CLOUD COMPUTING | DIGITAL TALENT TRAINING KOMINFO

MIGRASI INFRASTRUKTUR KOMPUTASI AWAN

PUSILKOM UI

Pusat Ilmu Komputer Universitas Indonesia
15 Oktober 2018 – 5 Desember 2018

Quality Result by Bridging Theories and Best Practices

AGENDA | MIGRASI INFRASTRUKTUR

1. INTRODUCTION
2. TYPES OF SERVER MIGRATION
3. COMPUTE MIGRATION IN AZURE
4. STORE AND NETWORK MIGRATION IN AZURE

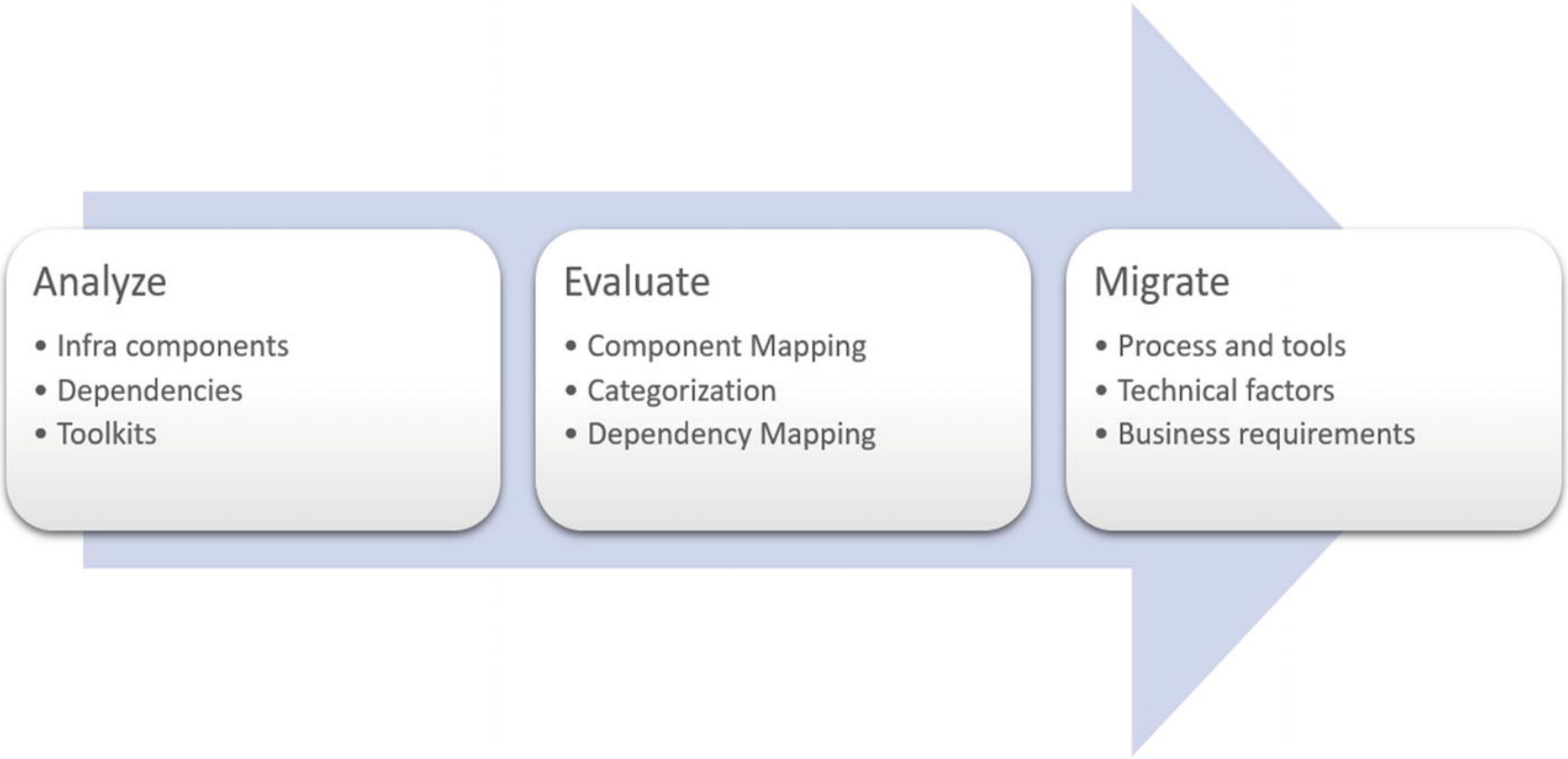
Some considerations when planning for infrastructure migration

Similarities and dissimilarities of design concept between on-premise environment with the one in the cloud provider

1. It is important to understand the existing infrastructure landscape and to identify equivalent component provided by cloud provider to ensure smooth migration
2. Including virtualization format for the VM being imported, e.g. VDI from Oracle, VMDK from VMware, VHD from Microsoft

Organizations typically prefer to use a hybrid cloud approach where part of the resources remain on-premise, and the architecture is designed to leverage resources in the cloud as well

Migration Workflow



Analyze

- A comprehensive document and an architecture diagram should be available to clearly understand the existing infrastructure layout.
- The interdependencies of the components should be etched out for clarity.
- For environments where this interrelationship is not documented—for example, legacy environments,
  - consider using options like the Microsoft Assessment and Planning (MAP) toolkit to generate a comprehensive report of existing environment.

