

HLD – SONAR

Version: 1.2.1

Date: 6 February 2023

Document purpose

This High-Level Design (HLD) is used to:

* Validate the Application solution from a technical perspective through architectural review
* Plan and execute implementation of the solution
* Support Technical Application Management

The document outlines:

* An overview of the application and its architecture
* Functional and non-functional requirements
* Solution description
  + By default, the solution will use standard services from the DXC catalog for UWV. Where applicable required variances will be described.

Relation to Reference Architecture, ABB’s, HLD VI, SBB’s and SAD

The UWV Reference Architecture provides the context for the HLD VI. The HLD VI is focused on the architectures enabling the datacentre hosting services, its building blocks and the integrations.

* **Architectures Building Blocks (ABB)**, maintained by UWV, are built up from a collections of solution building blocks (SBB’s), so most building blocks will interoperate with other building blocks (integrations).
* **Solution Building Blocks (SBBs),** maintained by DXC, represent components that will be used to implement the required capability for the datacenter hosting service.

This HLD leverages the ABB’s and SBB’s as a foundation for the solution.

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

* The Software Architecture Document
* Technisch Beheer Handboek (TBH – technical management handbook)
* Technisch Koppelvlak Document (TKD – technical interface document)
* Procedure HandBoek (PHB – procedure handbook – part 1 = standard, 2 – exceptions)

Structure of the document

High level flow: first the application overview and architecture are described followed by the functional and non-functional requirements that ‘drive’ the solution as described in the final chapter. The appendices include any additional details or specifics for the application described in this HLD. See table of contents on next page for further details.

Content of the document

DXC has prepared this document in good faith and is partly based on the information made available to it by UWV and IBM (e.g., HLD document). The statements and content in this document should be qualified accordingly. For the same reason some references in this document might be ‘outdated’ (i.e., not in this document anymore nor in other related documents).

Table of Contents

[1 Application Overview 4](#_Toc127191381)

[1.1 Introduction 4](#_Toc127191382)

[1.2 Application use cases 5](#_Toc127191383)

[1.3 Out of Scope 5](#_Toc127191384)

[2 Architecture 6](#_Toc127191385)

[2.1 Conceptual 6](#_Toc127191386)

[2.2 Context diagram 7](#_Toc127191387)

[3 Functional Requirements 45](#_Toc127191388)

[4 Non-Functional Requirements 46](#_Toc127191389)

[4.1 Security & Compliance classifications 46](#_Toc127191390)

[4.2 Capacity and performance (volumetrics) 46](#_Toc127191391)

[4.3 Availability 47](#_Toc127191392)

[4.4 Security requirements 47](#_Toc127191393)

[4.5 System management 47](#_Toc127191394)

[4.6 Backup and Recovery 48](#_Toc127191395)

[4.7 Storage replication 48](#_Toc127191396)

[4.8 Scalability 48](#_Toc127191397)

[4.9 Disaster Recovery 48](#_Toc127191398)

[4.10 Infrastructure Technical Constraints 48](#_Toc127191399)

[4.11 DXC TAB requirements 48](#_Toc127191400)

[5 Solution 49](#_Toc127191401)

[5.1 Architectural Decisions 49](#_Toc127191402)

[5.2 Node descriptions and zone-projections 51](#_Toc127191403)

[5.3 System diagram – Production 54](#_Toc127191404)

[5.4 System diagram Non-Production and Staging 55](#_Toc127191405)

[5.5 SBB’s 57](#_Toc127191406)

[5.6 Load balancers 57](#_Toc127191407)

[5.7 Deviations from standards (RAL / EtP) 58](#_Toc127191408)

[5.8 Licenses 58](#_Toc127191409)

[5.9 Service Management 58](#_Toc127191410)

[5.10 Security 59](#_Toc127191411)

[6 Potential future improvements 62](#_Toc127191412)

[Appendix A: Technology and Sizing (at design verification) 63](#_Toc127191413)

[*Node details* 63](#_Toc127191414)

[*Storage* 66](#_Toc127191415)

[*Software* 71](#_Toc127191416)

[*Load Balancers* 74](#_Toc127191417)

[Appendix B: Network Protocol Matrix 75](#_Toc127191418)

[Appendix C: Users and Groups 79](#_Toc127191419)

[Appendix D: Security 80](#_Toc127191420)

[Appendix F: Legenda 82](#_Toc127191421)

[Legenda Context Diagram 82](#_Toc127191422)

[Legenda System Diagram 82](#_Toc127191423)

[Appendix G: Control 83](#_Toc127191424)

# Application Overview

## Introduction

Sonar is a Siebel Business Application implemented in Oracle Siebel Innovation Pack (IP) 2018. Siebel IP 2018 is a continuation of the Siebel 8.1/8.2 release. After Siebel IP2018, the software updates that follow are IP2019/IP2020, and so on.

Siebel Public Sector is an integrated suite of Web-based applications designed for use by administrators and users who are associated with municipal governments, social services, tax and revenue management, public health, immigration agencies, and investigative agencies.

Sonar supports the following business processes:

* Service for jobseekers
* Support for the following processes
  + Re-integration
  + Execution of the WSW (Wet Sociale Werkvoorziening)
  + Wajong
* Export data to provide management information

SONAR refers in this document to the following components:

* Siebel components:
  + Siebel Application servers (Siebel Application Interface and Siebel Server)
    1. SONAR Public Sector
       1. SONAR Public Sector AI (Application Interface)
       2. SONAR Public Sector application
    2. SONAR EAI (eBusiness Application Integration)
       1. SONAR EAI AI (Application Interface)
       2. SONAR EAI application
    3. SONAR Document / Correspondence
  + Siebel Gateway Cluster (Zookeeper based native Application Level Clustered servers, which maintains configuration- and status data of the Siebel servers)

1. SONAR Gateway (servers)
   * Siebel Database
2. SONAR database
3. SONAR logical standby database
   * Siebel File System
4. SONAR file system

* Web service (End-user access to PDF / XFDF files with URL)

1. SONAR PDF converter

* SONAR Staging (previous Generieke services staging)

1. SONAR Staging

* OID (Oracle Internet Directory)

1. SONAR OID

* Windows file server (for SONAR documents which could not be migrated to EA, only needed in Production)

1. Stand-alone file server

**SONAR RUEI**

SONAR RUEI is the real user monitoring solution for the SONAR application based on the Oracle Real User Experience Insight (RUEI) product. RUEI is designed for measuring, analyzing, and improving the availability and performance of web applications and web services. Although SONAR RUEI is part of the CI SONAR it is described in its own HLD.

**KATO**

Next to Production and Acceptance (WATO) there is also a KATO (Kanban Acceptatie Test Omgeving) environment. KATO is a 'light version' of the official acceptance environment of Werkbedrijf. Acceptance tests are performed on this environment without a load and performance test. KATO is hosted in the acceptance domain and it is managed by DXC.

## Application use cases

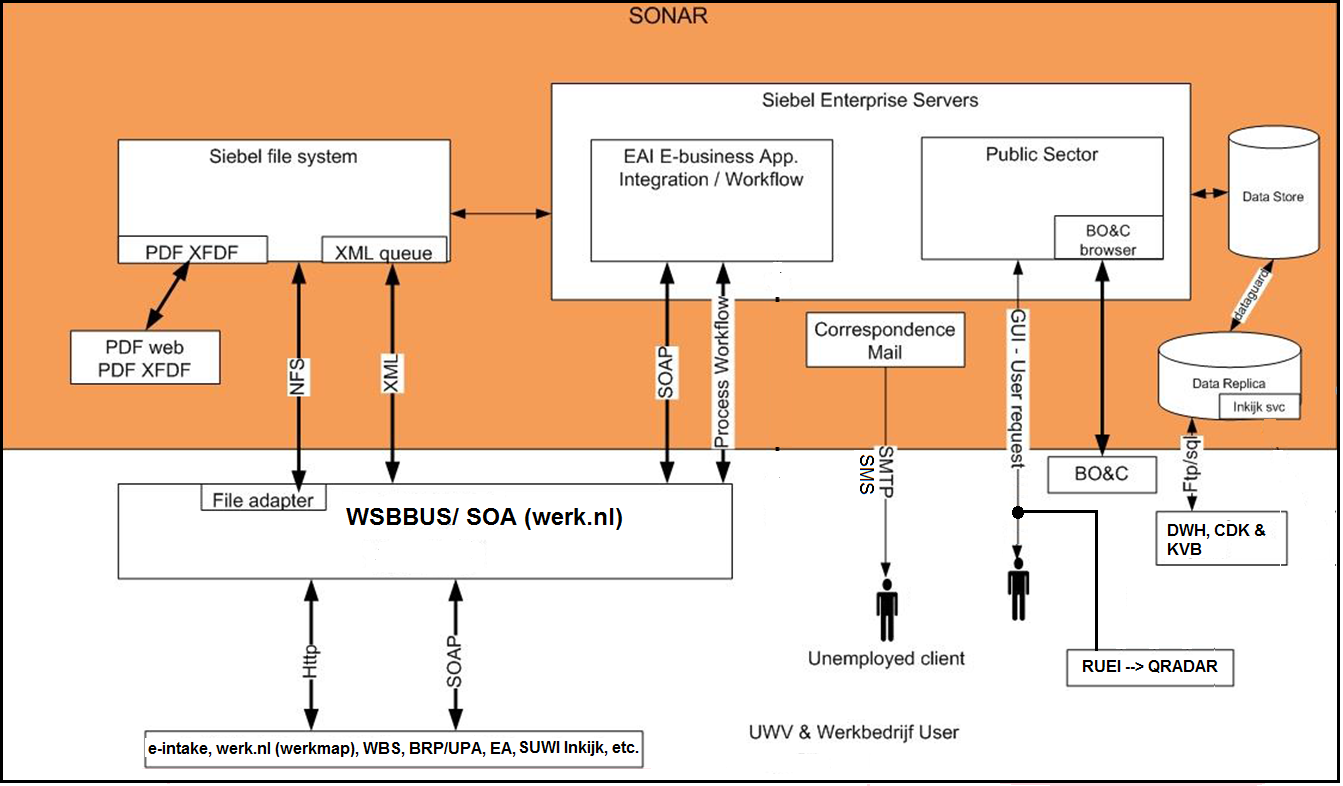
Application use cases are described in the SAD and are not further described in this HLD.

## Out of Scope

* The Development and Test environment are not managed by DXC and are out of scope for this HLD. (Production, Acceptance and Kanban are in scope)
* The SONAR client part is out of scope (Sonar OpenUI is used and only requires a standard Internet Browser).
* SONAR RUEI is 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



**Key concepts:**

1. Sonar can only be used from within the Intranet environment.
2. RUEI is used for user performance monitoring, a LoMo component has also been added to comply to UWV logging and monitoring policy
3. Users connect with a standard web browser to the Public sector application servers
4. Many Interfaces/data exchanges to both internal and external datasources are connected through WBSBUS (Werkbedrijf Service Bus) and Werk.nl SOA. Next to Webservices, the file adapter is used.
5. XML files are stored in XML-queues on the Siebel File System for some asynchronous message exchanges using the file adapter of WBSBUS/ Werk.nl SOA.
6. Some asynchronous messages are transferred via Oracle Advanced Queuing (AQ) Queues and forwarded via Oracle WebLogic Messaging Bridges to JMS Queues and vice versa. Both the Messaging Bridges (for incoming and outgoing messages) and the JMS Queues are located on Werk.nl SOA.
7. Data for documents generated by Sonar is transformed into XFDF code (data for PDF) and stored as an attachment on the Siebel filesystem.
8. Documents that need to be adjustable are generated as Word documents by the correspondence servers.
9. Acceptance and KATO will both be placed in the Acceptance environment
10. PTO environment is used for load & performance testing on Acceptance.
11. Sonar uses Generic OAM for authentication purpose.
12. Sonar uses its own OID instances as user store.
13. A separate Windows File server is added to Production to store SONAR documents which could not be migrated successfully to EA. UWV FB has the option to lookup manually a certain document via a network share (SMB).

## Context diagram

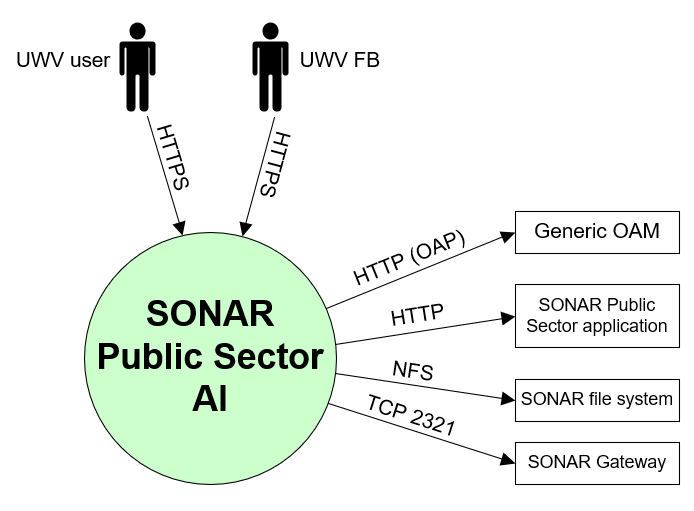
Diagram, schematic

Description automatically generated

The above diagrams shows the Context Diagram and the external entities for the SONAR 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.

