Symantec SiteMinder on vSphere Kubernetes Service on VMware Cloud Foundation

Reference Architecture

Table of contents

Executive Summary

The validation of Symantec SiteMinder on vSphere Kubernetes Service (VKS) platform represents a critical milestone in modern cloud-native infrastructure deployment. By selecting VMware by Broadcom, the private cloud of choice, enterprises can accelerate the adoption of Security applications such as SiteMinder (Single Sign On) with VKS by using their cloud admins current skillsets.

This integration helps enterprises accelerate the adoption of applications like SiteMinder by using the VKS platform. Choosing VMware by Broadcom, the private cloud of choice, allows organizations to leverage existing cloud administrator skills, easing the transition and reducing the learning curve. This boosts operational efficiency, ensures rapid deployment of messaging infrastructure, and supports agile application ecosystems.

Benefits of using VKS with modern applications:

- **Lower TCO:** With VKS organizations have the ability to reduce silos, leverage existing tools and skill sets without having to retrain staff and/or change existing processes. Utilizing unified lifecycle management across infrastructure components to stay up-to-date with the most recent patches and minimizing security risks.
- **Operational Simplicity**: VKS is engineered for unparalleled operational simplicity, leveraging the familiarity of existing vSphere tools, skills, and workflows. This design philosophy significantly reduces the learning curve for IT teams and streamlines management processes. With VKS, organizations benefit from automated cluster provisioning, which accelerates deployment times and minimizes manual configuration errors. Furthermore, its robust capabilities extend to automated upgrades and comprehensive lifecycle management. This integrated approach ensures consistent operations, reduces overhead, and frees up valuable resources to focus on innovation rather than infrastructure maintenance.
- **Run and Manage Kubernetes at Scale:** Effortlessly deploy and manage Kubernetes clusters at scale, leveraging a built-in, Cloud Native Computing Foundation (CNCF) certified Kubernetes distribution. VKS provides fully automated lifecycle management, streamlining operations from initial setup to ongoing maintenance and upgrades. This comprehensive approach ensures that organizations can harness the power of Kubernetes for their containerized applications with unparalleled efficiency and reliability, without the complexities typically associated with large-scale Kubernetes deployments.

vSphere Kubernetes Service

vSphere Kubernetes Service (VKS) is the Kubernetes runtime built directly into VMware Cloud Foundation (VCF). With CNCF certified Kubernetes, VKS enables platform engineers to deploy and manage Kubernetes clusters while leveraging a comprehensive set of cloud services in VCF. Cloud admins benefit from the support for N-2 Kubernetes versions, enterprise grade security, and simplified lifecycle management for modern apps adoption.

