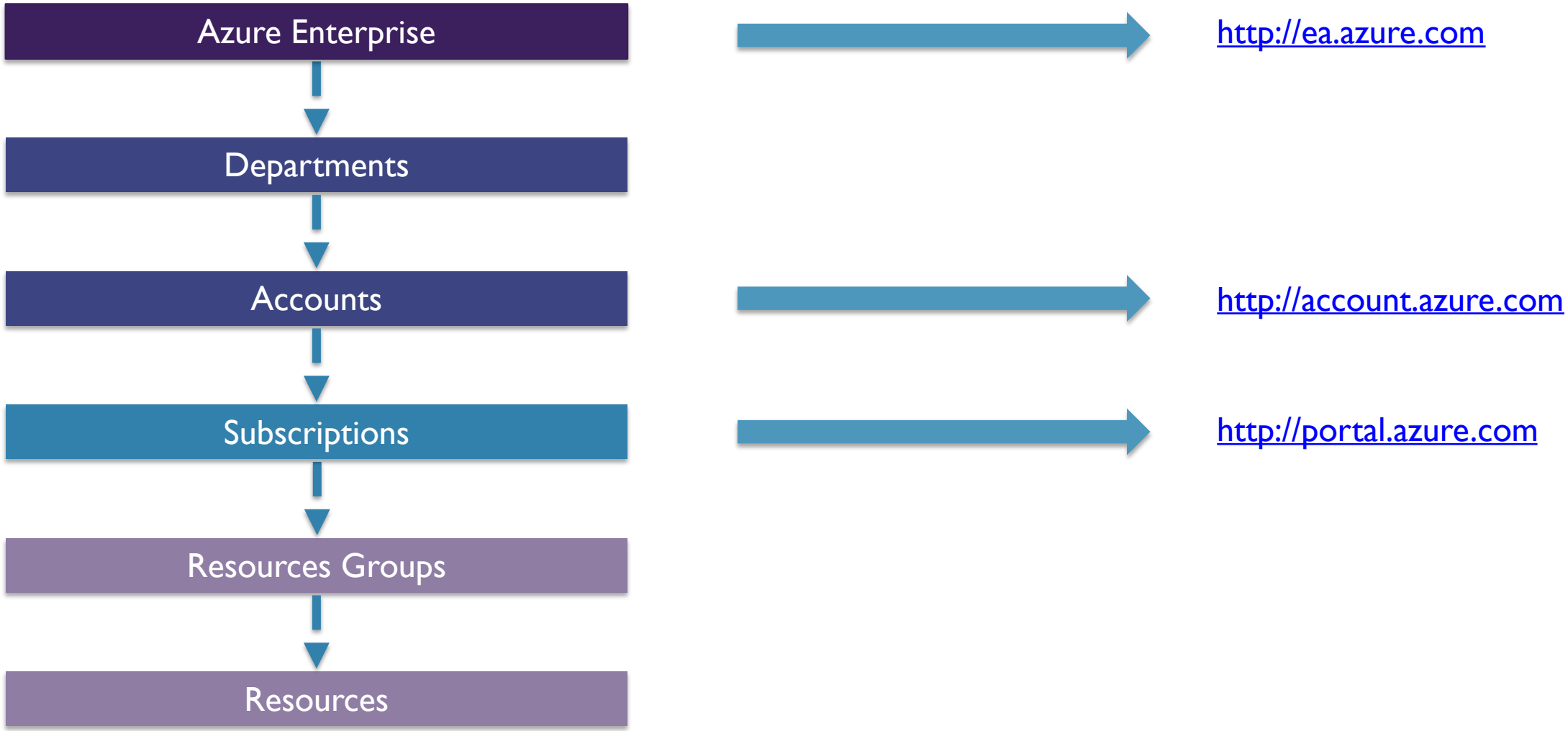
SKYLINES

ACADEMY

Module:
Manage Azure Subscriptions

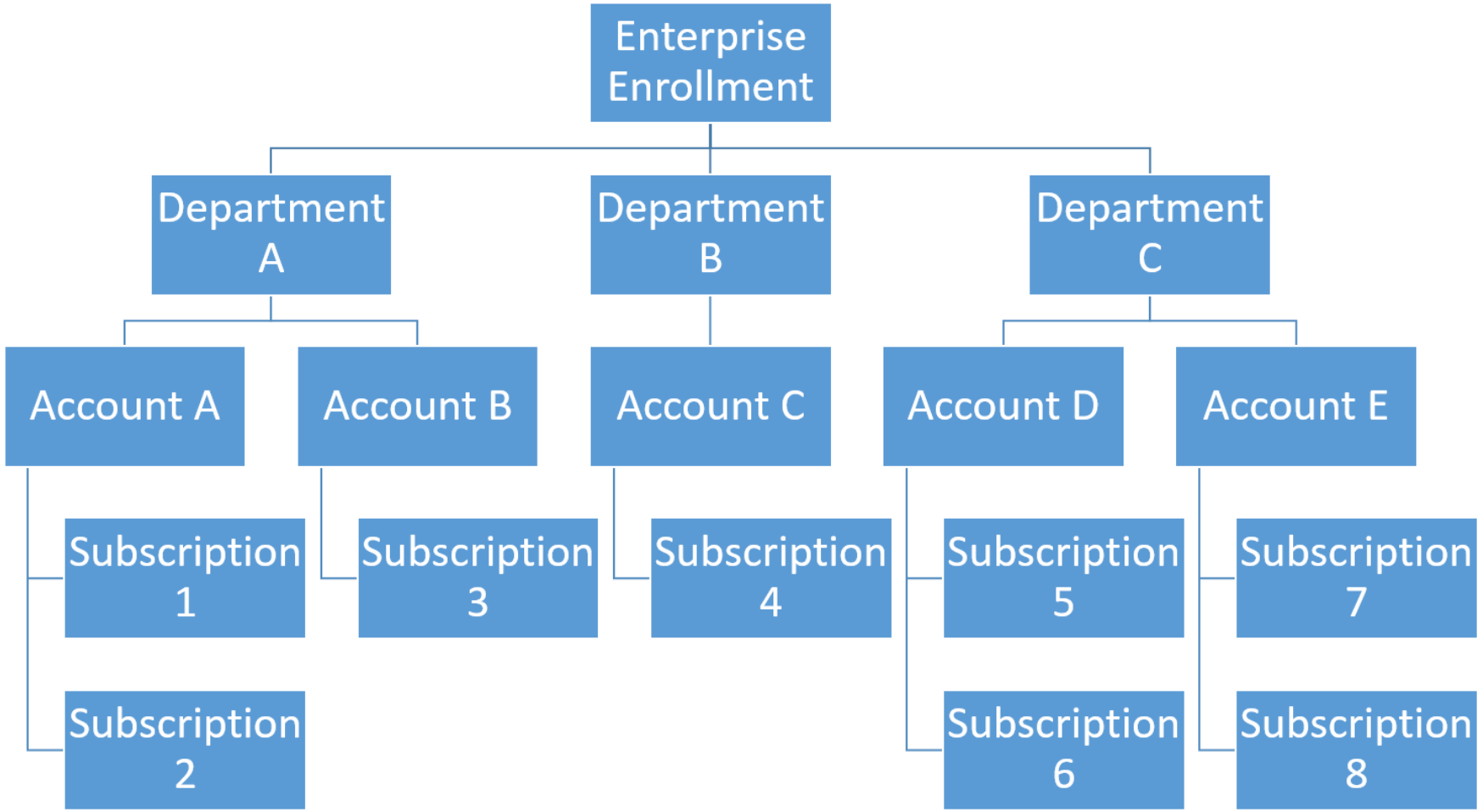
SKYLINES
ACADEMY

Azure Account Hierarchy



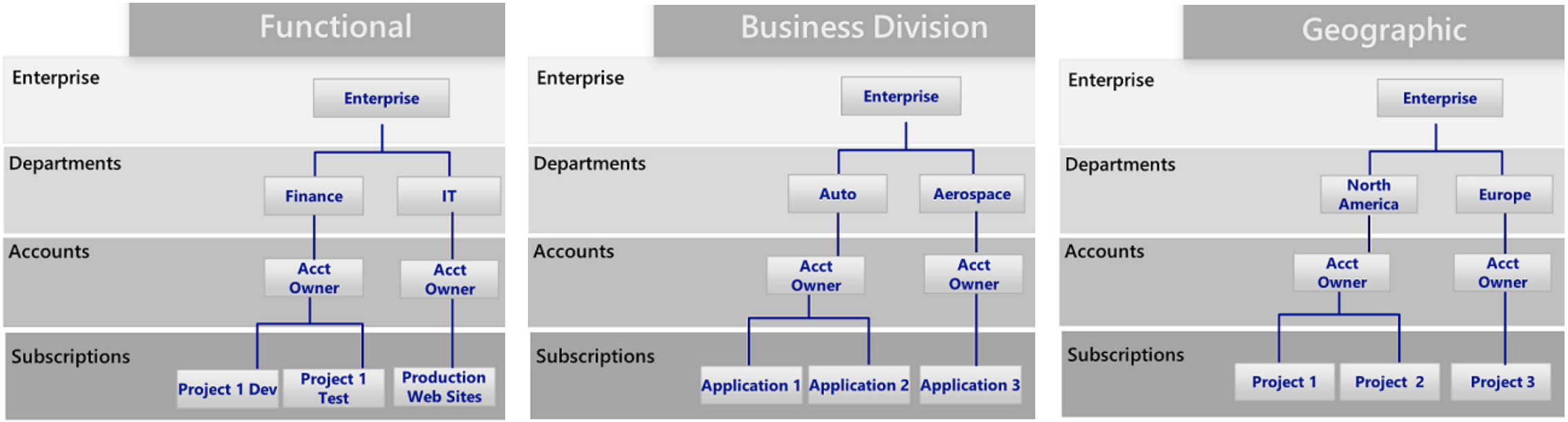
Account to Subscription Relationships

Enterprise Hierarchy Example



Common Scenarios

SKYLINES ACADEMY



EA Breakdown

SKYLINES ACADEMY

	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

SKYLINES
