TECHNICAL WHITE PAPER: February 2024

# VMware vSAN™ Features

Proof of Concept (PoC) Guide

# Table of contents

Introduction	
vSAN Space Efficiency Features	5
Overview	5
Compression Only	5
Deduplication and Compression	6
Testing Compression	8
ESA Cluster	9
OSA Cluster – Compression only	11
OSA Cluster – Deduplication and Compression	13
RAID-5/RAID-6 Erasure Coding	13
Trim/Unmap	25
vSAN Max™ - Disaggregated Storage	
vSAN Max Sizing Considerations	31
Disaggregated Storage for vSAN OSA (AKA: HCI Mesh)	31
Using Quickstart to Enable vSAN Max Cluster	32
Manually Enabling vSAN Max on a Cluster	37
Enabling vSAN Max/HCI Mesh Services on a VMware Cloud Foundation™ based Cluster	37
Encryption in vSAN	
vSAN Data-at-Rest Encryption	38
vSAN Data-in-Transit Encryption	50
vSAN File Services (vSAN ESA and OSA)	
Cloud Native Use Cases	57
Considerations	57
Pre-Requisites	57
Enabling File Services - vSAN ESA and OSA	58
Creating a File Share	64
Mounting a File Share	66
Quotas and Health Events	67
Failure Scenarios	69
File Services Snapshots	71
File Services Support for Stretched Clusters and Two Node Topologies	71

vSA	N Support for Kubernetes	72
API	PENDIX A: Creating Test VMs	73
	Requirements:	73
	Download govc:	73
	Connecting to vCenter	73
	Configure Test VM	74
	Import OVA to vCenter and Clone	76
API	PENDIX B: Cleanly Removing vSAN Configuration	. 78
	vCLS Retreat Mode	78
	Remove vSAN Partitions and Clear Data	78

# Introduction

The vSAN Features guide represents one of a series of vSAN Proof of Concept Guides covering a variety of vSAN related topics. The other guides being:

- vSAN Proof of Concept: vSAN Architecture Overview & Setup
- vSAN Proof of Concept: vSAN Management, Monitoring & Hardware Testing
- vSAN Proof of Concept: vSAN Performances Testing
- vSAN Proof of Concept: vSAN Stretched Cluster & Two-Node Overview & Testing

This guide is designed to stand largely separate from the other documents. That said, the assumption is that the reader has working knowledge of vSAN cluster creation and Storage Policy Management. Especially since the steps documented herein often assume a vSAN Cluster already exists in your test environment. If you require a refresher, please review the vSAN Proof of Concept: vSAN Architecture Overview & Setup guide

The particular focus of this guide is discussion and walkthrough of specific vSAN features such as:

- Space efficiency features (e.g., compression, deduplication, RAID-5/RAID-6 erasure coding, and Trim/Unmap)
- Encryption
- File Services

This document primarily focuses on vSAN Express Storage Architecture™ (ESA) cluster environments. vSAN Original Storage Architecture™ (OSA) environments are covered where they differ from vSAN ESA.

# vSAN Space Efficiency Features

#### Overview

Space efficiency technologies in enterprise storage play an important role improving value and decreasing costs. VMware vSAN has several technologies in place to help improve storage efficiency.

Space efficiency techniques can be categorized into the following:

- Opportunistic
  - These space efficiency techniques are dependent on conditions of the data, and not guaranteed to return a predetermined level of savings
  - vSAN offers several types of opportunistic space efficiency features such as Deduplication & Compression (in vSAN OSA), Compression-only, TRIM/UNMAP space reclamation, and thin provisioning
- Deterministic
  - These space efficiency techniques can be relied upon to deliver a guaranteed level of capacity savings
  - vSAN offers deterministic space efficiency capabilities through data placement schemes that are optimized for storing data in a resilient but efficient manner, including RAID-5/6 erasure coding

In vSAN, opportunistic and deterministic space efficiency features can be used independently or together.

For a deeper discussion vSAN space efficiency please refer to:

https://core.vmware.com/resource/vsan-space-efficiency-technologies

# **Compression Only**

#### vSAN ESA Compression

With vSAN ESA, **compression is defined at a storage policy level**, and is **enabled by default**. The compression mechanisms in vSAN ESA evaluate and compress data differently than in vSAN OSA. In vSAN ESA, each incoming 4KB block is evaluated on a 512 Byte sector size (vSAN OSA, uses larger 2KB sector sizing). The 512 Byte size equates to 8 sectors per 4KB block (8\*512 Bytes = 4096 Bytes or 4KB). This allows the 4KB block to reduce in increments of 512 bytes. Depending on how compressible the 4KB block, one can realize up to an 8:1 compression ratio. For example, a 4KB block could be compressed down to 7/8ths its original size is if it is not very compressible, or all the way down to 1/8th its original size, if it is h highly compressible. Ultimately, compressible data in vSAN ESA storage can be compressed at finer levels of granularity.

To *disable* compression on an vSAN ESA cluster, navigate to Home > Policies and Profiles > VM Storage Policies and create or amend an existing policy.

Under the storage rules > space efficiency setting, select 'no space efficiency':

Create VM Storage Policy	vSAN	×
1 Name and description	Availability Storage rules	Advanced Policy Rules Tags
2 Policy structure 3 vSAN	Encryption services (j)	<ul> <li>Data-At-Rest encryption</li> <li>No encryption</li> <li>No preference</li> </ul>
<ul><li>4 Storage compatibility</li><li>5 Review and finish</li></ul>	Space efficiency (i)	<ul> <li>Deduplication and compression</li> <li>Compression only</li> <li>No space efficiency</li> <li>No preference</li> </ul>
	Storage tier (j)	<ul> <li>All flash</li> <li>Hybrid</li> <li>No preference</li> </ul>
		CANCEL BACK NEXT

Note: This will update new writes only on the vSAN ESA cluster. Existing data will not be affected.

#### vSAN OSA Compression

vSAN OSA supports "Compression Only". Compression is applied directly at the cluster-level and implemented per disk group. The compression algorithm will take a 4K block and try to compress it to 2KB or less (2:1). If this is successful, the compressed block is then written to the capacity tier. If the compression algorithm cannot compress the block by this amount, the full 4KB will be written to the capacity tier. More information on enabling compression in vSAN OSA clusters is in the <u>vSAN</u> <u>OSA cluster deduplication and compression</u> section of this guide.

# Deduplication and Compression

#### vSAN ESA Cluster

vSAN ESA does not support deduplication as of the publication of this guide. That said, vSAN ESA supports a variety of space efficiency features:

- Up to 8:1 compression ratio
- Improvements to RAID-5/RAID-6 erasure coding
- Default trim/unmap support

Depending on the overall vSAN ESA design, actual space efficiency may, in fact, exceed a comparable vSAN OSA cluster leveraging deduplication.

#### vSAN OSA Cluster

In addition to just compressing the data, further savings may be achieved with deduplication in vSAN OSA. When data is destaged from the cache to capacity tier, vSAN will check to see if a match for that block exists. If true, vSAN does not write an additional copy of the block, and metadata is updated. However, if the block does not exist, vSAN will attempt to compress the block.

To demonstrate the effects of Deduplication and Compression, this exercise shows the capacity after deploying a set of identical VMs. Before starting this exercise, ensure that the Deduplication and Compression service is enabled on the cluster. When enabling the Deduplication and Compression service, vSAN will go through a rolling update process: vSAN will evacuate data from each disk group in turn and the disk group will be reconfigured with the features enabled. Depending on the number of disk groups on each host and the amount of data, this can be a lengthy process.

Note: Administrators have the option of enabling "Compression Only" or "Deduplication and compression" simultaneously. In this example we will select the "Deduplication and compression" option.

To enable Deduplication and Compression complete the following steps:

Navigate to [vSAN Cluster] > Configure > vSAN > Services > Data Services, then click the EDIT button that corresponds to the Data Services:

Toggle 'Compression only' or 'Deduplication and Compression' and select APPLY:

VSAN Services VSAN OSA Cluster	$\times$
Space efficiency (i)	
○ None	
O Compression only	
<ul> <li>Deduplication and compression</li> </ul>	
Encryption	
Data-At-Rest encryption (i)	
Wipe residual data (i)	
Key provider 🗸	
Data-In-Transit encryption (1)	
Rekey interval Default 🗸 1 day 🗸	
Predefined intervals	
<ul> <li>These settings require all disks to be reformatted. Moving large amount of stored data might be slow and temporarily decrease the performance of the cluster.</li> <li>Disk format change could fail if there are VMs with incompatible storage policy.</li> </ul>	
Disk format options	
Allow reduced redundancy (i)	
CANCEL	PLY

# **Testing Compression**

Compression rates, and the associated space savings) are very much dependent on the stored data. Further, data change rates mean that compression ratios are dynamic for a given system. This makes testing compression particularly challenging.

However, we can make reasonable attempts at a repeatable test, given a static, freely available dataset. One such dataset is from the human genome project, hosted by Ensembl (https://www.ensembl.org).

The top-level human genome data consists of a very large text file (consisting of a long string of letters), compressed using gzip. Our test here would be to distribute the data over several VMs on a vSAN datastore and then uncompress the data. Upon enabling compression (and later deduplication and compression for OSA clusters) we can see vSAN compression in action.

#### Importing the Dataset

First, create a VM that we can later template. A fast, repeatable method using an Ubuntu image is detailed in Appendix A.

Before the final steps marking the VM as a template and cloning, power on and open an SSH session to the VM. Download the human genome file (around 1GB in size):

curl -u anonymous:password 'https://ftp.ensembl.org/pub/release-108/fasta/homo sapiens/dna/Homo sapiens.GRCh38.dna sm.toplevel.fa.gz' -o dna.fa.gz

Once this has been downloaded, shutdown the VM and mark as a template. Then clone the VM: the number of clones will, of course, depend on the size of the vSAN datastore.

After cloning, we can inflate the downloaded genome file. The command below uses 'govc' utility, see <u>Appendix A</u> details on downloading the utility. Note, this will take some time:

```
govc find -type m -name 'ubuntu-vm*' | xargs -P0 -I '{}' bash -c 'ssh -o "StrictHostKeyChecking=no"
ubuntu@$(govc vm.ip {}) gzip -dv dna.fa.gz'
```

# ESA Cluster

Below is an example on an ESA cluster. Before the decompression phase (i.e. when the VMs have just been cloned), we have around 4.3TB used, which has been compressed to a ratio of around 1.13x (remember that for ESA compression is enabled by default):



After decompressing the dataset on all the VMs, we now have around 11.6TB used, with a compression ratio of around 4x (the consumption here with vSAN compression is greater than with gzip of course. This is balanced with the advantage of accessing and manipulating the data with greater performance):



# OSA Cluster - Compression only

Similarly, on an OSA cluster with just compression enabled, we have around 4TB used in the first instance, when the VMs have just been deployed:



After decompression we have around 15.6TB used and a compression rate of around 2x. This is around half of the ratio that we saw from the ESA cluster:

	ister	ACTIONS	,				1	'		1
Summary Monitor	Configu	re Permissions	Hosts VMs	Datastores	Networks	Updates				
		Capacity								
	~			<u>~</u> ]						
Triggered Alarms		CAPACITY USAGE	CAPACITY HISTOR	<u> </u>						
Performance	~	Capacity Over	rview							
Overview Advanced		🛇 Used 15.60 TB	3/23.29 TB (67.01%	6)					Free space on disk	is 7.68 TB ( i)
Tasks and Events	~									
Tasks		Compression savi	n 15.60 TB (67.019 ngs: 13.95 TB (Rati	%) io: 1.96x)						
vSphere HA	~	You can enable ca	apacity reserve and	d customize ale	rt thresholds.				RESERVATIO	ONS AND ALERTS
Summary Heartbeat Configuration Issues		What if analys	sis							
Datastores under APD or	r PDL	Effective free	space (withou	t deduplicati	ion and comp	ression)				
Resource Allocation	~	With the policy	vSAN Default Stora	ae Policy	~	The effective free spa	ace for a new wo	orkload would be: 4.4	6 TB (j)	
CPU				,,	_					
Memory		Oversubscript	ion 🕦							
Persistent Memory		Consider compr	ression							
Storage		If all thin provision	ned VMs and user	objects are use	d at full canacity	Capacity required: 12	80 TB ( 0 55x	the available capacit	v 23 29 TB)	
Utilization		in dir tillir provision		objects are use	a at rail capacity	capacity required. In		the available capacit	<i>y</i> 20.20 (0)	
Storage Overview										
Security		Usage breakd	own before co	ompression						
vSphere Cluster Services	~	Usage by categor	ries r	YRAND ALL						
Health		> VM 26.37	TB (89.23%)							
vSAN	~		cts 56 00 MR (0%	\ \						
Skyline Health		S Sel Obje	CLS 50.00 MB (0%)	)						
Virtual Objects		> 📕 System us	sage 3.45 TB (11.66	5%)		System use				
Resyncing Objects						System usag				
Proactive Tests								Transformer		
Performance						User objects		Total usage		
Performance Diagnostics								20.02 10		
Support										
Data Migration Pre-check	k								VM objec	cts
Cloud Native Storage	~									
Container Volumes										
Recent Tasks Alar	ms									

# OSA Cluster - Deduplication and Compression

Here we see the effects of enabling deduplication as well as compression. Note that this can take a long time to complete (as each disk group, in turn, will need to be taken offline, formatted, and brought online again) to enable the service.

As our dataset is the same across all VMs, we achieve an impressive 19x storage saving across the cluster.

inggeree rions	Consolition		
Performance ~ Overview	CAPACITY USAGE CAPACITY HISTORY		
Advanced	Capacity Overview		
Tasks and Events V Tasks Events	Used 2.67 TB/23.29 TB (11.44%)		Free space on disks 20.62 TB 👔
vSphere DRS ~	Actually written 2.67 TB (11.44%) Deduplication and compression savings: 25.83 TB (Ratio: 19.02x)		
Faults History	You can enable capacity reserve and customize alert thresholds.		RESERVATIONS AND ALER
VM DRS Score CPU Utilization	What if analysis		
Memory Utilization Network Utilization Resource Allocation V	Effective free space (without deduplication and compression) With the policy vSAN Default Storage Policy v	The effective free space for a new workload would be: 15.08 TB ()	
CPU Memory	Oversubscription ()		
Storage	Consider deduplication and compression     If all thin provisioned VMs and user objects are used at full capacity	Capacity required: 12.72 TB (0.55x) the available capacity 23.29 TB)	
Storage Overview Security	Usage breakdown before deduplication and compression		
vSphere Cluster Services $\checkmark$ Health vSAN $\checkmark$	Usage by categories EXPAND ALL		
Skyline Health	<ul> <li>User objects 56.00 MB (0%)</li> <li>System usage 2.25 TB (7.9%)</li> </ul>		
Resyncing Objects			
Proactive Tests		User objects	
Capacity		28.75 TB	
Performance Performance Diagnostics			
Support			
Data Migration Pre-check			VM objects

It is important to remember that this is very much an ideal scenario for deduplication. Realistically, it may be very rare to have such a highly compressible dataset that is exactly homogenous across the cluster.

# RAID-5/RAID-6 Erasure Coding

Storage policies that direct vSAN to use RAID-5/6 with erasure coding can provide better space efficiency compared to RAID-1 without erasure coding. Instead of the 200% or 300% overhead with traditional RAID-1 (assuming FTT = 1 or 2 respectively), RAID-5 requires only 33% additional storage, and RAID-6 requires only 50% additional overhead.