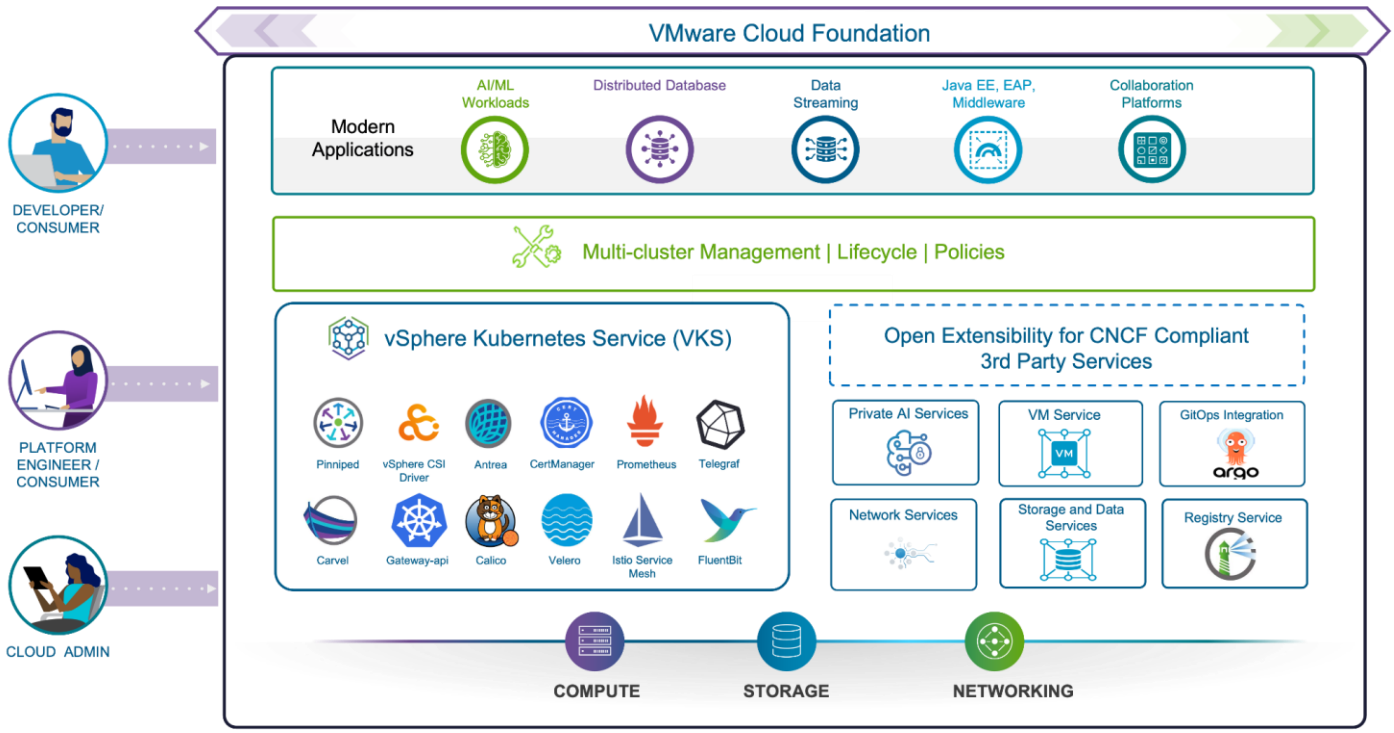

Figure 1: VKS on VCF Ecosystem

Symantec SiteMinder

Symantec® SiteMinder secures the modern enterprise through a unified, DevOps-friendly access management platform enabling secure access to cloud, mobile, and web apps through six key features:

- **Authentication Management.** SiteMinder enforces the appropriate level of login credentials and mechanisms based on context and risk.
- **Identity Federation.** SiteMinder provides frictionless access across identity providers and hybrid environments through native support for OpenID Connect, OAuth, and SAML.
- **Single Sign-On.** SiteMinder streamlines access across hundreds to thousands of cloud, mobile, and web applications by providing single sign-on services.
- **Authorization Management.** SiteMinder grants or denies access to protected resources by enforcing consistent security policies based on contextual data, resource requested, and risk.
- **Session Management.** SiteMinder enables continuous identity and device verification and prevents session hijacking by monitoring user activity as they engage with your apps.
- **Enterprise Scalability and Management.** SiteMinder achieves global service performance and availability through policy and session stores with distributed caching and seamless failover and/or failback with automatic data synchronization. SiteMinder also provides REST interfaces for policy creation and management as well as authentication and authorization services.

With these core features, SiteMinder applies the appropriate level of security to authenticate and authorize users across your hybrid environment with minimal impact to user experience.

