2. Recurrence profile

3. Default (Always) profile

In the example above, you would set up a Recurrence profile for Monday through Friday, 8 AM to 5 PM, and then set up a Fixed Date profile for a specific holiday, and the Fixed Date profile will take precedence on that one date.

For more information about autoscaling, including best practices, please check out this article: https://azure.microsoft.com/documentation/articles/insights-autoscale-best-practices/.

Azure Virtual Machines

Platform as a service (PaaS) is an attractive option for a certain category of workloads. However, not every solution can, or should, fit within the PaaS model. Some workloads require near-total control over the infrastructure: operating system configuration, disk persistence, the ability to install and configure traditional server software, and so on. This is where infrastructure as a service (IaaS) and

Azure Virtual Machines come into the picture.

What is Azure Virtual Machines?

Azure Virtual Machines is one of the central features of Azure's IaaS capabilities, together with Azure Virtual Networks. Azure Virtual Machines supports the deployment of Windows or Linux virtual machines (VMs) in a Microsoft Azure datacenter. You have total control over the configuration of the VM. You are responsible for all server software installation, configuration, and maintenance and for operating system patches.

Note The terminology used to describe the Azure Virtual Machines feature and a virtual machine instance can be a little confusing. Therefore, throughout this chapter, *Azure Virtual Machines* will refer to the feature, while *virtual machine* or *VM* will refer to an instance of an actual compute node.

There are two primary differences between Azure's PaaS and IaaS compute features: persistence and control. As discussed in Chapter

2, "Azure App Service and Web Apps," PaaS features such as Cloud Services (that is, web and worker roles) and App Services are managed primarily by the Azure platform, allowing you to focus on creating the application and not managing the server infrastructure. With an Azure Virtual Machines VM, you are responsible for nearly all aspects of the VM.

Azure Virtual Machines supports two types of durable (or persistent) disks: OS disks and data disks. An OS disk is required, and data disks are optional. The durability for the disks is provided by Azure Storage. More details on these disks will be provided later in this chapter, but for now understand the OS disk is where the operating system resides (Windows or Linux), and the data disk is where you can store other things, such as application data, images, and so on. By contrast, Azure PaaS cloud services use ephemeral disks attached to the physical host—the data on which can be lost in the event of failure of the physical host.

Because of the level of control afforded to the user and the use of durable disks, VMs are ideal for a wide range of server workloads that do not fit into a PaaS model. Server workloads such as database servers (SQL Server, Oracle, MongoDB, and so on), Windows Server Active Directory,

Microsoft SharePoint, and many more become possible to run on the Microsoft Azure platform. If desired, users can move such workloads from an on-premises datacenter to one or more Azure regions, a process often called *lift and shift*.

Billing

Azure Virtual Machines is priced on a per-hour basis, but it is billed on a per-minute basis. For example, you are only changed for 23 minutes of usage if the VM is deployed for 23 minutes. The cost for a VM includes the charge for the Windows operating system. Linux-based instances are slightly cheaper because there is no operating system license charge. The cost, and the appropriate licensing, for any additional software you install is your responsibility. Some VM images, such as Microsoft SQL Server, you acquire from the Azure Marketplace may include an additional license cost (on top of the base cost of the VM).

There is a direct relationship between the VM's status and billing:

- **Running** The VM is on and running normally (billable).
- **Stopped** The VM is stopped but still deployed to a physical host (billable)

- **Stopped (Deallocated)** The VM is not deployed to a physical host (not billable).

You are charged separately for the durable storage the VM uses. The status of the VM has no relation to the storage charges that will be incurred; even if the VM is stopped/deallocated and you aren't billed for the running VM, you will be charged for the storage used by the disks.

By default, stopping a VM in the Azure portal puts the VM into a Stopped (Deallocated) state. If you want to stop the VM but keep it allocated, you will need to use a PowerShell cmdlet or Azure command-line interface (CLI) command.

Stopping an Azure VM

To stop a VM but keep it provisioned, you would need to use the *Stop-AzureRmVM* PowerShell cmdlet such as in the following example:

```
Stop-AzureRmVM -Name "AzEssentialDev3" -
ResourceGroup "AzureEssentials" -
StayProvisioned
```

For classic VMs, a similar cmdlet, *Stop-AzureVM*, would be used.

When using the Azure CLI, there are two commands used to control the stopped state of a VM: *azure vm stop* and *azure vm deallocate*.

Shutting down the VM from the operating system of the VM will also stop the VM but will not deallocate the VM.

Note The Azure Hybrid Use Benefit program may offer additional savings by allowing you bring your on-premises Windows Server licenses to Azure. For more information, please see https://azure.microsoft.com/pricing/hybrid-use-benefit/.

Service level agreement

As of the time of this writing, Microsoft offers a 99.95 percent connectivity service level agreement (SLA) for multiple-instance VMs deployed in an availability set. That means that for the SLA to apply, there must be at least two instances of the VM deployed within an availability set. Additional details pertaining to availability sets for Azure Virtual Machines are discussed later in this chapter.

See Also See the SLA at http://azure.microsoft.com/support/legal/sla/ for full details.

Virtual machine models

As you may recall from earlier in this book, there are two models for working with many Azure resources: Azure Resource Manager (ARM) and Azure Service Management (often referred to as the classic model or ASM). Please see Chapter 1, "Getting started with Microsoft Azure," for a more detailed overview. It is recommended that you use the Resource Manager model for new deployments. The classic model is still supported; however, the newest innovations will be made available only for the Resource Manager model.

For the purposes of this chapter, both models are covered, but the emphasis is on the Resource Manager model.

There are significant and fundamental differences in working with Azure Virtual Machines in these models.

Azure Resource Manager model

When working with the Resource Manager model, you have explicit and fine-grained control over nearly all aspects of the Azure VM. You will explicitly add components such as a network interface card (NIC), public IP address, data disks, load balancer, and much more.

You may recall that Resource Manager uses various resource providers to enable access to and management of Azure resources. There are three main resource providers used when working with Azure Virtual Machines: Network, Storage, and Compute.

- The Network resource provider (Microsoft.Network) handles all aspects of network connectivity such as IP addresses, load balancers, NICs, and so on.
- The Storage resource provider (Microsoft.Storage) handles the storage of the disks for a VM (in the context of Azure Virtual Machines).
- The Compute resource provider (Microsoft.Compute) handles details related to the VM itself, such as naming, operating system details, and configuration (size, number of disks, and so on).

In addition to explicit control over the virtual machine's components, you have the ability to take advantage of other Resource Manager features, such as:

- Deployment and management of related resources as part of a resource group
- Tags to logically organize and identify resources
- Role Based Access Control (RBAC) to apply necessary security and control policies
- Declarative template files
- Deployment policies to enforce specific organizational rules
- Consistent, orchestrated deployment process

This ability affords you a great deal of control in configuring the environment to your exact needs.

Classic/Azure Service Management model

In the classic deployment model, VM deployments are always in the context of an Azure cloud service—a container for VMs. The container provides several key features, including

a DNS endpoint, network connectivity (including from the public Internet if desired), security, and a unit of management. While you get these things for free—because they're inherited from the cloud service model—you have limited control over them.

Use of the classic model also excludes the use of the additional value adding features available via Azure Resource Manager (tags, template files, and so on).

Virtual machine components

Like a car, there are many components that make up a virtual machine. Also like a car, there are multiple configuration options available to suit the specific functional needs and desires of the owner. The sections that follow describe several of the critical components of Azure Virtual Machines. Additionally, more advanced configuration options will be discussed later in the chapter. But first, the base model needs to be established.