Technical Debt: Overview

- This section outlines technical debt items from the NTxD to OCI migration project.
- Refers to shortcuts or suboptimal decisions in design and development.
- Issues can lead to future problems or additional work.
- Technical debt spans 4 categories as per box on the right.
- Addressed by:
  - Infrastructure updates.
  - Software and process improvements.
  - Transition to cloud-native solutions.

- TD1: Infrastructure & Region Coverage
  - TD1.1: Only using UK South (not multi-region)
  - TD1.2: DNS using on-prem servers
  - TD1.3: Dependency on on-prem FTP server (USVLFTP02)
  - TD1.4: Dependency on on-prem Internet Connection for NTxD in OCI Access
- TD2: Application & Data Security
  - TD2.1: Missing SSO for OSA APEX applications
  - TD2.2: Missing Request Validation Functions (ORDS) for ODT Online and NTxD
  - TD2.3: Missing HTTP Response Headers for NTxD Application
  - TD2.4: HSCN-facing ODT Online allows unauthenticated access
  - TD2.5: NTX-NPD-CDB-313 (non-prod) contains non-anonymised data
- TD3: Application Platform & Architecture
  - TD3.1: OSA APEX applications in APEX v5.1 compatibility mode
  - TD3.2: APEX platform static files dependency on internet connection
  - TD3.3: Oracle Glassfish is the preferred ORDS host, but currently using Jetty
  - TD3.4: APEX v23.2 support ends 31/05/2025
  - TD3.5: No Web Application Firewall (WAF) for ODT Online Non-Prod and LivingPath Training
- TD4: Software & Technology Choices
  - TD4.1: Glasgow Algorithm Server not using preferred software
  - TD4.2: PyRepGen PDF generation on IaaS VM
  - TD4.3: Email using on-prem servers
  - TD4.4: Email allowing downgrade to unencrypted connections (STARTTLS)

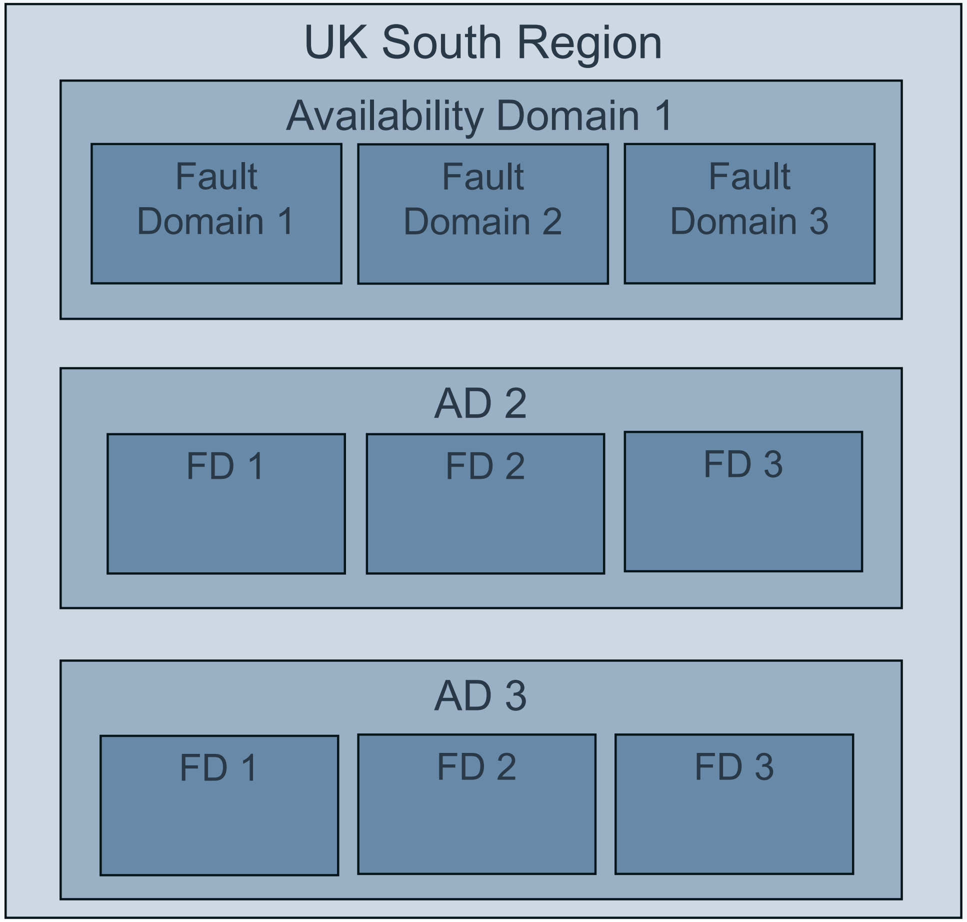
TD1: Infrastructure & Region Coverage

- This set of issues addresses the dependencies on specific geographic regions and on-premises infrastructure.
  - These issues can limit system resilience, scalability, and the ability to quickly recover from failures
- TD1.1: Only using UK South (not multi-region)
  - Single-region deployment, no redundancy.
  - Risk of regional outages.
  - Multi-region deployment would improve availability and disaster recovery options.
- TD1.2: DNS using on-prem servers
  - Single point of failure with on-prem DNS.
  - Cloud-based or distributed DNS could enhance resilience.
- TD1.3: Dependency on on-prem FTP server (USVLFTP02)
  - Outdated system (OS is Solaris)
  - No malware file scanning.
  - Migration to modern, secure FTP solution needed.
- TD1.4: Dependency on on-prem Internet Connection for NTxD in OCI Access
  - Potential bottleneck and a single point of failure.
  - Moving to a direct connection to OCI to reduce dependency on physical infrastructure.