### SONAR Public Sector AI

(Public Sector – Application Interface)



#### External entities

##### UWV user

|  |  |
| --- | --- |
| **Description** | UWV Sonar User. Web-based User Interface (inclusief Gemeente) |
| **Protocol and Port** | HTTPS (443) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Transport Layer Security (HTTPS), Role Based Access |
| **Number of users** | ~5000 avg. concurrent |
| **Number of transactions** | 50.000 per day in total for Siebel (2012, no recent data available) |
| **Frequency of transactions** | Daily |
| **Volume of data** | Not specified |

##### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV Functional Support. |
| **Protocol and Port** | HTTPS (443), |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Transport Layer Security (HTTPS), Role Based Access |
| **Number of users** | Less than 10 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### Generic OAM

|  |  |
| --- | --- |
| **Description** | User authentication providing single sign-on for Sonar users using Generic OAM. OAM is connecting to the OID instance of Sonar  Oracle Webgate component running on the Public sector webserver connects via https to the Detached Credential Collector (DCC) of Generic OAM - Oracle Access Manager. OAM validates the user credentials via LDAPS in the Oracle Internet Directory (OID). This OID instance is part of the Sonar CI. |
| **Protocol and Port** | OAP (5575) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Role Based Access, Secure transport |
| **Number of users** | 1 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### SONAR Public Sector application

|  |  |
| --- | --- |
| **Description** | Access to the SONAR Public Sector back-end |
| **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** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

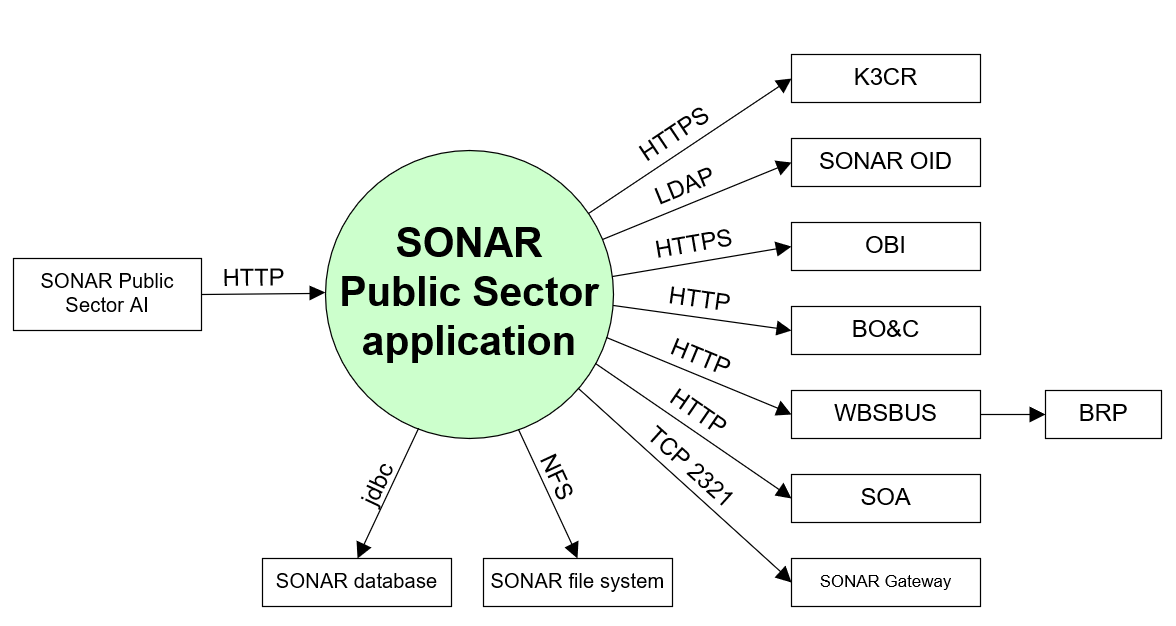
##### SONAR file system

|  |  |
| --- | --- |
| **Description** | Access to SONAR file system |
| **Protocol and Port** | NFS (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Gateway

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR Public Sector application



#### External entities

##### SONAR Public Sector AI

|  |  |
| --- | --- |
| **Description** | Access from the SONAR Public Sector application interface to the SONAR Public Sector back-end |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### K3CR

|  |  |
| --- | --- |
| **Description** | K3CR url |
| **Protocol and Port** | HTTPS (443) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Secure transport |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR OID

|  |  |
| --- | --- |
| **Description** | Retrieve users and groups from SONAR OID |
| **Protocol and Port** | LDAP (389) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### OBI

|  |  |
| --- | --- |
| **Description** | Access OBI in iFrame |
| **Protocol and Port** | HTTPS (7024) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Secure transport |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### BO&C (Werk.nl backend)

|  |  |
| --- | --- |
| **Description** | BO&C (Beroepen, Opleidingen, Competenties en Cursussen)  Client to BO&C web application: Beroepen, Opleidingen, Competenties en Cursussen informatie |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Role Based Access |
| **Number of users** | 1 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### BRP

|  |  |
| --- | --- |
| **Description** | BRP url (through WBSBUS) |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | No, via WBSBUS |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SOA

|  |  |
| --- | --- |
| **Description** | Several functions are accessed through SOA |
| **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** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Gateway

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR file system

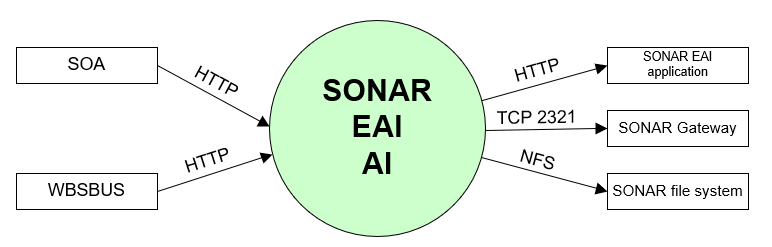
|  |  |
| --- | --- |
| **Description** | Access to SONAR file system |
| **Protocol and Port** | NFS (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR database

|  |  |
| --- | --- |
| **Description** | Access to SONAR Database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR EAI AI

(e-Business Application Integration – Application Interface)



#### External entities

##### WBSBUS

|  |  |
| --- | --- |
| **Description** | system communicating (through load balancer) with external SONAR businesses and users, among others: SMF, EAED, PeopleSoft, Prisma Satellite, K3CR, Werk.nl (Werkmap), E-Intake, DWH (database link to SONAR database), KOA aanvraag WW, BRP url |
| **Protocol and Port** | HTTP (8080) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SOA

|  |  |
| --- | --- |
| **Description** | SOA connections through the load balancer |
| **Protocol and Port** | HTTP (8080) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR EAI application

|  |  |
| --- | --- |
| **Description** | Access to the SONAR EAI back-end |
| **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** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

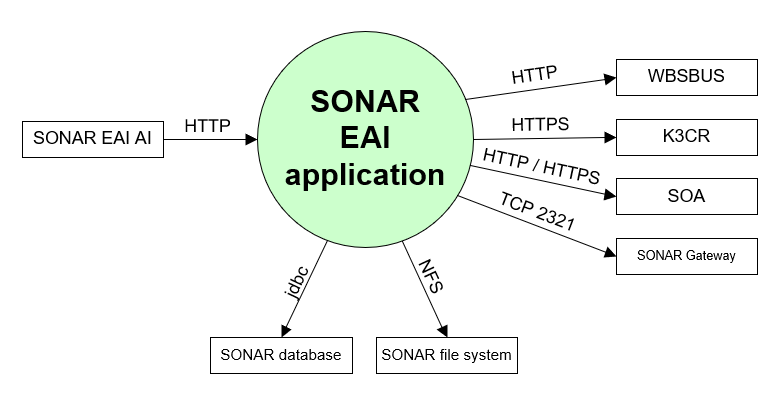
##### SONAR Gateway

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR file system

|  |  |
| --- | --- |
| **Description** | Access to SONAR file system |
| **Protocol and Port** | NFS (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR EAI application



#### External entities

##### SONAR EAI AI

|  |  |
| --- | --- |
| **Description** | Access from the SONAR EAI application interface to the SONAR EAI back-end |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### WBSBUS

|  |  |
| --- | --- |
| **Description** | system communicating with external SONAR businesses and users, among others: SMF, EAED, PeopleSoft, Prisma Satellite, K3CR, Werk.nl (Werkmap), E-Intake, DWH (database link to SONAR database), KOA aanvraag WW, BRP url |
| **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** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### K3CR

|  |  |
| --- | --- |
| **Description** | K3CR url |
| **Protocol and Port** | HTTPS (443) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Secure transport |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SOA

|  |  |
| --- | --- |
| **Description** | Several functions are accessed through SOA |
| **Protocol and Port** | HTTP (80), HTTPS (443) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Gateway

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

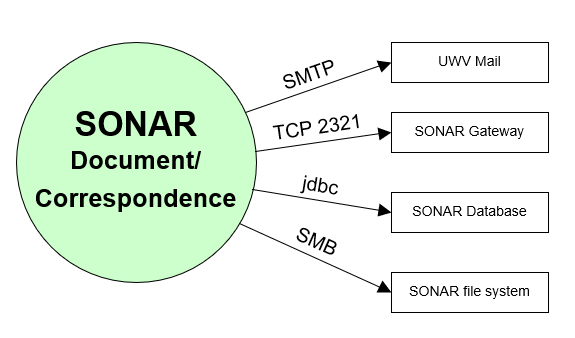
##### SONAR file system

|  |  |
| --- | --- |
| **Description** | Access to SONAR file system |
| **Protocol and Port** | NFS (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR database

|  |  |
| --- | --- |
| **Description** | Access to SONAR Database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR Document / Correspondence



#### External entities

##### UWV mail

|  |  |
| --- | --- |
| **Description** | Production: KPN Mail relay for sending mail to unemployed clients  Acceptance: Generieke Mail services for testing mail functionality |
| **Protocol and Port** | SMTP (25) with STARTTLS option |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Role Based Access, Secure transport |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Gateway

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

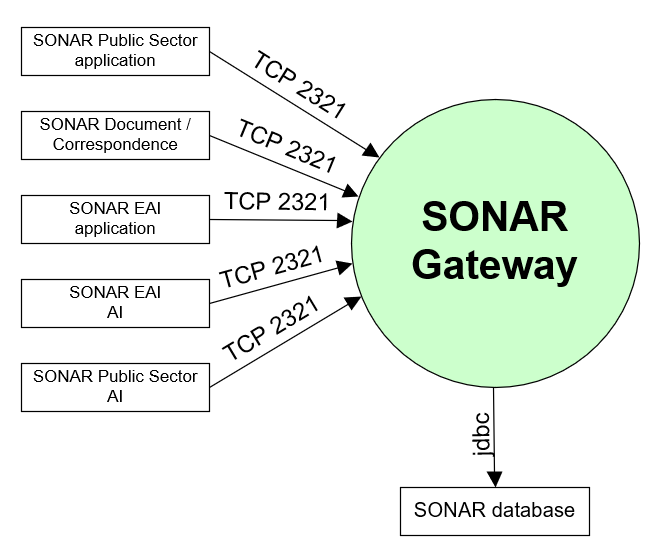
##### SONAR database

|  |  |
| --- | --- |
| **Description** | Access to SONAR Database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR file system

|  |  |
| --- | --- |
| **Description** | Access to SONAR file system |
| **Protocol and Port** | SMB v3 (445) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR Gateway



#### External entities

##### SONAR Public Sector application

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Document / Correspondence

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR EAI application

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR EAI AI

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

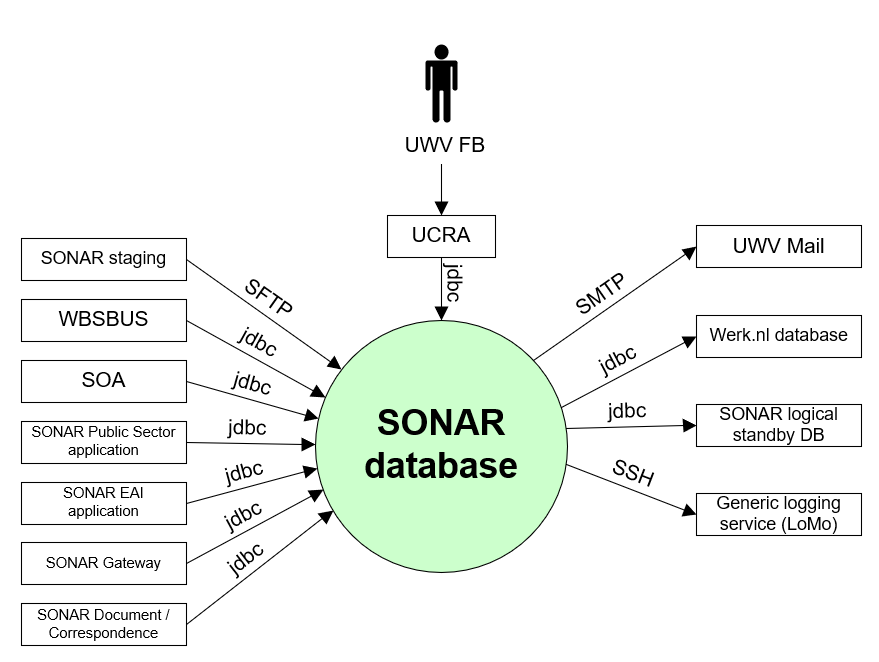
##### SONAR Public Sector AI

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | Proprietary (2321) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR database

|  |  |
| --- | --- |
| **Description** | Access to SONAR Database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR database



#### External entities

##### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV Functional Support |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Not specified |
| **Number of users** | 12 - 20 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### Werk.nl database

|  |  |
| --- | --- |
| **Description** | Support to compare Sonar SKB |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR logical standby database

|  |  |
| --- | --- |
| **Description** | Active DataGuard connection to the logical standby |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### Generic logging service

|  |  |
| --- | --- |
| **Description** | Shell script running on the database server that makes a coonection to the Generic logging service to transfer the LoMo (logging and Monitoring) log files. The Generic logging service provides the file via SI file transfer to QRADAR |
| **Protocol and Port** | SSH (22) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Document / Correspondence

|  |  |
| --- | --- |
| **Description** | Access to SONAR database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Gateway

|  |  |
| --- | --- |
| **Description** | Access to SONAR database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR EAI application

|  |  |
| --- | --- |
| **Description** | Access to SONAR database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Public Sector application

|  |  |
| --- | --- |
| **Description** | Access to SONAR database |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SOA

|  |  |
| --- | --- |
| **Description** | Access to SONAR database |
| **Protocol and Port** | JMS (1521, 2484) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### WBSBUS

|  |  |
| --- | --- |
| **Description** | Access to SONAR database |
| **Protocol and Port** | Oracle client (1521, 2484) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

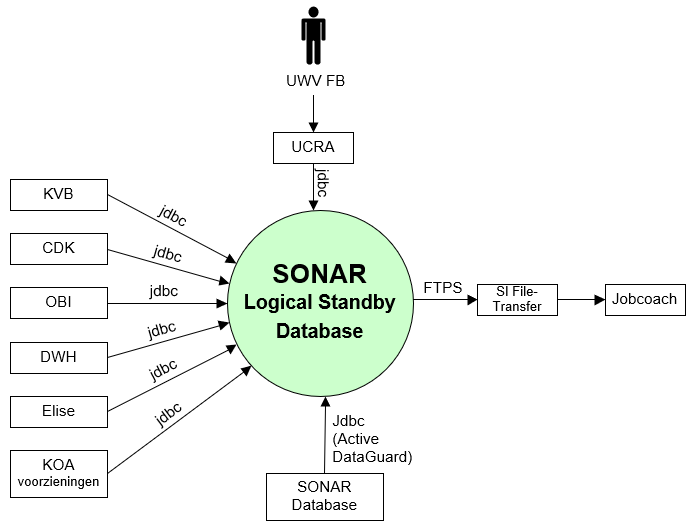
##### SONAR Staging

|  |  |
| --- | --- |
| **Description** | Provide templates |
| **Protocol and Port** | SFTP (22) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### UWV Mail

|  |  |
| --- | --- |
| **Description** | Sending mail notification to UWV FB from the SONAR DB servers |
| **Protocol and Port** | SMTP (25) |
| **DC (Datacenter) connection** | external |
| **Direction** | outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR logical standby database



