

Run a Windows virtual machine on Azure

12/13/2018 • 6 minutes to read • Contributors      all

In this article

[Resource group](#)

[Virtual machine](#)

[Disks](#)

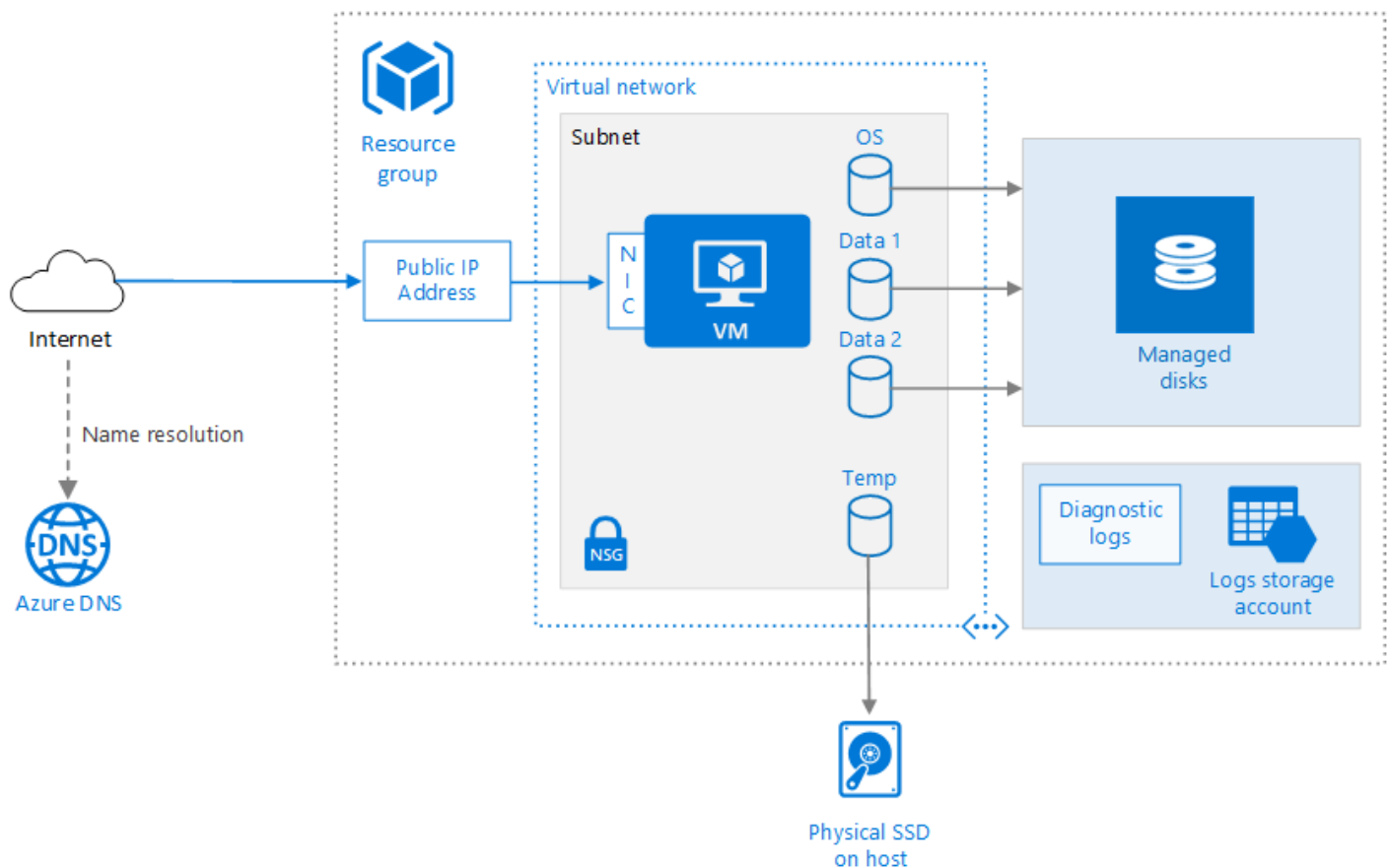
[Network](#)

[Operations](#)

[Security considerations](#)

[Next steps](#)

Provisioning a virtual machine (VM) in Azure requires some additional components besides the VM itself, including networking and storage resources. This article shows best practices for running a Windows VM on Azure.



Resource group

A [resource group](#) is a logical container that holds related Azure resources. In general, group resources based on their lifetime and who will manage them.


Put closely associated resources that share the same lifecycle into the same [resource group](#). Resource groups allow you to deploy and monitor resources as a group and track billing costs by resource group. You can also delete resources as a set, which is very useful for test deployments. Assign meaningful resource names to simplify locating a specific resource and understanding its role. For more information, see [Recommended Naming Conventions for Azure Resources](#).

Virtual machine

You can provision a VM from a list of published images, or from a custom managed image or virtual hard disk (VHD) file uploaded to Azure Blob storage.

Azure offers many different virtual machine sizes. For more information, see [Sizes for virtual machines in Azure](#). If you are moving an existing workload to Azure, start with the VM size that's the closest match to your on-premises servers. Then measure the performance of your actual workload in terms of CPU, memory, and disk input/output operations per second (IOPS), and adjust the size as needed.

Generally, choose an Azure region that is closest to your internal users or customers. Not all VM sizes are available in all regions. For more information, see [Services by region](#). For a list of the VM sizes available in a specific region, run the following command from the Azure command-line interface (CLI):

Azure CLI	 Copy
<pre>az vm list-sizes --location <location></pre>	

For information about choosing a published VM image, see [Find Windows VM images](#).

