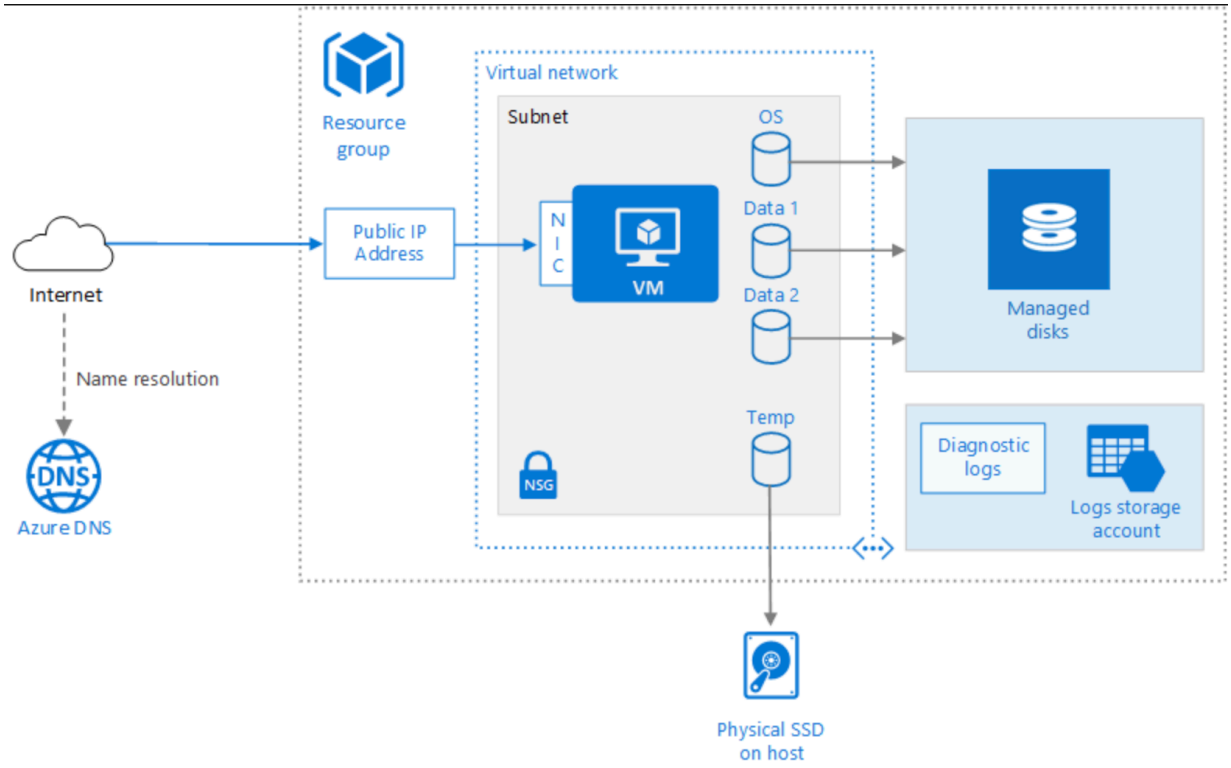
Azure VMs

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/linux-vm

Type-1

Run a Linux or Windows virtual machine on Azure
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 Linux 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 useful for test deployments.

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 supports running various popular Linux distributions, including CentOS, Debian, Red Hat Enterprise, Ubuntu, and FreeBSD.

Azure offers many different virtual machine sizes. 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 CLI:

az vm list-sizes --location <location>

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 (that is, data transfer rate) 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. For Linux VMs, the OS disk is /dev/sda1. We also recommend creating one or more data disks, which are persistent VHDs used for application data.
When you create a VHD, it is unformatted. Log into the VM to format the disk. In the Linux shell, data disks are displayed as /dev/sdc, /dev/sdd, and so on. You can run lsblk to list the block devices, including the disks. To use a data disk, create a partition and file system, and mount the disk. For example:

```
# Create a partition.
sudo fdisk /dev/sdc     # Enter 'n' to partition, 'w' to write the change.

# Create a file system.
sudo mkfs -t ext3 /dev/sdc1
```

```
# Mount the drive.
sudo mkdir /data1
sudo mount /dev/sdc1 /data1
```

You may want to change the I/O scheduler to optimize for performance on SSDs because the disks for VMs with premium storage accounts are SSDs. A common recommendation is to use the NOOP scheduler for SSDs, but you should use a tool such as iostat to monitor disk I/O performance for your workload.
The VM is created with a temporary disk. 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. For Linux VMs, the temporary disk is /dev/sdb1 and is mounted at /mnt/resource or /mnt.