#### External entities

##### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV Functional Support |
| **Protocol and Port** | Oracle client (1521) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Not specified |
| **Number of users** | Less than 10 total assumed |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### Jobcoach

|  |  |
| --- | --- |
| **Description** | Export data of Logical Standby database used by Jobcoach department for generating reports. |
| **Protocol and Port** | FTP (21) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No, via SI File-Transfer |
| **Security Controls** | Role Based Access, Secure transport |
| **Number of users** | 1 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | 1x week |
| **Volume of data** | Low |

##### SONAR database

|  |  |
| --- | --- |
| **Description** | Active DataGuard connection to the logical standby |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### KOA voorzieningen

|  |  |
| --- | --- |
| **Description** | KOA voorzieningen DB connection to the logical standby |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### Elise

|  |  |
| --- | --- |
| **Description** | Elise DB connection to the logical standby |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### DWH

|  |  |
| --- | --- |
| **Description** | DWH DB connection to the logical standby |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### OBI

|  |  |
| --- | --- |
| **Description** | OBI DB connection to the logical standby |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

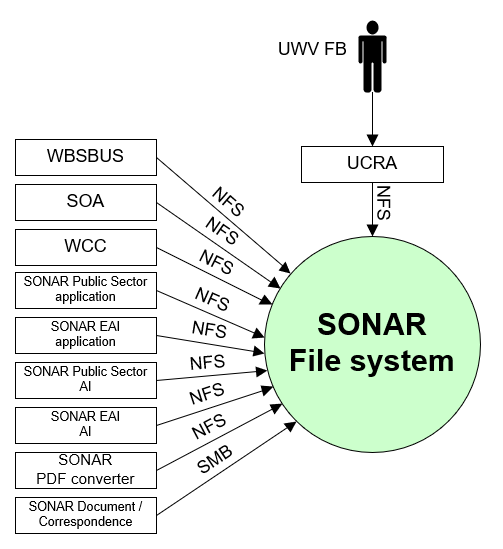
##### CDK

|  |  |
| --- | --- |
| **Description** | Queries for SUWI inkijk |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### KVB

|  |  |
| --- | --- |
| **Description** | KVB DB connection to the logical standby |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR file system



#### External entities

##### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV Functional Support – access to samba share |
| **Protocol and Port** | SMB v3 (445) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Not specified |
| **Number of users** | Less than 10 total assumed |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### SONAR Document / Correspondence

|  |  |
| --- | --- |
| **Description** | Access to Siebel file system |
| **Protocol and Port** | SMB v3 (445) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR PDF converter

|  |  |
| --- | --- |
| **Description** | Access to NFS |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR EAI AI

|  |  |
| --- | --- |
| **Description** | Access EAI Application servers to NFS |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Public Sector AI

|  |  |
| --- | --- |
| **Description** | Access EAI Application servers to NFS |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR EAI application

|  |  |
| --- | --- |
| **Description** | Access EAI Application servers to NFS |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Public Sector application

|  |  |
| --- | --- |
| **Description** | Access NFS share /siebelfs/queues |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### WCC

|  |  |
| --- | --- |
| **Description** | To PDF share |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

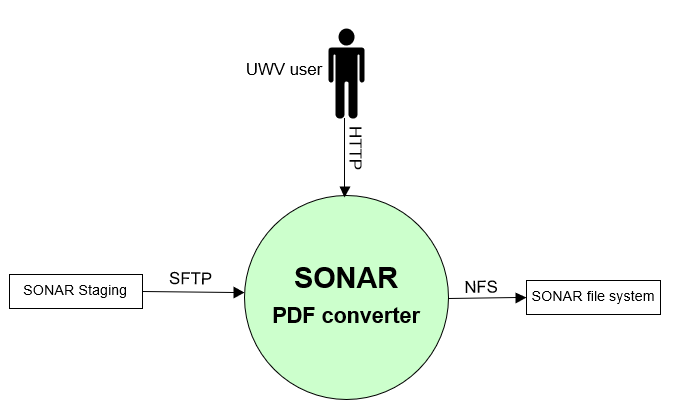
##### SOA

|  |  |
| --- | --- |
| **Description** | To PDF share |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### WBSBUS

|  |  |
| --- | --- |
| **Description** | To PDF share |
| **Protocol and Port** | NFS v4 (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR PDF converter



#### External entities

##### UWV user

|  |  |
| --- | --- |
| **Description** | HTTP access to Sonar PDF converter |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR Staging

|  |  |
| --- | --- |
| **Description** | Provide template |
| **Protocol and Port** | SFTP (22) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR file system

|  |  |
| --- | --- |
| **Description** | Access to SONAR file system |
| **Protocol and Port** | NFS (2049,111) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR Staging

Diagram

Description automatically generated

#### External entities

##### UWV FB

|  |  |
| --- | --- |
| **Description** | SSH access to SONAR Staging (from UCRA) |
| **Protocol and Port** | SSH (22) via UCRA  SFTP (22) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, SSH via UCRA  Yes. SFTP |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### SONAR database

|  |  |
| --- | --- |
| **Description** | Reading templates from staging server, staging server is placed in the DXC Application Management from where is connects to Production, Acceptance and KATO |
| **Protocol and Port** | SFTP (22) |
| **DC (Datacenter) connection** | internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

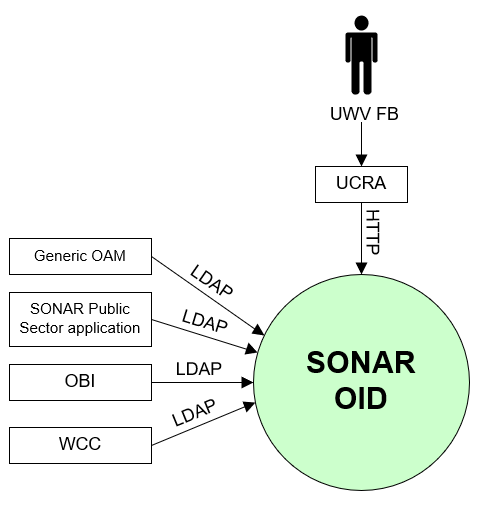
##### SONAR PDF converter

|  |  |
| --- | --- |
| **Description** | Reading templates from staging server, staging server is placed in the DXC Application Management from where is connects to Production, Acceptance and KATO |
| **Protocol and Port** | SFTP (22) |
| **DC (Datacenter) connection** | internal |
| **Direction** | outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### OBI

|  |  |
| --- | --- |
| **Description** | Connection from the OBI ETL server to SOANR staging |
| **Protocol and Port** | SFTP (22) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

### SONAR OID



#### External entities

##### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV Functional Support |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Not specified |
| **Number of users** | Less than 10 total assumed |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

##### WCC

|  |  |
| --- | --- |
| **Description** | SSO (Single Sign On) OID application, applications that share user single sign-on with SONAR are connecting read-only to the SONAR OID user store for their S2S (system to system) accounts. |
| **Protocol and Port** | LDAP (389, 3060) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### OBI

|  |  |
| --- | --- |
| **Description** | SSO (Single Sign On) OID application, applications that share user single sign-on with SONAR are connecting read-only to the SONAR OID user store for their S2S (system to system) accounts. |
| **Protocol and Port** | LDAP (389, 3060) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

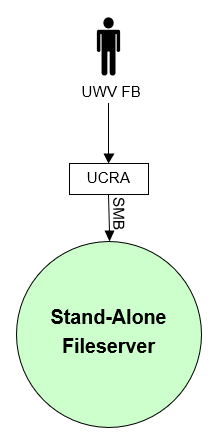
##### SONAR Public Sector application

|  |  |
| --- | --- |
| **Description** | Access to config and status data |
| **Protocol and Port** | LDAP (389, 3060) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

##### Generic OAM

|  |  |
| --- | --- |
| **Description** | User authentication providing single sign-on for Sonar users using Generic OAM. OAM is connecting to the OID instance of Sonar |
| **Protocol and Port** | LDAP (389, 3060) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | Role Based Access, Secure transport |
| **Number of users** | 1 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

### Stand-alone file server



#### External entities

##### UWV FB

|  |  |
| --- | --- |
| **Description** | UWV Functional Support, access to Word documents |
| **Protocol and Port** | SMB v3 (445) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Not specified |
| **Number of users** | Less than 10 |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Low |

# Functional Requirements

* Siebel eBusiness App Integration (EAI) and Siebel Public Sector must be separated, each must have its own web servers and application servers
* In the Sonar (Production only) environment an additional Windows File server is required to host customer data (The data involved are SONAR documents which could not be migrated properly to EA). UWV Sonar FB must be able to access the data via a network share.

# Non-Functional Requirements

## Security & Compliance classifications

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

|  |  |
| --- | --- |
| **Application** | SONAR |
| **Owner** | WB |
| **Availability (Beschikbaarheid)** | 3 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 2+ |
| **Type of information /Data Classification** | Private information for customers or 3rd party |
| **Direct or Indirect part of the primary information chain** | Direct |

### Risk analysis UWV

No risk analysis provided by UWV

### Applicable security and compliance frameworks

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

## Capacity and performance (volumetrics)

* The server sizing is based on the sizing before the transition. Performance tests after setting up the Acceptance environment should indicate whether the infrastructure must be up- or downscaled.
* The additional File server in Production is configured based on the current usage, no growth is expected.

## Availability

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Environment** | **Descripton** | **Application Target** | **Application Service Hours** | **Infra Target** | **Infra Service Hours** |
| Production | SONAR OID  SONAR file system  SONAR database | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 99,8% | 7 x 24 |
| Production | SONAR Public Sector  SONAR EAI  SONAR document / correspondence  SONAR Gateway  SONAR PDF converter  SONAR logical standby database | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 99,5% | 7 x 24 |
| Production | Stand-alone file server  Staging server | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) |
| Acceptance | All Acceptance and Kanban servers | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) |

## Security requirements

* SONAR end-users must be authenticated with Generic OAM (Generic OAM is configured to use Sonar OID as identity provider for Sonar).
* Only use SSL ciphers (certficates) that are supported by RUEI (applicable for SONAR and Generic OAM). Forward secrecy will not work for RUEI
* For the stand-alone File server, the following must be enabled:
  + File share auditing (Failure and Success)
  + Encryption for SMB (version 3) traffic
* UWV FB needs additional permissions on the Sonar DB, at least read / write

### System logging

No specific system logging requirements are applicable

Detailed Standard Security requirements are documented in Appendix D

## System management

No specific system management requirements applicable.

### Additional application related infra requirements

|  |  |
| --- | --- |
| **Requirements** | **Status** |
| Use STARTTLS option for UWV mail | No |
| Is Microsoft DTC used for inflight transactions | Not applicable |
| Is HTTPS cookie stickiness required on the load balancer | No |

## Backup and Recovery

No specific Backup and Recovery requirements applicable

## Storage replication

|  |  |  |
| --- | --- | --- |
| **Environment** | **Description** | **Storage Replication** |
| Production | Production servers | Replicated storage |
| Acceptance | Acceptance and KATO servers | Replicated storage |

## Scalability

* Vertical scalability is required to support a growing application workload that is below the boundaries of horizontal scalability.
* Horizontal scalability is required to support a growing application workload that cannot be mitigated with vertical scalability.
* No scalability limitations for the applications are specified

## Disaster Recovery

No specific disaster recovery requirements applicable.

## Infrastructure Technical Constraints

No infrastructure technical constraints.

## DXC TAB requirements

|  |  |
| --- | --- |
| **Cattegory** | **Description** |
| Deployment | Xldeploy is not applicable instead TAB deployment server (see HLD Werk.nl) is used  TAB NFS (see HLD Werk.nl) connections are required for applications that require shared storage (such as Weblogic) |
| Other TAB applicable requirement | Not specified at this moment .  If applicable (for example sitescope application monitoring), the information must come from DXC TAB after KT sessions are completed and the required App info is available.  This will be documented in HLD 1.1 |

