REQUIREMENTS CHECKLIST
Last Updated 18 SEPTEMBER 2019

VMWARE HORIZON CLOUD SERVICE ON MICROSOFT AZURE

Complete the following tasks to prepare your Microsoft Azure subscription and network for the deployment of VMware Horizon® Cloud Service™. Ensure every step is completed as described below to complete a successful deployment.

Setup Checklist

HORIZON CLOUD CONTROL PLANE REQUIREMENTS	
☐	Active My VMware account to log in to the Horizon Cloud Control Plane.
MICROSOFT AZURE SUBSCRIPTION REQUIREMENTS	
☐	Valid Microsoft Azure subscription in a supported Microsoft Azure environment (Public Azure, Azure China, Azure Germany and Azure Government).
☐	Valid Microsoft Azure administrative privileges in Microsoft Azure subscription. For additional information, see Get Started with Role-Based Access Control in the Azure portal.
☐	Minimum Microsoft Azure capacity available for Horizon Cloud infrastructure in addition to expected Desktop/App workload. Note that as long as this capacity is made available, Horizon Cloud will automatically deploy these VMs and no manual installation is required. • Deployment Engine/"Jumpbox" (Transient) – 1 x Standard_F2 • Pod/Pod Manager with High Availability Enabled – 2 x Standard_D4_v3 (if no Standard_D4_v3 in the region, 2 x Standard_D3_v2) • Pod/Pod Manager with High Availability Not Enabled – 1 x Standard_D4_v3 (if no Standard_D4_v3 in the region, 1 x Standard_D3_v2) • Microsoft Azure Database for PostgreSQL Service – Generation 5, Memory Optimized, 2 vCores, 10 GB Storage • External VMware Unified Access Gateway™ (optional) – 2 x Standard_A4_v2 • Internal VMware Unified Access Gateway™ (optional) – 2 x Standard_A4_v2 • Base images, Desktops and RDSH farms (See Horizon Cloud Base Image, Desktops and Farms section.)
☐	Service principal and authentication key created. For additional details, see Use portal to create an Azure Active Directory application and service principal that can access resources.
☐	Service principal must be assigned either Contributor role or a custom role with the required permitted actions at the subscription level. For addition details about the required role actions, see Role Operations Required by the Horizon Cloud Pod Deployer in Your Microsoft Azure Subscription.
☐	Required resource providers registered in Microsoft Azure subscription.
☐	Microsoft Azure subscription ID, directory ID, application ID and key identified.
NETWORK REQUIREMENTS	
☐	Microsoft Azure Virtual Network (VNet) created in desired Microsoft Azure region with applicable address space to cover required subnets. For additional details, see Azure Virtual Network.
☐	3 non-overlapping address ranges in CIDR format, reserved for subnets • Management subnet – /27 minimum • Tenant subnet – /27 minimum with /24 - /22 preferred, based on number of Desktops and RDS servers • DMZ subnet – /28 minimum when Unified Access Gateway is deployed (optional) Subnets can either be created manually on the VNet or by Horizon Cloud during deployment. If using manually created subnets, no other resources can be attached and Microsoft.Sql service endpoint must be enabled on the management subnet.
☐	NTP server(s) available and accessible from Horizon Cloud Pod and Unified Access Gateways.
☐	Configure the Virtual Network (VNet) DNS server, pointing to a valid DNS server that can resolve both internal machine names and external names.
☐	Outbound internet access on the Microsoft Azure Virtual Network (VNet) to specific DNS names, that must to be resolvable and reachable using specific ports and protocols. This is required for deployment and ongoing operations, see Horizon Cloud DNS, Ports, Protocol Requirements
☐	Proxy server information if required for outbound internet access on the Microsoft Azure Virtual Network (VNet), that is used during deployment and ongoing operations of the Horizon Cloud environment (optional)

