Request for proposal

Infrastructure as a Service

Table of Contents

1. Introduction

1.1. Who is DNS Belgium?

DNS Belgium is a nonprofit organization that manages and operates 3 top level domains within the public DNS infrastructure. This includes the registry platforms and the authoritative DNS service. The security and reliability of these services is of the highest importance to us. As a TLD-operator and provider of DNS-services DNS Belgium is categorized as an "Essential Entity" under the NIS 2 directive and a Critical Entity under the Critical Entities Resilience (CER)Directive.

DNS Belgium is also very conscientious about the sustainability of its service, its suppliers and all partners involved. It is an active promoter of corporate social responsibility. Our sustainability initiatives focus on the environment, social welfare and good governance.

1.2. Background

Our current technical environment is hosted mainly on Amazon Web Services and consists of a mixture of **Red Hat Enterprise Linux 8** virtual machines and **Kubernetes** clusters for application compute needs. We use several basic and more advanced services from AWS, such as:

- VPC-networking, security groups, NAT-gateway, VPN-connectivity, …
- EC2 virtual machines with custom images
- EKS Kubernetes clusters, and ECR private container registry
- Application (layer 7) and Network (layer 4) load balancers
- RDS relational databases (Oracle, PostgreSQL, MySQL, MariaDB)
- Opensearch (for logs)
- S3 (backup/archive storage, data-lake, …)
- SES for transactional email
- EBS storage
- …

All of these cloud-components are created and configured using **Terraform** infrastructure as code.

We have 5 stages for the registry platforms: development, automated acceptance, user acceptance, external testing and production. Each of these is fully separated from the other stages, with its own separate networks, virtual machines, Kubernetes cluster, databases, load balancers, …

Every stage is fully deployed within a single AWS-region, across multiple availability-zones. In case of disaster, we will move the production stage to another AWS-region. To ensure our infrastructure automation can handle multiple regions, at least one stage is deployed permanently to a different region than the production stage. To minimize data loss in case of disaster, databases and persistent filesystems are replicated near real-time to the designated disaster recovery region.

Next to the registry platforms there are also separate development and production stages for our infrastructure- and development-tooling and for applications that are not part of the registry platforms.

To decrease the potential impact of global political changes and reduce vendor lock-in DNS Belgium wants to move its footprint away from AWS into a provider that is fully owned and operated inside the EU. Initially, only the registry platforms are in scope. Other services and internal tooling may be migrated later.

1.3. Scope of Work

The purpose of this document is to solicit proposals from qualified service providers for the provisioning of **Infrastructure-as-a-Service (IaaS)** to support our organization's compute, storage, and networking needs. The selected provider will deliver a robust, scalable, and secure infrastructure capable of supporting modern DevOps workflows and containerized workloads.

The provider must demonstrate the ability to deliver services in compliance with relevant security and sustainability standards and provide clear documentation and support for onboarding, offboarding and ongoing operations.

Core Requirements:

- Provisioning of virtual machines that **do not reside on hardware shared with other customers**, ensuring dedicated compute resources for enhanced performance, isolation, and compliance.
- Separate virtual networks for each stage, with configurable policies for allowing traffic within and between virtual networks.
- Support for automated infrastructure deployment via Infrastructure-as-Code (IaC) tools, preferably Terraform.
- Role based access control according to the least privilege principle for users and services on the platform.
- Compatibility with container orchestration platforms, particularly Kubernetes.
- High availability, and disaster recovery capabilities across at least 2 geographically distributed datacenters.
- Possibility to integrate with our existing CI/CD pipelines and monitoring systems.

Optional Capabilities:

While we have the capability to manage our needs with basic infrastructure as-a-service, the availability of additional managed services will reduce the migration and long-term maintenance efforts for us. Providers can optionally offer one or more of the following services.