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 SSH, add an NSG rule that allows inbound traffic to TCP port 22.

Operations

SSH. Before you create a Linux VM, generate a 2048-bit RSA public-private key pair. Use the public key file when you create the VM. For more information,

see How to Use SSH with Linux and Mac on Azure.

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.

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.

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.

Sizes for Linux and Windows virtual machines in Azure:

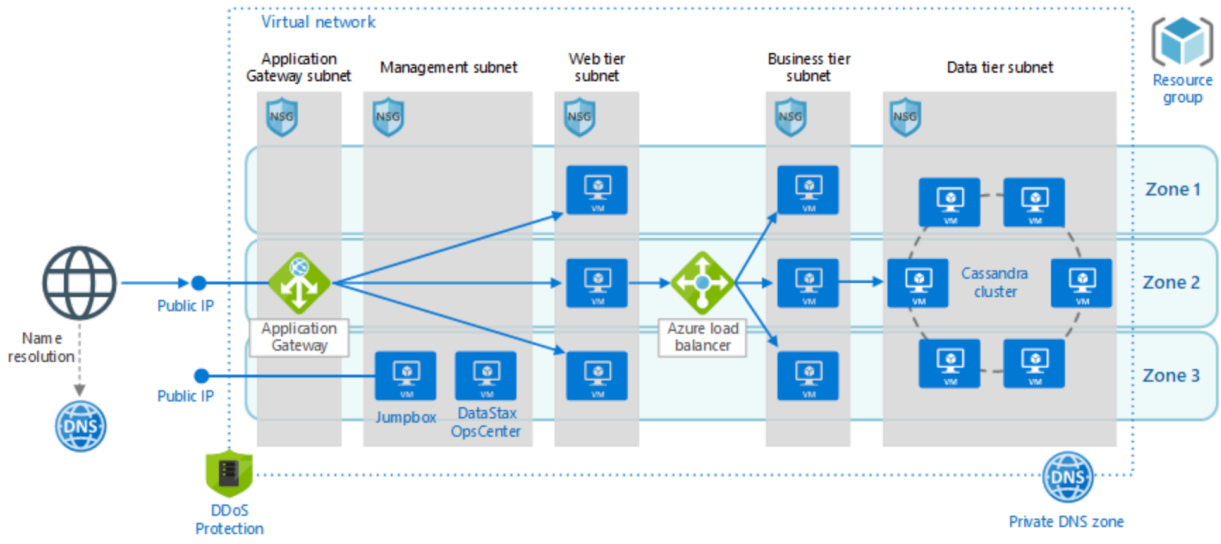
Type	Sizes	Description
General purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute optimized	Fsv2	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	Esv3, Ev3, Easv4, Eav4, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage optimized	Lsv2	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.

GPU	NC, NCv2, NCv3, ND, NDv2 (Preview), NV, NVv3	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
High performance compute	HB, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

Type-2

Linux N-tier application in Azure with Apache Cassandra

This reference architecture shows how to deploy virtual machines (VMs) and a virtual network configured for an N-tier application, using Apache Cassandra on Linux for the data tier.



General

- **Resource group**. Resource groups are used to group Azure resources so they can be managed by lifetime, owner, or other criteria.
- **Availability zones**. Availability zones are physical locations within an Azure

region. Each zone consists of one or more datacenters with independent power, cooling, and networking. By placing VMs across zones, the application becomes resilient to failures within a zone.

Networking and load balancing

- **Virtual network and subnets**. Every Azure VM is deployed into a virtual network that can be segmented into subnets. Create a separate subnet for each tier.
- **Application gateway**. Application Gateway is a layer 7 load balancer. In this architecture, it routes HTTP requests to the web front end. Application Gateway also provides a web application firewall (WAF) that protects the application from common exploits and vulnerabilities.
- **Load balancers**. Use Azure Standard Load Balancer to distribute network traffic from the web tier to the business tier, and from the business tier to SQL Server.
- **Network security groups** (NSGs). Use NSGs to restrict network traffic within the virtual network. For example, in the three-tier architecture shown here, the database tier does not accept traffic from the web front end, only from the business tier and the management subnet.