TD1.1: Only using UK South (not multi-region)

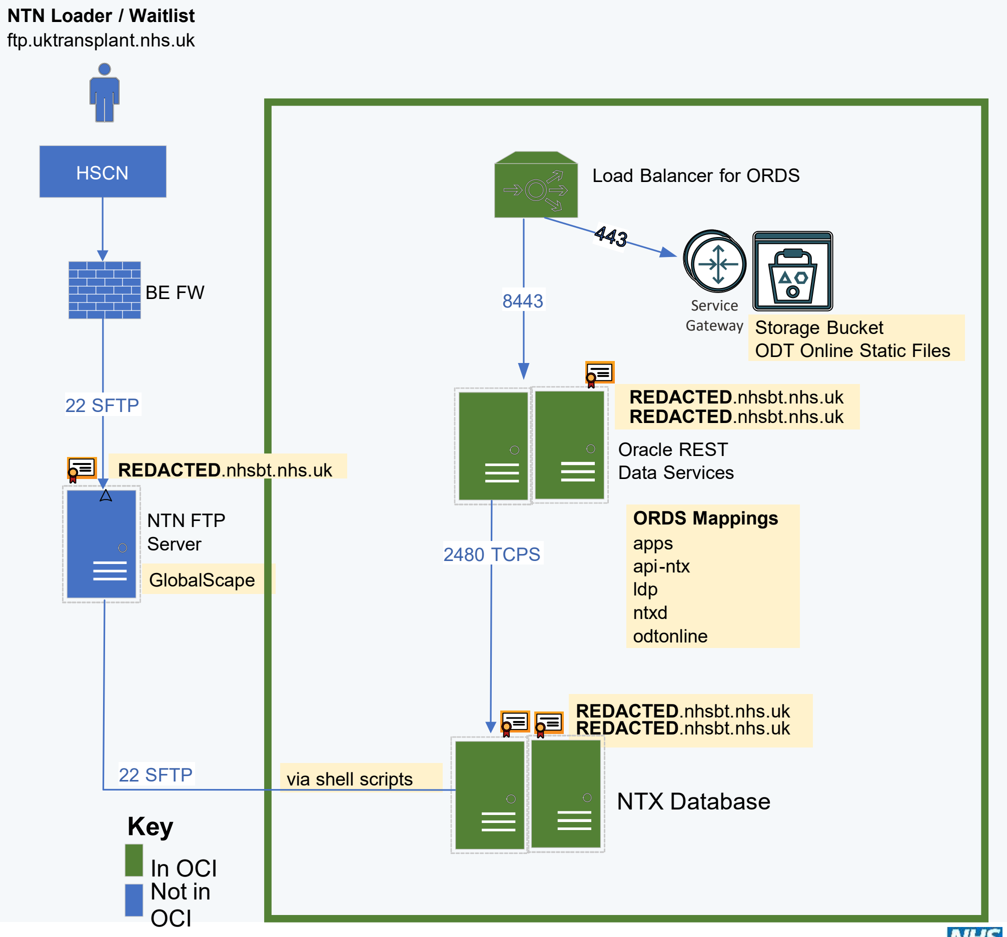
- NTxD is currently deployed only in UK South region of OCI, with no redundancy in UK West or other regions.
- OCI has experienced regional outages in the past which could lead to no availability of NTX and related services.
- The probability of complete regional outage is low – reasonably estimated to be once every 4-5 years.
- A multi-region setup could potentially enhance redundancy, but this is not a guarantee against outages.
  - The most notable OCI outage was multi-region, affecting both UK South and UK West simultaneously
- Adding redundancy in another region (UK West) would incur significant additional costs.
  - Additional Vodafone Cloud Connect and Fast Connect services.

See Appendix for further details about OCI outages



TD1.3: Dependency on on-prem FTP server (USVLFTP02)

- On-prem FTP server, USVLFTP02, is outdated, running on Solaris, and lacks essential security features like malware scanning.
- Being outdated introduces significant security risks, e.g. potential data leak, reputational damage, patient harm, ransomware attacks.
- Absence of malware scanning further exacerbates these risks, e.g. enables the transmission of malicious files.
- Reliance on aging on-prem hardware creates a bottleneck, limiting the scalability and security.
- Additionally, the OS, Solaris, is niche and increasingly difficult to support.
- Migrating to a modern, secure FTP solution hosted on OCI is recommended.
- Use OCI's built-in security features, such as VSS (Vulnerability Scanning) and Cloud Guard, to safeguard data transfers.



