VMware Virtual SAN Health Check Guide

Cormac Hogan
Storage and Availability Business Unit
VMware
v 6.1.0 / September 2015 / GA

Contents

Introduction

VMware's Virtual SAN is designed to be simple: simple to configure, and simple to operate. This simplicity masks a sophisticated and powerful storage product. This simplicity hides a lot of the complexities found in most modern day storage systems. Under the covers, Virtual SAN also has its complexities. While VMware does provide extensive documentation in the form of a Virtual SAN Administrators Guide and Virtual SAN Troubleshooting Reference Manual, there is a desire to continue with the simple approach and highlight, through Health check plugin, the component that may be at fault.

Virtual SAN Health check plugin checks all aspects of a Virtual SAN configuration. It implements a number of checks on hardware compatibility, networking configuration and operations, advanced Virtual SAN configuration options, storage device health as well as virtual machine object health. The health check will provide two main benefits to administrators of Virtual SAN environments:

1. It will give administrators peace of mind that their Virtual SAN deployment is fully supported, functional and operational
2. It will provide immediate indications to a root cause in the event of a failure, leading to speedier resolution times

The purpose of this document is to fully illustrate Virtual SAN Health check plugin. The document will cover how to install the feature, and how to use the feature. It will also provide some context related to the issue highlighted and how t go about problem solving on Virtual SAN.

It is recommended that the Health check plugin be utilized to do initial triage of any Virtual SAN problems. For those who wish to learn more about diagnosis and troubleshooting on Virtual SAN, the *Virtual SAN Troubleshooting Reference Manual* is a good starting point. There is a link at the end of this guide.

One final note is that a new feature called the Virtual SAN Support Assistant is also included. This allows administrators to upload VSAN log bundles directly to their support request (SR) opened with VMware Global Support Services (GSS).

***Note**: Presently, the Virtual SAN Health Services Plugin is only supported with Virtual SAN version 6.0 & 6.1. It is not supported with Virtual SAN version 5.5 at this time.*

Security Considerations

This section will describe the detailed security related information for Virtual SAN health check plugin, including:

1. A list of all external interfaces, ports, and services and which ones need to be open or enabled for proper operation of the product.
2. All resources that need to be protected such as security-relevant configuration files and passwords and the recommended access controls for secure operation.
3. Location of log files and description of how to interpret security related log messages
4. Log-on ID of accounts created during system install/bootstrap and instructions on how to change defaults.
5. Privileges assigned to "service" users.
6. Information on how customers can obtain and apply the latest security update/patch.

Exposed Interfaces, ports and Service

From an ESXi perspective, when the network multicast performance test is triggered from the Virtual SAN Health Check UI or via the relevant Ruby vSphere Console (RVC) command, port 5001 is temporarily opened on each ESXi host in the Virtual SAN cluster. This port is closed when the test completes. No ports are opened on vCenter Server side for this test.

Security Related Resource

VIRTUAL SAN Health check plugin has a configuration file on the vCenter Appliance in/etc/vmware-vsan-health/config.conf that may include the configuration item "proxy password" providing by user, which is security sensitive. On the vCenter Server for Windows, the file is located in %VMWARE_CIS_HOME%\vsan-health\config.conf. Currently we use a file system based protection mechanism, so that the Virtual SAN health user only has the privilege to read and write to this file, preventing other non-privileged users from viewing the password.

Log Location

The default log location for Virtual SAN health check plugin is /var/log/vmware/vsan-health. And user can change it by modifying the configuration item "logdir" in the configuration file under /usr/lib/vmware-vpx/vsan-health. On the vCenter Server for Windows, the file is located in %VMWARE_LOG_DIR%\vsan-health. No security related information is logged in the log file.

Log-on ID Account

On the vCenter Appliance, Virtual SAN Health check plugin creates a local user (vsan-health) under Users (100) group. This happens by default when first booting Virtual SAN health check plugin. It cannot be changed. There is no new user created on the vCenter Server for Windows.

Log-on ID Account Privileges

The vsan-health account will be added into CIS group so that it has the privilege to read/write/execute the java and relevant vCenter Server Appliance related files (e.g. cloudvm-ram-size.log). Also it has the read/execute privilege for its installation root directory, and read/write privilege for the Virtual SAN Health check log and configuration directory.

vCenter Server Privileges

This is the summary of the privilege that will be required by the vCenter server user who wishes to run the Virtual SAN health checks.

1. Cluster System.View/Read

The Cluster *System.View/Read* privileges are needed to be able to carry out the following health checks.

- All Query* API which include all health checks and proactive tests except for creating VM test
- Enable/Disable VSAN health, Enable/Disable Phone-Home, proxy setting.
  - The UI will apply the cluster-edit privilege check again to disable such operation if user hasn't proper privileges).

2. Cluster System.View/Read + Global.Setting

The Cluster *System.View/Read* and the *Global.Setting* privileges are needed to be able to carry out the following health checks.

- Send VSAN Telemetry
- Upload HCL DB From File
- Upload HCL DB From Web
- Set Proxy
- Set Periodical Health Check Time Interval

3. Cluster System.View/Read + Global.Diagnostics

These Cluster *System.View/Read* and the *Global.Diagnostics* privileges are needed to be able to carry out the following health check.

- AttachToSR/PR

4. Cluster System.View/Read + Virtual Machine.Create/Delete

The Cluster *System.View/Read* and the *Virtual Machine.Create/Delete* privileges are needed to be able to carry out the following health checks.

- Create VM Proactive Health Check Test

Upgrade Process

The upgrade process for Virtual SAN health check plugin on the vCenter Server involves two distinct steps. The first step is to upgrade the vCenter Server to the 6.0u1 version. This automatically updates the Virtual SAN health check plugin on vCenter server to version 6.1.0.

The next step is to upgrade the ESXi hosts. If the ESXi hosts were previously running version 6.0, then there are two options:

a) Upgrade the ESXi hosts to version 6.0U1. This version of ESXi has the necessary health check software and no further action is necessary.

b) Upgrade the Health Check VIB on the existing ESXi hosts that are running a lower version than 6.0U1. The VIB is included with the health check software on the vCenter server.

   The ESXi host health check VIB upgrade can be accomplished in a number of ways, but the easiest method is for the user to open the Virtual SAN health main page through Cluster > Manage > Settings > Virtual VSAN > Health, and click the “upgrade” button.

The upgrade process is covered in greater detail later on in this guide.

What's new in Virtual SAN Health Check 6.1.0?

VSAN Health Check 6.1.0 is included with vCenter Server 6.0U1 and ESXi 6.0U1.

The following set of new features and functionality are available in version 6.1.0 of the Virtual SAN Health Check:

- vCenter Events/Alarms support: If the plug-in detects any problem during health checks, events/alarms are surfaced. The backend health check runs periodically every 60 minutes by default. However the check interval is customizable through both vSphere UI and RVC.
- Health check support for VSAN Stretched Cluster: VSAN Stretched Cluster is a new feature of Virtual SAN 6.1. The list of health checks can be found in Appendix A.
- Improved user experience for Health UI installation: VSAN Health Check is now installed by default and automatically enabled when vSphere/ESX 6.0u1 is installed.
- Customers already running health check plugin version 6.0 are automatically upgraded to the new version when the upgrade from vSphere 6.0 GA to vSphere 6.0u1. This is true for both Windows vCenter server and vCenter Server Appliance.
- Unified CEIP (customer experience improvement program) with vCenter.
- Localization – includes German, English, French, Japanese, Korean, simplified Chinese and traditional Chinese.
- Proxy settings will use system default through auto-detection on vCenter, if it is not explicitly set. The proxy is used for sending VSAN CEIP information, support bundles and download latest HCL database.
- A number of bug fixes and UI improvements over version 6.0.

1. Installation & Upgrade - vCenter Server

In the previous 6.0 version of the Virtual SAN Health Check plugin, administrators needed to download the software and install it on the vCenter Server. In the new 6.1.0 version of the Virtual SAN Health Check, the necessary software is bundled with the vSphere 6.0u1 release. This means the Health Service will be installed/upgraded along with the vCenter server installation/upgrade.

1.1.1 Check the install status via vSphere Web Client

Once the services have been installed/upgraded and restarted, a quick way to check that the health check RPM /MSI has been successfully installed on the vCenter server is to run the health check. One of the checks is the installation status. If this passes, the health check has been successfully installed.

1.1.2 Checking the install status via RVC

Another way of checking that the services have been installed/upgraded successfully is to use the following Ruby vSphere Console (RVC) commands against the cluster. For details on how to access the RVC, please refer to the Troubleshooting Reference Manual or the RVC Command Reference Guide for Virtual SAN.

```
> vsan.health.cluster_status <path-to-cluster>
 Configuration of ESX VSAN Health Extension: installed (OK)
 Host 'cs-ie-dell01.ie.local' has health system version '6.1.0' installed
 Host 'cs-ie-dell03.ie.local' has health system version '6.1.0' installed
 Host 'cs-ie-dell04.ie.local' has health system version '6.1.0' installed
 Host 'cs-ie-dell02.ie.local' has health system version '6.1.0' installed
 vCenter Server has health system version '6.1.0' installed
```

As you can see the health check has been installed on both the ESXi hosts and the vCenter server.

For details on how to access RVC, please refer to the Virtual SAN 6.0 Troubleshooting Reference Manual or RVC Reference Guide, links to which are found at the end of this guide.

1.1.3 ESX Agents Resource Pool

When the health check has been deployed, customer will see a new resource pool created called ESX Agents. The Virtual SAN health uses a vSphere component called EAM, ESX Agent Manager. This component requires this resource pool. While this resource pool is harmless to the cluster, customers should note workloads should not be placed in this resource pool.

2. VIB Installation – ESXi 6.x

A VIB, or VMware Installation Bundle, is a VMware software patch. For ESXi 6.0U1, the ESXi hosts already have the Health Check software installed (inbox). No additional upgrade is needed. If you are running ESXi 6.0, each ESXi hosts must have a VIB installed as part of the health check installation process. The Health Check UI in the vSphere web client will prompt you to take this step.

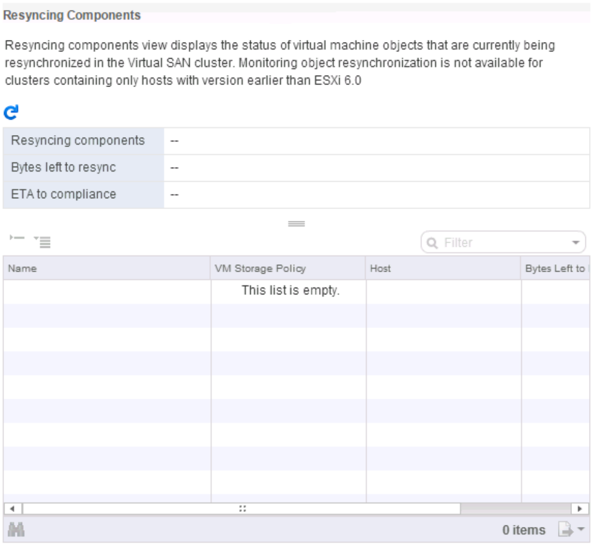
VMware recommends upgrading to ESXi 6.0U1 for a simpler health check install experience. If you are not planning to upgrade to ESXi 6.0U1, the following steps will guide you through the installation of the VIBs on ESXi 6.0 hosts.

2.1 Before you begin

Note*: The ESXi hosts in the Virtual SAN cluster need to be booted from disk. Stateless ESXi is currently not supported with Virtual SAN. If the ESXi hosts are booted from the network (e.g. stateless ESXi), the installation of VIBs will fail.*

Ensure that there is no rebuild taking place in the cluster before deploying the health check VIBs on the ESXi hosts in the Virtual SAN cluster. If there is, this can elongate the time to install the VIBs. There is a “Resyncing components” view in the vSphere web client that can be used to see if there is any resync activity in progress on the cluster. Administrators can also use the Ruby vSphere Console (RVC) command `vsan.resync_dashboard` to verify. It should report 0% activity. If there is rebuild activity, wait for it to complete before installing the health check VIBs.

To check if components are in a resync or rebuild state, select the cluster object, then Monitor > Virtual SAN > Resyncing components. It should be empty, as shown below:



Resyncing Components

Resyncing components view displays the status of virtual machine objects that are currently being resynchronized in the Virtual SAN cluster. Monitoring object resynchronization is not available for clusters containing only hosts with version earlier than ESXi 6.0

Resyncing components	--
Bytes left to resync	--
ETA to compliance	--

Name	VM Storage Policy	Host	Bytes Left to
	This list is empty.		

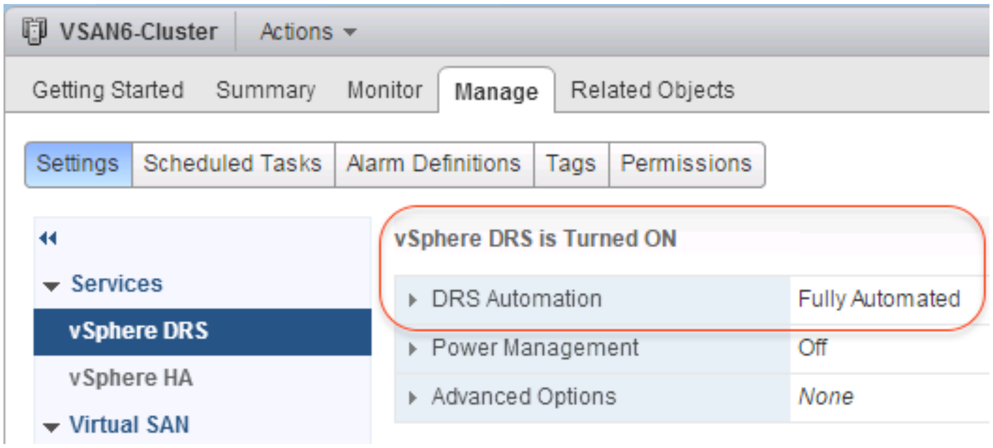
0 items

An alternative way to check resync activity is via the RVC `vsan.resync_dashboard <cluster>`:

```
> vsan.resync_dashboard <path-to-cluster>
 2015-08-14 08:58:21 +0000: Querying all VMs on VSAN ...
 2015-08-14 08:58:21 +0000: Querying all objects in the system from cs-ie-
dell01.ie.local ...
 2015-08-14 08:58:21 +0000: Got all the info, computing table ...
 +-----------+-----------------+---------------+
 | VM/Object | Syncing objects | Bytes to sync |
 +-----------+-----------------+---------------+
 +-----------+-----------------+---------------+
 | Total     | 0               | 0.00 GB       |
```

If there is rebuilding or resync activity taking place, please wait for that activity to complete before installing the health check VIBs.

There is also a requirement for DRS to be enabled in fully automated mode on the cluster. The installation will not proceed unless this requirement is met.



vSphere DRS is Turned ON

DRS Automation	Fully Automated
Power Management	Off
Advanced Options	*None*

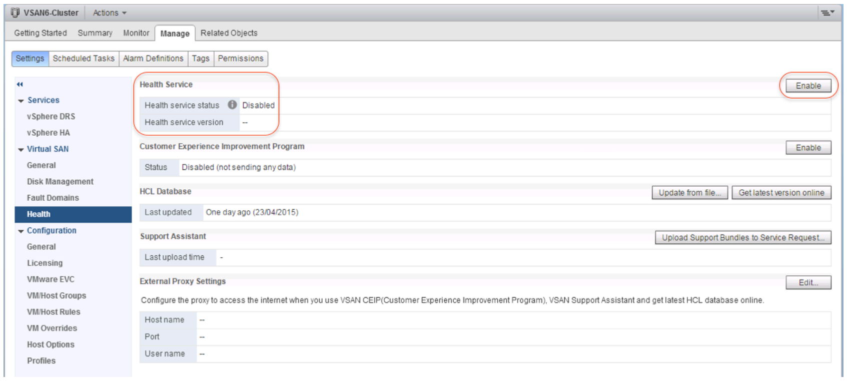
***Note**: Various errors will be observed in tasks and events during this installation process. This is due to the fact that the hosts require rebooting, and the other in the hosts in the Virtual SAN cluster will complain when they cannot communicate to the host being rebooted. This is normal behavior, and is not a cause for concern. The hosts will automatically be placed into maintenance mode, VMs will be migrated (compute and storage) to other hosts in the cluster, the hosts will then be rebooted, exit maintenance mode and automatically rejoin the cluster once they are successfully rebooted.*

2.2 vSphere Web Client UI installation method

The necessary Health check VIBs can be installed on the ESXi hosts via the vSphere web client UI. This can be done from two places in the UI.

2.2.1 Enable Health Checks – UI Method 1

This first location, via Manage -> Virtual SAN -> Health, is where the health checks can be installed. If this is an ESXi 6.0 host that does not had the VIBs inbox, then the Health check status will be shown as Disabled. Click on the *Enable* button to enable the health check. This will begin the rolling install of the health check VIB on all of the ESXi hosts in the Virtual SAN cluster.



Health Service

Health service status	Disabled
Health service version	--

Customer Experience Improvement Program

Status	Disabled (not sending any data)

HCL Database

Last updated	One day ago (23/04/2015)

Support Assistant

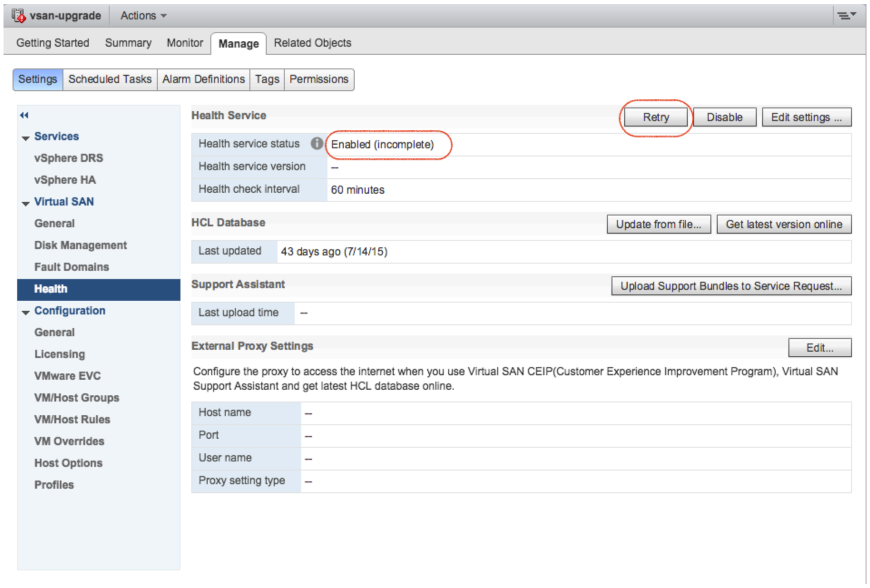
Last upload time	-

External Proxy Settings

Configure the proxy to access the internet when you use VSAN CEIP(Customer Experience Improvement Program), VSAN Support Assistant and get latest HCL database online.

Host name	--
Port	--
User name	--

If this is an ESXi 6.0u1 host, it already has the necessary VIBs. Therefore, once the cluster object is selected in the inventory, navigate to Manage -> Virtual SAN -> Health, Health check status is shown as *Enabled (incomplete)*. Click on the *Retry* button to enable the health check. This will enable the health check on all of the ESXi hosts in the Virtual SAN cluster.



Health Service

Health service status	Enabled (incomplete)
Health service version	–
Health check interval	60 minutes

HCL Database

Last updated	43 days ago (7/14/15)

Support Assistant

Last upload time	–

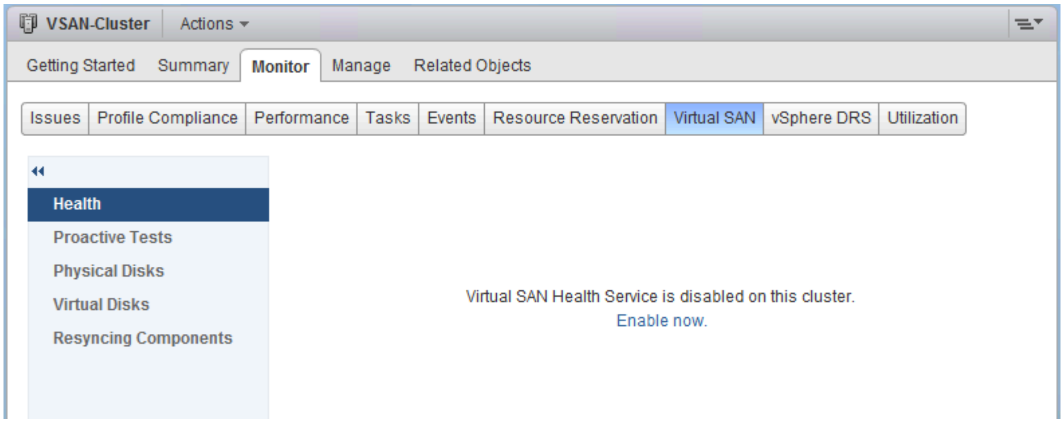
External Proxy Settings

Configure the proxy to access the internet when you use Virtual SAN CEIP(Customer Experience Improvement Program), Virtual SAN Support Assistant and get latest HCL database online.

Host name	–
Port	–
User name	–
Proxy setting type	–

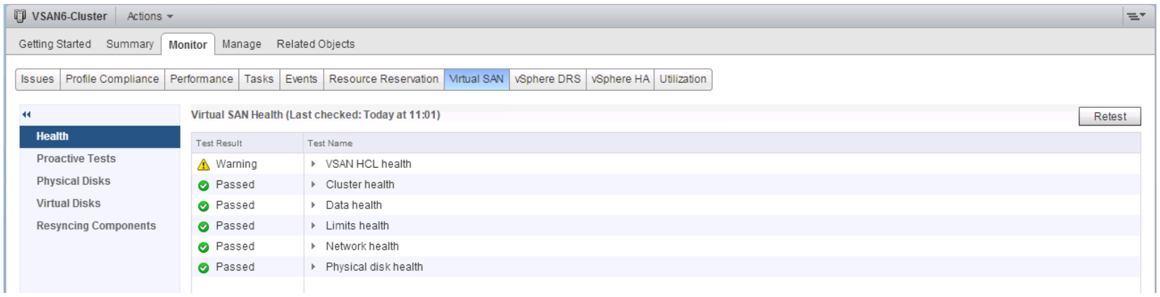
2.2.2 Enable Health Checks – UI Method 2

This is the second location where the health checks can be installed. This is done from Monitor -> Virtual SAN -> Health. Again, the cluster object is selected in the inventory, under Monitor > Virtual SAN > Health. For vSphere 6.0, the service is shown as disabled. Click on “*Enable now”* to start the roll out of the health check VIBs on the ESXi hosts in the Virtual SAN cluster.



Virtual SAN Health Service is disabled on this cluster.
Enable now.

The progress of the VIB installation (maintenance mode, reboots) may once again be monitored via the Tasks & Events view of the cluster. When complete, the Health check should show “Enabled” in the Cluster > Manage > Virtual SAN > Health view. Navigating to Cluster > Monitor > Virtual SAN, Health should display a list of health checks and associated test results:



Virtual SAN Health (Last checked: Today at 11:01)

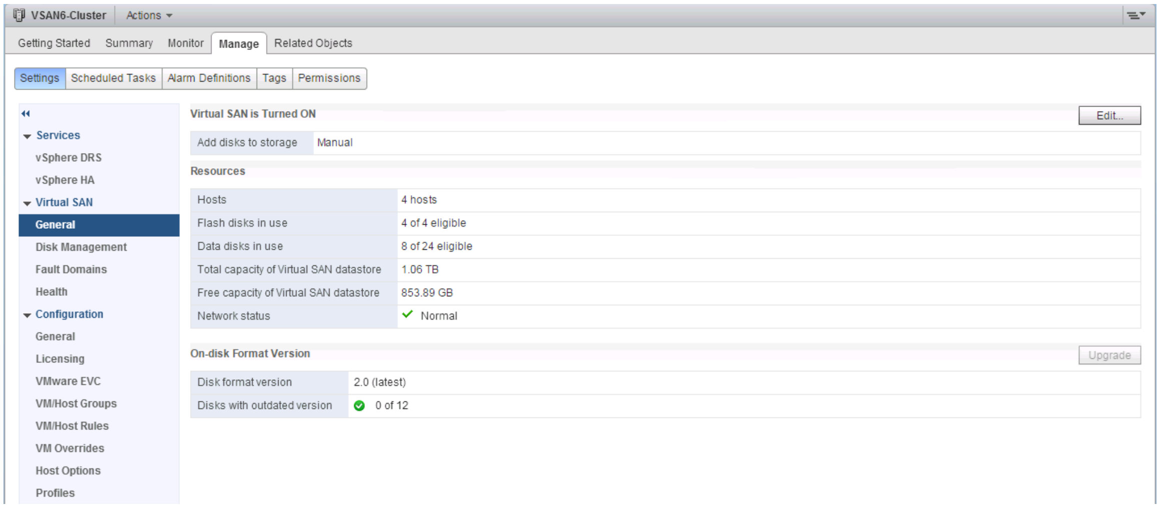
Test Result	Test Name
⚠ Warning	VSAN HCL health
✓ Passed	Cluster health
✓ Passed	Data health
✓ Passed	Limits health
✓ Passed	Network health
✓ Passed	Physical disk health

Note that if you have upgraded from the previous version of health check, you may need to click on the “Retest” button for the results to display correctly.

