Getting Started with VMware Horizon Cloud Service on Microsoft Azure

VMware Horizon Cloud Service

VMware Horizon Cloud Service on Microsoft Azure 1.4

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About this Getting Started Document

This *Getting Started* document for VMware Horizon Cloud Service™ on Microsoft Azure describes the process of deploying the necessary VMware Horizon Cloud Service on Microsoft Azure software components into the Microsoft Azure environment. You connect your own Microsoft Azure subscription to use with VMware Horizon® Cloud Service™ to manage and deliver virtual RDS-enabled Windows servers and remote applications.

For information about how to use the environment after you finish all the tasks outlined in this guide, see this product's *Administration* document.

Intended Audience

The information in this document is intended for experienced data center administrators with knowledge of Microsoft Azure, virtualization technology, and networking.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, visit http://www.vmware.com/support/pubs.

About the Screen Shots Used in this Document

The screen shots typically:

- Show only that portion of the overall user interface screen that corresponds to the text at which point the screen shot appears, and not necessarily the full user interface.
- Have blurred areas where appropriate to maintain data anonymity.

Note Some screen shots are taken at a higher resolution than others, and might look grainy when the PDF is viewed at 100%. However, if you zoom to 200%, those images start to look clear and readable.

Contacting VMware Support

Contact VMware Support when you need help with your Horizon Cloud environment.

- You can submit a support request to VMware Support online using your My VMware® account or by phone.
- KB 2144012 *Customer Support Guidelines* provides details for getting support depending on the issue encountered.
- You can submit a support request by logging in to the Administration Console and clicking ? **> Support**.

Introduction to a VMware Horizon Cloud Service on Microsoft Azure Environment

1

A VMware Horizon Cloud Service on Microsoft Azure environment combines the management simplicity of the Horizon Cloud control plane with the economics of Microsoft Azure. You connect your Microsoft Azure subscription to Horizon Cloud to manage and deliver virtual RDS-enabled Windows servers and remote applications. Setting up the environment involves deploying the required VMware software into your Microsoft Azure capacity. The deployed VMware software creates an appropriately configured entity, called a Horizon Cloud node, which pairs with the control plane. After the node is deployed, then you use the control plane to create RDSH farms and entitle remote desktops and applications to your end users.

VMware Horizon Cloud Service on Microsoft Azure Architecture

Horizon Cloud is a control plane that VMware hosts in the cloud. This cloud service enables the central orchestration and management of remote desktops and applications in your Microsoft Azure capacity.

VMware is responsible for hosting the service and providing feature updates and enhancements for a software-as-a-service experience.

The cloud control plane also hosts a common management user interface referred to as the Horizon Cloud Administration Console, or Administration Console for short. The Administration Console runs in industry-standard browsers and provides IT administrators a single location for management tasks involving user assignments and the virtual desktops, remote desktop sessions, and applications. The Administration Console is accessible from anywhere at any time, providing maximum flexibility.

Node Deployment in Microsoft Azure

A Horizon Cloud node, or node for short, has a physical regional location in a Microsoft Azure cloud. In the node deployment wizard, you select where to place the node, according to the regions available for your particular Microsoft Azure subscription. You also select an existing virtual network (vnet) that the node will use in your selected region.

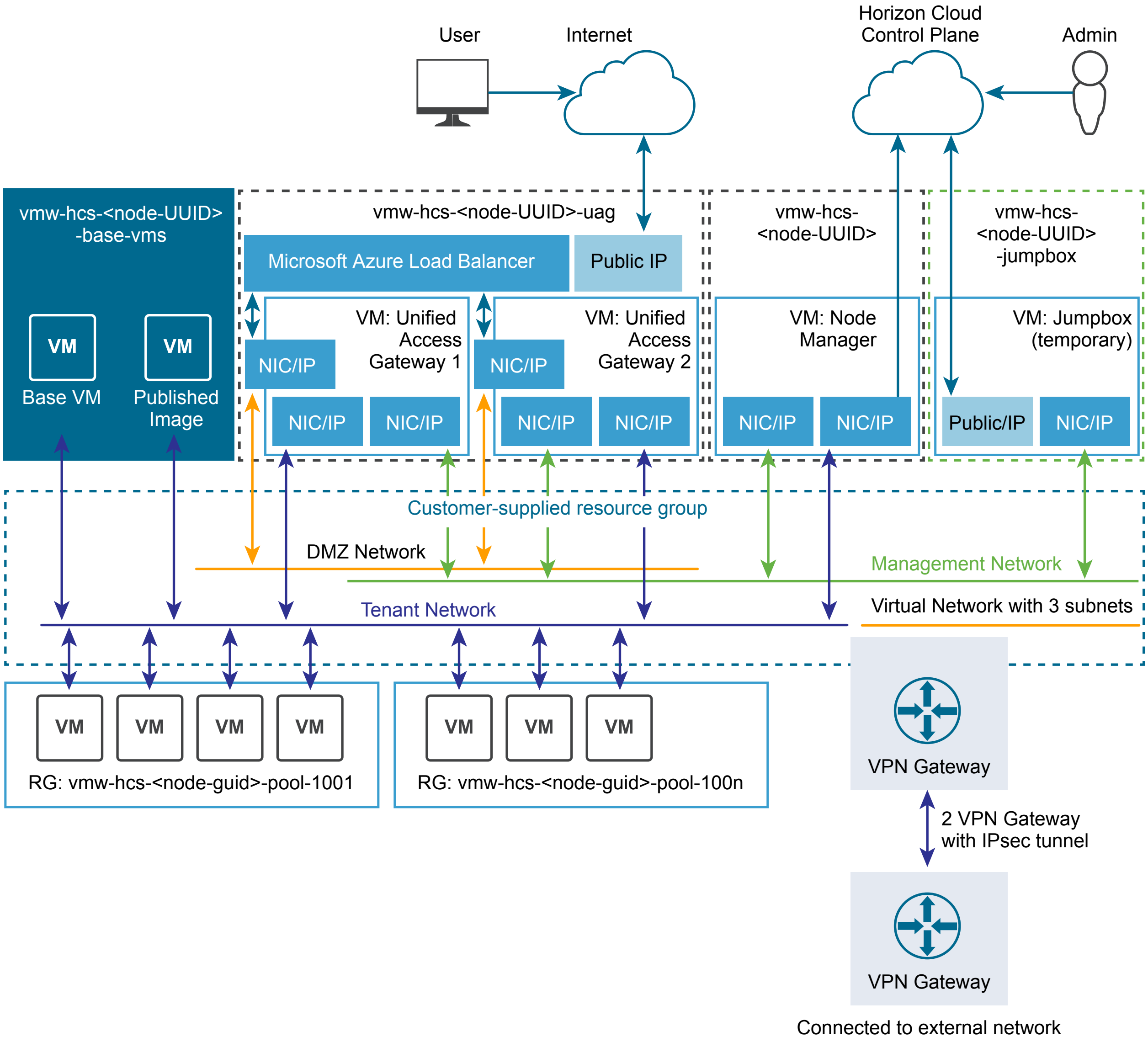
You can deploy more than one node and manage all of them from the Horizon Cloud Administrator Console. The nodes you deploy after the first one can reuse the same vnet as your first node or use different vnets. Also, each node can be in a different Microsoft Azure region, using a vnet in that region.

The node deployment process automatically creates a set of resource groups in your Microsoft Azure capacity. Resource groups are used to organize the assets that the environment needs, such as:

- Virtual subnets
- VMs for the node manager instance
- VMs for the Unified Access Gateway and load balancer instances
- VMs for the master RDS-enabled server images
- VMs for the assignable (published) images that are made from the master images
- VMs for the RDSH farms that provide the remote desktops and remote applications
- Additional assets that the VMs and the environment require for supported operations, such as network interfaces, IP addresses, disks, and various items along those lines.

All of the resource groups created by Horizon Cloud in your Microsoft Azure environment are named using the prefix `vmw-hcs`.

In the following diagram, `RG` means resource group.


User
Internet
Horizon Cloud Control Plane
Admin
vmw-hcs-<node-UUID> -base-vms
VM
Base VM
VM
Published Image
vmw-hcs-<node-UUID>-uag
Microsoft Azure Load Balancer
Public IP
VM: Unified Access Gateway 1
NIC/IP
NIC/IP
NIC/IP
VM: Unified Access Gateway 2
NIC/IP
NIC/IP
NIC/IP
vmw-hcs-<node-UUID>
VM: Node Manager
NIC/IP
NIC/IP
vmw-hcs-<node-UUID> -jumpbox
VM: Jumpbox (temporary)
Public/IP
NIC/IP
Customer-supplied resource group
DMZ Network
Management Network
Tenant Network
Virtual Network with 3 subnets
VM
VM
VM
VM
RG: vmw-hcs-<node-guid>-pool-1001
VM
VM
VM
RG: vmw-hcs-<node-guid>-pool-100n
VPN Gateway
2 VPN Gateway with IPsec tunnel
VPN Gateway
Connected to external network

Microsoft Azure Terminology and References

The VMware Horizon Cloud Service on Microsoft Azure product documentation uses the applicable Microsoft Azure terminology as appropriate in the descriptions and task steps of the VMware Horizon Cloud Service on Microsoft Azure workflows. If the Microsoft Azure terminology is unfamiliar to you, you can use the following applicable references in the Microsoft Azure product documentation to learn more.

