KubeOps

Solutions for modern IT in the public sector

Strategies for reliable, scalable and flexible Kubernetes infrastructures

Solutions for modern IT in the public sector

Strategies for reliable, scalable and flexible Kubernetes infrastructures

Introduction

The public sector is facing growing challenges: from modernising outdated IT systems to ensuring security and compliance with limited human and financial resources. Kubernetes has established itself as a proven technology to overcome these hurdles by bringing automation, flexibility and scalability to IT infrastructures.

Key messages for IT strategists in the public sector

This white paper is aimed at decision-makers and IT professionals in the public sector and shows how Kubernetes addresses IT challenges, makes modern infrastructures secure and efficient and enables the use of future-oriented technologies in the public sector.

→ **Security and compliance:** Kubernetes helps to meet strict security requirements and data protection regulations - essential for public organisations.

→ **Resource efficiency:** Automation and containerised applications reduce the workload of IT teams and optimise the use of limited budgets and capacities.

→ **Modernisation:** Kubernetes enables the gradual modernisation of legacy systems without affecting ongoing operations.

→ **Flexibility and independence:** Open source solutions with Kubernetes prevent vendor lock-in and offer maximum adaptability.

→ **Reliability and innovation:** Kubernetes offers highly available IT structures and creates a basis for digital sovereignty and new technologies.

With these key statements, the white paper shows ways in which IT solutions can not only meet challenges, but also promote future-proof innovations.

Table of Content

Kubernetes in the public sector: An overview

Why Kubernetes for the public sector?

A reliable IT infrastructure is essential in the public sector: it forms the basis for essential services, from administrative portals to real-time data processing. At the same time, public organisations face particular challenges, including strict data protection regulations, cyber threats and the need to work efficiently with limited resources.

Kubernetes, an open source solution for managing containerised applications, offers a powerful and flexible way to meet these requirements. It enables the dynamic scaling of IT systems, the integration of modern technologies and compliance with the highest security standards - all while optimising the use of resources.
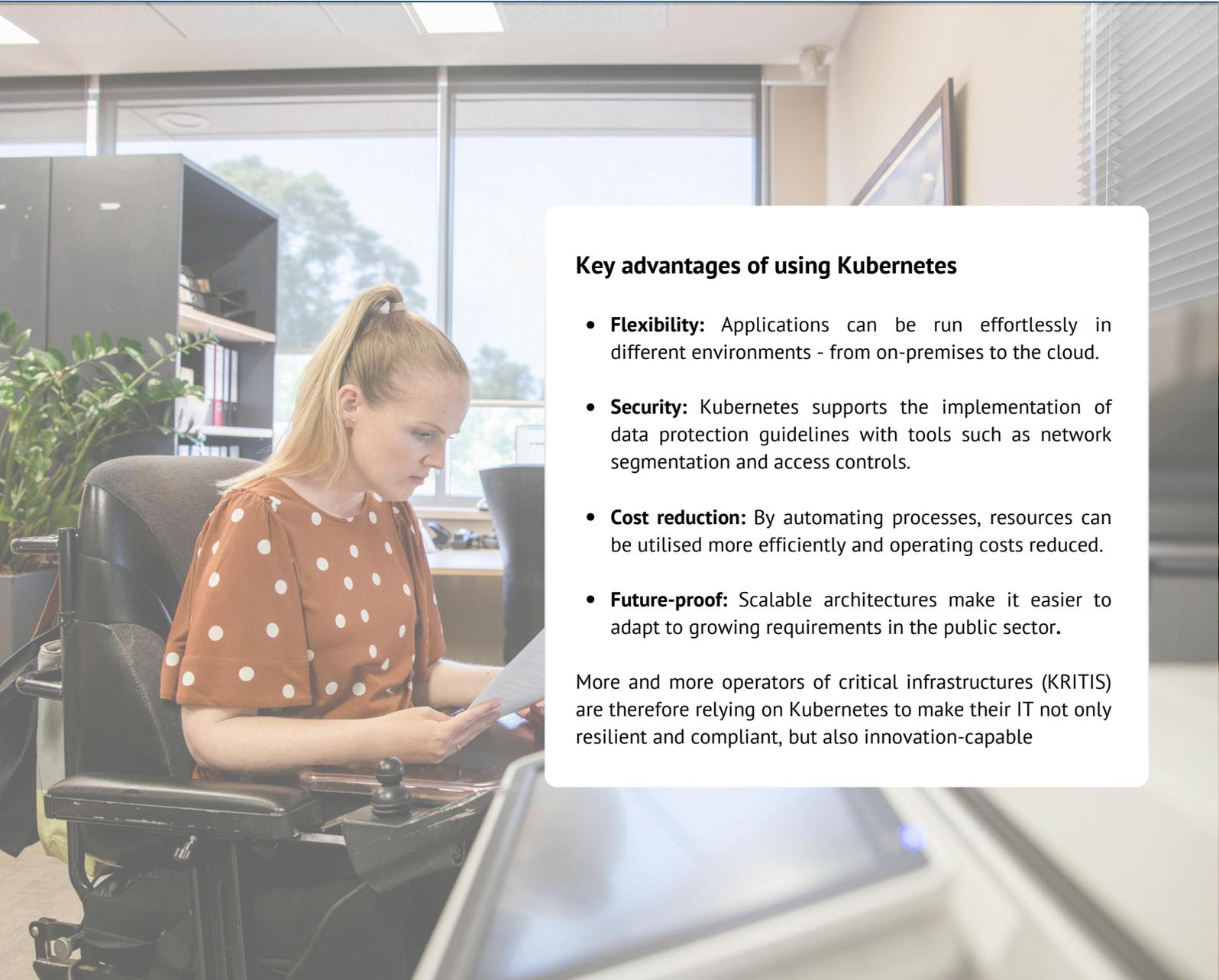
Key advantages of using Kubernetes