The Virtual SAN Health check is now successfully deployed.

2.2.3 Changes to General View with Health check

Once health checks have been deployed, a few additional pieces of information are displayed in the Virtual SAN > General view.



Virtual SAN is Turned ON

Add disks to storage	Manual

Resources

Hosts	4 hosts
Flash disks in use	4 of 4 eligible
Data disks in use	8 of 24 eligible
Total capacity of Virtual SAN datastore	1.06 TB
Free capacity of Virtual SAN datastore	853.89 GB
Network status	✓ Normal

On-disk Format Version

Disk format version	2.0 (latest)
Disks with outdated version	✓ 0 of 12

The *On-disk Format Version* displays how many of the disks have been upgraded to version 2, the VirstoFS on-disk format included with Virtual SAN 6.0. Customers should upgrade to version 2 to leverage new performance and scalability improvements with snapshots and clones. The upgrade can be done online via a rolling-upgrade mechanism. Refer to the *Virtual SAN Administrators Guide* for the detailed steps.

In the above example, all disks are at version 2. There are 0 disks with an outdated v1 on-disk format version. If disks are discovered with an outdated on-disk format, the “Upgrade” button will be available and may be used to update them to version 2.

2.3 VIB Installation Methods

As mentioned a number of times already, please note that with the release of ESXi 6.0U1, the health check VIB is bundled with ESXi. Therefore there is no need to push out the VIB from vCenter server, which is still a necessary step with ESXi 6.0. With ESXi 6.0U1, the health check will be automatically enabled in the web client UI.

However, if the plan is to continue to run with ESXi version 6.0 hosts, the VIB on the hosts needs to be installed. If a 6.0 version of the health check VIB already exists on the ESXi hosts, they will need to be have the VIB updated to version 6.0U1. There are four installation options for the health VIB:

1. Enable/Upgrade the health check via vSphere web client
2. RVC, the Ruby vSphere Console
3. VUM, the VMware Update Manager. Use of VUM is outside the scope of this document and users are directed to the official vSphere documentation on how to use VUM to install VIBs.
4. Manual install at the ESXi command line. This is done using *esxcli software vib* commands. Use of these commands is outside the scope of this document and users are directed to the official vSphere documentation on how to use *esxcli* commands.

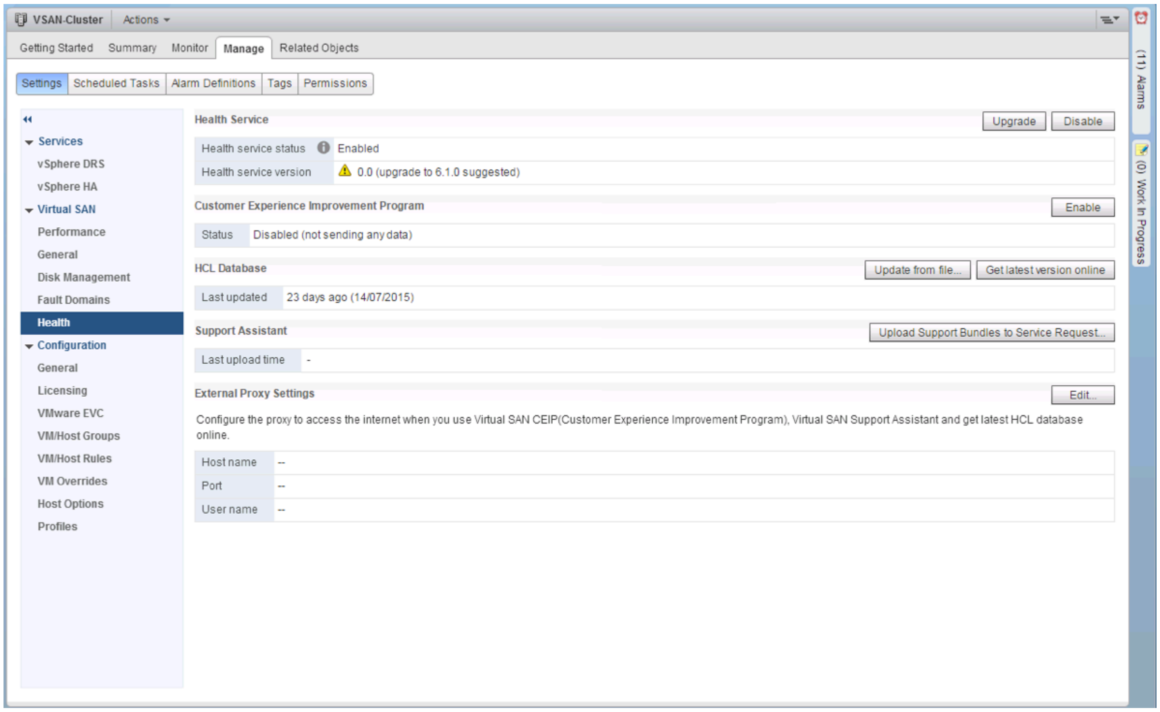
VMware recommends option 1 for ease of install, but the steps to install via option 2 are also covered here.

Warning*: Considering that this installation is doing a rolling upgrade, administrators should check that there is no component rebuild going on in the Virtual SAN cluster before starting this installation process on the ESXi hosts. This can be done via the UI or via the RVC command line*

As the health check installation proceeds, the status changes to “Enabling” and once the install is complete, it changes to “Enabled”. This can take some time, as each ESXi host has to be placed into maintenance mode, have the health check VIB upgraded, and then the ESXi host has to be rebooted. The time taken to install the VIB rises exponentially based on the number of hosts in the cluster. The progress may be monitored via the Tasks & Events view of the cluster.

2.3.1 Upgrading Health Check ESXi VIBs

The RPM (appliance) or MSI (Windows) health checks packages are automatically updated to version 6.1 on vCenter server when the vCenter server 6.0U1 is installed or upgraded. Once that step is done, and the vCenter Server services are restarted, the health checks will report that it is out of date, and recommend upgrading.



Health Service

Health service status	Enabled
Health service version	0.0 (upgrade to 6.1.0 suggested)

Customer Experience Improvement Program

Status	Disabled (not sending any data)

HCL Database

Last updated	23 days ago (14/07/2015)

Support Assistant

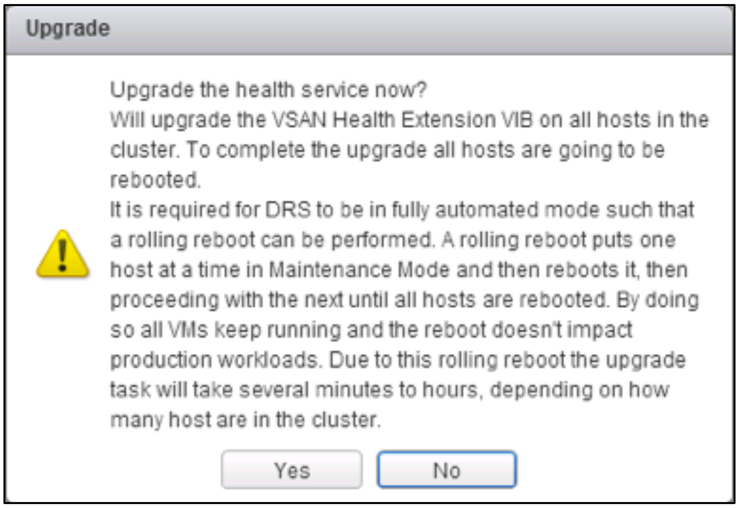
Last upload time	-

External Proxy Settings

Configure the proxy to access the internet when you use Virtual SAN CEIP(Customer Experience Improvement Program), Virtual SAN Support Assistant and get latest HCL database online.

Host name	--
Port	--
User name	--

To upgrade the health check VIB on the ESXi hosts to the latest version of 6.0U1, click on the *Upgrade* button. You will receive the following pop-up:



Upgrade the health service now?
Will upgrade the VSAN Health Extension VIB on all hosts in the cluster. To complete the upgrade all hosts are going to be rebooted.
It is required for DRS to be in fully automated mode such that a rolling reboot can be performed. A rolling reboot puts one host at a time in Maintenance Mode and then reboots it, then proceeding with the next until all hosts are rebooted. By doing so all VMs keep running and the reboot doesn't impact production workloads. Due to this rolling reboot the upgrade task will take several minutes to hours, depending on how many host are in the cluster.

Once again, as the message states, ensure that DRS is enabled, and fully automated, on the cluster. The upgrade process follows a rolling pattern of placing the hosts into maintenance mode, update the VIB to the VSAN 6.1 version, rebooting on a host-by-host basis, and exiting maintenance mode. This is similar to how the install process works.

This mismatch between ESXi hosts and vCenter server will also be highlighted in the actual health check tests. The test *VSAN Health Service up-to-date* verifies that the vCenter Server and ESXi hosts are running the same version.

2.3.2 Manual VIB Install

This section is applicable to ESXi version 6.0.0 only. It is not applicable to ESXi version 6.0U1 since that release of ESXi will already have the latest VIB installed. **VMware recommends** customers move to ESXi version 6.0U1 and vCenter Server 6.0U1 to simply the whole health check experience.

If customers are still running ESXi version 6.0.0, they can manually install the health check VIB rather than using the UI or RVC methods. The download location can be found in chapter 7, “Additional Information”. This manual install method may be desirable where customers wish to use VUM, or customers do not have DRS available to do a rolling upgrade/install.

Refer to the official vSphere documentation on how to use *esxcli software vib* commands to install this VIB on ESXi hosts.

Note that the ESXi6.0U1 version of the VIB can be rolled out from vCenter 60U1 to ESXi 6.0.0 hosts.

2.4 vSphere Update Manager users warning

For vSphere Update Manager users, once the VIB is manually installed, or installed via RVC, a scan or compliance check is run against the ESXi host will generate vSphere Update Manager (VUM) alerts stating that the hosts are *not compliant*.

The VIB should be installed as a vSphere Extension, not a vSphere Update.

2.5 Changing Default Certificates

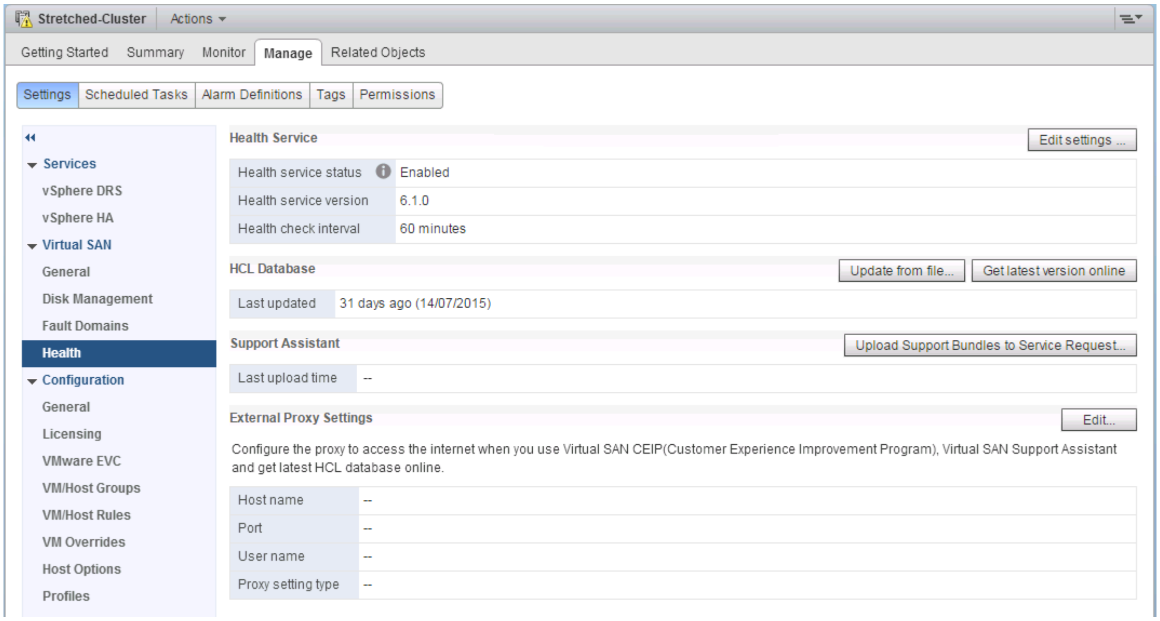
If you plan on changing from the default certificates to a Certificate of Authority, please be aware of some known behavior with the ESX Agent Manager, utilized by the Health Check.

VMware Knowledgebase Article 2112577 - http://kb.vmware.com/kb/2112577
 - has details on how to address the issue and enable EAM to use a CA.

Please note that replacing vCenter Certificates with SSL certificate tool (not sure of official name) may cause VSAN health check to stop functioning with Error HTTP status 503 – please see VMware Knowledgebase Article 2128353 – http://kb.vmware.com/kb/2128353

3. Health Check UI features

Once enabled, the Health service status changes to “Enabled” and the version of the Health check is displayed.



Health Service

Health service status	Enabled
Health service version	6.1.0
Health check interval	60 minutes

HCL Database

Last updated	31 days ago (14/07/2015)

Support Assistant

Last upload time	--

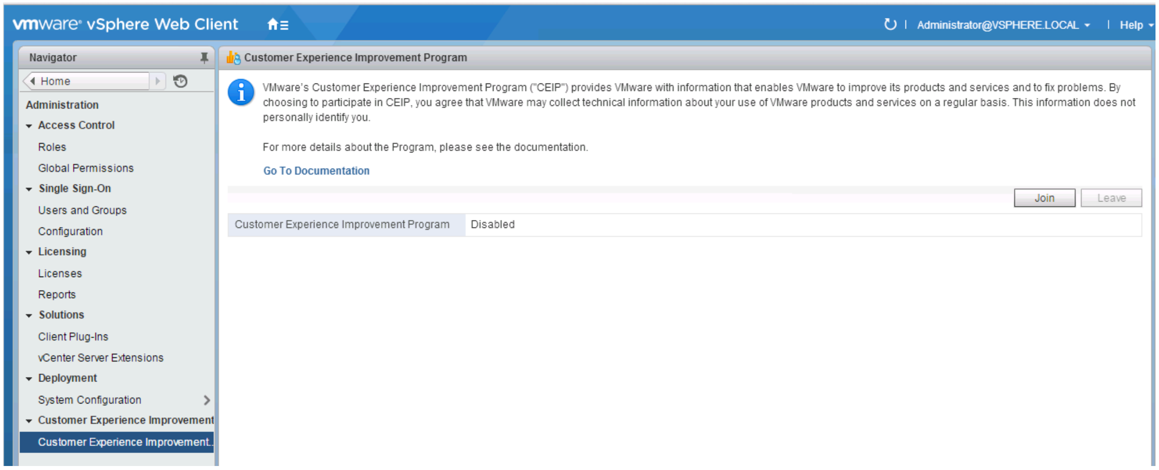
External Proxy Settings

Configure the proxy to access the internet when you use Virtual SAN CEIP(Customer Experience Improvement Program), Virtual SAN Support Assistant and get latest HCL database online.

Host name	--
Port	--
User name	--
Proxy setting type	--

3.1 Enable Customer Experience Improvement Program

As mentioned earlier, if you do not choose to enable the *Customer Experience Improvement Program* at health check install time, it can be done later in the vCenter web client via the Administration-> CEIP -> Join/Leave.



Customer Experience Improvement Program

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services and to fix problems. By choosing to participate in CEIP, you agree that VMware may collect technical information about your use of VMware products and services on a regular basis. This information does not personally identify you.

For more details about the Program, please see the documentation.

Go To Documentation

Customer Experience Improvement Program	Disabled

The data that this process collects is detailed in following location.

http://www.vmware.com/info?id=1379

3.2 HCL Database

One of the health checks ensures that your environment uses supported hardware, software and drivers. These checks are run against a HCL file that is regularly updated, adding support for newer hardware, software and drivers, and occasionally dropping support for older hardware, software and drivers. The HCL Database buttons allows the local HCL file to be updated. This may be done directly from the Internet, or if your vCenter server is not connected to the Internet, it can be updated via a file that was downloaded from VMware, and then transferred to the vCenter server. The location of the HCL file is in section 8.5 of this document.

3.3 Support Assistant

One final feature displayed in this view is the Support Assistant. This relates to the ability to upload support bundles to a Service Request opened with VMware Global Support Services (GSS). For further details on the Support Assistant, refer to the following documentation.

https://www.vmware.com/support/pubs/support-assistant-pubs.html

3.4 External Proxy Settings

If you do not have direct access to the Internet from your vCenter server, but you have a proxy that allows Internet connectivity, the external proxy settings can be used to provide this information to the health check.

Health check features such as the Support Assistant, CEIP and HCL database updates will use the proxy settings to access VMware.com via the proxy settings.

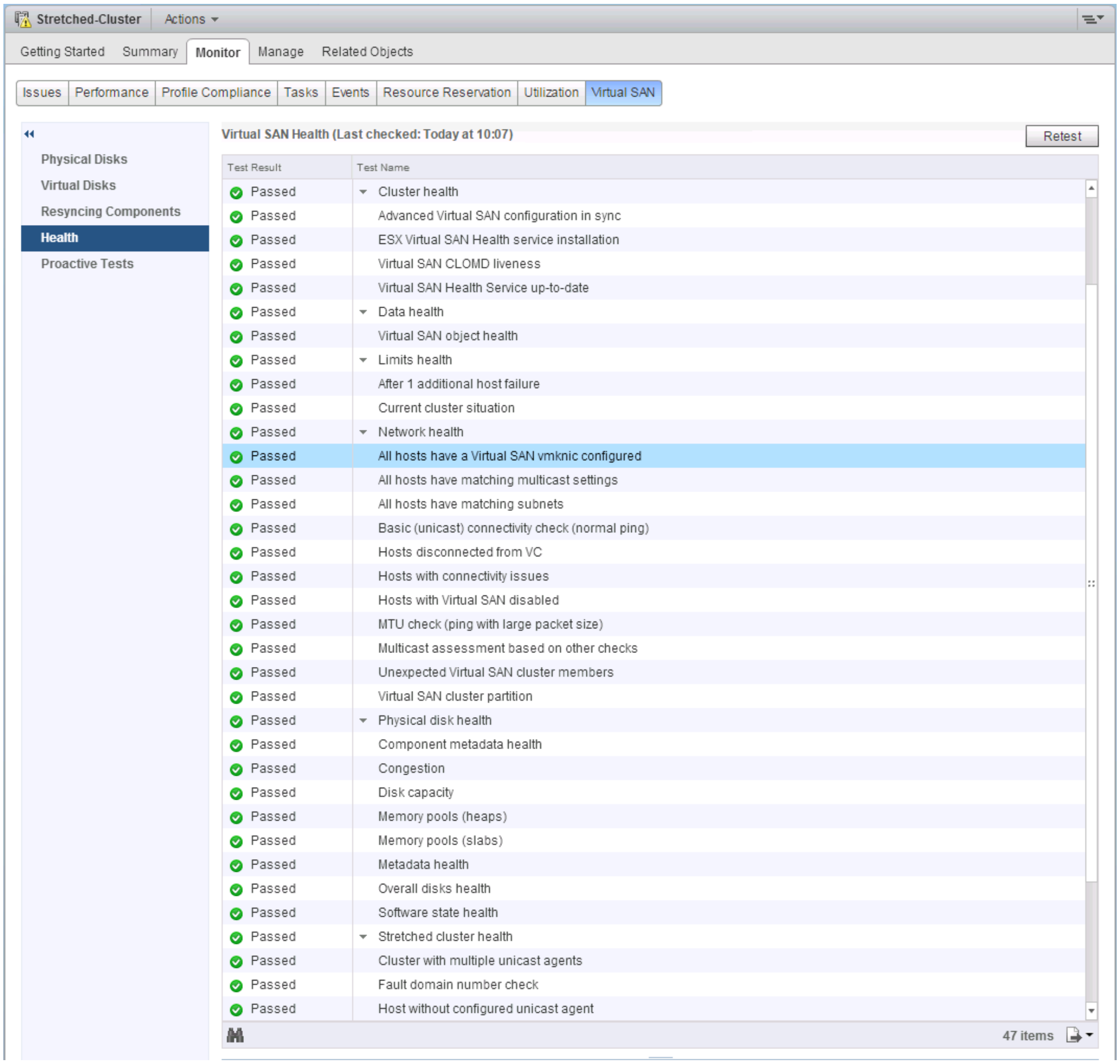
3.5 SNMP Traps from Alarms

This new Health Check release includes pre-defined vCenter alarms defined for each health check. This is an important new feature to customers from an operational management perspective. In particular, SNMP support via vCenter alarms allows for health check alerts to be emailed to administrators, informing them of a period health check failure. Further information on SNMP traps and alarms can be found in the vSphere Monitoring and Performance Guide.

4. Health checks via the UI

4.1 Health check tests and results via UI

Once the health checks are enabled, navigate to Cluster > Monitor > Virtual SAN > Health. The five categories of health check are displayed. Each of these can be expanded to see the individual health checks in each category. The tests can be rerun at any time by clicking on the "Retest" button on the right hand side.



Virtual SAN Health (Last checked: Today at 10:07)

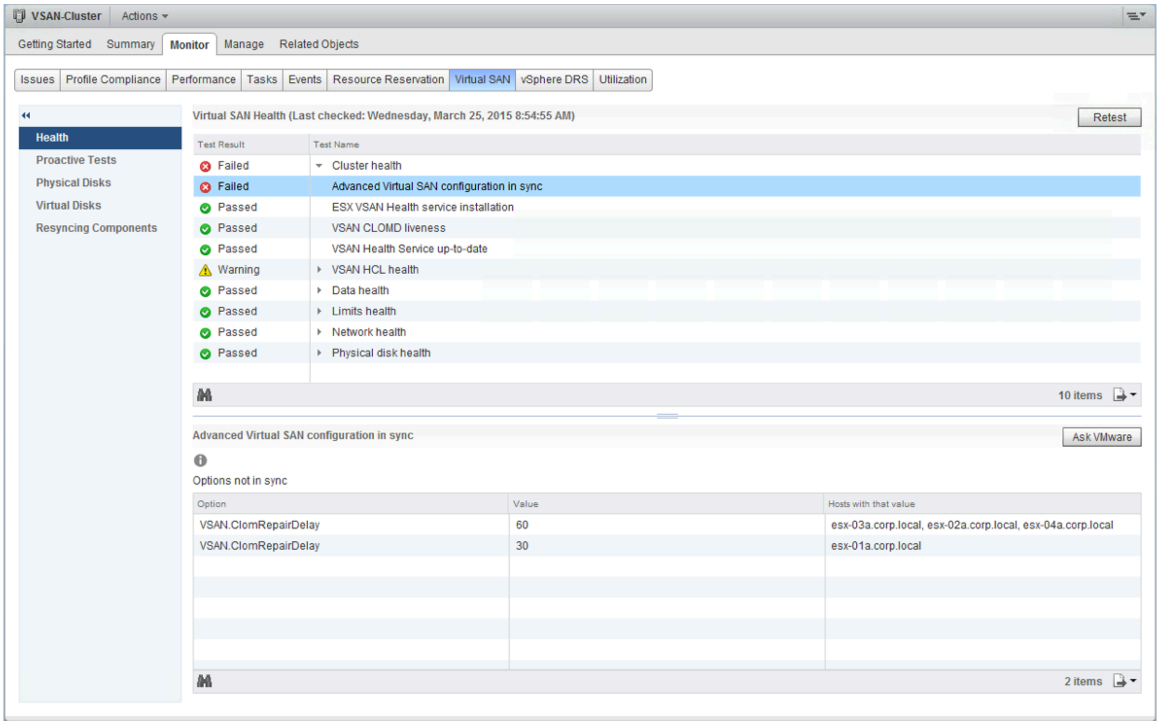
Test Result	Test Name
✓ Passed	Cluster health
✓ Passed	Advanced Virtual SAN configuration in sync
✓ Passed	ESX Virtual SAN Health service installation
✓ Passed	Virtual SAN CLOMD liveness
✓ Passed	Virtual SAN Health Service up-to-date
✓ Passed	Data health
✓ Passed	Virtual SAN object health
✓ Passed	Limits health
✓ Passed	After 1 additional host failure
✓ Passed	Current cluster situation
✓ Passed	Network health
✓ Passed	All hosts have a Virtual SAN vmknic configured
✓ Passed	All hosts have matching multicast settings
✓ Passed	All hosts have matching subnets
✓ Passed	Basic (unicast) connectivity check (normal ping)
✓ Passed	Hosts disconnected from VC
✓ Passed	Hosts with connectivity issues
✓ Passed	Hosts with Virtual SAN disabled
✓ Passed	MTU check (ping with large packet size)
✓ Passed	Multicast assessment based on other checks
✓ Passed	Unexpected Virtual SAN cluster members
✓ Passed	Virtual SAN cluster partition
✓ Passed	Physical disk health
✓ Passed	Component metadata health
✓ Passed	Congestion
✓ Passed	Disk capacity
✓ Passed	Memory pools (heaps)
✓ Passed	Memory pools (slabs)
✓ Passed	Metadata health
✓ Passed	Overall disks health
✓ Passed	Software state health
✓ Passed	Stretched cluster health
✓ Passed	Cluster with multiple unicast agents
✓ Passed	Fault domain number check
✓ Passed	Host without configured unicast agent

47 items

Note that the stretched cluster health checks only appear when Virtual SAN is deployed as a stretched cluster configuration. Otherwise these tests do not appear.