NTN Loader / Waitlist
ftp.uktransplant.nhs.uk

HSCN

BE FW

22 SFTP

REDACTED.nhsbt.nhs.uk

NTN FTP Server

GlobalScape

22 SFTP

via shell scripts

Load Balancer for ORDS

443

8443

Service Gateway

Storage Bucket
ODT Online Static Files

REDACTED.nhsbt.nhs.uk
REDACTED.nhsbt.nhs.uk

Oracle REST Data Services

ORDS Mappings
apps
api-ntx
ldp
ntxd
odtonline

2480 TCPS

REDACTED.nhsbt.nhs.uk
REDACTED.nhsbt.nhs.uk

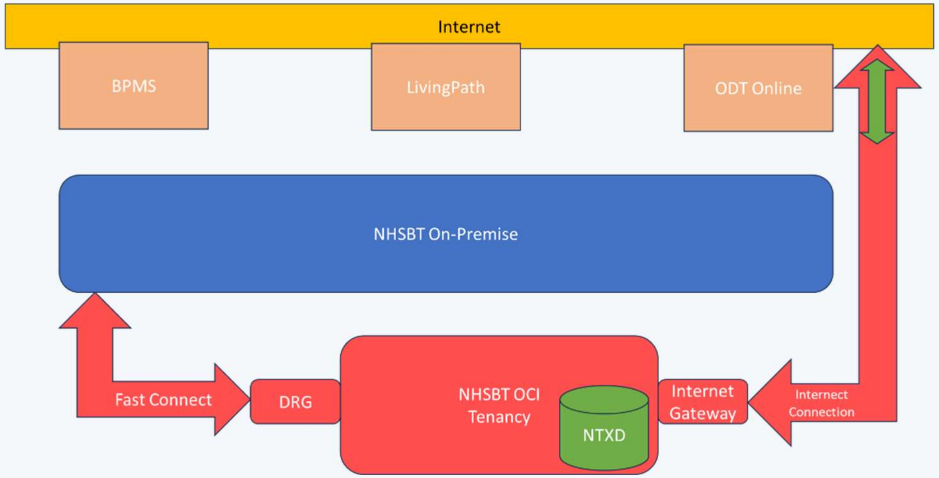
NTX Database

Key
🟩 In OCI
🟦 Not in OCI

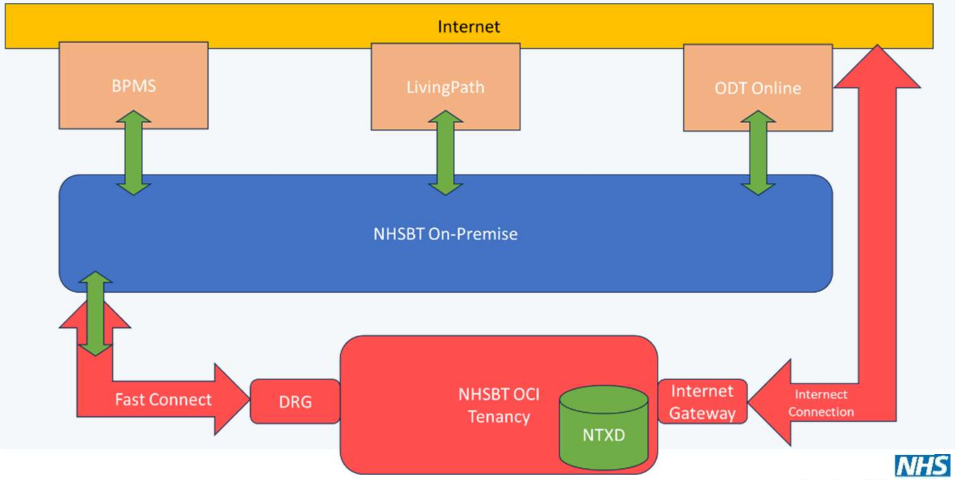
TD1.4: Dependency on on-prem Internet Connection for NTxD Access

- ODT Online & LivingPath have a dependency on on-prem internet connection to access NTxD that is now in OCI.
- Due to time constraints, the project implemented Option B.
- Option B routes internet connections through on-premise infrastructure before reaching Oracle Cloud Infrastructure (OCI) via Fast Connect.
- This decision introduces additional complexity and creates a potential bottleneck.
- It relies on legacy on-prem systems, which could hinder future scalability and resilience.
- The preferred approach, Option A, would have involved a direct internet connection into OCI.
- Option A aligns better with cloud-native architecture principles.