- **Flexibility:** Applications can be run effortlessly in different environments - from on-premises to the cloud.

- **Security:** Kubernetes supports the implementation of data protection guidelines with tools such as network segmentation and access controls.

- **Cost reduction:** By automating processes, resources can be utilised more efficiently and operating costs reduced.

- **Future-proof:** Scalable architectures make it easier to adapt to growing requirements in the public sector**.**

More and more operators of critical infrastructures (KRITIS) are therefore relying on Kubernetes to make their IT not only resilient and compliant, but also innovation-capable

IT challenges and solutions in critical infrastructures

Kubernetes can be a robust solution for operators of critical infrastructures (KRITIS), provided it is implemented and managed carefully. Especially in sensitive areas such as public administration, the use of this platform requires various prerequisites:

→ **Careful planning:**
All security, compliance and availability requirements must be fully taken into account.

→ **Precise configuration:**
Errors during setup can increase security and operational risks.

→ **Continuous monitoring:**
Regular audits and monitoring are essential to ensure compliance with requirements.

Critical hurdles for safety, availability and efficiency in the public sector

Skills shortage and increasing IT complexity
- **Lack of IT expertise:** Public organisations are struggling with a shortage of IT specialists, while the requirements for digital services are increasing.
- **Increasing system requirements:** Managing complex IT systems and implementing modern technologies requires highly specialised expertise that is often in limited supply.

Security and data protection
- **Strict data protection requirements:** Public organisations manage sensitive data that is subject to particularly strict data protection requirements (e.g. GDPR).
- **Increasing cyber threats:** At the same time, the threat of cyberattacks such as ransomware, which can jeopardise critical infrastructures and services, is increasing.

Budget restrictions
- **Tight budgets:** These limit the scope for investment in new technologies.
- **Focus on cost efficiency:** Increasing efficiency and reducing costs are therefore decisive criteria for IT solutions in the public sector.

Modernisation of legacy systems
- **High maintenance costs:** Outdated IT systems cause considerable operating costs.
- **Gradual transformation:** Modernisation must take place without affecting ongoing operations.

Digital sovereignty
- **Ensuring independence:** Dependence on foreign providers harbours risks for digital independence.
- **Open source as a solution:** Kubernetes enables the creation of sovereign IT infrastructures.

