

HLD - DIM-Infosphere

**(Data Integratie Magazijn – Infosphere)**

Version: 1.2

Date: 2 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 For the same reason some references in this document might be ‘outdated’ (i.e. not in this document anymore nor in other related documents).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](#_Toc113613273)

[1.1 Introduction 4](#_Toc113613274)

[1.2 Application use cases 4](#_Toc113613275)

[1.3 Out of Scope 4](#_Toc113613276)

[2 Architecture 5](#_Toc113613277)

[2.1 Conceptual 5](#_Toc113613278)

[2.2 Context diagram 6](#_Toc113613279)

[3 Functional Requirements 32](#_Toc113613280)

[4 Non-Functional Requirements 33](#_Toc113613281)

[4.1 Security & Compliance classifications 33](#_Toc113613282)

[4.2 Capacity and performance (volumetrics) 34](#_Toc113613283)

[4.3 Availability 35](#_Toc113613284)

[4.4 Security requirements 36](#_Toc113613285)

[4.5 System management 36](#_Toc113613286)

[4.6 Backup and Recovery 37](#_Toc113613287)

[4.7 Storage replication 37](#_Toc113613288)

[4.8 Scalability 37](#_Toc113613289)

[4.9 Disaster Recovery 37](#_Toc113613290)

[4.10 Infrastructure Technical Constraints 37](#_Toc113613291)

[4.11 DXC TAB requirements 37](#_Toc113613292)

[5 Solution 38](#_Toc113613293)

[5.1 Architectural Decisions 38](#_Toc113613294)

[5.2 Node descriptions and zone-projections 44](#_Toc113613295)

[5.3 System diagram – Production 45](#_Toc113613296)

[5.4 System diagram – non-Production 47](#_Toc113613297)

[5.5 SBB’s 48](#_Toc113613298)

[5.6 Load balancers 48](#_Toc113613299)

[5.7 Deviations from standards (RAL / EtP) 48](#_Toc113613300)

[5.8 Service Management 48](#_Toc113613301)

[5.9 Security 49](#_Toc113613302)

[6 Potential future improvements 51](#_Toc113613303)

[Appendix A: Technology and Sizing (at design verification) 52](#_Toc113613304)

[*Node details* 52](#_Toc113613305)

[*Storage* 54](#_Toc113613306)

[*Software* 56](#_Toc113613307)

[*Load Balancers* 59](#_Toc113613308)

[Appendix B: Network Protocol Matrix 60](#_Toc113613309)

[Appendix C: Users and Groups 63](#_Toc113613310)

[Appendix D: Security 65](#_Toc113613311)

[Appendix E: Glossary 67](#_Toc113613312)

[Appendix F: Legenda 68](#_Toc113613313)

[Legenda Context Diagram 68](#_Toc113613314)

[Legenda System Diagram 68](#_Toc113613315)

[Appendix G: Control 69](#_Toc113613316)

# Application Overview

## Introduction

Where in this document “DIM” is mentioned, the “DIM-Infosphere” application is meant.

The DIM deployment consists of a Linux, AIX and Windows Production, Acceptance, Test and Development environment with interfaces to several input sources for the ETL (Extract Transform Load) of business data.

DIM provides both a web-based interface for users located in the UWV KA domain and a Windows based FAT client which will be deployed in the DXC datacenter.

Implementation of DIM will be based on the generic services and building blocks.

DIM Infosphere consists of the following components:

* DIM Service: DIM services servers
* DIM Search: DIM search servers (zookeeper)
* DIM Engine: DIM Engine servers
* DIM Bridge: DIM Bridge servers
* DIM DB: DIM Infosphere database server
* DIM FS: DIM Infosphere NFS server (contains hot and cold data share)
* DIM Deploy: DIM management server used for promotions (deployments)
* DBA-GD RDP: Remote desktop server for DBA Gegevensdiensten

## Application use cases

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

## Out of Scope

* Functional Application Management is not in scope for DXC
* Technical Application Management is not in scope for DXC
* Database Administration is not in scope for DXC
* Dim Infosphere FATclient installation on UCRA is out of scope for this HLD and must be considered as part of the UCRA design
* All components that belong to the UWV Office Infrastructure such as workstations, web browsers are out of scope
* How InfoSphere licensing method

# Architecture

## Conceptual

UWV selected IBM InfoSphere Information Server as the new target solution for ETL.

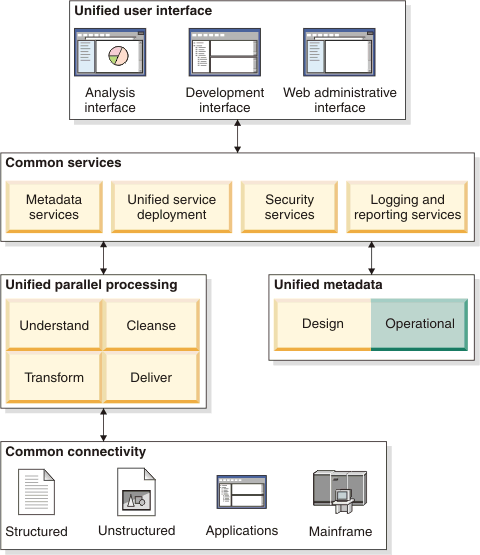
IBM® InfoSphere® Information Server provides a unified architecture that works with all types of information integration. Common services, unified parallel processing, and unified metadata are at the core of the server architecture.

The architecture is service-oriented, enabling IBM® InfoSphere® Information Server to work within evolving enterprise service-oriented architectures. A service-oriented architecture also connects the individual suite product modules of IBM® InfoSphere® Information Server.

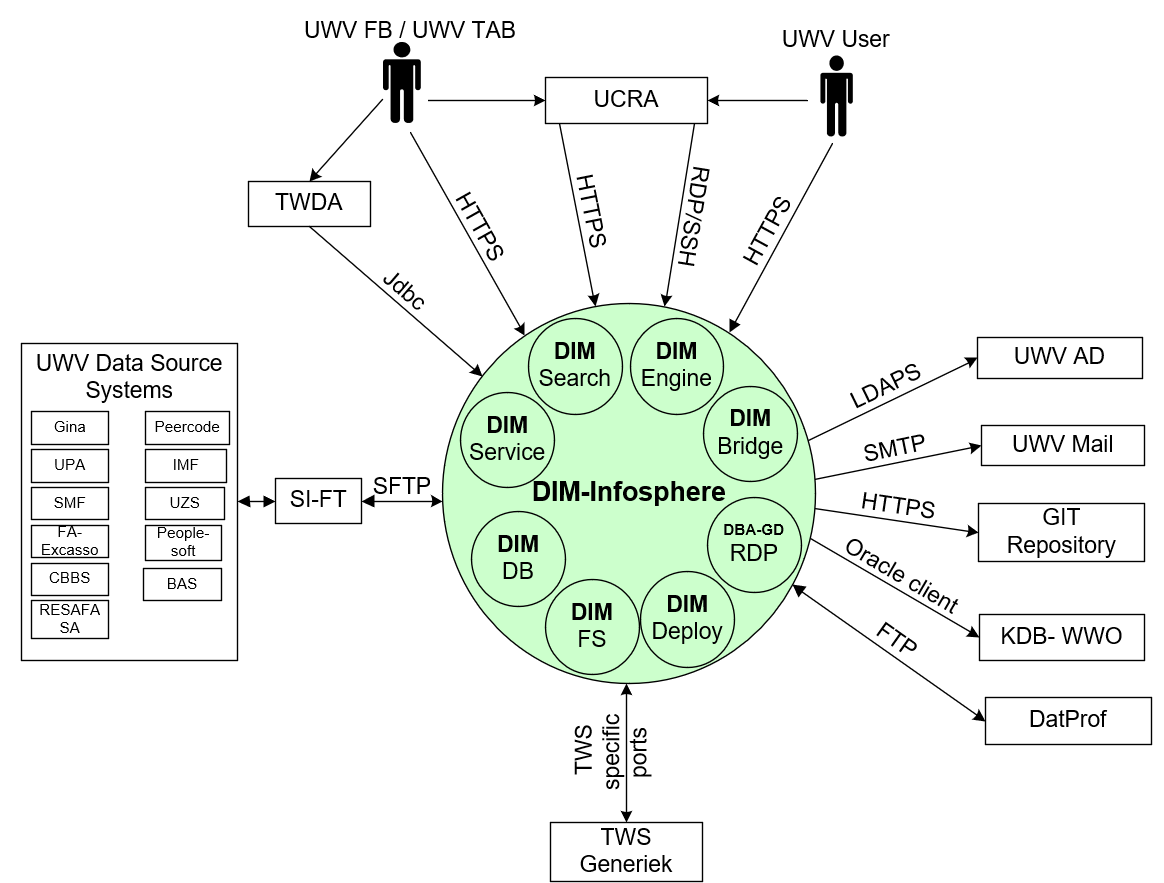
By eliminating duplication of functions, the architecture efficiently uses hardware resources and reduces the amount of development and administrative effort that are required to deploy an integration solution.

The main concepts are:

1. Unified parallel processing engine
2. Common connectivity (structured/unstructured data sources)
3. Unified metadata (enables shared understanding between business and technical domains)
4. Common services (set of shared services that centralize core tasks across the platform)
5. Unified user interface (common graphical interface and tool framework)

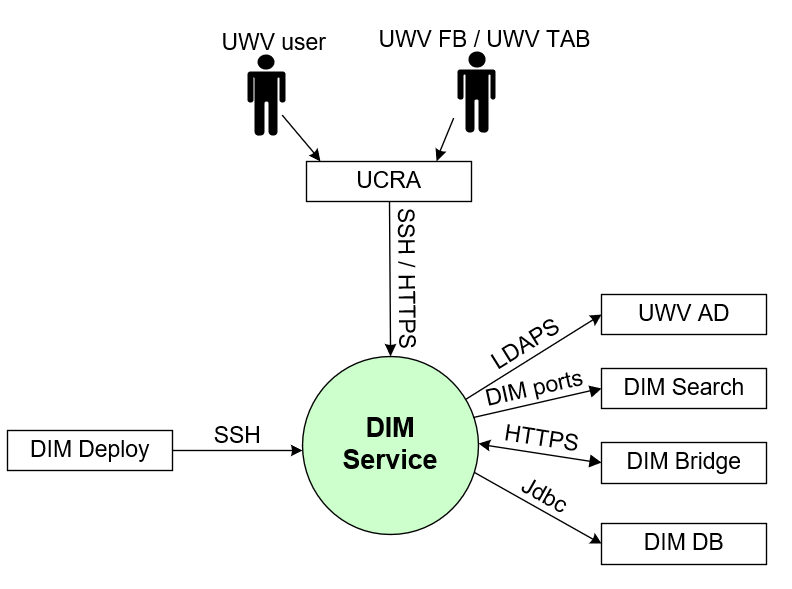


## Context diagram



The above diagram shows the Context Diagram and the external entities for the DIM-Infosphere application. Due to the complexicity of the application the application is split in different components. The different components are represented by the small green circles and wil be described in the next chapters in more detail.

### DIM Service



#### External entities

##### UWV Users

|  |  |
| --- | --- |
| **Description** | Developers and Data Engineers as part of UWV Users community |
| **Protocol and Port** | SSH, port 22; HTTPS, port 9443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | A user performing functional and technical Application Management tasks. This is mainly related to the configuration of ETL processes and reports, but also management of the application itself. Web Browser and several IIS clients are used for performing these tasks. |
| **Protocol and Port** | SSH, port 22; HTTPS, port 9443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | 2-5 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### UWV AD

|  |  |
| --- | --- |
| **Description** | Windows Active Directory domain containing resource groups of which UWV domain (KA prod or WPOL) user groups are member, and by which UWV accounts are granted rights. |
| **Protocol and Port** | Kerberos (88), LDAP (389), LDAPS (636), Global Catalog (3268, 3269) |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: AD authentication  Use certificates: No  Service account: Yes |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### DIM Search

|  |  |
| --- | --- |
| **Description** | Internal Application communication with DIM search |
| **Protocol and Port** | TCP: 2181, 9092 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Bridge

|  |  |
| --- | --- |
| **Description** | Internal Application communication with DIM Bridge |
| **Protocol and Port** | Connection 1: HTTPS, 19433  Connection 2: HTTPS, 9433 |
| **DC (Datacenter) connection** | Connection 1: Internal  Connection 2: Internal |
| **Direction** | Connection 1: Outbound  Connection 2: Inbound |
| **Direct connection** | Connection 1: Yes  Connection 2: Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

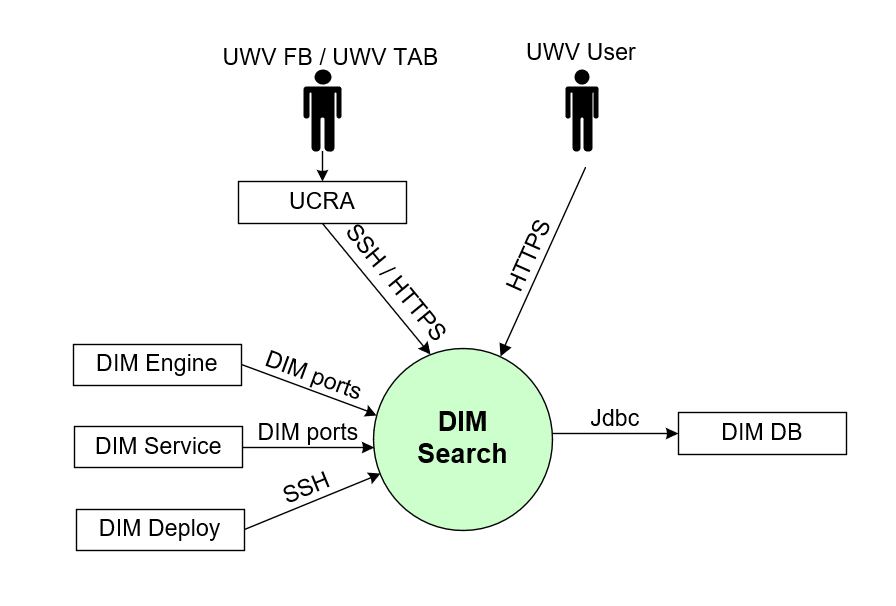
##### DIM DB

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Deploy

|  |  |
| --- | --- |
| **Description** | Internal Application communication with the DIM Management server |
| **Protocol and Port** | SSH, 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Local users  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 |

