21 SEPTEMBER 2021

World Organisation for Animal Health
Founded as OIE

IT ARCHITECTURE STANDARDS

Version

Version	Release date	Tasks	In charge of
v.0	2021/07/27	Document Creation	D.A
V0.1	2021/08/18	Update	D.A
V0.2	2021/09/09	Update	D.A
V0.3	2021/09/10	Update	D.A
V0.4	2021/09/11	Update (web browser)	D.A

These documents describe the current IT architecture standards and features used by WOAH to ensure cost control, security matters and to provide the right solution blocks regarding business needs and architecture block.

Aim of this document is also to describe roles of WOAH future tenderers and WOAH IT service provider along all projects.

Finally, it covers a part of IT internal control matters and GPDR requirements.

Summary

1   Roles and responsibilities

WOAH has already outsourced the management of their IT infrastructure building, IT security and IT platform building and maintenance to an identified IT service provider. This IT service provider will identify an IT infrastructure project manager in charge of all those tasks.

The future IT tenderer will be in charge of:

- Development of all features required by the WOAH
- Co-Writing of technical document architecture (segregation of duties must be cleary defined during the kick-off as it depends on the project type)
- Application maintenance and functional support to key users
- Liaise and participate to workshop with IT infrastructure project manager

The future IT tenderer will have to identify a project manager as a Single Point of Contact for all requests and meetings in close contact with the IT infrastructure project manager.

The IT service provider will be in charge of:

- Security and Network management. They are WOAH's Security operations center,
- Building the azure IT infrastructure.
- Building the IT platform (new website base etc.) if hosting is managed by WOAH based on information provided by the future IT tenderer
- Supporting the IT tenderer during development phases for K8s subjects and all infrastructures questions.

Once the IT platform is built, full access will be provided to the future IT tenderer

2   Infrastructure standards

2.1   Description of environment

For all projects, WOAH DTIS must provide few environments to tenderer:

- Development environment if required but not mandatory.,
- User testing environment is mandatory,
- Production environment.is mandatory also.
- Pre-staging environment could be added also if required but not mandatory.

All this environment must be created In Microsoft Azure Cloud and managed by WOAH DTIS team or a by an IT service provider.

In case WOAH decide that infrastructure is managed by a third-party and not hosted within WOAH Azure infrastructure and not handled by WOAH DTIS team, DTIS team will review the IT architecture proposal to ensure that those best practices are followed.

2.2   Use of Kubernetes as a standard

WOAH DTIS team has chosen to use Container technology and especially Kubernetes (Azure devops features) as a standard solution for all applications hosted and developed for WOAH. The aim is to manage scale economy.

For example, it is used for corporate website (www.WOAH.int) and some key applications in development already.

The building of application platform is managed by an external IT provider and WOAH IT teams :

- Building of pipeline,
- Setting-up of configuration files (yml etc.)
- Deploying Kubernetes cluster
    - One Cluster for production
    - One for cluster for others environment
- Etc.

The future tenderer, unless, it is difficult, will have to use those platforms and store all codes done for WOAH IT projects within this dedicated repository.

2.3 IT Platform for vendor software

If the chosen solution can't fit with use of Kubernetes, especially for vendor software, WOAH DTIS team, with IT service provider help, will provide required environments and access to the tenderer or software editor.

2.4 Application monitoring

Application monitoring is managed through Datadog. Level of services and features to be deployed will be discussed with WOAH business teams, WOAH project managers and IT developers (IT tenderer and IT service provider) regarding application criticality.

Datadog is a cloud monitoring tools that includes those features:

- Monitoring of cloud environment
- Measure of application performance
- Monitoring of Kubernetes containers
- Monitoring of datastreams between applications
- API supervision

Datadog is monitored by IT service provider and not tenderer.

3 WOAH Security Standards

All security subjects especially IT security or network will be managed by IT service provider and WOAH DTIS Team. Those best practices and IT security features help to ensure **GPDR compliance**.

3.1 Authentication to application managed through Azure Active Directory

Access to application must be managed with :

- Unique login
- Password

For security matters, all access – and not rights- to access to WOAH key applications should be managed through Azure Active directory and the use of MS API Graph.