Evaluate

- List of the infrastructure components (and their dependencies) that need to be migrated should be evaluated and mapped against the equivalent services in cloud provider
- Further subdivide the components into basic services;
  - For example, when migrating a server to Azure, you consume compute, storage, and network services
  - A mapping of the compute power to the available instance types in Azure should be done along with the mapping of storage.
- Decide the kind of storage to be used:
  - Between premium vs. standard storage and managed vs. unmanaged disks

Migrate

- After the assessment and evaluation phase, the primary decision involves the migration process and tools
- This depends on technical factors such as infrastructure type (i.e., virtualized or not, type of virtualization used, OS versions, and etc.)
- The business dependencies—such as consumption models, SLAs, acceptable downtimes, and so forth—should also be factored when selecting the migration method

TYPES OF SERVER MIGRATION

Types of Server Migration

- Physical to virtual
- Virtual to virtual
- Virtual to physical
- Storage data migration
- Online vs offline?

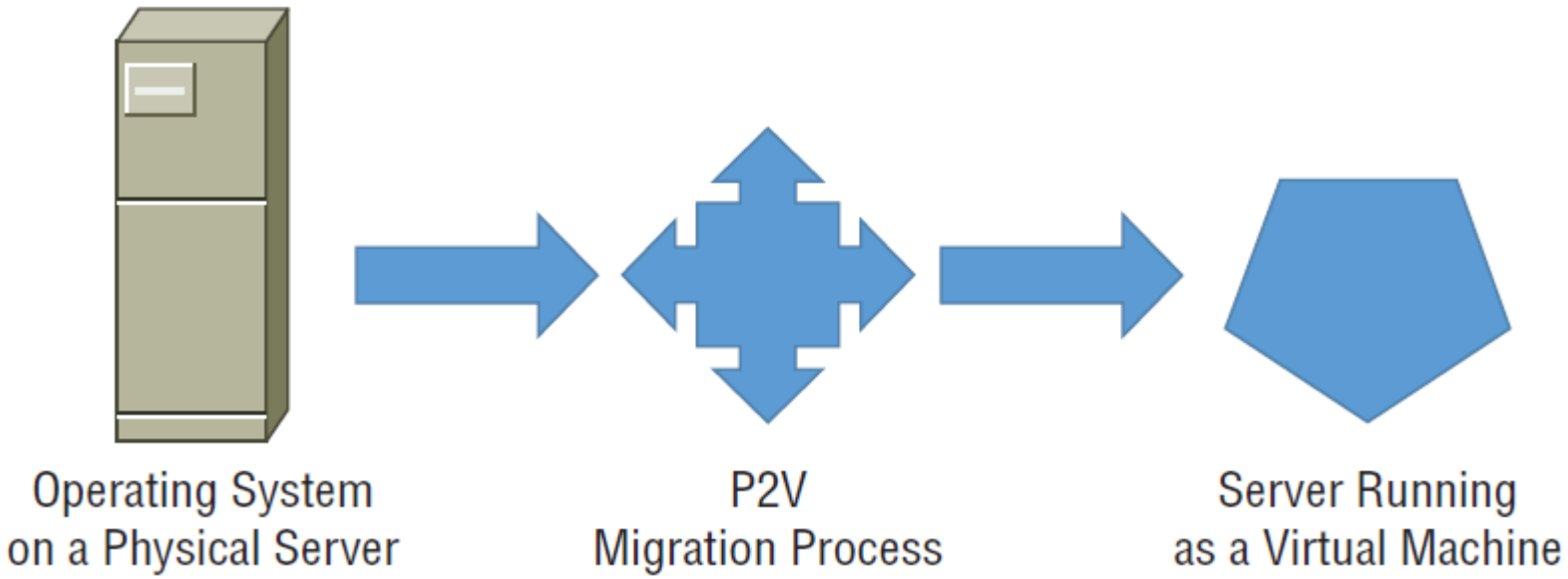
Physical to virtual (P2V)

- Taking a server that is running an operating system and applications and then migrating it to a VM running on top of a hypervisor
- May require reinstalling the operating system, application, and data files onto a new VM from scratch
- Software utilities are offered by some companies, e.g. VMware vCenter Converter and Microsoft's Virtual Machine Manager, that can perform the conversion
- Several 3rd party software companies and cloud providers offer fully automated P2V utilities