## RAID-5/RAID-6 Erasure Coding - vSAN OSA

In vSAN OSA, to support RAID-5 and RAID-6, the following host requirements must be met:

- RAID-5 (3+1): minimum of four hosts; 1.3x space capacity consumed
- RAID-6 (4+2): minimum of six hosts; 1.5x space capacity consumed

#### RAID-5/RAID-6 Erasure Coding - vSAN ESA

vSAN ESA, replaced the traditional 3+1 with RAID-5 scheme with two separate options:

- RAID-5 (2+1): three to five hosts; 1.5x space capacity consumed
  - Opens opportunities to reduce capacity usage for smaller vSAN clusters that relied on RAID-1 topologies requiring 2x space capacity consumed
  - For more information on RAID-1 Performance using RAID5/RAID-6 <u>https://core.vmware.com/blog/raid-56-</u> performance-raid-1-using-vsan-express-storage-architecture
- RAID-5 (4+1): minimum of five hosts; 1.25x space capacity consumed

vSAN ESA includes new *Adaptive RAID-5* functionality. Depending on the number of hosts in the cluster, vSAN ESA will automatically adjust the RAID-5 mode. vSAN ESA presents a single RAID-5 storage policy rule for you to select and will adapt the RAID-5 scheme based on the host count of the cluster. Additionally, it will determine which RAID-5 scheme to use not by the minimum hosts required, but by the minimum hosts *recommended* to ensure there is a spare fault domain (host) whenever possible. Adaptive RAID-5 automatically re-arranges data as the cluster size increases or decreases.

For more details on Adaptive RAID-5 Erasure Coding in vSAN ESA, visit: https://core.vmware.com/blog/adaptive-raid-5-erasure-coding-express-storage-architecture-vsan-8

Note: The erasure coding architecture in vSAN ESA provides the space savings with the same level of performance as RAID-1. Therefore, for most clusters, the recommended storage policy applied to the VMs should be RAID-5. For even higher levels of resilience and space efficiency without compromising performance, consider standardizing on FTT=2 using RAID-6 in clusters with 7 or more hosts.

Below we show how to create a RAID-5 policy and how components are distributed with vSAN OSA and ESA.

#### Create RAID-5 Storage Policy and Apply

We can easily create a RAID-5 storage policy through vCenter. Navigate to: Menu > Policies and Profiles > VM Storage Policies:



Next, navigate to 'VM Storage Policies' and click Create:

$\equiv$ vSphere Client $Q$ Search in all $e$	environments
<ul> <li>Policies and Profiles</li> <li>VM Storage Policies</li> <li>VM Customization Specifications</li> <li>Host Profiles</li> </ul>	VM Storage Policies CREATE Quick Filter Enter value
B Compute Policies	Name Name
C Storage Policy Components	VM Encryption Policy
	VSAN Default Storage Policy
	VVol No Requirements Policy
	Management Storage Policy - Regular
	Management Storage policy - Thin
	Management Storage Policy - Large
	Management Storage Policy - Stretched ESA

Select the appropriate vCenter Server, create a name and click **Next**:

Create VM Storage Policy	Name and description	
1 Name and description	vCenter Server	SC-PDOPS-VM02-DHCD-41-212 ENG VMWA
2 Policy structure	Name:	RAID-5
3 Storage compatibility	Description:	
4 Review and finish		
		li.
		CANCEL NEXT

## Ensure 'Enable rules for "vSAN" storage' is checked and click Next:

Create VM Storage Policy	Policy structure	×
1 Name and description	Host based services	
2 Policy structure 3 VSAN	Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.	
4 Storage compatibility 5 Review and finish	Datastore specific rules Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.	⊧cific
	CANCEL BACK NE	хт

Select 'None - standard cluster' from the 'Site disaster tolerance' drop-down' and 'I failure - RAID-5 (Erasure Coding)' for 'Failures to tolerate" drop-down, then click **Next**:

Create VM Storage Policy	vSAN	×
1 Name and description	Availability Storage rules Advanced Policy Rules Tags	
2 Policy structure	Site disaster tolerance (1) None - standard cluster	
3 vSAN	Failures to tolerate ① 1 failure - RAID-1 (Mirroring) No data redundancy No data redundancy with host affinity	
4 Storage compatibility	1 failure - RAID-1 (Mirroring)	
5 Review and finish	2 failures - RAID-1 (Mirroring) 2 failures - RAID-6 (Erasure Coding) 3 failures - RAID-1 (Mirroring)	
	CANCEL BACK	NEXT

Once "1 failure - RAID-5 (Erasure Coding)' is selected, you may see this warning 'RAID-5/6 (Erasure Coding) - Capacity requires an All-flash configuration." If so, select the 'Storage rules" tab:

Create VM Storage Policy	VSAN		$\times$
1 Name and description	Availability  Storage rules	Advanced Policy Rules Tags	
2 Policy structure	Site disaster tolerance (j)	None - standard cluster	
3 VSAN	Failures to tolerate (	1 failure - RAID-5 (Erasure Coding) ① RAID-5/6 (Erasure Coding) - Capacity requires an All flash configuration.	
4 Storage compatibility		Consumed storage space for 100 GB VM disk would be 133.33 GB	
5 Review and finish			
		CANCEL BACK N	EXT

Once in the Storage rules tab, you will see:



Check the 'All flash' radio, then click Next:

Create VM Storage Policy	VSAN		×
1 Name and description	Availability Storage rules	Advanced Policy Rules Tags	
2 Policy structure	Encryption services (	<ul> <li>Data-At-Rest encryption</li> <li>No encryption</li> </ul>	
3 VSAN		No preference	
4 Storage compatibility	Space efficiency (1)	<ul> <li>Deduplication and compression</li> <li>Compression only</li> </ul>	
5 Review and finish		<ul> <li>No space efficiency</li> <li>No preference</li> </ul>	
	Storage tier	<ul> <li>All flash</li> <li>Hybrid</li> <li>No preference</li> </ul>	CANCEL BACK NEXT

We see that the vSAN datastore is compatible with this policy (in this example there is both an OSA and ESA datastore listed), click **Next**:

Create VM Storage Policy	Storage compatibility >	×
1 Name and description 2 Policy structure	COMPATIBLE         INCOMPATIBLE           Expand datastore clusters         Compatible storage 45.12 TB (42.87 TB free)	
3 vSAN	Quick Filter	
4 Storage compatibility	Name         Datacenter         Type         Free Space         Capacity         Warnings           I vSAN-OSA-Datastore         vsan-test-dc         vSAN         22.89 TB         23.29 TB         Image: Capacity         Image: Capacity	
S REVIEW and milish		
	Manage Columns 2 items	
	CANCEL BACK NEXT	

#### Finally, review and click **Finish**:

Create VM Storage Policy	Review and finish				×
	General				
1 Name and description	Name	RAID-5			
2. Policy structure	Description				
2 Policy structure	vCenter Server	vsan-test-vc.colinlab.vsanpe.vmware.com			
3 VSAN	VSAN				
	Availability				
4 Storage compatibility	Site disaster tolerance	None - standard cluster			
	Failures to tolerate	1 failure - RAID-5 (Erasure Coding)			
5 Review and finish	Storage rules				
	Encryption services	No preference			
	Space efficiency	No preference			
	Storage tier	All flash			
	Advanced Policy Rules				
	Number of disk stripes per	1			
	object				
	IOPS limit for object	0			
	Object space reservation	Thin provisioning			
	Flash read cache reservation	0%			
	Disable object checksum	No			
	Force provisioning	No			
			CANCEL	BACK	FINISH

Next, we apply this storage policy to an existing VM. Navigate to [Virtual Machine] > Configure > Policies and click Edit VM storage policies:

🕏 ubuntu02-ES	SA 🖂 🖂 🗗 🖓 🔞 🕴 Actions				
Summary Monitor	Configure Permissions Datastores	Networks Snapshots Updates			
Settings 🗸 🗸	Policies			EDIT VM STC	DRAGE POLICIES
VM SDRS Rules	CHECK VM STORAGE POLICY COMPLIANCE	REAPPLY VM STORAGE POLICY			
Alarm Definitions	Name <b>T</b>	VM Storage Policy	T Compliance Status	T Last Checked	Ŧ
Scheduled Tasks	>>> 🗅 VM home	vSAN-ESA-Cluster - Optimal Datastore Default Policy - RAID5	Compliant	02/05/2024, 4:10:46 PM	
Policies	》 魯 Hard disk 1	vSAN-ESA-Cluster - Optimal Datastore Default Policy - RAID5	✓ Compliant	02/05/2024, 4:10:46 PM	
VMware EVC					
Guest User Mappings					

Select the newly created storage policy and click **OK**:

tit	: VM Storage	Policies	ubuntu02-ESA		
sto	orage policy RAID-5		~		Configure per disk 🔵
al v	/SAN storage consum	ption: 9.3 GB ( 🛧 12	2.64 MB) storage space		
	Name	Disk Size	Datastore	Datastore Type	
	D VM home	-	vSAN-ESA-Datastore	vSAN	
	🖺 Hard disk 1	100 GB	vSAN-ESA-Datastore	vSAN	
					2 ite
					CANCEL

After this has been set, vSAN will move the data components as per the policy. Once this has been completed, the VM's disks will show as compliant to the policy:

🕏 ubuntu02-ES	ট ubuntu02-ESA 🛛 Þ 🗖 🐯 🕴 🗄 Actions					
Summary Monitor	Configure Permissions Datastores Netwo	ks Snapshots Updates				
Settings 🗸 🗸	Policies					EDIT VM STORAGE POLICIES
VM SDRS Rules	CHECK VM STORAGE POLICY COMPLIANCE REAPPLY VM	STORAGE POLICY				
vApp Options	Name	VM Storage Policy	Compliance Status	T	Last Checked	Ŧ
Scheduled Tasks	>> D VM home	RAID-5	✓ Compliant		02/05/2024, 4:11:30 PM	
Policies	》	RAID-5	✓ Compliant		02/05/2024, 4:11:30 PM	
VMware EVC						
Guest User Mappings						

We can now observe the data objects are arranged in vSAN OSA and ESA clusters

#### RAID-5 Data Placement in vSAN OSA

Navigate to [Virtual Machine] > Monitor > Physical disk placement. This screen shows that the components are now spread over four hosts, i.e. RAID-5 3+1:

🕏 ubuntu01-OSA	D 🗆 🗳 🖗 🔯 🗄 Actions							
Summary Monitor C	onfigure Permissions Datastores Net	igure Permissions Datastores Networks Snapshots Updates						
Issues and Alarms 🗸	iysical disk placement							
All issues	Group components by host placement							
Triggered Alarms	Virtual Object Components							
Performance V	Туре	Component State	Host	Fault Domain	Cache Disk	Cache Disk UUID		
Advanced	✓							
Tasks and Events 🗸 🗸	Component	Active	10.156.130.209		E Local NVMe Disk (t10.NVMeINTEL_SS	522f3bbe-a33b-e497-b314-e2d0b1611ce3		
Tasks Events	Component	Active	10.156.130.211		E Local NVMe Disk (t10.NVMeINTEL_SS	5278c32d-48c9-58f1-8d6d-9e26e014f058		
Utilization	Component	Active	10.156.130.212		Ê Local NVMe Disk (t10.NVMeINTEL_SS	52fe6af5-e091-8960-ed68-4dc07fd24012		
vSAN 🗸	Component	Active	10.156.130.210		E Local NVMe Disk (t10.NVMeINTEL_SS	522af629-1bbd-b848-c562-7e6ff849e13d		
Physical disk placement	✓ Virtual machine swap object (RAID 5)							
I/O Trip Analyzer	Component	Active	10.156.130.209		Ê Local NVMe Disk (t10.NVMeINTEL_SS	522f3bbe-a33b-e497-b314-e2d0b1611ce3		
	Component	Active	10.156.130.211		E Local NVMe Disk (t10.NVMeINTEL_SS	52f51163-f6e1-0b9d-b168-55f89cbbf4f0		
	Component	Active	10.156.130.212		E Local NVMe Disk (t10.NVMeINTEL_SS	52806139-b858-f3a8-f134-1a0b95bbf0ef		
	Component	Active	10.156.130.210		E Local NVMe Disk (t10.NVMeINTEL_SS	522af629-1bbd-b848-c562-7e6ff849e13d		
	VM home (RAID 5)							
	Component	Active	10.156.130.209		Ê Local NVMe Disk (t10.NVMeINTEL_SS	526056c7-321c-9ce3-846b-d9bcfd26559c		
	Component	Active	10.156.130.211		E Local NVMe Disk (t10.NVMeINTEL_SS	5278c32d-48c9-58f1-8d6d-9e26e014f058		
	Component	Active	10.156.130.212		E Local NVMe Disk (t10.NVMeINTEL_SS	52fe6af5-e091-8960-ed68-4dc07fd24012		
	Component	Active	10.156.130.210		E Local NVMe Disk (t10.NVMeINTEL_SS	52528774-fe28-7e3c-7d92-f3db3a1ef357		

#### RAID-5 Data Placement in vSAN ESA

As above, we navigate to [Virtual Machine] > Monitor > Physical disk placement. As expected, we see the performance leg remain as RAID-1. Moreover, as we have four hosts, vSAN adaptive RAID-5 will select the 2+1 layout for the capacity leg. As shown below, the capacity leg is RAID-5, spread over three hosts, i.e., RAID-5 2+1:

🕏 ubuntu02-ESA	ট ubuntu02-ESA 🛛 Þ 🗖 🗳 🚳 🕴 : actions					
Summary Monitor C	onfigure Permissions Datastores Ne	tworks Snapshots	Updates			
Issues and Alarms 🗸	ysical disk placement					
All Issues	Group components by host placement					
Triggered Alarms	Virtual Object Components					
Performance 🗸	Туре	Component State	Host	Fault Domain	Disk	Disk UUID
Overview	✓				1	
Tasks and Events 🗸						
Tasks	* RAID I					
Events	Component	Active	10.156.130.219		Local NVMe Disk (TO.NVMeINTEL_SS	52616180-bddt-8811-9154-cd0b155c63df
Utilization	Component 🔮 Active 🗒 10.156.130.217 🛃 Local NVMe Disk (t10.NVMeINTEL_SS 5277858b-4117-bec3-0e4b-fbab0227a9b9					
VSAN V	V RAID 5					
Physical disk placement Performance	V RAID 0					
I/O Trip Analyzer	Component	Active	10.156.130.219		E Local NVMe Disk (t10.NVMeINTEL_SS	52f967c0-2507-c6be-f842-0e4e99a8b4ba
	Component	Active	10.156.130.219		E Local NVMe Disk (t10.NVMeINTEL_SS	52f967c0-2507-c6be-f842-0e4e99a8b4ba
	V RAID 0					
	Component	Active	10.156.130.218		E Local NVMe Disk (t10.NVMeINTEL_SS	52db45b5-53e4-454d-fc9b-6b8e5531e925
	Component	Active	10.156.130.218		E Local NVMe Disk (t10.NVMeINTEL_SS	52036101-a406-f0d8-bcbe-2cfdf64e8ab0
	✓ RAID 0					
	Component	Active	10.156.130.217		E Local NVMe Disk (t10.NVMeINTEL_SS	52913651-2472-8df5-f3b8-650a0543512d
	Component	Active	10.156.130.217		E Local NVMe Disk (t10.NVMeINTEL_SS	52913651-2472-8df5-f3b8-650a0543512d
	✓ Virtual machine swap object (Concatenation)	(				

# Trim/Unmap

vSAN supports space reclamation on virtual disks using trim commands issued from the guest VM operating system.

