


[< Previous](#)Unit 2 of 5 [Next >](#)✓ 200 XP 

# Deploy your site to Azure

12 minutes

Your first step will likely be to re-create your on-premises configuration in the cloud.

This basic configuration will give you a sense of how networks are configured, and how network traffic moves in and out of Azure.

## Your e-commerce site at a glance

Larger enterprise systems are often composed of multiple inter-connected applications and services that work together. You might have a front-end web system that displays inventory and allows customers to create an order. That might talk to a variety of web services to provide the inventory data, manage user profiles, process credit cards, and request fulfillment of processed orders.

There are several strategies and patterns employed by software architects and designers to make these complex systems easier to design, build, manage, and maintain. Let's look at a few of them, starting with *loosely coupled architectures*.

## Benefits of Loosely Coupled Architectures



## Using an N-tier architecture

An architectural pattern that can be used to build loosely coupled systems is *N-tier*.

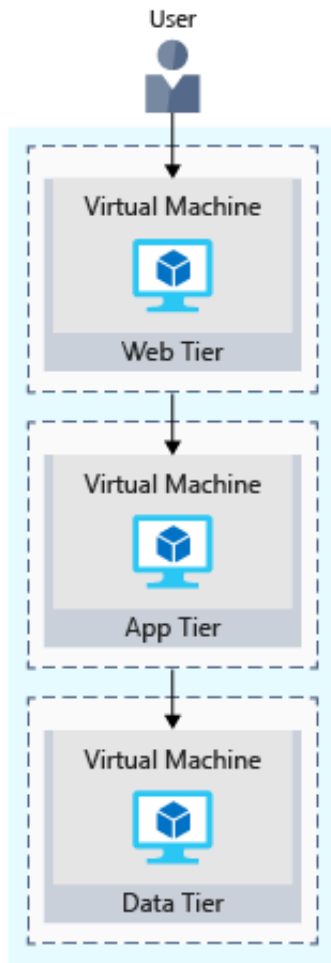
An [N-tier architecture](#) divides an application into two or more logical tiers. Architecturally, a higher tier can access services from a lower tier, but a lower tier should never access a higher tier.

Tiers help separate concerns and are ideally designed to be reusable. Using a tiered architecture also simplifies maintenance. Tiers can be updated or replaced independently, and new tiers can be inserted if needed.

*Three-tier* refers to an n-tier application that has three tiers. Your e-commerce web application follows this three-tier architecture:

- The **web tier** provides the web interface to your users through a browser.
- The **application tier** runs business logic.
- The **data tier** includes databases and other storage that hold product information and customer orders.

The following illustration shows the flow of a request from the user to the data tier.



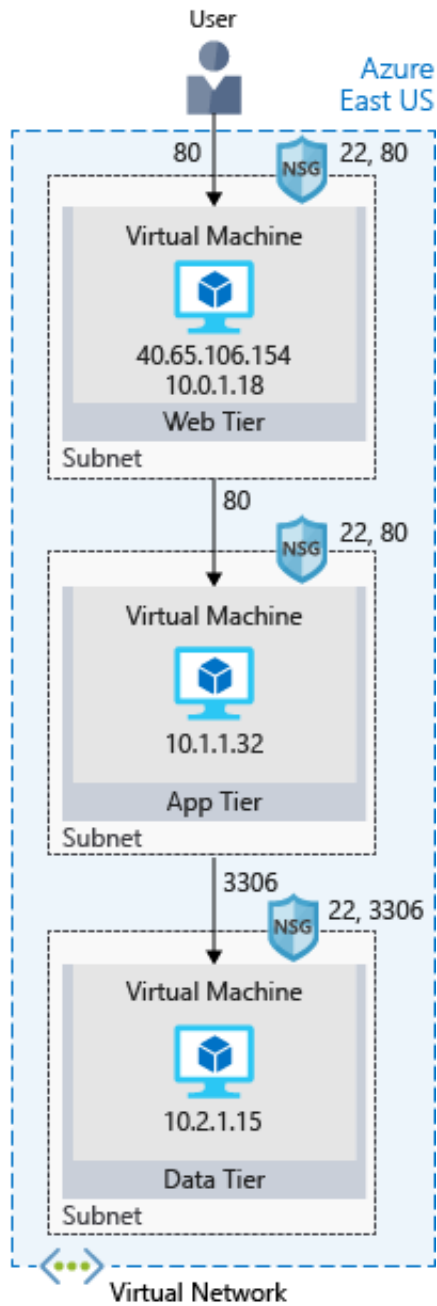
When the user clicks the button to place the order, the request is sent to the web tier, along with the user's address and payment information. The web tier passes this information to the application tier, which would validate payment information and check inventory. The application tier might then store the order in the data tier, to be picked up later for fulfillment.

