DOCUMENT – AUGUST 2021

PRINTED 15 JUNE 2022

AZURE VMWARE SOLUTION PLANNING AND DEPLOYMENT GUIDE

VMwareGeneral

vmware

Table of Contents

Azure VMware Solution Planning and Deployment Guide

Introduction

This guide introduces the planning considerations and initial deployment process supporting the successful deployment of an Azure VMware Solution (AVS) private cloud. This guide assists customers in learning AVS concepts, identifying AVS prerequisites, planning for the initial deployment, deploying the first AVS private cloud, and establishing connectivity between an on-premises datacenter and the AVS private cloud.

Summary and Considerations

Use Case	Azure VMware Solution combines VMware compute, networking, and storage running on top of dedicated bare-metal hosts in Microsoft Azure. AVS core capabilities are provided by vSphere, vCenter, vSAN, NSX-T, and HCX. These core capabilities can be extended with VMware services provided by VMware products that have been certified with AVS. Migrating virtual machines into AVS is facilitated through VMware HCX. AVS can be managed, monitored, and automated with the vRealize portfolio products. Networking extensions are available from NSX Advanced Load Balancer and VMware SD-WAN. VMware Tanzu Standard provides an application modernization platform, offering Tanzu Kubernetes Grid as a consistent Kubernetes runtime and Tanzu Mission Control for centralized management. VMware Horizon on AVS is the supported cloud virtual desktop solution. VMware Site Recovery Manager is the primary disaster recovery to the cloud solution.
Pre-requisites	• A new or existing Azure subscription associated with a Microsoft Enterprise Agreement (EA) or a Cloud Solution Provider (CSP) Azure plan. This guide assumes the subscription is under a Microsoft EA. • If VMware HCX will be deployed and leveraged for cloud migration, the connection between the on-premises environment and Azure must meet the HCX Network Underlay Minimum Requirements. At the time of this writing, HCX 4.1 is the currently deployed and supported version of HCX on AVS. This version requires an Azure ExpressRoute connection as the underlay. • Azure ExpressRoute is required to leverage VMware Site Recovery Manager for disaster recovery.
General Considerations/Recommendations	AVS is jointly engineered with Microsoft Azure as the operator. Periodic updates and fixes, remediation of failures, and general support are provided by Azure. Configuration Maximums: • Clusters per private cloud: 12 • Maximum hosts per cluster: 16 • Maximum hosts per private cloud: 96 • vCenter per private cloud: 1 • vSAN capacity limit: 75% of total usable space
Performance Considerations	vSphere runs on bare metal hardware, leveraging all-flash vSAN.
Network Considerations/Recommendations	• All gateways must support 4-byte Autonomous System Numbers (ASNs) • AVS resources do not have public internet access enabled by default • AVS requires a /22 CIDR network that does not overlap with any existing network segments deployed on-premises or in Azure • Applications and workloads running in the AVS private cloud require DNS and DHCP services. You can deploy these services as virtual machines within the private cloud, configure and leverage the DNS and DHCP services provided by NSX, or extend these services from on-premises infrastructure.
Cost Implications	A minimum of three Azure VMware Solution hosts are required. Customers are charged on-demand, per host, per hour. This cost can be reduced by purchasing 1-year or 3-year reserved instances. Refer to Microsoft's website for the most current, and up to date, pricing for AVS. Egress charges may apply to VM traffic on extended networks communicating from Azure VMware Solution to an on-premises environment. Other supporting resources that will generate additional monthly costs may include, but are not limited to: • Virtual Network Gateways • ExpressRoute Circuits • Azure Bastion Services • Azure Virtual Machines • Azure Virtual Machine Disks • Public IP addresses Refer to the Azure Pricing Calculator to estimate costs for Azure products.
Document Reference	Azure VMware Solution Documentation (Microsoft) Azure VMware Solution Tech Zone VMware Cloud Ready Framework for Azure VMware Solution: Planning Principles
Last Updated	August 2021

Core Concepts

Before planning a deployment, a working understanding of the following core Azure and Azure VMware Solution concepts is required.

Azure concepts

Subscriptions

Within Azure, a Subscription is a billing boundary for services. A user must have access to a valid Azure Subscription to deploy any Azure resources. Azure VMware Solution is supported only in subscriptions associated with a Microsoft Enterprise Agreement or a Cloud Solution Provider Azure plan.

