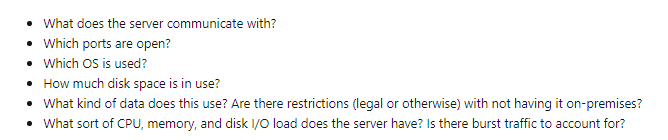
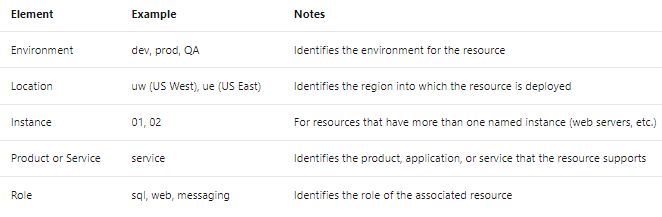
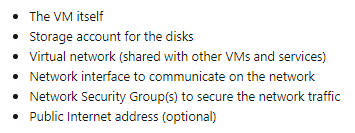
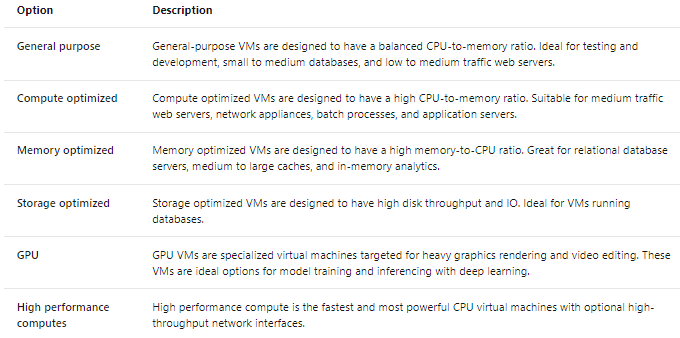
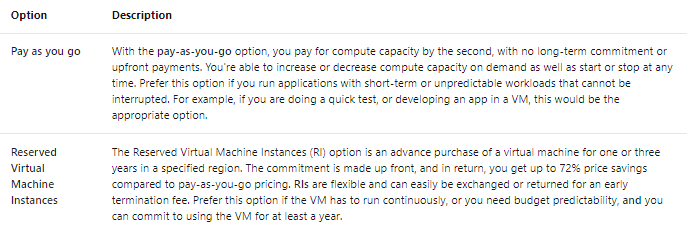
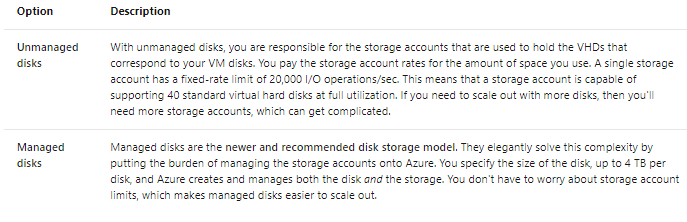
**Introduction to Azure Virtual Machines**

**Compile a checklist for creating an Azure Virtual Machine**

1. Start with the network
   1. The first thing you should think about isn't the virtual machine at all - it's the network
   2. Virtual networks (VNets) are used in Azure to provide private connectivity between Azure Virtual Machines and other Azure services
   3. When you set up a virtual network, you specify the available address spaces, subnets, and security
2. Segregate your network
   1. By default, there is no security boundary between subnets
   2. NSGs act as software firewalls
3. Plan each VM deployment
4. Name the VM
   1. The VM name is used as the computer name, which is configured as part of the operating system
   2. This name also defines a manageable Azure resource
   3. Good convention is to include the following information in the name:
   4. For example, devusc-webvm01
5. What is an Azure resource?
   1. An Azure resource is a manageable item in Azure



