

INFRASTRUCTURE APPLICATION HLD – DWH   
DataWareHouse Legacy

Version: 1.2

Date: 28 June 2023

Document purpose

This High Level Design (HLD) is used to:

1. Validate the Application solution from a technical perspective through architectural review
2. Plan and execute implementation of the solution
3. Support Technical Application Management

The document outlines:

1. An overview of the application and its architecture
2. Functional and non-functional requirements
3. Solution description
   1. 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.

1. **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).
2. **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:

1. The Software Architecture Document
2. Technisch Beheer Handboek (TBH – technical management handbook)
3. Technisch Koppelvlak Document (TKD – technical interface document)
4. 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 For the same reason some references in this document might be ‘outdated’ (i.e. not in this document anymore nor in other related documents).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](#_Toc135647146)

[1.1 Introduction 4](#_Toc135647147)

[1.2 Application use cases 4](#_Toc135647148)

[1.3 Out of Scope 4](#_Toc135647149)

[2 Architecture 5](#_Toc135647150)

[2.1 Conceptual 5](#_Toc135647151)

[2.2 Context diagram 6](#_Toc135647152)

[3 Functional Requirements 14](#_Toc135647153)

[4 Non-Functional Requirements 15](#_Toc135647154)

[4.1 Security & Compliance classifications 15](#_Toc135647155)

[4.2 System and Software requirements 15](#_Toc135647156)

[4.3 Availability 16](#_Toc135647157)

[4.4 Security requirements 17](#_Toc135647158)

[4.5 System management 17](#_Toc135647159)

[4.6 Backup and Recovery 17](#_Toc135647160)

[4.7 Storage replication 18](#_Toc135647161)

[4.8 Scalability 18](#_Toc135647162)

[4.9 Disaster Recovery 18](#_Toc135647163)

[4.10 Infrastructure Technical Constraints 18](#_Toc135647164)

[4.11 DXC TAB requirements 18](#_Toc135647165)

[5 Solution 19](#_Toc135647166)

[5.1 Architectural Decisions 19](#_Toc135647167)

[5.2 Node descriptions and zone-projections 20](#_Toc135647168)

[5.3 System diagram – Production 20](#_Toc135647169)

[5.4 System diagram Non-Production / Deployment 21](#_Toc135647170)

[5.5 SBB’s 21](#_Toc135647171)

[5.6 Load balancers 21](#_Toc135647172)

[5.7 Deviations from standards (RAL / EtP) 22](#_Toc135647173)

[5.8 Service Management 23](#_Toc135647174)

[5.9 Security 23](#_Toc135647175)

[6 Potential future improvements 25](#_Toc135647176)

[Version Control 26](#_Toc135647177)

[Appendix A: Technology and Sizing (at design verification) 29](#_Toc135647178)

[*Node details* 29](#_Toc135647179)

[*Storage* 29](#_Toc135647180)

[*Software* 30](#_Toc135647181)

[*Load Balancers* 30](#_Toc135647182)

[Appendix B: Network Protocol Matrix 31](#_Toc135647183)

[Appendix C: Users and Groups 32](#_Toc135647184)

[Appendix E: Glossary 33](#_Toc135647185)

[Appendix F: Legenda 34](#_Toc135647186)

[Legenda Context Diagram 34](#_Toc135647187)

[Legenda System Diagram 34](#_Toc135647188)

# Application Overview

## Introduction

DWH is not an application but a data integration and database infrastructure for the division GD DWH. All ETL programs are customer Oracle packages, procedures and shell scripts developed by UWV, no external party is involved for development.

Proprietary ETL software (MDT) MetaDataTool and (DoD) DatawarehouseOndemand (DWH2) and (OWB) Oracle Warehouse Builder (DWH3) is used to generate PL-SQL packages.

There is no OTOD environment, all environments (production, acceptance, test (includes development database) will be hosted on DXC managed servers.

TAB will be performed by UWV instead of DXC according to theso called C+ scenario, which is also applicable for DIM Infosphere and DWH-DMAP.

## Application use cases

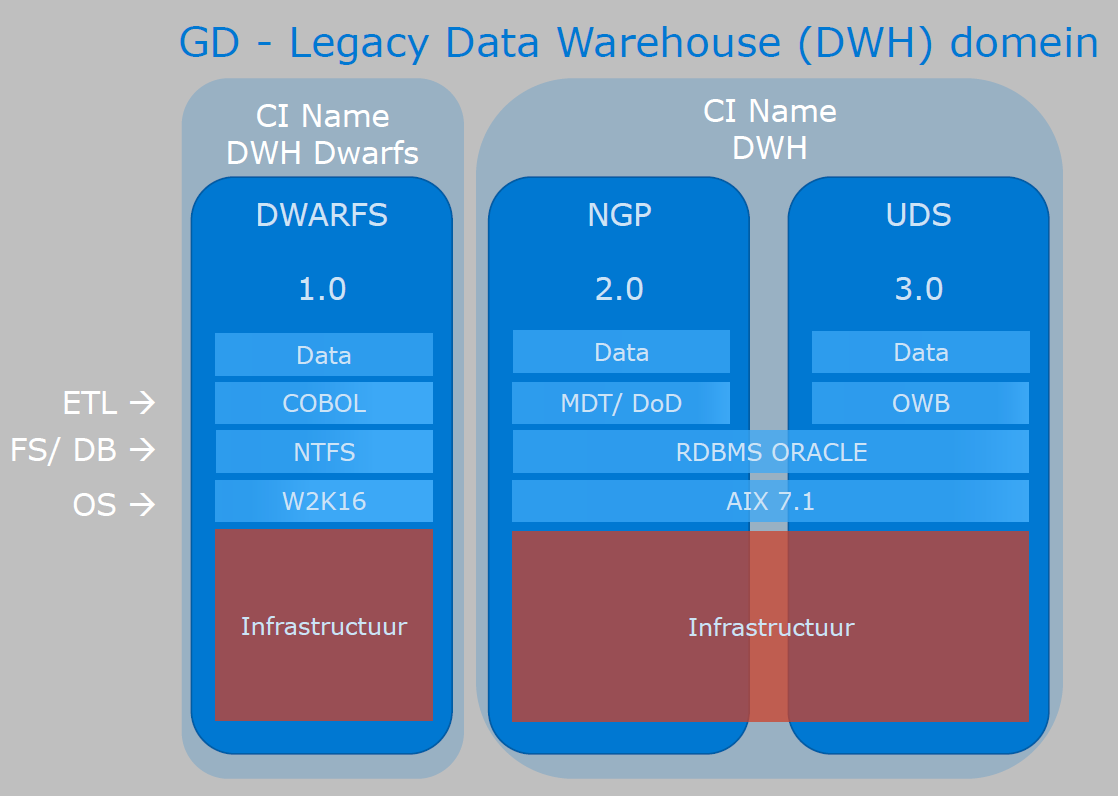
Application use cases are not defined, not applicable, or unknown to DXC.

