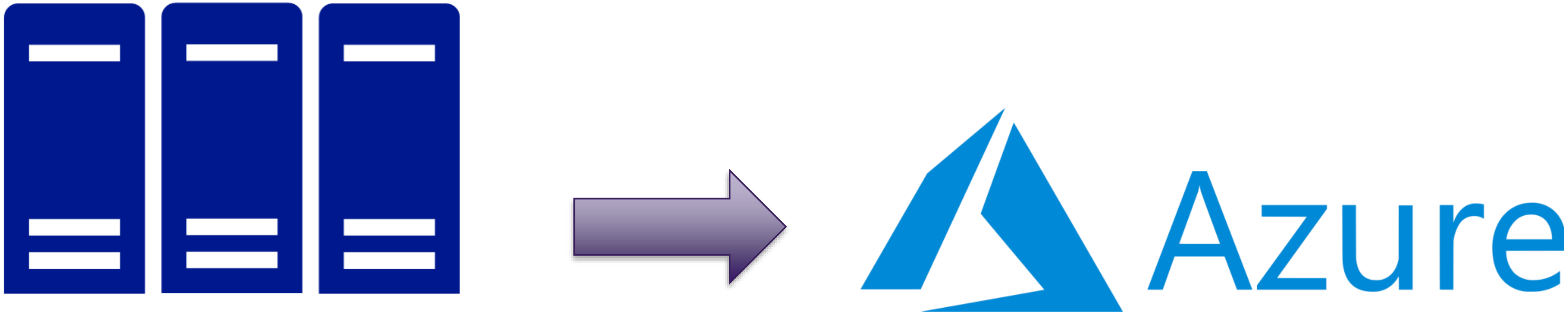
AZ-103: Azure Administrator

SKYLINES

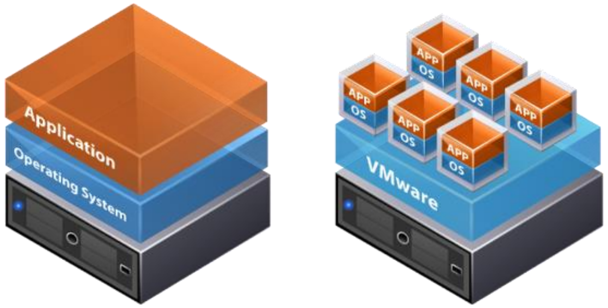
ACADEMY

Azure Quick Overview

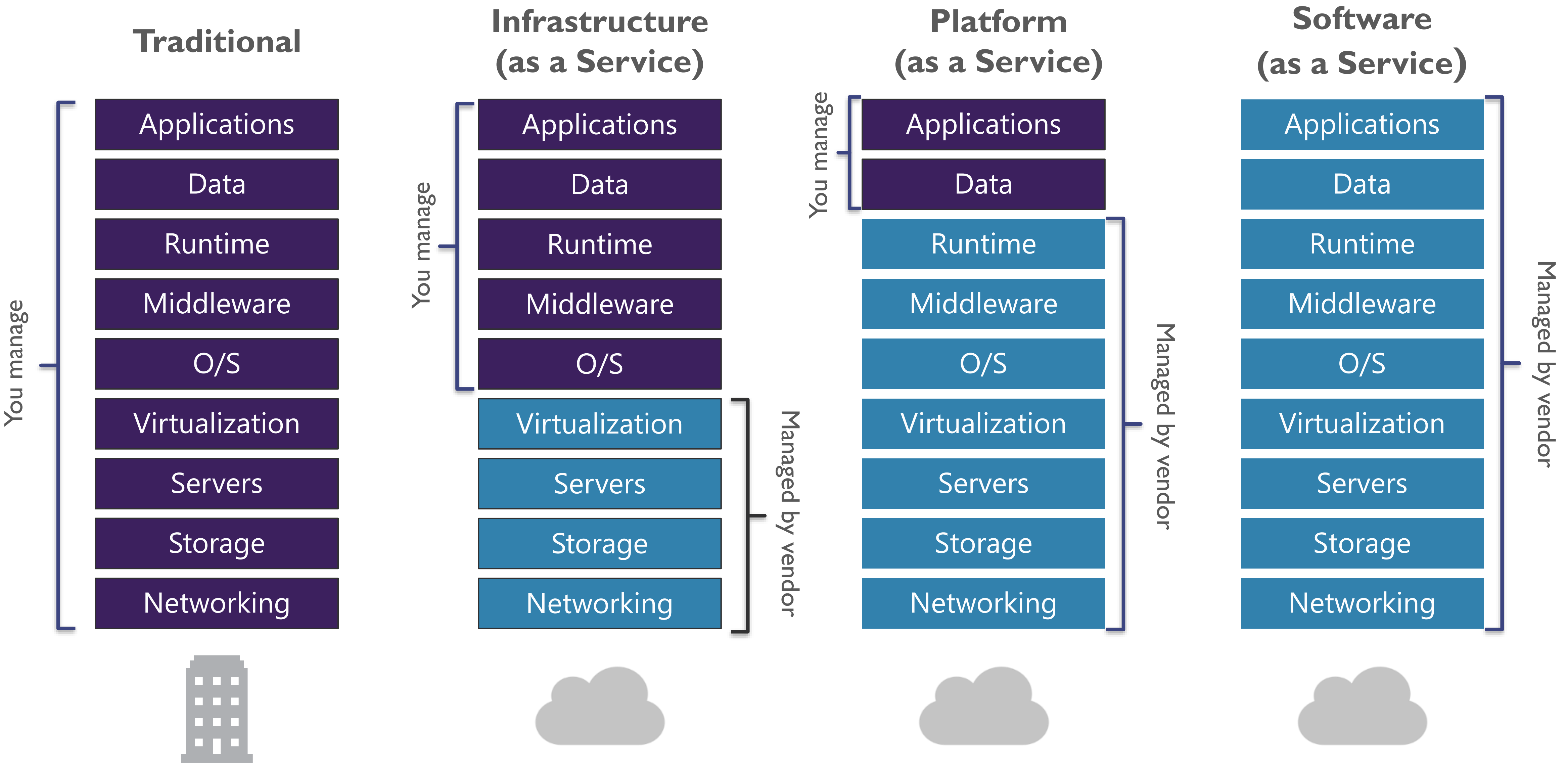
Cloud Computing Overview



Traditional Datacenter



Cloud Service Models



Traditional

You manage

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

Infrastructure (as a Service)

You manage

Applications
Data
Runtime
Middleware
O/S

Managed by vendor

Virtualization
Servers
Storage
Networking

Platform (as a Service)

You manage

Applications
Data

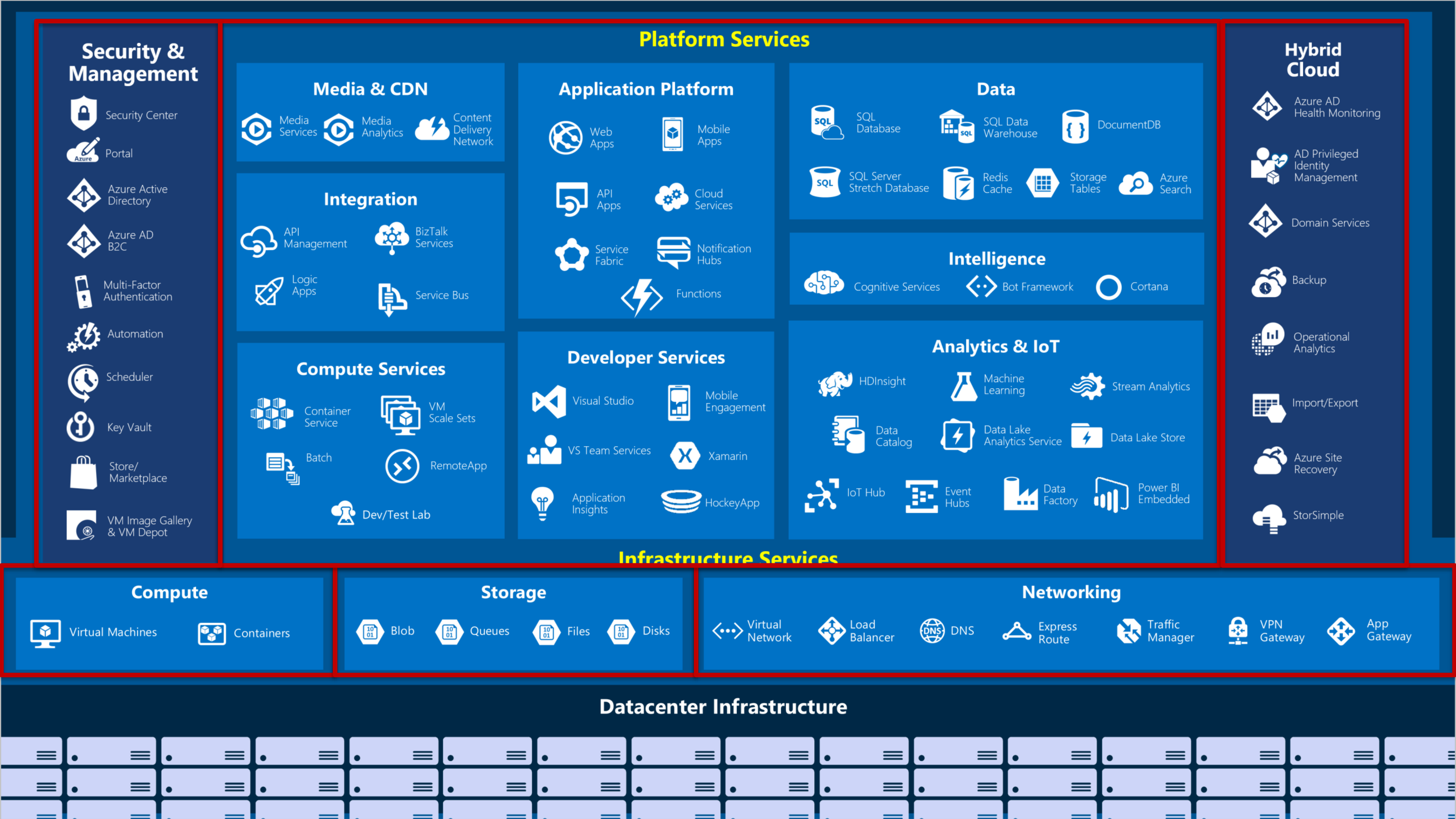
Managed by vendor

Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

Software (as a Service)

Managed by vendor

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking



Security & Management

- Security Center
- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Store/ Marketplace
- VM Image Gallery & VM Depot

Platform Services

Media & CDN

- Media Services
- Media Analytics
- Content Delivery Network

Integration

- API Management
- BizTalk Services
- Logic Apps
- Service Bus

Compute Services

- Container Service
- VM Scale Sets
- Batch
- RemoteApp
- Dev/Test Lab

Application Platform

- Web Apps
- Mobile Apps
- API Apps
- Cloud Services
- Service Fabric
- Notification Hubs
- Functions

Developer Services

- Visual Studio
- Mobile Engagement
- VS Team Services
- Xamarin
- Application Insights
- HockeyApp

Data

- SQL Database
- SQL Data Warehouse
- DocumentDB
- SQL Server Stretch Database
- Redis Cache
- Storage Tables
- Azure Search

Intelligence

- Cognitive Services
- Bot Framework
- Cortana

Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Catalog
- Data Lake Analytics Service
- Data Lake Store
- IoT Hub
- Event Hubs
- Data Factory
- Power BI Embedded

Hybrid Cloud

- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Operational Analytics
- Import/Export
- Azure Site Recovery
- StorSimple

Infrastructure Services

Compute

- Virtual Machines
- Containers

Storage

- Blob
- Queues
- Files
- Disks

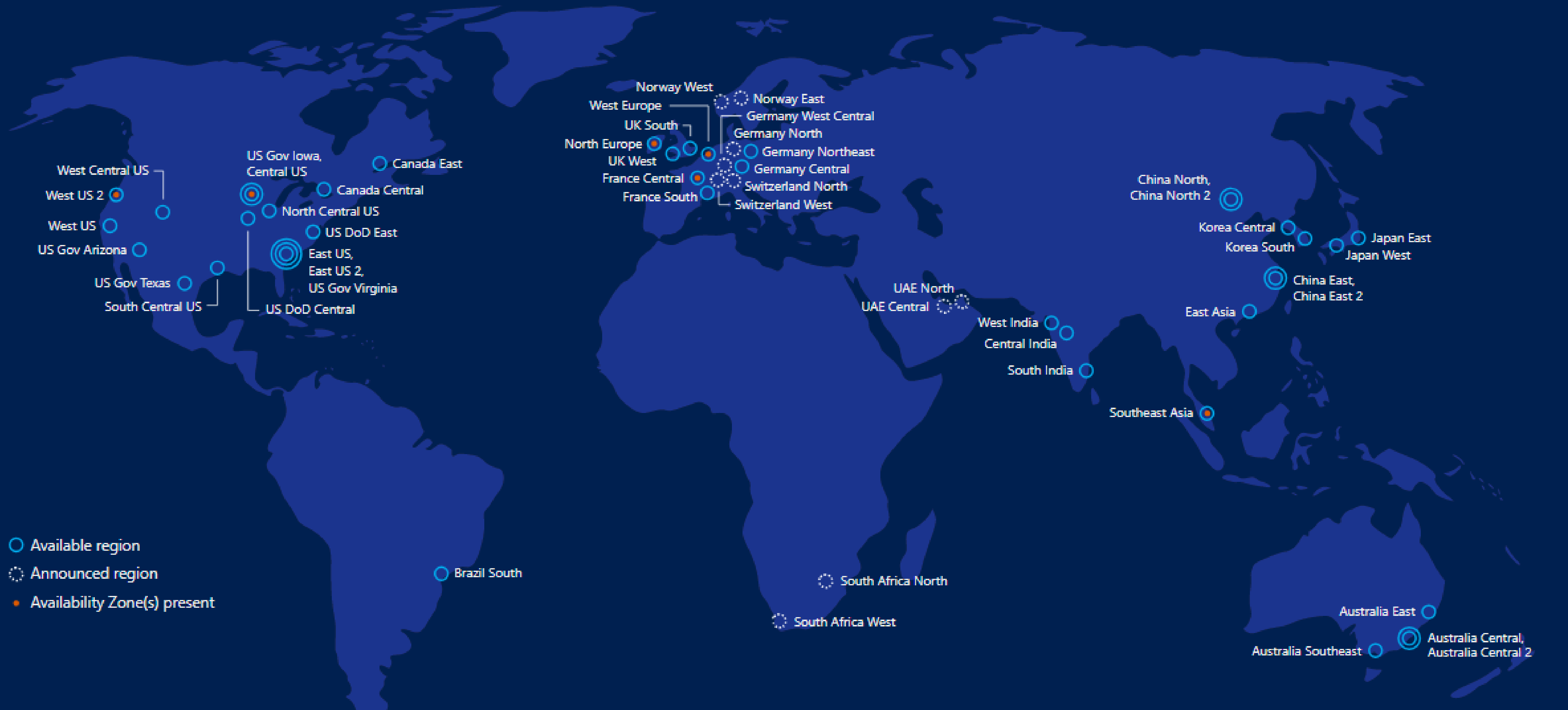
Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

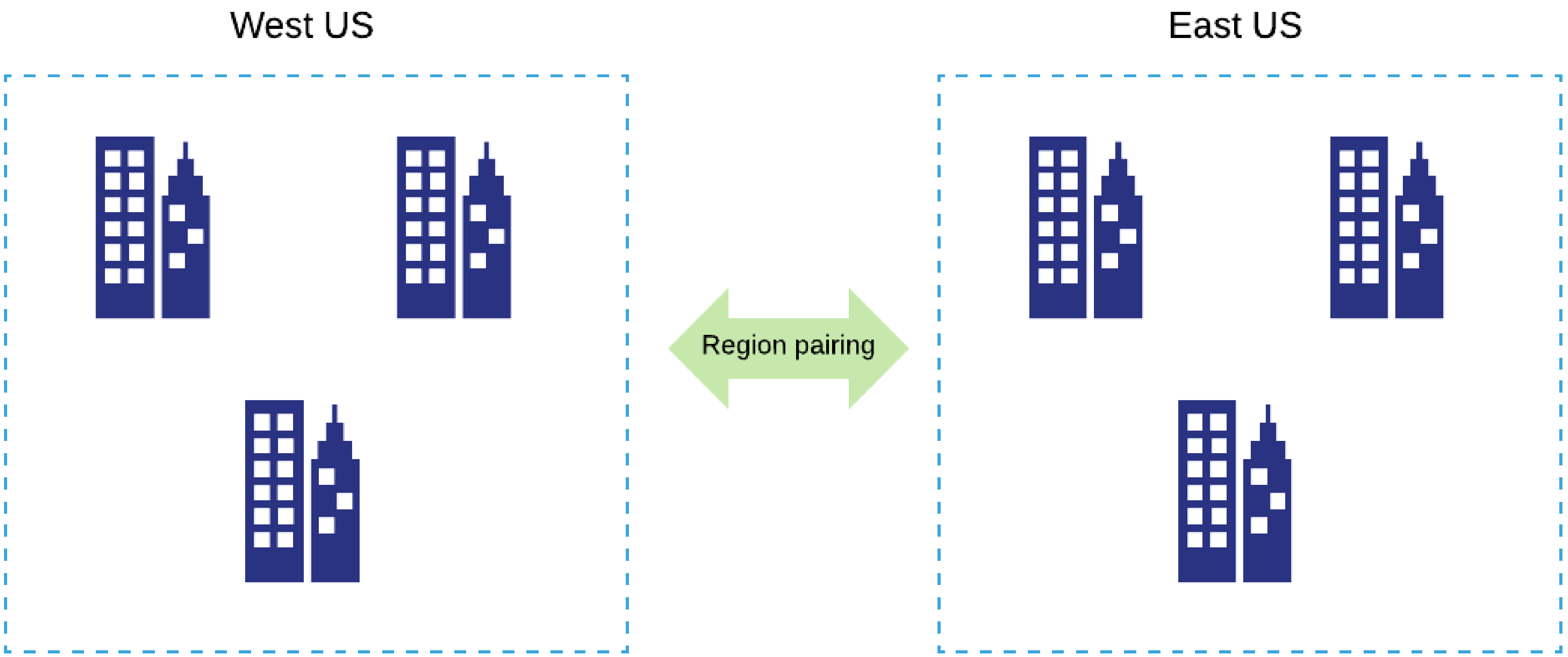
Datacenter Infrastructure

54 regions worldwide

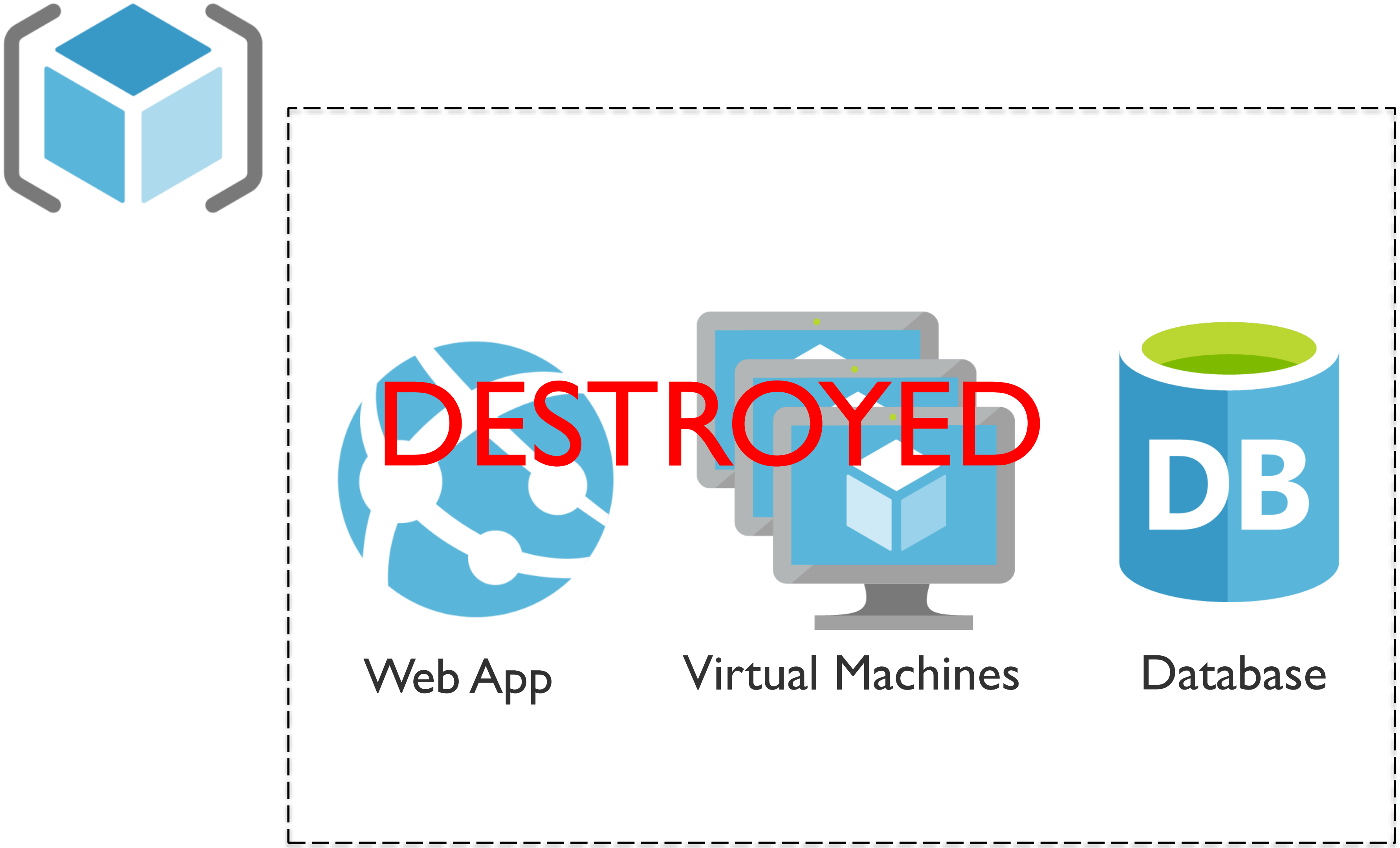
140 available in 140 countries



Region Pairs



Resource Group Overview



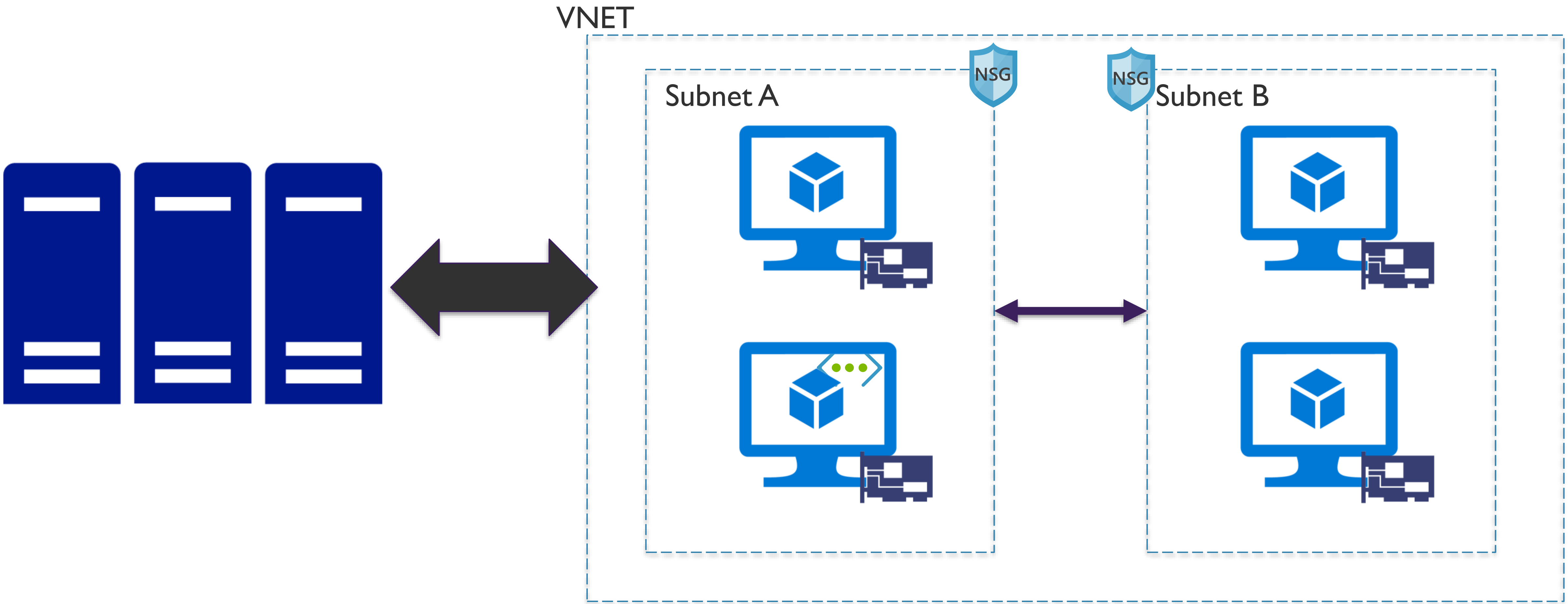
DESTROYED

Web App

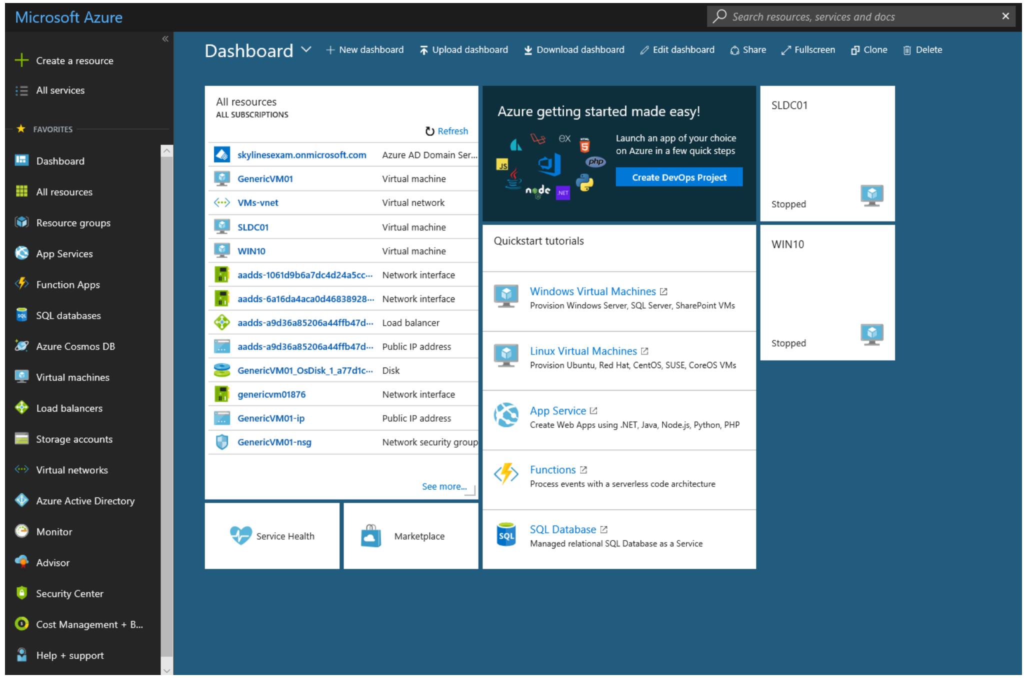
Virtual Machines

Database

Networking



Accessing Azure



All resources
ALL SUBSCRIPTIONS

skylinesexam.onmicrosoft.com	Azure AD Domain Ser...
GenericVM01	Virtual machine
VMs-vnet	Virtual network
SLDC01	Virtual machine
WIN10	Virtual machine
aadds-1061d9b6a7dc4d24a5cc...	Network interface
aadds-6a16da4aca0d46838928...	Network interface
aadds-a9d36a85206a44ffb47d...	Load balancer
aadds-a9d36a85206a44ffb47d...	Public IP address
GenericVM01_OsDisk_1_a77d1c...	Disk
genericvm01876	Network interface
GenericVM01-ip	Public IP address
GenericVM01-nsg	Network security group

Azure getting started made easy!