# Solution

## Architectural Decisions

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Decision** | **Comments** | **Status** |
| 1 | All SONAR production components will have infra service level gold | All Production components from 1 CI require the same infra service level. For SONAR this is not the same as the CMO (Kyndryl) situation | Approved |
| 2 | In Accepance a Power HA cluster is build for the SONAR database and the SONAR file system | A Power HA cluster is the solution for a gold AIX system. To keep Production and Acceptance the same we deviate in Acceptance where we have a Power HA cluster for some bronze systems (applicable for SONAR database and file system) | Approved |
| 3 | SONAR application and gateway servers in Production are not build with a Power HA cluster | The standard solution for a Gold AIX system is a Power HA cluster. For The SONAR application and gateway servers Power HA clusters are not implemented. High Availability for the webservers is provided by a load balancer and multiple servers and for the other application servers HA is provided by Zookeeper (native application clustering) and multiple servers. The AIX Infra is built as Silver | Approved |
| 4 | SONAR OID DB will be build a a silver PaaS solution which means that the database server is build on a single VM with replicated storage to the opposite datacenter | This setup provides sufficient availability for the OID DB, Passive dataguard is not required | Approved |
| 5 | SONAR will have a Logical Standby database server for queries and exports | It is not acceptable to allow activities on the production database that impact performance. Database is copied with Oracle Active DataGuard | Approved |
| 6 | Oracle Webgate is Installed on Public Sector Web Servers to be able to connect to the Generic OAM for access | An Oracle Webgate must be used to control access to Sonar and to ensure that users identify themselves. | Approved |
| 7 | For Windows servers the standard authentication (through nested AD groups) and authorization (ABS) is used. | This is only applicable for UWV supporting functions. | Approved |
| 8 | Use the native application clustering for the Siebel Gatway servers based on Zookeeper | Utilizing zookeeper native application-level clustering adds to the high availability and scalability capability of the gateway functionality. Adding extra nodes to the zookeeper ensemble, is handled on application clustering level, and supported by the software vendor out-of-the-box. | Approved |
| 9 | Stand-alone Fileserver for SONAR documents which could not be migrated to EA is only needed in Production | SONAR documents which could not be migrated properly to EA are stored on a stand-alone fileserver. The server has no relationship with the other component and is therefore not needed in other environments | Approved |
| **#** | **Decision** | **Comments** | **Status** |
| 10 | SONAR database will be hosted on AIX | UWV approves the recommendation in the exception report regarding SONAR databases, the recommendation is to migrate the SONAR databases on the DXC AIX platform and to migrate the OID databases to the DXC private cloud in the designated go-live weekend. It is advised to agree on the SONAR databases in the short term, to migrate to the private cloud to spread the migration time and to keep financial impact as minimal as possible. | Approved |
| 11 | SONAR OID application server will be hosted on Linux | During the transition the SONAR OID application will be hosted on RHEL instead of AIX | Approved |
| 12 | OID version 12.2.1.4.0 will be installed, in combination with Weblogic 12c | OID version will be 12.2.1.4.0 instead of 11c, in combination with Weblogic 12c (instead of 11g) | Approved |
| 13 | SONAR OID database server will be hosted on Linux | During the transition the SONAR OID database will be hosted on RHEL instead of AIX | Approved |
| 14 | SONAR OID database wil be Oracle 19.1 | SONAR OID database version will be upgraded from 12.1 to 19.1 | Approved |
| 15 | The PTO environment will be used for performance testing, the SONAR acceptance environment does not have their own load generators | PTO is the standard UWV solution for load and performance testing | Approved |
| 16 | Staging server is added to SONAR HLD with SLA Bronze | Generiek services, staging server is only used by SONAR therefore it is moved to this HLD | Approved |
| 17 | SONAR file system, SONAR database, SONAR logical standby database and Stand- alone file server are placed in the “Kluis” security zone | These components are identified by UWV as the components that hold the data with Convidentiality rating 2+ | Approved |
| 18 | The EAI AI (Web) servers are placed in the “BackOffice” security zone together with the EAI application servers | EAI AI (Web) server only interacts with other applications (through SOA / WBSBUS, no user connections) and is therefore placed in the BackOffice | Approved |
| 19 | Oracle HTTP (includes OAM Webgate plugin) 12.2.1.4.0 is used | Previous Oracle HTTP 11G was used to be compatible with Generic OAM. DXC Generic OAM is on a higher version (12.2.1.4.0) | Approved |
| 20 | Allow direct UWV FB SFTP access to staging server (DXC AM) | File transfer from UWV FB to staging server using UCRA/DSM are experienced as being ‘slow’. |  |

## Node descriptions and zone-projections

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Security Zone** | **Domain** | **Description** | **Server Type** | **Node ID** | **Infra Service Level** |
| FrontOffice | Production | PROD | Web server | Public-Web1-P | Gold |
| FrontOffice | Production | PROD | Web server | Public-Web2-P | Gold |
| FrontOffice | Production | PROD | Web server | Public-Web3-P | Gold |
| BackOffice | Production | PROD | Web server | EAI-Web1-P | Gold |
| BackOffice | Production | PROD | Web server | EAI-Web2-P | Gold |
| FrontOffice | Production | PROD | Web server | PDF-Web1-P | Gold |
| FrontOffice | Production | PROD | Web server | PDF-Web2-P | Gold |
| BackOffice | Production | PROD | Application server | Public-APP1-P | Gold |
| BackOffice | Production | PROD | Application server | Public-APP2-P | Gold |
| BackOffice | Production | PROD | Application server | Public-APP3-P | Gold |
| BackOffice | Production | PROD | Application server | Public-APP4-P | Gold |
| BackOffice | Production | PROD | Application server | Public-APP5-P | Gold |
| BackOffice | Production | PROD | Application server | EAI-APP1-P | Gold |
| BackOffice | Production | PROD | Application server | EAI-APP2-P | Gold |
| BackOffice | Production | PROD | Application server | EAI-APP3-P | Gold |
| BackOffice | Production | PROD | Application server | EAI-APP4-P | Gold |
| BackOffice | Production | PROD | Application server | DOC-COR1-P | Gold |
| BackOffice | Production | PROD | Application server | DOC-COR2-P | Gold |
| BackOffice | Production | PROD | Application server | DOC-COR3-P | Gold |
| BackOffice | Production | PROD | Application server | Gateway1-P | Gold |
| BackOffice | Production | PROD | Application server | Gateway2-P | Gold |
| BackOffice | Production | PROD | Application server | Gateway3-P | Gold |
| BackOffice | Production | PROD | Application server | OID-APP1-P | Gold |
| BackOffice | Production | PROD | Database server | OID-DB1-P | Gold |
| **Security Zone** | **Domain** | **Description** | **Server Type** | **Node ID** | **Infra Service Level** |
| Kluis | Production | PROD | File Server (primary) | SONAR-FS1-P | Gold |
| Kluis | Production | PROD | File Server (failover) | SONAR-FS2-P | Gold |
| Kluis | Production | PROD | Database server (primary) | SONAR-DB1-P | Gold |
| Kluis | Production | PROD | Database server (failover) | SONAR-DB2-P | Gold |
| Kluis | Production | PROD | Database server | COPY-DB1-P | Gold |
| Kluis | Production | PROD | File Server | FS1-P | Gold |
| DXC AM | Production | PROD | Staging Server | Staging1-AM | Gold |
| FrontOffice | Acceptance | WATO | Web server | Public-Web1-A | Bronze |
| FrontOffice | Acceptance | WATO | Web server | Public-Web2-A | Bronze |
| FrontOffice | Acceptance | WATO | Web server | Public-Web3-A | Bronze |
| BackOffice | Acceptance | WATO | Web server | EAI-Web1-A | Bronze |
| BackOffice | Acceptance | WATO | Web server | EAI-Web2-A | Bronze |
| FrontOffice | Acceptance | WATO | Web server | PDF-Web1-A | Bronze |
| FrontOffice | Acceptance | WATO | Web server | PDF-Web2-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | Public-APP1-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | Public-APP2-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | Public-APP3-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | Public-APP4-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | Public-APP5-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | EAI-APP1-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | EAI-APP2-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | EAI-APP3-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | EAI-APP4-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | DOC-COR1-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | DOC-COR2-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | DOC-COR3-A | Bronze |
| **Security Zone** | **Domain** | **Description** | **Server Type** | **Node ID** | **Infra Service Level** |
| BackOffice | Acceptance | WATO | Application server | Gateway1-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | Gateway2-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | Gateway3-A | Bronze |
| BackOffice | Acceptance | WATO | Application server | OID-APP1-A | Bronze |
| BackOffice | Acceptance | WATO | Database server | OID-DB1-A | Bronze |
| Kluis | Acceptance | WATO | File Server (primary) | SONAR-FS1-A | Bronze |
| Kluis | Acceptance | WATO | File Server (failover) | SONAR-FS2-A | Bronze |
| Kluis | Acceptance | WATO | Database server (primary) | SONAR-DB1-A | Bronze |
| Kluis | Acceptance | WATO | Database server (failover) | SONAR-DB2-A | Bronze |
| Kluis | Acceptance | WATO | Database server | COPY-DB1-A | Bronze |
| Kluis | Acceptance | KATO | DB+FS+PDF | DATA-K | Bronze |
| BackOffice | Acceptance | KATO | Siebel (web+app+ gateway) | SIEBEL-K | Bronze |
| BackOffice | Acceptance | KATO | Application server | DOC-COR1-K | Bronze |
| BackOffice | Acceptance | KATO | Database server | OID-DB1-K | Bronze |
| BackOffice | Acceptance | KATO | Application server | OID-APP1-K | Bronze |

### DNS (customer facing name)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Desription** | **Comments** | **Customer facing name** | **DNS suffix** |
| Production | PROD | SONAR Public Sector AI | sonar | P-dc.ba.uwv.nl |
| Production | PROD | SONAR EAI AI | sonar-eai | P-dc.ba.uwv.nl |
| Production | PROD | SONAR PDF Converter | pdfweb | P-dc.ba.uwv.nl |
| Production | PROD | SONAR file system | pdfshare | P-dc.ba.uwv.nl |
| Acceptance | WATO | SONAR Public Sector AI | sonar | A-dc.ba.uwv.nl |
| Acceptance | WATO | SONAR EAI AI | Sonar-eai | A-dc.ba.uwv.nl |
| Acceptance | WATO | SONAR PDF Converter | pdfweb | A-dc.ba.uwv.nl |
| Acceptance | WATO | SONAR file system | pdfshare | A-dc.ba.uwv.nl |
| Acceptance | KATO | SONAR Public Sector AI | sonar-kato | A-dc.ba.uwv.nl |
| Acceptance | KATO | SONAR EAI AI | sonar-kato-eai | A-dc.ba.uwv.nl |
| Acceptance | KATO | SONAR PDF Converter | pdfweb-k | A-dc.ba.uwv.nl |
| Acceptance | KATO | SONAR file system | pdfshare-k | A-dc.ba.uwv.nl |

## System diagram – Production



## System diagram Non-Production and Staging

### Staging

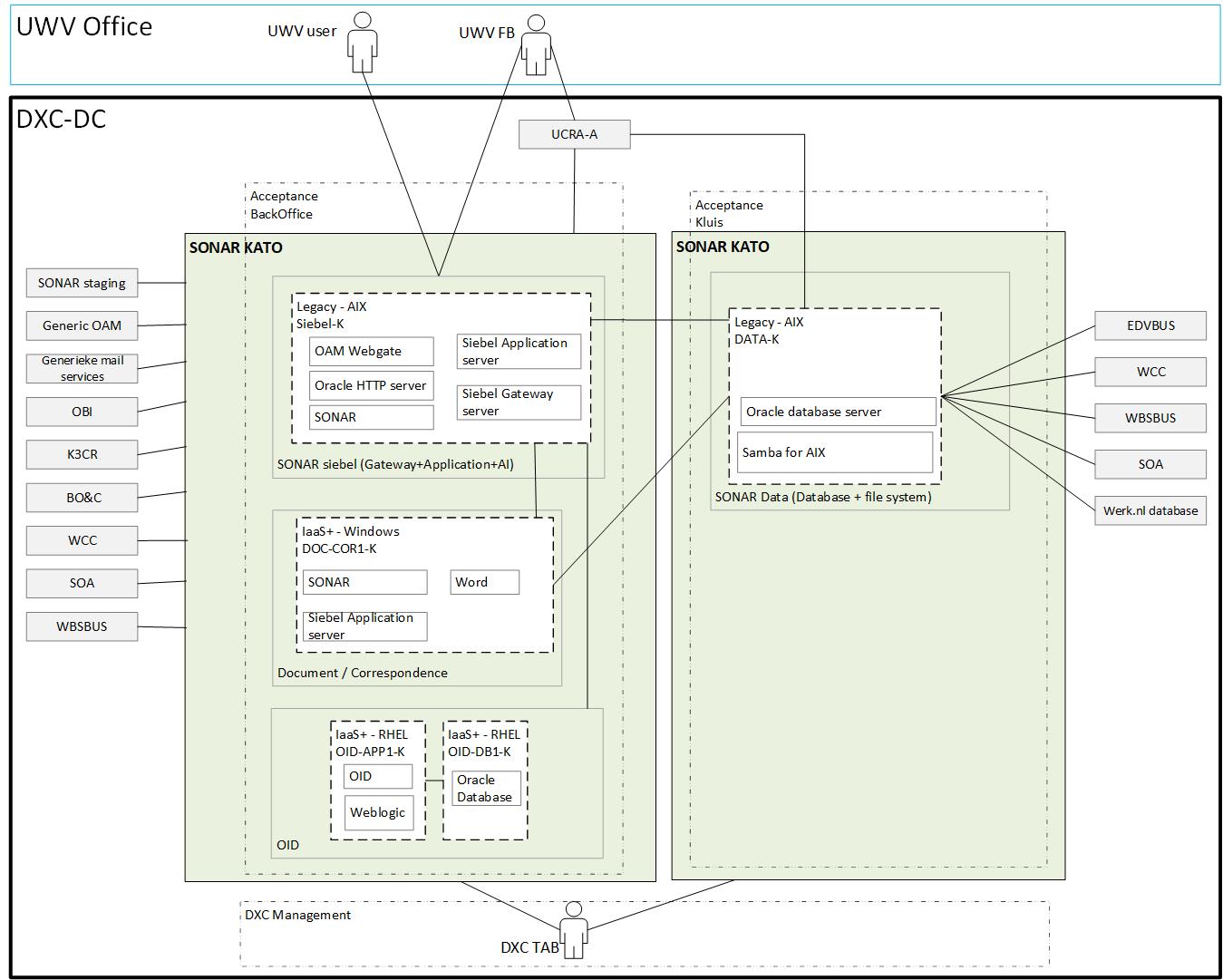
Diagram

Description automatically generated

Staging is used to share files between different environments (cross zone connections) therefore it is placed in the DXC Application Management zone.

