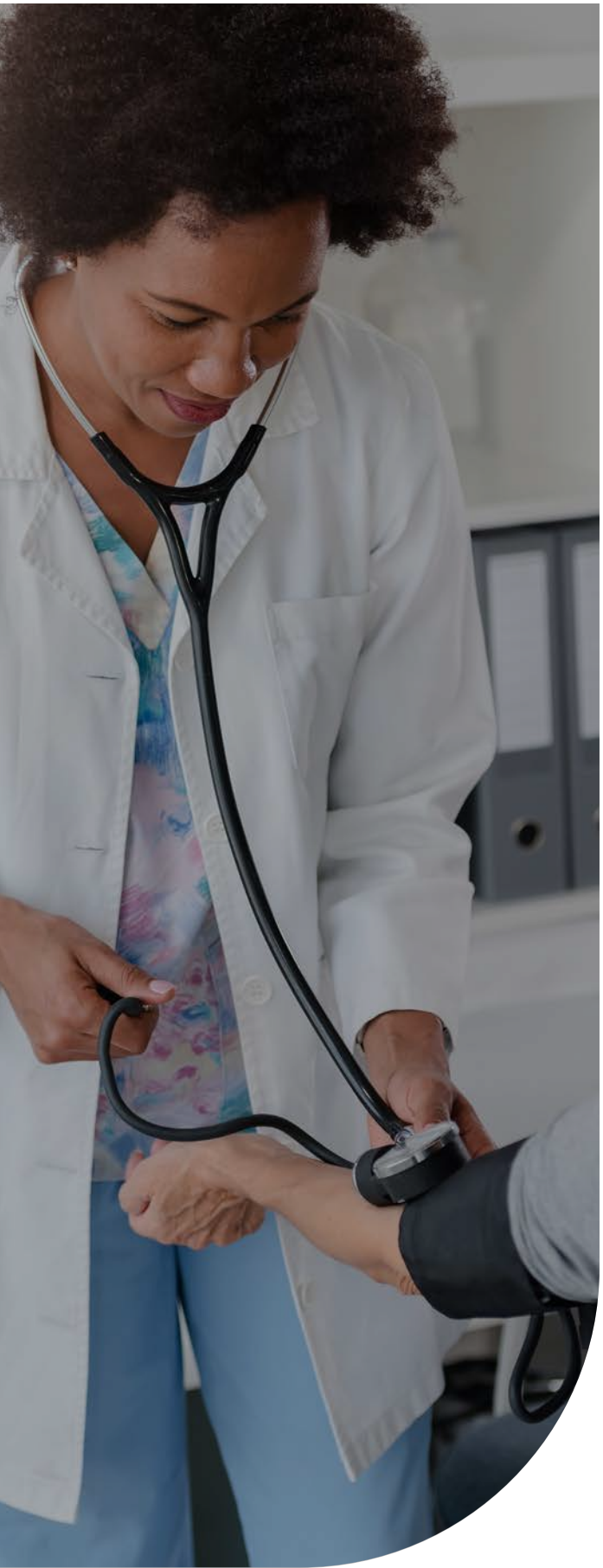
CDW PEOPLE WHO GET IT



CASE STUDY

# PARTNER OVERVIEW

CDW partnered with one of the nation's leading providers of healthcare services, comprising 182 hospitals and 2,300+ sites of care in the US and United Kingdom. Additionally, their sites of care include surgery centers, freestanding ERs, urgent cares, diagnostic and imaging centers, and walk-in and physician clinics. As a learning health system, they annually analyze data from more than 35 million patient encounters. This data helps develop technologies and best practices that improve patient care, which is then shared with the larger healthcare community and government agencies to improve care everywhere.

## Background

The customer wanted a standardized secrets management process across their different applications, and had chosen Vault as the vendor. Some of their application teams had started using secrets management specific to individual clouds, but the organization was looking for something cloud agnostic that started with applications deployed in Google.