Option A: *Internet Connection into OCI*



Option B: *Internet Connection into on-premise and into OCI via Fast Connect*

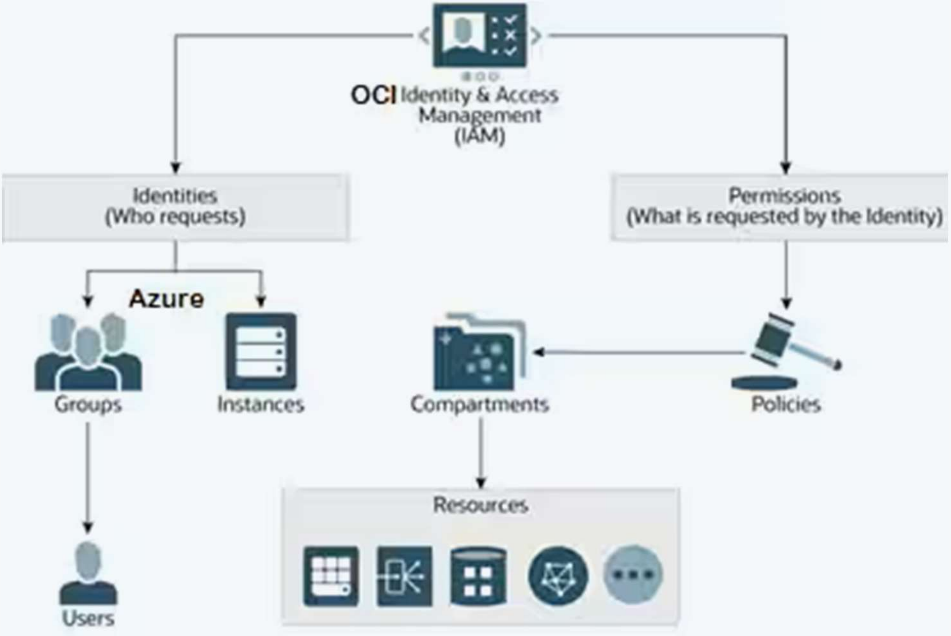


TD2: Application & Data Security

- This set of issues highlights the security concerns related to application access, data protection, and user authentication.
  - Proper security measures are essential to protect sensitive data and ensure that applications are accessed only by authorised users.
- TD2.1: Missing SSO for OSA APEX applications
  - Users manage Oracle application usernames and passwords, increasing security risks.
  - Implement SSO for centralised authentication.
- TD2.2: Missing Request Validation Functions (ORDS) for ODT Online and NTxD
  - Unauthorised access via URLs possible.
  - Implement validation to restrict access to authorised actions.
- TD2.3: Missing HTTP Response Headers for NTxD Application
  - Exposes application to security risks (e.g., XSS).
  - Add headers to mitigate vulnerabilities.
- TD2.4: HSCN-facing ODT Online allows unauthenticated access
  - Security vulnerability, sensitive info at risk.
  - Require authentication before accessing content – migrate to Internet-facing ODT Online
- TD2.5: NTX-NPD-CDB-313 (non-prod) contains non-anonymised data
  - Serious security/privacy risk, data should be anonymised.
  - Use the secure production VNET instead.

TD2.1: Missing SSO for OSA APEX Applications

- Require users to manage multiple login credentials for different applications.
- Absence of SSO increases the security risk: users are more likely to use weak or repetitive passwords across multiple systems.
- Fragmented authentication approach increases the risk of unauthorised access due to poor password management practices.
- Implementing SSO for the OSA APEX applications would centralise user authentication, simplify login processes and reduce the risk of security breaches.
- OCI's Identity and Access Management (IAM) can integrate with Microsoft Azure Active Directory (AAD) for SSO.
- Introducing SSO aligns with strategic best practices for secure authentication and enhances the overall security posture of NHSBT's applications.
- It also simplifies user management, reducing administrative overhead.