Regions

An Azure region is a collection of data centers interconnected by a dedicated, low-latency network hosting Azure services. Not all Azure services are available in all regions. At the time of this writing, Azure VMware Solution is supported in 15 regions. A current list of supported regions can be found here.

Resource groups

A Resource Group is a container object into which other Azure resources can be grouped to simplify management of multiple resources. Policies and lifecycle actions can be applied to the group to affect all resources within the group.

Virtual Networks (VNets) and Virtual Network Gateways

Azure Virtual Networks are the building blocks for private network communication within Azure. VNets enable Azure resources to security communicate with each other, the internet, and on-premises resources. A Virtual Network Gateway allows VNets to exchange routes and route traffic between each other.

ExpressRoute

An ExpressRoute circuit is a private connection to the Microsoft Azure global backbone. A customer can connect to an ExpressRoute location via an ExpressRoute connectivity provider and access all regions within a geopolitical region via that connection.

AVS concepts

Private cloud

An AVS private cloud consists of one or more vSphere clusters deployed on bare-metal server hosts, vCenter Server, NSX-T, vSAN, and various Azure underlay resources required for connectivity and operation. By default, only one AVS private cloud can be deployed per Azure subscription, but this limit can be scaled by support ticket.

AVS hosts

At the time of this writing, AVS supports a single host type. Each AV36 host includes:

- Two Intel 18-core, 2.3 GHz, processors
- 576 GB RAM
- Two dual-port 25GbE network adapters, configured as two vmnics for ESXi system traffic and two vmnics for workload traffic
- Two 1.6 TB NVMe storage devices and eight 1.92 TB SSDs, organized into two vSAN disk groups with a3.2 TB NVMe cache tier and a 15.2 TB capacity tier

Cluster configuration

An AVS private cloud will start with a single cluster with 3-16 hosts. Up to 12 clusters can be created in each AVS private cloud, with up to 96 hosts distributed between those clusters. All AVS management VMs, including vCenter, NSX Manager, and HCX components will be placed on the first cluster.

Identity and access management

A local user named `cloudadmin` assigned to the CloudAdmin role is used to administer vCenter in AVS. This role provides the permissions necessary to manage the environment but will not have access to specific management components supported and managed by Microsoft, including ESXi hosts, clusters, and datastores. The `cloudadmin` user can be used to assign the CloudAdmin role to Active Directory users and groups.

Connectivity

At provisioning, an ExpressRoute circuit is created connecting the AVS private cloud to the Microsoft Dedicated Enterprise Edge routers, allowing the AVS private cloud to connect to the Azure backbone and access Azure services. The AVS private cloud can be connected to an existing Azure VNet by way of an ExpressRoute Gateway. The preferred method for connecting an AVS private cloud to an on-premises datacenter is via ExpressRoute Global Reach. If an ExpressRoute circuit between the on-premises datacenter and Azure is not available, a Site-to-Site VPN connection can be used.

Planning

Topics in this section address considerations and actions to be taken prior to starting the deployment of the AVS private cloud. This includes planning for resource placement, resource naming, cluster sizing, requesting host quota, registering the AVS provider, and network allocation.

Identify Azure subscription, resource group, region, and resource name

An AVS private cloud must be created in a resource group. A resource group is associated with a subscription and a region. First, determine the subscription that will be used for AVS. This subscription must be associated with a Microsoft Enterprise Agreement (EA) or a Cloud Solution Provider (CSP) Azure plan. A resource group can contain resources deployed in multiple regions, but for the sake of simplicity and consistency it is recommended that the resource group be hosted in the same region as the AVS private cloud. The most current list of regions supporting AVS can be found here.

You may choose an existing resource group or create a new resource group specifically for AVS and related services. To create a new resource group, follow these steps:

1. Log into the Azure portal
2. Click **Create a resource**
3. Type “resource group” into the search bar and select the “Resource group” item.
4. Click **Create**
5. Select the appropriate subscription, provide a name for the Resource Group, and select the desired region.
6. Click **Review + create,** then **Create**

The following table lists the configuration items to collect in this step, and provides examples of each:

Table 1: AVS and supporting resource names

Item	Description	Example
Subscription	Azure subscription in which AVS resources will be deployed	Prod-Infra-01-Sub
Region	Azure region in which resources will be deployed	West US
Resource group	New or existing resource group that will contain AVS resources	Prod-AVS-01-RG
AVS private cloud name	A name for the AVS private cloud object	Prod-AVS-01-PC

Size hosts and clusters

Discovery and analysis of the existing environment will be necessary to determine the appropriate number of hosts and clusters needed in the AVS private cloud. At the time of this writing, only one host type is available, providing a fixed unit of compute,

storage, and network. You will need to determine the aggregate resource demands of the workloads you intend to deploy in the AVS private cloud. Storage capacity will also need to be considered—to remain eligible for the AVS SLA you must not exceed 75% consumption of usable disk space. Storage policies (RAID-1, RAID-5, RAID-6) will factor into usable storage calculations and impact required host count.

