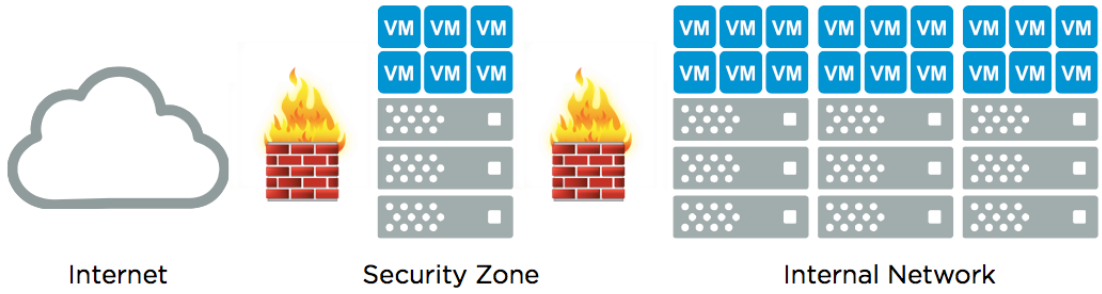
SOLUTION OVERVIEW

VMware vSAN

Security Zone Deployment

VMware vSphere Clusters in Security Zones

A security zone, also referred to as a “DMZ," is a sub-network that is designed to provide tightly controlled connectivity to an organization’s internal IT infrastructure and applications. A security zone typically contains external-facing services that are accessible from untrusted networks such as the Internet. Other common use cases for security zones are internal isolation for classified environments or development infrastructures. The primary purpose of this architecture is adding another layer of security to further reduce the risk of unauthorized access to an organization’s internal network, applications, and data.



One of the most significant threats to security in any environment is misconfiguration. Complexity increases the possibility of misconfiguration, which could lead to potential security incidents. VMware vSphere® uses “bare-metal” virtualization, so the hypervisor interfaces directly with server hardware without the need for a more complex, general operating system. This approach reduces the attack surface and helps safeguard from OS-related vulnerabilities making it the most robust and secure virtualization platform in the industry—an excellent platform for running workloads in security zones.

Examples of workloads typically found in security zones include web servers, email gateways, and proxy services. It is very common for these workloads to have high availability requirements. Features such as vSphere High Availability, vSphere Fault Tolerance, and vSphere Distributed Resource Scheduler™ help protect virtualized applications and services from downtime associated with hardware failures and resource contention. These features require shared storage, which means access to internally hosted storage networks (SAN and NAS) are commonly extended to security zones. This potentially opens up additional options for hackers to gain access to internal resources and leads to more complex firewall configurations. Another option is a dedicated storage appliance contained within the security zone, but this solution can be expensive and add management overhead.

Compute and storage resources for a security zone are ideally very secure, simple to implement, cost-effective, and provide the performance and availability levels necessary to run and protect critical, external-facing workloads. vSphere and VMware vSAN™ provide the hyper-converged infrastructure (HCI) best suited to meet these requirements.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by US and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

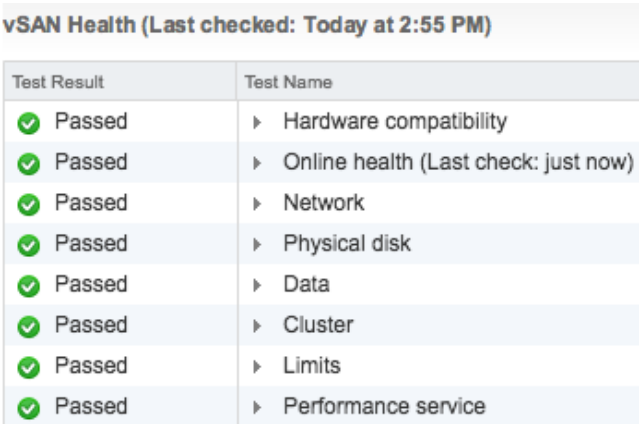
Why vSAN for a Security Zone?

vSAN is VMware's software-defined storage solution for HCI. vSAN and vSphere provide a complete, natively integrated platform consisting of compute, network, and storage resources that are secure and isolated from the rest of the infrastructure. Since disks internal to the vSphere hosts are used to create a vSAN datastore, there is no dependency on external shared storage appliances. Virtual machines can be assigned specific storage policies based on the availability and performance needs of the application. External-facing workloads benefit from dependable storage and predictable performance characteristics while minimizing risk.

vSAN is built on an optimized I/O data path in the vSphere hypervisor. It is managed as a core component of a vSphere environment meaning separate administration tools and connections are not required. This minimizes the attack surface and complexity of the compute and storage infrastructure. Lower complexity reduces the chances of a misconfiguration that could lead to vulnerability. Virtual machine-centric storage policies are created and assigned for various workload types. Policies are based upon the availability and performance services provided by vSAN. These policies can be modified and reassigned, as needed, with no downtime.

Access to the vSAN datastore is confined to the hosts in the same vSAN cluster. A dedicated HCI with vSphere and vSAN help ensure controlled access, predictable performance, and availability of applications and services in a security zone without increasing risk.

