



Magnolia Cloud Platform Security

Lars Fischer, Mathias Seiler, Florian Sacharuk, Adrien Manzoni, Alex Mansell

1.0, 2021-03-19: Security Briefing

Table of Contents

Copyright	1
Revision History	2
1. Introduction.....	3
2. Magnolia Cloud Platform	4
2.1. Technologies	4
3. Magnolia Cloud Platform Architecture.....	5
4. WAF and CDN	7
4.1. WAF	7
4.2. CDN.....	7
5. Identity and Access management.....	9
5.1. Authentication.....	9
5.2. Authorization.....	10
5.3. Cockpit.....	10
6. Database.....	11
Appendix A: GDPR	12
Appendix B: Auditing and certification.....	14

Copyright

Copyright of Magnolia International©. This document may not be duplicated, in whole or in part, by any means whatsoever, without the prior written permission of Magnolia International. The information contained in this document is confidential and is the valuable proprietary information of Magnolia International Ltd. Visit [the Magnolia official website](#) to learn more about us as a company.

Revision History

Revision	Date	Comments
1.0	2021-03-19	Security Briefing

Chapter 1. Introduction

The purpose of this document is to outline the high-level architecture of Magnolia Cloud Platform and provide an overview of the security measures developed and implemented for the Magnolia Cloud Platform project.

Magnolia Cloud Platform is a PaaS solution built for Magnolia partners and customers in mind and offers rapid deployment of Magnolia CMS. The cloud-based approach increases reliability, improves overall performance, scales more easily, and provides enhanced security benefits.



An [HTML version](#) of this document is available.

Chapter 2. Magnolia Cloud Platform

Magnolia Cloud Platform gives each customer (known as tenants) its own Rancher and Kubernetes clusters, IP addresses, and load balancers.

The [Kubernetes implementation](#) depends on the target IaaS provider. For example, if the IaaS is AWS, the Kubernetes would be implemented with [Elastic Kubernetes Service \(EKS\)](#).



Integration, quality assurance and developer reviews exist on separate clusters per tenant. Environments within a cluster are separated by namespaces.