## Out of Scope

* DWH Oracle Cloud Control (management server), this is moved to DIM Infosphere
* DWH Historical data, the solution is described in a separate document, storage details can befound in Appendix A of this HLD.
* Terminal Server for deployments, is part of DIM Infosphere
* All components that belong to the UWV Office Infrastructure such as workstations, web browsers are out of scope

# Architecture

## Conceptual

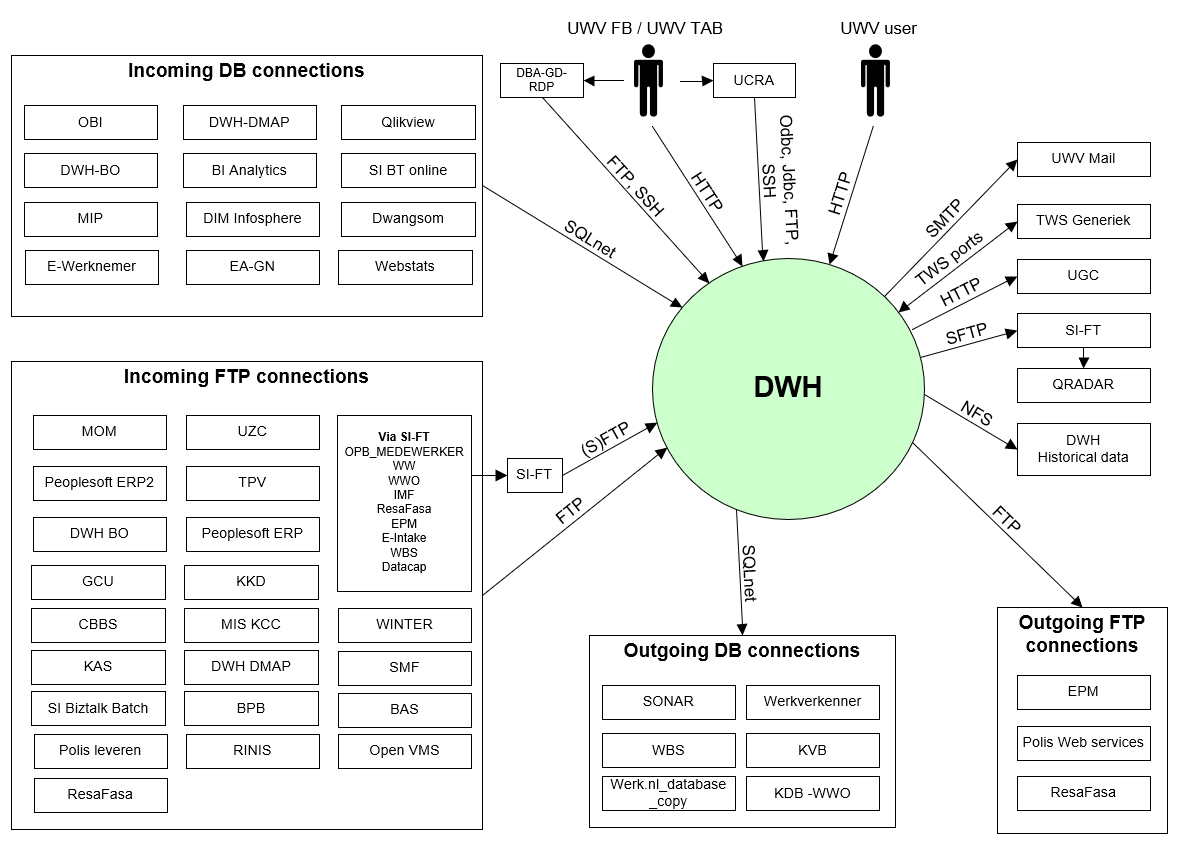


**DWH Key concepts:**

This paragraph specifies the key IT system level architectural concepts

* An AIX based Database server
* Oracle as the DBMS with:
  + MDT and DoD as ETL subsystems for DWH2
  + Oracle Warehouse Builder as a ETL subsystem for DWH 3
* A production environment
* An acceptance environment
* A test environment (includes development database, no infrastructure in the deployment environment)
* Database maintenance by UWV

## Context diagram



### External entities

#### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | 1. Functional management for MDT and DoD ETL applications are using a standard APEX webform for granting MDT/ DoD application role based acces (stored in Apex repository). 2. SQL Developers via UCRA and users who performs the ETL loading process and functional management of the application. The DWH functional managers are allowed) to exchange data with the DWH environment 3. DWH Deployments via DBA-GD-RDP (DBA-GD-RDP is only available in Production – DXC Application mgmt. zone) |
| **Protocol and Port** | 1. HTTP (8080) 2. Odbc/Jdbc (1526), FTP (20, 21, 22), SSH (22) 3. FTP (21), SSH (22) |
| **DC (Datacenter) connection** | 1. External 2. External 3. External |
| **Direction** | 1. Inbound 2. Inbound 3. Inbound |
| **Direct connection** | 1. Yes 2. No Via: UCRA 3. No Via: DBA-GD-RDP |
| **Security Controls** | Connection 1:  Authorisation method or authentication method: Apex DB account  Use certificates: No  Service account: No  Connection 2:  Authorisation method or authentication method: DB and AIX account  Use certificates: No  Service account: No  Other: Based on ABS (AD) role based acces in combination with equal Oracle DB role-based access.  Connection 3:  Authorisation method or authentication method: DB and AIX account  Use certificates: No  Service account: No  Other: Based on ABS (AD) role based acces in combination with equal Oracle DB role-based access. |
| **Number of users** | not specified |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### UWV users

