Azure Innovation Days
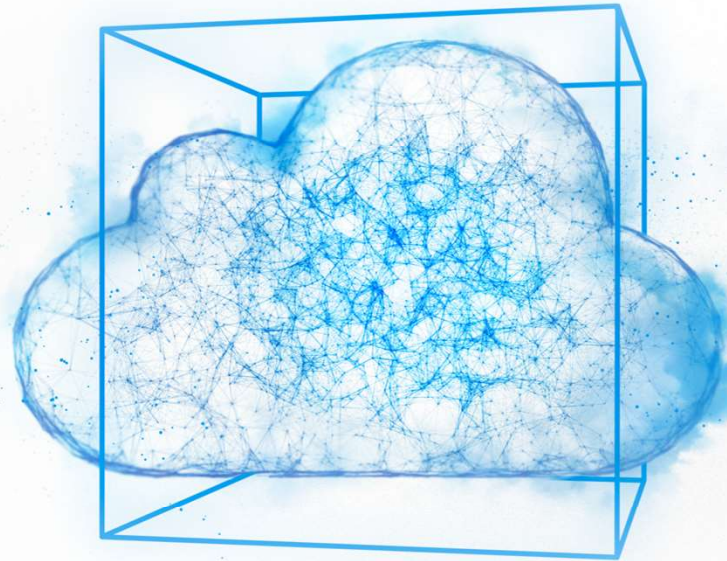
AHEAD®

Getting Started

You should have:

- Lab Guide

- Azure Account (Trial etc.)

- Internet Access

DISCLAIMER: AHEAD IS NOT RESPONSIBLE FOR ANY COSTS
INCURRED DURING THIS TRAINING. PLEASE DELETE YOUR
RESOURCE GROUP AT THE END OF THE COURSE.

Accessing the Code

https://github.com/AHEAD-Labs/AzureInnovationDay

Resource Groups & Regions

50 regions worldwide   **140** available in 140 countries

West Central US
West US 2
West US
US Gov Arizona
US Gov Texas
South Central US

US Gov Iowa
Central US
Canada Central
North Central US
US DoD East
East US, East US 2, US Gov Virginia
US DoD Central

Canada East

UK West
North Europe
UK South
France Central
France South

West Europe
Germany West Central
Germany North
Germany Northeast
Germany Central
Switzerland North
Switzerland West

China North
Korea Central
Korea South
China East
East Asia

Japan East
Japan West

UAE North
UAE Central
West India
Central India
South India

Southeast Asia

Brazil South

South Africa North

South Africa West

Australia East
Australia Southeast
Australia Central, Australia Central 2

○ Available region
⬭ Announced region
● Availability Zones present

Regions Overview

West US — East US (Region pairing)

Resource Group Overview

Name: AHEAD-Prod-App-RG
Location: Central US

Azure VM
West US

Azure SQL
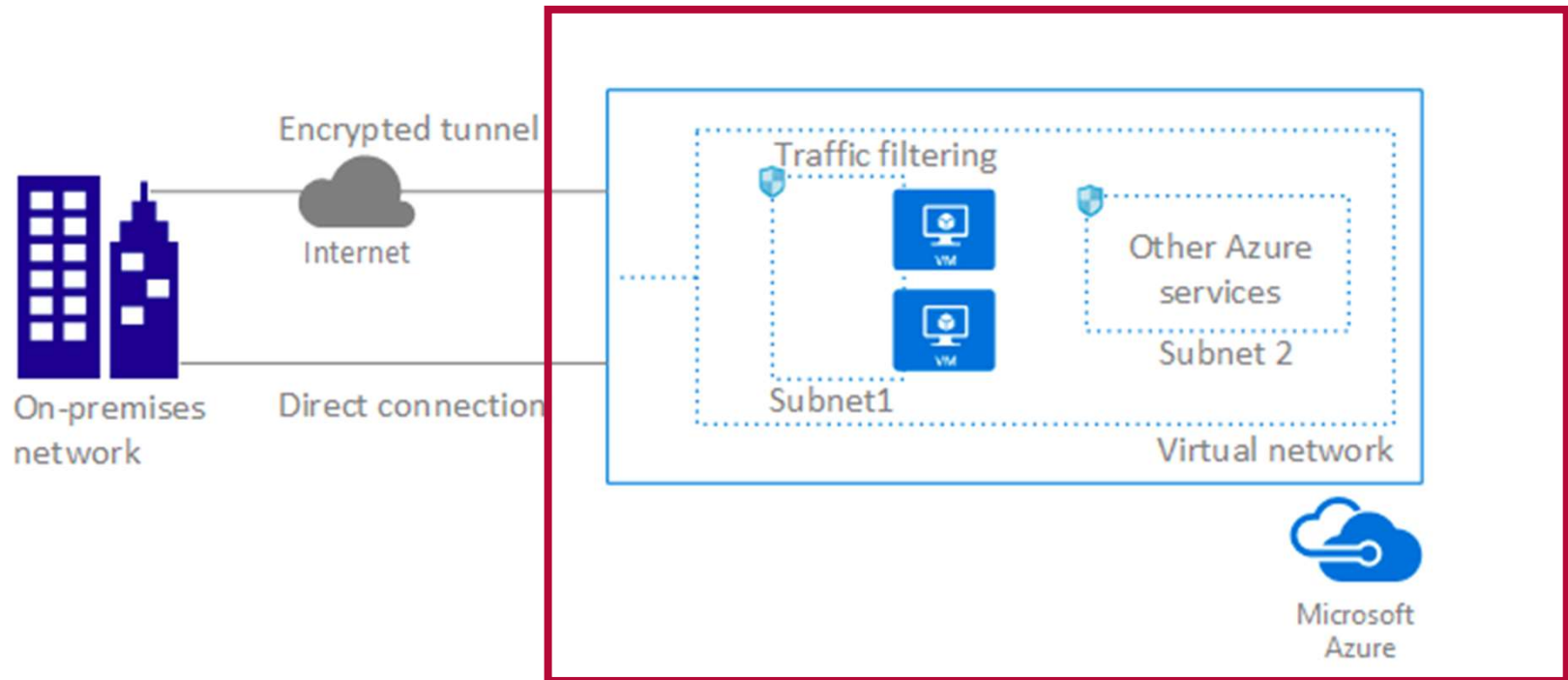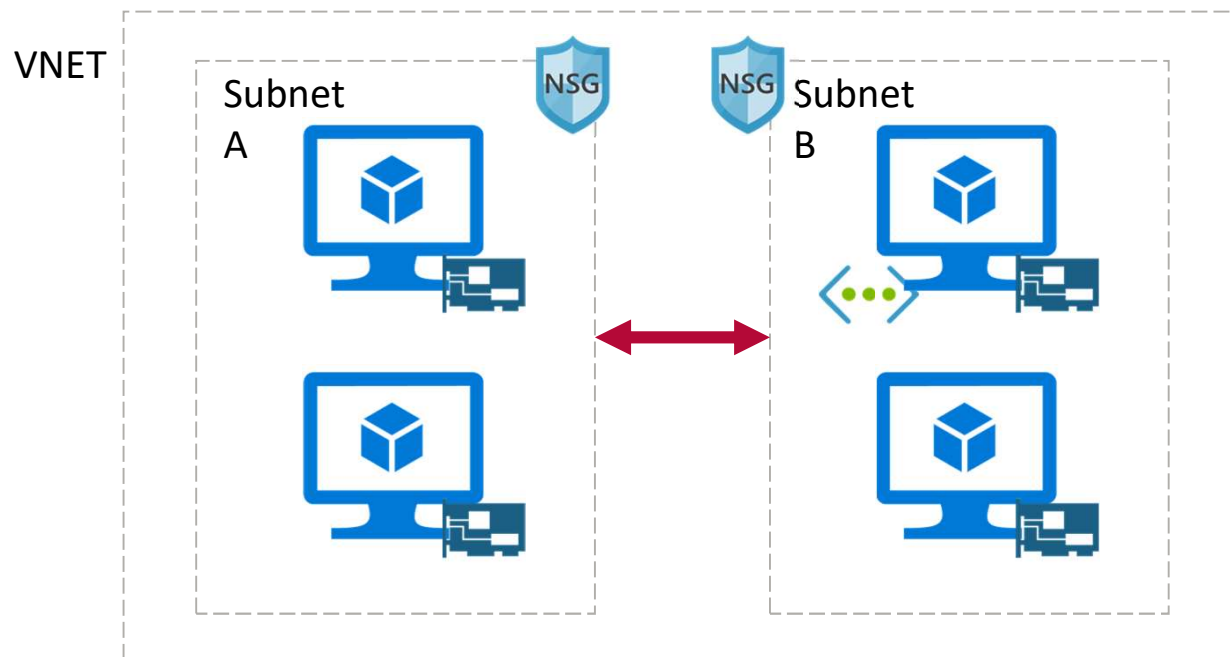East US
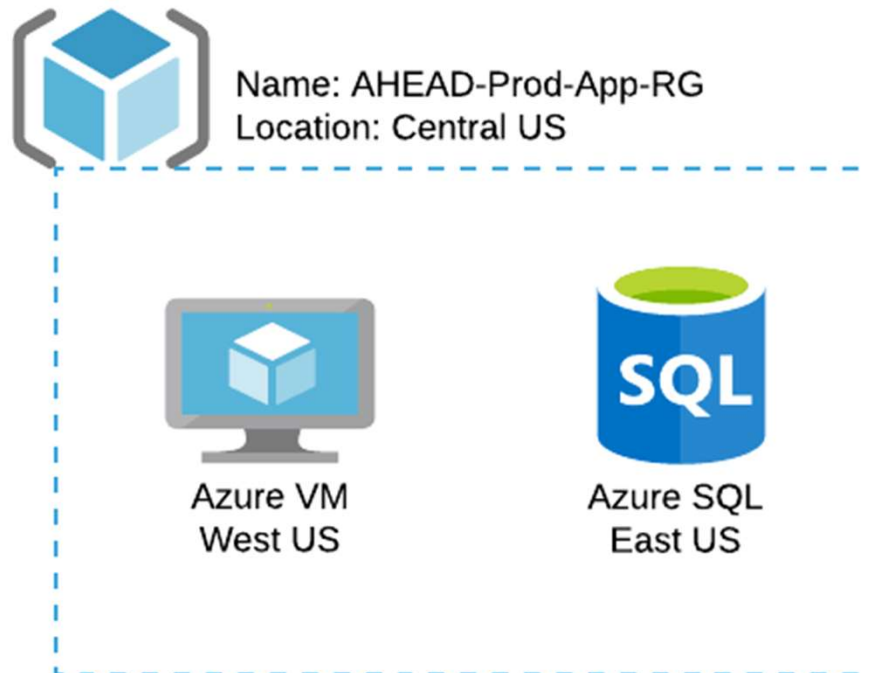
Networking