Physical server

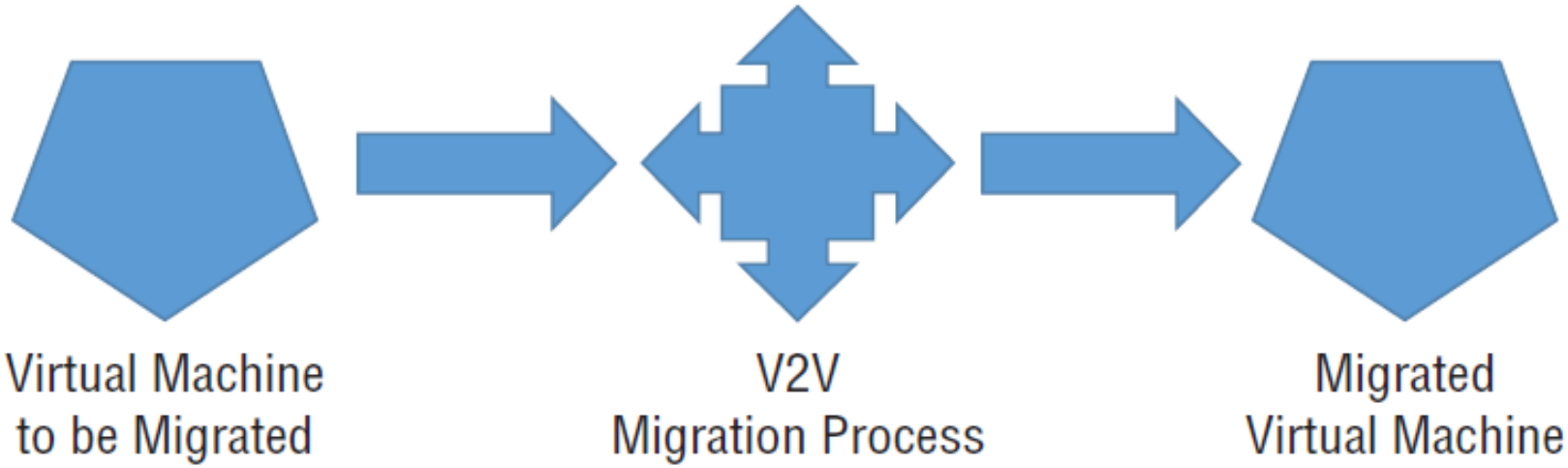
- Even though the majority of workloads nowadays use virtualization, some physical servers are still being used for special or specific use cases
  - For example, applications that need dedicated compute capacity without any processor sharing (GPUs ,etc)
  - Legacy applications may still run in original physical server due to ambiguity around design and dependencies
- The end goal is to convert the source machine to a compatible format in the cloud provider (e.g. Azure)
- Need to check equivalent components for special hardware requirements (e.g. GPU)
  - Azure N series virtual machines with NVIDIA GPUs can be an option when migrating to Microsoft Azure

Physical to virtual (P2V)



Virtual to virtual (V2V)

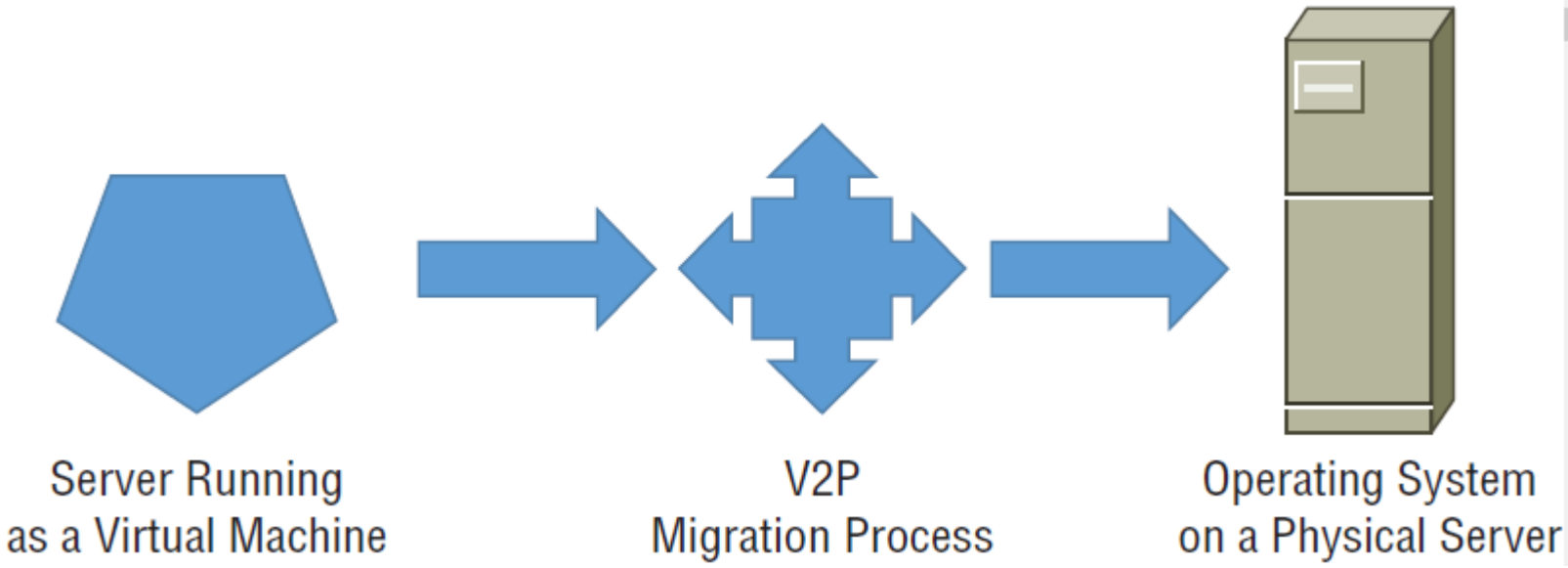
- It generally involves cloning the existing VM and installing that image at the cloud provider's hosting center