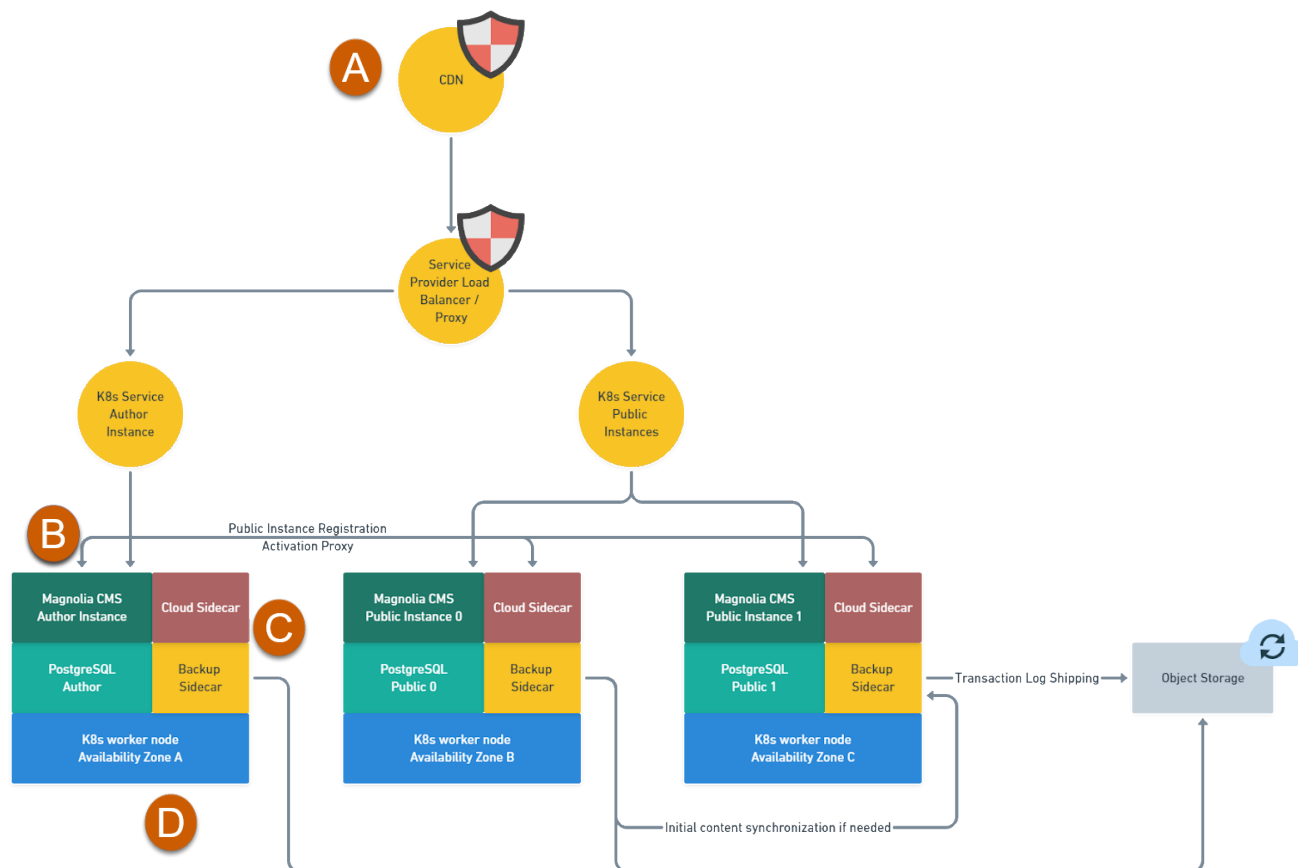
2.1. Technologies


The table below outlines the technologies per Magnolia Cloud Platform component.


Component	Technology	Multi-tenant	Hosted	Authentication
Platform	Kubernetes	n	AWS region(s)	IAM Solution
Cockpit	Magnolia and React	y	Private Switzerland	IAM with MFA
Monitoring & Logging	Prometheus and Loki	y	Private Switzerland	IAM with MFA
CDN	Fastly	y	Global network	Access token

Chapter 3. Magnolia Cloud Platform Architecture

Magnolia Cloud Platform uses [Kubernetes](#) for baseline orchestration of its environments. This is an **explicit** dependency. [Helm charts](#) are used to deploy releases on the Kubernetes cluster.



Item	Note
A	<p>The CDN is deployed between the end user and the Magnolia instances.</p> <div>  See the WAF and CDN section for more details. </div>
B	<p>Magnolia instances (<i>author/public</i>) are each deployed in a Kubernetes pod containing their own sidecars and K8s workers.</p>

Item	Note
C	<p>Sidecar containers are deployed to initialize containers before Magnolia CMS starts.</p> <div>  <p>Sidecars are secondary containers that focus on a specific task. They are placed in the same pod as the primary container because resources are shared. Typically sidecars come after the main container in the configuration so the main container is the default target for <code>kubectl execute</code> as shown in the example below (1):</p> <pre> apiVersion: v1 kind: Pod metadata: name: webserver spec: volumes: - name: shared-logs emptyDir: {} containers: - name: nginx image: nginx volumeMounts: - name: shared-logs mountPath: /var/log/nginx - name: sidecar-container ① image: busybox command: ["sh", "-c", "while true; do cat /var/log/nginx/access.log /var/log/nginx/error.log; sleep 30; done"] volumeMounts: - name: shared-logs mountPath: /var/log/nginx </pre> </div>
D	The K8s workers handle pod availability.

Chapter 4. WAF and CDN

This section contains important information related to the Web Application Firewall [WAF](#) and [CDN](#).

4.1. WAF

Magnolia Cloud Platform provides a **Web Application Firewall (WAF)** by default. This aligns with the [Open Web Application Security \(OWASP\)](#) Project's [core rule set](#). The Core Rule Set protects web applications from a common range of cyber attacks.

Top 10 attacks according to OWASP

- SQL Injection (SQLi)
- Cross Site Scripting (XSS)
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- PHP Code Injection
- Java Code Injection HTTPoxy
- Shellshock
- Unix/Windows Shell Injection
- Session Fixation
- Scripting/Scanner/Bot Detection
- Metadata/Error Leakages

4.2. CDN

The CDN oversees all bidirectional traffic (*encrypted and unencrypted*) between browsers and your web server and automatically filters all non-HTTP / HTTPS traffic at the global CDN nodes, blocking highly disruptive [Layer 3 \(network\)](#) and [Layer 4 \(transport\)](#) attacks.