### DIM Search



#### External entities

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | A user performing functional and technical Application Management tasks. This is mainly related to the configuration of ETL processes and reports, but also management of the application itself. Web Browser and several IIS clients are used for performing these tasks. |
| **Protocol and Port** | SSH, port 22; HTTPS, port 443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | 2-5 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### UWV User

|  |  |
| --- | --- |
| **Description** | A user interacting with the DIM-Infosphere Information Services, either by using the FAT client on the terminal server (UCRA) or directly access to the Webservices.  There are different kind of users:   1. PROD: access the data in the DIM-databases, and not the IIS-environment. 2. ACC: access the data in the DIM-databases, and not the IIS-environment. 3. DEV/TEST: No users, but there are developers and testers |
| **Protocol and Port** | HTTPS, port 443 (InfoSphere Client to IIS Services server) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: RBAC (AD)  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | PROD: 100  ACC: 10  DEV/TEST: 30 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### DIM DB

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Deploy

|  |  |
| --- | --- |
| **Description** | Internal Application communication with the DIM Management server |
| **Protocol and Port** | SSH, 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Local users  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 |

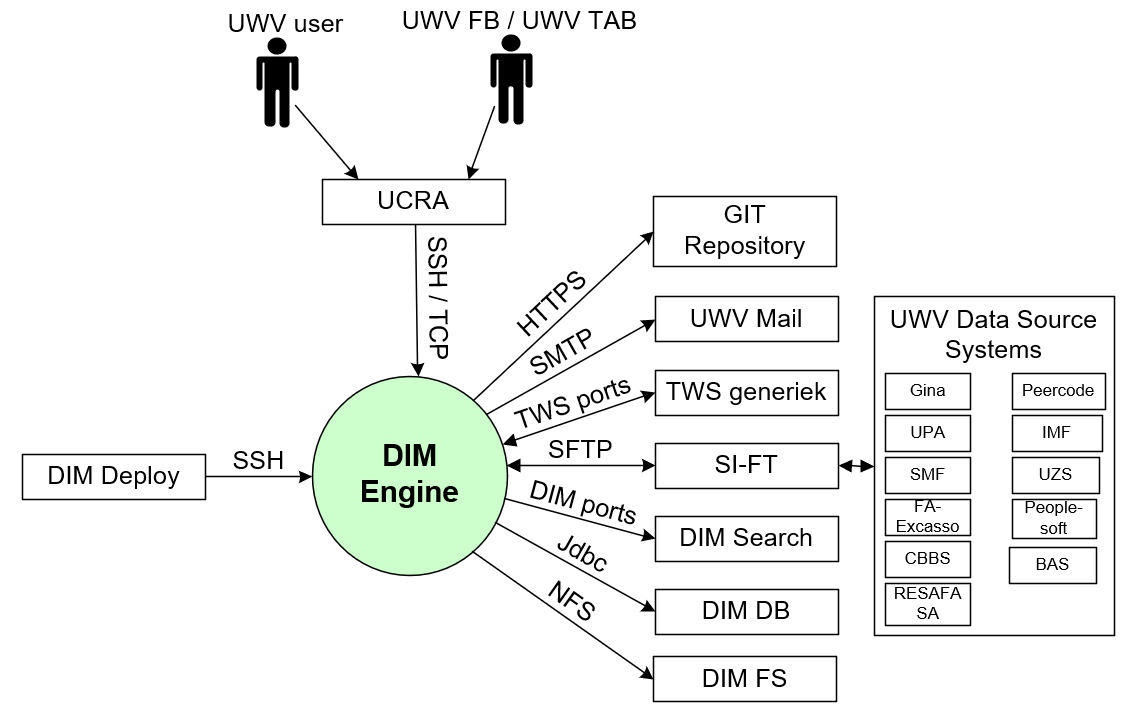
##### DIM Service

|  |  |
| --- | --- |
| **Description** | Internal Application communication with DIM Services server |
| **Protocol and Port** | TCP: 2181, 9092 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Engine

|  |  |
| --- | --- |
| **Description** | Internal Application communication with DIM Engine |
| **Protocol and Port** | TCP: 9092 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

### DIM Engine



#### External entities

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | A user performing functional and technical Application Management tasks. This is mainly related to the configuration of ETL processes and reports, but also management of the application itself. Web Browser and several IIS clients are used for performing these tasks. |
| **Protocol and Port** | SSH, port 22; TCP, port 31538 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | 2-5 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### UWV User

|  |  |
| --- | --- |
| **Description** | UWV users Developpers and Data Engineers as part of UWV Users community to connect only on O and T. |
| **Protocol and Port** | SSH, port 22; TCP, port 31538 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### GIT Repository

|  |  |
| --- | --- |
| **Description** | UWV GIT software version control and source code system in OToD. Used from Test and Development only. |
| **Protocol and Port** | HTTPS, port 443, 7070 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 2 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

##### UWV Mail

|  |  |
| --- | --- |
| **Description** | UWV MailRelay service used by Datastage to send notification mails. |
| **Protocol and Port** | SMTP, port 25 (STARTTLS Option see 4.5.1) |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: server must be added to Mail ACL.  Use certificates: No  Service account: No |
| **Number of users** | 4 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

##### TWS Generiek

|  |  |
| --- | --- |
| **Description** | Generic Workload Scheduler facility for UWV applications, communication over the default TWS ports |
| **Protocol and Port** | Connection 1: TCP, port 31111, 31116 (outbound)  Connection 2: TCP, port 34243 (inbound) |
| **DC (Datacenter) connection** | Connection 1: Internal  Connection 2: Internal |
| **Direction** | Connection 1: outbound  Connection 2: inbound |
| **Direct connection** | Connection 1: Yes  Connection 2: Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 1 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

##### SI-FT

|  |  |
| --- | --- |
| **Description** | Connection with SI-Filetransfer. SI-FT connects with UWV data source systems. It concerns systems with UWV business data from which the DIM fetches data for processing. This concerns only the file pattern.  Currently and during migration project SI-FT puts data only on the DIM Engine server. SI-FT is used for file and dump accesses.  The next data source systems will be accessed:  Gina, UPA, SMF, FA-Excasso, CBBS, Peercode, IMF, UZS, Peoplesoft, RESAFASA, BAS |
| **Protocol and Port** | SFTP, port 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Both (inbound and outbound) |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Database or domain account giving access to the data object.  Use certificates: No  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | All UWV systems can become a source system for DIM. This sizing based on DIM having roughly the same source systems as the combination of the current DWH's DWARFS, UDS and NGP (32 in total). Total volume of input data: typically, 2 TB/day, peaks at 5 TB/day (worst case; assumes all data processed using ETL-pattern).  Existing sourcing currently divided in equal parts export/import, bespoke extracts, and database links. Considering that not all sources will be able to deliver their data via SI FT, sourcing will therefore be roughly evenly split between direct transport and SI FT.  Volume of data (direct connection): 1TB/day, peaking at 2,5 TB/day |

##### DIM Search

|  |  |
| --- | --- |
| **Description** | Internal Application communication with DIM search |
| **Protocol and Port** | TCP: 9092 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM DB

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

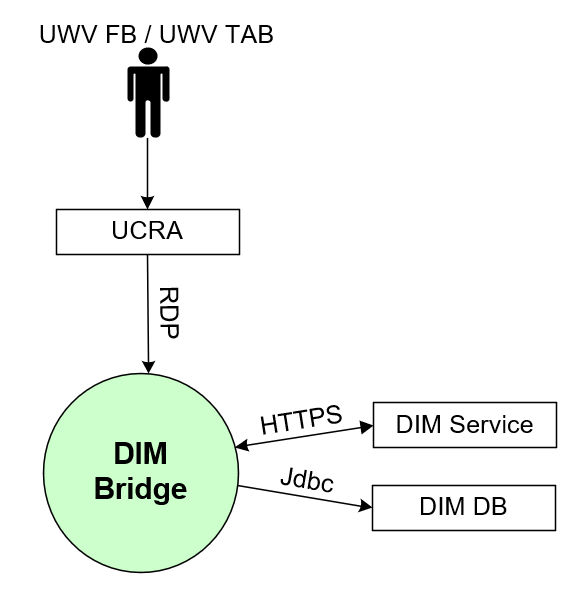
##### DIM FS

|  |  |
| --- | --- |
| **Description** | DIM-Infosphere NFS servers are setup to provide cold and hot storage for the engine and database servers. |
| **Protocol and Port** | NFS: 111, 635, 2049, 4045, 4046 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Deploy

|  |  |
| --- | --- |
| **Description** | Internal Application communication with the DIM Management server |
| **Protocol and Port** | SSH, 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Local users  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 |

### DIM Bridge



#### External entities

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | A user performing functional and technical Application Management tasks. This is mainly related to the configuration of ETL processes and reports, but also management of the application itself. Web Browser and several IIS clients are used for performing these tasks. |
| **Protocol and Port** | RDP 3389 |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | no, via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | 2-5 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

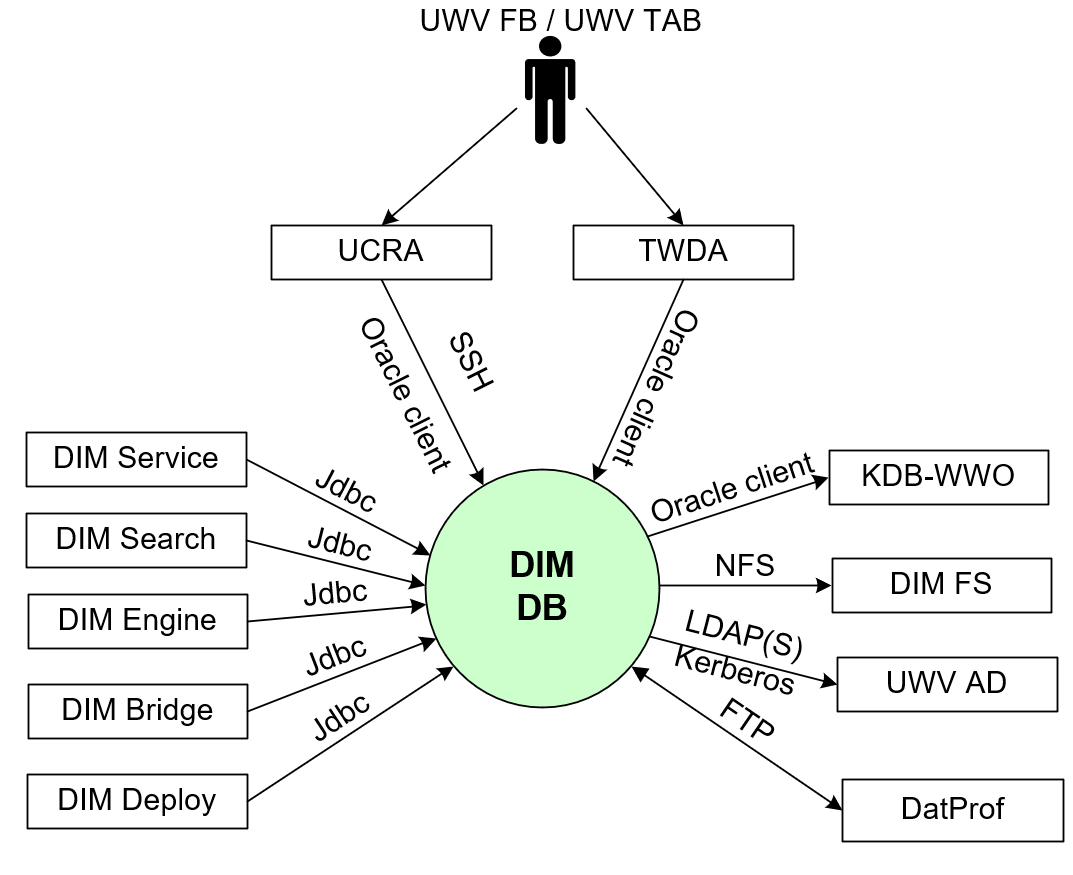
##### DIM Service

|  |  |
| --- | --- |
| **Description** | Internal Application communication with DIM Bridge |
| **Protocol and Port** | Connection 1: HTTPS, 19433  Connection 2: HTTPS, 9433 |
| **DC (Datacenter) connection** | Connection 1: Internal  Connection 2: Internal |
| **Direction** | Connection 1: Inbound  Connection 2: Oubound |
| **Direct connection** | Connection 1: Yes  Connection 2: Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  Use certificates: Yes (Entrust)  Service account: No |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### DIM DB

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

### DIM DB



#### External entities

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | A user performing functional and technical Application Management tasks. This is mainly related to the configuration of ETL processes and reports, but also management of the application itself. Web Browser and several IIS clients are used for performing these tasks. |
| **Protocol and Port** | SSH, port 22; Oracle client, port 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA / TWDA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: No  Service account: No |
| **Number of users** | 2-5 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### KDB-WWO

|  |  |
| --- | --- |
| **Description** | The KDB-WWO is a copy database from the WWO-database (DK instances and HK Instance) which is synchonized to realtime. Database schemas are equal to the schemas of WWO. |
| **Protocol and Port** | Oracle client, 1526 |
| **DC (Datacenter) connection** | Yes |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  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 |

##### DatProf

|  |  |
| --- | --- |
| **Description** | DatProf connection, used for anonymizing the database |
| **Protocol and Port** | FTP, 21 |
| **DC (Datacenter) connection** | Yes |
| **Direction** | Inbound andOutbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  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 |

