Azure -VM

Server 2008 R2 and above is supported. You can either use the templates provided or bring your own VHD. Server 2012 was introduced, Microsoft encouraged us to convert our VHDs to VHDXs.

Server 2003 64-bit is supported, but you are responsible for bringing your own image and managing the VM. This is a good option if you have an older 2003 server that is running a line of business application that cannot be upgraded for whatever reason. But to be very clear, this does not imply moving Server 2003 to Azure; means the operating system will be compliant or supported.

Azure also supports several application servers including SharePoint Server 2010, SQL Server 2008 64-bit versions, System Center 2012 with Service Pack One, and even Exchange Server 2013.

When using an Azure VM, you cannot install DHCP. You cannot install the Hyper-V role, Rights Management Services, and Windows Deployment Services are not supported, and neither is Remote Access/Direct Access. You will not even see the options to install these roles on the Azure Virtual Machine.

In addition to the five roles not being supported, the following features are not supported either; BitLocker Drive Encryption, Internet Storage Name Server, Multipath I/0, Network Load Balancing, Peer Name Resolution Protocol, SNMP Services, Storage Manager for SANs, Windows Internet Name Service, and of course the Wireless LAN service. knowing what you can and cannot do with your Azure Virtual Machines will dictate how you design your implementation.

The Active Directory Services are included, we can run the Application Server role, obviously the DNS Server, Failover clustering and File Services, Network Policy and Access Services, Print and Document Services, Remote Access, Remote Desktop Services; again another asterisks hold on, Web Server, and then Windows Server Update Service. In the cases of Failover Clustering and RDS there are some stipulations you need to be aware of.

The version I've indicated is the lowest version that is supported, and more recently LSASS (Local Security Authority Subsystem Service) will also be supported. Please be sure to refer to the Microsoft Azure website for the most recent and any caveat that may be associated with each version.

Other supported Microsoft Operating Systems include BizTalk Server, Several flavors of Dynamics, Forefront Identity Manager, HPC Pack, Project Server, and Team Foundation Server.

Microsoft takes care of everything from the concrete to the hypervisor layer. You are still responsible for backing up that VM, hardening it, patching it, and updating it. And remember, you only pay for the virtual machine when it is running.

you can shut down and deallocate your machines automatically, saving you money.

Create the resource group and network first, but you can create the resource group during the creation of the virtual machine. Next our VHDs, and yes, these are VHDs not VHDXs, are housed in a storage account. And finally, diagnostic logs are kept in a log storage account. All of these components are contained within the resource group with the exception of the Temp drive.

use the templates that Microsoft offers. If you use these images, in most cases the licensing costs are included. You can bring your own image. In this scenario, you will need to provide licensing and as I've already mentioned, these images that you bring into Azure must be VHD, not VHDX.

use a portal to create your virtual machines. You can also leverage PowerShell and the command line interface.

We're going to do everything in Resource Manager. I'm going to go ahead and click Create. We're going to go ahead and provide the basic information about our virtual machine. First thing is our name. I'm going to name it Prod1. Our disk type, I'm just going to use an HDD drive instead of the SSD. We must provide a user name and password.

Typically, you'll put your virtual machines in the location closest to you to reduce latency.

Next, you will be presented with some sizing options. You will notice that you'll have the number of cores, the number of gigabytes that are available in this virtual machine, how many data disks you can attach, your IOPS, whether or not load balancing is included. And in the case of the D1, we can also have a local SSD. Those are the recommended virtual machines.