4.2 What does a failure look like?

Note that if there is a failure in any of the health checks, the health check displays a failure in the topmost item of the health check tree, and a failure is shown against the particular check.



Virtual SAN Health (Last checked: Wednesday, March 25, 2015 8:54:55 AM)

Test Result	Test Name
Failed	Cluster health
Failed	Advanced Virtual SAN configuration in sync
Passed	ESX VSAN Health service installation
Passed	VSAN CLOMD liveness
Passed	VSAN Health Service up-to-date
Warning	VSAN HCL health
Passed	Data health
Passed	Limits health
Passed	Network health
Passed	Physical disk health

Advanced Virtual SAN configuration in sync

Options not in sync

Option	Value	Hosts with that value
VSAN.ClomRepairDelay	60	esx-03a.corp.local, esx-02a.corp.local, esx-04a.corp.local
VSAN.ClomRepairDelay	30	esx-01a.corp.local

In the scenario above, there appears to be a mismatch of the advanced setting *VSAN.ClomRepairDelay* where one host (esx-01a.corp.local) has a different value when compared to the other hosts in the cluster.

4.3 What to do when a health check fails?

Once the actual failed check is selected, details about the failure and a link to a VMware Knowledge Base article is provided via "Ask VMware" button. By clicking on the "**Ask VMware**" button, a knowledgebase (KB) article detailing the cause of the issue and steps on how to troubleshoot will be provided.

In the next sections, each of the individual health checks in each of the categories is explained, and the steps that can be taken to resolve the error are described.

5. Health check via the CLI

5.1 Health check overview

Once the Health check is installed, they can be used for verifying the health of the Virtual SAN environment. The first step is to verify that the health checks are enabled. Once they are enabled, the individual checks can be examined to see if there are any issues with this Virtual SAN deployment.

The health checks are split into five distinct categories:

1. Cluster health
2. Network health
3. Data health
4. Limits health
5. Physical disks health

Each of these categories has a number of individual checks, which explained in detail in the appendix. The health check provides checks at both the command line and the user interface. The command line checks are part of RVC, the Ruby vSphere Console. A list of RVC health check commands are here:

- `vsan.health.cluster_attach_to_sr`
- `vsan.health.cluster_debug_multicast`
- `vsan.health.cluster_install`
- `vsan.health.cluster_load_test_cleanup`
- `vsan.health.cluster_load_test_prepare`
- `vsan.health.cluster_load_test_run`
- `vsan.health.cluster_proxy_configure`
- `vsan.health.cluster_proxy_status`
- `vsan.health.cluster_repair_immediately`
- `vsan.health.cluster_status`
- `vsan.health.cluster_uninstall`
- `vsan.health.hcl_update_db`
- `vsan.health.health_check_interval_configure`
- `vsan.health.health_check_interval_status`
- `vsan.health.health_summary`
- `vsan.health.multicast_speed_test`

All of the commands can be run with a `–h (help)` option for further information. Many of these commands are related to proactive tests, which will be looked at in detail in chapter 7 of this guide.

5.2 Check status - vsan.health.cluster_status

Here is an example of what a successful installation looks like. This is from health check version 6.0, but version 6.1 works in an identical fashion:

```
> vsan.health.cluster_status <path-to-cluster>
Configuration of ESX VSAN Health Extension: installed (OK)
Host 'cs-ie-h04.ie.local' has health system version '6.0.0' installed
Host 'cs-ie-h01.ie.local' has health system version '6.0.0' installed
Host 'cs-ie-h03.ie.local' has health system version '6.0.0' installed
Host 'cs-ie-h02.ie.local' has health system version '6.0.0' installed
vCenter Server has health system version '6.0.0' installed
>
```

In the next check, it would appear that a host reboot is required on host cs-ie-h01 to complete the VIB installation (ignore the versions shown here as these were captured from a pre-release version of health check):

```
> vsan.health.cluster_status <path-to-cluster>
 Configuration of ESX VSAN Health Extension: installed (incomplete, see issues)
 Issues:
   Host reboot is required to complete agent VIB installation
 Per-Host details:
   Host 'cs-ie-h04.ie.local':
     Status: green
   Host 'cs-ie-h03.ie.local':
     Status: green
   Host 'cs-ie-h01.ie.local':
     Status: red
     Issues:
       Host reboot is required to complete agent VIB installation
   Host 'cs-ie-h02.ie.local':
     Status: green
 Host 'cs-ie-h04.ie.local' has health system version '0.4' installed
 Host 'cs-ie-h01.ie.local' has health system version '0.4' installed
 Host 'cs-ie-h02.ie.local' has health system version '0.4' installed
 Host 'cs-ie-h03.ie.local' has health system version '0.4' installed
 vCenter Server has health system version '0.4' installed
```

5.3 Display health - vsan.health.health_summary

Once the VIBs have all been successfully installed, additional health check commands can be performed from the Ruby vSphere Console (RVC). In this example, a check is being performance on all hosts in the cluster. Here is one such output from a fully healthy system:

```
/ie-vcsa-09.ie.local/VSAN6-DC/computers> vsan.health.health_summary <path-to-cluster>
 Overall health: green
 +----------------------------------------------------+---------+
 | Health check                                       | Result  |
 +----------------------------------------------------+---------+
 | Cluster health                                     | Passed  |
 |   ESX VSAN Health service installation             | Passed  |
 |   VSAN Health Service up-to-date                   | Passed  |
 |   Advanced Virtual SAN configuration in sync       | Passed  |
 |   VSAN CLOMD liveness                              | Passed  |
 +----------------------------------------------------+---------+
 | VSAN HCL health                                    | Passed  |
 |   VSAN HCL DB up-to-date                           | Passed  |
 |   SCSI Controller on VSAN HCL                      | Passed  |
 |   Controller Release Support                       | Passed  |
 |   Controller Driver                                | Passed  |
 +----------------------------------------------------+---------+
 | Network health                                     | Passed  |
 |   Hosts disconnected from VC                       | Passed  |
 |   Hosts with connectivity issues                   | Passed  |
 |   VSAN cluster partition                           | Passed  |
 |   Unexpected VSAN cluster members                  | Passed  |
 |   Hosts with VSAN disabled                         | Passed  |
 |   All hosts have a VSAN vmknic configured          | Passed  |
 |   All hosts have matching subnets                  | Passed  |
 |   All hosts have matching multicast settings       | Passed  |
 |   Basic (unicast) connectivity check (normal ping) | Passed  |
 |   MTU check (ping with large packet size)          | Passed  |
 |   Multicast assessment based on other checks       | Passed  |
 +----------------------------------------------------+---------+
 | Data health                                        | Passed  |
 |   Virtual SAN object health                        | Passed  |
 +----------------------------------------------------+---------+
 | Limits health                                      | Passed  |
 |   Current cluster situation                        | Passed  |
 |   After 1 additional host failure                  | Passed  |
 +----------------------------------------------------+---------+
 | Physical disk health                               | Passed  |
 |   Overall disks health                             | Passed  |
 |   Metadata health                                  | Passed  |
 |   Disk capacity                                    | Passed  |
 |   Software state health                            | Passed  |
 |   Congestion                                       | Passed  |
 |   Component metadata health                        | Passed  |
 |   Memory pools (heaps)                             | Passed  |
 |   Memory pools (slabs)                             | Passed  |
 +----------------------------------------------------+---------+
```

The individual tests will be discussed in the appendix of this guide.

***Note**: If you get a RuntimeError: when you run this command, log out of RVC and log back in to RVC once again.*

In this next check, a number of issues related to the HCL (Hardware Compatibility Guide) have been discovered. Note that the overall health is `yellow(VSAN HCL warning)`. In particular, there are issues with the controller not supported according to the HCL, especially for Virtual SAN 6.0, and there are warnings related to the driver. The font size of the output has been reduced to make it fit.

```
/ie-vcsa-09.ie.local/VSAN6-DC/computers> vsan.health.health_summary <path-to-cluster>
 Overall health: yellow (VSAN HCL warning)
 +----------------------------------------------------+---------+
 | Health check                                       | Result  |
 +----------------------------------------------------+---------+
 | Cluster health                                     | Passed  |
 |   ESX VSAN Health service installation             | Passed  |
 |   VSAN Health Service up-to-date                   | Passed  |
 |   Advanced Virtual SAN configuration in sync       | Passed  |
 |   VSAN CLOMD liveness                              | Passed  |
 +----------------------------------------------------+---------+
 | VSAN HCL health                                    | Warning |
 |   VSAN HCL DB up-to-date                           | Passed  |
 |   SCSI Controller on VSAN HCL                      | Warning |
 |   Controller Release Support                       | Warning |
 |   Controller Driver                                | Warning |
 +----------------------------------------------------+---------+
 | Network health                                     | Passed  |
 |   Hosts disconnected from VC                       | Passed  |
 |   Hosts with connectivity issues                   | Passed  |
 |   VSAN cluster partition                           | Passed  |
 |   Unexpected VSAN cluster members                  | Passed  |
 |   Hosts with VSAN disabled                         | Passed  |
 |   All hosts have a VSAN vmknic configured          | Passed  |
 |   All hosts have matching subnets                  | Passed  |
 |   All hosts have matching multicast settings       | Passed  |
 |   Basic (unicast) connectivity check (normal ping) | Passed  |
 |   MTU check (ping with large packet size)          | Passed  |
 |   Multicast assessment based on other checks       | Passed  |
 +----------------------------------------------------+---------+
 | Data health                                        | Passed  |
 |   Virtual SAN object health                        | Passed  |
 +----------------------------------------------------+---------+
 | Limits health                                      | Passed  |
 |   Current cluster situation                        | Passed  |
 |   After 1 additional host failure                  | Passed  |
 +----------------------------------------------------+---------+
 | Physical disk health                               | Passed  |
 |   Overall disks health                             | Passed  |
 |   Metadata health                                  | Passed  |
 |   Disk capacity                                    | Passed  |
 |   Software state health                            | Passed  |
 |   Congestion                                       | Passed  |
 |   Component metadata health                        | Passed  |
 |   Memory pools (heaps)                             | Passed  |
 |   Memory pools (slabs)                             | Passed  |
 +----------------------------------------------------+---------+

 Details about any failed test below ...
VSAN HCL health - SCSI Controller on VSAN HCL: yellow
  +--------------------+--------+-------------------------------------------+---------------------+---------+
  | Host               | Device | Display Name                              | PCI ID              | On HCL  |
  +--------------------+--------+-------------------------------------------+---------------------+---------+
  | cs-ie-h03.ie.local | vmhba1 | Hewlett-Packard Company Smart Array P410i | 103c,323a,103c,3245 | Warning |
  | cs-ie-h01.ie.local | vmhba1 | Hewlett-Packard Company Smart Array P410i | 103c,323a,103c,3245 | Warning |
  | cs-ie-h04.ie.local | vmhba1 | Hewlett-Packard Company Smart Array P410i | 103c,323a,103c,3245 | Warning |
  | cs-ie-h02.ie.local | vmhba1 | Hewlett-Packard Company Smart Array P410i | 103c,323a,103c,3245 | Warning |
  +--------------------+--------+-------------------------------------------+---------------------+---------+

VSAN HCL health - Controller Release Support: yellow
  +--------------------+---------------------------------------------------+----------------+-------------------+-----------------+
  | Host               | Device                                            | Release of ESX | Release supported | Releases on HCL |
  +--------------------+---------------------------------------------------+----------------+-------------------+-----------------+
  | cs-ie-h03.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | ESXi 6.0       | Warning           |                 |
  | cs-ie-h01.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | ESXi 6.0       | Warning           |                 |
  | cs-ie-h04.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | ESXi 6.0       | Warning           |                 |
  | cs-ie-h02.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | ESXi 6.0       | Warning           |                 |
  +--------------------+---------------------------------------------------+----------------+-------------------+-----------------+

VSAN HCL health - Controller Driver: yellow
  +--------------------+---------------------------------------------------+----------------------+---------------+----------------+
  | Host               | Device                                            | Driver in use        | Driver health | Drivers on HCL |
  +--------------------+---------------------------------------------------+----------------------+---------------+----------------+
  | cs-ie-h03.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | hpsa (5.5.0.74-1OEM) | Warning       |                |
  | cs-ie-h01.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | hpsa (6.0.0.44-4vmw) | Warning       |                |
  | cs-ie-h04.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | hpsa (6.0.0.44-4vmw) | Warning       |                |
  | cs-ie-h02.ie.local | vmhba1: Hewlett-Packard Company Smart Array P410i | hpsa (6.0.0.44-4vmw) | Warning       |                |
  +--------------------+---------------------------------------------------+----------------------+---------------+----------------+

 [[0.071033794, "initial connect"],
  [7.462449423, "cluster-health"],
  [0.006679754, "table-render"]]
 /ie-vcsa-09.ie.local/VSAN6-DC/computers>
```

6. Proactive health checks

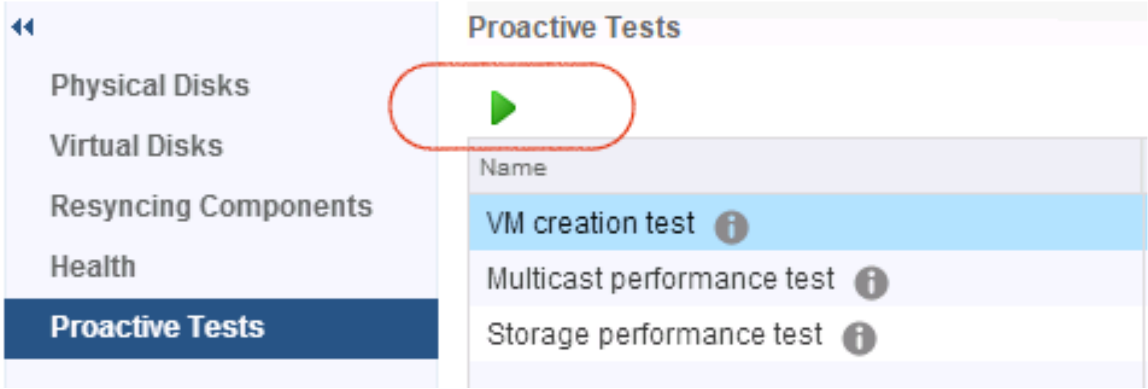
Health checks comes with a set of proactive health checks that can be run from the Ruby vSphere Console (RVC). This section of the guide looks at the set of proactive health checks available, and how to run them in your own Virtual SAN environment. Proactive tests are found in Monitor > Virtual SAN > Proactive Tests.

6.1 VM creation tests

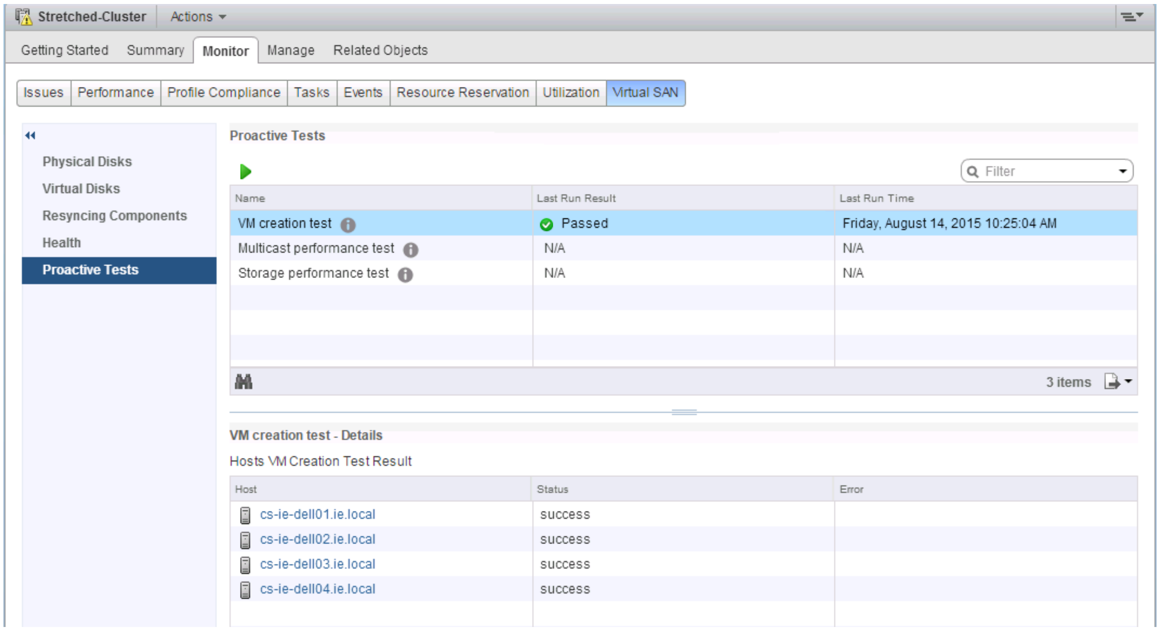
This test creates a very simple, tiny virtual machine on every ESXi host in the Virtual SAN cluster. If that creation succeeds, the virtual machine is deleted and it can be concluded that a lot of aspects of Virtual SAN are fully operational. The management stack is operational on all hosts, the Virtual SAN network is plumbed and is working, the creation, deletion and I/O to objects is working, etc. By doing this test, and administrator can reveal issues that the passive health checks may not be able to detect. By doing so systemically it is also very easy to isolate any particular faulty host and then take steps to remediate the underlying problem.

6.1.1 Running a VM creation test via the UI

To run the test, navigate to Monitor > Virtual SAN > Proactive Tests in the vSphere web client UI, select the VM Creationtest from the list of proactive tests, and click on the green triangle (highlighted below) in the upper left hand corned to start the test.



When the test is run, the following popup appears explaining the purpose of the proactive test.



Proactive Tests

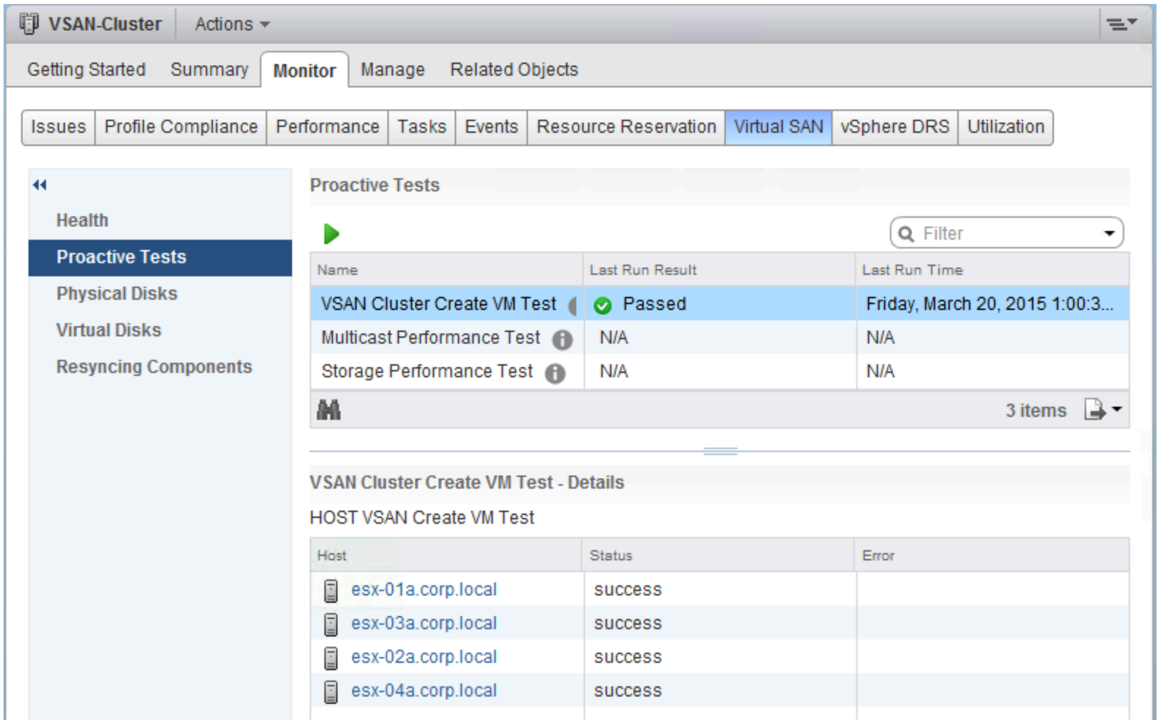
Name	Last Run Result	Last Run Time
VM creation test	Passed	Friday, August 14, 2015 10:25:04 AM
Multicast performance test	N/A	N/A
Storage performance test	N/A	N/A

VM creation test - Details

Hosts VM Creation Test Result

Host	Status	Error
cs-ie-dell01.ie.local	success	
cs-ie-dell02.ie.local	success	
cs-ie-dell03.ie.local	success	
cs-ie-dell04.ie.local	success	

If the test is successful, the following results are displayed:



Proactive Tests

Name	Last Run Result	Last Run Time
VSAN Cluster Create VM Test	Passed	Friday, March 20, 2015 1:00:3...
Multicast Performance Test	N/A	N/A
Storage Performance Test	N/A	N/A

VSAN Cluster Create VM Test - Details

HOST VSAN Create VM Test

Host	Status	Error
esx-01a.corp.local	success	
esx-03a.corp.local	success	
esx-02a.corp.local	success	
esx-04a.corp.local	success	

6.1.2 Running a create vm test via the CLI

When the `--create-vm-test` option is included with the `vsan.health.health_summary` command, it displays the cluster health check output first, and then adds the proactive VM creation test output to the end.

These outputs have been truncated for readability. The first example is taken from a cluster where one host (cs-ie-h01.ie.local) had *HardwareAssistedLocking* (ATS) advanced setting disabled. This lock setting is needed by Virtual SAN for the successful creation on virtual machine home namespaces:

```
> vsan.health.health_summary --create-vm-test <cluster>

<<truncated>>

Performing pro-active VM creation test ...
 +--------------------+------------------------------------------------------------+
 | Check              | Result                                                     |
 +--------------------+------------------------------------------------------------+
 | cs-ie-h01.ie.local | CannotCreateFile: Cannot complete file creation operation. |
 | cs-ie-h02.ie.local | Success                                                    |
 | cs-ie-h03.ie.local | Success                                                    |
 | cs-ie-h04.ie.local | Success                                                    |
 +--------------------+------------------------------------------------------------+
 [[0.086952653, "initial connect"],
  [7.337823925, "cluster-health"],
  [0.003172883, "table-render"],
  [6.373534267, "create-vm"],
  [0.000572188, "create-vm-table"]]
 /localhost/IE-VSAN-DC/computers>
```

Here is an example taken from a cluster where there are no issues:

```
> vsan.health.health_summary --create-vm-test <cluster>

<<truncated>>

 Performing pro-active VM creation test ...
 +--------------------+---------+
 | Check              | Result  |
 +--------------------+---------+
 | cs-ie-h01.ie.local | Success |
 | cs-ie-h02.ie.local | Success |
 | cs-ie-h03.ie.local | Success |
 | cs-ie-h04.ie.local | Success |
 +--------------------+---------+
 [[0.084946317, "initial connect"],
  [7.199865938, "cluster-health"],
  [0.0033262, "table-render"],
  [4.484202456, "create-vm"],
  [0.000735432, "create-vm-table"]]
 /localhost/IE-VSAN-DC/computers>
```

6.2 Multicast performance test

***Warning**: This test should only be run while the Virtual SAN cluster (or even the physical switch attached to the Virtual SAN cluster) are not running in production. It is advisable to run during a maintenance window or before placing the Virtual SAN cluster into production. The reason for this is because this test will flood the network with multicast packets, trying to find where an issue lies. If other users need bandwidth, they may not get enough bandwidth while this test is running.*

Before running this test, ensure that there is basic multicast connectivity in the cluster. This test is designed to assess connectivity and multicast speed between the hosts in the Virtual SAN cluster. It verifies that the multicast network setup can satisfy Virtual SAN's requirements.