Our CDN is deployed between the end user and the Kubernetes Ingress objects.



Load balancing and failover is done inside the Kubernetes cluster with help of the deployed [Ingress Controller](#).

We protect against

- Ping floods
- ICMP floods

- Reflection / amplification attacks
- Transaction floods
- Resource exhaustion
- UDP abuse

Using [Varnish Configuration Language \(VCL\)](#), we apply rules to protect your network from complex [Layer 7 \(application\)](#) attacks.

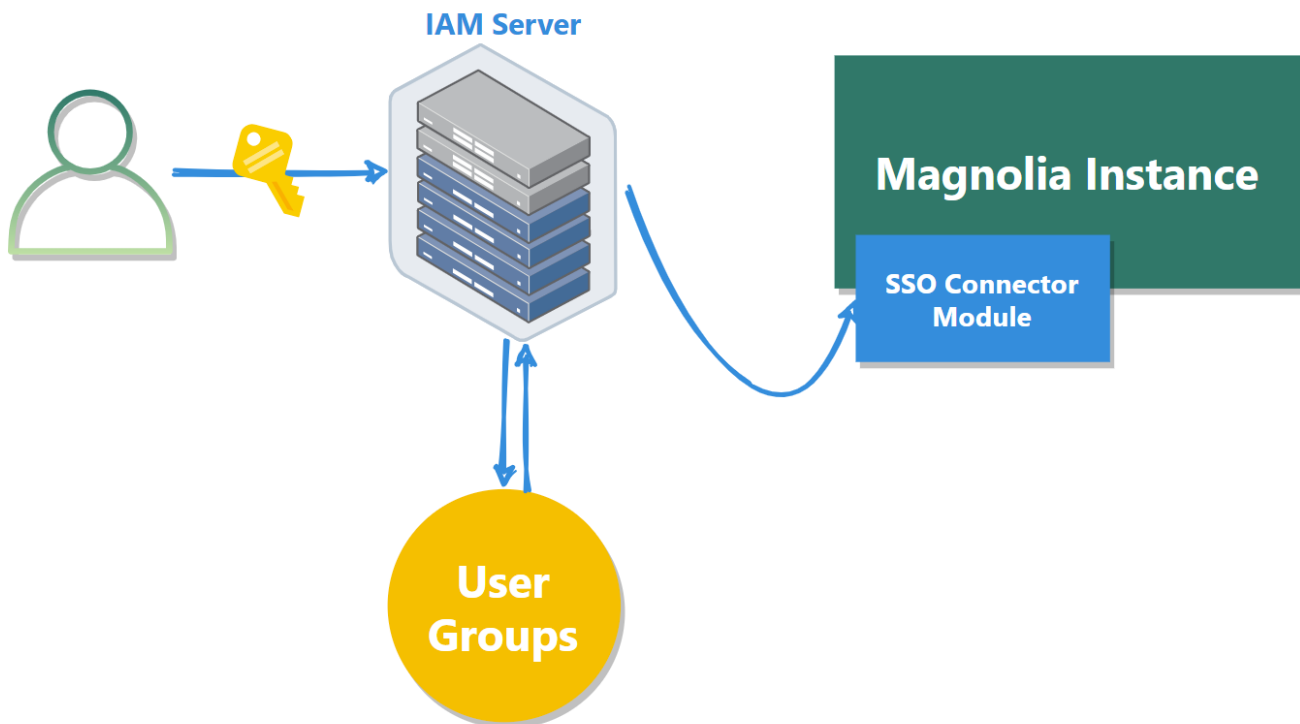


We inspect the entire HTTP / HTTPS requests, and block attacks based on client and request criteria such as headers, cookies, request paths, and client IP, or indicators such as geolocation.

Chapter 5. Identity and Access management

Magnolia Cloud Platform uses an **Identity and Access Management (IAM)** server that adheres to **OIDC** standards and protocol. User authentication is handled based on this OIDC approach.

Users are provided with Magnolia credentials that enable Single sign-on (SSO) for all Magnolia products and solution the customer has purchased or uses.