##### DIM FS

|  |  |
| --- | --- |
| **Description** | DIM-Infosphere NFS servers are setup to provide cold and hot storage for the engine and database servers. |
| **Protocol and Port** | NFS: 111, 635, 2049, 4045, 4046 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 AD

|  |  |
| --- | --- |
| **Description** | Windows Active Directory domain containing resource groups of which UWV domain (KA prod or WPOL) user groups are member, and by which UWV accounts are granted rights.  Kerberos implementation required to use Global groups |
| **Protocol and Port** | Kerberos (88), LDAP (389), LDAPS (636) |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: AD authentication  Use certificates: No  Service account: Yes |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### DIM Bridge

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Engine

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Search

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

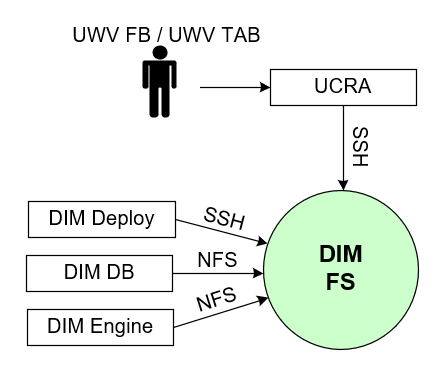
##### DIM Service

|  |  |
| --- | --- |
| **Description** | Database connection to Infosphere DB |
| **Protocol and Port** | Jdbc, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Deploy

|  |  |
| --- | --- |
| **Description** | Internal Application communication with the DIM Management server |
| **Protocol and Port** | Oracle client, 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Local users  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 |

### DIM FS



#### External entities

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | A user performing functional and technical Application Management tasks. This is mainly related to the configuration of ETL processes and reports, but also management of the application itself. Web Browser and several IIS clients are used for performing these tasks. |
| **Protocol and Port** | SSH, port 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: No  Service account: No |
| **Number of users** | 2-5 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### DIM Engine

|  |  |
| --- | --- |
| **Description** | DIM FS (NFS server connection) connection to cold and hot storage |
| **Protocol and Port** | NFS: 111, 635, 2049, 4045, 4046 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

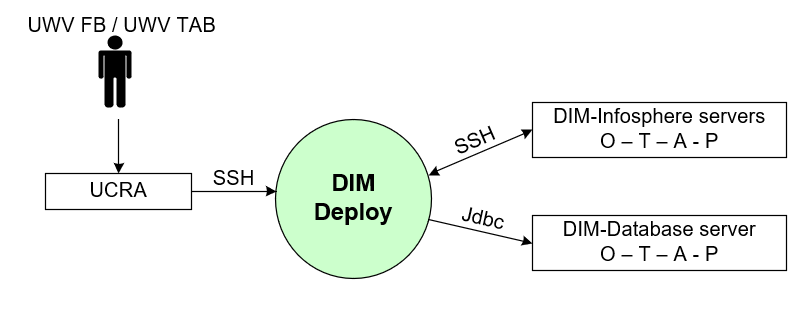
##### DIM DB

|  |  |
| --- | --- |
| **Description** | DIM FS (NFS server connection) connection to cold and hot storage |
| **Protocol and Port** | NFS: 111, 635, 2049, 4045, 4046 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: not specified  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 |

##### DIM Deploy

|  |  |
| --- | --- |
| **Description** | Internal Application communication with the DIM Management server |
| **Protocol and Port** | SSH, 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Local users  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 |

### DIM Deploy



#### External entities

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | A user performing functional and technical Application Management tasks. This is mainly related to the configuration of ETL processes and reports, but also management of the application itself. Web Browser and several IIS clients are used for performing these tasks. |
| **Protocol and Port** | SSH, port 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: No  Service account: No |
| **Number of users** | 2-5 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### DIM-Infosphere servers O – T – A - P

|  |  |
| --- | --- |
| **Description** | UWV FB provides promotions of new versions from DEVELOPMENT to TEST, ACCEPTANCE and PRODUCTION  This is the connection to all DIM Infosphere servers in the Deployment, Test, Acceptance and Production environment |
| **Protocol and Port** | SSH, port 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound and Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 2 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

##### DIM-database server O -T -A - P

|  |  |
| --- | --- |
| **Description** | UWV FB provides promotions of new versions from DEVELOPMENT to TEST, ACCEPTANCE and PRODUCTION  This is the connection to all DIM database servers in the Deployment, Test, Acceptance and Production environment |
| **Protocol and Port** | Oracle Client, port 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 2 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

### DBA-GD RDP



#### External entities

##### UWV FB / UWV TAB

|  |  |
| --- | --- |
| **Description** | DBA Gegegevensdiensten who need to be able to manage the database of DIM Infosphere and DWH |
| **Protocol and Port** | RDP, port 3389 |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: KA AD group membership, RBAC (AD)  Use certificates: No  Service account: No |
| **Number of users** | 5 concurrent users |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not significant |

##### DIM-Infosphere Windows O – T – A - P

|  |  |
| --- | --- |
| **Description** | UWV FB provides promotions of new versions from DEVELOPMENT to TEST, ACCEPTANCE and PRODUCTION  This is the connection to all DIM Infosphere Windows servers in the Deployment, Test, Acceptance and Production environment |
| **Protocol and Port** | RDP, port 3389 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 2 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

##### DIM-Infosphere Linux O – T – A - P

|  |  |
| --- | --- |
| **Description** | UWV FB provides promotions of new versions from DEVELOPMENT to TEST, ACCEPTANCE and PRODUCTION  This is the connection to all DIM Infosphere Linux servers in the Deployment, Test, Acceptance and Production environment |
| **Protocol and Port** | SSH, port 22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 2 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

##### DWH database server O -T -A - P

|  |  |
| --- | --- |
| **Description** | UWV FB provides promotions of new versions from DEVELOPMENT to TEST, ACCEPTANCE and PRODUCTION  This is the connection to all DIM database servers in the Deployment, Test, Acceptance and Production environment |
| **Protocol and Port** | SSH (22), FTP (21) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 2 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

##### DIM-database server O -T -A - P

|  |  |
| --- | --- |
| **Description** | UWV FB provides promotions of new versions from DEVELOPMENT to TEST, ACCEPTANCE and PRODUCTION  This is the connection to all DIM database servers in the Deployment, Test, Acceptance and Production environment |
| **Protocol and Port** | Oracle Client, port 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method or authentication method: Not specified  Use certificates: No  Service account: No |
| **Number of users** | 2 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not significant |

# Functional Requirements

* UWV FB must be able to perform cross environment deployments (DEV to TEST to ACC to PROD promotion flexibility)
* The Acceptance environment must be equally sized (CPU and RAM) as the Production environment and setup in another data center.

# Non-Functional Requirements

## Security & Compliance classifications

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

|  |  |
| --- | --- |
| **Application** | DIM-Infosphere |
| **Owner** | GD |
| **Availability (Beschikbaarheid)** | 2 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 3 |
| **Type of information /Data Classification** | Personal information |

### 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 | Not applicable |

## System and Software requirements

### System (Operating system (OS))

| **Component** | **Operating System** | **Version** |
| --- | --- | --- |
| DIM Service | RHEL | 7.9 |
| DIM Search | RHEL | 7.9 |
| DIM Engine | RHEL | 7.9 |
| DIM Bridge | Windows | 2019 |
| DIM DB | AIX | 7.2 |
| DIM FS | RHEL | 7.9 |
| DIM Deploy | AIX | 7.2 |

### Software (Licenses)

|  |  |
| --- | --- |
| **Software product / component** | **Version** |
| Oracle Database server | 19.3 |
| Oracle advanced compression (Option) | 19.3 |
| Oracle Partitioning (Option) | 19.3 |
| Oracle Tuning Pack | 19.3 |
| Oracle Diagnostics Pack | 19.3 |
| WebSphere Application Server | 9.0 |
| WebSphere Application Server Network Deployment | 9.0.0.9 |
| IBM Tivoli Workload scheduler |  |
| IBM InfoSphere application components |  |
| * Business Automation Workflow Enterprise | 19.0 |
| * InfoSphere Data Architect | 9.1 |
| * InfoSphere DataStage | 11.7 |
| * InfoSphere DataStage and QualityStage Designer | 11.7 |
| * InfoSphere FastTrack | 11.7 |
| * InfoSphere Information Analyzer | 11.7 |
| * InfoSphere Information Analyzer Workbench | 11.7 |
| * InfoSphere Information Governance Catalog | 11.7 |
| * InfoSphere Information Server | 11.7 |
| * InfoSphere Information Services Director | 11.7 |
| * InfoSphere QualityStage | 11.7 |
| * Process Designer | 8.5 |
| RDS License (for DBA-GD-RDP) | 2019 |

Note: This HLD is based on the use of Production licences for both P and A, as the licensed amount of Production licenses is sufficient for both. Should a scale up or out be required in the future, then Production licenses need to be moved from A to P to allow for the P scale up/out, and additional non-Production licenses need to be purchased (by UWV) to allow for the scale up/out of A, and compensate for the production licences moved to P

There is a maximum amount of PVUs (Processor Value Units) licensed (only the Engine- and Services Tier are relevant for PVU counting):

Production:         1540 PVU

Non-Production: 1120 PVU

### Capacity and performance (volumetrics)

Initial required capacity (estimated) P+A:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server** | **#**  **cores** | **#**  **RAM**  **(GB)** | **Persistent**  **Storage**  **(GB)** | **Comments** |
| Client Tier | Existing UCRA servers will be used to deploy the DIM clients.  UCRA sizing will be managed by UCRA functional management. | | | |
| Services Tier | 8 | 32 | 200 |  |
| Engine Tier | 8 | 64 | 1000  500  500 | Scratch disk  Persistent storage  Shared GRID disk (only first node) |
| Fileserver Tier |  |  | 2000  10000 | Shared disk with DB Tier and data providers (HOT)  Initial 10 TB “archive” growing to potentially 40 TB in 5 years. Separate filesystem. (COLD) |
| Database Tier | *A new AIX database server under the CI of DIM-InfoSphere. This server contains only the DIM-Databases.* 2 TB minimum, depending on datafabriek source additions growth in 2 years to 20 TB | | | |
| Metadata bridge Tier | 4 | 16 | 100 |  |
| Enterprise search Tier | 8 | 32 | 500 |  |

Initial required capacity (estimated) for 2 non-P environments O + T:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server** | **#**  **cores** | **#**  **RAM**  **(GB)** | **Persistent**  **Storage**  **(GB)** | **Comments** |
| Client Tier | Existing UCRA servers will be used to deploy the DIM clients.  UCRA sizing will be managed by UCRA functional management. | | | |
| Services Tier | 8 | 32 | 200 |  |
| Engine Tier | 8 | 32 | 200  500  500 | Scratch disk  Persistent storage Shared GRID disk  Shared GRID disk (only first node) |
| Fileserver Tier |  |  | 2000  4000 | Shared disk with DB Tier and data providers (HOT)  Separate filesystem. (COLD) technical equivalent to P+A. |
| Database Tier | *A new AIX database server under the CI of DIM-InfoSphere. This server contains only the DIM-Databases.* | | | |
| Metadata bridge Tier | 4 | 16 | 100 |  |
| Enterprise search Tier | 8 | 32 | 500 |  |

* All delivered source data must be processed within a 21:00 - 07:00 batch window.
* The OS version for the Services-, Engine- and Enterprise search Tier must be RedHat Enterprise Linux 7
* Shared GRID disk is required for application scalability (see also chapter 4.8)
* A Management server (OS = AIX) is needed for promotions between O-T-A-P
* IBM Infosphere implementation is based on 70 PVU’s (Processor Value Unit) per core, the processors in the DXC infrastructure must be compliant. For compliant processors see:

<https://www.ibm.com/software/passportadvantage/pvu_licensing_for_customers.html>

## Availability

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Application Target** | **Application Service Hours** | **Infra Target** |
| Production | UWV | UWV | 98% |
| Acceptance | UWV | UWV | 98% |
| Test | UWV | UWV | 98% |
| Development | UWV | UWV | 98% |

## Security requirements

* UWV FB / UWV TAB requires RDP and SSH access to all DWH environments. Special rights are required. (This does **not apply** to the UCRA environment).
* SSH access to Linux/AIX servers require users in the DXC AD.
* RDP access to DIM Bridge server is required.
* OS permissions are required for: UWV FB, Tester, Developer.
* UWV FB must be able to perform:
  + Updates and upgrades, bring services down for (OS) maintenance support.
  + Cleaning
  + Authorizations on group level
  + Monitoring and performance analyses
  + Deployments.
  + Full rights on Oinstall group on DB server.
* DIM must be connected to the UWV AD directly for end user authentication and authorization within the application environment.
* IIS software is identically designed in all OTAP environments. This requires authorization based on ABS groups, so users can only do what they are authorized to do.
* On the IBM InfoSphere MicroServices Tier a UWV signed certificate is used to run kubectl via console
* The Docker and Kubernetes technologies provide the foundation for running microservices (search servers). Networking has a crucial role in this architecture. Kubernetes manages an internal Software Defined Network (the cluster network) and an internal name resolution system (DNS).

### System logging

No specific system logging requirements are applicable

## System management

* UWV performs part of the system management, primarily focused on OTAP-promotion and software configuration, by itself. A separate management RACI (Responsible, Accountable, Consulted, and Informed) will be created to document the role segregation between DXC and UWV. A separate document describing the C+ level security rights is created. (See comment at 4.4)
* UWV provides the TAB service. To be able to perform these tasks RDP and SSH access to the servers is required. UWV requires additional rights on the server to be able to perform these tasks, this is described in a separate document.
* DXC provides operating system and backup management.

### 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 | No |

## Backup and Recovery

|  |  |  |
| --- | --- | --- |
|  | **Default** | **Deviation (when applicable)** |
| Backup | deviating backup | Backup exclusion: scratch and the grid disk on the engine server  Database: Archive log backup -> every 30 minutes |
| Restore | no specific restore order | Not applicable |
| Dependency | no dependencies | Not applicable |

## Storage replication

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

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

## Scalability

* The Engine Tier Must be able to scale horizontally and vertically. Horizontal scalability is provided by the application therefore the Engine Tier will be setup in an IBM Infosphere Data Stage GRID configuration.
* The Services Tier must be vertically scalable, it is setup on a single server as horizontal growth at this Tier is not expected in near future.
* The server topology of all environments (OTAP) needs to be the same.