#### **Guest Requirements**

The following should be met for trim/unmap to work:

- At least VM hardware version 11 (Windows) or version 13 (Linux)
- The setting 'disk.scsiUnmapAllowed' in the VM's VMX file set to true (default)
- The VM's operating system recognizes the disk as 'thin'

#### For more details, visit:

https://core.vmware.com/resource/vsan-space-efficiency-technologies#sec19560-sub5

#### Enabling Trim/Unmap on an ESA Cluster

Trim/Unmap functionality is enabled by default in vSAN ESA clusters.

Trim/Unmap functionality can be explicitly disabled in the VMX file by the setting disk.scsiUnmapAllowed set to false.

#### Enabling Trim/Unmap on an OSA Cluster

To enable this feature for vSAN OSA, a cluster-wide setting for enabling unmap is set by navigating to [vSAN Cluster] > Configure > Services > Advanced Options then click the EDIT button that corresponds to the Advanced Options section:

vSAN-OSA-Clust	er Eactions	
Summary Monitor Co	nfigure Permissions Hosts VMs Datastores Networks Updates	
Services 🗸	vSAN Services	SHUTDOWN CLUSTER TURN OFF VSAN
vSphere DRS vSphere Availability	> Storage	> Data Services
Configuration >	MOUNT REMOTE DATASTORES	EDIT GENERATE NEW ENCRYPTION KEYS
Licensing > Trust Authority	> Support Insight (Disabled)	vSAN ISCSI Target Service     (Disabled)
Alarm Definitions Scheduled Tasks	ENABLE	ENABLE
vSphere Cluster Services > vSAN ✓	> Performance Service (Enabled)	> Reservations and Alerts
Services Disk Management	EDIT	EDIT
Fault Domains Remote Datastores	> File Service (Disabled)	V Advanced Options
Desired State 🗸	ENABLE	Object repair timer 60 minutes Site read locality Enabled
Configuration	✓ Network	Thin swap Enabled Guest Trim/Unmap Disabled
	RDMA support Disabled	Automatic rebalance Disabled
	EDIT	
		> Historical Health Service (Enabled)
		EDIT

Then toggle the 'Guest Trim/Unmap' setting. Note that VMs will need to be power cycled for this setting to be effective:

Advanced Opti		OSA Cluster		×	
Object repair timer	60	\$			
	The amount of (absent failure	minutes vSAN waits before repa ) or in Maintenance Mode.	iring an object after a host is either in	a failed state	
Site read locality					
When enabled, reads to vSAN objects occur locally. When disabled, reads occur across both sites for stretched cluster.					
Thin swap					
When enabled, swap objects will not reserve 100% of their space on vSAN datastore; storage policy reservation will be respected.					
Guest Trim/Unmap					
When enabled, vSAN automatically reclaims blocks after Guest OS file deletions. VMs that are running need to be power cycled for the setting to take effect. Refer to the administrative guide for prerequisites.					
Automatic rebalance	1				
When the cluster is unba Rebalance can wait up to the resources before reb	alanced, rebalance o 30 minutes to st oalancing.	starts automatically after enablir rt, giving time to high priority ta:	ng automatic rebalance. sks like EMM, repair, etc. to use		
Rebalancing threshold %	30	$\hat{}$			
	Determines wh much variance disks is less the	en background rebalancing start then rebalancing begins. It will co n 1/2 of the rebalancing threshol	is in the system. If any two disks in the ontinue until it is turned off or the the d.	e cluster have this variance between	
			CANCE	APPLY	

Once unmap is enabled on the cluster, guest VMs can issue commands (such as fstrim) to free any previously deleted data. Trim/unmap is enabled by default on vSAN ESA.

#### Example on an OSA Cluster

To demonstrate the effects of this on a vSAN OSA cluster, firstly we observe how much space is in use currently, by navigating to [vSAN Cluster] > [Monitor] > [Capacity].

In this example, we can see that around 931GB of space is currently in use, with around 493GB of VM data:

CAPACITY USAGE CAPACITY HISTORY	
Capacity Overview	
Used 1.47 TB/21.83 TB (6.75%)	Free space on disks 20.36 TB ①
Actually written 931.49 GB (4.17%)	
Usable capacity analysis	
Use this panel to estimate the effective free space available if you deploy a new workload with the selected storage	policy, assuming dedup ratio is 1. ①
Change policy to vSAN Default Storage Policy v	Effective free space with the policy: 10.18 TB
Usage breakdown before dedup and compression	
Usage by categories EXPAND ALL	/ VM objects
<ul> <li>VM 493.25 0B (32.60%)</li> <li>User objects 686.22 GB (45.44%)</li> </ul>	
> System usage 330.61 GB (21.89%)	
	System usage Total usage
	1.47 TB
	User objects

Next, we create or copy a large file on our guest VM. In this case a Windows 2016 VM is used, and a large (~76GB) file has been created:



As expected, our space utilization increases by around 76GBx2 (as this is a RAID-1 object). Thus, 76GBx2 + 493GB gives us around 644GB, as we see below:



We now delete the file:

		S Windows2016x64en-US		
Recycle Bin				
Cygwin64 Terminal				
$\mathbf{P}$	I I I I I I I I I I I I I I I I I		-	linns.
Google	$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\blacksquare$ > This PC > New Volume (	2)	Search New Volume (E:) の	
	Cuick access Destop Downloads Documents Nusic Pictures Videos New Volume (E) New Volume (E)	Delete File X Are you sure you want to permanently delete this file? big.file Type: File Size: 76.2 GB Date modified: 4/8/2020 1:53 AM Yes No		
	1 item 1 item selected 76.2 GB			
م 🗉			∧ ⊲ <mark>∞ ⊡</mark> 2:06 AM 4/8/2020	

Looking back at the capacity view, we can see that the space consumed is still the same:

Capacity Overview
Used 1.63 TB/21.83 TB (7.44%)
Actually written 1.06 TB (4.86%) Reserved 578.59 GB (2.59%)

We now enable the guest trim/unmap advanced setting for the cluster (see above).

Looking back at vCenter, we see that the used space has been freed:

CAPACITY USAGE CAPACITY HISTORY		
Capacity Overview		
Sused 1.47 TB/21.83 TB (6.75%)		Free space on disks 20.36 TB (
Actually written 920 67 GR (d 16%)		
Reserved shous du (2.3.4)		
Usable capacity analysis		
Use this panel to estimate the effective free space available if you deploy a new workload with the selected storage policy, a	assuming dedup ratio is 1. ①	
Change policy toVSAN Default Storage Policy	Effective free space with the policy: 10.18 TB	
Usage breakdown before dedup and compression		
Usage by categories EXPAND ALL	/ VM objects	
> User objects 686.22 GB (45.47%)		
> 📕 System usage 330.61 GB (21.91%)		
	System usage Total usage 1.47 TB	
	User objects	

# vSAN Max<sup>™</sup> - Disaggregated Storage

What is vSAN Max? VMware's new disaggregated storage offering that provides Petabyte-scale centralized shared storage for your VMware vSphere® (vSphere) clusters.

Built on the foundation of vSAN ESA, vSAN Max is a fully distributed architecture, where access to data is NOT funneled through centralized I/O controllers. Instead, vSAN Max uses the full power of each node (host) in the vSAN Max cluster. Aggregated resources across all hosts in a vSAN Max cluster to the process I/O. Each additional host linearly scales capacity and performance.

For more additional technical information please review:

- Main vSAN Max informational page <u>- https://core.vmware.com/vsan-max</u>
- vSAN Max Design & Operations Guide <u>https://core.vmware.com/resource/vsan-max-design-and-operational-guidance</u>
- vSAN Max introduction blog post https://core.vmware.com/blog/introducing-vsan-max
- vSAN Max scalability blog post https://core.vmware.com/blog/vsan-max-and-advantage-scalability

#### vSAN Max Sizing Considerations

When sizing vSAN Max deployments, consider that vSAN Max clusters support:

- A maximum of 32 ESXi hosts in the cluster (24 ESXi hosts recommended)
- A maximum of 10 compute clusters mounting to a single vSAN Max cluster
- A maximum of 128 total ESXi hosts (both within the vSAN Max cluster and the vSAN Compute clusters connecting to a single vSAN Max datastore)

Note: Limiting the vSAN Max cluster size to 24 ESXi hosts will allow for up to 104 ESXI hosts from vSAN compute clusters to mount the datastore, offering a 4.3:1 ratio. A vSAN Max cluster size of 32 ESXi hosts would allow for up to 96 ESXI hosts from vSAN compute clusters to mount the datastore, offering a storage ratio of 3:1.

# Disaggregated Storage for vSAN OSA (AKA: HCI Mesh)

Although the vSAN Max is explicitly a vSAN ESA function, vSAN OSA deployments still support disaggregated storage.

vSAN OSA datastores can be shared between two vSAN clusters, utilizing vSAN's native data path for cross-cluster connections. Compute Only Clusters are also supported.

Each vSAN OSA client cluster can mount a maximum of ten remote vSAN OSA datastores. A vSAN OSA server cluster can export its datastore up to a maximum of ten client clusters.

All vSAN features are supported except for Data-in-Transit encryption, Cloud Native Storage (including vSAN Direct), Stretched Clusters, and 2-Node Clusters. Additionally, HCI Mesh will not support remote provisioning of File Services Shares, iSCSI volumes, or First-Class Disks (FCDs). File Services, FCDs, and the iSCSI service can be provisioned locally on clusters participating in a mesh topology but may not be provisioned on a remote vSAN datastore.

The same MTU sizing is required for both the Client and Server clusters.

# Using Quickstart to Enable vSAN Max Cluster

vSAN Max leverages vSAN ESA, as such the initial enablement process is very similar to the steps reviewed in the Using Quickstart to Enable Single vSAN HCI Cluster section of the vSAN Proof of Concept: vSAN Architecture Overview & Setup Guide.

#### Initialize Cluster

Navigate to your **Datacenter >** Click **Actions > New Cluster**.

vSphere Client Q Search in all environments		C <sup>i</sup> & Administrator@VSPHERE.LOCAL ~ 🙄 (?) ~
Vsan-test-dc     Actions     Summary Monitor C Actions - vsan-test-dc	VMs Datastores Networks Updates	
Add Host. Detacenter Details New Folder Uritual Virtual Virtual New Virtual Machine. Ousterr Storage Datate Edit Default VM Compa & Migrate VMs to Anothe Migrate VMs to Anothe	Image: Compacting and Usage     Image: Compacting an	utes II 🕲
Add Permission_	s > VIEW STATS ASSIGN ADD	
Alarms	<u> </u>	

The New Cluster screen pops-up and we are presented with a dialog to enable services. Provide a name for the cluster and select vSAN from the list of services. Ensure that vSAN ESA (the default). For the Quickstart workflow to configure the vMotion VMkernel, vSphere DRS must be set to enabled.

New Cluster	Basics		×
1 Basics	Name vSAN-Max		
2 Image	Location 🗈 vsan-test-dc		
3 Review	vSphere DRS		
	(1) vSphere HA		
	vSAN		
	Manage all hosts in the cluster with a single image 3		
	Choose how to set up the cluster's image Compose a new image Import image from an existing host in the vCenter inventory Import image from a new host Manage configuration at a cluster level ()		
		CANCEL	т

We can also setup the cluster to use a single image (thereby enabling vLCM). For more information on vLCM, see: <a href="https://core.vmware.com/resource/introducing-vsphere-lifecycle-management-vlcm">https://core.vmware.com/resource/introducing-vsphere-lifecycle-management-vlcm</a>.

#### Quickstart – Cluster Basics

The initial cluster creation above initializes the Quickstart process. Once the cluster has been created, navigate to [vSAN Cluster] > Configure > Quickstart. On this screen you will be able to confirm the basic services selected previously then move to the add hosts and configuration phases.



#### Quickstart – Add Hosts

The Adding Hosts steps for vSAN Max are identical to those for a single vSAN HCl cluster. Refer to the steps documented in the Enable a Single vSAN HCl, Quickstart – Add Hosts section of the vSAN Proof of Concept: vSAN Architecture Overview & Setup Guide.

#### Quickstart - Configure Cluster

The next step is to configure the vSAN Max cluster. After clicking on **Configure** under <u>Step 3: Configure Cluster</u>, the Configure Cluster workflow will start. Ensure that **vSAN Max** is selected.

#### Step 1: Select Cluster Type

Configure cluster	Cluster Type	×
Cluster Type     Distributed switches	<ul> <li>vSAN HCI</li> <li>A cluster of hosts providing tightly coupled storage and compute resources, integrated in the hypervisor to provide a single software defined infrastructure.</li> </ul>	vm vm vm vm vSAN
3 vMotion traffic 4 Storage traffic 5 Advanced options 6 Claim disks	• vSAN Max A dedicated cluster of hosts providing a distributed decoupled storage solution for vSphere clusters, integrated in the hypervisor for simplified management and maximum scalability.	
7 Réview		
		CANCEL NEXT

#### Steps 2 -7: Configuring the Cluster

The remaining steps to configure the vSAN Max cluster are identical to those for a single vSAN HCl cluster. Refer to the steps documented in the Enable a Single vSAN HCl, Quickstart – Configure Cluster section of section of the vSAN Proof of Concept: vSAN Architecture Overview & Setup Guide.

After the new vSAN Max cluster creation completes, navigate to [vSAN Cluster] > Configure > vSAN > Services. The screen will show that the vSAN Max cluster is ready to provide disaggregated storage to vSAN Computer clusters.

II VSAN-Max ACTIO	ONS			
Summary Monitor Config	gure Permissions Hosts VMs vSAN Services	Datastores Networks Updates	SHUTDOWN CLUSTER	TURN OFF VSAN
vSphere Availability	✓ Storage		> Data Services	
Quickstart	Cluster type VSAN Max	lustar of basts providing a distributed descurbed storage	EDIT GENERATE NEW ENCRYPTION KEYS	
Key Provider VMware EVC	solution for vs management	Sphere clusters, integrated in the hypervisor for simplified and maximum scalability.	> vSAN ISCSI Target Service	Disabled
VM/Host Groups VM/Host Rules	Storage types VSAN ESA		ENABLE	
VM Overrides I/O Filters	VSAN ESA	vSAN Express Storage Architecture is a next-	> Reservations and Alerts	
Host Options Host Profile		generation architecture designed to get the most out of high-performance storage devices, resulting in greater performance and efficiency.	EDIT	
Licensing V vSAN Cluster	vSAN managed disk claim Auto-Policy management	Disabled Enabled	> Advanced Options	
Trust Authority Alarm Definitions	EDIT		EDIT	
Scheduled Tasks	> Support Insight	Disabled	> Historical Health Service	Enabled
General Datastores	ENABLE		EDIT	
vSAN ~	> Performance Service	Enabled		
Disk Management Fault Domains	EDIT			

Now navigate to **[vSAN Cluster] > Configure > vSAN > Remote Datastore**. This screen shows the name of the remote datastore created by the vSAN Max cluster configuration workflow. The datastore name is a default name. If you wish to rename this datastore please refer to the <u>Post-Configuration – Renaming vSAN Datastore</u> section of this document.