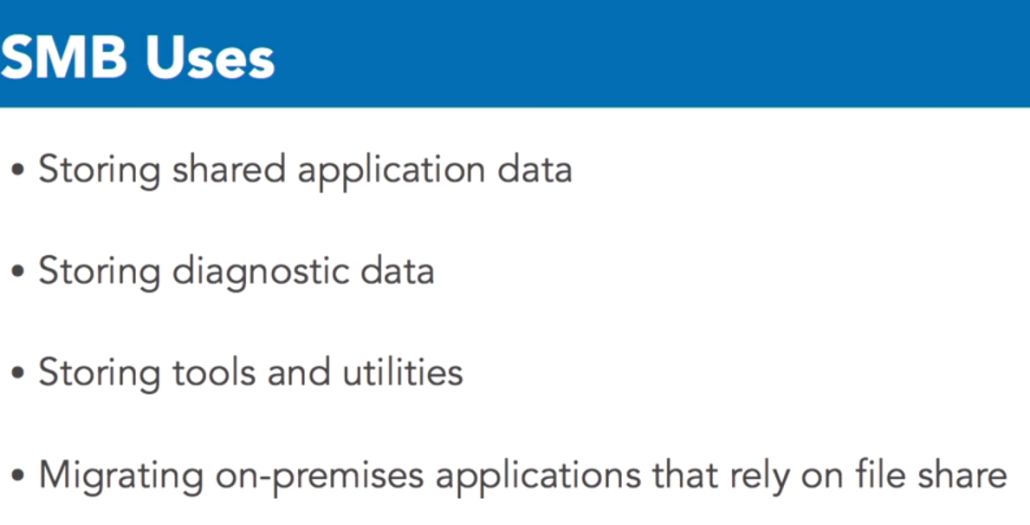
We have some basic details about it, the resource group it belongs to, the computer name, the size, the public IP address. If I scroll down, I can see some basic metrics about our virtual machine. I can go ahead and now connect to this virtual machine. To do so, click Connect. An RDP client will be downloaded for us. If you shut down the virtual machine from within the virtual machine, we go to our Windows key and shut down, and then click Shut Down from here, our virtual machine will still be running in Azure and you will be billed for it. The trick is to shut it down from within the portal. What will happen is your status here will turn from Running to Stopped Deallocated. Once it is stopped and deallocated, you'll no longer be billed for that virtual machine running. Yes, you'll still pay for the storage that it is consuming, but not for the virtual machine cycles. When we need to start it again, we just click the Start button.

Currently, Azure supports the following Linux distros, CoreOS, CentOS 6.2, Debian 7.0, Ubuntu 12.04, openSUSE 12.3, SUSE Linux Enterprise Server 11 SP2, Oracle Linux 6.4, and Red Hat 6.7.

One thing you'll want to do, not only with your Linux Virtual Machines, but also your Windows Virtual Machines, is always attach a disk. To do so, click "Attach New", and I'll go with the defaults here, and click "OK". That disk will now be attached to that Virtual Machine. You can back up your Virtual Machine, you can also schedule an auto shutdown of your Virtual Machine. You can do it through the schedules here, or if you want you can create a script to shut down all your Virtual machines let's say in your resource group.

Desired State Configuration, or DSC, was introduced for Server 2012 R2, back in 2013. It's an automation mechanism to ensure your servers, either physical or virtual, always have the same configuration applied to them. Here's an example of DSC. Let's imagine I have setup a server exactly the way I want it, then someone comes along and changes a setting, which messes up my configuration. This could have undesired consequences. Instead of me now trying to figure out what changed, I can use DSC and the server will automatically correct itself based on my scripts that I've applied to it.

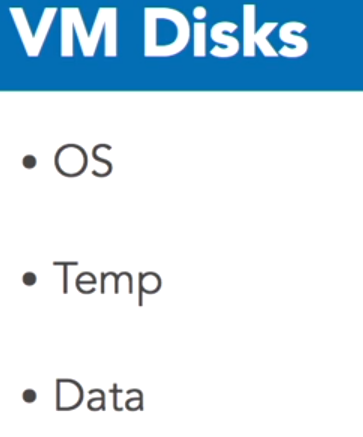
We can also use virtual machine extensions to configure our virtual machines. There are several extensions already available to you, or you can use custom scripts. Examples of configuration settings that you can manage through DSC include server roles and features, registry settings, files and directories, packages, environment variables, and deploying new software. DSC is a great automation tool, but it is out of scope for this course. There are two ways you can apply DSC to your virtual machines. You can use an automation account, or we can do it through the virtual machine extensions.