NB : Microsoft Azure password complexity criteria respects all security criteria (minimal length, Complexity, Password history)
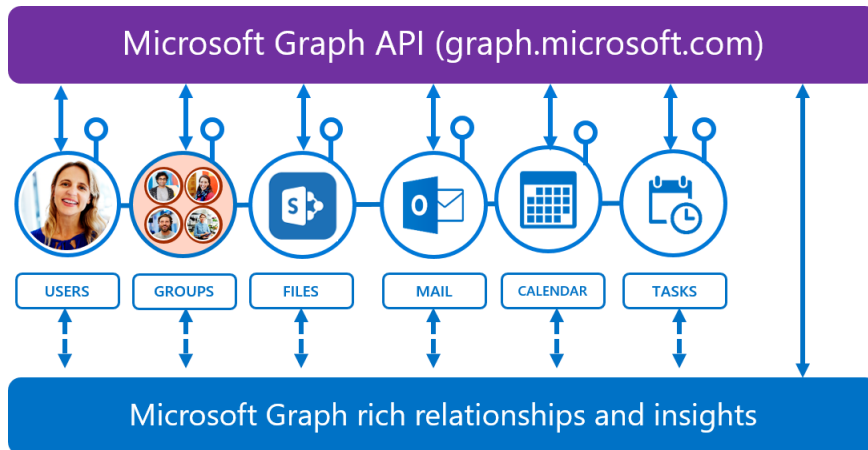
3.2   Security breach identification

3.2.1   Planification of a Code audit for security matters

To ensure that coding best practices are followed by tenderer, WOAH will schedule an IT audit code during testing phases to identify any security breaches such as :

- SQL injection,
- Rogue code,
- Login and password written directly in the code,
- Etc.

In case of a critical security breach is identified, the IT tenderer will be in charge to correct/apply a patch to solve the issue.

3.2.2   Organisation of pentest session for security matters

WOAH will also organize pen tests to identify security breaches twice :

- Before release,
- After release

In case of a critical security breach is identified, the IT tenderer will be in charge to correct/apply a patch to solve the issue.

3.3   Global security infrastructure

3.3.1   Use of a Content Delivery Network

To protect all WOAH websites and web applications from DDOS attack, WOAH has deployed a Content delivery network which is Cloudflare. Cloudflare is used to optimized access to web pages and to protect WOAH web applications of DDOS Attacks.

3.3.2   Use of SIEM - QRADAR

WOAH security information is managed through a SIEM – IBM QRADAR to detect, manage and prioritize all security threats. SIEM is also under the IT service provider monitoring.

4   Web standards

4.1   WOAH Web factory

For the development of all corporate security website and to standardize solution, WOAH has built a web factory on a Kubernetes IT platform. It is based on :

- Wordpress CMS,
- MySQL/MariaDB database,
- Development in PHP > 7.3x,
- Nginx as a reverse proxy,
- Redis as a database cache to optimize access to data etc.,
- Algolia for data indexation
- Matomo analytics for web statistics following.

This application base must be reused by all IT tenderers for any website development. If the tenderer wishes to use others IT components, it must be validated by WOAH It project manager and Architect especially for security matters.

4.2   Web features analytics

WOAH recommends the use of:

- Google analytics
- Matomo (SAAS version)

Those two applets, used within WOAH could be used to understand customer preferences, measure audiences and create a better experience for WOAH website visitors.

They are also **GPDR compliant** and includes data privacy features such as anonymization

4.3   MapBox for location features

To integrate easily maps or any location data features within WOAH websites and applications, WOAH recommends the use of MapBox to power maps and location services.

4.4 Translation features

WOAH is an international organization where some key information must be shared with international stakeholders and be translated in:

- French
- English
- Spanish

To easily translate any contents, WOAH recommends the use of DeepL translator that could files and text at the same time in several languages from several sources.

Example : Deepl is used to translate WOAH website contents

4.5 Internet browser compatibility

All websites and web application must be compatible with current major internet browsers and future versions:

- Opera
- Microsoft Edge
- Safari
- Mozilla Firefox
- Google Chrome

As some users access to them through Microsoft windows computers, personal mobile or mac OS computers.

5 Features and application bricks to be used

WOAH recommends the use of those Microsoft Azure features.

5.1 Use of Microsoft office 365 features for email sending

All future applications using email sending features must go through the Azure SMTP relay of WOAH. This relay ensures the good deliverability of the emails (SPF/DKIM).

5.2 Data and AI features and services

Use of Power BI for data and all reports creation

WOAH staff recommends the use of Power BI for data aggregation from multiple resources, data report creation and analysis.

