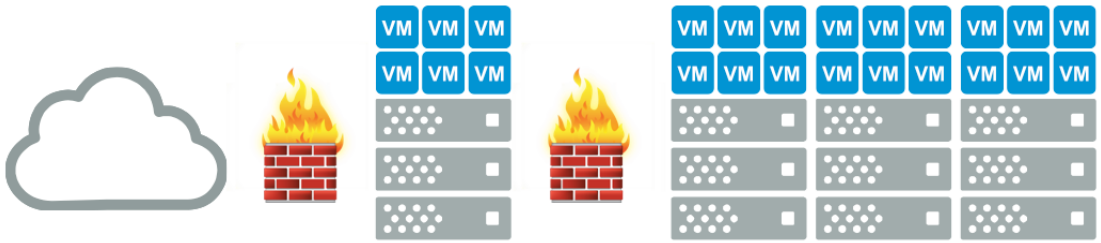
VMware Virtual SAN

Security Zone Deployment

VMware vSphere Clusters in Security Zones

A security zone, which is 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 computer hardware without the need for a more complex, general host operating system such as Windows or Linux. This approach reduces the attack surface and helps safeguard vSphere 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 creates another possible avenue for malicious attacks.

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

Why Virtual SAN for a Security Zone?

Virtual SAN is VMware's software-defined storage solution for HCI. Virtual SAN and vSphere can provide a complete, natively integrated platform consisting of compute, network, and storage resources that are easily isolated from the rest of the infrastructure. Since disks internal to the vSphere hosts are used to create a Virtual SAN 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 without increasing risk.

Virtual SAN 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 underlying compute and storage infrastructure. Lower complexity reduces the chances of a misconfiguration that could lead to vulnerability. Virtual machine-centric storage policies can be created and assigned for various workload types. Policies are based upon the availability and performance services provided by Virtual SAN. These policies can be modified and reassigned, as needed, with no downtime.

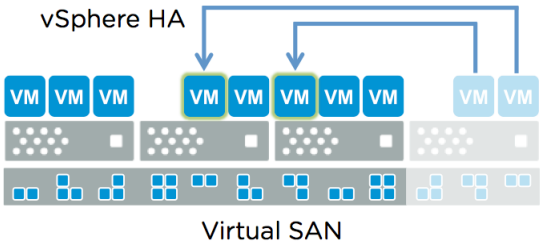
Access to the Virtual SAN datastore is confined to the hosts in the same Virtual SAN cluster. A dedicated HCI with vSphere and Virtual SAN help ensure controlled access, predictable performance, and availability of applications and services in a security zone without increasing risk. Running workloads on a separate compute and storage platform also facilitates more flexible maintenance schedules.

Virtual SAN includes a health check plugin for the vSphere Web Client, which automatically monitors and alerts on items such as overall disk health, hardware compatibility list (HCL) compliance, network connectivity issues, and utilization.

Virtual SAN with vSphere Availability

The use of local disks without Virtual SAN 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, in some cases, 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 to minimize data loss. The recovery of a second copy would also be a manual process in further increasing risk and recovery time.

Virtual SAN addresses these challenges by aggregating local disks into a shared datastore distributed across hosts in the cluster. Virtual SAN features a storage policy rule called "Number of failures to tolerate" or "FTT", which defines the number of copies of a virtual machine's files to distribute across the physical nodes in the cluster. The formula for determining the minimum number of hosts required to support an FTT rule is 2n+1. For example, five hosts are required for FTT=2.



vSphere HA requires shared storage and Virtual SAN 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 a failure such as a Windows blue screen.

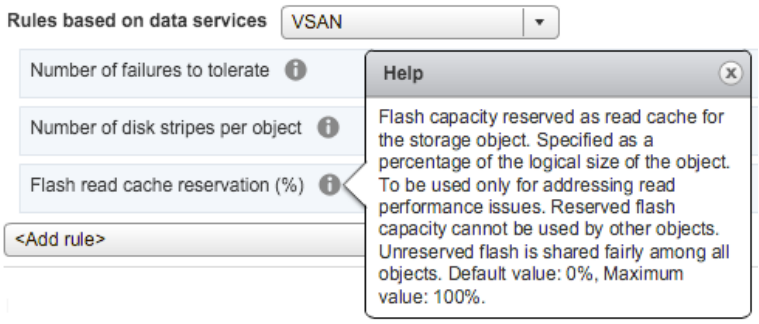
vSphere Fault Tolerance™ is also compatible with Virtual SAN and provides continuous availability for applications with up to four virtual CPUs in the event of a host failure.

A variety of data protection solutions are available to back up and recover virtual machines and applications in a Virtual SAN cluster including VMware vSphere Data Protection™. VMware vSphere Replication™ works seamlessly with Virtual SAN to enable rapid recovery with per-virtual machine a recovery point objective (RPO) as low as five minutes.