Virtual to physical (V2P)

- While not as common, there is an option of converting from a virtual server to a physical server known as virtual-to-physical (V2P)
- A use case would be if more processing power is needed and can be provided if the server is hosted on its own server hardware
- Have lots of details that must be sorted through based on the hardware
- May be that a fresh installation of the operating system and application will be required and virtualization software being used

Virtual to physical (V2P)



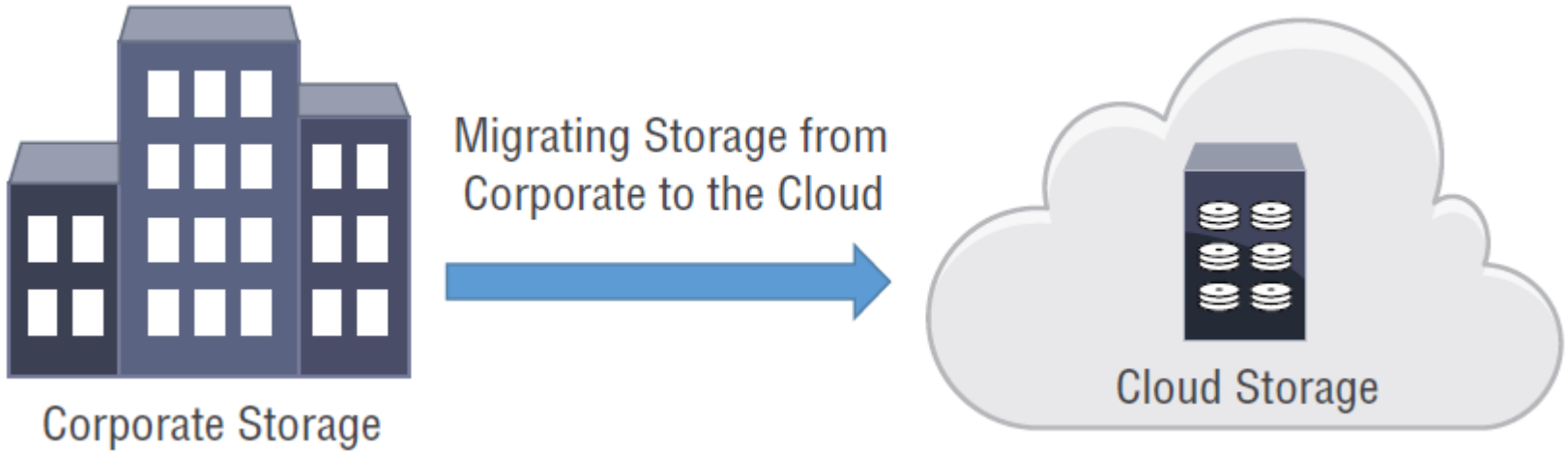
Storage data migration

- A server's data storage volumes can be migrated separately from or as part of a server migration
- The transition to the cloud accompanied by a cloud service provider will vary based on the cloud provider's storage offerings and infrastructure
- Things to take into account:
  - *the amount of bandwidth*
  - *how long it will take to upload the storage data from your internal data center to the cloud*
- However, with petabyte data in on-premise storage
  - *Data transfer over the network could literally take years*

Storage data migration

- Workarounds have been developed for such issue
  - Including appliances that can be shipped to the private data center and directly connected to the storage network for a local transfer of stored data, then it is shipped to the cloud service provider and directly transfer the data to cloud storage
- Some options are available to use these appliances
  - Including shipping-container-sized storage systems that are pulled by large semi-tractors

Storage data migration



Online vs Offline

	Pros	Cons
Online migrations	No delay for transport times Less expensive	Bad if the available bandwidth (either in the existing server or cloud provider) is limited
Offline migrations	No problem with bandwidth limitations	More delay in shipping the storage media Also more costly