Running workloads on a separate compute and storage platform facilitates more flexibility with maintenance schedules. vSAN includes a health dashboard, which automatically monitors and alerts on items such as overall disk health, hardware compatibility list (HCL) compliance, network connectivity issues, and high utilization. If an alert is raised, administrators can easily and quickly start assessing the issue by clicking the Ask VMware button in the vSAN Health user interface, which takes them directly to the relevant VMware knowledge base article. Timely alerts and issue resolution is one more way vSAN enables a secure and stable platform for business critical applications.

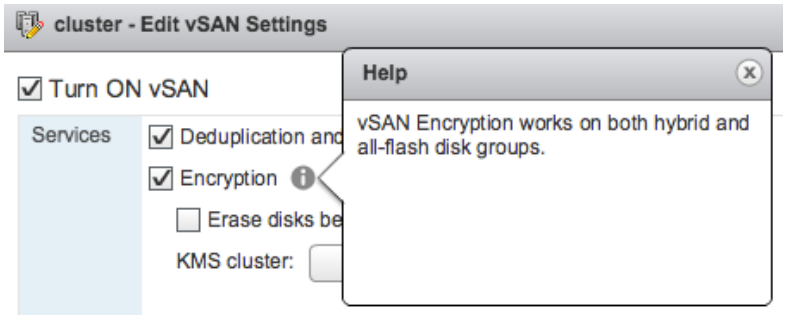


Native Data at Rest Encryption

vSAN encryption is an option for vSAN datastores to further improve security and provide compliance with increasingly stringent regulatory requirements. Since vSAN encryption is native to vSAN, it eliminates the extra cost, limitations, and complexity associated with procuring and maintaining self-encrypting drives.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by US and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



A Key Management Server (KMS) is required to enable and use vSAN encryption. Multiple KMS vendors are compatible including HyTrust, Gemalto (SafeNet), Thales e-Security, CloudLink, and Vormetric. After a trust relationship has been set up between VMware vCenter® Server and the KMS cluster, vSAN encryption is enabled with just a few mouse clicks.

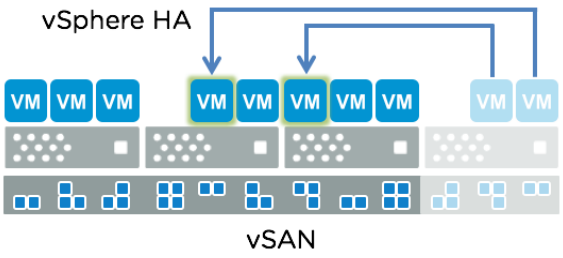
vSAN datastore encryption is enabled and configured at the datastore level. In other words, every object on the vSAN datastore is encrypted when this feature is enabled. Data is encrypted using an AES 256 cipher when it is written to persistent media in the cache and capacity tiers of a vSAN datastore. Encryption occurs just above the device driver layer of the vSphere storage stack, which means it is compatible with all vSAN features such as deduplication, compression, and RAID-5/6 erasure coding.

vSAN with vSphere Availability

The use of local disk datastores without vSAN introduces risk to application uptime. For example, only one copy of a virtual machine's files is stored on a local disk. If that disk fails, the virtual machine files must be restored from backup media, which is time consuming and unreliable. It is possible to create a second copy of virtual machine files on another disk, but the process is not automatic and must be performed frequently. The recovery from this second copy would also be a manual process increasing risk and recovery time.

vSAN addresses these challenges by aggregating local disks into a shared datastore distributed across hosts in the cluster. vSAN features a storage policy rule called "Primary level of failures to tolerate" or "PFTT," which defines the number of replicas of a virtual machine's files to distribute across physical nodes in the vSAN cluster. For example, when PFTT = 1, vSAN will create and maintain two mirrored replicas of the virtual machine's files and place them on separate hosts. If a disk or host containing one of those replicas is offline, the data is still accessible from the other replica.

vSphere HA requires shared storage and vSAN is tightly integrated with vSphere HA. If a host fails, virtual machines that were running on the failed host are automatically rebooted by vSphere HA on other hosts in the cluster to minimize downtime. vSphere HA can also monitor guest operating systems and automatically reboot a virtual machine in the event of an operating system failure such as a Windows blue screen.



vSphere Fault Tolerance™ is also compatible with vSAN and provides continuous availability for applications with up to four virtual CPUs in the event of a host failure.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by US and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

A variety of data protection solutions are available to back up and recover virtual machines and applications in a vSAN cluster. Check with your data protection vendor to verify support and look for the "VMware Ready for vSAN" logo. Virtual machine replication solutions such as Dell EMC RecoverPoint® for Virtual Machines and VMware vSphere Replication™ works seamlessly with vSAN to enable rapid, reliable per-virtual machine recovery.