|  |  |
| --- | --- |
| **Description** | DWH users that connect to the APEX web services for reading. |
| **Protocol and Port** | HTTP (8080) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Apex DB account  Use certificates: No  Service account: No  Other: ABS (AD) with equal Oracle DB role based acess. |
| **Number of users** | not specified |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### Incoming DB Connections

|  |  |
| --- | --- |
| **Description** | DWH Database access from UWV Business applications:  Is currently applicable for the following :  OBI, DWH-BO, MIP, e-Werknemer, DWH-DMAP, BI Analytics, DIM Infosphere, EA-GN, Qlikview, SI BT online, Dwangsom, Webstats |
| **Protocol and Port** | SQLnet (1526) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: 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 |

#### Incoming FTP Connections

|  |  |
| --- | --- |
| **Description** | UWV Business applications that send files to DWH  Is currently applicable for the following :  GCU, CBBS, KAS, SI Biztalk Batch, MOM, Peoplesoft ERP2, DWH-BO, KKD, MIS KCC, DWH DMAP, BpB, UZC, TPV Peoplesoft ERP, WINTER, SMF, BAS, Open VMS, RINIS, Polis Leveren, ResaFAsa  The following application send the files via SI-FT:  OPB\_MEDEWERKER, WW, WWO, IMF, ResaFasa, (Belastingsdienst via) EPM, E-Intake, WBS, Datacap |
| **Protocol and Port** | Direct connections: FTP (21)  Connections via SI-FTP: (S)FTP (21, 22) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Some connections are direct, and some connections are via SI-FT, see the above description |
| **Security Controls** | Authorisation method or authentication method: DWH 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 |

#### Outgoing DB Connections

|  |  |
| --- | --- |
| **Description** | DWH Database access to UWV Business applications:  Is currently applicable for the following :  SONAR, WBS, Werk.nl\_database\_copy, Werkverkenner, KVB, KDB-WWO |
| **Protocol and Port** | SQLnet (1526) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes  Via: not applicable |
| **Security Controls** | Authorisation method or authentication method: 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 |

#### Outgoing FTP Connections

|  |  |
| --- | --- |
| **Description** | UWV Business applications that DWH send files to  Mostly shared by ‘file-share’ delivery on the metioned UWV business applications domain  Is currently applicable for the following : EPM, Polis Web services, ResaFasa |
| **Protocol and Port** | FTP (21) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes  Via: not applicable |
| **Security Controls** | Authorisation method or authentication method: DWH 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 |

#### UWV mail

|  |  |
| --- | --- |
| **Description** | UWV mail relay services that sends outgoing mail to UWV FB |
| **Protocol and Port** | SMTP (25) |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | Yes  Via: not applicable |
| **Security Controls** | Authorisation method or authentication method: None required  Use certificates: No  Service account: No  Other: Whitelisting, STARTTLS |
| **Number of users** | not specified |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### TWS Generiek

|  |  |
| --- | --- |
| **Description** | TWS Generiek connection with DWH |
| **Protocol and Port** | Inbound: TCP (34243)  Outbound: TCP (31111, 31116) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound and Outbound |
| **Direct connection** | Yes  Via: not applicable |
| **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 |

#### UGC

|  |  |
| --- | --- |
| **Description** | Call by SUAG (DWH) |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound and Outbound |
| **Direct connection** | Yes  Via: not applicable |
| **Security Controls** | Authorisation method or authentication method: User and Password authenticated, to be verfified by UGC.  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 |

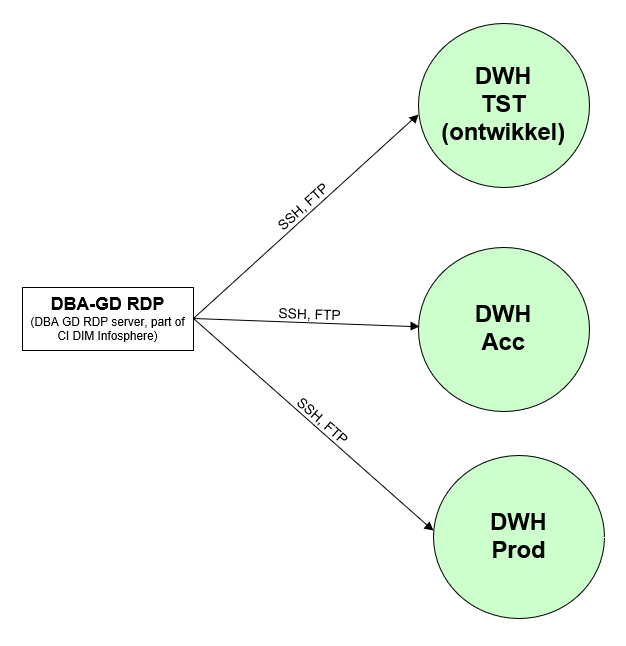
#### QRADAR

|  |  |
| --- | --- |
| **Description** | Application logs for QRADAR  Application logs are applicable for all environments, this requires an additonal connection from DWH Test to SI-FT Prod |
| **Protocol and Port** | SFTP (22) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No Via: SI-FT |
| **Security Controls** | Authorisation method or authentication method: DWH 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 |

#### DWH Historical data

|  |  |
| --- | --- |
| **Description** | DWH Historical Data solution – DWH requires the possibility to backup historical data and restore on request. Backup / Restore of this data is performed by UWV (only available in Production) |
| **Protocol and Port** | NFS (22) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: NFS mountpoints  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 |

### Context diagram - DWH Deployment



# Functional Requirements

No functional requirements specified.

