

Hans Jörg Wieland

DevOps / Systems Engineer

- ☎ +49 15123 583787
- ✉ mail@wieland.tech
- 🌐 <https://wieland.tech>
- 🏠 Munich, Germany



Open Source Contributions

- canonical/microk8s-community-addons
- cloudposse/terraform-aws-route53-cluster-hostname
- grafana/tempo
- jenkins-x/jx
- kubernetes-client/python
- kubernetes/autoscaler
- mattermost/mattermost-helm
- renovatebot/renovate
- cloudnative-pg/charts
- datreeio/CRDs-catalog
- helm/charts
- knative/docs
- kubernetes-sigs/kubebuilder
- litmuschaos/litmus-docs
- raspbernetes/k8s-security-policies
- VictoriaMetrics/helm-charts

Skills & Expertise

Public Cloud

- Amazon Web Services (AWS) ■■■■
- Microsoft Azure ■■□□
- Google Cloud Platform (GCP) ■■□□
- Oracle Cloud Infrastructure (OCI) ■■□□
- STACKIT ■■□□
- Alibaba Cloud ■■□□
- Kubernetes (On-Premise & Cloud) ■■■■

Kubernetes / CNCF

- Platform: Cluster API, Gardener ■■□□
- Provisioning: kubeadm, microk8s, k3s, kubespray ■■□□
- GitOps: ArgoCD, Flux ■■□□
- Templating: Helm, Kustomize ■■■■
- Observability: Prometheus, Grafana, Loki, Mimir, Tempo, Jaeger, Thanos ■■■■
- Operators: controller-runtime, kubebuilder, operator-sdk ■■□□
- Artifacts: Artifactory, Sonatype Nexus, Harbor, AWS ECR ■■□□

• Authn / Authz:	dex, oauth2-proxy, RBAC	■■□
• Autoscaling:	Karpenter, cluster-autoscaler, knative-serving	■■■
• Automation:	kured, Argo Workflows	■■□
• Chaos / Resiliency:	Chaos-Mesh, LitmusChaos	■■□
• CNI / Networking:	aws-vpc-cni, Cilium, Calico, Istio, Envoy, MetalLB	■■■
• Compliance:	Open Policy Agent (OPA-Gatekeeper), Kyverno, OpenCost	■■■
• CRI (Runtimes):	containerd, Docker	■■□
• Databases:	Crunchy Data Postgres Operator	■□□
• DNS:	external-dns, CoreDNS	■■■
• Events:	CloudEvents, knative-eventing	■□□
• GPU:	nvidia-gpu-operator, dcgm-exporter	■■□
• Ingress:	ingress-nginx, Istio Ingress Gateways, Kong	■■□
• Secrets:	Vault, sops, age	■■□
• Security:	cert-manager, kubesecc, kube-audit	■■□
• Storage:	Cloud (ebs-csi, efs-csi), On-Premise (Longhorn, OpenEBS)	■■□
• Service Mesh:	Istio, istio-ambient, Cilium Mesh	■■□

CI/CD

• Continuous Integration / Continuous Deployment		■■■
• Continuous Delivery		■■□
• Bitbucket		■■□
• GitHub Actions		■■□
• GitLab		■■■
• Prow		■□□