## Disaster Recovery

No specific disaster recovery requirements applicable.

## Infrastructure Technical Constraints

/var and rootvg require 350 GB.

## DXC TAB requirements

|  |  |
| --- | --- |
| **Category** | **Description** |
| Deployment | not applicable, is performed by UWV |
| Other TAB applicable requirement | not applicable, is performed by UWV |

# Solution

## Architectural Decisions

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 1** | 01 | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Deployment |
| **Decision** | Existing DXC UCRA servers will be used to host Infosphere FAT clients | | |
| **Problem Statement** | The Infosphere suite contains several FAT clients for which a host must be found. | | |
| **Assumptions** | The FAT clients are not use for analytics purposes. Current behaviour of the FAT clients show that he resources utilization is not high | | |
| **Motivation** | This is the preferred UWV option for "niche "development/admin clients. Use of UCRA for FAT clients is the preferred option of the DataFabriek project and has been approved by UWV functional management of UCRA. | | |
| **Alternatives** | Clients on dedicated notebooks. | | |
| **Justification** | The FAT client does not cause heavy load, the existing UCRA environment is able to handle this. | | |
| **Implications** | Clients need to be installed on the existing UCRA servers, this is out of scope for this HLD  The possibility exists clients produce more load then expected in which case additional resource capacity can be added. | | |

Decision 1: Existing DXC UCRA servers will be used to host Infosphere FAT clients

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 2** | 02 | **Topic** | VLAN |
| **Status** | Approved | **Subject Area** | Deployment |
| **Decision** | A new security zone “DWH” is created in the legacy network for OTAP | | |
| **Problem Statement** | UWV performs TAB activities and database management for which they require elevated access rights, therefore an isolated (ringfence) solution is required. | | |
| **Assumptions** | Systems can only exist in 1 security zone. The new DWH zone replaces all other security zones suchs a FrontOffice, BackOffice, Kluis, Application Mgmt for the DWH legacy systems | | |
| **Motivation** | Isolate the DWH legacy servers from other UWV business application servers. | | |
| **Alternatives** | Host servers in the same zone as the other servers in AIX legacy. | | |
| **Justification** | System Management and TAB tasks requiring elevated permissions are performed by UWV instead of DXC. | | |
| **Implications** | A new security zone is a special situation and not standard available. The security zone is created and documented in all relevant documentation. The default security zones available in the legacy network (FrontOffice, BackOffice, Kluis, Application Mgmt) should not be used by DWH legacy systems, only the new DWH security zone should be used | | |

Decision 2: A new security zone “DWH” is created in the legacy network for OTAP

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 3** | 03 | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Deployment |
| **Decision** | DIM-Infosphere databases will be hosted on a new DB server which will be part of the DIM-Infosphere CI. | | |
| **Problem Statement** | All DWH databases are hosted together on database servers. | | |
| **Assumptions** | N.A. | | |
| **Motivation** | To separate DIM-Infosphere databases from DWH databases and bring them under the DIM-Infosphere CI. | | |
| **Alternatives** | Host DIM-Infosphere databases on the current DWH database servers. | | |
| **Justification** | Agreed with UWV | | |
| **Implications** | N.A. | | |

Decision 3: DIM-Infosphere databases will be hosted on a new DB server which will be part of the DIM-Infosphere CI

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 4** | 04 | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Deployment |
| **Decision** | The DIM-Infosphere database server will be hosted on AIX | | |
| **Problem Statement** | Because all the DIM-Infosphere scripting is based on an AIX database server the databases for DIM-Infosphere must be run on an AIX server. | | |
| **Assumptions** | N.A. | | |
| **Motivation** | To avoid a huge amount of time to rewrite the existing scripts. | | |
| **Alternatives** | N.A. | | |
| **Justification** | Rewrite the scripts to function with a RHEL will take to much time | | |
| **Implications** | N.A. | | |

Decision 4: The DIM-Infosphere database server will be hosted on AIX

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 5** | 05 | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Security |
| **Decision** | The Legacy (AIX) DIM-Infosphere servers (DIM DB and DIM Deploy) will be hosted in the DWH security zone. | | |
| **Problem Statement** | In which security zone must the DIM-Infosphere AIX servers be hosted. | | |
| **Assumptions** | N/A | | |
| **Motivation** | UWV performs System Management and TAB tasks for DIM Infosphere, for these tasks UWV receives elevated permissions. The DIM-Infosphere are not fully managed by DXC therefore they must be isolated. In the legacy network this isolation is provided by a new dedicated DWH security zone | | |
| **Alternatives** | Host this server in the standard security zone in Legacy. | | |
| **Justification** | Due to the required elevated rights an isolated solution is necessary. | | |
| **Implications** | Standard security zones in Legacy are not available for DIM infosphere | | |

Decision 5: The Legacy (AIX) DIM-Infosphere servers (DIM DB and DIM Deploy) will be hosted in the DWH security zone.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 6** | 06 | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Hosting |
| **Decision** | RHEL NFS servers are used to host the cold and hot storage for the engine and database servers. | | |
| **Problem Statement** | A large amount of storage is required for the DIM-Infosphere archive (HOT and COLD storage). Initially the archive was planned to be hosted on the engine server but due to the large amount of data the maximum VM size (7 TB) in the Private Cloud is exceeded. How to host the the HOT and COLd storage in the Private Cloud without exceeding the maximum VM size | | |
| **Assumptions** | It is not mandatory that the HOT and COLD storage are hoisted by the engine server, it can be hosted separately. HOT and COLD can be separated as well | | |
| **Motivation** | Setting up an NFS servers has advantages; It is simple to extend the storage. Restore and backup is less complex to configure. | | |
| **Alternatives** | Use a physical server to avoid the VM size limitations, preferred is to use the Private Cloud | | |
| **Justification** | It is preferred to use the Private Cloud as a landing platform | | |
| **Implications** | Use one or more VM’s to host the COLD and HOT storage instead of assigning the storage to the Engine server | | |

Decision 6: RHEL NFS servers are used to host the cold and hot storage for the engine and database servers.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 7a** | 07a | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Hosting |
| **Decision** | In Production and Acceptance 2 NFS servers will be used (2 NFS servers in production and 2 NFS servers in Acceptance), 1 for the COLD storage and 1 for the HOT storage. | | |
| **Problem Statement** | How to host HOT and COLD storage based on the initial capacity requirement specified in chapter 4.2 | | |
| **Assumptions** | Cold storage must be initially 10 TB and can grow in 5 years till 40 TB, it is agreed that we can use a VM in the non-automated cloud that exceeds the limit of 7 TB | | |
| **Motivation** | DIM-Infosphere capacity requirements will change over the years. | | |
| **Alternatives** | Physical server | | |
| **Justification** | Initial storage requirements as specified in 4.2 | | |
| **Implications** | 1 RHEL VM in the non automated cloud for HOT storage (2 TB)  1 RHEL VM in the non automated cloud for COLD storage (10 TB)  The NFS server must be periodically monitored to see if the backup times are still acceptable or that another solution must be designed | | |

Decision 7a: In Production and Acceptance 2 NFS servers will be used, 1 for the COLD storage and 1 for the HOT storage

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 7b** | 07b | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Hosting |
| **Decision** | In Test and Development 1 NFS server for Test and 1 NFS server for Development will be used, COLD and HOT storage are combined. | | |
| **Problem Statement** | How to host HOT and COLD storage based on the initial capacity requirement specified in chapter 4.2 | | |
| **Assumptions** | HOT and COLD storage can be combined on the same NFS server | | |
| **Motivation** | DIM-Infosphere capacity requirements will change over the years. | | |
| **Alternatives** | Physical server | | |
| **Justification** | Initial storage requirements as specified in 4.2 | | |
| **Implications** | 1 RHEL VM in the non automated cloud for HOT and COLD storage (6 (2+4) TB | | |

Decision 7b: In Test and Development 1 NFS server for Test and 1 NFS Server for development will be used, COLD and HOT storage are combined.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 8** | 08 | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Deployment |
| **Decision** | A filesystem is configured on the first Engine server | | |
| **Problem Statement** | The Engine servers must share a filesystem with the NFS server and data (Inbox) providers (SI-FT, DRL). This share can be divided in a “Hot” (e.g. Inboxes) and a “Cold” (Archive) part.  Initially there is only 1 Engine server, but due to the GRID setup this amount can grow in future. Servers in the GRID should be as identical as possible. | | |
| **Assumptions** | This share can be seen as the master under the slaves. | | |
| **Motivation** | This choice adheres to the separation of duty between database and filesystem services. | | |
| **Alternatives** | 1. Deploy the NFS share at the Engine server 2. Deploy the NFS share at the DB server 3. Deploy the NFS share at another DIM server | | |
| **Justification** | Alternative 1 is most logical as the Engine will make most use it. | | |
| **Implications** | Network File system to be published by first Engine server and mounted on DB server(s). This first Engine server also must run an FTP server daemon to provide file services for data providers.  If in future the Engine GRID is expanded with more nodes, these nodes will differ slightly from the first one (no NFS shares and no FTP server). | | |

Decision 8: A filesystem is configured on the first Engine server

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 9** | 09 | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Hosting |
| **Decision** | DIM Deploy (management server) is hosted in DWH Production and will be used for promotion activities between O, T, A and P. | | |
| **Problem Statement** | New developed IIS configurations will have to be promoted from Development to Test to Acceptance and to Production, only the DWH security zone should be used (see decision 2) | | |
| **Assumptions** | Crosszone connections from the DWH production security zone to the Private Cloud security zones are allowed | | |
| **Motivation** | In legacy there is no micro segmentation therefore the dedicated DWH security zone is created | | |
| **Alternatives** | N.A. | | |
| **Justification** | OTAP deployments are done by UWV this requires crosszone connections | | |
| **Implications** | Connections to O, T, A and P legacy and other generic OTAP environments (for DIM-Infosphere) must be allowed from this server.  Management server is only available in Production not in A, T or O | | |

Decision 9: DIM Deploy (management server) is hosted in DWH Production and will be used for promotion activities between O, T, A and P

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 10** | See caption | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Security |
| **Decision** | UWV TAB (Technical Application Management) requires special permissions | | |
| **Problem Statement** | To be able to perform technical application management UWV needs the necessary permissions on the servers. | | |
| **Assumptions** | Permissions are described in a separated document. | | |
| **Motivation** | Necessary to be able to perform technical application management. | | |
| **Alternatives** | DXC will perform TAB | | |
| **Justification** | Decided and agreed between UWV and DXC management | | |
| **Implications** | UWV is responsible for a part of the system management. | | |

Decision 10: UWV TAB (Technical Application Management) requires special permissions

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 11** | See caption | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Security |
| **Decision** | The private cloud (Windows and Linux) DIM-Infosphere servers (DIM APP, DIM Engine, DIM Bridge and DIM FS) will be hosted in the Micro BackOffice security zone. | | |
| **Problem Statement** | How to keep the private cloud servers separated from other UWV business application servers due to the required elevated access rights | | |
| **Assumptions** |  | | |
| **Motivation** | Technical application management is performed by UWV which require elevated access rights. Micro BackOffice is a microsegmented security zone | | |
| **Alternatives** | Host these servers on a non-micro-segmented security zone. | | |
| **Justification** | UWV requires elevated access rights | | |
| **Implications** | Each connection requires a firewall opening (request) | | |

Decision 11: The private cloud (Windows and Linux) DIM-Infosphere servers (DIM APP, DIM Engine, DIM Bridge and DIM FS) will be hosted in the Micro BackOffice security zone

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 12** | See caption | **Topic** | Standards |
| **Status** | Approved | **Subject Area** | Security |
| **Decision** | The DIM-Infosphere Search server will be hosted in the Micro BackOffice Security Zone. | | |
| **Problem Statement** | UWV User connect to this server from UWV workplace. Normally servers that have primary a presentation function must be hosted in FrontOffice | | |
| **Assumptions** | N/A | | |
| **Motivation** | This server is an application server. IBM Information Server Enterprise Search is an extension to IBM InfoSphere Information Server services tier. This extension provides enterprise search and related capabilities. It consists of self-contained microservices, which run as Docker containers inside a Kubernetes cluster. | | |
| **Alternatives** | N/A | | |
| **Justification** | Confirmed with UWV and DXC security. | | |
| **Implications** | Each connection requires a firewall opening (request). | | |

Decision 12: The DIM-Infosphere Search server will be hosted in the Micro BackOffice Security Zone.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID 13** | See caption | **Topic** | Remote Access |
| **Status** | Approved | **Subject Area** | Remote Access for DBA-GD |
| **Decision** | A dedicated RDP server for DBA GD (GegegevensDiensten) is added to the DIM Infosphere application and is placed in the DXC Application management zone because RDP access to the different domains from 1 system is required for their daily work | | |
| **Problem Statement** | Currently UCRA-T is used to access the O-T-A-P environment for DIM infosphere and DWH | | |
| **Assumptions** | Only 4 persons should be able to access the RDP server | | |
| **Motivation** | The Generic UCRA solution cannot provide the required tooling and connectivity, therefor a dedicated system for DBA-GD is added | | |
| **Alternatives** | N/A | | |
| **Justification** | Confirmed with UWV architect | | |
| **Implications** | Each connection requires a firewall opening (request). | | |

Decision 13: A dedicated RDP server for DBA GD (GegegevensDiensten) is added to the DIM Infosphere application and is placed in the DXC Application management zone because RDP access to the different domains from 1 system is required for their daily work