☐	Microsoft Azure VPN/Express Route configured (optional)
☐	Internal DNS record created for direct connect to the pod that matches the certificate that is upload to the pod, pointing to the Microsoft Azure Pod Manager internal load balancer (optional).
	Certificate chain (CA Certificate, SSL Certificate, SSL Key File) matching the DNS record created for direct connect to the pod. For additional details, see Upload SSL Certificates to a Horizon Cloud Pod for Direct Connections
☐	FQDN for external and or internal user access (Required for Unified Access Gateway).
☐	Public DNS record created for external end-user access that matches the FQDN, pointing to Microsoft Azure external load balancer (optional). For additional details, see Configuring a custom domain name for an Azure cloud service.
☐	Internal DNS record created for internal end-user access that matches the FQDN, pointing to the Microsoft Azure internal load balancer (optional).
☐	Certificate(s) for Unified Access Gateway in pem format matching the FQDN (Required for Unified Access Gateway).
☐	Two-Factor Authentication to an on-premises RADIUS authentication server (optional) • DNS Addresses for Unified Access Gateway to resolve the name of the authentication server • Routes for Unified Access Gateway to resolve network routing to the authentication server
ACTIVE DIRECTORY REQUIREMENTS	
☐	One of the following supported Active Directory configurations: • On-premises Active Directory Server connected via VPN/Express Route • Active Directory Server located in Microsoft Azure • Microsoft Azure Active Directory Domain Services
☐	Supported Windows Active Directory Domain Services (AD DS) domain functional levels: • Windows Server 2003 • Windows Server 2008 R2 • Windows Server 2012 R2 • Windows Server 2016
☐	Domain bind account • Active Directory domain bind account (a standard user with read access) that has permission to read objects in AD • Set account password to “Never Expire” • For additional details and requirements, see Service Accounts That Horizon Cloud Requires For its Operations
☐	Auxiliary domain bind account (Cannot use the same account as above) • Active Directory domain bind account (a standard user with read access) that has permission to read objects in AD. • Set account password to “Never Expire” • For additional details and requirements, see Service Accounts That Horizon Cloud Requires For its Operations
☐	Domain join account • Active Directory domain join account which can be used by the system to perform Sysprep operations and join computers to the domain, typically a new account (“domain join user account”) • Is a member of the Horizon Cloud Administrators Group • Set account password to “Never Expire” • This account requires the following Active Directory permissions: List Contents, Read All Properties, Read Permissions, Reset Password, Create Computer Objects, Delete Computer Objects, and Write All Properties. • For additional details and requirements on Active Directory permissions, see Service Accounts That Horizon Cloud Requires For its Operations
☐	Auxiliary domain join account (Optional, cannot use the same account as above) • Active Directory domain join account which can be used by the system to perform Sysprep operations and join computers to the domain, typically a new account (“domain join aux user account”) • Is a member of the Horizon Cloud Administrators Group • Set account password to “Never Expire” • This account requires the following Active Directory permissions: List Contents, Read All Properties, Read Permissions, Reset Password, Create Computer Objects, Delete Computer Objects, and Write All Properties. • For additional details and requirements on Active Directory permissions, see Service Accounts That Horizon Cloud Requires For its Operations
☐	Active Directory groups • Horizon Cloud Administrators – Active Directory security group for Horizon Cloud administrators; contains the Horizon Cloud administrative users and domain join account. This group is added to the “Super Administrators” role in Horizon Cloud. • Horizon Cloud Users – Active Directory security group for the users which will have access to Desktops and RDS session-based desktops and published applications in Horizon Cloud.

☐	Active Directory organizational unit(s) (OU) for Desktops and RDS session-based desktops and/or published applications
PORTS AND PROTOCOL REQUIREMENTS	
☐	Specific ports and protocols are required for ongoing operations of the Horizon Cloud environment, see Horizon Cloud DNS, Ports, Protocol Requirements
HORIZON CLOUD BASE IMAGE, DESKTOPS and FARMS	
☐	Base for Master Image – One of the supported Microsoft Azure VM configurations • Standard_D4_v3 or Standard_D2_v2 • Standard_NV6
☐	Desktop Model selection for the Desktop Assignments – Any of the Microsoft Azure VM configurations available in your subscription, except for those not available in the Microsoft Azure region and ones not compatible with Horizon Cloud desktop operations. For production environments, VMware scale testing recommends using models having a minimum of 2 CPUs or larger.
☐	RDS Server Model selection for the RDS Farms – Any of the Microsoft Azure VM configurations available in your subscription, except for those not available in the Microsoft Azure region and ones not compatible with Horizon Cloud RDS farm operations. For production environments, VMware scale testing recommends using models having a minimum of 2 CPUs or larger.
LICENSING	
☐	Microsoft Windows 10 Licensing
☐	Microsoft Windows Server 2012 R2, Server 2016 Licensing and/or Server 2019 Licensing
☐	Microsoft Windows RDS Licensing Servers – VMware recommends redundant licensing servers for high availability.
☐	Microsoft RDS User and/or Device CALs

Deployment Workflow

After completing the preceding checklist, follow the Suggested Workflow for Your First Horizon Cloud Pod in Microsoft Azure to deploy and start administrating the service.

Reference Architecture

See the architecture diagram depicted in Introduction to Horizon Cloud Pods in Microsoft Azure.

Resources

See the following resources for additional information.

- Horizon Cloud Deployment Guide
- Horizon Cloud Administration Guide
- VMware Unified Access Gateway
- Quick Start Tutorial for VMware Horizon Cloud on Microsoft Azure
- Microsoft Azure Resource Manager overview (15 minutes)
- Create Microsoft Azure Service Principal (5 minutes)
- Microsoft Azure Virtual Network (VNet) (6 minutes)
- Microsoft Azure Virtual network peering (8 minutes)

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