circularo

Infrastructure Recommendations and Requirements

For Circularo on-premise deployment running Kubernetes

Date: 27.6.2025

Introduction

This document outlines the infrastructure requirements and deployment prerequisites for running the Circularo platform in an on-premise environment. It is intended to guide customer infrastructure teams in preparing a production-ready setup that ensures high availability, performance, and scalability.

Circularo leverages a lightweight Kubernetes distribution (K3s) to orchestrate services across a distributed cluster. This modern architecture eliminates the need for dedicated application or database servers, enabling uniform roles for all participating nodes. With built-in support for service resilience and load balancing, the platform is capable of maintaining continuous operation even in the event of a node failure.

The specifications provided here reflect the minimum standard for a typical deployment and are consistent across environments to simplify maintenance and support. They are designed to handle a workload of up to 150 concurrent users. While these guidelines provide a solid foundation, the deployment can be scaled to meet higher demands or tailored to accommodate specific customer infrastructure requirements.

By following these recommendations, customers can ensure a smooth deployment process and establish a reliable environment for running Circularo on-premise.

Hardware Requirements

To ensure a robust, scalable, and highly available deployment of Circularo on-premise, the infrastructure must consist of the following:

- **3 production servers** (required)
- **1 test/staging server** (optional but recommended)
- **(Optional) DMZ proxy server(s)** for load balancing (high-availability), network segmentation or external access control*

*While the DMZ server is not strictly required for running the application, it is strongly recommended. It ensures continued external accessibility even in the event of a node failure.

A **minimum of three identically configured production servers** is required to support Circularo's high availability model. This setup forms the backbone of the Kubernetes (K3s) cluster, ensuring redundancy and seamless workload distribution. Unlike traditional deployments with dedicated roles (e.g., application or database servers), all nodes in this architecture are functionally equivalent. They collectively run services, balance traffic, and manage failover scenarios.

K3s manages orchestration, service distribution, and resilience across the cluster. In the event of node failure, workloads are automatically rescheduled to healthy nodes, ensuring minimal disruption. The Elasticsearch database is deployed across all three nodes in a replicated, distributed fashion, preserving data integrity and availability even when one node is down.

Recommended Specifications (Per Server)

These hardware recommendations are optimized for standard deployments and support approximately **150 concurrent users**:

- **CPU**: 6 vCPUs
- **Memory**: 24 GB RAM
- **Local Storage**: 64 GB SSD
- **Network Storage**: Shared NFS storage (optional for UAT, **must support xattr)** of at least 100 GB accessible to all nodes.

All servers must be deployed within the same network segment, with **no firewalls or filtering** between them to allow unrestricted internal communication. Time synchronization across nodes (e.g., via NTP) is critical to ensure consistent operation of the Kubernetes cluster.

For larger deployments or environments with greater user concurrency, these resources can be scaled horizontally by adding more nodes or vertically by increasing CPU, memory, or storage on each node.

Software requirements

Operating System

All servers participating in the Circularo deployment must run a **Linux-based operating system**, with **Debian** as the recommended distribution.

To ensure the successful installation of system packages and Circularo dependencies, the operating system must have a **fully functional package manager**. This includes reliable access to official Debian repositories. The ability to run `apt-get` and `apt update` commands without errors is essential for both the initial setup and ongoing system maintenance.

Additional Requirements

To support a smooth installation and secure operation of the platform, the following additional software prerequisites must be fulfilled:

- **Root-level (sudo) access** must be available on all servers to perform administrative tasks during installation and maintenance.
- **SMTP server credentials** must be provided to enable email notifications from the Circularo platform.
- **DNS configuration** must be established to allow users to access the application via a consistent and user-friendly domain name.
- A valid **SSL certificate** must be supplied for the configured DNS to ensure secure HTTPS access to the system.

These requirements are critical to the reliability, security, and operational readiness of the Circularo deployment environment.

Network settings

All servers in the production cluster are required to be on the same network. It is also recommended to leave all ports open. The following ports are the minimal required to be open

Port	Reason
80/443	HTTP application interface

Internet Access Requirements

While **full internet access is recommended** for a smooth installation and update process of the Circularo platform, only a specific subset of outbound connections is strictly required. These connections enable installation, updates, container image retrieval, identity provider integration, certificate validation, and operational tools - such as the Envoy Gateway Controller and Elasticsearch Operator. The following table outlines all mandatory internet destinations, including associated ports and purposes:

Domain/URL	Port(s)	Purpose
*.github.com *.githubusercontent.com	80/443	Required by K3s/Helm installation scripts
get.k3s.io	443	K3s installation script
elastic.co, helm.elastic.co	443	Elasticsearch Operator (ECK) charts and CRDs

gateway.envoyproxy.io	443	Envoy Gateway Controller charts and configuration
quay.io, *.github.io	443	Container image registry used by some Helm charts and operators
login.microsoftonline.com	80/443	Microsoft Azure AD authentication
*.vault.azure.net	443	Azure Key Vault access for HSM/secrets
crcircularo.azurecr.io, *.westeurope.data.azurecr.io	443	Circularo application image registry
*.uaepass.ae	80/443	UAE Pass national identity integration
iamservices.semati.sa	80/443	Nafath authentication
*.ica.cz	80/443	I.CA digital certificate validation
*.postsignum.cz	80/443	PostSignum certificate authority validation

*.desc.gov.ae	80/443	DESC certificate authority validation
*.ica.gov.ae	80/443	ICA certificate validation
registry-1.docker.io, docker.io	443	Fallback container images and dependencies
widget.identomat.com	80/443	KYC liveness detection

Note: If your environment uses firewalls, proxies, or strict egress controls, ensure that access to these domains is explicitly permitted.

These network requirements ensure full operational capability of Circularo, supporting its Kubernetes-based architecture, container lifecycle management, integration with external services, and secure communication with third-party systems.

Installation and remote access

To facilitate on-premise installation and ongoing maintenance of the Circularo platform, the Circularo team requires remote access to the infrastructure.

Direct SSH access to the application servers is strongly preferred, as it provides the highest level of flexibility and efficiency for performing installation, troubleshooting, and maintenance tasks. This method allows our team to work swiftly and independently across the environment.

Alternatively, **indirect access via a bastion host** or through **monitored SSH sessions** is also acceptable, provided it allows sufficient administrative capabilities to complete all required tasks.

However, access methods involving **screen sharing tools** such as Microsoft Teams, Cisco WebEx, or similar platforms are not suitable. These approaches limit the efficiency and effectiveness of our deployment and support operations, and therefore **will not be accepted** as a viable method of access.