

# Legende

Titel

Der Titel steht bei jedem Themenbereich an vorderster Stelle. Dadurch wird eine bessere Orientierung gewährt.

Entscheidung

Zu treffende Entscheidungen werden durch prägnante Entscheidungssätze beschrieben.

Entscheidungsmöglichkeit

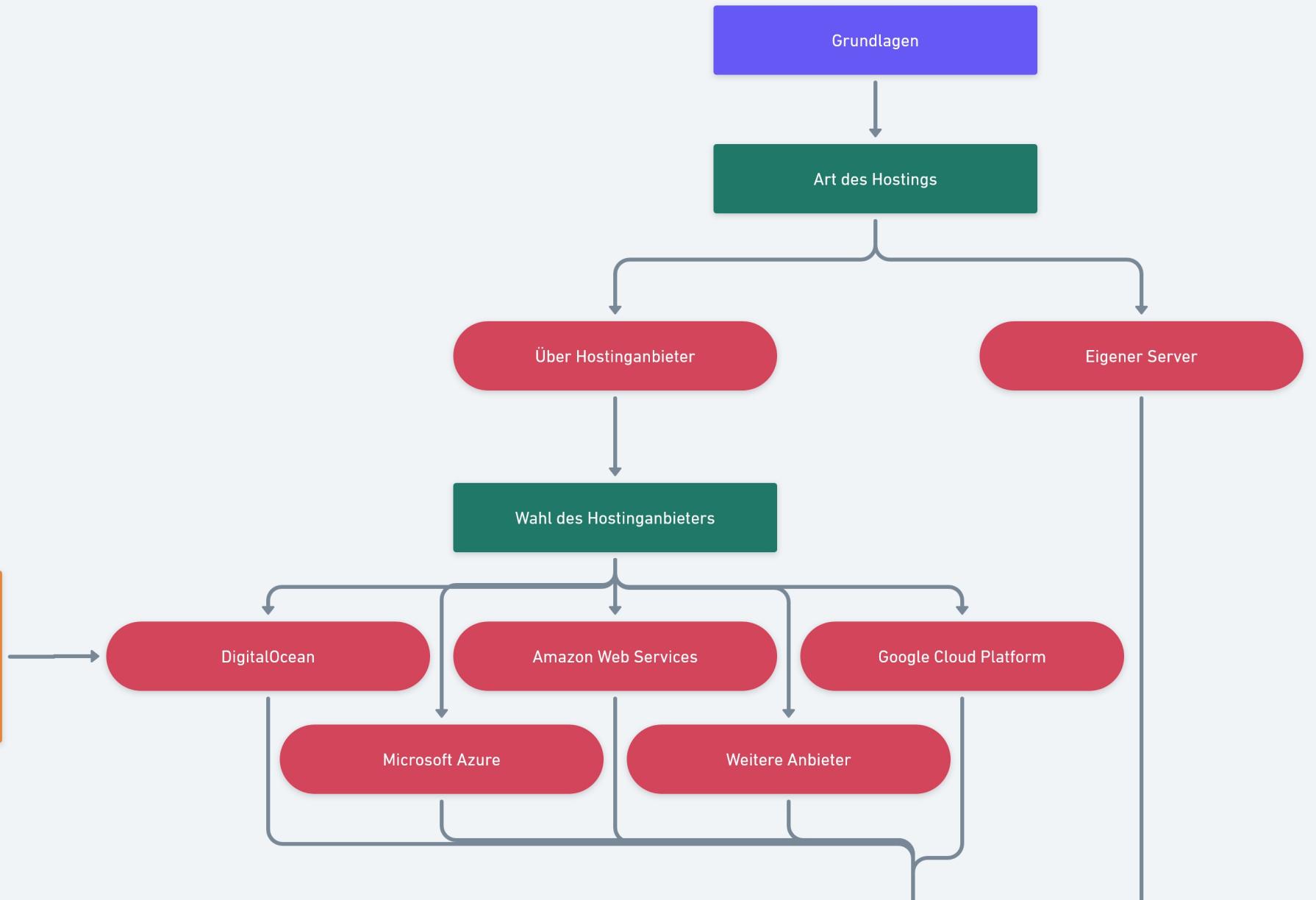
Jede Entscheidungsmöglichkeit wird als ein eigenes Element dargestellt.