Image: Summary Monitor       Configure       Permissions       Hosts       VMs       Datastores       Networks       Updates									
Services     Remote Datastores       Configuration     View and manage remote vSAN datastores mounted to this cluster.       Licensing     MOUNT REMOTE DATASTORE									
Trust Authority			Datastore	Cluster	VMware vCenter instance	Capacity Usage	Free Capacity	VM Count 🚯	Client Clusters
Alarm Definitions Scheduled Tasks		0	(Local) vsanDatastore(1)	[]] vSAN-Max	Ø. i i i i i	1.88 TB / 21.83 TB	19.96 TB	1	1 Cluster(s)
vSphere Cluster Service	s >								
vSAN	~								
Services									
Disk Management									
Remote Datastores									
Desired State	$\sim$								
Image									
Configuration									

#### Post-Configuration – Renaming vSAN Datastore (optional)

Once the vSAN Max cluster creation completes, the vSAN Max datastore is ready to be shared with vSAN Compute Clusters. The datastore will have the default name of "vsanDatastore." If the default name is not suitable for your environment, use these steps to rename the datastore as needed.

Navigate to **[vSAN Cluster] > Datastores**. Once on that screen, filter on vSAN (to make it easier to find the new datastore otherwise one may see the local datastore for each cluster host as well). Then right-click on the vSAN datastore and select **Rename**.

Image: Control of the second secon	itores Networks Updates
Datastores Datastore Clusters	
Quick Filter VSAN	
✓         Name         ↑         Status         Type         Datastor	re Cluster Capacity Free
	Actions - vsanDatastore(1)            ⓐ Actions - vsanDatastore(1)            ⓑ New Virtual Machine            ⓑ Register VM            ⓒ Refresh Capacity Information             Move To             Tags & Custom Attributes             Add Permission             Alarms
▼ 1 Manage Columns Export ~	items per page 35 v 1 item

This will open the Rename workflow. In the workflow rename the datastore as needed then select OK

Rename   vsanD	atastore(1)	×
Enter the new name	vSAN-Max-Datastore	
		CANCEL
The datastore will now reflect the newly assigned name.

SAN-Max ACTIONS							
Summary Monitor Configure	Permissions	Hosts	VMs	Datastores	Networks	Updates	
Datastores         Datastore Clusters           Quick Filter         ✓         vSAN							
Name	↑ Status	Туре		Datastore Cluster	Capacity	/ Free	
SAN-Max-Datastore	V Norn	nal vSAN	1		21.83 TI	в 19.96 тв	

# Manually Enabling vSAN Max on a Cluster

Note: If Quickstart was used (as per the earlier section) then this section can be skipped.

Manual vSAN Max enablement is available for those that do not wish to use the Quickstart process.

For this scenario, please follow the vSAN Max Cluster Services Configuration instructions in the vSAN Max Design and Operational Guidance document. Direct link to the section listed below:

https://core.vmware.com/resource/vsan-max-design-and-operational-guidance - sec32263-sub1

# Enabling vSAN Max/HCI Mesh Services on a VMware Cloud Foundation™ based Cluster

VCF includes dedicated processes to automate the deployment and configuration of core infrastructure including vSAN services. In fact, these processes are required and are the only supported methods within VCF.

As of the writing of this guide, VCF 5.1 supports HCI Mesh. For more information, please review below.

HCI Mesh with VCF - https://docs.vmware.com/en/VMware-Cloud-Foundation/5.1/vcf-admin/GUID-1F86850D-E95E-40A8-AFC5-BE58D504D739.html

# Encryption in vSAN

There are two (mutually exclusive) modes of encryption available with vSAN, namely:

- Data-at-Rest encryption Encrypts data on the configured physical devices within the vSAN cluster
- Data-in-Transit encryption
  - o Encrypts data as it moves across the network between hosts in the vSAN cluster
  - When you enable data-in-transit encryption, vSAN encrypts all data and metadata traffic between hosts

Either encryption is usable alongside all other vSAN features (such as deduplication and compression, RAID-5/6 erasure coding, and stretched cluster configurations among others). Additionally, all vSphere features, such as VMware vSphere® vMotion® (vMotion), VMware vSphere® Distributed Resource Scheduler™ (DRS), VMware vSphere® High Availability (HA), and VMware vSphere® Replication™ are supported.

Note: Although not covered in this guide, one can also encrypt at the virtual machine level via vSphere Virtual Machine Encryption. For more information please review:

https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-8D7D09AC-8579-4A33-9449-8E8BA49A3003.html

# vSAN Data-at-Rest Encryption

vSAN can encrypt data at rest in your vSAN datastore. Data is encrypted after all other processing, such as deduplication, is performed. Data at rest encryption protects data on storage devices in case a device is removed from the cluster.

Be aware that:

Self-encrypted drives are not required.

- vSAN OSA
  - Data is encrypted when it is written to persistent media and the encryption step occurs just before the write to the capacity device
  - o Data-at-Rest encryption can be enabled in an existing cluster in vSAN OSA
  - o If there is enough space in the cluster, data is evacuated from each device, which are then, in turn, formatted
- vSAN ESA
  - o The encryption step is higher in the stack (compared to OSA), just after the guest write
  - Once Data-at-Rest encryption is enabled it cannot be disabled

#### Key Management Server

A Key Management Server (KMS) is required to enable and use data-at-rest encryption, whether vSAN ESA or OSA. Either a native (built-in) key provider in vCenter or a third-party KMS solution can be used. Third-party KMS are commonly deployed in clusters of hardware appliances or virtual appliances for redundancy and high availability.

VMware maintains a HCL for KMS servers here: https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms

#### Internal Key Management Server

Integrated with vCenter, a built-in 'native' key provider is available to use, providing basic key functionality.

To enable, navigate to [Top Level-vCenter Server] > Configure > Key Providers > Add > Add Native Key Provider:

R vsan-test-vc.colinlab.vsanpe.vmware.com						
Summary Monitor	Configure Permissions Datacenters Hosts & Clusters VMs Datastores Networks Linke					
Settings 🗸	Key Providers					
General Licensing	ADD - BACK-UP RESTORE SET AS DEFAULT EDIT DELETE					
Message of the Day	Add Native Key Provider 1 Type					
Advanced Settings Authentication Proxy vCenter HA	Add Standard Key Provider					
Security 🗸	No items fo					
Trust Authority						
Key Providers						
Alarm Definitions						
Scheduled Tasks						
storage Providers						
VSAN V Update Internet Connectivity	Manage Columns					
Remote Datastores						

During the naming of the Key Provider, you are presented with the recommended option to only "Use the key provider with TPM protected VMware ESXi<sup>m</sup> (ESXi) Hosts." Note that it is advisable to use a TPM protected host. That said, If the checkbox is selected, this Key Provider will not work on non-TPM protected hosts. In that scenario, the workflow to enable data-at-rest encryption will fail (discussed later in this section). For the purposes of this walkthrough, in the Add Native Key Provider, the TPM selection checkbox is unchecked.

For more details visit:

https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-31F2B3D0-259A-4EFD-B675-F89BC27ACE55.html

Add N	Add Native Key Provider ×					
Name	nternal KMS provider only with TPM protected ESXi hosts (Recommended)					
	CANCEL ADD KEY PROVIDER					

🛱 vsan-test-vc.d	colinlab.vsanpe.vmware.com	ACTIONS		
Summary Monitor	Configure Permissions Datacenters	Hosts & Clusters VMs Datastores	Networks Linked vCenter Server Systems	Extensions Upda
Settings ~	Key Providers			
Licensing	ADD + BACK-OP RESTORE SET AS	S DEFAULT EDIT DELETE		
Message of the Day	Key Provider	Туре	↑ Status	
Authentication Proxy	Internal KMS (default)	Native	⊘ Active	
vCenter HA				
Security 🗸				
Trust Authority Key Providers Alarm Definitions Scheduled Tasks Storage Providers vSphere Zones VSAN Update Internet Connectivity Remote Datastores	Manage Columns Provider Internal KMS - Key Managemen	nt Servers		
	Details Constraints			
	Key ID b310b544-e218-4222-ae57-ec06	5329f92bf Back up Key Provi	ider	Active

To function, the native key provider must be backed up (a file will be downloaded locally):

When enabling vSAN Encryption, the added Native Key Provider will be available to select. You can add both the internal and external KMS servers to vCenter and use them in different clusters.

Utilizing the Native Key Provider is a quick and easy way to test the vSAN Encryption services. For more advanced functionality, such as redundancy across KMS servers (possibly located in different locations) you may want to consider utilizing external KMS in a cluster configuration.

## External Key Management Server

Given the multitude of Key Management Server (KMS) vendors, the setup and configuration of a KMS server/cluster is out of scope for this document. However, it is a prerequisite prior to enabling vSAN encryption. The initial configuration of the KMS server is done through vCenter; the KMS cluster is, and a trust relationship is established. The process for doing this is vendor-specific, so please consult your KMS vendor documentation prior to adding the KMS cluster to vCenter.

To add an external KMS cluster to vCenter, like above, navigate to [Top Level-vCenter Server] > Configure > Key Providers > Add > Add Standard Key Provider.

R vsan-test-vc.colinlab.vsanpe.vmware.com						
Summary Monitor	Configure Permissions Datacenters Hosts & Clusters VMs Datastores Networks L	Linke				
Settings 🗸	Key Providers					
General Licensing	ADD - BACK-UP RESTORE SET AS DEFAULT EDIT DELETE					
Message of the Day	Add Native Key Provider Type	$\uparrow$				
Authentication Proxy	Add Standard Key Provider	7				
vCenter HA		15				
Security V	No item	ns fo				
Trust Authority						
Alarm Definitions						
Scheduled Tasks						
Storage Providers						
vSphere Zones						
vSAN 🗸						
Update	Manage Columns					
Internet Connectivity						
Remote Datastores						

Enter the information for your specific KMS cluster/server:

Add Standard Key Provider				
Name				
кмѕ	Address	Port		
ADD KMS			0	
> Proxy configuration (op	tional)			
> Password protection (o	ptional)			
	CANCE	ADD KEY PR	OVIDER	

Once the KMS cluster/server has been added, you will need to establish trust with the KMS server. Follow the instructions from your KMS vendor as they differ from vendor to vendor.

vSphere Client	$Q_{c}$ Search in all environments				C	o_Administrator@∨	SPHERE.LOC		?
🔋 vC-dxb-8.vsa	npe.vmware.com	ONS							
Summary Monitor	Configure Permissions Data	centers Hosts	& Clusters VMs	Datastores	Networks Lir	nked vCenter Serve	r Systems	Extensions	-
Settings 🗸 🗸	Key Providers								
General	Multiple Native Key Providers are	configured. Consu	t the documentation fo	r guidelines and b	oest practices.				
Message of the Day Advanced Settings	ADD - BACK-UP RESTORE	SET AS DEFAI	JLT EDIT DEL	.ETE					
Authentication Proxy	Key Provider		Туре	$\uparrow$	Status		Certificates		
vCenter HA	Internal KMS non-TPM		Native		Active				
Security $\checkmark$	Internal KMS		Native		Active				
Trust Authority	• external KMS (default)		Standard		🛆 1 KMS not conn	ected	🛆 2 certific	cate issue(s)	
Key Providers Alarm Definitions	Provider external KMS - Key M	anagement Serv	vers						
Scheduled Tasks	ESTABLISH TOUST								
Storage Providers	ESTABLISH TRUST V								
	KMS trust vCenter	dress	Port	Connection S	itatus	vCenter Certifica	te	KMS Certificate	
VSAN V	Make KMS trust vCenter	.156.152.68	5696	\land No trust	ed connection				
Update	Upload Signed CSR Certificate								1 ite
Internet Connectivity	vCenter Trust KMS								
	Make vCenter Trust KMS								
	Upload KMS Certificate								

After the KMS has been properly configured, you will see that the connection status and the certificate have green checks, meaning we are ready to move forward with enabling vSAN encryption.

# Enabling vSAN Data-at-Rest Encryption - vSAN ESA

Prior to enabling vSAN ESA encryption, a KMS must have been deployed (and trusted by vCenter). Review the <u>Key</u> <u>Management Server</u> section for more information.

For a complete discussion of vSAN ESA cluster creation is available in the "vSAN Proof of Concept: vSAN Architecture Overview & Setup" guide.

Example of the Configure Cluster: Advanced Options screen:

Configure cluster	Advanced options	×
1 Cluster Type	Customize the cluster settings.	
2 Distributed switches	> vSphere HA	
3 vMotion traffic	> vSphere DRS	
4 Storage traffic	Deployment type	Single site vSAN cluster $\vee$
5 Advanced options	Data-At-Rest encryption	
6 Claim disks	Key provider	Internal KMS 🗸
7 Review	Space efficiency	Storage policy managed compression $\vee$ (1)
	Fault domains	
	RDMA support	
	Auto-Policy management	
	> Host Options	
	> Enhanced vMotion Compatibility	
		CANCEL BACK NEXT

Also note that Data-in-Transit encryption can be set in parallel to Data-at-Rest during initial vSAN ESA cluster creation. More details on Data-in-Transit encryption are available in the <u>vSAN ESA Data-in-Transit Encryption section</u>.

Example of the Configure Cluster: Advanced Options screen:

Configure cluster	Advanced options	×
1 Cluster Type	Customize the cluster settings.	
2. Distributed suitables	> vSphere HA	
2 Distributed switches	> vSphere DRS	
3 vMotion traffic	✓ vSAN Options	
4 Storage traffic	Deployment type	Single site vSAN cluster $\vee$
E. Advanced on Kings	Data-At-Rest encryption	
5 Advanced options	Key provider	Internal KMS \vee
6 Claim disks	Data-In-Transit encryption	
7 Review	Space efficiency	Storage policy managed compression $ \smallsetminus   ({f J})$
	Fault domains	
	RDMA support	
	Auto-Policy management	
	> Host Options	
	> Enhanced vMotion Compatibility	
		CANCEL BACK NEXT

## Enabling vSAN Data-at-Rest Encryption - vSAN OSA

Prior to enabling vSAN OSA encryption, a KMS must have been deployed (and trusted by vCenter). Review the <u>Key</u> <u>Management Server</u> section for more information.

There are two options for enabling Data-at-Rest encryption:

- Day 0 During vSAN OSA cluster creation
- Day N Post vSAN OSA cluster creation

Encrypting the vSAN OSA cluster after cluster creation can take quite some time. Especially if the cluster is in active use. The exact time varies depending on the amount of data that needs to be migrated during the rolling reformat. If you know encryption at rest is a requirement, go ahead and enable encryption during vSAN OSA cluster creation.

## Data-at-Rest Encryption Day 0 - During vSAN OSA Cluster Creation

As with vSAN ESA, one can configure vSAN OSA cluster Data-at-Rest encryption at initial cluster creation. Specifically, during the Advanced Options step. A complete discussion of vSAN OSA cluster creation is available in the "vSAN Proof of Concept: vSAN Architecture Overview & Setup" guide.

