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™.

Setup Checklist

HORIZON CLOUD CONTROL PLANE REQUIREMENTS	
☐	Active MyVMware 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, or Azure Germany).
☐	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 for Horizon Cloud infrastructure in addition to expected Desktop/App workload: • Deployment Engine/"Jumpbox" (Transient) – 1 x Standard_F2 • Node/Management Node – 1 x Standard_D2_v2 • VMware Unified Access Gateway™ (optional) – 2 x Standard_A4_v2 • Base image and RDSH farm (See Horizon Cloud Base Image 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 assigned **Contributor** role at the subscription level.
☐	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 subnets reserved in CIDR format (created on VNet during Horizon Cloud deployment) • Management subnet – /28 minimum • Tenant subnet – /28 minimum with /24 - /22 preferred, based on number of RDS servers • DMZ subnet – /28 minimum when Unified Access Gateway is deployed (optional)
☐	NTP server(s) available and accessible from Horizon Cloud Node and Unified Access Gateways
☐	DNS available and configured on the Microsoft Azure Virtual Network
☐	FQDN for external user access (Required for Unified Access Gateway.)

☐	Public DNS record created for external end-user access that matches the FQDN, pointing to Microsoft Azure load balancer (optional). For additional details, see Configuring a custom domain name for an Azure cloud service.
☐	Certificate for Unified Access Gateway in .pem format (Required for Unified Access Gateway.)
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 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 and is a member of the Horizon Cloud Administrators Group. **Note:** this account currently performs Domain Join Operations and should have the same permissions as the Domain Join Account. This is a known issue.
☐	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.
☐	Domain join account • Active Directory domain join account which can be used by the system to create computer objects, typically a new account ("domain join user account"). This account requires the following permissions: Create Computer Objects, Delete Computer Objects, and Write All Properties. For reference, see Domain Users Cannot Join Workstation or Server to a Domain.
☐	Active Directory groups • Horizon Cloud Administrators – Active Directory security group for Horizon Cloud administrators; contains the Horizon Cloud administrative users and domain bind 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 RDS session-based desktops and published applications in Horizon Cloud.
☐	Active Directory organizational unit(s) (OU) for RDS session-based desktops and/or published applications
PORTS AND FIREWALL REQUIREMENTS	
☐	LDAP port 389 (TCP and UDP)
☐	LDAP port 3268 (TCP)
☐	Kerberos port 88 (TCP and UDP)
☐	DNS port 53 (TCP and UDP)

☐	NTP port 123 (UDP)
☐	True SSO Enrollment Server port 32111 (TCP)
☐	Horizon Protocols – External Connection (Horizon Cloud deployment creates Network Security Group when deploying Unified Access Gateway). • TCP 443 – Login traffic, end-user portal, client drive redirection (CDR), multimedia redirection (MMR), and USB redirection • TCP/UDP 4172 – PCoIP • TCP 443 – Blast Extreme • UDP 8443 – Blast Extreme • UDP 443 – Blast Extreme Tunnel
☐	Horizon Protocols – Internal Connection • TCP 443 – Login traffic • TCP/UDP 4172 – PCoIP • TCP 22443 – Blast Extreme • UDP 22443– Blast Extreme • TCP 32111 – USB Redirection • TCP 9427 – Client drive redirection (CDR) and multimedia redirection (MMR) • TCP 32111 – USB redirection
HORIZON CLOUD BASE IMAGE AND FARMS	
☐	Base for Master Image – One of the supported Microsoft Azure VM configurations • Standard_D2_v2 • Standard_D3_v2 • Standard_D4_v2 • Standard_NV6
☐	RDS Server Model selection for the RDS Farms – One or more of the supported Microsoft Azure VM configurations • Standard_D2_v2 • Standard_D3_v2 • Standard_D4_v2 • Standard_NV6
LICENSING	
☐	Microsoft Windows Server 2012 R2 and/or 2016 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 to deploy and start administering the service.

1. Perform the preparatory tasks outside of Horizon Cloud. See Getting Started with VMware Horizon Cloud on Microsoft Azure.
2. Add cloud capacity and deploy the node. See Getting Started with VMware Horizon Cloud on Microsoft Azure.
3. Register your Active Directory domain with the deployed node. See *Register Your Horizon Cloud Node's First Active Directory Domain* in the Horizon Cloud Service on Microsoft Azure Administration Guide.
4. Upload SSL certificates, if you will have clients connecting directly to the node and not through Unified Access Gateway. See *Upload SSL Certificates to a Horizon Cloud Node* in the Horizon Cloud Service on Microsoft Azure Administration Guide.

   Uploading an SSL certificate is recommended, even if Unified Access Gateway is used. The SSL certificate ensures that clients making direct connections to the node environment can have trusted connections.
5. Configure an RDS-enabled server master image. See *Create a Master Virtual Machine from the Microsoft Azure Marketplace* in the Horizon Cloud Service on Microsoft Azure Administration Guide.
6. Convert that master image into an assignable image. See *Convert a Configured Master Virtual Machine to an Assignable Image* in the Horizon Cloud Service on Microsoft Azure Administration Guide.
7. Create an RDSH farm to provide session desktops and create assignments to use those desktops. See *Farms in Horizon Cloud* and *Create an RDSH Session Desktop Assignment* in the Horizon Cloud Service on Microsoft Azure Administration Guide.
8. Create an RDSH farm to provide remote applications and create assignments to those remote applications. See *Farms in Horizon Cloud, Importing New Applications from an RDSH Farm*, and *Create a Remote Application Assignment* in the Horizon Cloud Service on Microsoft Azure Administration Guide.
9. When a node is deployed to have Internet-enabled desktops, you must create a CNAME record in your DNS server that maps the fully qualified domain name (FQDN) that you entered in the deployment wizard to the node's load balancer's auto-generated public FQDN.

