandatory)** | **Disk1 Oracle Binaries (mandatory)** | **Disk2 ASM Binaries (mandatory)** | **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** |
| Werkverkenner Database Server\_P | 100 GB | 100 GB | 100 GB | 50 GB | 50 GB | 50 GB | 50 GB |
| Werkverkenner Database Server\_A | 100 GB | 100 GB | 100 GB | 50 GB | 50 GB | 50 GB | 50 GB |

***Software:***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported by vendor** | **Support contract** | **Latest version (N, N-1)** |
| Werkverkenner Application Server | 1-OS | Redhat | 7.9 | Y |  | Y |
|  | 4-Middleware | Apache Tomcat | 9.037 | Y |  | Y |
|  | 5-Application | Werkverkenner | 1.0.0.4 | Y |  | Y |
| Werkverkenner Database Server | 1-OS | Redhat | 7.9 | Y |  | Y |
|  | 3-Database | Oracle Database Server | 12.2.0.1.0 | Y |  | Y |
|  | 5-Application | Backend processing database |  | Y |  |  |

***Load Balancers: Not applicable***

# Appendix B: Network Protocol Matrix

*No firewall rules for Werkverkenner 2.0 application.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| n/a |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| n/a |  |  |  |  |

**Note:**

* no internal or external (outside DXC) connections are applicable.
* Internal (inside DXC) connections are documented in the application specific connectivity sheet

Connectivity sheet 1.1



# Appendix C: Users and Groups

***User Authentication and Authorisation:***

**Authentication with local users**

Local users in Linux are not used, a user account is created in P-DC and A-DC for the UWV FB users.

**AD authentication with nested groups (standard)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **UWV** | | **DXC** | |  |
| **Environment** | **Domain** | **Group** | **Domain** | **Group** | **Description** |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-WVK-Management | P-dc.ba.uwv.nl | L-RG-UWV-P-LL-WVK-Management | Access to local Linux group for WVK management. No integratuion UWV wpol AD. |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-WVK-Management | P-dc.ba.uwv.nl | L-RG-UWV-A-LL-WVK-Management | Access to local Linux group for WVK management. No integratuion UWV wpol AD. |

***Service Accounts:*** are maintained in the TBH / TMM (Technisch Beheer Handboek / Technical Maintenance Manual)

# Appendix D: Security

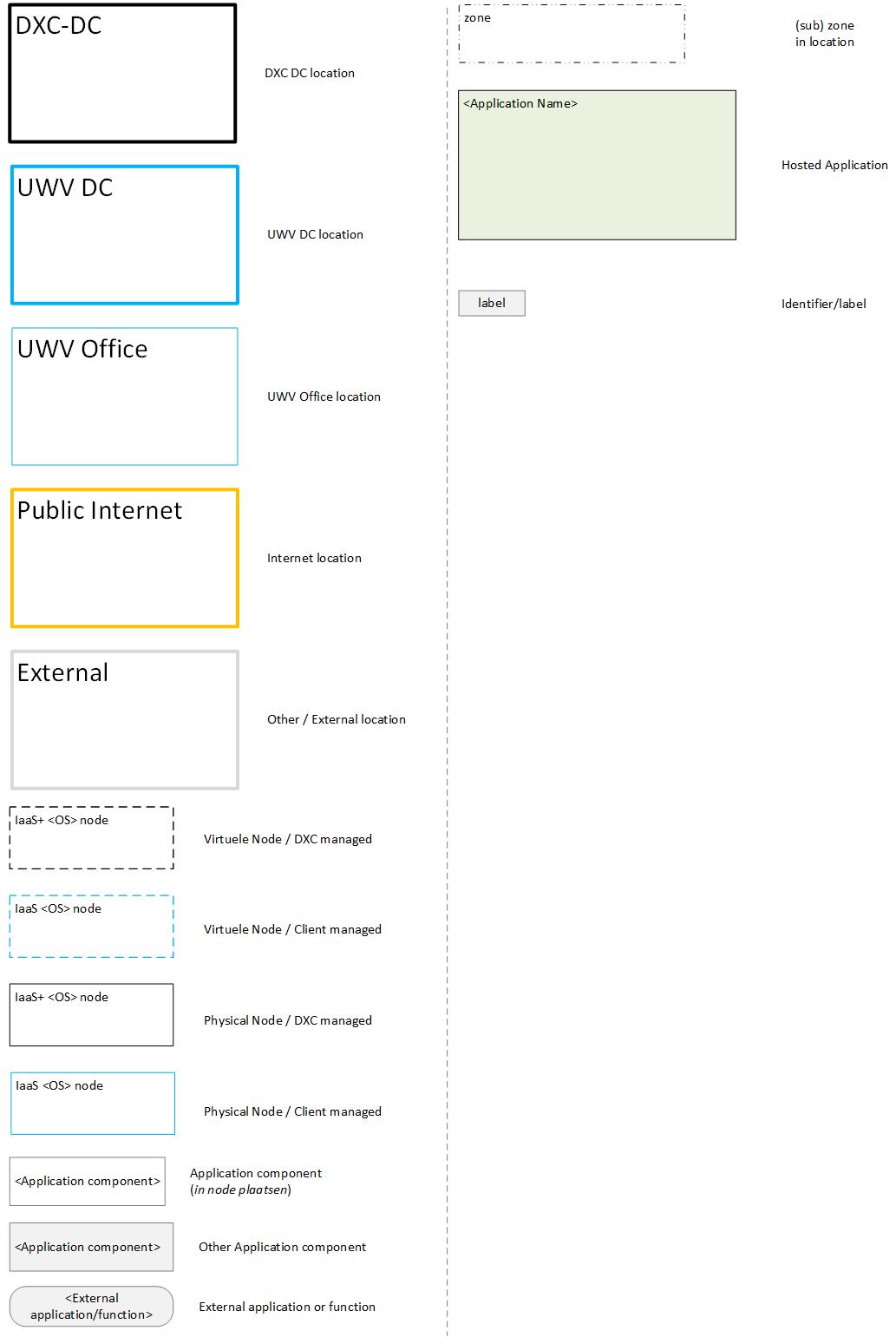
| Security & Compliance requirement | Deviations from the standard | Implementation of the requirements |
| --- | --- | --- |
| Authorization | Applicable | See Chapter 5.10.1 and Appendix C. |
| OS hardening | no deviation required | N/A |
| Additional Middleware / database security configuration settings | no deviation 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: HTTP over UCRA |
| Limit HTTP header information  (GRIP SSD-24) | Applicable. | HTTP header information must be limited to the bare minimum.  The HTTP header must not contain information such as  1) webserver software and version and  2) show detailed error messages |
| Limit HTTP methods  (GRIP SSD-26) | Applicable. | All non relevant http method information must be removed. By default, only GET and POST are allowed |
| Disable Directory Listing  (GRIP SSD-29) | Applicable | Directory listing is disabled. |
| TLS/SSL Certificates | Not applicable | No SSL/TLS encryption is used. |
| Session Encryption - HTTPS  (GRIP SSD-4) | Not applicable | No https is used |
| Session Encryption – SFTP  (GRIP SSD-4) | Not applicable | No sftp is used |
| Session Encryption – TLS version  (GRIP SSD-4) | Not applicable | No TLS is used |
| Security of Data in Transit External | N/A |  |
| Security of Data in Transit Internal | 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 |  |
| Security Logging and -Monitoring | Default is 1 year | 1 year. |