Networking Overview

Networking Overview

Core VNET Capabilities

- **Isolation**
- **Internet Access**
- **Azure Resources (VMs and Cloud Services)**
- **VNET Connectivity**
- **On-Premises Connectivity**
- **Traffic Filter**
- **Routing**

IP Addressing

- DHCP - Azure provided/managed service

- All addresses are DHCP based

- Addresses are not allocated until Azure object is created

- Addresses are recovered when object is deallocated
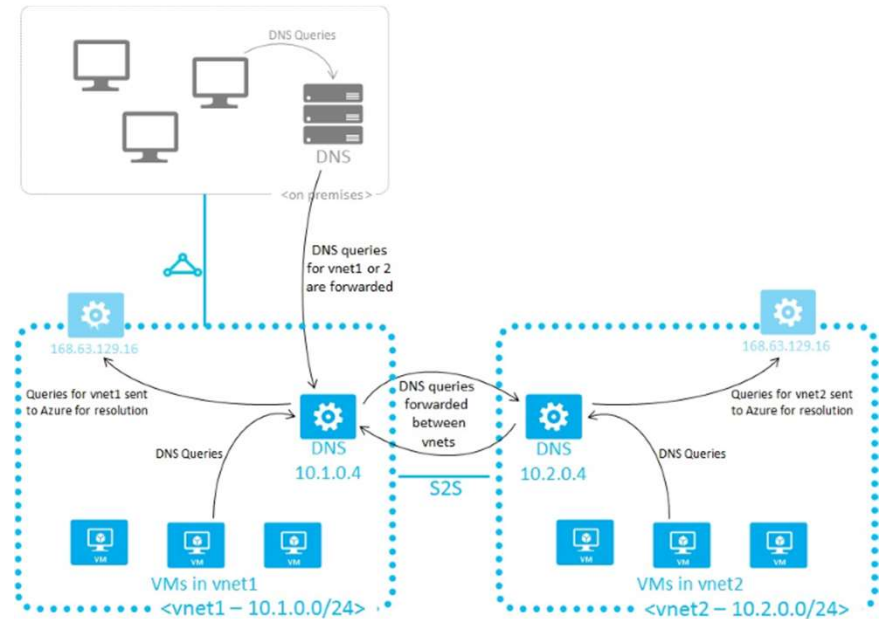
IP Addressing (cont.)

- Static addresses are the equivalent DHCP reservations

- Address prefix comes from VNET/subnet definitions

- Azure reserves the first three and the last IP from the pool

- First address of a /24 is .4

DNS in Azure

Azure provided DNS	Customer DNS Server

DNS Queries

DNS

<on premises>

DNS queries
for vnet1 or 2
are forwarded

168.63.129.16

Queries for vnet1 sent
to Azure for resolution

DNS queries
forwarded
between
vnets

168.63.129.16

Queries for vnet2 sent
to Azure for resolution

DNS Queries

DNS
10.1.0.4

DNS
10.2.0.4

DNS Queries

S2S

VMs in vnet1
<vnet1 – 10.1.0.0/24>

VMs in vnet2
<vnet2 – 10.2.0.0/24>

Configure Virtual Networking DNS

- **Select** Virtual Network in Azure

- **Select** DNS Servers from the **Settings** section

- Choose **Default** (Azure-Provided) to stick with Azure DNS

- Choose **Custom** to input your own DNS Servers

- **Add DNS Servers** (preferably more than 1)

- **Save**
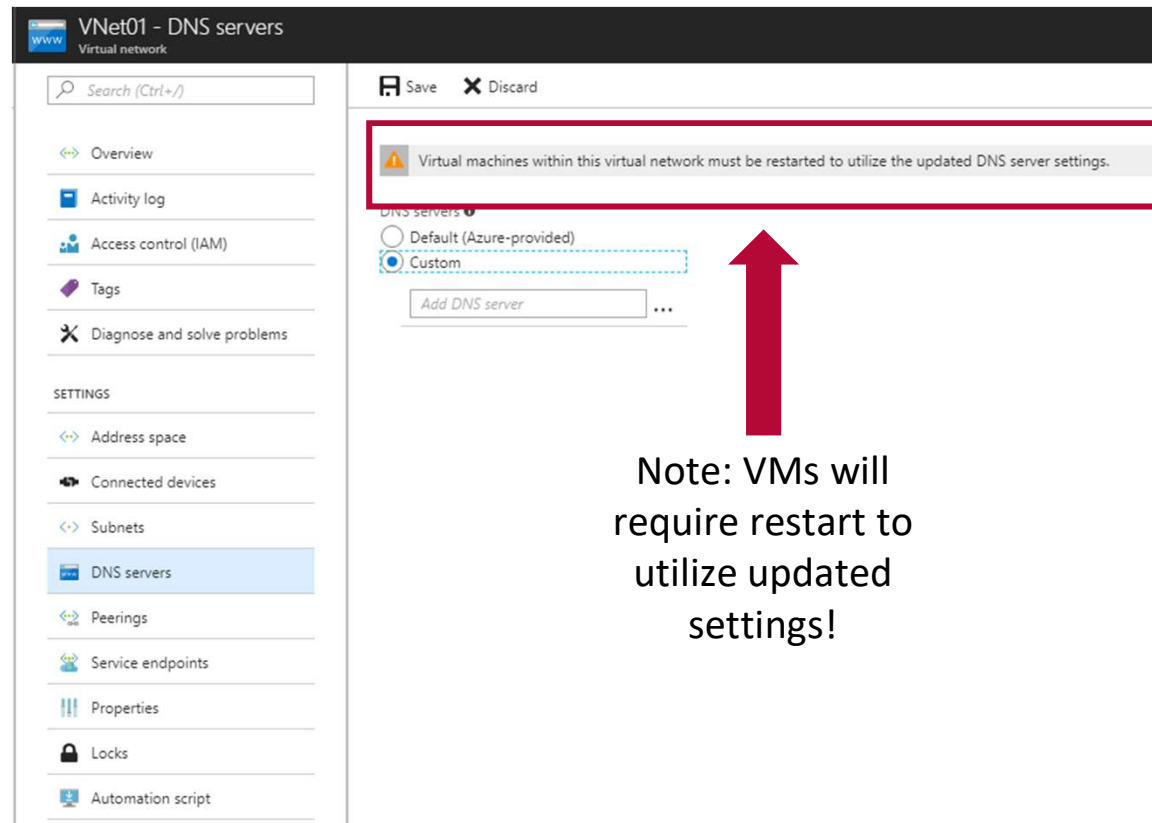
Note: VMs will require restart to utilize updated settings!