AWS

• Provisioning:	Terraform, CloudFormation, StackSets	■■□
• Container:	EKS, ECS, Fargate, ECR	■■■
• VM:	EC2, Auto Scaling, Load Balancing	■■■
• Observability:	CloudWatch, AMP, Container Insights	■■□
• AI/ML	AWS Bedrock	■□□
• Authn / Authz:	IAM Access Management, OIDC, Cognito, Policies, Analyzer	■■□
• Autoscaling:	AutoScaling Groups, LaunchTemplates, LaunchConfigurations	■■■
• Chaos / Resiliency:	Fault Injector Simulator (FIS)	■□□
• Compliance:	Config, CloudTrail, Detective, SecurityHub	■■□
• Databases:	RDS (PostgreSQL, MySQL, Aurora), DynamoDB, DocumentDB	■■□
• DNS:	Route53 (Failover Routing, weight-based, HealthChecks)	■■□
• Events:	AWS MSK (Kafka), EventBridge	■■□
• Load Balancing:	ALB, ELB, NLB, Route53	■■□
• Networking:	VPC, Route53, CloudFront	■■□
• Security:	GuardDuty, Config, WAF, KMS, ACM, SecurityGroups, NACLs	■■□
• Serverless:	API Gateway, Lambda, SQS, SNS	■■□
• Storage:	S3, EBS, EFS	■■■

Azure

• Provisioning:	Terraform	■■□
-----------------	-----------	-----

- Container: AKS ■■□
- VM: Virtual Machines, Scale Sets ■■□
- Observability: Log Analytics ■□□
- Authn / Authz: Azure AD, Entra DS ■□□
- DNS: Azure DNS ■■□
- Networking: VNets, Hub / Spoke, Azure DNS, Load Balancer ■■□

GCP

- Provisioning: Terraform ■■□
- Container: GKE ■■□
- AI/ML: Vertex AI Workbench, Model Garden ■■□
- Authn / Authz: ServiceAccounts, OIDC ■□□
- Networking: VPC, VPC Firewall Rules ■□□

AI & Machine Learning

- Langchain ■□□
- LlamaIndex ■■□
- Language Weaver ■■■
- nvidia-dcgm-exporter ■■□
- Ollama ■■□

Programming, Scripting & Automation

- Golang ■■□
- Python ■■□
- BASH ■■■
- Terraform / HCL ■■■
- CloudFormation ■■□
- Ansible ■■□
- cloud-init ■■□
- HTML, CSS, JavaScript ■■□
- SQL ■■□

Project Management

- Confluence ■■□
- Jira ■■□
- Kanban ■■■
- Scrum ■■□

Security / Compliance

- Burp Suite ■□□
- CIS Kubernetes Benchmark ■■■
- Image Hardening ■■■

- Image Scanning (Claire, Trivy, Aqua Anchore)
- kubeaudit
- kubesecc
- Least-Privilege
- nmap
- NetworkPolicies
- NSA/CISA Kubernetes Hardening
- OWASP Top 10
- PCI/DSS
- WebAppSec



Certificates & Trainings

- AWS Certified Solutions Architect – Associate
- Certified Kubernetes Administrator
- Certified Kubernetes Security Specialist

<https://www.credly.com/users/hajowieland/badges>



Projects/Contracts

Universitätsklinikum Erlangen

April 2024 – Present

Kubernetes Expert

i Supporting the team with Kubernetes and Open-Source tooling decisions for their NVIDIA GPU Clusters which are used by various research departments.

Tools & Services

- Architecture: On-Premise, kubescape
- Infrastructure as Code: Ansible
- Hardware: NVIDIA GPUs, nvidia-gpu-operator

STACKIT GmbH & Co. KG

January 2024 – March 2024

Kubernetes Security Expert



i Implemented Security controls, evaluated guidelines and supported the team regarding BSI C5 compliance for the central STACKIT Kubernetes Engine ("SKE") in a high security environment.

Tools & Services

- Architecture: On-Premise, Gardener
- Infrastructure as Code: Ansible, Terraform
- Observability: Loki, Cortex, Grafana
- CI/CD: GitHub, Prow

Tasks & Projects

- Consulted the SKE team regarding C5 compliance
- Evaluated security controls and implemented security measures for highly secure managed Kubernetes service
- Vulnerability Assessment & Fix for Snyk Findings

MARKANT Services International GmbH

June 2024 – April 2024

DevOps & Grafana Expert



i Consulted and helped the systems management team with the initial setup of a company wide metric and logging observability setup. This included helping with designing the architecture, supporting with the implementation and writing Infrastructure as Code.

