What's New in VMware vSAN 6.6

July 05, 2017

Table of Contents

1. Introduction

.

1.1 Enterprise-Class Storage for HCI

VMware vSAN™ is enterprise-class storage for hyper-converged infrastructure (HCI). Native to the VMware vSphere® hypervisor, vSAN delivers flash-optimized, secure storage. It utilizes commodity x86 server components to lower costs up to 50% versus traditional server and storage array architectures.

Seamless integration with vSphere and the VMware ecosystem makes it the ideal storage platform for business-critical applications, disaster recovery sites, remote office and branch office (ROBO) implementations, test and development environments, management clusters, security zones, and virtual desktop infrastructure (VDI). Today, customers of all industries and sizes trust vSAN to run their most important applications.

All-flash configurations provide the highest levels of performance with very low latencies for demanding business-critical applications. Space efficiency features such as inline deduplication and compression minimize capacity consumption, which reduces capital expenditures. Per-virtual machine (VM) storage policy-based management lowers operational expenditures by enabling administrators to manage performance, availability, and capacity consumption with ease and precision. This means no more LUN management.

Many deployment options are available for vSAN. These options range from single, 2-node clusters for small implementations to multiple clusters each with as many as 64 nodes—all centrally managed by vCenter Server. Stretched clusters can easily be configured to enable cross-site protection with no downtime for disaster avoidance and rapid, automated recovery from entire site failure.

vSAN 6.6, the sixth generation of vSAN, is designed to help customers modernize their infrastructure by addressing three key IT needs: higher security, lower costs, and faster performance. For example, vSAN 6.6 further lowers total cost of ownership by providing more resilient, economical stretched clusters that are easy to deploy and maintain.

The industry's first native HCI encryption solution and a highly available control plane is delivered in vSAN 6.6 to help customers evolve without risk without sacrificing flash storage efficiencies. Operational costs are reduced with 1-click firmware and driver updates, as well as, proactive cloud-connected health checks for real-time support.

vSAN has been enhanced with up to 50% greater flash performance enabling customers to scale to tomorrow's IT demands. vSAN storage services are integrated with the Photon Platform with full API management to support container technologies and take advantage of DevOps efficiency.

2. Security

2.1 Native Encryption

vSAN Encryption for data-at-rest is now an option for vSAN datastores to further improve security and provide compliance with increasingly stringent regulatory requirements. vSAN datastore encryption uses an AES 256 cipher. vSAN Encryption is hardware-agnostic, meaning it can be deployed on any supported hardware in all-flash or hybrid configurations. Self-encrypting drives (SEDs) are not required.

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 when it is written to persistent media in both the cache and capacity tiers of a vSAN datastore. Encryption occurs just above the device driver layer of the storage stack, which means it is compatible with all vSAN features such as deduplication and compression, RAID-5/6 erasure coding, stretched cluster configurations. All vSphere features including VMware vSphere vMotion®, VMware vSphere Distributed Resource Scheduler™ (DRS), VMware vSphere High Availability (HA), and VMware vSphere Replication™ are supported.

A Key Management Server (KMS) is required to enable and use vSAN encryption. Nearly all KMIP-compliant KMS vendors are compatible, with specific testing completed for vendors such as HyTrust®, Gemalto®, Thales e-Security®, CloudLink®, and Vormetric®. These solutions are commonly deployed in clusters of hardware appliances or virtual appliances for redundancy and high availability.

Initial configuration is done in the VMware vCenter Server® user interface of the vSphere Web Client. The KMS cluster is added to vCenter Server and a trust relationship is established. The process for doing this varies depending on the KMS vendor, but it is quite simple.

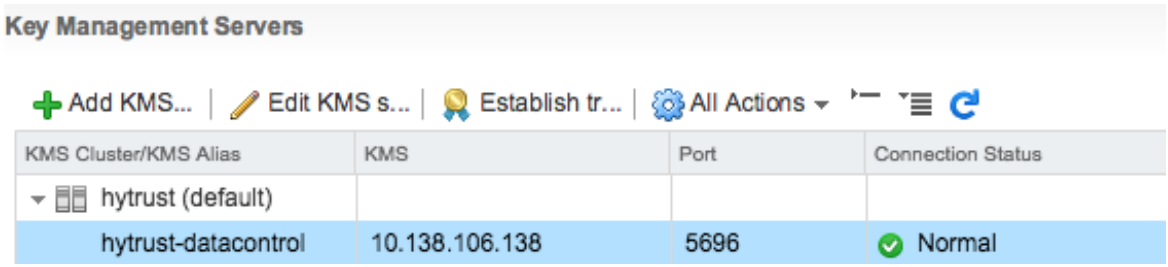

Figure 1. KMS configured for use with vCenter Server

Turning on encryption is a simple matter of clicking a checkbox. Encryption can be enabled when vSAN is enabled or after, with or without virtual machines (VMs) residing on the datastore.

Note: A rolling reformat is required when encryption is enabled. This can take a considerable amount of time—especially if large amounts of existing data must be migrated as the rolling reformat takes place.