Launch an app of your choice on Azure in a few quick steps

SLDC01

WIN10

Quickstart tutorials

Windows Virtual Machines
Provision Windows Server, SQL Server, SharePoint VMs

Linux Virtual Machines
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs

App Service
Create Web Apps using .NET, Java, Node.js, Python, PHP

Functions
Process events with a serverless code architecture

SQL Database
Managed relational SQL Database as a Service

http://portal.azure.com

PowerShell and Azure CLI

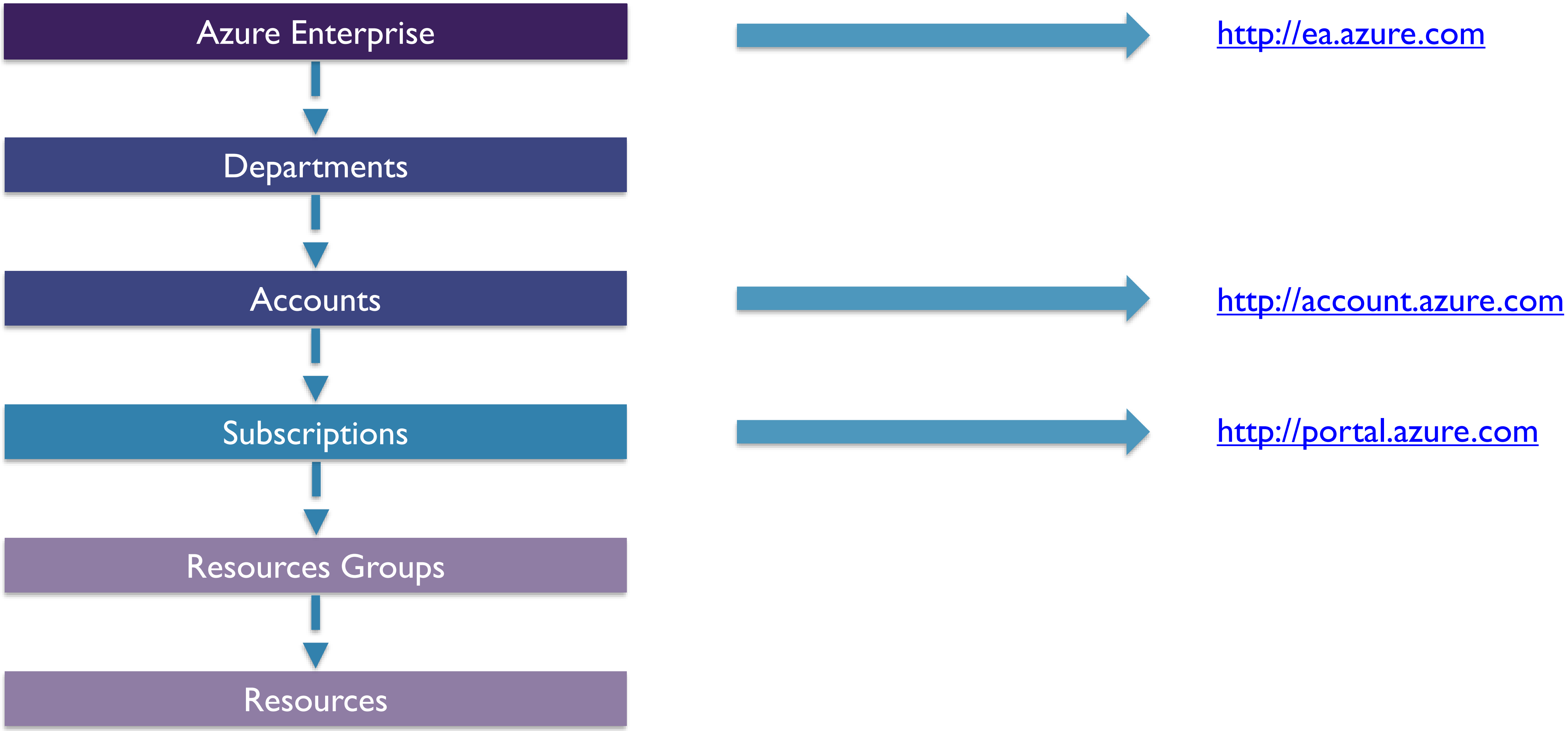
SKYLINES
ACADEMY

Module:
Manage Azure Subscriptions

SKYLINES

ACADEMY

Azure Account Hierarchy

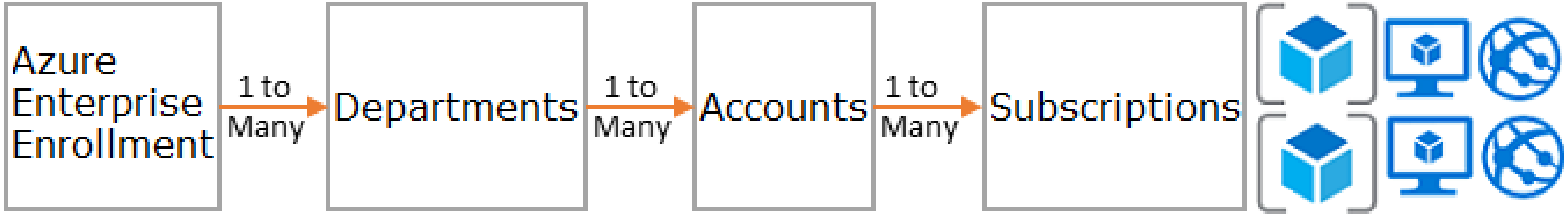


http://ea.azure.com

http://account.azure.com

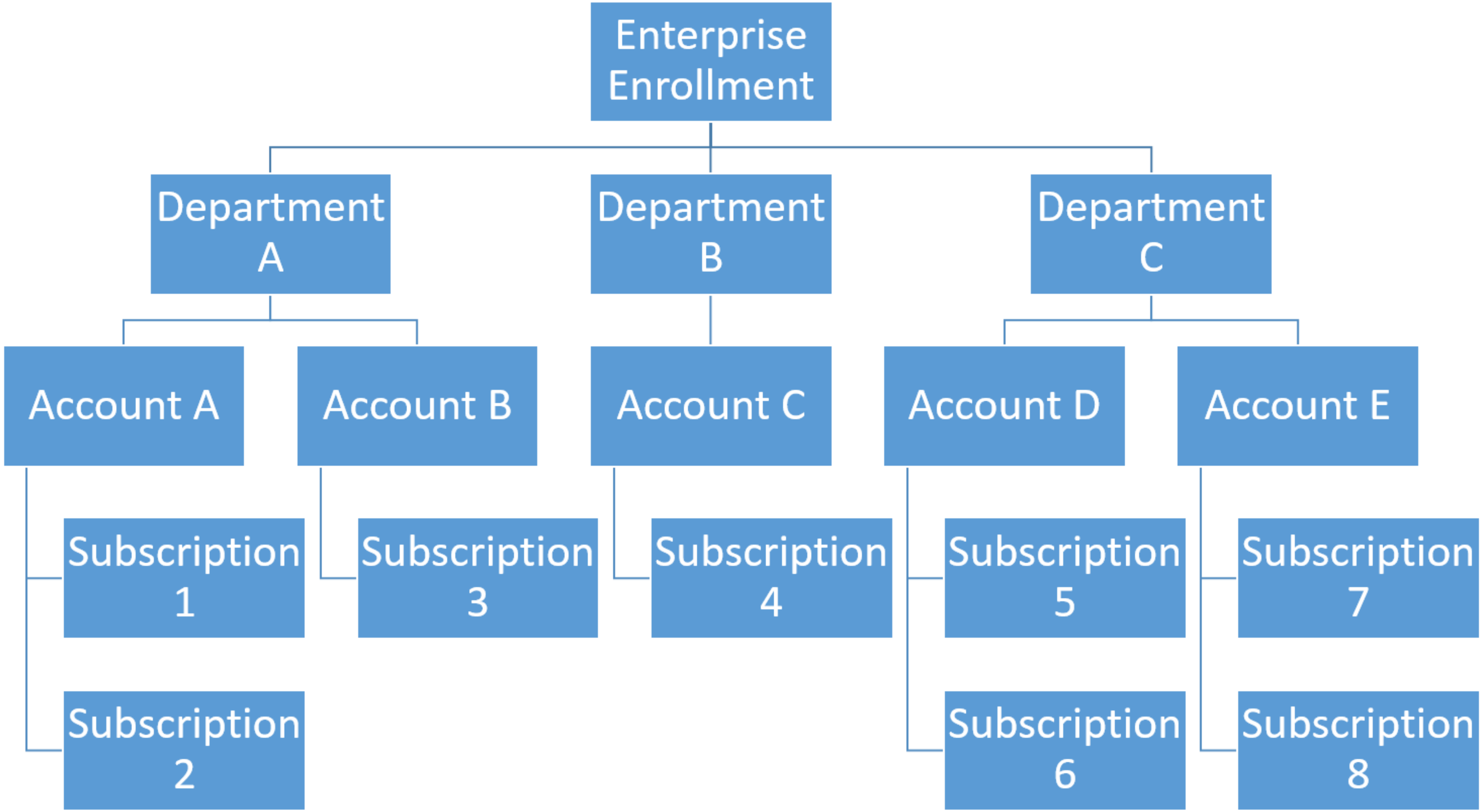
http://portal.azure.com

Account to Subscription Relationships

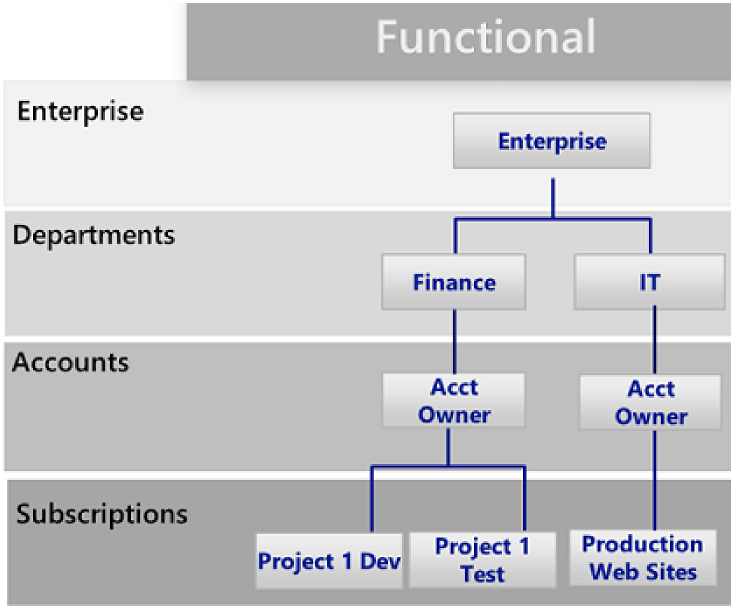


Azure Enterprise Enrollment → 1 to Many → Departments → 1 to Many → Accounts → 1 to Many → Subscriptions

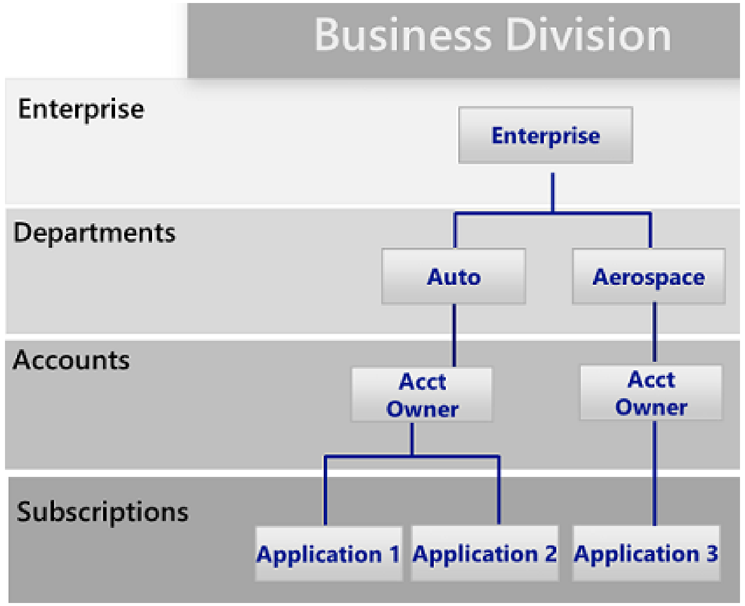
Enterprise Hierarchy Example



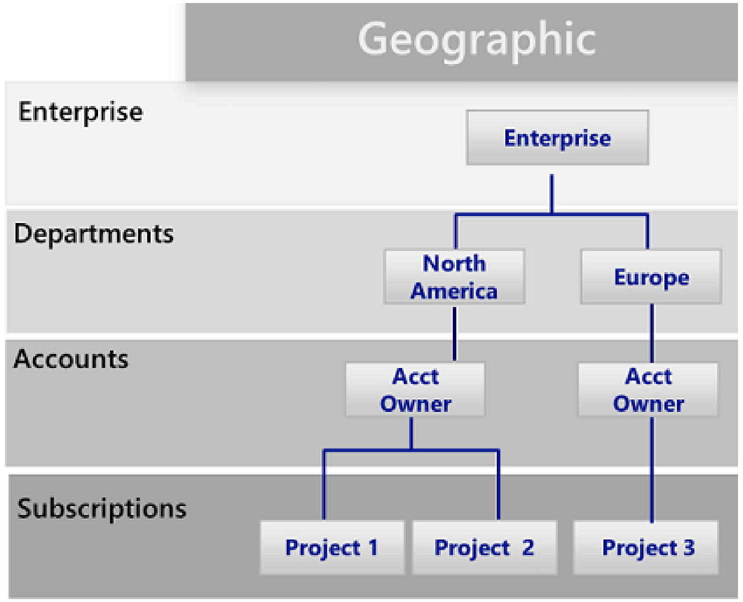
Common Scenarios



Functional



Business Division



Geographic

EA Breakdown

	Enterprise Admin	Department Admin	Account Owner	Service Admin
Add other admins	Enterprise Admins, Department Admins, and Account Owners	Account Owners	Add Service Admins	No
Departments	Add/Edit Departments	Edit Department	X	X
Add or associate accounts to the enrollment	Yes	Yes – to the department	No	No
Add Subscriptions	No – but can add themselves as AO	No	Yes	No
View usage and charges data	Across all Accounts and Subscriptions	Across Department	Across Account	No
View remaining balances	Yes	No	No	No

Module:
Analyze Resource Usage and Consumption

Azure Monitoring Overview

Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation, and performance of your systems.

Query and Analyze Logs

Logs are activity logs, diagnostic logs, and telemetry from monitoring solutions;Analytics queries help with troubleshooting and visualizations.

Setup & Alert Actions

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

Log Analytics Key Features

SKYLINES
ACADEMY

Central Role in Monitoring

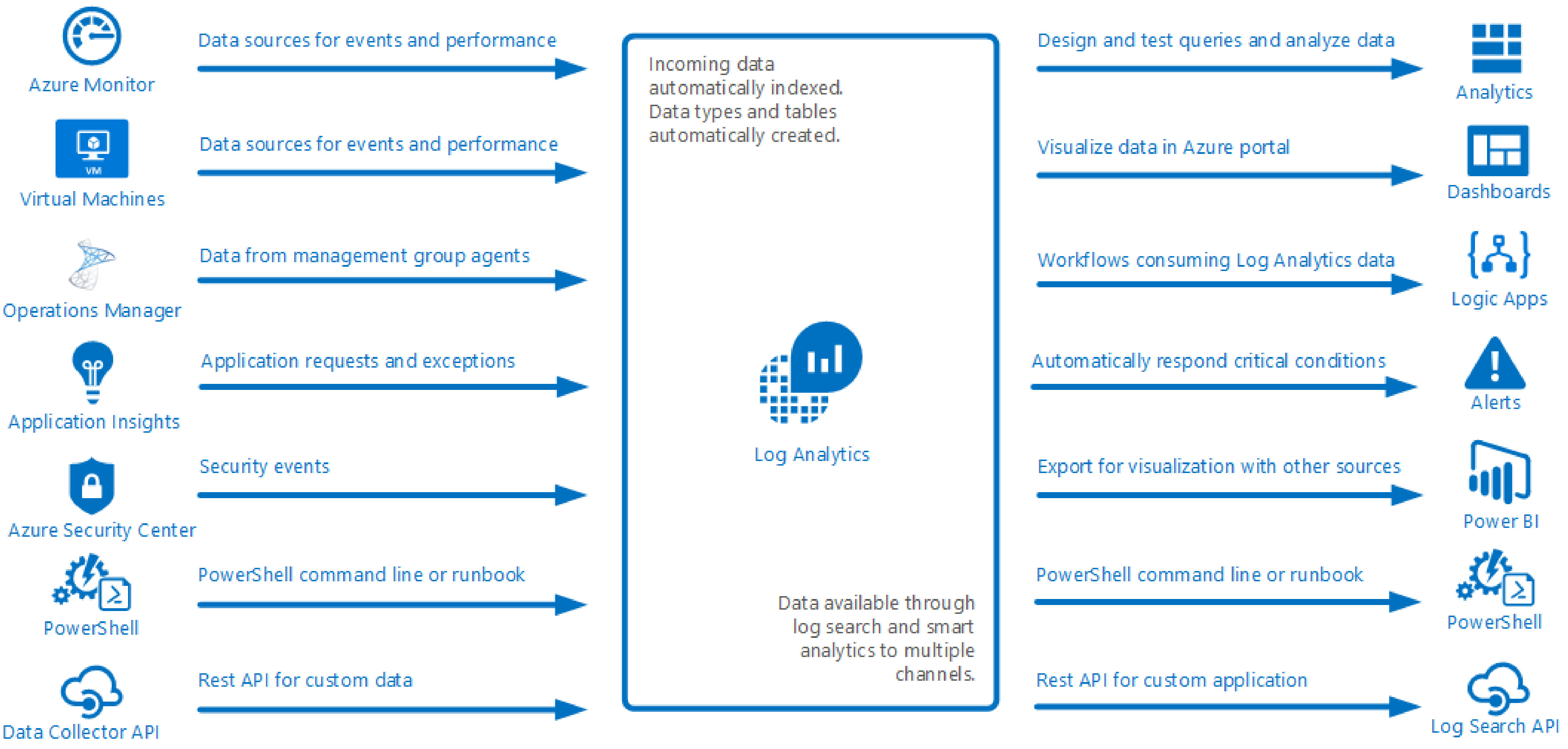
Data Sources

Other Log Analytics Sources (Security Center and App Insights)

Search Queries

Output Options

Log Search Use Cases



Azure Monitor — Data sources for events and performance

Virtual Machines — Data sources for events and performance

Operations Manager — Data from management group agents

Application Insights — Application requests and exceptions

Azure Security Center — Security events

PowerShell — PowerShell command line or runbook

Data Collector API — Rest API for custom data

Incoming data automatically indexed. Data types and tables automatically created.

Log Analytics

Data available through log search and smart analytics to multiple channels.

Design and test queries and analyze data — Analytics

Visualize data in Azure portal — Dashboards

Workflows consuming Log Analytics data — Logic Apps

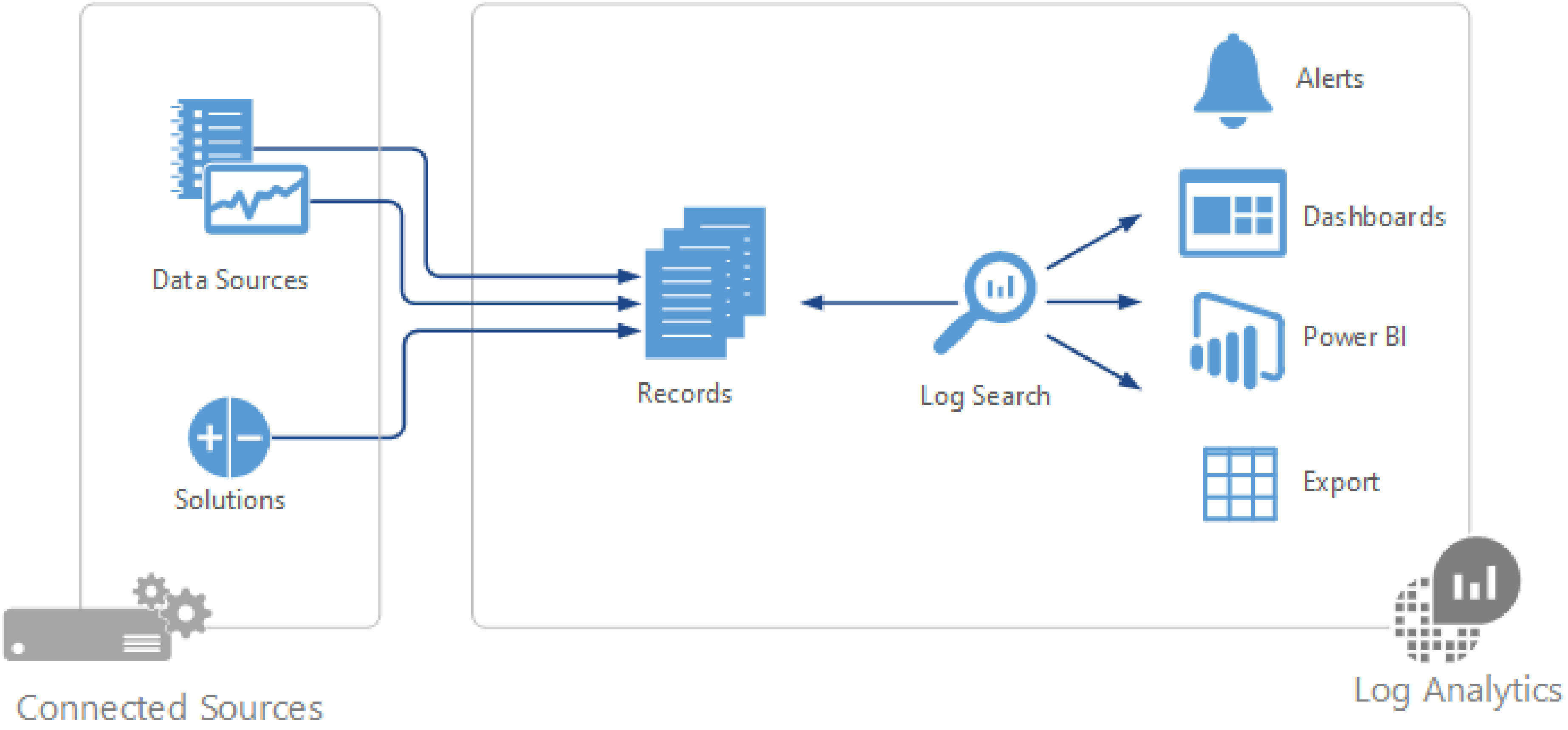
Automatically respond critical conditions — Alerts

Export for visualization with other sources — Power BI

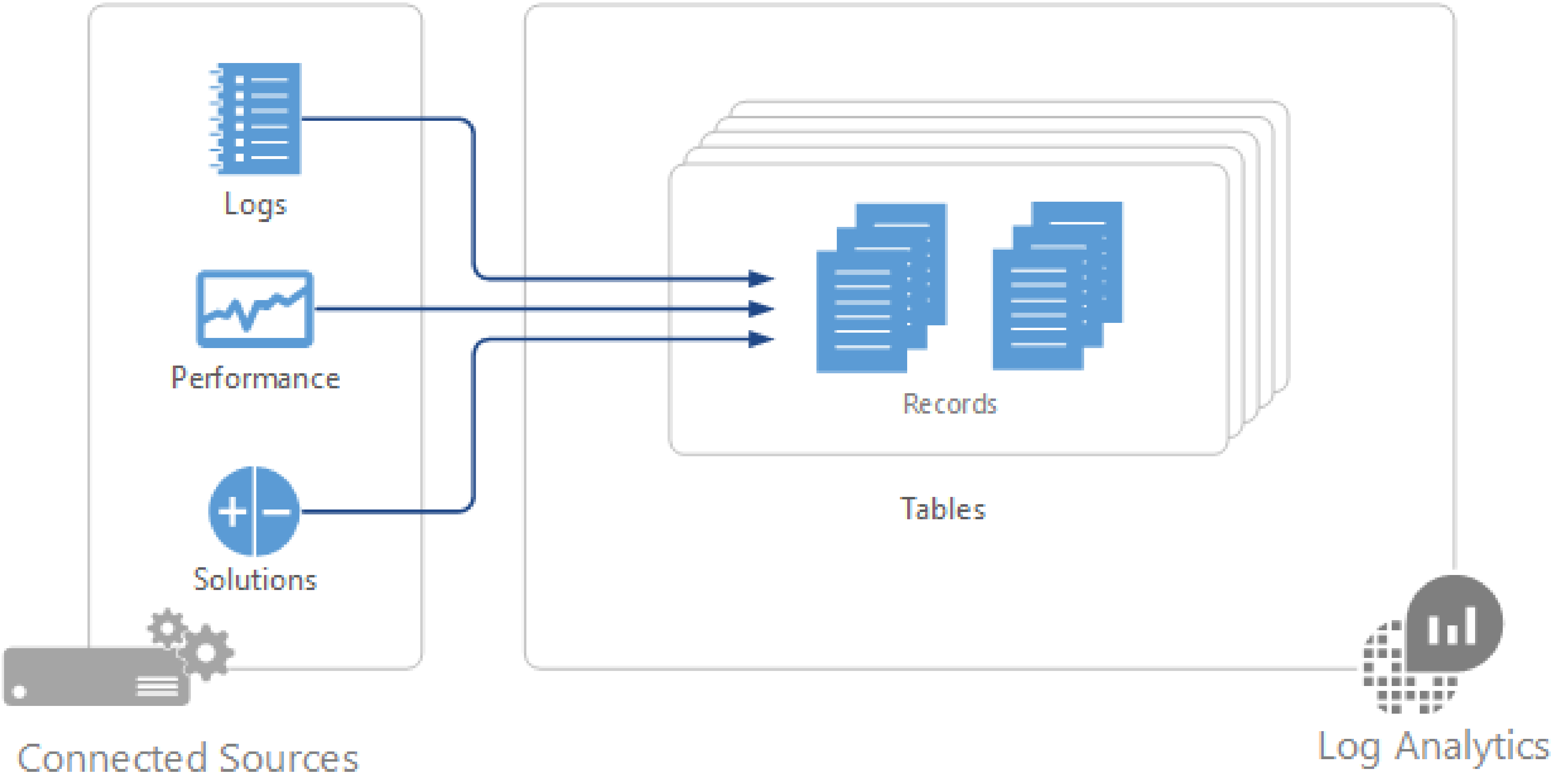
PowerShell command line or runbook — PowerShell

Rest API for custom application — Log Search API

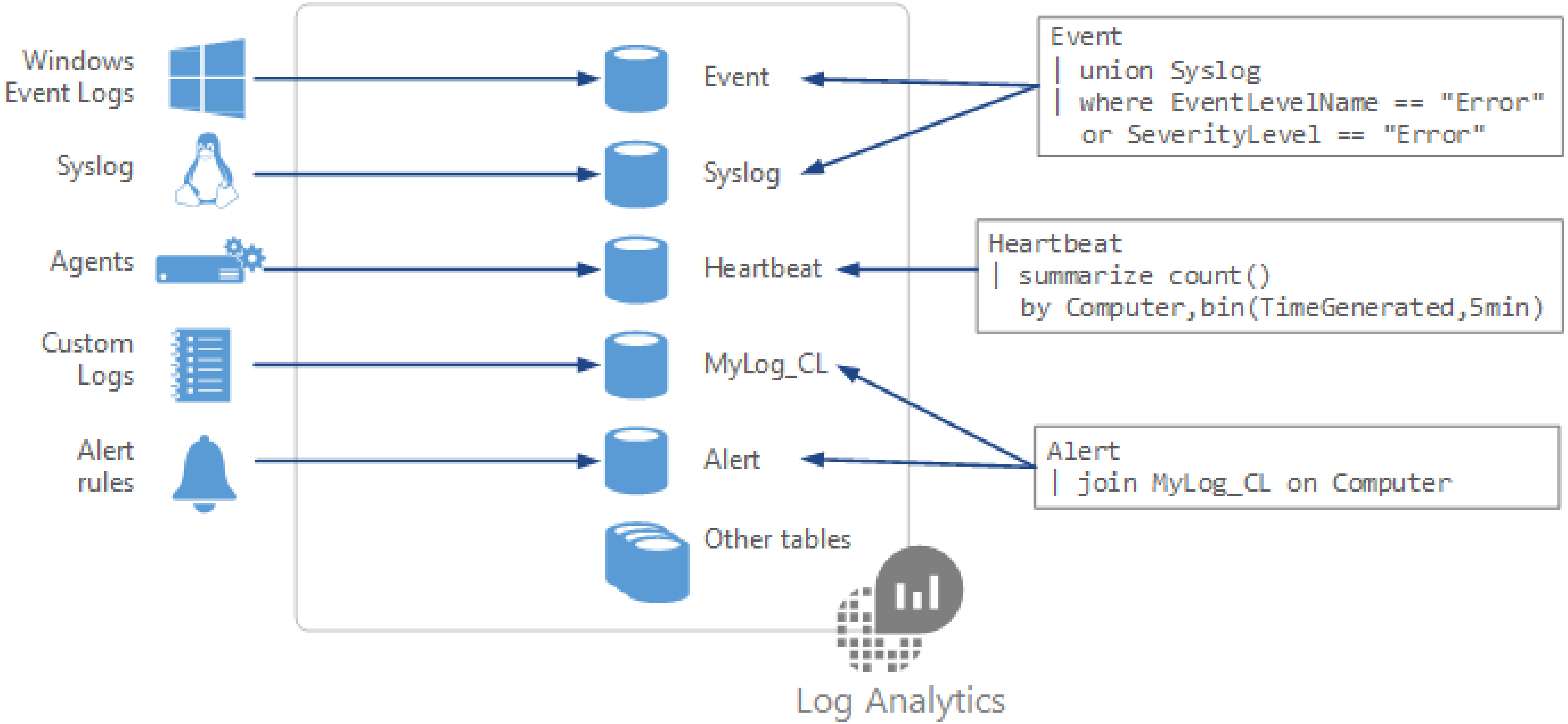
Log Analytics Architecture



Data Sources



Data Organization



```
Event
| union Syslog
| where EventLevelName == "Error"
  or SeverityLevel == "Error"
```

```
Heartbeat
| summarize count()
  by Computer,bin(TimeGenerated,5min)
```

```
Alert
| join MyLog_CL on Computer
```

Summary Data Sources

Data Source	Event Type	Description
Custom logs	<LogName>_CL	Text files on Windows or Linux agents containing log information.
Windows Event logs	Event	Events collected from the event logon Windows computers.
Windows Performance counters	Perf	Performance counters collected from Windows computers.
Linux Performance counters	Perf	Performance counters collected from Linux computers.
IIS logs	W3CIISLog	Internet Information Services logs in W3C format.
Syslog	Syslog	Syslog events on Windows or Linux computers.