## Node descriptions and zone-projections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Zone** | **Domain** | **Server Type** | **Node ID** | **Infra Service Level** |
| DWH | Production | Management server | DIM-Man-P | Bronze |
| DXC Application Mgmt | Production | RDP Server | DBA-GD-RDP-P | Bronze |
| Micro BackOffice | Production | Services Server | DIM-Serv-P | Bronze |
| Micro BackOffice | Production | Engine Server | DIM-Eng-P | Bronze |
| Micro BackOffice | Production | Bridge Server | DIM-Bri-P | Bronze |
| Micro BackOffice | Production | Search Server | DIM-Sea-P | Bronze |
| Micro BackOffice | Production | NFS Server | DIM-NFS-C-P | Bronze |
| Micro BackOffice | Production | NFS Server | DIM-NFS-H-P | Bronze |
| DWH | Production | Database server | DIM-DB-P | Bronze |
| Micro BackOffice | Acceptance | Services Server | DIM-Serv-A | Bronze |
| Micro BackOffice | Acceptance | Engine Server | DIM-Eng-A | Bronze |
| Micro BackOffice | Acceptance | Bridge Server | DIM-Bri-A | Bronze |
| Micro BackOffice | Acceptance | Search Server | DIM-Sea-A | Bronze |
| Micro BackOffice | Acceptance | NFS Server | DIM-NFS-C-A | Bronze |
| Micro BackOffice | Acceptance | NFS Server | DIM-NFS-H-A | Bronze |
| DWH | Acceptance | Database server | DIM-DB-A | Bronze |
| Micro BackOffice | Development | Services Server | DIM-Serv-D | Bronze |
| Micro BackOffice | Development | Engine Server | DIM-Eng-D | Bronze |
| Micro BackOffice | Development | Bridge Server | DIM-Bri-D | Bronze |
| Micro BackOffice | Development | Search Server | DIM-Sea-D | Bronze |
| Micro BackOffice | Development | NFS Server | DIM-NFS-CH-D | Bronze |
| DWH | Development | Database server | DIM-DB-D | Bronze |
| Micro BackOffice | Test | Services Server | DIM-Serv-T | Bronze |
| Micro BackOffice | Test | Engine Server | DIM-Eng-T | Bronze |
| Micro BackOffice | Test | Bridge Server | DIM-Bri-T | Bronze |
| Micro BackOffice | Test | Search Server | DIM-Sea-T | Bronze |
| Micro BackOffice | Test | NFS Server | DIM-NFS-CH-T | Bronze |
| DWH | Test | Database server | DIM-DB-T | Bronze |

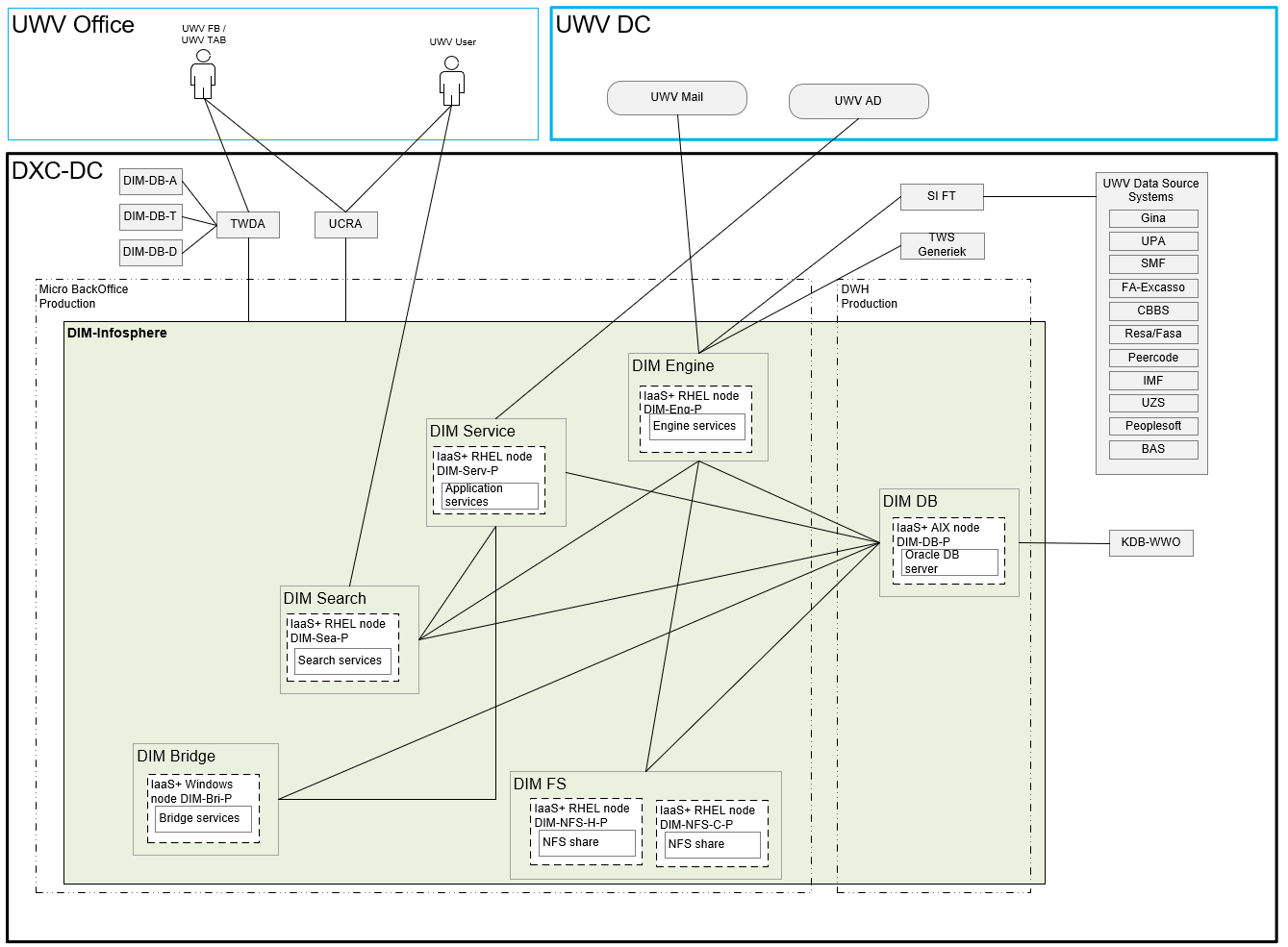
### DNS (customer facing name)

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

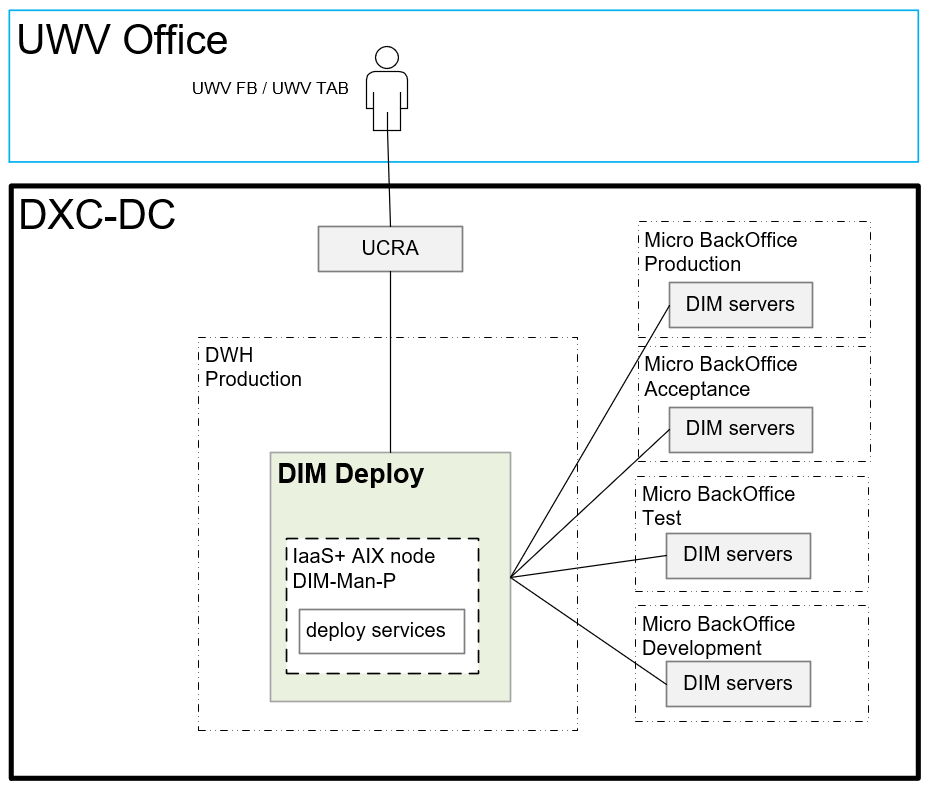
## System diagram – Production

To increase the readability 3 diagrams are displayed: Application, Deployment, DBA GD – RDP access