# Appendix E: Glossary

Glossary of terms used in this HLD.

|  |  | **Notes** |
| --- | --- | --- |
| **ABB** | Architectures Building Blocks |  |
| **AD** | Active Directory |  |
| **ASP** | Account Security Plan |  |
| **ASO** | Account Security Officer |  |
| **CIs** | Configuration Items |  |
| **CMO** | Current Mode of Operation |  |
| **CSD** | Customer Security Document |  |
| **CVA** | Customer Virtual Appliance |  |
| **DB** | DataBase |  |
| **DXC-AD** | Active Directory at the DXC site which stores the credentials for all DXC personnel. |  |
| **DXC-DC** | DXC DC’s for UWV hosting services |  |
| **DXC TAB** | DXC Technical Application Beheer |  |
| **DNS** | Domain naming Systems |  |
| **ESB** | Enterprise Service Bus |  |
| **EoS** | End of Support |  |
| **FTPs** | File Transfer Protocol - SSL |  |
| **FQDN** | Fully Qualified Domain Name |  |
| **GRC** | Governance risk and compliance |  |
| **HLD** | High Lvele Design |  |
| **ISMS** | Information Security management System |  |
| **KPN-AD** | Active Directory at the KPN site which stores the credentials for all UWV personnel. |  |
| **LB** | Load Balancer |  |
| **MEP** | Managed Endpoint Protection |  |
| **MSS** | DXC’s portfolio of Managed Security Services |  |
| **OTAP** | Ontwikkeling, Test, Acceptance and Production |  |
| **PAM** | Privilege Account Management |  |
| **PDXC** | Platform DXC |  |
| **SBB** | Solution Building Block |  |
| **SECMON** | Security monitoring |  |
| **(s)FTP** | Secure File Transfer Protocol - SSH |  |
| **SIEM** | Security Incidents and Event management |  |
| **SLA** | Service Level Agreement |  |
| **SME** | Subject matter expert |  |
| **SOA** | Service-oriented architecture |  |
| **SPCM** | Server policy and compliance monitoring |  |
| **TCM** | Technical compliance monitoring |  |
| **TCM** | Technology compliance management |  |
| **UWV FB** | UWV Functional Beheer |  |
| **UAM** | User Account Management |  |
| **WBSBUS** | Werkbedrijf Service Bus |  |
| **WEC** | Windows Event Collector |  |
| **WVK BE** | Werkverkenner Backend |  |

# 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 | 26-01-2021 | DXC architecture team | First iteration of the HLD |
| SharePoint version 0.3 | 29-01-2021  04 February 2021  01 April 2021  07 April 2021 | DXC architecture team | Second iteration of the HLD VI   * Version 0.5 * Version 0.6 * Version 0.7 |
| 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   * Context diagram and external entities updated according latest connectivity sheet * Added DXC TAB requirements (4.11) * Connectivity sheet added to Appendix B |