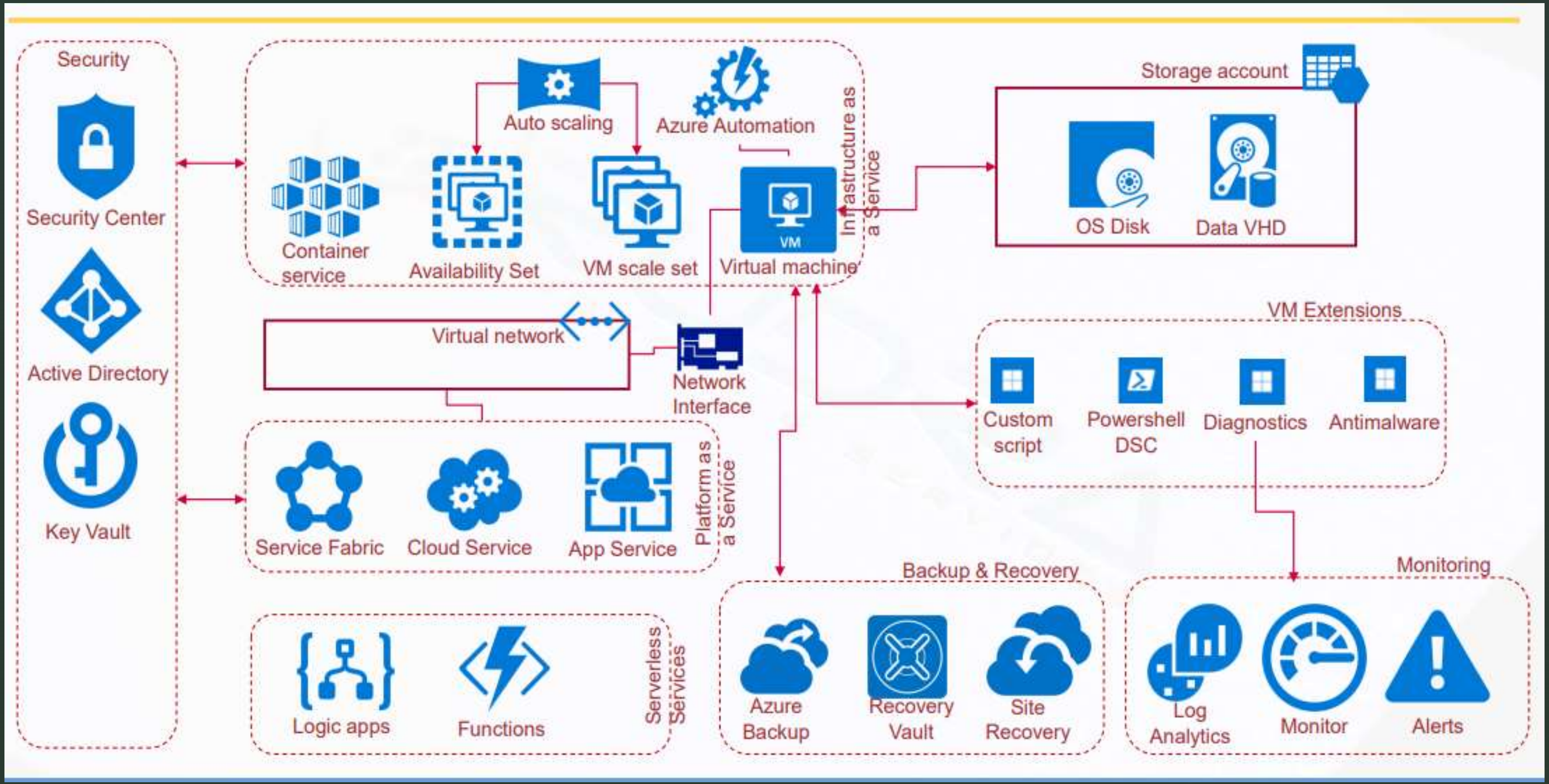
Ravindra Kudache

VM Management

Azure Compute Architect



Virtual Machine deployment options

- **AzureVirtualMachines**willletyoucreateandusevirtualmachinesinthecloudasInfrastructureasa Service.
- •YoucanuseanimageprovidedbyAzureorpartnersoruseyourowntocreatethesame.
- •Virtualmachinescanbecreatedandmanagedusing
- •Azureportal
- •AzurePowershellandARMtemplates
- •AzureCLI
- •ClientSDK’s
- •RESTAPIs

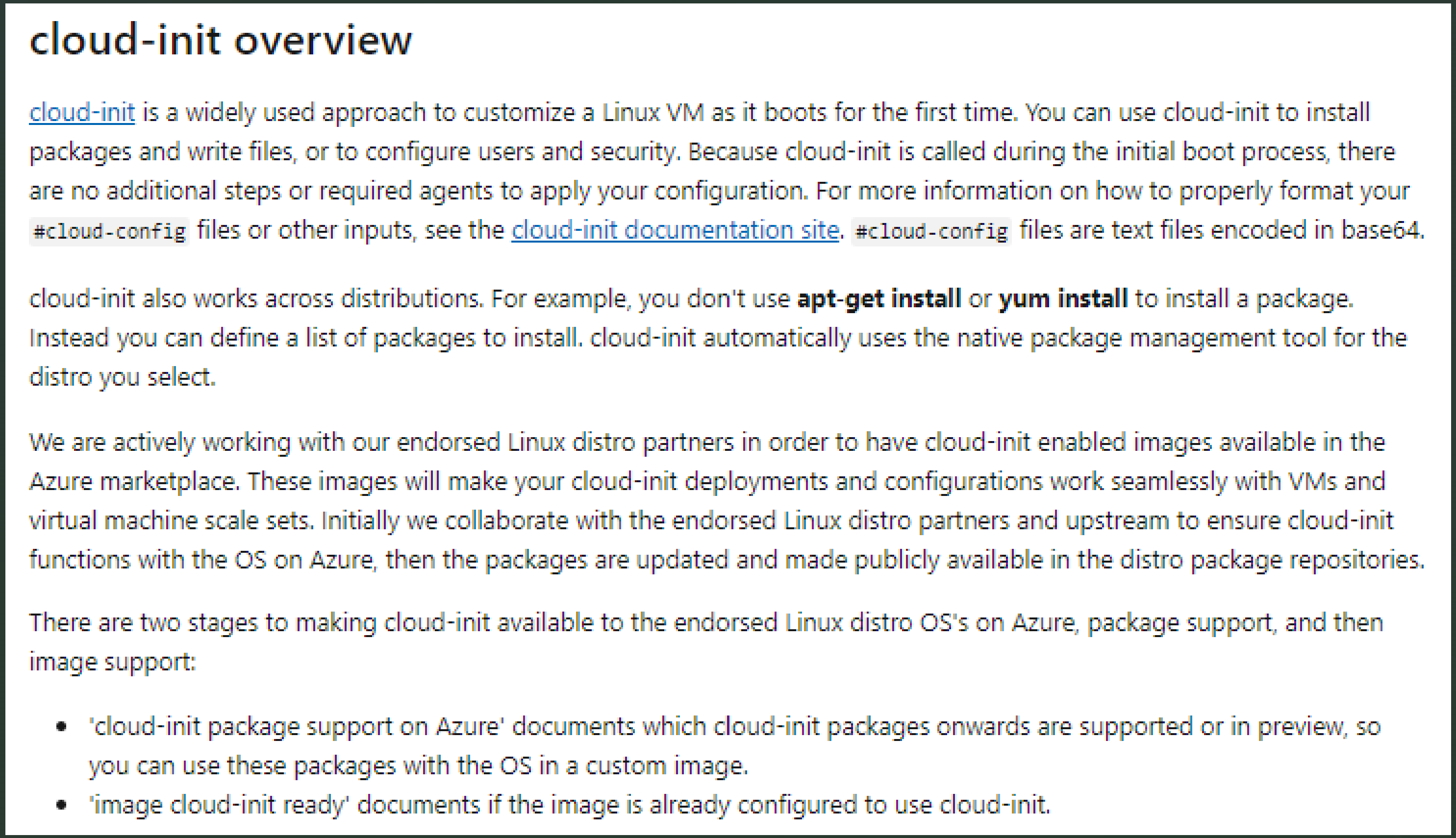
Virtual Machine configuration choices

- FollowingaretheconfigurationchoicesthatAzureofferswhilecreatingaVirtualMachine
- •Operatingsystem(Windows&Linux)
- •VMsizewhichdeterminesfactorssuchasprocessingpower,howmanydisksyoucanattachetc.
- •RegionwhereVMwillbehosted
- •VMextensionswhichgivesadditionalcapabilitiessuchasrunninganti-virusetc.
- •Compute,Networking&StorageelementswillgetcreatedduringtheprovisioningoftheVirtualMachine

DEMO

- 1) VM Creation
- 2) Disk attachment
- 3)Network Creation
- 4)Extension script windows
- 4) Linux script demo

cloud-init



cloud-init overview

cloud-init is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files, or to configure users and security. Because cloud-init is called during the initial boot process, there are no additional steps or required agents to apply your configuration. For more information on how to properly format your `#cloud-config` files or other inputs, see the cloud-init documentation site. `#cloud-config` files are text files encoded in base64.

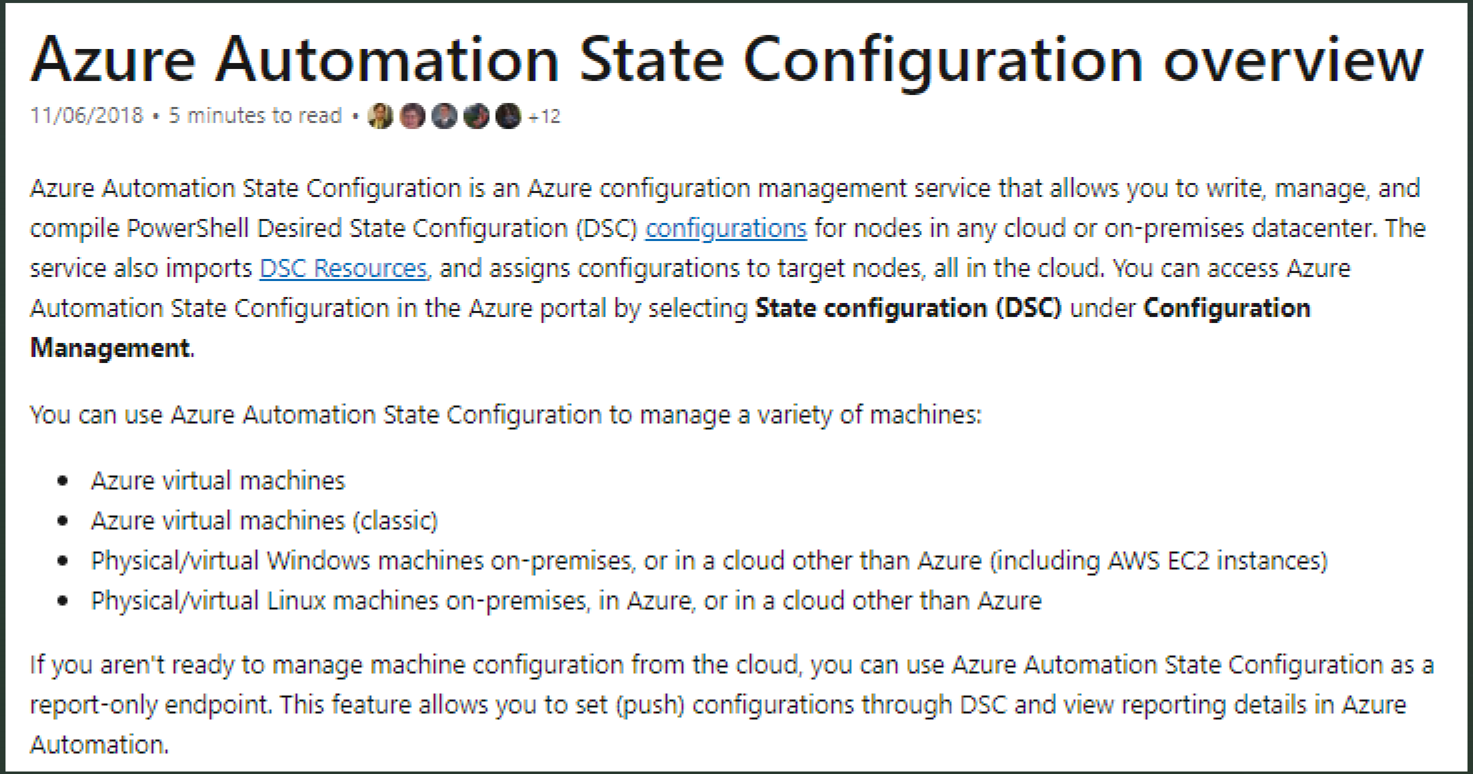
cloud-init also works across distributions. For example, you don't use **apt-get install** or **yum install** to install a package. Instead you can define a list of packages to install. cloud-init automatically uses the native package management tool for the distro you select.