# Non-Functional Requirements

## Security & Compliance classifications

Repository used is: “2022 UWV-brede Risico Applicatie Lijst v1.0”

|  |  |
| --- | --- |
| **Application** | DWH |
| **Owner** | GD |
| **Availability (Beschikbaarheid)** | 2 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 3 |
| **Type of information /Data Classification** | Personal information 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 | No |
| Additional frameworks | SSD |

## System and Software requirements

### System (Operating system (OS))

| **Operating System** | **Version** |
| --- | --- |
| AIX | 7.2 |

### Software (Licenses)

| **Software product / component** | **Version** |
| --- | --- |
| Oracle database server | 11.2.0.4 |
| Oracle Automatic Storage Manager ASM | 19c |
| Oracle Pack: Diagnostics Pack |  |
| Oracle Pack: Tuning Pack |  |
| Oracle REST services | 20.2.1 |
| Oracle Application Express (APEX) | 4.2.3 |
| IBM Workload scheduler Fault Tolerant Agent | 9.3 FP2 |
| Oracle Warehouse Builder standalone | 11.2.0.4 |
| OWB client (onderdeel van OWB) | 11g |
| Oracle Workflow (onderdeel van OWB) | 2.6.4 |
| Oracle Enterprise ETL option (paid option of OWB) | 11.2 |

### Capacity and performance (volumetrics)

Current sizing:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Environment** | **CPU** | **vCPU** | **RAM (GB)** | **DB Storage** | **FS Storage** |
| Production | 44 | 11 | 144 | 22+4 TB | 5.5 TB |
| Acceptance | 16 | 4 | 144 | 18+2 TB | 4 TB |
| Test | 20 | 5 | 120 | 8+2TB | 3.4 TB |

## Availability

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Application Target** | **Application Service Hours** | **Infra Target** |
| Production | n/a\* | n/a\* | 98% |
| Acceptance | n/a\* | n/a\* | 98% |
| Test | n/a\* | n/a\* | 98% |

\*TAB is preformed by UWV instead of DXC

## Security requirements

Because UWV performs TAB, UWV requires access to all DWH

environments. Special rights are required. (This does **not apply** to the UCRA environment).

* DWH infrastructure management / DBA role: not more than 2 persons. They need access to all DWH environments including A&P.
* Production managers. 6-8 persons. They need operational access to P for running and monitoring the ETL Data Feed processes. These managers need access to P environment to run installer script/wizard and refine pl/sql code to create or update production ETL process. This Production Access is due to the mostly manual ´enrichment process´.
* Developers, designers. Approx. 15-20 persons. They need access to O, T&Q and via regular access control also A.
* DWH Process managers, approx. 10-12 persons. They make information products in Q environment. Need access to Q and assist during Acceptance.
* For Production there are more than 100 ftp users/passwords on DWH.  In order to avoid having to change the passwords at the source application side, the passwords from DWH at CMO must be transferred to DWH DXC (This is for Acceptance and Prod). (The CMO passwords are very weak, this is a deviation documented in 5.7)

Note: Q=Query database, is hosted on the Production server together with the P database

### System logging

No specific system logging requirements are applicable

## System management

No system management requirements are applicable.

### Additional application related infra requirements

|  |  |
| --- | --- |
| **Requirements** | **Status** |
| Use STARTTLS option for UWV mail | Yes |
| Is Microsoft DTC used for inflight transactions | Not applicable |
| Is HTTPS cookie stickiness required on the load balancer | Not applicable |

## Backup and Recovery

|  |  |  |
| --- | --- | --- |
|  | **Default** | **Deviation (when applicable)** |
| Backup | standard backup | Database archivelog backups/purges every 30 minutes |
| Restore | no specific restore order |  |
| Dependency | no dependencies |  |

Note: Some Backup and Retore activites are performed by UWV using RMAN, this will be described in the so-called C+ document. Therefore, not able to specify at this moment, the C+ document specifies who is backing up what and how)

### Historical data

DWH makes use of historical data. For historical data an archiving solution is required, this archiving solution is not part of the DWH HLD and will be described separately, below the DWH historical data requirements.

* UWV Gegevensdiensten must be able to archive the following data
  + Zipped Oracle database export files with retention of 6 months
  + ETL Source files with a retention of 5 years
* UWV Gegevensdiensten must be able to restore the archived data themselves

## Storage replication

|  |  |
| --- | --- |
| **Environment** | **Storage Replication\*** |
| Production | Non-replicated storage |
| Acceptance | Non-replicated storage |
| Test | Non-replicated storage |

\* Storage replication is not available for Legacy (AIX) systems with SLA Bronze, in this case only Backup / Restore is available

## Scalability

No scalability limitations for the applications are specified

## Disaster Recovery

No specific disaster recovery requirements applicable.

## Infrastructure Technical Constraints

CMO systems at Kyndryl are running out of memory, RAM upgrade is requested.

## DXC TAB requirements

This chapter is not applicable, TAB is performend by UWV

# Solution

## Architectural Decisions

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Decision** | **Comments** | **Status** |
| 1 | The Oracle DBMS is supported by UWV instead of DXC which is not the default solution for DXC managed servers | The support model for DWH deviates from the standard DXC Managed / UWV managed models. This model is referred to as C+ and will be described in a separate document | Approved |
| 2 | The Oracle DBMS server is also an FTP server and hosts the Apex application which can be accessed through web services | Database and FTP server are combined on the same server this is not the preferred design solution but a consequence of migrating the current situation | Approved |
| 3 | (OT)AP for all Application Logic and is DWH responsibility up from the OS level | Application Logic changes follow (OT)AP in all cases | Approved |
| 4 | Query and production databases share one system | High data volumes have to be copied from the P database to the Q database during ETL processing. With different hardware systems it will be a host-based copy where network and CPU´s are heavily used. | Approved |
| 5 | A new security zone “DWH” is created in the legacy network for OTAP | UWV performs TAB activities and database management for which they require elevated access rights, therefore an isolated (ringfence) solution is required. | Approved |
| 6 | All DWH AIX systems are placed in the DWH security zone, this is the only available security zone for DWH | Standard security zones such as FrontOffice, BackOffice and Kluis are not available for DWH AIX systems. Database with confidentiality classification 3 are also placed here | Approved |
| 7 | DWH databases will be hosted on AIX | The databases are exceeding the maximum VM size in the Private Cloud and will therefore not be re-platformed | Approved |
| 8 | AIX 7.2 is used instead of AIX 7.1 | UWV confirmed that the OS for DWH can be AIX 7.2 instead of AIX 7.1 which is used in CMO | Approved |
| 9 | The requested Archive solution (Store / Restore) is not part of this HLD but will be described in a separate (KD) document | How to handle the requested Archive (Store/ Restore) function should be addressed. Function and Solution should be agreed on. | Approved |
| 10 | A dedicated DWH RDP server (in the DXC Application mgmt. zone) is used for deployments | In CMO UCRA-T was used for deployments this is no longer allowed, therefore the use of a dedicated application RDP server was advised by ICT services | Approved |