Scalable, secure and innovative IT structures with Kubernetes

Kubernetes unfolds its full potential in public sector organisations that rely on a secure, flexible and future-oriented IT architecture. As open source software for orchestrating containerised applications, Kubernetes automates central processes and optimises the use of resources. This enables:

- **Scalability:** dynamic adaptation to changing requirements, e.g. with growing data traffic.
- **Flexibility:** Applications run seamlessly in cloud, on-premises or hybrid environments.
- **Reliability:** Stable IT infrastructures promote high service availability and enable innovation and agility.

Advantages of Kubernetes-based solutions
Solutions based on Kubernetes offer centralised management and automation of clusters. Thanks to their open architecture, they can be flexibly adapted to the specific needs of public organisations. The result is simplified deployment and management of containerised applications - regardless of whether the infrastructure is operated in the cloud or locally.

Security and control through on-premises solutions
On-premises operation offers specific advantages for critical infrastructures:

- **Independence from internet bandwidth:** Critical applications remain available even with poor network coverage.
- **Maximum security:** Data and systems remain completely under the control of the organisation.
- **Adherence to compliance requirements:** Local processing facilitates regulatory requirements.

Fast implementation and reliable operation
'Out-of-the-box' solutions reduce the complexity of setting up Kubernetes clusters. Integrated tools such as Prometheus and Grafana ensure comprehensive monitoring and security mechanisms guarantee stable operation - ideal for authorities and public organisations that require reliable IT structures.
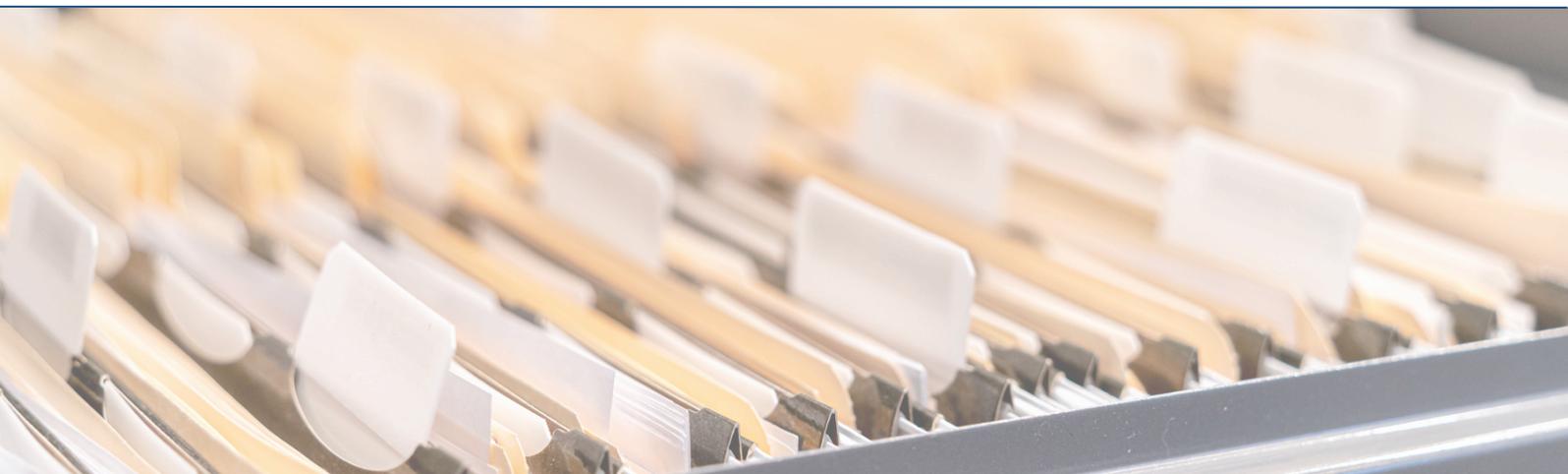
Case study

Digital transformation in local government

Initial situation

A municipal data centre was faced with outdated IT systems that required a lot of maintenance and made it difficult to introduce new digital services. At the same time, a shortage of IT specialists led to additional challenges in modernising the infrastructure.