- **DDoS Protection**. Although the Azure platform provides basic protection against distributed denial of service (DDoS) attacks, we recommend using DDoS Protection Standard, which has enhanced DDoS mitigation features.
- **Azure DNS**. Azure DNS is a hosting service for DNS domains. It provides name resolution using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

Virtual machines

- **Apache Cassandra database**. Provides high availability at the data tier, by enabling replication and failover.
- **OpsCenter**. Deploy a monitoring solution such as DataStax OpsCenter to monitor the Cassandra cluster.
- **Jumpbox**. Also called a bastion host. A secure VM on the network that administrators use to connect to the other VMs. The jumpbox has an NSG that allows remote traffic only from public IP addresses on a safe list. The NSG should permit remote desktop (RDP) traffic.

Recommandations

Load balancers
Do not expose the VMs directly to the Internet. Instead, give each VM a private IP address. Clients connect using the IP address associated with the Application Gateway.
Define load balancer rules to direct network traffic to the VMs. For example, to enable HTTP traffic, create a rule that maps port 80 from the front-end configuration to port 80 on the back-end address pool. When a client sends an HTTP request to port 80, the load balancer selects a back-end IP address by using a hashing algorithm that includes the source IP address. Client requests are distributed across all the VMs.

Network security groups
Use NSG rules to restrict traffic between tiers. For example, in the three-tier architecture shown above, the web tier does not communicate directly with the database tier. To enforce this, the database tier should block incoming traffic from the web tier subnet.

1. Deny all inbound traffic from the VNet. (Use the VIRTUAL_NETWORK tag in the rule.)
2. Allow inbound traffic from the business tier subnet.
3. Allow inbound traffic from the database tier subnet itself. This rule allows communication between the database VMs, which is needed for database replication and failover.
4. Allow ssh traffic (port 22) from the jumpbox subnet. This rule lets administrators connect to the database tier from the jumpbox.

Create rules 2 – 4 with higher priority than the first rule, so they override it.

Cassandra
We recommend DataStax Enterprise for production use, but these recommendations apply to any Cassandra edition. For more information on running DataStax in Azure.
Configure nodes in rack-aware mode. Map fault domains to racks in the cassandra-rackdc.properties file.
You don't need a load balancer in front of the cluster. The client connects directly to a node in the cluster.
The deployment scripts for this architecture use name resolution to initialize the seed node for intra-cluster communication (gossip). To enable name resolution, the deployment creates an Azure Private DNS zone with A records for the Cassandra nodes. Depending on your initialization scripts, you might be able to use the static IP address instead.

Jumpbox
Don't allow ssh access from the public Internet to the VMs that run the application workload. Instead, all ssh access to these VMs must come through the jumpbox.

An administrator logs into the jumpbox, and then logs into the other VM from the jumpbox. The jumpbox allows ssh traffic from the Internet, but only from known, safe IP addresses.
The jumpbox has minimal performance requirements, so select a small VM size. Create a public IP address for the jumpbox. Place the jumpbox in the same VNet as the other VMs, but in a separate management subnet.
To secure the jumpbox, add an NSG rule that allows ssh connections only from a safe set of public IP addresses. Configure the NSGs for the other subnets to allow ssh traffic from the management subnet.

Scalability considerations

Scale sets
For the web and business tiers, consider using virtual machine scale sets, instead of deploying separate VMs into an availability set. A scale set makes it easy to deploy and manage a set of identical VMs, and autoscale the VMs based on performance metrics. As the load on the VMs increases, additional VMs are automatically added to the load balancer.
There are two basic ways to configure VMs deployed in a scale set:

- Use extensions to configure the VM after it's deployed. With this approach, new VM instances may take longer to start up than a VM with no extensions.
- Deploy a managed disk with a custom disk image. This option may be quicker to deploy. However, it requires you to keep the image up-to-date.

Health probes
Application Gateway and Load Balancer both use health probes to monitor the availability of VM instances.

- Application Gateway always uses an HTTP probe.
- Load Balancer can test either HTTP or TCP. Generally, if a VM runs an HTTP server, use an HTTP probe. Otherwise, use TCP.