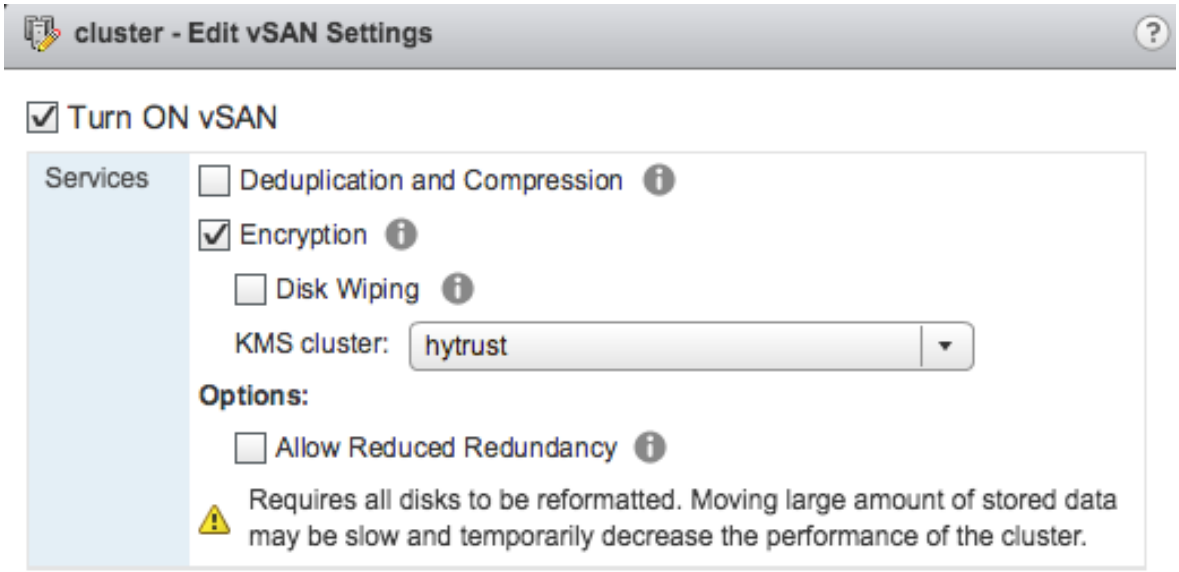

Figure 2. Enabling vSAN Encryption

Encryption keys are transferred to vSAN hosts using the Key Management Interoperability Protocol (KMIP). Industry standards and compliance with regulations often require the generation of new keys on a regular basis. This reduces the risk of a key being exposed or compromised by brute force. Generating new keys is performed in the vSAN UI with just a few clicks.

Encryption can be disabled for a cluster. Like enabling encryption, a rolling disk format change is required. Disabling encryption can take a significant amount of time.

2.2 Compliance

vSAN is native to the vSphere hypervisor and, because of that tight integration, shares the robust security and compliance benefits realized by the vSphere platform. 2-factor authentication methods, such as RSA SecurID® and Common Access Card (CAC), are supported by vSAN, vSphere and vCenter Server. vSAN is part of the core vSphere STIG, offering the only DISA-approved STIG for an HCI solution.

These native features help organizations achieve industry certifications and comply with regulatory requirements. Visit the Security portal on vmware.com for more details on VMware's well-established programs and practices to identify and remediate security vulnerabilities.

3. Management

.

3.1 Proactive Cloud Health Checks

Participating in the Customer Experience Improvement Program (CEIP) enables VMware to provide higher levels of proactive and reactive customer assistance. Benefits of participating in this program include streamlined troubleshooting, real-time notifications and recommendations for your environment, diagnostics, and the potential to remedy issues before they become problems.

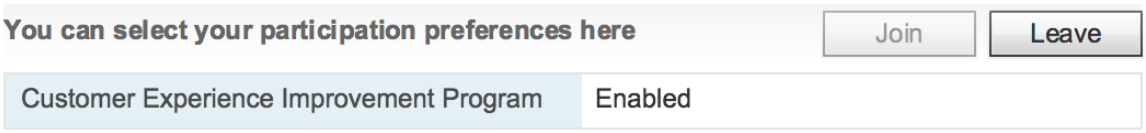

Figure 3. Customer Experience Improvement Program enabled

vSAN Health is cloud-connected. New health checks appear as new VMware Knowledge Base (KB) articles are created and published. An "Ask VMware" button is supplied in the user interface, which guides administrators to the relevant VMware knowledge base article. This benefit is delivered without the need to upgrade vSphere and vSAN. This enhancement consistently provides administrators with latest checks and remedies for optimal reliability and performance. An example is shown below where VMware has detected vSAN and non-vSAN disks attached to the same storage controller.

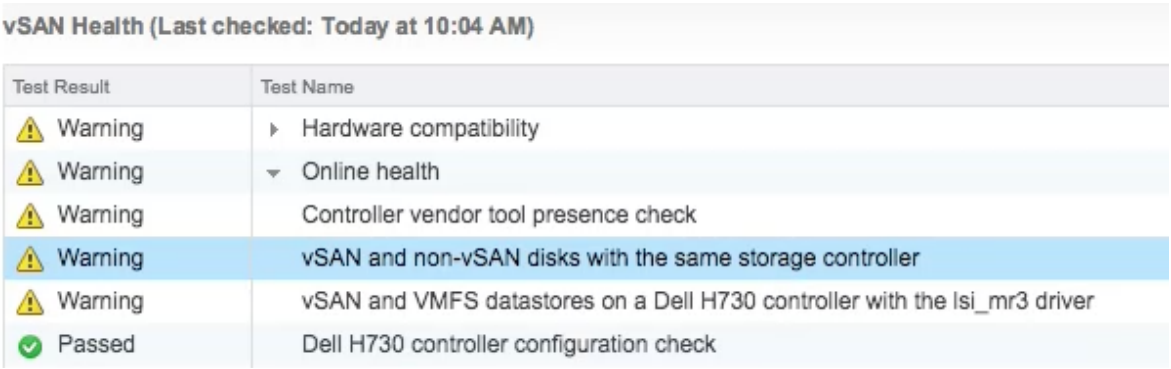

Figure 4. Online health recommendation

The "Ask VMware" button opens the Best practices when using vSAN and non-vSAN disks with the same storage controller (2129050) VMware KB article. New health checks appear as new KB articles are created and published. This benefit is delivered without the need to upgrade vSphere and vSAN. This feature also provides data to VMware, which is correlated and analyzed to help identify opportunities for product improvement. VMware uses this insight to provide customers effective recommendations on design, configuration, and management of vSAN clusters.

Note: CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. For additional information, see VMware Trust & Assurance.