ACADEMY

Azure Monitoring Overview

SKYLINES ACADEMY

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

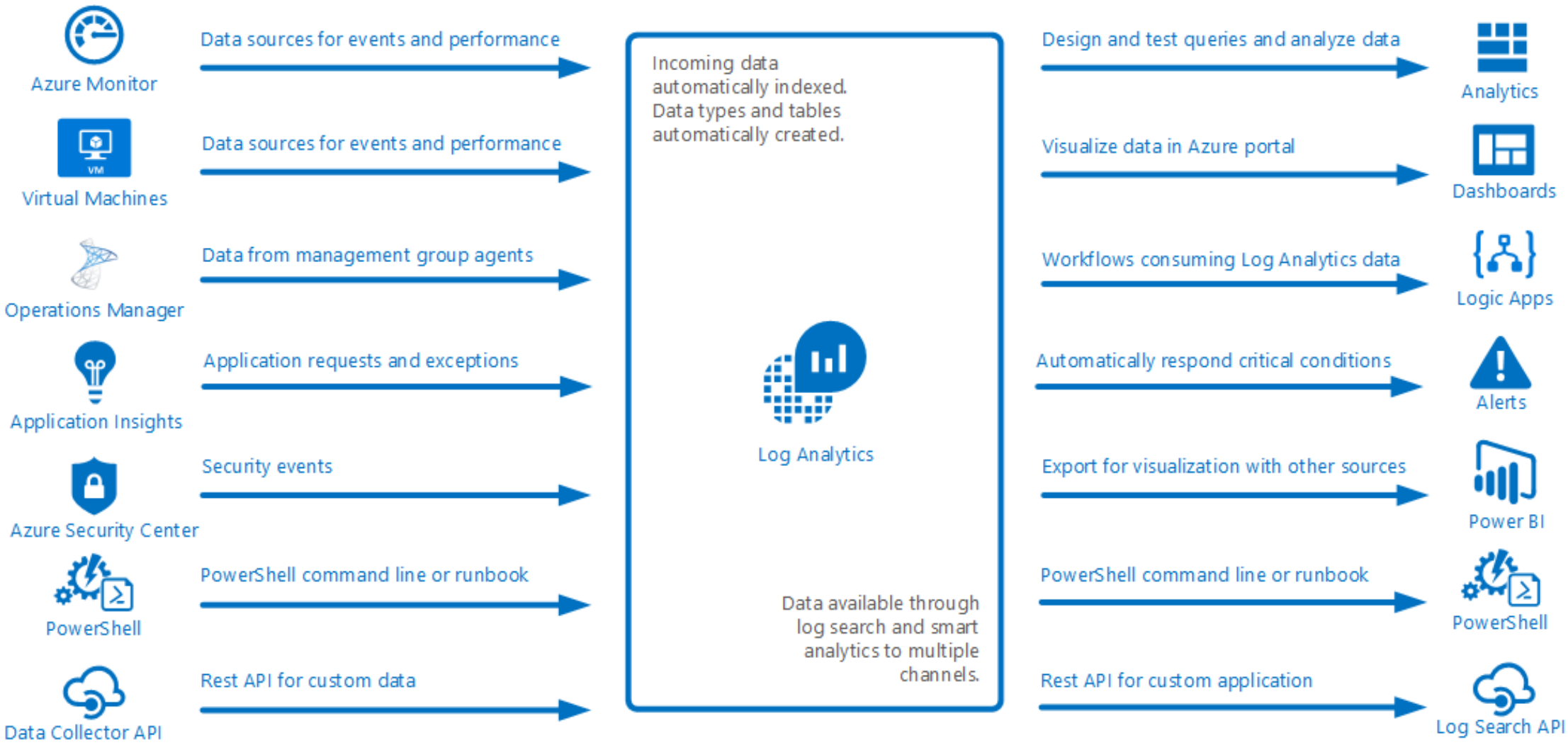
Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

Log Analytics Key Features

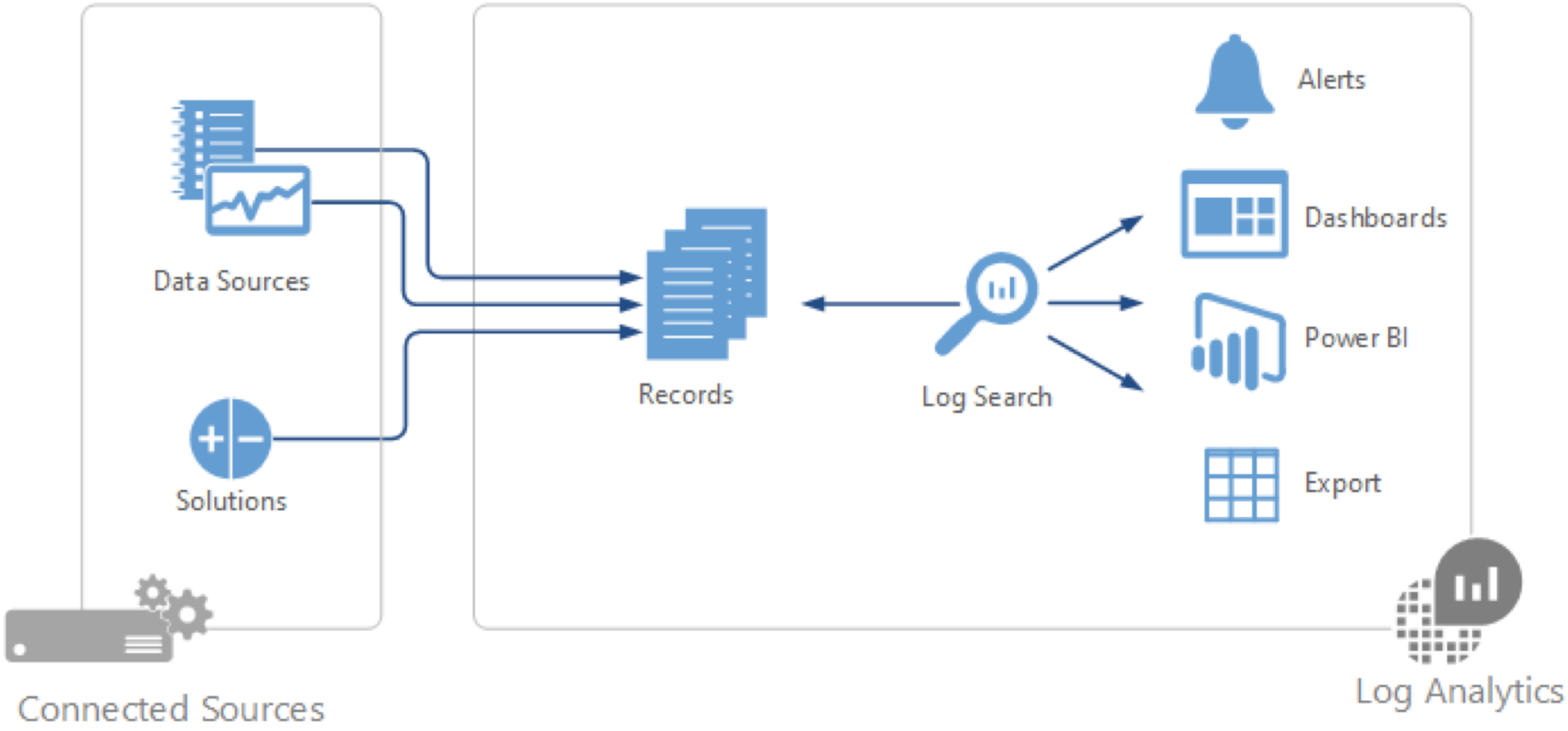
SKYLINES ACADEMY

- Central Role in Monitoring
- Data Sources
- Other Log Analytics Sources (Security Center and App Insights)
- Search Queries
- Output Options

