

INFRASTRUCTURE APPLICATION REQUIREMENTS – *KVB*Kandidaten Verkenner Banenafspraak

Version: 0.2

Date: 08-12-2023

Document purpose

This requirements document (REQ) is used to:

* Gain a common understanding of the application requirements
* Document the requirements relevant for the DXC Infrastructure Application design (IA HLD)

The document outlines:

* External entities
* Functional and non-functional requirements

Relation to other documents

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

* The Software Architecture Document (SAD)
* The Project Start Architecture (PSA) document
* Infrastructure Application design produced by DXC for related applications (interfaces)

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 it will be described in the DXC HLD.

Content of the document

UWV has prepared this document in good faith and is based on the information gathered during the requirement determination phase with all parties involved; application vendors, UWV architects, developers and UWV functional management.

Table of Contents

[1 Application Overview 4](#_Toc152919046)

[1.1 Introduction 4](#_Toc152919047)

[1.2 Scope of the desired change 4](#_Toc152919048)

[1.3 Out of Scope 4](#_Toc152919049)

[2 Architecture 5](#_Toc152919050)

[2.1 Conceptual 5](#_Toc152919051)

[2.2 Context diagram 6](#_Toc152919052)

[3 Functional Requirements 13](#_Toc152919053)

[4 Non-Functional Requirements 14](#_Toc152919054)

[4.1 Security & Compliance classifications 14](#_Toc152919055)

[4.2 Capacity and performance (volumetrics) 14](#_Toc152919056)

[4.3 Availability 14](#_Toc152919057)

[4.4 Security requirements 15](#_Toc152919058)

[4.5 System management 15](#_Toc152919059)

[4.6 Backup and Recovery 15](#_Toc152919060)

[4.7 Storage replication 15](#_Toc152919061)

[4.8 Scalability 15](#_Toc152919062)

[4.9 Disaster Recovery 15](#_Toc152919063)

[4.10 Infrastructure Technical Constraints 15](#_Toc152919064)

[4.11 DXC TAB requirements 16](#_Toc152919065)

[Appendix A: Template version control 17](#_Toc152919066)

[Appendix B: Document version control 19](#_Toc152919067)

[Appendix C: Legenda 20](#_Toc152919068)

[Legenda Context Diagram 20](#_Toc152919069)

[Appendix D: MCPaaS – Capacity allocation details 21](#_Toc152919070)

# Application Overview

## Introduction

KVB (Kandidaten Verkenner Banenafspraak - Candidates Explorer for Job Appointment) is an application that is exposed on the Internet and is accessible for registered Employers, UWV Workcoaches (UWV users) and UWV Functional Administrators (UWV FB).

The application provides employers with functions to match jobseekers having a Wajong qualification to vacancies. The application does not contain and/or provide any personal sensitive data. Instead, the application uses reference-IDs.

## Scope of the desired change

This changes will require an additional integration (Dutch: koppeling) from KVB to DIM. The exiting integration from KVB to DWH must stay alive.   
  
Functional; the same data sending to DWH must also send to DIM.  
Technical; We must sending data to DIM on the same way as we do to DWH, by using DBlink.