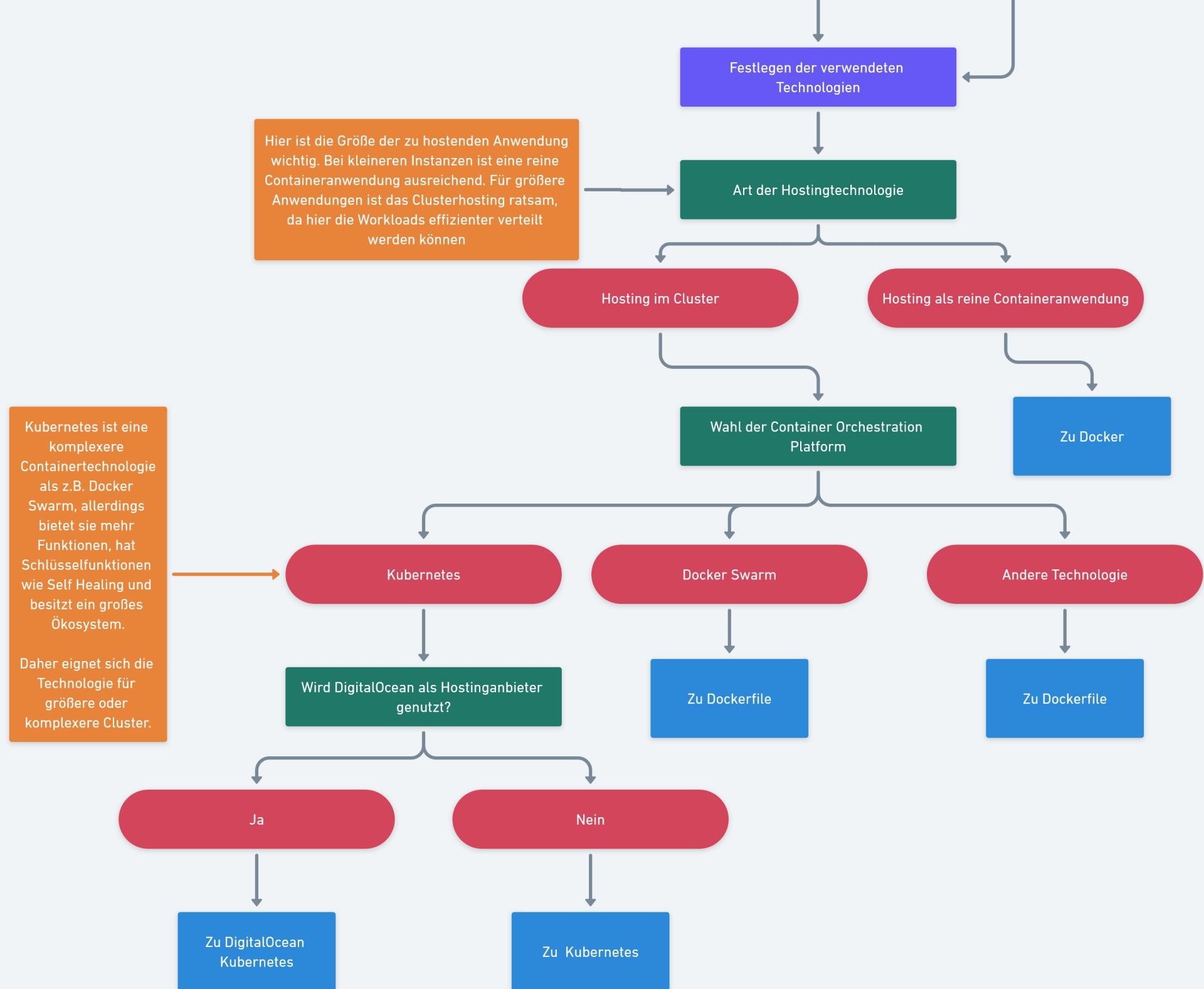
Inhaltsverweis

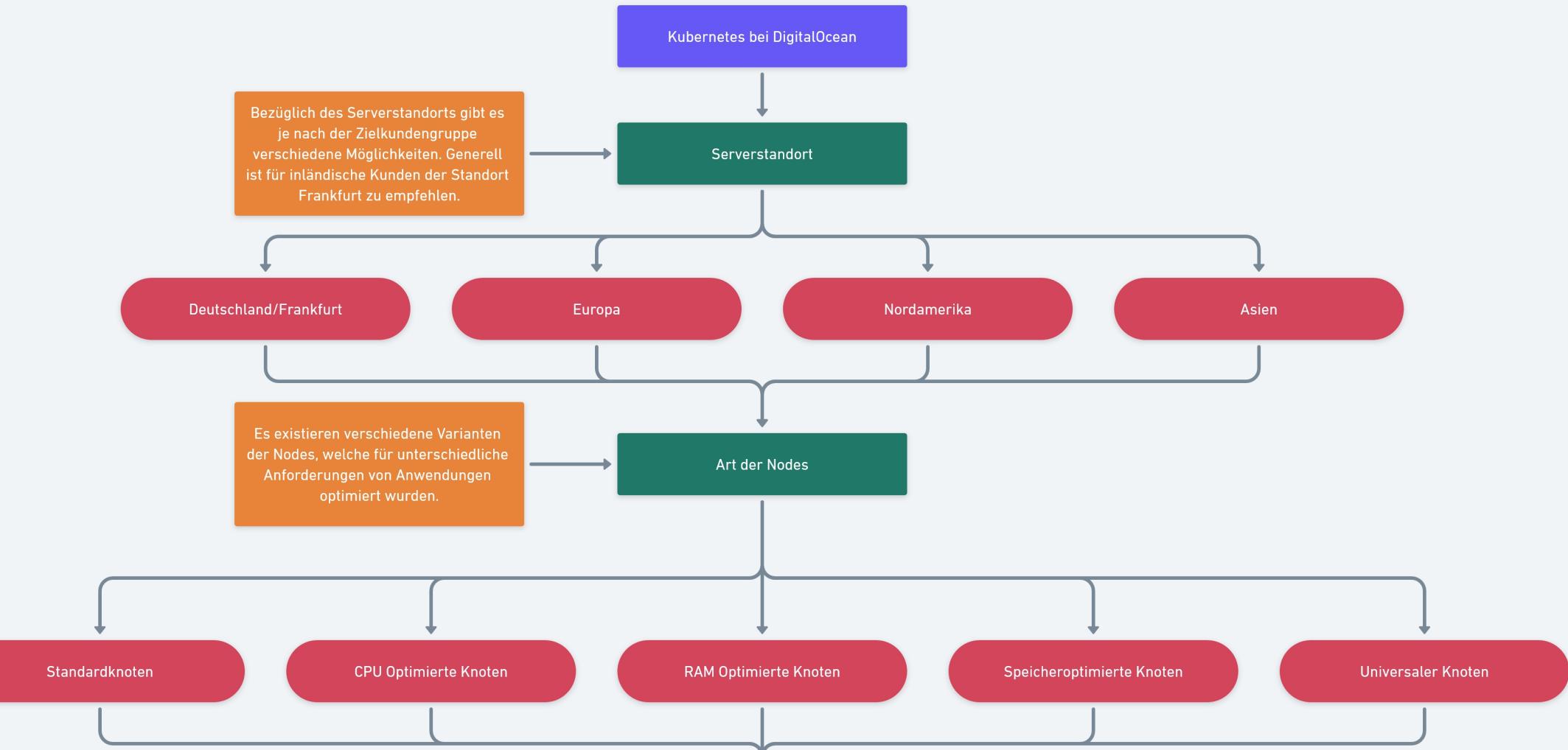
Wenn im Entscheidungsprozess an eine andere Stelle gesprungen werden soll, wird diese durch einen Inhaltsverweis angegeben.

Anmerkung

Einige Elemente im Entscheidungsfinder werden mit Anmerkungen versehen, damit ein größerer Kontext und weitere hilfreiche Informationen gegeben werden können.







Es existieren verschiedene Angebote an Rechenleistung. Diese sind in den grundlegenden Plan (1-2 Gb Ram und 1-2 vCPUs) und den Premium Plan (6-13 Gb Ram und 4-8 vCPUs) unterteilt.

### Leistung der Nodes

Grundlegend

Premium

Automatisches Hinzufügen und Entfernen von Knoten, wenn keine Pods mehr geschedulet werden können.

### Autoscaling

Ja

Nein

Erhöhung der Zuverlässigkeit kritischer Workloads. Der Preis dafür beträgt 40\$. Nach der Wahl der Option ist diese nicht mehr kündbar.

### High Availability

Ja

Nein

Wenn über das Comand Line Interface eine Verbindung hergestellt werden soll, muss dafür ein Zertifikat im System hinterlegt werden. Das Zertifikatmanagement lässt sich entweder automatisiert oder manuell ausführen. Manuell hinterlegte Zertifikate sind jeweils eine Woche gültig.