Example of the Configure Cluster: Advanced Options screen:

Configure cluster	Advanced options	×
1 Distributed switches	Customize the cluster settings.	
	> vSphere HA	
2 VMotion traffic	> vSphere DRS	
3 Storage traffic	✓ vSAN Options	
4 Advanced options	Deployment type	Single site vSAN cluster ~
5 Claim disks	Data-At-Rest encryption	
6 Review	Key provider	Internal KMS 🗸
o neven	Data-In-Transit encryption	
	Space efficiency	None V
	Auto-Policy management	
	> Host Options	
	> Enhanced vMotion Compatibility	
		CANCEL BACK NEXT

Also note that Data-in-Transit encryption can be set in parallel to Data-at-Rest during initial vSAN ESA cluster creation as well. More details on Data-in-Transit encryption are available in the <u>vSAN OSA Data-in-Transit Encryption section</u>.

Example of the Configure Cluster: Advanced Options screen configuring Data-at-Rest and Data-in-Transit:	
---	--

Configure cluster	Advanced options Customize the cluster settings.			$\times$
1 Distributed switches 2 vMotion traffic	> vSphere HA > vSphere DRS			
.3 Storage traffic	✓ vSAN Options			
4 Advanced options	Deployment type	Single site vSAN cluster $ \sim $		
5 Claim disks	Data-At-Rest encryption Key provider	Internal KMS ~		
6 Review	Data-In-Transit encryption			
	Space efficiency	None	<u>~</u> (i)	
	Fault domains			
	RDMA support	<b>(</b> )		
	Auto-Policy management	$\bigcirc$ (i)		
	> Host Options			
	> Enhanced vMotion Compatibility			
			CANCEL BACK	NEXT

#### Data-at-Rest Encryption Day N - Post vSAN OSA Creation

To enable vSAN OSA Data-at-Rest encryption on an existing vSAN OSA cluster, navigate to [vSAN Cluster] > Configure > vSAN > Services > Data Services, then click the EDIT button that corresponds to the Data Services section. Here we have the option to erase all disks before use (Wipe residual data). This will increase the time it will take to do the rolling format of the devices, but it will provide better protection. There is also an option to speed up the process by formatting more than one disk at a time (allow reduced redundancy).

Conce officiency		
Space efficiency	Ū.	
	iny and comprosision	
	ind compression	
Encryption		
Data-At-Re	t encryption (j)	
🗌 Wipe re	sidual data 🧃	
Key provid	r Internal KMS $ \smallsetminus $	
Data-In-Tra	nsit encryption (j)	
Rekey inter	val Default v 1 day v	
	Predefined intervals	
These settings and temporarily Disk format cha	equire all disks to be reformatted. Moving large decrease the performance of the cluster. nge could fail if there are VMs with incompatible	amount of stored data might be slow storage policy.
Disk format optio	IS	
Allow reduced	redundancy 🕦	
	_	

As the example indicates, Data-in-Transit encryption can be initialized at the same time (in parallel) with Data-at-Rest or separately as required.

After you click **APPLY**, vSAN will remove one disk group at a time, format each device, and recreate the disk group once the format has completed. It will then move on to the next disk group until all disk groups are recreated, and all devices formatted and encrypted. During this period, data will be evacuated from the disk groups, so you will see components resyncing:

Recent Tasks Alarms						
Task Name 🗸	Target	$\sim$	Status ↑		$\sim$	
Create disk group on vSAN	10.156.28.144			20%	$\odot$	
Convert disk format for vSAN	🗊 vSAN			22%	$\otimes$	
Reconfigure vSAN cluster	SAN VSAN			48%	$\otimes$	
Add disks to the vSAN cluster	10.156.28.144		✓ Completed			
Update option values	10.156.28.144		✓ Completed			
Remove disk group from the vSAN cluster	10.156.28.144		✓ Completed			

## Disabling vSAN Data-at-Rest Encryption - vSAN ESA

The only method to disable Data-at-Rest encryption on vSAN ESA clusters is a full rebuild of the cluster. For more information on cleanly removing a vSAN cluster, use the steps discussed in <u>Appendix B</u>.

## Disabling vSAN Data-at-Rest Encryption - vSAN OSA

Disabling vSAN OSA Data-at-Rest encryption follows a similar procedure as its enablement. Since the encryption is done at the disk group level, a disk reformat will also be conducted while disabling encryption.

To disable vSAN encryption on a vSAN OSA cluster, navigate to [vSAN Cluster] > Configure > vSAN > Services > Data Services, then click the EDIT button that corresponds to the Data Services section. Once in the configuration pop-up screen, simply toggle Data-at-Rest encryption to off, then click Apply.



Keep in mind that vSAN OSA will conduct a rolling reformat of the devices by evacuating the disk groups first, deleting the disk group and re-creating the disk group without encryption, at which point it will be ready to host data. The same process is conducted on all remaining disk groups until the vSAN OSA datastore is no longer encrypted.

Since the disk groups are evacuated, all data will be moved within the disk groups, so it may take a considerable amount of time depending on the amount of data present on the vSAN datastore.

#### **Encryption Rekey**

You have the capability of generating new encryption keys. Both vSAN ESA and OSA support:

- Shallow Rekey High-level rekey where the data encryption key is wrapped by a new key-encryption key
- **Deep Rekey**: A complete re-encryption of all data (performing full data re-encryption may be slow and temporarily decrease the performance of the cluster)

To generate new keys, navigate to **[vSAN Cluster] > Configure > vSAN > Services > Data Services**, then click the **Generate New Encryption Keys** button that corresponds to the **Data Services** section.

The Generate New Encryption Keys pop-up screen will appear.

- The default, unchecking "Also encrypt all data on the storage using the new keys" initiates the shallow rekey process
- Checking "Also encrypt all data on the storage using the new keys" initiates the deep rekey process

Generate New Encryption Keys	×
All encryption keys on the key management server cluster are regenerated.  Also re-encrypt all data on the storage using the new keys (1)  Allow reduced redundancy (1)	
CANCEL GENERATE	E

Note: It is not possible to specify a different KMS server when selecting to generate new keys during a deep rekey; however, this option is available during a shallow rekey.

For more information on key rotation, see: <u>https://core.vmware.com/blog/key-rotation-options-vsan-esa-vmware-cloud-foundation-51-and-vsan-8-u2</u>

# vSAN Data-in-Transit Encryption

Data-in-Transit Encryption can be enabled independently or together with Data-at-Rest encryption to fully protect vSAN data. Data-in-Transit encryption uses FIPS 140-2 validated VMware VMkernel Cryptographic module. Both Data and metadata are encrypted. Unlike Data-at-Rest encryption, Data-in-Transit encryption does not require an external KMS. Keys are managed internally.

When designing Data-in-Transit encryption services for your environment, be aware that:

- vSAN uses AES-256-bit encryption on data in transit
- vSAN data-in-transit encryption is not related to data-at-rest-encryption. You can enable or disable each one separately
- Forward secrecy is enforced for vSAN data-in-transit encryption
- Traffic between data hosts and witness hosts is encrypted
- File service data traffic between the VDFS proxy and VDFS server is encrypted
- vSAN file services inter-host connections are encrypted

#### Enabling Data-in-Transit Encryption - vSAN ESA

There are two options for enabling Data-in-Transit encryption:

- Day 0 During vSAN ESA cluster creation
- Day N Any time after vSAN ESA cluster creation

#### Enabling Data-in-Transit Encryption Day 0 - During vSAN ESA Cluster Creation

Data-in-Transit encryption can be enabled during the vSAN ESA cluster creation process. Specifically, during the Advanced Options step. A complete discussion of vSAN ESA cluster creation is available in the "vSAN Proof of Concept: vSAN Architecture Overview & Setup" guide.

Example of the Configure Cluster: Advanced Options screen with Data-in-Transit encryption enabled (Note that with vSAN ESA, Data-at-Rest encryption can be deployed in parallel during cluster creation):

Configure cluster	Advanced options	×
1 Cluster Type	Customize the cluster settings.	
2. Distributed switches	> vSphere HA	
	> vSphere DRS	
3 VMotion traffic	V vSAN Options	
4 Storage traffic	Deployment type	Single site vSAN cluster $\sim$
	Data-At-Rest encryption	
5 Advanced options	Key provider	<u> </u>
6 Claim disks	Data-In-Transit encryption	
7 Review	Space efficiency	Storage policy managed compression $\sim$ (
	Fault domains	
	RDMA support	
	Auto-Policy management	
	> Host Options	
	> Enhanced vMotion Compatibility	
		CANCEL BACK NEXT

## Enabling Data-in-Transit Encryption Day N - Post vSAN ESA Cluster Creation

To enable vSAN ESA Data-at-Rest encryption on an existing vSAN ESA cluster, navigate to **[vSAN Cluster] > Configure >** vSAN > Services > Data Services, then click the EDIT button that corresponds to the Data Services section. Tick Data-in-Transit encryption and select your Rekey Interval. The default for rekey interval is one (1) day. Click Apply:

vSAN Services vSAN-ESA-Cluster	$\times$
Space efficiency (1) Storage policy managed compression	
<ul> <li>Encryption</li> <li>Data-At-Rest encryption</li> <li>Wipe residual data (1)</li> <li>Key provider </li> <li>Data-In-Transit encryption (1)</li> <li>Rekey interval Default </li> <li>1 day </li> <li>6 hours rvals</li> <li>12 hours</li> <li>1 day</li> <li>3 days</li> <li>7 days</li> </ul>	
	CANCEL

Enabling Data-in-Transit Encryption - vSAN OSA There are two options for enabling Data-in-Transit encryption:

- Day 0 During vSAN OSA cluster creation
- Day N Any time after vSAN OSA cluster creation

# Enabling Data-in-Transit Encryption Day 0 - During vSAN OSA Cluster Creation

Data-in-Transit encryption can be enabled during the vSAN OSA cluster creation process. Specifically, during the Advanced Options step. A complete discussion of vSAN OSA cluster creation is available in the "vSAN Proof of Concept: vSAN Architecture Overview & Setup" guide.

Example of the Configure Cluster: Advanced Options screen with Data-in-Transit encryption enabled (Note that with vSAN OSA, Data-at-Rest encryption can be deployed in parallel both during and post cluster creation):

Configure cluster	Advanced options		×			
1 Distributed switches	Customize the cluster settings.					
2 vMotion traffic	> vSphere DRS	> vSphere DRS				
3 Storage traffic	✓ vSAN Options					
4 Advanced options	Deployment type	Single site vSAN cluster $\sim$				
5. China diska	Data-At-Rest encryption					
5 Claim disks	Key provider	Internal KMS 🖂				
6 Review	Data-In-Transit encryption					
	Space efficiency	None 🗸 🛈				
	Fault domains					
	RDMA support	3				
	Auto-Policy management	$\bigcirc$ (1)				
	> Host Options					
	> Enhanced vMotion Compatibility					
		CANCEL BACK	NEXT			

# Enabling Data-in-Transit Encryption Day N - Post vSAN OSA Cluster Creation

To enable vSAN OSA Data-at-Rest encryption on an existing vSAN OSA cluster, navigate to [vSAN Cluster] > Configure > vSAN > Services > Data Services, then click the EDIT button that corresponds to the Data Services section. Tick Data-in-Transit encryption and select your Rekey Interval. The default for rekey interval is one day. Click Apply:



## Disabling Data-in-Transit Encryption - vSAN ESA

Disabling vSAN ESA Data-in-Transit encryption follows a similar procedure as its post cluster creation enablement.

To disable vSAN encryption on a vSAN OSA cluster, navigate to [vSAN Cluster] > Configure > vSAN > Services > Data Services, then click the EDIT button that corresponds to the Data Services section. Once in the configuration pop-up screen, simply toggle Data-in-Transit encryption to off, then click Apply.



#### Disabling Data-in-Transit Encryption - vSAN OSA

Disabling vSAN OSA Data-in-Transit encryption follows a similar procedure as its enablement.

To disable vSAN encryption on a vSAN OSA cluster, navigate to [vSAN Cluster] > Configure > vSAN > Services > Data Services, then click the EDIT button that corresponds to the Data Services section. Once in the configuration pop-up screen, simply toggle Data-in-Transit encryption to off, then click Apply:



# vSAN File Services (vSAN ESA and OSA)

The addition of vSAN File Service quickly enables NFS and SMB shares on vSAN without the need to install or manage a dedicated file service appliance. File shares can be presented to both VMs and containers. Moreover, the entire life cycle of provisioning and managing file services can be seamlessly performed through vCenter.

The data stored in a file share can be accessed from any device that has access rights. vSAN File Service is a layer that sits on top of vSAN to provide file shares. It currently supports:

- SMBv2.1 & SMBv3
- NFSv3 & NFSv4.1

The vSAN Distributed File System (vDFS) which provides the underlying scalable filesystem by aggregating:

- vSAN objects
- A Storage Services Platform that provides:
  - o Resilient file server endpoints
  - o A control plane for deployment, management, and monitoring

File shares are integrated into the existing vSAN Storage Policy Based Management on a per-share basis. vSAN file service brings in capability to host the file shares directly on the vSAN cluster.



In this section we will focus on enabling vSAN File Service, creating and mounting shares, viewing file share properties, and failure scenarios.

# **Cloud Native Use Cases**

File services in its first instance was designed to support Cloud-Native workloads. Cloud-Native workloads built on microservices architecture require data access to be concurrent. Multiple micro-services read and update the same data repository at the same time from different nodes. Updates should be serialized, with no blocking, locking, or exclusivity. This approach differs from the current offering for Cloud-Native storage on vSAN. In the current model, vSAN backed VMDKs are presented to VMs and thus mounted to a single container.

For instance, web services applications like Apache, Nginx, and Tomcat require shared file access to support distributed operations. Rather than replicating this data to every instance, a single NFS share can be mounted into all containers running these workloads. Hence file storage is critical for Cloud-Native Applications.

## Considerations

- vSAN 8.0 supports two-node configurations and stretched clusters
- vSAN 8.0 supports 64 file servers in a 64-host setup
- vSAN 8.0 supports 100 file shares
- vSAN File Services does not support the following
  - Read-Only Domain Controllers (RODC) for joining domains because the RODC cannot create machine accounts (as a security best practice, a dedicated org unit should be pre-created in the Active Directory and the username mentioned here should be controlling this organization)
  - Disjoint namespace
  - Spaces in organizational units (OUs) names
  - o Multi domain and Single Active Directory Forest environments
- When a host enters maintenance mode
  - The file server moves to another FSVM
  - The FSVM on the host that entered maintenance mode is powered off
  - After the host exits maintenance mode, the FSVM is powered on
- vSAN File Services VM (FSVM) docker internal network may overlap with the customer network without warning or reconfiguration
  - There is a known conflict issue if the specified file service network overlaps with the docker internal network (172.17.0.0/16) causings routing problems for the traffic to the correct endpoint
  - As a workaround, specify a different file service network so that it does not overlap with the docker internal network (172.17.0.0/16)

## **Pre-Requisites**

Before enabling file services, you will need the following:

- An existing vSAN HCI cluster, vSAN stretched cluster, or a vSAN ROBO cluster
- vSAN ESA and OSA is supported
- A unique IP address for each file service agent (as per best practice, this will be equal to the number of hosts in the cluster)
- DNS entries (forward and reverse lookup should be working correctly)
- Network details (subnet mask, gateway, etc.)
- Dedicated distributed switch port group (for DVS)
- MAC Learning, MAC change, unknown unicast flooding and forged frames enabled on the segment (for NSX)

In addition, you will need the following information for the cluster:

- File Services Domain A unique namespace for the cluster that will be used across shares
- DNS Servers Multiple DNS entries can be added for redundancy
- DNS Suffix
- Active Directory domain information (for SMB shares or Kerberos authentication)

Below we show an example on how to enable and configure vSAN file services.

