magnolia®

Evaluating the Magnolia PaaS Deployment

Evaluating the Magnolia PaaS Deployment

Your mission, should you choose to accept it, is to evaluate and select a fit-for-purpose digital experience platform (DXP).

Your responsibility goes beyond selecting potential vendors and familiarizing yourself with their capabilities and services. Another significant consideration is the deployment of your DXP.

Before choosing any vendor, there are some prerequisite questions that you should ask. Do you want to deploy and manage the platform in-house? Or do you want to leverage the vendor's best practices for application management, infrastructure deployment, automation, and monitoring?
Choosing the latter will likely add several capabilities to your RFP's scope.

This document is designed to help you evaluate Magnolia's Platform-as-a-Service (PaaS), and explain the benefits and specific feature set of this deployment model.

Why Magnolia PaaS?

The Magnolia PaaS is the ideal solution for enterprises to deploy and manage the Magnolia platform in the cloud. The solution includes all cloud infrastructure and best practices that support your DevOps team. This allows you to focus on what matters most, get your projects up and running quickly, and deliver high-performance experiences to your customers.

The Magnolia PaaS includes:

- The Magnolia application
- Cloud infrastructure and provisioning
- Kubernetes orchestration
- Content delivery via a load balancer and CDN
- Code and Docker repository
- CI/CD pipelines
- Rolling upgrades
- Monitoring and diagnostics
- Enterprise security

Benefits

Fast and flexible deployment

Get immediate access to Integration, UAT and Production environments with integrated CI/CD to rapidly start development with Magnolia. Leverage pre-configured pipelines for Maven project deployments and low-code configuration deployments.

Spin up an unlimited number of temporary test environments to allow stakeholders to test new features.

Use rolling upgrades to bring Magnolia to the latest version without downtime.

High-performance experiences

With the Magnolia PaaS, your application runs on a high-performance and high-availability platform that adapts to your load. You can scale public instances up or down to handle traffic spikes. To deliver experiences to your users fast you can opt for Magnolia's Content Delivery Network (CDN) or use your own.

Multinational enterprises can opt for our multi-regional deployment option, and deploy multiple Magnolia environments across the globe. Start with a single deployment and reach a cross-continental presence seamlessly.

Efficient operations and tight security

If you are already pursuing a cloud strategy, you probably don't miss ordering servers, administering databases, and making backups. Let's keep it that way.

With the Magnolia PaaS, you get broad control over your platform via a self-service interface. Monitor your environment, provision instances, and recover your database, if needed, all in one place.

You can rely on our certified security concept, including DDoS, WAF, SSL, HA, role-based access control, OWASP, isolation, encryption, ISO, GDPR, single tenancy, backup, DR, IAM, physical security, and multi-region availability. Please consult our security document for further details.
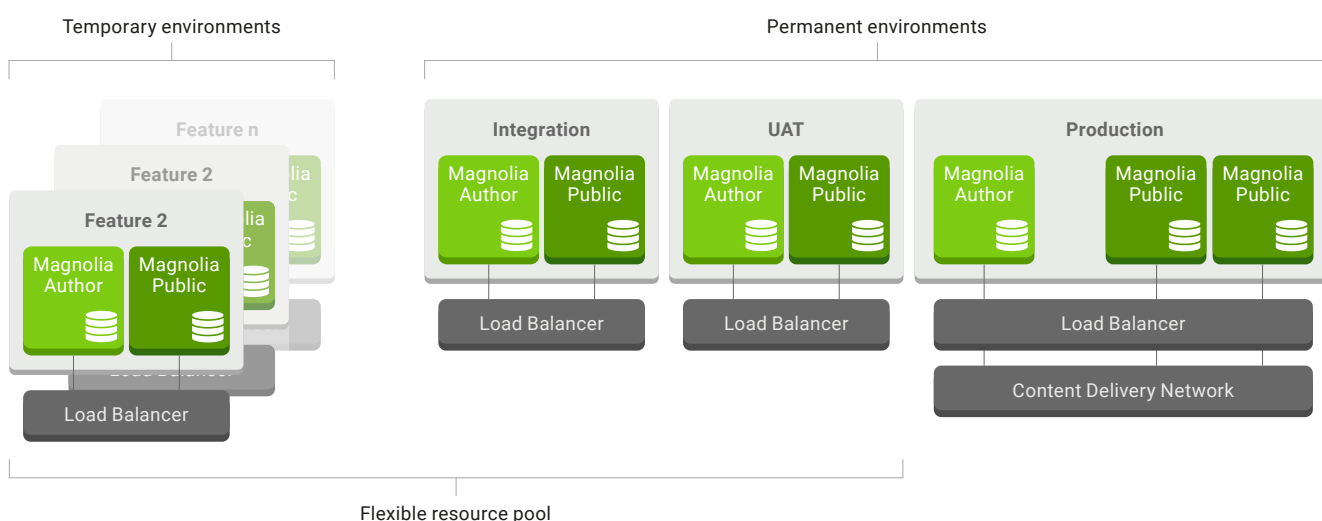
Magnolia PaaS

Design

For a smooth onboarding experience, you get immediate access to your cloud environments, management tools, and support.