If a probe can't reach an instance within a timeout period, the gateway or load balancer stops sending traffic to that VM. The probe continues to check and will return the VM to the back-end pool if the VM becomes available again.

Security considerations

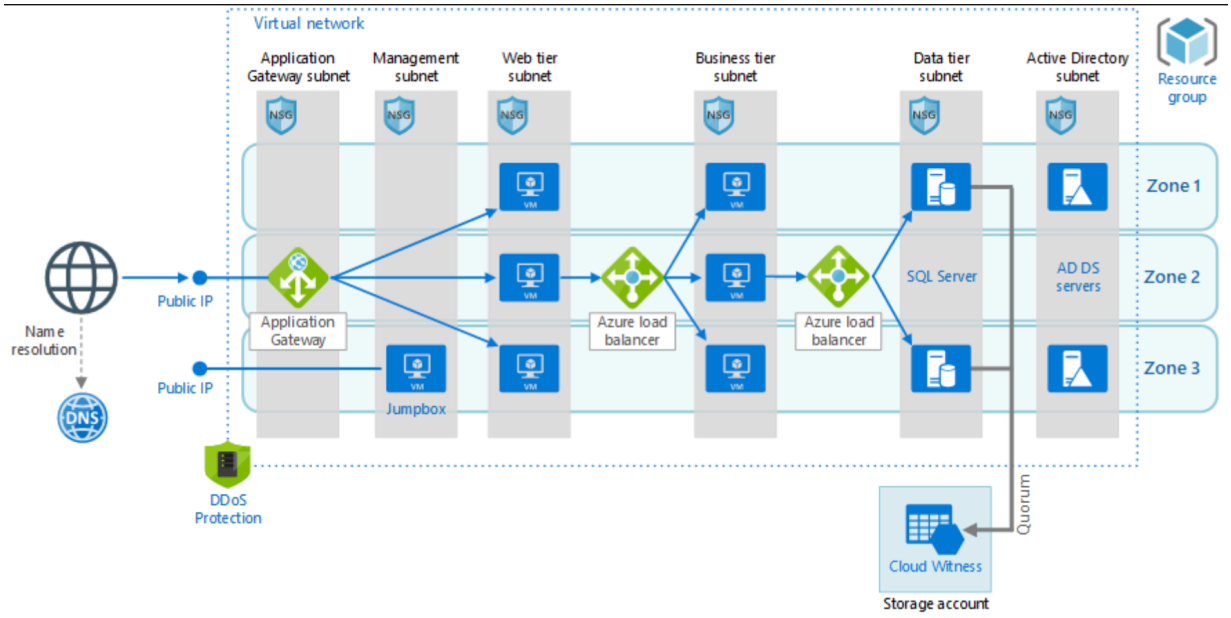
Virtual networks are a traffic isolation boundary in Azure. VMs in one VNet can't communicate directly with VMs in a different VNet. VMs within the same VNet can communicate, unless you create network security groups (NSGs) to restrict traffic. For incoming Internet traffic, the load balancer rules define which traffic can reach the back end. However, load balancer rules don't support IP safe lists, so if you want to add certain public IP addresses to a safe list, add an NSG to the subnet.

DMZ. Consider adding a network virtual appliance (NVA) to create a DMZ between the Internet and the Azure virtual network. NVA is a generic term for a virtual appliance that can perform network-related tasks, such as firewall, packet inspection, auditing, and custom routing.
Encryption. Encrypt sensitive data at rest and use Azure Key Vault to manage the database encryption keys. Key Vault can store encryption keys in hardware security modules (HSMs). It's also recommended to store application secrets, such as database connection strings, in Key Vault.
DDoS protection. The Azure platform provides basic DDoS protection by default. This basic protection is targeted at protecting the Azure infrastructure as a whole. Although basic DDoS protection is automatically enabled, we recommend using DDoS Protection Standard. Standard protection uses adaptive tuning, based on your application's network traffic patterns, to detect threats. This allows it to apply mitigations against DDoS attacks that might go unnoticed by the infrastructure-wide DDoS policies. Standard protection also provides alerting, telemetry, and analytics through Azure Monitor.

Type-3

Windows N-tier application on Azure with SQL Server

This reference architecture shows how to deploy virtual machines (VMs) and a virtual network configured for an N-tier application, using SQL Server on Windows for the data tier.