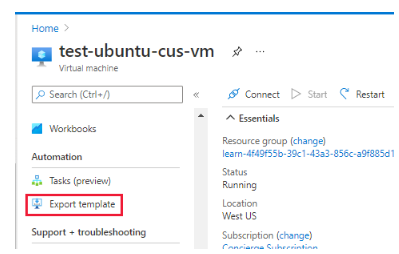
1. Decide the location for the VM
   1. Azure has datacenters all over the world filled with servers and disks
   2. Regions ('West US', 'North Europe', 'Southeast Asia', etc.) provide redundancy and availability
   3. When you create and deploy a virtual machine, you must select a region where you want the resources (CPU, storage, etc.) to be allocated
2. Determine the size of the VM
   1. Once you have the name and location set, you need to decide on the size of your VM
   2. Workload options are classified as follows on Azure:
3. What if my size needs change?
   1. You can **upgrade** or **downgrade** the VM - as long as your current hardware configuration is allowed in the new size
   2. The command line tools will report an error if you attempt to resize a VM to an unavailable size
   3. Be careful about resizing production VMs - they will be rebooted automatically which can cause a temporary outage
4. Understanding the pricing model
   1. There are two separate costs the subscription will be charged for every VM: compute and storage
   2. **Compute:** Compute expenses are priced on a per-hour basis but billed on a per-minute basis. For example, you are only charged for 55 minutes of usage if the VM is deployed for 55 minutes. You are not charged for compute capacity if you stop and deallocate the VM since this releases the hardware
   3. **Storage:** You are charged separately for the storage the VM uses. 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
   4. You're able to choose from two payment options for compute costs:
5. Storage for the VMs
   1. Best practice is that all Azure virtual machines will have at least two virtual hard disks (VHDs)
   2. The first disk stores the operating system, and the second is used as temporary storage
   3. You can add additional disks
   4. Maximum number is determined by the VM size selection
   5. The data for each VHD is held in Azure Storage as page blobs
6. What is Azure Storage?
   1. Azure Storage is Microsoft's cloud-based data storage solution
   2. Provides security, redundancy, and scalable access to the stored data
   3. Virtual disks can be backed by either Standard or Premium Storage accounts
   4. Azure Premium Storage leverages **solid**-**state** **drives** (**SSDs**) to enable high performance and low latency
   5. You can choose either **unmanaged** disks or **managed** disks:
7. Select an operating system
   1. Azure provides a variety of OS images that you can install into the VM, including several versions of Windows and flavours of Linux
   2. You can search the Azure Marketplace for more sophisticated install images
   3. Finally, if you can't find a suitable OS image, you can create your disk image with what you need

**Exercise - Create a VM using the Azure portalExercise - Create a VM using the Azure portal**

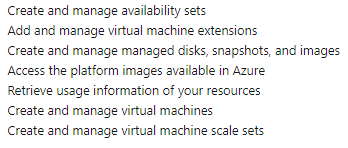
1. To deploy a VM you can use:
   1. ARM Templates
   2. Terraform
   3. Ansible
   4. Jenkins
   5. Cloud-init
2. Azure portal
   1. The **Azure** **portal** provides an easy-to-use browser-based user interface that enables you to create and manage all your Azure resources
   2. You can set up a new database, increase the compute power of your virtual machines, and monitor your monthly costs

**Describe the options available to create and manage an Azure Virtual Machine**

1. The Azure portal is the easiest way to create resources such as VMs
2. However, it's NOT necessarily the most efficient or quickest way to work with Azure, particularly if you need to create SEVERAL resources
3. Ways to create and administer resources in Azure:
   1. Azure Resource Manager
      1. Azure provides you with the option to create a template from which to create an exact copy of a VM
      2. Resource Manager also enables you to create templates, which can be used to create and deploy specific configurations
   2. What are Resource Manager templates?
      1. Resource Manager templates are JSON files that define the resources you need to deploy for your solution