3.2 vSAN Configuration Assist

An important aspect of a healthy vSAN environment is ensuring correct configurations, device firmware, and device drivers. vSAN 6.6 introduces vSAN Configuration Assist to check hardware compatibility, burn-in testing, network configuration, vSAN configuration, and adherence to VMware cluster recommendations.

vSAN Configuration Assist simplifies the creation of a VMkernel network adapter for vSAN on each host in a vSAN cluster. The figure below shows a 3-node cluster where the hosts do not have a vSAN vmknic configured. Configuration Assist identifies the issue configuration issue and includes the "Create VMkernel Network Adapter" button. Clicking this button initiates the process of configuring the vSAN vmknics on a virtual distributed switch. It eliminates a manual process and ensures consistency across the cluster. The Ask VMware button opens a relevant VMware knowledge base (KB) article in a new Web browser window.

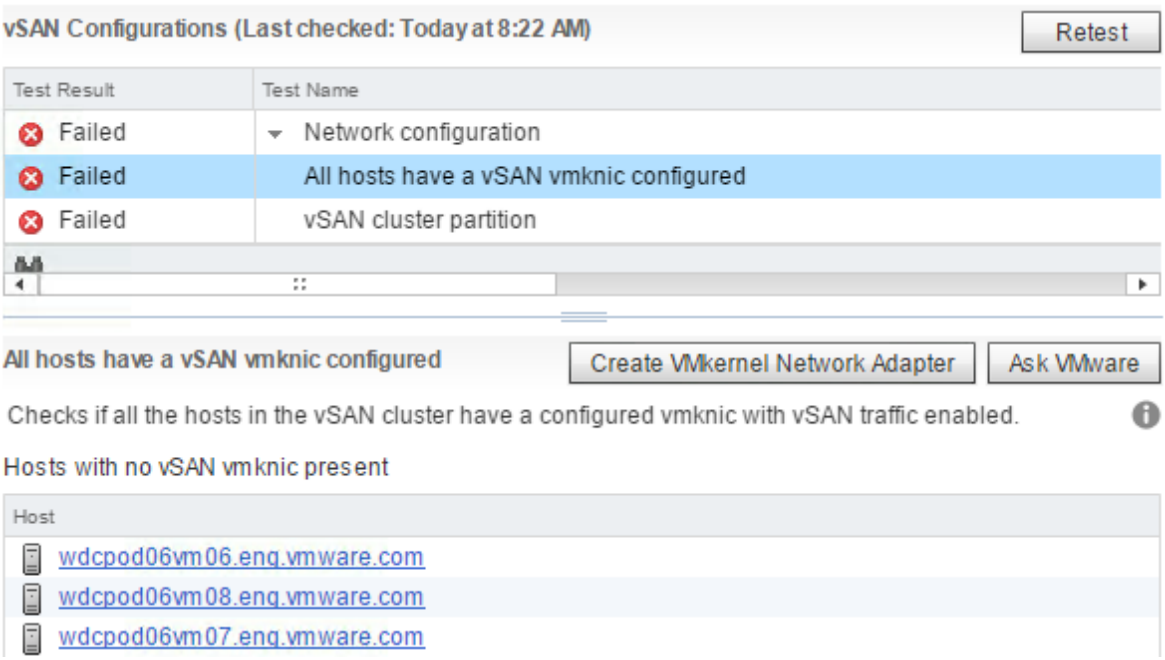

Figure 5. vSAN Configuration Assist Create VMkernel Adapter

3.3 Hardware Lifecycle Management

Reduce common hardware maintenance tasks by automating the hardware update process. Outdated controller firmware and driver versions are identified and the option to download and install the latest supported software is provided. Driver and firmware upgrades to controller hardware can now be initiated by a single click and orchestrated across the entire cluster to streamline hardware lifecycle management. This feature eliminates the need for hardware vendor-specific tools. Automatic download and notifications reduce management overhead and lower the risk associated with manual processes. Software can also be downloaded from an OEM website for offline use.

Note: A subset of the OEMs and server models that run vSAN are currently supported. Many do not yet support automated remediation. In these cases, the vSAN Health UI shows items that need attention, but remediation is a manual process.

3.4 Highly Available Control Plane for Health Checks

Previous versions of vSAN required vCenter Server and the vSphere Web Client server (part of vCenter Server) to be online to check the health of the cluster. vSAN 6.6 adds the ability to perform vSAN health checks using the VMware Host Client when vCenter Server is offline.

Hosts in a vSAN cluster cooperate in a distributed fashion to check the health of the entire cluster. Any host in the cluster can be used to view vSAN Health. This provides redundancy for the vSAN Health data to help ensure administrators always have this information available. The figure below shows the Network – vSAN Cluster Partition health.