The architecture has the following components.

General

- **Resource group**. Resource groups are used to group Azure resources so they can be managed by lifetime, owner, or other criteria.
- **Availability zones**. Availability zones are physical locations within an Azure region. Each zone consists of one or more datacenters with independent power, cooling, and networking. By placing VMs across zones, the application becomes resilient to failures within a zone.

Networking and load balancing

- **Virtual network and subnets**. Every Azure VM is deployed into a virtual network that can be segmented into subnets. Create a separate subnet for each tier.
- **Application gateway**. Application Gateway is a layer 7 load balancer. In this architecture, it routes HTTP requests to the web front end. Application Gateway also provides a web application firewall (WAF) that protects the application from common exploits and vulnerabilities.
- **Load balancers**. Use Azure Standard Load Balancer to distribute network traffic from the web tier to the business tier, and from the business tier to SQL Server.
- **Network security groups** (NSGs). Use NSGs to restrict network traffic within the virtual network. For example, in the three-tier architecture shown here, the database tier does not accept traffic from the web front end, only from the business tier and the management subnet.
- **DDoS Protection**. Although the Azure platform provides basic protection against distributed denial of service (DDoS) attacks, we recommend using DDoS Protection Standard, which has enhanced DDoS mitigation features.
- **Azure DNS**. Azure DNS is a hosting service for DNS domains. It provides name resolution using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

Virtual machines

- **SQL Server Always On Availability Group**. Provides high availability at the data tier, by enabling replication and failover. It uses Windows Server Failover Cluster (WSFC) technology for failover.
- **Active Directory Domain Services (AD DS) Servers**. The computer objects

for the failover cluster and its associated clustered roles are created in Active Directory Domain Services (AD DS).

- **Cloud Witness**. A failover cluster requires more than half of its nodes to be running, which is known as having quorum. If the cluster has just two nodes, a network partition could cause each node to think it's the master node. In that case, you need a *witness* to break ties and establish quorum. A witness is a resource such as a shared disk that can act as a tie breaker to establish quorum. Cloud Witness is a type of witness that uses Azure Blob Storage. To learn more about the concept of quorum, see Understanding cluster and pool quorum. For more information about Cloud Witness, see Deploy a Cloud Witness for a Failover Cluster.
- **Jumpbox**. Also called a bastion host. A secure VM on the network that administrators use to connect to the other VMs. The jumpbox has an NSG that allows remote traffic only from public IP addresses on a safe list. The NSG should permit remote desktop (RDP) traffic.

Recommandations

Network security groups

Use NSG rules to restrict traffic between tiers. In the three-tier architecture shown above, the web tier does not communicate directly with the database tier. To enforce this rule, the database tier should block incoming traffic from the web tier subnet.

1. Deny all inbound traffic from the virtual network. (Use the VIRTUAL_NETWORK tag in the rule.)
2. Allow inbound traffic from the business tier subnet.
3. Allow inbound traffic from the database tier subnet itself. This rule allows communication between the database VMs, which is needed for database replication and failover.
4. Allow RDP traffic (port 3389) from the jumpbox subnet. This rule lets administrators connect to the database tier from the jumpbox.

Create rules 2 – 4 with higher priority than the first rule, so they override it.

SQL Server Always On Availability Groups

We recommend Always On Availability Groups for SQL Server high availability. Prior to Windows Server 2016, Always On Availability Groups require a domain controller, and all nodes in the availability group must be in the same AD domain. Other tiers connect to the database through an availability group listener. The listener enables a SQL client to connect without knowing the name of the physical instance of SQL Server. VMs that access the database must be joined to the domain. The client (in this case, another tier) uses DNS to resolve the listener's

virtual network name into IP addresses.
Configure the SQL Server Always On Availability Group as follows:

1. Create a Windows Server Failover Clustering (WSFC) cluster, a SQL Server Always On Availability Group, and a primary replica.
2. Create an internal load balancer with a static private IP address.
3. Create an availability group listener, and map the listener's DNS name to the IP address of an internal load balancer.
4. Create a load balancer rule for the SQL Server listening port (TCP port 1433 by default). The load balancer rule must enable *floating IP*, also called Direct Server Return. This causes the VM to reply directly to the client, which enables a direct connection to the primary replica.