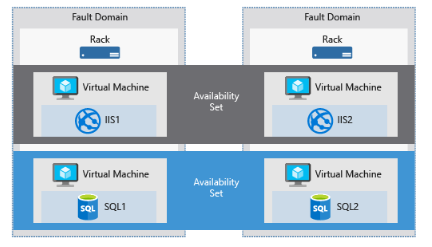
* + 1. You have the option to download or save a template for later use
    2. You can delete a resource group, tweak template and run it again
    3. After you have it working the way you want it, you can use that template to easily replicate multiple versions
  1. Azure PowerShell
     1. Azure PowerShell is ideal for one-off interactive tasks and/or the automation of repeated tasks
     2. **New-AzVM** cmdlet to create a new Azure virtual machine
  2. Azure CLI
     1. Another option for scripting and command-line Azure interaction is the Azure CLI
     2. Available for Windows, Linux and macOS, or in a browser using the Cloud Shell
     3. Azure CLI does not need PowerShell to function
     4. From the CLI, you can create an Azure VM with the **az** **vm** create command
     5. Azure CLI can be used with other scripting languages, such as Ruby and Python
  3. Programmatic (APIs)
     1. Azure PowerShell and Azure CLI are good options if you have simple scripts to run
     2. For complex scenarios, another approach is needed
     3. Azure REST API
        1. Operations are exposed as URIs with corresponding HTTP methods (GET, PUT, POST, DELETE, and PATCH)
        2. Azure Compute APIs give you access to:



* + 1. Azure Client SDK
       1. The Azure Client SDK encapsulates the Azure REST API, making it much easier for developers to interact with Azure
       2. C# code to create an Azure VM using the Microsoft.Azure.Management.Fluent NuGet package
  1. Azure VM extensions
     1. Azure VM extensions are small applications that enable you to configure and automate tasks on Azure VMs
     2. Azure VM extensions can be run with the Azure CLI, PowerShell, Azure Resource Manager templates, and the Azure portal
  2. Azure Automation services
     1. **Azure** **Automation** enables you to integrate services that allow you to automate frequent, time-consuming, and error-prone management tasks with ease.
     2. These services include:
        1. **Process** **Automation**: Process automation enables you to set up watcher tasks that can respond to events that may occur in your datacenter
        2. **Configuration** **Management**: Enables you to track updates and take action such as include or exclude
        3. **Update** **Management**: Assess the status of available updates, schedule installation, and review deployment results to verify updates applied successfully

**Manage the availability of your Azure VMs**

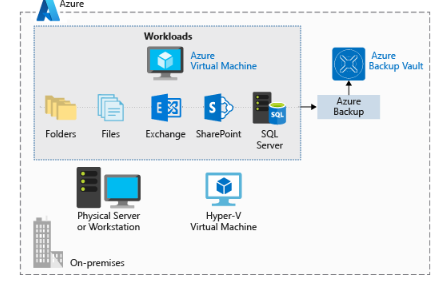
1. What is availability?
   1. Azure VMs run on physical servers hosted within the Azure Datacenter
   2. If the physical server fails, the virtual machines hosted on that server will also fail
   3. If this happens, Azure will move the VM to a healthy host server automatically
   4. VMs could also be affected by periodic updates
   5. Microsoft does not automatically update your VMs OS or software. You have complete control
   6. It is recommended to deploy at least two instances of each VM. This feature is called an availability set
2. What is an availability set?
   1. An availability set is a logical feature used to ensure that a group of related VMs are deployed so that they aren't all subject to a single point of failure
   2. **Microsoft** offers a **99**.**95%** external connectivity **service** **level** **agreement** (**SLA**) for multiple-instance VMs deployed in an **availability** **set**
   3. You can build availability sets with ARM templates
3. Fault Domains
   1. A fault domain is a logical group of hardware in Azure that shares a common set of hardware components
   2. The first two VMs in an availability set will be provisioned into two different racks