Note All capitalization and spelling in the citations below follow the same capitalization and spelling found in the linked-to articles in the Microsoft Azure documentation itself.

Table 1-1. References in the Microsoft Azure Documentation That Relate to Your Use of Horizon Cloud

Useful Microsoft Azure References	Description
Microsoft Azure glossary: A dictionary of cloud terminology on the Azure platform	Use this glossary to learn the meaning of terms as used in the Microsoft Azure cloud context, for terms such as load balancer, region, resource group, subscription, virtual machine, and virtual network (vnet). **Note** The Microsoft Azure glossary does not include the term service principal because the service principal is a resource automatically created in Microsoft Azure when an application registration is created in Microsoft Azure. The purpose of making an application registration in your Microsoft Azure subscription is because that is the way you authorize Horizon Cloud *as an application* to use your Microsoft Azure capacity. The application registration and its companion service principal enable the Horizon Cloud cloud service acting as an application to access resources in your Microsoft Azure subscription. Use the next reference below to learn about applications and service principals that can access resources in Microsoft Azure.
Use portal to create an Azure Active Directory application and service principal that can access resources	Use this article to learn about the relationship between an application and a service principal in a Microsoft Azure cloud.
Azure Resource Manager overview	Use this article to learn about the relationships between resources, resource groups, and the Resource Manager in Microsoft Azure.
Azure VNet	Use this article to learn about the Azure Virtual Network (VNet) service in Microsoft Azure. See also Azure Virtual Network FAQs.
Azure VNet Peering	Use this article to learn about virtual network peering with the Azure VNet.

Suggested Workflow for a Horizon Cloud Node in Microsoft Azure

2

You must first deploy a node into your Microsoft Azure capacity and complete some steps in the Administration Console before you begin setting up virtual RDSH server farms, RDSH session-based desktops, and remote RDSH applications in Horizon Cloud and making them available to your end users.

1. Fulfill the prerequisites, as described in the separate prerequisites checklist document. You can open that document from this PDF link or navigate to it from the Horizon Cloud documentation landing page.

2. Perform the preparatory tasks outside of Horizon Cloud. See Chapter 3 Preparing to Deploy a Horizon Cloud Node Into Microsoft Azure.

3. Deploy the node. See Chapter 4 Deploy a Node for VMware Horizon Cloud Service on Microsoft Azure.

4. Register your Active Directory domain with the deployed node. See *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

5. Upload SSL certificates, if you plan to use VMware Identity Manager™, with or without True SSO, or will have clients connecting directly to the node, not through Unified Access Gateway. See *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

   Uploading an SSL certificate is recommended, even if Unified Access Gateway is used and you are not using VMware Identity Manager™. The SSL certificate ensures that clients making direct connections to the node environment can have trusted connections.

6. Configure an RDS-enabled server master image. See *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

7. In the master image, install the third-party applications you want to provide to your end users from that RDS image and configure other applicable customizations, such as setting desktop wallpaper, install the NVIDIA GPU drivers (for an NV6-based image), and optionally install the User Environment Manager agent. See *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

8. Convert that master image into an assignable image. See *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

9. Create an RDSH farm to provide session desktops and create assignments to use those desktops. See *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

10. Create an RDSH farm to provide remote applications and create assignments to those remote applications. See *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

11 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 auto-generated public FQDN in the form `vmw-hcs-`*`nodeID`*`-uag.`*`region`*`.cloudapp.azure.com`, where *nodeID* 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 Horizon Client or use 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 *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

After the above 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.

Preparing to Deploy a Horizon Cloud Node Into Microsoft Azure

3

Before you log in to the Horizon Cloud Administration Console and run the node deployment wizard for the first time, you must perform these preparatory tasks.

1 Fulfill the prerequisites described in the separate prerequisites checklist document, especially:

   - Ensure your Microsoft Azure account and subscription encompasses the node's required number and sizes of virtual machines. See Chapter 5 Microsoft Azure Virtual Machine Requirements for a Horizon Cloud Node.
   - Ensure a virtual network exists in the region in which you are going to deploy the node and that virtual network meets the requirements for a Horizon Cloud node. If you do not have an existing virtual network, create one that meets the requirements. See Configure the Required Virtual Network in Microsoft Azure.
   - Ensure that virtual network is configured to point to a valid Domain Name Services (DNS) server that can resolve external names. See Configure the Virtual Network's DNS Server.
   - Ensure you have an Active Directory setup that is supported for use with this release, and your virtual network can reach it. See Chapter 6 Active Directory Domain Configurations.

2 Create a service principal and get your Microsoft Azure subscription ID, application ID, application authentication key, and Microsoft Azure AD Directory ID. These resources are used by Horizon Cloud to perform its operations on your Microsoft Azure environment. For detailed steps, see Create the Required Service Principal by Creating an Application Registration.

   Note Ensure the service principal has the Contributor role, and not the Owner role. The Microsoft Azure role-based access control (RBAC) provides the Contributor role to create and manage resources in your subscription. For details, see Built-in roles for Azure role-based access control in the Microsoft Azure documentation.

3 If you want to have Internet-enabled desktops, so that users outside of your corporate network can access them, obtain the SSL server certificate that can allow your end users' clients to trust connections to the desktops. This certificate should match your FQDN that your end users will use in their clients and be signed by a trusted Certificate Authority (CA).

   To support desktops and applications that users can access from the Internet,
   Unified Access Gateway is deployed as part of the node deployment process.
   Unified Access Gateway presents your CA-signed certificate, so that the clients can trust the connections.

4 Obtain a My VMware account and register for Horizon Cloud, if you are not already registered for it.

After you have completed those preparatory tasks, log in to the Horizon Cloud Administration Console at cloud.horizon.vmware.com using your My VMware account. After logging in, you'll see the **Add Cloud Capacity** area on the screen and can click **Add** to start the node deployment wizard. Complete the wizard by entering the required information in each screen. For detailed steps, see Chapter 4 Deploy a Node for VMware Horizon Cloud Service on Microsoft Azure.

This section includes the following topics:

- Configure the Required Virtual Network in Microsoft Azure
- Configure the Virtual Network's DNS Server
- Create the Required Service Principal by Creating an Application Registration
- Subscription-Related Information for the Deployment Wizard

Configure the Required Virtual Network in Microsoft Azure

Your Microsoft Azure environment must have an existing virtual network before you can deploy the Horizon Cloud node into the environment. If you do not already have a virtual network in the region into which you are deploying, you must create the virtual network.

In the node deployment wizard, you will select the virtual network and specify the address spaces for subnets that the node will create in the virtual network:

- Management subnet, for IP addresses used by the VMs involved in management activities of the node itself
- Desktop subnet, for IP addresses used for the RDSH VMs on that subnet

  Important The RDS images and every server in the node's RDS farms consume these IP addresses. Because this desktop subnet cannot be extended after the node is deployed, ensure you set this range large enough to accommodate the number of desktops you anticipate you will want this node to provide. For example, if you anticipate this node should provide over 1000 desktops in the future, ensure this range provides for more than that number of IP addresses.

- DMZ subnet, for IP address used by the Unified Access Gateway VMs, which are deployed when the **Internet Enabled Desktops** option is selected in the deployment wizard

When you specify subnet address spaces that are already contained within the virtual network's existing address space, the deployer creates the new subnets in the virtual network. When you specify subnet address spaces that are different from the virtual network's existing ones, the deployer automatically updates the virtual network configuration to add those address spaces, and then it creates the new subnets in the virtual network.

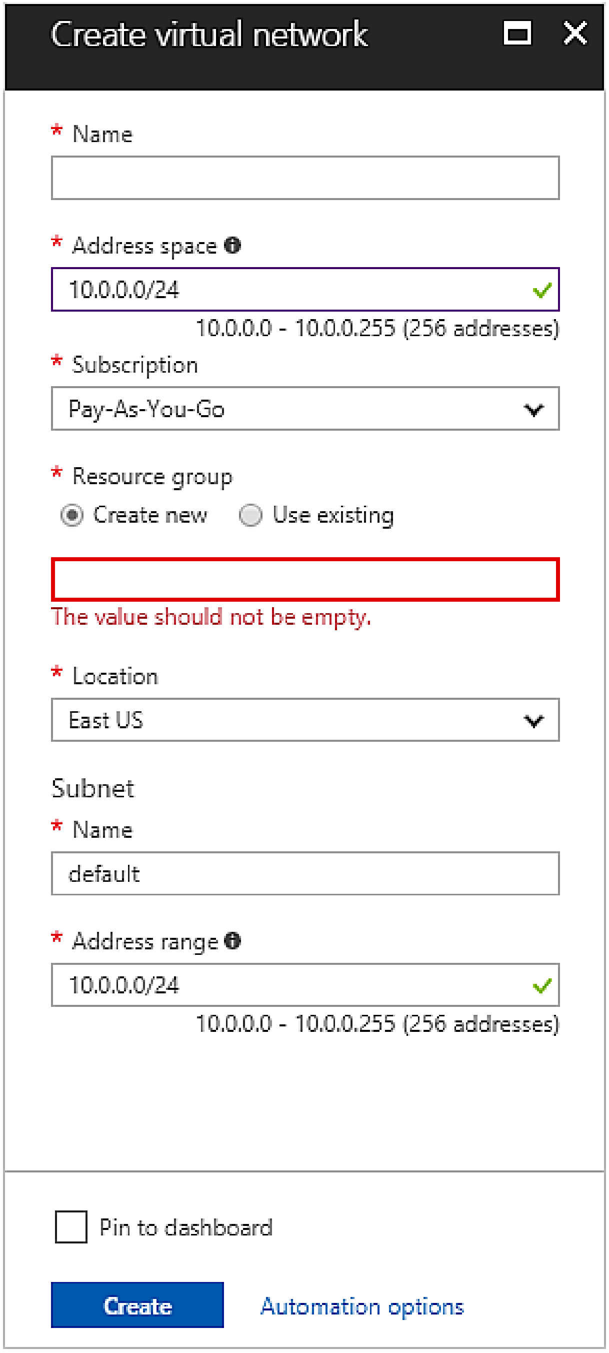
Note If your existing virtual network is peered, its address space cannot be updated. If the virtual network is peered and you specify subnet address spaces that are not contained within the virtual network's existing address space, the wizard will display an error message and you will need to specify valid subnet address spaces to proceed, or use an unpeered virtual network.