When a SQL client tries to connect, the load balancer routes the connection request to the primary replica. If there is a failover to another replica, the load balancer automatically routes new requests to a new primary replica.
During a failover, existing client connections are closed. After the failover completes, new connections will be routed to the new primary replica.

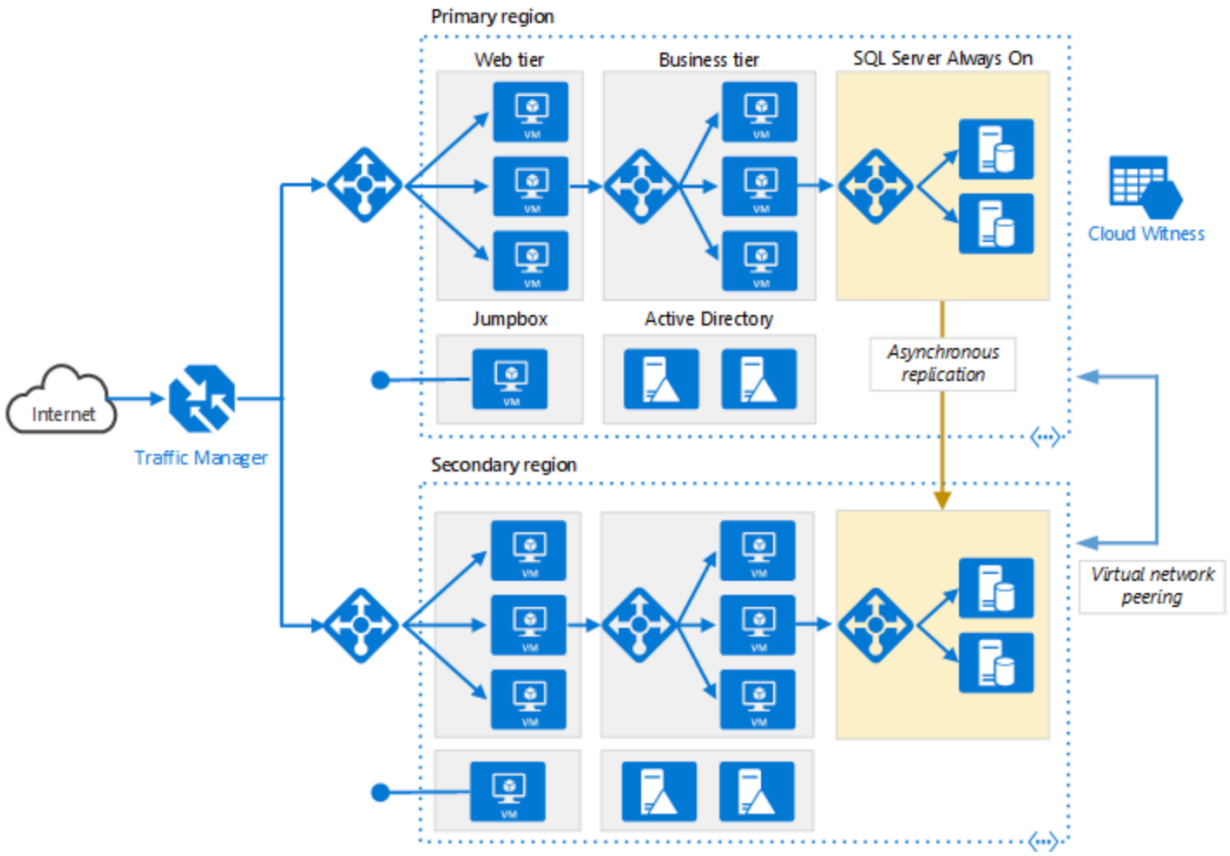
Jumpbox

Don't allow RDP access from the public Internet to the VMs that run the application workload. Instead, all RDP access to these VMs should go through the jumpbox. An administrator logs into the jumpbox, and then logs into the other VM from the jumpbox. The jumpbox allows RDP traffic from the Internet, but only from known, safe IP addresses.
The jumpbox has minimal performance requirements, so select a small VM size. Create a public IP address for the jumpbox. Place the jumpbox in the same virtual network as the other VMs, but in a separate management subnet.
To secure the jumpbox, add an NSG rule that allows RDP connections only from a safe set of public IP addresses. Configure the NSGs for the other subnets to allow RDP traffic from the management subnet.