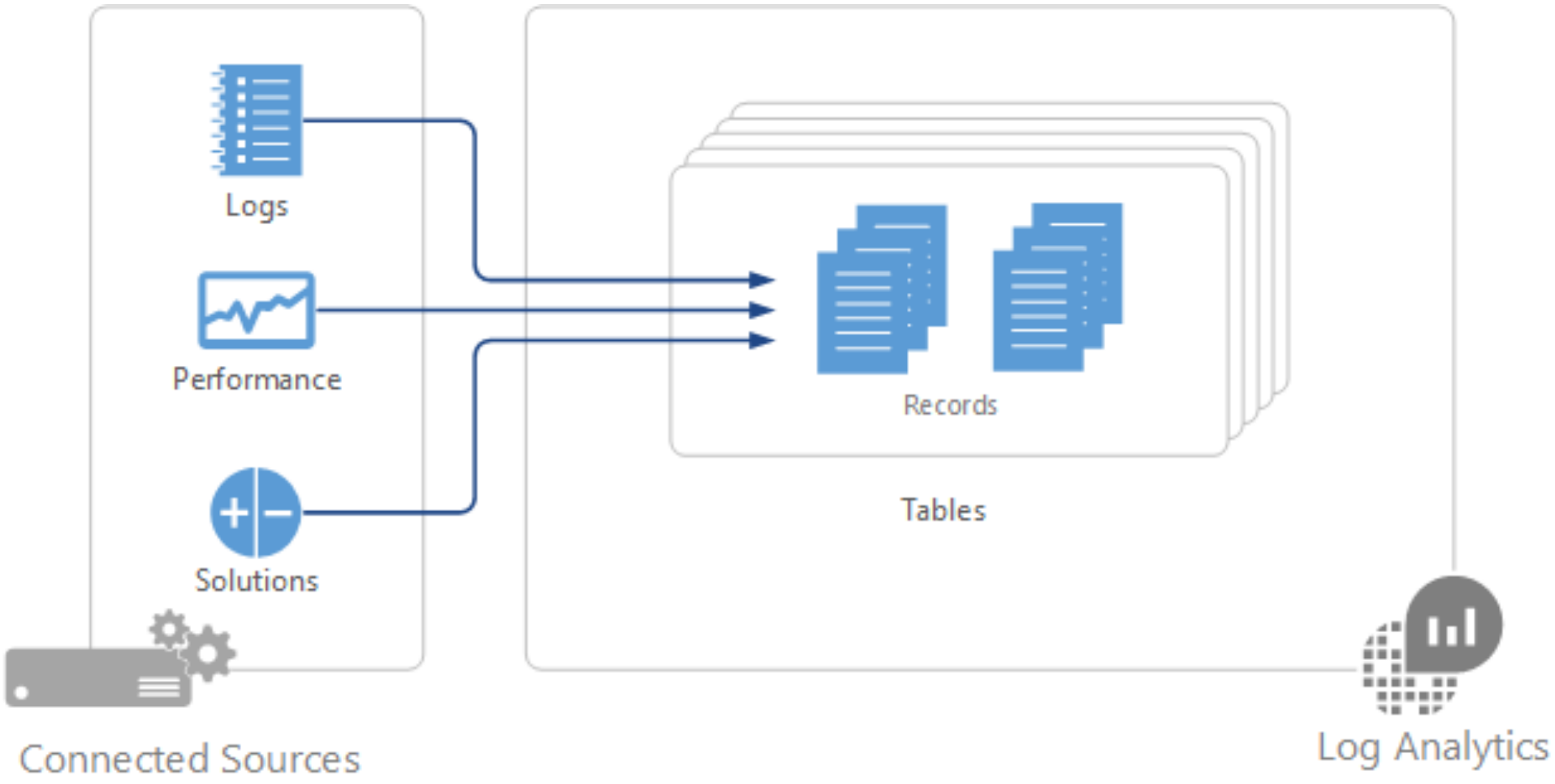
Log Search Use Cases



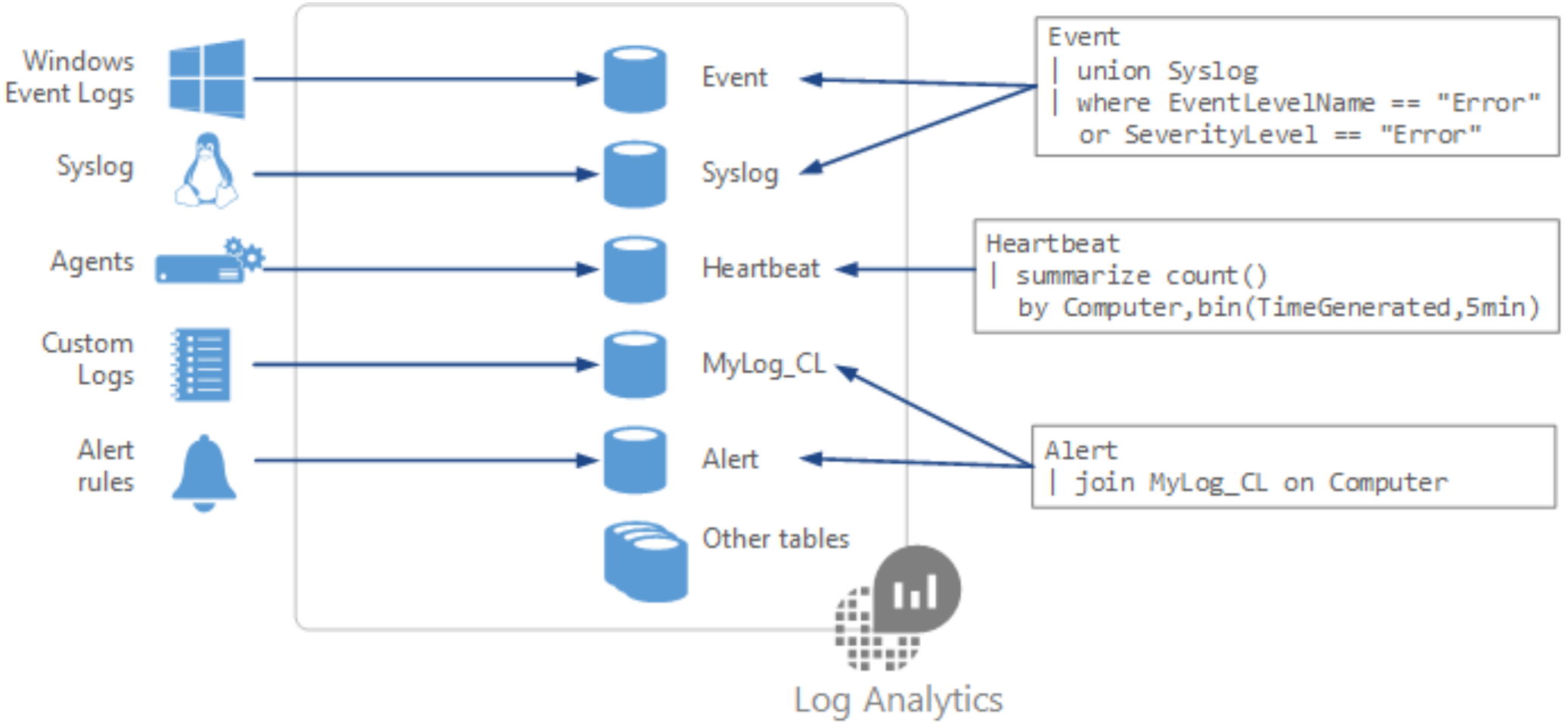
Log Analytics Architecture



Data Sources



Data Organization



Summary Data Sources

SKYLINES ACADEMY

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

SKYLINES ACADEMY

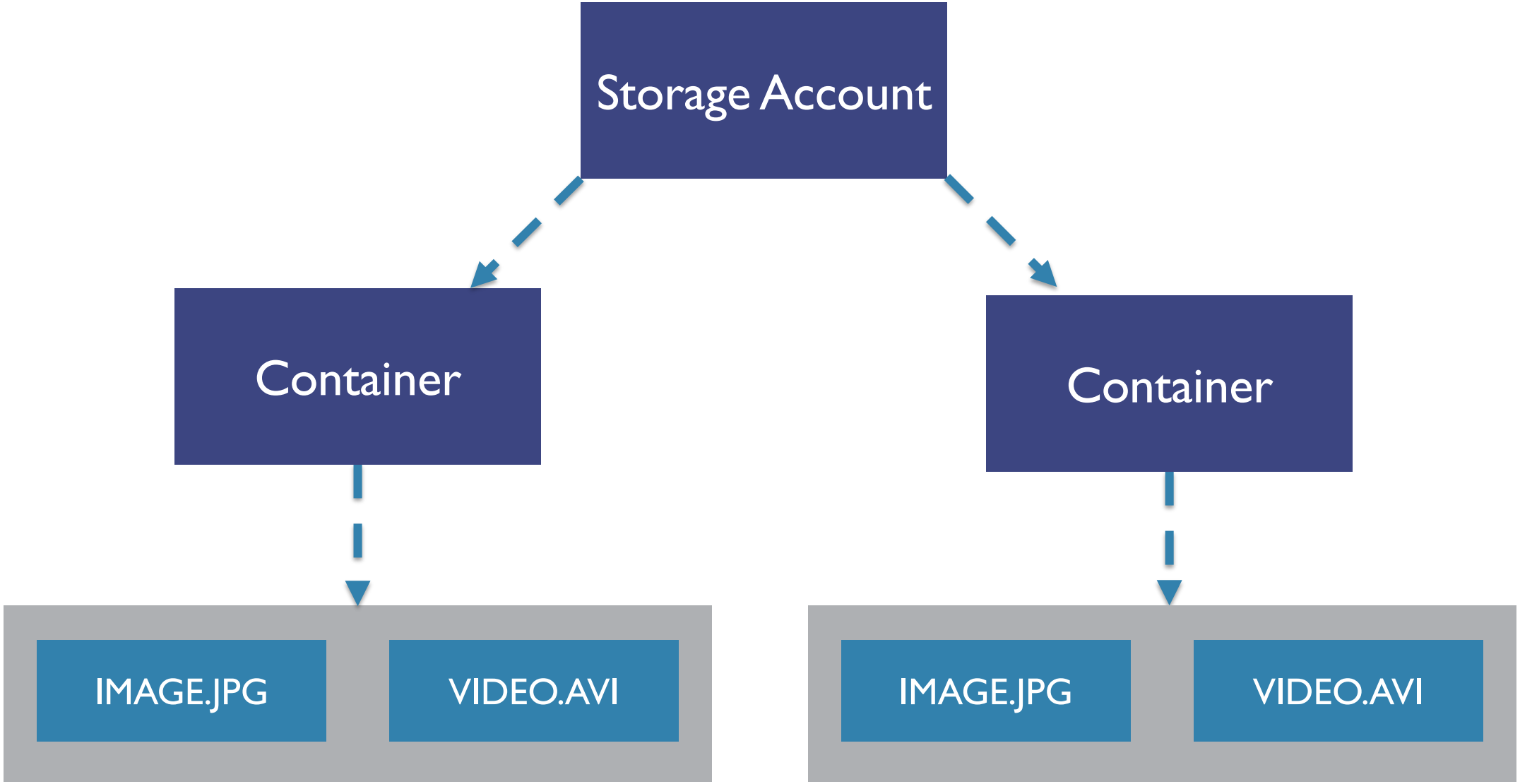
- Start with the source table (e.g. Event)
- Follow on with a series of operators
- Separate out additional operations by using pipe |
- Join other tables and workspaces using "union"

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

Module: Storage

Azure Blob Storage Overview

SKYLINES ACADEMY



Storage Account Types

SKYLINES ACADEMY

General Purpose v1 (GPV1)

Blob Account

General Purpose v2 (GPV2)