Use the Microsoft Azure portal appropriate for your registered account. If you registered with Microsoft Azure Germany or Microsoft Azure China, log in to the portal using the appropriate URL.

Procedure

1 From the Microsoft Azure portal's left navigation bar, click Virtual networks (**Virtual networks**) and then click **Add**.

   The **Create virtual network** screen appears.



Create virtual network

* Name

* Address space
10.0.0.0/24 ✓
10.0.0.0 - 10.0.0.255 (256 addresses)

* Subscription
Pay-As-You-Go

* Resource group
● Create new ○ Use existing

The value should not be empty.

* Location
East US

Subnet

* Name
default

* Address range
10.0.0.0/24 ✓
10.0.0.0 - 10.0.0.255 (256 addresses)

□ Pin to dashboard

2 Provide the information for the required fields.

You can either choose an existing resource group or have a new one created when the virtual network is created.

For the **Location** field, select the same region into which you are planning to deploy the Horizon Cloud node.

3 Click **Create**.

The virtual network is created in your Microsoft Azure account.

What to do next

Configure the newly created virtual network with a working DNS service and connectivity to the Active Directory service you will use with your node. See the steps in Configure the Virtual Network's DNS Server.

Configure the Virtual Network's DNS Server

The virtual network that you use for Horizon Cloud node must have the ability to resolve both internal machine names and external names. During and after the node deployment process, the Horizon Cloud node needs the ability to resolve external names. The ability to resolve internal virtual machine (VM) names is needed for the node's Horizon Cloud Active Directory domain-join operations with the VMs that get deployed in your Microsoft Azure environment.

In a Microsoft Azure subscription, internal network connectivity is not set up by default. For production environments, you would typically configure the virtual network's DNS settings to point at a valid DNS server that can resolve external names as well as work in Microsoft Azure for your corporate machines. For example, you might want to deploy a Microsoft Windows Server 2016 virtual machine in that virtual network to act as the DNS server, and configure the virtual network's DNS setting to point to the IP address of that deployed DNS server.

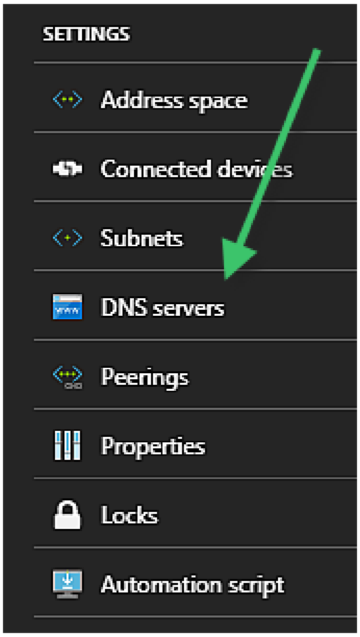
For proof-of-concept environments, if your organization's privacy and security policies allow, you can configure the internal DNS to delegate to an external public DNS for external name resolution. Some organizations and ISPs provide public recursive name servers to use for such purposes, such as OpenDNS at 208.67.222.222 or Google Public DNS at 8.8.8.8. For a sample list of public recursive name servers, see the Wikipedia article Public recursive name server.

Prerequisites

Ensure your Microsoft Azure region has the virtual network that you plan to use for your node. See Configure the Required Virtual Network in Microsoft Azure

Procedure

1. From the Microsoft Azure portal's left navigation bar, click (**Virtual networks**) and then click the virtual network that you are going to use for your node.
2. Display the virtual network's DNS server settings by clicking **DNS servers**.



3 Using the **Custom** option, add the address of the DNS server you want to use for name resolution and click **Save**.

Create the Required Service Principal by Creating an Application Registration

Horizon Cloud needs a service principal to access and use your Microsoft Azure subscription's capacity. When you register a Microsoft Azure AD application, the service principal is also created. Additionally, you must generate an authentication key and assign the Contributor role to the service principal at the subscription level.

You perform these steps in the Microsoft Azure portal appropriate for your registered account. If you registered with Microsoft Azure Germany or Microsoft Azure China, log in to the portal using the appropriate URL.

Note When performing these steps, you can collect some of the values that you will need for the deployment wizard, as described in Chapter 1 Introduction to a VMware Horizon Cloud Service on Microsoft Azure Environment, specifically:

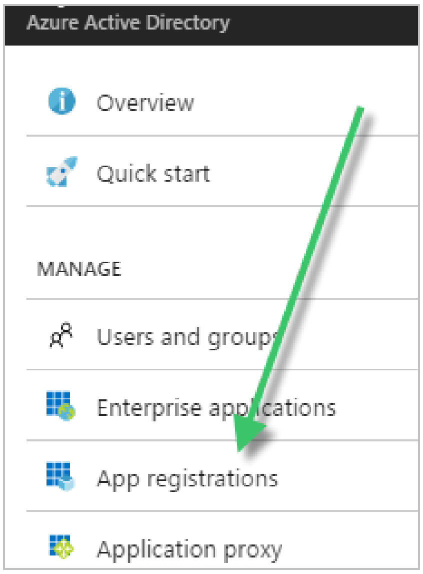
- Application ID
- Authentication key

Caution Even though you can set the key's expiration duration to a specific timeframe, if you do that, you must remember to refresh the key before it expires or the associated Horizon Cloud node will stop working. Horizon Cloud cannot detect or know what duration you set. For smooth operations, set the key's duration to **Never expires**.

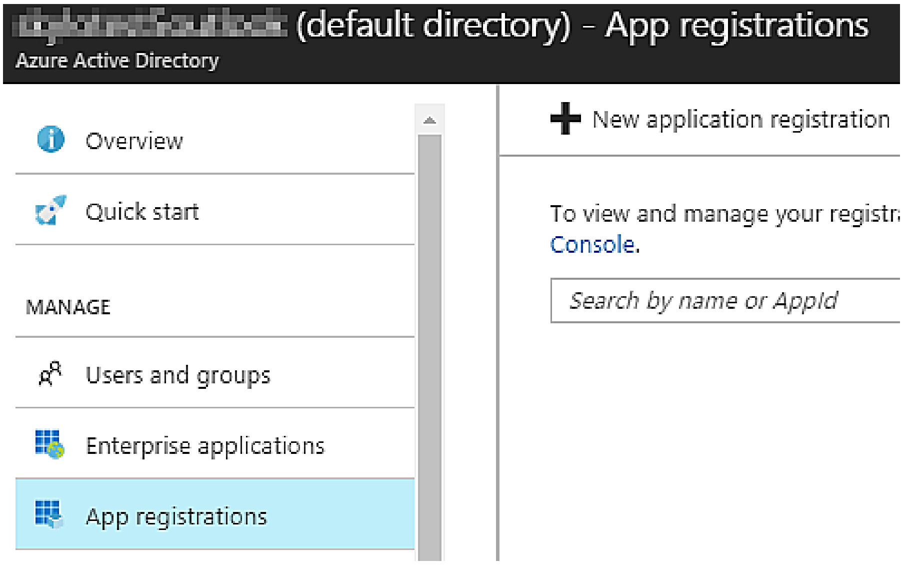
If you prefer not to set **Never expires** and prefer instead to refresh the key before it expires, you must remember to log in to the Horizon Cloud Administration Console and enter the new key value in the associated node's subscription information. For detailed steps, see Update the Subscription Information Associated with Deployed Nodes in the VMware Horizon Cloud Service on Microsoft Azure Administration Guide.

Procedure

1 From the Microsoft Azure portal's left navigation bar, click (**Azure Active Directory**), then click (**App registrations**).



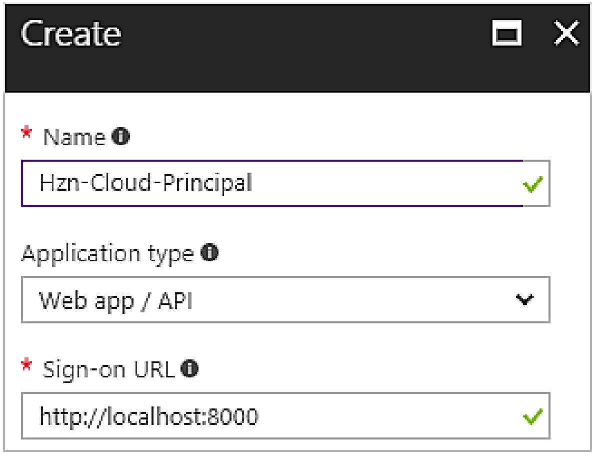
The **App registrations** screen appears.