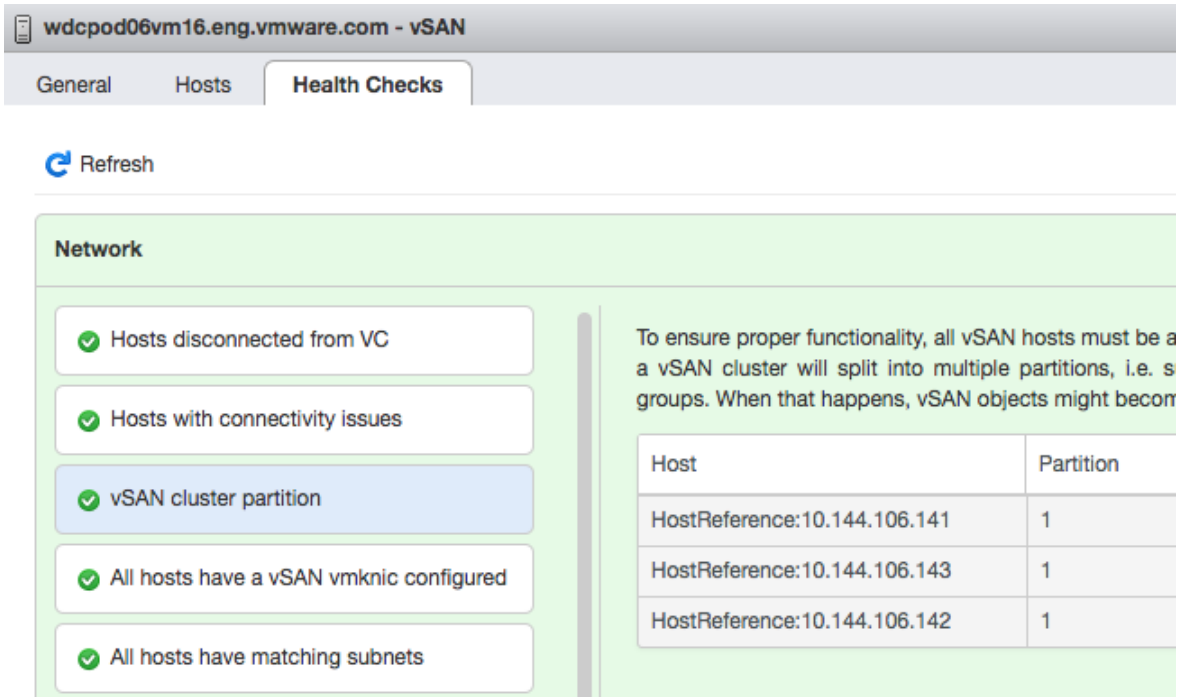

Figure 6. vSAN Health in the VMware Host Client

Command line functionality is keeping pace with information available in the vSAN and VMware Host Client graphical user interfaces. Administrators can use "esxcli vsan" commands to check vSAN health, perform debugging, and manage configurations for items such as fault domains, storage policies, and iSCSI targets.

```
Usage: esxcli vsan {cmd} [cmd options]

Available Namespaces:
  cluster               Commands for vSAN host cluster configuration
  datastore             Commands for vSAN datastore configuration
  debug                 Commands for vSAN debugging
  health                Commands for vSAN Health
  iscsi                 Commands for vSAN iSCSI target configuration
  network               Commands for vSAN host network configuration
  resync                Commands for vSAN resync configuration
  storage               Commands for vSAN physical storage configuration
  faultdomain           Commands for vSAN fault domain configuration
  maintenancemode       Commands for vSAN maintenance mode operation
  policy                Commands for vSAN storage policy configuration
  trace                 Commands for vSAN trace configuration
```

Figure 7. esxcli vsan commands

3.5 Health and Performance Monitoring

The vSAN Health function in the vSphere Web Client includes new features. Hardware compatibility checks now include verification of select storage device controllers, controller queue depth and environmental checks for all-flash and hybrid vSAN configurations. Monitoring and alerting has been

added or improved for items such as vSAN encryption, disk balancing, physical disk health, and networking.

Performance monitoring also received some updates including the ability to query and save performance data for specific time ranges, view detailed vSAN network and resynchronization activity, and monitor iSCSI performance. There are new metrics for network adapter throughput, packets per second, and packet loss rate.

3.6 vRealize Management Pack for vSAN

VMware vRealize® Operations streamlines and automates IT operations management. Intelligent operations management from applications to infrastructure across physical, virtual, and cloud environments can be achieved with vRealize Operations. vRealize Operations Management Packs extend the capabilities of vRealize Operations by including prebuilt dashboards that focus on design, management, and operations for a variety of solutions and use cases.

The vRealize Management Pack for vSAN provides additional visibility into and analytics for vSAN environments. An incredible number of metrics are exposed to assist with monitoring and issue remediation. vRealize Operations makes it easier to correlate data from multiple sources to speed troubleshooting and root cause analysis.

3.7 Stretched Cluster Witness Replacement

vSAN 6.6 makes it easier to replace the witness host in a stretched cluster configuration. The capability minimizes the amount of time a stretched cluster must run without a witness in cases where the witness goes offline permanently. An example of this might be a catastrophic failure at the site where the witness host is running.

The Fault Domains and Stretched Cluster section of the vSAN UI has a Change Witness Host button, which opens a simple, three-step wizard to change the witness host. This new feature is shown in the figure below.