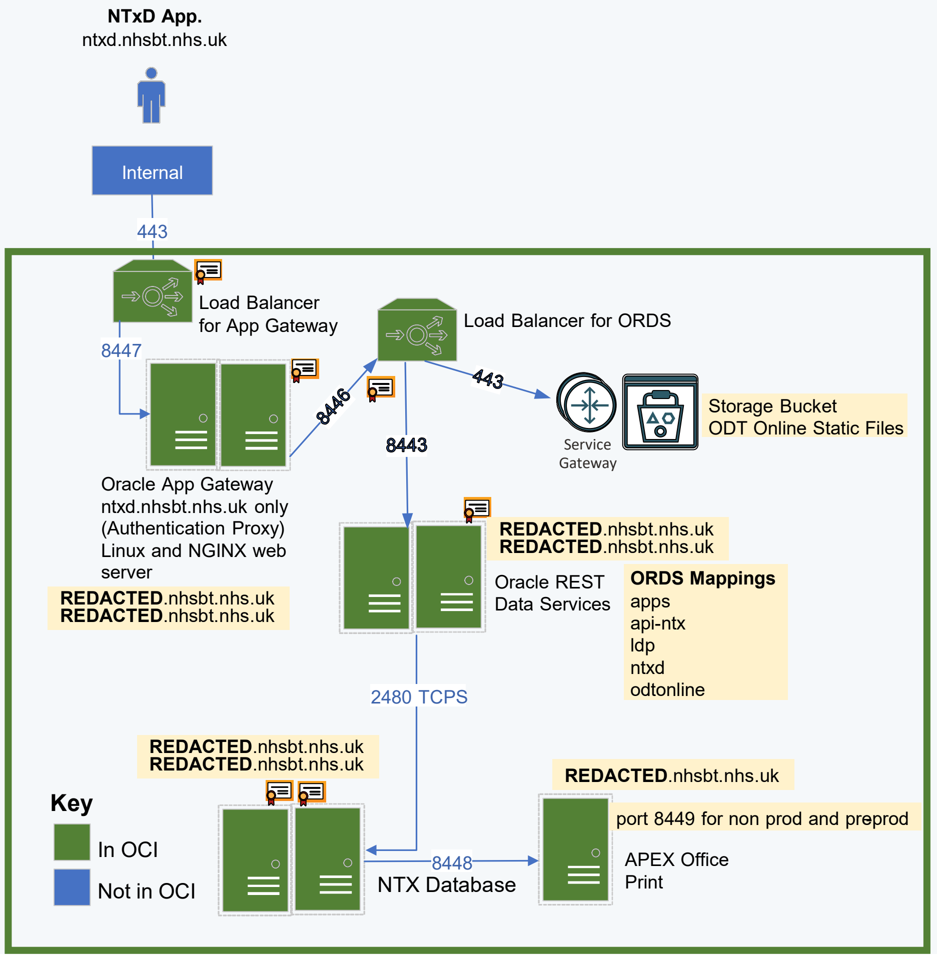

OCI Identity & Access Management (IAM)
Identities (Who requests)
Permissions (What is requested by the Identity)
Azure
Groups
Instances
Compartments
Policies
Users
Resources

TD2.2: Missing Request Validation Functions (ORDS) for ODT Online and NTxD

- The ODT Online and NTxD applications currently using ORDS without basic request validation functions.
- Malicious users could potentially bypass authentication and authorisation by directly manipulating URLs.
- Could lead to unauthorised actions, such as accessing sensitive data, executing unapproved operations, or altering critical information.
- Sensitive organ donor or recipient information could be exposed or altered compromising data integrity and posing privacy and regulatory compliance risks.
- Implement request validation functions within ORDS to ensure that all incoming requests are thoroughly validated before being processed.
- Ensure all parameters and inputs received in the URL or request body are properly validated to prevent SQL injection, cross-site scripting (XSS), and other injection attacks.
- Verify the user making the request is authorised to perform the requested action – including checking credentials, session validity, roles and access rights.

TD2.3: Missing HTTP Response Headers for NTxD Application

- The NTxD Application currently lacks several critical HTTP response headers (e.g. X-Content-Type-Options, X-XSS-Protection, X-Frame-Options, Strict-Transport-Security).
- The OCI Load Balancer can add these headers, but the application would need to be tested with the headers in place before the change is implemented in production.



NTxD App.
ntxd.nhsbt.nhs.uk

Internal

443

Load Balancer
for App Gateway

8447

Oracle App Gateway
ntxd.nhsbt.nhs.uk only
(Authentication Proxy)
Linux and NGINX web
server

REDACTED.nhsbt.nhs.uk
REDACTED.nhsbt.nhs.uk

8446

Load Balancer for ORDS

443

Service
Gateway

Storage Bucket
ODT Online Static Files

8443

REDACTED.nhsbt.nhs.uk
REDACTED.nhsbt.nhs.uk

Oracle REST
Data Services

ORDS Mappings
apps
api-ntx
ldp
ntxd
odtonline

2480 TCPS

REDACTED.nhsbt.nhs.uk
REDACTED.nhsbt.nhs.uk

NTX Database

8448

REDACTED.nhsbt.nhs.uk

port 8449 for non prod and preprod

APEX Office
Print

Key

🟩 In OCI

🟦 Not in OCI

TD3: Application Platform & Architecture

- This group focuses on the platform and architectural decisions that impact the performance, compatibility, and longevity of applications.
  - Keeping platforms up to date and following best practices is crucial for maintaining system stability and support.
- TD3.1: OSA APEX applications in APEX v5.1 compatibility mode
  - Limits functionality, potential security risks.
  - Upgrade to latest version for improved performance.
- TD3.2: APEX platform static files dependency on internet connection
  - Requires internet access, reliance on CDN (static.oracle.com).
  - Host files internally using Oracle REST Data Services (ORDS) for better reliability.
- TD3.3: Oracle Glassfish is the preferred ORDS host, but currently using Jetty
  - Jetty is a lightweight and standalone server for running ORDS thus limiting performance and compatibility.
  - Switch to Glassfish for best practices.
- TD3.4: APEX v23.2 support ends 31/05/2025
  - End of support means no further updates.
  - Plan upgrade to ensure continued support and security.
- TD3.5: No Web Application Firewall (WAF) for ODT Online Non-Prod and LivingPath Training
  - Vulnerable to web attacks like SQL injection, XSS.
  - Implement WAF for real-time protection.

TD3.1: OSA APEX Applications in APEX v5.1 Compatibility Mode

- 13 APEX applications currently running in APEX v5.1 compatibility mode on the OSA (OTDT Support Applications) server.
- Latest version of APEX is 24.1.
- This setup limits access to new features.
- Phase 1 (Minimal Upgrade): Upgrade all applications to APEX v23 in compatibility mode to mitigate immediate risks.
- Phase 2 (Full Upgrade): Perform a full upgrade to remove deprecated components, enhance security, and leverage APEX v23 features.
- Upgrading improves security by applying the latest fixes and updates.
- Enhanced performance and functionality will result from utilising new APEX v23 features.
- Standardising on the latest APEX version simplifies maintenance and ensures a consistent user experience.