- Provisioning of virtual machines on **shared hardware** for workloads that require **temporary or burst capacity**, such as testing environments or short-lived batch jobs.
- Managed **SaaS or IaaS offerings** for:
    - Relational databases (PostgreSQL and MySQL or its variants). Oracle Database however is not in scope for this.
    - Centralized logging and metrics collection (e.g., ELK stack, Prometheus with Grafana).
    - Kubernetes control plane management
    - Private container registry
    - Load balancers
    - S3-compatible storage
    - Sending transactional email

2. Instructions to Bidders

2.1. Submission Guidelines

- Vendors must announce their intention to participate before **January 20th EOD**. This can be done by sending the contact details of the primary contact for the process to technology-info@dnsbelgium.be.
- **Final submission deadline: January 30th 2026**
- All provided files must be numbered and clearly named. They must be archived together in a zip or tar.gz and uploaded to a unique upload link that will be provided to the primary contact of each of the participating parties.
- To comlete the submission you must send an email which includes the name of the archive that was uploaded and a list of all files it contains. This email must be sent to technology-info@dnsbelgium.be.

2.2. Questions & Clarifications

- Questions can be asked via email to technology-info@dnsbelgium.be.
- The last day questions can be asked is **January 23rd 2026**
- We will try to respond as quickly as possible.
- The questions received with their responses will be sent to all participating parties.

2.3. Evaluation Criteria

To ensure a fair and transparent selection process, proposals will be scored against the following criteria:

- Technical fit
- Security
- Corporate Social Responsibility & environmental sustainability
- Vendor experience & financial stability
- Applicable contractual terms and conditions (notice period, liability, etc.)
- Service level agreement.
- Indicative pricing.

2.4. Evaluation Process

This RFP is not intended to result in a best-and-final offer at this stage. The purpose of this process is **to identify a shortlist of qualified vendors** based on technical fit, compliance, sustainability, and pricing models.

Vendors shortlisted through this RFP process will be invited to present their proposed solution in detail. Following these presentations, DNS Belgium will finalize the ranking of candidates. The highest-ranked vendor will then be invited to enter into comprehensive negotiations, during which all contractual terms, pricing structures, and service level agreements will be defined and agreed upon.

Please note:

- Initial proposals should provide indicative pricing and technical details, not binding final offers.
- DNS Belgium reserves the right to request clarifications or additional information before creating the shortlist.