To view and manage your registr
Console.

2 Click + New application registration (**New application registration**).

3 Type a descriptive name, select **Web app / API** for the **Application Type**, type `http://localhost:8000` for the **Sign-on URL**, and click **Create**.



Create

* Name

Hzn-Cloud-Principal

Application type

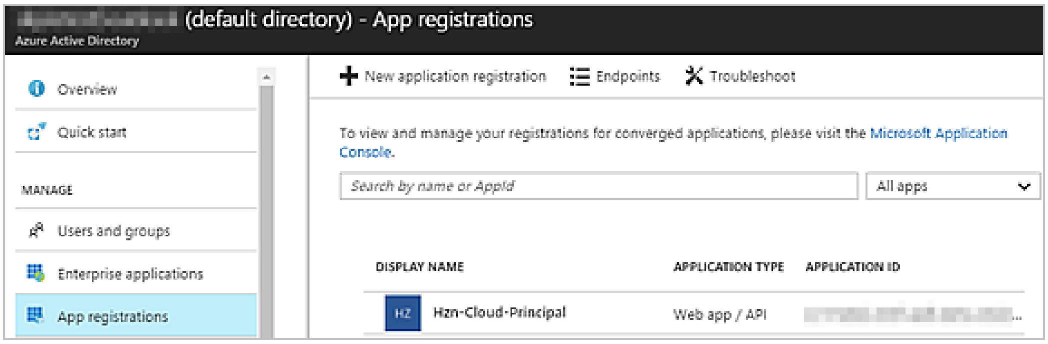
Web app / API

* Sign-on URL

http://localhost:8000

Option	Description
Name	The name is up to you. The name is a way you can differentiate this service principal used by Horizon Cloud from any other service principals that might exist in this same subscription.
Application type	Ensure **Web app / API** is selected (the default value).
Sign-on URL	Type `http://localhost:8000` as shown. Microsoft Azure marks this as a required field. Because Horizon Cloud does not need a sign-on URL for the service principal `http://localhost:8000` is used to satisfy the Microsoft Azure requirement.

Now the newly created item is displayed on screen.



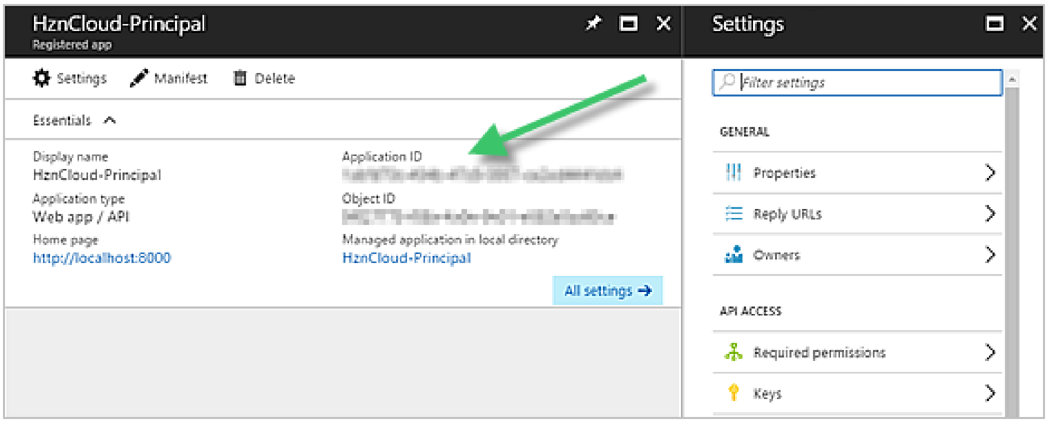
[redacted] (default directory) - App registrations

Azure Active Directory

To view and manage your registrations for converged applications, please visit the Microsoft Application Console.

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
HZ Hzn-Cloud-Principal	Web app / API	[redacted]...

4 Click the service principal's icon to collect its application ID from its details.

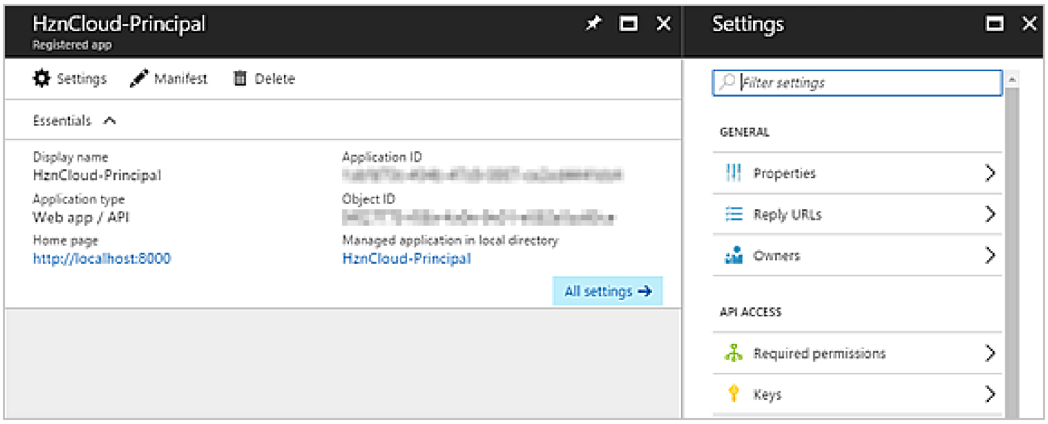


Display name: HznCloud-Principal
Application type: Web app / API
Home page: http://localhost:8000
Application ID: [redacted]
Object ID: [redacted]
Managed application in local directory: HznCloud-Principal

Copy the application ID to a location where you can retrieve it later when you run the deployment wizard.

5 From the service principal's details screen, create the service principal's authentication key.

a If the Settings menu is not visible, open it by clicking **Settings**.



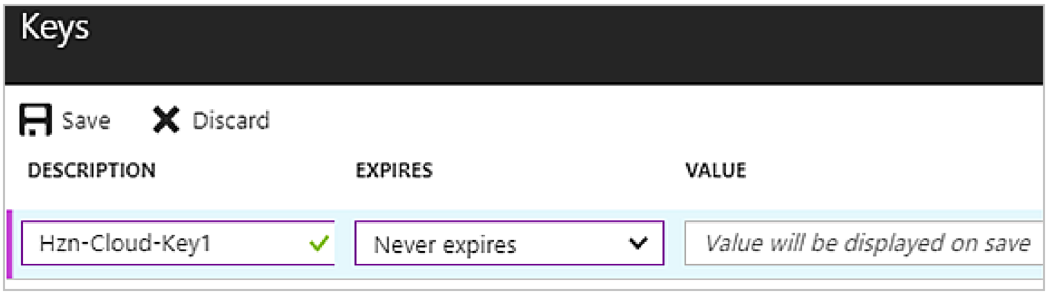
Display name: HznCloud-Principal
Application type: Web app / API
Home page: http://localhost:8000
Application ID: [redacted]
Object ID: [redacted]
Managed application in local directory: HznCloud-Principal

b Click 🔑 Keys (**Keys**).

c Type a key description, select an expiration duration, and click **Save**.

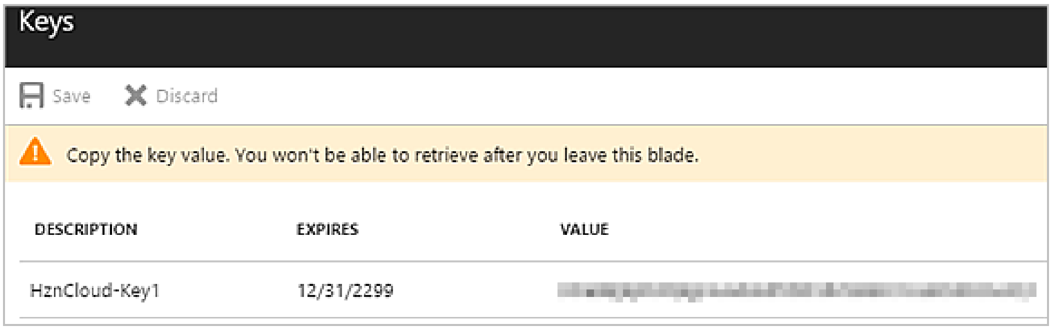
The key description must be 16 characters or less, for example `Hzn–Cloud–Key1`.

Note You can set the expiration duration to **Never expires** or to a specific timeframe. However, if you set a specific duration, you must remember to refresh the key before it expires and enter the new key into the node's subscription information in the Horizon Cloud Administration Console. Otherwise, the associated node will stop working. Horizon Cloud cannot detect or know what duration you set.



DESCRIPTION	EXPIRES	VALUE
Hzn-Cloud-Key1 ✓	Never expires	*Value will be displayed on save*

Important Keep the Keys screen open until you copy the key value and paste the value into a location where you can retrieve it later. Do not close the screen until you have copied the key value.



Copy the key value. You won't be able to retrieve after you leave this blade.