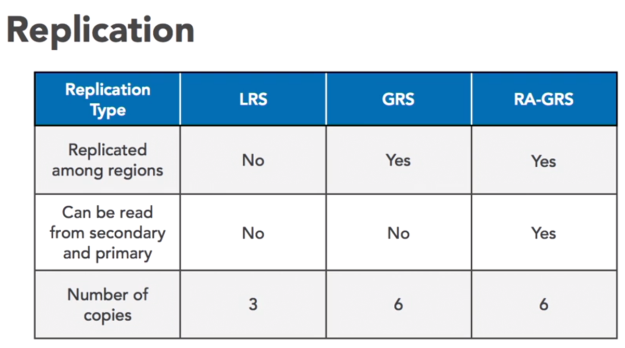
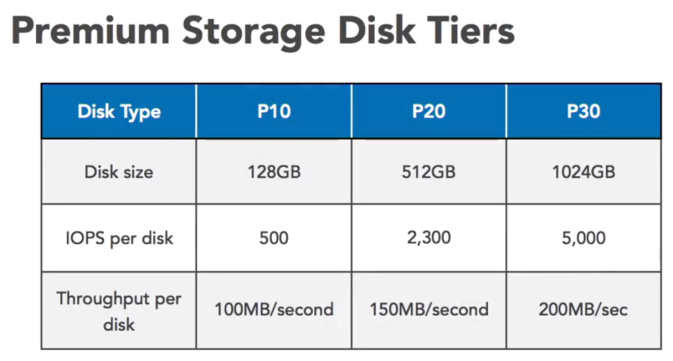


SMB file shares in Azure became generally available and IT pros rejoiced. You see, prior to this it was not possible to have a mounted shared drive accessible by not only the virtual machines in Azure, but also from the on-premise environment. If we wanted to have a shared drive, we either used one drive or created a shared drive on a virtual machine and shared that out. What we really wanted was storage on Azure that we treated as a disk. Some of the most common uses of SMB file shares include storing shared application data, storing diagnostic data, storing tools and utilities, and migrating on-premise applications that rely on a file share.

Shared storage in Azure has a very similar construct as our on-premise configuration. We start with the storage account. Within that storage account we have the share. You can keep unlimited files in that share, but it has a capacity of five terabytes. Keep that in mind during your planning stage. Again, you hear me say planning again and again. Then we have directories, which are optional but I would highly recommend you use a proper directory structure, just as we do with our on-premise environments. And finally, we have our files in our directories.

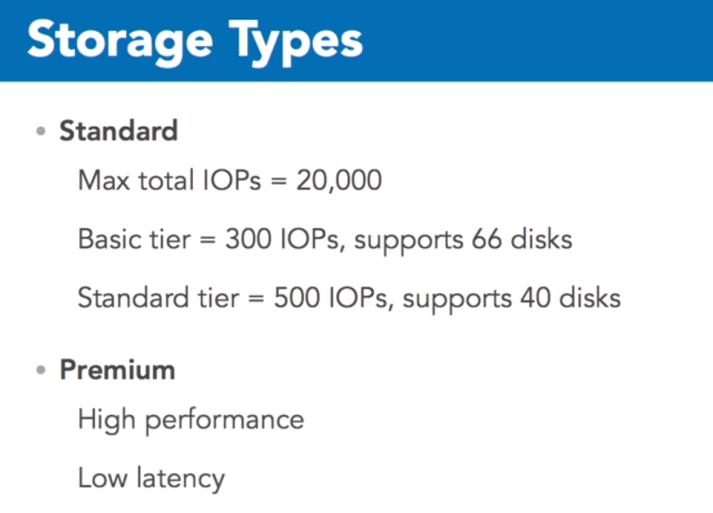
The maximum file size is one terabyte.