Use of on premisce data gateway

WOAH DTIS teams has deployed an on-premises data gateway on a azure dedicated Virtual. It allows multiple users to connect to multiple on-premises data sources especially for reports data refresh.
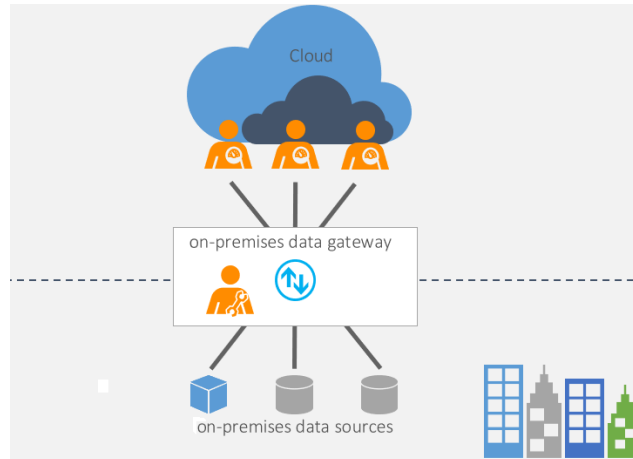

Figure O : On premisce data gateway

Data sets creation and update

To secure data access and to manage authorization, only the power BI hosted on WOAH data gateway virtual machine is able to connect to on-premises directly : Access to data-sources are managed **through a load balancer** and granted exceptionally only to specific and clearly identified users or applications.

Authorized key users will be granted with an access to this "Data virtual machine". Then, from there, they could access to :

- A specific Power BI desktop,
- Create data sets,
- Publish them on the dedicated Power BI services report,
- Create data source connexion and schedule data refreshment through data gateway settings within power BI using the admin account.

Features for data analysis and AI

WOAH has already setup several Microsoft tools for data engineering and analysis. All those features or Saas are Microsoft azure native tools or application and used as Proof of concept to assess their efficiency and to see if it fits WOAH expectation :

- Microsoft Azure data catalog that will be used for data digging and data governance
- Text analytics which is a text-mining AI service that uncovers insights such as sentiment analysis, entities, relations and key phrases in unstructured text
- Azure analysis services which can host semantic data models. Then our organization could connect those data models to excel, power BI and other services to create reports and perform ad-hoc data analysis.

5.3   Storage features

5.3.1   Use of Microsoft azure sharepoint

WOAH strongly recommends the use of Microsoft 365 sharepoint as an ECM - Entreprise Content Management to store all documents (attached files etc.). Microsoft Sharepoint is especially recommended if key-users need to access attached files outside from the application.

5.3.2   Use of blob storage for data

Azure blob storage is a Microsoft features already used by WOAH and recommended for

- Storing data for analysis by an on-premises or Azure-hosted service
- Serving images or documents directly to a browser
- Storing files for distributed access
- Streaming video and audio
- Writing to log files
- Storing data for backup and restore, disaster recovery and archiving

Already used within some existing WOAH application, it could be used especially for data matters such as a data lake creation and could be relevant.

5.3.3   Use of blob storage for static website

Blob storage could also be used to host static websites (HTML, CSS, and JavaScript files) within WOAH Azure infrastructure.
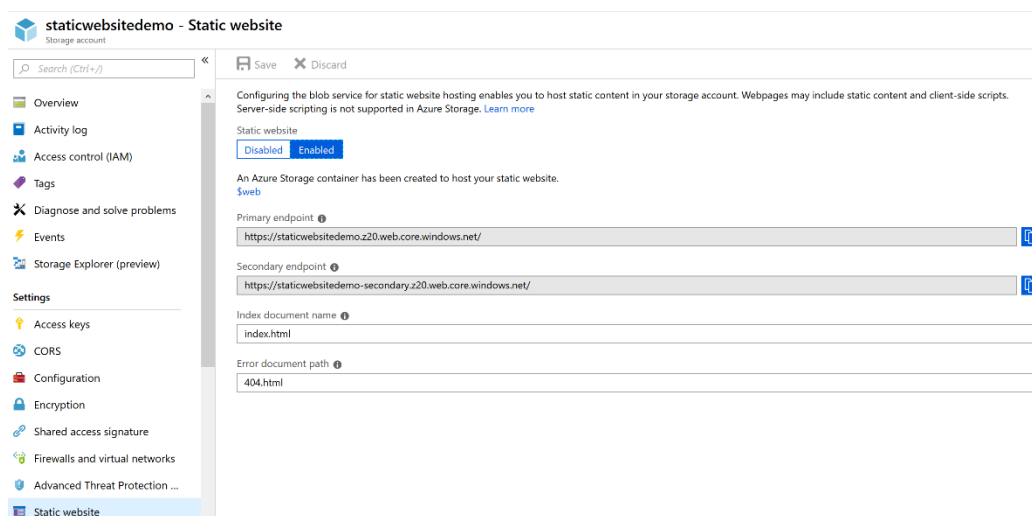

Figure 1 : blob storage static website

However, it can't be used for hosting data dynamic website with Java, Node runtime or ASP.