## Node descriptions and zone-projections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Zone** | **Domain** | **Server Type** | **Node ID** | **Infra Service Level** |
| DWH | Production | Database server | DWH-DB-P | Bronze |
| DWH | Acceptance | Database server | DWH-DB-A | Bronze |
| DWH | Test | Database server | DWH-DB-T | Bronze |

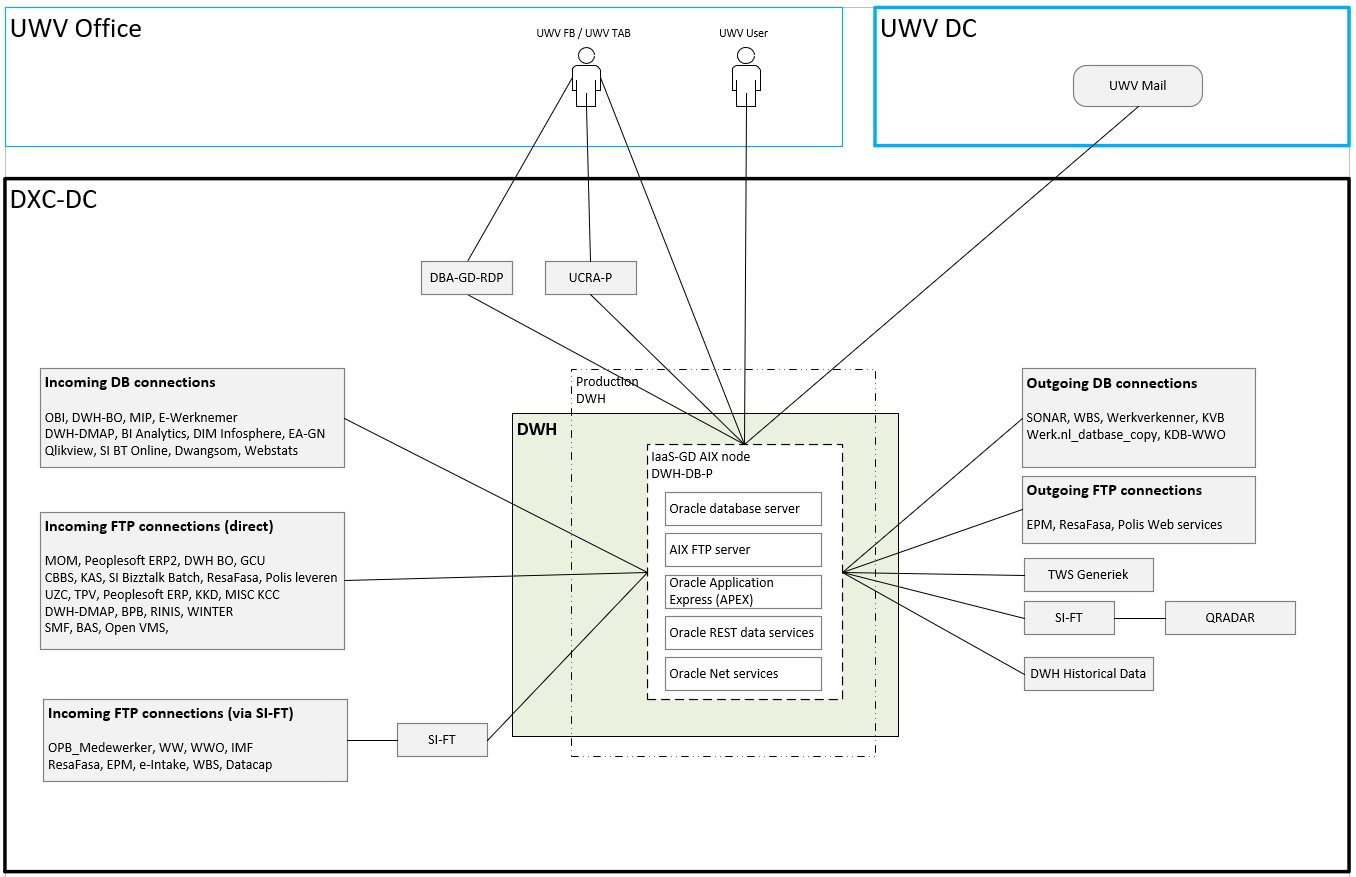
Remarks:

* DBA-GD-RDP is part of the DIM-Infosphere CI and is therefore not added to this overview. Details can be found in the DIM-Infosphere HLD
* DWH Historical data is described in a separate document, however the storage details are added to Appendix A of this HLD

### DNS (customer facing name)

|  |  |  |
| --- | --- | --- |
| **Domain** | **Customer facing name** | **DNS suffix** |
| Production | DWH | P-dc.ba.uwv.nl |
| Acceptance | DWH | A-dc.ba.uwv.nl |
| Test | DWH | T-dc.ba.uwv.nl |