Internet Access

All resources in a VNET can communicate to the internet by default	**Private IP is SNAT to a Public IP selected by Azure**	**Outbound connectivity can be restricted via routes or traffic filtering**	**Inbound connectivity without SNAT requires public IP**

Routing and NSGs

Default Routing in a Subnet

- If address is within the VNET address prefix – route to local VNET

- If the address is within the on premises address prefixes or BGP published routes (BGP or Local Site Network (LSN) for S2S) – route to gateway

- If the address is not part of the VNET or the BGP or LSN routes – route to Internet via NAT

- If destination is an Azure datacenter address and ER public peering is enabled, it is routed to the gateway.

- If the destination is an Azure datacenter with S2S or an ER without public peering enabled, then it is routed to the Host NAT for Internet path, but it never leaves the datacenter
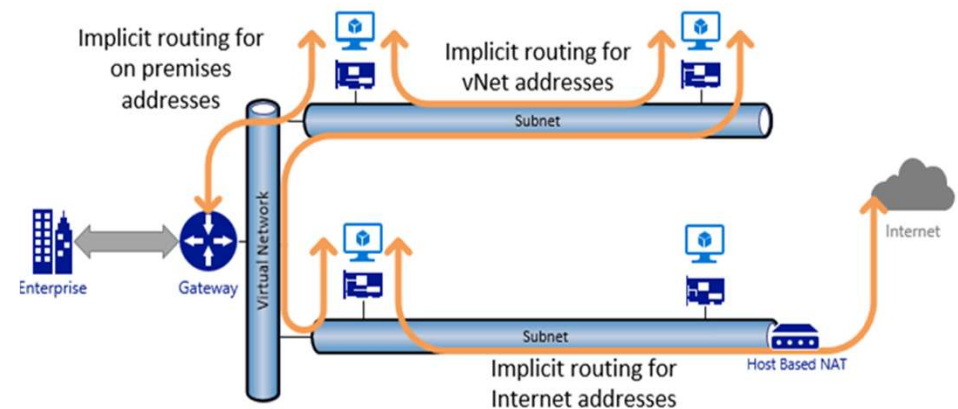
Network Security Groups (NSGs)

VNET

Subnet A

NSG ← NSG
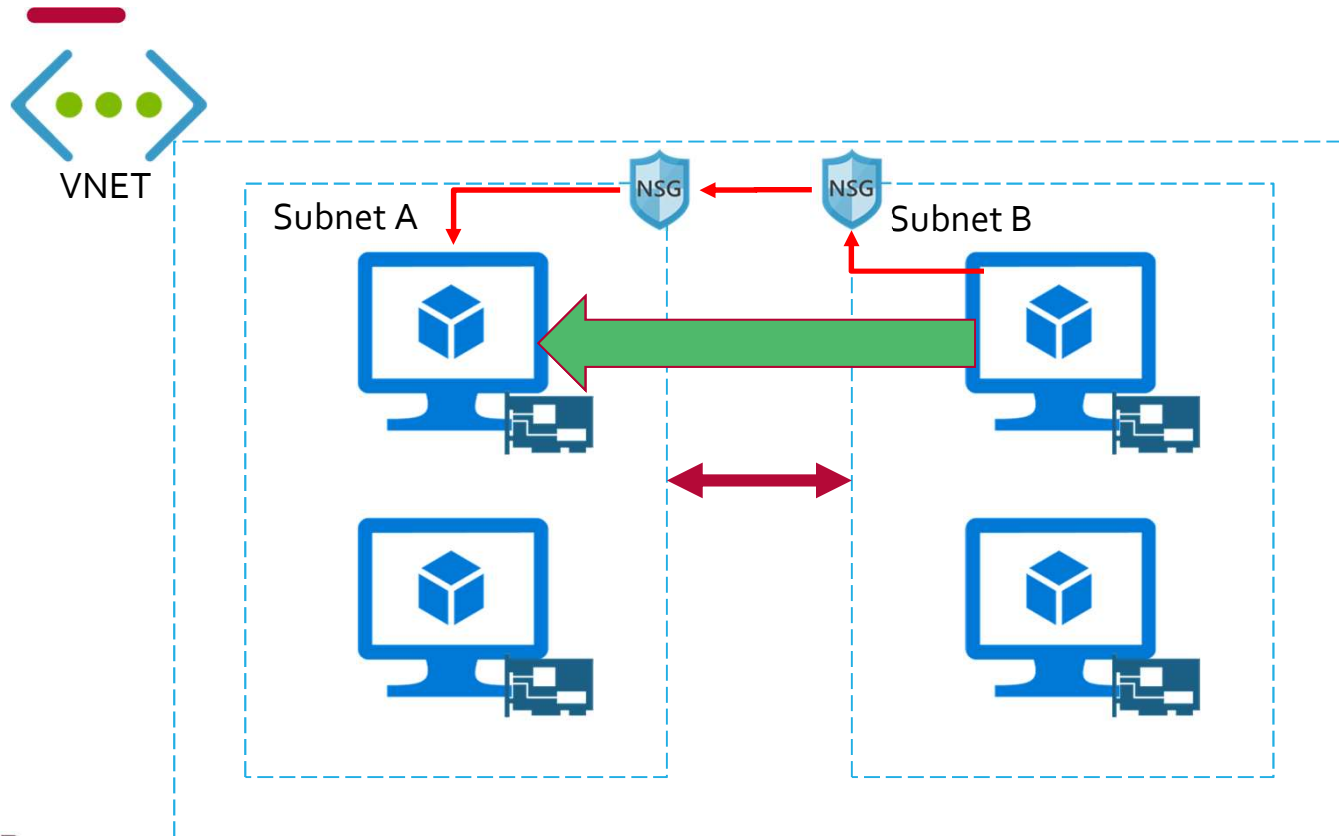
Subnet B

- Can be applied to Network Interface or Subnet
- Subnet rules apply to ALL resources in subnet

AHEAD

NSG Default Rules

Inbound default rules

Name	Priority	Source IP	Source Port	Destination IP	Destination Port	Protocol	Access
AllowVNet InBound	65000	VirtualNetwork	*	VirtualNetwork	*	*	Allow
AllowAzure LoadBalancer InBound	65001	AzureLoad Balancer	*	*	*	*	Allow
DenyAll InBound	65500	*	*	*	*	*	Deny

NSG Default Rules

Outbound default rules
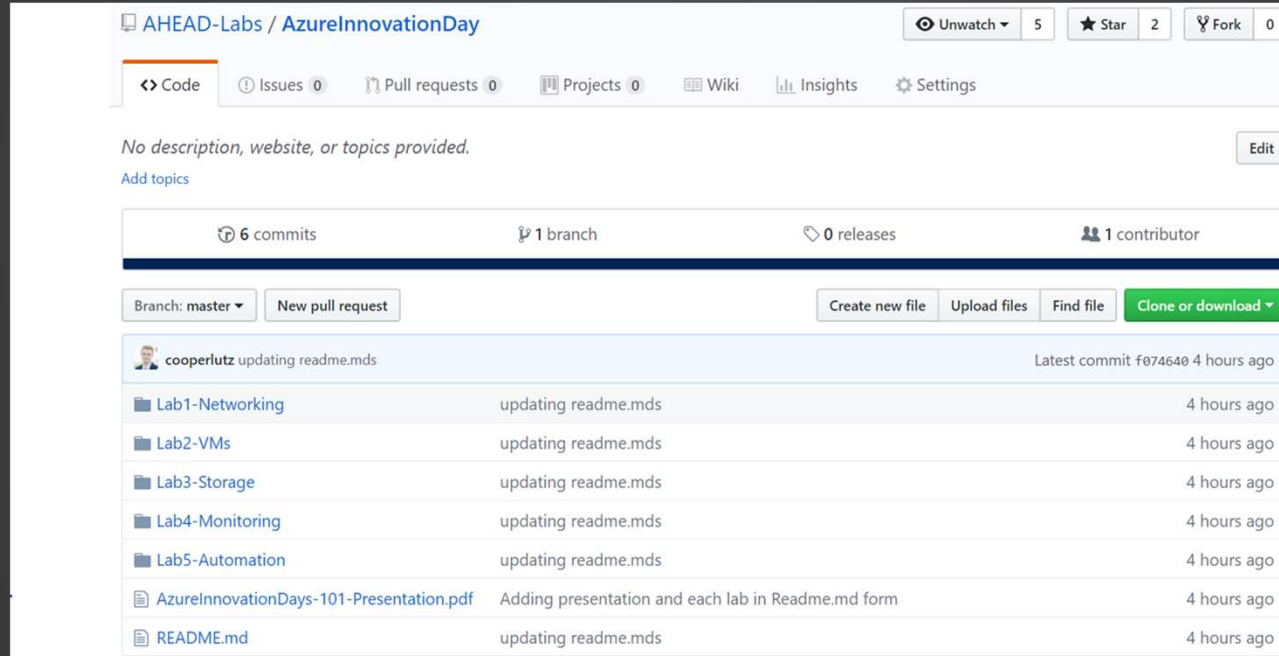
Name	Priority	Source IP	Source Port	Destination IP	Destination Port	Protocol	Access
AllowVnet OutBound	65000	VirtualNetwork	*	VirtualNetwork	*	*	Allow
AllowInternet OutBound	65001	*	*	Internet	*	*	Allow
DenyAll OutBound	65500	*	*	*	*	*	Deny