In Azure, we have different choices for our storage. We can have a local-redundant, geo-redundant, zone-redundant. An Azure Virtual Machine is provisioned with two disks, the OS and the Temp drive, and it is highly recommended that you add additional data disks. The operating system disk has a maximum capacity of 1023 gigabytes. And just as with any Windows System, this OS disk is labeled c drive. Next we have the Temp disk. This disk is used for storing the page file .cis. Before you get all excited and plan to use this disk for your storage, don't do it! This drive is a temp drive. And any data on that disk will be lost, when that system reboots. This is now clearly indicated on the disk within the virtual machine itself.

the operating system disks that are registered as SATA drives, the data disks are registered as SCSI drives. And each data disk has a maximum capacity of 1023 gigabytes. And the number of disks that can be attached to a virtual machine, again, is dependent on the size of the virtual machine that you select. Again, this is why planning is so important, when you're moving to Azure. When a disk is created, to prevent accidental deletion, Azure places a lease on that disk. Azure uses VHDs for all disks, and only fixed disks are supported.



The VHDs are stored in page blobs in your Azure storage account. And this storage account can either be a standard or premium storage account. A standard storage account has a maximum total request rate of 20,000 IOPs, and all of your virtual machine IOPs should not go passed that point. And within the standard storage type we have two additional tiers. The basic tier disk has a maximum IOP of 300, and the standard tier has a maximum IOP of 500.

These drives are SSD drives. And the maximum amount of storage you can have, with a premium drive per VM is 64 terabytes. Premium drives are best suited for applications, such as Dynamics AX, Dynamics CRM, Exchange, and Share Point Farms. Database workloads including Oracle, SQL Server, and MySQL will also benefit from using these drives. Premium storage accounts are only available on specific VMs. The way I like to remember which VMs can support premium storage, are VMs that have a "s" in the name.

Such as a DS, a DSV2, GS or an FS. Premium storage guarantees the capacity, IOPs and throughput are allocated to the disk. Premium storage is available in three tiers, the P10, P20 and P30. As you move up the tiers, your disk size increases. The number of IOPs per disk also increases and so does the throughput per disk. This also means that the price will increase, as you move through those tiers as well. The data in your Azure storage account, is always replicated.

You do not have to worry about configuring software mirroring on your Azure virtual machines. And this is done using the replication feature already provided to you within the Azure environment. You can configure the type of replication for your storage accounts. And for your VHDs which are stored as page blobs in your storage accounts. Our page blobs can support local redundant storage, LRS, Geo-Redundant Storage or GRS, and RA-GRS. Which is read access, Geo-Redundant Storage.

Our first option is LRS. This provides three copies within the region, and it's less expensive because we're only dealing with three copies. You may want to use LRS if you're dealing with governance restrictions or you may already have a replication strategy in place. GRS, replicates your data to a second region. Hundreds of miles from the primary data center. Therefore, we have six copies across two regions. And then we have read access GRS. In this case if the primary region is unavailable, the data can be read but not written from the secondary region. RA-GRS is designed for high availability scenarios. You may also come across zone redundant replication. Which is only available for general purpose storage accounts. And premium storage only supports LRS. Remember replication does not protect you from upgrades that go wrong or fat finger deletes. You are still responsible for maintaining the integrity of your data. I cannot stress enough the importance of planning your storage capacity. If you do not choose the appropriate size virtual machines, not only for now but for future use, you may find, as your infrastructure grows that you're going to have to recreate some of that infrastructure to accommodate more storage.

Again, what type of drive do you want? I'm going to go with the HDD. My maximum size, the location, you could change this. I'm going to leave this as is. You'll notice at the bottom we have host caching. Caching can hinder or help your application. For our data disk, we have three choices. We have a read/write, a read, or none. None is default and I am going to recommend going default until you are comfortable with Azure VMs themselves.