Environments

The platform consists of a production and non-production cluster. Your dedicated production environment is designed for performance and high availability. All non-production instances share a resource pool with flexible allocation between your Integration, UAT, and any temporary Feature environments.

Temporary environments — Permanent environments

| Feature n |
| Feature 2 |
| Feature 2 |

Magnolia Author · Magnolia Public — Load Balancer

Integration: Magnolia Author · Magnolia Public — Load Balancer

UAT: Magnolia Author · Magnolia Public — Load Balancer

Production: Magnolia Author · Magnolia Public · Magnolia Public — Load Balancer — Content Delivery Network

Flexible resource pool

Multi-region deployment

An optional multi-region deployment leverages clusters in multiple availability zones, ensuring 99.9% availability and disaster recovery.

There are two options for a multi-region deployment:

In the active/passive scenario, traffic is only routed to the active cluster. The passive cluster acts as a hot standby and only becomes active if the primary cluster goes down. The CDN automatically routes traffic to the active cluster.

In the active/active scenario, the CDN routes traffic to both clusters. If one cluster goes down, the CDN routes all traffic to the healthy cluster until the other cluster has recovered. This option supports a multi-cloud approach using different cloud vendors.

CDN

An embedded Content Delivery Network (CDN) enforces high security standards, including Web Application Firewall (WAF), DDoS protection, and more. Alternatively, you may implement a CDN of your choice with our platform.

Configuration

The platform's default configuration is optimized to run Magnolia containers in a cloud environment. It is based on industry standards and best practices for containerization, CI/CD, content caching, and delivery.

Frontend and Solr hosting

The design of the Magnolia PaaS allows you to host several services on the platform, including your frontend application and Solr search. We will add more applications in the future. For more information, see the "Add-on services" section below.
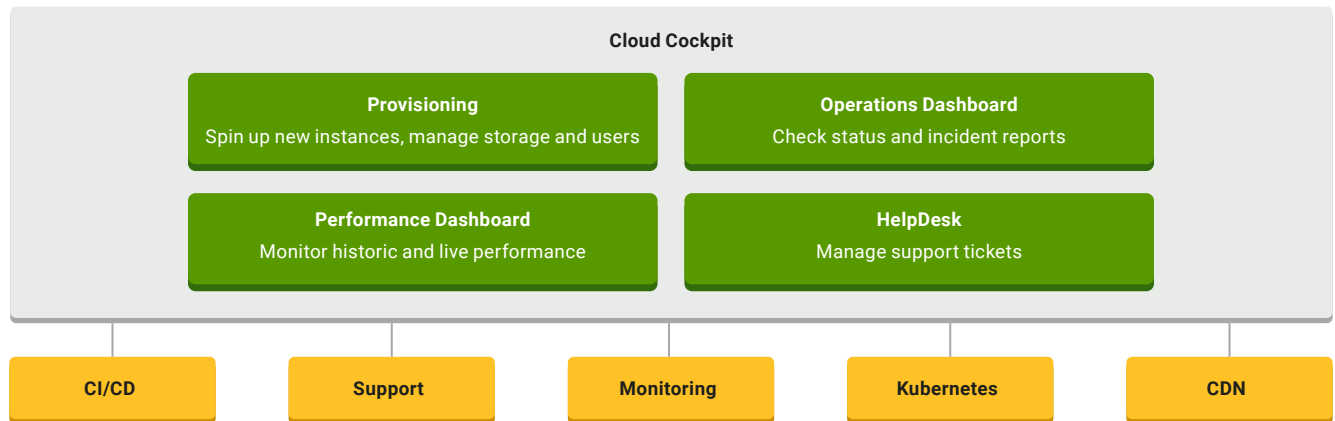
Support

Our cloud help desk is your single point of contact and handles all your change and support requests no matter whether they are application- or infrastructure-related.

