

VMware Operations and Management



Table of contents

VMware vSAN for Azure VMware Solution	3
Overview	3
vSAN Clusters	4
Default Configuration	4
Capacity	4
Slack Space	4
Storage Policies	5
Management Storage Policy	5
Default Storage Policy	5
Configuring Storage Policies	7
Run Commands	8
Monitoring and Alerts	9
Shared Responsibility	9
Real-time Health Status	9
Azure Alerts 1	0
Summary and Additional Resources 1	1
Additional Resources	1
Changelog1	1
About the Author and Contributors	1



Overview

VMware vSAN is the default storage platform for the Azure VMware Solution (AVS) private cloud. Local storage from each host within a vSphere cluster is pooled together to create a single, cluster-wide, vSAN datastore. Virtual machine files are distributed across hosts to ensure availability. vSAN is provisioned automatically during the private cloud deployment, or addition of a new cluster to an existing private cloud, and managed from the vSphere Web Client. It integrates core vSphere features including vMotion, HA, and DRS. vSAN delivers enterprise-class features, scale and performance, making it the ideal storage platform for VMs.

At the time this document was published, AVS private cloud clusters are using vSAN 7 Update 3c Enterprise with on-disk format v10. vSAN Enterprise licensing is included with the service.



vSAN Clusters

Default Configuration

Microsoft manages the vSAN cluster configuration, and customers do not have the ability to modify the configuration.

Enabled by default:

- Space efficiency services (deduplication and compression)
- Data-at-rest encryption
 - \circ Provider managed, encryption keys are created at the time of deployment and stored in Azure Key Vault.
 - If a host if removed from a cluster, the data on the local devices is invalidated immediately.
 - $\circ~$ Customers have the option to manage their own keys after deployment.

Disabled by default:

- Operations reserve
- Host rebuild reserve
- vSAN iSCSI Target Service
- File Service

Capacity

AVS offers three different host types; in addition to having different CPU and RAM specs, they also have different storage footprints. vSAN datastore capacity is increased by adding additional hosts to the cluster.



The total amount of storage per host is shown as raw capacity, for example, a 3 host AV36 cluster provides 46.2 TB of raw capacity. The total usable capacity will vary based on a number of variables such as RAID, Failures to Tolerate (FTT), compression, deduplication, thin vs thick provisioning, and slack space.

Slack Space

Slack space is the amount of storage space recommended to keep available for vSAN operational tasks and host failures/rebuilds. Not only will vCenter alarms be triggered, but Microsoft will also provide alerts and metrics via Azure Monitor when consumption of the vSAN datastore is greater than 75%. Microsoft requires customers to maintain 25% slack space to guarantee the AVS SLA.



Storage Policies

VMware vSAN leverages storage policy based management (SPBM) for VM placement, availability, and performance. Storage policies can be applied to multiple VMs, single VMs, and even single VMDKs. This allows you to apply specific attributes to multiple VM objects and disks. For example, we can apply RAID-1 mirroring to the VM as a whole, but apply RAID-5 erasure coding to a specific disk (VMDK) of the VM.

VMware and Microsoft have built a number of pre-defined storage policies for customer consumption. These policies cannot be modified or deleted, but new policies can be created. The pre-defined storage policies are well thought out and should meet the needs of most use cases.

Management Storage Policy

The default policy for all of the SDDC management VMs—including the vCenter Server Appliance, NSX-T Manager, and NSX-T Edges—is labeled **Microsoft vSAN Management Storage Policy** with the following configuration

General	
Name	Microsoft vSAN Management Storage Policy
Description	
Rule-set I. VSAN	
Placement	
Storage Type	VSAN
Site disaster tolerance	None - standard cluster
Failures to tolerate	1 failure - RAID-1 (Mirroring)
Number of disk stripes per object	1
IOPS limit for object	0
Object space reservation	Thick provisioning
Flash read cache reservation	0%
Disable object checksum	No
Force provisioning	No
Encryption services	No preference
Space efficiency	No preference
Storage tier	No preference

Default Storage Policy

If you're familiar with vSAN, you know there is a **vSAN Default Storage Policy**. In AVS, this does exist, however it is **NOT** the default storage policy applied to the cluster. This policy exists for historical purposes only, and this is where confusion may set in. This is a vSAN Default Storage Policy ... *policy*.

Upon closer inspection you'll notice that the Object space reservation is set to thick provisioning.





The actual default storage policy setting for this vSAN cluster is set to RAID-1 FTT-1, with Object space reservation set to Thin provisioning.