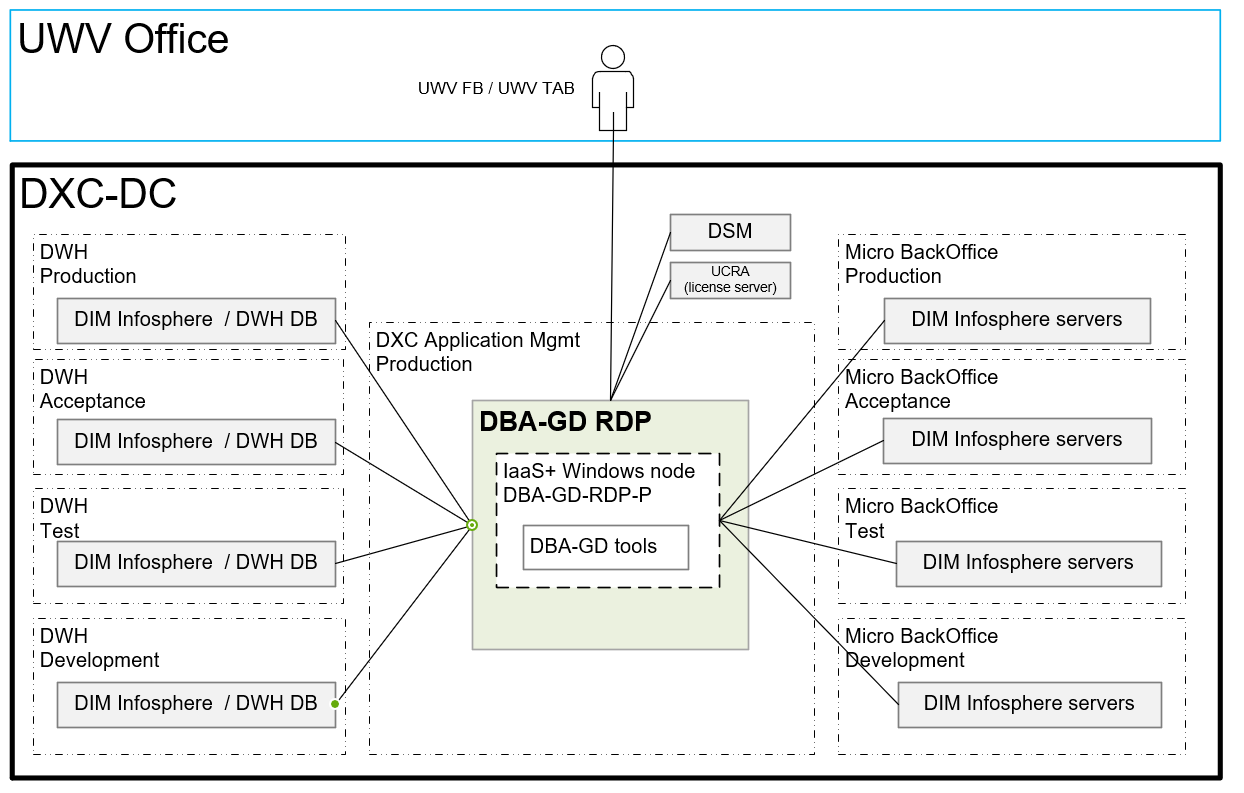
### Application



### Deployment

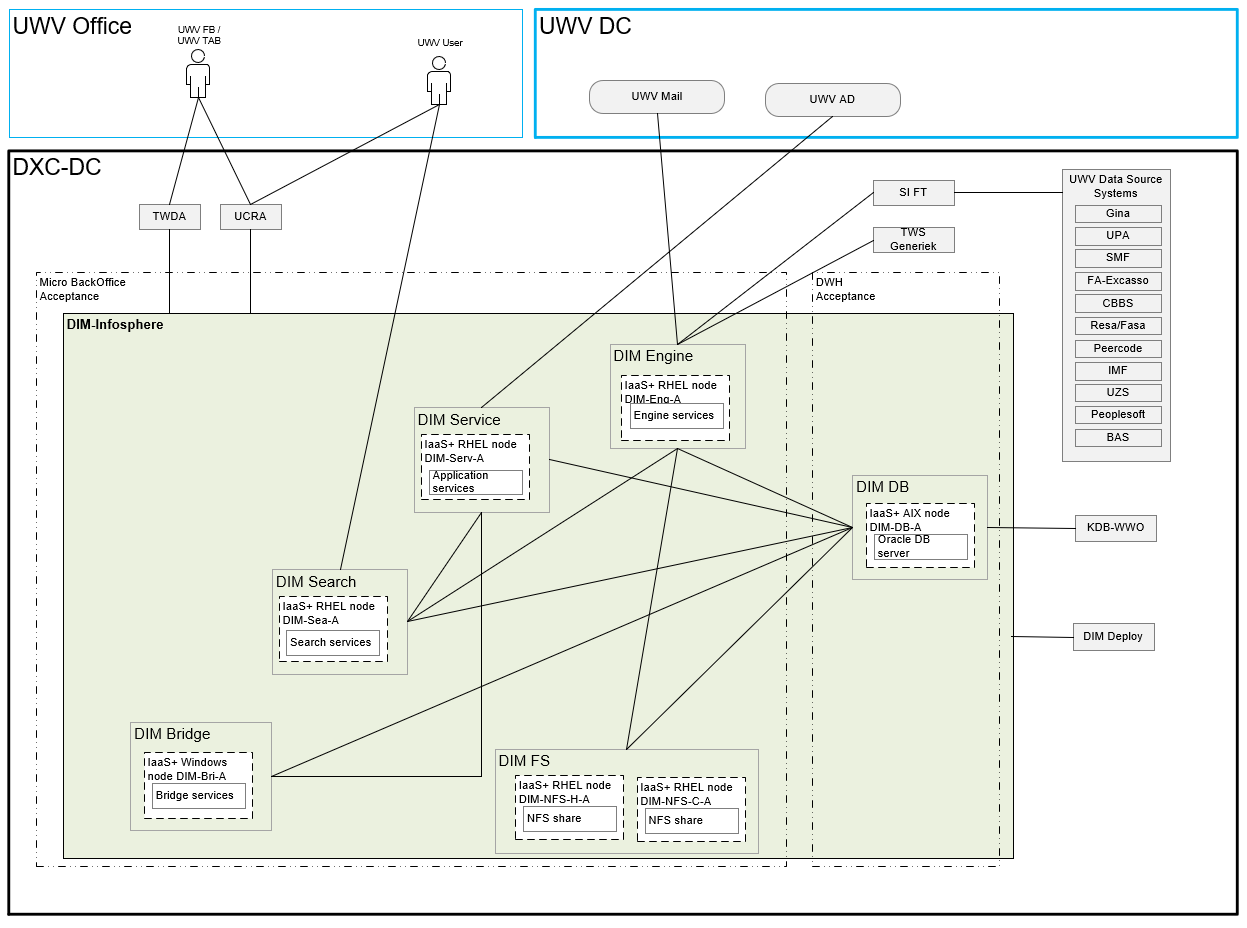


### DBA GD - RDP access

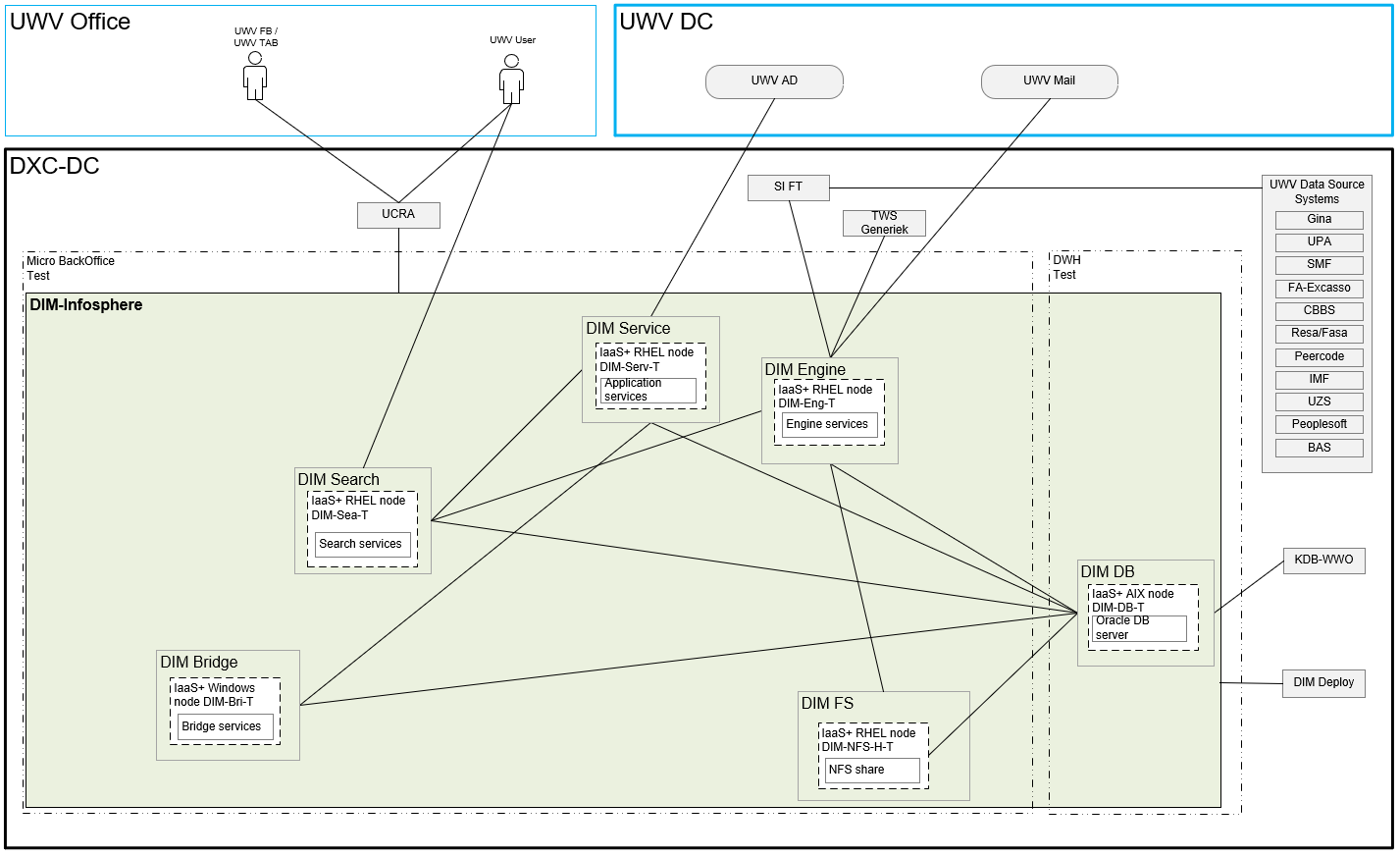


## System diagram – non-Production

### Acceptance



### Test



### Development

Separate diagram not provided because this is the same as test.

## SBB’s

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

Remark 1: No SBB’s are specified. IaaS-GD is delivered, and the service is described in the so-called C+ document.

Remark 2: The DXC Infrastructure uses processor type Xeon®2, which is compliant with the 70 PVU’s per core (requirement in 4.2.3).

## Load balancers

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Load balancer** | **Load balancer type** | **Description** |
| 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 DMZ security zone in Legacy is created | No |  |
| 2 | Crosszone connections from DWH Deploy (DWH Production) DIM servers in Acceptance, Test and Development | Yes | 20220810-007-A |
| 3 | UWV performs TAB Tasks. Special permissions are necessary | No | Mitigated by TAB C+ scenario |
| 4 | OS RedHat Enterprise 7.9 is not mainstream Middleware on technology roadmap | Yes | 20221021-001-A |
| 5 | Windows 2016SE OS not mainstream Middleware on technology roadmap | Yes | 20221019-002-A |
| 6 | Oracle Database Server Client software 12.2 not mainstream software | Yes | 20221024-002-A |
| 7 | Crosszone connection: DIM DB (Development) to KDB-WWO (Test) | Yes | 20230207-002-A |
| 8 | Crosszone connection: DIM DB (Development) to DWH-BO (Test) | Yes | 20230209-003-A |
| 9 | Patching not done: Apache Commons Arbitrary Code Execution (ACE) Vulnerability (Text4Shell) (CVE-2022-42889) Critical 9.8 score | Yes | 20230428-001-A |
| 10 | Patching not done: No Patching Apache Log4j Denial of Service (DOS) Vulnerability (Log4Shell) | Yes | 20230428-002-A |
| 11 | Old software IBM WebSphere | Yes | 20230428-003-A |
| 12 | Patching not done: IBM WebSphere | Yes | 20230428-004-A |
| 13 | JMX Authentication Not Enabled on Localhost Interface  20230428-006-A Patching not done: Spring Framework Denial of Service (DoS) Data Binding Vulnerability | Yes | 20230428-005-A |
| 14 | Bad configuration Weak SSL/TLS Key Exchange | Yes | 20230428-007-A |
| 15 | TWDA in Prod needs to be able to connect to DIM-Infosphere DBes in Development, Test and Acceptance.  These are Cross zone connections | Yes | PER0003193 |

## Service Management

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

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

The DIM search server (kubernets) require an Internal Docker IP range (see also 4.4). This IP range is only used internally therefore a private IP range is configured

The following URL describes the used application architecture in more detail:

[Architecture of IBM Information Server Enterprise Search - IBM Documentation](https://www.ibm.com/docs/en/iis/11.7?topic=concepts-architecture-information-server-enterprise-search)

## Security

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

### User Authentication and Authorization

UWV user and UWV FB / UWV TAB on windows server.

Variation 1 (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.

UWV user and UWV FB / UWV TAB on Linux server

Variation 2 (LDAP – UWV AD group - using nested groups is not possible): User Authentication and Authorization will be performed against the UWV AD using a direct LDAP connection, for applications that cannot use nested groups.

UWV FB / UWV TAB. For RDP and SSH access to servers and for access to UCRA

Variation 3 (Local - local login using DXC AD account): User Authentication and Authorization will be performed localy using a user account in the DXC resource domain, Linux OS access for UWV users requested through the ABS IAM system and changes in PDXC.

Details are specified in Appendix C

### Firewalls

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

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 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 DIM-Infosphere the following is applicable:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Connection Type** | **Between (component 1)** | **And (component 2)** |
| Internal | SSH | Management Server | DIM linux servers (V.S) |
| Internal | TCP | DIM Services server | DIM Bridge server |
| Internal | NFS | DIM Engine server | DIM NFS Servers |
| Internal | Oracle Client | DIM Engine server | DIM DB Server |
| Internal | TCP | DIM Services server | DIM search server (2) |
| Internal | Oracle Client | DIM Search server | DIM DB server |
| Internal | TCP/UDP | DIM Bridge server | DIM Services server |
| Internal | Oracle Client | DIM Bridge server | DIM DB Server |
| Internal | NFS | DIM DB server | DIM NFS Servers |
| External (outside DXC) | HTTPS | UWV Workplace | Search server |
| External (outside DXC) | HTTPS | UWV Workplace | Bridge server |
| Internal | Oracle Client | Services server | DIM DB Server |
| External (outside DXC) | SMTP | Engine server | UWV Mail |
| External (outside DXC) | LDAP/SSL | Services server | WPOL (UWV AD) |
| Internal | Oracle Client | DIM DB server | KDB-WWO |
| Internal | TCP | DIM Engine | DIM Search |
| Internal | RDP | Management Server | Bridge Server |

For details see Appendix B

# Potential future improvements

|  |  |  |
| --- | --- | --- |
| **ID** | **Proposed improvement** | **Reason** |
| 1 | UWV to separate Presentation and Application Tier | To comply with the NORA- based security model, presentation and application can be hosted in different security zones |
| 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 |

# 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) | 17-08-2022 |
| Nic van Sprongen | UWV Lead Architect (verification) | 11-10-2022 |
| Rick van Diemen (delegated to Hans Kreisel) | DXC Account Delivery Lead (acceptance) | 22-08-2022 |