Block Blobs vs. Page Blobs

SKYLINES ACADEMY

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

SKYLINES ACADEMY

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

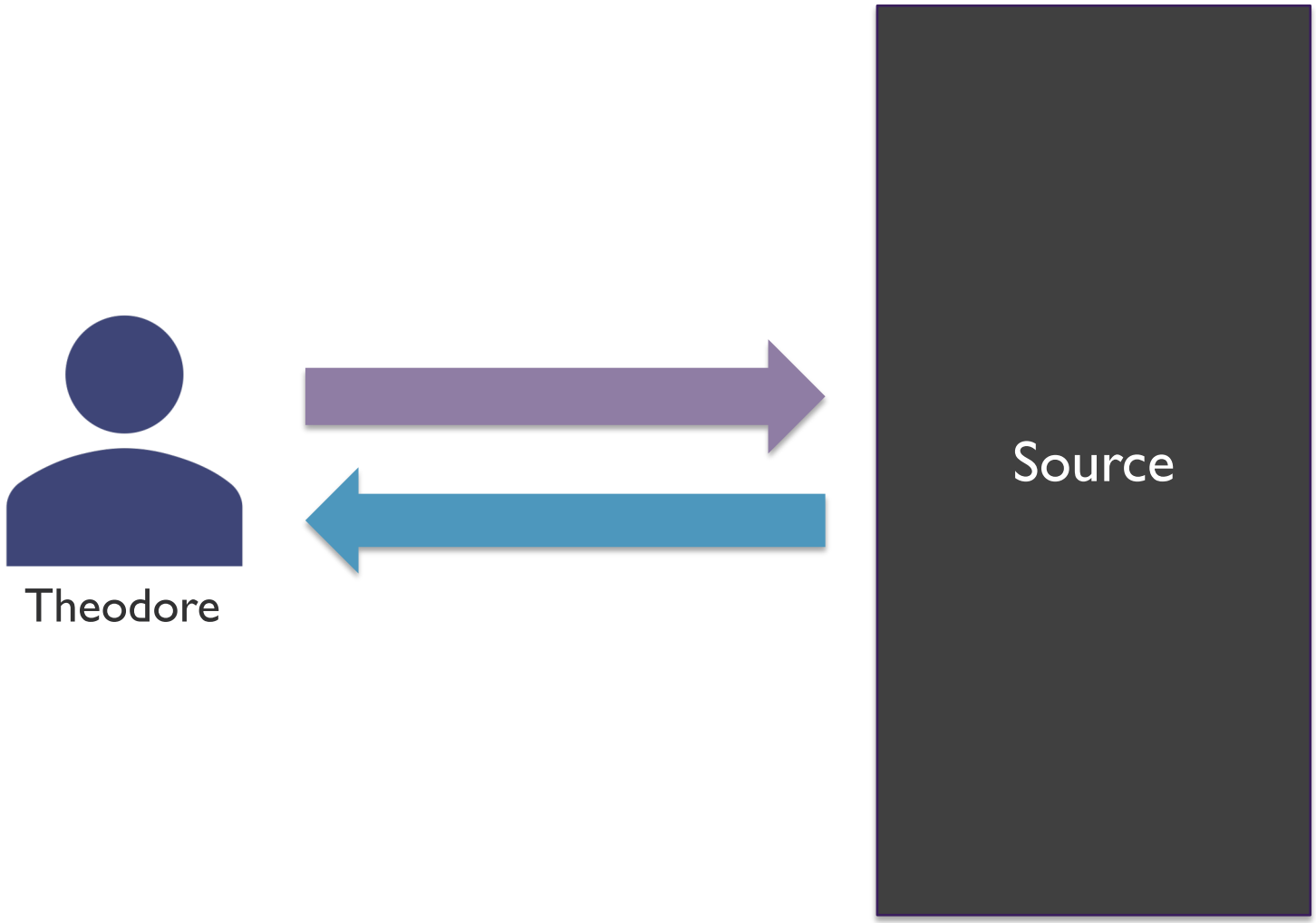
SKYLINES ACADEMY

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

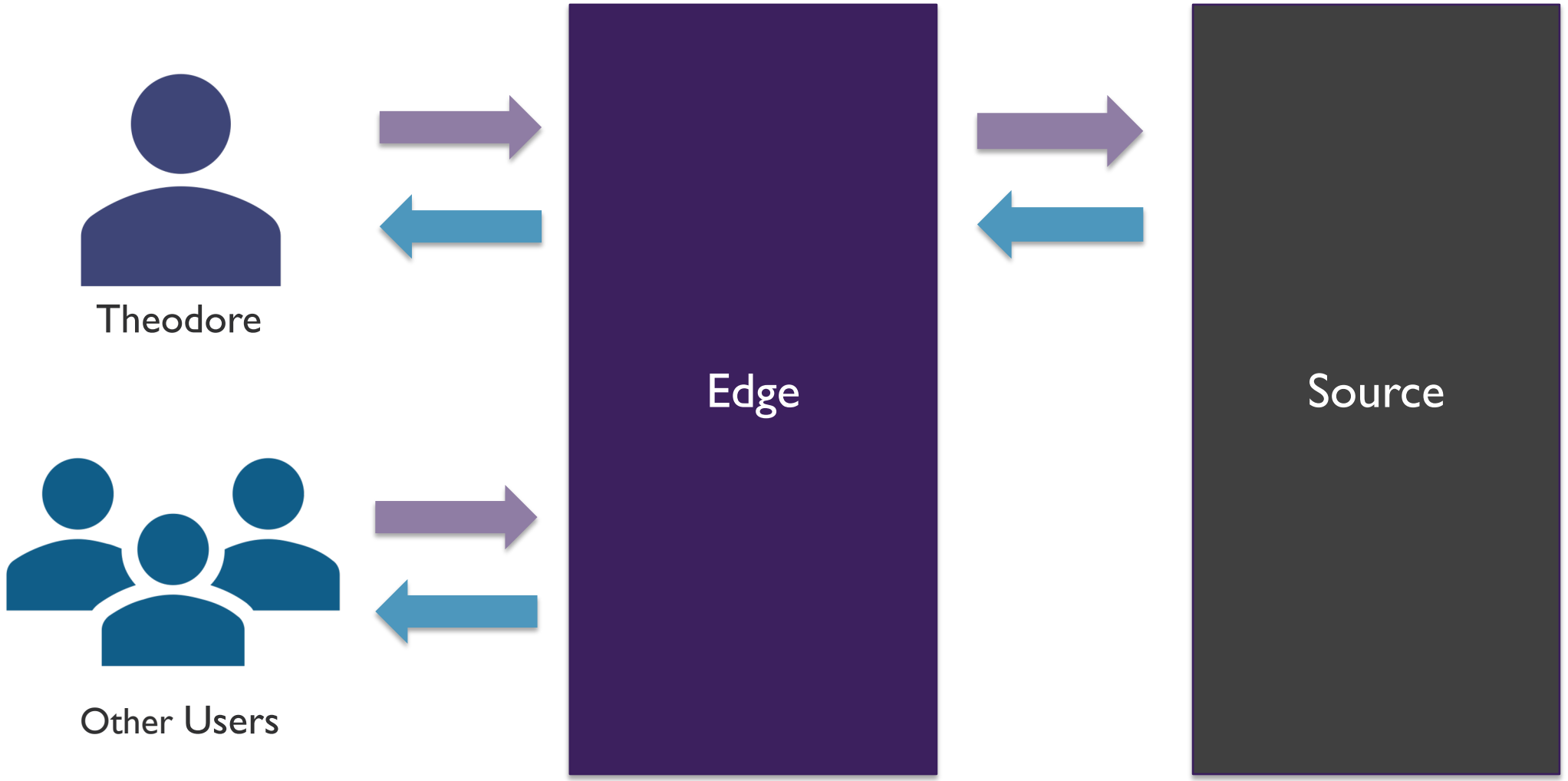
- Access files across multiple machines
- Jumpbox scenarios for shared development scenarios

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

CDN



CDN



Azure CDN Offerings

SKYLINES ACADEMY

Standard Akamai

Standard Verizon

Premium Verizon

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

Azure CDN Offerings

SKYLINES ACADEMY

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

Custom Domains

SKYLINES ACADEMY

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

SKYLINES ACADEMY

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.

SMB File Storage – Azure File Services

SKYLINES ACADEMY

Benefits

- Easy way to create file shares
- Supports SMB 2.1 (unsecured) and 3.0 (secured)
- Mount on Windows, Linux, or Mac
- Azure File Sync can be utilized to improve access from on-premises systems

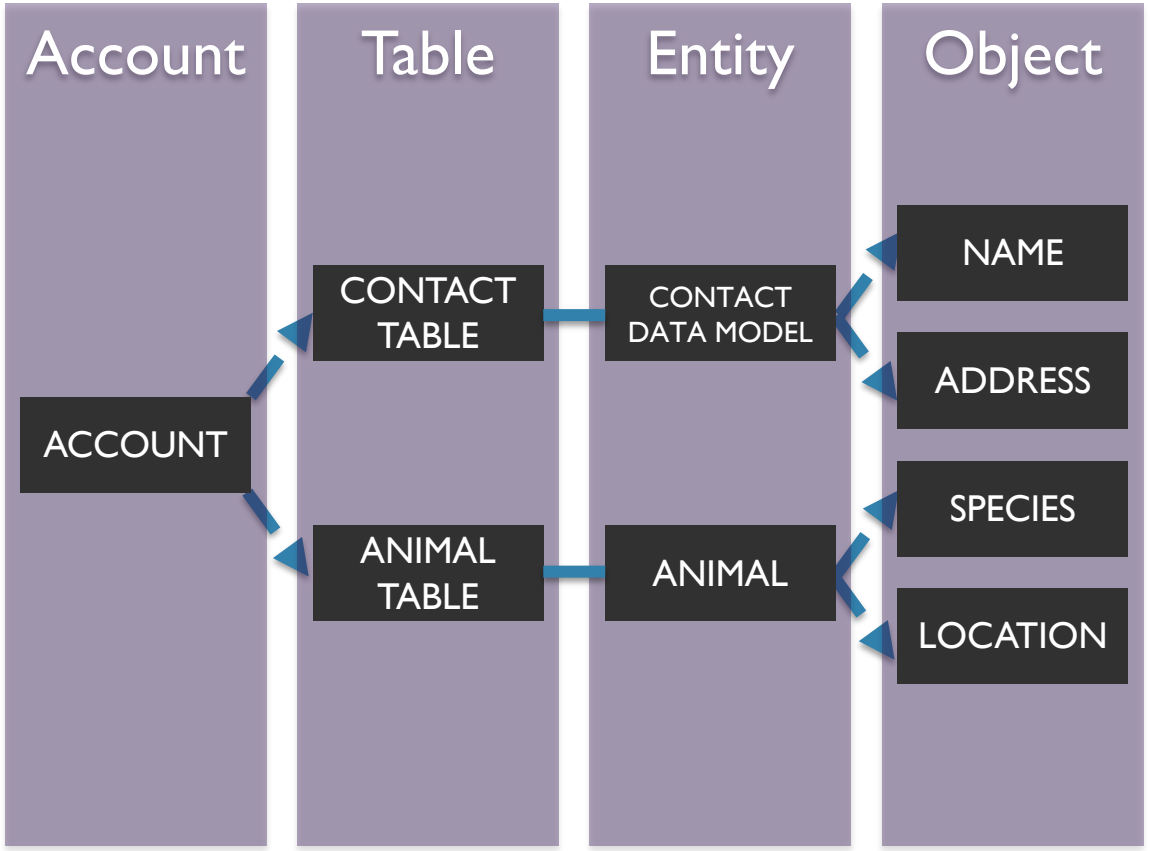
See Virtual Machines Module and Demo

Azure Table Storage

SKYLINES ACADEMY

Table Storage

- A NoSQL key-value store
- Schemaless design
- Structured or Unstructured Data
- Access using the Odata protocol and LINQ queries WCF Data Service .NET Libraries