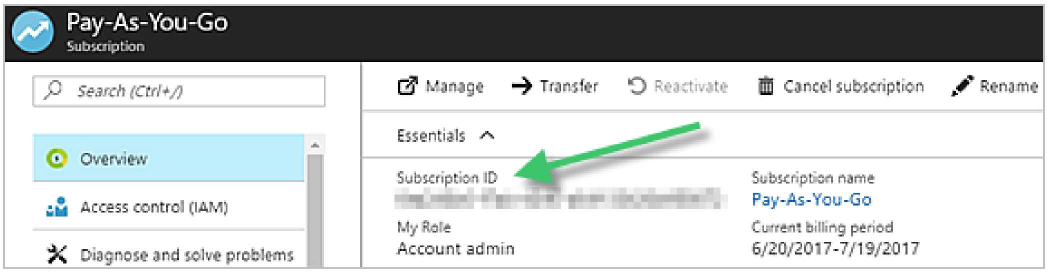
DESCRIPTION	EXPIRES	VALUE
HznCloud-Key1	12/31/2299	[redacted]

d Copy the key value to a location where you can retrieve it later when you run the deployment wizard.

6 Assign the Contributor role to the service principal at the subscription level.

a Navigate to your subscription's settings screen by clicking Subscriptions (**Subscriptions**) in the Microsoft Azure portal's main navigation bar and then click the name of the subscription that you will use with the node.

Note At this point, from the screen, you can copy the subscription ID which you will later need in the deployment wizard.



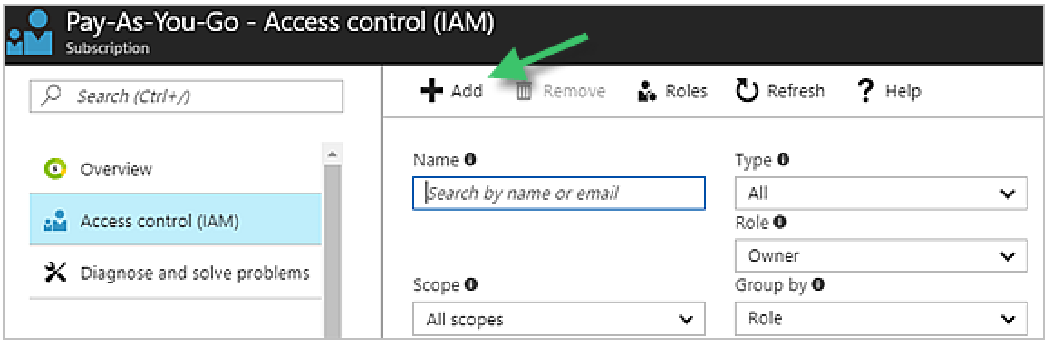
Subscription ID
[redacted]

Subscription name
Pay-As-You-Go

My Role
Account admin

Current billing period
6/20/2017-7/19/2017

b Click Access control (IAM) (**Access control (IAM)**) and then click **Add** to open the **Add permissions** screen.



Name
Search by name or email

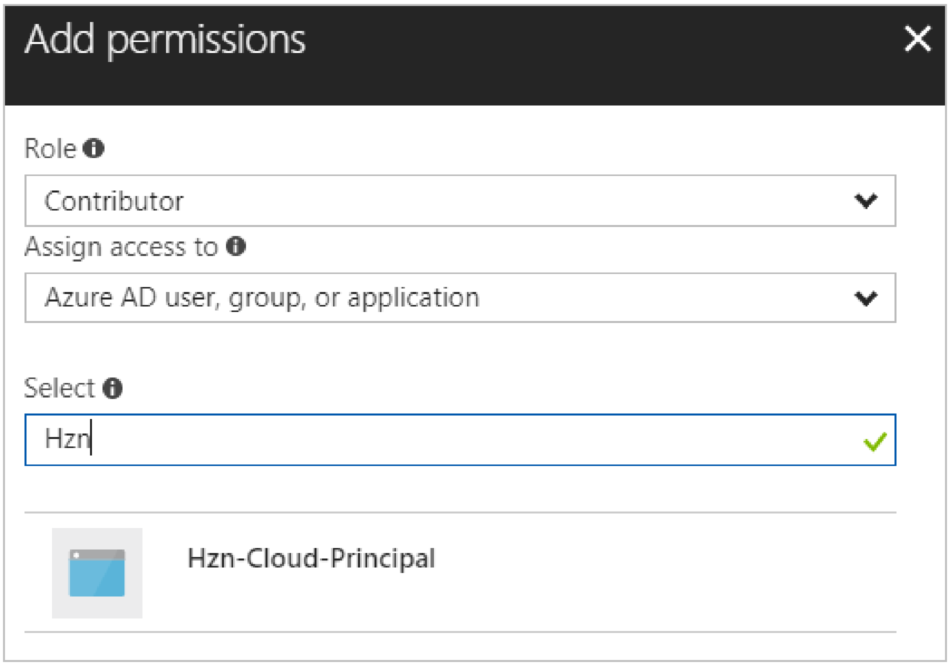
Type
All

Role
Owner

Scope
All scopes

Group by
Role

c In the **Add permissions** screen, select `Contributor` for **Role** and then use the **Select** box to search for your service principal by the name you gave it.



Add permissions

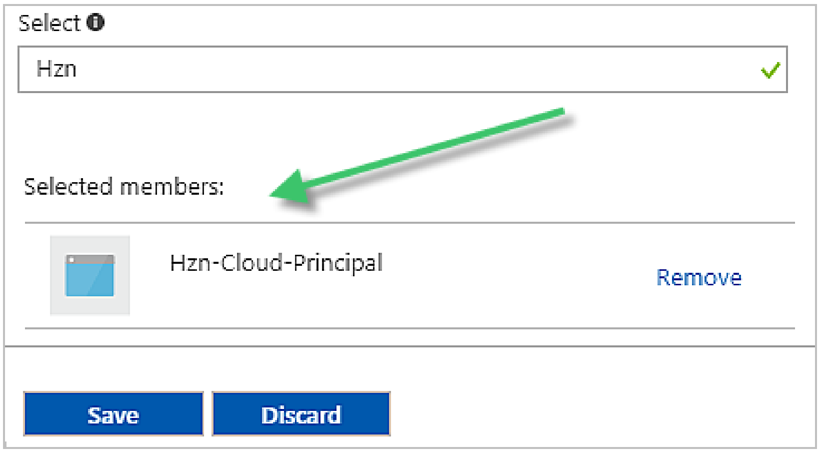
Role: Contributor

Assign access to: Azure AD user, group, or application

Select: Hzn

Note Make sure the **Assign access to** drop-down list is set to **Azure AD user, group, or application**.

d Click your service principal to make it a selected member and then click **Save**.

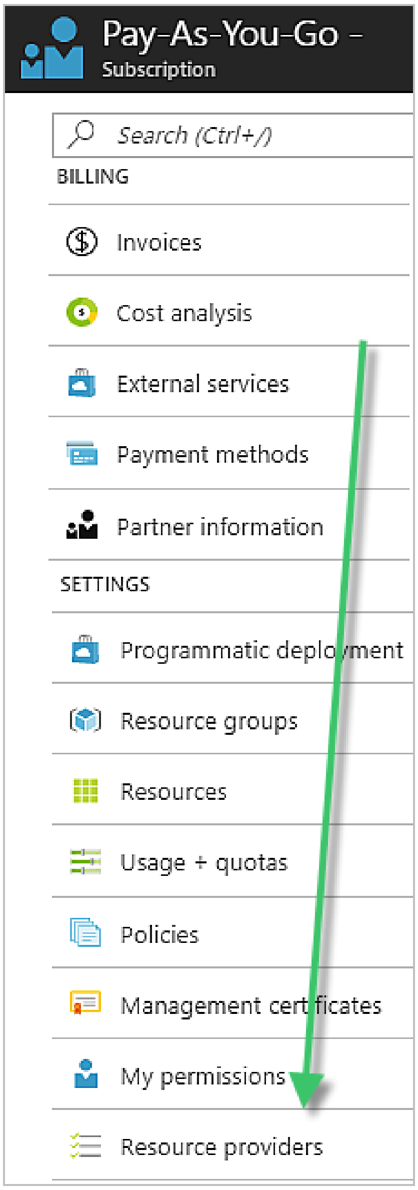


Select: Hzn

Selected members:

7 Verify that your subscription has the registered resource providers that the node requires.

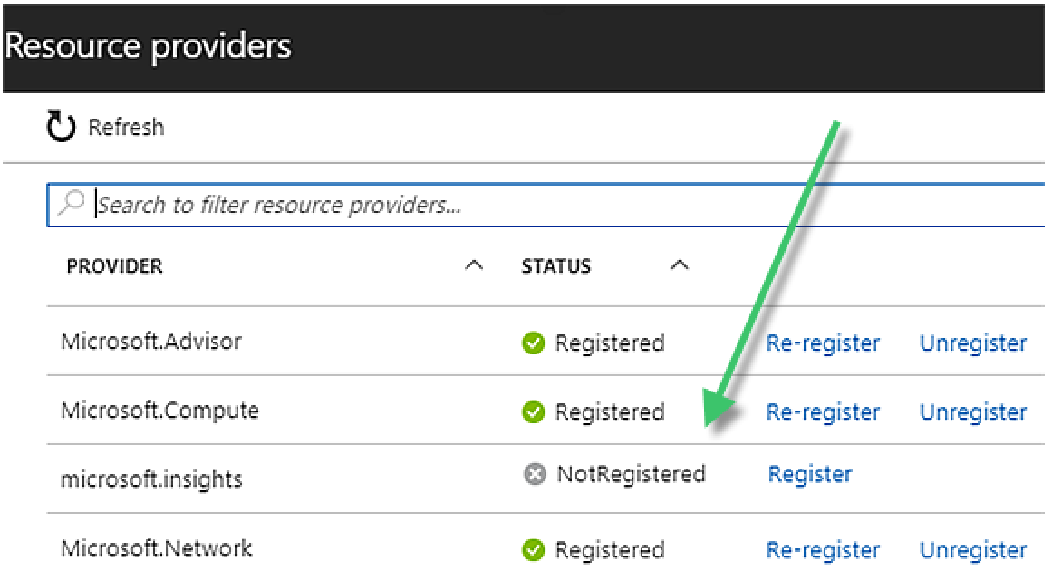
a From the Access control (IAM) screen you are on from the previous step, navigate to the subscription's list of resource providers by clicking ☰ Resource providers (**Resource providers**) in the subscription's menu.



b Verify that the following resource providers have ✓ Registered (**Registered**) status, and if not, register them.