Tools & Services

- Architecture: Docker, On-Premise
- Infrastructure as Code: Ansible, Terraform
- Observability: Loki, Mimir, Alloy, Grafana Cloud
- CI/CD: GitLab

Tasks & Projects

- Consulted the team for the launch of a new state of the art monitoring setup
- Developed multiple Ansible roles for deploying On-Prem

- Performed a Terraform workshop for the team and implemented the initial Grafana Cloud IaC
- CI/CD for Ansible & Terraform in GitLab pipelines

Bundesdruckerei GmbH

May 2023 – December 2024

Site Reliability Engineer



i Engineered and operationalized with the SRE team a data science & AI machine-learning platform in a highly secured, air-gapped, on-premise Kubernetes environment. Helped improve overall reliability, security and observability of the platform. Managed multitude of different Machine Learning, AI and data science open source software as well as custom applications for public sector customers.

Tools & Services

- Architecture: On-Premise K8s with Kubespray
- GitOps: FluxCD
- Infrastructure as Code (IaC): Ansible, Helm, Kustomize
- GPUs: 10x NVIDIA A100 GPU Cluster in K8s
- Networking: Calico
- Observability: Prometheus, Thanos, Grafana, Loki
- Data Science: ElasticSearch with eck-operator, POSIT Workbench, Argo Workflows
- Storage: MinIO, Longhorn
- Authentication: Keycloak
- CI/CD: GitLab

Tasks & Projects

- Constructed & operated a data science platform in a highly secure environment
- Managed, fixed, updated four (4) On-Premise Kubernetes clusters with Kubespray, Flux, Helm and GitLab CI
- Fully refactored the observability stack to improve automation & provisioning fully with IaC, conventionalize structure to be the same on all clusters and improve overall performance of metrics and logs read & write paths
- Owner of Kubernetes observability stack (Metrics, Logging)
- Streamlined Vault Kubernetes Setup with HA and custom auto-unseal
- Regular debugging and deep-dive into various On-Premise K8s issues regarding networking & storage
- Planned, created and implemented CI for gitOps repository
- Planned, created and implemented Machine-Learning (transformer based) Tools for Translation services (Language Weaver) with NVIDIA GPUs
- Planned, created and implemented multiple Helm Charts and common CI/CD, testing (helm-unitest) and JSON schema validation
- Created Terraform tests for VM-based Multi-Node MinIO Clusters modules
- Security & RBAC for Rstudio to use with NVIDIA GPU Clusters
- nvidia-gpu-operator Deployments with Flux & Helm Releases
- Deployment Llama3 with vLLM using NVIDIA GPUs and Autoscaling, integrated with Flux gitOps
- Setup highly available production Argo Workflows heavily used by data engineers
- Created Helm Charts and deployment automation for custom AI Chatbot applications using NVIDIA GPUs

- Refactored two dozen Grafana dashboards with standardized configs and variables

HanseMerkur

June 2023 – March 2024

Kubernetes Consultant



i Consulted and helped the infrastructure team with the migration of On-Premise Kubernetes setup to AWS EKS, K8s Networking, Service Mesh, RBAC and NetworkPolicies. Build a custom Kubernetes controller with controller-runtime for automating admission webhook config patching.

Tools & Services

- Architecture: AWS EKS, On-Premise vanilla K8s (Kubespray, Tigera Calico Enterprise)
- GitOps: ArgoCD
- Infrastructure as Code: Terraform
- Networking: Calico, Cilium
- Service Mesh: Cilium, Istio
- Observability: Prometheus Operator, Grafana, ElasticSearch
- CI/CD: GitLab
- AutoScaling: Karpenter