The test works by selecting one ESXi host in the Virtual SAN cluster as the sender, and designating all other hosts to being receivers. By virtue of this being multicast traffic, any packet that the "sender" sends should be delivered to all receivers. Thus, in theory, if there were no bottlenecks in ESXi, and if the physical network could run at full wire speed, a 10Gbit/s sender would result in 10Gbit/s being received by all receivers. However, in practice, this test is not able to fully saturate the sender link since almost no physical switch is able to perform multicast at full wire speed.

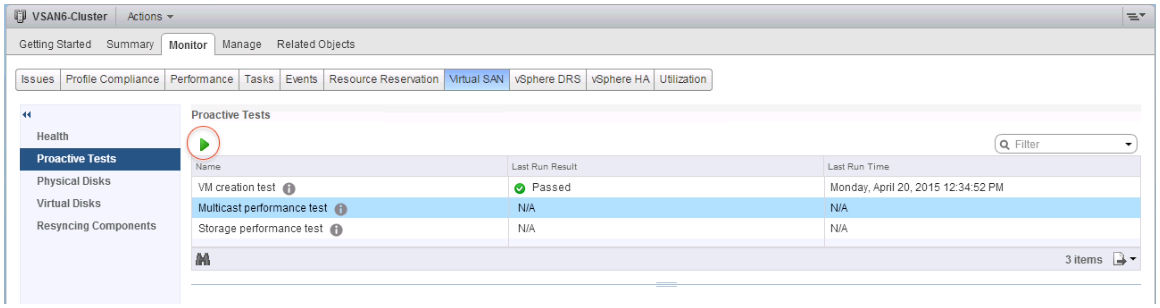
Virtual SAN does not need to run at full wire speed. Virtual SAN requires more than 20MB/s (or 200 Mbit/s) of multicast speed during peak load. On typical enterprise grade switches, this test should be able to achieve at least 70-80 MB/s. On some very low-end switches VMware has observed speeds as low as 10MB/s.

Given these ranges, the test will conclude that anything below 20MB/s is too low. It will also conclude that and any speeds between 20MB/s and 50MB/s is also low but acceptable. A speed above 50MB/s is what VMware would expect for the Virtual SAN network.

***Note**: A bandwidth limit of 1000Mb/s has been set on this multicast performance test implementation. Therefore there will be no major difference in results between running this test on a 1GbE network and a 10GbE network environment. The reason we set bandwidth limit to 1000Mb/s is that any speed above 70MB/s is acceptable. Hence, it is not necessary to saturate the full network.*

6.2.1 Running a multicast speed test via the UI

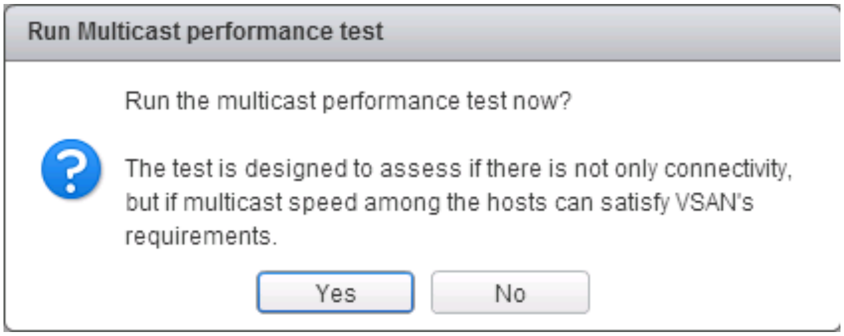
This test is to ensure that there is adequate network bandwidth between all the nodes in a cluster. Here is an example of running a successful test. First, select the appropriate proactive test, and then click on the start icon highlighted below:



Proactive Tests

Name	Last Run Result	Last Run Time
VM creation test	✓ Passed	Monday, April 20, 2015 12:34:52 PM
Multicast performance test	N/A	N/A
Storage performance test	N/A	N/A

Acknowledge the multicast speed test popup:

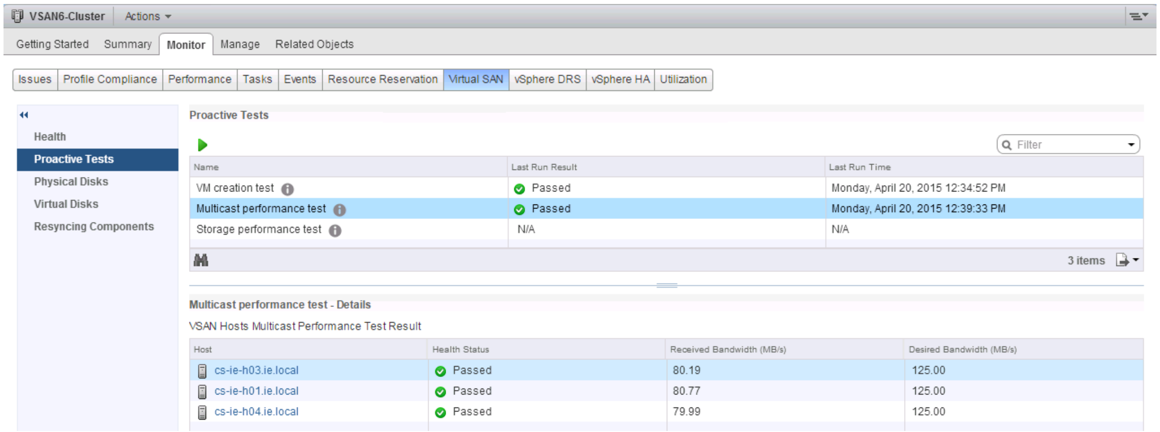


Run Multicast performance test

Run the multicast performance test now?

The test is designed to assess if there is not only connectivity, but if multicast speed among the hosts can satisfy VSAN's requirements.

When the test completes, the performance and status is displayed:



Proactive Tests

Name	Last Run Result	Last Run Time
VM creation test	✓ Passed	Monday, April 20, 2015 12:34:52 PM
Multicast performance test	✓ Passed	Monday, April 20, 2015 12:39:33 PM
Storage performance test	N/A	N/A

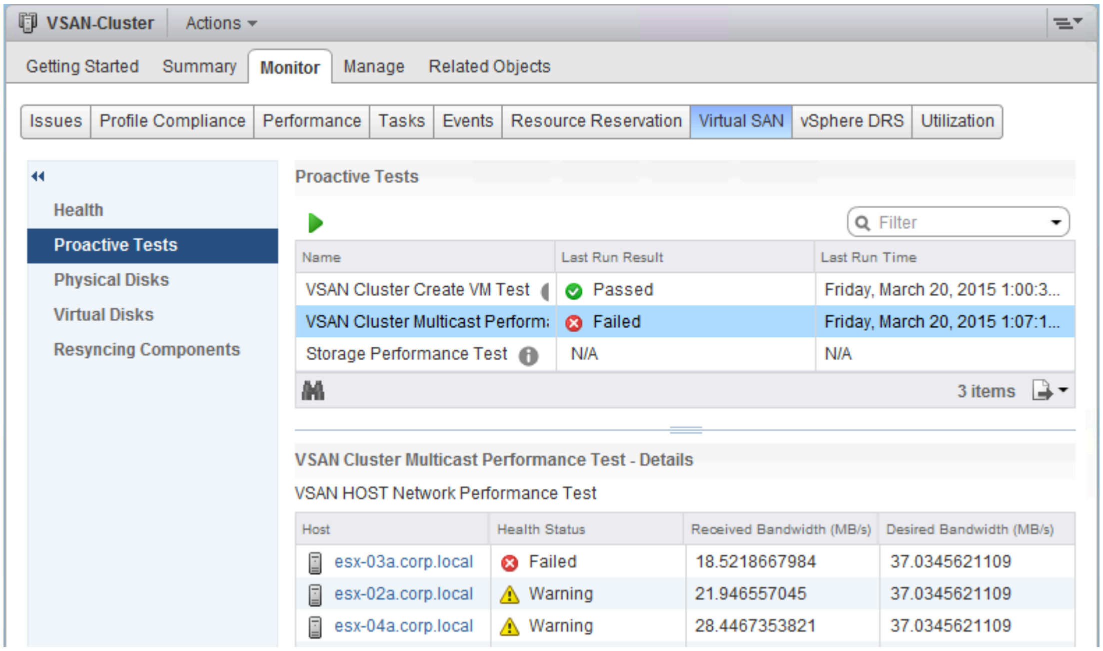
Multicast performance test - Details

VSAN Hosts Multicast Performance Test Result

Host	Health Status	Received Bandwidth (MB/s)	Desired Bandwidth (MB/s)
cs-ie-h03.ie.local	✓ Passed	80.19	125.00
cs-ie-h01.ie.local	✓ Passed	80.77	125.00
cs-ie-h04.ie.local	✓ Passed	79.99	125.00

All hosts have passed. Remember that one host is designated as the sender, so only the results from the other nodes in the cluster are displayed. Bandwidth is above acceptable levels in all cases.

Here is the output from a non-successful test. This was run in a "nested" lab environment using virtual ESXi hosts, so no surprise that the network bandwidth was below accepted levels. However it gives you an idea as to how this test might fail:



Proactive Tests

Name	Last Run Result	Last Run Time
VSAN Cluster Create VM Test	Passed	Friday, March 20, 2015 1:00:3...
VSAN Cluster Multicast Perform:	Failed	Friday, March 20, 2015 1:07:1...
Storage Performance Test	N/A	N/A

VSAN Cluster Multicast Performance Test - Details

VSAN HOST Network Performance Test

Host	Health Status	Received Bandwidth (MB/s)	Desired Bandwidth (MB/s)
esx-03a.corp.local	Failed	18.5218667984	37.0345621109
esx-02a.corp.local	Warning	21.946557045	37.0345621109
esx-04a.corp.local	Warning	28.4467353821	37.0345621109

6.2.2 Running a multicast speed test via the CLI

The multicast performance speed test can also be run from RVC. Here is an example of such a test, with successful results. It takes the cluster as a single argument.

```
> vsan.health.multicast_speed_test <cluster>
 Performing a multicast speed test. One host is selected to send multicast
 traffic, all other hosts will attempt to receive the packets. The test
 is designed such that the sender sends more than most physical networks
 can handle, i.e. it is expected that the physical network may drop packets
 which then won't be received by the receivers. Assuming a TCP speed test
 shows good performance, the most likely suspect for failing the multicast
 speed test are multicast bottlenecks in physical switches.
 The key question this test tries to answer is: What bandwidth is the
 receiver able to get? For VSAN to work well, this number should be at
 least 20MB/s. Typical enterprise environments should be able to do 50MB/s
 or more.

 Now running test ...

 Overall health: Passed
 +--------------------+---------------+---------------------------+--------------------------+
 | Host               | Health Status | Received Bandwidth (MB/s) | Desired Bandwidth (MB/s) |
 +--------------------+---------------+---------------------------+--------------------------+
 | cs-ie-h03.ie.local | Passed        | 81.14                     | 125.00                   |
 | cs-ie-h01.ie.local | Passed        | 81.46                     | 125.00                   |
 | cs-ie-h04.ie.local | Passed        | 81.83                     | 125.00                   |
 +--------------------+---------------+---------------------------+--------------------------+
>
```

6.3 Storage performance test

This test assumes that the Virtual SAN cluster has been correctly formed. It will then create somewhere in the region of 10 to 20 VMDKs per host (which will be distributed by Virtual SAN onto physical disks). Once that step is complete the test issues a synthetic I/O workload on all VMDKs on all hosts in parallel. Afterwards, the VMDKs are deleted. The storage performance tests allow you to set a duration value that determines how long the test should run.

6.3.1 A note about storage performance tests

Since Virtual SAN has a caching tier (read cache and write buffer for hybrid configurations, write caching for all-flash configurations), initial workload performance is dependent on the state of the cache.

Consider the case of an empty cache at the start of an experiment: read-intensive workloads will exhibit lower than expected performance as the cache warms up and a write workload will exhibit better than expected performance as the caching tier absorbs all the initial writes. Over time, read cache will be populated with data that is of interest to the workload, and write buffer will be cleared of data from previous experiments and there will be an equilibrium between the caching tier writes and the capacity tier writes. Therefore, we recommend measuring performance over longer periods to get an accurate estimate of Virtual SAN performance.

There are a number of different tests available in this initial version of health checks:

A. **Basic sanity test, focus on Flash cache layer**. This simulates the “active working set” using a realistic 70/30 split but staying within the hot area of 1GB per host.
B. **Stress test**. This is a stress test, latencies are expected to be on the high side, but it should nicely stress all layers. Uses 1TB of space per host.
C. **Performance Characterization - 100% Read, optimal RC usage**. This should demonstrate the RC (Read Cache) nicely; have enough parallelism to max out Virtual SAN, while not maxing it out so much as to cause high latencies. Uses 10GB of space per host,
D. **Performance Characterization - 100% Write, optimal WB usage**. This should demonstrate the WB (Write Buffer) nicely. Uses 5GB per host.
E. **Performance Characterization - 100% Read, optimal RC usage after warm-up**. This should demonstrate the RC (Read Cache) nicely after a warm-up period; have enough parallelism to max out Virtual SAN, while not maxing it out so much as to cause high latencies. Uses 10GB of space per host,
F. **Performance Characterization – 70/30 Read/Write, realistic, optimal flash cache usage.** This simulates the “active working set” using a realistic 70/30 split but staying within the hot area of 30GB per host.

G. **Performance Characterization – 70/30 Read/Write, high I/O size, optimal flash cache usage.** This simulates the "active working set" using a realistic 70/30 split but staying within the hot area of 30GB per host. Use a big I/O size of 64K, and shows that I/O size impacts latency when compared to the regular version of this test that uses 4K I/O size.

H. **Performance Characterization - 100% Read, Low RC hit rate / All-Flash demo.** This test will perform badly on hybrid configurations but well on All-Flash configurations, i.e. this is the All-Flash demo test. Uses 1TB of space per host.

I. **Performance Characterization - 100% Streaming Reads.** Simulates a pure streaming read workload, like a media cache server. Uses 1TB of space per host.

J. **Performance Characterization - 100% Streaming Writes.** Simulates a pure streaming read workload, like a backup destination. Uses 1TB of space per host.

There are two primary use cases for this test:

1. Burn-in hardware to detect faulty hardware. As the test is very stressful to all aspects of the Virtual SAN stack, including the network, flash devices, storage capacity devices and storage controllers, it should be able to detect unreliable hardware.
2. A simple-to-use tool to assess the performance characteristics of a Virtual SAN cluster. The test can run a number of different workloads, varying between random and sequential, small and large I/O, and different mixes of read and write I/O.

While storage experts may be interested in studying the affects of different workload characteristics, the main purpose from this performance test is to verify that the cluster achieves roughly the performance that one may expect with a given hardware configuration.

VMware has observed various reasons for poor Virtual SAN performance, including misconfigured storage I/O controller settings, faulty hardware and the use of unqualified and untested driver versions. The performance test is a simple way to verify that the IOPS and bandwidth meets requirements.

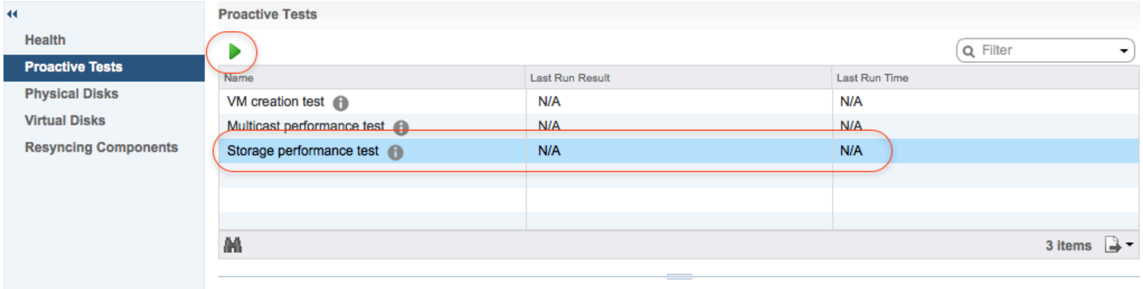
The storage test is a 3-step process via RVC:

1. Create the VMDKs.
2. Run a benchmark against the VMDKs.
3. Delete the VMDKs.

This allows an administrator to run many different workloads against the same set of VMDKs. Workload can currently be one of the list provided above.

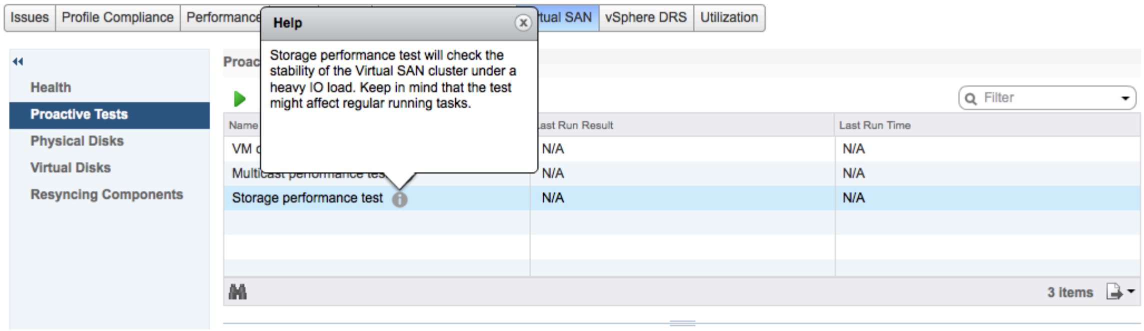
6.3.2 Running storage performance test from the UI

To run this test from the UI, you do exactly the same as the other Proactive Tests. Select the Storage performance test in the UI, and click on the green triangle to begin.



Name	Last Run Result	Last Run Time
VM creation test	N/A	N/A
Multicast performance test	N/A	N/A
Storage performance test	N/A	N/A

To learn more about the test, simply click (i) for information:

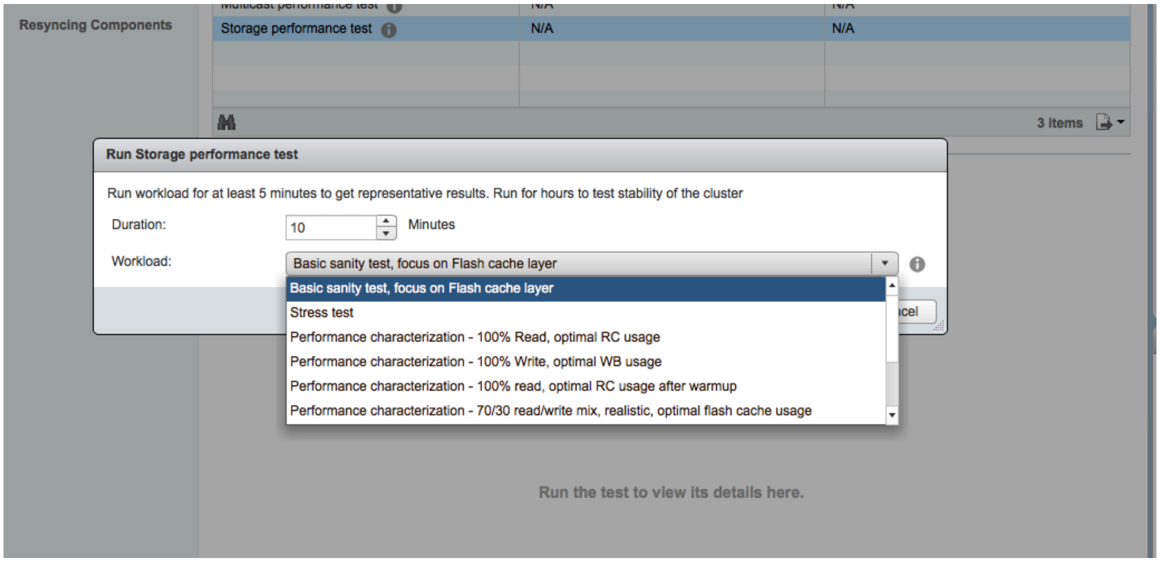


Help

Storage performance test will check the stability of the Virtual SAN cluster under a heavy IO load. Keep in mind that the test might affect regular running tasks.

Name	Last Run Result	Last Run Time
VM c…	N/A	N/A
Multicast performance tes…	N/A	N/A
Storage performance test	N/A	N/A

Before the test starts, you are prompted for a type of test and a duration. By default, a test will run for 10 minutes, but this can be modified. The list of tests are shown below:



Run Storage performance test

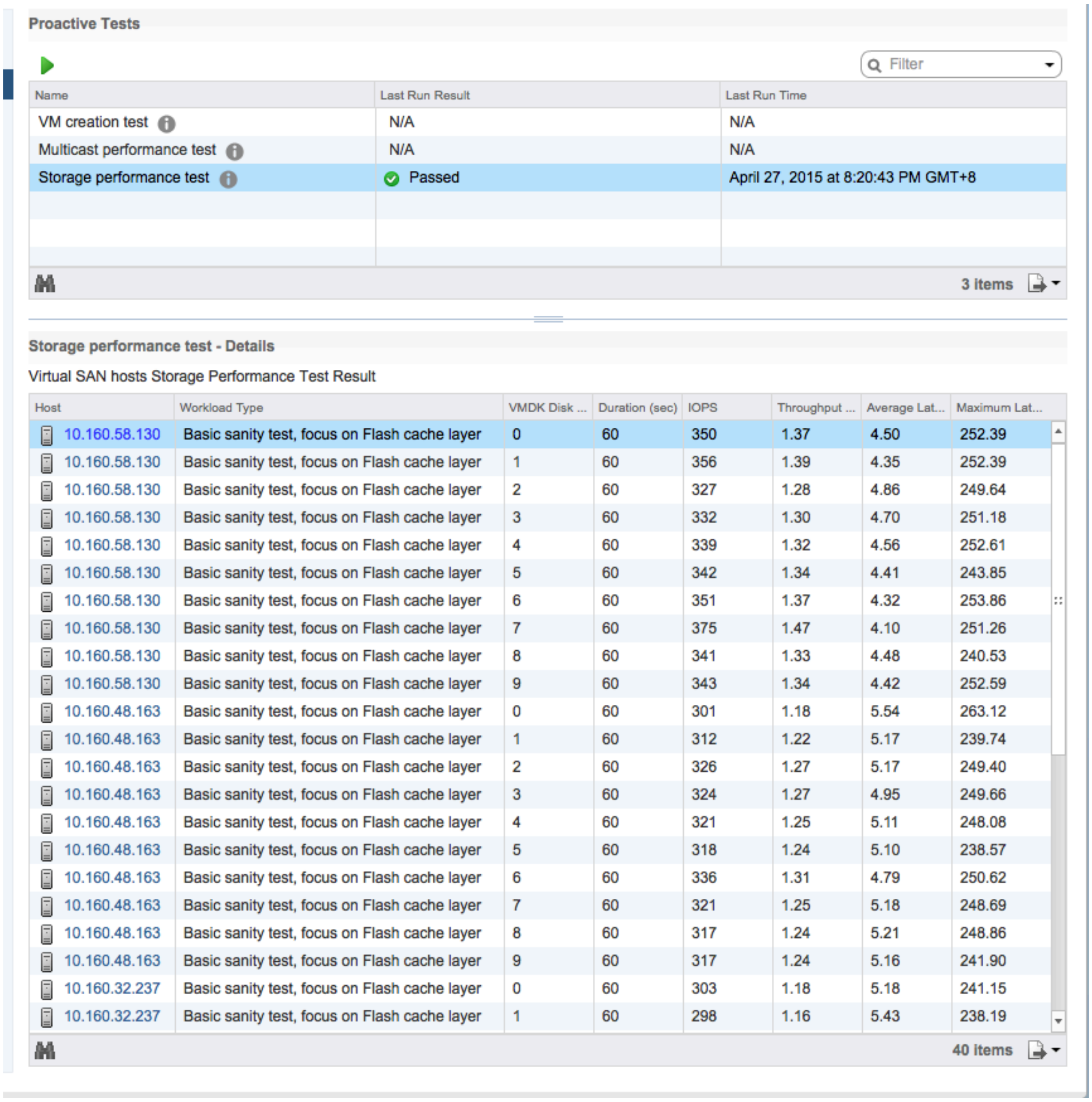
Run workload for at least 5 minutes to get representative results. Run for hours to test stability of the cluster

Duration: 10 Minutes

Workload: Basic sanity test, focus on Flash cache layer

- Basic sanity test, focus on Flash cache layer
- Stress test
- Performance characterization - 100% Read, optimal RC usage
- Performance characterization - 100% Write, optimal WB usage
- Performance characterization - 100% read, optimal RC usage after warmup
- Performance characterization - 70/30 read/write mix, realistic, optimal flash cache usage

When the test completes, the resulting metric are displayed, including the type of test that was run.