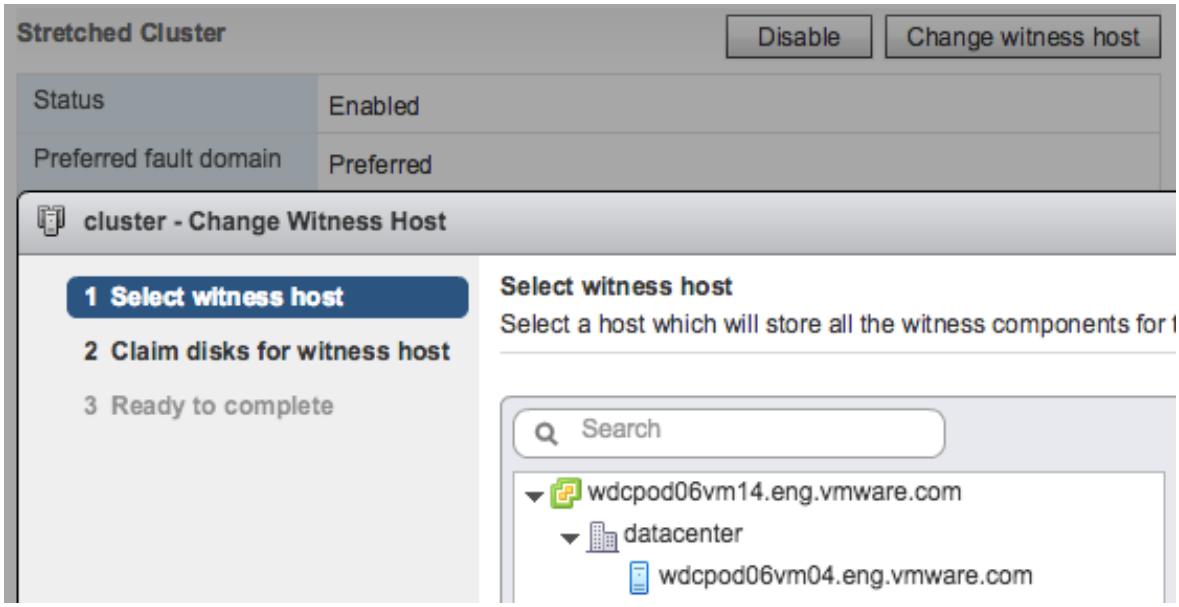

Figure 8. Change Witness Host

3.8 Host Evacuation

A "pre-check" is included in vSAN 6.6 to help ensure adequate capacity remains after a host is evacuated. This function is built into the maintenance mode operation and is also utilized when removing a disk or disk group. Performing a pre-check prior to removing a host provides a better understanding of how the cluster will be impacted. This is one more example of how vSAN reduces complexity, minimizes risk, and lowers operational overhead.

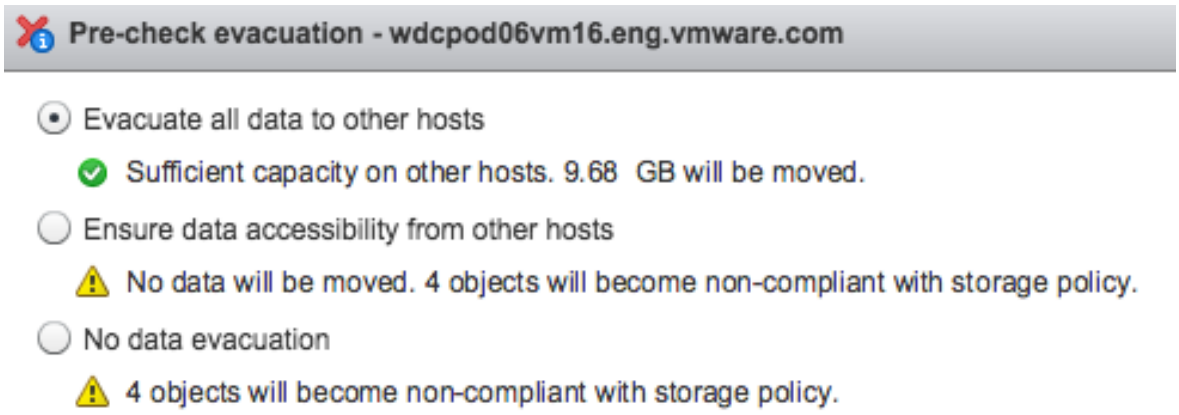

Figure 9. Pre-Check Evacuation

3.9 vSAN API and PowerCLI

Enhancements were made to the vSAN API for organizations that prefer to use a DevOps approach to manage infrastructure. A Host-level API can query cluster-level information. S.M.A.R.T. device data can also be obtained through the vSAN API.

VMware vSphere PowerCLI includes new commandlets to automate items such as performance monitoring, cluster upgrades, and vSAN iSCSI operations.

4. Deployment

.

4.1 Easy Install

Deployment of a vSAN cluster is easier than ever before. The vCenter Server Appliance (VCSA) installation wizard enables administrators to install vSphere on a single host, configure a vSAN datastore, and deploy a VCSA to this datastore. Additional vSphere hosts are then added to finish the build out of the vSAN cluster. This eliminates the need to provision additional disks to run the VCSA prior to enabling vSAN, which simplifies and streamlines the deployment process. This enhancement is especially useful when deploying a new cluster where there is no existing infrastructure to host the VCSA.

The following figure shows a step in the VCSA deployment wizard where the vSAN datastore is initially configured. In this case, three flash devices will be utilized in the host—one for write caching and the other two for capacity.

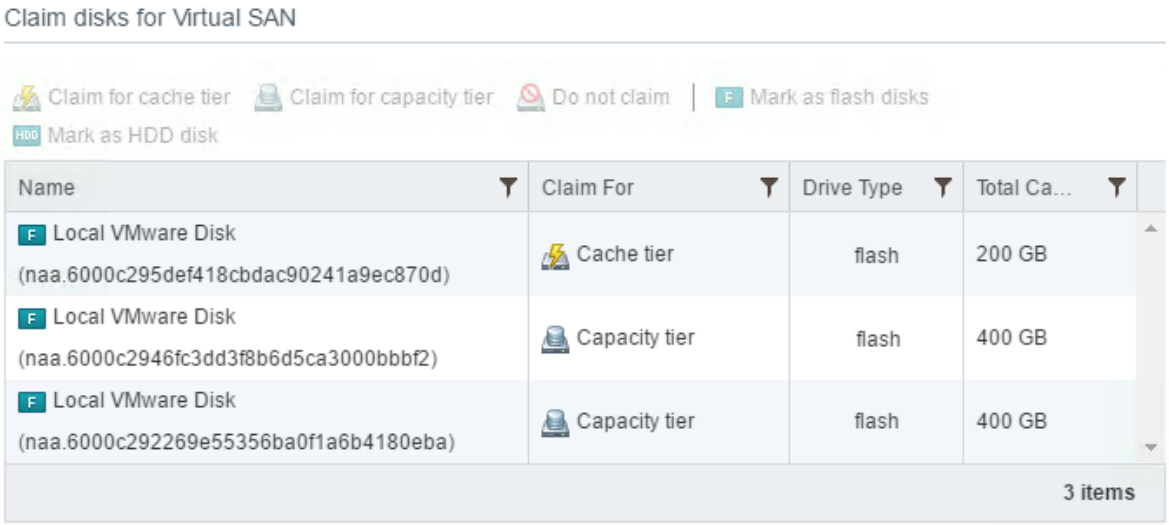

Figure 10. Claiming disks for the vSAN datastore

The figure below shows the selection of the vSAN datastore where the VCSA will be deployed. A datacenter name and cluster name are also specified in this step.