Search Query Fundamentals

- Start with the source table (e.g. Event)
- Follow on with a series of operators
- Separate out additional operations by using pipe |
- Join other tables and workspaces using "union"

https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-tutorial-viewdata

Module:
Manage Resource Groups

SKYLINES ACADEMY

Azure Resource Locks

- Mechanism for locking down resources you want to ensure have an extra layer of protection before they can be deleted
- 2 options available:
  - **CanNotDelete:** Authorized users can read and modify but not delete the resource
  - **ReadOnly:** Authorized users can read the resource but cannot update or delete

Azure Policies

Enforce Governance

Built-in or Custom Code

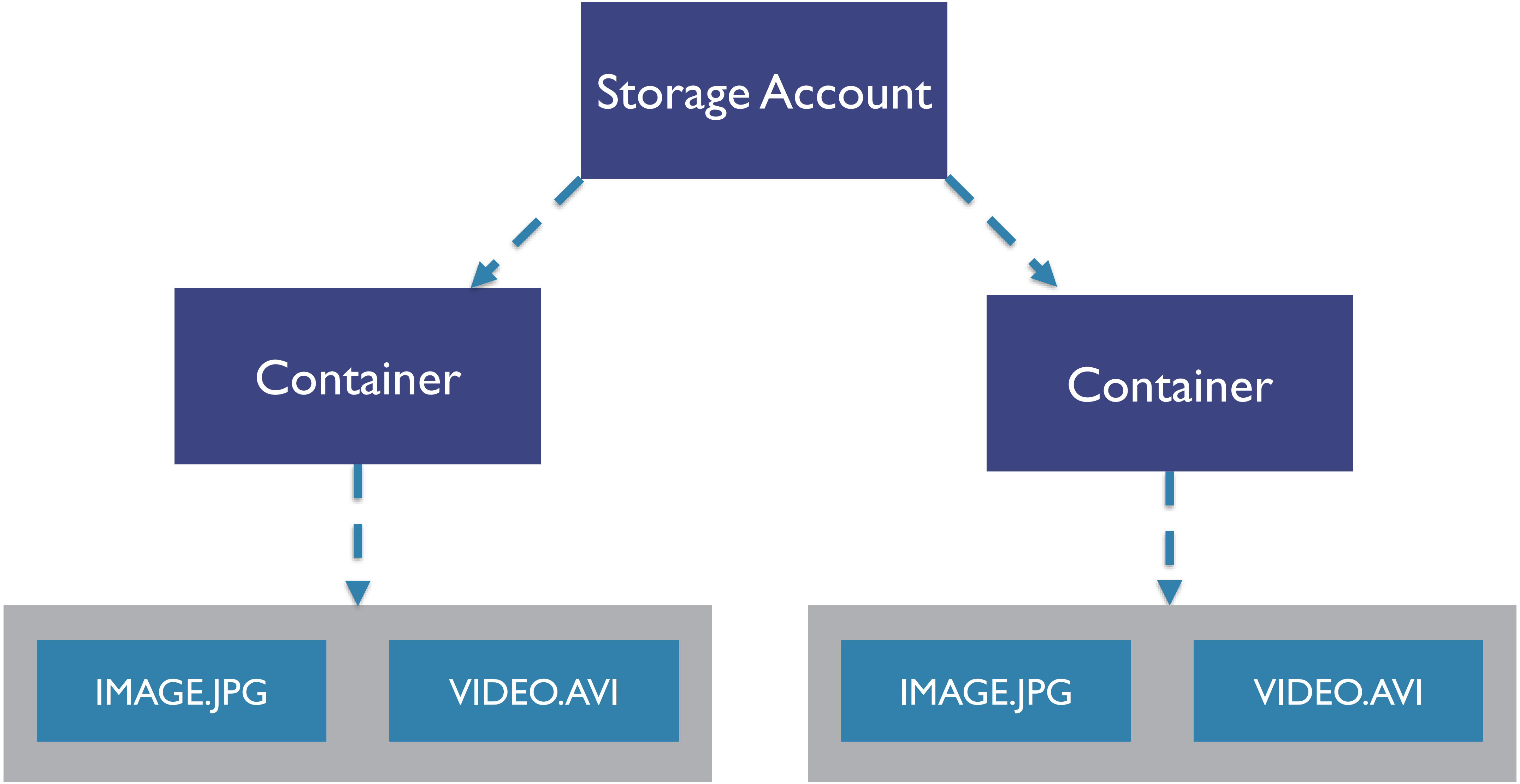
Assigned to Subscriptions or Resource Groups

Create > Assign

Module:
Create and Configure Storage

SKYLINES ACADEMY

Azure Blob Storage Overview



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

Storage Tiers

Hot

- Higher storage costs
- Lower access costs

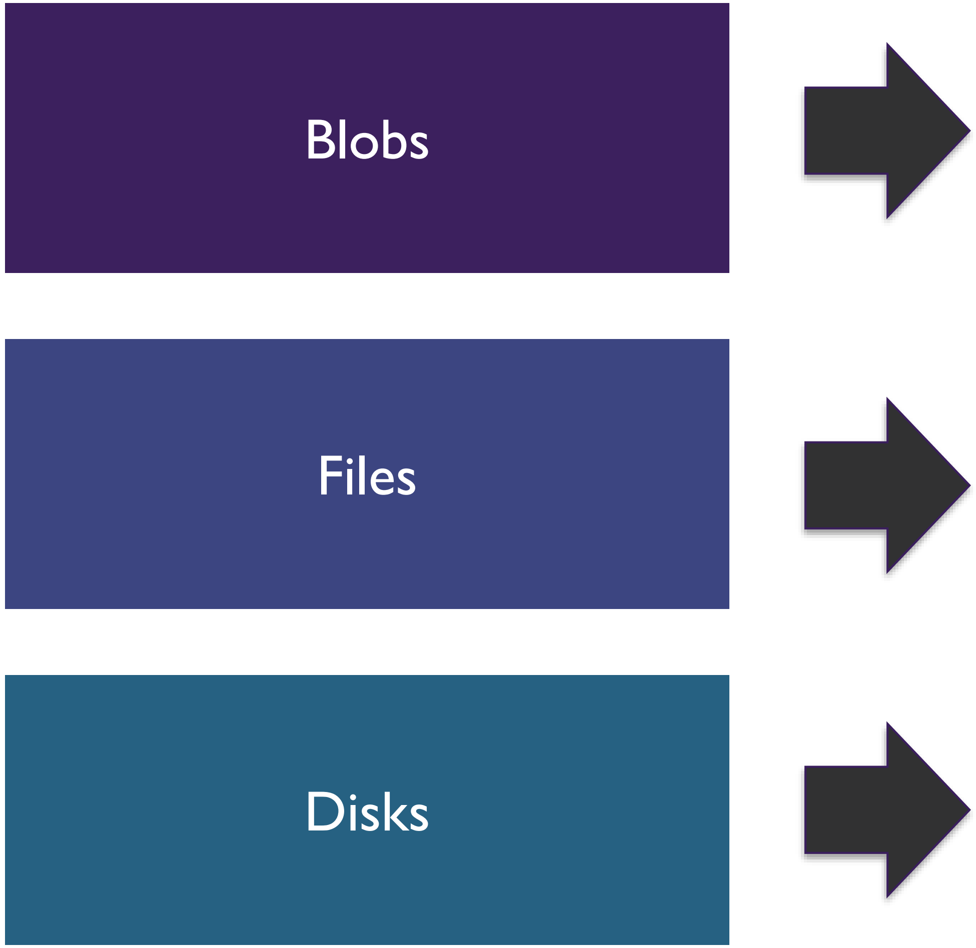
Cold

- 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

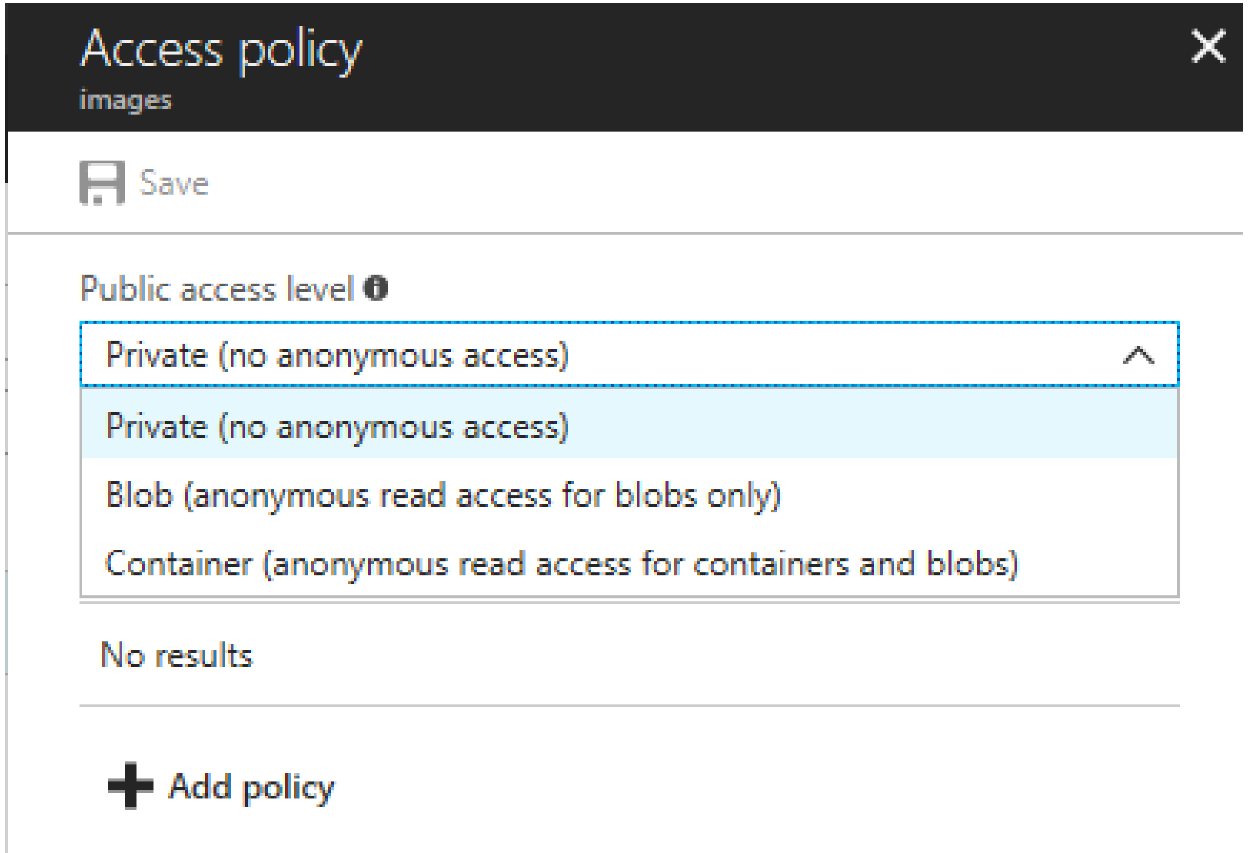
- Do not need to access the data outside of the VM
- Lift-and-shift of machines from on-premises
- Disk expansion for application installations

Manage 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

SKYLINES ACADEMY

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 (continued)

https://slsasdemo.blob.core.windows.net/images/image.jpg	The Blob
sv=2017-07-29	Storage Service Version
ss=bfqt	Signed Services
srt=sco	Signed Resource Types
sp=rwdlacup	Signed Permission
se=2018-02-24T01:21:26Z&st=2018-02-23T17:21:26Z	Signed Expiry & Start
spr=https	Signed Protocol
sig=dctAWsi39LncBNC1ZRn%2FQMjMMA5CPByLzagfsF7MVYc%3D	Signature

Stored Access Policies

- Method for controlling SAS
- Group shared access signatures and provide additional restrictions
- Can be used to change the start time, expiry time, permissions, or revoke it after it has been issued
- Only supported on service SAS
  - Blob containers
  - File shares
  - Queues
  - Tables

Custom Domains

Resource Type	Default URL	Custom Domain URL
Storage account	http://mystorageaccount.blob.core.windows.net	http://skylinesacademy.com
Blob	http://mystorageaccount.blob.core.windows.net/mycontainer/myblob	http://skylinesacademy.com/mycontainer/myblob
Root container	http://mystorageaccount.blob.core.windows.net/mycontainer	http://skylinesacademy.com/mycontainer

Custom Domain Mapping

Create a CNAME record with your DNS provider that points from…

1. *Your domain*

- Such as www.skylinesacademy.com to sldscdemo.blob.core.windows.net.
- This method is simpler, but results in a brief downtime while Azure verifies the domain registration.

2. *The ”asverify” subdomain*

- Such as as verify.skylinesacademy.com to asverify.sldscdemo.blob.core.windows.net.
- After this step completes, you can create a CNAME record that points to sldscdemo.blob.core.windows.net.
- This method does not incur any downtime.
- To use this method, select the "Use Indirect CNAME Validation" checkbox.

Module:
Import and Export Data to Azure

SKYLINES ACADEMY

Azure Import/Export Use Cases

Data Migration to Cloud

Move large amounts of data to Azure quickly.

e.g. Large migration from your datacenter.

Content Distribution

Sending data to customer sites.

Backup

Backing up your on-premises data to store it in Azure.

Data Recovery

Recover data from storage and send back to your on-premises datacenter.

Import/Export Components

SKYLINES ACADEMY

Import/Export Service

- Accessed via the Azure Portal
- Used to track data import (upload) jobs
- Used to track data export (download) jobs

Import/Export Components

- Command line tool for:
  - Preparing disk drives that are shipped
  - Copying data to your drive
  - Encrypts data with BitLocker
  - Generates drive journal files
  - Determines number of drives
- Use V1 for blob and V2 for files

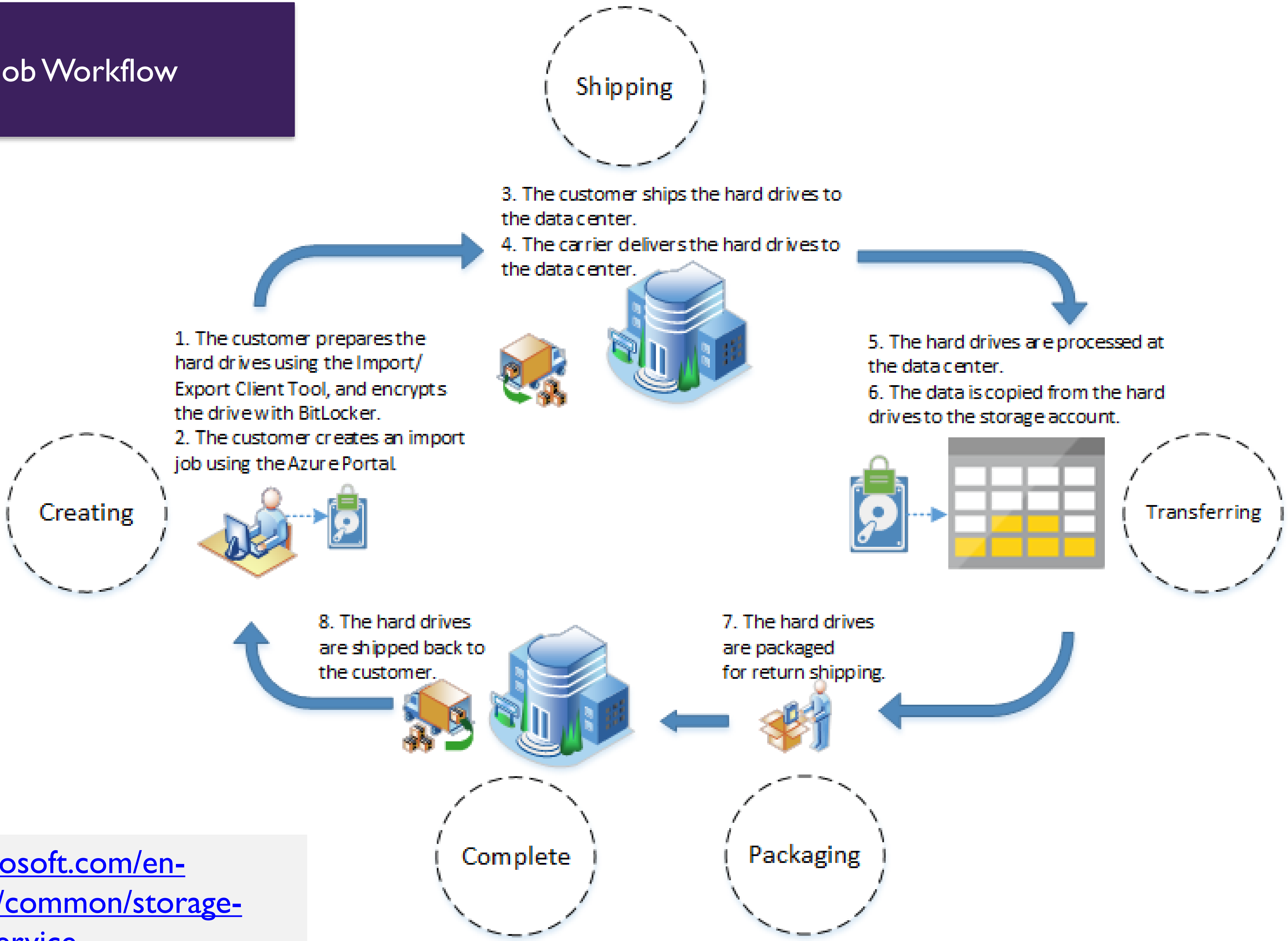
Import/Export Components

Disk Drives

- HDDs
- SSDs
- Import Jobs:You ship drives containing your data.
- Export Jobs:You ship empty drives.

Supported Disks:
https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements#supported-hardware

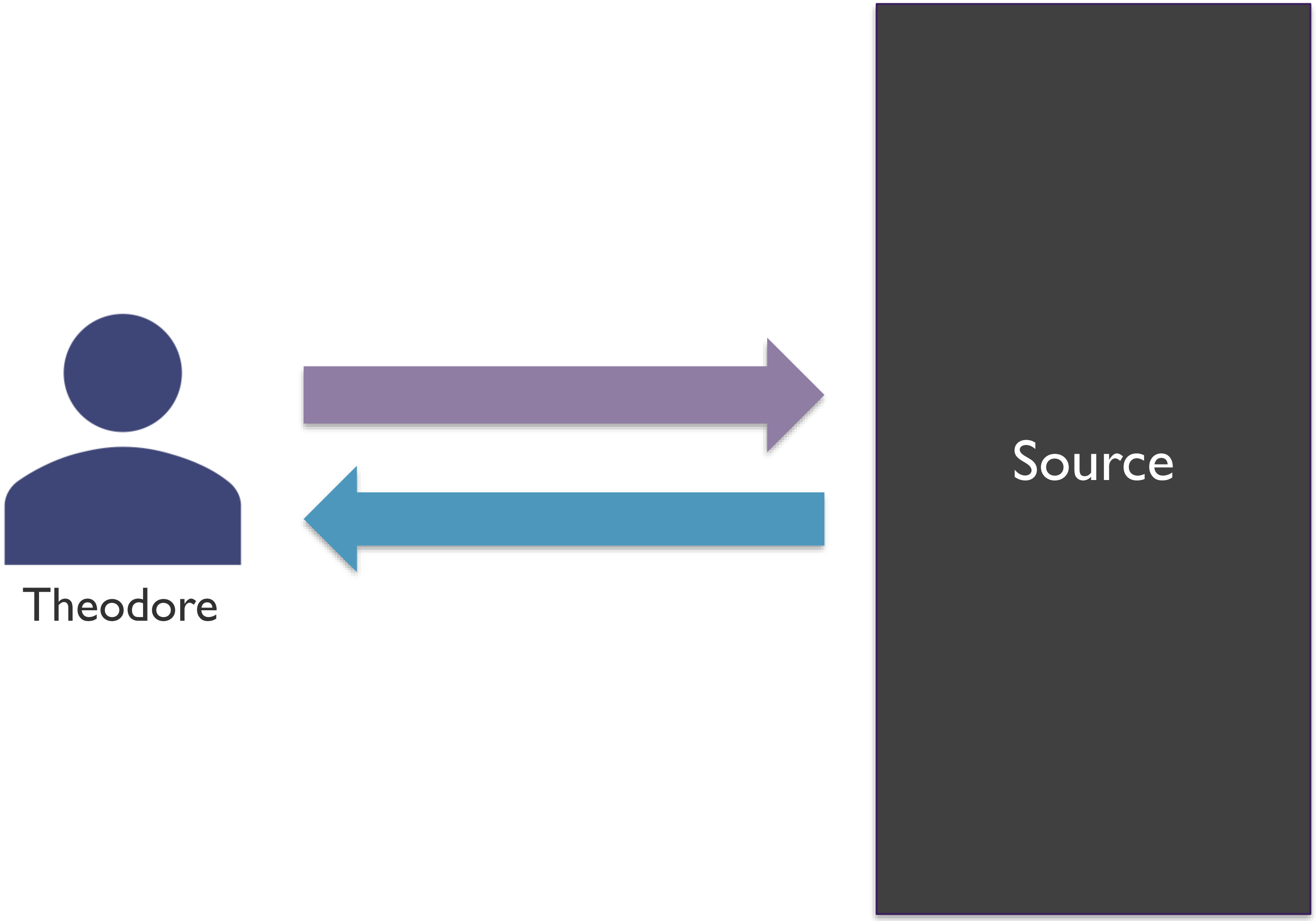
Import Job Workflow



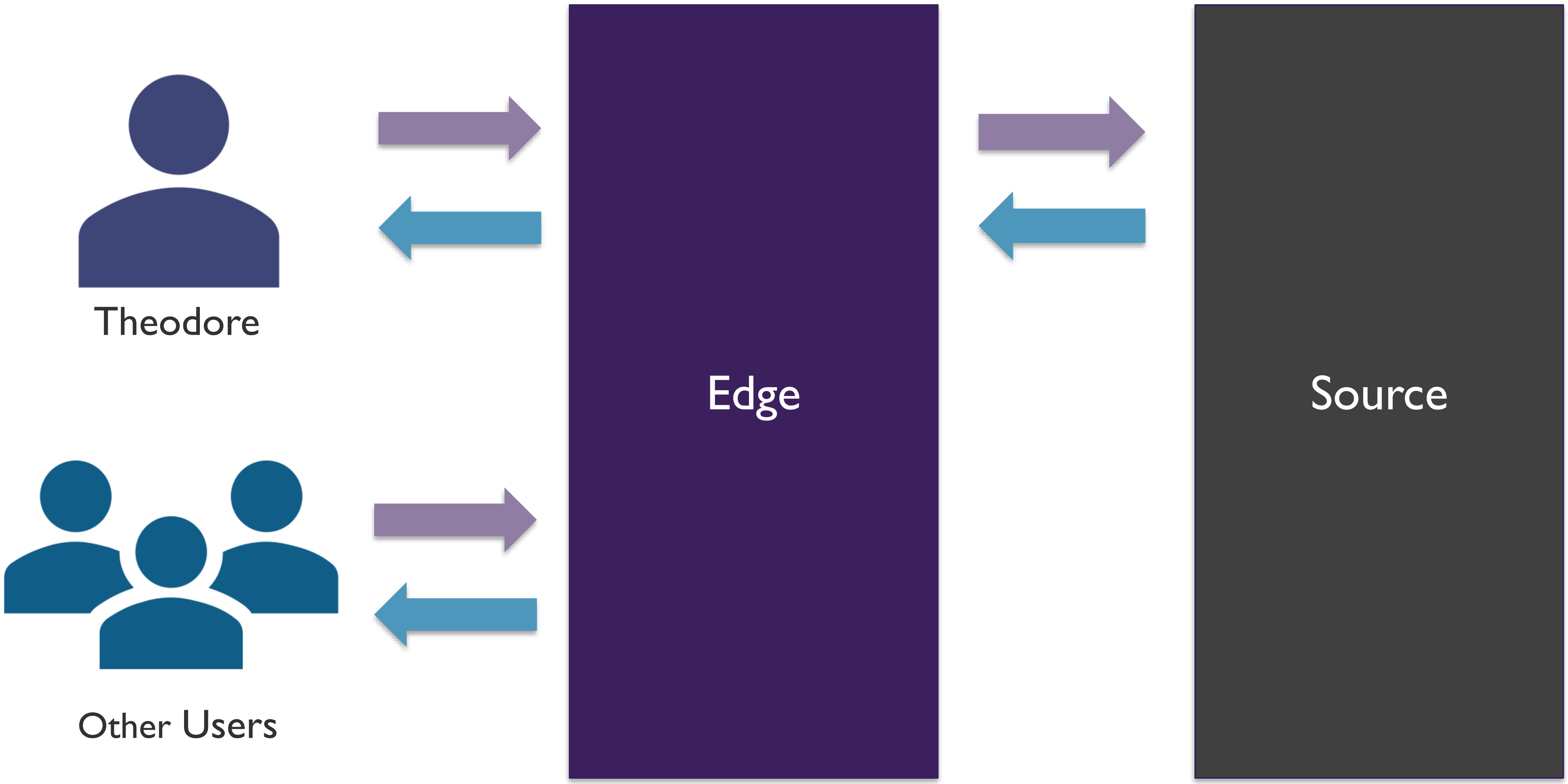
1. The customer prepares the hard drives using the Import/ Export Client Tool, and encrypts the drive with BitLocker.
2. The customer creates an import job using the Azure Portal.
3. The customer ships the hard drives to the data center.
4. The carrier delivers the hard drives to the data center.
5. The hard drives are processed at the data center.
6. The data is copied from the hard drives to the storage account.
7. The hard drives are packaged for return shipping.
8. The hard drives are shipped back to the customer.