Proactive Tests

Name	Last Run Result	Last Run Time
VM creation test	N/A	N/A
Multicast performance test	N/A	N/A
Storage performance test	✓ Passed	April 27, 2015 at 8:20:43 PM GMT+8

3 items

Storage performance test - Details

Virtual SAN hosts Storage Performance Test Result

Host	Workload Type	VMDK Disk ...	Duration (sec)	IOPS	Throughput ...	Average Lat...	Maximum Lat...
10.160.58.130	Basic sanity test, focus on Flash cache layer	0	60	350	1.37	4.50	252.39
10.160.58.130	Basic sanity test, focus on Flash cache layer	1	60	356	1.39	4.35	252.39
10.160.58.130	Basic sanity test, focus on Flash cache layer	2	60	327	1.28	4.86	249.64
10.160.58.130	Basic sanity test, focus on Flash cache layer	3	60	332	1.30	4.70	251.18
10.160.58.130	Basic sanity test, focus on Flash cache layer	4	60	339	1.32	4.56	252.61
10.160.58.130	Basic sanity test, focus on Flash cache layer	5	60	342	1.34	4.41	243.85
10.160.58.130	Basic sanity test, focus on Flash cache layer	6	60	351	1.37	4.32	253.86
10.160.58.130	Basic sanity test, focus on Flash cache layer	7	60	375	1.47	4.10	251.26
10.160.58.130	Basic sanity test, focus on Flash cache layer	8	60	341	1.33	4.48	240.53
10.160.58.130	Basic sanity test, focus on Flash cache layer	9	60	343	1.34	4.42	252.59
10.160.48.163	Basic sanity test, focus on Flash cache layer	0	60	301	1.18	5.54	263.12
10.160.48.163	Basic sanity test, focus on Flash cache layer	1	60	312	1.22	5.17	239.74
10.160.48.163	Basic sanity test, focus on Flash cache layer	2	60	326	1.27	5.17	249.40
10.160.48.163	Basic sanity test, focus on Flash cache layer	3	60	324	1.27	4.95	249.66
10.160.48.163	Basic sanity test, focus on Flash cache layer	4	60	321	1.25	5.11	248.08
10.160.48.163	Basic sanity test, focus on Flash cache layer	5	60	318	1.24	5.10	238.57
10.160.48.163	Basic sanity test, focus on Flash cache layer	6	60	336	1.31	4.79	250.62
10.160.48.163	Basic sanity test, focus on Flash cache layer	7	60	321	1.25	5.18	248.69
10.160.48.163	Basic sanity test, focus on Flash cache layer	8	60	317	1.24	5.21	248.86
10.160.48.163	Basic sanity test, focus on Flash cache layer	9	60	317	1.24	5.16	241.90
10.160.32.237	Basic sanity test, focus on Flash cache layer	0	60	303	1.18	5.18	241.15
10.160.32.237	Basic sanity test, focus on Flash cache layer	1	60	298	1.16	5.43	238.19

40 items

6.3.3 What constitutes a pass or failure?

This proactive storage performance test will fail if, and only if, I/O doesn't flow successfully to disk, as seen from the client. Since the VMDKs are deployed with a *NumberOfFailuresToTolerate = 1*, should a single disk group fail during the test, Virtual SAN, the test would not fail as I/O would still be able to flow to the other replica.

The net result of the test is that it would simply report a lower performance number when the test completes.

To be clear, this storage performance test does not judge the performance results in any way. It simply reports them.

This test is not designed to test disk drives. It tests Virtual SAN, with the Cluster Level Object Manager (CLOM) doing the placement using *NumberOfFailuresToTolerate*=1, etc.

One cannot derive per-physical-disk or even per-host performance from the test results. This needs to be done with VSAN Observer or vRealize Operations Manager.

6.3.4 Using Storage Performance Tests as Burn-in Tests

Considering the fact that this test may be run for an extended period of time, it can indeed be considered as a type of burn-in test for Virtual SAN hardware. As mentioned earlier, this test does stress all aspects of the Virtual SAN stack, including the network, flash devices, storage capacity devices and storage controllers. As a result, it should be able to detect unreliable hardware.

VMware recommend running this test as part of a burn-in for Virtual SAN deployments prior to placing the cluster into production.

This test may also be useful for detecting intermittent hardware issues.

6.3.5 Running a storage performance test from the CLI

There are two options to run the storage performance test from the CLI via RVC. The first is to run everything in a single step; the other is to run the test as 3 distinct steps. Whichever way you choose, there are 3 parts to running the storage performance test from RVC.

1. Prepare
2. Run
3. Cleanup

The storage performance test can be done as three separate steps, outlined above. However, as mentioned, all three parts can also be run in a single step. We will look at some working examples shortly, but first lets examine the help outputs of the different parts of the tests:

Prepare

```
> vsan.health.cluster_load_test_prepare -h
 usage: cluster_load_test_prepare [opts] cluster...
 Prepares a load test for the cluster
   cluster: Path to a ClusterComputeResource
   --runname, -r <s>:   Runname
      --type, -t <s>:   The VMDK workload type
          --help, -h:   Show this message
```

Run

```
> vsan.health.cluster_load_test_run -h
 usage: cluster_load_test_run [opts] cluster...
 Run a load test on the cluster in one command
   cluster: Path to a ClusterComputeResource
        --runname, -r <s>:   Runname
           --type, -t <s>:   The VMDK workload type
   --duration-sec, -d <i>:   The duration for running the load test in second
         --action, -a <s>:   The possible actions are 'prepare', 'run',
                             'cleanup' and 'fullrun'. Default is fullrun
               --help, -h:   Show this message
```

Cleanup

```
> vsan.health.cluster_load_test_cleanup -h
 usage: cluster_load_test_cleanup [opts] cluster...
 Cleanup a load test for the cluster
   cluster: Path to a ClusterComputeResource
   --runname, -r <s>:   Runname
          --help, -h:   Show this message
```

The two main pieces of information required are a run name for the test and a test type. Once you have this information, a test can be prepared, run and cleaned up afterwards.

There are two ways to input the test type. The first is to input a type string as a parameter; the other is to choose the type of test in interactive mode after issuing the command. If the latter option is chosen, the user does not need input the long type string. Instead only the number associated with the type of test needs to be chosen from the list.

In the following examples, we will first look at doing 3 individual steps, while also imputing the type of test as an option to the commands. In the second example, we will look at running the 3 steps in one command, whilst also choosing the test from the list provided.

6.3.6 Working Example I – 3 steps

Step 1. Prepare the load test. The command takes as arguments (i) cluster, (ii) name of test and (iii) type of test to perform.

The valid test types are:

- "Basic sanity test, focus on Flash cache layer"
- "Stress test"
- "Performance characterization - 100% Read, optimal RC usage"
- "Performance characterization - 100% Write, optimal WB usage"
- "Performance characterization - 100% read, optimal RC usage after warmup"
- "Performance characterization - 70/30 read/write mix, realistic, optimal flash cache usage"
- "Performance characterization - 70/30 read/write mix, high IO size, optimal flash cache usage"
- "Performance characterization - 100% read, Low RC hit rate / All-Flash demo"
- "Performance characterization - 100% Streaming reads"
- "Performance characterization - 100% Streaming writes"

Make sure to include the “” around the names of the tests as shown here:

```
> vsan.health.cluster_load_test_prepare -r cortest --type "Stress test" 0
 Preparing VMDK test on VSAN6-Cluster
  VSAN6-Cluster: success
 Preparing VMDK load test is completed for the cluster VSAN6-Cluster with
status green
 +--------------------+--------+-------+
 | Host               | Status | Error |
 +--------------------+--------+-------+
 | cs-ie-h02.ie.local | Passed |       |
 | cs-ie-h03.ie.local | Passed |       |
 | cs-ie-h01.ie.local | Passed |       |
 | cs-ie-h04.ie.local | Passed |       |
 +--------------------+--------+-------+
 >
```

Step 2. Run benchmark, including type and duration:

```
> vsan.health.cluster_load_test_run -r cortest --type "Stress test" -d 300 0
 This command will run the VMDK load test for the given cluster
 If the action is 'fullrun' or not specified, it will do all of steps
 to run the test including preparing, running and cleaning up. And
 it will only run the test based on the VMDK which is created by
 cluster_load_test_prepare if action is 'run'. In this sitution, the
 VMDK cleanup step is required by calling cluster_load_test_cleanup
  VSAN6-Cluster: VimFault: Cannot complete the operation. See the event log for
details.
 VMDK load test completed for the cluster VSAN6-Cluster: red
 +--------------------+--------+-----------------------------------------------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-------+
 | Host               | Status | Error
|
 +--------------------+--------+-----------------------------------------------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-------+
 | cs-ie-h02.ie.local | Error  | cs-ie-h02.ie.local: Prepare VMDK load test
failed: Cannot complete the operation because the file or folder
[vsanDatastore] 2c953755-ea45-dbab-1727-001517a69c72/cortest-cs-ie-
h02.ie.local-0.vmdk already exists. |
 | cs-ie-h03.ie.local | Error  | cs-ie-h03.ie.local: Prepare VMDK load test
failed: Cannot complete the operation because the file or folder
[vsanDatastore] 5d953755-6dc9-9433-fce7-0010185def78/cortest-cs-ie-
h03.ie.local-0.vmdk already exists. |
 | cs-ie-h01.ie.local | Error  | cs-ie-h01.ie.local: Prepare VMDK load test
failed: Cannot complete the operation because the file or folder
[vsanDatastore] 3a953755-a5b1-5d93-bf4e-001f29595f9f/cortest-cs-ie-
h01.ie.local-0.vmdk already exists. |
 | cs-ie-h04.ie.local | Error  | cs-ie-h04.ie.local: Prepare VMDK load test
failed: Cannot complete the operation because the file or folder
[vsanDatastore] 1f953755-b1e6-6cad-8aae-001b21168828/cortest-cs-ie-
h04.ie.local-0.vmdk already exists. |
 +--------------------+--------+-----------------------------------------------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-------+

  >
```

Reason for failure: In the introduction, we mentioned that this test could be run as three individual steps or as a single step. Since we are doing the former (three individual tests), the prepare step has already been run using the run name *cortest*. If "run" is not specified as an action to the above command (using *-a run*), this command tries to run all three steps again. Therefore another 'prepare' step is once again attempted, and because VMDKs already existed using the run name, the test failed. This time we run the test with the "run" action that avoids another prepare step:

```
> vsan.health.cluster_load_test_run -r cortest --type "Stress test" -d 300 0 -a
run
 This command will run the VMDK load test for the given cluster
 If the action is 'fullrun' or not specified, it will do all of steps
 to run the test including preparing, running and cleaning up. And
 it will only run the test based on the VMDK which is created by
 cluster_load_test_prepare if action is 'run'. In this sitution, the
 VMDK cleanup step is required by calling cluster_load_test_cleanup
  VSAN6-Cluster: success
 VMDK load test completed for the cluster VSAN6-Cluster: green
 +--------------------+--------------+------------------+----------------+------+-------
----------+---------------------+----------------------+
 | Host               | Workload Type | VMDK Disk Number | Duration (sec) | IOPS |
Throughput MB/s | Average Latency (ms) | Maximum Latency (ms) |
 +--------------------+--------------+------------------+----------------+------+-------
----------+---------------------+----------------------+
 | cs-ie-h02.ie.local | Stress test   | 0                | 300            | 446  | 3.49
| 5.26                | 632.15               |
 | cs-ie-h02.ie.local | Stress test   | 1                | 300            | 421  | 3.29
| 5.73                | 563.64               |
 | cs-ie-h02.ie.local | Stress test   | 2                | 300            | 645  | 5.05
| 3.96                | 582.75               |
 | cs-ie-h02.ie.local | Stress test   | 3                | 300            | 363  | 2.84
| 6.12                | 257.60               |
 | cs-ie-h02.ie.local | Stress test   | 4                | 300            | 373  | 2.92
| 6.70                | 596.79               |
 | cs-ie-h02.ie.local | Stress test   | 5                | 300            | 504  | 3.94
| 4.03                | 327.78               |
 | cs-ie-h02.ie.local | Stress test   | 6                | 300            | 635  | 4.96
| 4.15                | 264.63               |
 | cs-ie-h02.ie.local | Stress test   | 7                | 300            | 595  | 4.66
| 4.29                | 586.81               |
 | cs-ie-h02.ie.local | Stress test   | 8                | 300            | 355  | 2.78
| 6.27                | 602.28               |
 | cs-ie-h02.ie.local | Stress test   | 9                | 300            | 580  | 4.53
| 4.22                | 588.04               |
 | cs-ie-h02.ie.local | Stress test   | 10               | 300            | 663  | 5.18
| 3.65                | 678.54               |
 | cs-ie-h02.ie.local | Stress test   | 11               | 300            | 418  | 3.26
| 5.58                | 593.18               |
 | cs-ie-h02.ie.local | Stress test   | 12               | 300            | 1278 | 9.98
| 1.77                | 519.26               |
 | cs-ie-h02.ie.local | Stress test   | 13               | 300            | 589  | 4.60
| 4.22                | 586.64               |
 | cs-ie-h02.ie.local | Stress test   | 14               | 300            | 1219 | 9.53
| 1.91                | 602.22               |
 | cs-ie-h02.ie.local | Stress test   | 15               | 300            | 356  | 2.79
| 6.59                | 241.13               |
 | cs-ie-h02.ie.local | Stress test   | 16               | 300            | 327  | 2.56
| 7.42                | 576.66               |
 | cs-ie-h02.ie.local | Stress test   | 17               | 300            | 348  | 2.72
| 6.86                | 373.44               |
 | cs-ie-h02.ie.local | Stress test   | 18               | 300            | 1145 | 8.95
| 2.15                | 579.80               |
 | cs-ie-h02.ie.local | Stress test   | 19              | 300           | 1188 | 9.28
| 1.98                | 520.77               |
 <<truncated>>
```

The command ran successfully. Once you are ready to cleanup, the following commands removes the VMDKs built for the storage performance test.

Step 3. Cleanup the VMDKs created for the test

The final step is cleanup.

```
> vsan.health.cluster_load_test_cleanup -r cortest 0
 Cleaning up VMDK test on cluster VSAN6-Cluster
  VSAN6-Cluster: success
 Cleanup VMDK load test is completed for the cluster VSAN6-Cluster with status
green
 +--------------------+--------+-------+
 | Host               | Status | Error |
 +--------------------+--------+-------+
 | cs-ie-h02.ie.local | Passed |       |
 | cs-ie-h03.ie.local | Passed |       |
 | cs-ie-h01.ie.local | Passed |       |
 | cs-ie-h04.ie.local | Passed |       |
 +--------------------+--------+-------+
```

6.3.7 Working Example II – 1 step

Here is another test, but this time we will do it all in one command, rather than 3 individual commands. The duration for this run has been set to just 1 second in this example. As mentioned earlier, if no test type is specified, a list of available types is displayed and the user can choose which test to run from the list:

```
> vsan.health.cluster_load_test_run -r test -d 1 0
This command will run the VMDK load test for the given cluster
If the action is 'fullrun' or not specified, it will do all of steps
to run the test including preparing, running and cleaning up. And
it will only run the test based on the VMDK which is created by
cluster_load_test_prepare if action is 'run'. In this sitution, the
VMDK cleanup step is required by calling cluster_load_test_cleanup

0: Basic sanity test, focus on Flash cache layer
1: Stress test
2: Performance characterization - 100% Read, optimal RC usage
3: Performance characterization - 100% Write, optimal WB usage
4: Performance characterization - 100% read, optimal RC usage after warmup
5: Performance characterization - 70/30 read/write mix, realistic, optimal flash cache
usage
6: Performance characterization - 70/30 read/write mix, high IO size, optimal flash cache
usage
7: Performance characterization - 100% read, Low RC hit rate / All-Flash demo
8: Performance characterization - 100% Streaming reads
9: Performance characterization - 100% Streaming writes
Choose the storage workload type [0]: 0

 VSAN-Cluster: success
VMDK load test completed for the cluster VSAN-Cluster: green
+----------------+-------------------------------------------------+------------------+----
-----------+------+-----------------+----------------------+----------------------+
| Host           | Workload Type                                   | VMDK Disk Number |
Duration (sec) | IOPS | Throughput MB/s | Average Latency (ms) | Maximum Latency (ms) |
+----------------+-------------------------------------------------+------------------+----
-----------+------+-----------------+----------------------+----------------------+
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 0                |
1              | 97   | 0.38            | 12.20                | 577.37               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 1                |
1              | 86   | 0.34            | 14.09                | 579.62               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 2                |
1              | 119  | 0.47            | 9.99                 | 556.80               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 3                |
1              | 140  | 0.55            | 8.61                 | 551.80               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 4                |
1              | 108  | 0.42            | 11.26                | 579.51               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 5                |
1              | 93   | 0.36            | 13.01                | 574.71               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 6                |
1              | 174  | 0.68            | 6.97                 | 508.73               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 7                |
1              | 122  | 0.48            | 9.81                 | 573.99               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 8                |
1              | 112  | 0.44            | 10.76                | 576.81               |
| 10.160.239.125 | Basic sanity test, focus on Flash cache layer | 9                |
1              | 144  | 0.56            | 8.24                 | 578.16               |
| 10.160.231.97  | Basic sanity test, focus on Flash cache layer | 0                |
1              | 91   | 0.36            | 19.09                | 533.78               |
| 10.160.231.97  | Basic sanity test, focus on Flash cache layer | 1                |
1              | 93   | 0.36            | 12.72                | 562.95               |
| 10.160.231.97  | Basic sanity test, focus on Flash cache layer | 2                |
1              | 72   | 0.28            | 16.38                | 572.51               |
| 10.160.231.97  | Basic sanity test, focus on Flash cache layer | 3                |
1              | 94   | 0.37            | 13.20                | 549.46               |
<<truncated>>
```

6.4 Host Debug Multicast

This RVC command runs a debug multicast test. It ensures that all hosts in the cluster can receive multicast packets. Each host is represented with a character. In this 4-node cluster, there are 4 characters: [ABCD]. If there are any spaces in [ABCD] in front of each packet, that host did not receive the packet.

This test cannot be run directly from the UI.

6.4.1 Running a multicast debug test via the CLI

```
> vsan.health.host_debug_multicast -h
 usage: host_debug_multicast [opts] cluster_or_hosts...
 Debug multicast
   cluster_or_hosts: Path to a ClusterComputeResource
   --password, -p <s>:   ESX Password
     --vmknic, -v <s>:   vmknic name
   --duration, -d <i>:   Duration to watch for packets. 1 minute is recommend
                         (default: 60)
     --no-agenthb, -n:   Don't display Agent heartbeats
           --help, -h:   Show this message
```

```
> vsan.health.host_debug_multicast 0 --password VMware123! --vmknic vmk2
2015-04-13 09:28:31 +0000: Gathering information about hosts and VSAN
 2015-04-13 09:28:31 +0000: Watching packets for 60 seconds
 2015-04-13 09:29:34 +0000: Got observed packets from all hosts, analysing

 Automated system couldn't derive any issues.
 Either no problem exists or manual inspection is required.

 To further help the network admin, the following is a list of
 packets with source and destination IPs. As all these packets
 are multicast, they should have been received by all hosts in
 the cluster. To show which hosts actually saw the packets, each
 host is represented by a character (A-Z). If the character is
 listed in front of the packet, the host received the packet. If
 the space is left empty, the host didn't receive the packet.

 A = Host cs-ie-h01.ie.local
 B = Host cs-ie-h02.ie.local
 C = Host cs-ie-h03.ie.local
 D = Host cs-ie-h04.ie.local
 [ABCD] 1428917359.91:           MASTER_HEARTBEAT (#00289121) from:172.32.0.1()
to:224.2.3.4
 [ABCD] 1428917345.91:           MASTER_HEARTBEAT (#00289107) from:172.32.0.1()
to:224.2.3.4
 [ABCD] 1428917301.91:           MASTER_HEARTBEAT (#00289063) from:172.32.0.1()
.
.
.
 [ABCD] 1428917347.91:           MASTER_HEARTBEAT (#00289109) from:172.32.0.1()
to:224.2.3.4
 [ABCD] 1428917319.91:           MASTER_HEARTBEAT (#00289081) from:172.32.0.1()
to:224.2.3.4
```

7. Additional Information

7.1 Documentation

Link to Virtual SAN 6.1 Release Notes
Link to Virtual SAN 6.1 Administrators Guide
Link to Virtual SAN 6.0 Health Check Plugin Guide

Link to Virtual SAN 6.0 Release Notes
Link to Virtual SAN 6.0 Administrators Guide
Link to Virtual SAN 6.0 Troubleshooting Reference Manual
Link to Ruby vSphere Console (RVC) Reference Guide for VSAN 6.0

7.2 Virtual SAN Resources

https://www.vmware.com/products/virtual-san/resources

7.3 Support Issues

Collecting Virtual SAN Logs - http://kb.vmware.com/kb/2072796

7.4 Where does one locate the Health Check software?

The official location of the health check 6.0.1 RPM, MSI and VIB is the following URL:

https://my.vmware.com/group/vmware/get-download?downloadGroup=VSANHEALTH600

No details were available on the health check 6.1 components at the time of going to print. Check the VSAN download site on vmware.com.

7.5 Where does one locate the latest HCL file?

The official location of the HCL download file is the following URL:

http://partnerweb.vmware.com/service/vsan/all.json

Appendix A Health Check Details

Although the individual health checks have links to knowledgebase articles which provide additional details on the health check, why they might fail and actions to take in the event of a failure, the details are also included in this appendix.

A.1 Cluster Health – ESX VSAN Health Check installation

A.1.1 What does this check do?

This check verifies that all ESXi hosts have the Virtual SAN Health Check VIB installed.

A.1.2 What does it mean when it is in an error state?

If the check reports an error, it may means that one or more ESXi hosts do not have the health check VIB installed.

Administrators should correlate the result of this health check with the one from the Virtual SAN Health version check. Check the version of the VIB installed on the ESXi hosts and if the correct version is installed on all hosts, then everything is fine.

If the version is not correct, then it can be upgraded. From the vSphere web client UI, navigate to the cluster, Manage -> Virtual SAN, and in the Health check section, click on *update*.

If the VIB was installed via vSphere Update Manager or manually, this check will fail and can safely be ignored.

A.1.3 How does one troubleshoot and fix the error state?

Install the Virtual SAN Health Check VIB on all ESXi hosts that are participating in the Virtual SAN cluster.

A.2 Cluster Health - VSAN Health Checks up-to-date

This check ensures that all health check VIBs installed on the ESXi hosts are up to date.

A.2.1 What does this check do?

This check ensures that all health check VIBs installed are up to date. The health check is initially installed on the vCenter Server. From there it is pushed out to the ESXi hosts in the Virtual SAN cluster.

This health check verifies that the ESXi hosts in the Virtual SAN cluster have the latest version of the Virtual SAN Health Check VIB installed. It is comparing the version of health checks installed on the vCenter server to the version installed on the ESXi hosts.

Note that this is not checking the "latest" version of the health check available on vmware.com. It is simply checking that the ESXi hosts are running the latest version of health check installed on the vCenter server.

Any host running an older version, or no version, will be highlighted in the output.

A.2.2 What does it mean when it is in an error state?

All ESXi hosts should be running the same version of the health checks VIB. If this check displays an error, then one or more hosts are running old, out of date versions of the health check VIB, or the host does not have the health check VIB installed. if a host does not have health check VIB installed, this host will not be listed in the table under service-up-to-date.

A.2.3 How does one troubleshoot and fix the error state?

In such cases, it is recommended to update the version of the Virtual SAN health check VIB. This is as simple as navigating to Cluster -> Manage -> Virtual SAN -> General and clicking the "Update" or "Retry" button. When all hosts are running the latest version of the VIB, only a "Disable" button is visible. See the previous sections of this guide on the installation and updating of the Virtual SAN Health check for a complete description on what is required to install the health checks VIB.

Note that mixed versions are supported, but to ensure a consistent and pleasant user experience, and to ensure that all the latest health checks can be reliably executed, it is highly recommended to keep the Virtual SAN Health Check versions synchronized across all hosts in the cluster, and to use the most up to date version of the VIB.

A.3 Cluster Health - Advanced Virtual SAN configuration in sync

Virtual SAN has a number of advanced configuration options that can be used for tuning, or to address the special requirements of particular deployments. One would not normally change these advanced settings, unless guidance from VMware Technical Support is provided, or there was a detailed procedure on how and why to change the advanced setting in a VMware Knowledge Base article. These advanced configurations options are set on a per host basis, which makes it easy to create inconsistent advanced setting configurations across a Virtual SAN cluster.