## Zertifikatmanagement

Automatische Erneuerung

Manuelle Erneuerung

## Automatische Updates von Kubernetes Minorversionen

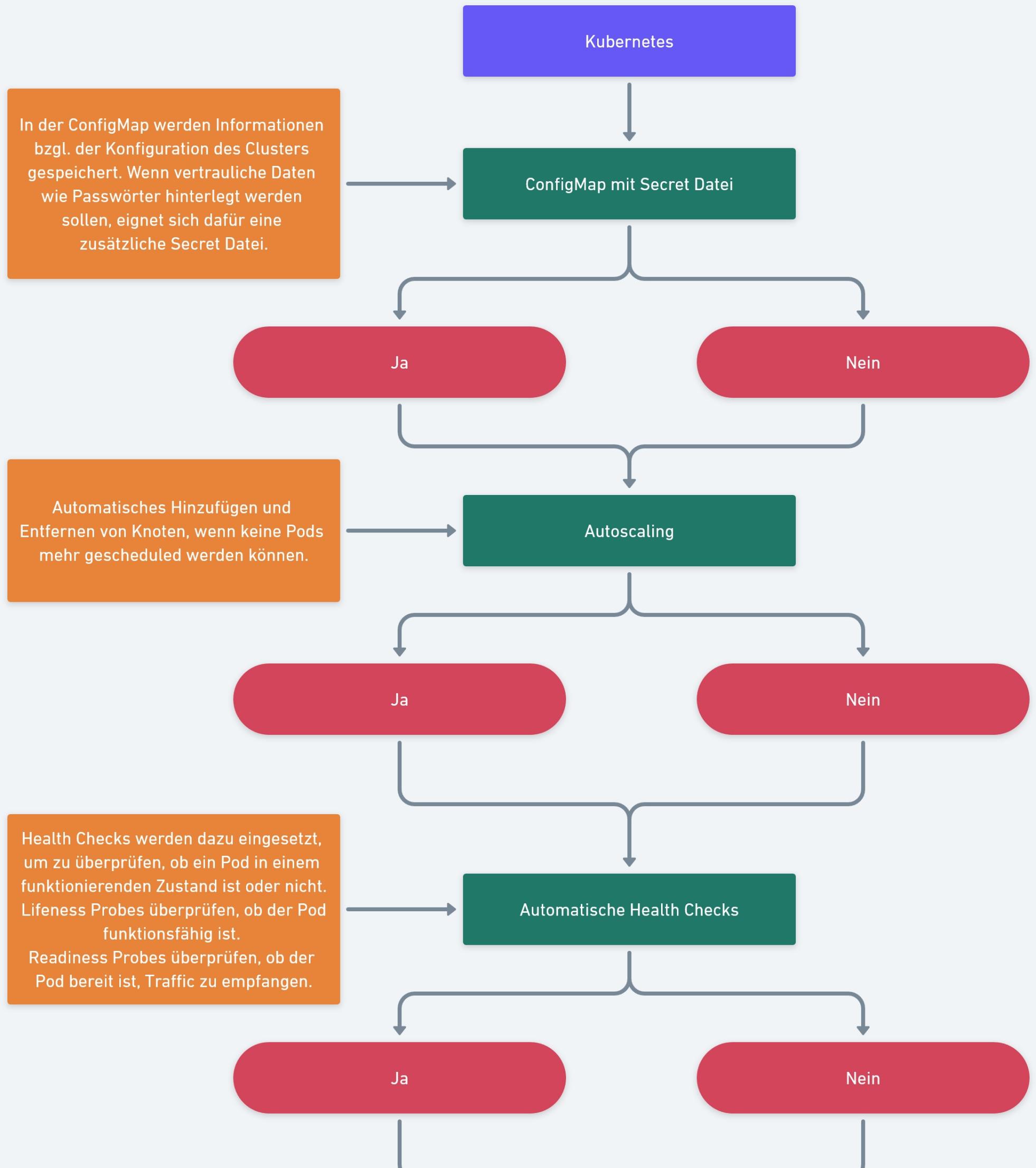
Ja

Nein

Grundlegende Kennzahlen beinhalten die CPU Nutzung, den Belastungsdurchschnitt oder die Bandweite. Erweiterte Metriken bieten Kennzahlen zum Status des Deployments.

## Detailgrad der Kennzahlen

Zu Kubernetes



Im Falle eines Ausfalls von Komponenten kann durch Redundante Nodes, Load Balancing oder Self Healing dennoch der Service fehlerfrei angeboten werden.

## High Availability

Ja

Nein

Für einen möglichen Ausfall können Backupdaten erstellt werden. Anwendungsdaten lassen sich in einer externen über das Cluster werden in dem etcd Verzeichnis gespeichert. Außerdem können Backupools wie z. B. Velero genutzt werden.

## Backup

Ja

Nein

Um eine gute Übersicht über das Clusterhalten zu erlangen, sollten die Logs der Nodes und Pods an einem zentralen Ort gespeichert werden, um deren Auswertung zu vereinfachen. Beispiele für Loggingtools sind Graylog oder Fludentd.

## Central Logging

Ja

Nein

Über das einzufügende Kubernetes Dashboard lassen sich wichtige Daten wie die CPU Nutzung in einer grafischen Benutzeroberfläche auswerten. Außerdem können andere Tools wie Prometheus genutzt werden.

### Central Monitoring

Ja

Nein

Wenn mehrere Nutzer\*innen administrativ am System beteiligt sind, ist es hilfreich, über eine Protokoll festzuhalten, wer an der Anwendung Änderungen durchgeführt hat.