LAB | Networking

AHEAD

Lab1-Networking

https://github.com/AHEAD-Labs/AzureInnovationDay

Virtual Machines

Azure VM Overview

Introduction to Virtual Machines

Application
Operating System
Hardware

CPU   Memory   Disk

VM

App	App	App
OS	OS	OS

Hypervisor
Hardware

CPU   Memory   Disk
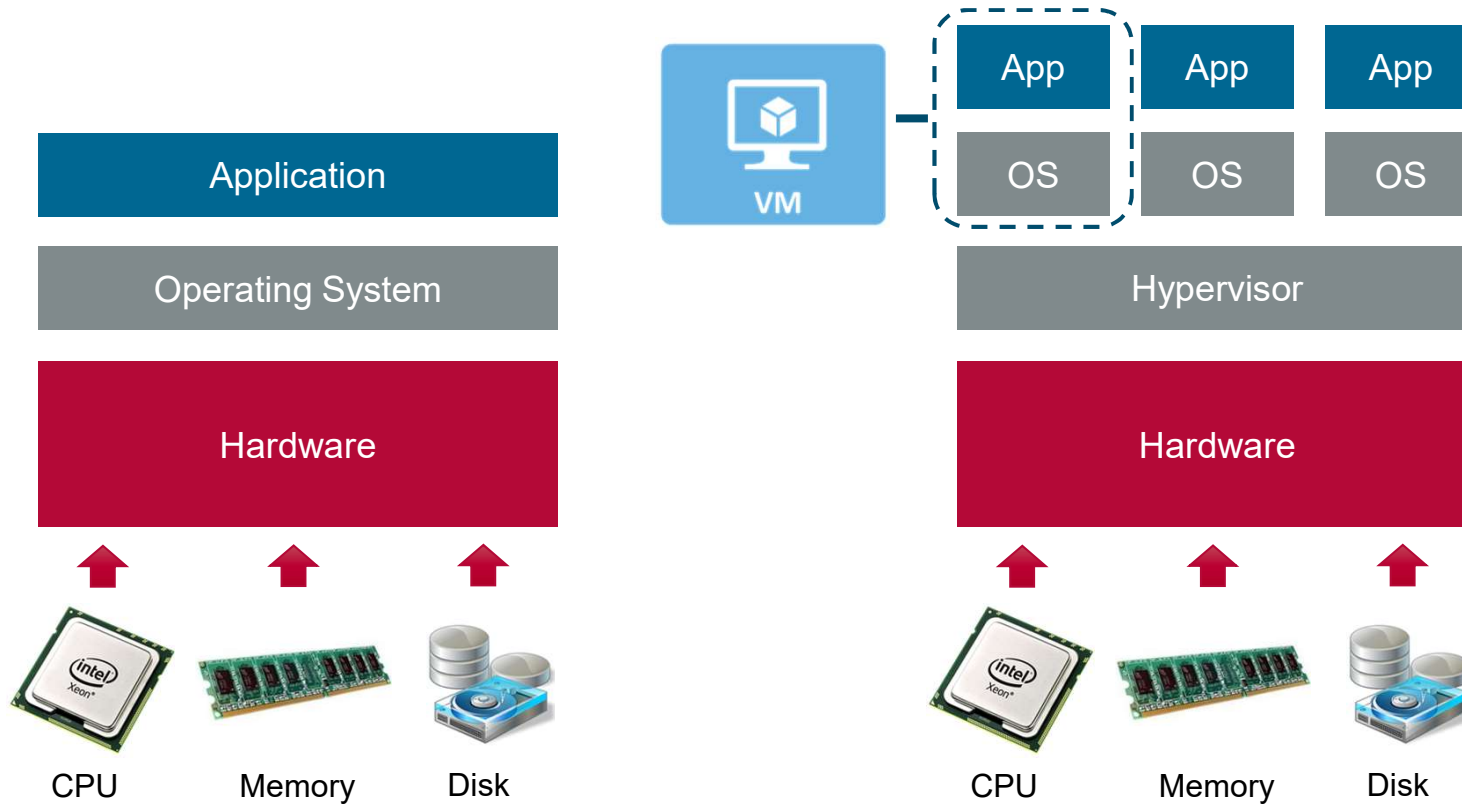
VM Types

Type	Purpose
A - Basic	Basic version of the A series for testing and development.
A – Standard	General-purpose VMs.
B – Burstable	Burstable instances that can burst to the full capacity of the CPU when needed.
D – General Purpose	Built for enterprise applications. DS instances offer premium storage.
E – Memory Optimized	High memory-to-CPU core ratio. ES instances offer premium storage.
F – CPU Optimized	High CPU core-to-memory ratio. FS instances offer premium storage.
G - Godzilla	Very large instances ideal for large databases and big data use cases.

VM Types (Continued)

Type	Purpose
H – High performance compute	High performance compute instances aimed at very high-end computational needs such as molecular modelling and other scientific applications.
L – Storage optimized	Storage optimized instances which offer a higher disk throughput and IO.
M – Large memory	Another large-scale memory option that allows for up to 3.5 TB of RAM.
N – GPU enabled	GPU-enabled instances.
SAP HANA on Azure Certified Instances	Specialized instances purposely built and certified for running SAP HANA.

VM

VM Specializations

S	M	R
Premium Storage options available	Larger memory configuration of instance type	Supports remote direct memory access (RDMA)

Example: DSv2

Example: Standard A2m_v2

Example: H16mr

Azure Compute Units (ACUs)

Way to compare CPU performance between different types/sizes of VM

Microsoft created performance benchmark

A VM with an ACU of 200 has twice the performance of a VM with an ACU of 100

AHEAD®

OS Reference Documentation

- Windows Virtual Machines
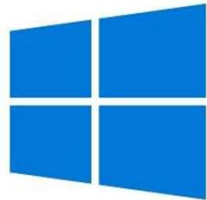
  https://docs.microsoft.com/en-us/azure/virtual-machines/windows/

- Linux Virtual Machines

  https://docs.microsoft.com/en-us/azure/virtual-machines/linux/
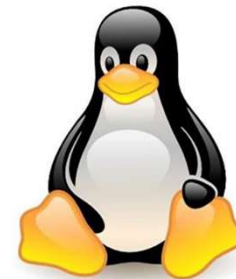
Windows Server Support

OS	Key Points
Pre-Windows 2008 R2 (e.g. Windows Server 2003)	•Windows 2003 and later are supported for deployment. •Must bring own image. •No marketplace support. •Need to have your own custom support agreement (CSA).
Windows Server 2008 R2	•Supported. •Specific support matrix for server roles.
Windows Server 2012	•Supported – Datacenter version in marketplace.
Windows Server 2016	•Supported – Datacenter and nano versions in marketplace.
Desktop OS	•Windows 10 Pro and Enterprise in marketplace.

https://support.microsoft.com/en-us/help/2721672/microsoft-server-software-support-for-microsoft-azure-virtual-machines