COMPUTE MIGRATION IN AZURE

Types of server migrations

In this case, we will discuss 2 types of server migration:

- P2V (physical to virtual)
- V2V (virtual to virtual)

P2V migration in Azure

- Two options are available to perform migration from physical server to Azure:
  1. Upload the VHD
  2. Use Azure Size Recovery (ASR)

P2V migration by uploading VHD

- Convert the physical server to VHD format using tools such as Sysinternal Disk2VHD or System Center Virtual Machine Manager
- The VHD can be sysprepped and uploaded to Microsoft storage by using PowerShell, AzCopy, or Azure Storage blob APIs
- This VHD can be eventually used to create the VM in Azure

P2V migration with ASR

- ASR is a disaster recovery solution for physical servers
- The physical server–based environment can be replicated to Azure using ASR
  - It can be used for migration where the replicated environment is failed over and then continues to run from Azure
- An additional VM or physical machine should be available on-premise to set up the ASR components:
  - Configuration server: Manages data replication and coordinated communication to Azure
  - Process server: The data being sent to Azure is cached, compressed, and encrypted by the process server component. A mobility agent is deployed to all target machines to be replicated

The procedures with ASR

1. Install and configure the configuration server on-premise
   - It should be setup and discovered in Azure
2. Configure the target environment
   - Ensure that a compatible storage, network, and so forth, are available in the subscription
3. Configure a replication policy
   - Refines the replication intervals, RPOs, etc
4. Install mobility agent on the physical server
5. Refresh the configuration server in Azure Portal
6. Enable replication for the physical server

V2V migration in Azure

- Two options are available to perform migration from virtual environment (e.g. Vmware or Hyper-V) to Azure:
  1. Use Azure Migrate
  2. Use Azure Site Recovery (ASR)

V2V migration with Azure Migrate

- Some limitations
  - Currently, you can only assess on-premises VMware virtual machines (VMs) for migration to Azure VMs. The VMware VMs must be managed by vCenter Server (version 5.5, 6.0, or 6.5).
  - If you want to assess Hyper-VMs and physical servers, use the Azure Site Recovery Deployment Planner for Hyper-V, and our partner tools for physical machines.
  - You can discover up to 1500 VMs in a single discovery and up to 1500 VMs in a single project. Additionally, you can assess up to 1500 VMs in a single assessment.
  - If you want to discover a larger environment, you can split the discovery and create multiple projects. Learn more. Azure Migrate supports up to 20 projects per subscription.
  - Azure Migrate only supports managed disks for migration assessment.
  - You can only create an Azure Migrate project in the United States geography

V2V migration with ASR

- Specifically for VMWare and Hyper-V
- **VMWare:**
  - The configuration server can be downloaded in OVF (Open Virtualization Format) from Azure portal, then provide the vCenter server or vSphere ESXi server to connect to the server
  - After that, the steps are the same as P2V migration with ASR
- **Hyper-V:**
  - The steps are more or less the same as migration with VMWare
  - Another option is to upload the VHDs from Hyper-V environment to Azure Storage and converted to images to create VMs (using VHD upload method, not ASR)

Other options

- AWS to Azure migration using disaster recovery as a service (DRaaS) solution
- Using third party vendors as another option for migrating from VMWare, Hyper-V and physical workload to Azure, e.g.:
  - Veeam (https://www.veeam.com/)
  - Zerto (https://www.zerto.com/)

STORAGE AND NETWORK MIGRATION IN AZURE

Storage consideration in migration

- The on-premise storage capabilities are provided either by local HDDs/SSDs in servers or storage solutions such as network attached storage (NAS) or storage area networks (SANs)
- In Azure, the underlying storage is provided by storage as a service
- We can draw parallels between different on-premise storage features and the options available in cloud

Raid configuration (1)

- For on-premise storage, RAID (redundant array of independent disks) is used to distribute data across multiple disks for resiliency and improved performance
  - It is implemented as either hardware RAID or software RAID
- There are several RAID levels; the most common are RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10:
  - **RAID 0 is used for stripping data across multiple disks**, thereby resulting in improved performance. However, it does not provide resiliency, as the data is lost, even in single disk failures.
  - **RAID 1 is also called disk mirroring .** All data blocks are written in two disks in parallel so that the data is available if even one of the disks fails. Once the failed disk is replaced, data is rebuilt from the available disk.

Raid configuration (2)

- **RAID 5 stores data across multiple disks along with the parity bits.**
  If one of the disks fails, data can be re-created from the remaining disks and parity. It offers a balance between speed and redundancy.
- **RAID 6 strips the data across disks like RAID 5;** however, it stores extra parity bits that help recover data even if two disks fail.
- **RAID 10 combines the capabilities of RAID 1 and RAID 0,** where data is stripped and mirrored across additional disks for optimal performance and resiliency.