5.1. Authentication

Authentication occurs using our IAM server solution, which is separated from the Magnolia instance. The IAM server recognises Magnolia as a validated client application and thus the users can authenticate with this method. Magnolia uses the SSO Connector Module to interact with the IAM server.

The SSO setup involves registering Magnolia as a client application and providing the configuration details necessary such as the **client ID**, **client secret**, and **callback URL**.

User Access

User access is protected using industry-standard security settings such as:

- Multi-factor authentication (OTPs)
- Password security settings
- Blacklisting



Magnolia's IAM solution is able to integrate with existing IAM solutions.

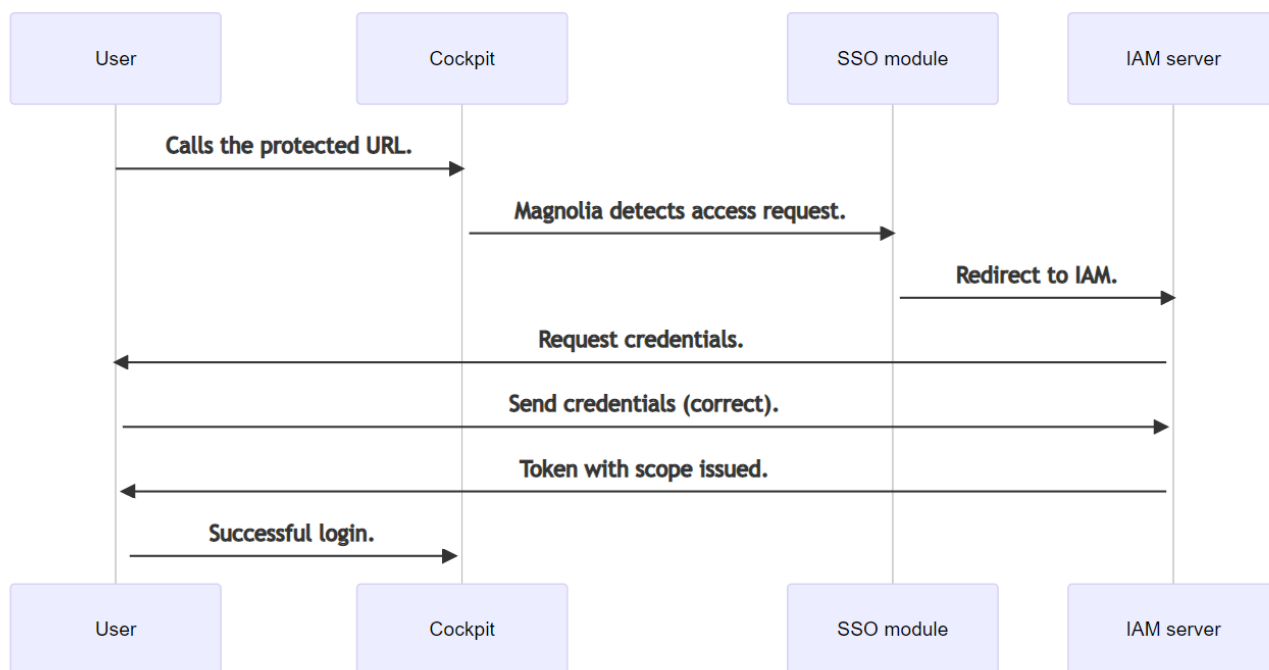
5.2. Authorization

User accounts and their associated roles are managed in workspaces. Each customer/partner has their own workspace. Because of this, customer-specific configuration is possible without impacting other existing configuration.

Permissions are based on group and role assignments. These assignments are handled in the IAM server before allowing access to the Magnolia instance.

5.3. Cockpit

Users connect to the Cockpit via a custom JSON Web Token implementation. This is an additional layer of security on top of the IAM server solution.