The team is available 24/7 and offers guaranteed response times.

Self-service management

Magnolia's PaaS Cockpit is the platform's operations and control center. It is an intuitive user interface that allows you to manage your Magnolia PaaS.

Cloud Cockpit

Provisioning Spin up new instances, manage storage and users	**Operations Dashboard** Check status and incident reports
Performance Dashboard Monitor historic and live performance	**HelpDesk** Manage support tickets

CI/CD	Support	Monitoring	Kubernetes	CDN

Infrastructure management

The PaaS Cockpit is where you take control over your Magnolia PaaS resources. View and adapt resources such as memory, vCPUs, and storage, or provision entirely new Magnolia instances and increase traffic bandwidth.

Content delivery

Manage domains, certificates, and redirects in one place, and check CDN information about traffic origin and geographic location.

Backup and restore

Your Production environment's content, configuration, release, and software version are backed up automatically. You can also trigger manual backups in the PaaS Cockpit. Should you ever need to do so, you can restore to any point in time. For more information check the section about "Disaster Recovery".

Upgrades

The Magnolia PaaS provides the latest Magnolia version as well as additional features and connectors. New versions can be installed seamlessly via the PaaS Cockpit through rolling upgrades, making it easy to test upgrades in UAT and deploy them to Production once tested.

Access control

The Magnolia PaaS has a default set of roles. Alternatively, you can integrate your Identity Management Service. Use the PaaS Cockpit to manage users and roles.

Subscription management

Get insights into your subscription and usage. Transparent cost communication and embedded approval workflows guarantee total cost control. Adjust provisioning and subscriptions according to anticipated growth, traffic spikes and marketing activities.

Activity log

Check all major actions that were triggered from the PaaS Cockpit.

Monitoring and troubleshooting

The Magnolia PaaS' monitoring stack collects metrics and logs from a variety of sources, providing an end-to-end view of overall traffic and health of your platform. For more information check the "Monitoring and Troubleshooting" of this white paper.

CI/CD

Magnolia's tools and best practices provide a streamlined development and deployment process. The platform provides two separate CI/CD pipelines based on GitLab: one pipeline for low-code frontend deployments and another pipeline for backend deployments. The blueprints can be adjusted to match your development workflows.

CI/CD pipeline for low-code configuration

Magnolia Light Development allows you to use slim YAML configuration files to complete the most common tasks including templating, content modelling, provisioning REST clients, templating, and creating Magnolia apps. A dedicated CI/CD pipeline for configurations ensures fast and reliable deployments.

CI/CD Pipeline: Low-Code Config

Integration
Configure features prior to testing

Commit   Deploy

UAT
Test features prior to live deployment

Commit   Deploy

Production
Live environment for authors and public visitors

Commit   Deploy

CI/CD Pipeline: Java Backend

Feature
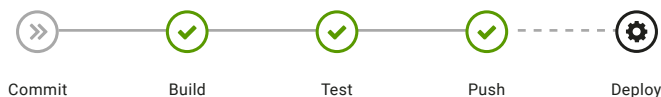Develop and test features in a dedicated, temporary environment

Commit   Build   Test   Push   Deploy   Stop

Integration
Develop and merge features prior to testing
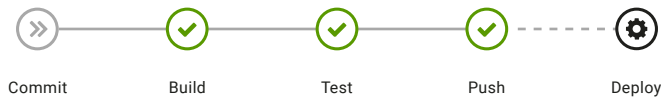
Commit   Build   Test   Push   Deploy

UAT
Test features prior to live deployment

Commit   Build   Test   Push   Deploy

Production
Live environment for authors and public visitors

Commit   Build   Test   Push   Deploy
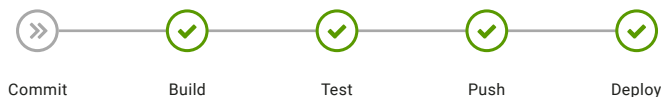
CI/CD pipeline for Maven deployments

Leverage the platform's pre-configured CI/CD pipeline for backend deployments to promote and merge code from your local development machine. Each branch and commit gets its own deployment in line with resource usage limits. Once a feature has been reviewed, changes can be integrated into a common deployment.

Content copy

Sync content between environments to test new features with real content.

Availability and performance

The Magnolia PaaS helps you deliver great customer experiences anytime and anywhere by ensuring high availability and performance for your Magnolia application.

Hosting

The Magnolia PaaS is currently available on AWS, Microsoft Azure, Tencent, and our Swiss hosting partner Mironet. Please consult our team for further cloud providers.