For full details, visit:

https://docs.vmware.com/en/VMware-vSphere/8.0/vsan-administration/GUID-82565B82-C911-42F7-85B1-E9EF973EE90C.html

# Enabling File Services - vSAN ESA and OSA

vSAN file services are implemented as a set of file server agent VMs (managed by the vSphere ESX Agent Manager). Each agent is a lightweight virtual appliance running Photon OS with a containerized file server. The agent VM is deployed using an OVF file stored in vCenter.

The process to enable vSAN file services is identical across both vSAN ESA and vSAN OSA. Although the walkthrough describes the process using a vSAN ESA cluster, the steps apply equally to vSAN OSA.

For clusters using DVS, it is recommended that a new network port group be created on the distributed switch that the hosts are connected to, as vSAN file services will enable both forged transmits and promiscuous mode. In the example below, we are creating a new port group on VLAN 1002:

New Distributed Port Group	Configure settings Set general properties of the new port group.				×
1 Name and location	Port binding	Static binding $\checkmark$			
2 Configure settings	Port allocation	Elastic 🗸 (j)			
3 Ready to complete	Number of ports	8			
	Network resource pool	(default) \vee			
	VLAN				
	VLAN type	VLAN ~			
	VLAN ID	1002			
	Advanced				
	Customize default policies configuration				
			CANCEL	ВАСК	NEXT

Next, navigate to **[vSAN Cluster] > Configure > vSAN >Services.** In the list of services, we see that **File Services** is currently disabled. Begin by clicking **Enable**.

D vSAN-ESA-Clust	III VSAN-ESA-Cluster EACTIONS							
Summary Monitor Co	Summary Monitor Configure Permissions Hosts VMs Datastores Networks Updates							
Services V vSphere DRS	> Support Insight (Disabled)	vSAN ISCSI Target Service     Disabled						
vSphere Availability Configuration	ENABLE	ENABLE						
Quickstart General	> Performance Service (Enabled)	Reservations and Alerts						
Key Provider VMware EVC	EDIT	EDIT						
VM/Host Groups VM/Host Rules	V File Service (Disabled)	✓ Advanced Options						
VM Overrides I/O Filters Host Options	vSAN file service allows a vSphere admin to provision a file share from their vSAN cluster. The file share can be accessed using NFS or SMB.	Object repair timer 60 minutes Site read locality Enabled						
Host Profile	Pod 1 Pod 2	Thin swap Enabled Guest Trim/Unmap Enabled						
Licensing 🗸	VM VM VM ···	Automatic rebalance Disabled						
vSAN Cluster Trust Authority	$\neg \neg $	EDIT						
Alarm Definitions	File Share (NFS/SMB)							
Scheduled Tasks	Distributed File System	> Historical Health Service						
vSphere Cluster Services 🗸	UCANI							
General	VSAIN	2011						
Datastores								
Services								
Disk Management	ESXi ESXi ESXi							
Fault Domains								
Remote Datastores	ENABLE							
Desired State								

Next, select whether to download the File Service Agent OVF automatically or manually. In this example, "Automatically load latest OVF" as well as 'Trust the certificate' are selected.

<ul> <li>vSAN file service is supported on D are enabled as part of the vSAN file configured for the provided network</li> </ul>	VS version 6.6.0 or higher. Create a dedicated port group for vSAN file service in the DVS Promiscuous to service enablement process for provided network entity. If NSX based networks are being used, ensure k entity from the NSX admin console.	Mode and Forged Transmits that similar settings are
etwork		
Network	SELECT ~	
le service agent		
<ul> <li>Automatically load latest O</li> </ul>	VF	
Let the system download th	ie OVF from: https://download3.vmware.com/software/VSAN-FILE-SERVICES-8002/VM	ware-vSAN-File-Services-
Appliance-8.0.2.1000-2238	0479_OVF10.ovf	
The thumbprint of the certif	ficate is:	
50:FF:BE:B6:A4:89:60:82:65	5:63:00:5E:F8:6F:9C:E9:CA:6D:50:E6	
I rust the certificate		
The system will verify and	download the OVF. You can monitor the process in the task panel.	
0		
Files: BROWSE		
		CANCEL ENABL

For air-gapped environments, download the agent OVF file from the link below (ensure it corresponds to the versions of vSphere/vSAN in your environment). Then select the 'Manually load OVF option to upload the file.

Direct Download:

https://customerconnect.vmware.com/en/downloads/info/slug/datacenter\_cloud\_infrastructure/vmware\_vsan/8\_0#drivers \_tools

Next, select the port group that was created in the first step:

are enabled as part of the vSAN file service enablement pr configured for the provided network entity from the NSX a	ccess for provided network entity. If NSX based networks are being dmin console.	used, ensure that similar settings are
etwork		
Network	SELECT Y	
e service agent  Automatically load latest OVF	Q Search	]
Let the system download the OVF from: https:/	vSAN-ESA-Cluster	80U2/VMware-vSAN-File-Services
Appliance-8.0.2.1000-22380479_OVF10.ovf	🕺 VM Network	
The thumbprint of the certificate is:	Ø Management Network	
50:FF:BE:B6:A4:89:60:82:65:63:00:5E:F8:6F:9C	🕼 vsan-test-vds-VM Network (vsan-test-vds)	
Trust the certificate	🛞 vsan-test-vds-Management Network (vsan-test-v	
() The system will verify and download the OVF. You	🕼 vsan-test-vds-vSAN-3921 (vsan-test-vds)	
O Manually load OVF	🕼 vsan-test-vds-vMotion-3920 (vsan-test-vds)	
Files: BROWSE	읍 vsan-test-vds-vSAN-FileServices (vsan-test-vds)	
	•	

On clicking enable, vCenter will download the File Services OVF then deploy the agent VMs. A new resource pool named 'ESX Agents' will be created, and the stored OVF deployed and cloned:

ACTIONS	5	
Configure	Permissions Res	esource Pools VMs
Tasks		
EXPORT ¥	COPY TO CLIPBOARD	FILTER
	Task Name 🔻	Target <b>y</b> Status <b>y</b> Details <b>y</b> Ini
U ~	Deploy OVF template	(j) <u>vSAN File Service Nod</u> 46% (⊗ co
	Task Name	Deploy OVF template
	Status Initiator	46% ⊗ Q com.vmware.vim.eam
	Target	<u>VSAN File Service Node (1)</u>
	Server Related events:	😥 <u>vsan-test-vc.colinlab.vsanpe.vmware.com</u>
	Date Time	Description
	02/02/2024, 4:01:07 PM	PM Created virtual machine <u>vSAN File Service Node (1)</u> on <u>10.156.130.219</u> , in <u>vsan-test-dc</u>
	02/02/2024, 4:01:07 PM	PM New MAC address (00:50:56:87:42:df) assigned to adapter 50 07 0f 57 9d 9f 68 5f-c6 00 28 53 e7 78 53 20 for <u>vSAN File Service Node (1)</u>
	02/02/2024, 4:01:07 PM	PM Assigned new BIOS UUID (4207163b-0429-7e95-7d64- 36f26087316f) to <u>vSAN File Service Node (1)</u> on <u>10.156.130.219 in vsan-test-dc</u>
	02/02/2024, 4:01:07 PM	PM Assign a new instance UUID (50076591-3276-68e3- d1f2-89c259fc7ed7) to <u>vSAN File Service Node (1)</u>
	02/02/2024, 4:01:07 PM	PM Creating <u>vSAN File Service Node (1) on 10.156.130.219</u> , in <u>vsan-test-dc</u>
	02/02/2024, 4:01:06 PM	PM Task: Deploy OVF template
	Configure	Configure       Permissions       Ref         Tasks       COPY TO CLIPBOARD         □       Task Name       T         □       O2/02/2024, 4:01:07       O2/02/2024, 4:01:07         02/02/2024, 4:01:07       O2/02/2024, 4:01:07       O2/02/2024, 4:01:07         02/02/2024, 4:01:07       O2/02/2024, 4:01:07       O2/02/2024, 4:01:07

Once this process has finished, the service VMs will be visible in the inventory view:

<ul> <li>Image: Construction of the second of the sec</li></ul>	O ESX Agents       : ACTIONS         Summary       Monitor       Configure       I         Virtual Machines       VM Templates         Quick Filter         Enter value	Permissions Resource vApps	ce Pools VMs			
10.156.130.218	Name ·	State State	tus Provisioned Space	Used Space	Host CPU	Host Mem
10.156.130.219	SAN File Service Node (1)	Powered O 🗸	Normal 71.33 GB	1.25 MB	0 Hz	0 B
10.156.130.220	🔲 🗄 📅 <u>vSAN File Service Node (2)</u>	Powered O 🗸	Normal 71.33 GB	1.25 MB	0 Hz	44 MB
v G ESX Agents が vSAN File Service Node (1)	SAN File Service Node (3)	Powered O 🗸	Normal 71.33 GB	1.25 MB	0 Hz	44 MB
舒 vSAN File Service Node (2) 舒 vSAN File Service Node (3)	SAN File Service Node (4)	Powered O 🗸	Normal 71.33 GB	1.25 MB	0 Hz	62 MB
🗊 vSAN File Service Node (4)						

The file service agent VMs will use a customized storage policy "FSVM\_Profile\_DO\_NOT\_MODIFY". As the name suggests, do not modify this policy (or assign a different policy to the file service VM).

The next step is to create a file service domain. Navigate again to [vSAN cluster] > Configure > vSAN > Services > File Service and click on CONFIGURE DOMAIN:

D vSAN-ESA-Cluste									
Summary Monitor Cor	nfigure Permissions Hosts VMs Dat	astores Networks Updates							
Services 🗸	vSAN Services					SHUTDOWN CLUSTER	TURN OFF VSAN		
vSphere DRS vSphere Availability	> Storage			> Data Services					
Configuration >	EDIT			EDIT GENERATE NEW ENCRYPTION KEYS					
Trust Authority	> Support Insight	Disable	ed	> vSAN iSCSI Target Service			Disabled		
Scheduled Tasks	ENABLE			ENABLE					
vSphere Cluster Services > General	> Performance Service	Enable	ed	> Reservations and Alerts					
vSAN ~	EDIT			EDIT					
Services Disk Management	✓ File Service	Domain not configure	ed	✓ Advanced Options					
File Shares Remote Datastores	Pile service is enabled. In order to be able to create file  Network	shares, the file service domain must be configured.		Object repair timer Site read locality	60 minutes Enabled				
Desired State V Image	Version	Last upgrade: 02/02/2024, 4:02:56 PM; OVF file version: 8.0.2.1000-22380479		Thin swap Guest Trim/Unmap Automatic rebalance	Enabled Enabled Disabled				
Configuration	EDITY	CONFIGURE DOMAI	IN	EDIT					

Name the domain. In this example, we have chosen the name 'vSAN-fs-cluster1':

File service domain	File service domain					
1 File service domain	File service domain vSAN-fs-cluster1 A vSAN file service domain is a unique namespace for nei and security configuration for managing a list of file share	twork				
2 Networking	Checklist The following information is needed to configure file service.					
3 Directory service	<ul> <li>Static IP address, subnet masks and gateway for file servers</li> <li>DNS name for each IP address or allow the system to do a reverse DN</li> </ul>	NS lookup.				
4 Review	For SMB share and NFS share with Kerberos Security, the following info needed. • AD domain, organizational unit (optional), and a user account with suf delegated permissions.	rmation is				
	CANCEL	NEXT				

On the next screen, enter the networking details (DNS server, suffix, gateway, etc.) and the IP addresses that will be used by the vSAN file service. For consecutive addresses, use **AUTOFILL** option to save on typing. Once the IP addresses have been specified, click on **LOOKUP DNS** to ensure that vCenter can resolve the addresses:

File service domain	Networking	×
1 File service domain	Protocol	IPv4 ~
	DNS servers	10.156.128.10
2 Networking		IP address of the DNS server, which is used to resolve the host names within the DNS domain. Add multiple DNS servers by separating them by comma.
2. Directory convice	DNS suffixes	vsanpe.vmware.com
S Directory service		The list of DNS suffixes, which can be resolved by the DNS servers. Provide exhaustive list of all DNS domains and subdomains from where clients can access the file shares. Add multiple DNS suffixes by separating them by comma.
4 Review	Subnet mask	255.255.248.0
	Gateway	10.156.183.253
	For best operation, add the	same number of IP addresses as the number of hosts in the cluster. file service domain through the primary IP address or DNS name. If necessary, NFS v4.1 referral is to other IP addresses automatically.
	Primary IP address (i)	AUTOFILL DNS name (i) LOOKUP DNS
	10.156.179.1	db-fs1.vsanpe.vmware.com
	0 10.156.179.2	db-fs2.vsanpe.vmware.com
	0 10.156.179.3	db-fs3.vsanpe.vmware.com
	0 10.156.179.4	db-fs4.vsanpe.vmware.com
		CANCEL BACK NEXT

On the next screen, click to enable Active Directory services, if required. Again, this is needed for SMB shares or Kerberos authentication with NFS:

File service domain	Directory service $ imes$
1 File service domain	Directory service (i) Active directory
2 Networking	Active directory configuration is required by SMB shares or NFS shares with Kerberos
3 Directory service	authentication within the file service domain. In
4 Review	can only have NFS shares with AUTH_SYS.
	CANCEL BACK NEXT

Click Review and finally Finish on the next screens. If all is well, vCenter will then proceed to enable the vSAN file service.

# Creating a File Share

Once file services are enabled navigate to [vSAN Cluster] > Configuration > vSAN > File Shares and click on ADD:

I VSAN-ESA-Cluster										
Summary Monitor	Con	figure	Permissions	Hosts	VMs	Datastores	Networks	Updates		
Services	>	File Sh	ares							
Configuration	>	File se	ervice domain: vS	AN-fs-clus	ter1					
Licensing	>	ADD								
Trust Authority				Name				т	Deployment type	
Scheduled Tasks										
vSphere Cluster Service	s∨									
General										
Datastores										
vSAN	~									
Services										
Disk Management										
Fault Domains										
Remote Datastores										

In this example, we are creating an NFS share called 'app-share' with the vSAN default storage policy. We have set a 90GB warning for space usage, with a hard quota of 100GB. Additionally, we have created a label 'mac-open-source' with the key of 'applications':

Create File Share	General				×
	Name	app-share			
1 General	Protocol	NFS	~		
2 Net access control		Enable active directo SMB protocol.	ory configuration in the file service confi	iguration before using	
3 Review	Versions	NFS 4.1 and NFS	3	~	
	Security mode	AUTH_SYS			
		Enable active directo Kerberos authentica	ory configuration in the file service confi tion.	iguration before using	
	Storage policy	vSAN-ESA-Clust	er - Optimal Datastore Default Po	olicy - RAID5 🗸 🗸	
	Storage space quotas				
	Share warning threshold	90	GB ~		
	Share hard quota	100	GB 🗸		
	Labels (j)	"key"	"value"	ADD	
		applications (ma	c-open-source ×		
				CANCEL	NEXT

On the next screen we have a defined specific range of read-only clients (here we have defined a subnet, but a range of IP addresses could also be used):

Create file share	Net access control		×								
1 General	<ul> <li>No access</li> <li>Allow access from any IP</li> </ul>										
2 Net access control • Customize net access											
3 Review	<ol> <li>The rules are honored from top to both specific ones. You can use "*" to denot</li> <li>IP set/subnet</li> <li>10.156.128.0/24</li> <li></li></ol>	tom. Top rules override bottom ones. Put more general rules below the te "any other IP addresses not mentioned above".           Permission         Squash option           Readonly									

Click **Review** and **Finish** to create the share. Once vCenter has created to file share, it will be displayed in the File Services Shares:

) (]) vSAN-ESA-C	(I) VSAN-ESA-Cluster : ACTIONS											
Summary Monitor Configure Permissions Hosts VMs Datastores Networks Updates												
Services	>	File Shares										
Configuration	>	File service domain: vSAN-fs-cluster1	ile service domain: vSAN-fs-cluster1									
Licensing	>	ADD										
Trust Authority Alarm Definitions		Name       V       Deployment type       Protocol       V       Storage Policy       Usage/Quoti       Actual Usage/Quoti	ige									
Scheduled Tasks		🗌 🖻 🗈 app-share vSAN File Sha NFS 4.1 and NFS 🥫 vSAN-ESA-Cluster - Optimal Datastore Default Policy - RAID5 🗾 0% 0.00 B										
vSphere Cluster Service	\$ >											
vSAN	~											
Services												
Disk Management												
Fault Domains												
File Shares												
Remote Datastores												

After the share has been created any quota, labels or network permissions can be made by selecting the file share and selecting **EDIT**.