- `Microsoft.Compute`
- `microsoft.insights`
- `Microsoft.Network`

- `Microsoft.Storage`



Resource providers

PROVIDER	STATUS		
Microsoft.Advisor	Registered	Re-register	Unregister
Microsoft.Compute	Registered	Re-register	Unregister
microsoft.insights	NotRegistered	Register	
Microsoft.Network	Registered	Re-register	Unregister

At this point, you've created and configured the service provider for the node, and you have three of the subscription-related values you need in the first step of the node deployment wizard. You also need the Azure Active Directory ID. Obtain that ID in the Microsoft Azure portal by clicking Azure Active Directory > Properties (under **Manage**).

The four subscription-related values are:

- Subscription ID
- Azure Active Directory ID
- Application ID
- Application key value

What to do next

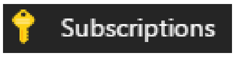
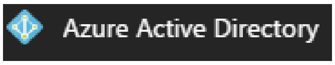
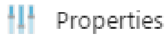
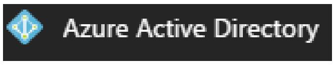
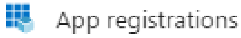
Verify that you have collect all of the subscription-related information you will enter in the deployment wizard. See Subscription-Related Information for the Deployment Wizard.

Subscription-Related Information for the Deployment Wizard

The Horizon Cloud node deployment wizard requires you to provide the following pieces of information from your Microsoft Azure subscription.

Note You must obtain the application key at the moment you generate it in the Microsoft Azure portal. For information, see Create the Required Service Principal by Creating an Application Registration. You can obtain the other pieces of information at any time by logging in to your Microsoft Azure portal using your Microsoft Azure account credentials.

The IDs are UUIDs, in the form 8-4-4-4-12. These IDs and key described in the following table are used in the first step of the node deployment wizard.

Required Value	How to Collect	Your Values
Environment	You determine the Microsoft Azure cloud environment when you register for your Microsoft Azure subscription. At that point in time, your account and subscription is created within the specific Microsoft Azure environment.	
Subscription ID	In the Microsoft Azure portal, click  in the left menu.	
Directory ID	In the Microsoft Azure portal, click  >  (under **Manage**).	
Application ID	In the Microsoft Azure portal, click  > , and then click the application registration that you created for Horizon Cloud using the steps in Create the Required Service Principal by Creating an Application Registration.	
Application Key	Obtain the key when you generate it in the Microsoft Azure portal. See Create the Required Service Principal by Creating an Application Registration.	

Deploy a Node for VMware Horizon Cloud Service on Microsoft Azure 4

You run the node deployment wizard to deploy the component called a Horizon Cloud node, or node for short. This component pairs with Horizon Cloud so that you can use your Microsoft Azure capacity with Horizon Cloud.

Note The IP addresses mentioned in these steps are examples. You should use the address ranges that meet your organization's needs. For each step that mentions an IP address range, substitute ones that are applicable for your organization.

Prerequisites

Verify that all of the preparatory tasks are completed, as described in Chapter 3 Preparing to Deploy a Horizon Cloud Node Into Microsoft Azure.

Verify that you have an existing virtual network in your Microsoft Azure subscription, and in the region in which you are deploying the node, as described in Configure the Required Virtual Network in Microsoft Azure.

Verify that virtual network is configured to point to a DNS that can resolve external addresses.

Verify that the management subnet, desktop subnet, and DMZ subnet (when choosing Internet-enabled desktops) that you want to use do not overlap. You enter these subnets using CIDR notation (classless inter-domain routing notation). The wizard will display an error if the entered subnets overlap. For the management and DMZ subnets, a CIDR of at least /28 is required. If you want to keep the management and DMZ subnet ranges co-located, you can make the DMZ subnet the same as the management subnet with an IP specified. For example, if the management subnet is 192.168.8.0/28, the DMZ subnet would be 192.168.8.32/28.

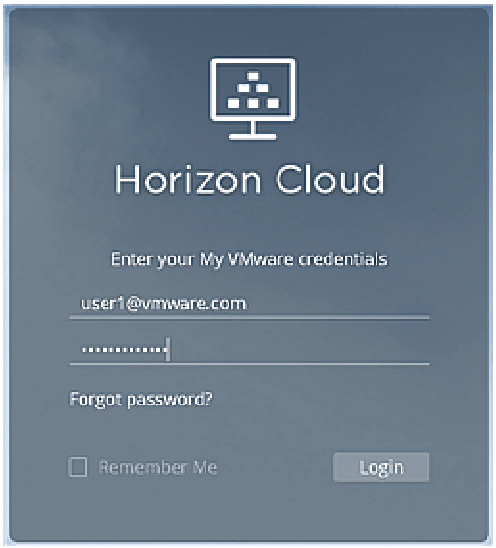
Important The CIDRs you enter must be defined so that each combination of prefix and bit mask results in an IP address range having the prefix as the starting IP address. Microsoft Azure requires that the CIDR prefix be the start of the range. For example, a correct CIDR of 192.168.182.48/28 would result in an IP range of 192.168.182.48 to 192.168.182.63, and the prefix is the same as the starting IP address (192.168.182.48). However, an incorrect CIDR of 192.168.182.60/28 would result in an IP range of 192.168.182.48 to 192.168.182.63, where the starting IP address is not the same as the prefix of 192.168.182.60. Ensure that your CIDRs result in IP address ranges where the starting IP address matches the CIDR prefix.

If you are planning to use the Unified Access Gateway capability to have Internet-enabled desktops, you must have the required fully qualified domain name (FQDN) which your end users will use to access the service and have a signed SSL certificate (in PEM format) based on that FQDN. The certificate must be signed by a trusted CA.

Procedure

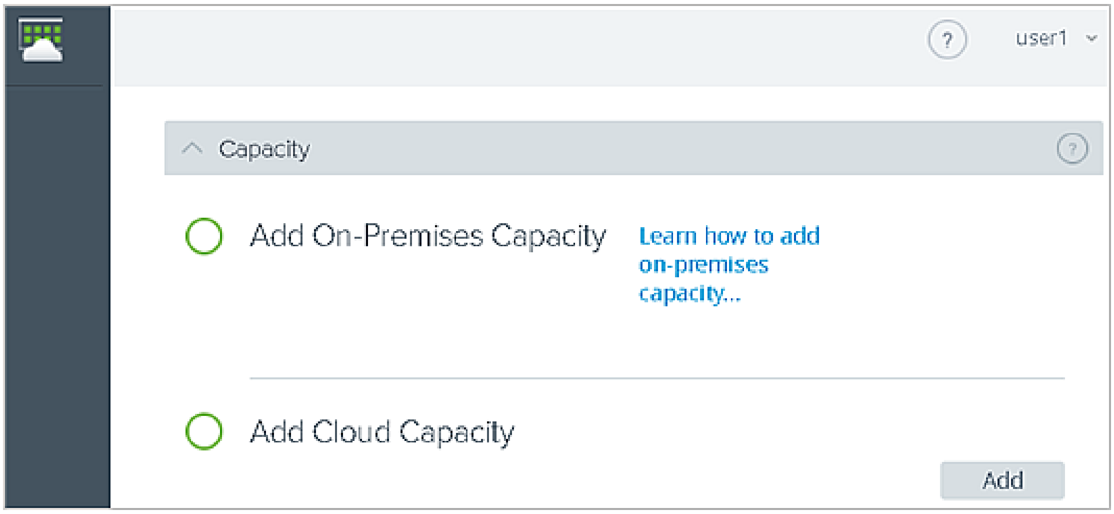
1 Log in to the Horizon Cloud Administration Console at https://cloud.horizon.vmware.com using your My VMware account ID and password.