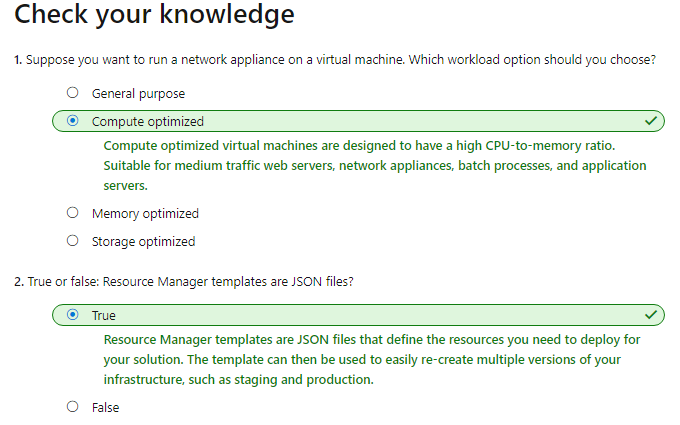
1. Uptime Domains
   1. Azure will automatically place availability sets into update domains to minimize the impact
   2. Availability sets are not fool proof
2. Failover across locations
   1. Azure Site Recovery replicates workloads from a primary site to a secondary location
   2. If an outage happens at your primary site, you can fail over to a secondary location
   3. Site recovery advantages:
      1. eliminating the cost and complexity of maintaining a secondary physical datacentre
      2. Makes it easy to test your planned or unplanned failovers

**Back up your virtual machines**

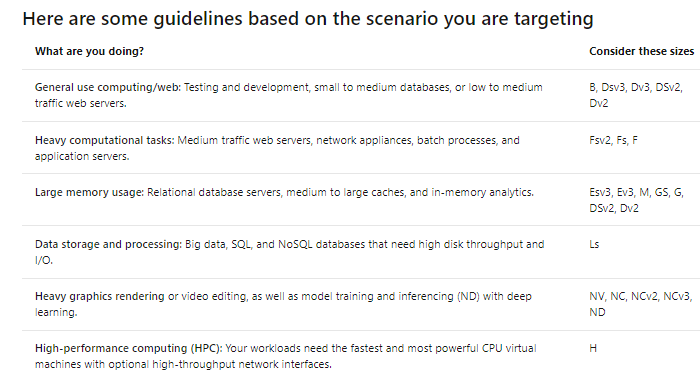
1. Azure Backup is a backup as a service offering that protects physical or virtual machines no matter where they reside: on-premises or in the cloud
2. Data backup scenarios:
   1. Files and folders on Windows OS machines
   2. Application-aware snapshots
   3. Popular Microsoft server workloads such as Microsoft SQL Server, Microsoft SharePoint, and Microsoft Exchange
   4. Native support for Azure Virtual Machines, both Windows, and Linux
   5. Linux and Windows 10 client machines



1. Advantages of using Azure Backup
   1. Azure Backup was designed to work in tandem with other Azure services and provides several distinct benefits:
      1. Automatic storage management
      2. Unlimited scaling
      3. Multiple storage options
      4. Unlimited data transfer
      5. Data encryption
      6. Application-consistent backup
      7. Long-term retention
2. Use Azure Backup
   1. The component depends on what you want to protect:
      1. Azure Backup agent
      2. System centre data protection manager
      3. Azure backup server
      4. Azure backup VM extension
3. A **vault** is backed by **Azure** **Storage** **blobs**, making it a very efficient and economical long-term storage medium