Tasks & Projects

- Consulted for new Kubernetes platform on AWS migrated from On-Premise
- Developed custom K8s controller with controller-runtime in Golang + Helm Chart to patch admission controller webhook configurations. Helped with a restriction when running EKS without aws-vpc-cni and implemented a compliance requirement to limit the amount of different software running in Pods with hostNetwork.
- Consulted, reviewed and demoed multiple CNI solutions (Cilium, Calico, aws-vpc-cni)
- Consulted about Service Mesh, RBAC and NetworkPolicies Best Practices
- Planned and executed 2h demo showing Istio Service Mesh use-cases: A/B Testing, Retries, Mirror, Locality routing, observability, mTLS
- Debugged and root cause analysis for On-Premise K8s IPVS networking which fixed issues with failing blackbox-exporter probes
- Consulted, implemented and demoed multiple PoCs for autoscaling with Karpenter for NVIDIA GPU & ARM64 Graviton EC2 Kubernetes Nodes.

Eventim CTS AG

October 2021 – May 2023

Kubernetes Engineer



i Engineered and operationalized with the Cloud team a Multi-Account AWS Setup with several AWS EKS Clusters, IaC and Observability running the backend infrastructure of Olympia 2024 Paris ticket sales.

Tools & Services

- Architecture: AWS EKS
- GitOps: ArgoCD
- Infrastructure as Code: Terraform, Terragrunt
- Networking: aws-vpc-cni
- Service Mesh: Istio
- Observability: Prometheus Operator, Mimir, Grafana, Tempo, Jaeger, Loki
- CI/CD: GitLab
- AutoScaling: Karpenter, knative-serving
- Events: CloudEvents, knative-eventing, Kafka (MSK)

Tasks & Projects

- Planned, created, deployed central gitOps with ArgoCD for all three stages with two K8s clusters each
- Analyzed the existing environment and implement Security Best-Practices
- Implemented fully automated Istio version update process
- Implemented various Knative & Istio Service Mesh administration and enhancement tasks
- Debugged issues with Istio and Knative (performance issues, AWS Cost optimization, Knative bugs reported and communicated to Knative devs on their Slack)
- Refactored Knative setup with eventing-kafka (AWS MSK)
- Planned, created, deployed highly-available Harbor registry running in K8s with Image Scanning (Trivy, Claire)
- Planned, created a complete overhauled of the K8s monitoring setup: Replaced kube-prometheus-stack (Prometheus, Grafana) with highly scalable Grafana Mimir for metrics
- Replaced Jaeger tracing setup with Grafana Tempo
- Planned and implemented new logging setup with Grafana Loki
- Refactored Grafana setup and all dashboards for uniformity and cross-references of Metrics/Logs/Traces which greatly helped developers & SREs when debugging issues
- Planned, created, deployed authn & authz SSO for all internal tools (Monitoring, Web UIs, etc.) with oauth2-proxy via Keycloak
- Updated and refactored a dozen Terraform modules (implemented Terraform and Security Best Practices)
- Implemented automation for automated nightly EKS updates in non-prod environments
- Ran regular automated Load- and Scaling tests with k6 of K8s infra
- Planned and implemented faster autoscaling with AWS Karpenter
- Implemented semi-automated Updates of all Open-Source Cloud Native components (renovate, gitOps)
- Implemented auto-start/auto-stop for development EKS Cluster which reduced costs for DEV by 38%
- Held workshops for developers about Kubernetes and Helm Charts with best practices

Kassenärztliche Vereinigung Bayerns
(Health sector)

July 2021 – November 2022

Kubernetes Engineer



i Architected & Engineered an On-Premise Kubernetes VMware PKS (now Tanzu) based platform with the cross-functional team in a greenfield project for healthcare services.