Storage replication in Azure

- Azure has built-in replication for all storage accounts
- There are **three copies of the virtual hard disk in the same datacenter by default:** the resiliency is similar to that of RAID 1
- This default replication option is called **locally redundant storage (LRS)**
  - If the data is replicated to a different region asynchronously, there are six copies of data, and three of these copies are in a paired geographical region.
  - All copies are mirror copies, like that in a RAID 1 configuration

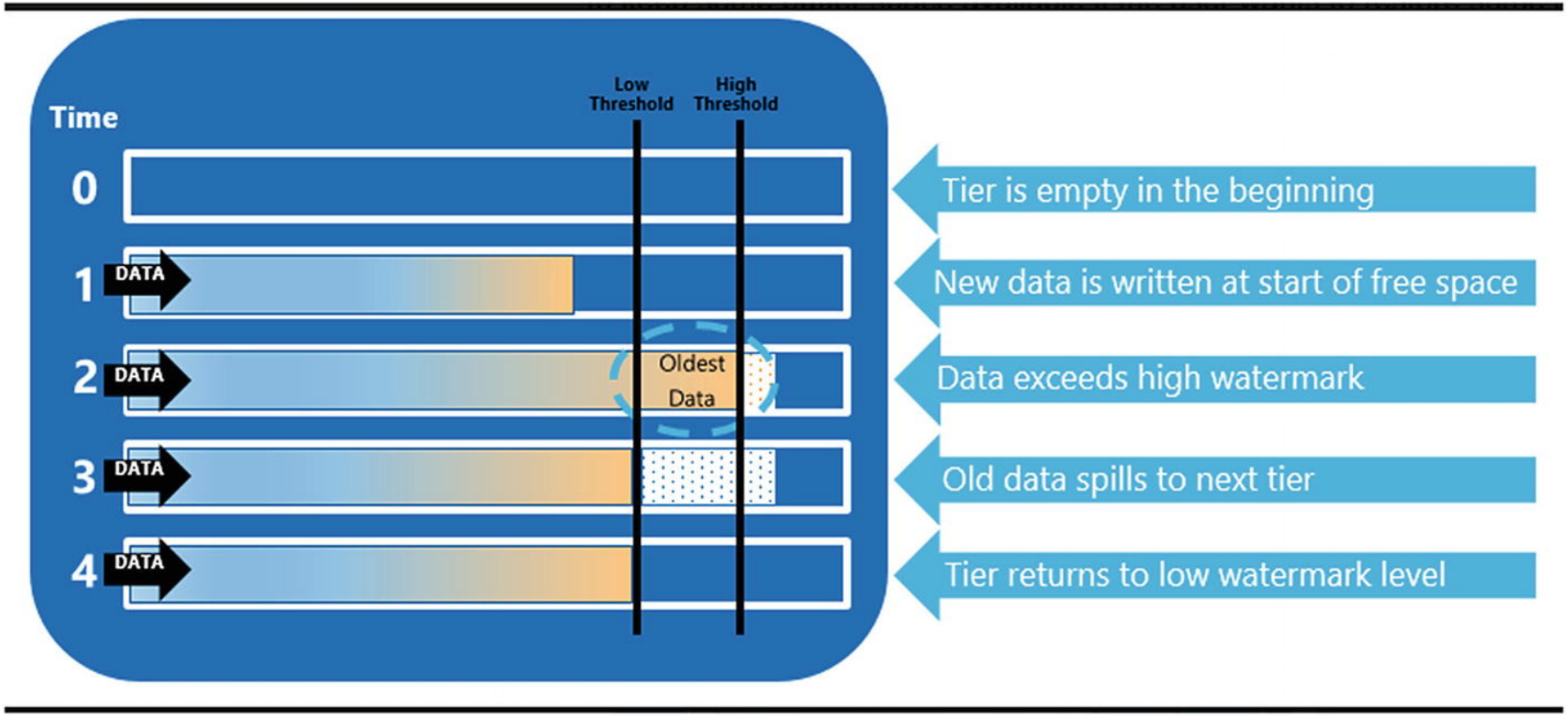
Storage Spaces

- Azure Storage Spaces aggregates multiple data disks to create virtual disks inside Azure VMs at the OS level
  - Parallel to RAID 0 configuration, where data is spread across multiple disks
  - The only difference is that here the resiliency is taken care of by the underlying Azure storage layer
  - For example, the maximum size of data disks that can be attached to an Azure VM is 4 TB.
  - If you want to have a drive size greater than 4 TB, you can do the same by adding multiple disks in a storage pool and then create a virtual disk from the pool