A.3.1 What does this check do?

This check ensures that critical Virtual SAN advanced configuration options have a consistent value across all hosts in a given Virtual SAN cluster.

Note that this does not check if the value is "good", or even if it is the "default". It is purely a check for consistency. If you have set any advanced settings to values that are not appropriate, this check will not highlight this if they have been set to consistently inappropriate values across all the hosts in the cluster.

A.3.2 What does it mean when it is in an error state?

If this check fails, it means that some advanced configuration settings have different values on different hosts in the cluster. The advanced configuration parameter that is not in sync is displayed in the health check details.

A.3.3 How does one troubleshoot and fix the error state?

An administrator should ensure that all advanced configuration options that are relevant to Virtual SAN are set to the same value across all ESXi hosts in the Virtual SAN cluster.

To change an Advanced Setting, navigate to Hosts & Clusters in the vSphere web client, select the ESXi host from the inventory that this health check has highlighted as having the incorrect advanced settings, then select Manage -> Settings, then Advanced System Settings. Update the advanced setting to ensure that all settings are consistent throughout the cluster. Note that changing some advanced settings may require a restart of services. Reach out to VMware Global Support Services if you are unsure.

Note that host profiles is one sure way to keep all nodes in a Virtual SAN cluster consistent, and will highlight if any settings are not in sync. Refer to the vSphere documentation on host profiles for further information.

A.4 Cluster Health - VSAN CLOMD liveness

This knowledge base article explains the purpose of the ”Cluster health – CLOMD liveness check”, and provides details on why it might report an error.

CLOMD (Cluster Level Object Manager Daemon) plays a key role in the operation of a Virtual SAN cluster. It runs on every host and is responsible for new object creation, initiating repair of existing objects after failures, all types of data moves and evacuations (e.g. Enter Maintenance Mode, Evacuate data on disk removal from Virtual SAN), maintaining balance and thus triggering rebalancing, implementing policy changes, etc.

It doesn't actually participate in the data path, but it triggers data path operations and as such is a critical component during a number of management workflows and failure handling scenarios.

VM power on, or Storage vMotion to Virtual SAN are two operations where CLOMD is required (and which are not that obvious), as those operations require the creation of a swap object, and object creation requires CLOMD.

Similarly, starting with Virtual SAN 6.0, memory snapshots are maintained as objects, so taking a snapshot with memory state will also require CLOMD.

A.4.1 What does this check do?

This checks if CLOMD, the Cluster Level Object Manager daemon is alive or not. It does so by first checking that the service is running on all ESXi hosts, and then contacting the service to retrieve run-time statistics to verify that CLOMD can respond to inquiries.

Note that this does not ensure that all of the functionalities discussed above (e.g. object creation, rebalancing) actually work, but it gives a first level assessment as to the health of CLOMD.

A.4.2 What does it mean when it is in an error state?

CLOMD may still have issues, but this test does a very basic check to make sure that it can process requests. If this reports an error, the state of the CLOMD process needs to be checked on the relevant hosts.

A.4.3 How does one troubleshoot and fix the error state?

If any of the ESXi hosts are disconnected, the CLOMD liveness state of the disconnected host is shown as 'unknown'. If the Health check is not installed on a particular ESXi host, the CLOMD liveness state of all the hosts is also reported as 'unknown'.

If the CLOMD service is not running on a particular ESXi hosts, the CLOMD liveness state of one host is 'abnormal'.

For this test to succeed the health check needs to be installed on the ESXi host and the CLOMD service needs to be running. The command `/etc/init.d/clomd status` can be used at the CLI of an ESXi host to get the state of the CLOMD service. Note that this commands simply reports that the CLOMD daemon is running. It doesn't say if CLOMD is responding to requests, and it doesn't say if it can successfully handle them.

The CLOMD service can be restarted on an ESXi host via `/etc/init.d/clomd restart`

If the CLOMD health check is still failing after these steps, open a support request with VMware Global Support Services (GSS). If the CLOMD health check continues to fail on a regular basis, customers should also consider opening a support request.

If the CLOMD health check passes, another good way to further probe into CLOMD health is to perform a VM creation test (Proactive tests), as that will involve object creation that will exercise and test CLOMD thoroughly.

A.5 VSAN HCL health – VSAN HCL DB up-to-date

Adherence to the VMware Compatibility Guide (VCG) is critically important to the stability of Virtual SAN environments. Experience has shown that failing to observe the VCG often leads to production outages over time. It is therefore very important to keep an eye on the health checks in the HCL checker category.

A.5.1 What does this check do?

This health check verifies the VMware Compatibility Guide database used for the HCL checks is up-to-date. These VCG checks are not done against the HCL on vmware.com, but rather against a copy stored on vCenter server.

The health feature originally shipped with a copy of the database, which was current at the time shortly before version 6.0 released. This copy of the database will most definitely get out-dated over time. This is especially true as new certifications with partners get added to the VCG.

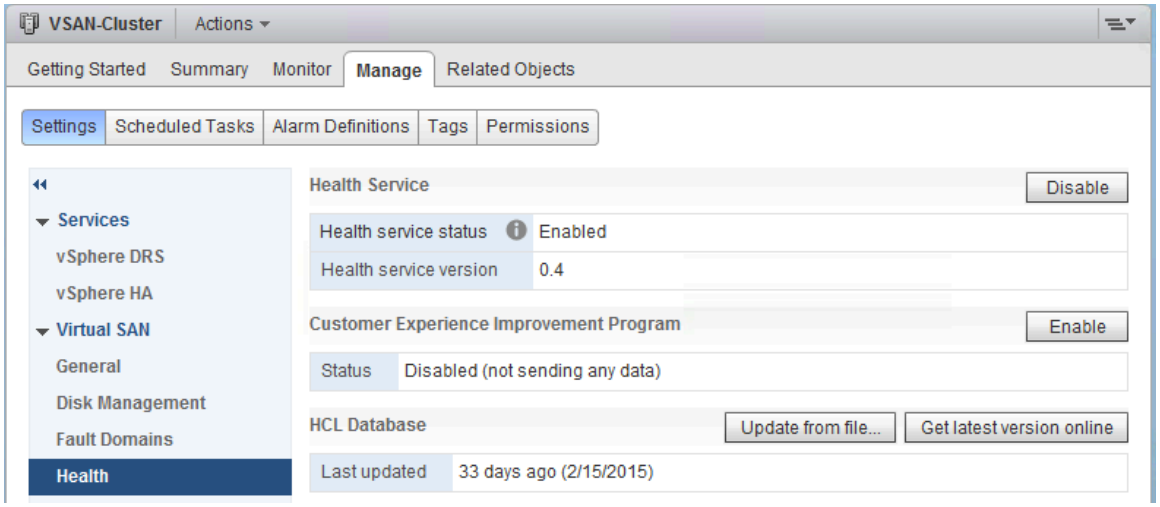
Note that hardware vendors regularly update their drivers and VMware adds certification for them. Older drivers may even get removed from the VCG to reflect issues found. Hence it is critically important to keep the local copy up-to-date.

A.5.2 What does it mean when it is in an error state?

This check uses thresholds of 90 or 180 days of age to show a warning or error, respectively. Those thresholds are on the high side, and VMware's recommendation to keep the database updated as often as operationally possible.

A.5.3 How does one troubleshoot and fix the error state?

Quite simply, administrators need to keep the HCL database up to date on their vCenter server. Navigate to the **Manage -> Settings -> Health**, and there you will find different options for updating the HCL database. If your vCenter has access to the Internet, you can get the latest version online with the click of a button. Alternatively, a HCL file can be downloaded and manually uploaded using the update from file button. The official site for downloading the HCL file is the following URL: http://partnerweb.vmware.com/service/vsan/all.json



Health Service

Health service status: Enabled

Health service version: 0.4

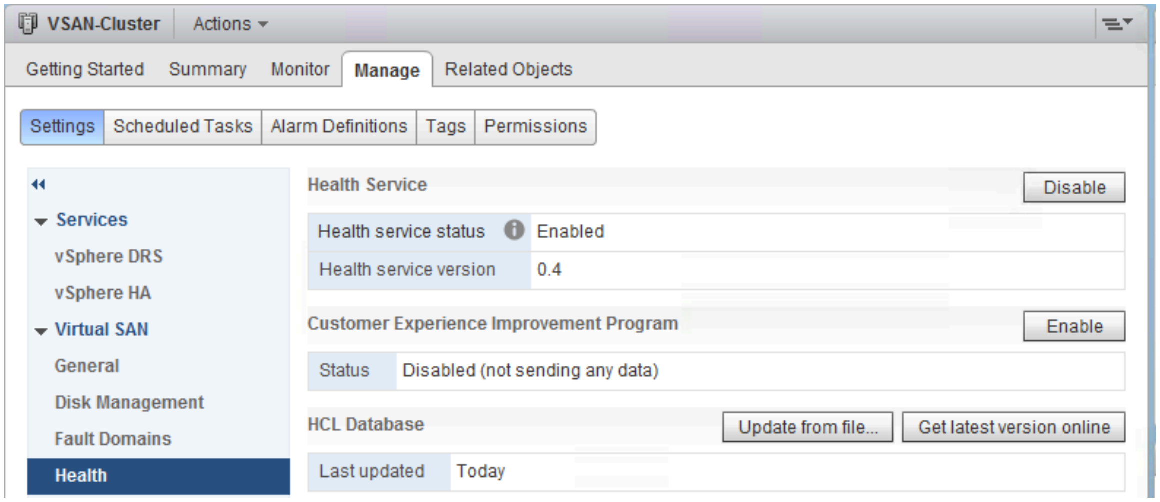
Customer Experience Improvement Program

Status: Disabled (not sending any data)

HCL Database

Last updated: 33 days ago (2/15/2015)

Once the database has been updated, the Last updated field shows the date of the HCL database:



Health Service

Health service status: Enabled

Health service version: 0.4

Customer Experience Improvement Program

Status: Disabled (not sending any data)

HCL Database

Last updated: Today

Note that the HCL database refresh can be done in the main health page as shown here, and also via the action button associated with the health check.

A.6 VSAN HCL health – SCSI Controller on VSAN HCL

We've already mentioned how important it is to adhere to the VMware Compatibility Guide (VCG). This next check relates to the SCSI controller on the ESXi hosts.

A.6.1 What does this check do?

This check displays information regarding the local storage I/O controller on the ESXi host.

The check verifies that this critical piece of the hardware is listed on the VCG at all. The lookup is performed based on the PCI ID information (Vendor ID, Device ID, SubVendor ID, SubDevice ID).

Note that PCI IDs can change with firmware changes.

A.6.2 What does it mean when it is in an error state?

The first step to take if this check fails is to update the VCG database. It is possible the hardware (or its firmware) were recently added to the VCG. If the device is still not listed in the VCG (and the health check fails), the Virtual SAN environment may be at risk.

A.6.3 How does one troubleshoot and fix the error state?

Detailed instructions on how to query the make, model and version of your storage I/O controller can be found in the *Virtual SAN 6.0 Troubleshooting Reference Manual*. If you still have difficultly determining storage I/O controller information, we recommend contacting VMware Global Support Services to assess the situation fully. Do not simply rely on the automated health checks. VMware Support will also assist with any mitigation steps.

A.7 VSAN HCL health – Controller Release Support

A.7.1 What does this check do?

This check displays information about storage I/O controller drivers, and whether or not there is a supported driver for a given controller on the current release of ESXi. This could vary on a per ESXi release basis, i.e. driver was supported in version 5.5 but not 6.0. This is also considered when the check is run.

A.7.2 What does it mean when it is in an error state?

Assuming that the health check "Controller on VSAN HCL" passed, (HCL standing for hardware compatibility guide), this check will further verify that there is support for the release of ESXi in use. This is especially important as major new releases trigger a re-certification requirement, which means a controller supported on an earlier release of ESXi may not (yet) be supported on the current version.

Note that if the "Controller on VSAN HCL" check failed, then this check will also fail.

A.7.3 How does one troubleshoot and fix the error state?

If this check fails, the first step is to update the VCG database. It is possible the hardware (or its firmware) were recently added to the VCG. If the device is still not listed in the VCG (and the health check fails), the Virtual SAN environment may be at risk.

Detailed instructions on how to query the make, model and version of your storage I/O controller can be found in the Virtual SAN 6.0 Troubleshooting Reference Manual. If you still have difficultly determining storage I/O controller information, we recommend contacting VMware Global Support Services to assess the situation fully. Do not simply rely on the automated health checks. VMware Support will also assist with any mitigation steps.

A.8 VSAN HCL health – Controller Driver

A.8.1 What does this check do?

This health check displays whether or not the storage I/O controller driver is supported for controller installed on the host running ESXi, and whether it is supported with that release of ESXi.

Assuming that the "Controller on VSAN HCL" and "Controller Release Support" health checks have passed, this check will further verify that there the driver version in use is on the list of supported drivers.

This is important as drivers play a critical role in stability and integrity of Virtual SAN. Vendors often update their drivers to address critical bugs. In such cases VMware may revoke the certification status of an old driver and only support the new version of the driver. Hence it is possible this check to turn from a healthy "green" state to showing warnings after refreshing the VCG DB. In such cases it is strongly recommended to upgrade the driver to the recommended version.

Note that here is also the possibility of a vendor updating a driver, and making it downloadable from their website. If VMware has not certified the driver for Virtual SAN (either because the certification hasn't happened yet, or because it actually failed the certification) VMware does not recommend upgrading to this driver unless it appears on the VCG.

Before upgrading a driver we recommend to refresh the VCG DB, look up the details section and check for the supported drivers. If the new driver is supported, proceed with the upgrade.

A.8.2 What does it mean when it is in an error state?

Note that if the "Controller on VSAN HCL" or "Controller Release Support" check failed, then this check will also fail. If the driver is not listed in the VCG for this device and ESXi release, the Virtual SAN environment may be at risk.

A.8.3 How does one troubleshoot and fix the error state?

If this test fails, updating the VCG database is recommended as a first step. It is possible the hardware (or its firmware) or the release of the driver were recently added to the VCG. Detailed instructions on how to query the make, model and version of your storage I/O controller can be found in the *Virtual SAN 6.0 Troubleshooting Reference Manual*. If you still have difficultly determining storage I/O controller information, we recommend contacting VMware Global Support Services to assess the situation fully. Do not simply rely on the automated health checks. VMware Support will also assist with any mitigation steps.

A.9 HCL health – Host issues retrieving hardware info

This health check only appears if there are issues communicating to one or more hosts in the cluster from vCenter.

A.9.1 What does this check do?

It is informing the administrator that it cannot get HCL related information from the ESXi host in question in order to check the HCL compatibility.

A.9.2 What does it mean when it is in an error state?

In all likelihood, there is a host disconnected from vCenter. This health check error probably accompanied with a Network Health issue, such as “Host disconnected from vCenter.

A.9.3 How does one troubleshoot and fix the error state?

Administrators should address the host disconnect issue, and allow the health check plugin to communicate successfully with all hosts in the cluster. Check also the recommendations made in section 6.13.3 on how to deal with disconnected hosts.

A.10 Network health - Hosts disconnected from vCenter

If an ESXi host that is part of a Virtual SAN cluster is disconnected from vCenter (or is otherwise not responding), it could cause operational issues. This could be due to a power outage or some other event. Virtual SAN Still considers it a member of the cluster.

It *may* mean that Virtual SAN is unable to use the capacity or resources available on this ESXi host, and it *may* also imply that components residing on the disks on this ESXi host are now in an absent state, placing virtual machines at risk should another failure occur in the cluster. However, because it is disconnected, its overall state is not known.

A.10.1 What does this check do?

This checks whether vCenter server has an active connection to all ESXi hosts in the vSphere cluster.

A.10.2 What does it mean when it is in an error state?

If an ESXi host that is part of a Virtual SAN cluster is disconnected from vCenter (or is otherwise not responding), it could cause operational issues. It *may* mean that Virtual SAN is unable to use the capacity or resources available on this ESXi host, and it *may* also imply that components residing on the disks on this ESXi host are now in an ABSENT state, placing virtual machines at risk should another failure occur in the cluster. However, because it is disconnected from vCenter, the overall state of this ESXi host is not known. This checks whether vCenter server has an active connection to all ESXi hosts in the vSphere cluster.

A.10.3 How does one troubleshoot and fix the error state?

An administrator should immediately check why an ESXi host that is part of the Virtual SAN cluster is no longer connected to vCenter. One option is to manually try to reconnect the host to vCenter server via the vSphere web client UI. Right click on the disconnected ESXi host in question, select “Connection” from the drop-down menu and then select “Connect”. Provide the appropriate responses to the connection wizard where required.

If the host fails to do a manual connect, an administrator could try to connect to the host via SSH, if it available, to assess its status. Another option would be to connect to the server’s console (iLO for HP, DRAC for DELL, etc) and ascertain if there is some underlying problem with the server in question. VMware KB Article 1003409 provides additional information on how to troubleshoot disconnected ESXi hosts.

A.11 Network Health – Hosts with connectivity issues

A.11.1 What does this check do?

This check refers to situations where vCenter lists the host as connected, but API calls from vCenter to the host are failing. This situation should be extremely rare, but in case it happens it leads to similar issues as the "Host disconnected from VC" situation and it could cause operational issues.

A.11.2 What does it mean when it is in an error state?

If this health check highlights that an ESXi host has connectivity issues, vCenter server does not know its state. The host *may* be up, and *may* be participating in the Virtual SAN cluster, serving data, and playing a critical role in the storage functions of the Virtual SAN cluster.

However it could also mean that the host *may* be down and unavailable. vCenter server, and hence the Virtual SAN Health check, cannot fully asses the situation as long the host is disconnected.

A.11.3 How does one troubleshoot and fix the error state?

An administrator should immediately check why an ESXi host that is part of the Virtual SAN cluster is no longer connected to vCenter.

One option is to manually try to reconnect the host to vCenter server via the vSphere web client UI. Right click on the disconnected ESXi host in question, select “Connection” from the drop-down menu and then select “Connect”. Provide the appropriate responses to the connection wizard where required.

If the machine *cannot* be connected to vCenter but *can* be connected to via the vSphere web client, then the issue is likely related to network connectivity or communication problems rather than management-agent problems.

If the host fails to do a manual connect, an administrator could try to connect to the host via SSH, if it available, to assess its status. Another option would be to connect to the server’s console (iLO for HP, DRAC for DELL, etc) and ascertain if there is some underlying problem with the server in question.

VMware KB Article 1003409 provides additional information on how to troubleshoot disconnected ESXi hosts.

A.12 Network health – VSAN cluster partition

In order to function properly, all Virtual SAN hosts should be able to talk to each other over both multicast and unicast. If that is not the case, a Virtual SAN cluster will split into multiple network "partitions", i.e. sub-groups of ESXi hosts that can talk to each other, but not to other sub-groups. When that happens, Virtual SAN objects may become unavailable until the network misconfiguration is resolved. For smooth operations of production Virtual SAN clusters it is very important to have a stable network with no extra network partitions (i.e. only one partition).

A.12.1 What does this check do?

In order to function properly, all Virtual SAN hosts should be able to talk to each other over both multicast and unicast.

For further details on multicast and unicast, refer to the explanations in the following article: http://blogs.vmware.com/vsphere/2014/09/virtual-san-networking-guidelines-multicast.html

If it is the case that all the nodes in the cluster cannot communicate, a Virtual SAN cluster will split into multiple network "partitions", i.e. sub-groups of ESXi hosts that can talk to each other, but not to other sub-groups.

When that happens, Virtual SAN objects may become unavailable until the network misconfiguration is resolved. For smooth operations of production Virtual SAN clusters it is very important to have a stable network with no extra network partitions (i.e. only one partition)

This health check examines the cluster to see how many partitions exist. It displays an error if there is more than a single partition in the Virtual SAN cluster. Note that this check really determines if there is a network issue, but doesn't attempt to find a root cause. Other network health checks need to be used to root cause.

A.12.2 What does it mean when it is in an error state?

This health check is said to be OK when only one single partition is found. As soon as multiple partitions are found, the cluster is unhealthy.

There are likely to be other warnings displayed in the vSphere web client when a partition occurs. For instance, the network configuration status in the Virtual SAN General view is likely to state network misconfiguration detected.

Another interesting view is the Virtual SAN Disk Management view. This contains a column detailing which network partition group a host is part of. To see how many partitions the cluster has been split into, examine this column. If each host is in its own network partition group, then there is a cluster-wide issue. If only one host is in its own network partition group and all other hosts are in a different network partition group, then only that host has the issue. This may help to isolate the issue at hand and focus the investigation effort. Note that the health UI will display the same information in the details section of this check.

A.12.3 How does one troubleshoot and fix the error state?

The network configuration issue needs to be located and resolved. Additional health checks on the network are designed to assist an administrator to find the root cause of what may be causing the network partition. The reasons can range from misconfigured subnets (*All hosts have matching subnets*), misconfigured Virtual SAN traffic VMkernel adapters (*All hosts have a VSAN vmknic configured*), misconfigured VLANs or general network communication issues to specific multicast issues (*All hosts have matching multicast settings*). The additional network health checks are designed to isolate which of those issues may be the root cause, and should be viewed in parallel with this health check.

Aside from misconfigurations, it is also possible to have partitions when the network is overloaded, leading to substantial dropped packets. Virtual SAN can tolerate a small amount of dropped packets but once there is above a medium amount of dropped packets, performance issues may ensure.

If none of the misconfiguration checks indicate any issue, it is advisable to watch for dropped packet counters, as well as perform a pro-active network performance test. Proactive network performance tests, which may be initiated from RVC, are discussed later in the guide.

To examine the dropped packet counters on an ESXi host, use `esxtop` network view (n) and examine the field `%DRPRX` for excessive dropped packets. You may also need to watch the switch and switch ports, as they may also drop packets. Another metric that should be checked for is an excessive of *pause frames* that can slow down the network and impact performance. This is something we will look to automate in a future version of the health check plugin.

Useful blog - Troubleshooting multicast issues.

A.13 Network Health – Unexpected VSAN cluster members

This check tests whether all hosts participating in Virtual SAN are part of the same vSphere cluster. This is important, as cluster-wide processes such as enabling DRS, or enabling vSphere HA will not include hosts that are not part of the vSphere cluster.

A.13.1 What does this check do?

This health check tests whether all hosts participating in Virtual SAN are part of the same vSphere cluster. This is important, as cluster-wide processes such as enabling DRS, or enabling vSphere HA will not include hosts that are not part of the vSphere cluster and may lead to operation issues.

This check compares the vSphere cluster members to the Virtual SAN cluster members. If an administrator only ever uses vCenter server to manage Virtual SAN, this check should never fail, as by definition a Virtual SAN cluster and a vSphere cluster should in effect have all the same members.

However, if an administrator used the command line at any time for cluster membership, e.g. "`esxcli vsan cluster join`" it is quite possible to create a misconfigured cluster, where an ESXi host that participates in Virtual SAN is not part of the vSphere cluster. Another possibility is where host profiles was used to join the host to the cluster.

A.13.2 What does it mean when it is in an error state?

Even though the ESXi host might not be part of the vSphere cluster, Virtual SAN will still utilize the host, use it to store data and service I/O. In other words, the datastore functions properly and correctly.

ESXi hosts that are disconnected from vCenter could show up in this way, and that reconnecting them to vCenter will resolve this health check issue.

However, when the cluster is in such a situation, it can give rise to operational hazards. As the host is not tracked as a part of the vSphere cluster, it is very easy to overlook the critical role the host plays in the availability and persistence of data on Virtual SAN.

For example, inadvertently rebooting or repurposing the host for another use, or by simply placing it into maintenance mode may cause issues to the Virtual SAN cluster and impact the availability of the virtual machines running on the cluster. The administrator may not notice that impact based on what the vSphere web client UI reports. There may be no warning generated that the host is about to be repurposed for some other user, as vCenter doesn't recognize the host to be part of the cluster.

A.13.3 How does one troubleshoot and fix the error state?

To get an overall view of the Virtual SAN cluster state, Ruby vSphere Console (RVC) commands such as “`vsan.cluster_info`” can help. This will display all hosts that are participating in Virtual SAN, and can be used to compare against the list of hosts that are part of the vSphere cluster to determine which one is not included.

To get an individual hosts view of the cluster, the command "`esxcli vsan cluster get`" may be used.

An administrator should check why the host is not part of the Virtual SAN cluster but is part of the vSphere cluster. If a host was joined to the cluster in error using the CLI, another CLI command, "`esxcli vsan cluster leave`" may be used to take the ESXi host back out of the cluster.

However the ESXi host should first be put into maintenance mode using the “full data migration” option to evacuate all data first to ensure data availability.