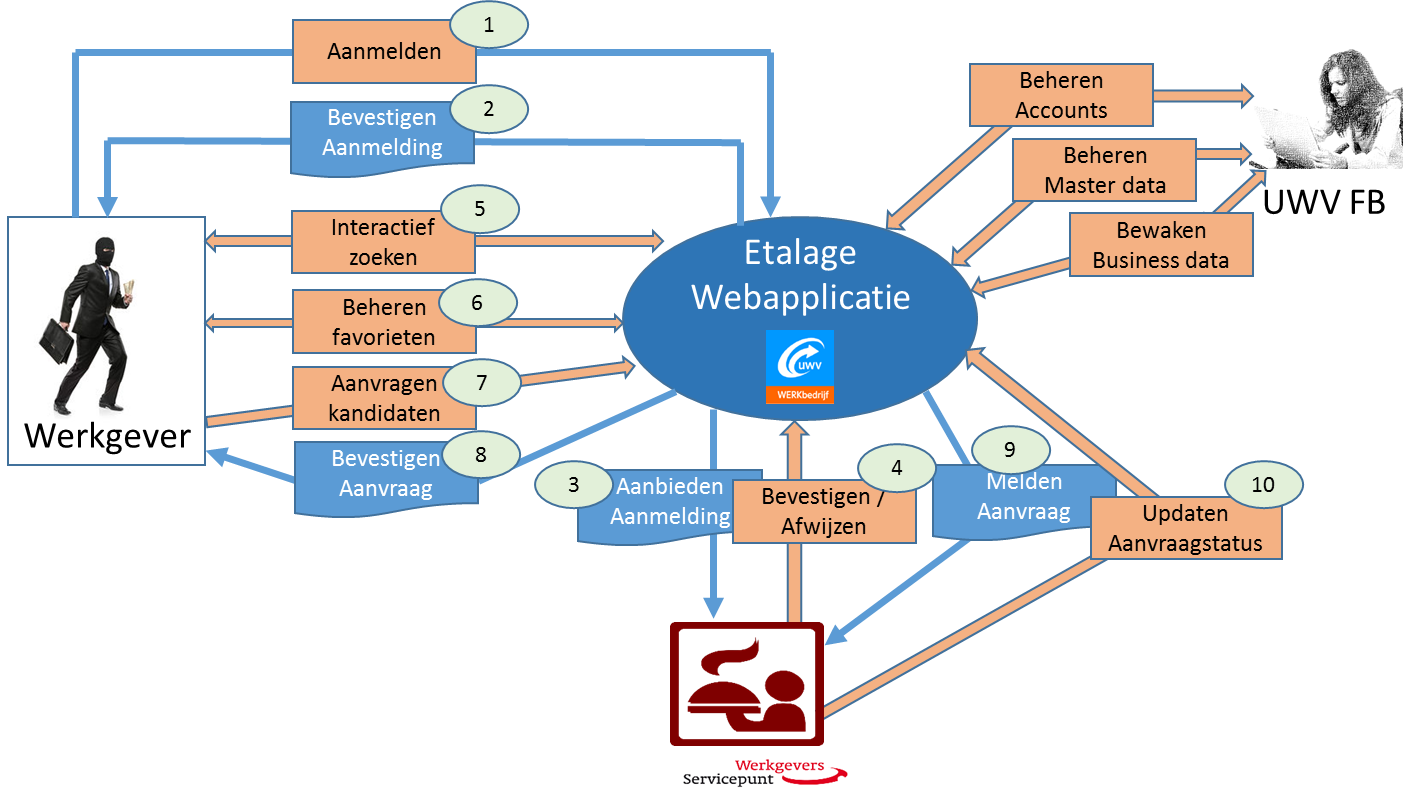
This new integration is to be established in the Production and all Accept environments (including KATO)  
  
Remark: During the fase 2 of the BMS project the integration with DWH will stop. A new HLD requirement document wil be created for this change. So this is out of scpe of this HLD.

## Out of Scope

* KVB Application development & test is performed by UWV in the OTOD and out of scope for this HLD.
* All components that belong to the UWV Office Infrastructure such as workstations, web browsers are out of scope.