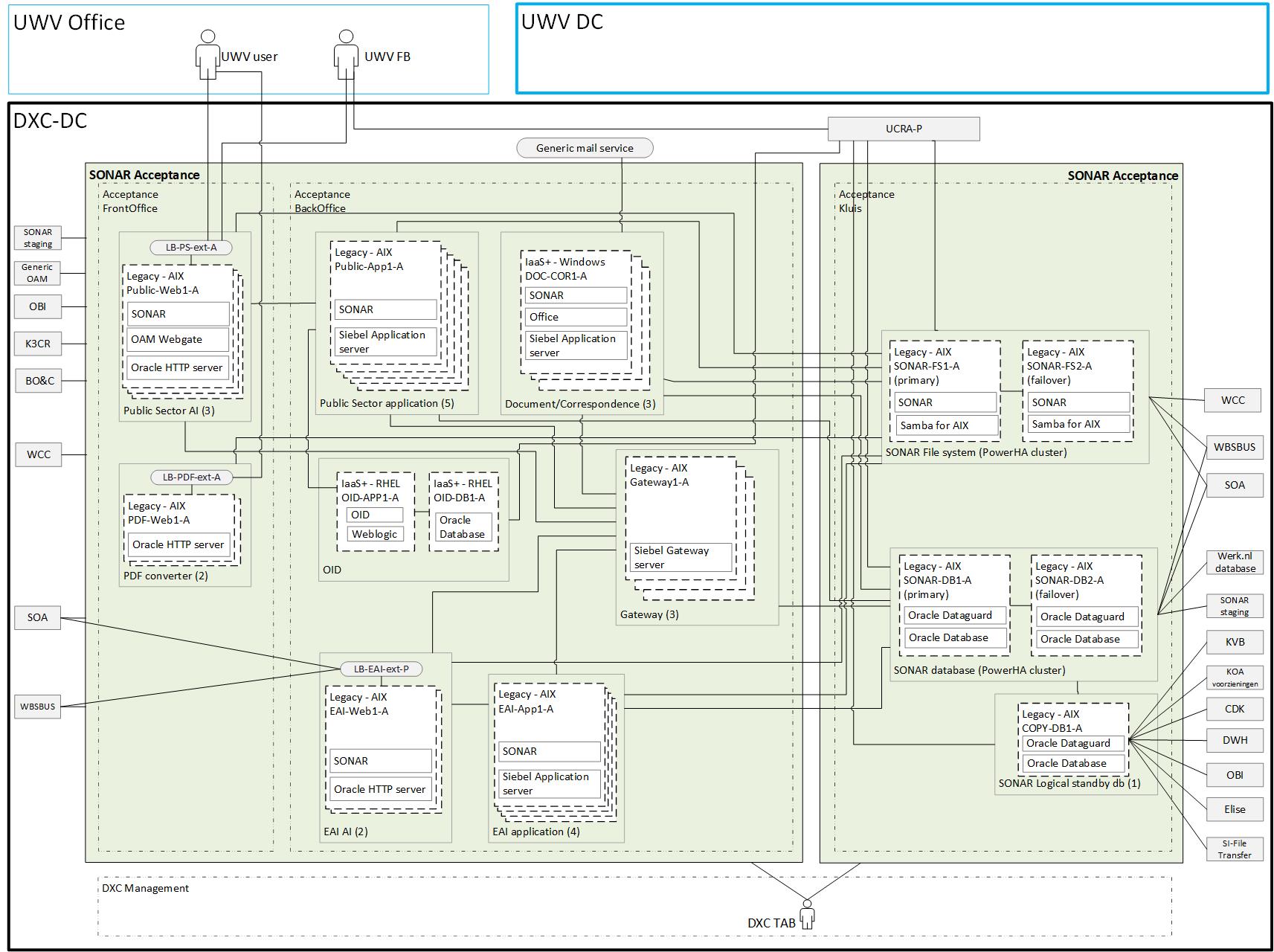
Note: KATO is part of Acceptance.

### KATO



Note: KATO is an acceptance “light” environment where several functions are combined on 1 system, it is used for technical tests.

### Acceptance



Note: Acceptance is almost the same as production but does not use UWV mail (instead the Generic mail service is used) and does not include the stand-alone fileserver.

## SBB’s

|  |
| --- |
| **Standard Building Block Type** |
| IaaS+ - VM- DXC Managed |
| PaaS - Virtual Oracle database - DXC Managed |
| Legacy hosting - AIX LPAR - DXC Managed |

## Load balancers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Domain** | **Load balancer** | **Type**  **inline/onearm** | **Description** | **LB ID** |
| Production | Fortinet Fortigate (Legacy) | inline | Public Sector AI | LB-PS-ext-P |
| Production | Fortinet Fortigate (Legacy) | inline | EAI AI | LB-EAI-ext-P |
| Production | Fortinet Fortigate (Legacy) | inline | PDF converter | LB-PDF-ext-P |
| Acceptance | Fortinet Fortigate (Legacy) | inline | Public Sector AI | LB-PS-ext-A |
| Acceptance | Fortinet Fortigate (Legacy) | inline | EAI AI | LB-EAI-ext-A |
| Acceptance | Fortinet Fortigate (Legacy) | inline | PDF converter | LB-PDF-ext-A |

Details can be found in Appendix A – Load balancers

## 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 | FrontOffice connection(s) to SONAR file system (Kluis) from:   * SONAR Public sector AI * SONAR PDF Converter * WBSBUS * UCRA (UWV FB) | Yes | 20220818-004 |
| 2 | FrontOffice connection(s) to SONAR database (Kluis) from:   * WBSBUS * UCRA (UWV FB) | Yes | 20220818-005 |
| 3 | FrontOffice connection(s) to Stand-alone Fileserver (Kluis) from:   * UCRA (UWV FB) | Yes | 20220818-006 |
| 4 | FrontOffice connection(s) to SONAR logical standby database (Kluis) from:   * UCRA (UWV FB) | Yes | 20220818-007 |
| 5 | HTTP (unencrypted) connection from UWV user (UWV werkplek) to load balancer PDF converter (FrontOffice) | Yes | 20220818-008 |
| 6 | Read / write permissions granted to UWV FB on the Sonar DB (Kluis) | Yes | 20220818-009 |
| 7 | TLS 1.0 instead of TLS 1.2 or higher | Yes | 20220729-001 |
| 8 | CrossConnection: SMTP from kluis through KPN UWV mail relay | Yes | 20220726-003 |
| 9 | Cross Connection: Direct communication from UWV Werkplek for UWV FB to Sonar Staging for SFTP. Risk of also SSH (same port). Connection through UCRA to slow.  Application: SONAR staging | Yes | 20230206-002-A |

## Licenses

| **License required for** |
| --- |
| Oracle HTTP server (includes OAM Webgate) 12.2.1.4.0 |
| Oracle Weblogic server 12.2.1.4.0 |
| Oracle OID 12.2.1.4.0 |
| Apache HTTP server 2.2.15 |
| Siebel applicatie server 21.4 |
| Siebel gateway server 21.4 |
| Office 2016 (Word, Excel, Powerpoint) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Environment** | **Description** | **Infra Hosting** | **Database / Middleware Management** | **Technical Application Management** |
| Production | All Production servers | Gold | TAB Basis | TAB Basis |
| Acceptance | All Acceptance and KATO servers | Bronze | TAB Basis | TAB Basis |

## Service Management

Note: In chapter 4.3 there are different availability and service window requirements for the different Production components. Since al components belong to 1 CI, they are all set to the same infra service level. It is agreed with UWV to use infra service level gold.

## Security

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

### User Authentication and Authorization

* UWV user (SONAR access)

Authentication and authorization are done through Generic OAM with SONAR OID as identity store, user / group management is done by UWV

* UWV FB (UCRA access)

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. Access for UWV users requested through the ABS IAM system and changes in PDXC.

* UWV FB (AIX access)

Variation 4 (Local - local login using local account): User Authentication and Authorization will be performed localy using a local user account, Middleware or AIX access for UWV users requested through the ABS IAM system and changes in PDXC.

* UWV FB (SONAR database access)

Variation 4 (Local - local login using local account): User Authentication and Authorization will be performed localy using a local user account, Middleware or AIX access for UWV users requested through the ABS IAM system and changes in PDXC.

* UWV FB (Stand-alone fileserver access)

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. 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.

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

* *Internal:* Connection within the application. For example, ODBC connection between the application- and the database server, if they are in different security zones a firewall is required and the Internal connection is document in the table below
* *External (inside DXC):* Connection external for the application but inside the DXC data center. For example, FTP connection between Application server and SI-File Transfer. To determine if these connections require a Firewall request the security zones must be known, this level of detail is not available in the HLD. The external (inside DXC) connections are not documented in the HLD but can be found in the application connectivity overview sheet.
* *External (outside DXC):* Connection external for the application and outside the DXC data center. For example, HTTP connection between Application server and the UWV Citrix KA farm. All external (outside DXC) connections are documented in the table below

For SONAR the following is applicable:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Connection Type** | **Between (component 1)** | **And (component 2)** |
| Internal | TCP (2321) | Public Sector AI servers | Gateway servers |
| Internal | HTTP | Public Sector AI servers | Public Sector application servers |
| Internal | NFS | Public Sector AI servers | SONAR file system |
| Internal | NFS | Public Sector application servers | SONAR file system |
| Internal | jdbc | Public Sector application servers | SONAR database |
| Internal | NFS | EAI AI servers | SONAR file system |
| Internal | NFS | EAI application servers | SONAR file system |
| Internal | jdbc | EAI application servers | SONAR database |
| Internal | jdbc | Document / Correspondence servers | SONAR database |
| Internal | NFS | Document / Correspondence servers | SONAR file system |
| Internal | jdbc | Gateway servers | SONAR database |
| Internal | jdbc | SONAR database | SONAR logical standby |
| Internal | SFTP | SONAR Staging | SONAR database |
| Internal | NFS | PDF Converter | SONAR file system |
| Internal | SFTP | SONAR Staging | PDF Converter |
| Internal | jdbc | UCRA | SONAR database |
| Internal | NFS | UCRA | SONAR file system |
| Internal | HTTP | UCRA | SONAR OID |
| Internal | SSH | UCRA | SONAR Staging |
| Internal | jdbc | UCRA | SONAR logical standby |
| Internal | SMB | UCRA | Stand-alone fileserver |
| External (outside DXC) | HTTPS | UWV Werkplek (UWV user + UWV FB) | Public Sector AI servers |
| External (outside DXC) | HTTP | UWV Werkplek (UWV user) | PDF Converter |
| External (outside DXC) | SMTP | Document / Correspondence servers | UWV mail |
| External (outside DXC) | SFTP | UWV Werkplek (UWV FB) | SONAR Staging |

For details see Appendix B

# Potential future improvements

|  |  |  |
| --- | --- | --- |
| **ID** | **Proposed improvement** | **Reason** |
| 1 | UWV to migrate WBS OID to SONAR OID | It is more efficient to use one OID for the users |
| 2 | UWV to use HTTPS connection to SONAR PDF converter | HTTP for external datacentre connections is considered as not secure |
| 3 | UWV to investigate if SMTP with STARTTLS can be used | Since recently this option is available and the preferred way to use SMTP within UWV |
| 4 | UWV to migrate from Legacy AIX to Private Cloud | AIX systems must be replaced by Linux because the private cloud is the preferred landing zone |
| 5 | UWV to design the SONAR application in such a way that the FrontOffice components no longer require a connection to the SONAR file system in the Kluis | Currently all SONAR components have a connection with the SONAR file system (including the AI servers) |
| 6 | UWV to organize the support for the SONAR application in such a way that UWV FB does not require direct access to components in the Kluis | Currently UWV FB connect (through UCRA) directly to all SONAR components in the Kluis |
| 7 | UWV to organize the support for the SONAR database in such a way that UWV FB does not require read / write permissions | Currently UWV FB requires read / write permissions to a database in the Kluis, this is not preferred |
| 8 | UWV to analyze the external connections from FrontOffice to the SONAR database and file system | FrontOffice to Kluis connections require an EtP and if possible, this needs to be prevented |
| 9 | UWV to investigate if the current NFS and SMB connection can be replaced by more secure connections | NFS and SMB are considered by UWV as unsecure and require analysis if they should be used in the future |
| 10 | UWV FB to use DSM instead of direct SFTP to transfer files to the staging server | DSM is the UWV standard for these kinds of file transfers |