OTDT Supporting Applications

- Organ Retrieval Database
- Antibody Incompatible Tx Form
- Split Liver Form
- Supplementary Pancreas Islet Registration
- Pancreas Database Application
- Stored Vessel
- Organ Damage HOT B
- EnTrack (Database Environment Tracker)
- Blue Light Data Uploader
- Password Reset Application
- TAS Billing
- Database URL Tracking

TD3.3: Oracle Glassfish is the preferred ORDS host, but currently using Jetty

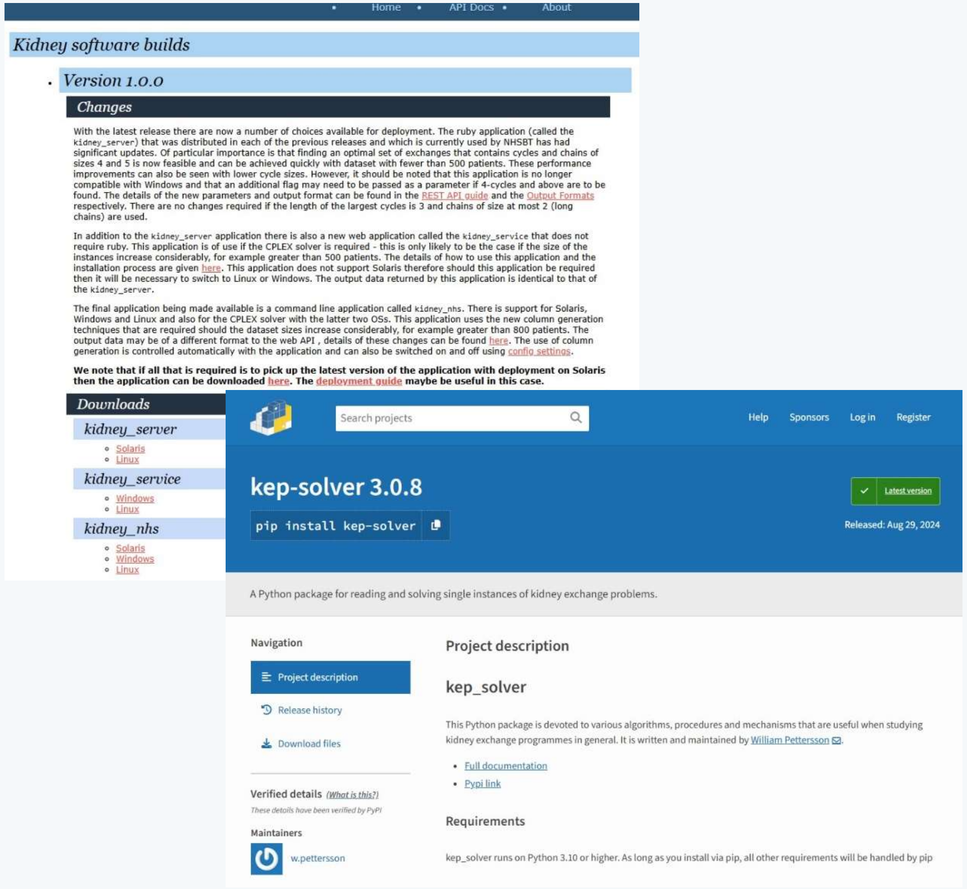
- Oracle Glassfish is the recommended Java EE Application Server for hosting Oracle REST Data Services (ORDS).
- However, the current implementation uses the open-source Jetty from Eclipse, a lightweight, embeddable web server and servlet container.
- Oracle supports Oracle REST Data Services (ORDS) running in standalone mode (i.e. no app server required) using the built-in Jetty web server.
- Using Jetty instead of Glassfish limits the performance and compatibility of the ORDS implementation.
- Jetty does not support all enterprise-grade features required for optimal ORDS performance, leading to potential issues with scalability and maintenance.
- Jetty lacks advanced clustering and load balancing features, which are essential for distributing workloads efficiently.
- Glassfish is a full-featured application server that provides better support for ORDS, including enhanced performance, scalability, and integration capabilities.
- Jetty has limited built-in tools for monitoring and managing performance, increasing maintenance complexity.
- Glassfish provides more granular security controls, therefore better suited for protecting enterprise applications like ORDS.
- Migrating from Jetty to Oracle Glassfish is recommended.
- Switching to Glassfish aligns with Oracle’s best practices, future-proofs the infrastructure and ensures that the ORDS environment is fully supported and optimised for NHSBT’s needs.

TD4: Software & Technology Choices

- This group discusses specific software and technology decisions that impact the system's efficiency, supportability, and alignment with best practices.
  - Optimising these choices can reduce operational burdens and improve system performance. Keeping platforms up to date and following best practices is crucial for maintaining system stability and support.
- TD4.1: Glasgow Algorithm Server not using preferred software
  - Support and maintenance challenges as Glasgow Uni currently use kidney_server (old Ruby application).
  - Align with preferred software for better support – would rather use kep_solver (new Python application).
- TD4.2: PyRepGen PDF generation on IaaS VM
  - Unnecessary complexity and overhead.
  - Move to serverless PaaS for simplicity and scalability.
- TD4.3: Email using on-prem servers
  - Limits scalability, requires more maintenance.
  - Cloud-based email solution could improve reliability.
- TD4.4: Email allowing downgrade to unencrypted connections (STARTTLS)
  - Significant security risk, vulnerable to attacks.
  - Enforce encryption to prevent downgrade attacks.