We are actively working with our endorsed Linux distro partners in order to have cloud-init enabled images available in the Azure marketplace. These images will make your cloud-init deployments and configurations work seamlessly with VMs and virtual machine scale sets. Initially we collaborate with the endorsed Linux distro partners and upstream to ensure cloud-init functions with the OS on Azure, then the packages are updated and made publicly available in the distro package repositories.

There are two stages to making cloud-init available to the endorsed Linux distro OS's on Azure, package support, and then image support:

- 'cloud-init package support on Azure' documents which cloud-init packages onwards are supported or in preview, so you can use these packages with the OS in a custom image.
- 'image cloud-init ready' documents if the image is already configured to use cloud-init.

Extension PowerShell desired services



Azure Automation State Configuration overview

11/06/2018 • 5 minutes to read • +12

Azure Automation State Configuration is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations for nodes in any cloud or on-premises datacenter. The service also imports DSC Resources, and assigns configurations to target nodes, all in the cloud. You can access Azure Automation State Configuration in the Azure portal by selecting **State configuration (DSC)** under **Configuration Management**.

You can use Azure Automation State Configuration to manage a variety of machines:

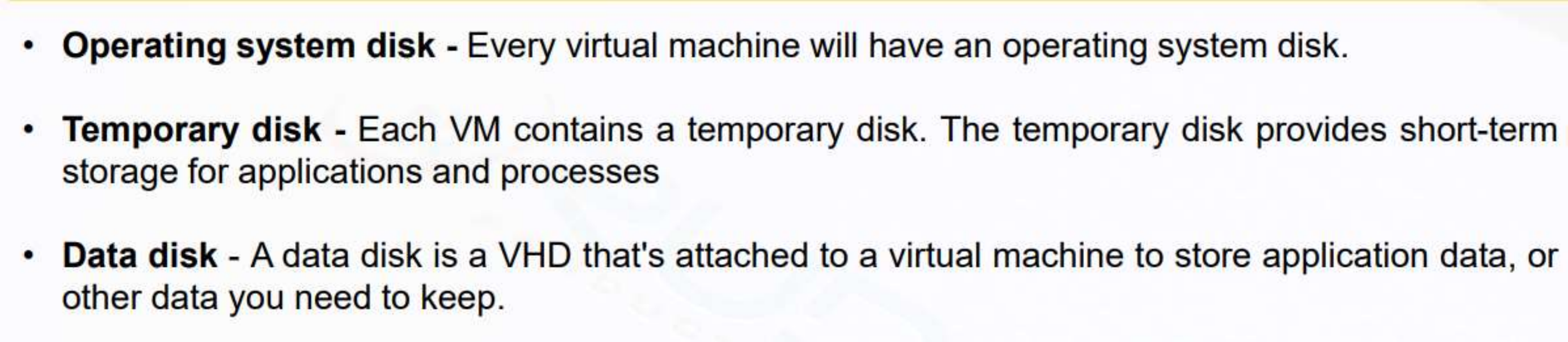
- Azure virtual machines
- Azure virtual machines (classic)
- Physical/virtual Windows machines on-premises, or in a cloud other than Azure (including AWS EC2 instances)
- Physical/virtual Linux machines on-premises, in Azure, or in a cloud other than Azure

If you aren't ready to manage machine configuration from the cloud, you can use Azure Automation State Configuration as a report-only endpoint. This feature allows you to set (push) configurations through DSC and view reporting details in Azure Automation.

Demo

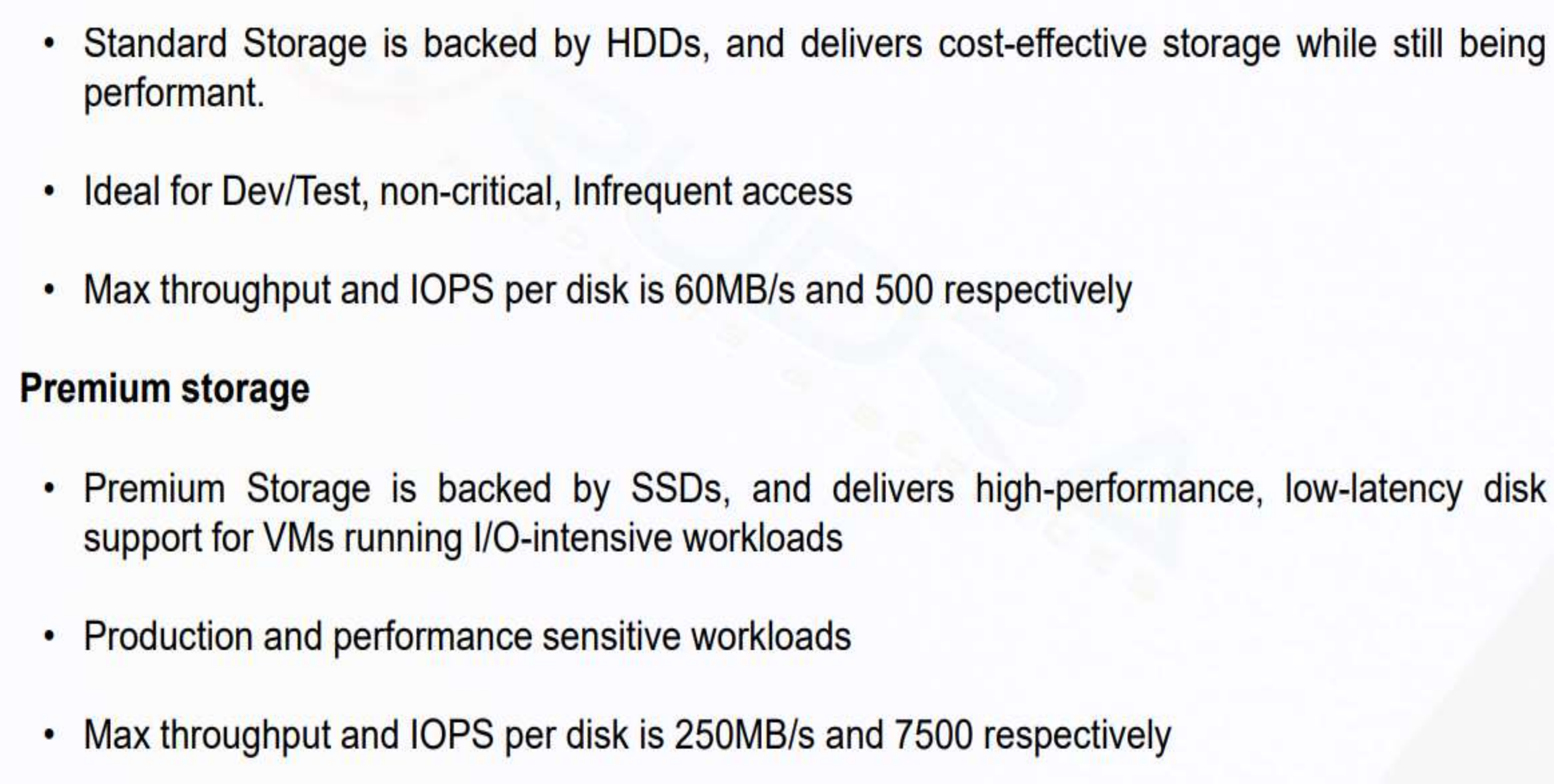
- PowerShell Desired State Configuration

Disks used by VMs



- **Operating system disk -** Every virtual machine will have an operating system disk.
- **Temporary disk -** Each VM contains a temporary disk. The temporary disk provides short-term storage for applications and processes
- **Data disk** - A data disk is a VHD that's attached to a virtual machine to store application data, or other data you need to keep.

Performance tiers



- Standard Storage is backed by HDDs, and delivers cost-effective storage while still being performant.
- Ideal for Dev/Test, non-critical, Infrequent access
- Max throughput and IOPS per disk is 60MB/s and 500 respectively

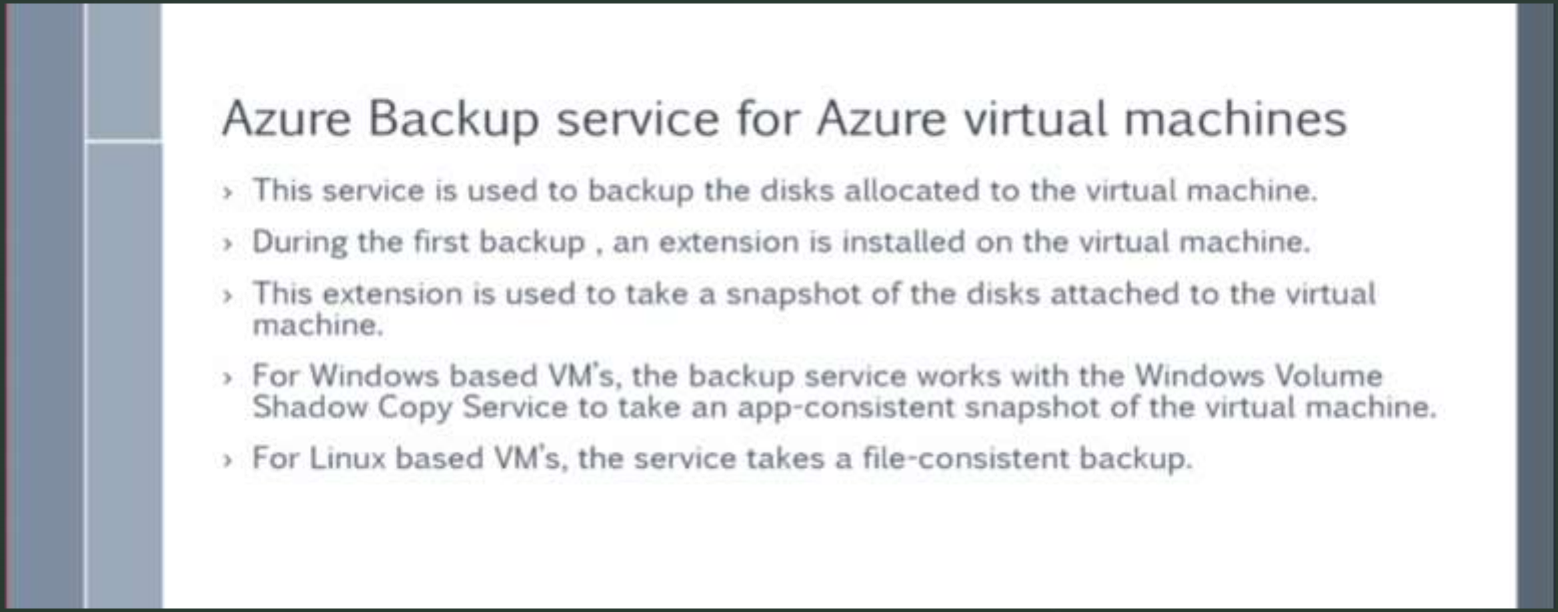
Premium storage

- Premium Storage is backed by SSDs, and delivers high-performance, low-latency disk support for VMs running I/O-intensive workloads
- Production and performance sensitive workloads
- Max throughput and IOPS per disk is 250MB/s and 7500 respectively