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

## *Node details*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **DC** | **Domain** | **Node ID** | **(v)CPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Legacy Hosting AIX | Kluis | AM2 | Production | SONAR-DB1-P  uwvm2vapora0008 | 7 | 208 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | Kluis | AM3 | Production | SONAR-DB2-P  uwvm3vapora0008 | 7 | 208 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | Kluis | AM2 | Production | SONAR-FS1-P  uwvm2napfsc0001 | 1 | 24 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | Kluis | AM3 | Production | SONAR-FS2-P  uwvm3napfsc0001 | 1 | 24 | AIX 7.2 | Legacy | Gold | yes |
| Private Cloud Oracle DB | BackOffice | AM2 | Production | OID-DB1-P  UWVA2VLPORA0034 | 2 | 32 | RHEL7.9 | PaaS | Gold | yes |
| Private Cloud Oracle MW | BackOffice | AM2 | Production | OID-APP1-P  UWVA2VLPAPP0052 | 1 | 6 | RHEL7.9 | Iaas+ | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Gateway1-P  uwvm2vapapp0024 | 1 | 16 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Gateway2-P  uwvm2vapapp0025 | 1 | 16 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Gateway3-P  uwvm2vapapp0026 | 1 | 16 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | Kluis | AM2 | Production | COPY-DB1-P  uwvm2vapora0006 | 2 | 128 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | FrontOffice | AM2 | Production | Public-Web1-P  uwvm2vapweb0004 | 1 | 64 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | FrontOffice | AM2 | Production | Public-Web2-P  uwvm2vapweb0005 | 1 | 64 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | FrontOffice | AM2 | Production | Public-Web3-P  uwvm2vapweb0006 | 1 | 64 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | EAI-Web1-P  uwvm2vapweb0002 | 1 | 24 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | EAI-Web2-P  uwvm2vapweb0003 | 1 | 24 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Public-APP1-P  uwvm2vapapp0015 | 3 | 92 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Public-APP2-P  uwvm2vapapp0016 | 3 | 92 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Public-APP3-P  uwvm2vapapp0017 | 3 | 92 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Public-APP4-P  uwvm2vapapp0018 | 3 | 92 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Public-APP5-P  uwvm2vapapp0019 | 3 | 92 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | EAI-APP1-P  uwvm2vapapp0020 | 3 | 40 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | EAI-APP2-P  uwvm2vapapp0021 | 3 | 40 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | EAI-APP3-P  uwvm2vapapp0022 | 3 | 40 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | EAI-APP4-P  uwvm2vapapp0023 | 3 | 40 | AIX 7.2 | Legacy | Gold | yes |
| Legacy Hosting AIX | Frontoffice | AM2 | Production | PDF-Web1-P  uwvm2vapweb0007 | 1 | 4 | AIX 7.2 | Legacy | Gold | yes |
| **Landing Zone** | **Security Zone** | **DC** | **Domain** | **Node ID** | **CPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Legacy Hosting AIX | Frontoffice | AM2 | Production | PDF-Web2-P  uwvm2vapweb0008 | 1 | 4 | AIX 7.2 | Legacy | Gold | yes |
| Private Cloud | BackOffice | AM2 | Production | DOC-COR1-P  UWVA2VWPAPP0048 | 2 | 6 | Windows 2016 SE | Iaas+ | Gold | yes |
| Private Cloud | BackOffice | AM2 | Production | DOC-COR2-P  UWVA2VWPAPP0049 | 2 | 6 | Windows 2016 SE | Iaas+ | Gold | yes |
| Private Cloud | BackOffice | AM2 | Production | DOC-COR3-P  UWVA2VWPAPP0050 | 2 | 6 | Windows 2016 SE | Iaas+ | Gold | yes |
| Private Cloud | Kluis | AM2 | Production | FS1-P  UWVA2VWPAPP0070 | 1 | 4 | Windows 2016 SE | Iaas+ | Gold | yes |
| Legacy Hosting AIX | DXC AM | AM2 | Production | Staging1-AM  uwvm2vapapp0014 | 1 | 4 | AIX 7.1 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Kluis | AM3 | Acceptance | SONAR-DB1-A  uwvm3vaaora0005 | 7 | 204 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Kluis | AM2 | Acceptance | SONAR-DB2-A  uwvm2vaaora0002 | 7 | 204 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Gateway1-A  uwvm3vaaapp0033 | 1 | 16 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Gateway2-A  uwvm3vaaapp0034 | 1 | 16 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Gateway3-A  uwvm3vaaapp0035 | 1 | 16 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Kluis | AM3 | Acceptance | SONAR-FS1-A  uwvm3vaaapp0023 | 1 | 24 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Kluis | AM2 | Acceptance | SONAR-FS2-A  uwvm2vaaapp0011 | 1 | 24 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Kluis | AM3 | Acceptance | COPY-DB1-A  uwvm3vaaora0006 | 2 | 128 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Frontoffice | AM3 | Acceptance | Public-Web1-A  uwvm3vaaweb0003 | 1 | 64 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Frontoffice | AM3 | Acceptance | Public-Web2-A  uwvm3vaaweb0004 | 1 | 64 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Frontoffice | AM3 | Acceptance | Public-Web3-A  uwvm3vaaweb0005 | 1 | 64 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | EAI-Web1-A  uwvm3vaaweb0008 | 1 | 24 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | EAI-Web2-A  uwvm3vaaweb0009 | 1 | 24 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Public-APP1-A  uwvm3vaaapp0024 | 3 | 90 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Public-APP2-A  uwvm3vaaapp0025 | 3 | 90 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Public-APP3-A  uwvm3vaaapp0026 | 3 | 90 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Public-APP4-A  uwvm3vaaapp0027 | 3 | 90 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Public-APP5-A  uwvm3vaaapp0028 | 3 | 90 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | EAI-APP1-A  uwvm3vaaapp0029 | 3 | 40 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | EAI-APP2-A  uwvm3vaaapp0030 | 3 | 40 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | EAI-APP3-A  uwvm3vaaapp0031 | 3 | 40 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | EAI-APP4-A  uwvm3vaaapp0032 | 3 | 40 | AIX 7.2 | Legacy | Bronze | yes |
| **Landing Zone** | **Security Zone** | **DC** | **Domain** | **Node ID** | **CPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Legacy Hosting AIX | Frontoffice | AM3 | Acceptance | PDF-Web1-A  uwvm3vaaweb0006 | 1 | 4 | AIX 7.2 | Legacy | Bronze | yes |
| Legacy Hosting AIX | Frontoffice | AM3 | Acceptance | PDF-Web2-A  uwvm3vaaweb0007 | 1 | 4 | AIX 7.2 | Legacy | Bronze | yes |
| Private Cloud | BackOffice | AM3 | Acceptance | DOC-COR1-A  UWVA3VWAAPP0052 | 2 | 6 | Windows 2016 SE | Iaas+ | Bronze | yes |
| Private Cloud | BackOffice | AM3 | Acceptance | DOC-COR2-A  UWVA3VWAAPP0053 | 2 | 6 | Windows 2016 SE | Iaas+ | Bronze | yes |
| Private Cloud | BackOffice | AM3 | Acceptance | DOC-COR3-A  UWVA3VWAAPP0054 | 2 | 6 | Windows 2016 SE | Iaas+ | Bronze | yes |
| Private Cloud Oracle DB | BackOffice | AM3 | Acceptance | OID-DB1-A  UWVA3VLAORA0027 | 2 | 32 | RHEL7.9 | PaaS | Bronze | yes |
| Private Cloud Oracle MW | BackOffice | AM3 | Acceptance | OID-APP1-A  UWVA3VLAAPP0053 | 1 | 6 | RHEL7.9 | Iaas+ | Bronze | yes |
| Legacy Hosting AIX | Kluis | AM3 | Acceptance | DATA-K  uwvm3vaaora0008 | 1 | 130 | AIX 7.2 | Legacy | Bronze | no |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Siebel-K  uwvm3vaaapp0040 | 1 | 24 | AIX 7.2 | Legacy | Bronze | no |
| Private Cloud | BackOffice | AM3 | Acceptance | DOC-COR1-K  UWVA3VWAAPP0086 | 2 | 8 | Windows 2016 SE | Iaas+ | Bronze | no |
| Private Cloud Oracle DB | BackOffice | AM3 | Acceptance | OID-DB1-K  UWVA3VLAORA0041 | 2 | 16 | RHEL7.9 | PaaS | Bronze | no |
| Private Cloud Oracle MW | BackOffice | AM3 | Acceptance | OID-APP1-K  UWVA3VLAAPP0084 | 1 | 6 | RHEL7.9 | Iaas+ | Bronze | no |

## *Storage*

|  |  |  |  |
| --- | --- | --- | --- |
| **Node ID** | **Domain** | **C-drive OS (Fixed)** | **D-drive App (mandatory)** |
| DOC-COR1-P UWVA2VWPAPP0048 | Production | 100 | 50 |
| DOC-COR2-P UWVA2VWPAPP0049 | Production | 100 | 50 |
| DOC-COR3-P UWVA2VWPAPP0050 | Production | 100 | 50 |
| FS1-P UWVA2VWPAPP0070 | Production | 100 | 1000 |
| DOC-COR1-A UWVA3VWAAPP0052 | Acceptance | 100 | 50 |
| DOC-COR2-A UWVA3VWAAPP0053 | Acceptance | 100 | 50 |
| DOC-COR3-A UWVA3VWAAPP0054 | Acceptance | 100 | 50 |
| DOC-COR1-K UWVA3VWAAPP0086 | Acceptance | 100 | 100 |

*Windows Application server(s)*

*Linux Application server(s)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App (mandatory)** |
| OID-APP1-P UWVA2VLPAPP0052 | Production | 100 | 100 |
| OID-APP1-A UWVA3VLAAPP0053 | Acceptance | 100 | 100 |
| OID-APP1-K UWVA3VLAAPP0084 | Acceptance | 100 | 100 |

*Linux / AIX Oracle Database server(s)*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk0 OS (Fixed)** | **Disk1 Oracle Binaries (Fixed)** | **Disk2 ASM Binaries (Fixed)** | **ASM DATA1 DiskGroup1 Data Files, Control Files** | **ASM DATA2 DiskGroup1 Data Files, Control Files** | **ASM FRA1 DiskGroup2 Archive and Flashback Logs** | **ASM FRA2 DiskGroup2 Archive and Flashback Logs** | **ASM DATA3 DiskGroup1 Data Files, Control Files** | **ASM DATA4 DiskGroup1 Data Files, Control Files** |
| OID-DB1-P UWVA2VLPORA0034 | Production | 100 | 100 | 100 | 250 | 250 | 50 | 50 |  |  |
| OID-DB1-A UWVA3VLAORA0027 | Acceptance | 100 | 100 | 100 | 250 | 250 | 50 | 50 |  |  |
| OID-DB1-K UWVA3VLAORA0041 | Acceptance | 100 | 100 | 100 | 50 | 50 | 50 | 50 |  |  |
| DATA-K uwvm3vaaora0008 | Acceptance | 100 | 100 | 100 | 1000 | 1000 | 200 | 200 | 1000 | 1000 |
| COPY-DB1-P uwvm2vapora0006 | Production | 100 | 100 | 100 | 1000 | 1000 | 200 | 200 | 1000 | 1000 |
| COPY-DB1-A uwvm3vaaora0006 | Acceptance | 100 | 100 | 100 | 1000 | 1000 | 200 | 200 | 1000 | 1000 |

*AIX Oracle Database cluster (AIX GOLD – PowerHA Cluster)*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Cluster node Type**  **(active / passive)** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk1 Oracle Binaries (Fixed)** | **Disk2 ASM Binaries (Fixed)** | **SHARED Disk 3 – Mountpoint 1 Cluster (fixed)** | **SHARED Disk 4 – Mountpoint 1 Qourum (fixed)** | **SHARED - ASM DATA DiskGroup1 Data Files, Control Files (mandatory** | | **SHARED - ASM FRA DiskGroup2 Archive and Flashback Logs (mandatory)** | | **SHARED**  **Script folder (Batches)** |
| SONAR-DB1-P uwvm2vapora0008 | Active | Production | 100 GB | 100 GB | 100 GB | 10 GB | 1 GB | 4 x | 1 TB | 2 x | 200 GB | 50 GB |
| SONAR-DB2-P uwvm3vapora0008 | Passive | Production | 100 GB | 100 GB | 100 GB |
| SONAR-DB1-A uwvm3vaaora0005 | Active | Acceptance | 100 GB | 100 GB | 100 GB | 10 GB | 1 GB | 4 x | 1 TB | 2 x | 200 GB | 50 GB |
| SONAR-DB2-A uwvm2vaaora0002 | Passive | Acceptance | 100 GB | 100 GB | 100 GB |

*AIX Fileserver cluster (AIX GOLD – PowerHA Cluster)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Cluster node Type**  **(active / passive)** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **SHARED Disk 1 – Mountpoint 1 Cluster (fixed)** | **SHARED Disk 2 – Mountpoint 1 Qourum (fixed)** | **SHARED Disk 3 – Mountpoint 1 (Mandatory)** |
| SONAR-FS1-P uwvm2napfsc0001 | Active | Production | 100 GB | 10 GB | 1 GB | 2500 GB |
| SONAR-FS2-P uwvm3napfsc0001 | Passive | Production | 100 GB |
| SONAR-FS1-A uwvm3vaaapp0023 | Active | Acceptance | 100 GB | 10 GB | 1 GB | 2500 GB |
| SONAR-FS2-A uwvm2vaaapp0011 | Passive | Acceptance | 100 GB |

*AIX Production Application server(s)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App (mandatory)** |
| Staging1-AM uwvm2vapapp0014 | Production | 100 | 650 |
| Gateway1-P uwvm2vapapp0024 | Production | 100 | 50 |
| Gateway2-P uwvm2vapapp0025 | Production | 100 | 50 |
| Gateway3-P uwvm2vapapp0026 | Production | 100 | 50 |
| Public-Web1-P uwvm2vapweb0004 | Production | 100 | 150 |
| Public-Web2-P uwvm2vapweb0005 | Production | 100 | 150 |
| Public-Web3-P uwvm2vapweb0006 | Production | 100 | 150 |
| EAI-Web1-P uwvm2vapweb0002 | Production | 100 | 100 |
| EAI-Web2-P uwvm2vapweb0003 | Production | 100 | 100 |
| Public-APP1-P uwvm2vapapp0015 | Production | 100 | 200 |
| Public-APP2-P uwvm2vapapp0016 | Production | 100 | 200 |
| Public-APP3-P uwvm2vapapp0017 | Production | 100 | 200 |
| Public-APP4-P uwvm2vapapp0018 | Production | 100 | 200 |
| Public-APP5-P uwvm2vapapp0019 | Production | 100 | 200 |
| EAI-APP1-P uwvm2vapapp0020 | Production | 100 | 150 |
| EAI-APP2-P uwvm2vapapp0021 | Production | 100 | 150 |
| EAI-APP3-P uwvm2vapapp0022 | Production | 100 | 150 |
| EAI-APP4-P uwvm2vapapp0023 | Production | 100 | 150 |
| PDF-Web1-P uwvm2vapweb0007 | Production | 100 | 50 |
| PDF-Web2-P uwvm2vapweb0008 | Production | 100 | 50 |

*AIX Acceptance application server(s)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App (mandatory)** |
| Gateway1-A uwvm3vaaapp0033 | Acceptance | 100 | 50 |
| Gateway2-A uwvm3vaaapp0034 | Acceptance | 100 | 50 |
| Gateway3-A uwvm3vaaapp0035 | Acceptance | 100 | 50 |
| Public-Web1-A uwvm3vaaweb0003 | Acceptance | 100 | 150 |
| Public-Web2-A uwvm3vaaweb0004 | Acceptance | 100 | 150 |
| Public-Web3-A uwvm3vaaweb0005 | Acceptance | 100 | 150 |
| EAI-Web1-A uwvm3vaaweb0008 | Acceptance | 100 | 100 |
| EAI-Web2-A uwvm3vaaweb0009 | Acceptance | 100 | 100 |
| Public-APP1-A uwvm3vaaapp0024 | Acceptance | 100 | 200 |
| Public-APP2-A uwvm3vaaapp0025 | Acceptance | 100 | 200 |
| Public-APP3-A uwvm3vaaapp0026 | Acceptance | 100 | 200 |
| Public-APP4-A uwvm3vaaapp0027 | Acceptance | 100 | 200 |
| Public-APP5-A uwvm3vaaapp0028 | Acceptance | 100 | 200 |
| EAI-APP1-A uwvm3vaaapp0029 | Acceptance | 100 | 150 |
| EAI-APP2-A uwvm3vaaapp0030 | Acceptance | 100 | 150 |
| EAI-APP3-A uwvm3vaaapp0031 | Acceptance | 100 | 150 |
| EAI-APP4-A uwvm3vaaapp0032 | Acceptance | 100 | 150 |
| PDF-Web1-A uwvm3vaaweb0006 | Acceptance | 100 | 50 |
| PDF-Web2-A uwvm3vaaweb0007 | Acceptance | 100 | 50 |
| Siebel-K uwvm3vaaapp0040 | Acceptance | 100 | 100 |