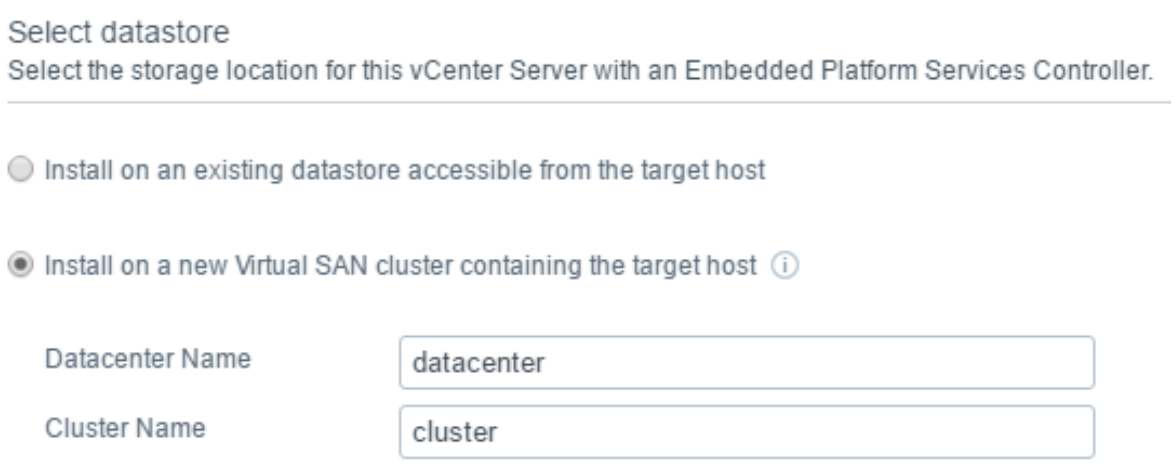

Figure 11. Selecting the new vSAN datastore for the VCSA

With just a few more clicks, a vSAN datastore is configured on the host and the VCSA is deployed on this new datastore.

4.2 Multicast Dependency Removed

Simplicity is an important element in providing a software defined storage solution. vSAN 6.6 takes a major step in simplifying the design and deployment by removing the need for multicast network traffic. This enhancement makes deployment easier for single site and stretched cluster configurations.

When upgrading from prior versions of vSAN to vSAN 6.6, multicast is required until all hosts in the cluster are running version 6.6. vSAN automatically changes to unicast once the upgrade is complete.

Figure 12. Unicast Networking Mode

4.3 Extensibility

Certified solutions for data protection and file services are available through the VMware Ready for vSAN™ program. Customers can deploy these solutions with confidence to extend HCI environments with proven, industry-leading solutions. Using these solutions with vSAN provides benefits such as simplified setup and management, documented recommendations, and robust support.

5. Availability

.

5.1 Stretched Cluster Local Failure Protection

A vSAN stretched cluster mirrors data across sites to provide resiliency from the loss of an entire site. This has been the case since vSAN stretched clusters were first introduced in vSAN version 6.0. vSAN 6.6 builds on this resiliency by including local failure protection, which provides storage redundancy within each site and across sites. Local failure protection is achieved by implementing local RAID-1 mirroring or RAID-5/6 erasure coding within each site.

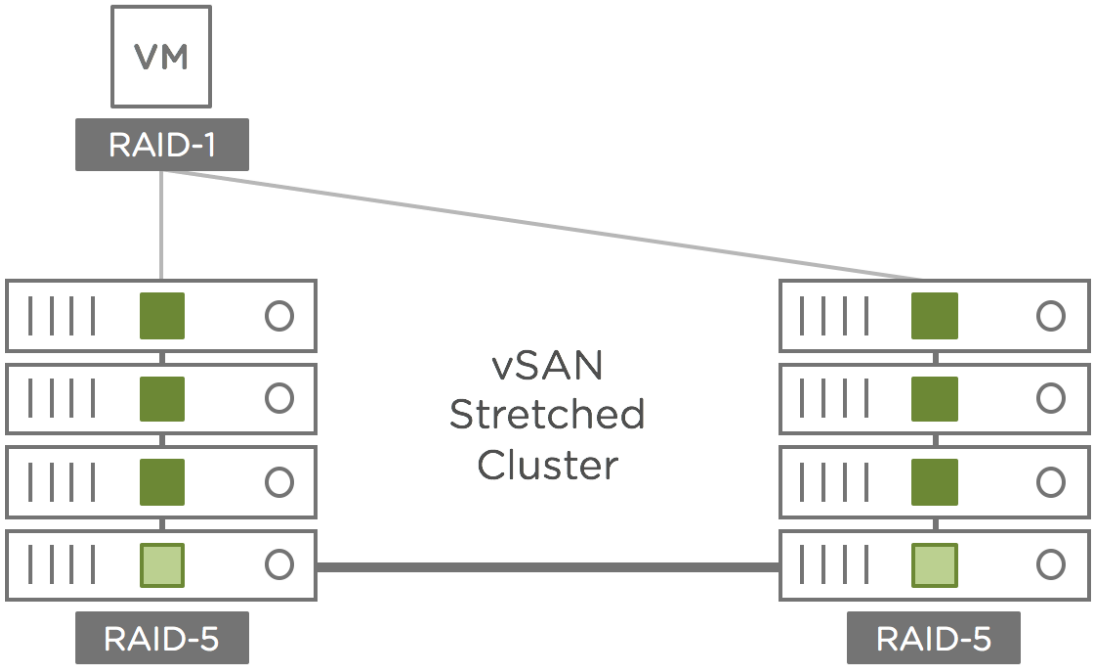

Figure 13. Stretched cluster with local failure protection

This is configured and managed through a storage policy in the vSphere Web Client. The figure below shows rules in a storage policy that is part of an all-flash stretched cluster configuration. The primary level of failures to tolerate is set to 1, which instructs vSAN to mirror data across the two main sites of the stretched cluster. The secondary level of failures to tolerate specifies how data is protected within the site. In the example storage policy below, RAID-5 erasure coding is used, which can tolerate the loss of a host within the site.