) (]) vSAN-ESA-C	uste	er	ACT	IONS									
Summary Monitor	Summary Monitor Configure Permissions Hosts VMs Datastores Networks Updates												
Services	>	File S	hares	5									
Configuration	>	File	File service domain: vSAN-fs-cluster1										
Licensing	>	ADD	EDIT	DELETE	SNAPSHOTS	COPY PATH ~							
Trust Authority Alarm Definitions		~		Name		Ŧ	Deployment type	Protocol T	Storage Policy		Usage/Quoti	Actual Usage	
Scheduled Tasks			Ð	app-share			vSAN File Sha	NFS 4.1 and NFS	🗟 vSAN-ESA-Cluster - Op	timal Datastore Default Policy - RAID5	0%	0.00 B	
vSphere Cluster Service	5>												
VSAN	~												
Services													
Disk Management													
Fault Domains													
File Shares													
Remote Datastores													

# Mounting a File Share

First, obtain the path of the share by navigating to [vSAN Cluster] > Configure > vSAN > File Shares. Select the appropriate file share and click on COPY PATH:

CII VSAN-ESA-Clust     Summary Monitor Ci	ter ACTIONS	As Datastores	Networks	Updates			
			- Hethorito	opdates			
Services >	File Shares						
Configuration >	File service domain: vSAN-fs-cluster1						
Licensing >	ADD EDIT DELETE SNAPSHOTS	COPY PATH ~					
Trust Authority	Name .	NES 3	Deployment type	Drotocol -	Starson Delinu	Usage/Oust	A stual Usage
Alarm Definitions	Name	1100	Deployment type	Protocol T	Storage Policy	Usage/Guota	Actual Usage
Scheduled Tasks	🗹 🖃 🗈 app-share	NFS 4.1	vSAN File Sha	NFS 4.1 and NFS	😡 vSAN-ESA-Cluster - Optimal Datastore Default Policy - RAID5	0%	0.00 B
vSphere Cluster Services >							
vSAN 🗸							
Services							
Disk Management							
Fault Domains							
File Shares							
Remote Datastores							

We can then mount the share as desired, for instance:

```
$ mount db-fs1.vsanpe.vmware.com:/vsanfs/app-share /mnt/app-share
```

#### **Quotas and Health Events**

During file share creation, quotas and hard limits can be set. In this sample file share, a warning threshold of 90 GB was specified and a hard limit of 100GB was set. As part of this test copy some data to the file share to fill the space required to trigger the quota. Once the warning threshold is exceeded the Usage over the Quota field in the UI will turn red.



Once the hard quota is reached writes to the share will fail with a disk quota exceeded error as shown below.

```
cp: error writing 'file13.txt': Disk quota exceeded
```

If the quota is reached an alarm in Skyline Health is also triggered. The details of the alarm can be viewed by expanding the Share Health finding.

VSAN-ESA-Cl	uster	ACTIONS														
Summary Monitor	Confi	gure Permissions	Hosts	VMs	Datastores	Networks	Updates									
Issues and Alarms	>				100											
Performance	Ś	60			100											
Tasks and Events	(		80	score												
vSphore DDS		⊘97	100	fealth	98											
vsphere DRS	2	Unhealthy	Healthy	-												
Vsphere HA	2				2/04, 11:47	2/04,	2/04,	2/04,	2/04,	2/04,	2/05,	2/05,	2/05,	2/05,	2/05,	2/05, 2/05, 10:00 11:20
Resource Allocation	>					14.00	10.00	10.00	20.00	22.00	24.00	02.00	04.00	00.00	00.00	10.00 11.20
Storage Overview				VIEW	DETAILS											
Security																
vSphere Cluster Services	\$}	lealth findings														88
vSAN	~	UNHEALTHY (1) HEAL	THY (55)	INFO (2)	SILENCED (2)										Sort by	Root cause      V
Skyline Health		Finding														
Resyncing Objects		: 🔣 Share Health	ı				4	Share Health								Score impact
Proactive Tests							Occ	urred on: Feb 5,	2024, 11:20:14 AM	1						
Capacity							Cat	egory: File Servic	е							
Performance Diagnosti	cs						Imp	act area: Compli	ance							
Support							Des	cription: Check if	the file service s	hare is in good	state.					
Data Migration Pre-che	ck						Risi	if no action taken	Check AskVM	ware for more o	details.					
Cloud Native Storage	~															
Container volumes																
		1-1/1				< 1	>		EW HISTORY DET	AILS						SILENCE ALERT
		1-1/1				< 1	>		EW HISTORY DET	AILS						SILENCE ALERT
) 🕼 vsan-esa-cli	uster	1-1/1	_	-		< 1	>	ROUBLESHOOT	EW HISTORY DET	AILS						SILENCE ALERT
) ((b) VSAN-ESA-Clu Summary Monitor	uster	11/1 ACTIONS gure Permissions	Hosts	VMs	Datastores	< 1 Networks	> T	ROUBLESHOOT	EW HISTORY DET	AILS						SILENCE ALERT
Ith VSAN-ESA-Clt     Summary Monitor     Issues and Alarms	uster Config	11/1 ACTIONS gure Permissions kyline Health	Hosts	VMs	Datastores	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	AILS						SILENCE ALERT
Clim VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance	uster Config	H/1 ACTIONS gure Permissions kyline Health VERVIEW > SHARE H	Hosts	VMs	Datastores	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	AILS						SILENCE ALERT
(1) VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance     Tasks and Events	Config S S Config	H/1 ACTIONS gure Permissions kyline Health IVERVIEW > SHARE H TROUBLESHOOT HIST	Hosts IEALTH DRY DETAILS	VMs	Datastores	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	NILS						SILENCE ALERT
(1) VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     visiblere DPS	Config > s	H/1 ACTIONS gure Permissions kyline Health IVERVIEW > SHARE H TROUBLESHOOT HIST Unnealthy	Hosts REALTH ORY DETAILS	VMs	Datastores	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	AILS						SILENCE ALERT
VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA	Config > S > Config	H/1 ACTIONS gure Permissions kyline Health IVERVIEW > SHARE H TROUBLESHOOT HIST Unnealthy Sed capacity of this shall	Hosts IEALTH ORY DETAILS	VMs	Datastores	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	AILS						SILENCE ALERT
Company Monitor      Summary Monitor      Issues and Alarms      Performance      Tasks and Events      vSphere DRS      vSphere HA      Descurse Allocation	config > S > Config	H/1 ACTIONS gure Permissions kyline Health VERVIEW > SHARE H TROUBLESHOOT HIST Unnealthy sed capacity of this shau > Why is this issue occur	Hosts IEALTH ORY DETAILS re exceeds t	VMs	Datastores	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	AILS						SILENCE ALERT
(Marking Schemer 2014)     (Marking Schemer	Config Config S Config Config Config	H/1 ACTIONS gure Permissions kyline Health VERVIEW > SHARE H TROUBLESHOOT HIST UDREATRY Sed capacity of this sha VMy is this issue occu Used capacity of thi	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce	VMs the soft of eeds the	Datastores uota soft quota.	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	MLS						SILENCE ALERT
Clim VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview	Config Config S Config Config Config	H/1  ACTIONS  gure Permissions kyline Health VERVIEW > SHARE H TROUBLESHOOT HIST UDREADTY Sed capacity of this sha VM'y is this issue occu Used capacity of thi	Hosts IEALTH DRY DETAILS re exceeds t irring? is share exce and fix?	VMs the soft of eeds the	Datastores uota	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	MLS						SILENCE ALERT
Kimmary Monitor     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security	Config S S Config S Config S Config Config Config S Config C	H/1  ACTIONS  gure Permissions kyline Health VERVIEW > SHARE H  TROUBLESHOOT HIST UDREATHY Sed capacity of this sha VM'y is this issue occu Used capacity of thi Share Health	Hosts IEALTH ORY DETAILS re exceeds t rring? is share exce and fix?	VMs the soft of eeds the	Datastores uota	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	MLS						SILENCE ALERT
Kimmary Monitor     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services	uster Config S Config S C Config S C C C C C C C C C C C C C	H/1  Construction  Actions  Ac	Hosts IEALTH DRY DETAILS re exceeds t irring? Is share exce and fix?	VMs the soft of eeds the	Datastores uota	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	MLS		Spare has	- Dh			SILENCE ALERT
Key VSAN-ESA-Clu Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSAN	uster Config S Config Config Config	H/1  Construction  Actions  Ac	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores uota	< 1 Networks	Updates	ROUBLESHOOT	EW HISTORY DET	MLS		Share hea	- th			SILENCE ALERT
Kimmary Monitor     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSA     Skyline Health     Virtual Objects	uster Config S Config	H/1  Control C	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores uota soft quota.	< 1 Networks	Updates S a	ROUBLESHOOT V	EW HISTORY DET	MLS		Share hea	10h			SILENCE ALERT
Kim VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSAN     Skyline Heastth     Virtual Objects     Resyncing Objects	Configuration S	H/1  Control C	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores uota	< 1 Networks	Updates S a	ROUBLESHOOT V		MLS		Share hea	th			SILENCE ALERT
Kimmary Monitor     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSAN     Skyline Health     Virtual Objects     Resyncing Objects     Proactive Tests	uster config > Config >	H/1  Control C	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores uota soft quota.	< 1 Networks	Updates s a	ROUBLESHOOT V				Share hea	10h			SILENCE ALERT
Kimmary Monitor     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSAN     Skyline Heastth     Virtual Objects     Resyncing Objects     Proactive Tests     Capacity     Performance	uster config > config >	H/1  Control C	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores uota soft quota.	< 1 Networks	Updates s a	ROUBLESHOOT V				Share hea	th			SILENCE ALERT
Kimmary Monitor     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSAN     Skyline Health     Virtual Objects     Proactive Tests     Capacity     Performance     Performance     Deprocemance	uster Config > Config >	H/1  Control C	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores uota soft quota.	< 1 Networks	Updates S	NOUBLESHOOT N				Share hea	th			SILENCE ALERT
Kimmary Monitor     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSA     Skyline Health     Virtual Objects     Resyncing Objects     Proactive Tests     Capacity     Performance     Performance     Performance     Performance     Diagnostic     Support	uster Config > S Config > Config > Config	H/1  Control C	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores	< 1 Networks	Updates S	NOUBLESHOOT V				Share hea	th			SILENCE ALERT
VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSAN     Skyline Health     Virtual Objects     Proactive Tests     Capacity     Performance     Performance     Diagnostic     Support     Data Migration Pre-chee	Luster Config S Config Con	H/1  ACTIONS  gure Permissions kyline Health VERVIEW > SHARE H  TROUBLESHOOT HIST Unnealth Used capacity of this shaa VMY is this Issue occu Used capacity of this shaa VMY is this Issue occu Used capacity of thi Share Health Domain VSAN-fs-cluster1 Diagnose the issue: Navigate to File Sha Recommendation to	Hosts IEALTH ORY DETAILS re exceeds t irring? is share exce and fix?	VMs	Datastores	< 1 Networks	Updates S	NOUBLESHOOT N				Share hea	th .			SILENCE ALERT
VSAN-ESA-Clu     Summary Monitor     Issues and Alarms     Performance     Tasks and Events     vSphere DRS     vSphere HA     Resource Allocation     Utilization     Storage Overview     Security     vSphere Cluster Services     vSAN     Skyline Health     Virtual Objects     Resyncing Objects     Performance Diagnostic     Support     Data Migration Pre-chec     Cloud Native Storage     Constitute Values	uster Confis S Confis Co	H/1  ACTIONS  pure Permissions kyline Health VERVIEW > SHARE H  TROUBLESHOOT HIST Unestity Sed capacity of this sha VM'y is this issue occu Used capacity of this sha VM'y is this issue occu Used capacity of thi Share Health Domain VSAN-fs-cluster1 Diagnose the issue: Navigate to File Sha Recommendation to DEFAULT 0 File Sha	Hosts IEALTH ORY DETAILS re exceeds the rring? is share exceeds and fix?	VMs	Datastores	< 1 Networks	Updates	NOUBLESHOOT N				Share hea	th .			SILENCE ALERT

Once data has been removed from the Share Health alert is cleared and the File Service health reports as normal.

# **Failure Scenarios**

Storage policies apply to file service objects just as they do other virtual disk objects. Health and placement details of file shares are shown in the **Virtual Objects** view.

> (I) vSAN-ESA-C	D VSAN-ESA-Cluster											
Summary Monitor	Summary Monitor Configure Permissions Hosts VMs Datastores Networks Updates											
Issues and Alarms	Issues and Alarms > Virtual Objects											
Performance	>	Browse all virtual objects and check their state in real time and view their placement across the physical infrastructure. Get information about each object state and common remediation. About vSAN Object Health 👩										
Tasks and Events	>	VIEW PLACEMENT DETAILS VIEW PERFORMANCE VIEW FILE SHARE CLEAR FILTERS										
vSphere DRS	>			Name T	Туре т	Object State	Storage Policy T	UUID T				
vSphere HA	>	>		@ ubuntu02	VM	Healthy	SAN-ESA-Cluster - Optimal Datastore					
Resource Allocation	>	>		🔀 vCLS-6b82996a-c8ae-4b5c-bb20-7f51	VM	Healthy	😰 vSAN-ESA-Cluster - Optimal Datastore					
Utilization		>		@ vCLS-955a74fd-105c-4f0a-9fbb-7423f	VM	Healthy	😨 vSAN-ESA-Cluster - Optimal Datastore					
Security		>		@ vCLS-b4ce388e-f905-47f1-9b1b-cb53d	VM	Healthy	😥 vSAN-ESA-Cluster - Optimal Datastore					
vSphere Cluster Service	es >	>		🗇 vSAN File Service Node (1)	VM	Healthy	FSVM_Profile_DO_NOT_MODIFY					
vSAN	~	>		🗇 vSAN File Service Node (2)	VM	Healthy	FSVM_Profile_DO_NOT_MODIFY					
Skyline Health		>		vSAN File Service Node (3)	VM	Healthy	FSVM_Profile_DO_NOT_MODIFY					
Resyncing Objects		>		🗑 vSAN File Service Node (4)	VM	Healthy	E FSVM_Profile_DO_NOT_MODIFY					
Proactive Tests		~		🗅 app-share	File share							
Capacity Performance				File Share	File share object	Healthy	R vSAN-ESA-Cluster - Optimal Datastore	c185bd65-9cfc-53eb-22cd-ac1f6b549e30				

By clicking **VIEW PLACEMENT DETAILS** the layout of the underlying vSAN object can be viewed. This view shows component status, and on which hosts components of the share reside.