A My VMware account ID has the form of `user@vmware.com.`



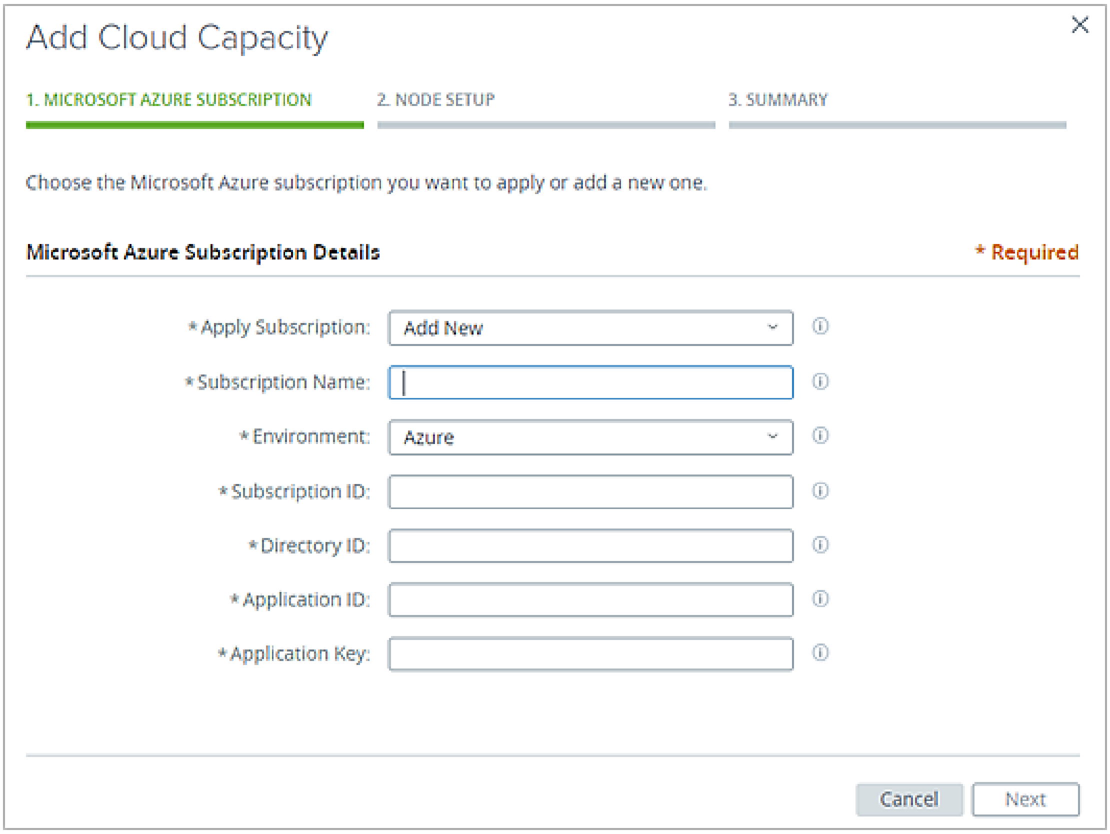
user1@vmware.com

After signing in, the Horizon Cloud Administration Console opens. When you have no existing nodes, the Getting Started wizard is displayed by default with the Capacity section expanded.



2 In the Add Cloud Capacity area, click **Add**.

The Add Cloud Capacity wizard opens to its first step.



Add Cloud Capacity

Choose the Microsoft Azure subscription you want to apply or add a new one.

Microsoft Azure Subscription Details

* Required

*Apply Subscription: Add New

*Subscription Name:

*Environment: Azure

*Subscription ID:

*Directory ID:

*Application ID:

*Application Key:

3 Provide the required information.

Note If you use your mouse, keyboard, or touchpad to copy and paste a value from the Microsoft Azure portal user interface directly into one of these fields, ensure the copy action does not include any extra spaces or tabs at the beginning or end of the value before pasting it into the field.

Option	Description
Apply Subscription	Select the name of a previously entered subscription or select **Add New** to enter new subscription information.
Subscription Name	When providing new subscription information, enter a friendly name so you can identify this subscription from other previously entered subscriptions.
Environment	Select the cloud environment associated with your subscription.
Subscription ID	Enter your cloud capacity subscription ID (in UUID form). This subscription ID must be valid for the environment you selected. For Microsoft Azure, you can obtain this UUID from your Microsoft Azure portal's Subscriptions area.
Directory ID	Enter your Microsoft Azure AD Directory ID (in UUID form). For Microsoft Azure, you can obtain this UUID from your Microsoft Azure Active Directory properties in the Microsoft Azure portal.

Option	Description
Application ID	Enter the application ID (in UUID form) associated with the service principal you created in the Microsoft Azure portal. Creating an application registration and its associated service principal in your Microsoft Azure Active Directory is a prerequisite.
Application Key	Enter the key value for the service principal's authentication key that you created in the Microsoft Azure portal. Creating this key is a prerequisite.

4 Click **Next**.

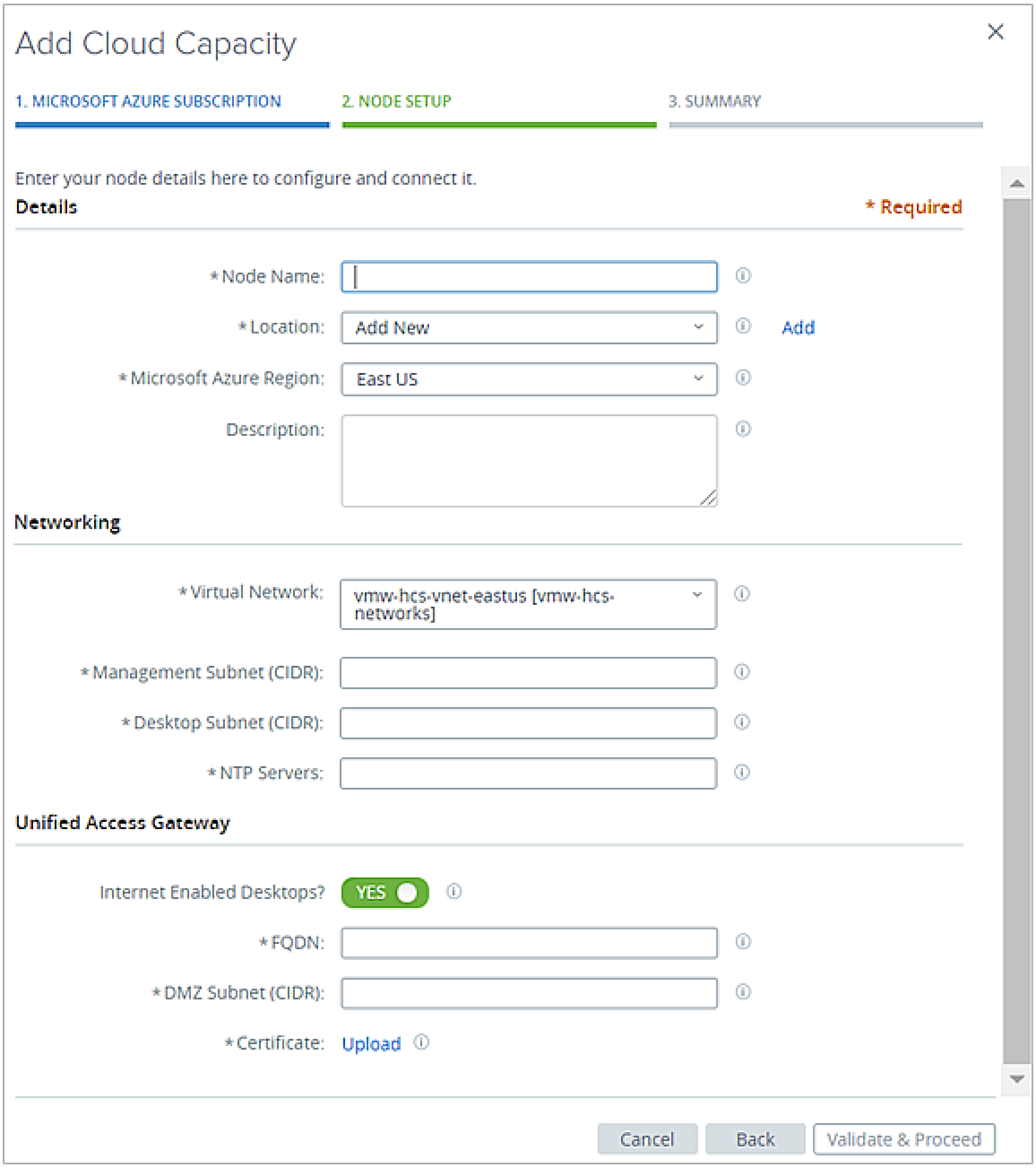
When you click **Next**, the system verifies the validity of all of the specified values and whether they are appropriately related to each other, such as:

- Is the specified subscription ID valid in the selected environment.
- Are the specified directory ID, application ID, and application key valid in that subscription.
- Is the `Contributor` role configured on the application's service principal for the specified application ID.

If you see an error message about checking values, at least one of the values is invalid either by not existing in your subscription or not having a valid relationship with another of the values. For example, if you specified a **Directory ID** that is in your subscription but you specified an **Application ID** value that is in a different directory, the error message will display.

More than one value might be invalid if that error message appears. If you see that error message, verify the subscription-related information that you collected and the configuration of the service principal.

5 In this step of the wizard, provide the required networking information.



Add Cloud Capacity

Enter your node details here to configure and connect it.