Implementation and setup

- **Kubernetes solution:** A containerised IT environment based on vanilla Kubernetes was created with the KubeOps PLATFORM. This enables operation both on-premises and in hybrid environments.
- **Managed Kubernetes Service:** Maintenance-intensive tasks such as updates and security monitoring were outsourced to the Managed Kubernetes Service from KubeOps.
- **Automation:** Routine tasks were automated by Kubernetes to increase efficiency and reduce the workload of the IT teams.

Additional installations:

- An alternative virtualisation solution reduced licensing costs.
- Logging and monitoring tools such as Prometheus and Grafana were integrated to monitor operations.
- Automated backups were set up with Velero to ensure data availability.

Security measures

- Container images were checked for vulnerabilities and hardened by removing insecure components.
- Security policies were implemented to ensure data integrity and compliance.
- Access was regulated by Role-Based Access Control (RBAC) to prevent unauthorised access.

Results

- **Increased efficiency:** Automated processes reduced manual effort and enabled the IT team to focus on strategic projects.
- **Modernisation:** Containerisation of legacy applications simplified maintenance and reduced operating costs.
- **Reliability:** Thanks to the Kubernetes infrastructure, service availability was increased so that citizen services could be provided more reliably.

Best practices and recommendations for Kubernetes in the public sector

Ensuring security and compliance

Security and compliance strategies
- **Regular audits:** Conduct regular vulnerability assessments and security audits to identify potential risks early.
- **Implement access control:** Implement Role-Based Access Control (RBAC) to strictly regulate access to Kubernetes clusters.
- **Supply chain security:** Only use verified container images and harden them before use to minimise security vulnerabilities.

Monitoring and troubleshooting
- **Set up centralised monitoring:** Use tools such as Prometheus and Grafana to comprehensively monitor the infrastructure and detect problems at an early stage.
- **Proactive troubleshooting:** Implement alarms and log analyses to be able to react to critical events in real time.

Efficient orchestration and automation
- **Activate self-healing functions:** Ensure that Kubernetes automatically restarts failed applications to minimise downtime.
- **Utilise CI/CD pipelines:** Automate development and deployment processes with tools like ArgoCD to ensure fast and reliable application deployment.

Promote flexibility and independence
- **Favour open source solutions:** Rely on vanilla Kubernetes to avoid vendor lock-in and ensure digital sovereignty.
- **Use hybrid strategies:** Use hybrid cloud and on-premises solutions to fulfil specific requirements and achieve maximum flexibility.