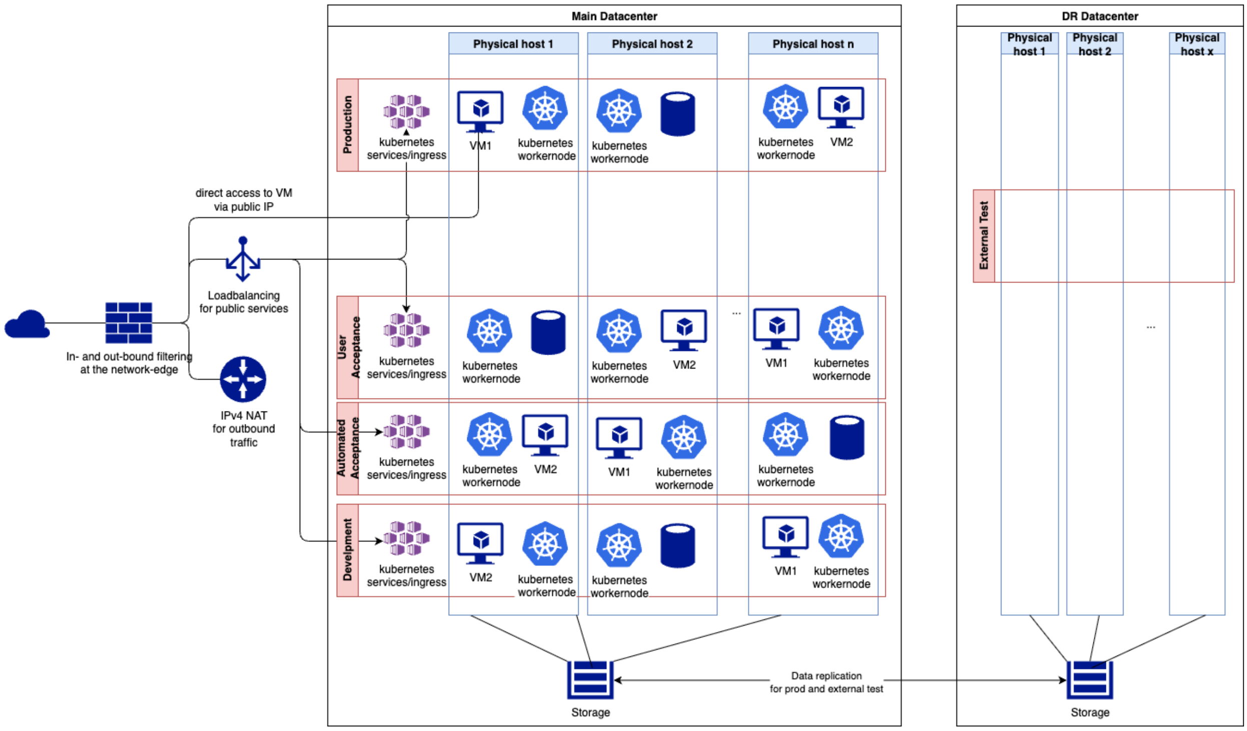
2.5. Timeline summary

1. This document was intitially published on December 3rd 2025.
2. Interested vendors must notify DNS Belgium of the intention to participate by January 20th 2026.
3. The last day vendors can send questions to DNS Belgium is January 23rd 2026.
4. All submissions must be completed before Janurary 30th 2026.
5. DNS Belgium will review the submissions and create a shortlist. We can ask vendors for additional information at this stage.
6. DNS Belgium will provide feedback to participating vendors by March 16th 2026 at the latest.
7. Vendors on the shortlist will get the opportunity to present their solution, after which DNS Belgium will make its final ranking.
8. Start of technical finetuning and negiotiations with our preferred partner.

3. Technical Requirements

3.1. Architecture & Deployment

Reference diagram



Schema 1. *This diagram shows the intended setup at a high level. Every stage of the platform consists of virtual machines, a Kubernetes control plane and worker nodes, and several databases. Most publicly available services are Kubernetes Service or Ingress resources. A few virtual machines are assigned public IPs directly. The DR datacenter permanently runs the External Test stage to ensure its availability. Virtual machines for this stage were left out to make the diagram more compact.*

Requirements

- The proposed solution should provide a method for provisioning virtual machines with a custom Linux based operating system. It should also have the ability to provide the initial configuration for virtual machines when they start for the first time. For example, by providing the virtual machines with cloud-init userdata.
- Virtual machines must be provisioned **on dedicated physical hosts**, equipped with **recent-generation 64-bit x86 processors** from **Intel or AMD.**
- The platform must **support Kubernetes-based container orchestration,** either self-managed or via a managed control plane.
- The virtualization platform should be **well supported** and widely adopted in infrastructure-as-code solutions, preferably **terraform**.
- The **storage** included in the proposal must be compatible to provision persistent volumes for Kubernetes with a CSI-driver to support PersistentVolumeClaims. The ability to provide persistent volumes that allow simultaneous access by multiple containers is of added value.

- The storage solution may be centralized, converged or a mixture of both as long as the requirements are met.
- The solution should provide the capability to **backup** the virtual machines and Kubernetes volumes without incurring downtime. It should be possible to restore these backups to new volumes or virtual machines.
- Each stage should have its own private network, with multiple subnets. The network should support both IPv4 and IPv6 simultaneously.
- It should be possible to configure in- and outbound rules for the network traffic of every virtual machine.
- It must be possible to assign a fixed public IPv4 address to a virtual machine. This can be achieved using one-to-one NAT at the network edge or using a secondary interface attached to the virtual machine.
- All physical hosts and storage part of the offered solution must reside within datacenters in the EU.
- The DR data center should have enough capacity to run the “Production” and “External Test” stages simultaneously.
- It should be possible to set up near real-time data-replication between the Main and DR datacenter for databases and storage-volumes.
- The current amount of CPU and memory in use can be found in Appendix 10.1
- The services in the initial scope do not require powerfull GPUs.

3.2. Scalability, Reachability & Performance

- The registry platforms are quite stable with regard to resource consumption, therefore we have no immediate need for automatic scaling of the available resources. When resource requirements grow, capacity expansions should be provisioned within **5 business days** of request, unless otherwise agreed.
- The solution should provide either external, publicly reachable load balancers, or it should be possible to expose the service and ingress objects in Kubernetes to the public internet.
    - We require layer 7 HTTP-load balancing that supports host & path-based rules for routing to different backends, with optional configuration of fixed responses such as redirects or 404 responses directly from the load balancer.
    - Layer 4 load balancing for non-HTTP TCP or UDP based services.
    - Load balancers should support backend health-checks and they should integrate with Kubernetes Ingress and Service objects.