### Central Audit

Ja

Nein

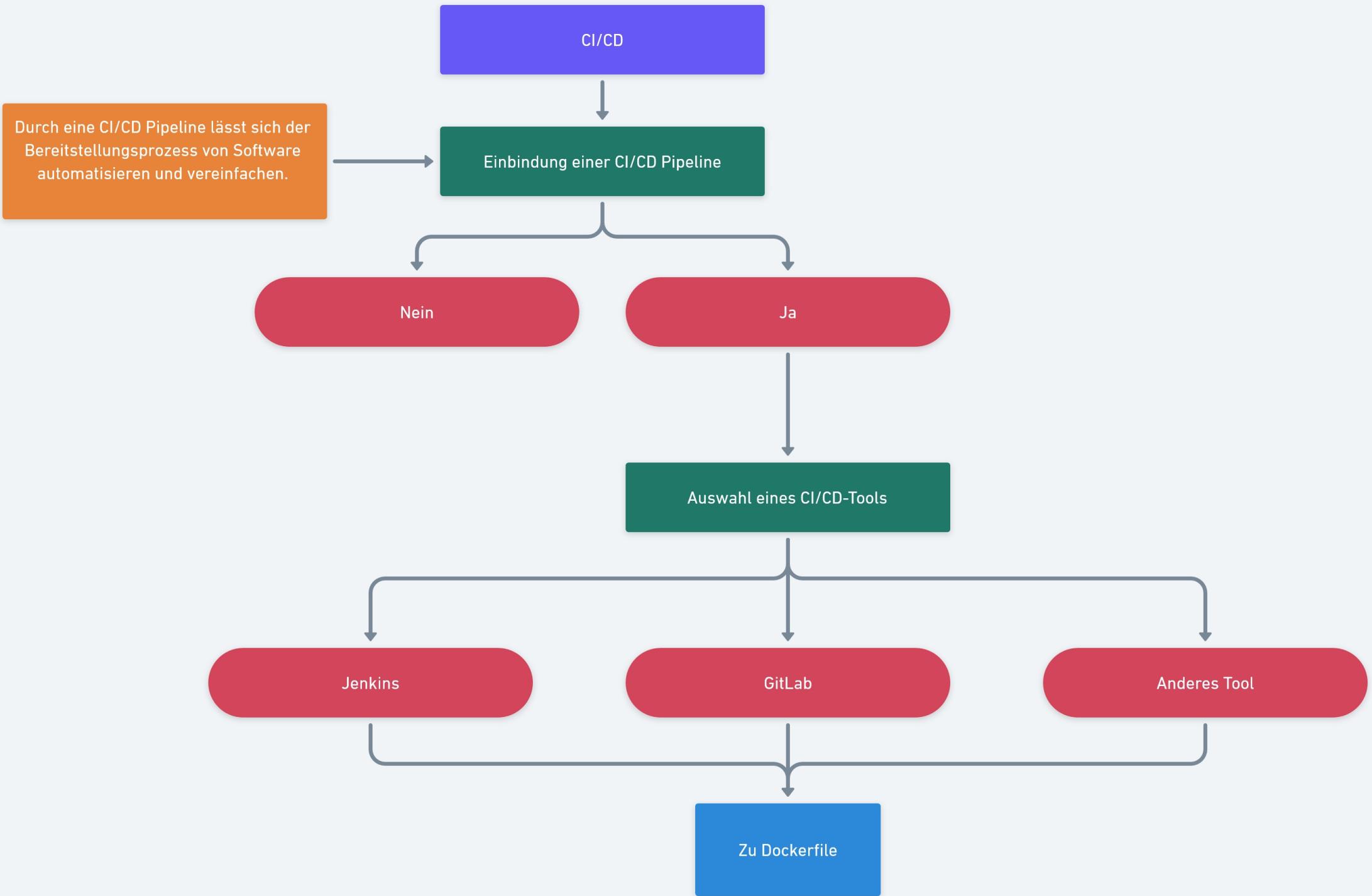
Neuer Code und Konfigurationsdateien können direkt über ein Git-Repository implementiert und geupdatet werden.