Disks

For best disk I/O performance, we recommend [Premium Storage](#), which stores data on solid-state drives (SSDs). Cost is based on the capacity of the provisioned disk. IOPS and throughput also depend on disk size, so when you provision a disk, consider all three factors (capacity, IOPS, and throughput).

We also recommend using [Managed Disks](#). Managed disks simplify disk management by handling the storage for you. Managed disks do not require a storage account. You simply specify the size and type of disk and it is deployed as a highly available resource

The OS disk is a VHD stored in [Azure Storage](#), so it persists even when the host machine is down. We also recommend creating one or more [data disks](#), which are persistent VHDs used for application data. When possible, install applications on a data disk, not the OS disk. Some legacy applications might need to install components on the C: drive; in that case, you can [resize the OS disk](#) using PowerShell.

The VM is also created with a temporary disk (the D: drive on Windows). This disk is stored on a physical drive on the host machine. It is *not* saved in Azure Storage and may be deleted during reboots and other VM lifecycle events. Use this disk only for temporary data, such as page or swap files.

Network

The networking components include the following resources:

- **Virtual network.** Every VM is deployed into a virtual network that can be segmented into multiple subnets.
- **Network interface (NIC).** The NIC enables the VM to communicate with the virtual network. If you need multiple NICs for your VM, be aware that a maximum number of NICs is defined for each [VM size](#).
- **Public IP address.** A public IP address is needed to communicate with the VM — for example, via remote desktop (RDP). The public IP address can be dynamic or static. The default is dynamic.
- Reserve a [static IP address](#) if you need a fixed IP address that won't change — for example, if you need to create a DNS 'A' record or add the IP address to a safe list.
- You can also create a fully qualified domain name (FQDN) for the IP address. You can then register a [CNAME record](#) in DNS that points to the FQDN. For more information, see [Create a fully qualified domain name in the](#)

[Azure portal](#).

- **Network security group (NSG).** [Network security groups](#) are used to allow or deny network traffic to VMs. NSGs can be associated either with subnets or with individual VM instances.

All NSGs contain a set of [default rules](#), including a rule that blocks all inbound Internet traffic. The default rules cannot be deleted, but other rules can override them. To enable Internet traffic, create rules that allow inbound traffic to specific ports — for example, port 80 for HTTP. To enable RDP, add an NSG rule that allows inbound traffic to TCP port 3389.

Operations

Diagnostics. Enable monitoring and diagnostics, including basic health metrics, diagnostics infrastructure logs, and [boot diagnostics](#). Boot diagnostics can help you diagnose boot failure if your VM gets into a non-bootable state. Create an Azure Storage account to store the logs. A standard locally redundant storage (LRS) account is sufficient for diagnostic logs. For more information, see [Enable monitoring and diagnostics](#).

Availability. Your VM may be affected by [planned maintenance](#) or [unplanned downtime](#). You can use [VM reboot logs](#) to determine whether a VM reboot was caused by planned maintenance. For higher availability, deploy multiple VMs in an [availability set](#). This configuration provides a higher [service level agreement \(SLA\)](#).

Backups To protect against accidental data loss, use the [Azure Backup](#) service to back up your VMs to geo-redundant storage. Azure Backup provides application-consistent backups.

Stopping a VM. Azure makes a distinction between "stopped" and "deallocated" states. You are charged when the VM status is stopped, but not when the VM is deallocated. In the Azure portal, the **Stop** button deallocates the VM. If you shut down through the OS while logged in, the VM is stopped but **not** deallocated, so you will still be charged.

Deleting a VM. If you delete a VM, the VHDs are not deleted. That means you can safely delete the VM without losing data. However, you will still be charged for storage. To delete the VHD, delete the file from [Blob storage](#). To prevent accidental deletion, use a [resource lock](#) to lock the entire resource group or lock individual resources, such as a VM.

Security considerations

Use [Azure Security Center](#) to get a central view of the security state of your Azure resources. Security Center monitors potential security issues and provides a comprehensive picture of the security health of your deployment. Security Center is configured per Azure subscription. Enable security data collection as described in [Onboard your Azure subscription to Security Center Standard](#). When data collection is enabled, Security Center automatically scans any VMs created under that subscription.

Patch management. If enabled, Security Center checks whether any security and critical updates are missing. Use [Group Policy settings](#) on the VM to enable automatic system updates.

Antimalware. If enabled, Security Center checks whether antimalware software is installed. You can also use Security Center to install antimalware software from inside the Azure portal.

Access control. Use [role-based access control \(RBAC\)](#) to control access to Azure resources. RBAC lets you assign authorization roles to members of your DevOps team. For example, the Reader role can view Azure resources but not create, manage, or delete them. Some permissions are specific to an Azure resource type. For example, the Virtual Machine Contributor role can restart or deallocate a VM, reset the administrator password, create a new VM, and so on. Other [built-in RBAC roles](#) that may be useful for this architecture include [DevTest Labs User](#) and [Network Contributor](#).



Note

RBAC does not limit the actions that a user logged into a VM can perform. Those permissions are determined by the account type on the guest OS.

Audit logs. Use [audit logs](#) to see provisioning actions and other VM events.

Data encryption. Use [Azure Disk Encryption](#) if you need to encrypt the OS and data disks.

Next steps

- To provision a Windows VM, see [Create and Manage Windows VMs with Azure PowerShell](#)
- For a complete N-tier architecture on Windows VMs, see [Windows N-tier application on Azure with SQL Server](#).