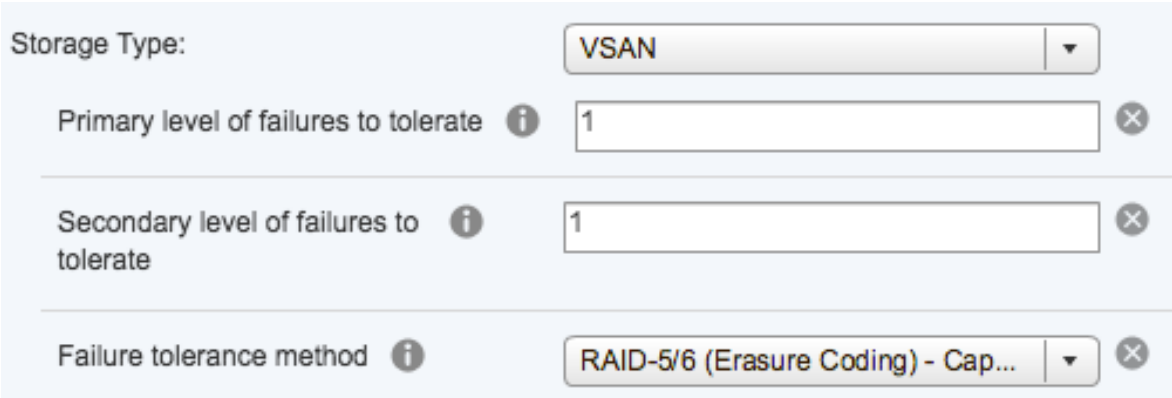

Figure 14. Stretched Cluster with Local Failure Protection Storage Policy Rule

Local failure protection within a stretched cluster further improves the resiliency of the cluster to minimize unplanned downtime. This feature also reduces or eliminates cross-site traffic in cases where

components need to be resynchronized or rebuilt. vSAN lowers the total cost of ownership of a stretched cluster solution as there is no need to purchase additional hardware or software to achieve this level of resiliency.

5.2 Stretched Cluster Site Affinity

vSAN 6.6 improves the flexibility of storage policy-based management for stretched clusters by introducing the "Affinity" rule. You can specify a single site to locate VM objects in cases where cross-site redundancy is not necessary. Common examples include applications that have built-in replication or redundancy such as Microsoft Active Directory and Oracle Real Application Clusters (RAC). This capability reduces costs by minimizing the storage and network resources used by these workloads.

Affinity is easy to configure and manage using storage policy-based management. A storage policy is created and the Affinity rule is added to specify the site where a VM's objects will be stored.

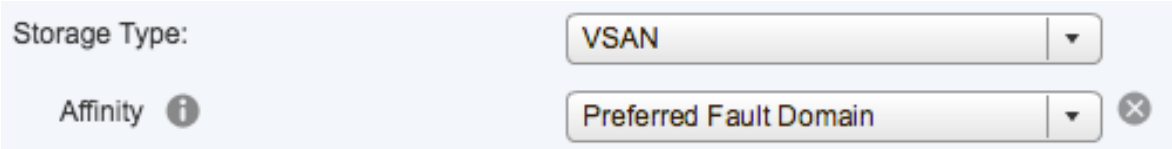

Figure 15. Stretched Cluster Site Affinity Storage Policy Rule

5.3 Degraded Device Handling

VMware continues to improve how vSAN handles hardware issues such as a storage device that is showing symptoms of impending failure. In some cases, storage devices issues are easily detected through errors reported by the device, e.g., SCSI sense codes. In other cases, issues are not so obvious. To proactively discover these types of issues, vSAN will track performance characteristics of a device over time. A significant discrepancy in performance is a good indicator that a problem might exist with a device. vSAN uses multiple samples of data to help avoid "false positives" where the issue is transient in nature.

When failure of a device is anticipated, vSAN evaluates the data on the device. If there are replicas of the data on other devices in the cluster, vSAN will mark these components as "absent". "Absent" components are not rebuilt immediately as it is possible the cause of the issue is temporary. vSAN waits for 60 minutes by default before starting the rebuild process. This does not affect the availability of a VM as the data is still accessible using one or more other replicas in the cluster. If the only replica of data is located on a suspect device, vSAN will immediately start the evacuation of this data to other healthy storage devices.

Intelligent, predictive device failure handling lowers the cost of operations by minimizing the risk of downtime and data loss.

6. Performance

6.1 General

In addition to providing new features in vSAN 6.6, several enhancements are introduced to further increase all-flash performance up to 50% compared to vSAN 6.5. These enhancements make vSAN 6.6 the premier hyper-converged storage solution for running the most demanding business critical applications and services.

6.2 Deduplication and Compression

Deduplication and compression reduces capacity consumption and lowers the cost-per-usable-gigabyte of flash devices. As with any storage platform, these features require slightly higher resource utilization. vSAN 6.6 includes changes to how data is de-staged from the cache tier to the capacity tier to minimize this overhead. Compression metadata compaction reduces overhead for VM and vSAN "backend" I/O. These changes further minimize resource utilization and provide more predictable performance—especially for large numbers of sequential writes.

6.3 Rebuild and Resynchronization Enhancements

vSAN achieves high availability and extreme performance through the distribution of data across multiple hosts in a cluster. Data is transmitted between hosts using the vSAN network. There are cases where a significant amount of data must be copied across the vSAN network. One example is when you change the fault tolerance method in a storage policy from RAID-1 mirroring to RAID-5 erasure coding. vSAN copies the mirrored components to a new set of striped components.