- The platform should provide sub-millisecond round-trip-times between virtual machines in the same virtual network.

3.3. Service Management

- The offered solution should have both a user interface that can be used by humans and an API for use by our terraform based infrastructure-as-code.
- It should be possible to perform all infrastructure configuration (network setup, traffic policies, creation of virtual machines, load balancer config, …) by using infrastructure as code.
- The platform should provide **relevant runtime metrics** about the virtual and physical machines, for example: cpu & memory usage, amount of network traffic received and sent, storage metrics such as IOPS and bytes read/written.
- It should be possible to have a real-time **inventory** of the provisioned physical hosts and virtual machines and monitor the metrics of them in our existing monitoring system. The platform should expose metrics via **Prometheus-compatible endpoints** or support integration with **Check Mk**.
- The vendor should provide DNS Belgium with best-practices for using the offered solution with regards to performance, security, backup and disaster-recovery.

3.4. Requirements for optional managed services

Transactional Email

- Outbound email must be signed with DKIM.
- SPF TXT-records for the service for inclusion in our SPF policy must exist.
- There should be a mechanism to provide the sending application feedback of email deliveries and bounces.

Object storage

- The API must be compatible with S3
- It should be possible to define access-rules who or what can read and/or write specific data.

Centralized logging

- At least 2 weeks online searchable logs and at least 1year of retention of all logs.
- The logging service should be compatible to receive logs from fluent-bit.
- The logging service should have the possibility to create dashboards and predefined searches of the log-data.
- Logs should be stored immutable.

Managed Database

- Support for different major and minor versions of PostgreSQL.
- Support for different major and minor versions of MySQL or one of it’s variants.
- Support databases with a size up to 1Tb.

- Connections to the database must be encrypted using the database engine's standards.
- Audit logging and general performance metrics should be available. The availability of query-level performance metrics is a nice-to-have.
- The service should provide daily backups with at least 2 weeks retention. The recovery-point-objective in case of failure or disaster is 5 minutes.
- It should be possible to restore a database up to a specific time.
- It should be possible to restore a database into a different instance or create a copy of an existing database.

4. Security & Compliance

4.1. Data Protection

- All customer data should be encrypted **at rest and in transit** using strong encryption standards.
- The keys used for data-encryption should be uniquely used for DNS Belgium, or we should be able to provide our own encryption keys.
- Storage systems should support **versioning and immutability** for backup and archival purposes.
- Data replication between regions must be encrypted and comply with EU data residency requirements.

4.2. Access Control

- The platform must support **Role-Based Access Control (RBAC)** fine-grained access management.
- **Multi-Factor Authentication (MFA)** should be enforced for all administrative access by users.
- Integration with **federated identity providers** (e.g., SAML, OIDC), in particular Microsoft Entra-ID, is a clear benefit.
- Access and audit logs of the platform should be retained for a minimum of **12 months** and be exportable for audit purposes.

4.3. Compliance Standards

- The provider must maintain certification or demonstrate compliance with:
  - **GDPR** (General Data Protection Regulation)
  - **ISO/IEC 27001** (Information Security Management)
  - **ISO/IEC 27017 and 27018** (Cloud services Security Techniques and protection of PII data)
  - **ISO/IEC 22301** (Business continuity management)
  - **SOC 2 Type II** (Security, Availability, Confidentiality)
  - **NIS 2 Directive** (as applicable to essential entities)

- Vendors must provide up-to-date certificates and third-party audit reports.
- The provider must support data residency within the EU, with all physical infrastructure located in EU member states.

4.4. Incident Response

- The provider must have a documented **incident response plan**, including:
  - Detection and containment procedures
  - Notification timelines (within 24 hours of detection for critical incidents)
  - Root cause analysis and remediation reporting

- The provider must inform DNS Belgium of serious incidents relating to cybersecurity that occur in his organization. DNS Belgium shall treat this information with the utmost care and shall use it only to comply with legal (reporting) requirements.
- The platform should support centralized logging, audit trails, and SIEM integration.