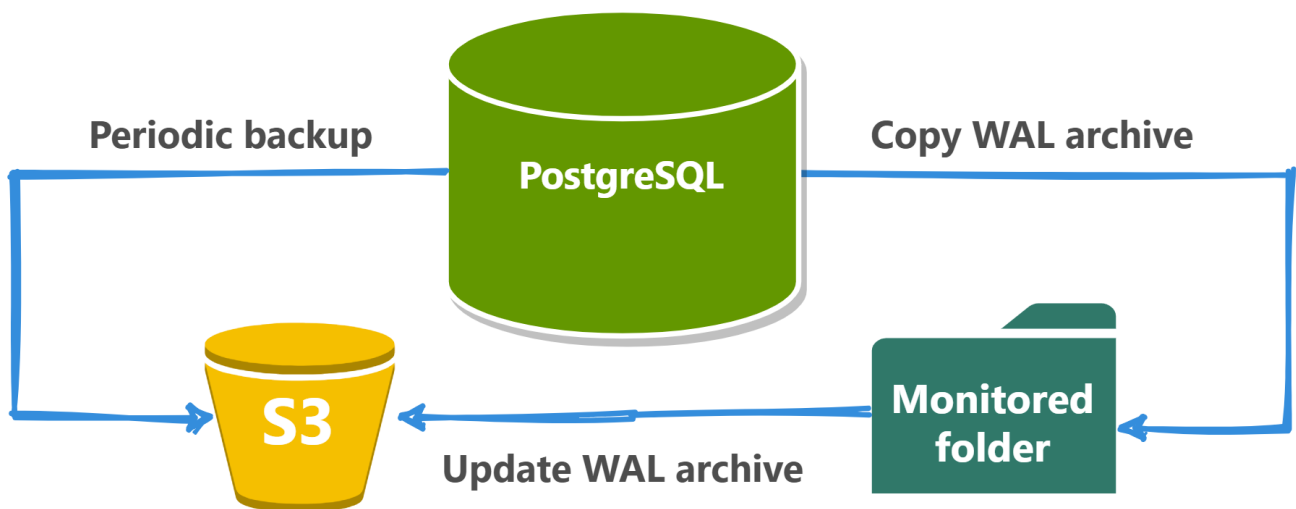


Chapter 6. Database

Magnolia Cloud Platform users [PostgreSQL](#) as its default database. The database ships transaction logs to the [S3 bucket](#) in defined intervals or as soon a configured threshold is met regarding the delta in data.

Each Magnolia instance (e.g., `public1`, `public2`) has a provisioned database. Some of the benefits of this are:

- increased backup performance
- reduced resource usage on the storage target
- point-in-time recovery



Good to know

This approach allows you to rapidly replicate new instances out of existing instances.

Appendix A: GDPR

For Magnolia Cloud Platform, Magnolia is the [processor](#) and you (the customer) are the [controller](#). Magnolia hosts your site(s) in the cloud and collects, stores, and processes data on your behalf.



As the data controller, you are responsible for GDPR compliance.

Hosting GDPR

Each underlying hosting provider has their own GDPR compliance commitment. Here are a few:

- [AWS](#)
- [Azure](#)
- [Google Cloud](#)

Item	Notes
Controller-Processor relationship	To define the relationship between Controller and Processor, Magnolia and the Cloud Platform customer enter in a “Data Protection Agreement”. Such agreement states how information will be handled, the legal basis of processing, the technical measures implemented by the processor, the code of conduct and the cloud user protection requirements.
Security measures	Magnolia Cloud Platform implements appropriate measures that ensure a level of security on the cloud. These measures ensure ongoing confidentiality, integrity, availability and resilience of the processing system and the ability to restore and access personal data in case of an incident. Magnolia tests the effectiveness of the technical and organizational measures in order to ensure security of processing and provide a safe information hosting environment for our customers and their end users.

Item	Notes
Data location	<p>Location of the data is one of the most important elements under GDPR. Magnolia Cloud Platform is available in multiple Regions around the world. The location however, is chosen by the customer, by selecting the Main Data center and Satellite Data centers (if applicable). Considering that the GDPR requirements cover organizations that operate within the EU or process data of EU citizens, data mapping and location identification activities must be considered. Magnolia Cloud Platform ensures that information is stored in safe locations and that agreements with the state in which it operates exist. Those insurances are based on the commitment of the underlying Hosting Provider, which are selected only if compliant to the GDPR guidelines.</p>

Appendix B: Auditing and certification

Magnolia conducts yearly security audits which are assessed from an external and independent security consultant firm based in Switzerland.

What does the audit consist of?

- Revision of the security concepts provided by Magnolia
- Multiple penetration tests (both anonymous and as a customer). A recheck is done to validate the reaction on potential vulnerabilities.
- Major releases of the Magnolia CMS is subject to its own risk and security assessment.

magnolia®