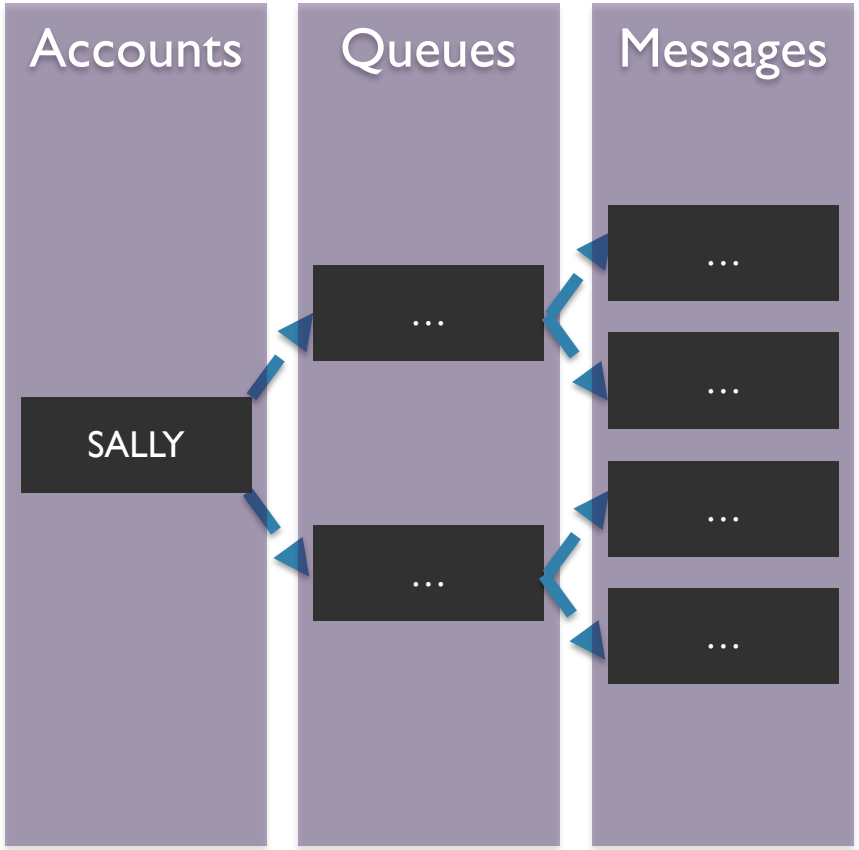


Azure Queue Storage

SKYLINES ACADEMY

Queue Storage

- Provides a reliable mechanism for storage and delivering messages for applications
- A single queue message can be up to **64 KB in size**, and a queue can contain millions of messages, up to the total capacity limit of a storage account



Blob Storage Scalability

SKYLINES ACADEMY

Resource	Target
Storage Account	500 TiB
Max size of single blob container	500 TiB
Max number of blocks in a block blob or append blob	50,000 blocks
Max size of a block in a block blob	100 MiB
Max size of a block blob	50,000 X 100 MiB (approx. 4.75 TiB)
Max size of a block in an append blob	4 MiB
Max size of an append blob	50,000 x 4 MiB (approx. 195 GiB)
Max size of a page blob	8 TiB
Max number of stored access policies per blob container	5
Target throughput for single blob	Up to 60 MiB per second, or up to 500 requests per second

https://docs.microsoft.com/en-us/azure/storage/common/storage-scalability-targets

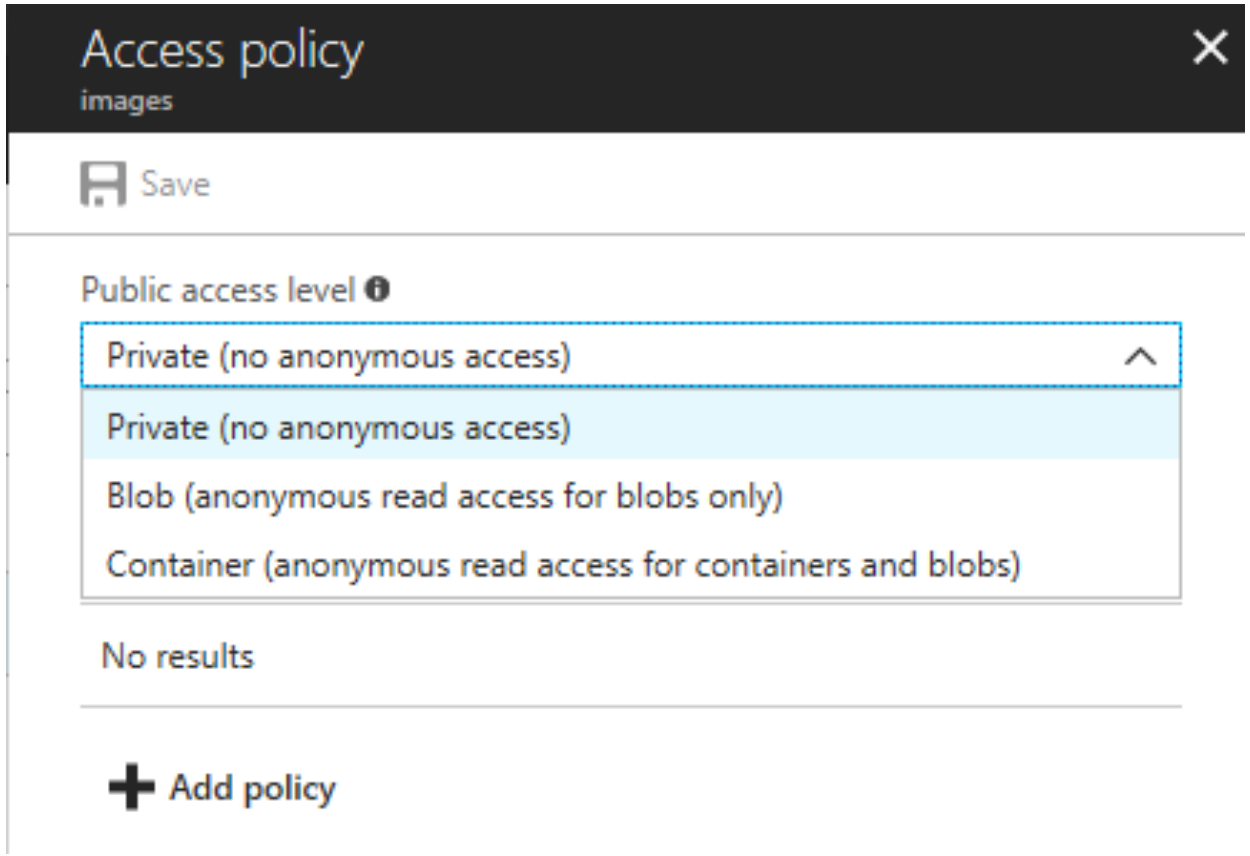
Container Permissions

SKYLINES ACADEMY

Private
(No Anonymous Access)

Blob
(Anonymous read access for blobs only)

Container
(Anonymous read access for containers and blobs)



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

SKYLINES ACADEMY

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)