Some consideration should be given to growth expectations. You will want to allocate enough hosts to provide reasonable excess capacity to support potential host failure and support near-term growth expectations. The cluster can be scaled up and down as needed.

Tools such as vRealize Operations Manager and vRealize Operations Cloud can be used to analyze current resource allocation and demand, make re-sizing recommendations, and forecast the number of AVS hosts needed to support a migration.

Each cluster requires a minimum of three hosts and supports a maximum of 16 hosts. Keep this in mind during sizing calculations and, if necessary, create multiple clusters to account for scalability if you plan to use the maximum number of hosts.

Request host quota

Before you can deploy an AVS Private cloud, you must request host quota be assigned to your Azure account. It can take up to 5 days for the hosts to be allocated within the quota, so keep this in mind when planning the deployment. If you plan to scale your cluster for future growth or disaster recovery use cases, consider requesting the additional hosts in your initial quota request. You are not billed for these hosts unless they are allocated to your account, and this will save time if you need to scale out quickly. To request your host quota, open a support ticket by following these steps:

1. In the Azure portal, expand the upper left blade and select **Help + Support**
2. Click **Create a support request**
3. On the Basics tab, supply the following values:
   - Summary: “Need capacity”
   - Issue Type: **Technical**
   - Subscription: The subscription you intend to deploy AVS into
   - Service: **All services**
   - Service type: **Azure VMware Solution**
   - Resource: **General question**
   - Problem type: **Capacity Management Issues**
   - Problem subtype: **Customer Request for Additional Host Quota/Capacity**
4. Click Next: Solutions >> and then Next: Details >>
5. On the Details tab, provide the following information in the Description text box:
   - Whether this deployment will be for a POC or Production
   - The region you intend to deploy into
   - The number of hosts required
6. Select whether you want to share diagnostic information, provide your preferred contact method and contact info, then click **Next: Review + create >>**
7. Review the information, then click **Create**

Register Microsoft.AVS provider

The Microsoft.AVS resource provider must be registered to enable AVS-related features and functions. Confirm this resource provider is registered by following these steps:

1. Log into the Azure portal
2. Select (or search for) Subscriptions
3. Click your subscription object
4. Click **Settings > Resource providers**
5. Search for Microsoft.AVS. If not already registered, select **Register**

Identify network requirements

AVS requires a /22 CIDR network that does not overlap with any existing network segments that are deployed on-premises or in Azure. This network block is automatically carved up into supporting subnets for management, provisioning, vMotion, and related purposes. Permitted ranges for this address block are the RFC 1918 private address spaces (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16), with the exception of 172.16.0.0/16).

As an example, if the block 10.2.0.0/22 were provided, the following subnets would be created:

Table 2: Auto-generated subnets

Purpose	Subnet	Example
Private cloud management	/26	10.2.0.0/26
HCX Management Migrations	/26	10.2.0.64/26
Global Reach Reserved	/26	10.2.0.128/26
NSX-T DNS Service	/32	10.2.0.192/32
Reserved	/32	10.2.0.193/32
Reserved	/32	10.2.0.194/32
Reserved	/32	10.2.0.195/32
Reserved	/30	10.2.0.196/30
Reserved	/29	10.2.0.200/29
Reserved	/28	10.2.0.208/28
ExpressRoute Peering	/27	10.2.0.224/27
ESXi Management	/25	10.2.1.0/25
vMotion Network	/25	10.2.1.128/25
Replication Network	/25	10.2.2.0/25
vSAN	/25	10.2.2.128/25
HCX Uplink	/26	10.2.3.0/26
Reserved	/26	10.2.3.64/26
Reserved	/26	10.2.3.128/26
Reserved	/26	10.2.3.192/26

The AVS private cloud requires an Azure VNet. You can connect AVS to an existing Azure VNet or create a new one. A non-overlapping IP range must be defined for the VNet, and a subnet named `GatewaySubnet` must be created. The `GatewaySubnet` subnet should be a /27 network or larger. Two additional VLANs should be defined as well. These will be used for a Jumpbox VM and for the Azure Bastion Service for connectivity to the Jumpbox VM. The Bastion subnet must be named `AzureBastionSubnet`.