General	
Name	RAID-1 FTT-1
Description	
Dulo cot 1: VCAN	
Rule-set I: VSAN	
Placement	
Storage Type	VSAN
Site disaster tolerance	None - standard cluster
Failures to tolerate	1 failure - RAID-1 (Mirroring)
Number of disk stripes per object	1
IOPS limit for object	0
Object space reservation	Thin provisioning
Flash read cache reservation	0%
Disable object checksum	No
Force provisioning	No
Encryption services	No preference
Space efficiency	No preference
Storage tier	No preference

The difference between the two is one is set to thick provisioning, and one is set to thin provisioning.

In a 3 host cluster, this policy enables RAID-1 mirroring and protects VMs against a single host failure. However, this policy also requires double the storage per virtual machine.

Configuring Storage Policies

As hosts are added to the cluster, it's recommended to change both the default storage policy and VM disk policies to ensure appropriate capacity utilization, availability, and performance for each virtual machine based on the number of hosts provisioned.

It's important to understand that storage policies are applied during initial VM deployment, or during specific VM operations – cloning or migrating. The default storage policy cannot be changed on a VM after it's deployed, but the storage policy can be changed per disk.

In most cases customers should be using RAID-5 or RAID-6 with FTT set to 1 or 2 depending on their cluster size. If you start off with a 3 host cluster, the policy will default to RAID-1 FTT-1. If you know that you'll expand the cluster in the near future, I recommend deploying with 4-6 hosts from the start. The table below shows the different RAID configurations with FTT and the minimum required hosts for each.

Note: A storage policy for RAID-0 is not available out of the box, but can be created. Any storage policy created and used with no data redundancy options is not covered under the Microsoft SLA.

RAID	FTT	Minimum Hosts
RAID-0	0	3
RAID-1 (Default)	1	3
RAID-5	1	4
RAID-1	2	5
RAID-6	2	6
RAID-1	3	7

Run Commands

Azure Run commands allow admins to perform tasks via the Azure portal that they don't have privileges to perform directly in the vSphere Client. As it relates to storage policies, there are seven Run commands.

- Get-StoragePolicies
 - $\circ~$ Lists all the vSAN storage policies available to apply to a VM.
- New-AVSStoragePolicy
 - $\circ~$ Creates a new, or overwrites an existing, storage policy.
- Remove-AVSStoragePolicy
 - Removes a storage policy.
- Set-ClusterDefaultStoragePolicy
 - $\circ\;$ Allows an admin to set the default storage policy for a cluster.
- Set-LocationStoragePolicy
 - Allows an admin to modify the storage policy for all VMs in a specific cluster, resource pool, or folder.
- Set-VMStoragePolicy
 - Allows an admin to modify the storage policy on VMs sharing the same name (example: "Web*")
- Set-vSANCompressDedupe
 - $\circ~$ Sets compression and deduplication on vSAN cluster(s).
 - Deduplication and compression are already enabled on the vSAN cluster by default. The admin can choose to disable both, or just disable deduplication, leaving only compression enabled. If deduplication is enabled, compression is always enabled along with it.

To perform these tasks, simply login to the Azure portal, and navigate to your AVS Private cloud. Select Run command > Microsoft.AVS.Management (under Packages).