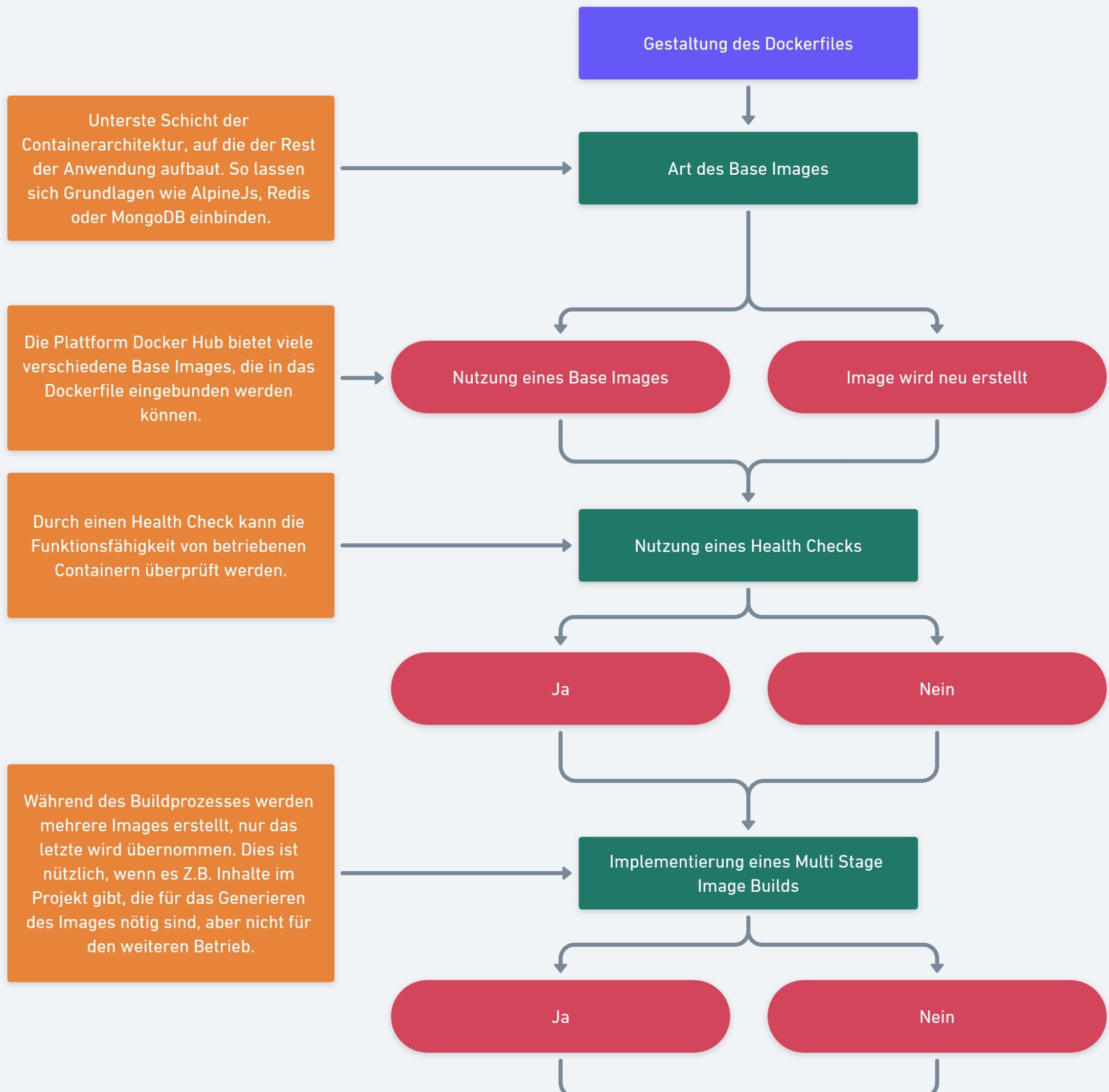
### Automated Operations

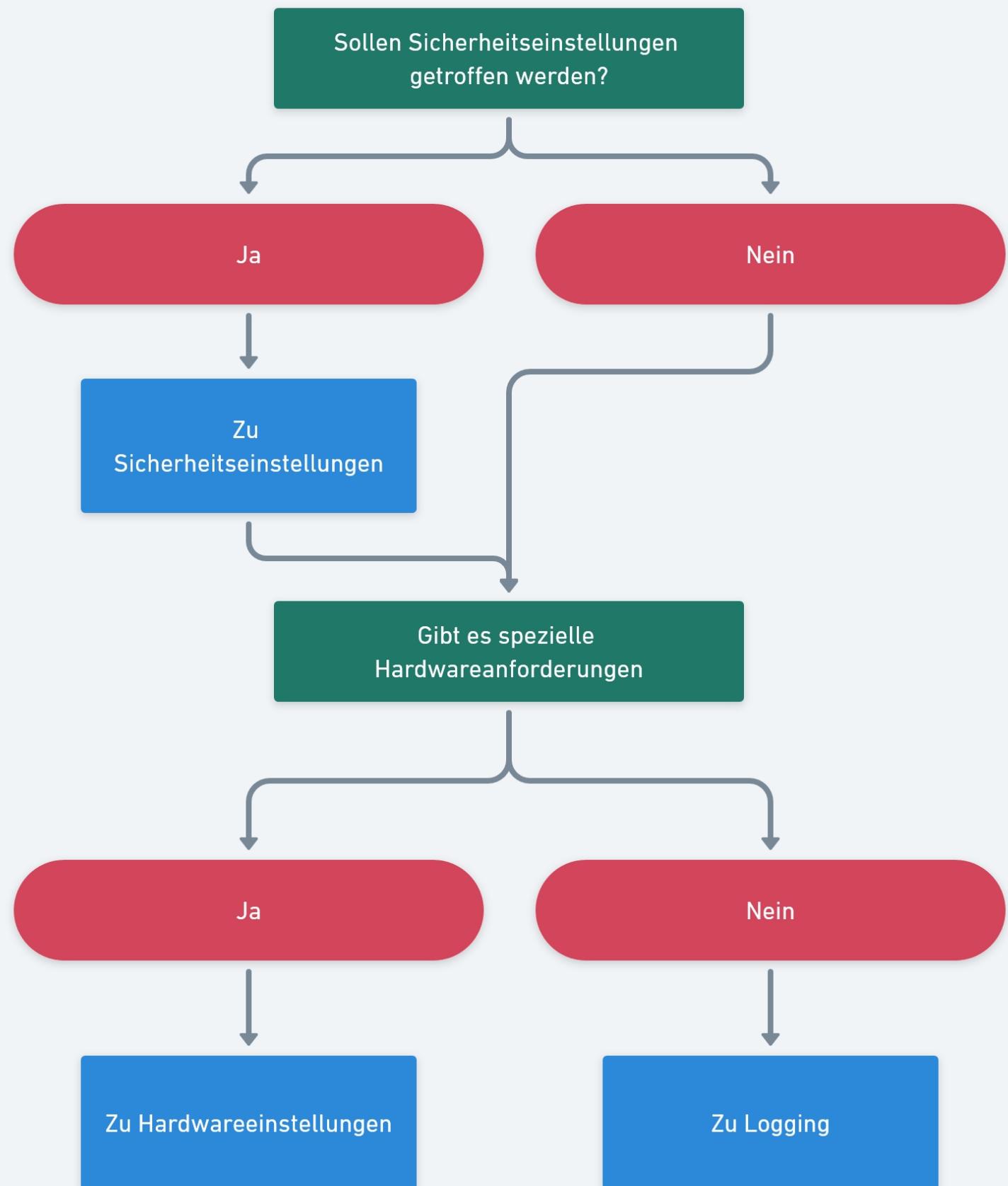
Ja

Nein

### CI/CD







Sicherheit

Container sollten nur in Ausnahmefällen als Privileged konfiguriert werden. Denn einem als privileged eingestellten Container ist eine volle Zugriffserlaubnis auf alle Instanzen erteilt. So wird ein Zugriff auf alle Geräte im Hostsystem ermöglicht

Container als Privileged

Nein

Nein

Es werden sicherheitsrelevante Beschränkungen an Containern durchgesetzt, wodurch diese effizienter voneinander abgegrenzt werden. Hierfür kann SELinux, Apparmor, oder Seccomp genutzt werden.

Nutzung der Mandatory Access Control

Ja

Nein

Durch das Definieren als Read Only wird es Außenstehenden erschwert, Änderungen an den Daten im System vorzunehmen.

Filesystem als Read Only

Docker Desktop

Docker Toolbox

Durch Sicherheitsguidelines kann der Erstellungsprozess von Containern sicherer gestaltet werden. Beispiele für mögliche Guidelines sind regelmäßiges Auditing oder das ausschließliche Benutzen von vertrauenswürdigen Registries.

## Sicherheitsguidelines

Ja

Nein

Bei Images mit sensiblen Nutzerdaten ist es empfehlenswert, anstatt eines öffentlichen Registries ein privates zu verwenden, um Zugriffen auf die Daten vorzubeugen.

## Registryverwaltung

Privates Registry

Öffentliches Registry

Durch den Einsatz von etables kann der Traffic genauer gefiltert werden, der durch die Ethernetbridge geleitet wird.

## etables

Ja

Nein

Zurück zu Dockerfile

Es werden x86, x86-64, ARM, ARM64, PowerPC LE und IBMs POWER und Z Architekturen unterstützt. Bei Docker Hub lassen sich Base Images nach deren Architektur filtern.

Eine Anpassung der Reboothäufigkeit der Anwendung führt zu einer Verringerung des Software Agings

Es lassen sich Software Guard Extensions aktivieren, welche Remote Computing auf nicht vertrauenswürdigen fremden Geräten durch gesicherte Container ermöglichen.

Hardwareeinstellungen Docker

Wird eine spezielle CPU Architektur vorausgesetzt?

Ja

Nein

Treten Probleme mit Software Aging auf?

