03 · BETREIBEN · DEVOPS

Wir bauen eine automatisierte, nachvollziehbare und sichere Pipeline vom Code bis zur Produktion.

Mit Enterprise-Kubernetes-Plattformen, CI/CD-Pipelines und Infrastructure as Code beschleunigen wir die Softwarebereitstellung und machen den Betrieb wiederholbar. Ob Ihre Plattform in Ihrem Rechenzentrum oder in der Cloud läuft – wir unterstützen Sie von der Installation bis zum 24/7-Betrieb.

DAS PROBLEM, DAS WIR LÖSEN

Jedes Release bedeutet eine lange Nacht und manuelle Schritte.

Konfigurationsunterschiede zwischen Umgebungen führen zu Fehlern.

Die Entscheidung für Container ist gefallen, aber es ist unklar, wer die Plattform betreiben wird.

LEISTUNGSUMFANG

DevOps in Ihrem Rechenzentrum (On-Premises)

Aufbau und Betrieb einer durchgängigen DevOps-Plattform in Ihrem Rechenzentrum – auch in Umgebungen ohne Internetverbindung.

Kubernetes

Aufbau, Absicherung und Betrieb von Enterprise-Kubernetes-Plattformen.

CI/CD-Pipeline

Automatisierte, nachvollziehbare Deployment-Pipelines vom Code bis zur Produktion.

Container-Transformation

Containerisierung von Anwendungen und deren Verlagerung auf Orchestrierungsplattformen.

Infrastructure as Code

Wiederholbares Infrastrukturmanagement mit Terraform und ähnlichen Tools.

GitOps

Verwaltung von Infrastruktur- und Anwendungskonfigurationen mit git-basierter Versionskontrolle.

Observability

Durchgängige Observability durch das Zusammenspiel von Logs, Metriken und Traces.

TECHNOLOGIEN

Kubernetes · Terraform · GitOps · CI/CD · Prometheus · Grafana

SCHNELLSTART

Paket	Dauer	Ergebnisse
Kubernetes Health Check	5 Werktage	Befundbericht und Maßnahmenplan

Kostenloses Erstgespräch

In 45 Minuten lernen wir Ihre Umgebung und Ihre Prioritäten kennen. Kostenlos.

KONTAKT

info@turncloudon.com

0850 346 30 49

www.turncloudon.com.tr/de/uzmanlik/devops

Istanbul · Ankara · Konya · Prag

LEICHT AUFZUSETZEN, SCHWER ZU BETREIBEN

Architektur und Aufbau

- Vanilla Kubernetes, RKE2, OpenShift oder EKS/AKS/GKE
- Hochverfügbare Control Plane mit drei Knoten
- Cilium oder Calico; Default-Deny-Kommunikation über Network Policies
- Ceph, Longhorn oder Cloud-Disk-Treiber
- NGINX Ingress oder Gateway API, TLS-Automatisierung

Täglicher Betrieb

- Geplante, stufenweise Versions-Upgrades mit Rollback-Plan
- Backups mit etcd-Snapshots und Velero
- Namespace-Isolation, Ressourcenquoten
- Abstimmung von HPA, VPA und Cluster Autoscaler
- Zyklus aus Node-Draining, Patching und Image-Erneuerung

Sicherheit und Kosten

- RBAC-Design und Least-Privilege-Prinzip
- Durchsetzung von Richtlinien mit Pod Security Standards und OPA/Kyverno
- Einschränkung von Image-Quellen und Signaturprüfung
- Anpassung von Ressourcen-Requests/-Limits an die tatsächliche Nutzung
- Kostenzuordnung pro Namespace

MESSBARE ZUSAGE

Eine Cluster-Wiederherstellungsübung aus einem etcd-Backup wird mindestens zweimal jährlich durchgeführt, ihre Dauer gemessen und berichtet. Einen nicht geübten Wiederherstellungsplan betrachten wir nicht als Zusage.

LÖSUNGSDETAILS

Referenz-DevSecOps-Pipeline	Sichere Delivery-Pipeline in 12 Schritten vom Quellcode bis zum GitOps-Deployment, mit einem Gate in jedem Schritt.
Infrastructure as Code und Konfigurationsmanagement	Provisionierung mit Terraform/OpenTofu, Konfiguration mit Ansible; Drift-Erkennung und Policy-Prüfung.
Quellcode- und Artefaktmanagement	Einrichtung von GitLab/Gitea, Harbor/Nexus/Artifactory; Signierung, SBOM und lokaler Cache.