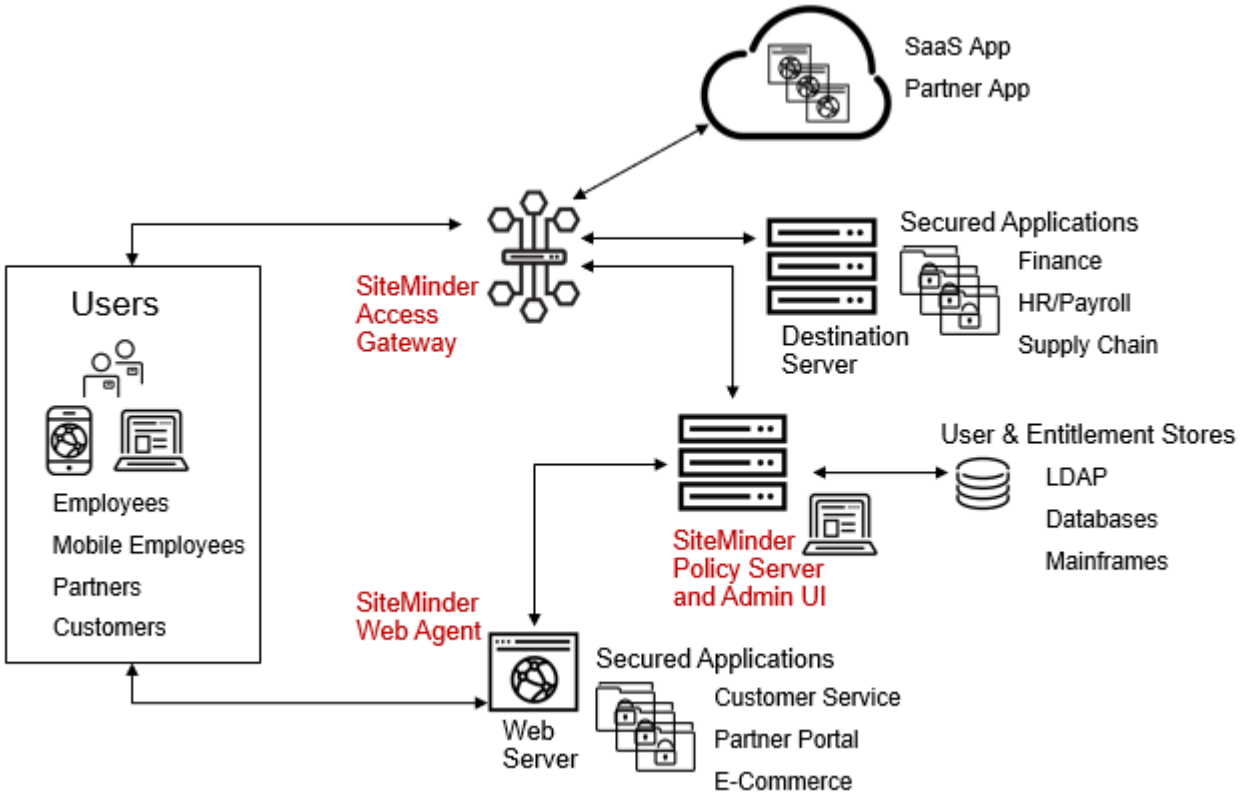

Figure 2: Typical SiteMinder Environment

Solution Architecture

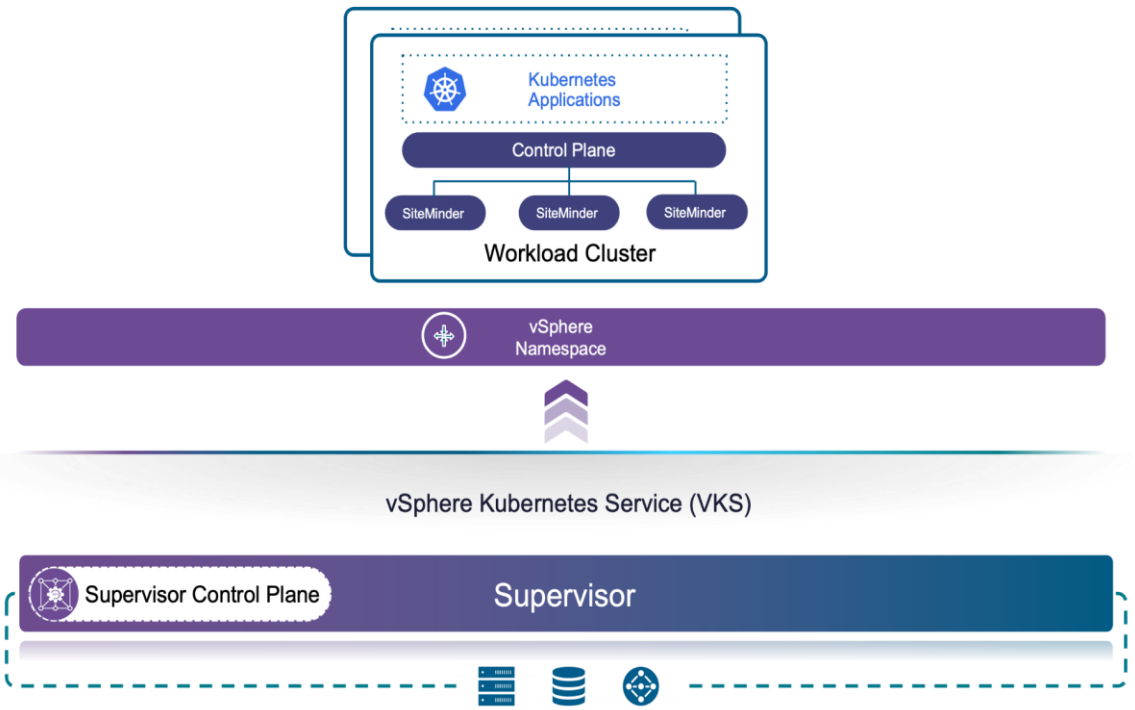

Figure 3: Solution Architecture Diagram of SiteMinder on VKS

Component	Version	Notes
SiteMinder for Containers	12.9	Symantec SiteMinder support matrix (VKS certified)
vSphere Kubernetes Service	3.4	
vSphere Cloud Foundation	9.0	
Kubernetes version	1.32	VKr (vSphere Kubernetes Release)
Helm	3.19	

