stack8s

stack8s – Managed Backend Service

G-Cloud 15 Service Definition

1. Service description

stack8s Managed Backend Service is a sovereign-first, Kubernetes-powered Backend-as-a-Service (BaaS) platform that provides fully managed backend infrastructure across UK and EU cloud providers. It enables public sector and regulated organisations to build and run modern applications while maintaining strict control over data location and regulatory compliance, without needing to manage underlying cloud infrastructure.

The service abstracts the complexity of provisioning, securing, and operating backend components such as databases, authentication, object storage, messaging, and APIs. Customers interact with the platform through a web management console and RESTful APIs, while stack8s operates the multi-cloud infrastructure, high-availability Kubernetes clusters, monitoring, and security controls.

Data residency is constrained to the United Kingdom and the European Economic Area. Customers can select preferred regions or jurisdictions (for example, UK-only or UK+EEA) within those bounds to align with departmental data protection policies. The platform is designed to support workloads at “OFFICIAL” and equivalent sensitivity levels, with strong identity and access controls, encrypted data-in-transit and at-rest, and comprehensive audit logging.

The stack8s Managed Backend Service uses a Kubernetes-native architecture to deploy and manage open-source BaaS technologies such as Supabase, Appwrite, PocketBase, Parse Server, and Directus as managed services. Customers benefit from these feature-rich backends (real-time APIs, RBAC, storage, etc.) while stack8s handles scaling, patching, resilience, and security hardening.

The service is delivered as SaaS in both public and private cloud deployment models:

- Public cloud: multi-tenant platform with strong logical isolation between customers, suitable for most OFFICIAL workloads.
- Private cloud: dedicated environments for customers that require stronger isolation or specific provider/region constraints.

The platform is aimed at digital delivery teams that want to accelerate the delivery of API-driven services, citizen-facing applications, and internal tools, while meeting data sovereignty and assurance requirements.

---

2. Service features and benefits

CONFIDENTIAL - DO NOT DISTRIBUTE WITHOUT PERMISSION

stack8s

2.1 Service features

- **Data sovereignty with EU and UK cloud hosting**
  - All application data, backups, logs, and metadata are stored and processed only within UK and EEA regions.
  - Customers can choose UK-only or UK+EEA deployment options to meet internal policy and assurance needs.
  - Data location is controlled at the platform level to simplify compliance with GDPR and UK government guidance.
- **Multi-cloud infrastructure deployment that abstracts provider complexity**
  - The platform runs across multiple UK/EU sovereign cloud providers (for example, different UK and EU regions) but exposes a single, unified control plane and API.
  - stack8s is responsible for provider selection, regional configuration, resilience, and capacity management within agreed data residency boundaries.
  - Customers do not need to understand or manage each provider's proprietary services, IAM model, or networking constructs.
- **Managed open-source backends (Supabase, Appwrite, PocketBase, Parse Server, Directus)**
  - Popular open-source BaaS platforms are provisioned, maintained, and monitored by stack8s as managed services.
  - Customers gain features such as real-time APIs, role-based access control, authentication flows, object storage, and schema management out-of-the-box.
  - Patching, version upgrades, security configuration, performance tuning, and scaling of these components are handled by stack8s.
- **GDPR-aligned infrastructure meeting UK government data requirements**
  - Platform-level controls for encryption, access management, logging, and retention are designed to support GDPR principles and common public sector security expectations.
  - Data in transit is protected using modern TLS versions; data at rest is encrypted on all physical media managed by underlying providers.
  - Logging, audit, and data retention policies are designed to support typical security assurance and DPIA requirements.
- **Kubernetes-native platform ensuring portability and vendor independence**
  - All workloads are deployed as containers and managed via Kubernetes, using common patterns (Deployments, StatefulSets, Ingress, etc.).
  - This enables consistent configuration, scaling, and observability across cloud providers and regions.
  - Architectures can be replicated or migrated to other compliant Kubernetes environments if sourcing strategies or regulatory requirements change, reducing vendor lock-in.
- **Integrated authentication, authorisation, and database management out of the box**
  - Identity and access management (IAM) features include user registration, sign-in flows, multi-factor authentication (where enabled), and identity federation via standard protocols.
  - Role-based access control (RBAC) and fine-grained permissions can be defined at application, API, and data levels.
  - Databases (relational and non-relational) are provisioned with secure defaults, backup policies, and monitoring baked in, with configuration exposed through the console and APIs.
- **Unified management console and API**