AHEAD®

Linux-Supported Distributions

Distribution	Version	Drivers	Agent
CentOS	CentOS 6.3+, 7.0+	CentOS 6.3: LIS download CentOS 6.4+: In kernel	Package: In repo under "WALinuxAgent" Source code: GitHub
CoreOS	494.4.0+	In kernel	Source code: GitHub
Debian	Debian 7.9+, 8.2+	In kernel	Package: In repo under "waagent" Source code: GitHub
Oracle Linux	6.4+, 7.0+	In kernel	Package: In repo under "WALinuxAgent" Source code: GitHub
Red Hat Enterprise Linux	RHEL 6.7+, 7.1+	In kernel	Package: In repo under "WALinuxAgent" Source code: GitHub
SUSE Linux Enterprise	SLES/SLES for SAP 11 SP4 12 SP1+	In kernel	Package: for 11 in Cloud:Tools repo for 12 included in "Public Cloud" Module under "python-azure-agent" Source code: GitHub
openSUSE	openSUSE Leap 42.2+	In kernel	Package: In Cloud:Tools repo under "python-azure-agent" Source code: GitHub

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros

Regional Limitations

Products	NON-REGIONAL*	United States								Canada	
		EAST US	EAST US 2	CENTRAL US	NORTH CENTRAL US	SOUTH CENTRAL US	WEST CENTRAL US	WEST US	WEST US 2	CANADA EAST	CANADA CENTRAL
− Compute											
Virtual Machines		●	●	●	●	●	●	●	●	●	●
A0 - A7		●	●	●	●	●	●	●	●	●	●
Av2		●	●	●	●	●	●	●	●	●	●
B-series		●							●		
A8 – A11 (Compute Intensive)		●			●	●		●			
D-series		●	●	●	●	●		●			
Dv2-series		●	●	●	●	●	●	●	●	●	●
Dv3-series		●	●					●	●	●	●
DS-series		●	●	●	●	●		●			
DSv2-series		●	●	●	●	●	●	●	●	●	●
DSv3-Series		●	●						●		
Ev3-series		●	●					●	●	●	●
F-series		●	●	●	●	●	●	●	●	●	●

VM Images

- Custom Images

  - Do-it-yourself image
  - Windows - Sysprep
  - Linux - sudo waagent – deprovision+user
  - Generalize in Azure
  - Create image

- Marketplace Images

  - Provided for you in the Azure Marketplace
  - Properties:
    - Publisher
    - Offer
    - SKU

PowerShell VM Commands

Task	PowerShell Example
New Resource Group	New-AzureRmResourceGroup -Name myResourceGroup -Location EastUS
New Virtual Machine	New-AzureRmVM
Must provide names for reach of the required resources:	
Create VM Configuration	$vm = NewAzureRmVMConfig – VMName $Vmname
-Name "SL-VM01" ` -Location "East US" ` -VirtualNetworkName "SLVNET" `	
Start and Stop VMs	Start-AzureRmVM Stop-AzureRmVM
-OpenPorts 80,3389	

VM Storage

VM Storage Types

- Standard Storage

Backed by traditional HDD
Most cost effective
Max throughput – 60MB/S per disk
Max IOPS – 500 IOPS per disk

- Premium Storage

Backed by SSD drives
Higher performance
Max throughput – 250MB/S per disk
Max IOPS – 7500 IOPS per disk

Managed Disk – Standard Storage Sizes

	S4	S6	S10	S20	S30	S40	S50
Disk size (GB)	32	64	128	512	1024	2048	4095

- Max IOPS for all sizes above is 300 IOPS/Disk
- Max throughput for all sizes is 60MB/s

Managed Disk – Premium Storage Sizes

	P4	P6	P10	P15	P20	P30	P40	P50
Disk size (GB)	32	64	128	256	512	1024	2048	4095
Max IOPS	120	240	500	1100	2300	5000	7500	7500
Max throughput	25 MB/s	50 MB/s	100 MB/s	125 MB/s	150 MB/s	200 MB/s	250 MB/s	250 MB/s

Managed vs. Unmanaged Disks

Unmanaged Disks

DIY option

Management overhead
(20000 IOPS per storage
account limit)

Supports all replication modes
(LRS, ZRS, GRS, RA-GRS)
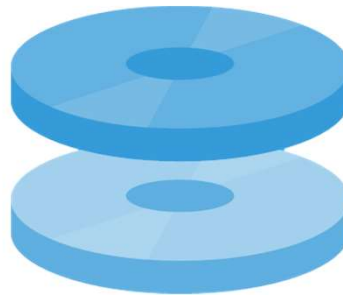
Managed Disks

Simplest option

Lower management overhead
as Azure manages the
storage accounts

Only LRS replication mode
currently available

Replication Options

Logically Replicated Storage (LRS)	Zone Replicated Storage (ZRS)	Geographically Replicated Storage (GRS)	Read Only Geographically Replicated Storage (RA-GRS)
Replicated three times within a storage scale unit (collection of racks of storage nodes) hosted in a datacenter in the same region as your storage account was created.	Replicated three times across one or two datacenters in addition to storing three replicas similar to LRS. Data stored in ZRS is durable even in the event that the primary datacenter is unavailable or unrecoverable.	Replicates your data to a second region that is hundreds of miles away from the primary region. Your data is curable even in the event of a complete region outage.	Same replication as per GRS but also provides read access to the data in the other region.

Replication Options

Replication Strategy	LRS	ZRS	GRS	RA-GRS
Data is replicated across multiple datacenters?	No	Yes	Yes	Yes
Data can be read from a secondary location *and* the primary location?	No	No	No	Yes
Number of copies of data maintained on separate nodes:	3	3	6	6

Availability Sets

- Potential for VM Impact

- Planned maintenance

- Unplanned hardware maintenance

- Unexpected downtime

- Availability Sets

- Group two or more machines in a set

- Separated based on Fault Domains and Update Domains

Fault Domains and Update Domains
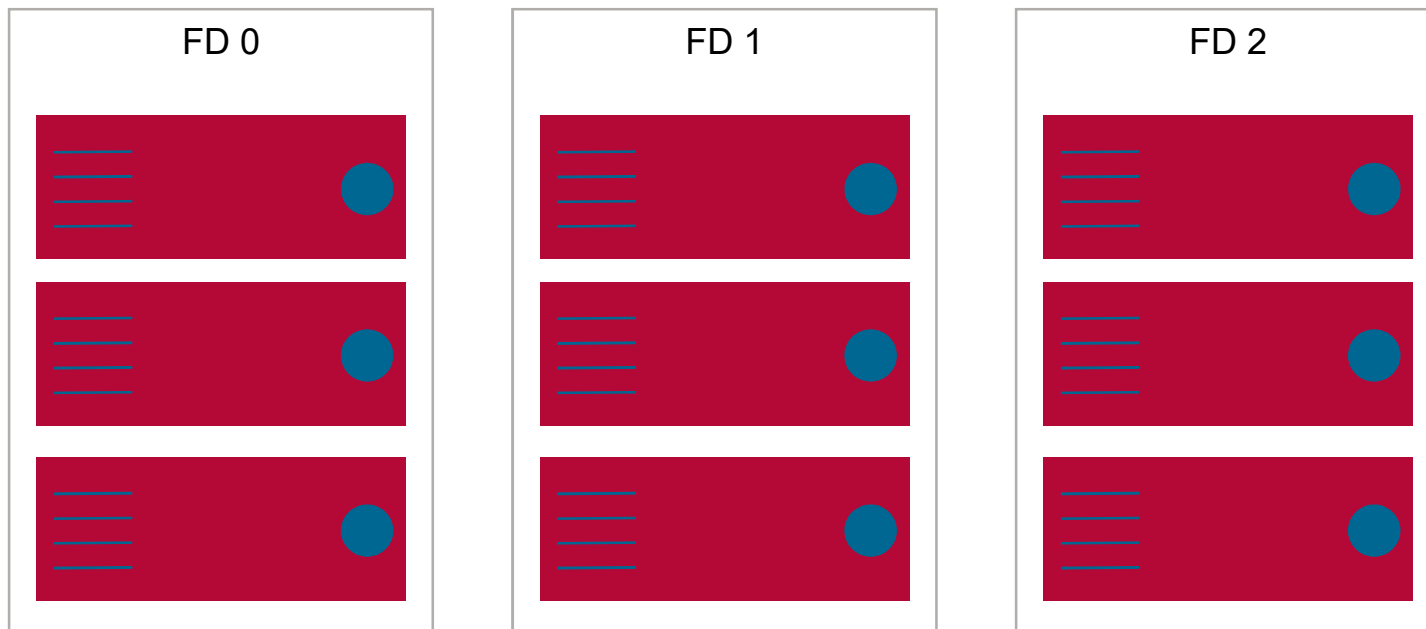
Fault Domains and Update Domains
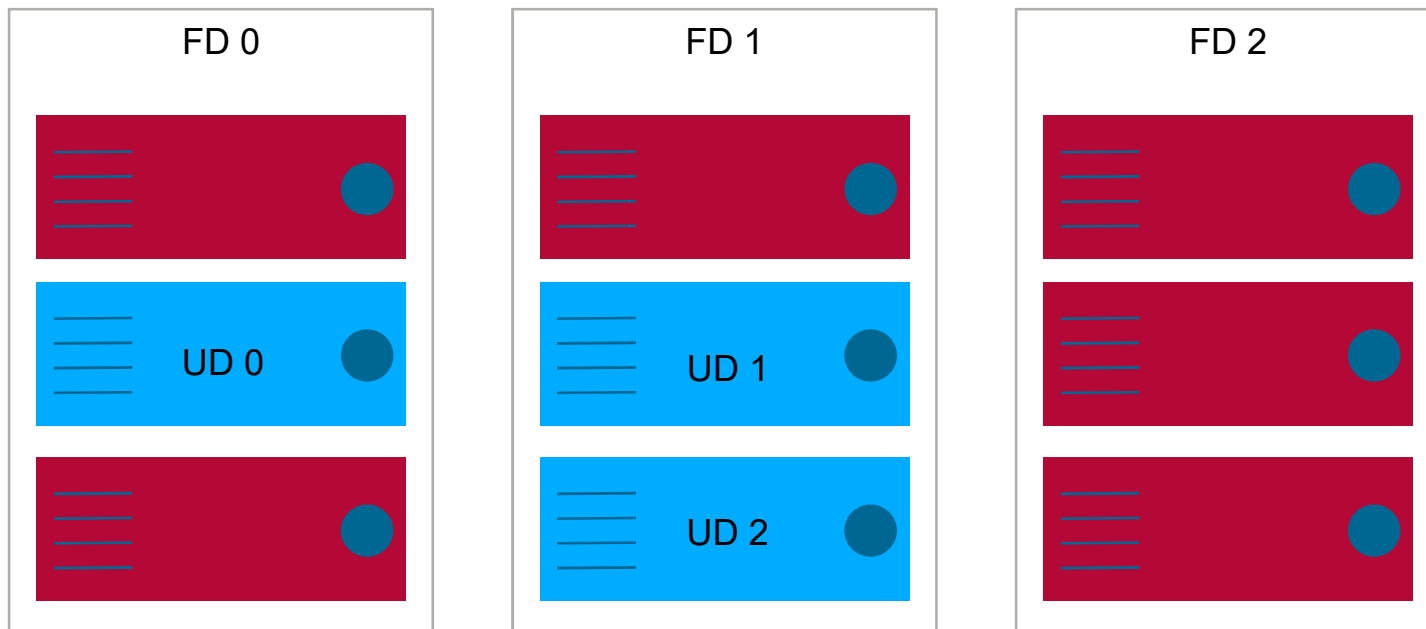
Planning for Availability