Sample values for these configurations are captured below:

Table 3: AVS network configuration elements

Item	Description	Example
AVS private cloud network range	The network range to be assigned to the AVS private cloud	10.2.0.0/22
VNet name	New or existing VNet that will be connected to AVS	Prod-AVS-01-vnet
VNet IP space	IP block for the new VNet	172.24.0.0/16
VNet subnets	Subnets to create in the new VNet. `GatewaySubnet` is used by the Virtual Network Gateway that will connect to the AVS ExpressRoute. `AzureBastionSubnet` is used for the private connection between Azure bastion and deployed VMs. A third subnet is used to host a Jumpbox VM to confirm vCenter operation. This name is user-specified, "Management" is used as an example.	`GatewaySubnet` – 172.24.0.0/24 `AzureBastionSubnet` – 172.24.1.0/24 Management – 172.24.2.0/24

Deployment

Topics in this section address the deployment of the AVS private cloud, connecting the AVS private cloud to an Azure VNet, and connecting the AVS private cloud to an on-premises data center.

Deploy the private cloud

After host quota has been allocated, you can create your first AVS Private cloud by following these steps:

1. Log into the Azure portal
2. Navigate to and open your Resource Group
3. Click **Create**
4. Type "azure vmware solution" into the search bar and select the "Azure VMware Solution" item.
5. Click **Create**
6. The "Create a private cloud" wizard opens. The "Prerequisites" tab reminds us of the need to have host quota assigned and a /22 network available. Click **Next: Basics >**.
7. Subscription and resource group will be pre-populated with the appropriate values. Provide values for the remaining fields, as shown in Tables 1 and 3:
   - Resource name: A name for the AVS Private cloud object
   - Location: The region in which host quota was assigned
   - Size of host: The AVS node type. At the time of writing, **AV36** is the only host type available.
   - Number of hosts: Select the number of hosts for the initial cluster
   - Address block for private cloud: The /22 network to be assigned
8. Click **Review + create**
9. Review the settings specified and click **Create**. The deployment process may take up to five hours to complete.

Configure Azure VNet and connect to AVS ExpressRoute

By default, there will be no connectivity between the AVS Private cloud and other Azure resources deployed in your subscription. You can connect a new or existing Azure VNet to the AVS Private cloud when the AVS deployment is complete. This VNet must have a subnet named `GatewaySubnet` defined. A Virtual Network Gateway will be created in this VNet and connected to the AVS ExpressRoute connection, allowing communication between resources attached to this VNet and AVS VMs. To create a new VNet, follow these steps:

1. Log into the Azure portal
2. Navigate to and open your AVS private cloud object

3. Click **Manage > Connectivity**
4. On the "Azure vNet connect" tab, click **Create new** under the Virtual network dropdown
5. Provide a VNet name, VNet address range, subnet names, and subnet address ranges. An entry for `GatewaySubnet` will be pre-populated. Add additional rows for the `AzureBastionSubnet` and the Jumpbox VM subnet. Refer to Table 3 for example values.
6. Click **OK**
7. Click **Save**. This operation will take several minutes to complete.

Create a Jumpbox VM for private cloud administration (Optional)

To confirm that private cloud resources are online and operational, you can deploy a Jumpbox VM into the VNet peered with the AVS private cloud and use that VM to access the vCenter and NSX-T Manager consoles.

Deploy Azure Bastion

Azure Bastion is a service that lets you connect to an Azure virtual machine using your browser and the Azure portal. It provides a secure RDP/SSH connection to all of your virtual machines over TLS in the VNet in which it is provisioned.

1. Open the Azure portal and navigate to the resource group hosting the AVS private cloud object
2. Click **Create**
3. Type "bastion" into the search bar and select the "Bastion" item.
4. Click **Create**
5. Subscription and resource group will be pre-populated with the appropriate values. Provide values for the remaining fields:
   - Name: A name for the Bastion object
   - Location: The region used for the AVS private cloud
   - Tier: Select **Basic**
   - Virtual network: Select the VNet connected to the AVS private cloud
   - Accept default options for Public IP address and Public IP address name
6. Click **Review + create**
7. Review the settings specified and click **Create**. This operation will take several minutes to complete.