## Goals

The goals agreed upon included:

- Have a central, secure place to store and manage secrets such as API keys, passwords, certificates, etc. that applications need to work with other applications and services
- Create applications that authenticate all requests and provide secure access only to authorized resources, regardless of whether they are human or machine
- Implement Encryption-as-a-Service
- Implement Dynamic Secrets

Additionally, the project was extended to include the following goals:

- Document the performance cluster configuration process
- Assist the customer's Vault maintainers with the configuration of performance clusters to multiple regions in GCP
- Prepare the customer's SMEs for the namespace, policy, and roles definition process
- Implement Dynamic Secrets

## Plan

The original plan included a two-phase concept: design and training. The design phase outlined how the cluster should be stood up, which was a Vault cluster in GCP, with VMs with a DR cluster and two Vault clusters for replication. Kubernetes was initially recommended instead of VMs, and that recommendation was implemented later in the engagement, alongside training for the customer, as they were new to Kubernetes.

Once the primary and DR clusters were stood up, the customer determined they also wanted a performance cluster, which instigated a PCR. Through this additional component, working lab sessions were given to provide recommendations and the needed code, which was later implemented by the customer. The lab sessions also included information around setup (namespaces, policies, structure, configuration, etc.) and Terraform code for basic configurations and backups. Hashi modules for Terraform and a Hashi-provided helm chart were used. This was configured to deploy the Vault clusters inside of GKE by setting up certificates and the customer's environment-specific items to handle the performance and primary clusters.

Once the clusters were stood up, the training phase gave use cases and provided a workshop and "lunch-and-learn" outlining how to use Vault. Examples were provided of how to use the code with Vault and how to use it from an application perspective.

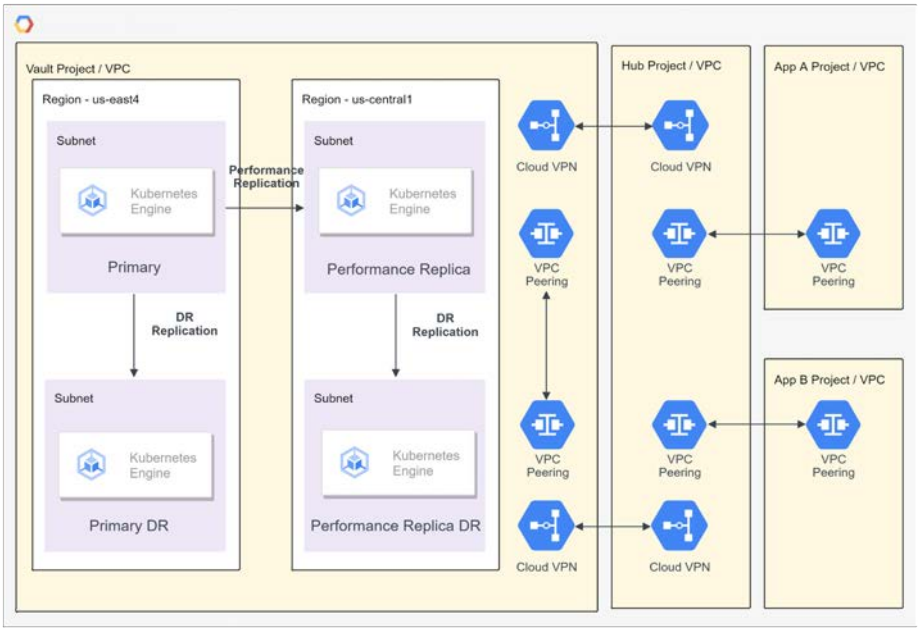



*Figure 1: Multi-cluster Replication Topology*

## Conclusion & Impact

As a result of the engagement, the customer's Vault implementation is highly available and ready for optimal performance. The engagement went beyond deployment to assist with failover and upgrade tests, an upgrade of Kubernetes, and an upgrade with Vault.

Through the engagement, the customer learned to set up and execute deployments from inception to failover, failback, restore from backup, etc. for different scenarios and components of the Vault cluster. The engagement provided major upskilling for their team that will last long after the work is complete. Further, CDW now has repeatable code, providing the ability to enter into Vault engagements prepped and ready for deployments.