**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 0.1 | 11-03-2022 | DXC architecture team | First iteration of the HLD based on IBM HLD v1.4.1 |
| SharePoint version 0.6 | 15-07-2022 | DXC architecture team | Second iteration of the HLD   1. Updated with input of UWV 2. NFS servers added to design 3. DWH (ring fenced) VLAN added to design for Legacy AIX servers. |
| Verification version 0.8 | 17-08-2022  22-08-2022  09-09-2022 | DXC architecture team | Third iteration of the HLD   1. 0.8 – Ready for Account review   0.8.1 – Account review comments processed (context diagram updated for complex application to have a good understanding of the connectivity and some other minor updates)  0.8.2 – DIM TDA review comments processed. Updated some context diagrams, renamed component DIM app to DIM service, removed 1 EtP, added DIM Infosphere licenses to chapter 4.2.1 and modified the NFS (O and T) architechtural decion to provide more clarity |
| Verification version 0.9 | 12-09-2022 | DXC architecture team | Design Office verification |
| Version 1.0 | 7-10-2022 | DXC architecture team | Positive verified HLD  Update 7-10-2022   * Updated to the latest template version (1.86) * 4.1: Updated BIV rating to 2, 2, 3 as mentioned in the latest repository (was wrongly documented as 2, 2, 1 with a remark that 2,2,3 was used) * 4.2.2: Added note regarding PVU licensing based on the TDA GD feedback * 4.2.3: Added PVU=70 processor requirement based on the TDA GD feedback (in 5.5 a remark is added that the DXC Infrastructure is compliant) * 5.5 Updated SBB, stating that IaaS GD is delivered instead of the standard IaaS+ for DXC Managed systems   Update 12-10-2022   * Comments form UWV Design Office processed |
| Version 1.1 | 03-05-2023 | DXC architecture team | Post implementation HLD   * 18-10-2022: Updated Appendix A -> changed security zone BackOffice to Micro BackOffice for Acceptance servers * 19-10-2022: Updated Appendix A -> changed Windows 2019 to Windows 2016 in node details * 25-10-2022: Updated database disk size from 256 to 250 GB   09-11-2022: Update storage layout for the DIM Search servers: OS: 100 GB, APP1: 400 GB (250+150), APP2: 250 GB  09-11-2022: Appendix A – Software: Updated IBM Websphere application server from 4-middleware to 5-application, it is not a stand-alone installation but comes with the Infosphere installation  14-11-2022: Added Kerberos to the DIM DB Context Diagram and included Kerberos in the Appendix A Software  Added DIM Deploy to the Dim DB Context Diagram and added DIM database servers to the DIM Deploy Context Diagram  16-11-2022:  Added UWV AD ports 88, 389, 3268, 3269 to DIM Service -> UWV AD connection  22-11-2022:   * Updated storage layout for the Management server (DIM-Man-P), Server was requested as application server but should have been requested as an Oracle database servers (ASM) disk (from 100+500 to 100+100+100+300+100+150+50) * Added Oracle Cloud control, Oracle NET service and Oracle NET client to the software for DIM-Man-P as 5-application   24-11-2022   * UWV requested additional RAM and storage for DIM-DB-D and DIM-DB-T, updated HLD (appendix A) accordingly:   + RAM: from 32 GB to 80 GB   + Data (disks): from 2 TB to 10 TB   + Fra (disks): from 200 GB to 1000 GB   30-11-2022   * On request of UWV the following was updated in Appendix A – Software:   + Removed Websphere application server from the engine, bridge, and search server   + Added 5-application - Websphere application server ABS agent to the engine servers * On request of UWV the following was update in Appendix A- Storage:   + Added 1 TB to the management server (DIM-Man-P), needed for the deployment pipeline and the data transfer between the different servers   + Added 250 GB to the engine servers to be able to create the file system for   /w001/app and /w001/logs   01-12-2022   * On request of UWV the following was updated in Appendix A – Storage to support the IIS installation:   + Added 250 GB to the search servers   + Replaced 500 GB disk with 250 GB disk on the engine servers * NFS servers for O and T were missing 2 TB of storage (compared with the requirements)   + Added 2 TB disk to the NFS servers in O and T   31-01-2023  Updated the following on request of UWV   * Added storage to DIM-DB-A and DIM-DB-P (Appendix A – storage) :   + ASM DATA: + 6 TB (2 x 3TB)   + ASM FRA: + 1 TB (4 x 250 GB) * Increased cpu and memory for DIM-DB-A and DIM-DB-P (Appendix A – node details):   + From 4 to 5 CPU   + From 32 GB to 100 GB RAM   13-02-2023   * Added DBA GD RDP (So-called DBA “opstap server” for DBA Gegevensdiensten (so they can perform their deployments) instead of using UCRA-T)   + Updated introduction, licenses, context diagram, architectural decisions, system diagram, Appendix A * Added EtP for the crosszone connection DIM DB -O to KDB-WWO-T * Added EtP for the crosszone connection DIM DB -O to DWH-BO-T * Added TWDA connection to DIM-DB * Added DIM-DB <-> DatProf connection * Added reference to Docker IP in 4.4 and 5.8   01-03-2023  Updated the following on request of UWV   * Added storage to DIM-DB-A and DIM-DB-P (Appendix A – storage) :   + ASM DATA: + 12 TB (4 x 3TB)   31-03-2023:  Updated Backup requirements:   * Archive log backup -> every 30 minutes   Updates Appendx A – Software:   * Added “IBM Workload scheduler Fault Tolerant Agent: for the Engine servers * Added dos2unix and unix2dos to the engine servers   Updated Appendix A – Node details:   * DIM-DB-P and DIM-DB-A: cpu from 5 to 8   21-04-2023:  Updated Appendx A – Storage on request of UWV:   * DIM-DB-P , DIM-DB-A , DIM-DB-D , DIM-DB-T: additional 300 GB disk for backups   03-05-2023:  Changes to chapter 5.7:   * RAL ID’s 9 to 14 added   Changes to chapter 2.2.8   * SSH connection added to the context diagram from the jump server to the DIM-DB server |
| Version 1.2 | 02-06-2023 | DXC architecture team | TWDA Production needs to have access to DIM-DB in Acceptance, Test and Development   * 5.7: EtP 15 added * 5.3.1: Updated system diagram |
| Version 1.2.1 | 06-07-2023 | DXC architecture team | Updated storage details in Appendix A for DIM-Eng-P and DIM-Eng-A to reflect reality |

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

## *Node details*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **Location** | **Domain** | **Node ID** | **(v)CPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Private Cloud | DXC Application Mgmt | AM2 | Production | DBA-GD-RDP-P | 16 | 48 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2019 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | yes |
| Legacy Hosting AIX | DWH | AM2 | Production | DIM-Man-P | 6 | 24 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 |  | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | Legacy | no |
| Private Cloud | Micro BackOffice | AM2 | Production | DIM-Serv-P | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | yes |
| Private Cloud | Micro BackOffice | AM2 | Production | DIM-Eng-P | 8 | 64 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | yes |
| Private Cloud | Micro BackOffice | AM2 | Production | DIM-Bri-P | 4 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | yes |
| Private Cloud | Micro BackOffice | AM2 | Production | DIM-Sea-P | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | yes |
| Private Cloud | Micro BackOffice | AM2 | Production | DIM-NFS-C-P | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | yes |
| Private Cloud | Micro BackOffice | AM2 | Production | DIM-NFS-H-P | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | yes |
| Legacy Hosting AIX | DWH | AM2 | Production | DIM-DB-P | 8 | 100 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | Legacy | no |
|  |  |  |  |  |  |  |  |  |  |  |
| Private Cloud | Micro BackOffice | AM3 | Acceptance | DIM-Serv-A | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM3 | Acceptance | DIM-Eng-A | 8 | 64 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM3 | Acceptance | DIM-Bri-A | 4 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM3 | Acceptance | DIM-Sea-A | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM3 | Acceptance | DIM-NFS-C-A | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM3 | Acceptance | DIM-NFS-H-A | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Legacy Hosting AIX | DWH | AM3 | Acceptance | DIM-DB-A | 8 | 100 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | Legacy | no |
| **Landing Zone** | **Security Zone** | **Location** | **Domain** | **Node ID** | **(v)CPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Private Cloud | Micro BackOffice | AM2 | Development | DIM-Serv-D | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Development | DIM-Eng-D | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Development | DIM-Bri-D | 4 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Development | DIM-Sea-D | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Development | DIM-NFS-CH-D | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Legacy Hosting AIX | DWH | AM2 | Development | DIM-DB-D | 4 | 80 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | Legacy | no |
|  |  |  |  |  |  |  |  |  |  |  |
| Private Cloud | Micro BackOffice | AM2 | Test | DIM-Serv-T | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Test | DIM-Eng-T | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Test | DIM-Bri-T | 4 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Test | DIM-Sea-T | 8 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | Micro BackOffice | AM2 | Test | DIM-NFS-CH-T | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Legacy Hosting AIX | DWH | AM2 | Test | DIM-DB-T | 4 | 80 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | Legacy | no |

## *Storage*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **C-drive OS (Fixed)** | **D-drive App (mandatory)** | **E-drive (optional)** | **F-drive (optional)** | **…-drive (optional)** |
| DIM-Bri-P | Production | 100 GB | 100 GB | n/a | n/a | n/a |
| DIM-Bri-A | Acceptance | 100 GB | 100 GB | n/a | n/a | n/a |
| DIM-Bri-D | Development | 100 GB | 100 GB | n/a | n/a | n/a |
| DIM-Bri-T | Test | 100 GB | 100 GB | n/a | n/a | n/a |
| DBA-GD-RDP-P | Production | 100 GB | 500 GB | n/a | n/a | n/a |

*Bridge + RDP server(s) (Windows)*

*Engine servers (Linux)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App1 (mandatory)** | **Disk 1 – Mountpoint 2 App 2 (optional)** | **Disk 1 – Mountpoint 3 (optional)** | **Disk 1 – Mountpoint 4 (optional)** |
| DIM-Eng-P | Production | 100 GB | 250 GB + 250 GB | 1 TB | 500 GB | 50 GB |
| DIM-Eng-A | Acceptance | 100 GB | 250 GB + 250 GB | 1 TB | 500 GB | 50 GB |
| DIM-Eng-D | Development | 100 GB | 250 GB + 250 GB | 200 GB | 500 GB | n/a |
| DIM-Eng-T | Test | 100 GB | 250 GB + 250 GB | 200 GB | 500 GB | n/a |

*Service servers (Linux)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App1 (mandatory)** | **Disk 1 – Mountpoint 2 App 2 (optional)** | **Disk 1 – Mountpoint 3 (optional)** | **Disk 2 – Mountpoint 1 (optional)** |
| DIM-Serv-P | Production | 100 GB | 200 GB | n/a | n/a | n/a |
| DIM-Serv-A | Acceptance | 100 GB | 200 GB | n/a | n/a | n/a |
| DIM-Serv-D | Development | 100 GB | 200 GB | n/a | n/a | n/a |
| DIM-Serv-T | Test | 100 GB | 200 GB | n/a | n/a | n/a |

*Search servers (Linux)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App1 (mandatory)** | **Disk 1 – Mountpoint 2 App 2 (optional)** | **Disk 1 – Mountpoint 3 (optional)** |
| DIM-Sea-P | Production | 100 GB | 150GB + 250 GB + 250 GB | 250GB | n/a |
| DIM-Sea-A | Acceptance | 100 GB | 150GB + 250 GB + 250 GB | 250GB | n/a |
| DIM-Sea-D | Development | 100 GB | 150GB + 250 GB + 250 GB | 250GB | n/a |
| DIM-Sea-T | Test | 100 GB | 150GB + 250 GB + 250 GB | 250GB | n/a |

*NFS servers (Linux)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 (mandatory)** |
| DIM-NFS-C-P | Production | 100 GB | 10 TB |
| DIM-NFS-H-P | Production | 100 GB | 2 TB |
| DIM-NFS-C-A | Acceptance | 100 GB | 10 TB |
| DIM-NFS-H-A | Acceptance | 100 GB | 2 TB |
| DIM-NFS-CH-D | Development | 100 GB | 6 TB |
| DIM-NFS-CH-T | Test | 100 GB | 6 TB |

*Oracle Database servers (AIX)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Node ID** | DIM-Man-P | DIM-DB-P | DIM-DB-A | DIM-DB-D | DIM-DB-T |
| **Domain** | Production | Production | Acceptance | Development | Test |
| **Disk0 OS (Fixed)** | 100 GB | 100 GB | 100 GB | 100 GB | 100 GB |
| **Disk1 Oracle Binaries (Fixed)** | 100 GB | 100 GB | 100 GB | 100 GB | 100 GB |
| **Disk2 ASM Binaries (Fixed)** | 100 GB | 100 GB | 100 GB | 100 GB | 100 GB |
| **Disk3 Deployments and Data Transfer** | 1 TB | 300 GB | 300 GB | 300 GB | 300 GB |
| **ASM DATA1 DiskGroup1** | 300 GB | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA2 DiskGroup1** | 100 GB | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA3 DiskGroup1** |  | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA4 DiskGroup1** |  | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA5 DiskGroup1** |  | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA6 DiskGroup1** |  | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA7 DiskGroup1** |  | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA8 DiskGroup1** |  | 3 TB | 3 TB | 1 TB | 1 TB |
| **ASM DATA9 DiskGroup1** |  |  |  | 1 TB | 1 TB |
| **ASM DATA10 DiskGroup1** |  |  |  | 1 TB | 1 TB |
| **ASM FRA1 DiskGroup2** | 150 GB | 250 GB | 250 GB | 100 GB | 100 GB |
| **ASM FRA2 DiskGroup2** | 50 GB | 250 GB | 250 GB | 100 GB | 100 GB |
| **ASM FRA3 DiskGroup2** |  | 250 GB | 250 GB | 100 GB | 100 GB |
| **ASM FRA4 DiskGroup2** |  | 250 GB | 250 GB | 100 GB | 100 GB |
| **ASM FRA5 DiskGroup2** |  | 250 GB | 250 GB | 100 GB | 100 GB |
| **ASM FRA6 DiskGroup2** |  | 250 GB | 250 GB | 100 GB | 100 GB |
| **ASM FRA7 DiskGroup2** |  |  |  | 100 GB | 100 GB |
| **ASM FRA8 DiskGroup2** |  |  |  | 100 GB | 100 GB |
| **ASM FRA9 DiskGroup2** |  |  |  | 100 GB | 100 GB |
| **ASM FRA10 DiskGroup2** |  |  |  | 100 GB | 100 GB |