Disk Type

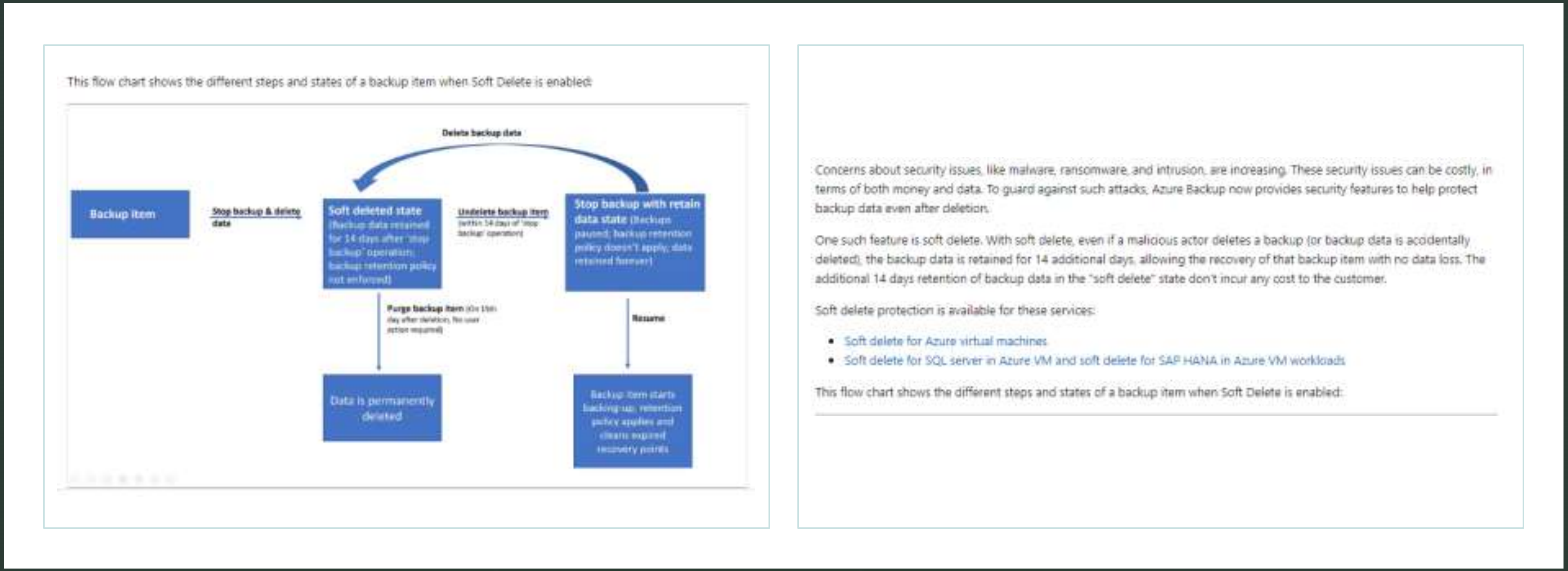
- Unmanaged disks • It is the traditional types of disks that have been used by VMs • You create your own storage account (SA) and specify SA when you create the disk • You need to make sure that scalability targets of SA (20,000 IOPS) are not exceeded •
- Managed disks • Managed Disks handles the storage account creation/management • You do not have to worry about the scalability limits of the storage account • Microsoft recommends use of Azure Managed Disks for new VMs.

Azure backup services for VM



Azure Backup service for Azure virtual machines

- This service is used to backup the disks allocated to the virtual machine.
- During the first backup , an extension is installed on the virtual machine.
- This extension is used to take a snapshot of the disks attached to the virtual machine.
- For Windows based VM's, the backup service works with the Windows Volume Shadow Copy Service to take an app-consistent snapshot of the virtual machine.
- For Linux based VM's, the service takes a file-consistent backup.



This flow chart shows the different steps and states of a backup item when Soft Delete is enabled:

Delete backup data
Backup item
Stop backup & delete data
Soft deleted state (Backup data retained for 14 days after "stop backup" operation; backup retention policy not enforced)
Undelete backup item (within 14 days of "stop backup" operation)
Stop backup with retain data state (Backups paused; backup retention policy doesn't apply; data retained forever)
Purge backup item (On 15th day after deletion, No user action required)
Resume
Data is permanently deleted
Backup item starts backing-up; retention policy applies and cleans expired recovery points

Concerns about security issues, like malware, ransomware, and intrusion, are increasing. These security issues can be costly, in terms of both money and data. To guard against such attacks, Azure Backup now provides security features to help protect backup data even after deletion.

One such feature is soft delete. With soft delete, even if a malicious actor deletes a backup (or backup data is accidentally deleted), the backup data is retained for 14 additional days, allowing the recovery of that backup item with no data loss. The additional 14 days retention of backup data in the "soft delete" state don't incur any cost to the customer.

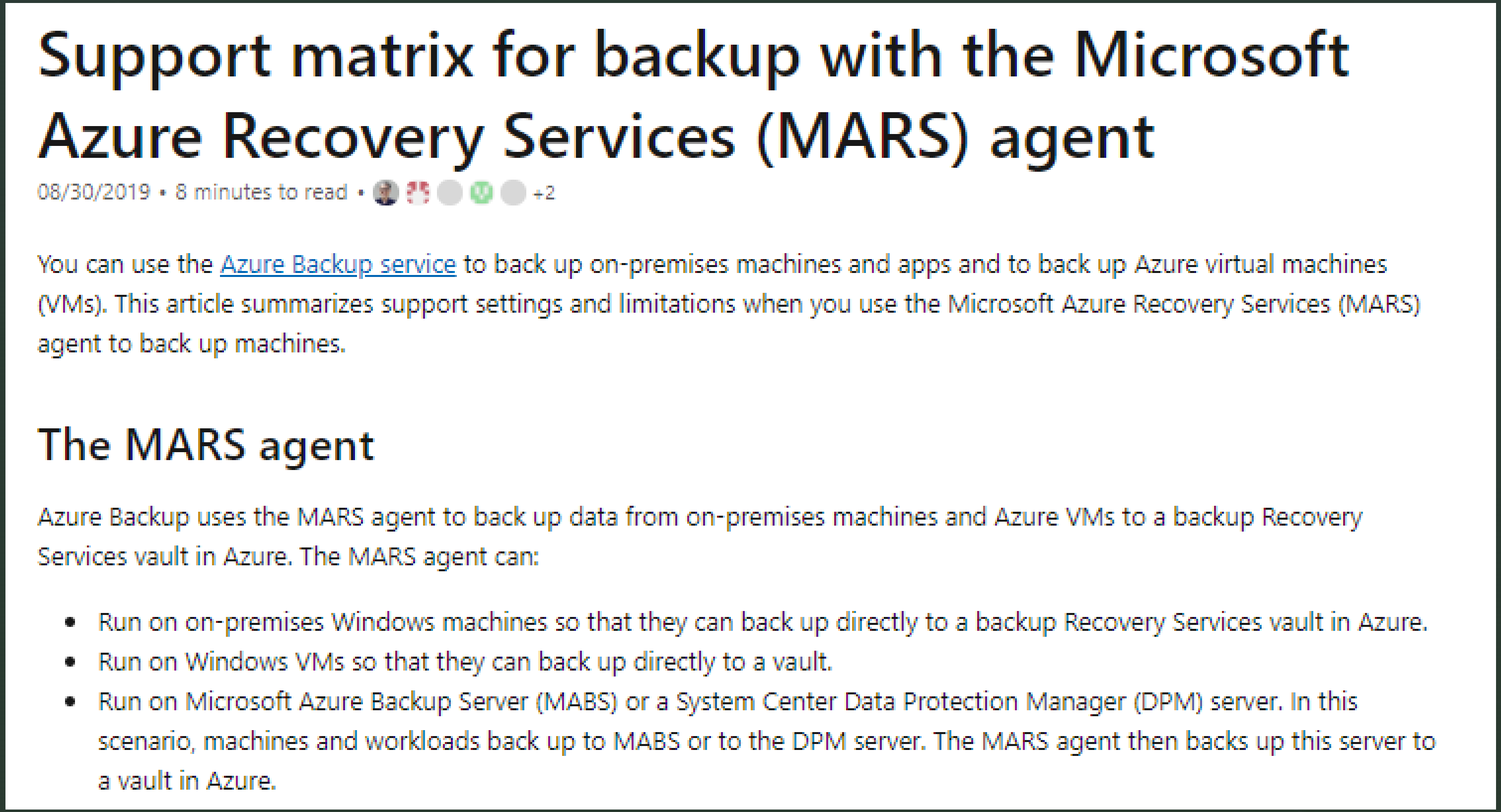
Soft delete protection is available for these services:

- Soft delete for Azure virtual machines
- Soft delete for SQL server in Azure VM and soft delete for SAP HANA in Azure VM workloads

This flow chart shows the different steps and states of a backup item when Soft Delete is enabled:

Soft delete Azure VM

MARS AGENT



Support matrix for backup with the Microsoft Azure Recovery Services (MARS) agent

08/30/2019 • 8 minutes to read • +2

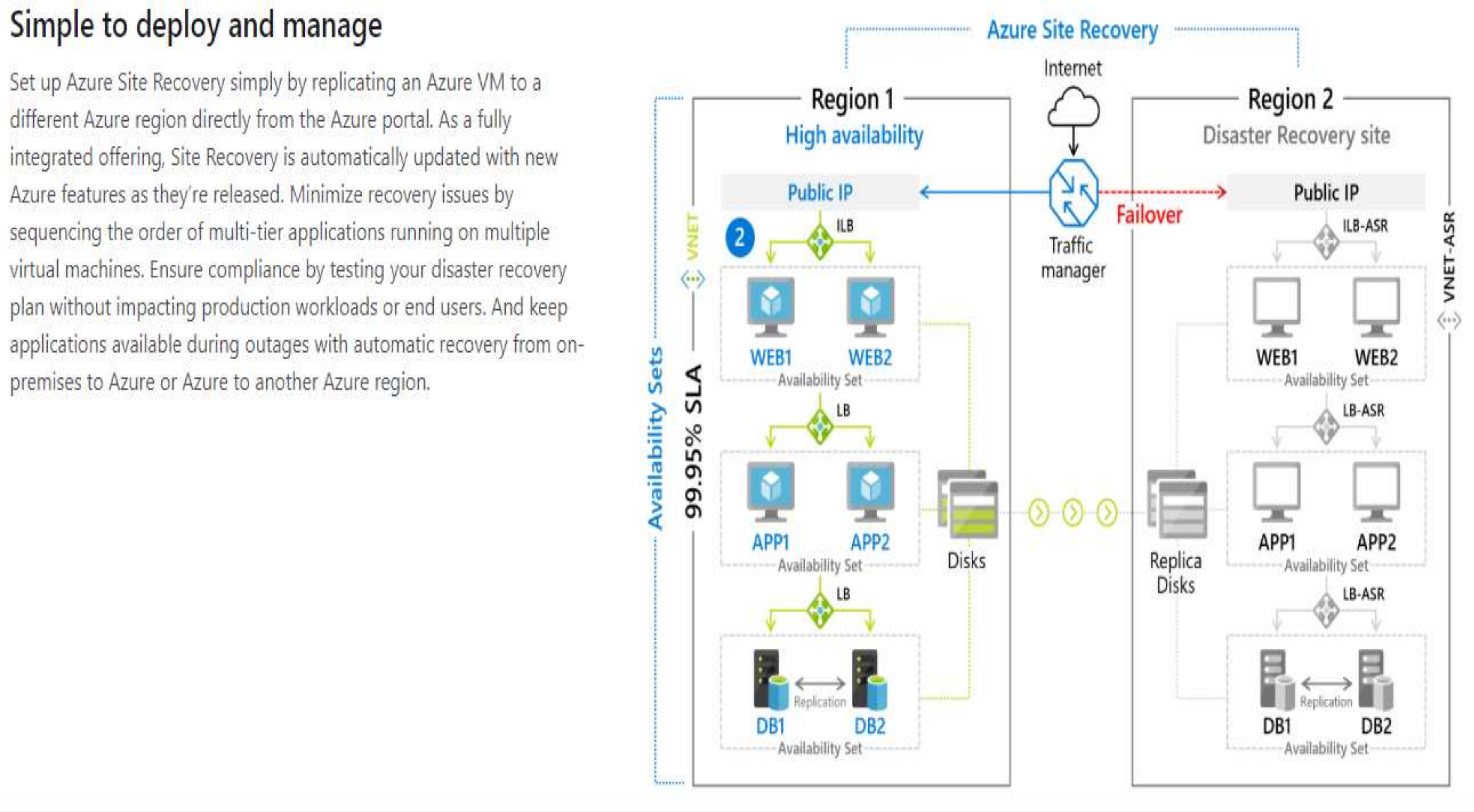
You can use the Azure Backup service to back up on-premises machines and apps and to back up Azure virtual machines (VMs). This article summarizes support settings and limitations when you use the Microsoft Azure Recovery Services (MARS) agent to back up machines.