## *Software*

Production / Acceptance

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Node description** | **Suite** | **Software** | **Version** | **Supported by vendor** | **Latest version (N, N-1)** |
| SONAR Public Sector AI servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR Public Sector AI servers | 4-Middleware | Oracle HTTP server | 12.2.1.4.0 | Oracle |  |
| SONAR Public Sector AI servers | 4-Middleware | OAM Webgate | 12.2.1.4.0 | Oracle |  |
| SONAR Public Sector AI servers | 5-Application | Sonar | 7.3.3 |  |  |
|  |  |  |  |  |  |
| SONAR PDF converter servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR PDF converter servers | 4-Middleware | Oracle HTTP server | 12.2.1.4.0 | Oracle |  |
|  |  |  |  |  |  |
| SONAR EAI AI servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR EAI AI servers | 4-Middleware | Oracle HTTP server | 12.2.1.4.0 | Oracle |  |
| SONAR EAI AI servers | 5-Application | Oracle Client | 12.2.0.1.0 |  |  |
| SONAR EAI AI servers | 5-Application | Sonar | 7.3.3 |  |  |
|  |  |  |  |  |  |
| SONAR Public Sector Application servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR Public Sector Application servers | 5-Application | Siebel application server | 21.4 | Oracle |  |
| SONAR Public Sector Application servers | 5-Application | Oracle Client | 12.2.0.1.0 | Oracle |  |
| SONAR Public Sector Application servers | 5-Application | Sonar | 7.3.3 |  |  |
| SONAR Public Sector Application servers | 5-Application | JMS software pack |  |  |  |
|  |  |  |  |  |  |
| SONAR EAI application servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR EAI application servers | 5-Application | Siebel application server | 21.4 | Oracle |  |
| SONAR EAI application servers | 5-Application | Oracle Client | 12.2.0.1.0 | Oracle |  |
| SONAR EAI application servers | 5-Application | Sonar | 7.3.3 |  |  |
| SONAR EAI application servers | 5-Application | JMS software pack |  |  |  |
|  |  |  |  |  |  |
| SONAR database servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR database servers | 1-OS | PowerHA Cluster manager | 7.2 | IBM |  |
| SONAR database servers | 3-Database | Oracle database server | 12.2 | Oracle |  |
| SONAR database servers | 3-Database | Oracle dataguard | 12.2 | Oracle |  |
| SONAR database servers | 3-Database | Oracle Automatic Storage Manager ASM | 12.2 | Oracle |  |
|  |  |  |  |  |  |
| Stand-alone file server | 1-OS | Windows | 2016 SE | Microsoft |  |
| Stand-alone file server | 1-OS | Windows File Service role |  | Microsoft |  |
| **Node description** | **Suite** | **Software** | **Version** | **Supported by vendor** | **Latest version (N, N-1)** |
| SONAR Document / Correspondence servers | 1-OS | Windows | 2016 SE | Microsoft |  |
| SONAR Document / Correspondence servers | 5-Application | Siebel application server | 21.4 | Oracle |  |
| SONAR Document / Correspondence servers | 5-Application | Oracle Client | 12.2.0.1.0 | Oracle |  |
| SONAR Document / Correspondence servers | 5-Application | Internet Explorer | 11 | Microsoft |  |
| SONAR Document / Correspondence servers | 5-Application | Word | 2016 | Microsoft |  |
| SONAR Document / Correspondence servers | 5-Application | Excel | 2016 | Microsoft |  |
| SONAR Document / Correspondence servers | 5-Application | Powerpoint | 2016 | Microsoft |  |
|  |  |  |  |  |  |
| SONAR Gateway servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR Gateway servers | 5-Application | Oracle Client | 12.2.0.1.0 | Oracle |  |
| SONAR Gateway servers | 5-Application | Siebel Gateway Server | 21.4 | Oracle |  |
|  |  |  |  |  |  |
| SONAR OID application servers | 1-OS | RHEL | 7.9 | RedHat |  |
| SONAR OID application servers | 4-Middleware | OID (Oracle Internet Directory) | 12.2.1.4.0 | Oracle |  |
| SONAR OID application servers | 4-Middleware | Oracle Weblogic server | 12c | Oracle |  |
|  |  |  |  |  |  |
| SONAR OID database servers | 1-OS | RHEL | 7.9 | RedHat |  |
| SONAR OID database servers | 3-Database | Oracle database server | 19.1 | Oracle |  |
|  |  |  |  |  |  |
| SONAR file system servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR file system servers | 1-OS | PowerHA Cluster manager | 7.2 | IBM |  |
| SONAR file system servers | 4-Middleware | Samba for AIX |  | OpenSource |  |
| SONAR file system servers | 5-Application | Sonar | 4.7 |  |  |
|  |  |  |  |  |  |
| SONAR staging server | 1-OS | AIX | 7.1 | IBM |  |
| SONAR staging server | 2-Library | AIX FTP server | 7.1 | IBM |  |
| SONAR staging server | 5-Application | OpenSSH | 6.8 | OpenBSD Project |  |
|  |  |  |  |  |  |
| SONAR Logical Standby database servers | 1-OS | AIX | 7.2 | IBM |  |
| SONAR Logical Standby database servers | 3-Database | Oracle Database Server | 12.2 | Oracle |  |
| SONAR Logical Standby database servers | 3-Database | Oracle Data Guard | 12.2 | Oracle |  |
| SONAR Logical Standby database servers | 3-Database | Oracle ASM | 12.2 | Oracle |  |
| SONAR Logical Standby database servers | 5-Application | Export Sonar incremental for DWH |  |  |  |
| SONAR Logical Standby database servers | 5-Application | Export Sonar for Jobcoach |  |  |  |

**KATO**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Node description** | **Suite** | **Software** | **Version** | **Supported by vendor** | **Latest version (N, N-1)** |
| SONAR Data (DB+NFS) | 1-OS | AIX | 7.2 | IBM |  |
| SONAR Data (DB+NFS) | 1-OS | SAMBA for AIX |  | Open Source |  |
| SONAR Data (DB+NFS) | 3-Database | Oracle Database Server | 12.2 | Oracle |  |
| SONAR Data (DB+NFS) | 3-Database | Oracle Automatic Storage Manager ASM | 12.2 | Oracle |  |
| SONAR Data (DB+NFS) | 5-Application | MergePDF (shellscripts) |  |  |  |
|  |  |  |  |  |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 1-OS | AIX | 7.2 | IBM |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 4-Middleware | Oracle HTTP server | 12.2.1.4.0 | Oracle |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 4-Middleware | OAM Webgate | 12.2.1.4.0 | Oracle |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 5-Application | Oracle Client | 12.2.0.1.0 | Oracle |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 5-Application | Jms Software stack |  |  |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 5-Application | Siebel Gateway Server | 21.4 | Oracle |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 5-Application | Siebel Applicatie Server | 21.4 | Oracle |  |
| SONAR Siebel (Siebel Gateway + APP + AI) | 5-Application | Sonar | 7.3.3 |  |  |
|  |  |  |  |  |  |
| SONAR Document / Correspondence | 1-OS | Windows Server | 2016 SE | Microsoft |  |
| SONAR Document / Correspondence | 5-Application | Oracle Client | 12.2.0.1.0 | Oracle |  |
| SONAR Document / Correspondence | 5-Application | Siebel Tools | 21.4 | Oracle |  |
| SONAR Document / Correspondence | 5-Application | Siebel Applicatie Server | 21.4 | Oracle |  |
| SONAR Document / Correspondence | 5-Application | Office Word | 2016 | Microsoft |  |
| SONAR Document / Correspondence | 5-Application | Adobe reader | 10 | Adobe |  |
|  |  |  |  |  |  |
| SONAR OID application server | 1-OS | RHEL | 7.9 | RedHat |  |
| SONAR OID application server | 4-Middleware | OID (Oracle Internet Directory) | 12.2.1.4.0 | Oracle |  |
| SONAR OID application server | 4-Middleware | Oracle Weblogic server | 12c | Oracle |  |
|  |  |  |  |  |  |
| SONAR OID database server | 1-OS | RHEL | 7.9 | RedHat |  |
| SONAR OID database server | 3-Database | Oracle database server | 19.1 | Oracle |  |

## *Load Balancers*

***Production***

|  |  |  |  |
| --- | --- | --- | --- |
| **LB ID** | LB-PS-ext-P | LB-EAI-ext-P | LB-PDF-ext-P |
| **Security zone** | FrontOffice | BackOffice | FrontOffice |
| **Domain** | Production | Production | Production |
| **Clients zone (Internal / External)** | External | External | External |
| **Members (Name / IP)** | Public-Web1-P  Public-Web2-P  Public-Web3-P | EAI-Web1-P  EAI-Web2-P | PDF-Web1-P  PDF-Web2-P |
| **Application Layer Protocol** | HTTPS | HTTP | HTTP |
| **Application Port** | 443 | 8080 | 80 |
| **Application and Function** | User access to SONAR Public Sector | External application access to SONAR EAI | User access to SONAR PDF converter |
| **Expected concurrent connections** | < 10.000 | < 10.000 | < 10.000 |
| **LB Name (/ VIP)** | Sonar.p-dc.ba.uwv.nl | Sonar-eai.p-dc.ba.uwv.nl | pdfweb.p-dc.ba.uwv.nl |
| **Description** | Inline LB for Public Sector AI | Inline LB for EAI AI | Inline LB for PDF converter |
| **Algorithm** | Round-Robin | Round-Robin | Round-Robin |
| **Stickiness** | Source IP | HTTP/HTTPS cookie | No stickiness |
| **Health monitor** | TCP | HTTP | HTTP |
| **Port for use with Health Monitor** | 443 | 8080 | 80 |
| **Alias FQDN for VIP** | n/a | n/a | n/a |
| **Additional comments** | URL Probe GET online.html | URL Probe GET online.html | URL Probe GET online.html |

***Acceptance***

|  |  |  |  |
| --- | --- | --- | --- |
| **LB ID** | LB-PS-ext-A | LB-EAI-ext-A | LB-PDF-ext-A |
| **Security zone** | FrontOffice | BackOffice | FrontOffice |
| **Domain** | Acceptance | Acceptance | Acceptance |
| **Clients zone (Internal / External)** | External | External | External |
| **Members (Name / IP)** | Public-Web1-A  Public-Web2-A  Public-Web3-A | EAI-Web1-A  EAI-Web2-A | PDF-Web1-A  PDF-Web2-A |
| **Application Layer Protocol** | HTTPS | HTTP | HTTP |
| **Application Port** | 443 | 8080 | 80 |
| **Application and Function** | User access to SONAR Public Sector | External application access to SONAR EAI | User access to SONAR PDF converter |
| **Expected concurrent connections** | < 10.000 | < 10.000 | < 10.000 |
| **LB Name (/ VIP)** | Sonar.a-dc.ba.uwv.nl | Sonar-eai.a-dc.ba.uwv.nl | pdfweb.a-dc.ba.uwv.nl |
| **Description** | Inline LB for Public Sector AI | Inline LB for EAI AI | Inline LB for PDF converter |
| **Algorithm** | Round-Robin | Round-Robin | Round-Robin |
| **Stickiness** | Source IP | HTTP/HTTPS cookie | No stickiness |
| **Health monitor** | TCP | HTTP | HTTP |
| **Port for use with Health Monitor** | 443 | 8080 | 80 |
| **Alias FQDN for VIP** | n/a | n/a | n/a |
| **Additional comments** | URL Probe GET online.html | URL Probe GET online.html | URL Probe GET online.html |

# 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).*

*Application – Internal connections (Production / Acceptance)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Public-Web1-P  Public-Web2-P  Public-Web3-P | Gateway1-P  Gateway2-P  Gateway3-P | TCP | 2321 |  |
| Public-Web1-A  Public-Web2-A  Public-Web3-A | Gateway1-A  Gateway2-A  Gateway3-A | TCP | 2321 |  |

**Public Sector AI servers to Gateway servers**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Public-Web1-P  Public-Web2-P  Public-Web3-P | Public-APP1-P  Public-APP2-P  Public-APP3-P  Public-APP4-P  Public-APP5-P | HTTP | 80 |  |
| Public-Web1-A  Public-Web2-A  Public-Web3-A | Public-APP1-A  Public-APP2-A  Public-APP3-A  Public-APP4-A  Public-APP5-A | HTTP | 80 |  |

**Public Sector AI servers to Public Sector application servers**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Public-Web1-P  Public-Web2-P  Public-Web3-P | SONAR-FS1-P  SONAR-FS2-P | NFS | 2049, 111 |  |
| Public-Web1-A  Public-Web2-A  Public-Web3-A | SONAR-FS1-A  SONAR-FS2-A | NFS | 2049, 111 |  |

**Public Sector AI servers to SONAR File system (EtP)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Public-APP1-P  Public-APP2-P  Public-APP3-P  Public-APP4-P  Public-APP5-P | SONAR-FS1-P  SONAR-FS2-P | NFS | 2049, 111 |  |
| Public-APP1-A  Public-APP2-A  Public-APP3-A  Public-APP4-A  Public-APP5-A | SONAR-FS1-A  SONAR-FS2-A | NFS | 2049, 111 |  |

**Public Sector application servers to SONAR File system**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Public-APP1-P  Public-APP2-P  Public-APP3-P  Public-APP4-P  Public-APP5-P | SONAR-DB1-P  SONAR-DB2-P | jdbc | 1521 |  |
| Public-APP1-A  Public-APP2-A  Public-APP3-A  Public-APP4-A  Public-APP5-A | SONAR-DB1-A  SONAR-DB2-A | jdbc | 1521 |  |

**Public Sector application servers to SONAR database**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| EAI-Web1-P  EAI-Web2-P | SONAR-FS1-P  SONAR-FS2-P | NFS | 2049, 111 |  |
| EAI-Web1-A  EAI-Web2-A | SONAR-FS1-A  SONAR-FS2-A | NFS | 2049, 111 |  |

**EAI AI servers to SONAR File system**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| EAI-APP1-P  EAI-APP2-P  EAI-APP3-P  EAI-APP4-P | SONAR-FS1-P  SONAR-FS2-P | NFS | 2049, 111 |  |
| EAI-APP1-A  EAI-APP2-A  EAI-APP3-A  EAI-APP4-A | SONAR-FS1-A  SONAR-FS2-A | NFS | 2049, 111 |  |

**EAI Application servers to SONAR File system**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| EAI-APP1-P  EAI-APP2-P  EAI-APP3-P  EAI-APP4-P | SONAR-DB1-P  SONAR-DB2-P | jdbc | 1521 |  |
| EAI-APP1-A  EAI-APP2-A  EAI-APP3-A  EAI-APP4-A | SONAR-DB1-A  SONAR-DB2-A | jdbc | 1521 |  |

**EAI application servers to SONAR database**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DOC-COR1-P  DOC-COR2-P  DOC-COR3-P | SONAR-DB1-P  SONAR-DB2-P | jdbc | 1521 |  |
| DOC-COR1-A  DOC-COR2-A  DOC-COR3-A | SONAR-DB1-A  SONAR-DB2-A | jdbc | 1521 |  |

**Document / Correspondence servers to SONAR database**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DOC-COR1-P  DOC-COR2-P  DOC-COR3-P | SONAR-FS1-P  SONAR-FS2-P | SMB | 445 |  |
| DOC-COR1-A  DOC-COR2-A  DOC-COR3-A | SONAR-FS1-A  SONAR-FS2-A | SMB | 445 |  |

**Document / Correspondence to SONAR File system**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Gateway1-P  Gateway2-P  Gateway3-P | SONAR-DB1-P  SONAR-DB2-P | jdbc | 1521 |  |
| Gateway1-A  Gateway2-A  Gateway3-A | SONAR-DB1-A  SONAR-DB2-A | jdbc | 1521 |  |