https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service

CDN



CDN



Azure CDN Offerings

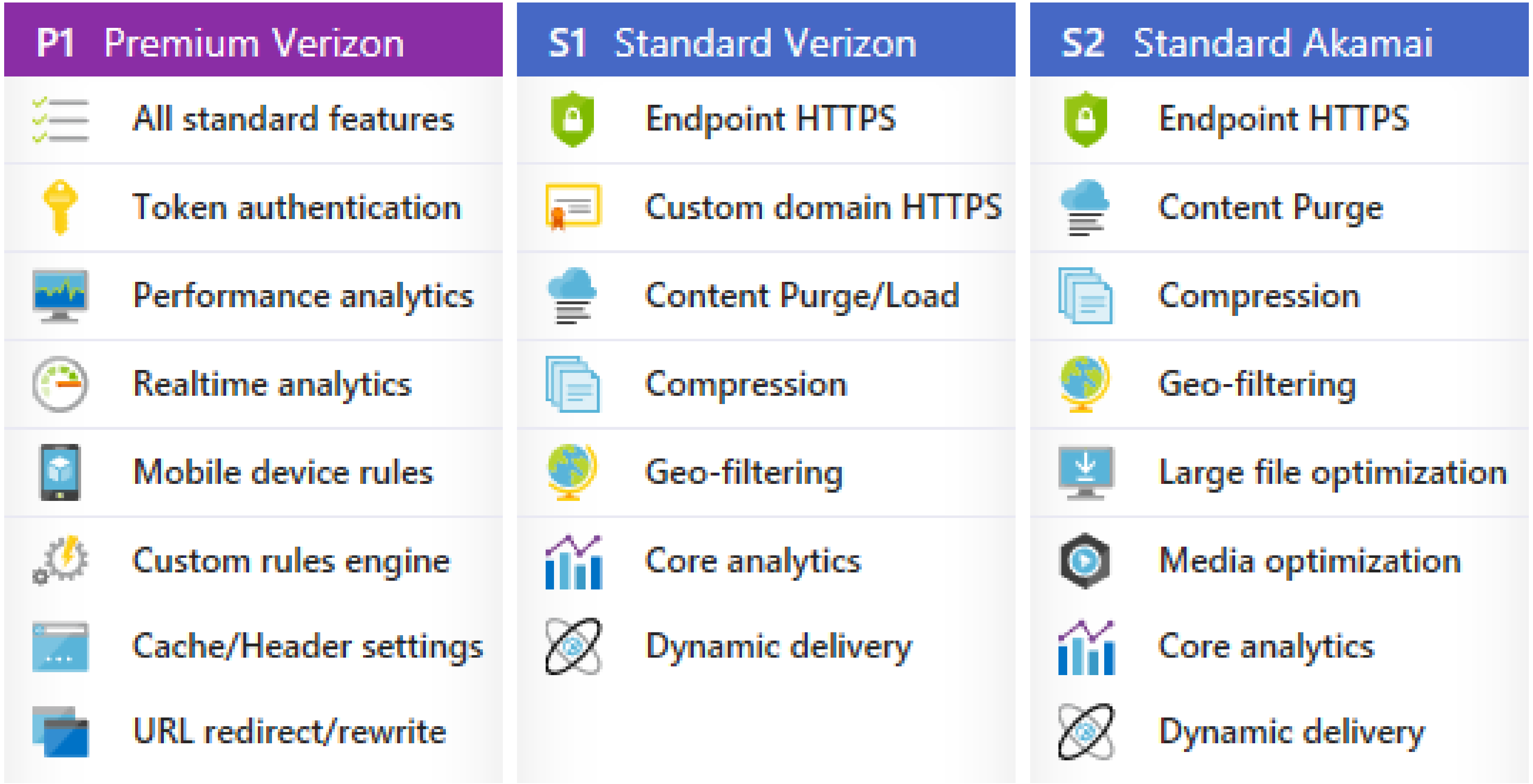
Standard Akamai

Standard Verizon

Premium Verizon

https://docs.microsoft.com/en-us/azure/cdn/cdn-overview

Azure CDN Offerings

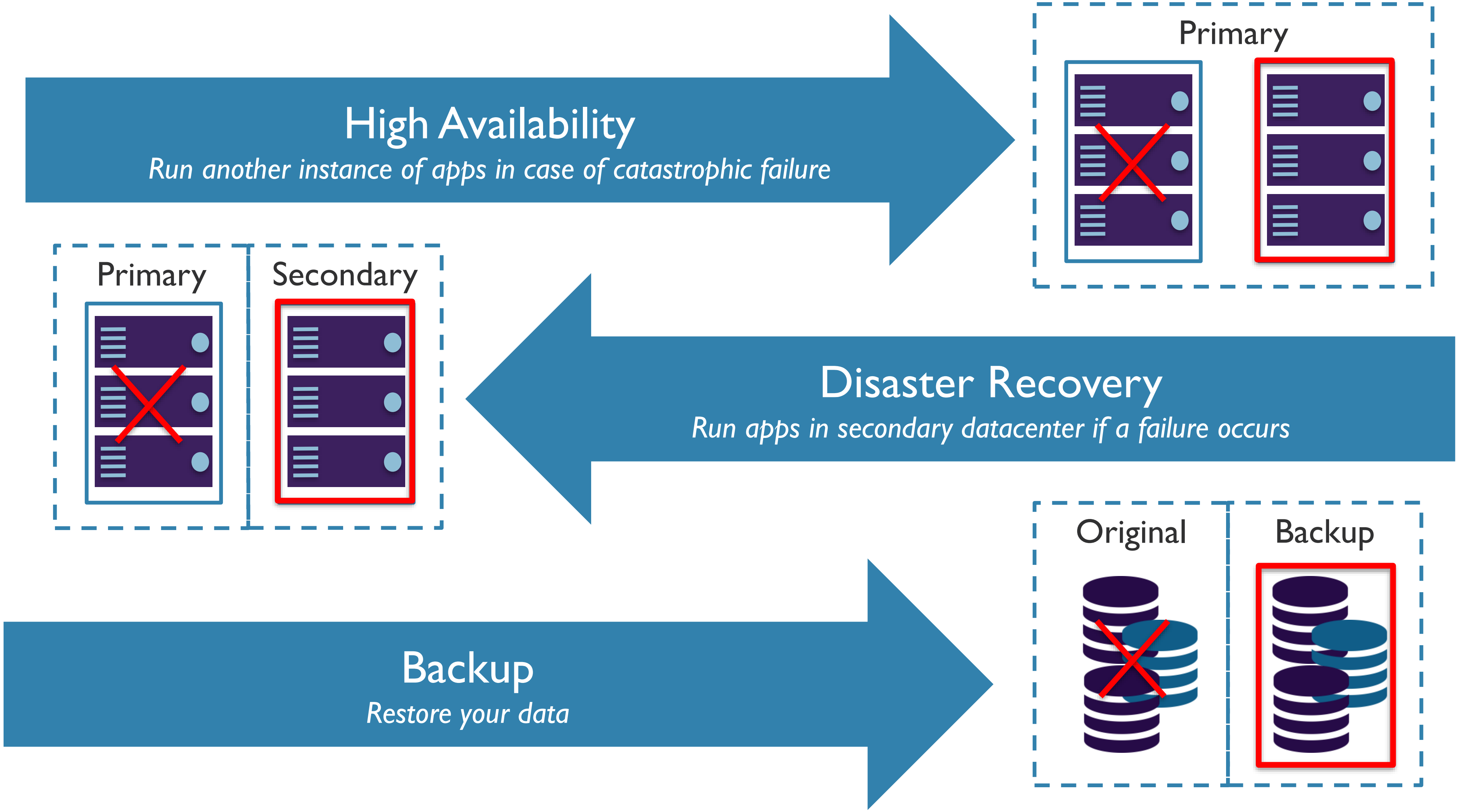


P1 Premium Verizon	S1 Standard Verizon	S2 Standard Akamai
All standard features	Endpoint HTTPS	Endpoint HTTPS
Token authentication	Custom domain HTTPS	Content Purge
Performance analytics	Content Purge/Load	Compression
Realtime analytics	Compression	Geo-filtering
Mobile device rules	Geo-filtering	Large file optimization
Custom rules engine	Core analytics	Media optimization
Cache/Header settings	Dynamic delivery	Core analytics
URL redirect/rewrite		Dynamic delivery

Missing Module: Implement Azure Backup

SKYLINES ACADEMY

Business Continuity Strategies



High Availability

Run another instance of apps in case of catastrophic failure

Disaster Recovery

Run apps in secondary datacenter if a failure occurs

Backup

Restore your data

Azure Backup Overview

- Backup solution purpose built for Cloud
- Unlimited Scaling
- Unlimited Data Transfer
- Multiple Storage Options (LRS/GRS)
- Long Term Retention
- Application-Consistent Backups
- Data Encryption

Other Recovery Options

Snapshot Recovery

- Blob snapshots taken of VM page blob
- Snapshots can be copied into the same or different regions
- VMs get created from snapshot
- Application-consistent if VM was shutdown, otherwise crash-consistent

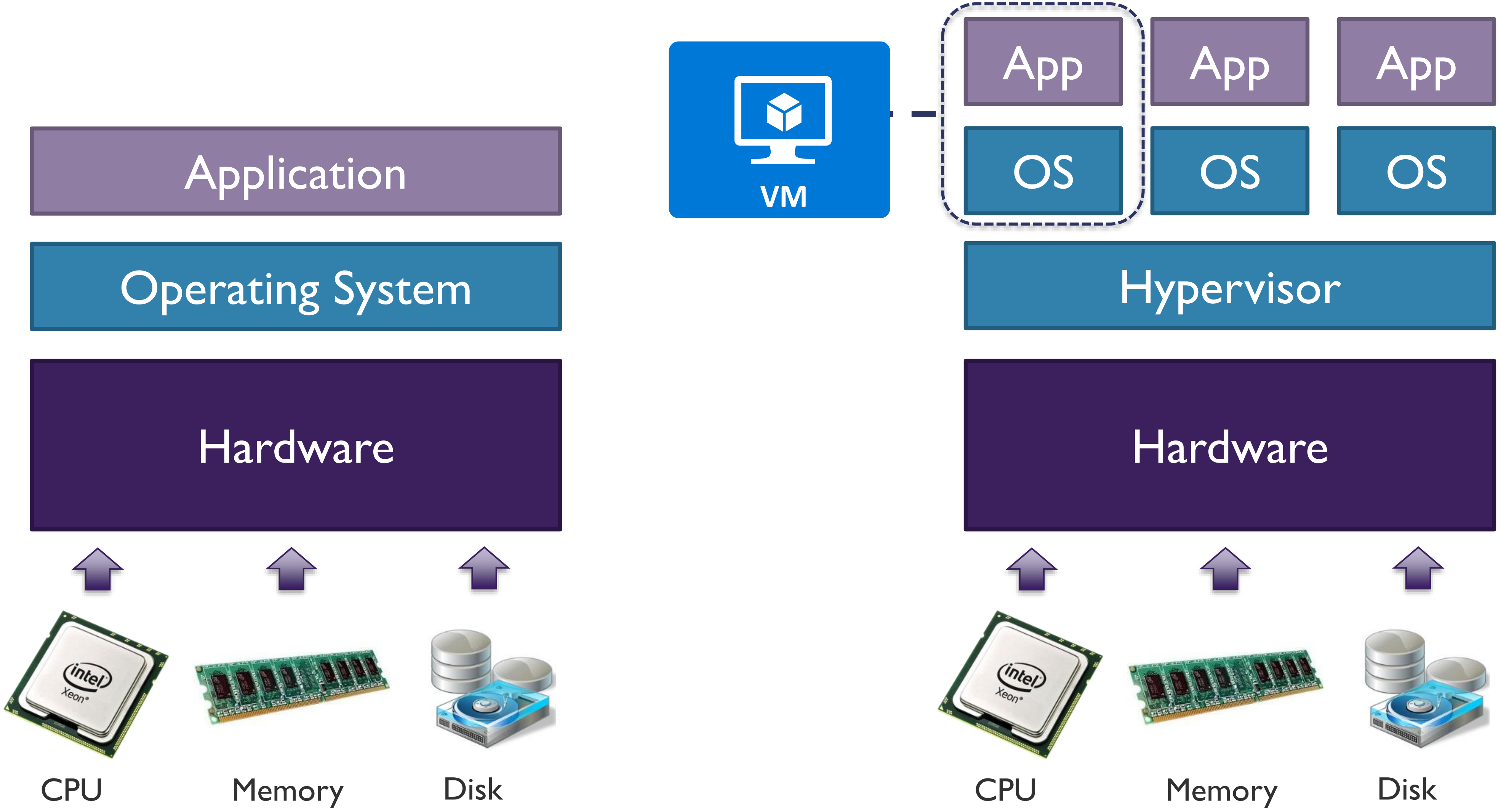
Geo-Replication

- Uses Azure Storage Geo-Redundant Storage (GRS)
- Data is replicated to a paired region far away from the primary copy
- Data Recovered in the event of an outage or entire region unavailable
- RA-GRS option available as well

Module:
Create and Configure a VM for Windows or Linux

SKYLINES ACADEMY

Introduction to Virtual Machines



VM Types

VM

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.

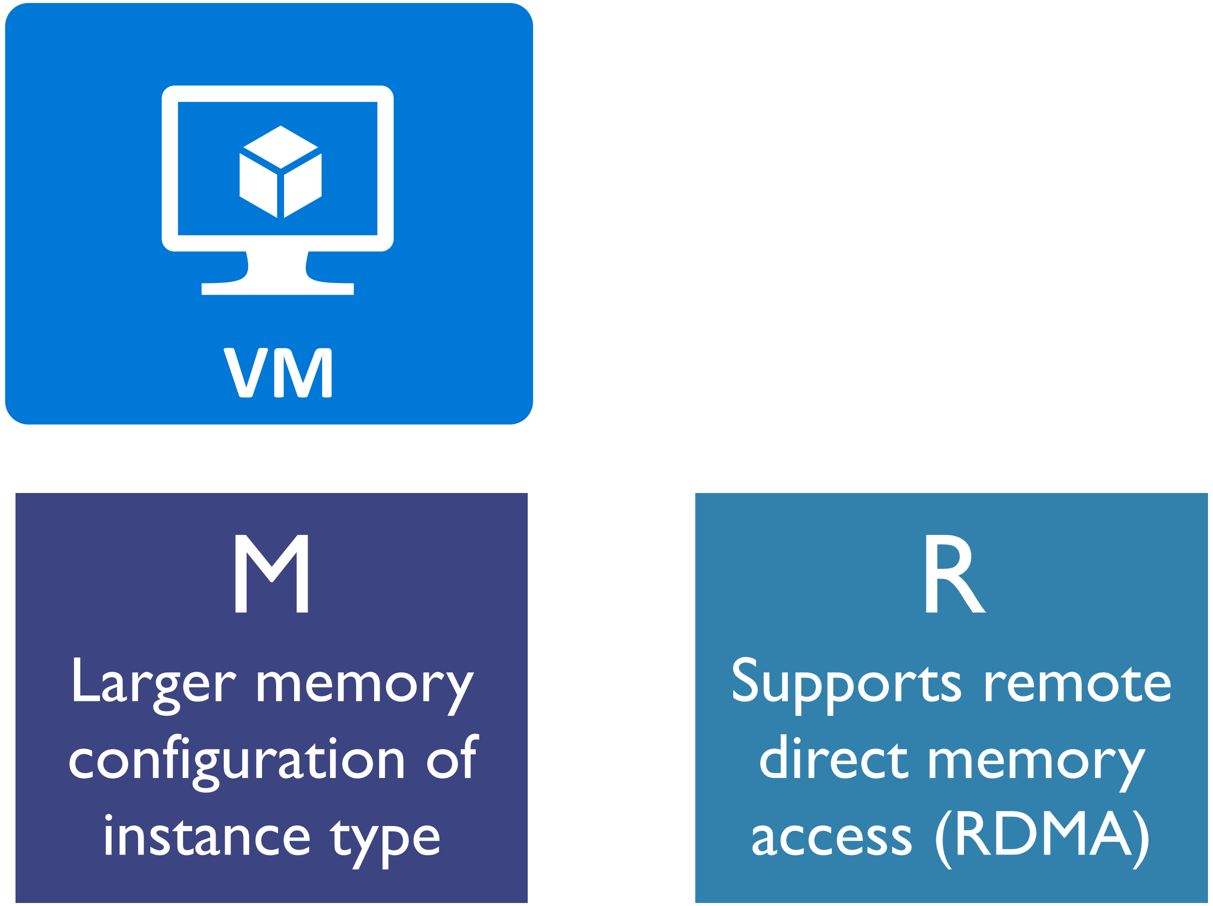
VM Types (continued)

SKYLINES ACADEMY

VM

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 Specializations



VM

S

Premium Storage options available

Example: DSv2

M

Larger memory configuration of instance type

Example: Standard A2m_v2

R

Supports remote direct memory access (RDMA)

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

OS Reference Documentation

Windows Virtual Machines

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

Linux Virtual Machines

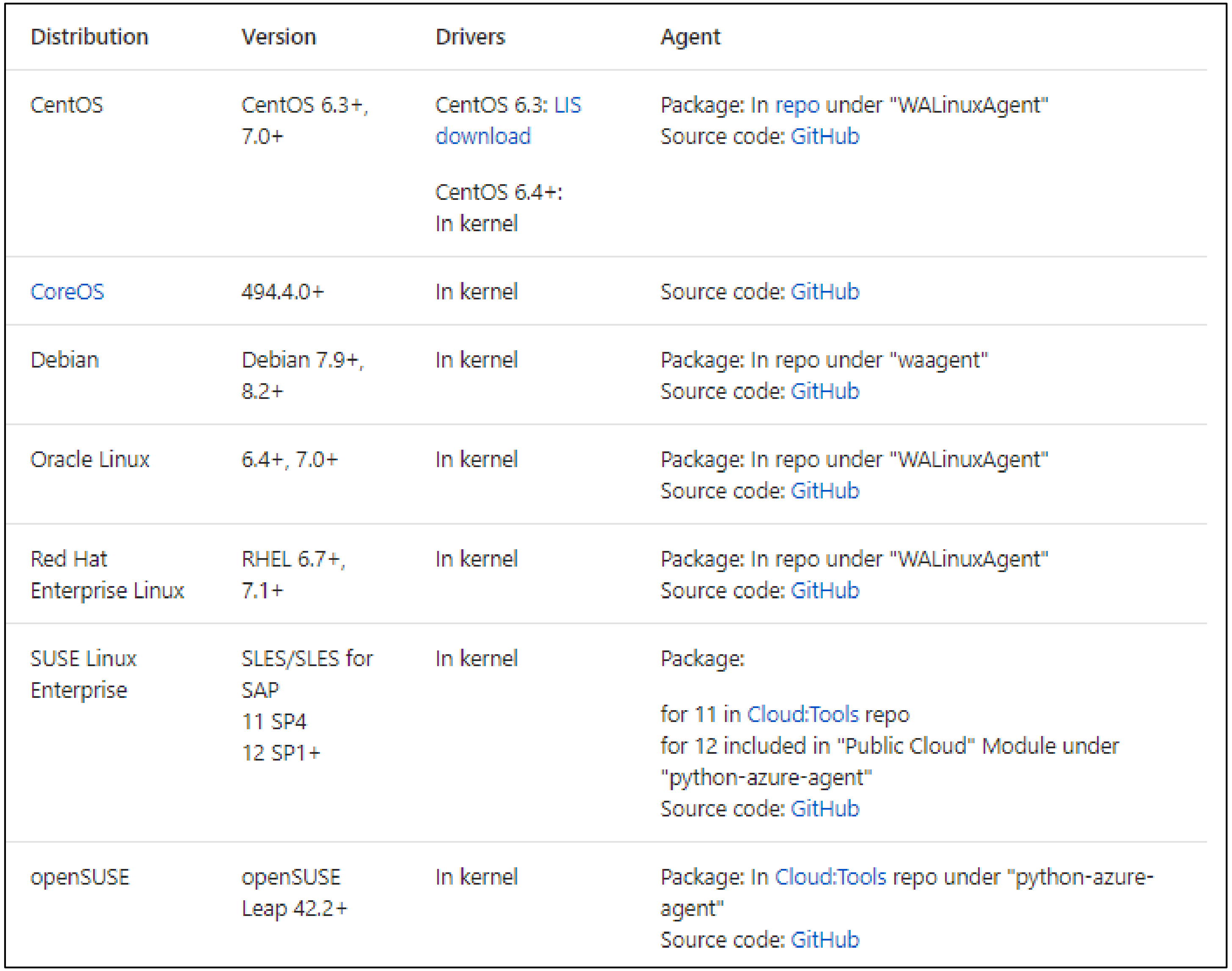
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/

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

Linux-Supported Distributions



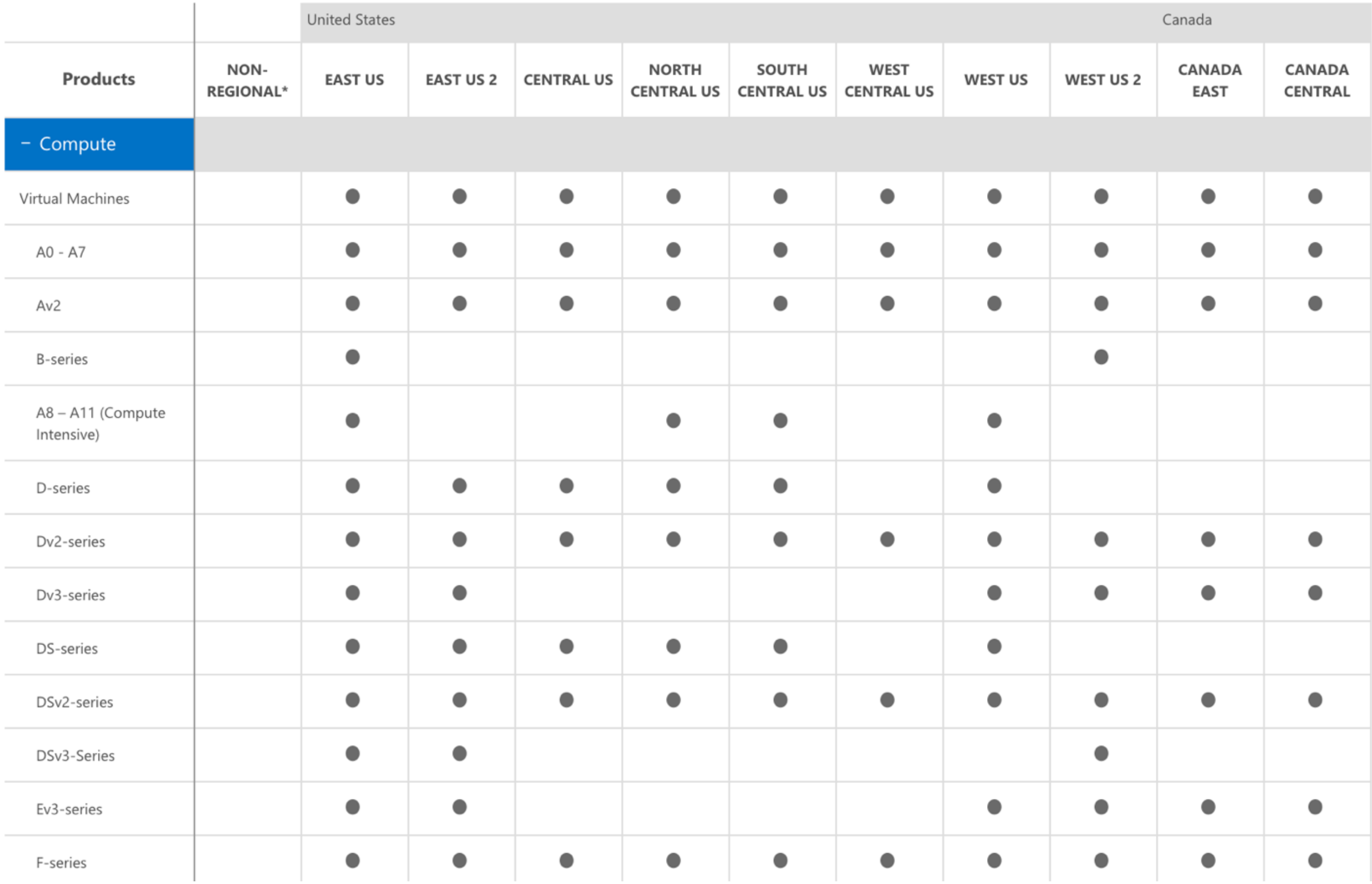
Distribution	Version	Drivers	Agent
CentOS	CentOS 6.3+, 7.0+	CentOS 6.3: LIS download CentOS 6.4+: In kernel	Package: In repo under "WALinuxAgent" Source code: GitHub
CoreOS	494.4.0+	In kernel	Source code: GitHub
Debian	Debian 7.9+, 8.2+	In kernel	Package: In repo under "waagent" Source code: GitHub
Oracle 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



		United States								Canada	
Products	NON-REGIONAL*	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		●	●	●	●	●	●	●	●	●	●

Restricted Usernames

administrator	admin	user	user1
test	user2	test1	user3
admin1	1	123	a
actuser	adm	admin2	aspnet
backup	console	david	guest
john	owner	root	server
sql	support	support_388945a0	sys
test2	test3	user4	user5

You cannot use any of these names for your VM username when creating an Azure VM

Module:
Automate Deployment of VMs

SKYLINES ACADEMY

VM Images

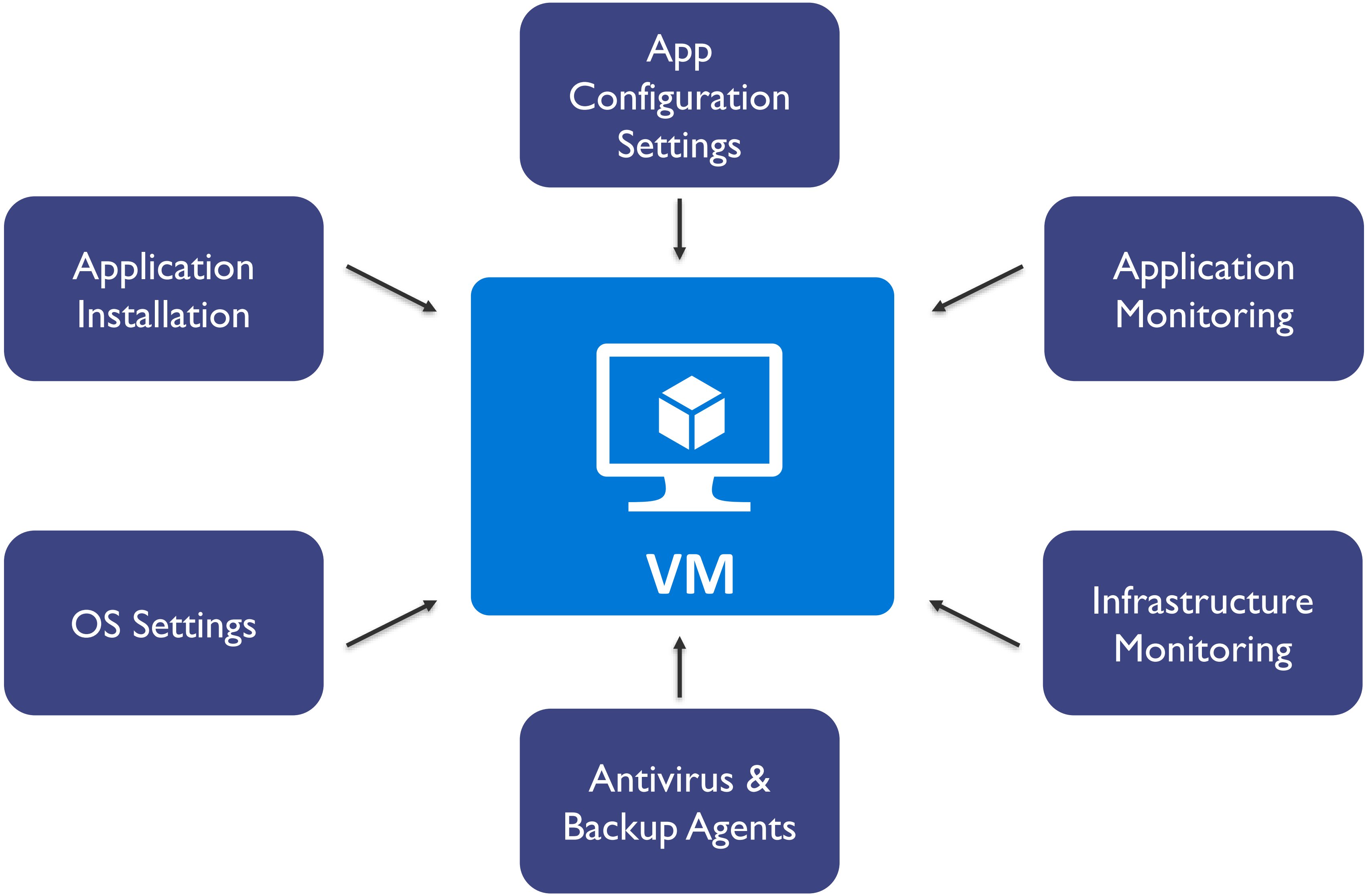
Custom Images

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

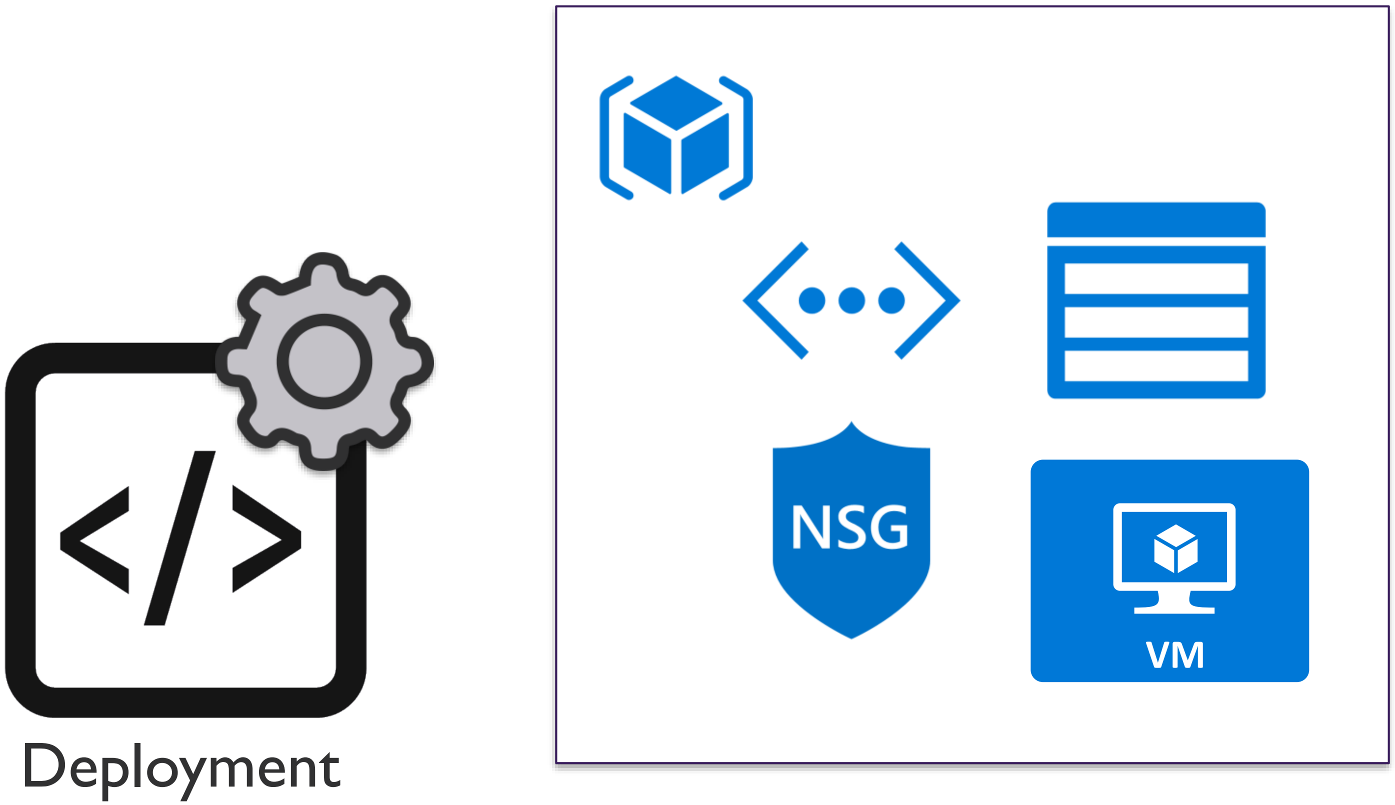
Marketplace Images

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

Introduction to Configuration Management


App Configuration Settings
Application Installation
Application Monitoring
VM
OS Settings
Infrastructure Monitoring
Antivirus & Backup Agents

VM Extensions



VM Extensions

DSC

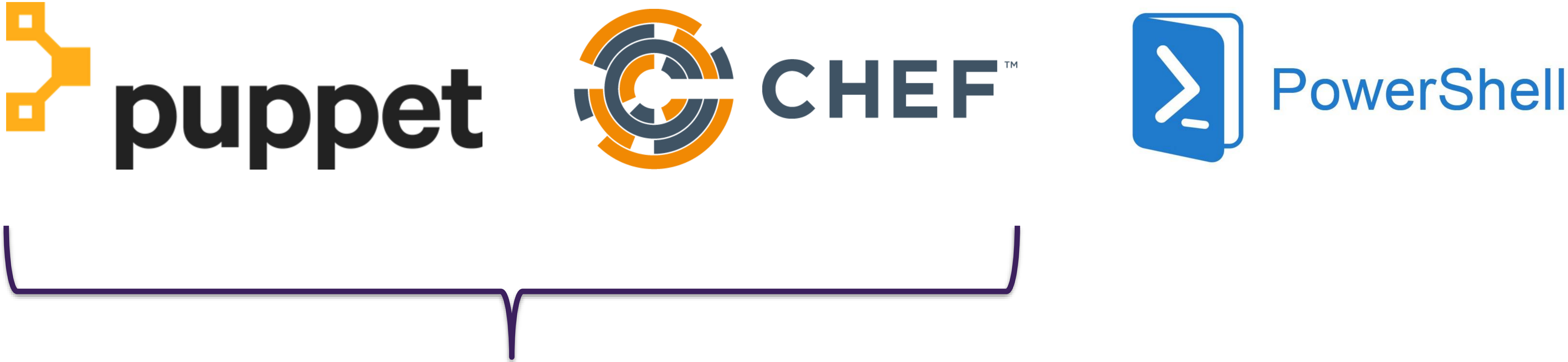
Scripts

Configuration Management

puppet
CHEF™
PowerShell

Extensions available in Azure

Configuration Management (continued)



Enterprise-level configuration management for multiple nodes

PowerShell DSC Key Components

Configurations

Resources

Logical Configuration Manager

PowerShell DSC Example

```
Configuration SkylinesWebSite
{
 Node 'localhost'
 {
  #Install IIS - Enabled via Windows
feature
  WindowsFeature IIS
  {
   Ensure = “Present”
   Name = “Web-Server”
  }
  #Install ASP.NET 4.5
  WindowsFeature ASP
  {
   Ensure = “Present”
   Name = “Web-Asp-Net45”
  }
 }
}
```

The name of the configuration.