The MARS agent

Azure Backup uses the MARS agent to back up data from on-premises machines and Azure VMs to a backup Recovery Services vault in Azure. The MARS agent can:

- Run on on-premises Windows machines so that they can back up directly to a backup Recovery Services vault in Azure.
- Run on Windows VMs so that they can back up directly to a vault.
- Run on Microsoft Azure Backup Server (MABS) or a System Center Data Protection Manager (DPM) server. In this scenario, machines and workloads back up to MABS or to the DPM server. The MARS agent then backs up this server to a vault in Azure.

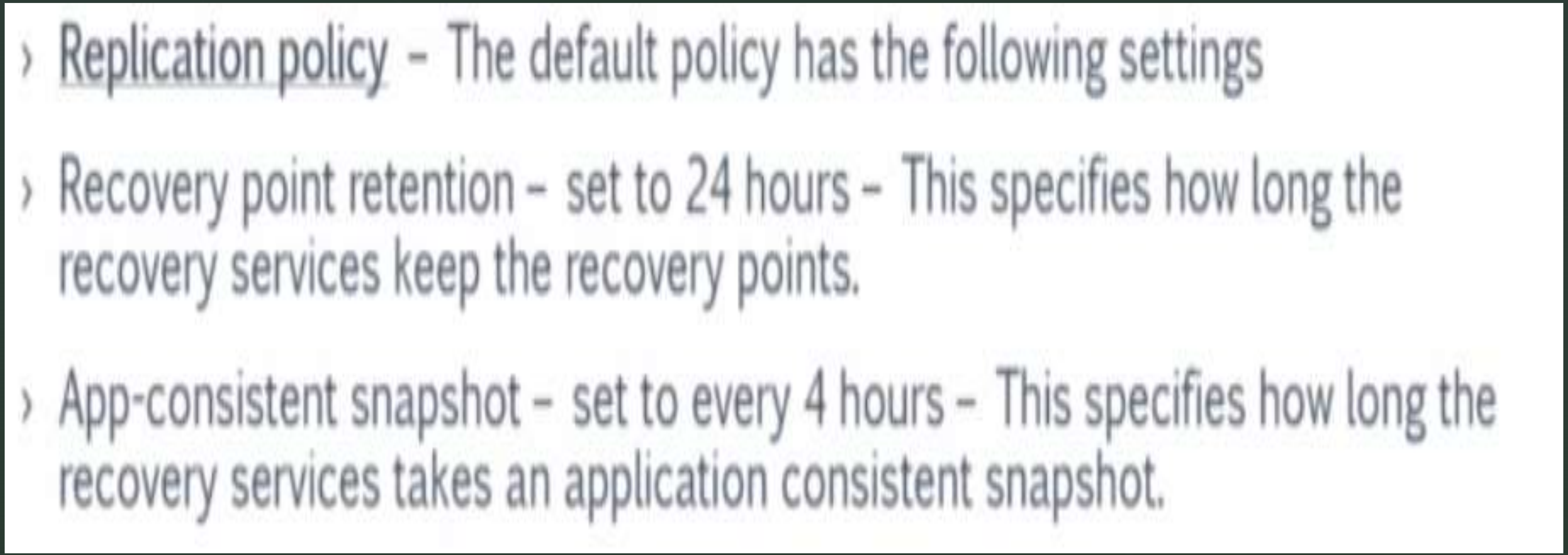
Azure site recovery



Simple to deploy and manage

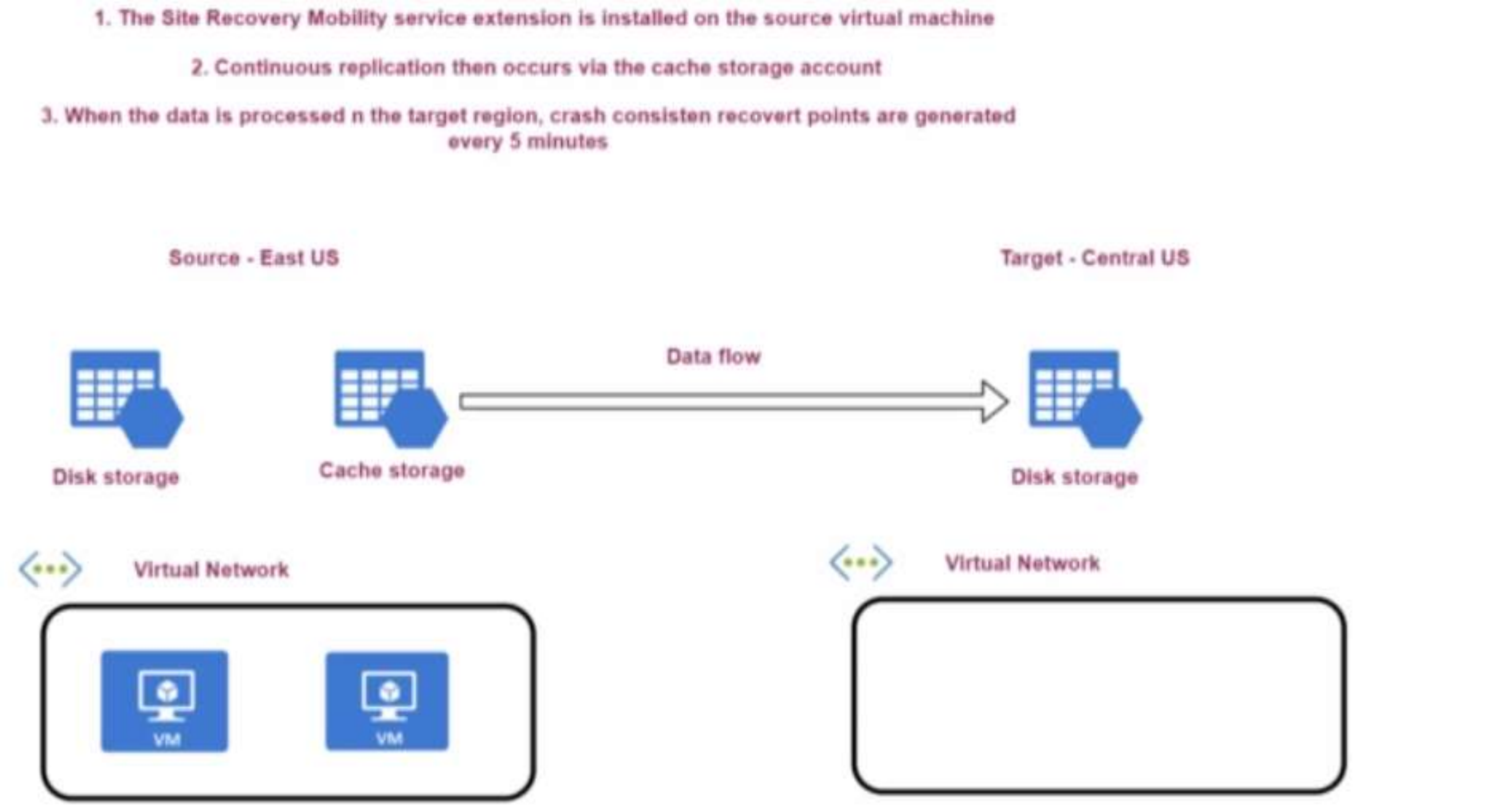
Set up Azure Site Recovery simply by replicating an Azure VM to a different Azure region directly from the Azure portal. As a fully integrated offering, Site Recovery is automatically updated with new Azure features as they're released. Minimize recovery issues by sequencing the order of multi-tier applications running on multiple virtual machines. Ensure compliance by testing your disaster recovery plan without impacting production workloads or end users. And keep applications available during outages with automatic recovery from on-premises to Azure or Azure to another Azure region.

Azure site recovery



- Replication policy – The default policy has the following settings
- Recovery point retention – set to 24 hours – This specifies how long the recovery services keep the recovery points.
- App-consistent snapshot – set to every 4 hours – This specifies how long the recovery services takes an application consistent snapshot.