Virtual SAN Performance

Virtual SAN is uniquely embedded in the vSphere hypervisor kernel. It is able to deliver the highest levels of performance without taxing the CPU or consuming high amounts of memory resources, as compared to other storage virtual machine appliances that run separately on top of the hypervisor. A combination of magnetic and solid state disks is used to enable flash-accelerated hybrid architectures. This approach provides a good balance of performance and price.

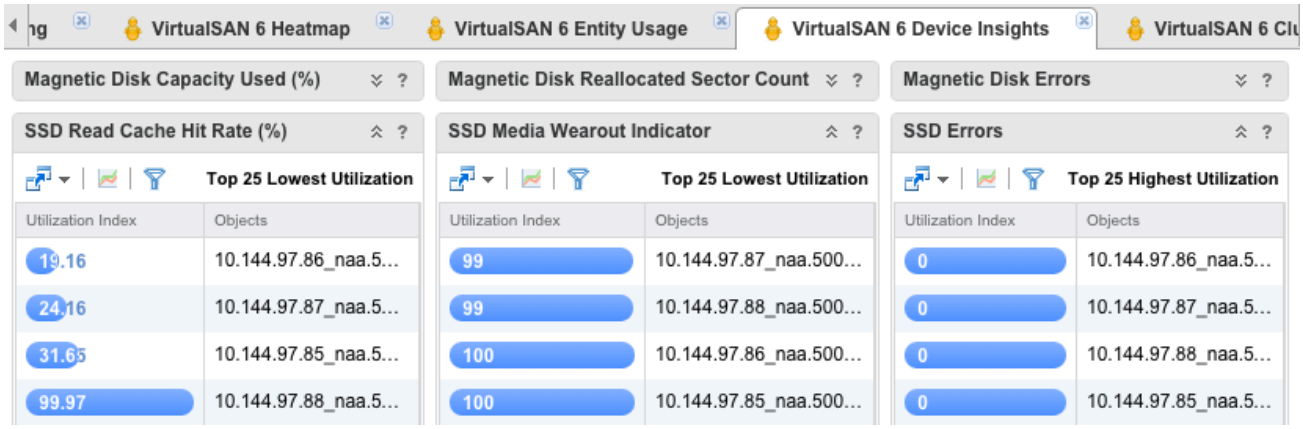
Specific rules such as "Number of disk stripes per object" and "Flash read cache reservation (%)" can be used to further accelerate read-intensive workloads. With Virtual SAN, it is possible to apply policies with precision. For example, database servers are commonly deployed with the guest OS on one 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.



In most cases, performance can be further enhanced simply by adding more flash capacity and magnetic drives to existing hosts in a cluster. This is true even for a two-node Virtual SAN configuration.

Visibility and Proactive Notifications with vRealize Operations

Virtual SAN 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 Virtual SAN clusters at multiple ROBO locations are available with VMware vRealize® Operations™ Management Pack for Storage Devices.



vRealize Operations features predictive analytics and smart alerts to help ensure optimum performance and availability of applications and infrastructures. The vRealize Operations Management Pack for Storage Devices includes Virtual SAN dashboards enabling administrators to monitor several factors such as throughput, latency, capacity, and cache hits. Device and hardware-specific reports and alerts are provided using SMARTS.

If there is an issue in the environment, vRealize Operations makes it easy to review symptoms and recommendations for remediation. The vRealize Operations Management Pack for Storage Devices can also be used to monitor, alert, and remediate issues for other storage types such as NFS and FC.

Easily Add Capacity without Downtime

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

In hybrid deployments with flash devices and magnetic disks, Virtual SAN delivers top-end performance out of industry-standard hardware by using flash devices for read caching/write buffering and magnetic disks for data persistence to balance performance and cost requirements. If higher performance is needed, an all-flash Virtual SAN architecture can deliver up to 90K IOPS per host with consistent sub-millisecond response times. Virtual SAN Advanced licensing is required for an all-flash configuration.

Summary

Virtual SAN and vSphere is the best platform for running virtual machine workloads requiring predictable performance and availability in security zone environments. vSphere has achieved multiple security certifications and has a proven track record. The integration of Virtual SAN 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. Virtual SAN makes it simple to add capacity using a scale up or scale out approach without incurring downtime. Maintenance windows are easier to schedule and there are features such as vSphere HA and vSphere Replication to enable rapid recovery from unplanned downtime. Virtual SAN health monitoring is included and, optionally, vRealize Operations Management Pack for Storage Devices provides multiple Virtual SAN dashboards for proactive alerting, heat maps, device and cluster insights, and streamlined issue resolution.

Learn More

Virtual SAN Product Page

VMware Security Page

vRealize Operations Product Page

Virtual Blocks Blog

Customer Stories

vmware®

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