TD4.1: Glasgow Algorithm Server not using preferred software

- The Glasgow Algorithm Server uses kidney_server, a Ruby-based application developed by the University of Glasgow for optimising donor-recipient matches in the UKLKSS.
- Maintaining the Ruby-based kidney_server is increasingly challenging due to Glasgow University's preference for other technologies, like Python, and the potential decline in Ruby expertise.
- Glasgow University prefers transitioning to kep_solver, a Python-based application, which is more recent and better maintained.
- Continuing with the Ruby-based solution could lead to security and maintenance risks.
- By moving away from the Ruby-based kidney_server, NHSBT can reduce the technical debt associated with using a technology that may not have widespread support.



Kidney software builds

- Version 1.0.0

Changes

With the latest release there are now a number of choices available for deployment. The ruby application (called the kidney_server) that was distributed in each of the previous releases and which is currently used by NHSBT has had significant updates. Of particular importance is that finding an optimal set of exchanges that contains cycles and chains of sizes 4 and 5 is now feasible and can be achieved quickly with dataset with fewer than 500 patients. These performance improvements can also be seen with lower cycle sizes. However, it should be noted that this application is no longer compatible with Windows and that an additional flag may need to be passed as a parameter if 4-cycles and above are to be found. The details of the new parameters and output format can be found in the REST API guide and the Output Formats respectively. There are no changes required if the length of the largest cycles is 3 and chains of size at most 2 (long chains) are used.

In addition to the kidney_server application there is also a new web application called the kidney_service that does not require ruby. This application is of use if the CPLEX solver is required - this is only likely to be the case if the size of the instances increase considerably, for example greater than 500 patients. The details of how to use this application and the installation process are given here. This application does not support Solaris therefore should this application be required then it will be necessary to switch to Linux or Windows. The output data returned by this application is identical to that of the kidney_server.

The final application being made available is a command line application called kidney_nhs. There is support for Solaris, Windows and Linux and also for the CPLEX solver with the latter two OSs. This application uses the new column generation techniques that are required should the dataset sizes increase considerably, for example greater than 800 patients. The output data may be of a different format to the web API , details of these changes can be found here. The use of column generation is controlled automatically with the application and can also be switched on and off using config settings.

We note that if all that is required is to pick up the latest version of the application with deployment on Solaris then the application can be downloaded here. The deployment guide maybe be useful in this case.

Downloads

kidney_server
- Solaris
- Linux

kidney_service
- Windows
- Linux

kidney_nhs
- Solaris
- Windows
- Linux

kep-solver 3.0.8

```
pip install kep-solver
```

Released: Aug 29, 2024

A Python package for reading and solving single instances of kidney exchange problems.

Verified details (What is this?)

These details have been verified by PyPI

Maintainers

w.pettersson

Project description

kep_solver

This Python package is devoted to various algorithms, procedures and mechanisms that are useful when studying kidney exchange programmes in general. It is written and maintained by William Pettersson.

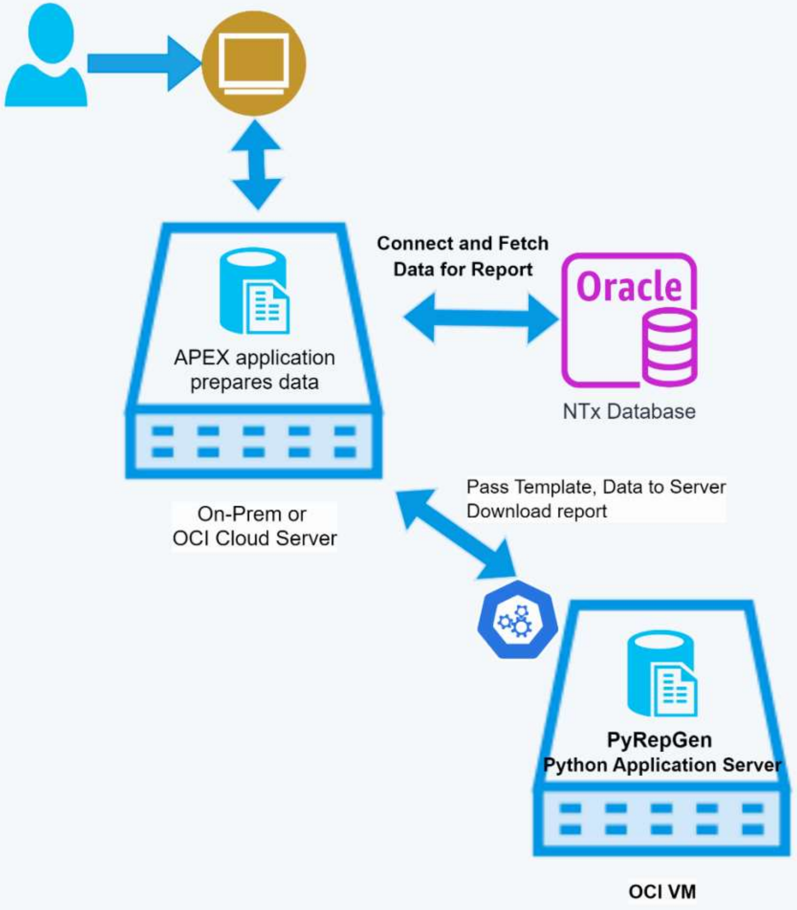
- Full documentation
- Pypi link

Requirements

kep_solver runs on Python 3.10 or higher. As long as you install via pip, all other requirements will be handled by pip