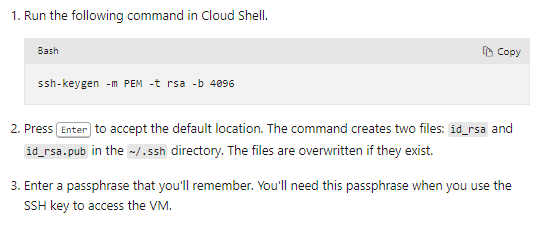


**Create a Linux virtual machine in Azure**

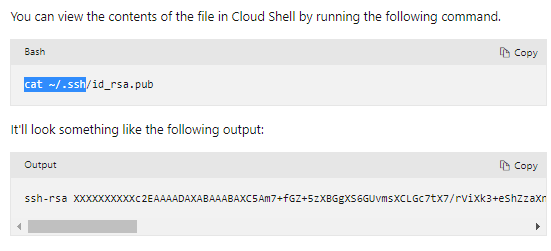
1. You can also use a remote Secure Shell (SSH) to connect directly to the running VM
2. Run Linux in Azure
   1. Microsoft has partnered with prominent Linux vendors to ensure their distributions
3. Create an Azure VM
   1. VMs can be defined and deployed on Azure in several ways: the **Azure** **portal**, **a** **script** (using the **Azure** **CLI** or **Azure** **PowerShell**), or an **Azure** **Resource** **Manager** template
4. Resources used in a Linux VM
   1. These must exist (and be selected during VM creation), or they will be created with the VM:
      1. CPU and memory resources
      2. Azure Storage
      3. Virtual disks to hold the OS and data
      4. A virtual network (VNet) to connect Azure to on-premises
      5. A network interface to communicate with the VNet
      6. An optional public IP address
5. Choose the VM image
   1. First and most important decisions
   2. n image is a template that's used to create a VM
6. Size your VM
   1. VMs have certain amount of memory and CPU power
   2. VM sizes are grouped into **categories**, starting with the **B-series** for **basic** testing and running up to the **H-series** for **massive** **computing** **tasks**
7. Choose storage options
   1. First choose disk technology
   2. Choose between HDD and SSD
   3. There are two levels of SSD storage available: standard and premium
8. Map storage to disks
   1. Azure uses virtual hard disks (VHDs) to represent physical disks for the VM
   2. VHDs are stored as page blobs in an Azure Storage account
   3. By default, two virtual hard disks (VHDs) will be created for your Linux VM:
      1. **Operating** **system** **disk**: Primary driver. Maximum capacity of 2048 GB. It will be labeled as **/dev/sda** by default
      2. **Temporary** **disk:** This provides temporary storage for the OS or any apps
   4. The temporary disk is not persistent
9. What about data?
   1. You can store data on the **primary** **drive** along with the OS, but a better approach is to create **dedicated** **data** **disks**
10. Unmanaged vs. managed disks
    1. Final choice is to use unmanaged or managed disks
    2. With **unmanaged** **disks**, you are responsible for the storage accounts
    3. **Managed** **disks** are the newer and recommended disk storage model
    4. You specify the disk type (Premium or Standard)
    5. Managed disks benefits:
       1. Increase reliability
       2. Better security
       3. Snapshot support
       4. Backup support
11. Network communication
    1. Virtual machines communicate with external resources using a virtual network (VNet)
    2. You can divide them up with subnets to isolate resources
12. Plan your network
    1. When you create a new VM, you will have the option of creating a new virtual network or using an existing VNet

**Exercise - Decide an authentication method for SSH**

1. The default approach to administering Linux VMs hosted in Azure is **SSH**
2. What is SSH?
   1. Secure Shell (SSH) is an encrypted connection protocol
   2. Allows secure sign-ins over unsecured connections
   3. SSH allows you to connect to a terminal shell from a remote location
   4. There are two approaches we can use to authenticate an SSH connection: **username** and **password**, or an **SSH** **key** **pair**
   5. Using passwords with SSH connections leaves the VM vulnerable to brute-force attacks of passwords
   6. Rather use **public**-**private** **key** **pair**, also known as **SSH** **keys**
   7. With an SSH key pair, you can sign in to Linux-based Azure virtual machines without a password
   8. There are two parts to an SSH key pair: a public key and a private key:
      1. The **public** **key** is placed on your **Linux** **VM**. Can be shared with anyone
      2. The **private** **key** is what you present to **verify** your identity to your Linux VM
3. Create the SSH key pair
   1. Use the built-in **ssh**-**keygen** command to generate the SSH public and private key files



1. Private key passphrase
   1. You can provide a passphrase while generating your private key
   2. This passphrase is used to access the private SSH key file
   3. encrypts the private key using 128-bit AES
2. Use the SSH key pair with an Azure Linux VM