Resource optimisation
- **Introduce auto-scaling:** Configure Kubernetes to automatically scale resources as needed, avoiding over- or under-provisioning.
- **Implement cost monitoring:** Use resource utilisation tracking tools to plan budgets effectively.
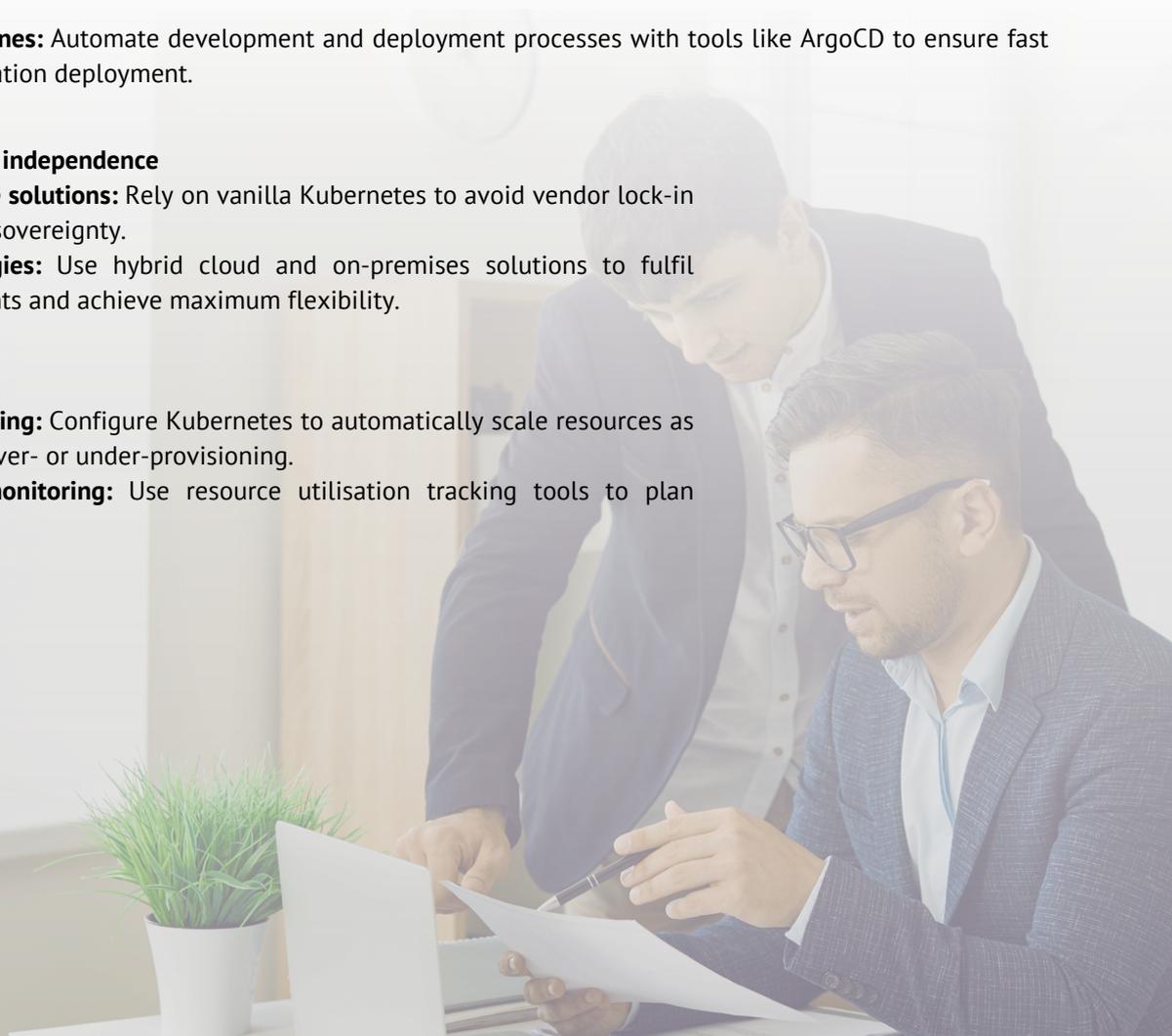
Exkurs: DevOps und containerisierte Anwendungen

DevOps in the public sector

A combination of development and operations that integrates both areas into a seamless, continuous process.

Objectives:
- Acceleration of software development and deployment
- Increase reliability
- Improve efficiency

Measures:
- Process automation
- Continuous integration and close collaboration between development and operations teams

Proven approach in industry and business:
- Shortened development cycles
- faster time-to-market
- higher quality

This approach is now also being applied in the public sector, where secure and efficient software solutions are particularly important.

Containerised applications

Software programmes that are executed in isolated containers.

These containers contain
- code
- Runtime environment
- System tools
- libraries and
- configurations

Advantages:
- **Portability:** can be executed independently of the underlying infrastructure
- **Consistency:** Reduces the probability of errors, facilitates the transition between development and production **phases**
- **Improved resource utilisation:** shared use of the host operating system kernel

Executable in different environments:
- Local development computer
- Production environment

About KubeOps

KubeOps GmbH was founded in 2019 as a subsidiary of ARWINET GmbH.

Our mission is to enable KRITIS organisations to build a robust container infrastructure quickly and efficiently. We understand the specific requirements of our customers, support them in setting up secure, resilient Kubernetes clusters and ensure their stable operation.

By using open source Kubernetes and carefully integrated components, we create automated, highly available and hardened clusters that are independent of vendor lock-ins to maximise our customers' flexibility and security.

We also offer training and certification to enhance your Kubernetes expertise.

Do you have any questions?
Get in touch with us!

Your advantages at a glance:
- Getting to know each other
- Focus on bottleneck analysis
- Initial solution proposals
- Objectives for the future

- www.kubeops.net
- info@kubeops.net
- +49 7433 93724 90

To the free initial consultation