Other considerations on storage

- **VM Data Size**
- **VM Disk Performance (IOPS)**
- **File services**
  - **Azure file share** allows you to create server message block (SMB)-based file shares in Azure storage → equivalent with NAS-based file shares on-premise
  - **Azure File Sync** is in preview: it syncs file shares in Azure with file shares in your on-premise server to provide a hybrid solution
- **Hybrid storage: StorSimple**
  - Capable of doing all key storage requirements, such as primary storage, data archival, tape replacement, intelligent tiering, offsite storage, and so forth
  - It has automatic storage tiering and can tier all lesser-used and archival data to Azure cloud storage

Automatic tiering in StorSimple



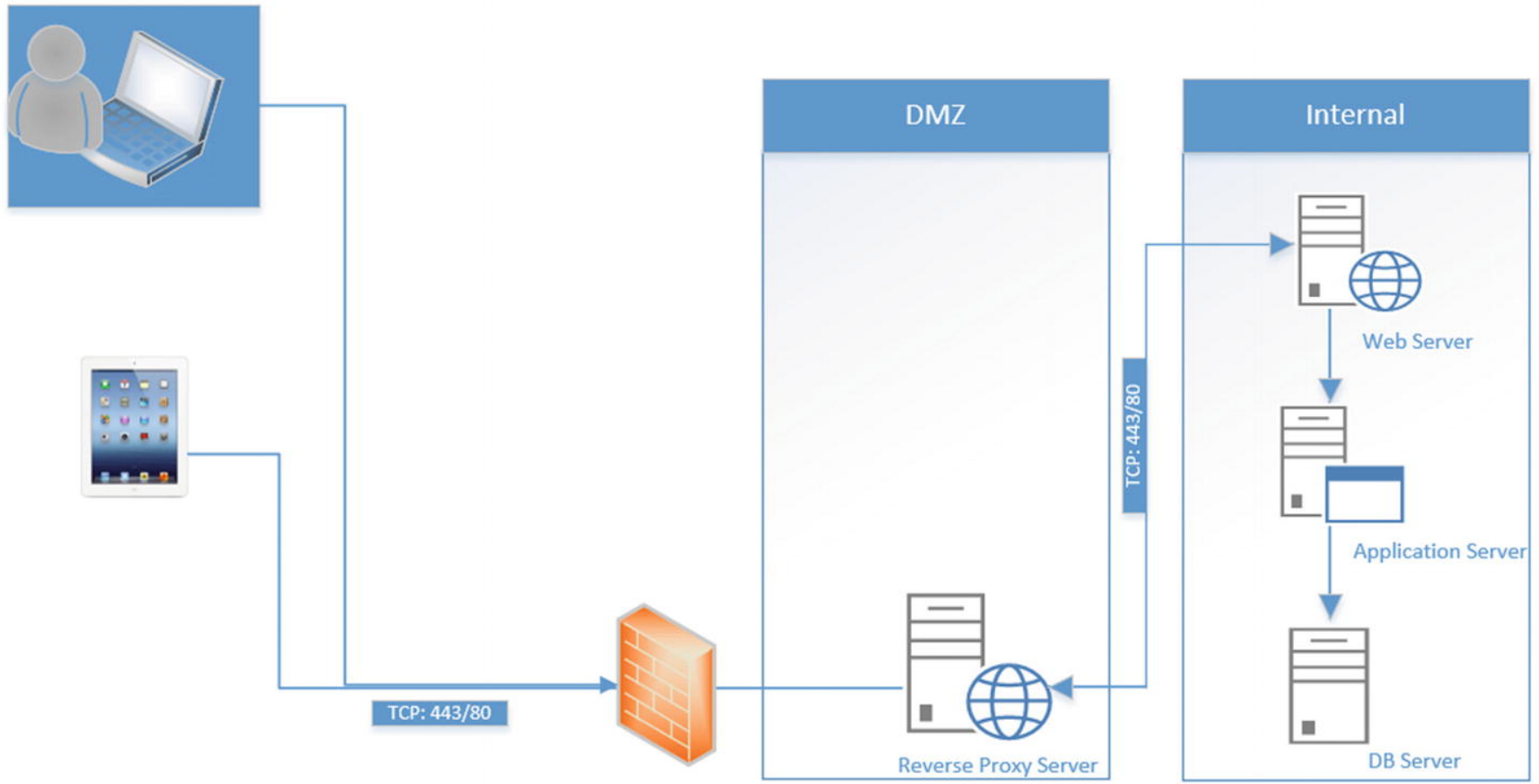
Automatic tiering in StorSimple

- StorSimple uses three layers of storage: **SSD, HDD, and cloud storage**
  - The **read and write** of fresh data always happens in the **SSD tier**
  - When data gets aged and is accessed less, it is tiered to the HDD layer
  - The cold data (i.e., the least accessed data) is tiered to the Azure cloud storage tier
  - **Lower and higher thresholds are always kept empty** because we want to keep some buffer space available if the user ever wants to restore archival data
  - After which data is migrated from **SSD to HDD** and from **HDD to Azure Storage**

