

Bare-Metal & On-Prem Platform Engineering

Physical Servers · Virtualisation · Kubernetes · Enterprise Services

Client Project Portfolio · April 2026 · Confidential

7	100%	Bare-Metal I	Zero Vendor
Capability Domains	On-Premise Deployment	Kubernetes Approach	Cloud Lock-in

This portfolio documents hands-on expertise in fully on-premise infrastructure engineering — covering bare-metal Kubernetes, hypervisor virtualisation, Linux administration, enterprise application deployment, storage systems, and self-hosted observability stacks. All capabilities are delivered without cloud dependency, on physical hardware or internal virtualised environments.

1

BARE-METAL KUBERNETES (KUBEADM)

- Bootstrap and manage production-grade Kubernetes clusters using kubeadm on physical servers
- Configure control plane HA (stacked etcd or external etcd), worker node joins, and TLS bootstrapping
- Manage CNI plugins (Calico, Flannel, Cilium) for pod networking, network policies, and segmentation
- Administer cluster upgrades, certificate rotation, etcd snapshots, and disaster recovery procedures
- Deploy ingress controllers (NGINX, HAProxy), cert-manager, MetalLB, and persistent volume provisioners
- Implement RBAC, Pod Security Standards, OPA/Gatekeeper policies, and audit logging

kubeadm	etcd HA	Calico / Cilium	MetalLB	NGINX Ingress	cert-manager	RBAC
---------	---------	-----------------	---------	---------------	--------------	------

2

VIRTUALISATION — KVM / PROXMOX / VMWARE

- Deploy and manage KVM hypervisors on bare-metal Linux hosts with libvirt and virsh tooling
- Administer Proxmox VE clusters: node management, VM/LXC lifecycle, HA groups, and migration
- Manage VMware ESXi hosts and vCenter: VM provisioning, snapshots, vMotion, and resource pools
- Design VM templates, cloud-init configurations, and automated provisioning workflows
- Implement storage backends for VMs: local LVM, NFS, Ceph RBD, and iSCSI targets
- Monitor hypervisor performance, capacity planning, and physical-to-virtual (P2V) migrations

KVM / libvirt	Proxmox VE	VMware ESXi	vCenter	cloud-init	P2V Migration
---------------	------------	-------------	---------	------------	---------------

3

LINUX ADMINISTRATION & NETWORKING

- Administer RHEL, CentOS Stream, Debian, and Ubuntu server environments at scale
- Manage systemd services, kernel parameters, cgroups, namespaces, and performance tuning
- Configure networking: static IPs, bonding, VLANs, bridges, iptables/nftables, and routing tables
- Harden servers: SSH hardening, PAM, SELinux/AppArmor policies, auditd, and CIS benchmarks
- Automate OS configuration and provisioning using Ansible playbooks and roles
- Manage PKI, TLS certificates, internal CA, and mTLS for service-to-service communication

RHEL / Debian	systemd	iptables / nftables	Ansible	SELinux	Internal PKI
---------------	---------	---------------------	---------	---------	--------------



4 ENTERPRISE APPLICATION DEPLOYMENT

- Deploy and manage Keycloak for on-premise Identity and Access Management, SSO, and OIDC/SAML federation
- Administer RabbitMQ clusters: exchanges, queues, bindings, policies, HA mirrors, and dead-letter handling
- Deploy and manage Apache Kafka: brokers, topics, partitions, replication, and consumer group management
- Configure and operate self-hosted SMTP (Postfix / Exim): relay configuration, TLS, DKIM, and SPF
- Deploy and administer production databases on bare-metal: PostgreSQL, MySQL, and MongoDB
- Manage database HA: Patroni/repmgr for PostgreSQL, Galera Cluster for MySQL, replica sets for MongoDB

Keycloak	RabbitMQ	Apache Kafka	Postfix SMTP	PostgreSQL / MySQL	MongoDB
----------	----------	--------------	--------------	--------------------	---------

5 STORAGE SYSTEMS — NFS / CEPH

- Design and manage NFS server infrastructure: exports, client mounts, ACLs, and Kerberos security
- Deploy and operate Ceph clusters: OSDs, monitors, managers, MDS, and CRUSH map tuning
- Manage Ceph storage pools: replication, erasure coding, RBD block devices, and CephFS
- Integrate Ceph RBD and CephFS as persistent storage backends for on-prem Kubernetes (Rook-Ceph)
- Monitor storage health using Ceph dashboard, Prometheus exporters, and capacity trend analysis
- Implement backup strategies: rsync, Restic, Velero (for K8s), and snapshot-based recovery

NFS	Ceph RBD	CephFS	Rook-Ceph	Rook Operator	Velero / Restic
-----	----------	--------	-----------	---------------	-----------------

6 SELF-HOSTED MONITORING & OBSERVABILITY

- Deploy and manage Prometheus with custom scrape configs, relabelling, and recording rules
- Build Grafana dashboards for infrastructure, Kubernetes, databases, and application metrics
- Configure Alertmanager: routing trees, inhibition rules, silences, and multi-channel notifications
- Deploy Loki and Promtail for centralised log aggregation from all on-prem nodes and services
- Implement distributed tracing with Jaeger or Tempo integrated into the observability stack
- Manage SNMP exporters, node exporters, blackbox exporter, and custom application exporters

Prometheus	Grafana	Alertmanager	Loki / Promtail	Jaeger / Tempo	Node Exporter
------------	---------	--------------	-----------------	----------------	---------------

7 INTERNAL DATA PIPELINES ★ PREFERRED



- Design and maintain internal data pipelines using Kafka Streams, Apache Flink, or custom consumers
- Orchestrate batch and streaming workflows with Apache Airflow deployed on bare-metal / Kubernetes
- Manage data ingestion pipelines: ETL design, schema registry (Confluent / Apicurio), and serialisation
- Implement data pipeline observability: pipeline-level metrics, lag monitoring, and dead-letter analysis
- Support integration between internal services via event-driven architecture on RabbitMQ / Kafka

★ Preferred / Value-Add Capability

Apache Kafka	Apache Airflow	Kafka Streams	Schema Registry	ETL / ELT	Event-Driven Arch
--------------	----------------	---------------	-----------------	-----------	-------------------

All capabilities are delivered entirely on-premise — no cloud dependency, no vendor lock-in. Infrastructure is managed as code using Ansible, Terraform (local providers), and GitOps workflows, ensuring repeatable, auditable, and resilient operations across physical and virtualised environments.