Web Tier
Availability Set

App Tier
Availability Set

Data Tier
Availability Set
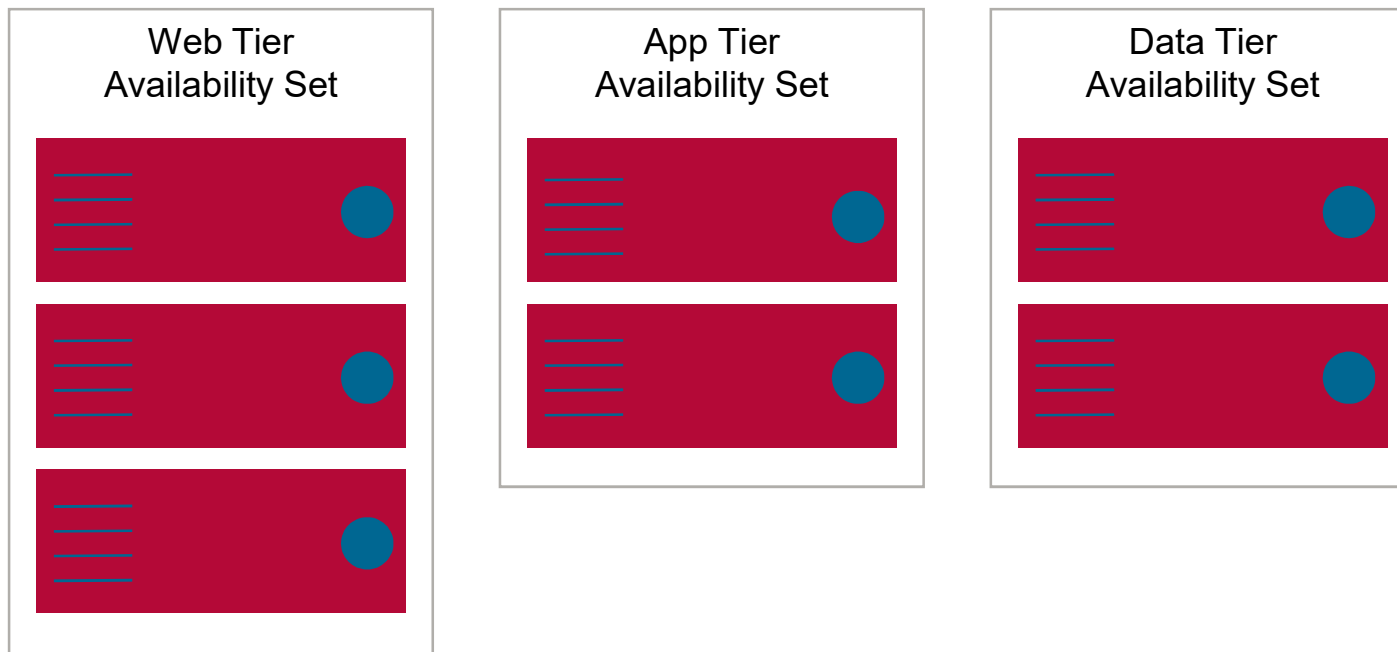
LAB | Azure Virtual Machines

Lab2-VMs

https://github.com/AHEAD-Labs/AzureInnovationDay

Storage

Storage Overview

Azure Blob Storage Overview

Storage Account → Container → IMAGE.JPG, VIDEO.AVI

Storage Account → Container → IMAGE.JPG, VIDEO.AVI
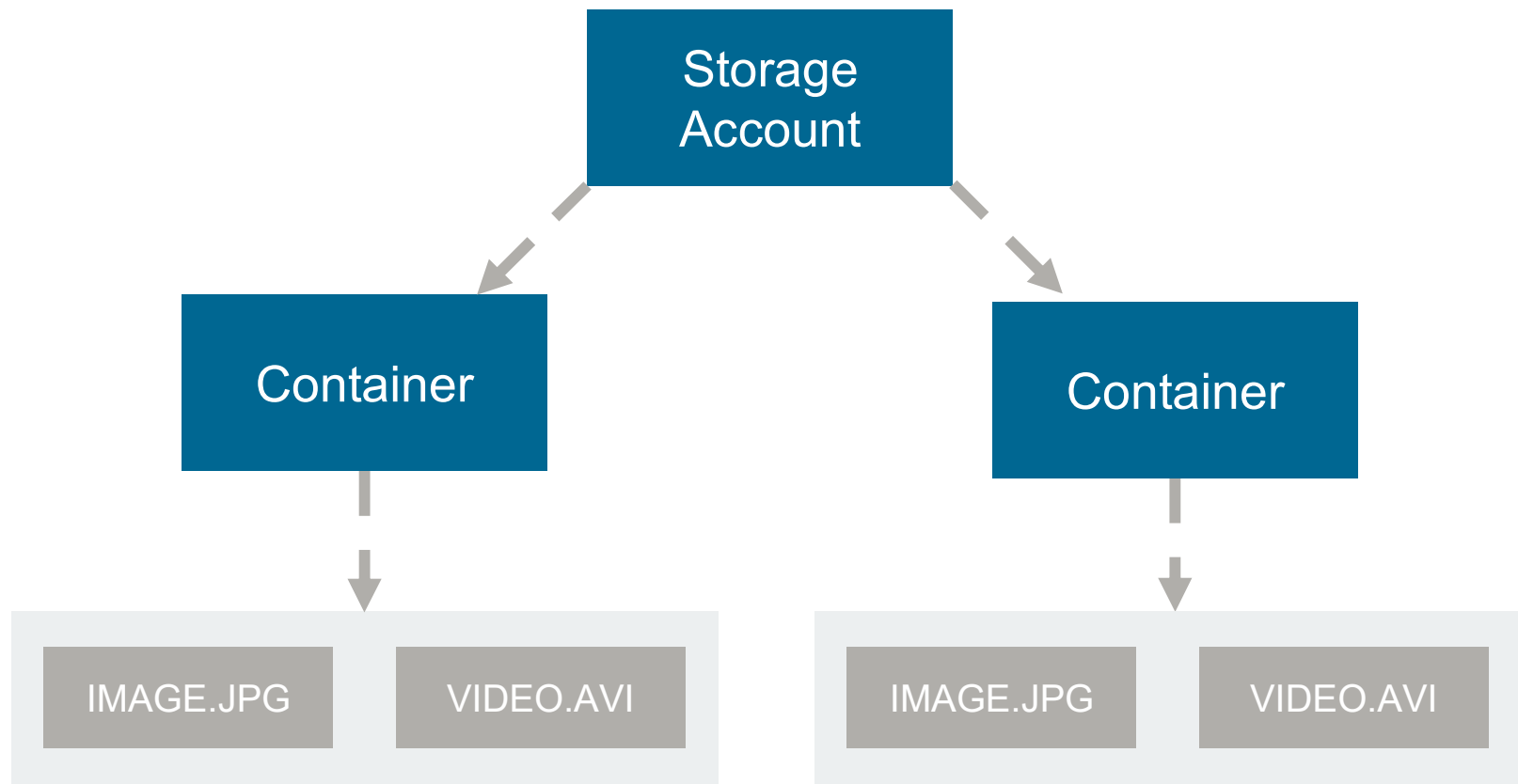
Storage Account Types