# Architecture

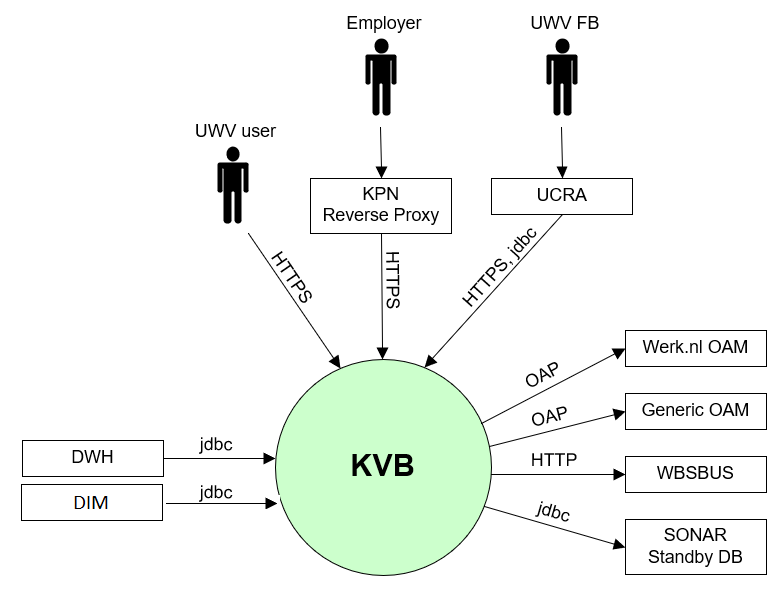
## Conceptual

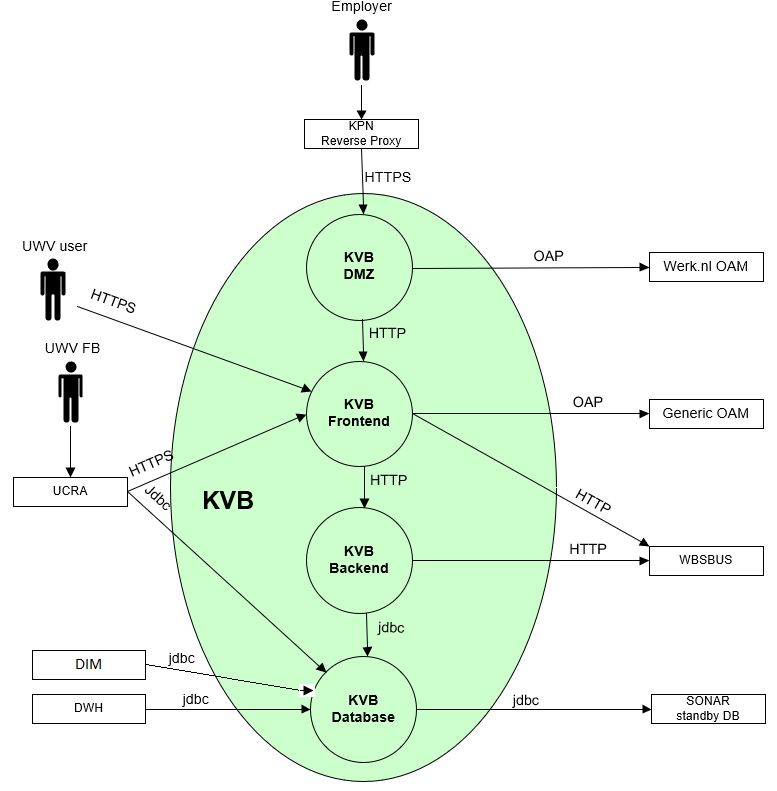


The application provides the following functions:

1. Login and registration screens
2. Confirmation mail for the employer
3. Signin mail to UWV approver
4. Approve or reject by UWV
5. Select: persons
6. Select: characteristics
7. Select: statistics
8. Submit information request
9. Request email to WSP (Werkgevers servicepunt – Employer service point)
10. WSP status management

## Context diagram



Below the same context diagram with some more detail to have a good understanding of the DMZ connections.   


### External entities

The characteristics of each external entity to the system are specified in the following paragraphs.

#### UWV user (Workcoach)

|  |  |
| --- | --- |
| **Description** | The Workcoach (adviseurs) are UWV employees that use various applications (e.g., WBS, SONAR) to support employers and facilitate jobseekers in finding a suitable job.  The Workcoaches are grouped in “WerkGeversServicepunt”, which is organised in several regions and one central location (the National WerkgeversServicePunt). |
| **Protocol and Port** | HTTPS (443) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Yes, Workcoach must logon to their applications (e.g., SONAR).  (Sonar OID user authentication) |
| **Number of users** | There are 300 workcoaches that will access the application in a month during working days/hours.  From this number and by doubling it, it can be derived that 0,3 Workcoaches will access the system concurrently in a 5-minute period during working days (Mon-Fri) and working hours (07.00-19.00h). |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### Employer