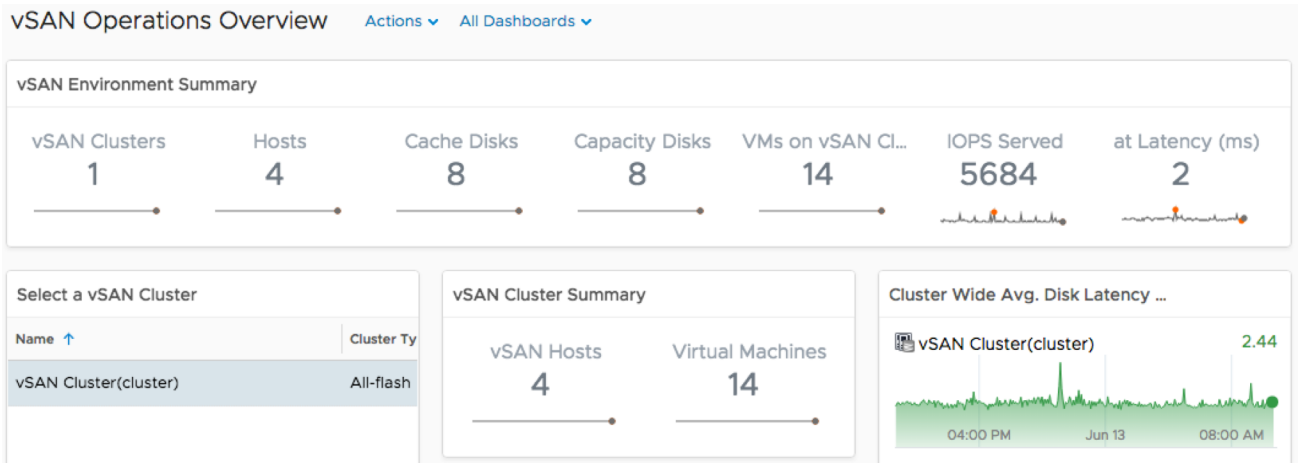
vSAN Performance

vSAN is uniquely embedded in the vSphere hypervisor kernel and sits directly in the I/O data path. It can deliver the highest levels of performance without taxing the CPU or consuming high amounts of memory resources, as compared to other virtual storage appliances that run separately on top of the hypervisor. All-flash vSAN configurations provide excellent performance with predictable, low latencies. A combination of magnetic and solid state drives can be used to enable flash-accelerated hybrid configurations.

Specific rules such as "Number of disk stripes per object" and "Flash read cache reservation (%)" can be used to accelerate read-intensive workloads—especially in hybrid vSAN configurations. With vSAN, it is possible to apply policies with precision. For example, database servers are commonly deployed with the guest OS on one virtual disk and databases on other virtual disks. A storage policy that reserves a higher percentage of flash read cache could be assigned specifically to the virtual disks containing databases to help guarantee performance.

Visibility and Proactive Notifications with vRealize Operations

vSAN includes a health check feature to monitor items such as network connectivity, disk capacity, component metadata, and compliance with the hardware compatibility list (HCL). While this might be sufficient in many cases, enhanced visibility and management capabilities across vSAN clusters at multiple locations are available with VMware vRealize® Operations™. vRealize Operations Manager includes dashboards for vSAN such as Capacity Overview, Optimize vSAN Deployments, and Operations Overview.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by US and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

vRealize Operations features predictive analytics and smart alerts to help ensure optimum performance and availability of applications and infrastructures. vRealize Operations Manager enables administrators to monitor several factors such as read and write IOPS, throughput, latency, cache hits, write buffer utilization, and capacity.

Capacity utilization and time remaining metrics are also included. vRealize Operations analyzes consumption trends and provides estimates on the amount of time remaining before resources are exhausted. This makes it easier for administrators to procure additional capacity in a timely manner to avoid project delays and more serious issues such as application downtime due to lack of free space.

Easily Add Capacity without Downtime

vSAN is a distributed architecture that allows for elastic, non-disruptive scaling. Compute and storage capacity is scaled out simply by bringing a new host into the cluster. Storage capacity and performance can be scaled up independently by adding new drives to existing hosts. This "grow-as-you-go" model provides predictable, linear scaling for remote office environments with affordable investments spread out over time.

Summary

vSAN and vSphere provide the best HCI platform for running virtual machine workloads requiring predictable performance and availability in secure environments. vSphere has achieved multiple security certifications and has a proven track record. vSphere and vSAN is the first and only HCI solution that is part of a DISA STIG. The integration of vSAN with vSphere reduces risk through policy-based management and role-based access control. Important services such as external-facing web sites, email, and employee remote access can benefit from shared storage without the cost and complexity of dedicated storage hardware. Virtual machine-centric storage policies are created, assigned, and modified, as needs change in the environment. Maintenance windows are easier to schedule and there are features such as vSphere HA and vSphere Replication to enable rapid recovery from unplanned downtime. vSAN health monitoring is included and, optionally, vRealize Operations Management Pack for Storage Devices provides multiple vSAN dashboards for proactive alerting, heat maps, device and cluster insights, and streamlined issue resolution.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by US and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.