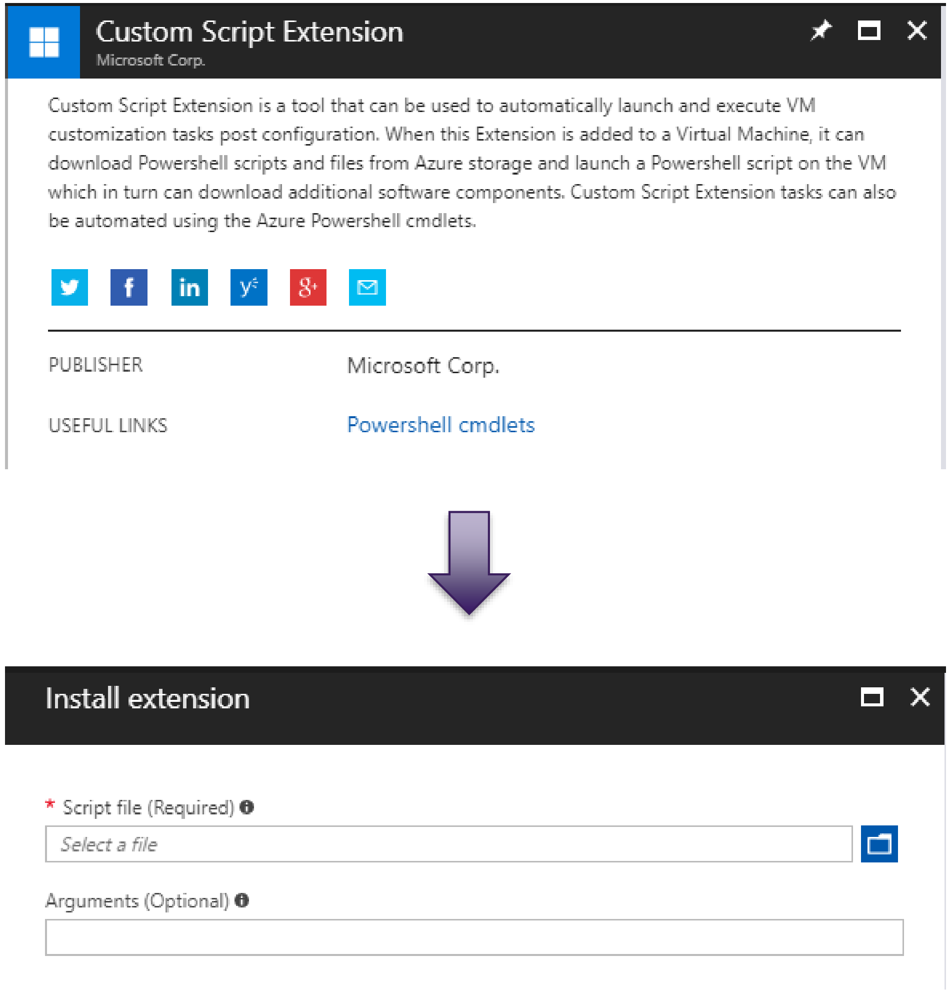
Specifies which targets the configuration applies to.

Declarative statement about what we are configuring. In this case, we want IIS installed.

A second declarative statement. This time to ensure .NET 4.5 is installed.

Custom Script Extension

- Execute VM Tasks without logging into the VM
- Upload via Portal or download scripts from Azure Blob storage or GitHub
- Can be automated using PowerShell



Custom Script Extension
Microsoft Corp.

Custom Script Extension is a tool that can be used to automatically launch and execute VM customization tasks post configuration. When this Extension is added to a Virtual Machine, it can download Powershell scripts and files from Azure storage and launch a Powershell script on the VM which in turn can download additional software components. Custom Script Extension tasks can also be automated using the Azure Powershell cmdlets.

PUBLISHER: Microsoft Corp.

USEFUL LINKS: Powershell cmdlets

Install extension

* Script file (Required)
Select a file

Arguments (Optional)

Custom Script Extension (continued)

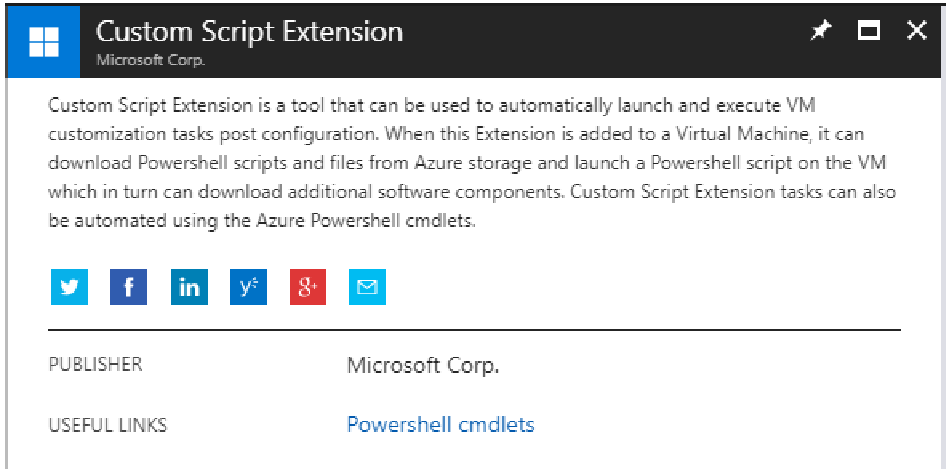
SKYLINES ACADEMY

Benefits

- No local or domain credentials needed to login to Azure VM
- VM does not need an accessible IP Address to remotely connect
- Simple to implement

Drawbacks

- Must be enabled for each VM you want to run your script on
- VMs will need internet access if using GitHub or Blob storage for scripts
- Relatively slow

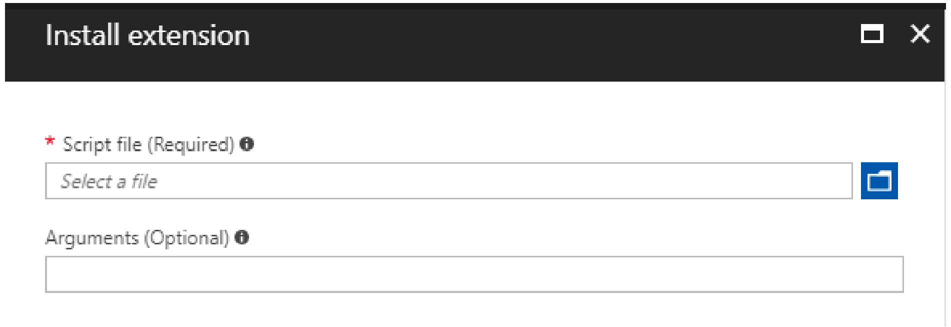


Custom Script Extension
Microsoft Corp.

Custom Script Extension is a tool that can be used to automatically launch and execute VM customization tasks post configuration. When this Extension is added to a Virtual Machine, it can download Powershell scripts and files from Azure storage and launch a Powershell script on the VM which in turn can download additional software components. Custom Script Extension tasks can also be automated using the Azure Powershell cmdlets.

PUBLISHER Microsoft Corp.

USEFUL LINKS Powershell cmdlets



Install extension

* Script file (Required)

Select a file

Arguments (Optional)

Module:
Manage Azure VM Storage and Networking

SKYLINES ACADEMY

VM Storage Types

Standard Storage	Premium Storage
Backed by traditional HDD	Backed by SSD drives
Most cost effective	Higher performance
Max throughput – 60MB/S per disk	Max throughput – 250MB/S per disk
Max IOPS – 500 IOPS 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

SKYLINES ACADEMY

	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 through	25 MB/s	50 MB/s	100 MB/s	125 MB/s	150 MB/s	200 MB/s	250 MB/s	250 MB/s

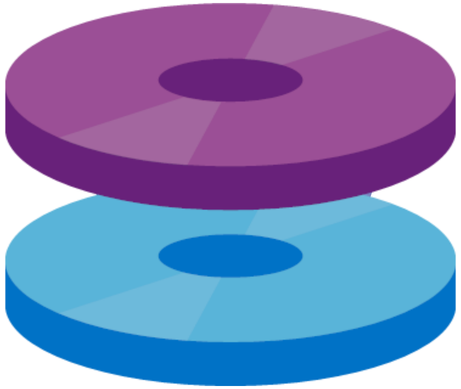
Managed vs. Unmanaged Disks

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

SKYLINES
ACADEMY

Logically Replicated Storage (LRS)

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.

Zone Replicated Storage (ZRS)

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.

Geographically Replicated Storage (GRS)

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.

Read Only Geographically Replicated Storage (RA-GRS)

Same replication as per GRS but also provides read access to the data in the other region.

Replication Strategies

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

Disk Caching

- Method for improving performance of VHDs
- Utilizes local RAM and SSD drives on underlying VM host
- Available on both standard and premium disks

Disk Caching (continued)

Default and Allowed Settings

Disk Type	Default Cache Setting	Allowed Settings
OS disk	Read-Write	Read-Only or Read-Write
Data disk	None	None, Read-Only, or Read-Write

- Read-Only Caching
  - Improve latency and potentially gain higher IOPS per disk
- Read-Write Caching
  - Ensure you have a proper way to write data from cache to persistent disks

Module:
VM Availability

Availability Sets

SKYLINES ACADEMY

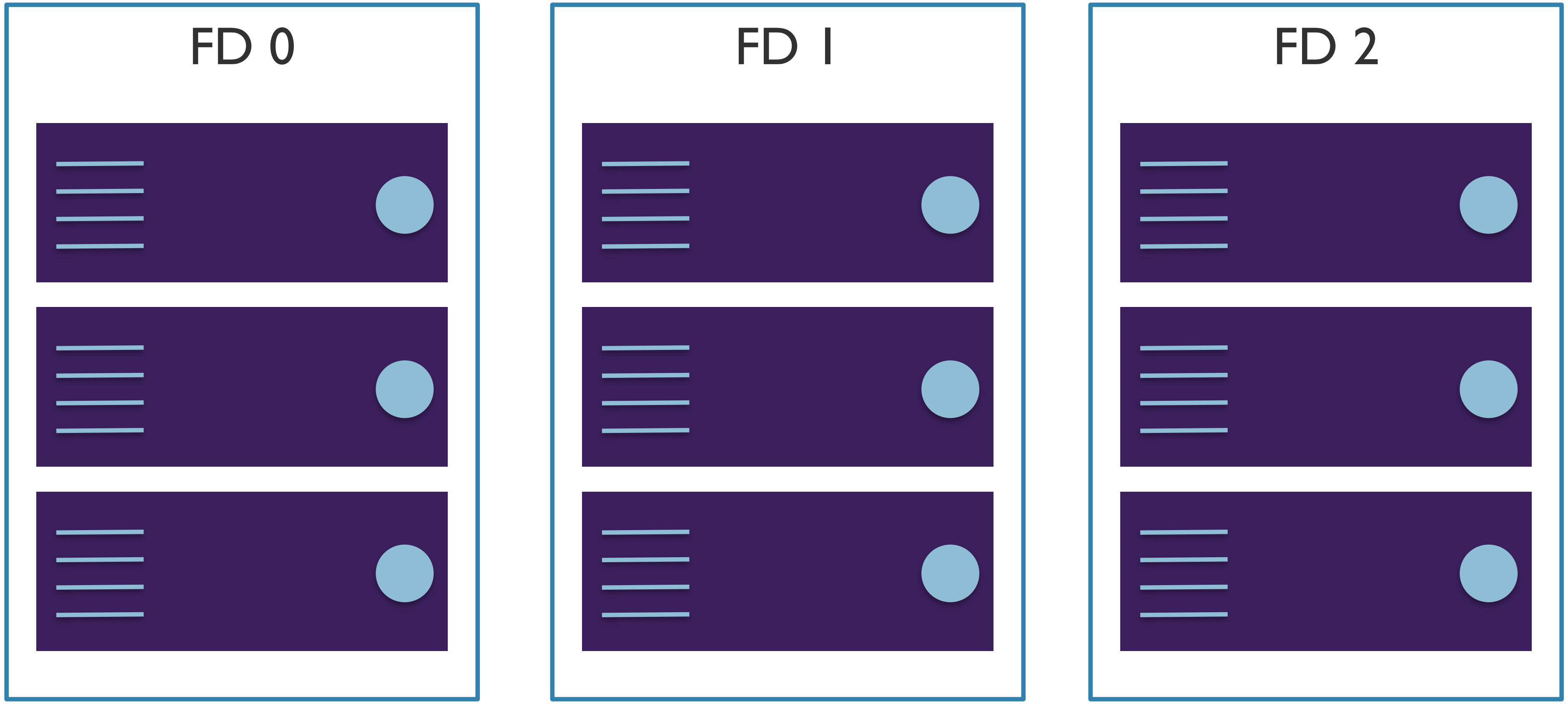
Potential for VM Impact

- Planned maintenance
- Unplanned hardware maintenance
- Unexpected downtime

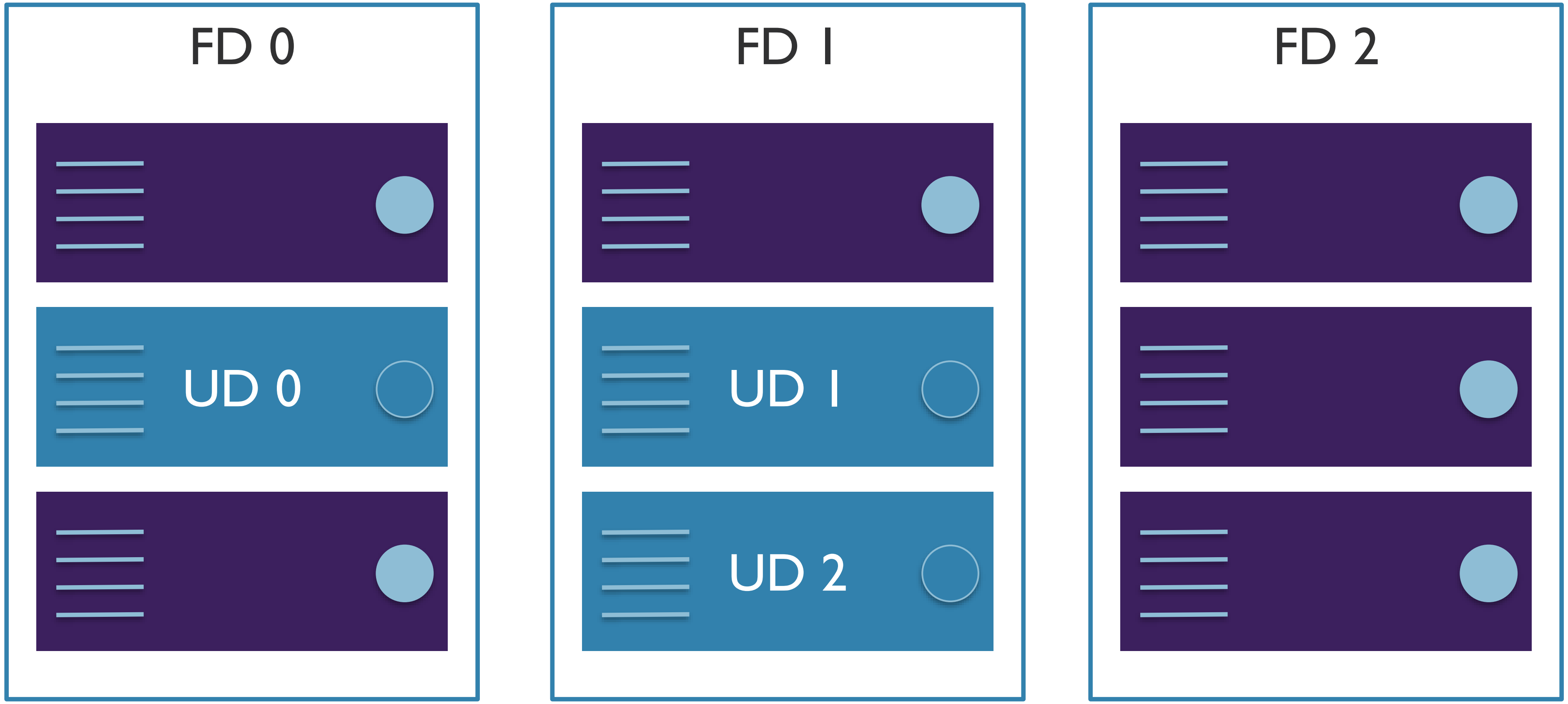
Availability Sets

- Group two or more machines in a set
- Separated based on Fault Domains and Update Domains

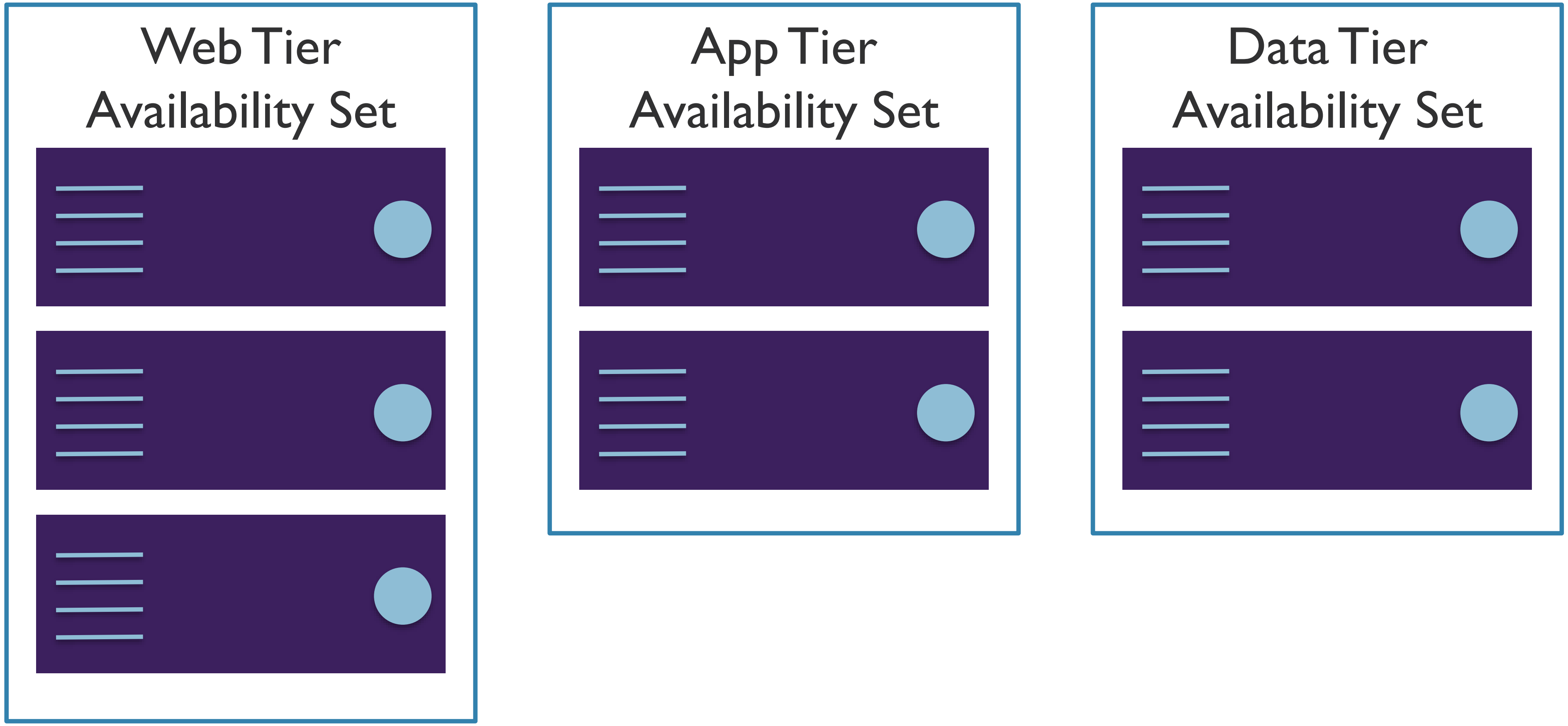
Fault Domains and Update Domains



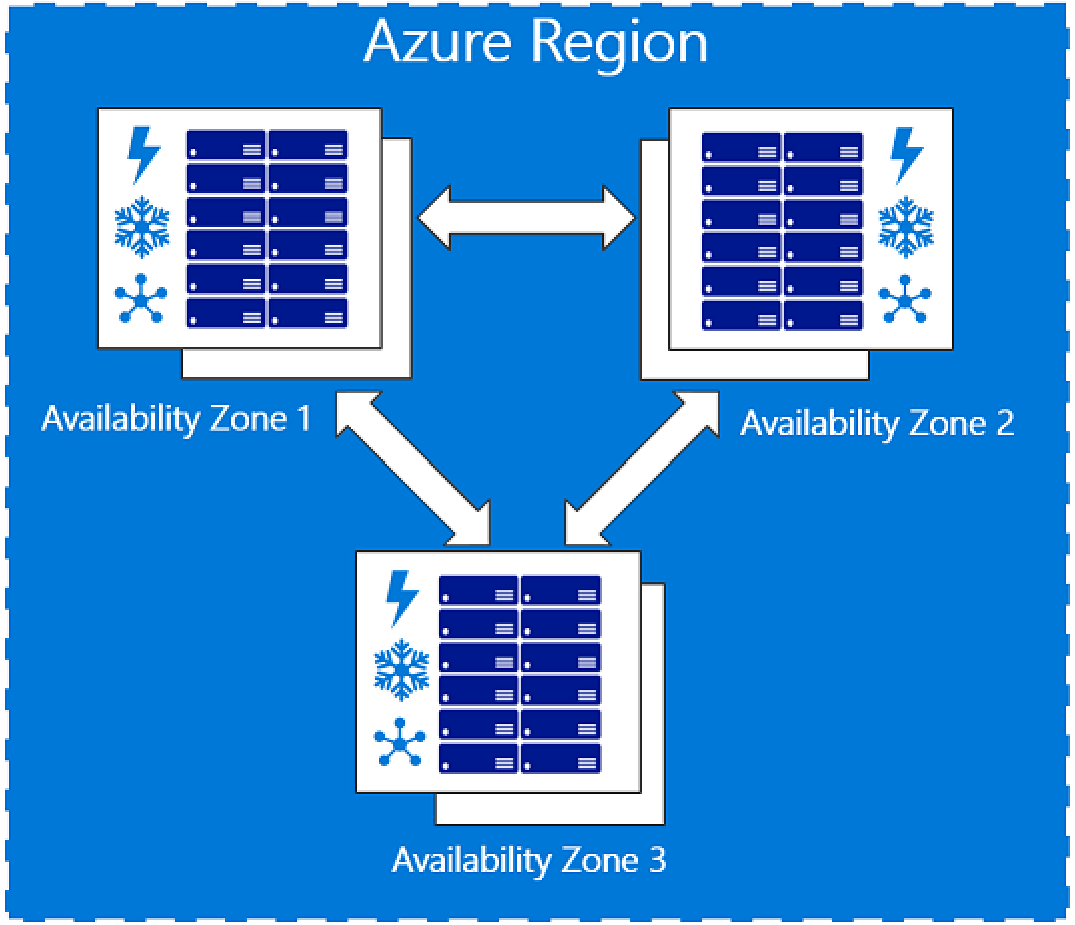
Fault Domains and Update Domains



Planning for Availability



Availability Zones



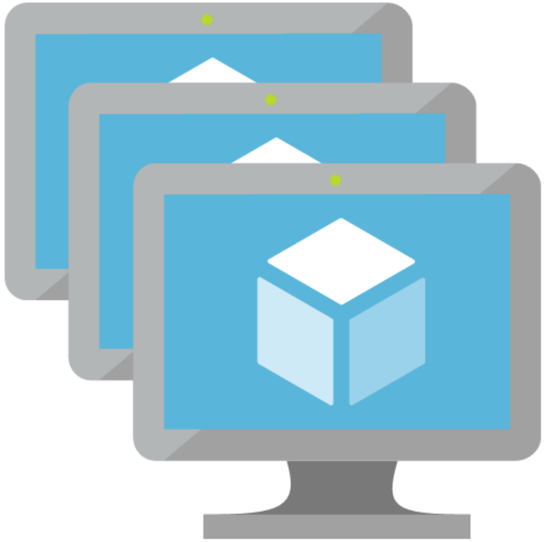
- Offer 99.99% availability
- Minimize impact of planned and unplanned downtime
- Enforce them like Availability Sets, but now you choose your specific zone in Azure

Module:
VM Scale Sets

SKYLINES
ACADEMY

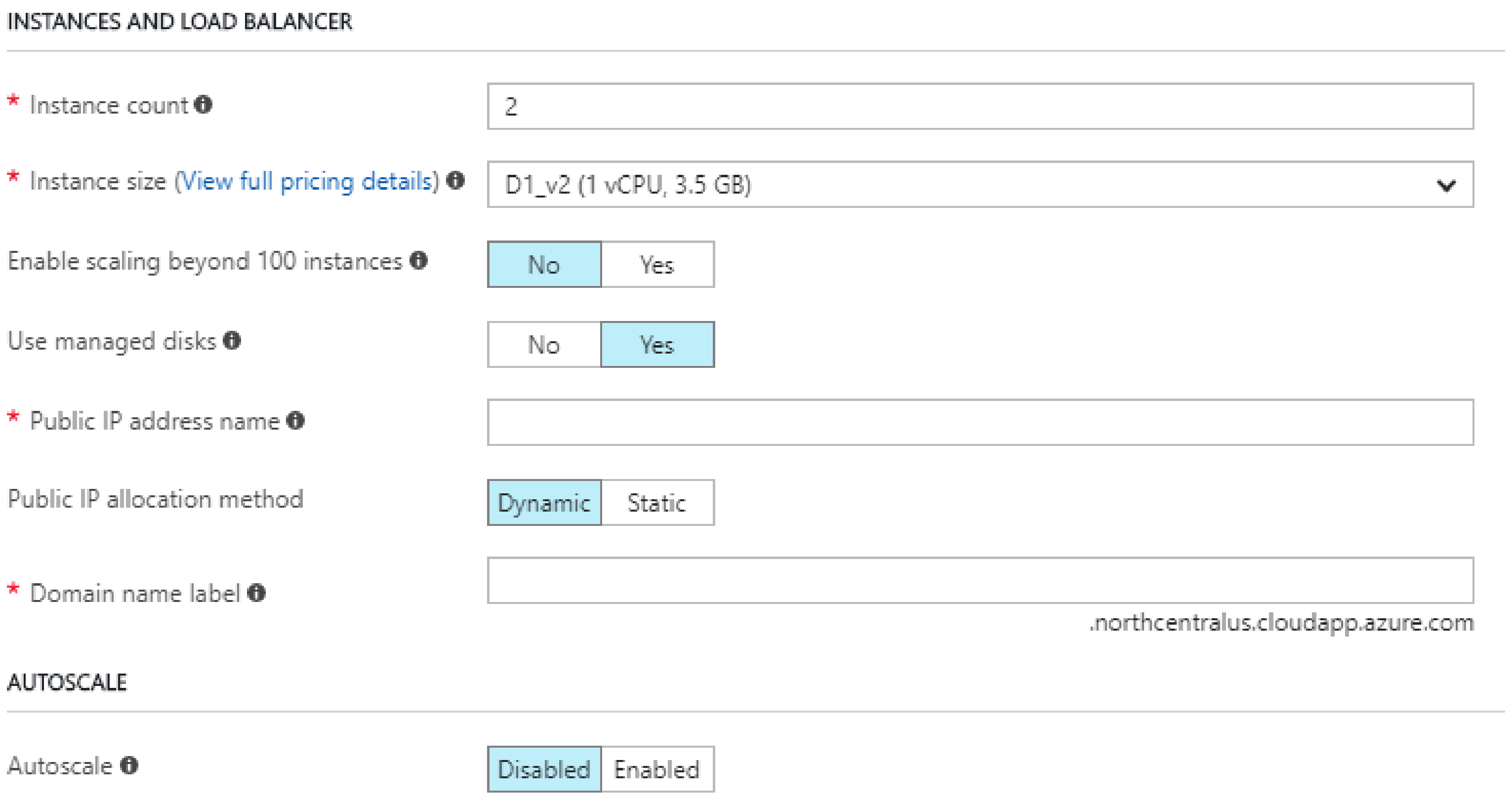
Scale Sets

vs.