|  |  |
| --- | --- |
| **Description** | Employer represents HR personnel and intermediaries (like Randstad). |
| **Protocol and Port** | HTTPS (443) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | No, via KPN Reverse Proxy |
| **Security Controls** | Yes, Employers must successfully identify & authenticate before they are allowed access to the application.  (Werk.nl OID user authentication) |
| **Number of users** | There will be 4000 Employers that access the application in a month during working days/hours.  From this number and by doubling it, it can be derived that 3 Employers will access the system concurrently in a 5-minute period during working days (Mon-Fri) and working hours (07.00-19.00h).  However, from usage statistics it has been determined that there are less than 5 Employer sessions per day. |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### UWV FB

|  |  |
| --- | --- |
| **Description** | Functional Support can manage access of Employers and settings in the application. |
| **Protocol and Port** | HTTPS (443), jdbc (1526) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Yes, Role Based Access (Generieke OAM / Sonar OID) |
| **Number of users** | Less than 5 totals assumed |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | Low |

#### Werk.nl OAM

|  |  |
| --- | --- |
| **Description** | Identification and Access control using Werk.nl/OAM solution. OAM user store (Werk.nl OID (Oracle Internet Directory)) contains account information of Employers |
| **Protocol and Port** | OAP (5575) |
| **DC (Datacenter) connection** | internal |
| **Direction** | outbound |
| **Direct connection** | yes |
| **Security Controls** | Yes, therefore https is used by the UWV user to prevent exchange of clear text passwords over the network. |
| **Number of users** | 4300 in a month (for P environment), (<250/day for A environment) |
| **Number of transactions** | 3,3 logons/5 minutes |
| **Frequency of transactions** | During working days/hours |
| **Volume of data** | Small |

#### Generic OAM

|  |  |
| --- | --- |
| **Description** | Identification and Access control for Workcoaches and Functional Support using Generic OAM solution. |
| **Protocol and Port** | OAP (5575) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Yes, therefore https is used by the UWV user to prevent exchange of clear text passwords over the network. |
| **Number of users** | 4300 in a month (for P environment), (<250/day for A environment) |
| **Number of transactions** | 3,3 logons/5 minutes |
| **Frequency of transactions** | During working days/hours |
| **Volume of data** | Small |

#### WBSBUS

|  |  |
| --- | --- |
| **Description** | Werk.nl Middleware Services, Werk.nl has reference data that KVB needs. Reference data is obtained from BO&C (Beroepen, Opleidingen en Competencies) services, Postcode services and WSP-services through the WBSBUS. |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Low |
| **Frequency of transactions** | Not specified |
| **Volume of data** | 250MB |

#### DWH

|  |  |
| --- | --- |
| **Description** | DataWareHouse gathers data from a materialized view in the KVB database. DWH provides this data to the MIP application. |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | No, the data does not contain sensitive personal data. |
| **Number of users** | 1 database user for P (also 1 user for A). |
| **Number of transactions** | <10 queries per environment for the data export and extract |
| **Frequency of transactions** | Weekly refresh |
| **Volume of data** | 45MB (30,000 records of 1,5kB each) |

#### DIM

|  |  |
| --- | --- |
| **Description** | Data Integratie Magazijn (DIM) gathers data from a materialized view in the KVB database. DIM provides this data to the MIP application. |
| **Protocol and Port** | jdbc (1521) ???? |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | No, the data does not contain sensitive personal data. |
| **Number of users** | 1 database user for P (also 1 user for A). |
| **Number of transactions** | <10 queries per environment for the data export and extract |
| **Frequency of transactions** | Weekly refresh |
| **Volume of data** | 45MB (30,000 records of 1,5kB each) |

#### Sonar Standby database

|  |  |
| --- | --- |
| **Description** | The Sonar standby database is queried using a dblink over SQLNet to get candidates that apply for KVB. The Sonar standby database is kept up to date with the primary Sonar database. The Sonar standby database also contains authorization information for the workcoaches that can access the KVB application. The authorization information is obtained using jdbc over SQLNet from the standby database. |
| **Protocol and Port** | Jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | outbound |
| **Direct connection** | yes |
| **Security Controls** | No, the data does not contain sensitive personal data. |
| **Number of users** | * Candidate’s query: 1 database user for P (also 1 user for A). * Security controls: 300 for P environment, <30 for A environment. |
| **Number of transactions** | <10 queries per environment for data extract |
| **Frequency of transactions** | The security control queries are performed every time a user starts a session in the KVB application to obtain user roles.  Daily sync (in the evening) |
| **Volume of data** | 45MB (30,000 records of 1,5kB each) |