Azure Site recovery

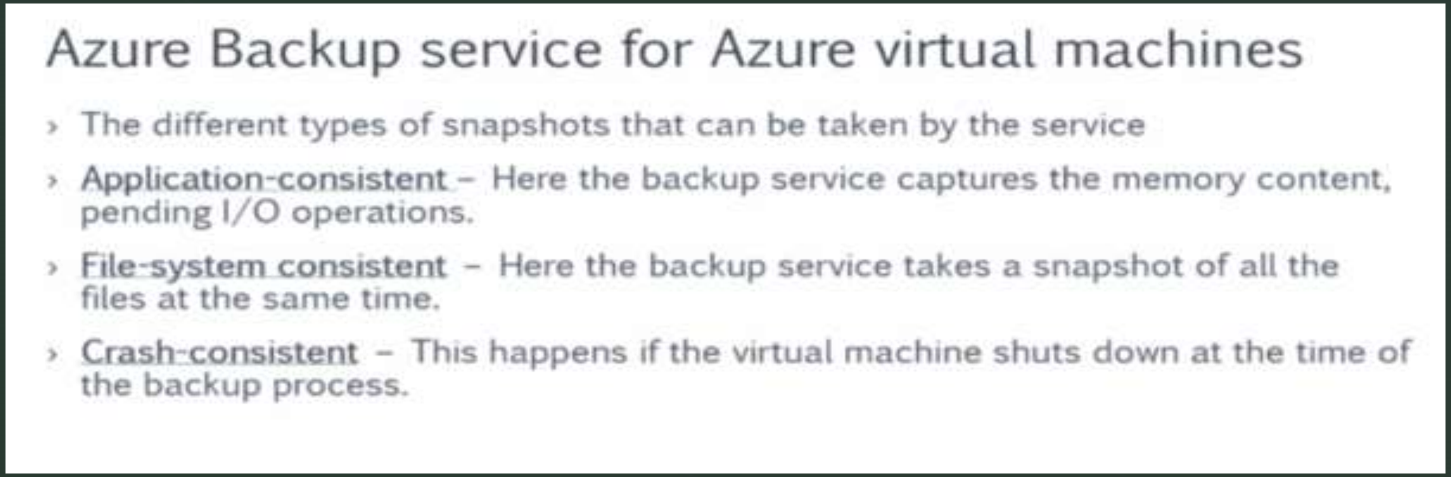


1. The Site Recovery Mobility service extension is installed on the source virtual machine

2. Continuous replication then occurs via the cache storage account

3. When the data is processed n the target region, crash consisten recovert points are generated every 5 minutes

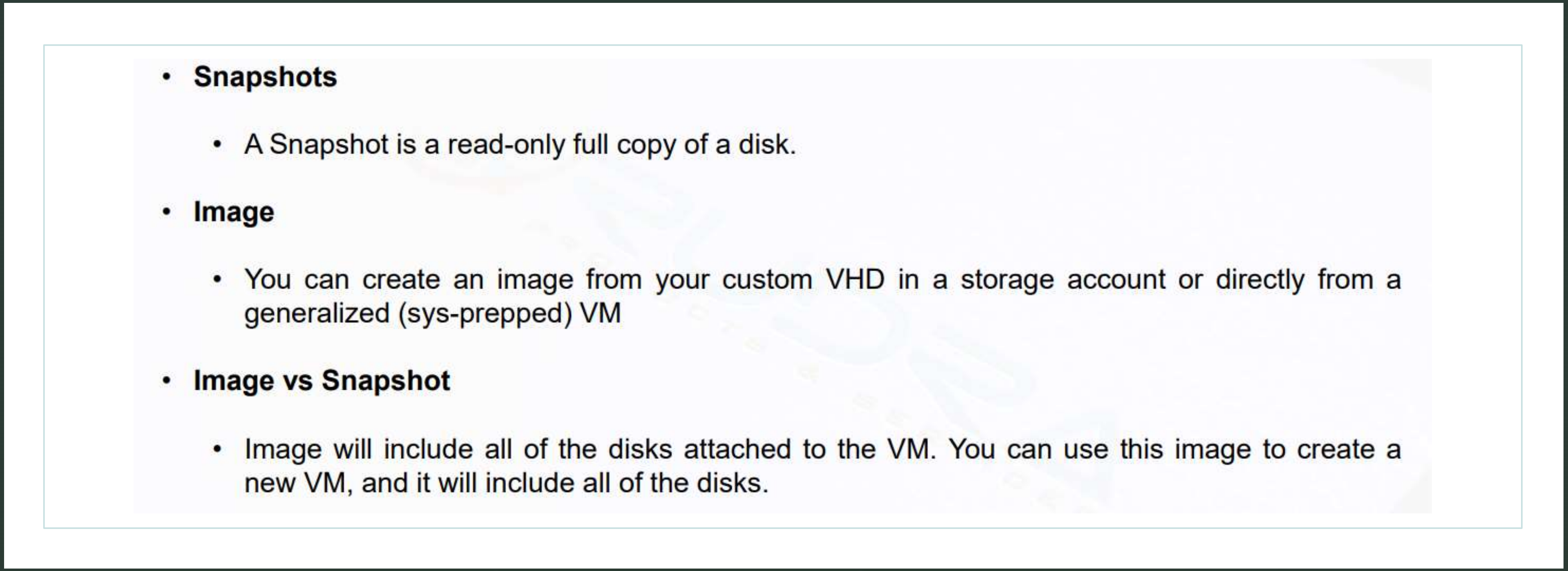
Azure backup services for VM



Azure Backup service for Azure virtual machines

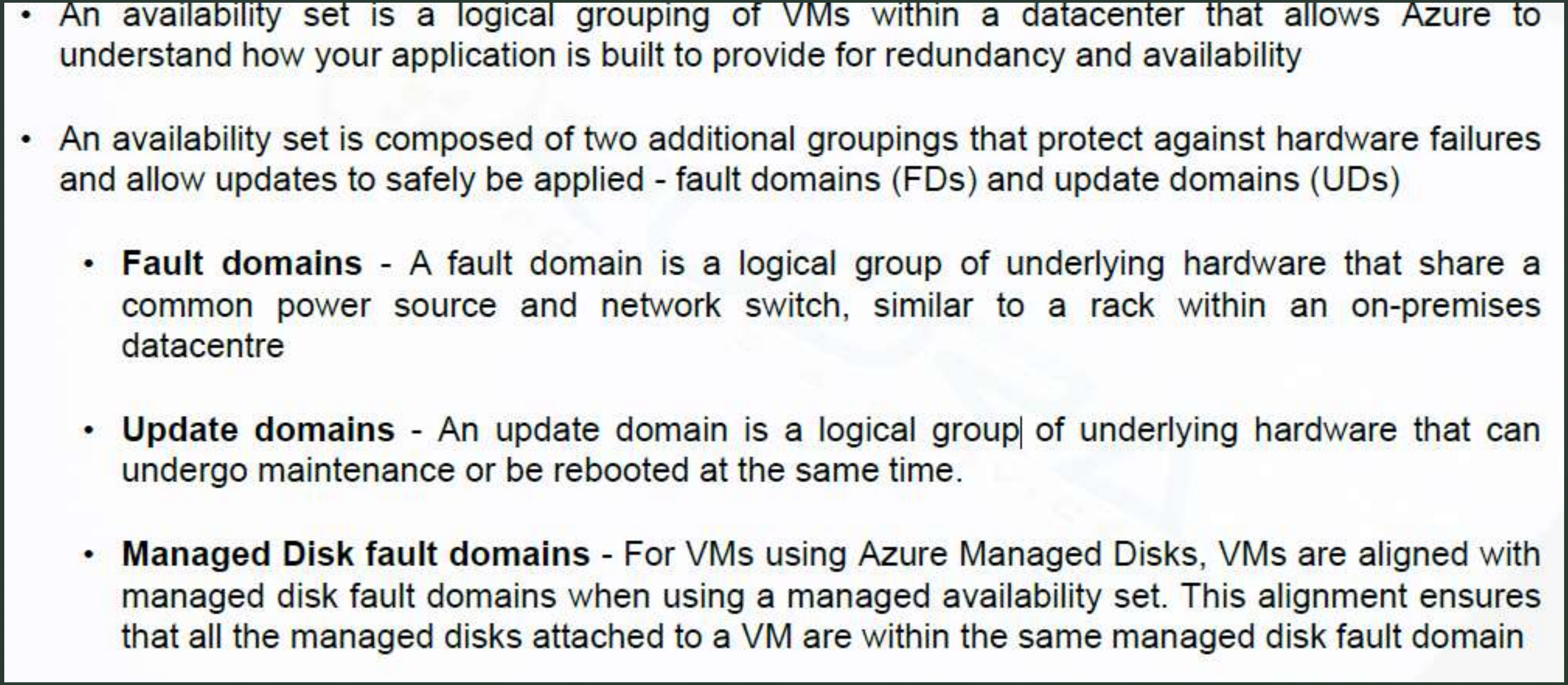
- The different types of snapshots that can be taken by the service
- Application-consistent – Here the backup service captures the memory content, pending I/O operations.
- File-system consistent – Here the backup service takes a snapshot of all the files at the same time.
- Crash-consistent – This happens if the virtual machine shuts down at the time of the backup process.

Snapshots & Images



- **Snapshots**
  - A Snapshot is a read-only full copy of a disk.
- **Image**
  - You can create an image from your custom VHD in a storage account or directly from a generalized (sys-prepped) VM
- **Image vs Snapshot**
  - Image will include all of the disks attached to the VM. You can use this image to create a new VM, and it will include all of the disks.

Availability sets



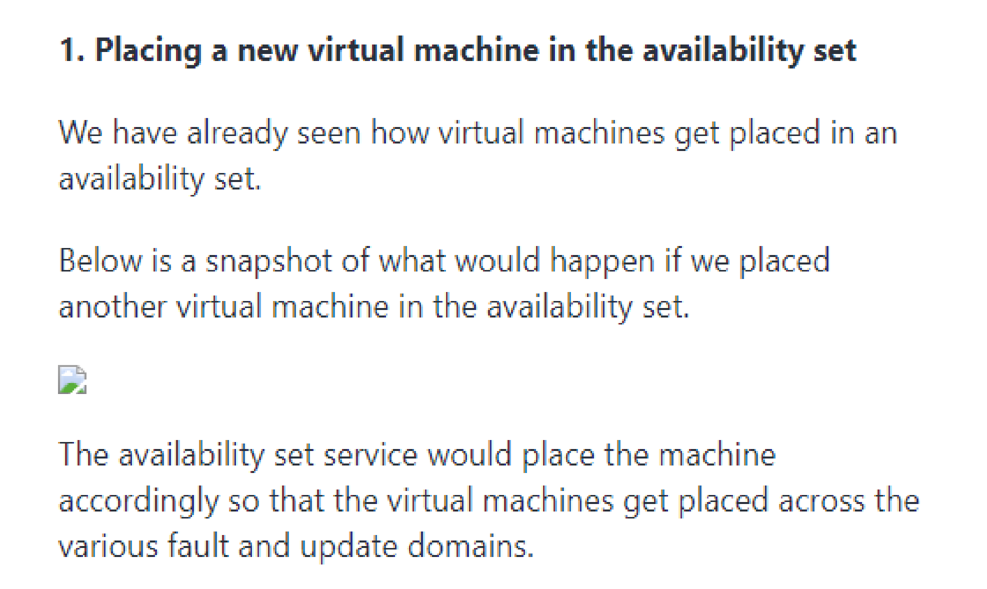
- An availability set is a logical grouping of VMs within a datacenter that allows Azure to understand how your application is built to provide for redundancy and availability

- An availability set is composed of two additional groupings that protect against hardware failures and allow updates to safely be applied - fault domains (FDs) and update domains (UDs)

  - **Fault domains** - A fault domain is a logical group of underlying hardware that share a common power source and network switch, similar to a rack within an on-premises datacentre

  - **Update domains** - An update domain is a logical group of underlying hardware that can undergo maintenance or be rebooted at the same time.

  - **Managed Disk fault domains** - For VMs using Azure Managed Disks, VMs are aligned with managed disk fault domains when using a managed availability set. This alignment ensures that all the managed disks attached to a VM are within the same managed disk fault domain

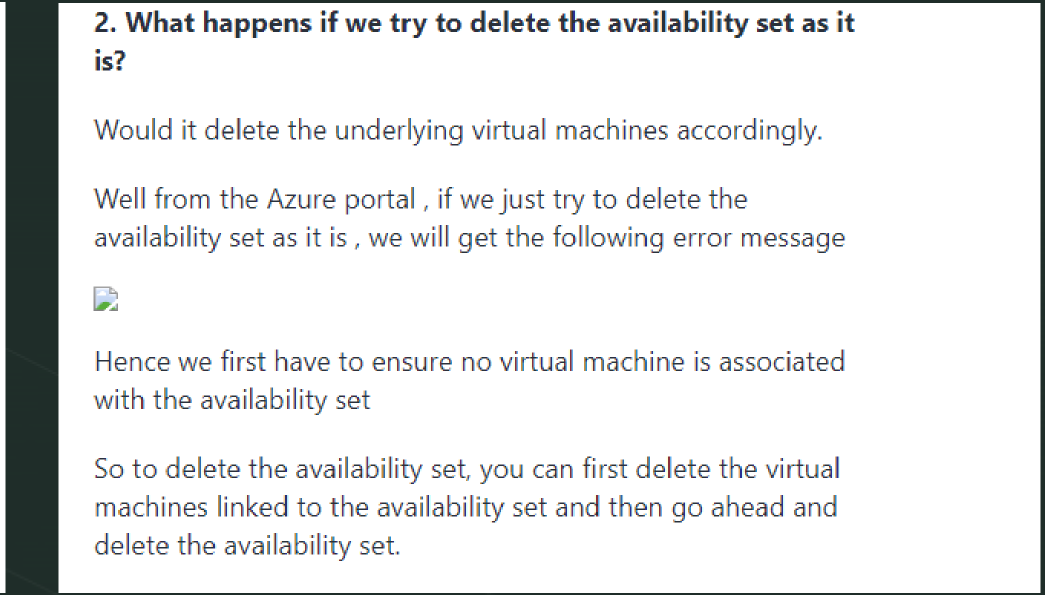


1. Placing a new virtual machine in the availability set

We have already seen how virtual machines get placed in an availability set.

Below is a snapshot of what would happen if we placed another virtual machine in the availability set.

The availability set service would place the machine accordingly so that the virtual machines get placed across the various fault and update domains.



2. What happens if we try to delete the availability set as it is?

Would it delete the underlying virtual machines accordingly.