Ja

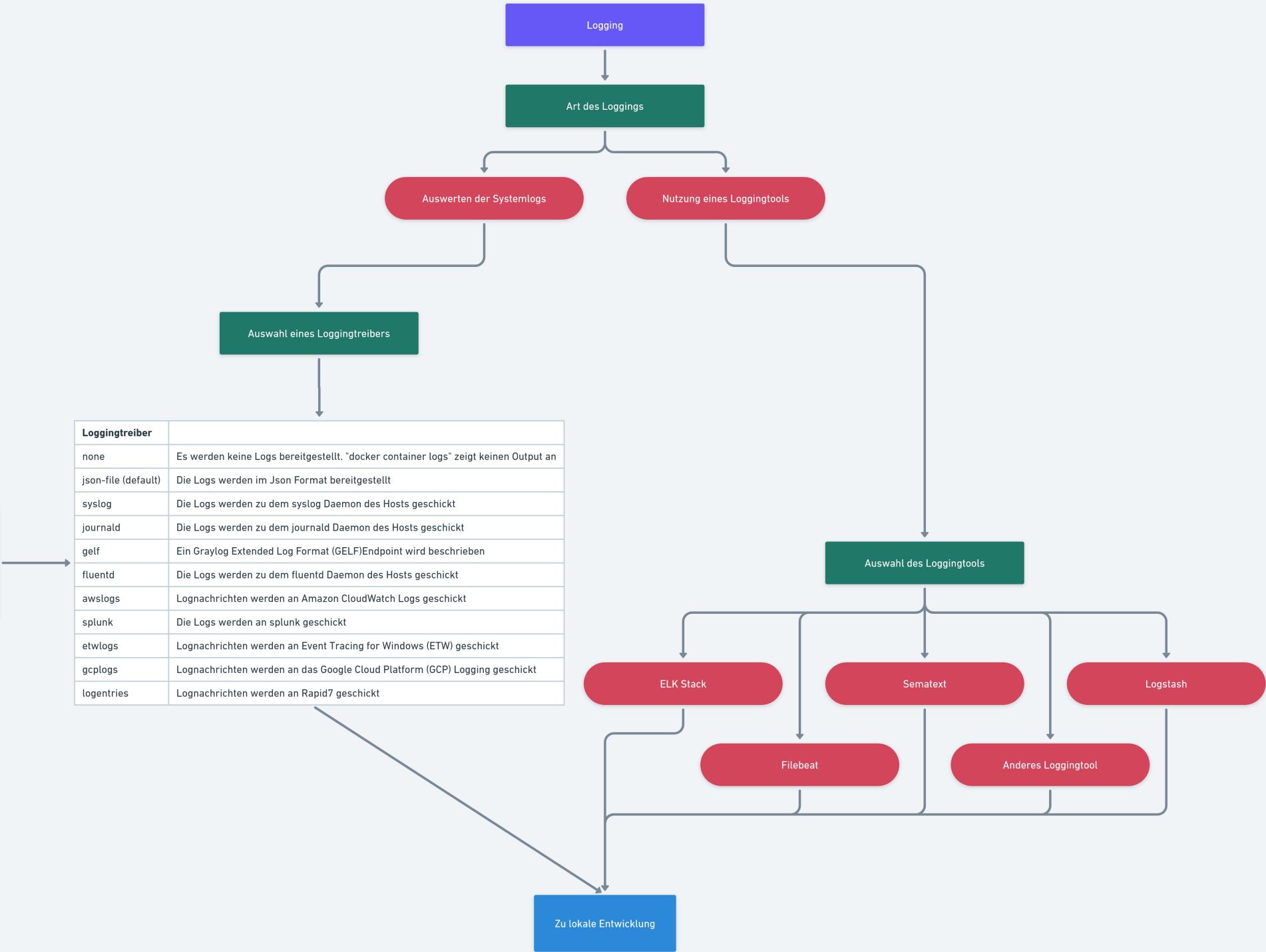
Nein

Wird Remote Computing durchgeführt?

Ja

Nein

Zu Logging



Docker Desktop ist ein Programm zum Management von Containeranwendungen. Durch seine grafische Oberfläche bietet es eine bessere Übersicht als das Command Line Interface.

Lokale Entwicklung

Nutzung von Docker Desktop

Ja

Nein

Bei älteren Betriebssystemen ist Docker Desktop nicht verfügbar. Stattdessen kann Docker Toolbox eingesetzt werden. Bei macOS ist die Mindestanforderung Version 10.15. Bei Windows muss mindestens Windows 10 genutzt werden.

Docker Desktop vs Docker Toolbox

Docker Desktop

Docker Toolbox



Minikube ist eine Implementierung von Kubernetes, welche durch die Nutzung einer virtuellen Maschine den lokalen Einsatz von Kubernetesclustern ermöglicht. Auch Docker Desktop hat die Funktion inne, Cluster zu betreiben.

Soll beim Einsatz von Kubernetes minikube installiert werden?

Ja

Nein

Docker Community ist kostenlos und für Entwickler konzipiert. Die Enterprise Version ist eine Container as a Service Lösung, welche mit der Universal Control Plane ein Interface zum Managen von Containern und Containerclustern bietet.

Docker in der Enterprise oder Community Edition

Hiermit ist der Durchlauf des Entscheidungshelfers abgeschlossen. Viel Erfolg bei der Umsetzung der Containerisierung des Systems. Für die Unterstützung der Implementierung wurden Cheatsheets zu Docker und Kubernetes erstellt.

Ende des Entscheidungshelfers

Zu Docker  
Cheatsheet

Zu Kubernetes  
Cheatsheet