General Purpose v1 (GPV1)

Blob Account

General Purpose v2 (GPV2)

Block Blobs vs. Page Blobs

- **Block Blob**

  - Ideal for storing text or binary files

  - A single block blob can contain up to 50,000 blocks of up to 100 MB each, for a total size of 4.75 TB

  - Append blobs are optimized for append operations (e.g. logging)

- **Page Blob**

  - Efficient for read/write operations

  - Used by Azure VMs

  - Up to 8 TB in size

AHEAD®

Storage Tiers

Hot

- Higher storage costs
- Lower access costs

Cold

- Lower storage costs
- Higher access costs
- Intended for data that will remain cool for 30 days or more

Archive

- Lowest storage costs
- Highest retrieval costs
- When a blob is in archive storage it is offline and cannot be read

Choosing Between Blobs, Files, and Disks

Blobs
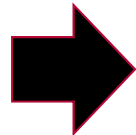
- Access application data from anywhere
- Large amount of objects to store, images, videos etc.

Files
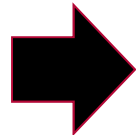
- Access files across multiple machines
- Jumpbox scenarios for shared development scenarios

Disks
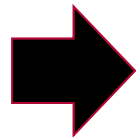
- Do not need to access the data outside of the VM
- Lift-and-shift of machines from on-premises
- Disk expansion for application installations
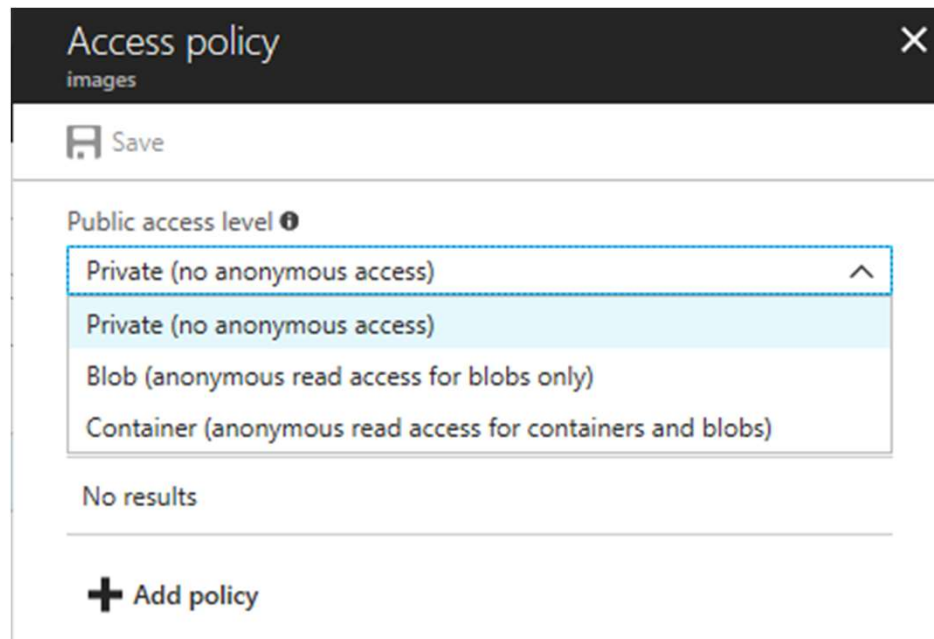
Storage Permissions

Managing Access: Container Permissions

Private
(No Anonymous Access)

Blob
(Anonymous read access for blobs only)

Container
(Anonymous read access for containers and blobs)

Access policy
images

💾 Save

Public access level ⓘ

Private (no anonymous access)   ∧

Private (no anonymous access)

Blob (anonymous read access for blobs only)

Container (anonymous read access for containers and blobs)

No results

➕ Add policy

Managing Access: SAS Overview

Shared Access Signature (SAS)

- It is a query string that we add on to the URL of a storage resource.

- The string informs Azure what access should be granted.

Account SAS Tokens

- Granted at the account level to grant permissions to services within the account.

Service SAS Tokens

- Grants access to a specific service within a Storage Account.

Encrypted

- Utilizes hash-based message authentication

SAS Breakdown

Storage Resource URI

https://slsasdemo.blob.core.windows.net/images/image.jpg

SAS Token

?sv=2017-07-29&ss=bfqt&srt=sco&sp=rwdlacup&se=2018-02-24T01:21:26Z&st=2018-02-23T17:21:26Z&spr=https&sig=dctAWsi39LncBNC1ZRn%2FQMjMMA5CPByLzagfsF7MVYc%3D

SAS Breakdown

- https://slsasdemo.blob.core.windows.net/images/image.jpg

- sv=2017-07-29

- ss=bfqt

- srt=sco

- sp=rwdlacup

- se=2018-02-24T01:21:26Z&st=2018-02-23T17:21:26Z

- spr=https

- sig=dctAWsi39LncBNC1ZRn%2FQMjMMA5CPByLzagfsF7MVYc%3D

| The Blob |
| Storage Service Version |
| Signed Services |
| Signed Resource Types |
| Signed Permission |
| Signed Expiry & Start |
| Signed Protocol |
| Signature |

LAB | Storage

Lab3-Storage

https://github.com/AHEAD-Labs/AzureInnovationDay

Operations and Monitoring

Azure Log Analytics

- Collects data from Azure IaaS, PaaS, and On-Prem resources
- Create Alerts or take action on Log Search query results
- Serves as base framework for existing and upcoming Azure Features

    - Azure Security Center relies on OMS

- Enhances Automation and Operational tasks within Azure environment

- Integration with SCOM and ITSM solutions

Log Analytics Architecture
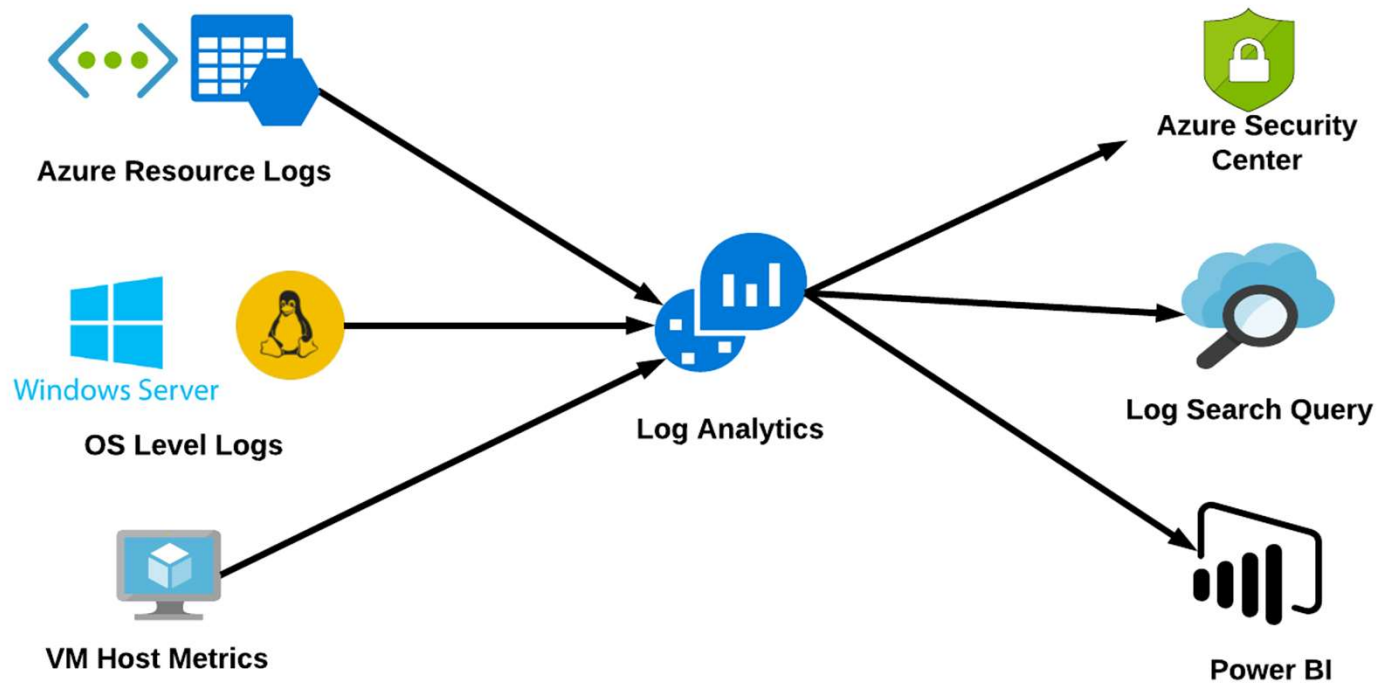
Log Analytics Solutions