You would select a read/write if you were reading and writing large amounts of data. Re-cache can improve your sequential IO when the data is read during the input/output and stored to cache. And as I said, our default is none and does not use any cache. I'm going to leave it as default. The OS disk also has similar options. It has the read/write and it has read only. None is not an option on your OS disk. By default, the read/write is enabled on your operating system disk.

Azure Disk Encryption safeguards your Windows and Linux virtual machines by ensuring you have complete control over those virtual machines. The keys to the kingdom, or in our case, your virtual machines, are in your hands. Encryption is only available for your Windows and Linux v2 virtual machines, which means it's only available in the Azure Resource Manager. Windows machines are encrypted using BitLocker, and your Linux machines are encrypted using dm-crypt. An Azure Key Vault is integrated to help you control and manage the encryption keys

The virtual machine disks are encrypted at rest to comply with your organization's security and compliance requirements. Some of the more typical scenarios we see for disk encryption include encrypting an existing virtual machine in Azure. You may want to encrypt your new virtual machines that you've created from the Azure gallery. You may want to encrypt new virtual machines that have been created from a previously-encrypted VHD. You may need to disable encryption on a Windows virtual machine. You can also disable encryption on Linux data drives, and you can back up and restore encrypted virtual machines.

Now let's take a look at what we can't do with encryption. First of all, we can't encrypt our basic virtual machine tiers. Your virtual machines must be at the standard tier. You cannot disable encryption on the Linux OS drives. Disk encryption is only available in the Azure Resource Manager. You cannot integrate with your on-premise key management service, but you can bring your own key management service into Azure.

And you cannot encrypt Azure file shares, dynamic volumes, network file systems, or virtual machines using software RAID. The Azure Key Vault is your container under your control. It keeps the owner key separated from the data owner. And you can deploy quickly and easily using the Azure Key Vault. The Azure Key Vault is backed by Microsoft's hardware security module. Azure Key Vault is a multitenant service. You do not have a dedicated hardware security module, and your virtual machine and Key Vault must reside in the same region.

And finally, to use the Azure Key Vault, you're going to have to register an Azure Active Directory application, because Azure Active Directory authentication is used to manage the keys in the vault. You have three options for managing your keys. You can use the Azure Key vault and allow Microsoft to manage the keys for you. You can bring your own keys, and use the Azure Key Vault, and you still maintain control over those keys. And finally, you can use your own on-premise key management service, which keeps you in complete control.

The supported operating systems for encryption include 2008 R2 and above, Windows 8 and above, Ubuntu 16.04, CentOS 7.2, Red Hat Enterprise 7.2, and SUSE Linux Enterprise.

encrypt a disk first thing we need to do is register an application in Azure Active Directory. Because any applications that use a key vault must authenticate to Azure Active Directory.

application to be created and registered. Before we leave this section, we need to grab a couple keys from that application we just created. I'm going to go ahead and copy that. I'm going to paste that application ID into Notepad. And we also need the secret key. I'm going to go back into Azure, and that will be under Keys. We don't have anything in here right now, we have to go ahead and create that. Provide a name. When does this key expire? I'm going to choose a year.

Copy the key value. You won't be able to retrieve after you leave this blade. If you do not copy this now, you're not going to have a chance to come back later and do so, so please do this as soon as you can.

remember those two keys I had you copy? This is where we're going to use them. Enter the key vault name. And then the key vault resource group. We're going to leave the rest of the fields as-is. Now, you'll notice here, there is a Terms and Conditions. Read through it, maybe send it to your lawyer, and then you have to agree to the Terms and Conditions, because we've all read them all the time. And then click Purchase. This will take a few moments. While we're waiting, I'm going to go ahead and click in my Virtual Machines blade. As you can see, disk encryption on data2 (HARDDISK) has not been enabled as of yet. This can take several minutes, 10 to 15 minutes, for the disk to be encrypted. You now see that data2, the disk is now encrypted. I'm going to open up data2. I'm going to click on Disk, and our OS disk, encryption is now enabled.

Microsoft does recommend encrypting your disk on your Azure Virtual Machines, and as you can see, it's a very simple process to do.