Performance

The Magnolia PaaS can be deployed in one or multiple regions. Each region provides high availability and redundancy. Before we deploy your environments, we discuss your requirements and determine where to host your platform for the optimal balance between cost and performance.

Scaling

Thanks to Docker and Kubernetes, you can flexibly scale your environments up or down when experiencing a traffic peak. You can also add regions with a single click.

SLA

Magnolia guarantees 99.8% availability and a performance of <200ms / http roundtrip. We constantly monitor these metrics and provide reports in the cockpit on demand.

Global support

The support team is available 24/7/365. Their response time depends on your Magnolia subscription.

Disaster recovery

The Magnolia PaaS is configured to regularly make a full backup of all instances in the production environment. In addition, each instance's PostgeSQL database continuously ships transaction logs to a remote object storage, allowing you to restore the database to any point in time in case of a disaster - or to clone data into a new instance.

Add-on services

Frontend hosting

Leverage all advantages of the headless approach without needing an additional third-party frontend hosting platform while efficiently reusing all Magnolia PaaS tools and deploying your frontend applications to dedicated pods in the same clusters.

End-to-end insights enable you to follow the journey of a request from the CDN, to the frontend pod, to the backend and its underlying infrastructure, and simplify troubleshooting and optimization.

Solr hosting

Similar to frontend hosting, you can host the search platform Solr within the Magnolia PaaS. Monitoring data and logs are exposed in the Magnolia PaaS Cockpit.

Fastly Image Optimizer

Fastly's Image Optimizer (IO) optimizes and caches image versions on Fastly's global points of presence (POP). A regional POP responds to requests directly, reducing the load on your Magnolia instances.

Fastly Streaming Media Delivery

Fastly's streaming services help you deliver low-latency streaming experiences with minimal rebuffering for high-quality live broadcasts and video-on-demand.

Fastly waiting room

Fastly's waiting room handles traffic surges from the edge. The feature uses cookies and efficiently flattens the traffic curve, for example, during campaigns or ticket sales. Our platform provides blueprints for static pages, including 'start waiting', 'keep waiting', and 'access denied'.

Monitoring and troubleshooting

Keep an eye on the performance of your applications and environments using real-time monitoring and advanced metrics in Magnolia's PaaS Cockpit.

The platform's logging and monitoring stack collects metrics and logs from a variety of sources, providing an end-to-end view of overall traffic and requests handled by your sites and transparency into subscription costs.

Collected metrics and logs help to:
- Identify where a problem has occurred
- Trace a request from the browser to the CDN to the cluster to Magnolia and back
- Provide an overview of traffic flow

Log management

Track and monitor how your applications are performing in real time. Review stack traces for troubleshooting and analyze instance metrics to identify patterns.

Health metrics

Monitor the health of your services, application and instances across environments and clusters to know when things don't go as expected.

Performance metrics

Monitor all layers of the platform using real-time metrics from the delivery, application, and infrastructure layer.

Alerts

Receive real-time alerts about application availability or service level objectives.

Reports

Contractually agreed parameters including availability, performance, and usage are available for reporting, aggregation, control, and subscription optimization.

Tools

The Magnolia PaaS uses Grafana loki for logging, Grafana for application alerts and dashboards, and Thanos for monitoring and system alerts.

External status page

The external service, BetterUptime, monitors and displays the status of your environments 24/7. The status page includes the health of your cluster, your platform's components, the Magnolia application and CDN, and your public-facing websites. Conveniently manage any incidents directly from this page.

Enterprise security

Magnolia's secure architecture and infrastructure security features allow you to deploy with confidence.

Separation of concern

Every Author and Public instance runs on a dedicated virtual machine.

Single tenancy

Magnolia PaaS instances are provided as single tenants running on a dedicated cluster, ensuring that your data is clearly separated. Monitoring and logging data is stored on a central cluster following the quality standards of Swiss Hosting.

Encryption

Traffic between services and browsers is encrypted and secured. TLS is enabled for any communication between instances and certificates originally provided by Magnolia are renewed automatically.

Firewall

The Magnolia PaaS provides a WAF which aligns closely to the OWASP ModSecurity Core Rule Set (CRS). The OWASP CRS aims to protect web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts.

DDoS

The embedded CDN scans encrypted and unencrypted traffic between your web server and your visitor's browsers. It automatically filters all non-HTTP and non-HTTPS traffic at the global CDN nodes, blocking highly disruptive layer-3 and layer-4 attacks. It protects against ping floods, ICMP floods, reflection and amplification attacks, transaction floods, resource exhaustion, and UDP abuse.