- Solutions provide feature sets built on top of the data collected by Log Analytics.

Common Solutions
- Update Management
- Antimalware
- Change Tracking
- Network Monitoring
- Activity Log Analytics
- Security and Audit

OMS Solutions: Update Management

- Integrates with Azure Automation Account.
- Apply scheduled update times
- Target a computer or group of computers
- Blacklist specific update KB numbers
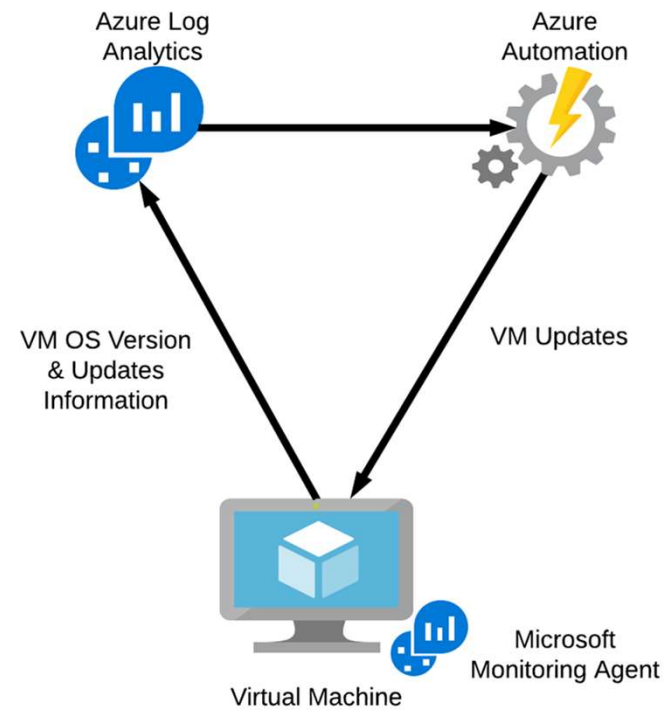
OMS Solutions: Update Management
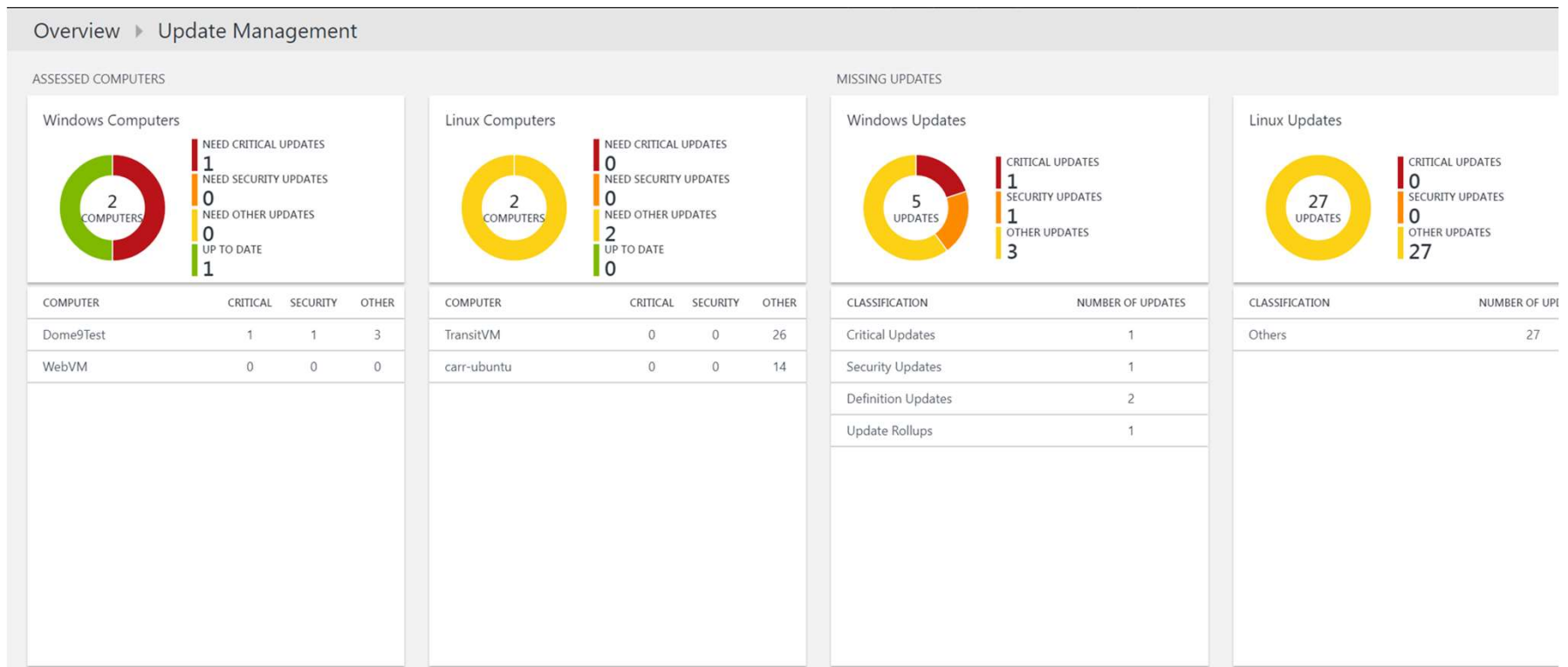
Security Center

Azure Security Center Overview

Centralized Policy Management	Continuous Security Assessment	Recommended Actions
Advanced Cloud Defenses	Prioritized Alerts and Incidents	Integrated Security Solutions

Lab4-Monitoring

https://github.com/AHEAD-Labs/AzureInnovationDay

Automation

ARM Overview

ARM Templates Overview

```json
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
  },
  "variables": {
  },
  "resources": [
    {
      "name": "[concat('storage', uniqueString(resourceGroup().id))]",
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2016-01-01",
      "sku": {
        "name": "Standard_LRS"
      },
      "kind": "Storage",
      "location": "North Central US",
      "tags": {},
      "properties": {}
    }
  ],
  "outputs": { }
}
```

Resource
(E.g. Storage Account)

- Apply Infrastructure as Code

- Download templates from Azure Portal

- Author new templates

- Use Quickstart templates, provided by Microsoft

AHEAD

Quickstart Templates

https://azure.microsoft.com/en-us/resources/templates/

https://github.com/Azure/azure-quickstart-templates

ARM File Types

ARM Template File	ARM Template Parameter File	Deployment Scripts
Describe the configuration of your infrastructure via a JSON file	Separate your parameters (optional)	E.g. PowerShell for Deployment

ARM Template Constructs

Parameters	Variables	Resources	Outputs
Define the inputs you want to pass into the ARM template during deployment.	Values that you can use throughout your template. Used to simplify your template by creating reuse of values.	Define the resources you wish to deploy or update.	Specify values that are returned after the ARM deployment is completed.

Lab5-Automation

https://github.com/AHEAD-Labs/AzureInnovationDay

Thank You

AHEAD®

Experts in Enterprise Cloud

thinkahead.com