Group components by host placeme	ent				
tual Object Components					
Гуре	Component State	Host	Fault Domain	Disk	
✓ 🗅 app-share > File Share (Cor	ncatenation)				
V RAID 1					
Component	Active	10.156.130.217		E Local NVMe Disk (t10.NVMe	
Component	Active	10.156.130.220		E Local NVMe Disk (t10.NVMe	
V RAID 5					
V RAID 0					
Component	Active	10.156.130.217		E Local NVMe Disk (t10.NVMe	
Component	Active	10.156.130.217		E Local NVMe Disk (t10.NVMe	
V RAID 0					
Component	Active	10.156.130.219		E Local NVMe Disk (t10.NVMe	
		_			Þ
			32 vSAN con	nponents on 4 hosts I < 1 / 3	>

To test host failure, we will power off one of the hosts containing an active copy of the file share data. Once the host is powered off, we see that the component of the corresponding host is displayed as absent.

There are connectivity issues in the system.	this cluster. One or more hosts are a	unable to communicate with	the vSAN datastore. Da	ata below does not reflect the real state of
] Group components by host placer	ment			
rtual Object Components				
Туре	Component State	Host	Fault Domain	Disk
✓ □ app-share > File Share (Control of the state)	oncatenation)			
V RAID 1				
V RAID_D				
Component	🛕 Absent	Object not found		52913651-2472-8df5-f3b8-650a0543512e
Component	Active	10.156.130.219		톱 Local NVMe Disk (t10.NVMeINTE
Component	Active	10.156.130.220		튼 Local NVMe Disk (t10.NVMeINTE
V RAID 5				
V RAID 0				
				_
			39 vSAN	components on 4 hosts $ \zeta \langle 1   / 4 \rangle$

Now that the host has been shut down, you can validate from any of the client virtual machines through a file browser or logs to verify that file share is still accessible.

When ready power the host back on.

# File Services Snapshots

vSAN includes a new snapshotting mechanism allowing for point-in-time recovery of files. Snapshots for file shares can be created through the UI. Recovery of files is available through API allowing backup partners to extend current backup platforms to protect vSAN file shares.

VSAN-ESA-Cluster									
Summary Monite	or Co	onfigure Permissions	Hosts VMs	Datastores	Networks	Updat	es		
Services	>	File Shares							
Configuration	>	File service domain: vS	AN-fs-cluster1						
Licensing	>	ADD EDIT DELETE	SNAPSHOTS C	OPY PATH ~					
Trust Authority Alarm Definitions		Name		τ [	Deployment ty	🖻 app-s	share		
Scheduled Tasks		🔽 📄 🗈 app-sha	re	١	/SAN File Sh	Basics	Physical Placement	Performance	Snapshots
vSphere Cluster Ser	vices >					NEW SNAF	рянот		
vSAN	~					□ Sn	apshot name		
Services									
Disk Management									
Fault Domains									
File Shares									
Remote Datastore	?S								

# File Services Support for Stretched Clusters and Two Node Topologies

File services can now be used in vSAN stretched clusters and two node topologies. The site affinity setting for file shares defines where the presentation layer resides. Site affinity for file shares is defined by the storage policy associated with the individual file shares. The storage policy and site affinity settings to be applied to the file share are defined as part of the creation process.

The image below is an example of the site affinity setting available when creating a file share in a stretched cluster.

Create file share	General		×
1 General	Name	Imaging	
	Protocol	SMB ~	
2 Review	Protocol encryption		
	Storage policy	vSAN Default Storage Policy ~	
	Affinity site (1)	V Preferred (Preferred) Secondary (Secondary) Either	
	Storage space quotas		
	Share warning threshold	1 TB ~	
	Share hard quota	2 TB ~	
	Labels (1)	"key" "value" ADD	
		department (maging X) site (Raleigh X)	
		CANCEL	NEXT

# vSAN Support for Kubernetes

vSAN fully supports native VMware Tanzu® as well as 'vanilla' Kubernetes clusters.

In VMware Tanzu deployments, vSAN natively provides both block and file storage services to persistent volumes (PV).

For more information on leveraging vSAN within VMware Tanzu, please refer to:

- vSphere with Tanzu Planning Guide- <u>https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-with-tanzu-concepts-planning/GUID-E297DD43-AEEB-4B6D-8C93-4212CA62309A.html#GUID-E297DD43-AEEB-4B6D-8C93-4212CA62309A
  </u>
- vSphere with Tanzu Installation Guide <u>https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-with-tanzu-installation-configuration/GUID-B09BFD99-DF1F-4831-BBA5-BAA78580AB47.html</u>
- Tanzu Proof of Concept Guide https://core.vmware.com/resource/tanzu-proof-concept-guide

For native Kubernetes deployments (non-Tanzu), Cloud-Native Storage (CNS), offers a platform for stateful cloud-native applications to persist state on vSphere backed storage. The platform allows users to deploy and manage containerized applications using cloud-native constructs such as Kubernetes persistent volume claims and maps these to native vSphere constructs such as storage policies. CNS integrates with vSphere workflows and offers the ability for administrators to perform tasks such as defining storage policies that could be mapped to storage classes, list/search and monitor health and capacity for PVs.

For more information on CNS, please refer to:

- vSphere Container Storage Plug-in Documentation Main Page <u>- https://docs.vmware.com/en/VMware-vSphere-</u> <u>Container-Storage-Plug-in/index.html</u>
- Getting Started with VMware vSphere Container Storage Plug <u>https://docs.vmware.com/en/VMware-vSphere-Container-Storage-Plug-in/3.0/vmware-vsphere-csp-getting-started/GUID-74AF02D7-1562-48BD-A9FE-C81A53342AC3.html</u>
- vSphere CSI Driver GitHub <u>https://github.com/kubernetes-sigs/vsphere-csi-driver</u>
## **APPENDIX A: Creating Test VMs**

Here we demonstrate how to quickly create a set of identical VMs for testing.

## **Requirements:**

- FreeBSD, Linux or MacOS VM/host environment
- Latest version of govc (download instructions below)

## Download govc:

Govc is a lightweight, open-source CLI tool written in Go (and part of the Govmomi/Go library for the vSphere API). Project page: https://github.com/vmware/govmomi/tree/master/govc

### To download the latest release, use the command below, or visit the release page:

https://github.com/vmware/govmomi/releases

As with the majority of Go projects, it is packaged as a single binary (note that the tar command requires root privileges to copy the binary to the correct location):

```
curl -L -o - "https://github.com/vmware/govmomi/releases/latest/download/govc_$(uname -s)_$(uname -
m).tar.gz" | tar -C /usr/local/bin -xvzf - govc
```

## Connecting to vCenter

To authenticate with vCenter, we need to define the username, password and URL, as per the example below:

```
export GOVC_USERNAME=administrator@vsphere.local
export GOVC_PASSWORD=P@ssw0rd
export GOVC_INSECURE=1
export GOVC_URL=10.156.163.1
```

Additionally, we will need to specify the default datastore and resource pool (we can define this as the default/top-level cluster, as per blow) for deploying our VMs:

```
export GOVC_DATASTORE=ESA-vsanDatastore
export GOVC_RESOURCE_POOL='vSAN_ESA_Cluster/Resources'
```

Finally test the connection to vCenter by issuing the command below, it should return with details:

```
govc about
FullName: VMware vCenter Server 8.0.0 build-20519528
Name: VMware vCenter Server
Vendor: VMware, Inc.
Version: 8.0.0
Build: 20519528
...
```

## Configure Test VM

First, specify a location of an OVA file to use. In the example below, we use an Ubuntu 22.04 cloud image:

export vmLocation=https://cloud-images.ubuntu.com/releases/22.04/release/ubuntu-22.04-servercloudimg-amd64.ova

We can then add our customizations, etc. by extracting the JSON from the OVA:

govc import.spec \$vmLocation > ubuntu-vm.json

Ubuntu uses cloud-init to setup the OS environment. As we will be cloning the deployed VM, we need to define specific userdata (which will be encoded in base-64 and added to the customization JSON). Here we ensure that vSphere specific configuration is not disabled, and we modify the default netplan configuration file to ensure DHCP addresses are assigned by mac address (rather than machine-id).

To simplify the process, the user-data file can be downloaded from the link below: https://raw.githubusercontent.com/vmware-tanzu-experiments/vsphere-with-tanzu-proof-of-conceptsamples/main/VCF/test\_vms/user-data

```
#cloud-config
runcmd:
    - 'echo "disable_vmware_customization: false" >> /etc/cloud/cloud.cfg'
    - echo -n > /etc/machine-id
    - |
      sed -i '' -e 's/match.*/dhcp-identifier: mac/g' -e '/mac/q' /etc/netplan/50-cloud-init.yaml
final_message: "The system is prepped, after $UPTIME seconds"
power_state:
    timeout: 30
    mode: poweroff
```

If available, use the cloud-init CLI to check the user-data file:

```
$ cloud-init schema --config-file user-data
```

Next, we encode the user-data to base64:

```
base64 -i user-data
```

Now we can edit the JSON file we extracted earlier. Change the file with the following:

- Disk provisioning set to 'thin'
- Add the public key of the machine we are connecting from
- Remove the hostname and password data
- Set the network for the VM (the name of the relevant portgroup in vCenter)

- Set the name of the VM
- In the 'user-data' section, paste in the base64 encoded data

Note we can avoid hand-editing the JSON by using jq. For example, we can update the user-data field directly in the JSON file:

```
jq 'select(.Key=="user-data").Value="$(base64 -i user-data)"' ubuntu-vm.json
```

Similarly, adding a public key stored in a user's GitHub profile:

```
jq 'select(.Key=="public-keys").Value="$(curl -sk https://api.github.com/users/[github user]/keys |
jq -r '.[].key')"' ubuntu-v.json
```

An example of this file can be seen here: <u>https://raw.githubusercontent.com/vmware-tanzu-experiments/vsphere-with-tanzu-proof-of-concept-</u> <u>samples/main/VCF/test\_vms/ubuntu-vm.json</u>

```
{
 "DiskProvisioning": "thin",
 "IPAllocationPolicy": "dhcpPolicy",
 "IPProtocol": "IPv4",
 "PropertyMapping": [
   {
      "Key": "instance-id",
      "Value": "id-ovf"
   },
   {
      "Key": "hostname",
      "Value": ""
   },
    {
      "Key": "seedfrom",
      "Value": ""
   },
    {
      "Key": "public-keys",
      "Value": "ssh-rsa AAAAB3NzaC1yc2EAAAAD..."
    },
    {
      "Key": "user-data",
      "Value": "I2Nsb3VkLWNvbmZpZwpy..."
   },
   {
     "Key": "password",
      "Value": ""
   }
 ],
 "NetworkMapping": [
   {
      "Name": "VM Network",
      "Network": "DSwitch-DHCP"
   }
 ],
```

```
"MarkAsTemplate": false,
"PowerOn": false,
"InjectOvfEnv": false,
"WaitForIP": false,
"Name": "ubuntu-vm"
```

}

Once this JSON file has been defined, we can double-check our user-data encoding is still correct:

awk -F '"' '/user-data/{getline; print \$4}' ubuntu-vm.json | base64 -d

This should return the user-data as we defined above.

### Import OVA to vCenter and Clone

We can then import the OVA into vCenter, specifying our JSON customization file:

govc import.ova -options=ubuntu-vm.json -name=ubuntu-template \$vmLocation

After this has imported, we can update the virtual disk size. Here we set it to 100G:

govc vm.disk.change -vm ubuntu-template -disk.label "Hard disk 1" -size 100G

Power on the VM to allow it to run cloud-init (and thus our previously defined commands). Once complete, the VM will shutdown:

govc vm.power -on ubuntu-template

Once the VM has shutdown, mark it as a template:

govc vm.markastemplate ubuntu-template

Finally, we can clone our template VM as we need to. In the example below, we clone it ten times:

for x in {1..10};do govc vm.clone -vm ubuntu-vm ubuntu-vm\$x;done

To do this for a large number of VMs, in parallel (and output to a log file) we could run:

for x in {1..250};do (govc vm.clone -vm ubuntu-template ubuntu-vm\$x >>  $(date +%d%m-%H%M)_clone.log 2>&1 &);done$ 

We can monitor progress by probing the vCenter task-list:

### govc tasks -f -l

After cloning, we can batch-execute commands on all the VMs. For example, the 'ls' command:

govc find -type m -name 'ubuntu-vm\*' | xargs -P0 -I '{}' bash -c 'ssh -o "StrictHostKeyChecking=no" ubuntu@\$(govc vm.ip {}) ls'

# APPENDIX B: Cleanly Removing vSAN Configuration

## vCLS Retreat Mode

On occasion, it may become necessary to remove a vSAN cluster and reset hosts to a 'clean' state.

To expedite the process, it is advisable to first put vCLS into retreat mode. This will delete the vCLS VMs and make it easier to remove the vSAN datastore and put hosts into maintenance mode, etc.

To achieve this, an vCenter advanced setting, 'config.vcls.clusters.[domain].enabled' needs to be set.

The procedure to do this is detailed in the documentation here: <u>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-F98C3C93-875D-4570-852B-37A38878CE0F.html</u>

To make this easier a script is available here to use (download to a Linux or Mac host, uses govc): <a href="https://github.com/vmware-tanzu-experiments/vsphere-with-tanzu-proof-of-concept-samples/blob/main/VCF/vCLS.sh">https://github.com/vmware-tanzu-experiments/vsphere-with-tanzu-proof-of-concept-samples/blob/main/VCF/vCLS.sh</a>

## Remove vSAN Partitions and Clear Data

The next step is to turn off vSAN from vCenter, under [cluster] > Configure > Services > vSAN. If for some reason this step encounters errors, the method below may be useful.

First, open an SSH session to all hosts in the cluster and list the disks used by vSAN by using the command:

### vdq -iH

The next step depends on the type of cluster

### **OSA Clusters**

Remove the cache device from each disk group, using the command:

esxcli vsan storage remove -s [cache device]

### **ESA Clusters**

Remove disks from the storage pool, using the command:

### esxcli vsan storagepool remove -d [device]

Next, relabel the disks:

partedUtil mklabel /vmfs/devices/disks/[disk] gpt

Again, to make this easier, a script is available to help with this:

OSA: <u>https://github.com/vmware-tanzu-experiments/vsphere-with-tanzu-proof-of-concept-samples/blob/main/VCF/vsan-</u>remove-esa.sh

ESA: <u>https://github.com/vmware-tanzu-experiments/vsphere-with-tanzu-proof-of-concept-samples/blob/main/VCF/vsan-remove-esa.sh</u>



Copyright © 2024 Broadcom. All rights reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others. Item No: vmw-bc-wp-tech-temp-uslet-word-2024 1/24