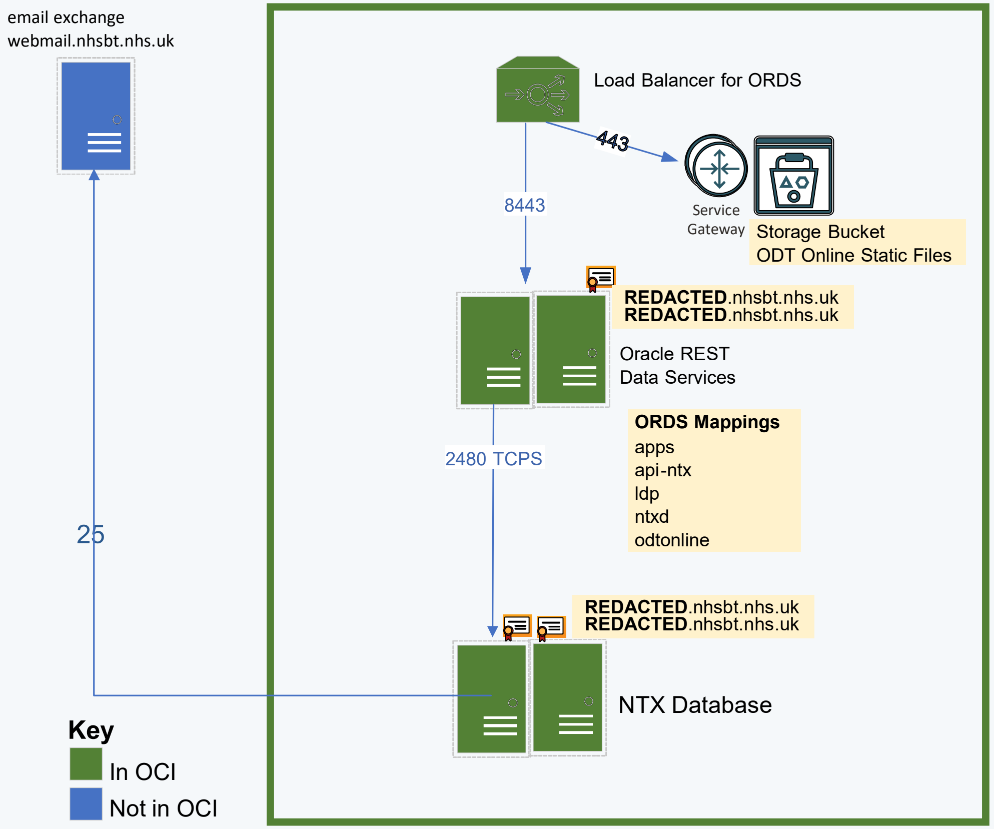
TD4.2: PyRepGen PDF Generation on IaaS VM

- PyRepGen is hosted on an IaaS VM within OCI, requiring management of the underlying infrastructure.
- The current setup involves maintaining the OS, managing resources, and handling scalability manually, adding operational overhead.
- Scaling requires provisioning more VMs or upgrading existing ones, leading to potential downtime and inefficiencies.
- Move PyRepGen to a serverless PaaS solution to simplify architecture and reduce maintenance.
- PaaS abstracts infrastructure management, focusing on application performance and serverless platforms automatically scale based on demand.
- Transitioning to PaaS aligns with NHSBT's strategy of modernising infrastructure, enhancing scalability, and reducing operational overhead.



TD4.3: Email Using On-Prem Servers

- NHSBT's email services are currently hosted on on-premise servers.
- The reliance on on-prem email servers creates challenges in terms of scalability, reliability, and security.
- Added complexity and operational overhead as on-prem email servers require ongoing maintenance, including hardware upgrades, software patches, and security management.
- Transitioning to a cloud-based email solution, such as Oracle Cloud Email or another cloud provider, would enhance scalability, reliability, and security.
- Cloud-based email services offer built-in redundancy, automatic updates, and advanced security features.
- Moving email services to the cloud aligns with NHSBT's broader strategy of reducing on-premise dependencies and leveraging cloud technologies to improve operational efficiency and security.


email exchange
webmail.nhsbt.nhs.uk
Load Balancer for ORDS
443
8443
Service Gateway
Storage Bucket
ODT Online Static Files
REDACTED.nhsbt.nhs.uk
REDACTED.nhsbt.nhs.uk
Oracle REST Data Services
ORDS Mappings
apps
api-ntx
ldp
ntxd
odtonline
2480 TCPS
25
REDACTED.nhsbt.nhs.uk
REDACTED.nhsbt.nhs.uk
NTX Database
Key
🟩 In OCI
🟦 Not in OCI