## System diagram – Production

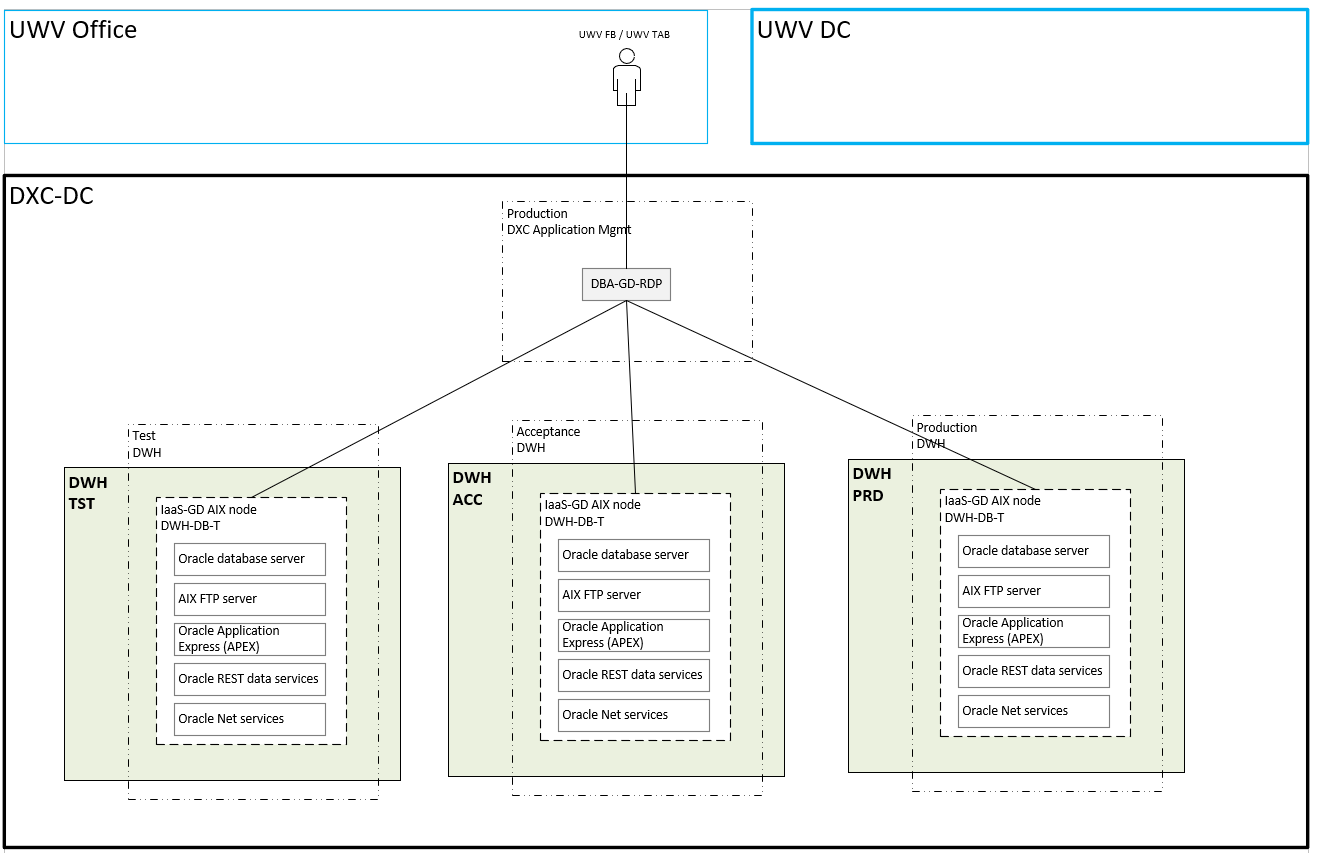


Remark: DWH is a new security zone which is created in Legacy to ringfence the DWH systems

## System diagram Non-Production / Deployment

* Production, Acceptance and Test are the same, therefore no separate diagram
* A diagram (without the external entities) is displayed below to show the deployment setup

**DWH Deployment – System diagram**



## SBB’s

|  |
| --- |
| **Standard Building Block Type** |
| N/A |

No SBB’s are specified. IaaS-GD is delivered, and the service is described in the so-called C+ document.

## Load balancers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Load balancer** | **Load balancer type** | **LB ID** | **Description** |
| Production | No | not applicable | n/a | n/a |
| Acceptance | No | not applicable | n/a | n/a |
| Test | No | not applicable | n/a | n/a |

## 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 | Separate DWH security zone in Legacy is created for all DWH AIX systems | No |  |
| 2 | UWV performs TAB Tasks. Special permissions are necessary | No |  |
| 3 | Non-mainstream software: Oracle database server 11.2.0.4 | Yes | 20221129-007A |
| 4 | Direct user access (UWV FB, UWV TAB, UWV user) to data with confidentiality classification 3 | Yes | 20221129-008 A |
| 5 | No encryption: UWV FB and UWV TAB HTTP connection to DWH | Yes | 20221129-009 A |
| 6 | No encryption: UWV USER HTTP connection to DWH | Yes | 20221129-010 A |
| 7 | old software: JVM for AIX 1.8.0 | Yes | 20221129-012 A |
| 8 | old software: JAVA JDK 1.8.0.311 | Yes | 20221129-013 A |
| 9 | old software: JAVA JRE 6 | Yes | 20221129-014 A |
| 10 | old software: Oracle Automatic Storage Manager ASM 19c | Yes | 20221129-015 A |
| 11 | old software: Oracle Application Express (APEX) 3.2 | Yes | 20221129-016 A |
| 12 | old software: IBM Workload scheduler Fault Tolerant Agent 9.3 FP2 | Yes | 20221129-017 A |
| 13 | Passwords FTP accounts: The provided hashes are encrypted with the legacy password hashing algorithm called crypt() which is very weak and vulnerable to brute force password guessing attacks. | Yes | 20230414-001-A |
| 14 | Using old protocol X11 Forwarding | Yes | PER0003227 |

### Detailed deviation description

1. Separate DWH security zone: TAB will be performed by UWV this requires the systems to be ringfenced. In the Private Cloud micro segmentations is used for this. Since micro segmentation is not available in Legacy a separate security zone specific for DWH systems is created. Although this is a deviation it does not require an EtP. This is the mitigation on an infrastructure level on how to deal with the UWV TAB managed systems in Legacy.
2. UWV performs TAB tasks: Although this is a deviation that normally requires an EtP it is not necessary in this case because a deviating support model is used. This deviation is described in the so-called C+ document. The C+ document is considered as a mitigation for this deviation.
3. For Production there are more than 100 ftp users/passwords on DWH.  In order to avoid having to change the passwords at the source application side, the passwords from DWH at CMO are transferred to DWH DXC.  This is applicable for Acceptance and Prod.
4. X11 Forwarding is needed to get the graphical java-programs working:  OWB-client,  DBUA (DB Upgrade Assistant) en DBCA (DB Configuration Assistant)

## Service Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Infra Hosting** | **Database / Middleware Management** | **Technical Application Management** |
| Production | Bronze | N/A \* | N/A \* |
| Acceptance | Bronze | N/A \* | N/A \* |
| Test | Bronze | N/A \* | N/A \* |

\* UWV is responsible for Technical Application-, database- and middleware management

## Security

Deviations are document in chapter 5.7’.