    - A web-based management console provides dashboards for service health, performance metrics, resource utilisation, logs, and events.
    - Customers can configure backend services, manage schemas, set scaling rules, configure backups, and manage access controls from a single interface.
    - All major operations are also exposed via a RESTful API, with OpenAPI/Swagger documentation and an API sandbox/test environment.
- **Real-time monitoring, metrics, and logging**
    - Metrics include API request volumes and latency, database performance and connections, storage utilisation, authentication events, and error rates.
    - Real-time dashboards allow teams to monitor service health, performance, and usage across environments.
    - Logs can be viewed via the console or consumed through APIs/integrations with customer SIEM and observability tooling.
- **Automated scaling and high availability**
    - The platform uses Kubernetes scaling capabilities to automatically scale backend components in response to load and defined thresholds.
    - Multi-zone deployments, replicated storage, and health checks support high availability and self-healing behaviour.
    - Customers can configure scaling profiles and thresholds, while the platform ensures capacity and resilience within agreed limits.
- **Structured onboarding, documentation, and learning resources**
    - Online tutorials, video guides, and self-paced learning paths are available for developers, administrators, and architects.
    - Documentation includes quickstart guides, API references, architecture patterns, and troubleshooting sections.
    - Higher support tiers include guided onboarding sessions with stack8s engineers to design initial architecture and configure services.
- **Data export, migration, and lock-in minimisation**
    - Customers can export data (including databases, files, configuration, and logs) via APIs or the console.
    - Standard formats such as JSON, CSV, and SQL dumps are provided, with options for binary backups where appropriate.
    - A defined post-termination grace period and optional assisted migration services are available to support clean exit.

2.2 Service benefits

- **Rapid application delivery without managing infrastructure**
    - Teams can move from idea to production-ready backend in days, rather than weeks or months, because all infrastructure provisioning and platform operations are handled by stack8s.
    - This directly supports agile delivery, continuous improvement, and rapid iteration on user needs.
- **Assured data sovereignty and compliance alignment**

    - By constraining data location to UK/EEA and providing strong platform controls, the service helps buyers demonstrate alignment with departmental data policies and regulatory obligations.
    - Project teams can inherit platform-level controls rather than inventing their own, simplifying security and privacy assurance.
- **Lower development and operational cost**
    - Consuming managed open-source BaaS stacks avoids proprietary licence costs and reduces the need for internal platform engineering teams.
    - Organisations can focus budgets on feature development and service improvement rather than on building and operating backend platforms.
- **Reduced vendor lock-in through Kubernetes and open-source**
    - Use of open-source components and Kubernetes makes architectures more portable and transparent.
    - Organisations retain more control over future sourcing decisions and can move or replicate workloads if providers or requirements change.
- **Improved security posture and observability**
    - Built-in authentication, RBAC, encryption, logging, and monitoring provide a strong baseline security posture by default.
    - Real-time metrics and logs make it easier to detect issues, support incident response, and satisfy audit requirements.

---

3. Use cases

The service is suitable for a range of public sector and regulated workloads, including:

- **Citizen-facing digital services**
    - Building web and mobile backends for citizen portals, forms, case management frontends, and transactional services that require secure user authentication, data storage, and audit trails.
    - Supporting rapid delivery of new services or replacing legacy backends while ensuring data stays in UK/EEA regions.
- **Internal line-of-business applications**
    - Creating internal applications for staff (for example, workflow tools, knowledge systems, or operational dashboards) that rely on structured data, permissions, and integrations with existing systems.
    - Providing a modern backend without asking internal teams to run databases, messaging systems, or identity services.
- **Data-centric and API platforms**
    - Hosting APIs that expose data or functionality to other departments, partners, or external suppliers, with consistent authentication and authorisation controls.
    - Building microservice-style architectures where multiple services share common backend capabilities and observability.
- **Innovation, pilots, and proofs of concept**