		Search resources, services, and docs (G+/)	VONML
Home > AVS-SDDC			
AVS-SDDC Run con	nmand 🖈 …		×
₽ Search «	🕐 Refresh 🔗 Feedback		
Overview	Packages Pup everytion status		
Activity log	rackages Run execution status		
Access control (IAM)	∨ Name	Description	
Tags	> JSDR.Configuration (\$0.0) Powershell N	todule for configuration of Jedfanam Software on AVS. See <u>artifyzem Software loc.</u> for support	
Diagnose and solve problems	V Microsoft.AVS.Management (53.54)	arrous cmdlets for administrator level tasks in managing Azure VMware Solutions	
Settings	Add-GroupToCloudAdmins	Add a group from the external identity to the CloudAdmins group	
🔒 Locks	Get-CloudAdminGroups	Get all groups that have been added to the cloud admin group	
Manage	Get-ExternalIdentitySources	Gets all external identity sources	
Connectivity	Get-StoragePolicies	Gets all the vSAN based storage policies available to set on a VM.	
Clusters	New-AVSStoragePolicy	This function creates a new or overwrites an existing v5phere Storage Policy. Non v5AN-Based, v5AN Only, VMEncryption Only, Tag Only based and/or any combination of these policy types are supported.	
Encryption	New-LDAPIdentitySource	Not Recommended (use New-LDAP-SidentitySource): Add a not secure external identity source (Active Directory over LDAP) for use with vCenter Server Single Sign-On.	
VMware credentials	New-LDAPSIdentitySource	Recommended: Add a secure external identity source (Active Directory over LDAPS) for use with vCenter Server Single Sign-On.	
? Identity	Remove-AVSStoragePolicy	This function removes a storage policy.	
Storage	Remove-ExternalIdentitySources	Removes supplied identity source, or, if no specific identity source is provided, will remove all identity sources.	
Placement policies	Remove-GroupFromCloudAdmins	Remove a previously added group from an external identity from the CloudAdmins group	
+ Add-ons	Restart-HCXManager	Restarts the HCX Manager VM	
Workload networking	Set-ClusterDefaultStoragePolicy	Specify default storage policy for a cluster(s)	
Segments	Set-CustomDRS	This allows the customer to change DRS from the default setting to one step more conservative.	
T DHCP	Set-HcxScaledCpuAndMemorySetting	Scale the HCX manager vm to the new resource allocation of 8 vCPU and 24 GB RAM (Default 4 vCPU/12GB)	
Port mirroring	Set-LocationStoragePolicy	Modify vSAN based storage policies on all VMs in a Container	
O DNS	Set-ToolsRepo	This will create a folder on every datastore (/vmfs/volumes/datastore/tools-repo) and set the ESXI hosts to use that folder as the tools-repo. The customer is responsible for putting the VMware Tools zip file in a downloadable location.	
Internet connectivity	Set-VMStoragePolicy	Modify vSAN based storage policies on a VM(s)	
Operations	Set-vSANCompressDedupe	Set vSAN compression and deduplication on a cluster or clusters. If deduplication is enabled then compression is required. The default cluster configuration is deduplication and compression but the customer can change that. Choosing neither compression nor deduplication will disable both. This requires action on every physical disk and will take time to complete.	
Anura hubrid banafit	Update-IdentitySourceCertificates	Update the SSL Certificates used for authenticating to an Active Directory over LDAPS	
- Azure nyoria beñéfit	Update-IdentitySourceCredential	Update the password used in the credential to authenticate an LDAP server	
Monitoring			



Monitoring and Alerts

Shared Responsibility

Customers are responsible for applying appropriate storage policies to their VMs, and adding hosts to maintain adequate vSAN slack space.

Microsoft is responsible for:

- Compute / Network / Storage
 - $\,\circ\,$ Rack, power, bare metal hosts, and devices
- SDDC Lifecycle
 - ESXi deployment, patching and upgrades
 - $\circ\;$ vCenter Server deployment, configuration, patching, and upgrades
 - $\circ~$ vSAN deployment, configuration, patching, and upgrades
- SDDC Compute
 - Cluster configuration
 - $\circ~$ Virtual networking for vMotion, Management, vSAN, etc.
- SDDC Health
 - $\circ~$ Monitoring and corrective actions
 - Replacement of failed hosts

For more information pertaining to responsibility, please refer to the AVS Shared Responsibility Model.

Real-time Health Status

The vSAN health service is used to monitor the health status of the cluster. Here you can check the status of cluster components, capacity, performance and more.







Azure Alerts

It's recommended that customers configure Azure health alerts to receive notifications of triggered events that administrators can define. Refer to the Microsoft documentation for manually configuring Azure Action Groups, Azure Alerts, and Azure Monitor Metrics, or you can use the Microsoft Enterprise-Scale for AVS ARM templates for Monitoring to automate much of the configuration.

In the video below, we demonstrate how to use the AVS ARM templates to setup basic monitoring of the Azure VMware Solution private cloud.

Customers are encouraged to leverage vRealize Operations for more in-depth metrics, alerting, and capacity planning. In the video below, we demonstrate creating an Azure application registration and using that to add an Azure VMware Solution private cloud as an endpoint in vRealize Operations.



Summary and Additional Resources

Additional Resources

For more information about vSAN, you can explore the following resources:

- VMware vSAN Design Guide
- vSAN on Tech Zone
- VMware Documentation: Administering VMware vSAN
- VMware Documentation: vSAN Monitoring and Troubleshooting
- Configure vRealize Operations for AVS
- vRealize Operations vSAN Capacity Dashboard

Changelog

The following updates were made to this guide:

Date	Description of Changes
2023/05/23	
2023/05/01	

About the Author and Contributors

• Jeremiah Megie, Principal Cloud Solutions Architect, Cloud Services, VMware