SKYLINES ACADEMY

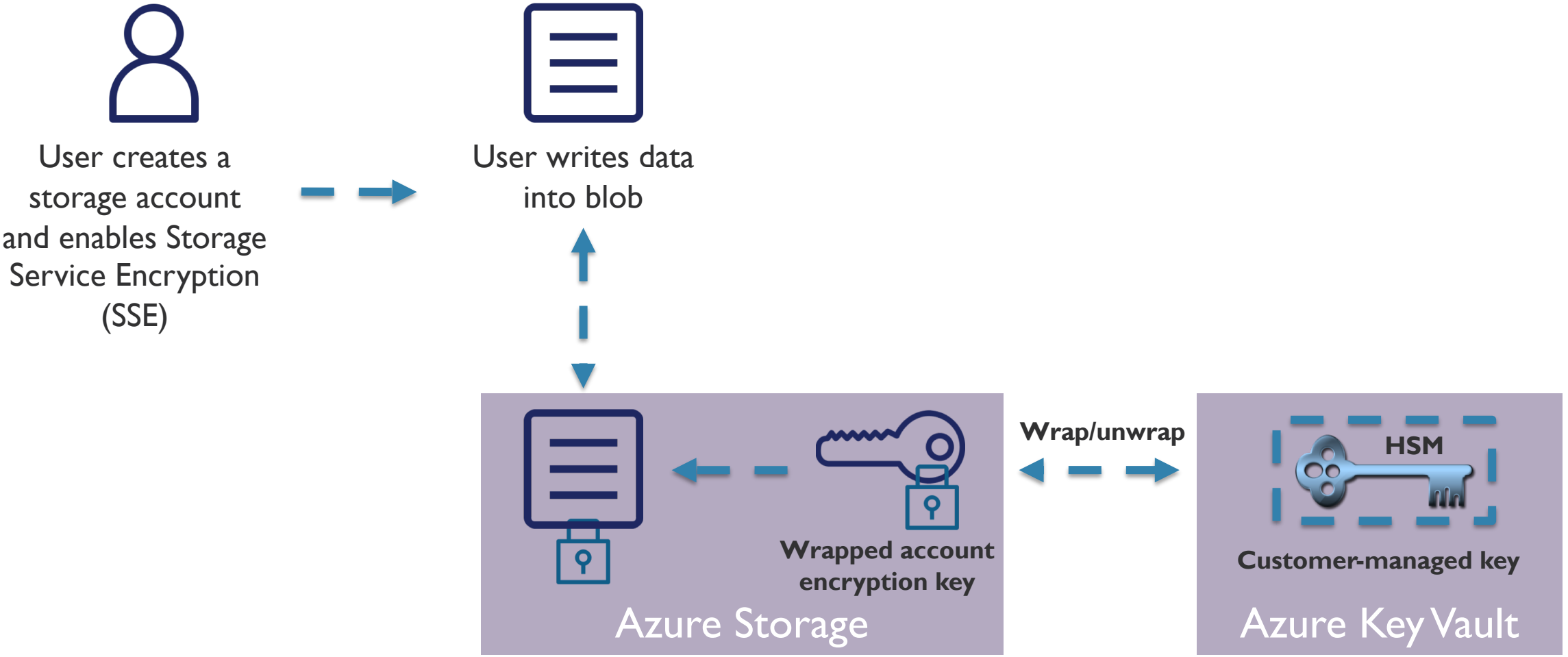
- https://slsasdemo.blob.core.windows.net/images/image.jpg — The Blob
- sv=2017-07-29 — Storage Service Version
- ss=bfqt — Signed Services
- srt=sco — Signed Resource Types
- sp=rwdlacup — Signed Permission
- se=2018-02-24T01:21:26Z&st=2018-02-23T17:21:26Z — Signed Expiry & Start
- spr=https — Signed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