Tools & Services

- Architecture: VMware PKS
- GitOps: FluxCD
- Infrastructure as Code: Ansible
- Networking: NSX-T
- Observability: Prometheus Operator, Grafana, ElasticSearch, Graylog
- CI/CD: GitLab

Tasks & Projects

- Consult and support migration VM-based VMware infrastructure to containerized VMware PKS Kubernetes setup On-Premise for health services.
- Planned and implemented internal Kubernetes platform for all company microservices developed in multiple programming languages (Java Spring Boot, NodeJS, Python)
- Planned and implemented single source of truth with gitOps via Flux and encrypted secrets with sops
- Planned and implemented the Monitoring setup (Prometheus Operator, Grafana), Alerting, documentation
- Planned and implemented Ansible playbook to fully automate cluster creation via VMware PKS API and provision with Flux
- Planned, created, deployed Kubernetes security measures and enforcement with Helm Charts & OPA Gatekeeper
- Documented and implemented Blueprints for Compliance and internal guidelines (Security, Best Practices)
- Planned, created and supported first-time creation of Helm Charts for Webapp software, core services for Kubernetes (nginx-ingress, Monitoring, Security)
- Planned, created, deployed CI/CD for all custom Helm Charts via Jenkins multi-branch pipelines, testing with kubeval, kubesecc, chart-testing, Helm unittest.
- Planned, created and enhanced Helm Charts for Spring Boot & NodeJS to be used by all teams
- Consulted other teams for implementing Jenkins pipelines to deploy to K8s
- Integrated external software with very custom/special deployment process into our infrastructure (Terraform SDK, Helm SDK, Mage)

Munich Re AG

January 2019 – September 2021

AWS Cloud/DevOps Engineer



i Owner and lead engineer of the infrastructure team managing the complete AWS & Kubernetes infrastructure for financial services products sold to international banks and insurance companies.

Tools & Services

- Architecture: kops, AWS EKS
- GitOps: FluxCD

- Infrastructure as Code: Terraform, Ansible, cloud-init
- Networking: aws-vpc-cni
- Observability: Prometheus Operator, Thanos, Grafana, Loki
- CI/CD: Bitbucket

Tasks & Projects

- Owner and main contact for all five AWS Accounts, Kubernetes Clusters, Deployments and Pipelines
- Planned, created, deployed EKS-based Kubernetes clusters in multiple stages, migrated from kops-based setup. Unmanaged node groups in IaC for Spot + Ondemand (mixed). For workloads with and w/o persistent storage and for Fargate serverless.
- Planned, created and enhanced 64 Helm Charts with CI and enhanced testing. Committed back to upstream Jenkins & Mattermost charts.
- Created and Implemented gitOps-based automated deployment flow with Flux v1 for all K8s resources with encrypted secrets in git as a single source of truth. Charts for internal (mainly open-source based) tooling as of over a dozen application source code components.
- Planned, created and enhanced 41 Terraform IaC Modules (mainly AWS, some Mongo Atlas).
- Set up AWS Security with IAM, SSM, CloudTrail, Secret Manager, SecurityHub, Detective, Inspector
- Planned and implemented highly available OpenVPN with MFA
- Planned and implemented least-privilege RBAC
- Planned and implemented Sonatype Nexus artifact storage running in K8s
- Planned and implemented CI/CD Pipelines with BitBucket for integration and K8s automation jobs
- Planned and implemented highly-available Jenkins running in K8s with JCasC
- Planned and implemented multiple Ingress Controllers with ingress-nginx for different access requirements (public, private / VPN-only, internal) and Private / Public Route53 Zones
- Planned and implemented isolated VPC networking setup with Peering between AWS Accounts
- AWS Cost Optimization and alerting and Kubernetes cost optimization with mixed On-Demand & Spot instances
- Planned and implemented highly available self-managed Monitoring with Prometheus, Grafana, Loki
- Planned and implemented CIS Kubernetes Benchmark for compliance
- Planned and implemented hardening of K8s worker nodes with AWS Inspector, SSM and CIS Amazon Linux Benchmark

Professional Experience

ventx GmbH

October 2018 – March 2024

Cloud/DevOps/Kubernetes Engineer



i Lead Kubernetes consultant in a cloud & infrastructure agency, working in a multitude of different DevOps and Kubernetes projects.