## *Software*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported** |
| DIM-Man-P | 1-OS | AIX | 7.2 TL5 |  |
| DIM-Man-P | 3-Database | Oracle Database Server | 19.3 | Y |
| DIM-Man-P | 5-Application | QRADAR Client |  |  |
| DIM-Man-P | 5-Application | Oracle Cloud Control |  |  |
| DIM-Man-P | 5-Application | Oracle NET client |  |  |
| DIM-Man-P | 5-Application | Oracle NET services |  |  |
| DIM-Serv-P; DIM-Serv-A; DIM-Serv-D; DIM-Serv-T | 1-OS | RedHat Enterprise Linux | 7.9 | Y |
| DIM-Serv-P; DIM-Serv-A; DIM-Serv-D; DIM-Serv-T | 5-Application | IBM WebSphere Application Server | 9.0.0.9 ND + fix packs | Y |
| DIM-Serv-P; DIM-Serv-A; DIM-Serv-D; DIM-Serv-T | 5-Application | IBM InfoSphere Services | 11.7.1.1 |  |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 1-OS | RedHat Enterprise Linux | 7.9 | Y |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 1-OS | Linux GNU C++ Compiler Collection | 4.8.5 |  |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 2-Library | NFS Client | 7.9 |  |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 4-Middleware | IBM Workload scheduler Fault Tolerant Agent | 9.3 FP2 | Y |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 5-Application | WebSphere Application Server ABS agent | 9.0.0.9 ND + fix packs | Y |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 5-Application | Oracle Database Server Client software | 12.2 |  |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 5-Application | IBM InfoSphere Engine | 11.7.1.1 | Y |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 5-Application | Dos2unix |  |  |
| DIM-Eng-P; DIM-Eng-A; DIM-Eng-D; DIM-Eng-T | 5-Application | Unix2dos |  |  |
| DIM-Bri-P; DIM-Bri-A; DIM-Bri-D; DIM-Bri-T | 1-OS | Microsoft Windows Server | 2016SE | Y |
| DIM-Bri-P; DIM-Bri-A; DIM-Bri-D; DIM-Bri-T | 2-Library | Microsoft .NET framework | 4.7 | Y |
| DIM-Bri-P; DIM-Bri-A; DIM-Bri-D; DIM-Bri-T | 5-Application | Micorsoft Edge |  |  |
| DIM-Bri-P; DIM-Bri-A; DIM-Bri-D; DIM-Bri-T | 5-Application | IBM InfoSphere Metadata Integration bridge | 11.7.1.1 | Y |
| DIM-Bri-P; DIM-Bri-A; DIM-Bri-D; DIM-Bri-T | 5-Application | Google Chrome | 90.0.4430.85 |  |
| DIM-Bri-P; DIM-Bri-A; DIM-Bri-D; DIM-Bri-T | 5-Application | Oracle Database Server Client software | 12.2 |  |
| DIM-Sea-P; DIM-Sea-A; DIM-Sea-D; DIM-Sea-T | 1-OS | RedHat Enterprise Linux | 7.9 | Y |
| DIM-Sea-P; DIM-Sea-A; DIM-Sea-D; DIM-Sea-T | 5-application | IBM InfoSphere Search node | 11.7.1.1 |  |
| DIM-NFS-C-P; DIM-NFS-H-P; DIM-NFS-C-A; DIM-NFS-H-A; DIM-NFS-CH-D; DIM-NFS-CH-T | 1-OS | RedHat | 7.9 | Y |
| DIM-NFS-C-P; DIM-NFS-H-P; DIM-NFS-C-A; DIM-NFS-H-A; DIM-NFS-CH-D; DIM-NFS-CH-T | 4-Middleware | NFS Server |  | Y |
| DIM-DB-P; DIM-DB-A; DIM-DB-D; DIM-DB-T | 1-OS | AIX | 7.2 TL5 | Y |
| DIM-DB-P; DIM-DB-A; DIM-DB-D; DIM-DB-T | 1-OS | AIX Kerberos |  |  |
| DIM-DB-P; DIM-DB-A; DIM-DB-D; DIM-DB-T | 2-Library | Java JRE | 8.0.6.35 |  |
| DIM-DB-P; DIM-DB-A; DIM-DB-D; DIM-DB-T | 2-Library | NFS Client |  |  |
| DIM-DB-P; DIM-DB-A; DIM-DB-D; DIM-DB-T | 3-Database | Oracle Database Server | 19.3 |  |
| DIM-DB-P; DIM-DB-A; DIM-DB-D; DIM-DB-T | 5-Application | IBM Workload scheduler Fault Tolerant Agent | 9.3 FP2 |  |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported** |
| DBA-GD-RDP-P | 1-OS | Microsoft Windows Server | 2019 | Y |
| DBA-GD-RDP-P | 1-OS | Remote desktop server | 2019 | Y |
| DBA-GD-RDP-P | 5-application | Oracle full client | 12.2 |  |
| DBA-GD-RDP-P | 5-application | Toad for oracle |  |  |
| DBA-GD-RDP-P | 5-application | Putty |  |  |
| DBA-GD-RDP-P | 5-application | Moba x-term |  |  |
| DBA-GD-RDP-P | 5-application | Winscp |  |  |
| DBA-GD-RDP-P | 5-application | Notepad++ |  |  |

## *Load Balancers*

Not applicable

# 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).*

**Production**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KWN Workplace | DIM Search Server | HTTPS | 443 |  |
| DIM Services Server | DIM Bridge Server | TCP | 19443 |  |
| DIM Bridge Server | DIM DB server | Oracle Client | 1526 |  |
| DIM Engine Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM DB Server | DIM NFS Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| DIM Engine Server | DIM NFS Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| SI-FT | DIM Engine Server | SFTP | 22 |  |
| Generieke TWS | DIM Engine Server | TCP/UDP | 34342 |  |
| DIM Engine Server | UWV Mail | SMTP | 25 |  |
| DIM Services Server | UWV WPOL | LDAP/SSL | 636 |  |
| DIM Services Server | DIM Search Server | TCP | 2181 |  |
| DIM Services Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Services Server | DIM Search Server | TCP | 9092 |  |
| DIM Search Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Management Server | DIM RHEL Servers | SSH | 22 |  |
| DIM RHEL Servers | DWH Management Server | SSH | 22 |  |
| DIM Bridge Server | DIM Services Server | TCP/UDP | 9443 |  |
| DIM Engine | DIM Search | TCP | 9092 |  |
| DIM Management Server | DIM Bridge | RDP | 3389 |  |
| DIM Bridge | DIM Management Server | RDP | 3389 |  |

**Acceptance**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KWN Workplace | DIM Search Server | HTTPS | 443 |  |
| DIM Services Server | DIM Bridge Server | TCP | 19443 |  |
| DIM Bridge Server | DIM DB server | Oracle Client | 1526 |  |
| DIM Engine Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM DB Server | DIM NFS Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| DIM Engine Server | DIM NFS Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| SI-FT | DIM Engine Server | SFTP | 22 |  |
| Generieke TWS | DIM Engine Server | TCP/UDP | 34342 |  |
| DIM Engine Server | UWV Mail | SMTP | 25 |  |
| DIM Services Server | UWV WPOL | LDAP/SSL | 636 |  |
| DIM Services Server | DIM Search Server | TCP | 2181 |  |
| DIM Services Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Services Server | DIM Search Server | TCP | 9092 |  |
| DIM Search Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Management Server | DIM RHEL Servers | SSH | 22 |  |
| DIM RHEL Servers | DWH Management Server | SSH | 22 |  |
| DIM Bridge Server | DIM Services Server | TCP/UDP | 9443 |  |
| DIM Engine | DIM Search | TCP | 9092 |  |
| DIM Management Server | DIM Bridge | RDP | 3389 |  |
| DIM Bridge | DIM Management Server | RDP | 3389 |  |

**Development**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KWN Workplace | DIM Search Server | HTTPS | 443 |  |
| DIM Services Server | DIM Bridge Server | TCP | 19443 |  |
| DIM Bridge Server | DIM DB server | Oracle Client | 1526 |  |
| DIM Engine Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM DB Server | DIM NFS Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| DIM Engine Server | DIM NFS Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| DIM Engine Server | UWV Mail | SMTP | 25 |  |
| DIM Services Server | UWV WPOL | LDAP/SSL | 636 |  |
| DIM Services Server | DIM Search Server | TCP | 2181 |  |
| DIM Services Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Services Server | DIM Search Server | TCP | 9092 |  |
| DIM Search Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Management Server | DIM RHEL Servers | SSH | 22 |  |
| DIM RHEL Servers | DWH Management Server | SSH | 22 |  |
| DIM Bridge Server | DIM Services Server | TCP/UDP | 9443 |  |
| DIM Engine | DIM Search | TCP | 9092 |  |
| DIM Management Server | DIM Bridge | RDP | 3389 |  |
| DIM Bridge | DIM Management Server | RDP | 3389 |  |

**Test**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KWN Workplace | DIM Search Server | HTTPS | 443 |  |
| DIM Services Server | DIM Bridge Server | TCP | 19443 |  |
| DIM Integration Server | DIM DB server | Oracle Client | 1526 |  |
| DIM Engine Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM DB Server | DIM Engine Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| DIM Engine Server | DIM Engine Server | NFS | 111, 635, 2049, 4045, 4046 |  |
| DIM Engine Server | UWV Mail | SMTP | 25 |  |
| DIM Services Server | UWV WPOL | LDAP/SSL | 636 |  |
| DIM Services Server | DIM Search Server | TCP | 2181 |  |
| DIM Services Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Services Server | DIM Search Server | TCP | 9092 |  |
| DIM Search Server | DIM DB Server | Oracle Client | 1526 |  |
| DIM Management Server | DIM RHEL Servers | SSH | 22 |  |
| DIM RHEL Servers | DWH Management Server | SSH | 22 |  |
| DIM Bridge Server | DIM Services Server | TCP/UDP | 9443 |  |
| DIM Engine | DIM Search | TCP | 9092 |  |
| DIM Management Server | DIM Bridge | RDP | 3389 |  |
| DIM Bridge | DIM Management Server | RDP | 3389 |  |

**Only for HLD version 1.1: <**add embedded connectivity sheet>

# Appendix C: Users and Groups

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

**Variation 1: LDAP - nested groups**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **UWV** | | **DXC** | |
| **Environment** | **Domain** | **Group** | **Domain** | **Group** |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-DIM-INFOSPHERE-GEBRUIKER | P-dc.ba.uwv.nl | L-RG-UWV-P- DIM-INFOSPHERE-GEBRUIKER |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-DIM-INFOSPHERE-ANALIST | P-dc.ba.uwv.nl | L-RG-UWV-P-DIM-INFOSPHERE-ANALIST |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-DIM-INFOSPHERE-ONTWIKKELAAR | P-dc.ba.uwv.nl | L-RG-UWV-P-DIM-INFOSPHERE-ONTWIKKELAAR |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-DIM-INFOSPHERE-TESTER | P-dc.ba.uwv.nl | L-RG-UWV-P-DIM-INFOSPHERE-TESTER |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-DIM-INFOSPHERE-BEHEER | P-dc.ba.uwv.nl | L-RG-UWV-P-DIM-INFOSPHERE-BEHEER |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-DIM-INFOSPHERE-ADMINISTRATOR | P-dc.ba.uwv.nl | L-RG-UWV-P-DIM-INFOSPHERE-ADMINISTRATOR |
|  |  |  |  |  |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-DIM-INFOSPHERE-GEBRUIKER | A-dc.ba.uwv.nl | L-RG-UWV-A-DIM-INFOSPHERE-GEBRUIKER |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-DIM-INFOSPHERE-ANALIST | A-dc.ba.uwv.nl | L-RG-UWV-A-DIM-INFOSPHERE-ANALIST |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-DIM-INFOSPHERE-ONTWIKKELAAR | A-dc.ba.uwv.nl | L-RG-UWV-A-DIM-INFOSPHERE-ONTWIKKELAAR |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-DIM-INFOSPHERE-TESTER | A-dc.ba.uwv.nl | L-RG-UWV-A-DIM-INFOSPHERE-TESTER |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-DIM-INFOSPHERE-BEHEER | A-dc.ba.uwv.nl | L-RG-UWV-A-DIM-INFOSPHERE-BEHEER |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-DIM-INFOSPHERE-ADMINISTRATOR | A-dc.ba.uwv.nl | L-RG-UWV-A-DIM-INFOSPHERE-ADMINISTRATOR |
|  |  |  |  |  |
| Development | Uwv.wpol.nl | UWV SP G-UG-UWV-O-DIM-INFOSPHERE-GEBRUIKER | O-dc.ba.uwv.nl | L-RG-UWV-O-DIM-INFOSPHERE-GEBRUIKER |
| Development | Uwv.wpol.nl | UWV SP G-UG-UWV-O-DIM-INFOSPHERE-ANALIST | O-dc.ba.uwv.nl | L-RG-UWV-O-DIM-INFOSPHERE-ANALIST |
| Development | Uwv.wpol.nl | UWV SP G-UG-UWV-O-DIM-INFOSPHERE-ONTWIKKELAAR | O-dc.ba.uwv.nl | L-RG-UWV-O-DIM-INFOSPHERE-ONTWIKKELAAR |
| Development | Uwv.wpol.nl | UWV SP G-UG-UWV-O-DIM-INFOSPHERE-TESTER | O-dc.ba.uwv.nl | L-RG-UWV-O-DIM-INFOSPHERE-TESTER |
| Development | Uwv.wpol.nl | UWV SP G-UG-UWV-O-DIM-INFOSPHERE-BEHEER | O-dc.ba.uwv.nl | L-RG-UWV-O-DIM-INFOSPHERE-BEHEER |
| Development | Uwv.wpol.nl | UWV SP G-UG-UWV-O-DIM-INFOSPHERE-ADMINISTRATOR | O-dc.ba.uwv.nl | L-RG-UWV-O-DIM-INFOSPHERE-ADMINISTRATOR |
| Development | Uwv.wpol.nl | UWV SP G-UG-UWV-O-DIM-INFOSPHERE-IIS-METADATA-INTEGRATION | O-dc.ba.uwv.nl | L-RG-UWV-O-DIM-INFOSPHERE-IIS-METADATA-INTEGRATION |
|  |  |  |  |  |
| Test | Uwv.wpol.nl | UWV SP G-UG-UWV-T-DIM-INFOSPHERE-GEBRUIKER | T-dc.ba.uwv.nl | L-RG-UWV-T-DIM-INFOSPHERE-GEBRUIKER |
| Test | Uwv.wpol.nl | UWV SP G-UG-UWV-T-DIM-INFOSPHERE-ANALIST | T-dc.ba.uwv.nl | L-RG-UWV-T-DIM-INFOSPHERE-ANALIST |
| Test | Uwv.wpol.nl | UWV SP G-UG-UWV-T-DIM-INFOSPHERE-ONTWIKKELAAR | T-dc.ba.uwv.nl | L-RG-UWV-T-DIM-INFOSPHERE-ONTWIKKELAAR |
| Test | Uwv.wpol.nl | UWV SP G-UG-UWV-T-DIM-INFOSPHERE-TESTER | T-dc.ba.uwv.nl | L-RG-UWV-T-DIM-INFOSPHERE-TESTER |
| Test | Uwv.wpol.nl | UWV SP G-UG-UWV-T-DIM-INFOSPHERE-BEHEER | T-dc.ba.uwv.nl | L-RG-UWV-T-DIM-INFOSPHERE-BEHEER |
| Test | Uwv.wpol.nl | UWV SP G-UG-UWV-T-DIM-INFOSPHERE-ADMINISTRATOR | T-dc.ba.uwv.nl | L-RG-UWV-T-DIM-INFOSPHERE-ADMINISTRATOR |

***Service Accounts:***

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

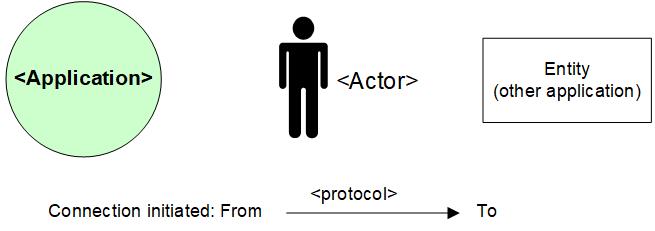
|  |  |  |  |
| --- | --- | --- | --- |
| **Account** | **Domain / local location** | **Noncompliant setting** | **Description** |
|  |  |  |  |
|  |  |  |  |

# 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