Stored Access Policies

SKYLINES ACADEMY

- 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

Encryption Keys and Key Vault



Module:
Import and Export Data to Azure

SKYLINES
ACADEMY

Azure Import/Export Use Cases

SKYLINES ACADEMY

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

SKYLINES ACADEMY

- 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

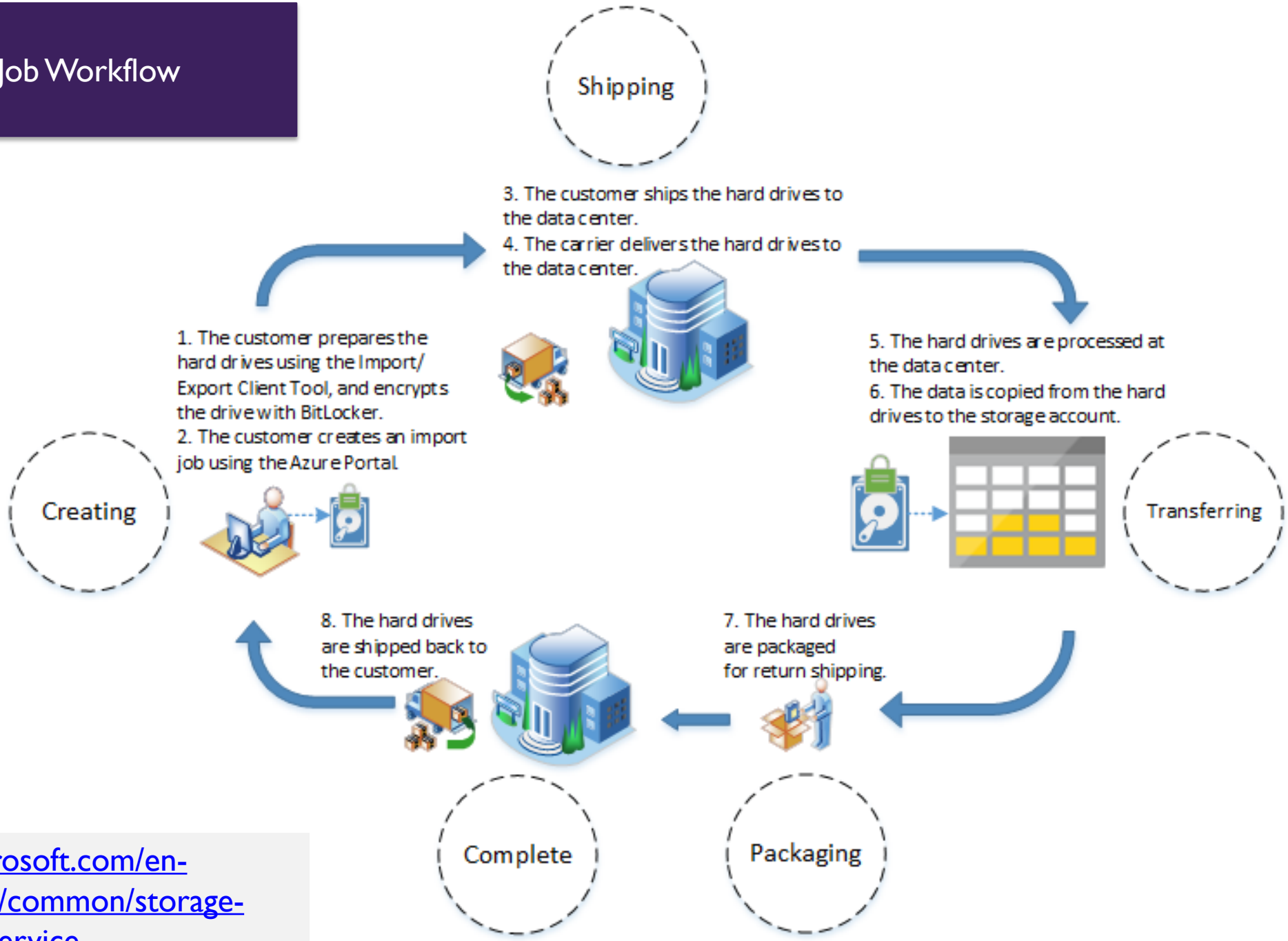
SKYLINES ACADEMY

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



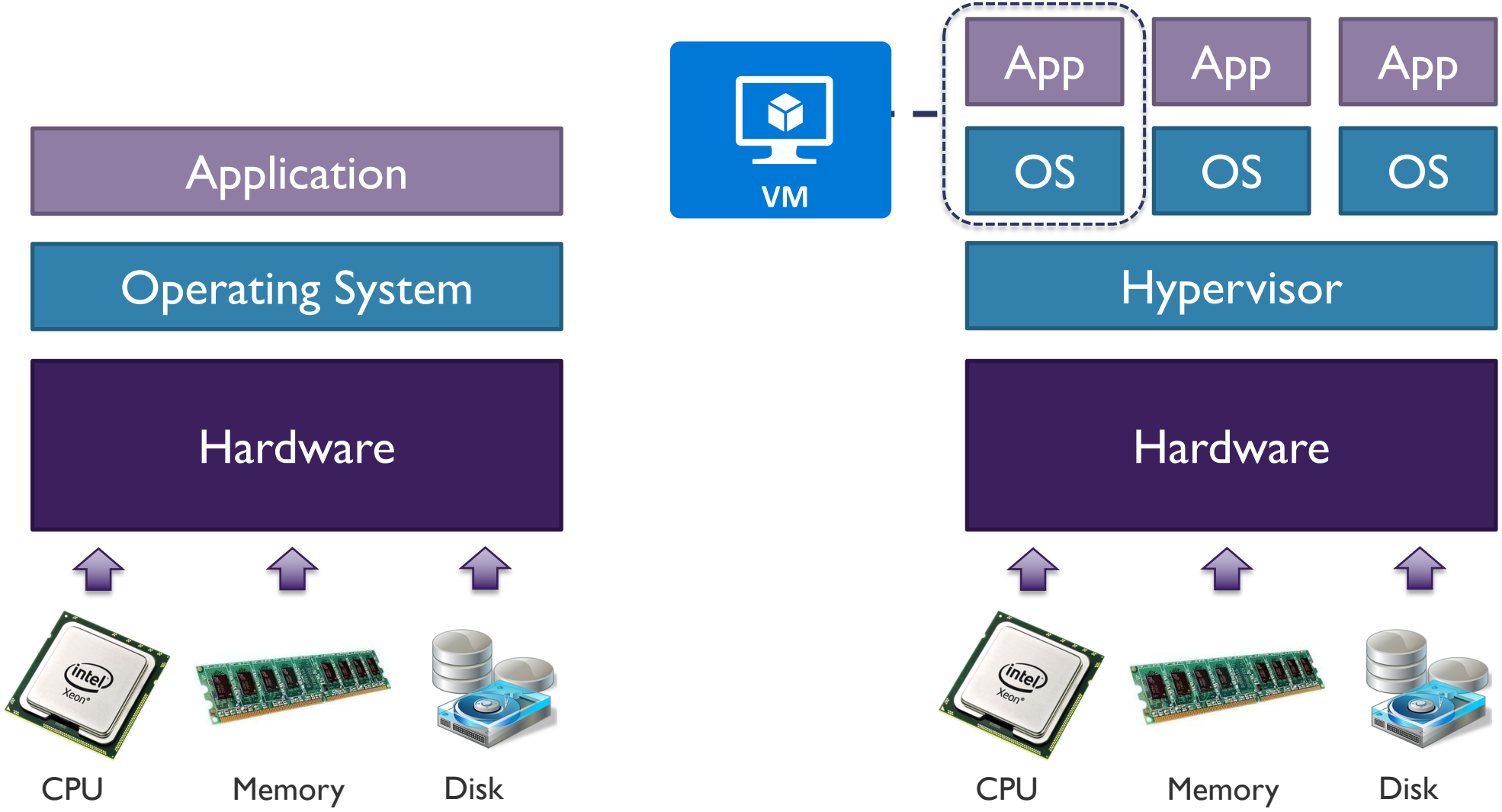
https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service

Module:
Virtual Machines

SKYLINES
ACADEMY

Introduction to Virtual Machines

SKYLINES ACADEMY



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 Specializations

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)

SKYLINES ACADEMY

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

SKYLINES ACADEMY

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

SKYLINES ACADEMY

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

SKYLINES ACADEMY

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		●	●	●	●	●	●	●	●	●	●

Restricted Usernames

SKYLINES ACADEMY

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

PowerShell VM Commands

SKYLINES ACADEMY

Task	PowerShell Example