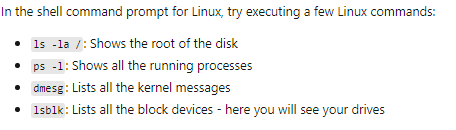


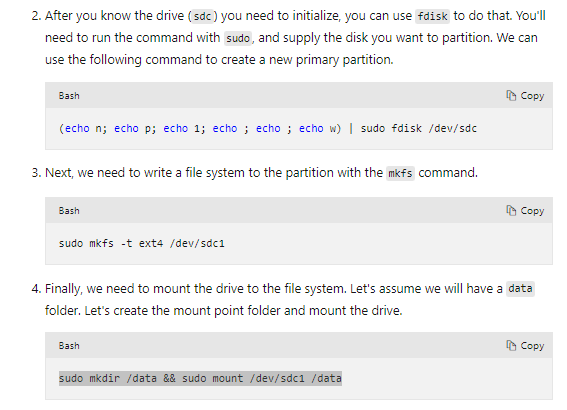
1. Use the SSH key when creating a Linux VM
   1. To apply the SSH key while creating a new Linux VM, you will need to copy the contents of the public key and supply it to the Azure portal, or supply the public key file
2. Add the SSH key to an existing Linux VM
   1. If you have already created a VM, you can install the public key onto your Linux VM with the **ssh**-**copy**-**id** command
   2. After the key has been authorized for SSH, it grants access to the server without a password
   3. For example, if we had a Linux VM named myserver with a user azureuser, we could run the following command to install the public key file, and authorize the user with the key

**Azure virtual machines IP addresses and SSH options**

1. Azure VM IP addresses
   1. With a public IP, we can interact with the VM over the Internet
   2. Alternatively, we can set up a virtual private network (VPN) that connects our on-premises network to Azure
   3. Public IP addresses in Azure are dynamically allocated by default
2. Connect to the VM with SSH
   1. To connect to the VM via SSH:
      1. Public IP address
      2. Username of the local account on the VM
      3. Public key configured in that account
      4. Access to the corresponding private key
      5. Port 22 open on the VM

**Exercise - Connect to a Linux virtual machine with SSH**

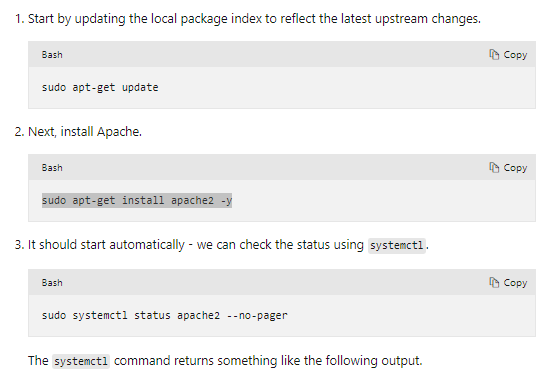


**Initialize data disks**

**Install software onto the VM**

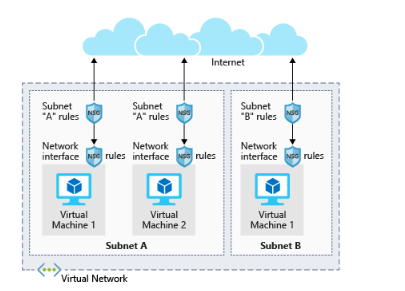
1. You can also install software from the internet when you are connected to the VM via SSH
2. Azure machines are, by default, internet connected

**Install the Apache web server**



**Network and security settings**

1. Open ports in Azure VMs
   1. By default, new VMs are locked down
   2. Apps can make outgoing requests, but the only inbound traffic allowed is from the virtual network
   3. When you create a new VM, you have an opportunity to open a few common ports (RDP, HTTP, HTTPS, and SSH)
   4. The process for this involves two steps:
      1. Create a network security group
      2. Create a network security group.
2. Create a network security group.
   1. Network security groups (NSGs) are the primary tool you use to enforce and control network traffic rule
   2. **NSGs** are an **optional** **security** layer that provides a software firewall by filtering inbound and outbound
3. Security group rules
   1. NSGs use **rules** to allow or deny traffic moving through the network



* 1. These default rules cannot be modified but can be overridden

**How Azure uses network rules**

1. For **inbound** **traffic**, Azure processes the security group associated to the subnet, and then the security group applied to the network interface
2. **Outbound** **traffic** is handled in the opposite order (the network interface first, followed by the subnet)
3. If no security group is applied, then all traffic is allowed by Azure
4. The rules are evaluated in priority order, starting with the lowest priority rule
5. The last rule is always a **Deny** **All** rule

**Exercise - Configure network settings**