Details

* Required

*Node Name:

*Location: Add New

*Microsoft Azure Region: East US

Description:

Networking

*Virtual Network: vmw-hcs-vnet-eastus [vmw-hcs-networks]

*Management Subnet (CIDR):

*Desktop Subnet (CIDR):

*NTP Servers:

Unified Access Gateway

Internet Enabled Desktops? YES

*FQDN:

*DMZ Subnet (CIDR):

*Certificate: Upload

Option	Description
Node Name	Enter a friendly name for this node. This name is used in the Administration Console to identify this node from your other nodes.
Location	Select an existing location or click **Add** to specify a new one. Locations group your nodes according to names you provide (Business Unit A, Business Unit B, East Coast Stores, and so on).

Option	Description
Microsoft Azure Region	Select the physical geographic Microsoft Azure region into which you want the node to be deployed. The available regions are determined by the previously selected Microsoft Azure environment. Consider choosing the region based on its proximity to the end users you intend to serve with this node. Nearer proximity would provide lower latency.
Description	Optional: Enter a description for this node.
Virtual Network	Select a virtual network from the list. Only virtual networks (vnets) that exist in the region selected in the Microsoft Azure Region field are shown here. You must have already created the vnet you want to use in that region in your Microsoft Azure subscription.
Management Subnet (CIDR)	Enter a subnet (in CIDR notation) to which the node and Unified Access Gateway instances get connected, such as 192.168.8.0/28. For the management subnet, a CIDR of at least /28 is required.
Desktop Subnet (CIDR)	Enter the subnet (in CIDR notation) to which all of this node's RDSH servers for end-user remote desktops and applications get connected, such as 192.168.12.0/22. Minimum: /28. Recommended: /22.
NTP Servers	Enter the list of NTP servers to use for time synchronization, separated by commas (for example 10.11.12.13, time.example.com)
Internet Enabled Desktops?	When **Yes** is selected, access to desktops and applications is enabled for users located outside of your corporate network. The node includes a load balancer and Unified Access Gateway instances to enable this access. **Note** Leaving the default **Yes** setting is recommended. When set to **No**, clients must connect directly to the node and not through Unified Access Gateway. In this case, some post-deployment steps are required. See the information in *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.
FQDN	Enter the required fully qualified domain name (FQDN), such as `ourOrg.example.com`, which your end users will use to access the service. You must own that domain name and have a certificate in PEM format that can validate that FQDN.
DMZ Subnet (CIDR)	Enter the subnet (in CIDR notation) for the DMZ (demilitarized zone) network that will be configured to connect the Unified Access Gateway instances to the load balancer.
Certificate	Upload the certificate in PEM format that Unified Access Gateway will use to allow clients to trust connections to the Unified Access Gateway instances running in Microsoft Azure. The certificate must be based on the FQDN you entered and be signed by a trusted CA.

6 Click **Validate & Proceed**.

When you click **Validate & Proceed**, the system verifies the validity and appropriateness of your specified values, such as:

- Are the subnets valid and non-overlapping with other networks in the selected region within your subscription.
- Are there enough virtual machine (VM) and cores in your subscription's quota to build out the node.
- Is the certificate in the correct PEM format.

If everything validates OK, the summary page displays.

7 Review the summarized information and click **Submit** .

The system starts deploying the node into your Microsoft Azure environment.

Deploying your first node can take up to an hour. Until the node is successfully deployed, a progress icon is displayed in the Administration Console's Getting Started screen. You might need to refresh the screen in your browser to see the progress.

Important When deploying a node in Microsoft Azure China cloud, the process can take up to seven (7) hours to complete. The process is subject to geographic network issues that can cause slow download speeds as the binaries are downloaded from the cloud control plane.

When the node is successfully deployed, a green checkmark is displayed in the Getting Started screen along with a message about completing the domain join process.

Note If the deployment process fails for some reason or if you dislike the values you used and want to start over before registering your Active Directory domain, a **Delete** button is displayed. Click the **Delete** button to delete the artifacts that were deployed. When the screen indicates the node is successfully deleted, you can start the process over by clicking **Add** again.

What to do next

Expand the General Setup section of the Horizon Cloud Getting Started wizard and complete the required task of registering an Active Directory domain. Registering Active Directory is the next required step. After registering the domain, you continue management of this node in the Administration Console. See the Getting Started chapter of *VMware Horizon Cloud Service on Microsoft Azure Administration Guide*.

After registering the Active Directory domain, follow the Getting Started wizard to see which task to complete next.

If you deployed the node with the **Internet-Enabled Desktops** option set to **Yes** (the default), before your end users can access their RDS desktops and remote applications, you must configure a CNAME record in your DNS server to map the auto-generated public FQDN of the node's deployed load balancer to the FQDN that you entered in the deployment wizard. The public load balancer IP address has an auto-generated public FQDN in the form `vmw-hcs-`*`nodeID`*`-uag.`*`region`*`.cloudapp.azure.com`, where *nodeID* is the node's UUID and *region* is the Microsoft Azure region where the node is located. Your DNS server record maps that auto-generated public FQDN of the load balancer with the FQDN that your end users will use, and which is used in the uploaded certificate.

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

For the steps to obtain the load balancer's public FQDN in the Microsoft Azure portal, see the *VMware Horizon Cloud Service on Microsoft Azure Administration Guide* .

Microsoft Azure Virtual Machine Requirements for a Horizon Cloud Node

5

Node deployment and standard operations require specific types and sizes of virtual machines (VMs) in your Microsoft Azure cloud capacity. Your subscription needs the appropriate quotas and configuration to support these VMs.

The node deployment wizard validates that your Microsoft Azure environment has sufficient quota of cores to build the node.

Table 5-1. Horizon Cloud Node Virtual Machine Requirements

VM	Microsoft Azure VM Specification	Quantity	Description
Jumpbox	F-Series size: Standard_F2 (2 cores, 4 GB memory)	1 per node	A VM created in your Microsoft Azure environment and used during initial node creation, and during subsequent software updates on the environment. One jumpbox VM for each node you deploy. This jumpbox VM is deleted automatically when the node creation or update process are finished and the VM is no longer needed.
Management node instances	Dv2-Series: Standard_D2_v2 (2 cores, 7 GB memory)	1 per node during steady-state operations 2 per node while a software upgrade is being performed	Your environment needs to be sized to accommodate both these instances running during an upgrade process. During steady-state operations, one VM exists, is powered on, and runs the node. When an upgrade is being performed on the node, an additional instance is created and powered on to run software updates on the environment. After the upgrade is completed, the node migrates to using the newly created VM for steady-state operations and the previous one is deleted.

Table 5-1. Horizon Cloud Node Virtual Machine Requirements (Continued)

VM	Microsoft Azure VM Specification	Quantity	Description
Unified Access Gateway instances	Av2-Series: Standard_A4_v2 (4 cores, 8 GB memory)	2 per node during steady-state operations 4 per node while a software upgrade is being performed	Unified Access Gateway is an optional feature that is deployed when you select **Yes** to have Internet-enabled desktops. If you choose to have Unified Access Gateway for the node, your environment needs to be sized to accommodate these instances running during an upgrade process. During steady-state operations, two instances exist, are powered on, and provide the Unified Access Gateway capabilities. During an upgrade process, two additional instances are created and powered on to run the software updates on Unified Access Gateway. After the upgrade is completed, the node migrates to using the newly created instances and the previous ones are deleted.
Base image	You choose the sizes that you want to use for your base server images. Unless you want GPU-enabled desktops, D2_v2 is recommended for the base image. To have server farms with GPU-enabled, use Standard_NV6 for your base image so that you can install the GPU drivers into it.	Varied, based on your needs	A base image is an RDS-enabled Microsoft Windows server operating system VM configured with the Horizon Agent and DaaS Agents. This VM provides the base that the environment then uses to create the RDSH farms that provide session-based desktops and remote applications to your end users. One VM is required per Microsoft Windows Server operating system. The system automatically powers off the base image when it is published (when you perform the **Convert to Image** action on the base image in the Administration Console). When you update a published image, the system powers the VM on again.
RDSH farm	Options: Dv2-Series: ■ Standard_D2_v2 (2 cores, 7 GB memory) ■ Standard_D3_v2 (4 cores, 14 GB memory) ■ Standard_D4_v2 (8 cores, 28 GB memory) NV instances, GPU-enabled: ■ Standard_NV6 (6 cores, 56 GB memory, 1 GPU) **Note** GPU-enabled VMs are only available in some Microsoft Azure regions. See Microsoft Azure Products by region for details.	Varied, based on your needs	RDSH farm VMs are the server instances that provide session-based desktops and remote applications to your end users. You need at least one RDSH farm to deliver session desktops and an additional farm to deliver remote applications. To meet administrator or end user needs, you can choose to deploy additional farms. The power state of these VMs varies, depending on the farm configuration settings and the end user demand.

Active Directory Domain Configurations

6

A Horizon Cloud environment requires registering at least one Active Directory (AD) domain with the Horizon Cloud node. This topic describes the configurations that are supported for use with your Horizon Cloud nodes in Microsoft Azure.

The supported configurations are:

- On-premises AD server and using VPN/Express Route to connect that on-premises AD with your Microsoft Azure environment.
- AD server running in your Microsoft Azure environment.
- Using Microsoft Azure Active Directory Domain Services. For an overview of theses services that Microsoft Azure provides, see this Azure AD Domain Services article in the Microsoft documentation.