Another example is repair operations such as when a vSAN components are offline due to a host hardware issue. These components are marked "absent" and vSAN waits 60 minutes by default before starting the repair operation. vSAN has this delay as many issues are transient. In other words, vSAN expects absent components to be back online in a reasonable amount of time and we want to avoid copy large quantities of data unless it is truly necessary. An example is a host being temporarily offline due to an unplanned reboot.

vSAN will begin the repair process for absent components after 60 minutes to restore redundancy. For example, an object such as a virtual disk (VMDK file) protected by a RAID-1 mirroring storage policy will create a second mirror copy from the healthy copy. This process can take a considerable amount of time depending on how much data must be copied. The rebuild process continues even if the absent copy comes back online in versions of vSAN prior to 6.6.

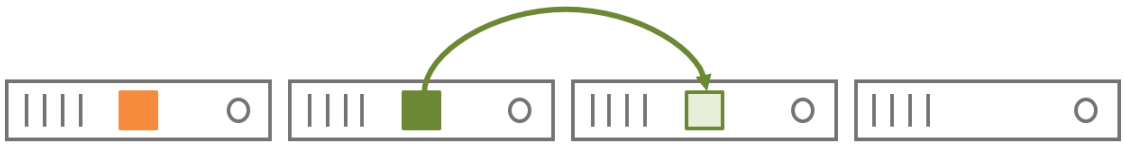

Figure 16. vSAN Component Rebuild

The object repair process is improved in vSAN 6.6. If absent components come back online while vSAN is rebuilding another copy, vSAN will determine whether it is more efficient to continue building an entirely new copy or update the existing copy that came back online. vSAN will restore redundancy using the most efficient method and cancel the other action. This enhancement to vSAN rebuilds improves the speed and efficiency of object repair operations to reduce risk and minimize resource usage.

In cases where there are not enough resources online to comply with all storage policies, vSAN 6.6 will repair as many objects as possible. This helps ensure the highest possible levels of redundancy in environments affected by unplanned downtime. When additional resources come back online, vSAN will continue the repair process to comply with storage policies.

There are a few other operations that can temporarily increase vSAN "backend" traffic flow. Rebalancing of disk utilization is one of these operations. When a disk has less than 20% free space, vSAN will automatically attempt to balance capacity utilization by moving data from that disk to other disks in the vSAN cluster. Achieving a well-balanced cluster from a disk capacity standpoint can be more challenging if there are many large components. vSAN 6.6 improves efficiency by splitting large components into smaller components to achieve a better balance.

Excessive amounts of vSAN backend resynchronization traffic might affect cluster performance. Resynchronization operations in previous versions of vSAN are automated and controlled entirely by vSAN. In other words, administrators are unable to adjust the rate at which resynchronization operations are performed.

vSAN 6.6 introduces the option to adjust the throughput of resynchronization operations. If cluster performance is being severely impacted by excessive resynchronizing activity, you can minimize the impact by reducing the throughput allowed for resynchronizing.

Note: It is highly recommended to use the default setting (throttling disabled). Throttling resynchronization traffic will increase the amount of time needed to rebuild and/or resynchronization components, which increases the risk of downtime.

6.4 Checksum

Native checksum operations in vSAN help ensure data integrity. To further improve performance, checksum read and write paths have been optimized in vSAN 6.6 to avoid redundant table lookups.

6.5 De-staging

vSAN 6.6 includes changes in how data is de-staged from the cache tier to the capacity tier. In rare cases, the buildup of metadata can have a slight impact to VM I/O and resynchronization operations. An example of this is many delete operations, which invokes metadata changes. vSAN 6.6 proactively de-stages data to avoid a buildup of metadata changes. More aggressive de-staging provides more consistent performance and is especially beneficial to write-intensive workloads.

6.6 iSCSI

In addition to de-staging improvements discussed previously, the version of FreeBSD used for the vSAN iSCSI service was upgraded to version 10.3. These changes result in better iSCSI performance in vSAN 6.6.

7. Summary

.

7.1 vSAN is the Leading HCI Storage Solution

VMware vSAN is software-defined storage that powers industry-leading hyper-converged infrastructure systems. vSAN and vSphere work with the broadest ecosystem of hardware platforms and complementary software solutions. Protect current storage investments with the only HCI solution built on policy-based management that extends per-VM storage policies and automated provisioning to modern SAN and NAS storage systems.

vSAN 6.6 delivers the first native HCI security solution with data-at-rest-encryption that is easily enabled with just a few clicks. Native security protects business-critical data from unwanted access and eliminates the need for complicated and costly management and disposal processes.

Simplify ongoing maintenance with proactive cloud-connected health checks that decrease operational costs with real-time support notifications and recommendations. Utilizing anonymized "phone home" data, this new functionality identifies specific issues based on official support documentation and offers recommendations to correct problems and make improvements. Continuous monitoring and management are possible even in rare cases when vCenter Server is offline.

Hardware lifecycle management is improved in vSAN 6.6. Outdated firmware and driver versions are identified and the option to download and install the latest supported software is provided. Software upgrades are initiated by a single click and orchestrated across the entire cluster.

The new vSAN Management Pack for VMware vRealize Operations Manager provides additional options for monitoring, managing and troubleshooting. Expanded automation with vSAN SDK and PowerCLI enables customers to manage vSAN clusters at scale, including vSAN cluster creation, updates, and performance monitoring.

New unicast networking support simplifies the initial setup and ongoing management of vSAN networking, eliminating potential network changes and expanded the flexibility of vSAN to be rapidly deployed in multi-cloud environments.

Reduce the risk of hardware failures impacting availability with new proactive drive evacuation. This helps ensure efficient movement of data out of harm's way before drive failure occurs.

Lower site protection costs with highly available, cost-effective vSAN stretched clusters. Enhanced stretched clusters with local failure protection provide resiliency against local host and entire site failures. With a comprehensive stretched cluster solution, customers can now confidently address an area that is commonly underserved: disaster recovery and business continuity.

Scale to tomorrow with a platform that is ready for today's enterprise workloads as well as next-generation applications and hardware. Build the foundation for a multi-cloud architecture with a common enterprise storage platform that extends from on-premises deployments to the public cloud.