5. Sustainability & Environmental Impact

DNS Belgium values **environmental sustainability** and **Corporate Social Responsibility** (CSR) in general. We expect the service provider to actively contribute to environmental sustainability and corporate social responsibility. Vendors must provide transparent reporting and measurable data to support DNS Belgium's annual sustainability reports and CSR initiatives.

5.1. General obligation

- All datacenters hosting DNS Belgium workloads should make maximal use of renawable energy sources.
- At least once a year DNS Belgium must receive reports of energy consumption and carbon-emissions, both for the vendor as a whole and for the emissions associated with DNS Belgium workloads.
- The vendor should provide contact details for CSR related questions.

5.2. Mandatory disclosures

- Carbon footprint per workload (e.g., per VM-hour or per GB stored) including a clear overview of the scope and the used calculation standard (e.g. GHG Protocol).
- Energy mix: the percentage of renewable vs. non-renewable energy used
- Annual water usage (for cooling)
- Overview of efforts on electronic waste reduction (incl. lifetime extension, repair, refurbishment and recycling pratices)
- Overview of climate reduction efforts and targets, where available, including an overview of the scope, base year and the used standards (e.g. Science-Based Targets initiative (SBTi) or equivalent
  - Vendors demonstrating tangible progress in reducing climate impact will score higher on sustainability.
- Overview of other recent CSR-related efforts (e.g. CSR reports)

5.3.: Life Cycle Assessment (Preferred Vendors)

Vendors able to provide a full Life Cycle Assessment (LCA) will be favoured in the sustainability scoring. The LCA should:

- Include climate impact (carbon footprint) expressed in CO_2-equivalents, calculated according to:
  - GHG Protocol: Product Life Cycle Accounting and Reporting Standard or similar.
- Present a breakdown by life cycle stages:
  - Raw material extraction.
  - Production.
  - Downstream transport.

- Use.
- *(End-of-life optional; if included, show separately.)*

- If manufacturers offer ISO 14040 and ISO 14044 standards, this standard should be used.

6. Service Level Agreements (SLAs)

6.1. Availability

- The provider must guarantee a minimum monthly uptime of **99.95%** for core infrastructure services (compute, storage, networking), with higher availability targets preferred. The SLA must clearly define measurement methodology, exclusions (e.g., scheduled maintenance), and remedies for non-compliance (e.g., service credits).
- Availability must be measured **per region/datacenter and per service**, with monthly reporting.
- Vendors must describe their redundancy and failover mechanisms, including multi-zone and multi-region capabilities.

6.2. Support

- The provider must offer **24/7 technical support** with defined response times:
  - **Critical issues**: Response within 1 hour.
  - **High priority**: Response within 4 hours.
  - **Standard issues**: Response within 1 business day.

- Support channels must include email, ticketing system, and optionally live chat or phone.
- Escalation paths must be clearly documented.

7. Pricing Model

7.1. Cost Structure

- The provider must offer transparent pricing for:
  - **Compute resources** (dedicated and shared VMs)
  - **Storage** (block, object, backup)
  - **Networking** (bandwidth, load balancers, VPN)
  - **Optional managed services**

- Pricing models may include pay-as-you-go, reserved capacity, or subscription-based options.

7.2. Billing Transparency

- Monthly invoices should include a **detailed breakdown** of the costs.
- DNS Belgium should be able to **tag and track costs** per project or stage.

7.3. Optional Services

- Vendors may propose pricing for:
  - Migration support
  - Training and onboarding
  - Managed services (e.g., managed Kubernetes, databases)

- Optional services must be clearly separated from core infrastructure pricing.

8. Vendor Qualifications

8.1. Experience

- Vendors must provide:
  - **Case studies** of similar IaaS deployments within the EU.
  - **References** from at least two clients with comparable workloads.
- Experience with **regulated environments** is a plus.

8.2. Financial Stability

- Vendors must provide:
  - **Annual financial statements** or equivalent documentation.
  - Evidence of **long-term viability** and investment in infrastructure.
- DNS Belgium reserves the right to conduct **due diligence** on financial health.