## Your e-commerce site running on Azure

Azure provides many different ways to host your web applications, from fully pre-configured environments that host your code, to virtual machines that you configure, customize, and manage.

Let's say you choose to run your e-commerce site on virtual machines. Here's what that might look like in your test environment running on Azure. The following illustration shows a three-tier architecture running on virtual machines with security features enabled to restrict inbound

requests.



Let's break this down.



## What's an Azure region?

A *region* is one or more Azure data centers within a specific geographic location. East US, West US, and North Europe are examples of regions. In this instance, you see that the application is running in the East US region.



## What's a virtual network?

A *virtual network* is a logically isolated network on Azure. Azure virtual networks will be familiar to you if you've set up networks on Hyper-V, VMware, or even on other public clouds. A virtual

network allows Azure resources to securely communicate with each other, the internet, and on-premises networks. A virtual network is scoped to a single region; however, multiple virtual networks from different regions can be connected together using virtual network peering.

Virtual networks can be segmented into one or more *subnets*. Subnets help you organize and secure your resources in discrete sections. The web, application, and data tiers each have a single VM. All three VMs are in the same virtual network but are in separate subnets.

Users interact with the web tier directly, so that VM has a public IP address along with a private IP address. Users don't interact with the application or data tiers, so these VMs each have a private IP address only.

You can also keep your service or data tiers in your on-premises network, placing your web tier into the cloud, but keeping tight control over other aspects of your application. A *VPN gateway* (or virtual network gateway), enables this scenario. It can provide a secure connection between an Azure Virtual Network and an on-premises location over the internet.

Azure manages the physical hardware for you. You configure virtual networks and gateways through software, which enables you to treat a virtual network just like your own network. You choose which networks your virtual network can reach, whether that's the public internet or other networks in the private IP address space.



## What's a network security group?

A *network security group*, or NSG, allows or denies inbound network traffic to your Azure resources. Think of a network security group as a cloud-level firewall for your network.

For example, notice that the VM in the web tier allows inbound traffic on ports 22 (SSH) and 80 (HTTP). This VM's network security group allows inbound traffic over these ports from all sources. You can configure a network security group to accept traffic only from known sources, such as IP addresses that you trust.

### ⓘ Note

Port 22 enables you to connect directly to Linux systems over SSH. Here we show port 22 open for learning purposes. In practice, you might configure VPN access to your virtual network to increase security.

## Summary

Your three-tier application is now running on Azure in the East US region. A *region* is one or more Azure data centers within a specific geographic location.

Each tier can access services only from a lower tier. The VM running in the web tier has a public IP address because it receives traffic from the internet. The VMs in the lower tiers, the application and data tiers, each have private IP addresses because they don't communicate directly over the internet.

*Virtual networks* enable you to group and isolate related systems. You define *network security groups* to control what traffic can flow through a virtual network.

The configuration you saw here is a good start. But when you deploy your e-commerce site to production in the cloud, you'll likely run into the same problems as you did in your on-premises deployment.

## Check your knowledge

### 1. What is an Azure *region*?

- ☒ One or more Azure data centers within a specific geographical location. ✓

**Azure regions help you deliver your apps and services closest to your users. West US and North Europe are examples.**

- ☐ A way of breaking networks into smaller networks.
- ☐ Firewall rules which define the flow of traffic in and out of Azure.

### 2. Which of the following is true about virtual networks?

- ☒ You configure virtual networks through software. ✓

**Software enables you to treat a virtual network just like your own network. Azure maintains the physical hardware for you.**

- ☐ A virtual network accepts network traffic on all ports. You configure the firewall through virtual machines.
- ☐ Virtual networks are always reachable from the internet.



## Next unit: Scale with Azure Load Balancer

Continue >

---