CONFIDENTIAL - DO NOT DISTRIBUTE WITHOUT PERMISSION

    - Standing up experimental or pilot services quickly to test user needs and policy ideas, with a clear path to production without replatforming.
    - Allowing teams to experiment with open-source BaaS technologies under the operational umbrella of a managed service.
- **Modernisation of legacy applications**
    - Gradually migrating legacy backends to a cloud-native, Kubernetes-based platform while preserving data sovereignty.
    - Exposing legacy data and functions via modern APIs, then progressively refactoring or replacing components with managed BaaS services.

---

4. Pricing overview

Pricing for stack8s Managed Backend Service is set out in the stack8s UK G-Cloud 15 Pricing Document in the Digital Marketplace.

That document details:

- Service pricing models (for example, per-environment, per-backend, or usage-based elements).
- Included allowances (such as baseline storage, compute, and support).
- Additional charges for higher support tiers, enterprise features, or extended retention.
- Any minimum terms, onboarding packages, or volume discounts.

Buyers should refer to the pricing document to understand the exact cost model applicable to their deployment.

---

5. Service constraints

- **Dependency on underlying UK/EU cloud providers**
    - Overall availability and performance are influenced by the sovereign cloud providers used for compute, storage, and networking.
    - While the platform is designed for resilience (e.g. multi-zone and multi-region) and can mitigate many issues, widespread provider incidents may still cause temporary degradation or outages.
- **Planned maintenance windows**
    - Platform components and underlying infrastructure require regular maintenance, including security patching, upgrades, and configuration changes.
    - Maintenance windows are scheduled outside normal business hours where possible and notified to customers at least 48 hours in advance.
    - During maintenance, brief service interruptions or reduced functionality may occur.
- **SaaS-only delivery model**

CONFIDENTIAL - DO NOT DISTRIBUTE WITHOUT PERMISSION

    - The service is provided as a managed SaaS platform. It cannot be installed on customer premises or run in customer-managed cloud accounts.
    - Customers integrate via the management console and APIs rather than having direct access to the underlying Kubernetes control planes or host operating systems.
- **No direct control over datacentre selection**
    - Customers can specify jurisdictional and regional preferences (e.g. UK-only), but do not select specific datacentres or availability zones.
    - stack8s manages placement within those constraints to balance resilience, performance, and capacity.
- **Feature and quota limits**
    - There may be limits on the number of environments, services, API requests, connections, or storage allocated per service tier.
    - These quotas are documented and can typically be increased via commercial or technical agreement, subject to capacity planning.

---

6. Technical requirements

- **Modern web browser with JavaScript enabled**
    - Users need a current version of a mainstream browser (for example, Microsoft Edge, Google Chrome, Mozilla Firefox, or Apple Safari).
    - JavaScript must be enabled to use interactive dashboards, configuration flows, and analytics views in the management console.
- **Secure network connectivity (HTTPS/TLS)**
    - All access to the management console and APIs must be over HTTPS with modern TLS support.
    - Customer environments (on-premises or cloud) must permit outbound TLS traffic to the service endpoints and handle certificate verification.
- **Client and integration capabilities**
    - Customer applications and integration platforms must be able to call RESTful APIs (including handling authentication, pagination, and error responses).
    - For automated integration (CI/CD, monitoring, etc.), tools must support HTTPS and standard HTTP authentication mechanisms (for example, tokens or OAuth where used).
- **Identity and access prerequisites**
    - Organisations should have processes for managing user accounts and assigning appropriate roles within the platform.
    - Where identity federation is used, customers must manage their identity providers (such as enterprise IdPs) and ensure they are configured to federate with the service.
- **Internal security and networking configuration**
    - Firewalls, proxies, and endpoint security solutions within customer networks must allow the required outbound connections and not interfere with TLS or API traffic.
    - Where customers integrate logs or metrics into their own SIEM/monitoring tools, appropriate endpoints and credentials must be configured on their side.

CONFIDENTIAL - DO NOT DISTRIBUTE WITHOUT PERMISSION