If the host does not leave the cluster, make a note of the reason why. Also note any warnings or errors that are created in the vmkernel.log when this operation is attempted. Contact VMware Global Support Services if the issue persists.

A.14 Network Health – Hosts with VSAN disabled

This health check is similar to a previous check, the unexpected Virtual SAN cluster members. It is also possible to have ESXi hosts participating in a vSphere cluster that has Virtual SAN enabled, but individual ESXi hosts do not have Virtual SAN enabled. This can arise when administrators use a combination of command line and UI to manage the Virtual SAN cluster. If a user only uses vCenter server to manage Virtual SAN, this check should never fail.

The most common cause of such a misconfiguration is that during the course of troubleshooting a Virtual SAN issue, an administrator has issued commands such as "`esxcli vsan cluster leave`" on an ESXi host, and if the host is not re-added to the Virtual SAN cluster, the host no longer participates in Virtual SAN.

A.14.1 What does this check do?

This check ensures that all hosts in a Virtual SAN cluster have Virtual SAN enabled.

A.14.2 What does it mean when it is in an error state?

While it may look from a vCenter server perspective that the host is fully participating in the Virtual SAN cluster, this may not be the case. By not participating in the cluster, available capacity for both space and performance is reduced.

More importantly, if this ESXi host stores any Virtual SAN data (e.g. virtual machine objects) on its local disks, having it removed from Virtual SAN will impact object health.

By disabling Virtual SAN on a host, all components on the host entering ABSENT states from the perspective of the active Virtual SAN hosts in the cluster. If the host is disconnected from the Virtual SAN cluster for longer than 60 minutes, the components marked as ABSENT will be rebuilt elsewhere in the cluster, leading to unnecessary rebuild I/O, which may in turn impact virtual machine I/O.

A.14.3 How does one troubleshoot and fix the error state?

Verify that all ESXi hosts that are part of the cluster have Virtual SAN enabled. The command "`esxcli vsan cluster get`", when run on individual ESXi hosts, can tell if a host is participating in the Virtual SAN cluster. Here is an example of running the command on an ESXi host that is part of a healthy 4-node Virtual SAN cluster?

```
[root@cs-ie-h01:~] esxcli vsan cluster get
 Cluster Information
    Enabled: true
    Current Local Time: 2015-02-16T10:20:48Z
    Local Node UUID: 545ca9af-ff4b-fc84-dcee-001f29595f9f
    Local Node State: MASTER
    Local Node Health State: HEALTHY
    Sub-Cluster Master UUID: 545ca9af-ff4b-fc84-dcee-001f29595f9f
    Sub-Cluster Backup UUID: 54188e3a-84fd-9a38-23ba-001b21168828
    Sub-Cluster UUID: 529ccbe4-81d2-89bc-7a70-a9c69bd23a19
    Sub-Cluster Membership Entry Revision: 3
    Sub-Cluster  Member  UUIDs:  54188e3a-84fd-9a38-23ba-001b21168828,  545ca9af-
ff4b-fc84-dcee-001f29595f9f,   54196e13-7f5f-cba8-5bac-001517a69c72,   5460b129-
4084-7550-46e1-0010185def78
    Sub-Cluster Membership UUID: 9884dc54-4560-3036-0019-001f29595f9f
 [root@cs-ie-h01:~]
```

Note that the local node UUID can be retrieved here. You can also see the Sub-Cluster Member UUIDS, of which there are four.

To get the UUID of an ESXi host that is not part of the Virtual SAN Cluster, the following command may be used:

```
[root@cs-ie-h01:~] esxcli system uuid get
 545ca9af-ff4b-fc84-dcee-001f29595f9f
 [root@cs-ie-h01:~]
```

If a host is identified as not participating in the cluster, the command "`esxcli vsan cluster join`" may be used to add a host back into the cluster. One could also use RVC commands such as “`vsan.cluster_info`” to display the hosts are currently participating in the cluster. Refer to the *Virtual SAN Troubleshooting Manual – Using RVC to verify Virtual SAN functionality section* for further tips on how to troubleshoot this configuration issue.

Re-check the health status after running the "`esxcli vsan cluster join`" command, as there may be other underlying issues that caused the host to leave the cluster in the first place.

A.15 Network Health – All hosts have a VSAN vmknic configured

In order to participate in a Virtual SAN cluster, and form a single partition of fully connected hosts, each ESXi host in a Virtual SAN cluster must have a vmknic (VMkernel NIC or VMkernel adapter) configured for Virtual SAN traffic.

A.15.1 What does this check do?

This check ensures each ESXi host in the Virtual SAN Cluster has a VMkernel NIC configured for Virtual SAN traffic. Note that even if an ESXi is part of the Virtual SAN cluster, but is not contributing storage, it must still have a VMkernel NIC configured for Virtual SAN traffic.

Note that this check just ensures that one vmknic is configured. While multiple vmknics are supported, this test does not check consistent network configurations, i.e. some hosts may have 2 vmknics while others hosts only have 1 vmknic.

A.15.2 What does it mean when it is in an error state?

If this test fails, it means that at least one of the hosts in the cluster does not have a VMkernel NIC configured for Virtual SAN traffic.

A.15.3 How does one troubleshoot and fix the error state?

Ensure that each ESXi host participating in the Virtual SAN cluster has a VMkernel NIC enabled for Virtual SAN traffic. This can be done from the vSphere web client, where each ESXi host's networking configuration can easily be checked, Navigate to Hosts and Clusters -> host -> Manage -> Networking -> VMkernel Adapters and check the Virtual SAN Traffic column and ensure that at least 1 vmknic is "Enabled" for this traffic type.

It can also be checked from the CLI using "`esxcli vsan network list`":

```
[root@cs-ie-h01:~] esxcli vsan network list
Interface
   VmkNic Name: vmk2
   IP Protocol: IPv4
   Interface UUID: 264ed254-5aa5-0647-9cc7-001f29595f9f
   Agent Group Multicast Address: 224.2.3.4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group Multicast Port: 12345
   Multicast TTL: 5
[root@cs-ie-h01:~]
```

In the above output, the VMkernel NIC **vmk2** is used for Virtual SAN traffic.

It can also be checked from the RVC using the "`vsan.cluster_info`" command. This will display which VMkernel adapter, if any, is being used on each host for Virtual SAN traffic.

```
<<truncated>>

 Host: cs-ie-h01.ie.local
   Product: VMware ESXi 6.0.0 build-2391873
   VSAN enabled: yes
   Cluster info:
     Cluster role: agent
     Cluster UUID: 529ccbe4-81d2-89bc-7a70-a9c69bd23a19
     Node UUID: 545ca9af-ff4b-fc84-dcee-001f29595f9f
     Member   UUIDs:   ["5460b129-4084-7550-46e1-0010185def78",   "54196e13-7f5f-cba8-5bac-
001517a69c72",      "54188e3a-84fd-9a38-23ba-001b21168828",      "545ca9af-ff4b-fc84-dcee-
001f29595f9f"] (4)
   Node evacuated: no
   Storage info:
     Auto claim: no
     Checksum enforced: no
     Disk Mappings:
       SSD: HP Serial Attached SCSI Disk (naa.xxx) - 186 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
   FaultDomainInfo:
     Not configured
   NetworkInfo:
     Adapter: vmk2 (172.32.0.1)

 <<truncated>>
```

This provides both the VMkernel NIC used for Virtual SAN Traffic as well as the IP address of the interface.

Refer to the *Virtual SAN Troubleshooting Manual – Networking section* for further tips on how to troubleshoot this configuration issue.

A.16 Network Health – All hosts have matching subnets

In order to participate in a Virtual SAN cluster, and form a single partition of fully connected hosts, each host in a Virtual SAN cluster must be able to talk to every other host in the cluster. The *most common* network configuration is for Virtual SAN hosts to share a single layer-2 non-routable network, i.e. a single IP subnet and single VLAN. However Virtual SAN 6.0 introduces support for layer-3 network, i.e. routed connections, but this is not a very common deployment configuration.

A.16.1 What does this check do?

This check tests that all ESXi hosts in a Virtual SAN cluster have been configured so that all Virtual SAN VMkernel NICs are on the same IP subnet.

A.16.2 What does it mean when it is in an error state?

As mentioned earlier, in Virtual SAN 6.0, VMware introduces support for L3/routing on the Virtual SAN network. In cases where Virtual SAN is deployed over an L3 network, this subnet health check will report an error and may be safely ignored.

If however, the Virtual SAN network is deployed on an L2 network configuration, then this health check will identify ESXi hosts that are not on the same IP subnets. The check will also show an issue when multiple vmknics have been configured but not consistently across the cluster. For example if one host has 2 vmknics, and one host has only 1, then this check will also alert to that.

A.16.3 How does one troubleshoot and fix the error state?

Ensure that all ESXi hosts that share the same L2 Virtual SAN network have matching subnets. This can be done from the vSphere web client, where each host's networking configuration can easily be checked. It can also be checked from the ESXCLI via "`esxcli network ip interface ipv4 get -i vmkX`" where vmkX is the VMkernel adapter.

```
[root@cs-ie-h01:~] esxcli network ip interface ipv4 get -i vmk2
 Name  IPv4 Address  IPv4 Netmask   IPv4 Broadcast  Address Type  DHCP DNS
 ----  ------------  -------------  --------------  ------------  --------
 vmk2  172.32.0.1    255.255.255.0  172.32.0.255    STATIC           false
 [root@cs-ie-h01:~]
```

It may also be checked from RVC via “`vsan.cluster_info`”.

```
<<truncated>>

 Host: cs-ie-h01.ie.local
   Product: VMware ESXi 6.0.0 build-2391873
   VSAN enabled: yes
   Cluster info:
     Cluster role: agent
     Cluster UUID: 529ccbe4-81d2-89bc-7a70-a9c69bd23a19
     Node UUID: 545ca9af-ff4b-fc84-dcee-001f29595f9f
     Member   UUIDs:   ["5460b129-4084-7550-46e1-0010185def78",   "54196e13-7f5f-cba8-5bac-
001517a69c72",      "54188e3a-84fd-9a38-23ba-001b21168828",      "545ca9af-ff4b-fc84-dcee-
001f29595f9f"] (4)
   Node evacuated: no
   Storage info:
     Auto claim: no
     Checksum enforced: no
     Disk Mappings:
       SSD: HP Serial Attached SCSI Disk (naa.xxx) - 186 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
       MD: HP Serial Attached SCSI Disk (naa.xxx) - 136 GB, v2
   FaultDomainInfo:
     Not configured
   NetworkInfo:
     Adapter: vmk2 (172.32.0.1)

 <<truncated>>
```

Refer to the *Virtual SAN Troubleshooting Manual – Networking section* for further tips on how to troubleshoot this configuration issue.

A.17 Network Health – All hosts have matching multicast settings

In order to participate in a Virtual SAN cluster, and form a single partition of fully connected hosts, each host in a Virtual SAN cluster must use the same IP multicast address range.

A.17.1 What does this check do?

It is very rare for users to have to change the IP multicast address range for Virtual SAN. However this might be a necessary step if there are multiple Virtual SAN clusters on the same network. The procedure to change multicast addresses is described in VMware KB Article 2075451.

If an administrator does change the multicast addresses, using esxcli or API, then it is important that they are consistently configured across the cluster. This health check ensures that is the case.

Please note that this health checks doesn't check ports or TTL inconsistencies. It is only checking the multicast IP addresses.

A.17.2 What does it mean when it is in an error state?

It means that the at least one host has a misconfigured multicast addresses. In addition to an error detected by the health check, this type of issue may also result in a partitioned cluster. This will be visible in the health check, but will also be visible in the vSphere web client UI on the Virtual SAN Custer -> Disk Management. In the Group column, different values will be shown for the hosts that are in different network partitions (i.e. isolated).

A.17.3 How does one troubleshoot and fix the error state?

The IP multicast addresses that Virtual SAN uses can be changed and checked from the CLI. The ESXCLI command “`esxcli vsan network list`“ will display the multicast addresses used by each host.

```
[root@cs-ie-h01:~] esxcli vsan network list
 Interface
    VmkNic Name: vmk2
    IP Protocol: IPv4
    Interface UUID: 264ed254-5aa5-0647-9cc7-001f29595f9f
    Agent Group Multicast Address: 224.2.3.4
    Agent Group Multicast Port: 23451
    Master Group Multicast Address: 224.1.2.3
    Master Group Multicast Port: 12345
    Multicast TTL: 5
```

Refer to the *Virtual SAN Troubleshooting Manual – Networking section* for further tips on how to troubleshoot this configuration issue. There is also a section on *Changing multicast settings when multiple Virtual SAN clusters are present* which should be referenced when running multiple Virtual SAN clusters on the same network.

A.18 Network Health – Basic (unicast) connectivity check (normal ping)

While most other network related Virtual SAN health checks assess various aspects of the network configuration, this health check takes a more active approach. As Virtual SAN is not able to check the configuration of the physical network, one way to ensure that IP connectivity exists among all ESXi hosts in the Virtual SAN cluster is to simply ping each ESXi host on the Virtual SAN network from each other ESXi host.

A.18.1 What does this check do?

The "Hosts small ping test (connectivity check)" health check automates the pinging of each ESXi host from each of the other hosts in the Virtual SAN cluster, and ensures that there is connectivity between all the hosts on the Virtual SAN network. In this test all nodes ping all other nodes in the cluster.

A.18.2 What does it mean when it is in an error state?

If the small ping tests fail, it indicates that the network is misconfigured. This could be any number of things, and the issue may lie in the virtual network (vmknic, virtual switch) or the physical network (cable, physical NIC, physical switch). The other network health check results should be examined to narrow down the root cause of the misconfiguration. If all the other health checks indicate a good ESXi side configuration, the issue may reside in the physical network.

This ping test is performed using very small packets, so it ensures basic connectivity. The other health checks are designed to assess MTU misconfiguration and multicast aspects of connectivity.

A.18.3 How does one troubleshoot and fix the error state?

To resolve the networking issue, refer to the *Virtual SAN Troubleshooting Manual – Networking section* for further tips on how to troubleshoot this configuration issue. The manual includes various `ping` tests that may be run to identify the misconfiguration as well as a set of other commands to identify the root cause of the ping test failure. However this test may be used with other health checks to focus the network misconfiguration investigation.

A.19 Network Health – MTU check (ping with large packet size)

This health check complements the basic ping connectivity check. MTUs, the Maximum Transmission Unit size, are increased to improve network performance. Incorrectly configured MTUs will frequently NOT show up as a Virtual SAN network partition, but instead cause performance issues or I/O errors in individual objects. It can also lead to virtual machine deployment failures on Virtual SAN. For stability of Virtual SAN clusters, it is critically important for the large ping test check to succeed.

A.19.1 What does this check do?

While the basic check used small packets, this check uses large packets (9000 bytes). These are often referred to as jumbo frames. Assuming the small ping test succeeds, the large ping test should also succeed when the MTU size is consistently configured across all VMkernel adapters (vmknics), virtual switches and any physical switches.

Note that if the source vmknic has an MTU of 1500, it will fragment the 9000 byte packet, and then those fragments will travel perfectly fine along the network to the other host where they are reassembled. As long as all network devices along the path use a higher or equal MTU, then this test will pass.

A.19.2 What does it mean when it is in an error state?

What will cause a failure is if the vmknic has an MTU of 9000 and then the physical switch enforces an MTU of 1500. This is because then the source doesn't fragment the packet and the physical switch will drop the packet.

If however there is an MTU of 1500 on the vmknic and an MTU 9000 on the physical switch (e.g. because there is also iSCSI running which is using 9000) then there is no issue and the test will pass.

Virtual SAN supports different MTU sizes. It does not care if it is set to 1500 or 9000, as long as it is consistently configured across the cluster.

A.19.3 How does one troubleshoot and fix the error state?

To resolve the networking issue, refer to the *Virtual SAN Troubleshooting Manual – Networking section* for further tips on how to troubleshoot this configuration issue. The manual includes various `ping` tests that may be run to identify the misconfiguration, including how to test with larger packets (`ping –S 9000`) as well as a set of other commands to identify the root cause of the ping test failure. However this test may be used with other health checks to focus the network misconfiguration investigation.

A.20 Network health – multicast assessment based on other checks

This health check is a simple rollup of previous network health checks.

Basically, if Virtual SAN is correctly configured and the ping tests are succeeding but there is a Virtual SAN network partition, this check will report that multicast as the most likely cause of the network partition issue.

Note however that although multicast is the likely cause, it doesn't have to be. Other causes could include performance issues. Problems like excessive dropped packets or excessive pause frames could also lead to this health check failing.

A.20.1 What does this check do?

If this health check reports that multicast may be an issue, a proactive "host debug multicast" check is performed. The "host debug multicast" check only runs if this health check triggers it. This check will add ~10 seconds to the run time of the health check. See section 7.4 for further details on the "host debug multicast" check.

A.20.2 What does it mean when it is in an error state?

That multicast is most like the root cause of a network partition.

A.20.3 How does one troubleshoot and fix the error state?

First, refer the result of the "active multicast connectivity check" health check. This may have further information about the problem.

Refer to the *Virtual SAN Troubleshooting Manual – Networking section* for further tips on how to troubleshoot this configuration issue. There is also section on how to checked for excessive dropped packets and excessive pause frames. There is also a section on *Changing multicast settings when multiple Virtual SAN clusters are present* which should be referenced when running multiple Virtual SAN clusters on the same network.

If you experience difficulty locating the root cause of the network partition, please contact VMware Global Support Services for assistance.

A.21 Network health – Active Multicast connectivity check

If the “Network health – Multicast assessment based on other checks” fails, network multicast may be an issue. At that point, an “active multicast connectivity check” is performed. Otherwise this check is skipped.

A.21.1 What does this check do?

This health check captures multicast packets on all hosts in the cluster for a period of time. It specifically looks for what is known as the "CMMDS Master Heartbeat". All hosts elected to be a "VSAN/CMMDS Master" (one per partition) will send this heartbeat once every second. Such heartbeats are sent over multicast and all hosts in the cluster have to receive them in order for the cluster to function properly. Therefore if a host sends a heartbeat and another host does not hear/receive it, it indicates a multicast misconfiguration, usually in the physical network.

This health check uses the packet captures from all the hosts, and checks which heartbeats were heard by which hosts, and which hosts did not hear a certain heartbeat. The health check then attempts to describe the situation it encountered.

A.21.2 What does it mean when it is in an error state?

The common cases are:

1. Multicast is not working at all. In this case, the check will identify all hosts as individual groups that can’t hear each other. This usually means the physical switch, to the hosts are attached, have multicast disabled.
2. There is a clear split in the network. One group of hosts can talk to each other, and another group can talk to each other, but the two groups cannot talk to each other. This usually is a result of network topologies where the first group is attached to one multicast enabled switch, and the second group is attached to another multicast enabled switch, but the two switches are not configured to allow multicast to flow between them.
3. Multicast connectivity is having issues, but no clear groups are forming. So we have a situation where host A can hear host B's heartbeat, but host B cannot hear host A's heartbeat. This should never happen and indicates a bug in the physical switch. VMware has seen this extremely rarely, but when it was seen an update of the switch firmware and a restart of the switch resolved the issue. Afterwards the issue could no longer be reproduced.

A.21.3 How does one troubleshoot and fix the error state?

VMware recommends engaging with your network administrator if Network health – Active Multicast connectivity check fails. Use the output of the health check to work with your network administrator. The detailed picture (which of the categories it falls into, and the exact groups) will help the network admin figure out where the issue may reside.

A.22 Data Health – Virtual SAN Object Health

The object health checks are designed to provide two pieces of information to the administrator at a glance. It provides a cluster wide overview of objects by summarizing all objects in the cluster, and it also provides categories related to an object's health.

A.22.1 What does this check do?

The object health checks are designed to provide two aspects at a very fast glance.

1. It provides a cluster wide overview by summarizing all objects in the cluster
2. It categories object health to help a user assess not only if an object is healthy or unhealthy, but what it means to the user, whether he should take action, whether he is at risk, etc.

A.22.2 What does it mean when an object is not in a healthy state?

These are the possible states that an object might have when it is not healthy.

Data move: Virtual SAN is building data on the hosts and storage in the cluster either because the administrator requested some form of maintenance mode or evacuation, or because of rebalancing activities. Objects in this state are fully compliant with their policy and "healthy", but Virtual SAN is actively rebuilding them. Administrators should not be worried, as the object is not at risk. However a performance impact can be expected while objects are in this state. Users can cross reference to the resync'ing components view to learn more about active data sync activities.

Healthy: The object is in perfect condition, exactly aligned with its policy, and is not currently being moved or otherwise worked on.

Inaccessible: An object has suffered more failures (permanent or temporary) than it was configured to tolerate, and is currently unavailable and inaccessible. If the failures are not temporary (e.g. host reboot), administrators should work on the underlying root cause (e.g. failed hosts, failed network, removed disks, etc.) as quickly as possible to restore availability, as virtual machines that are using these objects cannot function correctly while in this inaccessible state.

Non-availability related reconfig: Virtual SAN is rebuilding data on the hosts and storage in the cluster because the administrator requested a storage policy change that is unrelated to availability. In other words, such an object is fully in compliance with the *NumberOfFailuresToTolerate* policy and the data movement is to satisfy another policy change, such as *NumberOfDiskStripesPerObject*. The administrator does not need to worry about an object in this state, as it is not at risk.

Reduced availability - active rebuild: The object has suffered a failure, but it was configured to be able to tolerate the failure. I/O continues to flow and the object is accessible. Virtual SAN is actively working on re-protecting the object by rebuilding new components to bring the object back to compliance.

Reduced availability with no rebuild: The object has suffered a failure, but Virtual SAN was able to tolerate it, i.e. IO is flowing and the object is accessible. Virtual SAN is however NOT working on re-protecting the object. This is not due to the delay timer (reduced availability - no rebuild - delay timer) but due to other reasons. This could be because there are not enough resources in the cluster. Or this could be because there weren't enough resources in the past, or there was a failure to re-protect in the past and Virtual SAN has yet to retry. Refer to the limits health check for a first assessment if any resources may be exhausted. Users should resolve the failure or add resources as quickly as possible in order to get back to being fully protected against a subsequent failure.

Reduced availability with no rebuild - delay timer: The object has suffered a failure, but Virtual SAN was able to tolerate it. I/O is flowing and the object is accessible. Virtual SAN is however NOT yet working on re-protecting the object, as it is waiting for the 60-minute (default) delay timer to expire before issuing the re-protect.

The `vsan.clomrepairdelay` setting specifies the amount of time Virtual SAN waits before rebuilding a disk object. By default, the repair delay value is set to 60 minutes; this means that in the event of a failure that renders components ABSENT, Virtual SAN waits 60 minutes before rebuilding any disk objects. This is because Virtual SAN is not certain if the failure is transient or permanent.

Administrators can choose to issue an explicit request to skip the delay timer and start re-protect immediately, if it is known that the failed entity won't be recovered within the delay period.

If however the administrator knows that the failed host is actively rebooting, or knows that he pulled the wrong drive and it is being reinserted, then it is advisable to just wait for those tasks to finish, as that will be the quickest way to fully re-protect the object.

Non-availability related incompliance: This is a catch all state when none of the other states apply. An object with this state is not compliant with its policy, but is meeting the availability (*NumberOfFailuresToTolerate*) policy.

Here is an example of how one might end up with non-availability related incompliance. Consider a Virtual SAN cluster with 3 hosts, where each host has 1 x SSD for cache and 3 x magnetic disks for capacity. Each host is placed in a different fault domain. The default storage policy has *NumberOfFailuresToTolerate*=1, *NumberOfDiskStripesPerObject* =4, and *ForceProvisioning*=True.

If a VM is now created, and considering that every fault domain has less than 4 disks, the stripe width requirement cannot be honored.

But since *ForceProvisioning* is set to True, the StripeWidth=1 object is created successfully. This object will have the state "non-availability-related-incompliance

A.22.3 How does one troubleshoot and fix the error state?

By reviewing the object state from the above list, an administrator will know what activities are occurring on the Virtual SAN cluster from an object perspective, and whether any corrective actions should be taken.

The Health check provides a “Repair Objects Immediately” button as part of this health check. Note that this is an asynchronous task, and even though the task completes, it does not mean that VSAN has carried out the repair action. The “Repair Objects Immediately” button simply places the objects into re-protecting queue, and a repair attempt is tried some time later.

If objects are still not fixed after the “Repair Objects Immediately” task completes, please contact VMware Global Support Services if there is any concern with the object states, or the objects are in an unexpected state.

A.23 Limits Health – Current cluster situation

This particular health check looks at free disk capacity and ensures that the “components per host” limit has not been exceeded, and that there is some flash read cache capacity remaining (note that flash read cache is only relevant to hybrid configurations and is not relevant on all-flash configurations). The components per host limit should not be too much of a concern in 6.0 since the limit has been raised to 9,000 components per host.

A.23.1 What does this check do?