Typical SiteMinder Components Deployed in VKS environment

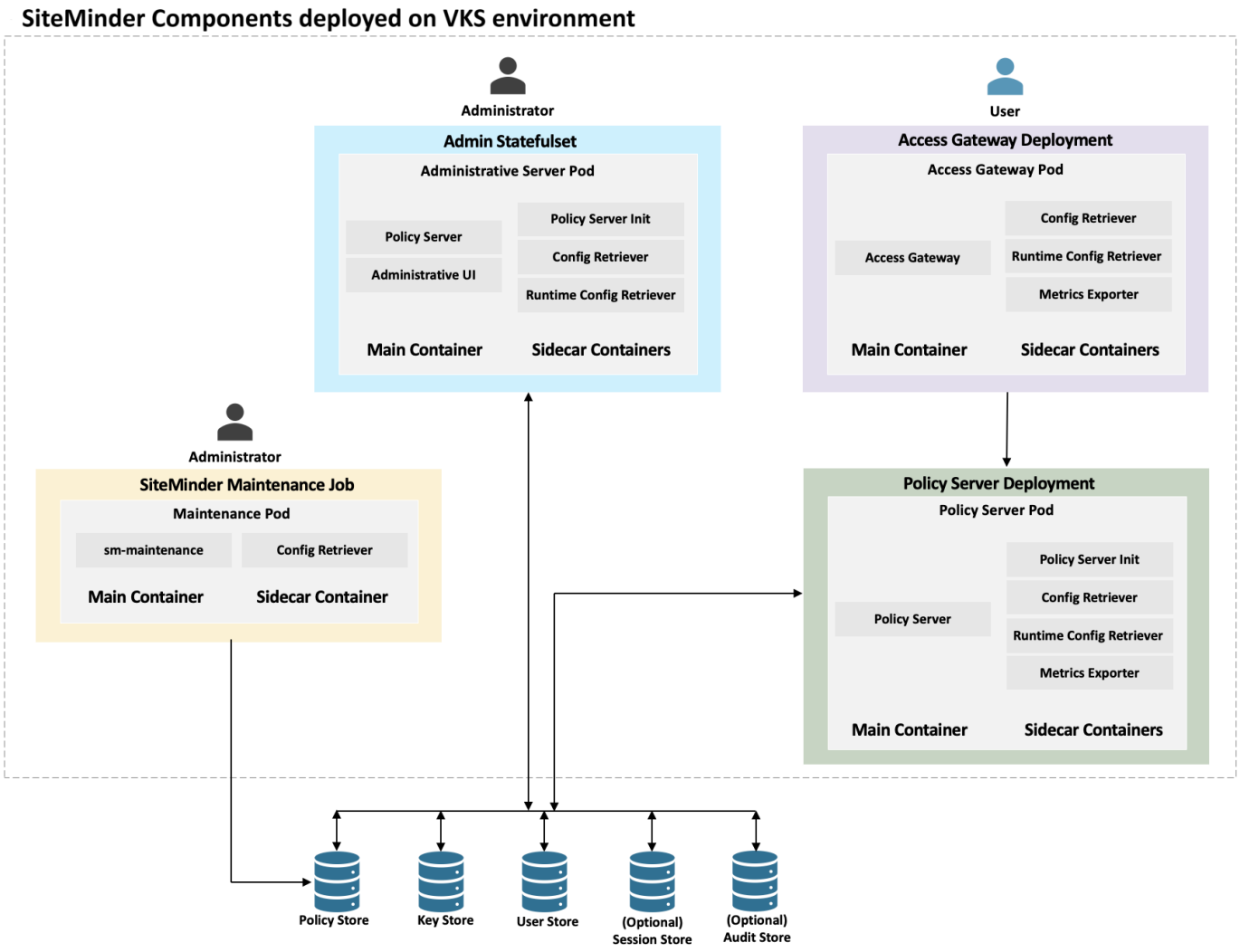

Figure 4: Typical SiteMinder Components Deployment

Deployment Of VKS Cluster

1. Create a context in the provided cluster with the following command:
   vcf context create <ContextName> --endpoint=<SupervisorIP> --insecure-skip-tls-verify -u <UserName> --workload-cluster-namespace=<ClusterNameSpace> --workload-cluster-name=<ClusterName>
2. Upon issuing the above command will prompt for password. Provide password and hit enter.
   ContextName: Name of the context
   SupervisorIP: IP Address of the Supervisor Node
   UserName: Your account userName
   ClusterNameSpace: NameSpace in which cluster is created
   ClusterName: Name of the Cluster provided
3. To validate that the cluster is operational, run the following command and verify the nodes are in ready state

   Command: ***kubectl get nodes***

4. List the contexts and verify the context you created is the current one.

   Command: ***vcf context list***

For more details, please refer to Deploy VKS Clusters documentation.