Define Virtual Machine Scale Set (VMSS)

- Use Portal, PowerShell or API
- Number of instances you wish to run, instance size, etc.
- Determine if you want to auto-scale



INSTANCES AND LOAD BALANCER

* Instance count: 2

* Instance size (View full pricing details): D1_v2 (1 vCPU, 3.5 GB)

Enable scaling beyond 100 instances: [✓ No] Yes

Use managed disks: No [✓ Yes]

* Public IP address name:

Public IP allocation method: [✓ Dynamic] Static

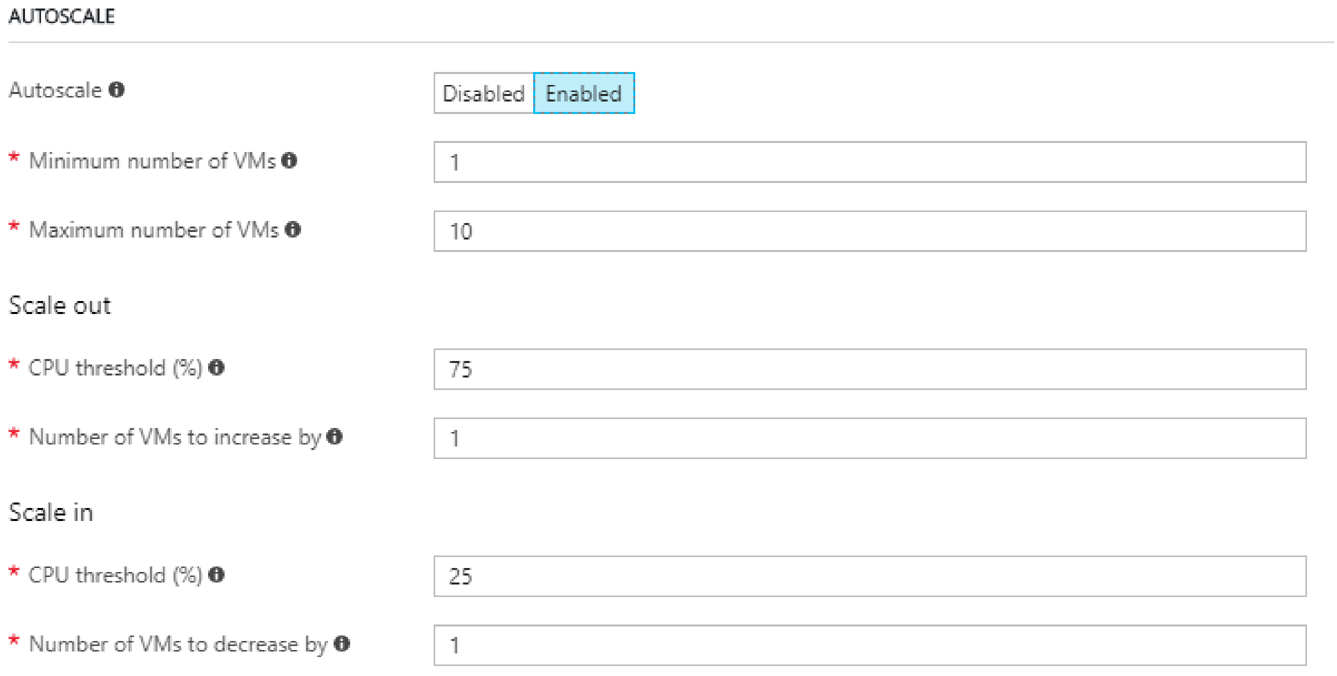
* Domain name label: .northcentralus.cloudapp.azure.com

AUTOSCALE

Autoscale: [✓ Disabled] Enabled

Configure Autoscale Rules

- Set minimum and maximum instance counts
- Scale out based on a variety of metrics – infrastructure or application
- Scale out based on a schedule
- Remember to account for sessions when scaling in on web servers

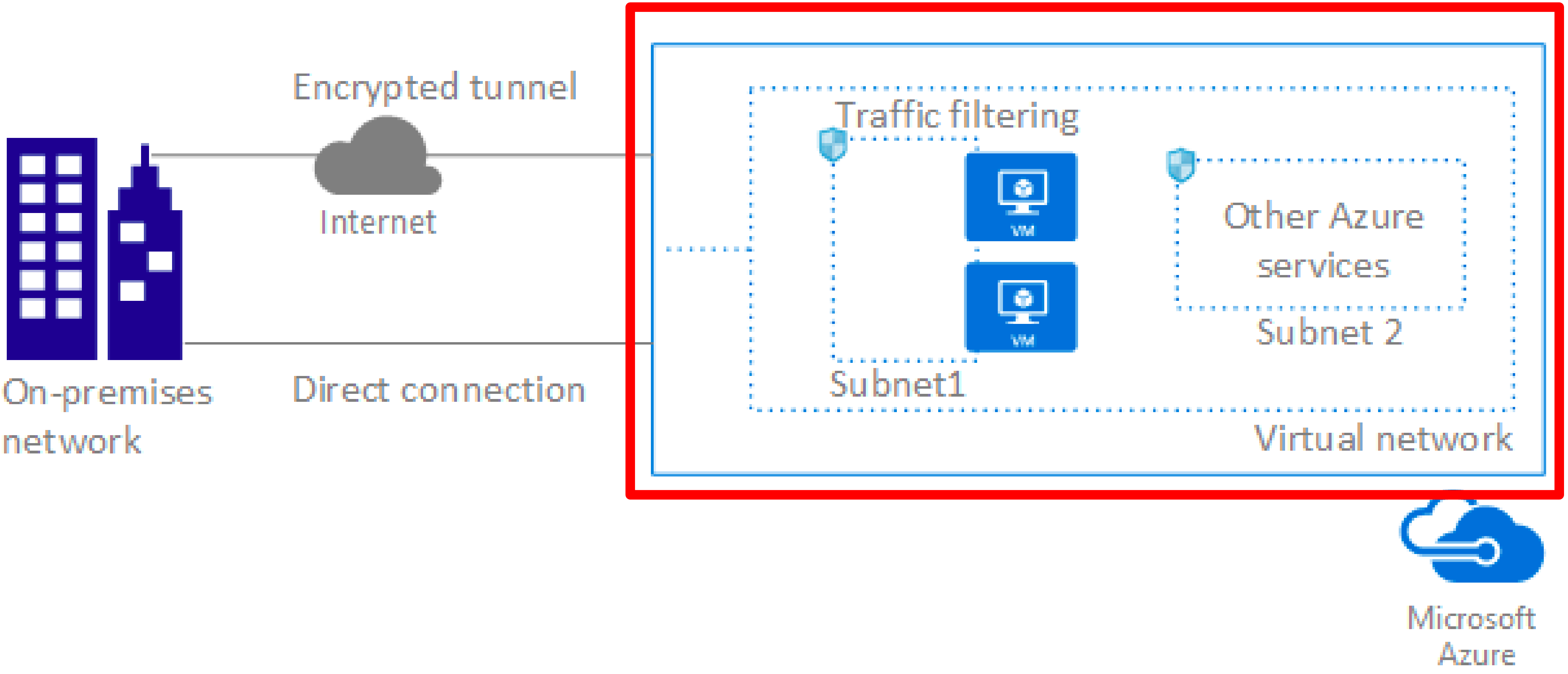


AUTOSCALE

Autoscale	Disabled **Enabled**
* Minimum number of VMs	1
* Maximum number of VMs	10
Scale out	
* CPU threshold (%)	75
* Number of VMs to increase by	1
Scale in	
* CPU threshold (%)	25
* Number of VMs to decrease by	1

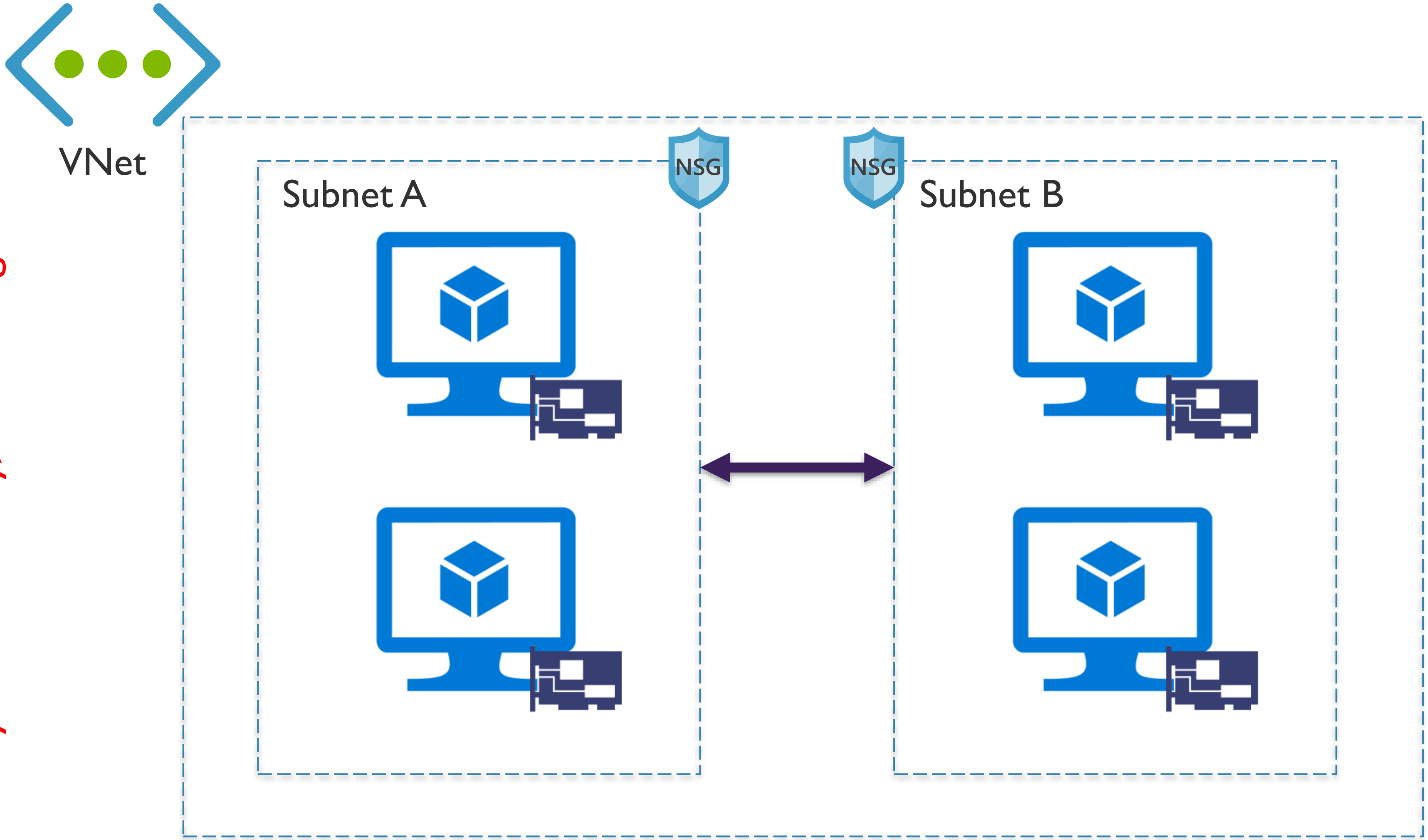
Module:
Azure Networking

Networking Overview



Source: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Networking Overview (continued)



Core VNet Capabilities:

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

VNets: Key Points

SKYLINES ACADEMY

- Primary building block for Azure networking
- Private network in Azure based on an address space prefix
- Create subnets in your VNet with your own IP ranges
- Bring your own DNS or use Azure-provided DNS
- Choose to connect the network to on-premises or the internet

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 (continued)

- 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

Module:
Create Connectivity Between Virtual Networks

SKYLINES ACADEMY

Hybrid Connectivity Options

Site-to-Site (S2S)

ExpressRoute

Point-to-Site (P2S)

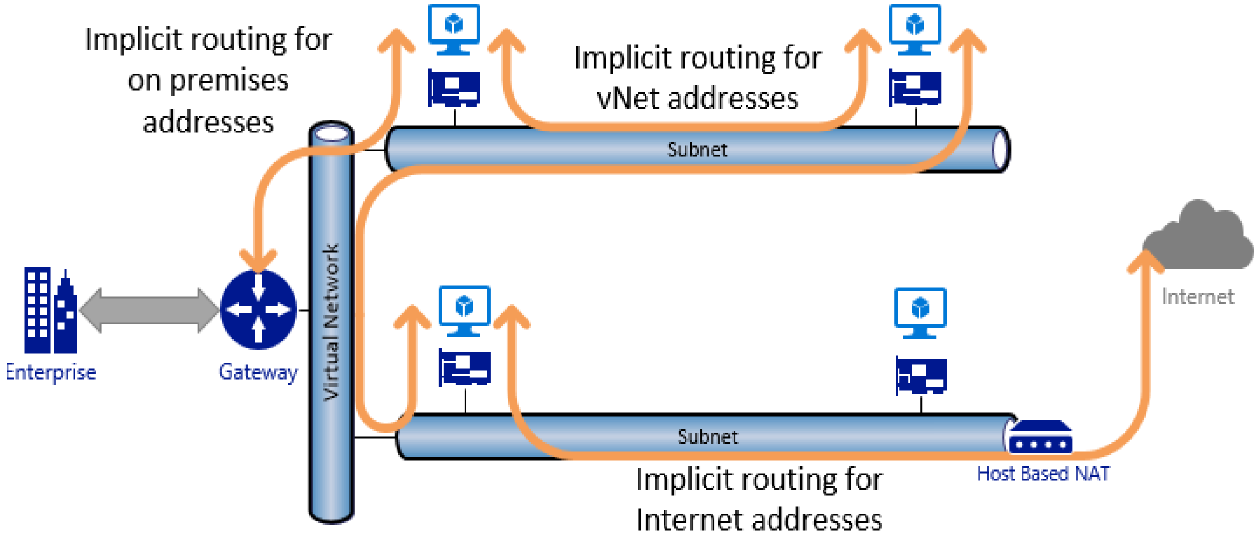
System Routes

Every subnet has a route table that contains the following minimum routes:

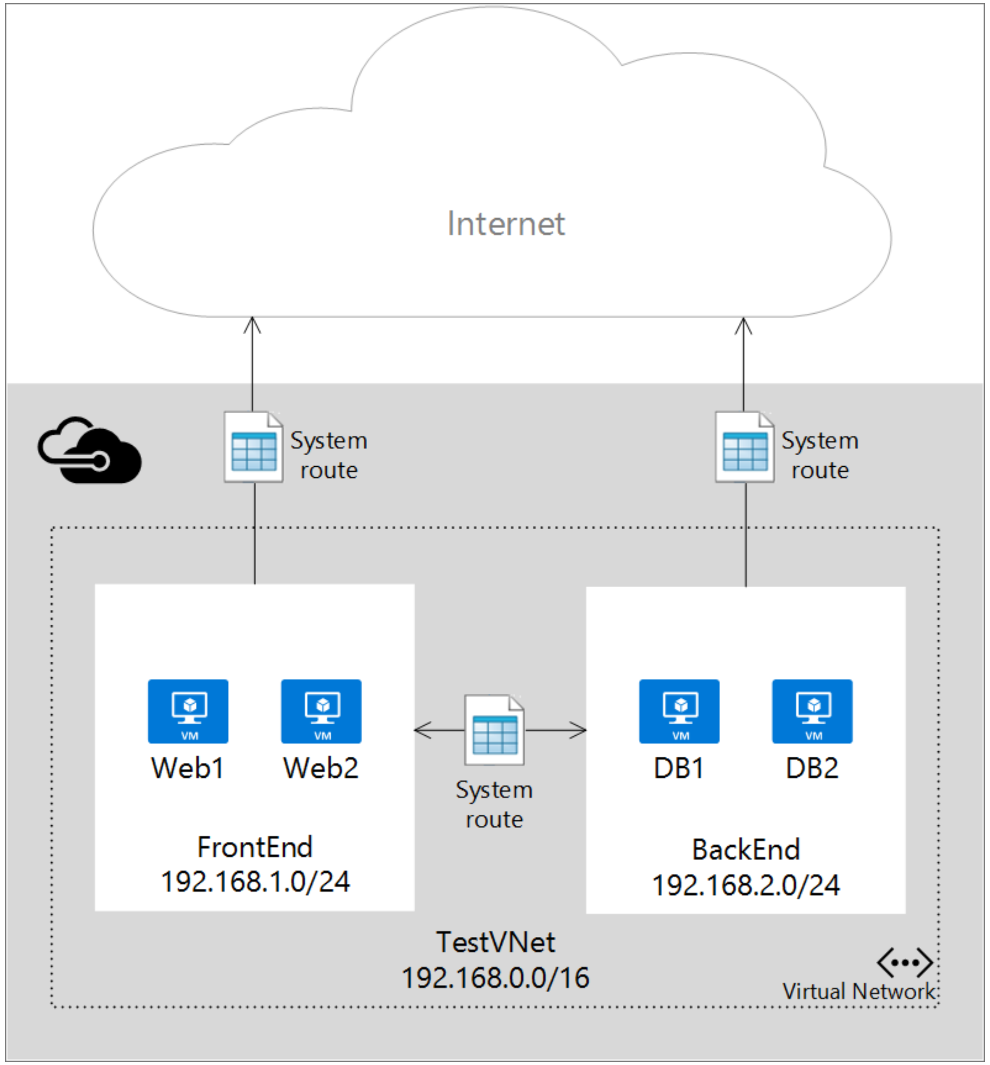
Route	Description
Local VNet	Route for local addresses (no next-hop value)
On-Premises	Route for defined on-premises address space (VNet gateway is next-hop address)
Internet	Route for all traffic destined to the Internet (Internet Gateway is the next-hop address)

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, *it is routed to the Host NAT for internet path, but it never leaves the datacenter*

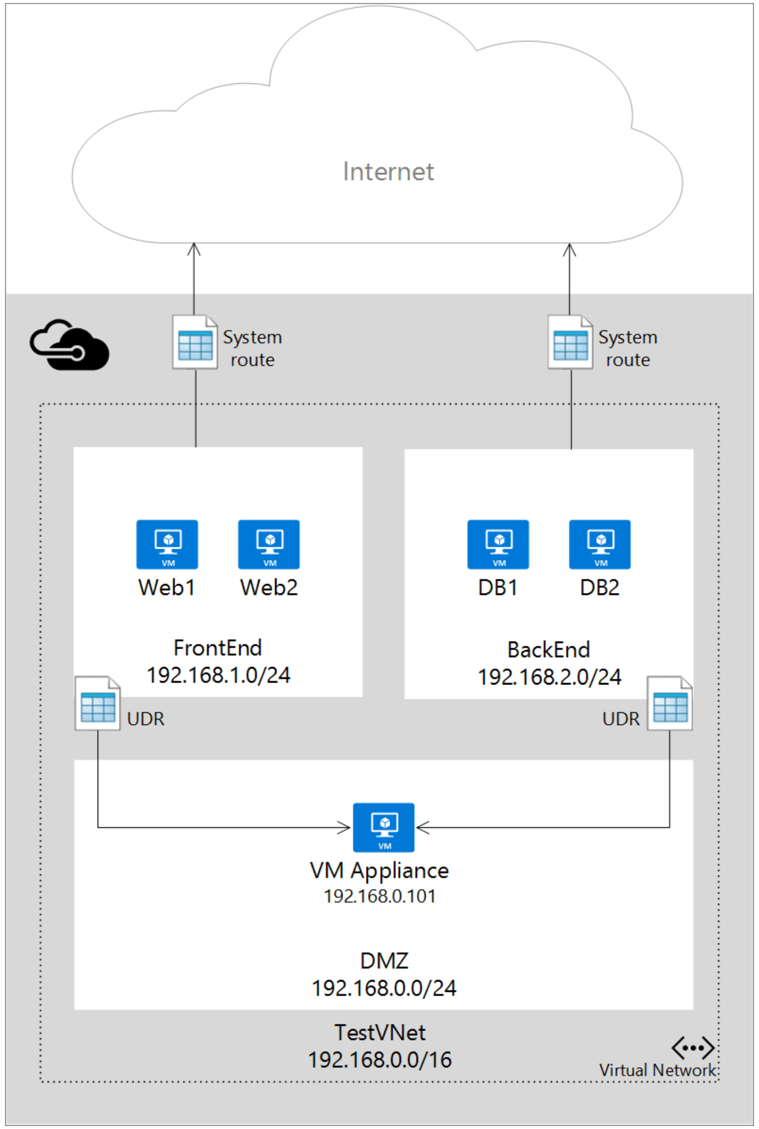

Implicit routing for on premises addresses
Implicit routing for vNet addresses
Subnet
Enterprise
Gateway
Virtual Network
Internet
Subnet
Host Based NAT
Implicit routing for Internet addresses

User-Defined Routes

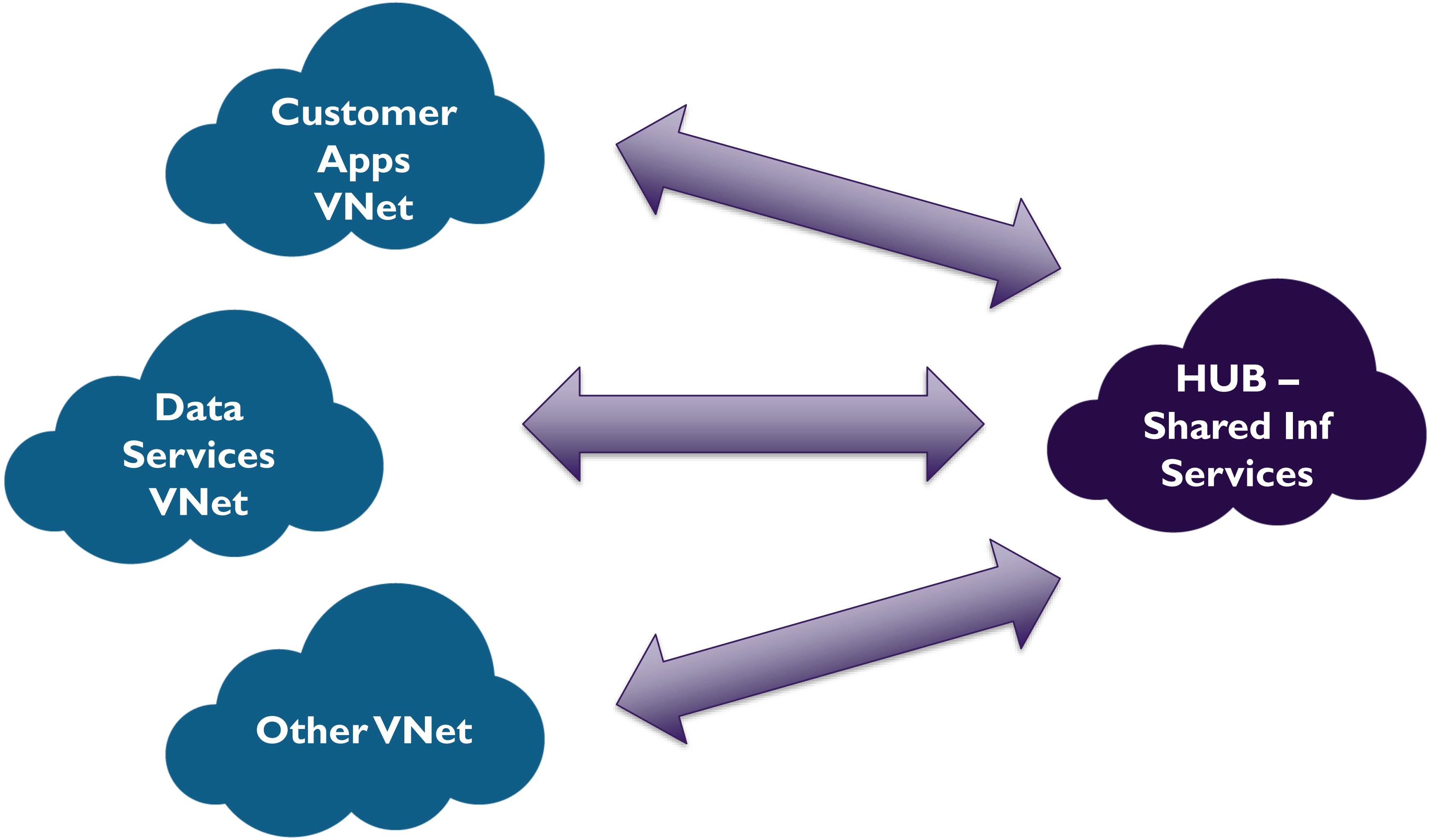


https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

User-Defined Routes (continued)