Tools & Services

- Architecture: AWS, Azure, GCP, Proxmox
- GitOps: FluxCD
- Infrastructure as Code: Terraform, Cloudformation, CDK (Golang), Ansible, cloud-init
- Networking: aws-vpc-cni, Wireguard
- Observability: Prometheus Operator, Thanos, Grafana, Loki
- CI/CD: Bitbucket, Gitlab

Tasks & Projects

- Worked in multiple freelance projects (full-time & part-time)
- Developed internal Multi-Cloud Kubernetes platform (Golang, AWS Lambda, AWS/Azure/GCP, Python, ReactJS)
- Planned and developed a internal Slack Bot in Python with Langchain for GPT3.5/GPT4 access directly from Slack
- Supported Juniors on their internal on-premise K8s platform (microk8s)
- Planned, build, managed internal "DevOps Companion AI" (Streamlit UI with Python, Langchain, llamaindex for RAG with DevOps tools' GitHub releases, llama2, codellama, GPT-3.5, GPT-4)

BodyWorldGroup GmbH

October 2015 – September 2018

Linux-Administrator

i Renewed, improved and ran the complete in-house and later cloud based IT infrastructure for an E-commerce company with half a dozen shops.



Tools & Services

- Architecture: On-Premise, VMware ESXi, Proxmox
- Networking: pfSense
- Observability: Icinga, Prometheus
- CI/CD: Jenkins

Tasks & Projects

- Planned, created and managed internal self-hosted VMware ESXi platform
- Planned, created and managed containerized mail platform with AntiSpam with Linux LXD/LXC
- Planned, created and evaluated self-managed K8s Cluster to replace LXC / VMware
- Build and enhanced several Jenkins pipelines for infrastructure automation and report generation
- Network monitoring
- Mailserver Setup, Maintenance, Anti-Spam, Monitoring

m.a.x. Informationstechnologie AG

May 2014 – September 2014

VMware Administrator



i Managed and configured large VMware vSphere infrastructure running with InfiniBand based storage. Part of the infrastructure team managing customer environments for German public broadband TV programs.

Tools & Services

- VMware vSphere

Tasks & Projects

- Administration multiple VMware vSphere Clusters
- High Performance InfiniBand SAN Storage for VMware
- Automation, Backup & Restore, Provisioning

IP-Exchange GmbH

April 2013 – December 2013

Linux-Technician in Network Operations Center



i Member of the Network Operation Center (NOC) team servicing multiple datacenters for international customers.

Tools & Services

- Linux
- OTRS

Tasks & Projects

- Linux Administration & Support
- NOC Support working in changing shifts
- Network Monitoring
- On-Call for Linux and Hardware related issues/problems
- Setup and configuration of internal & customer server racks
- Datacenter technician

petaFuel GmbH

July 2009 – December 2012

Linux-System Administrator (apprentice)



i Managed and enhanced the in-house and datacenter VMware infrastructure in compliance with PCI/DSS as part of the System Administration team for a MasterCard payment processor.

Tools & Services

- VMware ESX
- OSSEC
- Windows Server
- Nagios / Icinga

Tasks & Projects

- Linux System Administration (Ubuntu, Debian)
- Configured, administered, updated highly-available VMware ESXi Clusters
- Implemented PCI-DSS compliance regulation requirements
- Planned and implemented Host-based Intrusion Detection System (OSSEC) on all Linux servers
- Replaced Datacenter Hardware for On-Premise Servers
- Updated and administered central Windows Update Server (WSUS)
- Managed Windows Active Directory
- Planned and implemented central Nagios / Icinga Monitoring with various dashboards for visualization

Education

September 2009 - September 2012

IT Specialist System Integration ("Fachinformatiker Systemintegration")
petaFuel GmbH, Freising, Germany

Languages

- **German:** native
- **English:** fluent (spoken and written, experience working in international and multilingual teams)