# Functional Requirements

* Access to the application is only allowed with the https protocol.
* Eures Webtier also needs to be hosted on the KVB DMZ system (Eures Webtier connections are documented in the Eures HLD)

# Non-Functional Requirements

## Security & Compliance classifications

For the BIV Rating the following repository is used: “2020 UWV-brede Risico Applicatie Lijst v1.0”

|  |  |
| --- | --- |
| **Application** | KVB |
| **Owner** | WB |
| **Availability (Beschikbaarheid)** | 3 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 1 |
| **Type of information /Data Classification** | Persoonsgegevens klanten of derden |
| **Direct or Indirect part of the primary information chain** | Indirect |

### Risk analysis UWV

No risk analysis provided by UWV

### Applicable security and compliance frameworks

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

## Capacity and performance (volumetrics)

* Regular data update: new data is uploaded at regular intervals (i.e. every week). The solution must support a minimum of 10 years of weekly increments of data to the database.
* Maximum size of data updates: One Sonar data update (obtained from Sonar standby database) has a maximum size of 500 kB.

## Availability

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

## Security requirements

### Application Access Controls

Access to the application must be secured. Only registered Employers and registered Workcoaches are allowed to access the application. A valid User-ID and password are required to access the application. Authorization information must be retrieved from Sonar standby database

### Identity and Access Management

* Employers that access the application must be registered in the Werk.nl OID (Oracle Internet Directory). Access to resources must be managed and controlled with Werk.nl OAM (Oracle Access Manager).
* UWV users (WSP / work coaches) or UWV FB that access the application must be registered in the Sonar OID (Oracle Internet Directory). Access to resources must be managed and controlled with the Generic OAM (Oracle Access Manager).

### System logging

No specific system logging requirements are applicable

Detailed Standard Security requirements are documented in Appendix D

## System management

UWV standard system management is applicable.

## Backup and Recovery

No specific Backup and Recovery requirements are applicable.

## Storage replication

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

## Scalability

The solution must be scalable (both horizontally and vertically) to support increased numbers of users and requests.

## Disaster Recovery

No specific disaster recovery requirements applicable.

## Infrastructure Technical Constraints

No infrastructure technical constraints.

## DXC TAB requirements

|  |  |
| --- | --- |
| **Category** | **Description** |
| Deployment (existingTAB Deployment server) | TAB Deployment server is used, exact ports will be determined during implementation (see Appendic B - connectivity sheet v1.1) |
| Deployment (XLdeploy) | XLdeploy is used |
| Shared Storage (existing TAB NFS server) | Shared storage is not used |
| Application monitoring (Sitescope) | No specific requirements |