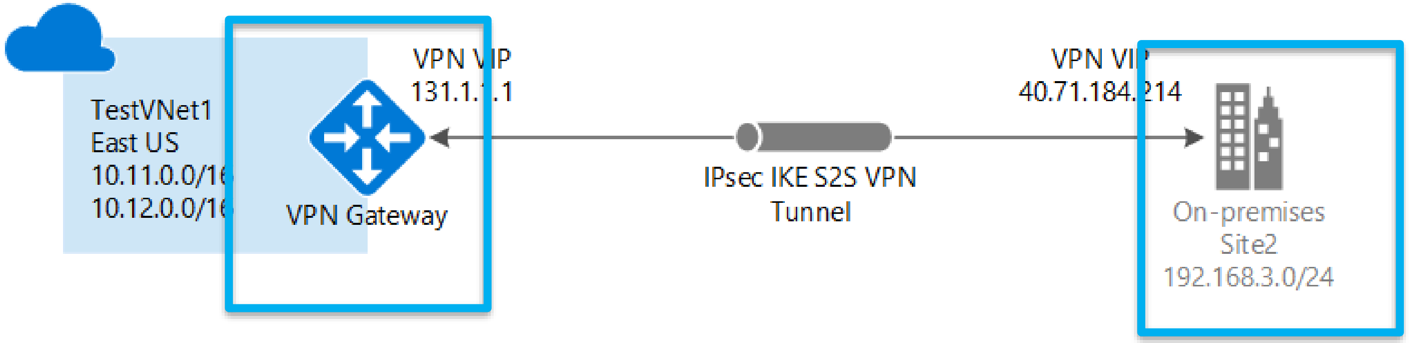


VNet Peering

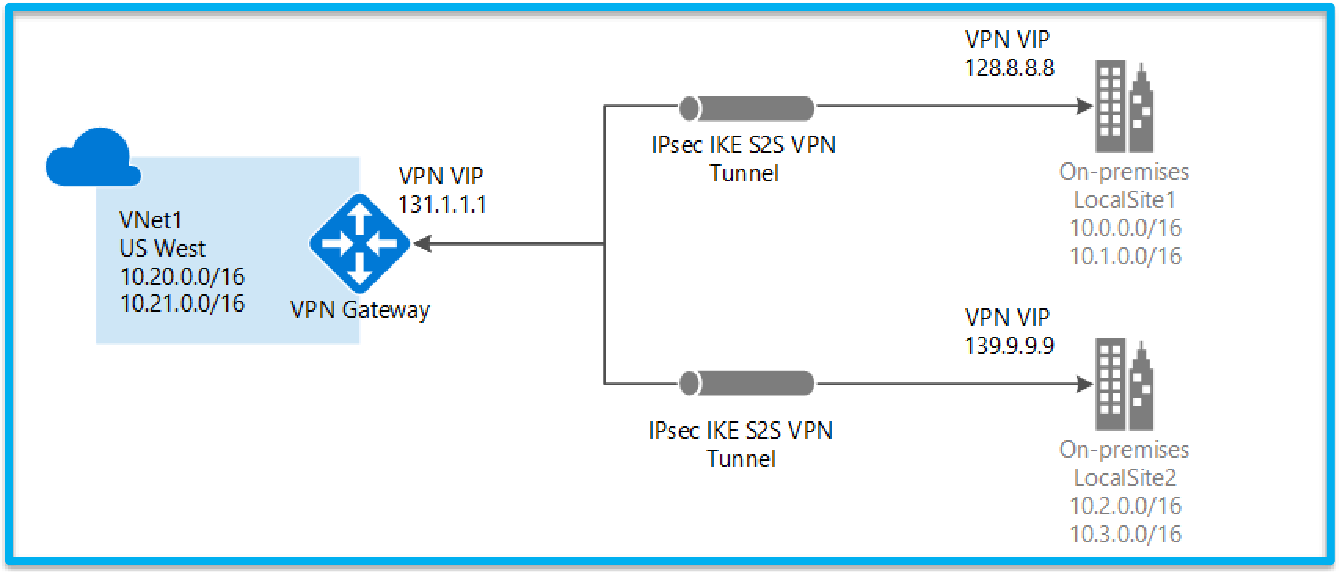


S2S

S2S

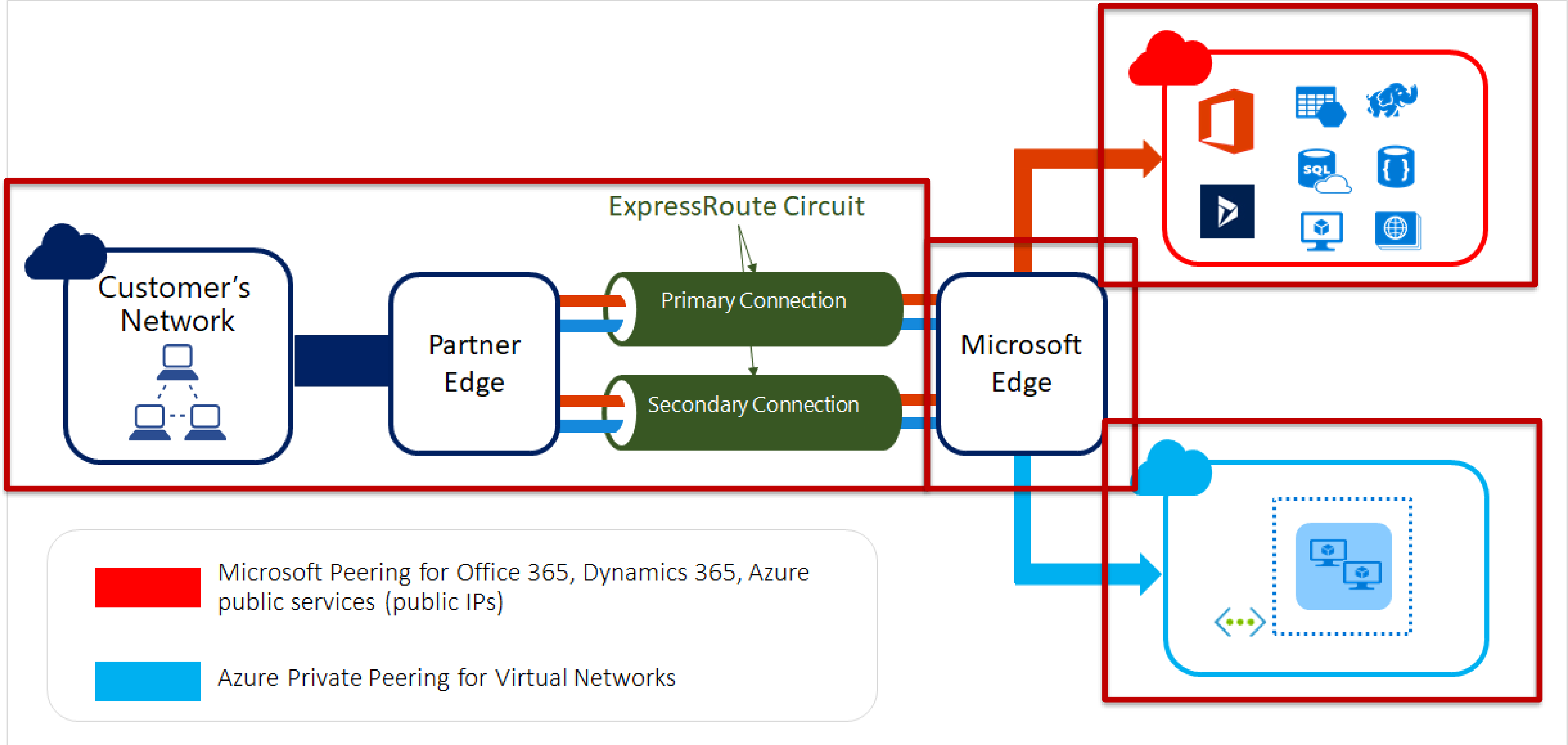


Multi-Site



https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

ExpressRoute

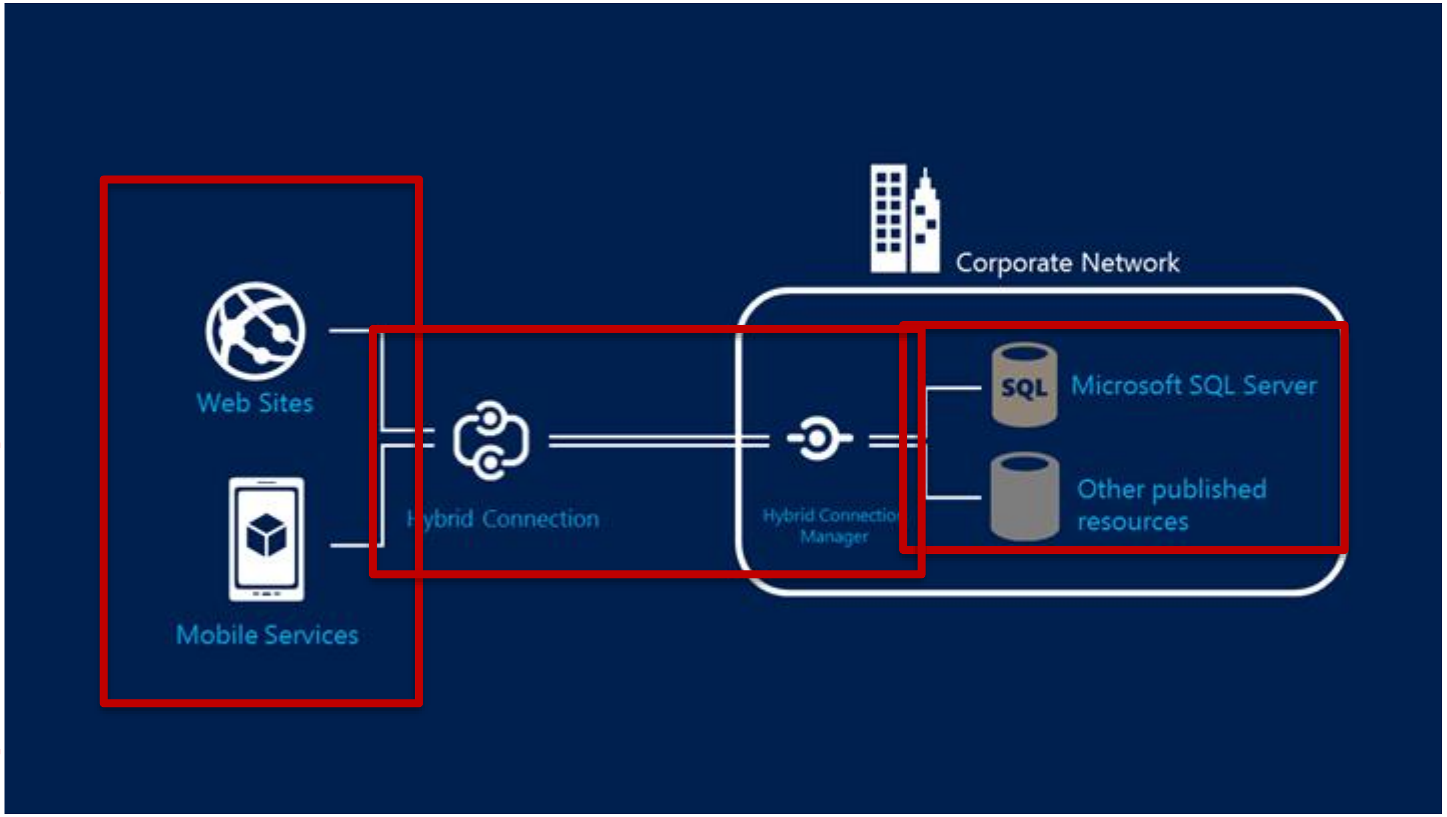


🟥 Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)

🟦 Azure Private Peering for Virtual Networks

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction

Hybrid Connection



- Allows Web App to talk to the datacenter
- Hybrid Connection can be shared across Web Apps and Mobile Apps
- All Web App Frameworks supported

Hybrid Connection Scenarios

- .NET Framework Access to SQL Server
- .NET Framework Access to HTTP/HTTPS Services with Web Client
- PHP Access to SQL Server, MySQL
- Java Access to SQL Server, MySQL and Oracle
- Java Access to HTTP/HTTPS Services

Hybrid Connection Manager Requirements

Hybrid Connection Manager can be installed on the following operating systems:

•Windows Server 2008 R2 (.NET Framework 4.5+ and Windows Management Framework 4.0+ required)

•Windows Server 2012 (Windows Management Framework 4.0+ required)

•Windows Server 2012 R2

Module:
Configure Name Resolution

SKYLINES
ACADEMY

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

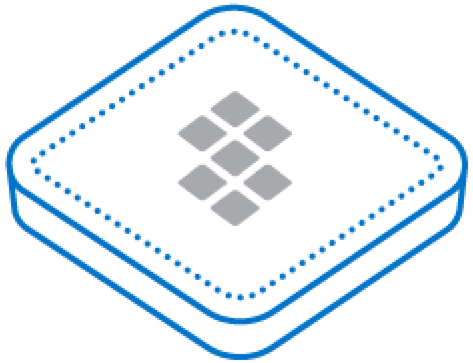
Inbound connectivity without SNAT requires public IP

DNS in Azure

Azure-provided DNS

Customer DNS Server

IaaS Server with DNS



Infoblox Virtual Appliance

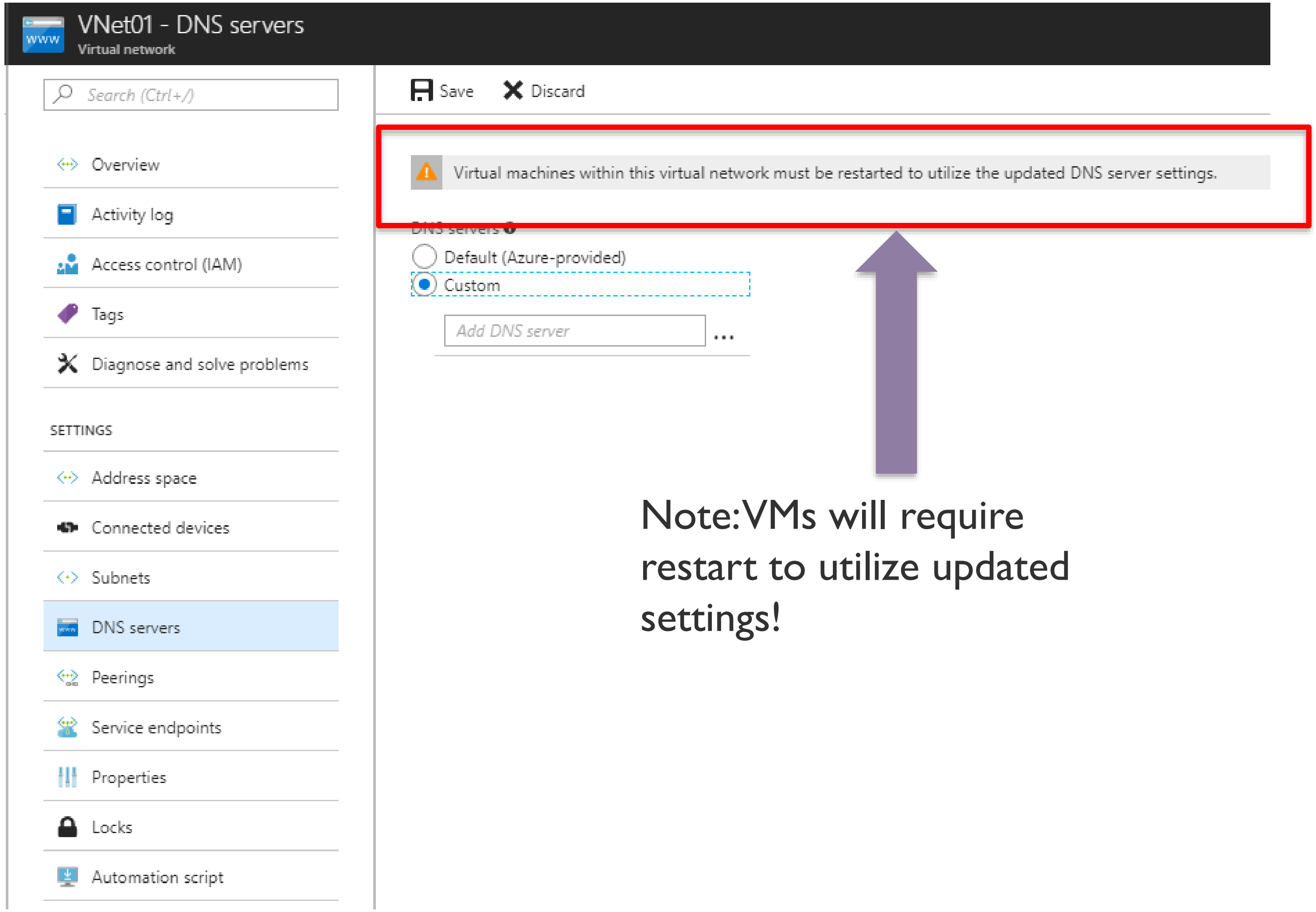
DNS Scenarios and Recommendations

SKYLINES ACADEMY

Scenario	Recommendation
Name resolution between role instances or virtual machines in the same virtual network	Azure provided DNS
Name resolution between role instances or virtual machines in different virtual networks	Customer-managed DNS Servers
Resolution of on-premises computers and service names from role instances or virtual machines in Azure	Customer-managed DNS Servers
Resolution of Azure hostnames from on-premises computers	Customer-managed DNS Servers

Configuring 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**



Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings.

DNS servers

○ Default (Azure-provided)
● Custom

Add DNS server ...

Note: VMs will require restart to utilize updated settings!

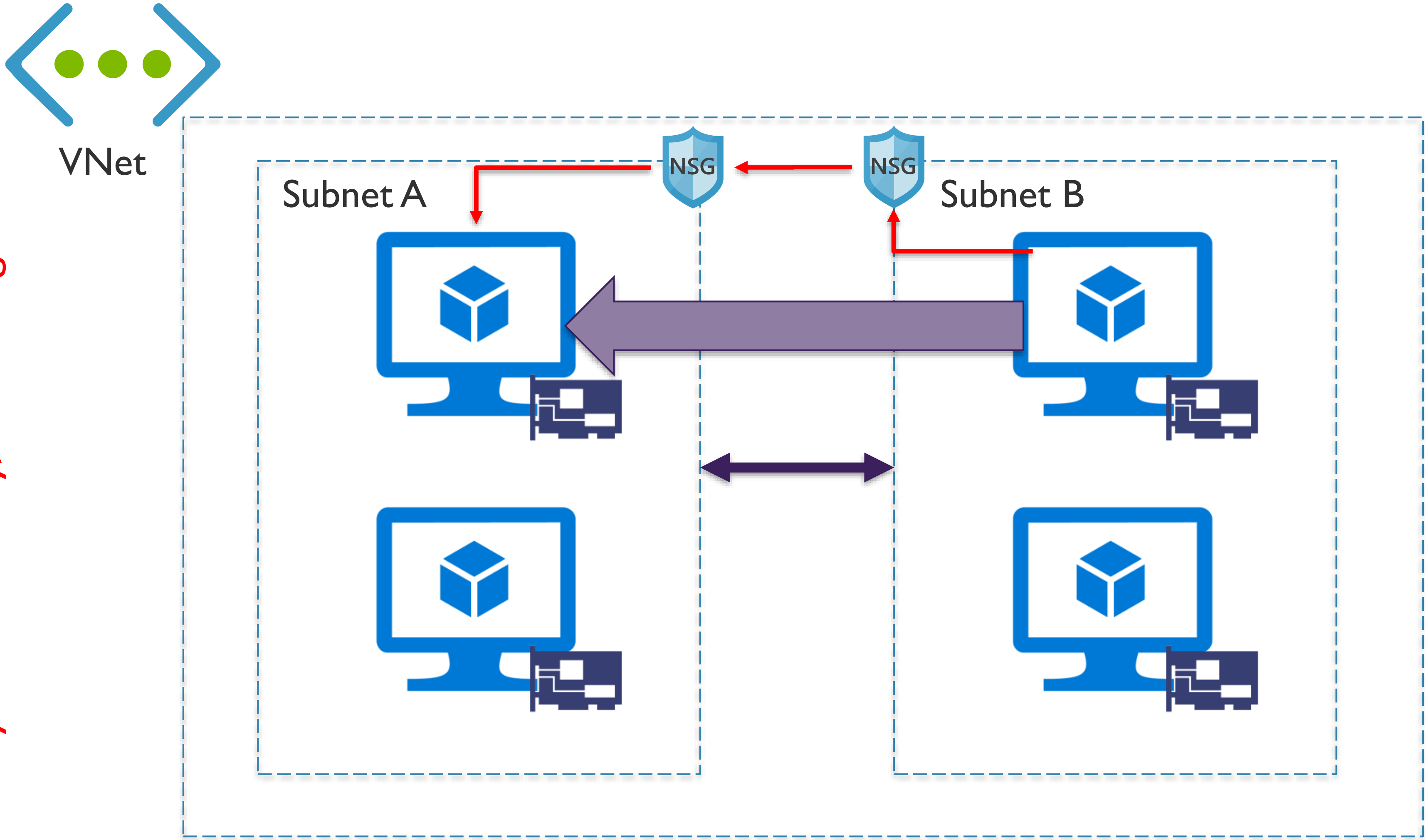
Module:
Create and Configure a Network Security Group (NSG)

SKYLINES
ACADEMY

Network Security Groups (NSGs)

- Is a network filter
- Used to allow or restrict traffic to resources in your Azure network
- Inbound rules
- Outbound rules
- Associated to subnet or NIC (and individual VMs in classic)

NSGs (continued)



- Can be applied to network interface or subnet
- Subnet rules apply to ALL resources in subnet

NSG Properties

Protocol (e.g. TCP, UDP)

Source and destination port range (1-65535 or * for all)

Source and destination address prefix (use ranges or default tags)

Direction (inbound or outbound)

Priority

Access (allow/deny)

NSG Rule Priority

SKYLINES
ACADEMY

Rules are enforced based on priority

Range from 100 to 4096

Lower numbers have higher priority

NSG Default Tags

System-provided to identify groups of IP addresses

Virtual network

Azure Load Balancer

Internet

NSG Default Rules

INBOUND

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

OUTBOUND

Name	Priority	Source IP	Source Port	Destination IP	Destination Port	Protocol
AllowVnet OutBound	65000	VirtualNetwork	*	VirtualNetwork	*	*
AllowInternetOutBound	65001	*	*	Internet	*	*
DenyAll OutBound	65500	*	*	*	*	*

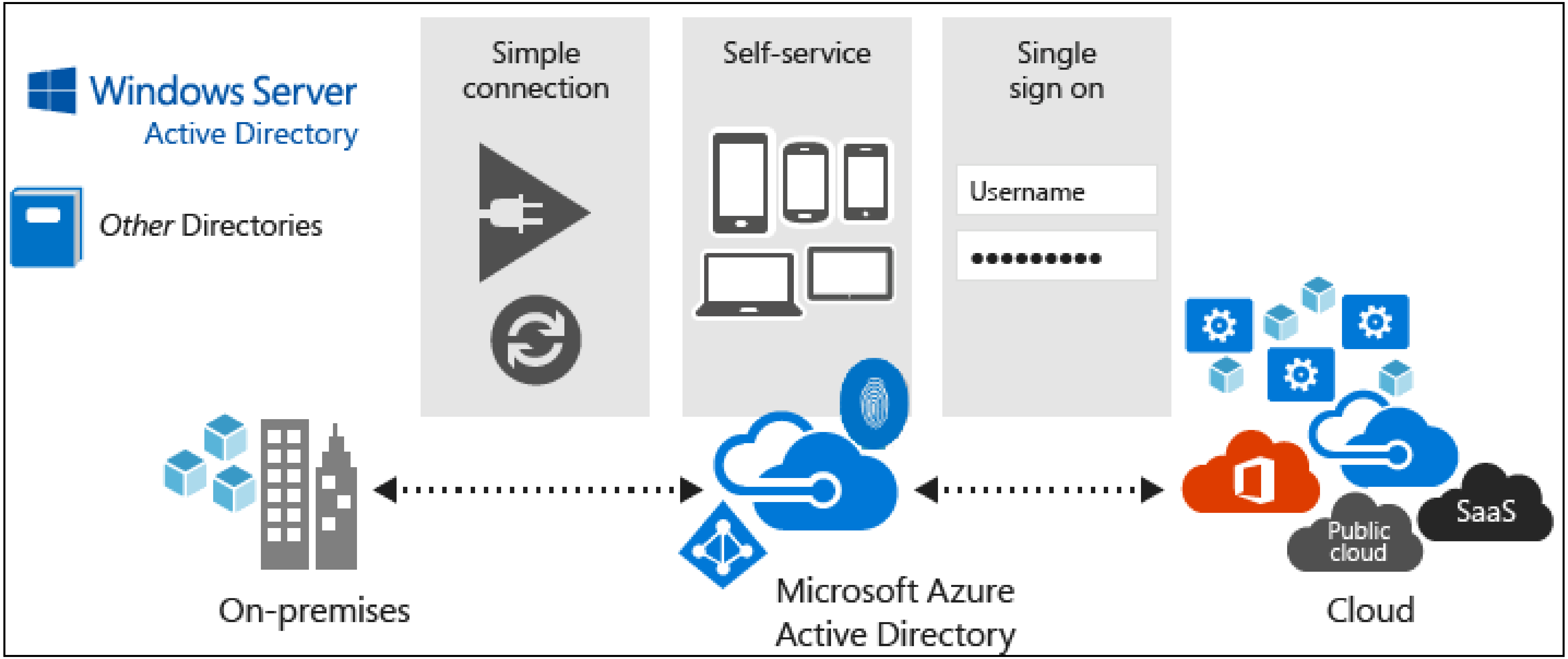
Networking Limits

The following limits apply only for networking resources managed through ARM per region per subscription:

Resource	Default Limit	Maximum Limit
Virtual networks per subscription	50	500
DNS Servers per virtual network	9	25
Virtual machines and role instances per virtual network	2048	2048
Concurrent TCP connections for a virtual machine or role instance	500k	500k
Network Interfaces (NIC)	300	1000
Network Security Groups (NSG)	100	400
NSG rules per NSG	200	500
User defined route tables	100	400
User defined routes per route table	100	500
Public IP addresses (dynamic)	60	Contact Support
Reserved public IP adresses	20	Contact Support
Load balancers (internal and internet facing)	100	Contact Support
Load balancer rules per load balancer	150	150
Public front end IP per load balander	5	Contact Support
Private front end IP per load balancer	1	Contact Support
Application Gateways	50	50

Module:
Manage Azure Active Directory (AAD)

Azure AD Overview



https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Azure AD Features

Enterprise Identity Solution

Create a single identity for users and keep them in sync across the enterprise.

Single Sign-On

Provide single sign-on access to applications and infrastructure services.

Multifactor Authentication (MFA)

Enhance security with additional factors of authentication.

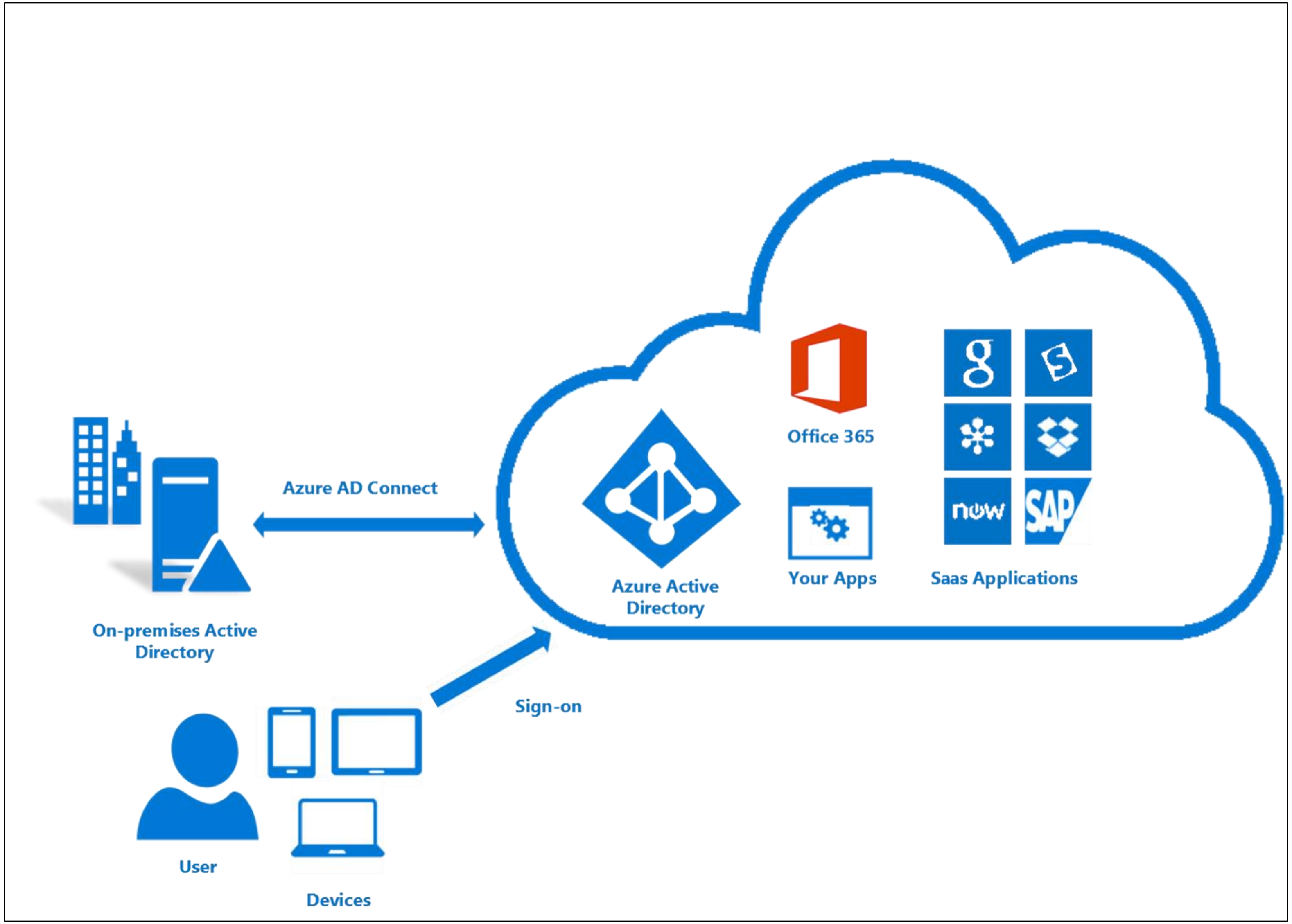
Self Service

Empower your users to complete password resets themselves, as well as request access to specific apps and services.

Missing Module:
Implement and Manage Hybrid Identities

SKYLINES ACADEMY

AD Connect Overview



AD Connect Components

Synchronization Services

Active Directory Federation Services (optional)

Health Monitoring

AD Connect Sync Features

Filtering

Password hash syncronization

Password writeback

Device writeback

Prevent accidental deletes

Automatic upgrade

Password Sync Options

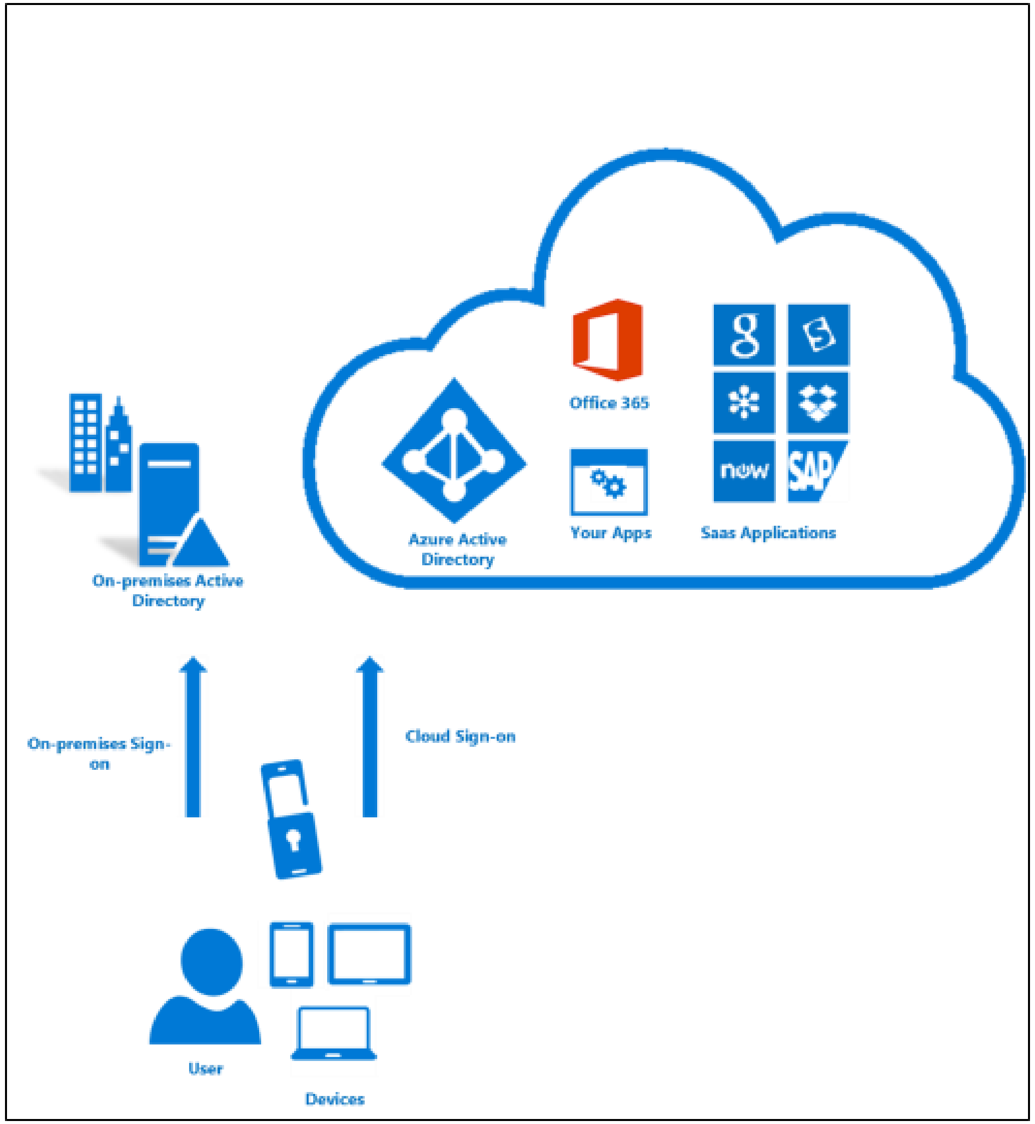
- Password Sync – Ensures user passwords are the same in both directories (AD DS and Azure AD)
- Passthrough Authentication – Easy method to keep users and passwords aligned. When a user logs into Azure AD, the request is forwarded to AD DS. Essentially, a single source.
- AD FS – Use AD Federation Services server to fully federate across AD DS and Azure AD, along with other services.

