Safety and Standardization:
A Key to National Security

industry

Government

location

Germany

key challenges

- Environment Segregation
- High Security Requirements
- Container Hosting

VMware products

- VMware Cloud Foundation with Tanzu
- VMware Aria Automation
- VMware Aria Operations
- VMware Tanzu Kubernetes Grid
- VMware Log Insight

"I've always wanted to say this," Marcus Schoen, Cloud Solution Architect at comdivision, began, "due to national security reasons, we cannot disclose the name of our client." It might sound more dramatic than it is, but it's rare for such an agency to provide insights into its structure or infrastructure setup. However, they deal with financial management. Even without knowing the client's identity, Marcus has an interesting story to tell about maximizing standardization measures.

New security policies and outdated technology forced our clients to rethink their approaches to their data center infrastructure. They primarily relied on legacy infrastructure, which was highly standardized for security reasons. However, the virtualization environment had reached the end of its lifecycle (support end-of-life).

our lead architect on the case

Marcus Schoen

Having a state-of-the-art – software-defined – data center was their top priority. However, the project leader contended that "it had to be standardized and secured to anticipate future needs. We had a reference architecture in mind that would support future platform and application requirements without significant adjustments."

They further expounded that "the central prerequisite for the new system was the design of the infrastructure stack, including hardware and the flexibility for various usage scenarios. Although we have internal expertise for routine operations, specialized knowledge was required here." This is where Marcus and his team came into play.

The Challenge

In addition to designing the infrastructure, it was necessary for all services, such as automation and monitoring of system services, to be provided directly by the platform.

The final blueprint required autonomy without external dependencies. The system needed to have a certain mobility, because, although it seems unlikely, in the event of a national crisis, it should be possible to relocate the technology without encountering incompatibilities with essential components like network cards (virtual or physical).

The Solution

"With VMware Cloud Foundation, complimented by Tanzu, we already had a highly standardized foundation," Schoen asserted. However, it was necessary to document and review each component – from hardware to workflow – according to our requirement profile. When deficits were identified, we worked closely with our VMware contacts in Palo Alto to address them. For example, we had to adapt new technologies for network segmentation, incorporate external security solutions, and improve the flexibility and expandability of workload domain deployments – to name just a few challenges.

Schoen noted that "everything was recorded in a reference architecture that includes optional components depending on the area of application. The security aspects, autonomy, and the customization of the deployment process to include specific steps are particularly noteworthy."

The Result

In summary, the client received a renewed infrastructure where:

- VMware Cloud Foundation ensures the character of blueprints and their repeatability,
- VMware Tanzu Kubernetes Grid is integrated as a "module" for specific application scenarios,
- VMware NSX-T is used in a high-load environment with many groups and rules,
- all end-user services are covered by VMware Aria Automation,
- VMware Aria Operations serves as a key tool providing operation teams with customized health dashboards,

solution

Our client implemented VMware solutions to efficiently address their security, segregation, and container hosting challenges.

business benefits

- Standardized infrastructure through VMware Cloud Foundation
- Enhanced security standards to protect sensitive data and systems
- Adaptability for future requirements and technologies with easier resource scaling
- Simplified and automated IT processes
- Improved insight and control over the IT infrastructure

- and finally, VMware Aria Log Insight acts as the central log receiver, transmitting data to the agency's central Security Information and Event Management (SIEM).

Over time, the system will be implemented hundreds of times and will be able to respond much more flexibly to new technologies like containers than the outdated system could."

Further details?

Would you like more details on this or other projects by comdivision? Contact us via email: info@comdivision.com, by phone at: +49 251 703839 0, or check out more case studies and our proven solutions at https://www.comdivision.com/cd-solutions/modern-apps#Case-Study-Section.