Well from the Azure portal , if we just try to delete the availability set as it is , we will get the following error message

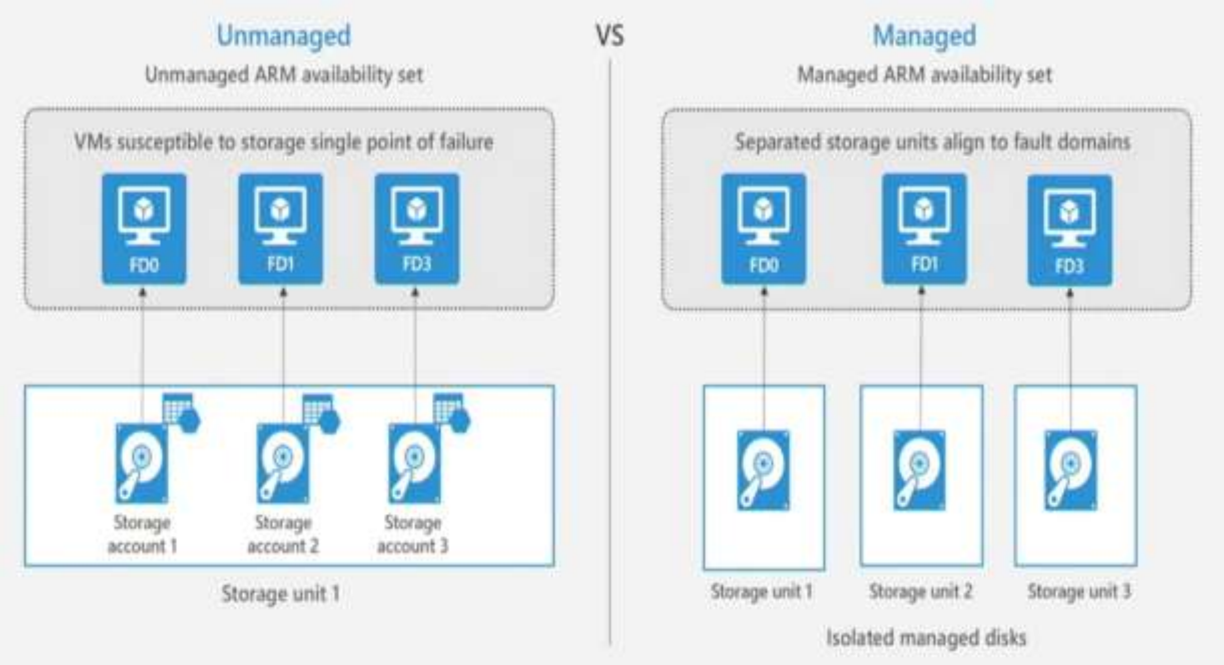
Hence we first have to ensure no virtual machine is associated with the availability set

So to delete the availability set, you can first delete the virtual machines linked to the availability set and then go ahead and delete the availability set.

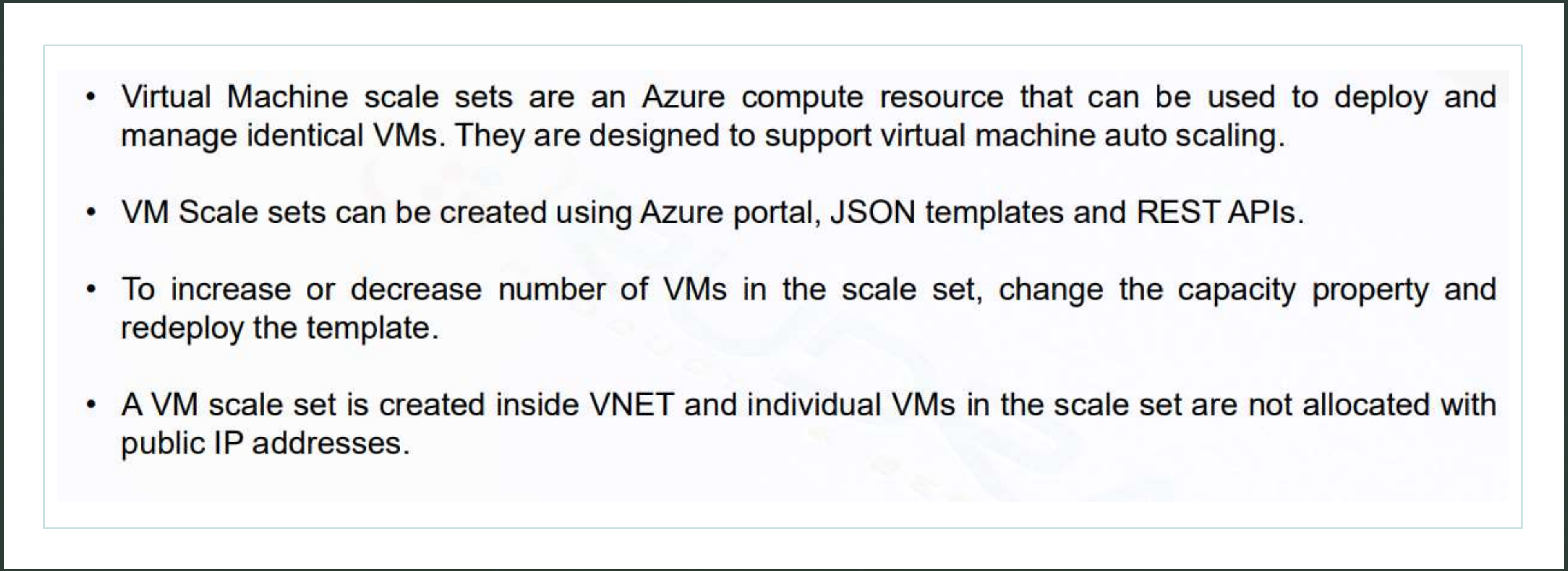
Storage availability

- •Azure Managed Disks
- •Locally redundant storage(LRS)
- •Storage account-based disks
- •Locally redundant storage(LRS)
- •Zone redundant storage(ZRS)
- •Geo-redundant storage(GRS)
- •Read-access geo-redundant storage(RA-GRS)

Managed Vs Unmanaged Disk

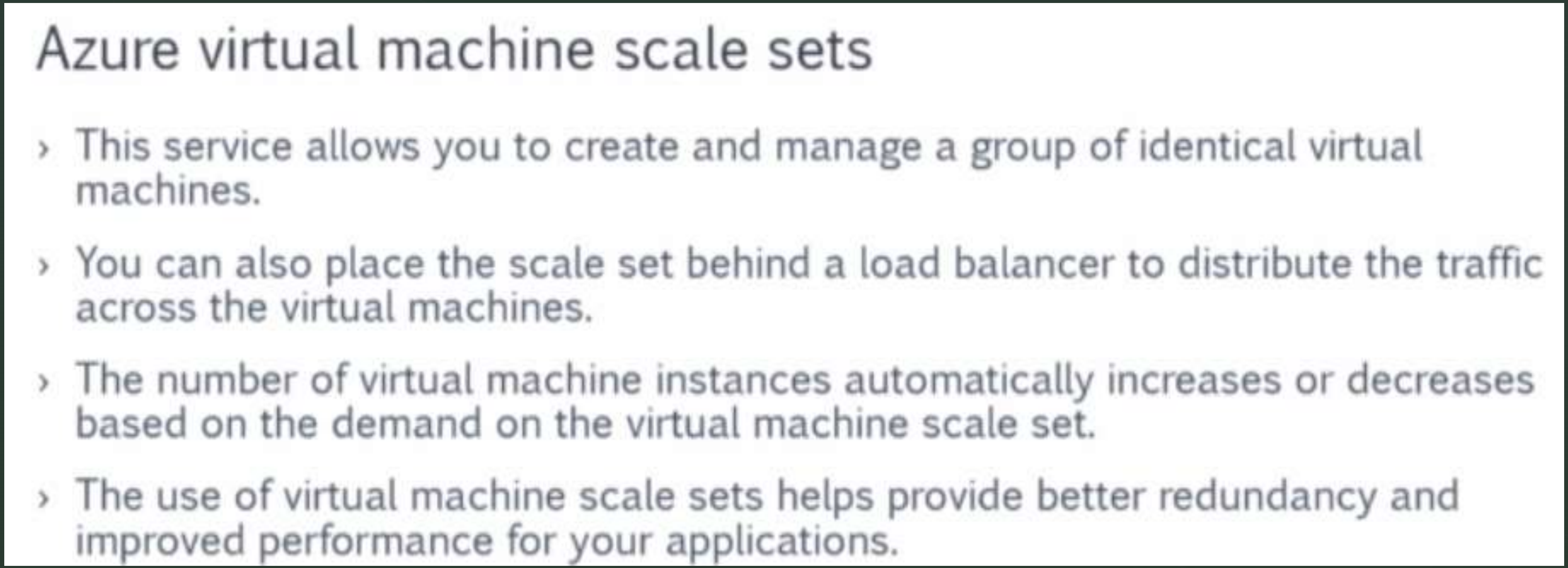


Virtual Machine scale sets



- Virtual Machine scale sets are an Azure compute resource that can be used to deploy and manage identical VMs. They are designed to support virtual machine auto scaling.
- VM Scale sets can be created using Azure portal, JSON templates and REST APIs.
- To increase or decrease number of VMs in the scale set, change the capacity property and redeploy the template.
- A VM scale set is created inside VNET and individual VMs in the scale set are not allocated with public IP addresses.

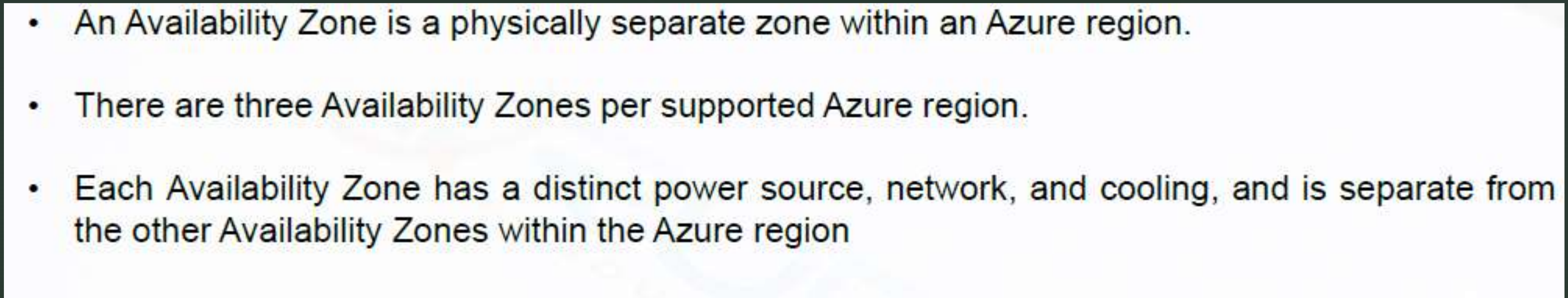
Azure virtual machine scale set



Azure virtual machine scale sets

- This service allows you to create and manage a group of identical virtual machines.
- You can also place the scale set behind a load balancer to distribute the traffic across the virtual machines.
- The number of virtual machine instances automatically increases or decreases based on the demand on the virtual machine scale set.
- The use of virtual machine scale sets helps provide better redundancy and improved performance for your applications.

Availability zones



- An Availability Zone is a physically separate zone within an Azure region.
- There are three Availability Zones per supported Azure region.
- Each Availability Zone has a distinct power source, network, and cooling, and is separate from the other Availability Zones within the Azure region

Availability zones

Review on Availability Zones

This features help provides better availability for your application by protecting them from datacenter failures.

Each Availability zone is a unique physical location in an Azure region.

Each zone comprises of one or more data centers that has independent power, cooling, and networking

Hence the physical separation of the Availability Zones helps protect applications against data center failures

Using Availability Zones, you can be guaranteed an availability of 99.99% for your virtual machines. You need to ensure that you have 2 or more virtual machines running across multiple availability zones.