# Appendix A: Template version control

**TEMPLATE CHANGE HISTORY**

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Changes |
| 0.1 | 08-07-2022 | * Initial version UWV requirements template, ready for review |
| 0.2 | 13-07-2022 | * Included review comments Giuliana to prepare for follow-up meeting |
| 0.3 | 14-07-2022 | * Included review comments Giuliana and Henk-Jan to prepare for REQ template pilot |
| 0.8 | 14-07-2022 | * Cora marked the REQ template v0.8.  Prepared for final UWV review and the additional writer’s instruction from Thomas H, Remco H and Walter |
| 0.9 | 25-07-2022 | * Pre-pilot version |
| 0.91 | 27-07-2022 | * Split Appendix A in A and B for document control |
| 0.92 | 11-08-2022 | * improved instructions after 1st workshop with IO&R hosting team and evaluation of pilot (use case: edit HLD for existing application) |
| 0.93 | 24-08-2022 | * improved instructions after 2nd workshop with IO&R hosting team |
| 0.99 | 28-10-2022 | * Improved and added instructions by Henk-Jan after evaluation of first use in production and to finalize template to v1.0 |
| 1.0 | 11-01-2022 | Finalized with the following adjustments   * Updated 4.4 includes service level and service hours * Updated 4.8 Added note for AIX Bronze systems |
| 1.1 | 02-01-2023 | * Updated instructions for certificate selection |
| 1.2 | 23-02-2023 | Updated the template with MCPaaS (Managed Container Platform as a Service) specific requirements   * Removed Chapter 3 (functional requirements), Evaluation shows that this is either not filled or when it is filled the requirements are non-funtional. Functional requirements for the application are documented in the application design (SAD) * Moved chapter 4.8 (storage replication) under 3.2.1 to bundle the Private Cloud (build)requirements together * Moved chapter 4.4 (Availibility), 4.6 (System management) and 4.10 (TAB requirements) under 3.2.1 and 3.2.2 to bundle the Private Cloud system and Container application requirements together * Moved chapter under 3.2.1 and 3.2.2 to bundle the Private Cloud system and Container application requirements together * Updated 4.2 System and Software requirements: seperate section for Private Cloud and MCPaaS * Updated 4.4 Availability: seperate section for Private Cloud and MCPaaS * 4.6.1 – added addition MCPaaS related infra requirement: Can the standard azure container registry be used by the MCPaaS application |
| 1.21 |  | Added Chapter 3 again: Functional requirements, to keep all chapter the same also for old documentation and to have the possibility to document functional requirements that might seem relevant  Updated 4.2.1.5 System management   * Added load balancer requirements * Added known application scalability limitations |

# Appendix B: Document version control

**USED TEMPLATE**

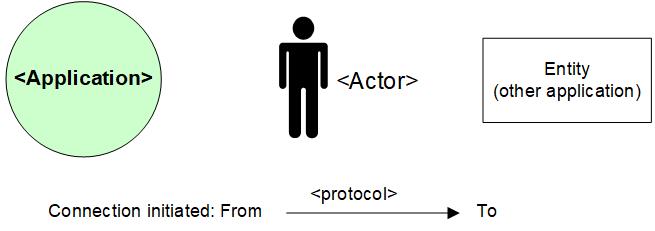
|  |
| --- |
| Based on REQ Template: UWV REQ – TEMPLATE 1.2.docx |

**CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Summary of Changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix C: Legenda

## Legenda Context Diagram



# Appendix D: MCPaaS – Capacity allocation details

**EXAMPLE**

**Capacity allocation for <CompetentNL>**

To manage the resource allocation and assure the project uses only appropriate or agreed resources on the cluster, the quotas and limits to compute resources for the CompetentNL projects on the MCPaaS will be based on below details.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Service (pod)** | **Mem Reservation** | **Mem Limit** | **CPU Reservation** | **CPU Limit** | **Scale - nr of containers (Development)** | **Scale - nr of containers (Test)** |
| CNL-Backend | 256M | 512M | 0,1 | 0,3 | 1 | 1 |
| CNL-Frontend | 128M | 256M | 0,1 | 0,5 | 1 | 1 |
| CNL-IAM | 256M | 512M | 0,1 | 0.5 | 1 | 1 |
| CNL-Dataloader | 256M | 512M | 0,1 | 0,2 | 1 | 1 |
| CNL ActiveMQ | 256M | 512M | 0,1 | 0,3 | 1 | 1 |
| CNL-Config-server | 128M | 256M | 0,1 | 0,2 | 1 | 1 |
| CNL-api | 256M | 512M | 0,1 | 0,5 | 1 | 1 |
| CNL-Synchronization | 128M | 256M | 0,1 | 0,3 | 1 | 1 |
| CNL-DB Management | 128M | 256M | 0,1 | 0,2 | 1 | 1 |
| CNL-Search | 1024M | 3072M | 0,1 | 1 | 1 | 1 |

*Total Required resource allocation*

*Note: Required resource allocation for Development and Test is an initial estimation. After initial tests on these environments resource allocation for all environments will be finalized and updated. Besides the resource allocation for Acceptance and Production are based on the experiences from Development and Test.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Size description** | **Development** | **Test** | **Acceptance** | **Production** |
| Mem minimum run | 2816M | 2816M | TBD | |
| Mem maximum run | 6656M | 6656M |
| CPU reservations | 1 | 1 |
| CPU reservations limit | 4 | 4 |