VMware’s best practice recommendations on disk capacity are to maintain a slack space of 30% in order to avoid excessive rebalance operations.

Note also that this way of looking at the resources has some limitations. For example, if there are 3 hosts in a Virtual SAN cluster, and 2 hosts are filled to capacity while one is empty, the cluster summaries may look like there are plenty of free resources across all 3 hosts. However VM provisioning may fail, as Virtual SAN will require capacity on at least 2 hosts for the 2 replicas that it needs to create.

A.23.2 What does it mean when it is in an error state?

If this check has a warning or error, it may means that the number of components has reached its host limit, or that there is no free storage capacity, or that the flash read cache reservations have been exhausted. If components limits have been reach, or there is no free capacity, an administrator will not be able to deploy new virtual machines, nor will rebuild operations be allowed. If flash reads cache is exhausted, it means that there is very little read cache available for those virtual machines that do not have reservations. This will impact the performance of these virtual machines.

The following table displays the thresholds at which warnings and errors are displayed in this health check.

Resource	Green(OK)	Yellow(Warning)	Red(Danger)
Components	< 80%	80% - 90%	> 90%
Free disk space	< 80%	80% - 90%	> 90%
RC reservation	< 70%	70% - 90%	> 90%

A.23.3 How does one troubleshoot and fix the error state?

To troubleshoot this issue, there may be a need to add additional resources in the cluster. An administrator will be able to see where resources are required through the health check UI.

Alternatively, an administrator may have to free up some already consumed capacity. To see where the resource issue lies, there are a number of very useful RVC commands such as "`vsan.check_limits`" and "`vsan.disks_stats`". Refer to the *Virtual SAN Troubleshooting Manual – Storage section* for further tips on how to troubleshoot and monitor the Virtual SAN limits discussed here.

Please note that in Virtual SAN 6.0, there is a new Proactive Rebalance mechanism that can be enabled to proactively rebalance cluster components. Refer to the *Virtual SAN Administrators Guide* for more information on this feature.

A.24 Limits Health – After 1 additional host failure

In addition to the basic limit health check, there is also a simulation of how resources would look like after an ESXi host failure has occurred. If a single host were to fail, two things will happen. First, the resources on that ESXi host (such as cache and capacity) are no longer available. Second, Virtual SAN will attempt to re-protect (rebuild) all components belonging to objects that are now currently running with reduced redundancy due to the failure.

A.24.1 What does this check do?

This health check simulates both actions described above. If the host with the most resources consumed were to fail, this health check calculates how much resources would be used from the remaining hosts in the cluster, and how much resources would still be available.

Note that if there is already a failure in the cluster, this test will report on one additional failure. Therefore this test reports on the results of the current failure and the additional failure that it introduces.

A.24.2 What does it mean when it is in an error state?

If this check reports that after a host failure, more than 100% of resources will be used, it means that re-protection will fail for some objects because there are not enough resources available. Note that this health check simulation is very simple. It only looks at cluster aggregate resources, so just like the basic limits check, it won't consider the distribution and placement rules.

However, this simple simulation will verify that, after a failure, a Virtual SAN cluster has been configured with enough resources to operate in an operationally safe manner after a re-protection. Note however that this test does not check for balance and fault domains, so this needs to be considered independently of this test.

For example, a user may enforce an operational business policy to have no less than 25% free disk space under normal conditions and no less than 15% free disk space after one failure. This check can be used to implement such a policy and to verify that this is indeed the case.

A.24.3 How does one troubleshoot and fix the error state?

There is no troubleshooting involved in this health check. It is primarily for information only. If this health check fails, customers may wish to add additional resources to the cluster to facilitate a successful rebuild after a failure. If you feel that there should be enough capacity in the cluster to rebuild after a failure, check to see if any of the components (e.g. disk drives) are in a failed state.

A.25 Physical Disk Health – Overall disks health

This is the main test in the physical Virtual SAN disks category. It assesses many aspects of what Virtual SAN believes the health of the disk is.

A.25.1 What does this check do?

This check includes an end-to-end assessment of the physical disk drives. It will check for drive surface issues, controller issues, driver issues, ESXi storage device stack issues, and issues with the Virtual SAN disk layer. As such, the overall health of a physical disk is computed by assessing multiple sub-health status.

This health check will show an error if any of the following tests fail: Metadata health, Congestion, Software state or Disk capacity.

A.25.2 What does it mean when it is in an error state?

One would need to examine the information displayed as part of the health check. Is the issue an operational one, for example is the disk offline? Is it a problem with trying to read the metadata of the drive? This implies that the drive is offline and unavailable for use. Is it a congestion issue, which could have a serious impact on the performance of the Virtual SAN cluster? Perhaps it is the Virtual SAN software state that is the root cause, which in all likelihood will impact all of the disks on this host? Or is it a capacity issue, where too much space on the physical disk has been consumed? Each of these individual checks would need to be considered to determine the corrective course of action. Some of the checks imply that the drive is offline, others imply that the drive is still online, but some corrective action might be needed.

A.26 Physical Disk Health – Metadata health

A.26.1 What does this check do?

This check verifies that the metadata of the disk can be read.

A.26.2 What does it mean when it is in an error state?

If this health status is not green/OK, Virtual SAN has encountered an issue reading the metadata of the disk, and is hence not able to use this disk. The disk may have suffered a physical drive failure.

This check could also fail due to a software problem.

When this health check fails, it means the disk is not usable, which means any data stored on the physical disk is currently unavailable. This will also impact capacity of the Virtual SAN datastore.

A.26.3 How does one troubleshoot and fix the error state?

The physical drive failure will need to be addressed. Procedures for replacing failed components, including disk drives, are documented in the Virtual SAN Administrators Guide.

If there is no failed drive, or there is difficulty identifying a failure drive, a support request should be opened with VMware Global Support Services.

A.27 Physical Disk Health – Disk Capacity

This health check is only applicable to capacity tier drives. It does not apply to the cache devices.

A.27.1 What does this check do?

This check reports on the physical capacity of the drives on the Virtual SAN cluster and reports warnings and/or errors if consumed storage capacity is becoming an issue.

A.27.2 What does it mean when it is in an error state?

If this health status not green/OK, it indicates that this disk is low on free disk space. If free disk space on a physical disk is below 80% usage, a state if green (OK) health is displayed. If usage is between 80% and 95%, health will be shown as yellow (warning) and if physical disk usage is above 95% usage, a red (alert) health is displayed.

A.27.3 How does one troubleshoot and fix the error state?

First step is to ensure that all the storage is valid and that there are no missing capacity devices. If a capacity device fails, it will most likely entail a rebuild of components on the remaining disks in the cluster, possibly pushing disk usage above 80% on some devices. Disk status can be checked via the UI. Ensure that the Virtual SAN datastore capacity is what you expect it to be.

Virtual SAN attempts to balance the space usage of disks when they reach 80%. If one disk has reached 80%, Virtual SAN will automatically remediate the situation. If all physical disks are using greater than 80% of their capacity, Virtual SAN still tries to keep the amount of consumed capacity balanced. At this point, administrators should consider introducing additional capacity to the cluster. VMware recommends a slack space of somewhere in the region of 30%.

Rebalancing activity can be monitored via the UI in version 6.0, and can also be monitored via the Ruby vSphere Console (RVC) using the `vsan.resync_dashboard` command. There is no way to monitor this activity via the UI in version 5.5; an administrator must use the RVC command.

If one physical disk is consistently showing close to full, while other disks are not, this could indicate an issue with the Virtual SAN balancing system. At this point, VMware Global Support Services should be engaged to figure out why balancing is not occurring automatically.

Once a physical disk gets close to being full, virtual machines that use this disk and that are thin provisioned (Object space reservation < 100%) and which need additional space to service I/O, will be stunned. In this case, a question will be posted to the administrator of the virtual machine. The user has the choice to either cancel or to retry the I/O. If some disk space has become available in the meantime, a retry will resume the VM and I/O will succeed.

This behaviour is not unique to Virtual SAN. This is the same behaviour on traditional VMFS and NFS datastores when they become full.

A.28 Physical Disk Health – Software state health

A.28.1 What does this check do?

This check ensures that Virtual SAN can utilize the physical disks in the cluster.

A.28.2 What does it mean when it is in an error state?

If this health status is not green/OK, Virtual SAN has encountered a problem preventing it from using the disk.

A.28.3 How does one troubleshoot and fix the error state?

If no other health check is showing an error, the issue might lie with the Virtual SAN software. The "In CMMDS/VSI" field should be examined for additional information. One known cause for this is a system with very low amounts of available memory.

One known cause for this is a system with very low amounts of available memory. VMware KB article 1002604 provides information on how to check memory usage of an ESXi host. If memory consumption is high, you may need additional memory resources.

For all other possible causes of this issue, VMware Global Support Services should be contacted.

A.29 Physical Disk Health – Congestion

Congestion in Virtual SAN happens when the lower layers fail to keep up with the I/O rate of higher layers. If this health status not green/OK, Virtual SAN is still using the disk, but it is in a state of (possibly severely) reduced performance, manifesting in low throughput/IOPS and high latencies for Virtual SAN objects using this disk group. Congestion in these cases will be applicable to all objects on the disk group.

A.29.1 What does this check do?

This check is to make sure that congestion is not unduly impacting the performance of the Virtual SAN Cluster.

A.29.2 What does it mean when it is in an error state?

Typical reasons for congestion are bad or badly sized hardware, misbehaving controller firmware, bad controller drivers, a low queue depth on the controller, or some problems in the software. For example, if the flash cache device is not sized correctly, virtual machines performing a lot of write operations could fill up of write buffers on the flash cache device. These buffers have to be destaged to magnetic disks in hybrid configurations. To facilitate the destaging operations that now occur very frequently, congestion might be used to slow down the writes from the virtual machine.

One common scenario is a high read cache miss rate, which can also lead to congestion to slow down virtual machine read I/O.

High congestion could be the root cause of virtual machine storage performance degradation, operation failures, or even ESXi hosts going unresponsive.

A.29.3 How does one troubleshoot and fix the error state?

Under high load, when Virtual SAN is operating at its maximum performance, a low amount of "congestion" (typically under a value of 32) is expected and is not a cause of concern. However, any value of congestion above 0 combined with low throughput/IOPS is an indication of an issue. This health check will be green (OK) for congestion values below 32, yellow (warning) for values between 32 and 64, and red (alert) for values above 64. The maximum value for congestion is 255.

The "Congestion info" field for the value, and area that is causing the congestion. It is recommended to engage VMware Global Support Services on congestion related issues to ensure identification of the root cause.

A.30 Physical Disk Health – component metadata health

Each object deployed in Virtual SAN is made up of one or more components. Each component has associated metadata. For details related to objects and components, refer to the Virtual SAN Troubleshooting Reference Manual.

A.30.1 What does this check do?

This health check checks the integrity of the component metadata on a disk.

A.30.2 What does it mean when it is in an error state?

If this health status from this check is not green/OK, Virtual SAN has encountered an issue with an individual component.

This error does not mean that Virtual SAN will decommission the disk on which the component resides. But in rare cases where bad metadata is detected, it could lead to additional issues with the object (that the component is a part of).

A.30.3 How does one troubleshoot and fix the error state?

This issue could be due to faulty drives, faulty controller or a misbehaving device driver, but could also originate from a problem in the Virtual SAN software. Refer to the *Virtual SAN Troubleshooting Manual – Storage section* for further tips on how to troubleshoot and monitor the Virtual SAN objects and components discussed here.

The best course of action if this test fails is to engage VMware Global Support Services.

A.31 Physical Disk Health – memory pools (heaps)

Physical disks have a requirement on adequate memory pools for heaps when used with Virtual SAN.

A.31.1 What does this check do?

This health check is responsible for checking the memory pools used by Virtual SAN, and reports if they are running low. Physical disks have a requirement on adequate memory when used with Virtual SAN.

A.31.2 What does it mean when it is in an error state?

If this health check is not green, it indicates that Virtual SAN is running low on a vital memory pools needed for the operation of the physical disks.

When under load, Virtual SAN will use congestion as a means to throttle down the incoming I/O rate in order to relieve pressure on memory pools and keep them at safe levels. Because of this safeguard, memory pool depletion should not happen.

It is highly likely that the physical disk will also report a "congestion health" error.

This can lead to a variety of performance issues such as virtual machine storage performance degradation, operation failures, or even ESXi hosts going unresponsive.

If there is a really high load running on Virtual SAN, for example, a very high amount of concurrent read cache misses, this can lead to memory pool pressures.

Note that this health check is not OK, it will typically not be as a result of any issue with the hardware or software but simply the result of a genuine high load running on Virtual SAN.

A.31.3 How does one troubleshoot and fix the error state?

If this health check fails, please contact VMware Global Support Services.

A.32 Physical Disk Health – memory pools slabs

This is very similar to the previous health check, but it is looking at different memory pools. This test is looking at *slabs* rather than *heaps*.

A.32.1 What does this check do?

This health check is responsible for checking the memory pools used by Virtual SAN, and reports if they are running low. Physical disks have a requirement on adequate memory when used with Virtual SAN.

A.32.2 What does it mean when it is in an error state?

If this health check is not green, it indicates that Virtual SAN is running low on a vital memory pools needed for the operation of the physical disks.

When under load, Virtual SAN will use congestion as a means to throttle down the incoming I/O rate in order to relieve pressure on memory pools and keep them at safe levels. Because of this safeguard, memory pool depletion should not happen.

It is highly likely that the physical disk will also report a "congestion health" error.

This can lead to a variety of performance issues such as virtual machine storage performance degradation, operation failures, or even ESXi hosts going unresponsive.

If there is a really high load running on Virtual SAN, for example, a very high amount of concurrent read cache misses, this can lead to memory pool pressures.

Note that this health check is not OK, it will typically not be as a result of any issue with the hardware or software but simply the result of a genuine high load running on Virtual SAN.

A.32.3 How does one troubleshoot and fix the error state?

Once again, if this health check fails, please contact VMware Global Support Services.

A.33 Physical Disk Health – Physical Disk Health Retrieval Issues

This is very similar to the health check described in a previous check – host retrieval issues when trying to verify that the host is compliant with the HCL. This health check also only appears if there are issues communicating to one or more hosts in the cluster.

A.33.1 What does this check do?

It is informing the administrator that it cannot get physical disk related information from the ESXi host in question in order to perform a check on the health of the physical disks.

A.33.2 What does it mean when it is in an error state?

In all likelihood, there is a host disconnected from vCenter. This health check error probably accompanied with a Network Health issue, such as "Host disconnected from vCenter.

A.33.3 How does one troubleshoot and fix the error state?

Administrators should address the host disconnect issue, and allow the health check plugin to communicate successfully with all hosts in the cluster. Check also the recommendations made in section 6.13.3 on how to deal with disconnected hosts.

A34. Stretched Cluster Health – Cluster with multiple unicast agents

In a stretched cluster, each of the hosts in the data sites runs a unicast agent for communication to the witness sites. Since there is only be one witness host, there should only be a single unicast agent in the cluster.

A.34.1 What does this check do?

This check verifies that there is only a single unicast agent configured in the VSAN stretched cluster, and that the unicast address on all data hosts is pointing to the witness host.

A.34.2 What does it mean when it is in an error state?

It means that there is a misconfiguration in the VSAN stretched cluster, in so far as that there appears to be hosts with different unicast agents configured.

A.34.3 How does one troubleshoot and fix the error state?

Identify the running unicast configuration on each of the data hosts and determine which one is correct and which one(s) are not correct. The CLI command *esxcli vsan cluster unicastagent* can be run on an ESXi hosts to remove and re-add a unicast configuration from an ESXi host. The unicast agent on the ESXi data hosts should be configured with the IP address and port of the witness host. Configure all hosts in each data site with the same IP address and port for the unicast agent. All hosts in a stretched cluster must have a consistent configuration.

A35. Stretched Cluster Health – Fault domain number check

In a VSAN stretched cluster, there should be a total of 3 fault domains; data site1, data site 2 and the witness site. The presence of additional fault domains could mean that a virtual machine is not deployed optimally across data sites.

A.35.1 What does this check do?

This check verifies that there are no extra default domains configured in the cluster.

A.35.2 What does it mean when it is in an error state?

If this check fails, it implies that there are additional fault domains detected in the cluster.

A.35.3 How does one troubleshoot and fix the error state?

Administrators need to revisit the VSAN Stretched cluster configuration and ensure that there are only 3 default domains configured on the host:

- Preferred
- Secondary
- External witness host for VSAN Stretched Cluster

No other fault domains should exist in a VSAN stretched cluster configuration. The witness host must not be in the same fault domain as the data hosts. The `esxcli vsan faultdomain` command can be used to view fault domains, although the recommendation is that the vSphere Web Client UI is used for fault domain, and stretched cluster configuration.

A36. Stretched Cluster Health – Host without configured unicast agent

As mentioned in a previous check, all data hosts run a unicast agent to communicate to the witness host. The unicast agent enables the data host to communicate with the witness host in the stretched cluster.

A.36.1 What does this check do?

This check ensures that all hosts on the data sites have a running unicast agent to communicate with the witness host.

A.36.2 What does it mean when it is in an error state?

If this check fails, it means that there is a problem with the unicast agent on the host or hosts in question. Details about the erred hosts will be displayed in the health check UI.

A.36.3 How does one troubleshoot and fix the error state?

This issue could be due to a number of reasons. The CLI command *esxcli vsan cluster unicastagent list* should be run on the host in question. When functioning normally it should return the IP Address of the witness host and the port used for communication, e.g.

```
[root@esx:~] esxcli vsan cluster unicastagent list
 IP Address   Port
 ----------  -----
 172.3.0.15  12321
```

If the command fails, examine the vmkernel.log file on the host in question to see if the root cause can be identified. If not, consider opening a service request with VMware Global Support Services (GSS). Note that this command does not run on the witness host. If the command is run on the witness host, it is expected to fail as follows:

```
[root@esx:~] esxcli vsan cluster unicastagent list
Unable to list unicast agent: Failed to get unicast agent: Sysinfo
error on operation returned status : Not supported. Please see the
VMkernel log for detailed error information
```

Note however that the witness host uses the first available Virtual SAN network interface to listen for unicast IP traffic. For simplicity, use only a single VSAN network interface on the witness host.

A37. Stretched Cluster Health – Some hosts do not support stretched cluster

ESXi hosts need to be running vSphere 6.0u1 in order to support VSAN Stretched Cluster. Previous versions of ESXi do not support this functionality.

A.37.1 What does this check do?

This check ensures that the ESXi hosts that are part of the VSAN stretched cluster are running vSphere 6.0U1 minimum. This version was released in September 2015. The Virtual SAN stretched cluster is a new feature introduced in vSphere 6.0 Update 1. An ESXi host running an earlier version does not form a stretched cluster properly.

A.37.2 What does it mean when it is in an error state?

If this check fails, it means that there is a host running an earlier version of ESXi than 6.0U1 in the VSAN stretched cluster. This is unsupported

A.37.3 How does one troubleshoot and fix the error state?

Ensure that all hosts that are in the VSAN stretched cluster are running ESXi 6.0u1 minimum.

A38. Stretched Cluster Health – Stretched cluster with no disk mapping witness host

Although a witness host does not store virtual machine data components, it must still store witness components. For this reason, it must have a disk group, which is created during the stretched cluster setup.

A.38.1 What does this check do?

This check verifies that the disk group belonging to the witness host is intact and is functioning.

A.38.2 What does it mean when it is in an error state?

If this check fails, it implies that there is an issue with the disk group on the witness host.

A.38.3 How does one troubleshoot and fix the error state?

The disk group on the witness hosts should be examined for issues, and if an issue is found, it should be addressed. If for some reason there is no disk group, a disk group should be created on the witness host. This can be done via the vSphere web client UI or the CLI.

If the witness host does not have any disk claimed, the fault domain for the witness host is not available and Virtual SAN cannot provision any objects with *Number of Failures To Tolerate* set to one (FTT = 1).

A39. Stretched Cluster Health – Stretched cluster without a witness host

A stretched cluster requires a witness host. The witness host is used to host virtual machine witness components to allow virtual machines to remain active in the event of a failure.

A.39.1 What does this check do?

This check verifies that a witness host is present and can be reached over the network.

A.39.2 What does it mean when it is in an error state?

If this check fails, then there is an issue communicating with the witness host. It could mean that there is a failure on the witness host, and that it has gone down for maintenance (reboot).

A.39.3 How does one troubleshoot and fix the error state?

One would need to check the state of the witness host and its network connectivity. Initially check the state of the witness host via the vSphere web client UI. Additionally connecting to the host using SSH and verifying that it is operational could be tried. If there are issues with connecting to the host, you may need to connect to the console of the host and verify functionality from there.

If the witness host has a fatal error, and cannot be brought back online, a new witness host can be created and added to the stretched cluster.

A40. Stretched Cluster Health – Witness host inside one of the fault domains

A witness host should be in it's own fault domain. It should not be in a fault domain with any data hosts. It should be a standalone host outside of the VSAN cluster and in its own fault domain.

A.40.1 What does this check do?

This check verifies that the witness host is not in the same fault domain as any of the data hosts.

A.40.2 What does it mean when it is in an error state?

The witness host resides in the same fault domain as the data host(s). It could mean that the witness host is also behaving as a data node in the VSAN stretched cluster.

A.40.3 How does one troubleshoot and fix the error state?

The witness host should be moved out of the fault domain that it currently reside in with data hosts. A fault domain in a stretched cluster should never contain both a witness host and a data node. To move a witness out of a fault domain:

1. In the vSphere Web Client UI, click Manage > Settings.
2. Under Virtual SAN, click Fault Domains.
3. Select the witness host, and click the Move hosts into or out of fault domain icon.

A41. Stretched Cluster Health – Witness host part of the cluster

The witness host should not be in the VSAN Cluster inventory in vCenter. The witness host needs to remain outside of the cluster.

A.41.1 What does this check do?

This check ensure that the witness host is outside of the VSAN cluster, and that only data hosts are inside of the cluster object in vCenter.

A.41.2 What does it mean when it is in an error state?

It means that the witness host has been inadvertently moved into the VSAN cluster. It needs to be moved back out of the cluster.

A.41.3 How does one troubleshoot and fix the error state?

Place the witness host into maintenance mode. Choose the option "No data migration" when doing this operation. Note this will temporarily cause some additional health check failures. When the witness host is in maintenance mode, it can be moved out of the VSAN cluster. When it has been successfully moved out of the VSAN cluster, maintenance mode can be exited. Users will now need to reconfigure the VSAN stretched cluster via vSphere Web Client.

A42. Stretched Cluster Health – Witness host with invalid preferred fault domain

When a split-brain occurs in a VSAN stretched cluster, most likely due to the inter-site network link failing, the preferred data site and the witness form a cluster so that there are a majority of virtual machine components available on the preferred sites. This allows virtual machines to remain accessible.

A.42.1 What does this check do?

This check ensures that the preferred fault domain configured for the witness host is valid.

A.42.2 What does it mean when it is in an error state?

If there is a configuration change or failure in the cluster, and the preferred domain no longer exists in the current configuration, then this check will report an error.

A.42.3 How does one troubleshoot and fix the error state?

There are two options to address this issue. The first is to remedy the cluster failure or configuration issue. The alternative is to setup the stretched cluster once more, selecting the preferred default domain in the process.

One can also run the `esxcli vsan cluster preferredfaultdomain` command to view and set the preferred fault domain. You can run the command on any host to view the preferred fault domain. To set the preferred fault domain, you must run the command on the witness host.

A43. Stretched Cluster Health – Witness host with non-existing fault domain

When a witness host is added to the stretch cluster, it is given the name of the preferred default domain. When a split-brain occurs in a VSAN stretched cluster, most likely due to the inter-site network link failing, the preferred data site and the witness form a cluster so that there are a majority of virtual machine components available on the preferred sites. This allows virtual machines to remain accessible.

A.43.1 What does this check do?

This check verifies that the default domain that is associated with the witness host does indeed exist.

A.43.2 What does it mean when it is in an error state?

If this check fails, it means that the witness host was associated with a non-existing default domain. Most likely, this will be as a result of the witness being added to the cluster through the use of ESXCLI, e.g.

# esxcli vsan cluster join -u <id> -t -p="Preferred"

The –p option specifies the fault domain that the witness node prefers to respond in case of network partition. It should be either of the two fault domains for existing data sites.

If this option was mistyped, then it is possible to have an invalid preferred fault domain associated with the witness.

A.43.3 How does one troubleshoot and fix the error state?

Try removing the witness from the VSAN cluster and add it back again, ensuring that the preferred default domain is spelt correctly. The option is case sensitive.

One can also run the `esxcli vsan cluster preferredfaultdomain` command to view and set the preferred fault domain. You can run the command on any host to view the preferred fault domain. To set the preferred fault domain, you must run the command on the witness host.

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