Deployment of Server Components (Policy Server, Admin UI)

1. Create a namespace for server components with the command: ***kubectl create ns siteminder***

Note: *To avoid the Pod Security error in VKS Kubernetes during the deployment, assign the privileged control to the namespace with the command:* ***kubectl label namespace siteminder pod-security.kubernetes.io/enforce=privileged***

---

2. Refer the Product Documentation For Server Components Deployment using helm charts: TechDocsLink
3. Once the deployment is done, verify the PolicyServer and AdminPolicyServer pods are in "Ready" State and the Status of them is shown as "Running". If not, verify the logs for any configuration errors with the command: ***kubectl logs adminpolicyserver-siteminder-admin-0 -n siteminder***
4. Execute the command to see the ports and host address on which the admin ui could be accessible: ***kubectl get ing -n siteminder***

Deployment of Access Gateway

1. Create a namespace for Access Gateway with the command: ***kubectl create ns cassoag***

Important: *To avoid the Pod Security error in VKS Kubernetes during the deployment, assign the privileged control to the namespace with the command:*

kubectl label namespace cassoag pod-security.kubernetes.io/enforce=privileged

2. Refer the Product Documentation For AG Deployment using helm charts: TechDocsLink
3. Once the deployment is done, verify the Access Gateway pod is in Ready State and Status of them is shown as Running. If not, verify the logs for any configuration errors with the command: ***kubectl logs agserver-siteminder-access-gateway -n cassoag***
4. Execute the command to see the ports and host address on which the AG server could be accessible: ***kubectl get ing -n cassoag***

Deployment of Enclave Services

1. As a prerequisite, deploy the SiteMinder Infra chart to deploy Prometheus Adapter and Fluent Bit for autoscaling and logging the services that are deployed in the SiteMinder containers. Refer Product Documentation: TechDocsLink
2. Create a namespace each for logging and monitoring with the commands:
   kubectl create ns logging
   kubectl create ns monitoring

Important: *To avoid the Pod Security error in VKS Kubernetes during the deployment, assign the privileged control to the namespaces with the command:* ***kubectl label namespace <namespace> pod-security.kubernetes.io/enforce=privileged***

3. *For Observability we used to* deploy Enclave Services, please refer to the Documentation here: EnclaveServicesDeployment.

Note: *For downloading Bitnami Secure Images (BSI) use your customer entitlement to download it. For more details on downloading and Bitnami Secure Images FAQ is mentioned here.*

SiteMinder Solution Validated

- Server Components (Policy Server and Admin UI) successfully deployed on VKS.
- Access Gateway successfully deployed and configured on VKS.
- Basic Object creations such as Domain, Agent, Auth Scheme, User Directory through Admin UI were verified
- Authentication and Authorization functionality verified.
- OIDC functionality verified.

- Integrating SiteMinder components with Enclave services such as Elastic Search and Kibana for logging, Prometheus and Grafana for monitoring and verifying the data is shown on those tools.
- Autoscaling of Policy Server and Access Gateway verified.

Conclusion

In conclusion, deploying SiteMinder on vSphere Kubernetes Service (VKS) within VMware Cloud Foundation (VCF) transforms infrastructure management into streamlined application operations. VKS provides enterprise-grade Kubernetes with integrated Cloud Native Storage (CNS) for persistent data management—essential for maintaining SiteMinder's application state. This platform simplifies scaling, failover, and hardware lifecycle tasks while improving resource utilization and deployment density. By standardizing on VKS/VCF, organizations gain Kubernetes agility with VMware reliability, ensuring SiteMinder infrastructure is resilient, scalable, and ready for modern demand.

Reference

- *VMware Cloud Foundation*
- *vSphere Kubernetes Service*
- *SiteMinder Solution*
- *Siteminder 12.9 Platform Support Matrix*

About the Author

Krishna Kanth Annamreddy (SiteMinder), Software Engineer, Broadcom wrote the original version of this paper

The following reviewers also contributed to the paper contents:

- Mallikharjuna Chari Srisaila Kolagani (SiteMinder) Software Engineer, Broadcom
- Palani Murugan (VCF) Product Marketing Engineer, Broadcom
- Mark Xu (VCF) Product Marketing Engineer, Broadcom

Item No: vmw-bc-wp-tech-temp-a4-word-2024 1/24