9. Proposal Format

To ensure consistency and ease of evaluation, vendors must structure their proposals as follows:

1. Executive Summary
   - Overview of the proposed solution
   - Key differentiators and value proposition
2. Technical Proposal
   - Responses to all technical requirements
   - Architecture diagrams and service descriptions
   - Security and compliance documentation
3. Pricing Proposal
   - Detailed cost breakdown
   - Optional services pricing
   - Licensing terms (if applicable)
4. Vendor Profile
   - Company background
   - Certifications and references
   - Financial documentation
5. Appendices
   - Completed version of the Excelfile with questions
   - Supporting documents
   - SLA terms
   - Terms & Conditions
   - Template contract
   - CSR Policy documentation
   - Sustainability reports & Certificates

10. Appendices

10.1. Current Infrastructure Summary

This summary is provided to give an idea of the current size of the workload of the platforms in scope. The required size at the time of the migration can deviate from the data presented here.

Compute – Kubernetes

Stage	*Number of nodes*	*Total CPU's*	*Total memory*	*Total size of PVC storage volumes*
Development	20	40vCPU	160Gb	162Gb
Automated Acceptance	6	12 vCPU	48Gb	142Gb
User Acceptance	13	26 vCPU	104Gb	142Gb
External Test	13	26 vCPU	104Gb	142Gb
Production	24	48 vCPU	192Gb	162Gb

Our registry platforms generally require more memory and less CPU.

- Average **CPU-usage** within the clusters is **about 10%** with occasional **spikes up to 25%**
- **Memory Requested by Pods** is about **60% of the available capacity**. Actual memory used is slightly lower.
- In addition to PVCs linked to a single pod, each cluster also has **NFS storage, writable by multiple pods**. This adds up to **140Gb in total** for all clusters.
- Resources required for the control planes are not known, as these are currently managed by AWS EKS.

Compute – Classic VMs

Next to the Kubernetes workernodes, we have several regular linux VMs.

Stage	*Number VMs*	*Total vCPUs*	*Total memory*	*Total size of storage volumes*
Development	7	20	40Gb	270Gb
Automated Acceptance	4	8	5Gb	120Gb
User Acceptance	20	42	60Gb	750Gb
External Test	9	20	40Gb	300Gb
Production	25	70	100Gb	1050Gb

- We have about **35Tb of volume snapshots** of these virtual machines as backups. (non-deduplicated)

Databases

Stage	*DB engine*	*Number of databases*	*Total vCPUs*	*Total memory*	*Total size of storage volumes*
Development	Oracle	1	2	8Gb	1000Gb
	PostgreSQL	6	12	8Gb	120Gb
	MySQL	2	4	2Gb	40Gb
Automated Acceptance	PostgreSQL	3	6	4Gb	60Gb
User Acceptance	Oracle	1	2	16Gb	1000Gb
	PostgreSQL	3	6	4Gb	60Gb
	MySQL	2	4	2Gb	40Gb
External Test	Oracle	2	4	8Gb	400Gb
	PostgreSQL	6	12	7Gb	120Gb
	MySQL	1	2	1Gb	20Gb
Production	Oracle	2	8	64Gb	2000Gb
	PostgreSQL	12	24	14Gb	240Gb
	MySQL	2	4	3Gb	40Gb

- Production and External test include the online replicas in the DR datacenter.
- **Oracle will be migrated to PostgreSQL** prior to migrating that part of the platform.
- We have about **115TB of volume snapshots** of these databases as backups.

Central Logging (OpenSearch clusters)

We currently use OpenSearch clusters to centralize logging per stage.

Stage	*Number of cluster-members*	*Total vCPUs*	*Total memory*	*Total size of storage volumes*
Development	4	8	16Gb	600Gb
Automated Acceptance	2	4	8Gb	200Gb
User Acceptance	4	8	16Gb	520Gb
External Test	2	4	8Gb	390Gb
Production	2	4	16Gb	1700Gb

- Production averages 50% CPU-usage, the other clusters average 15% to 20% CPU-usage. All clusters have occasional spikes up to 80%.
- The current storage volumes store 14 days of logs available for online search. Next to that, we store logs with 1 year retention on S3. This amounts to 50Tb.

Transactional Email

- We currently send about 30.000 transactional emails every month.