Blueprint for Infrastructure and Operations for this Government Agency

Industry

Government

Location

Germany

Key Challenges

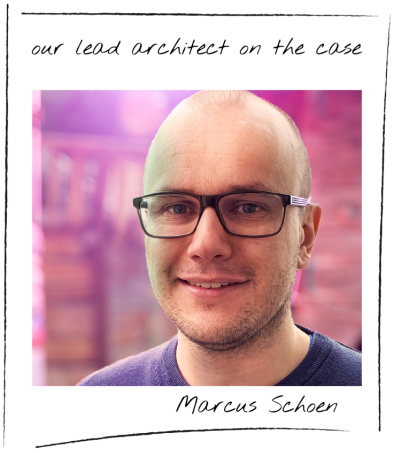
- Strong environment segregation
- Security requirements
- Container hosting

VMware Footprint

- VMware Cloud Foundation with Tanzu
- VMware vRealize Automation
- VMware vRealize Operations
- VMware Tanzu Kubernetes Grid
- VMware LogInsight

"I always wanted to say that" started Marcus Schoen, Cloud Solution Architect at comdivision "for reasons of national security we cannot disclose the customer name". It isn't quite as dramatic, but hardly any government agency would disclose who they are and how their respective infrastructure is set up. Let's just say they are in the field of governing finances and similar stuff. However, even without exactly knowing who the customer is, Marcus has a good story to tell, a story about taking standardization to the extreme.

New security regulations and outdated hardware required our customer to rethink their approach to the datacenter infrastructure. They were relying largely on legacy infrastructure in the past, that was very standardized to ensure security. But the virtualization environment reached support end of life.



"A state-of-the-art software defined datacenter was very desirable for us" said the customer's project lead "but it had to be standardized and secured, while foreseeing future needs. What we had in mind was a reference architecture that would enable future platform and application requirements without significant changes to its architecture."

The project lead continued "key requirement for new environment is blueprinting of the infrastructure stack including the hardware and its portability for different use cases. We have experts in our team for our day-to-day operations, but this is something that required expert help" this is where Marcus and team came in.

The Challenge

"Besides the blueprinting of the infrastructure, all services, like infrastructure service automation and monitoring, needed to be served by the platform itself" said Schoen, lead architect on the case "the disaster recovery to a second cold by datacenter had to include all components such as security policies, cloud management, monitoring, and logging."

The final blueoprint had to be self-sufficient, so that it had no external dependencies. "In a way, the system had to be portable" explained Schoen "although not likely, but if – literally – the nations ability to act is depending on it, you want to be able to take the system and roll it out somewhere else and not discover that the, let's say network interface cards (virtual or physical) are not compatible."

The Solution

"Through VMware Cloud Foundation with Tanzu we already had a highly standardized base" said Schoen "but we had to document and verfiy every component, from hardware to workflow against our requirement profile, and if there were gaps, we worked closely with our contacts at VMware in Palo Alto to solve the issues" he explained, and continued "for network segmentation for expample, we had to adapt new technologies, we also had to integrate external security components and increase the flexibiliy of and expand the workload domain deployments, to name a few."

"Everything was written down in a reference architecture that also contains optional modules depending on the application. A special feature is the security, the self-sufficiency and the expansion of the provisioning process by customer-specific steps" Schoen added.

In summary, the customer got a new infrastructure where

- VMware Cloud Foundation ensures the blueprint and repeatability character
- VMware Tanzu Kubernetes Grid was integrated for certain use cases as a "module"

- VMware NSX-T was integrated in a high-load environment with a high number of groups and rules
- All end-user services are consumable from VMware vRealize Automation
- VMware vRealize Operations is the key tool for the operation teams with custom health dashboards
- and finally, where VMware vRealize Log Insight serves as central log receiver that forwards the information to the agencies' central security information and event management (SIEM)

"Eventually, the system will be rolled out hundreds of time and can react much more flexible to new technologies such as containers then the old system could" concluded Schoen.