Create the Jumpbox VM

1. Log into the Azure portal
2. Navigate to and open your resource group
3. Click **Create**
4. Type "Windows 10" into the search bar and select the "Microsoft Windows 10" item.
5. Click **Create**
6. On the "Basics" tab, Subscription and Resource group should be pre-populated. Update the following fields:
   - Virtual machine name: A name for your VM
   - Region: The region into which your AVS private cloud is deployed
   - Username: A login name for the VM
   - Password: Password for the user specified above
   - Public inbound ports: Select **None**. We will use Azure Bastion to connect to the VM.
   - Check the box next to "I confirm I have an eligible Windows 10 license with multi-tenant hosting rights."
7. Click the "Networking" tab
8. Ensure the appropriate Virtual network and subnet are selected
9. Set "Public IP" to **None**, and "Public inbound ports" to **None**
10. Click **Review + create**
11. Click **Create**

Log into jumpbox and access management consoles

1. Log into the Azure portal and navigate to the AVS private cloud object
2. Select **Manage > Identity**. This page lists the web client URLs, admin usernames, and admin passwords for vCenter and NSX-T Manager.
3. Open a new Azure portal tab and navigate to the Windows 10 VM deployed in the previous section
4. Select **Connect > Bastion**
5. Click **Use Bastion**
6. Enter the username and password defined in the previous section, then click **Connect**

7. If prompted to allow sharing clipboard contents, click **Allow**
8. The Windows VM desktop will render in the open tab. Click through the Windows 10 first time setup wizard
9. Open Edge on the Windows VM
10. In your web browser, switch to the tab open to the AVS private cloud Identity panel
11. Copy the vCenter URL, switch to the Windows 10 VM tab, and paste the URL into the search bar
12. Accept all of the certificate warnings and launch the vSphere client
13. Switch between the Windows 10 VM tab and AVS Identity panel, copy and pasting the vCenter admin username and password into the Windows 10 VM tab
14. Explore the vCenter client
15. Repeat steps 10-14 with the NSX-T Manager URL and credentials

Peer on-premises networks with ExpressRoute Global Reach

ExpressRoute Global Reach allows you to connect your on-premises environment to your Azure VMware Solution private cloud. ExpressRoute Global Reach peers the private cloud ExpressRoute circuit with an existing ExpressRoute circuit connecting your on-premises and Azure environments.

To complete this step, an existing, functioning ExpressRoute circuit must exist connecting the on-premises environment to Azure. This will be referred to as “on-prem ExpressRoute.” Additionally, all gateways must support 4-byte Autonomous System Numbers (ASNs).

Create an ExpressRoute authentication key for the on-prem ExpressRoute.

1. From the Azure Portal, navigate to the ExpressRoute circuits page and select the on-prem ExpressRoute
2. Under **Settings**, select **Authorizations**
3. Enter a name for the new Authorization and click **Save.** The Authorization will begin provisioning and should complete within a few minutes.
4. Copy the on-prem ExpressRoute Resource ID and the Authorization key. These will be used to complete the peering.

Peer the AVS private cloud to on-prem ExpressRoute

1. From the Azure Portal, navigate to the Private cloud object and click **Manage > Connectivity > ExpressRoute Global Reach > Add**
2. Enter the on-prem ExpressRoute Resource ID and Authorization key created in the previous steps, then click **Create**. These operations will take a few minutes to complete.

Verify connectivity between on-premises networks and AVS networks

1. From the Azure Portal, navigate to the ExpressRoute circuits page, and select the on-prem ExpressRoute
2. Under **Settings**, select **Peerings**
3. Click the **Azure private** row, then click **View route table** in the top menu
4. Examine the route table and confirm the AVS management networks and any NSX-T segments are listed
5. From your on-premises edge router, confirm routes exist to the AVS management networks and any NSX-T segments
6. From an on-premises device, attempt to access the AVS-hosted vCenter management console

Summary and Additional Resources

Summary

This guide provided an overview of the planning and deployment steps for getting started with Azure VMware Solution.

Topics included:

- Core Azure and AVS concepts
- Planning considerations
- Deployment process
- ExpressRoute configuration

Authors

- Jeremiah Megie, Principal Cloud Solutions Architect, Cloud Services, VMware
- Steve Pantol, Senior Technical Marketing Architect, Cloud Services, VMware

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