### User Authentication and Authorization

UWV user, UWV FB and UWV TAB

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.

### 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.

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

1. *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
2. *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.
3. *External (outside DXC):* Connection external for the application and outside the DXC data center. For example, HTTPS connection between Application server and the UWV Citrix KA farm. All external (outside DXC) connections are documented in the table below

For DWH the following is applicable:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Connection Type** | **Between (component 1)** | **And (component 2)** |
| External (outside DXC) | HTTP | UWV Werkplek (UWV user, UWV FB and UWV TAB) | DWH server |
| External (outside DXC) | SMTP | DWH server | UWV mail |
| Internal | FTP, SCP | DWH server P | DWH server A |
| Internal | FTP, SCP | DWH server P | DWH server T |
| Internal | FTP, SCP | DWH server A | DWH server T |

For details see Appendix B

# Potential future improvements

|  |  |  |
| --- | --- | --- |
| **ID** | **Proposed improvement** | **Reason** |
| 1 | UWV to provide another solution for the deployments instead of using UCRA-T | Preferred for deployments is a dedicated system for DWH (environments) that is placed in the DXC Application Management zone |
| 2 | UWV to investigate how the AIX servers/services can be transferred to the private cloud | The intention is to move all systems to the private cloud, legacy should only be a temporary solution |
| 3 | UWV to evaluate the chosen support model (C+) for DWH | DXC Managed systems (including database, middleware, and TAB) or UWV managed systems are the preferred support models |

# Version Control

**USED TEMPLATE**

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

**DOCUMENT AUTHORISATION**

| Name | Role | Date |
| --- | --- | --- |
| Cora Kuijper | DXC Account Technical Lead (verification) | 06-01-2023 |
| Nic van Spronsen | UWV Lead Architect (verification) |  |
| Rick van Diemen, delegated to Hans Kreisel | DXC Account Delivery Lead (acceptance) | 06-01-2023 |

**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 | 19-09-2022  22-09-2022  17-10-2022  27-10-2022 | DXC architecture team | First iteration of the HLD   1. 0.1 – Initial version based on CMO documentation 2. 0.3 – Updated according DXC HLD template 3. 0.4 – Processd comment of the co-creation session 4. 0.41 – Processed review comment form UWV |
| SharePoint version | 16-11-2022  17-11-2022  14-12-2022 | DXC architecture team | Second iteration of the HLD  0.6   * Received updated CMO (Kyndryl) HLD, added the following requirement: Access to Oracle DB must be available via Single Sign On (SSO), UWV AD connection is added to the Context Diagram * Added the solution (Chapter 5, 6 and Appendixes)   0.61   * Removed the requirement: Access to Oracle DB must be available via Single Sign On (SSO), UWV AD connection is removed from the Context Diagram. Removed Kerberos from Appendix A - Software (UWV Feedback above is only applicable for DIM and not for DWH).   0.7   * Processed UWV feedback |
| Verification version 0.8 | 19-12-2022 | DXC architecture team | Account review |
| Verification version 0.9 | 06-01-2023 | DXC architecture team | Design Office verification |
| Version 1.0 | 11-01-2023 | DXC architecture team | Positive verified HLD  Conditions:   * Deployment method needs to be updated; UCRA-T cannot be used for this (related EtP 20221129-006 A is removed so it cannot be used accidentily) * So-called C+ document (especially the RACI) needs to be available and approved by all involved parties before Go-Live |
| Version 1.1 | 23-05-2023 | DXC architecture team | Post implementation HLD  18-01-2023:   * Update Appendix A – Software JVM version 1.8.0 instead of 1.4.2   21-02-2023:   * Added QRADAR entity to 2.2.1 * Added EtP for cross-domain between DWH Test and SI-FTP production   01-03-2023:  Updated with DBA-GD RDP server   * Added seperate context diagram (and external entity to the existing) * Added separate system diagram in 5.4 * Added decision 10 to 5.1  1. 07-03-2023:   UWV requested to update Appendix A – storage:   * DWH-DB-A: additional 2 TB (ASM DATA) * DWH-DB-P: additional 4 TB (ASM DATA)  1. 31-03-2023: 2. Updated Backup requirements:  * - Archive log backup -> every 30 minutes  1. Updated Appendix A – Node details:  * DWH-DB-P from 144 GB to 174 GB RAM (due to change at Kyndryl side)   Updated Appendix A – Software:   * Updated Java JDK from 1.6.0.210 to 1.8.0\_311 * Updated Java JRE from 6 to 8   23-05-2023:  Updated with DWH Historical data info   * Added DWH Historical data to out of scope (details are described in a separate document) * Added a description in 4.6.1 * Added as decision (9) in 5.1 * Added details to Appendix A for billing purposes   Added EtP for weak passwords for the FTP accounts |
| Version 1.2 | 26-07-2023 | DXC architecture team | Aftercare implementation HLD  06-06-2023  Adjusted Appendix A - storage to be in line with actual storage assigned  DWH-DB-P  **From**: 26x1TB + 4x1TB = 30TB **To** 15x2TB=2x1TB = 32TB  DWH-DB-A  **From**: 20x1TB + 2x1TB = 22TB **To** 11x2TB=2x1TB = 24TB  DWH-DB-T  **From**: 8x1TB + 2x1TB = 10TB **To** 10x1TB=2x1TB = 12TB  UWV requested to add 30 GB RAM to DWH PROD, Adjusted Appendix A – Node details:  DWH-DB-P  RAM **From**: 174 GB **To:** 204 GB  28-06-2023  Added EtP for X11 forwarding   * 5.7: EtP added * 5.7.1: detailed description added   Expanded dump disk for DWH Historical data on request of UWV, disk is almost full and additional storage (2 TB) is required   * Appendix A – Storage: DWH Historical data – dump disk changed from 27TB to 29 TB   CHG0089348: DWH-DB-A FS Data disk is expanded with 200 GB   * Appendix A – Storage: DWH-DB-A – FS data changed from 4 TB to 4.2 TB |

# 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** | **Replication** |
| Legacy Hosting AIX | DWH | AM2 | Production | DWH-DB-P | 11 | 204 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS-GD\* | no |
| Legacy Hosting AIX | DWH | AM3 | Acceptance | DWH-DB-A | 4 | 144 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS-GD\* | no |
| Legacy Hosting AIX | DWH | AM3 | Test | DWH-DB-T | 5 | 120 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS-GD\* | no |

\*Instead of IaaS+ (DXC Managed), IaaS-GD is delivered, the associated service is described in the so-called C+ document (ITAB).