Type-4

Run an N-tier application in multiple Azure regions for high availability

This reference architecture shows a set of proven practices for running an N-tier application in multiple Azure regions, in order to achieve availability and a robust disaster recovery infrastructure.



This architecture builds on the one shown in N-tier application with SQL Server.

- **Primary and secondary regions**. Use two regions to achieve higher availability. One is the primary region. The other region is for failover.
- **Azure Traffic Manager**. Traffic Manager routes incoming requests to one of the regions. During normal operations, it routes requests to the primary region. If that region becomes unavailable, Traffic Manager fails over to the secondary region.
- **Resource groups**. Create separate resource groups for the primary region, the secondary region, and for Traffic Manager. This gives you the flexibility to manage each region as a single collection of resources. For example, you could redeploy one region, without taking down the other one. Link the resource groups, so that you can run a query to list all the resources for the application.
- **Virtual networks**. Create a separate virtual network for each region. Make sure the address spaces do not overlap.
- **SQL Server Always On Availability Group**. If you are using SQL Server, we recommend SQL Always On Availability Groups for high availability. Create a single availability group that includes the SQL Server instances in both regions.
- **Virtual network peering**. Peer the two virtual networks to allow data replication from the primary region to the secondary region.

Recommendations

A multi-region architecture can provide higher availability than deploying to a single region. If a regional outage affects the primary region, you can use Traffic Manager to fail over to the secondary region. This architecture can also help if an individual subsystem of the application fails.
There are several general approaches to achieving high availability across regions:

- Active/passive with hot standby. Traffic goes to one region, while the other waits on hot standby. Hot standby means the VMs in the secondary region are allocated and running at all times.
- Active/passive with cold standby. Traffic goes to one region, while the other waits on cold standby. Cold standby means the VMs in the secondary region are not allocated until needed for failover. This approach costs less to run, but will generally take longer to come online during a failure.
- Active/active. Both regions are active, and requests are load balanced between them. If one region becomes unavailable, it is taken out of rotation.

This reference architecture focuses on active/passive with hot standby, using Traffic Manager for failover. Note that you could deploy a small number of VMs for hot standby and then scale out as needed.

Regional pairing

Each Azure region is paired with another region within the same geography. In general, choose regions from the same regional pair (for example, East US 2 and US Central). Benefits of doing so include:

- If there is a broad outage, recovery of at least one region out of every pair is prioritized.
- Planned Azure system updates are rolled out to paired regions sequentially, to minimize possible downtime.
- Pairs reside within the same geography, to meet data residency requirements.

However, make sure that both regions support all of the Azure services needed for your application.

Traffic Manager configuration

Consider the following points when configuring Traffic Manager:

- **Routing**. Traffic Manager supports several routing algorithms. For the scenario described in this article, use *priority* routing (formerly called *failover* routing). With this setting, Traffic Manager sends all requests to the primary region, unless the primary region becomes unreachable. At that point, it automatically fails over to the secondary region. See Configure

Failover routing method.

- **Health probe**. Traffic Manager uses an HTTP (or HTTPS) probe to monitor the availability of each region. The probe checks for an HTTP 200 response for a specified URL path. As a best practice, create an endpoint that reports the overall health of the application, and use this endpoint for the health probe. Otherwise, the probe might report a healthy endpoint when critical parts of the application are actually failing. For more information

When Traffic Manager fails over there is a period of time when clients cannot reach the application. The duration is affected by the following factors:

- The health probe must detect that the primary region has become unreachable.
- DNS servers must update the cached DNS records for the IP address, which depends on the DNS time-to-live (TTL). The default TTL is 300 seconds (5 minutes), but you can configure this value when you create the Traffic Manager profile.

If Traffic Manager fails over, we recommend performing a manual failback rather than implementing an automatic failback. Otherwise, you can create a situation where the application flips back and forth between regions. Verify that all application subsystems are healthy before failing back.
Note that Traffic Manager automatically fails back by default. To prevent this, manually lower the priority of the primary region after a failover event. For example, suppose the primary region is priority 1 and the secondary is priority 2. After a failover, set the primary region to priority 3, to prevent automatic failback. When you are ready to switch back, update the priority to 1.