   When a node is deployed with the **Internet Enabled Desktops** option set to **Yes** (the default), the deployed Unified Access Gateway is configured with a load balancer IP address that has an autogenerated public FQDN in the form `vmw-hcs-nodeID-uag.region.cloudapp.azure.com`, where `node-ID` is the node's UUID and `region` is the Microsoft Azure region where the node is located. In the deployment wizard, you provided:

   - Your FQDN (for example, `ourOrg.example.com` or `ourApps.ourOrg.example.com`). This FQDN is the one which your end users use to access their desktops.
   - An SSL certificate that is associated with that FQDN and which is signed by a trusted certificate authority.

   Your DNS server must map those two FQDNs. When the addresses are mapped, your end users can enter your provided FQDN as the server address in the VMware Horizon Client™ or use the FQDN with HTML Access to access their desktops.

   ```
   ourApps.ourOrg.example.com
   vwm-hcs-nodeID-uag.region.cloudapp.azure.com
   ```

   For details on how to locate the load balancer's public FQDN in the Administration Console, see *Obtain the FQDN of the Node's Load Balancer to Map in your DNS Server* in the Horizon Cloud Service on Microsoft Azure Administration Guide.

   After the preceding workflow steps are completed, your end users can launch their assigned RDSH session-based desktops and remote applications using your FQDN in the Horizon Client or with HTML Access.

Reference Architecture

Use the architecture diagram below for reference. For additional details, see the VMware Horizon Cloud Service on Microsoft Azure Administration Guide.

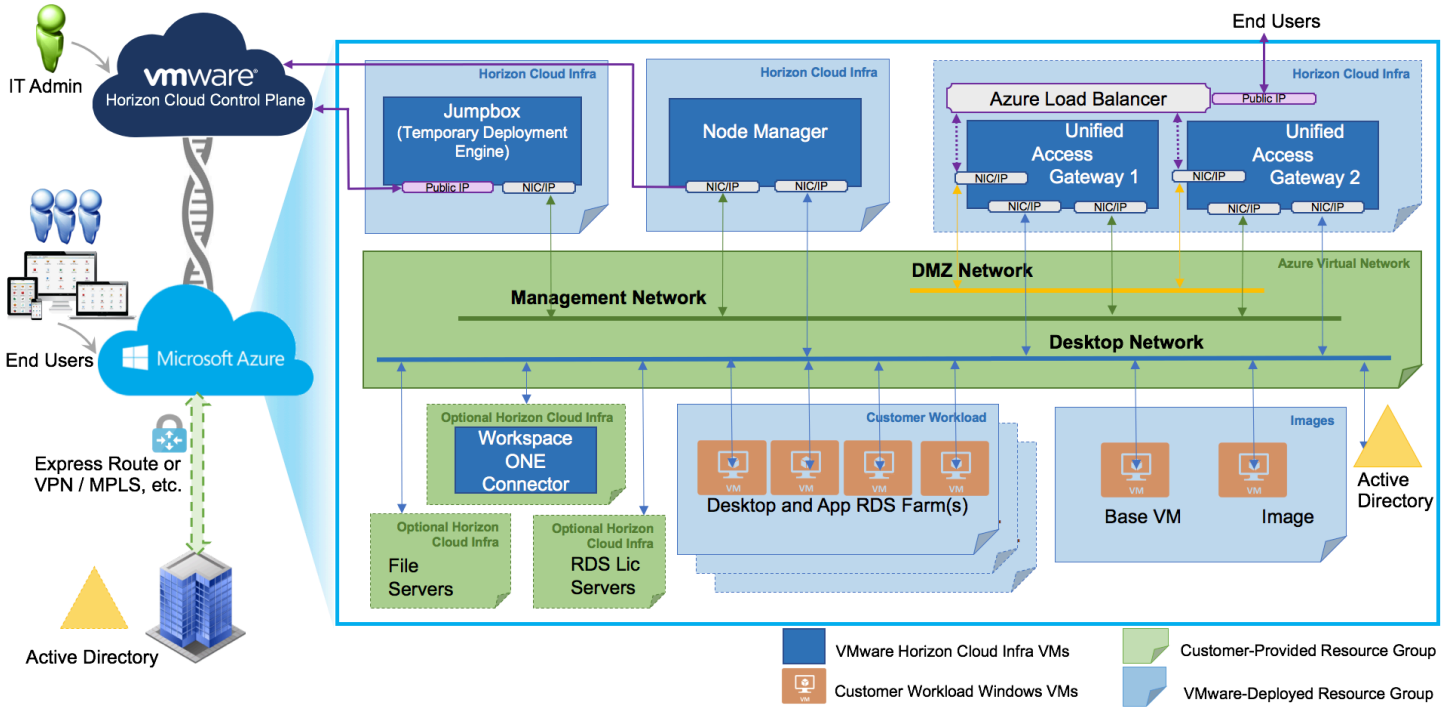

Figure 1: Horizon Cloud Service on Microsoft Azure Architecture

Resources

See the following resources for additional information.

- Getting Started with VMware Horizon Cloud on Microsoft Azure
- VMware Horizon Cloud Service on Microsoft Azure Administration Guide
- VMware Unified Access Gateway
- 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