**DWH Historical data:** Is considered as a platform and not an application and is therefore described in a sperate KD (Knowledge Document - DXC\_KD\_Historical Data Solution v1.0). The data is hosted on an AIX file server that is only used by DWH and is therefore added to this Appendix

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **Location** | **Domain** | **Node ID** | **vCPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Legacy Hosting AIX | DWH | AM2 | Production | DWH Historical data | 1 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | IaaS-GD\* | yes |

\*Instead of IaaS+ (DXC Managed), IaaS-GD is delivered, the associated service is described in the so-called C+ document (ITAB).

## *Storage*

*Oracle Database server(s)*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk0 OS (Fixed)** | **Disk1 Oracle Binaries (Fixed)** | **Disk2 ASM Binaries (Fixed)** | **ASM DATA DiskGroup1 Data Files, Control Files (mandatory)** | | **ASM FRA DiskGroup2 Archive and Flashback Logs (mandatory)** | | **FS DATA DiskGroup3** |
| DWH-DB-P | Production | 100 GB | 100 GB | 100 GB | 15 x | 2 TB | 2 x | 1 TB | 5.5 TB |
| DWH-DB-A | Acceptance | 100 GB | 100 GB | 100 GB | 11 x | 2 TB | 2 x | 1 TB | 4.2 TB |
| DWH-DB-T | Test | 100 GB | 100 GB | 100 GB | 10 x | 1 TB | 2 x | 1 TB | 3.4 TB |

**DWH Historical data:** Is considered as a platform and not an application and is therefore described in a sperate KD (Knowledge Document - DXC\_KD\_Historical Data Solution v1.0). The data is hosted on an AIX file server that is only used by DWH and is therefore added to this Appendix

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **OS** | **Dumps** | **Transit** | **Archief 2018** | **Archief 2019** | **Archief 2020** | **Archief 2021** | **Archief 2022** | **Archief 2023** |
| DWH Historical data | Production | 100 GB | 29 TB | 21 TB | 2,5 TB | 7,5 TB | 11 TB | 14 TB | 14 TB | 14 TB |

## *Software*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported by vendor** |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 1-OS | AIX | 7.2 | Y |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 2-Library | JVM for AIX | 1.8.0 | N |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 2-Library | Java JDK | 1.8.0\_311 | N |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 2-Library | Java JRE | 8 | N |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 2-Library | AIX FTP server | 7.1 | N |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 3-Database | Oracle Database Server | 11.2.0.4 | N |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 3-Database | Oracle Automatic Storage Manager ASM | 19c | N |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 4-Middleware | Oracle Application Express (APEX) | 3.2 | N |
| DWH-DB-P; DWH-DB-A | 4-Middleware | IBM Workload scheduler Fault Tolerant Agent | 9.3 FP2 | N |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 5-Applicatie | Oracle REST data services | 20.2.1 |  |
| DWH-DB-P; DWH-DB-A; DWH-DB-T | 5-Applicatie | Oracle Net Services |  |  |
| DWH-DB-T | 5-Applicatie | OWB client | 11g |  |
| DWH-DB-T | 5-Applicatie | Oracle Warehouse Builder standalone | 11.2.0.1.0 |  |
| DWH-DB-T | 5-Applicatie | Oracle Workflow | 2.6.4 |  |
| DWH-DB-T | 5-Applicatie | Oracle Enterprise ETL option | 11.2 |  |

## *Load Balancers*

Load balancers are NOT used in this solution

# 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 Werkplek | DWH-DB-P | HTTP | 8080 |  |
| UWV Werkplek | DWH-DB-A | HTTP | 8080 |  |
| UWV Werkplek | DWH-DB-T | HTTP | 8080 |  |

**UWV Werkplek (UWV user, UWV FB and UWV TAB) to DWH server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DWH-DB-P | UWV Mail | SMTP | 25 | STARTTLS is used |
| DWH-DB-A | UWV Mail | SMTP | 25 | STARTTLS is used |
| DWH-DB-T | UWV Mail | SMTP | 25 | STARTTLS is used |

**DWH server to UWV mail**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DWH-DB-P | DWH-DB-A | FTP, SCP | 21, 22 |  |

**DWH server P to DWH server A**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DWH-DB-P | DWH-DB-T | FTP, SCP | 21, 22 |  |

**DWH server P to DWH server T**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DWH-DB-A | DWH-DB-T | FTP, SCP | 21, 22 |  |

**DWH server A to DWH server T**

**Only for HLD version 1.1:** connectivity sheet provided as a separate file “UWV - Connectivity sheet - DWH - v1.1.xlsb”

# 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)

***Service Accounts:***

The following accounts are not compliant to the default settings, will be added in version 1.1

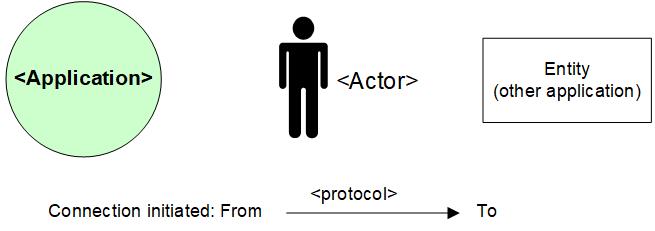
|  |  |  |  |
| --- | --- | --- | --- |
| **Account** | **Domain / local location** | **Noncompliant setting** | **Description** |
|  |  |  |  |

# 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