Single Sign On

- Provided by Azure AD Connect for users using password sync or passthrough authentication
- Company device with modern browser required
- User not required to authenticate with Azure AD if they are logged on with their AD DS credentials

Multifactor Authentication (MFA)

- Works by requiring 2 or more of the following verification methods:
  - Something you know (Password)
  - Something you have (e.g. Cellphone)
  - Something you are (Biometrics)



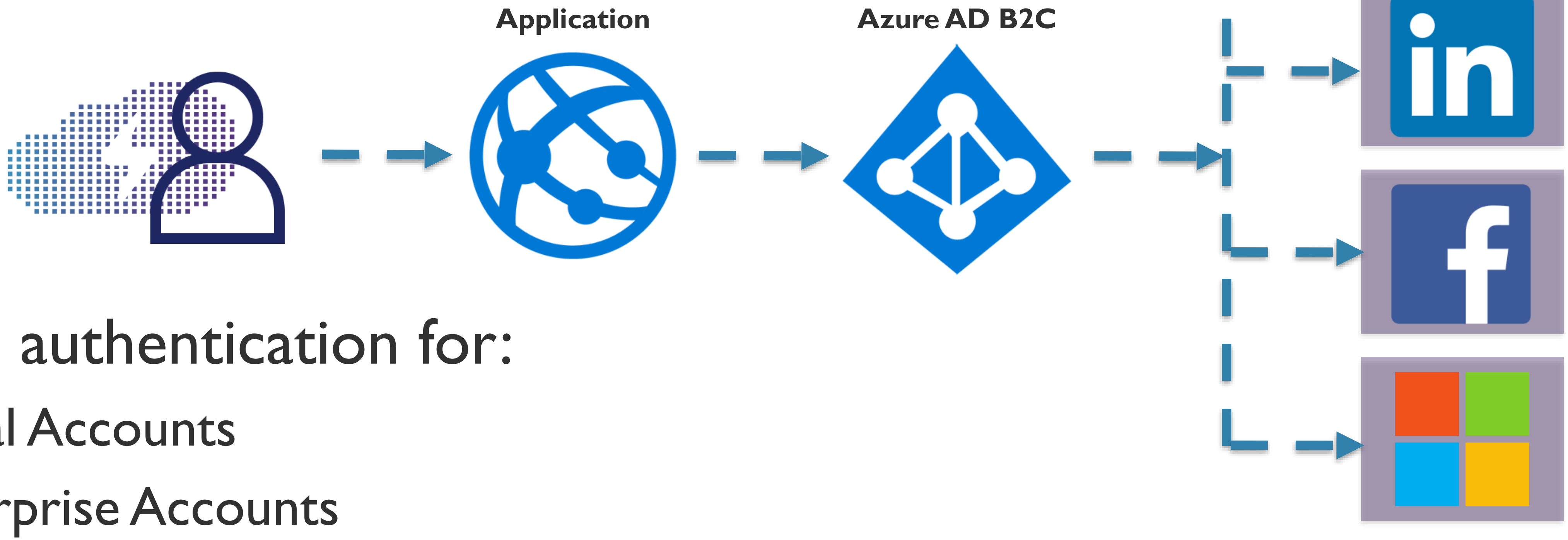
Multifactor Authentication (MFA)

SKYLINES ACADEMY

Verification Method	Description
Phone call	A call is placed to a user's registered phone. The user enters a PIN if necessary then presses the # key.
Text message	A text message is sent to a user's mobile phone with a six-digit code. The user enters this code on the sign-in page.
Mobile app notification	A verification request is sent to a user's smart phone. The user enters a PIN if necessary then selects **Verify** on the mobile app.
Mobile app verification code	The mobile app, which is running on a user's smart phone, displays a verification code that changes every 30 seconds. The user finds the most recent code and enters it on the sign-in page.
Third-party tokens	Azure Multi-Factor Authentication Server can be configured to accept third-party verification methods.

Azure AD B2C

- Cloud Identity Solution for Web and Mobile Apps
- Highly scalable to hundreds of millions of identities



- Enables authentication for:
  - Social Accounts
  - Enterprise Accounts
  - Local Accounts

Azure AD B2B

- Allows you to collaborate with partners outside of your organization
- Users receive an email with a confirmation link upon invitation
- Imported users are "Azure AD External User Objects"
- Access to shared apps, resources, documents, etc.
- Partners access with their own credentials
- Enterprise-level security

Module:
Azure Resource Manager (ARM)

SKYLINES ACADEMY

Resource Manager Overview

Resource

Individual manageable item available to you in Azure

Resource Group

Container where you can house your resources for management

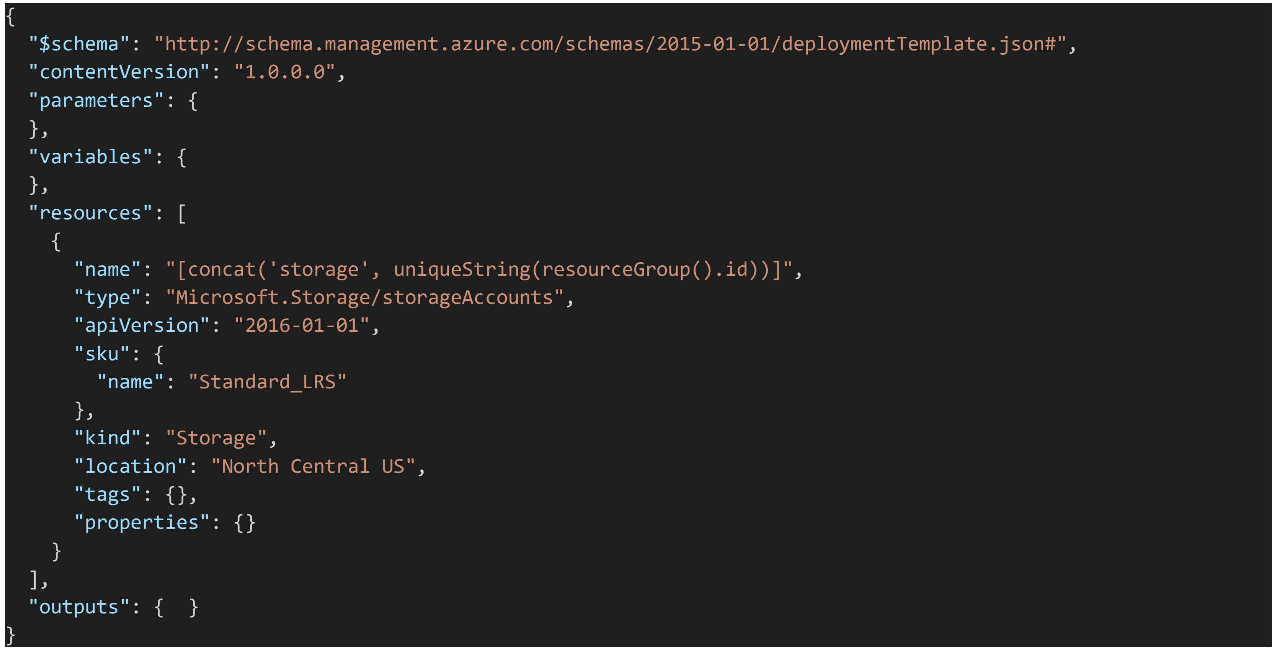
Resource Provider

Provider of services you can deploy in Azure e.g. Microsoft.Compute

ARM Templates

Files used to define resources you wish to deploy to a resource group

ARM Templates Overview

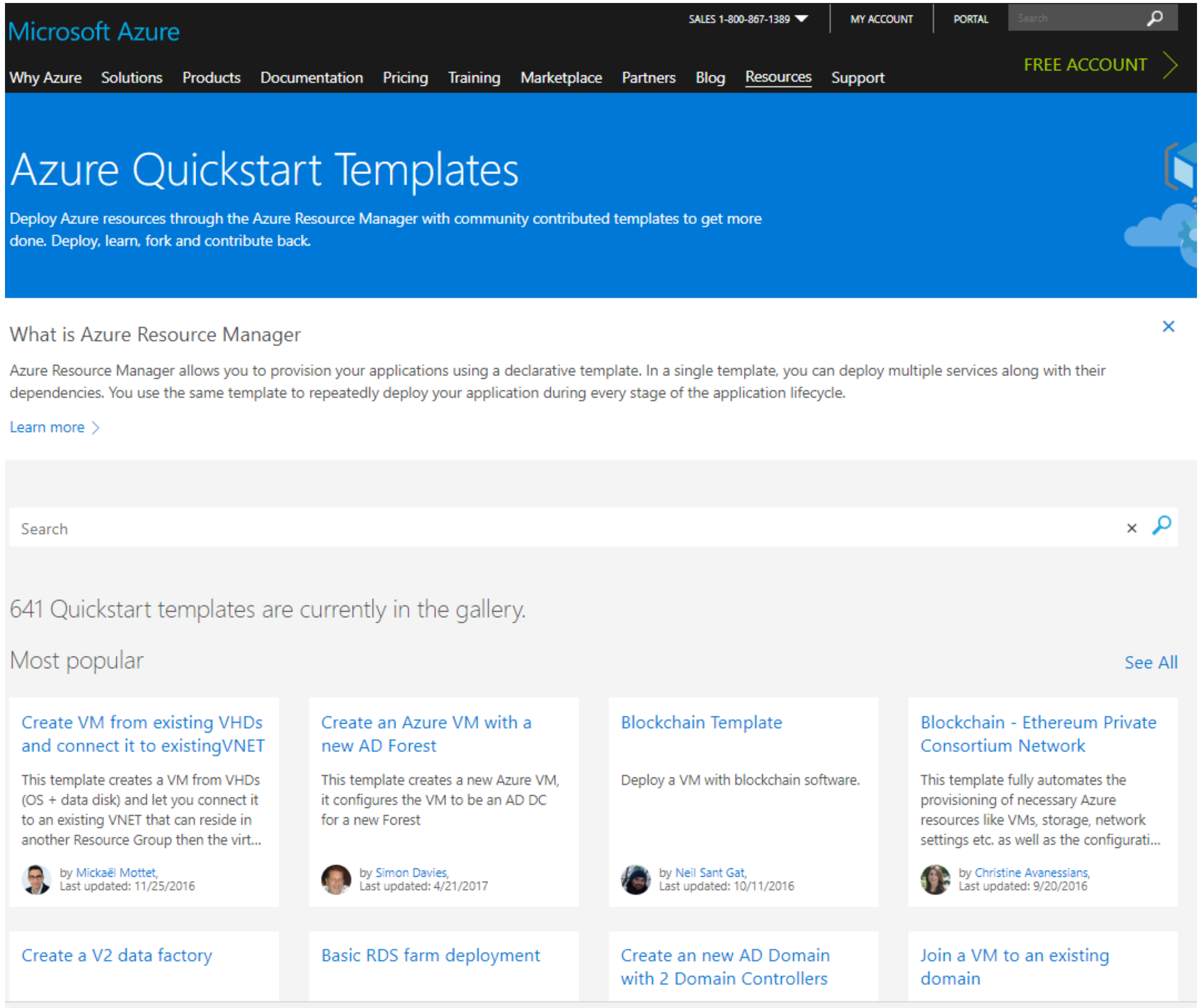


```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
  },
  "variables": {
  },
  "resources": [
    {
      "name": "[concat('storage', uniqueString(resourceGroup().id))]",
      "type": "Microsoft.Storage/storageAccounts",
      "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

Quickstart Templates



Azure Quickstart Templates

Deploy Azure resources through the Azure Resource Manager with community contributed templates to get more done. Deploy, learn, fork and contribute back.

What is Azure Resource Manager

Azure Resource Manager allows you to provision your applications using a declarative template. In a single template, you can deploy multiple services along with their dependencies. You use the same template to repeatedly deploy your application during every stage of the application lifecycle.

Learn more

Search

641 Quickstart templates are currently in the gallery.

Most popular

See All

Create VM from existing VHDs and connect it to existingVNET

This template creates a VM from VHDs (OS + data disk) and let you connect it to an existing VNET that can reside in another Resource Group then the virt...

by Mickaël Mottet,
Last updated: 11/25/2016

Create an Azure VM with a new AD Forest

This template creates a new Azure VM, it configures the VM to be an AD DC for a new Forest

by Simon Davies,
Last updated: 4/21/2017

Blockchain Template

Deploy a VM with blockchain software.

by Neil Sant Gat,
Last updated: 10/11/2016

Blockchain - Ethereum Private Consortium Network

This template fully automates the provisioning of necessary Azure resources like VMs, storage, network settings etc. as well as the configurati...

by Christine Avanessians,
Last updated: 9/20/2016

Create a V2 data factory

Basic RDS farm deployment

Create an new AD Domain with 2 Domain Controllers

Join a VM to an existing domain

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

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

ARM File Types

ARM Template File

Describe the configuration of your infrastructure via a JSON file

ARM Template Parameter File

Separate your parameters (optional)

Deployment Scripts

E.g. PowerShell for Deployment

ARM Template Constructs

Parameters

Define the inputs you want to pass into the ARM template during deployment.

Variables

Values that you can use throughout your template. Used to simplify your template by creating reuse of values.

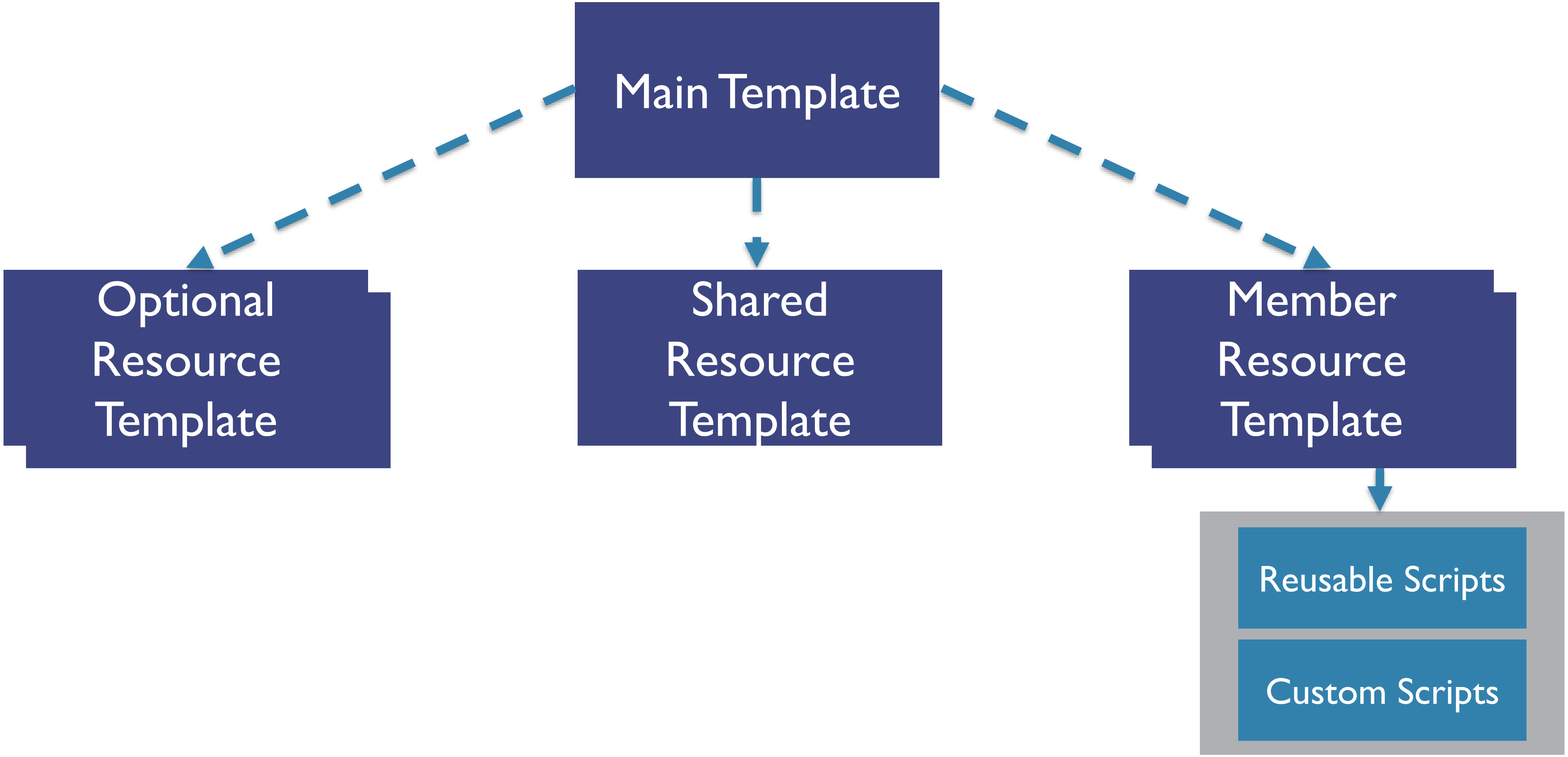
Resources

Define the resources you wish to deploy or update.

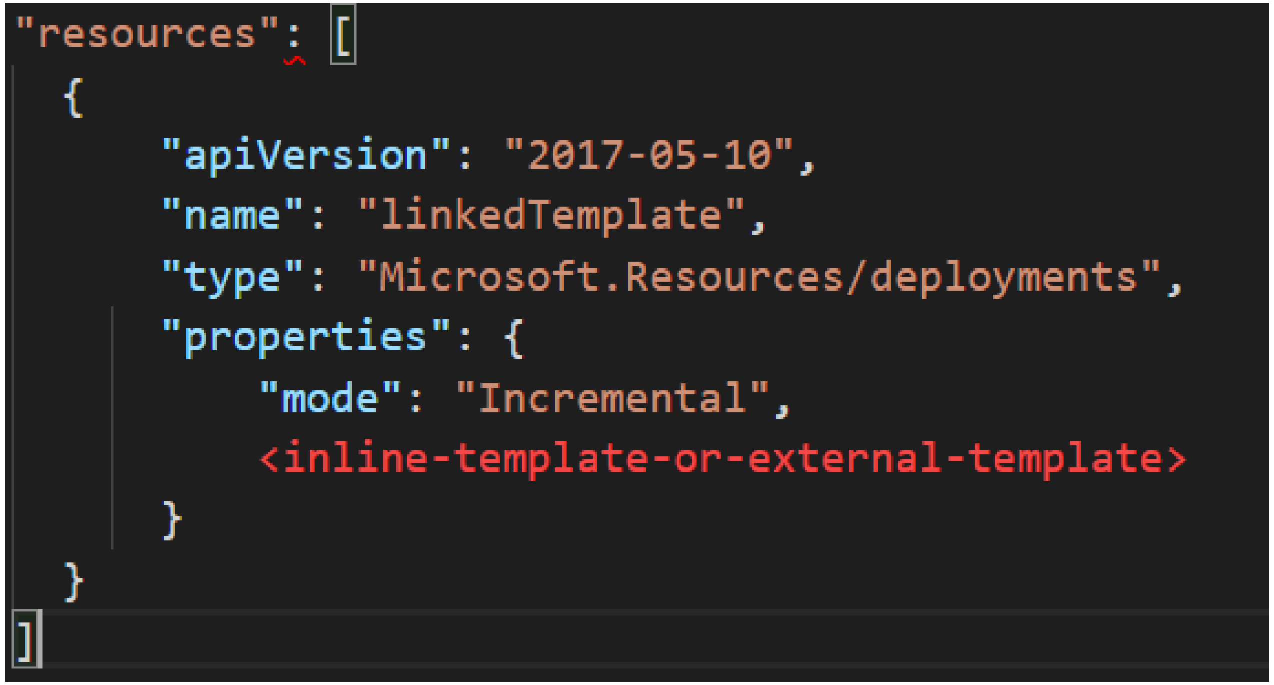
Outputs

Specify values that are returned after the ARM deployment is completed.

Linking Templates



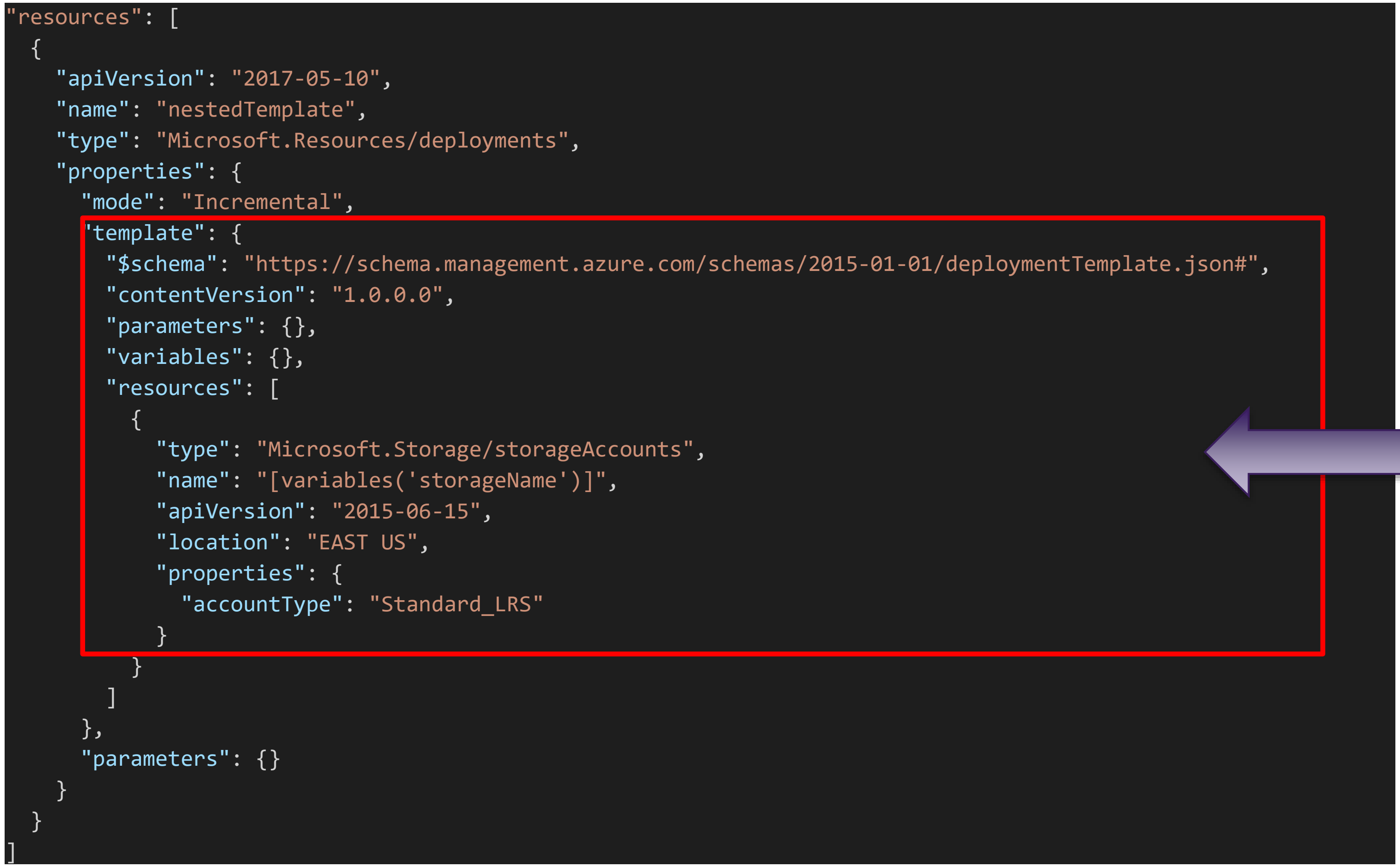
Linking Templates (continued)



```
"resources": [
  {
      "apiVersion": "2017-05-10",
      "name": "linkedTemplate",
      "type": "Microsoft.Resources/deployments",
      "properties": {
          "mode": "Incremental",
          <inline-template-or-external-template>
      }
  }
]
```

- Inline
  - Create entire ARM template in body of existing template
- External
  - Link to an external template with an INLINE or EXTERNAL parameter set

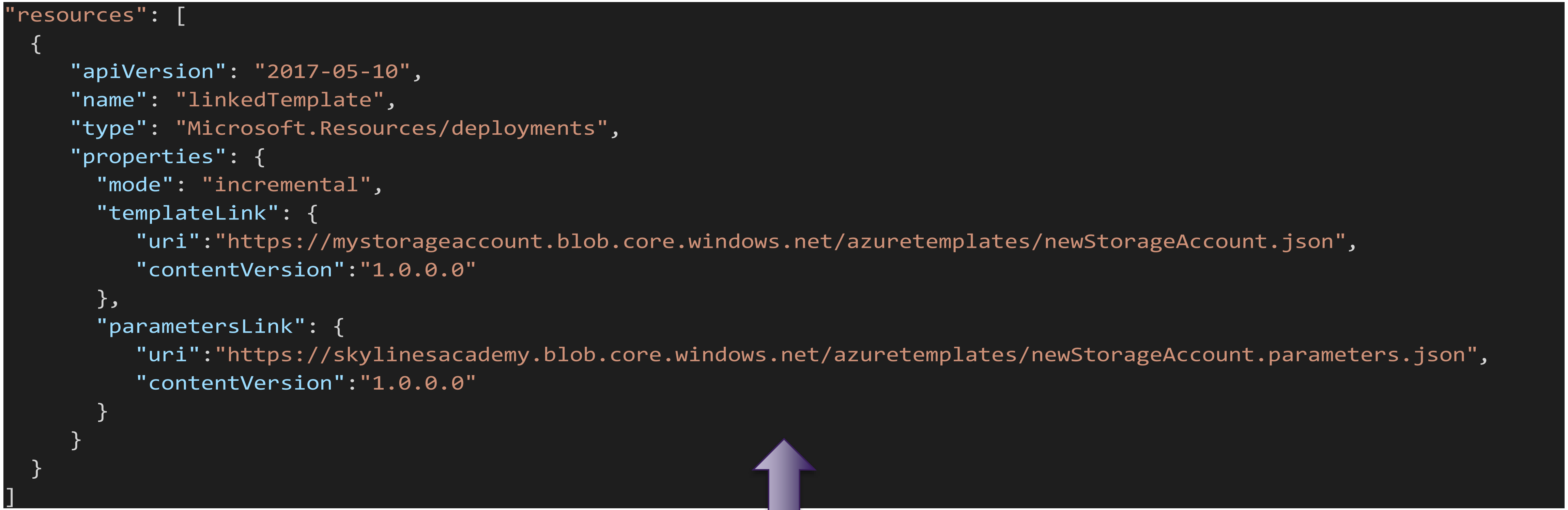
Inline Example



```
"resources": [
  {
    "apiVersion": "2017-05-10",
    "name": "nestedTemplate",
    "type": "Microsoft.Resources/deployments",
    "properties": {
      "mode": "Incremental",
      "template": {
        "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
        "contentVersion": "1.0.0.0",
        "parameters": {},
        "variables": {},
        "resources": [
          {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[variables('storageName')]",
            "apiVersion": "2015-06-15",
            "location": "EAST US",
            "properties": {
              "accountType": "Standard_LRS"
            }
          }
        ]
      },
      "parameters": {}
    }
  }
]
```

New Template created in the body of the current ARM template

External Example



```
"resources": [
  {
     "apiVersion": "2017-05-10",
     "name": "linkedTemplate",
     "type": "Microsoft.Resources/deployments",
     "properties": {
       "mode": "incremental",
       "templateLink": {
          "uri":"https://mystorageaccount.blob.core.windows.net/azuretemplates/newStorageAccount.json",
          "contentVersion":"1.0.0.0"
       },
       "parametersLink": {
          "uri":"https://skylinesacademy.blob.core.windows.net/azuretemplates/newStorageAccount.parameters.json",
          "contentVersion":"1.0.0.0"
       }
     }
  }
]
```

Template and parameters linked inside current ARM templates

Key ARM Functions

Copy

copyIndex()

dependsOn

SKYLINES

ACADEMY