Creating custom image

- In production env if you want to create template image
- Important note we cannot use same image once use an template you can use only for new vm creation
-

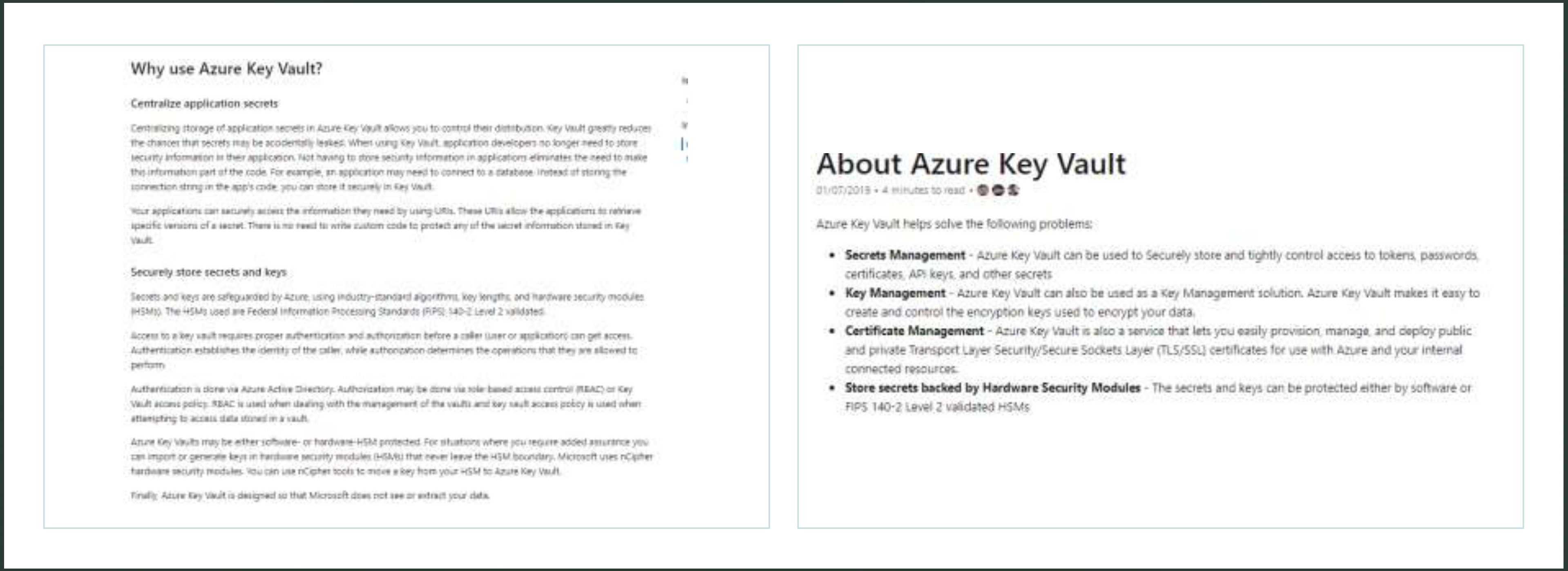
Resource limit

- 1) First go to your subscriptions
- 2) Then go to your subscription
- 3) For the subscription , go to Usage + quotas
- 4) In the right pane, then go to the "Select a provider" and choose Microsoft.Compute
- You will then see the quotas
- So here , we have the Total Regional vCPUs quota for the West US region. I had gone ahead and create a virtual machine with 2 vCPU in the West US region, and that is why it shows that i have consumed 2 vCPUs out of 10 vCPUs in my quota.
- Hence in the West US region, i can only spin up virtual machines that would together only have a maximum of 10 vCPUs.
- If you want an increase in the quota limit, you can request an increase from Azure support
- For more information on service limits , one can visit the URL - https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits

Proximity group

- Proximity placement groups
- You can place multiple virtual machines in a proximity group. This ensures that the virtual machines are located as close together as possible on the underlying physical infrastructure. This would ensure low latency between the virtual machines.
- Let's say that you need to deploy virtual machines as part of an availability set or a scale set. And lets say that there is a lot of communication required between these virtual machines. It's ideal to have them physically located as close together as possible to ensure the latency to the communication is as less as possible.
- To use Proximity groups, you first have to create a new proximity placement group resource in a particular region
- Then when you create a virtual machine in the same region, in the Advanced Tab, you can place the virtual machine in that proximity group
- For more information - https://docs.microsoft.com/en-us/azure/virtual-machines/linux/co-location?ocid=AID754288&wt.mc_id=azfr-c9-dbrown&wt.mc_id=CFID0493

Azure Encryption Method



Why use Azure Key Vault?

Centralize application secrets

Centralizing storage of application secrets in Azure Key Vault allows you to control their distribution. Key Vault greatly reduces the chances that secrets may be accidentally leaked. When using Key Vault, application developers no longer need to store security information in their application. Not having to store security information in applications eliminates the need to make this information part of the code. For example, an application may need to connect to a database. Instead of storing the connection string in the app's code, you can store it securely in Key Vault.

Your applications can securely access the information they need by using URIs. These URIs allow the applications to retrieve specific versions of a secret. There is no need to write custom code to protect any of the secret information stored in Key Vault.

Securely store secrets and keys

Secrets and keys are safeguarded by Azure, using industry-standard algorithms, key lengths, and hardware security modules (HSMs). The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated.

Access to a key vault requires proper authentication and authorization before a caller (user or application) can get access. Authentication establishes the identity of the caller, while authorization determines the operations that they are allowed to perform.

Authentication is done via Azure Active Directory. Authorization may be done via role-based access control (RBAC) or Key Vault access policy. RBAC is used when dealing with the management of the vaults and key vault access policy is used when attempting to access data stored in a vault.

Azure Key Vaults may be either software- or hardware-HSM protected. For situations where you require added assurance you can import or generate keys in hardware security modules (HSMs) that never leave the HSM boundary. Microsoft uses nCipher hardware security modules. You can use nCipher tools to move a key from your HSM to Azure Key Vault.

Finally, Azure Key Vault is designed so that Microsoft does not see or extract your data.

About Azure Key Vault

01/07/2019 • 4 minutes to read •

Azure Key Vault helps solve the following problems:

- **Secrets Management** - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- **Key Management** - Azure Key Vault can also be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.
- **Certificate Management** - Azure Key Vault is also a service that lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.
- **Store secrets backed by Hardware Security Modules** - The secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs

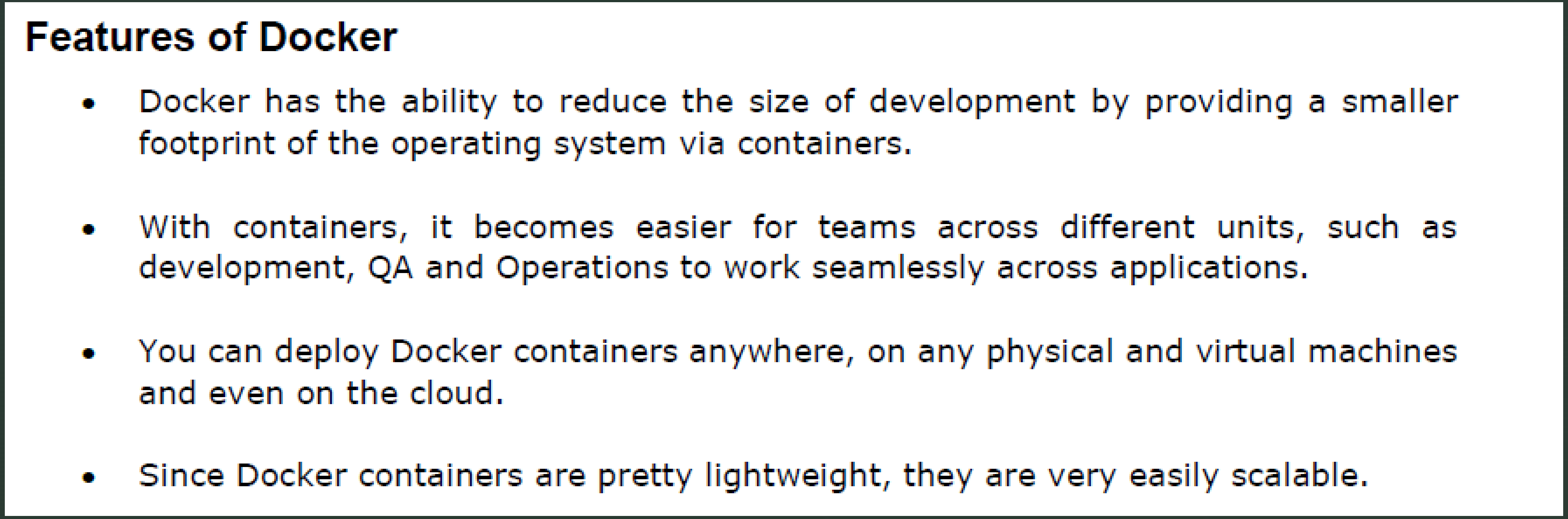
App Service plans

- https://azure.microsoft.com/en-us/pricing/details/app-service/plans/

DEMO

- Azure Service plan
- Azure Docker deployment on VM centos VM

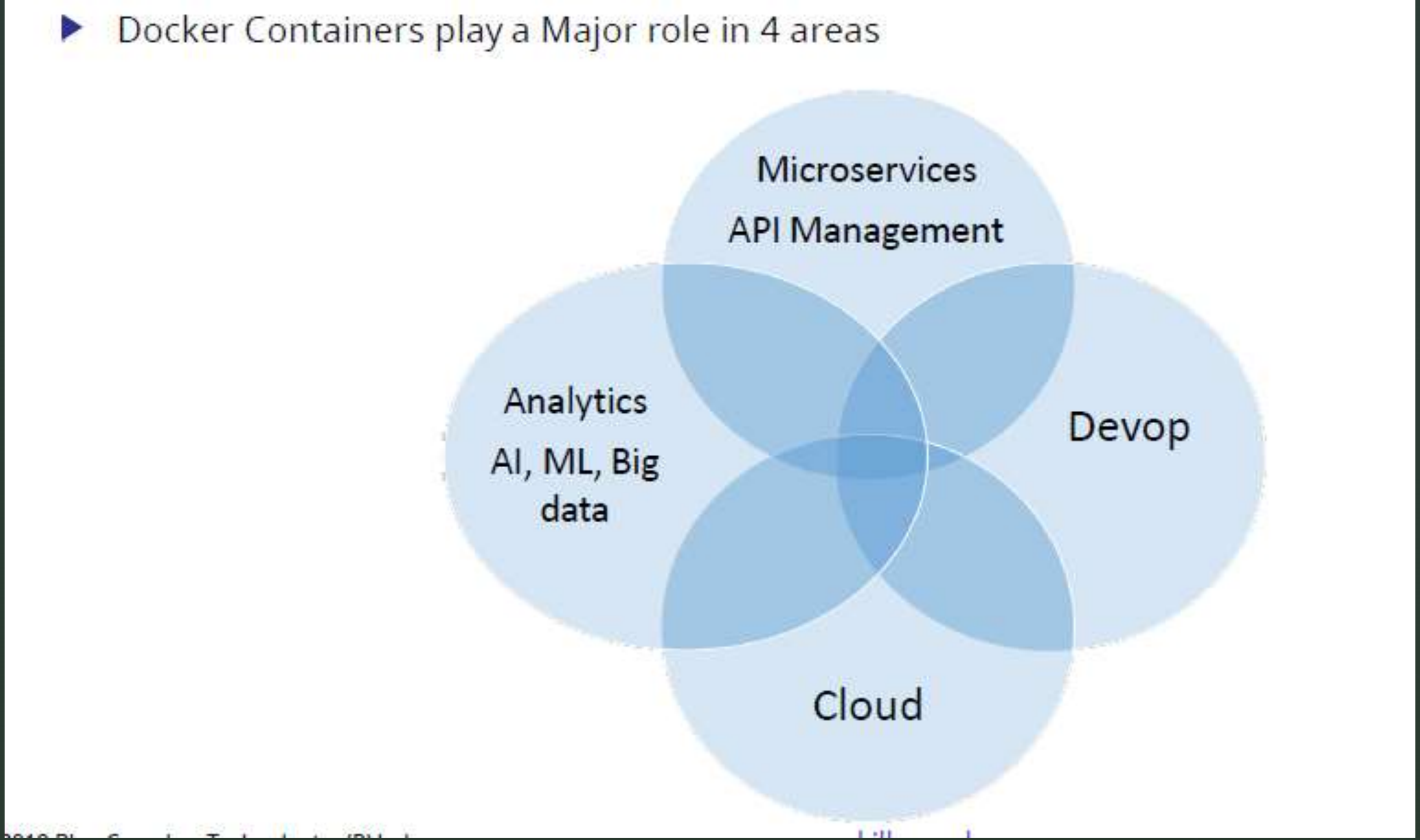
What is Container



Features of Docker

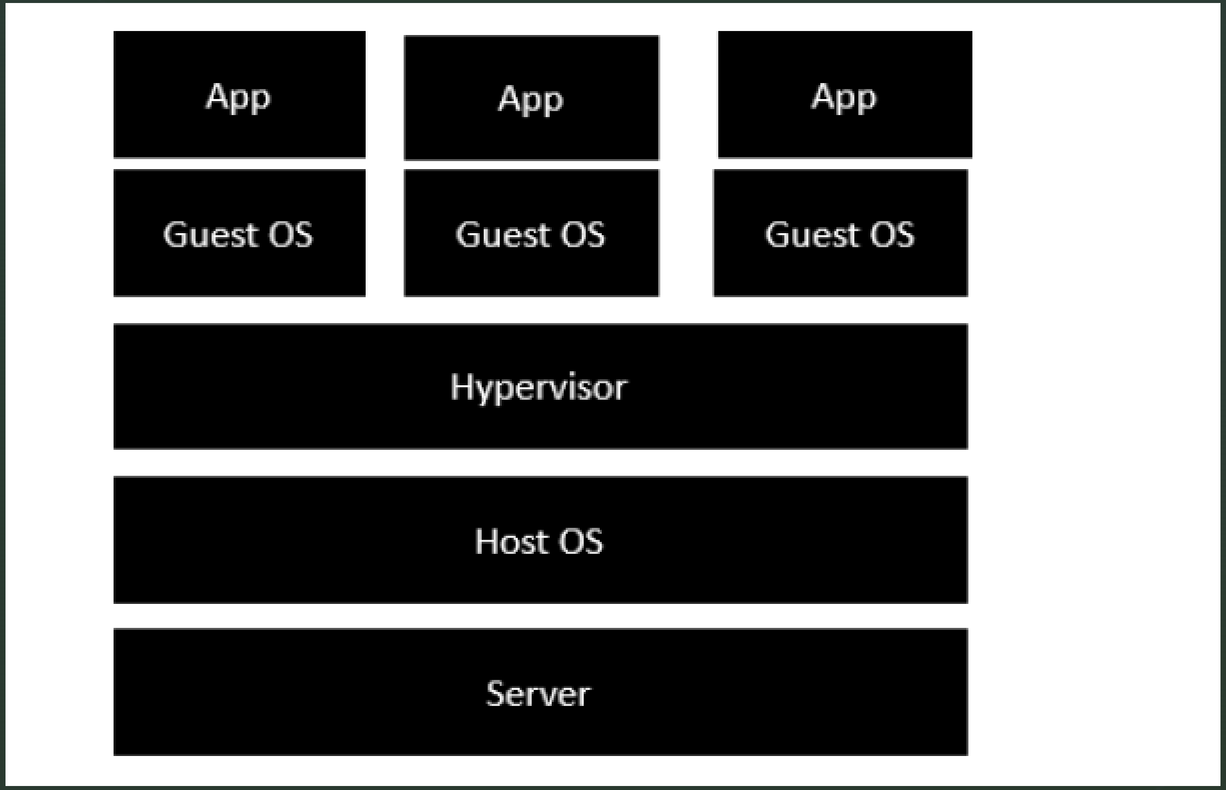
- Docker has the ability to reduce the size of development by providing a smaller footprint of the operating system via containers.
- With containers, it becomes easier for teams across different units, such as development, QA and Operations to work seamlessly across applications.
- You can deploy Docker containers anywhere, on any physical and virtual machines and even on the cloud.
- Since Docker containers are pretty lightweight, they are very easily scalable.

Docker

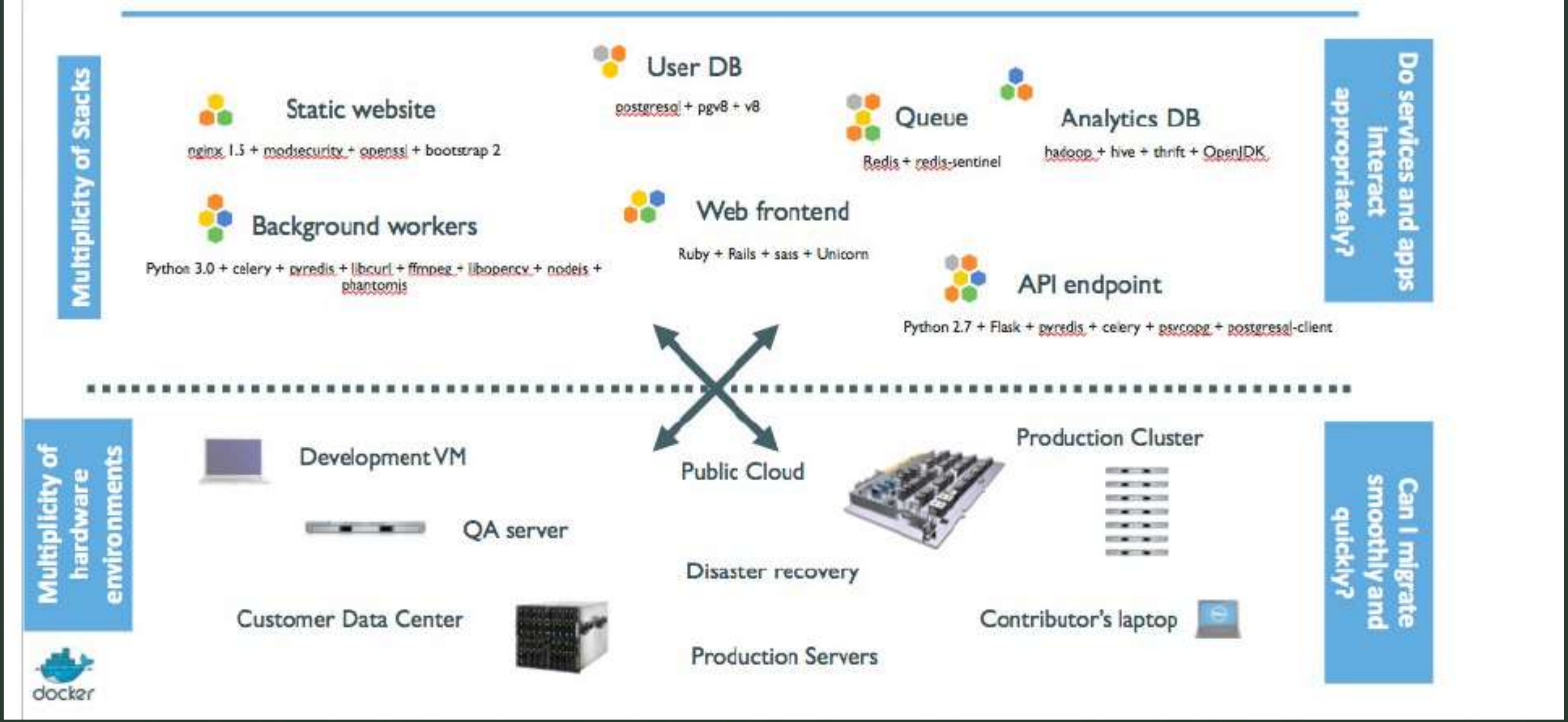


- Docker Containers play a Major role in 4 areas

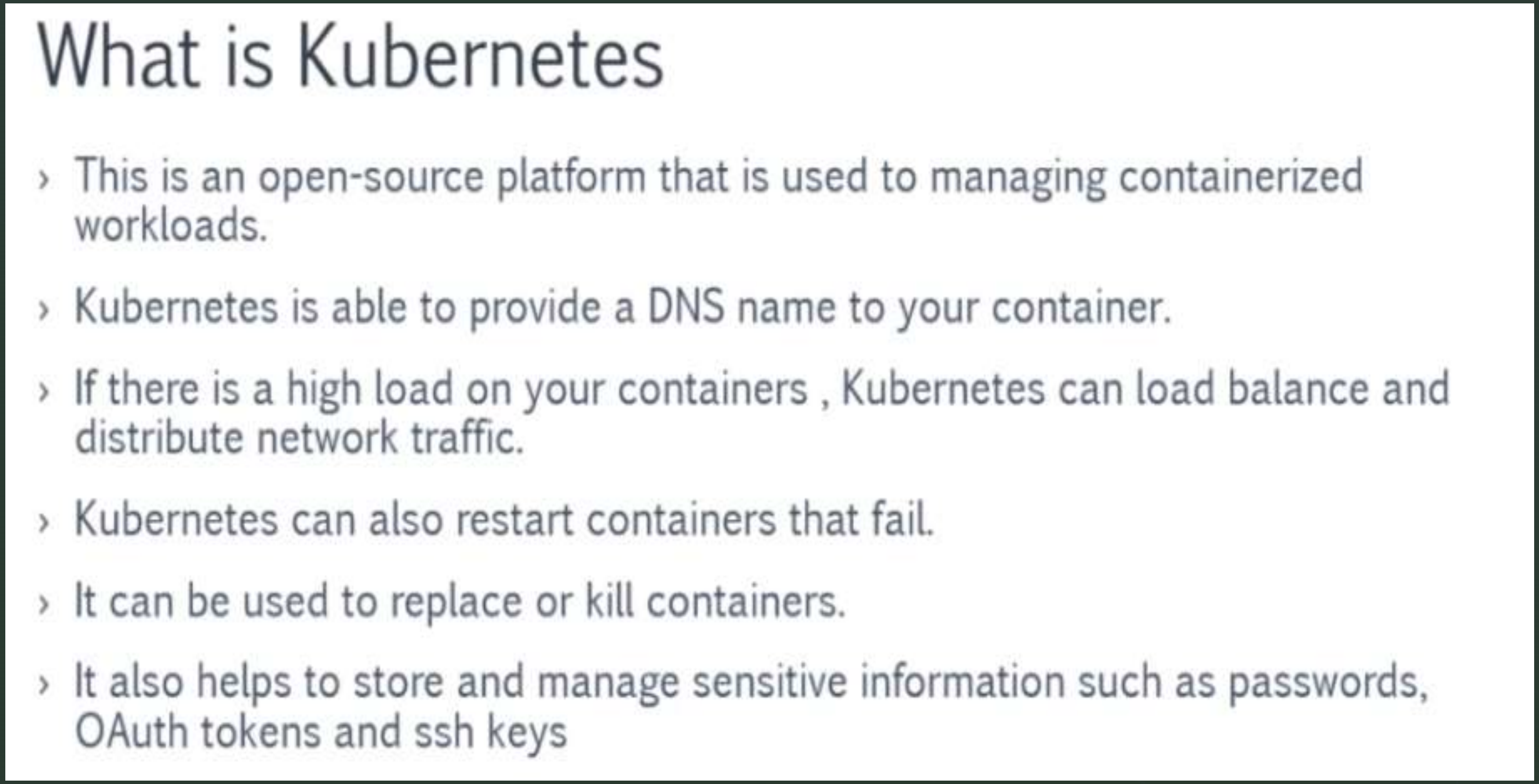
Docker – Docker Architecture



Docker


Multiplicity of Stacks
Static website
nginx 1.5 + modsecurity + openssl + bootstrap 2
User DB
postgresql + pgv8 + v8
Queue
Redis + redis-sentinel
Analytics DB
hadoop + hive + thrift + OpenJDK
Background workers
Python 3.0 + celery + pyredis + libcurl + ffmpeg + libopencv + nodejs + phantomjs
Web frontend
Ruby + Rails + sass + Unicorn
API endpoint
Python 2.7 + Flask + pyredis + celery + psycopg + postgresql-client
Do services and apps interact appropriately?
Multiplicity of hardware environments
Development VM
QA server
Public Cloud
Production Cluster
Disaster recovery
Customer Data Center
Contributor's laptop
Production Servers
Can I migrate smoothly and quickly?
docker

Kubernete



What is Kubernetes

- This is an open-source platform that is used to managing containerized workloads.
- Kubernetes is able to provide a DNS name to your container.
- If there is a high load on your containers , Kubernetes can load balance and distribute network traffic.
- Kubernetes can also restart containers that fail.
- It can be used to replace or kill containers.
- It also helps to store and manage sensitive information such as passwords, OAuth tokens and ssh keys

To be Continue