Identity and Access Management (IAM)

The Cockpit and all Magnolia instances are tightly integrated with an IAM server using the OpenID Connect protocol standards.

Database encryption

All data at rest and in transit is encrypted.

Advanced security package

Our optional advanced security package provides additional protection:

- Advanced WAF
- Advanced DDoS
- Secure key storage
- Active threat monitoring
- Vulnerability scanning
- Malware detection, e.g., for file uploads
- Annual penetration test by a third party
- Bot protection
- Web defacing protection
- Dedicated security dashboard

Compliance and GDPR

Magnolia completed the ISO 27001 and SOC 2 certifications, and is GDPR compliant. We also continually monitor compliance or potential vulnerabilities. Furthermore, the The Magnolia PaaS is subject to a yearly, external security assessment including pen tests and re-checks.

A copy of our certificates and a penetration test report by Compass Security are available on request.

GDPR

Magnolia hosts your website as a cloud service and collects, stores, and processes data on your behalf. You are the controller while Magnolia is the processor. Our Data Protection Agreement (DPA) defines the relationship between controller and processor.

Security measures

Magnolia implements appropriate measures to ensure confidentiality, integrity, availability, and resilience of the processing system and the ability to restore and access personal data in case of an incident. Magnolia also tests the effectiveness of the technical and organizational measures.

Location of data

The Magnolia PaaS is available in multiple regions and you choose which data centea The Magnolia PaaS is available in multiple regions and you choose which data centers you want to deploy to. Our hosting providers ensure that information is stored in safe locations and that agreements with the state in which it operates exist.

© 2023 Magnolia International Ltd.
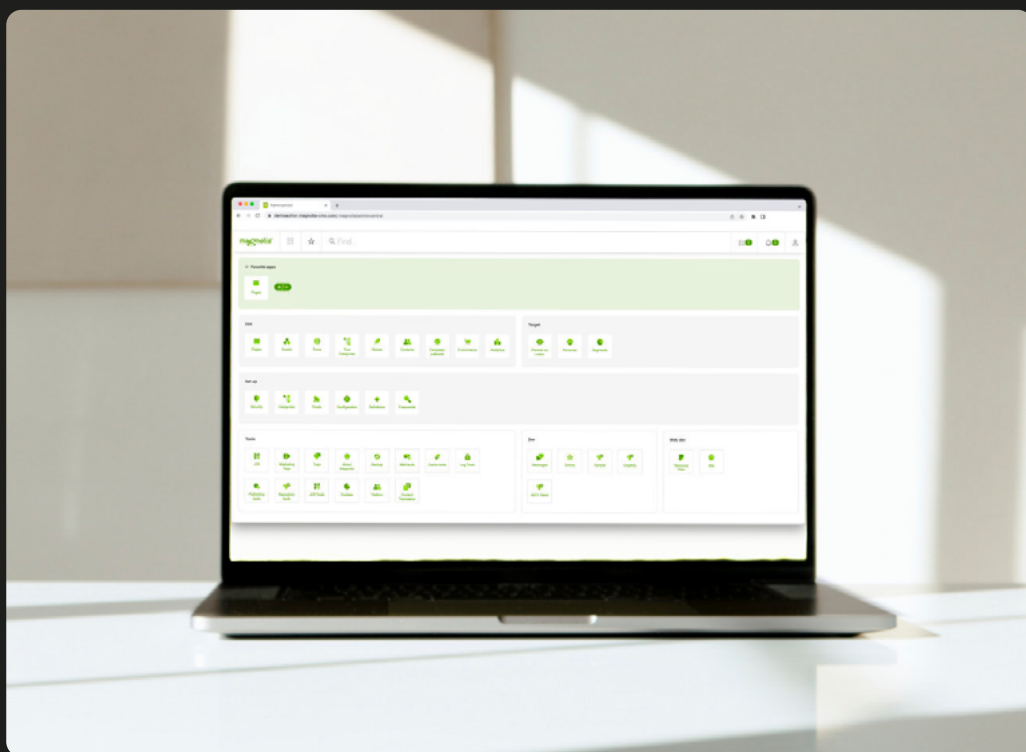
Get in touch

To learn how Magnolia can help you launch great digital experiences faster, contact us at:

Magnolia HQ Switzerland

📞 **Office** +41 61 228 90 00

✉️ contact@magnolia-cms.com

📍 [Or see our offices worldwide](#)

🖥️ www.magnolia-cms.com