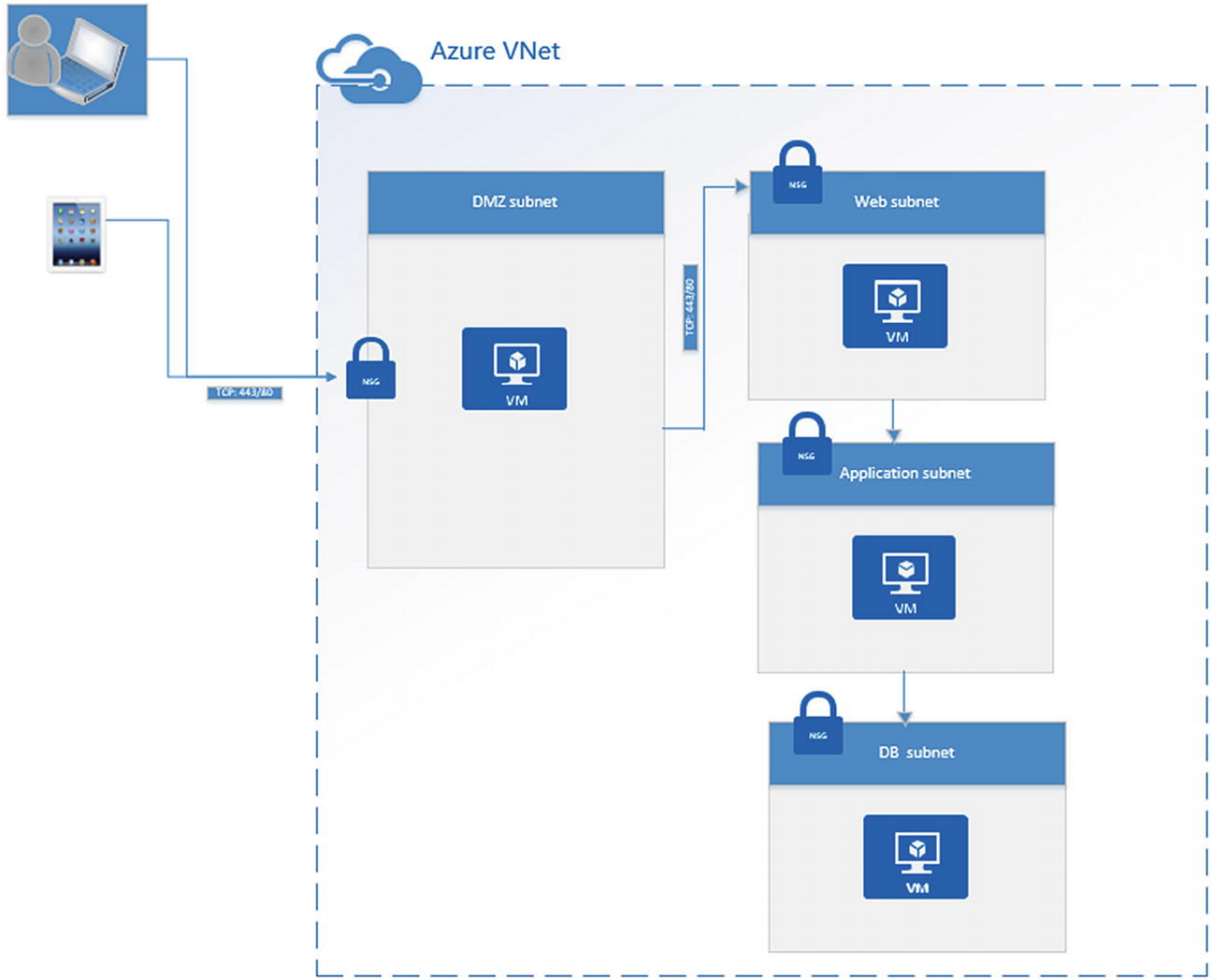
Network consideration when migrating to Azure

- Network segmentation
  - Normally network is segmented with VLAN, but Azure network configuration works at Layer 3 (no VLAN equivalent)
  - The segmentation in Azure can be achieved by VNet with network segregation (subnets)
- Allowed and denied communication between networks
  - Network security groups (NSGs) provide basic incoming and outgoing traffic management capabilities
- Expected traffic flow
  - User defined routes can be configured to change the default traffic flow
- Traffic monitoring

On-premise network architecture example



Azure network architecture example



Azure network architecture example

- NSGs can replace the firewall to filter the incoming traffic
- The DMZ network and application tiers can be configured in different subnets
  - with attached NSGs to allow only the required traffic to traverse

References

- T. Montgomery, S. Olson, “CompTIA Cloud+ Study Guide,” John Willey & Sons, 2nd ed, 2018
- S. A. Karthikeyan, “Practical Microsoft Azure IaaS: Migrating and Building Scalable and Secure Cloud Solutions,” Apres, 2018