**Gateway servers to SONAR database**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| SONAR-DB1-P  SONAR-DB2-P | COPY-DB1-P | jdbc | 1521 | Active Dataguard |
| SONAR-DB1-A  SONAR-DB2-A | COPY-DB1-A | jdbc | 1521 | Active Dataguard |

**SONAR database to SONAR Logical Standby**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Staging1-AM | SONAR-DB1-P  SONAR-DB2-P | SFTP | 22 |  |
| Staging1-AM | SONAR-DB1-A  SONAR-DB2-A | SFTP | 22 |  |

**SONAR Staging to SONAR database**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| PDF-Web1-P  PDF-Web2-P | SONAR-FS1-P  SONAR-FS2-P | NFS | 2049, 111 |  |
| PDF-Web1-P  PDF-Web2-P | SONAR-FS1-A  SONAR-FS2-A | NFS | 2049, 111 |  |

**SONAR PDF converter servers to SONAR File system (EtP)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Staging1-AM | PDF-Web1-P  PDF-Web2-P | SFTP | 22 |  |
| Staging1-AM | PDF-Web1-A  PDF-Web2-A | SFTP | 22 |  |

**SONAR staging to SONAR PDF converter servers**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UCRA-P | SONAR-DB1-P  SONAR-DB2-P | jdbc | 1521 | Database (EtP) |
| UCRA-P | SONAR-FS1-P  SONAR-FS2-P | NFS | 2049, 111 | File system (EtP) |
| UCRA-P | FS1-P | SMB | 2049, 111 | Standalone FS (EtP) |
| UCRA-P | OID-APP1-P | HTTP | 80 | OID |
| UCRA-P | COPY-DB1-P | jdbc | 1521 | Logical standby (EtP) |
| UCRA-P | Staging1-AM | SFTP | 22 | Staging |

**UCRA P connections**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UCRA-A | SONAR-DB1-A  SONAR-DB2-A | jdbc | 1521 | Database (EtP) |
| UCRA-A | SONAR-FS1-A  SONAR-FS2-A | NFS | 2049, 111 | File system (EtP) |
| UCRA-A | OID-APP1-A | HTTP | 80 | OID |
| UCRA-A | COPY-DB1-A | jdbc | 1521 | Logical standby (EtP) |

**UCRA A connections**

*Application – External connections (Outside DXC DC) - (Production / Acceptance)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UWV Werkplek | LB-PS-ext-P | HTTPS | 443 |  |
| UWV Werkplek | LB-PS-ext-A | HTTPS | 443 |  |

**UWV Werkplek to Load balancer Public Sector AI**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UWV Werkplek | LB-PDF-ext-P | HTTP | 80 |  |
| UWV Werkplek | LB-PDF-ext-A | HTTP | 80 |  |

**UWV Werkplek to Load balancer PDF Converter (EtP)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DOC-COR1-P  DOC-COR2-P  DOC-COR3-P | UWV Mail | SMTP | 25 |  |

**Document / Correspondence servers to UWV mail**

*Application – Internal connections (KATO)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Siebel-K | DATA-K | Jdbc, NFS | 1521, 2049, 11 |  |

**SONAR Siebel to SONAR data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DOC-COR1-K | DATA-K | Jdbc, SMB | 1521, 445 |  |

**Document / Correspondence server to SONAR data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UCRA-A | DATA-K | Jdbc, NFS | 1521, 2049, 11 | KATO data (EtP) |
| UCRA-A | Siebel-K | HTTP | 80 | Siebel |

**UCRA A connections**

*Application – External connections (Outside DXC DC) - (KATO)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UWV Werkplek | Siebel-K | HTTP /HTTPS | 80 / 443 |  |

**UWV Werkplek to SONAR Siebel**

*Application – External connections (Outside DXC DC) – UWV FB*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UWV FB | Staging1-AM | SFTP | 22 |  |

**UWV FB to Staging server**

**Only for HLD version 1.1:**

****

# Appendix C: Users and Groups

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

DXC Managed Users and groups are documented by DXC TAB in the TBH / TMM (Technisch Beheer Handboek / Technical Maintenance Manual) during the realization phase

***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** |
|  |  |  |  |

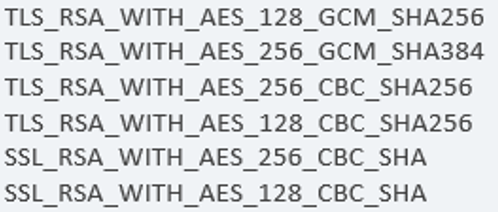
# Appendix D: Security

| Security & Compliance requirement | Deviations from the standard | Implementation of the requirements |
| --- | --- | --- |
| Authorization | No deviation | See Appendix C |
| OS hardening | No deviation | Standard hardening |
| Additional Middleware / database security configuration settings | No deviation | Standard hardening |
| Firewall ports (GRIP SSD-1) | Applicable | See Appendix B |
| UWV Admin / console interface  (GRIP SSD-17) | Applicable | Admin console available: Yes |
| Limit HTTP header information  (GRIP SSD-24) | Applicable | HTTP header information must be limited to the bare minimum to limit the impact of fingerprinting.  A review of header information must be held and approved by UWV.  The HTTP header information is not allowed to show:   1. webserver software 2. webserver version 3. http protocol   detailed error messages |
| Limit HTTP methods  (GRIP SSD-26) | Applicable | All non-relevant http method information must be removed. By default, only GET and POST are allowed |
| Disable Directory Listing  (GRIP SSD-29) | Applicable |  |
| TLS/SSL Certificates | Applicable | New SSL certificates must be created. Specify the details on all SSL certificates necessary for this application |
| Session Encryption - HTTPS  (GRIP SSD-4) | Applicable | If applicable specify: HTTPS |
| Session Encryption – SFTP  (GRIP SSD-4) | Applicable | If applicable specify: FTP / SFTP |
| Session Encryption – TLS version (GRIP SSD-4) | Applicable | TLS1.0 version is used because the application will otherwise not work, added this as an EtP |
| Security of Data in Transit External | No deviation | If applicable mention the relevant settings |
| Security of Data in Transit Internal | No deviation | NFS v4 is required on the SONAR file system |
| Segregation in security zones for Production | No deviation | See Appendix A |
| Segregation of Development, Test, Acceptance and Production environment | No deviation | See Appendix A |
| All software used must be supported by the vendor | No deviation | See Appendix A |
| Malware protection | No deviation | Standard scanning |
| Security Logging and -Monitoring retention  (default=1 year) | No deviation | 1 year |

1) *Based upon the latest NCSC recommendations and the used technologies within UWV (At design verification the allowed* *Cyphers are):*

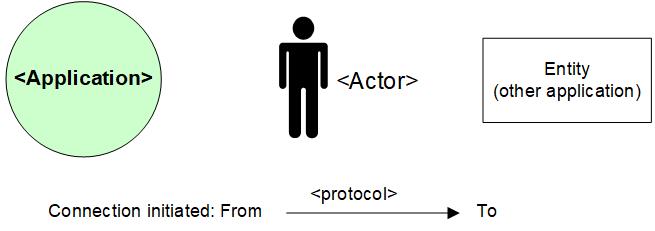
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA*
* *TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA*
* *TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA*

2) *SONAR RUEI compatible cyphers*

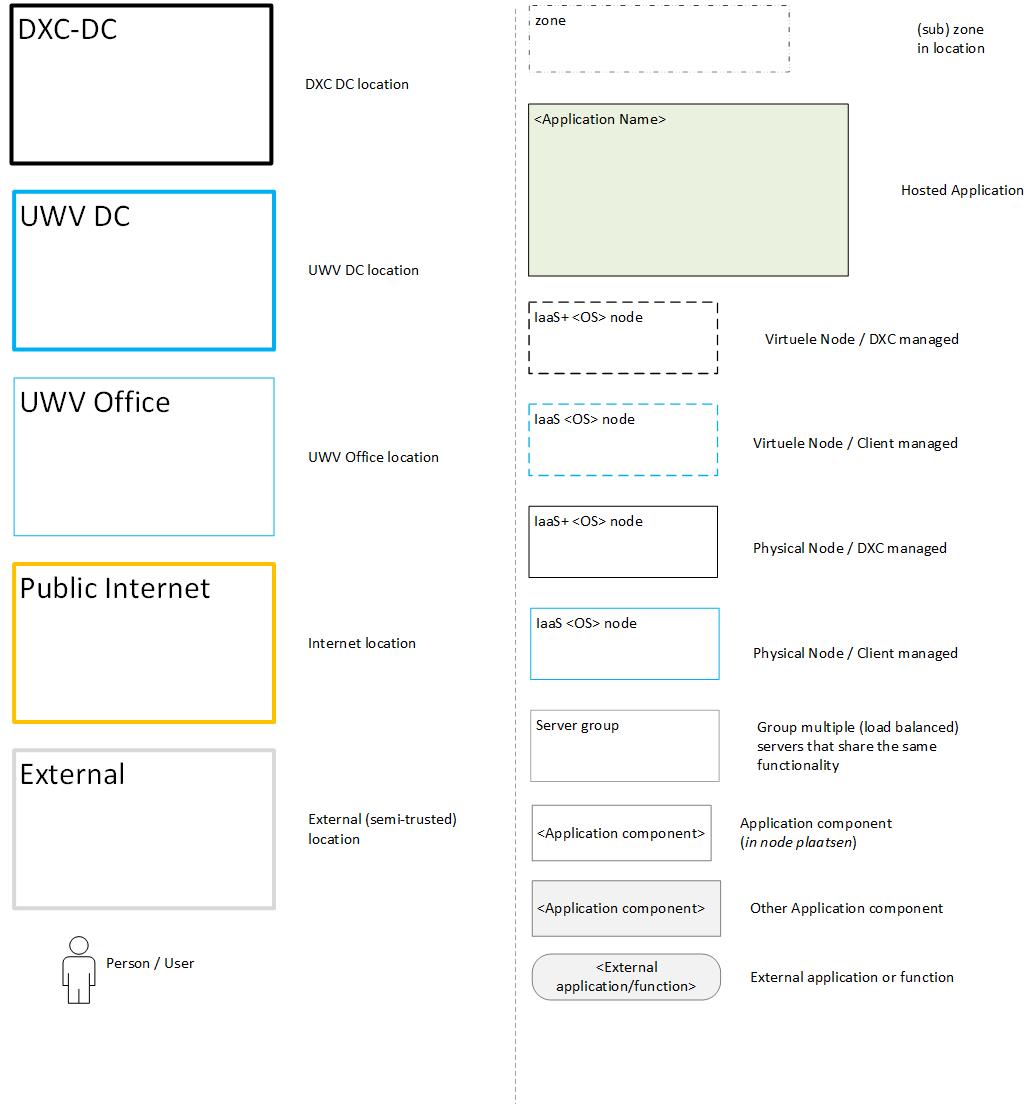
**

# Appendix F: Legenda

## Legenda Context Diagram



## Legenda System Diagram



# Appendix G: Control

**USED TEMPLATE**

|  |
| --- |
| Based on HLD Template: UWV HLD - TEMPLATE 1.81.docx |

**DOCUMENT AUTHORISATION**

| Name | Role | Date |
| --- | --- | --- |
| Hans Kreisel | DXC Account Architect (verification) |  |
| Raymond Groenewoud | UWV Lead Architect (verification) |  |
| Rick van Diemen, delegated to Hans Kreisel | DXC Account Delivery Lead (acceptance) |  |

**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 | 30-06-2021 | DXC architecture team | First iteration of the HLD   * 0.1 - Creation ( chapter 1-4 + 5.1 copied from IBM HLD) * 0.2 - Removed irrelevant CMO references * 0.3 – Where needed, relevant FMO information is added |
| SharePoint version | 13-10-2021  26-10-2021  01-12-2021  10-12-2021 | DXC architecture team | Second iteration of the HLD (V0.4 / 0.5)   * 0.4: Update 1 (based on co-creation session and connectivty sheet) * 0.5: review comments processed * 0.7: Added solution (chapter 5, 6 and Appendix) ready for UWV, DXC security and peer review * 0.75: Review comments UWV processed |
| Verification version 0.8 | 15-12-2021 | DXC architecture team | Third iteration of the HLD   * 0.8: Ready for Account review (pending approval exception report) |
| Verification version 0.9 | 21-12-2021 | DXC architecture team | Design Office verification |
| Version 1.0 | 13-01-2022 | DXC architecture team | Positive verified HLD |
| Version 1.1 | 18-08-2022 | DXC architecture team | Post implementation HLD   * Added decisions for usage of Power HA clusters * Added version 4 for NFS * Added UWV FB security control * Customer facing DNS (+ LB config) adjusted * Update Application Management zone according to the latest agreed specification: Domain=Production, Security zone = DXC AM (application management) * Appendix B: added connectivity sheet * Appendix A: added servernames * Updated 5.7, added EtP RAL ID’s and added additional EtP for TLS 1.0 and |
| Version 1.2 | 03-02-2023 | DXC architecture team | Post Aftercare HLD  19-08-2022: COPY-DB1-P and COPY-DB1-A -> vcpu changed from 1 to 2 for better performance (CPU procs raised from 1.0 to 1.4)  30-09-2022: Staging1-AM -> SLA changed from Gold to Bronze (was moved from Generieke Services to SONAR therefore deviation SLA)  30-09-2022: Public-APP1-5-P adjusted from 90 Gb RAM to 92 GB to be in line with the actual deployment  12-10-2022: Updated storage layout in Appendix A for AIX clusters according to the latest template to make it clearer  13-10-2022: SONAR-DB1-P and SONAR-DB2-P, adjusted from 204 Gb RAM to 208 GB to be in line with the actual deployment  19-10-2022: Updated FS1-P, updated storage from 400GB to 1000 GB, additional storage was needed for proper working  26-10-2022: updated Appendix A storage AIX Cluster (oracle), added missing 100 GB for Oracle Binaries and 100 Gb ASM binaries for each node, and added 50 GB shared storage for the script folder which is used to run batches  27-10-2022: Adjusted Appendix A – Software: removed Oracle HTTP server from Sonar DATA (KATO), this software is not installed / useD |
| Version 1.2.1-TC | 06-02-2023 | DXC architecture team | CHG0079043 DXC HLD aanpassen  Direct SFTP connectivity for UWV FB to SONAR staging server:   * 2.2 Context Diagram * 2.2.11 SONAR staging * 2.2.11.1.1 UWV FB * 5.4.1 Staging * 5.10.2 Firewalls * Appendix B: Network Protocol Matrix * 5.1 Architecture decisions * 5.7 Deviations from standards (RAL / EtP) * 6 Potential future improvements (use DSM) |