New Resource Group	New-AzureRmResourceGroup -Name myResourceGroup -Location EastUS
New Virtual Machine	New-AzureRmVM
Create VM Configuration	$vm = NewAzureRmVMConfig –VMName $Vmname
Start and Stop VMs	Start-AzureRmVM Stop-AzureRmVM

-OpenPorts 80,3389

Connecting via WinRM

WinRMHttps

- Connectivity over SSL
- Uses port 5986
- Recommended to use this option if you are going over the Internet, as it is much more secure

WinRMHttp

- No SSL required
- Uses port 5985
- Ideal for connections from the same private network which is already secure

WinRM Self-Signed Certificate Procedures

SKYLINES ACADEMY

Steps

- Create a Key Vault
- Create a self-signed certificate
- Upload certificate to the Key Vault
- Get the URL for your certificate from the Key Vault
- Reference your self-signed certificate when you create the VM

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

VM Images

SKYLINES ACADEMY

Custom Images

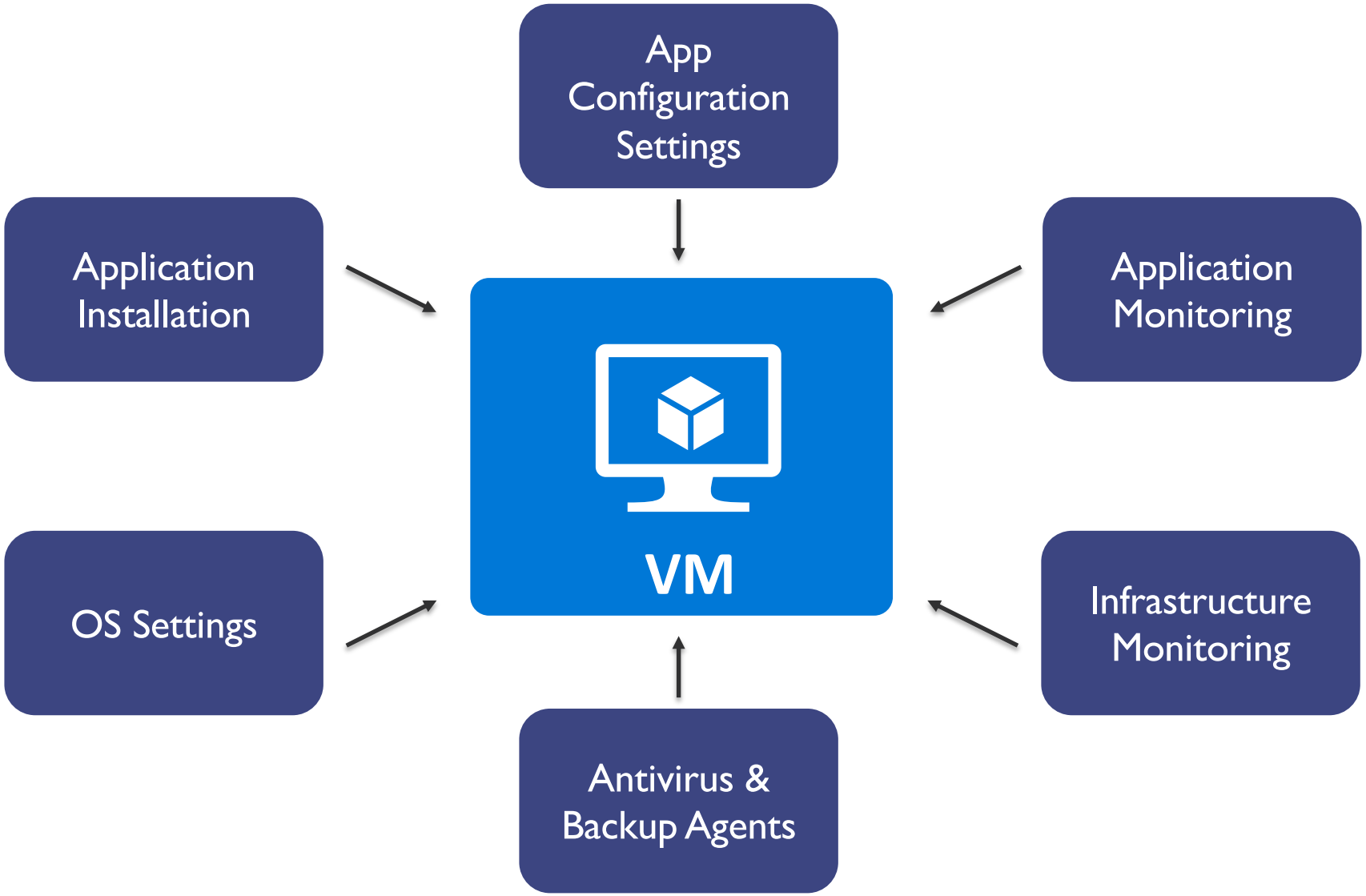
- Do-it-yourself image
- Windows - Sysprep
- Linux - sudo waagent –deprovision+user
- Generalize in Azure
- Create image

Marketplace Images

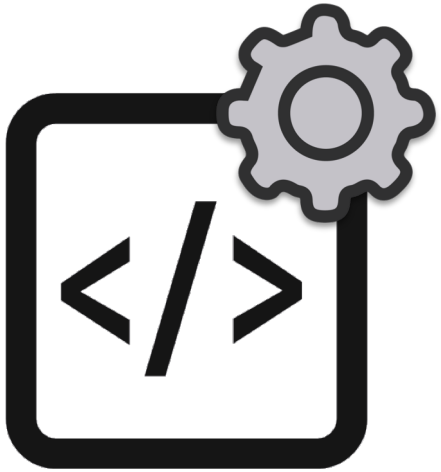
- Provided for you in the Azure Marketplace
- Properties:
  - Publisher
  - Offer
  - SKU

Introduction to Configuration Management

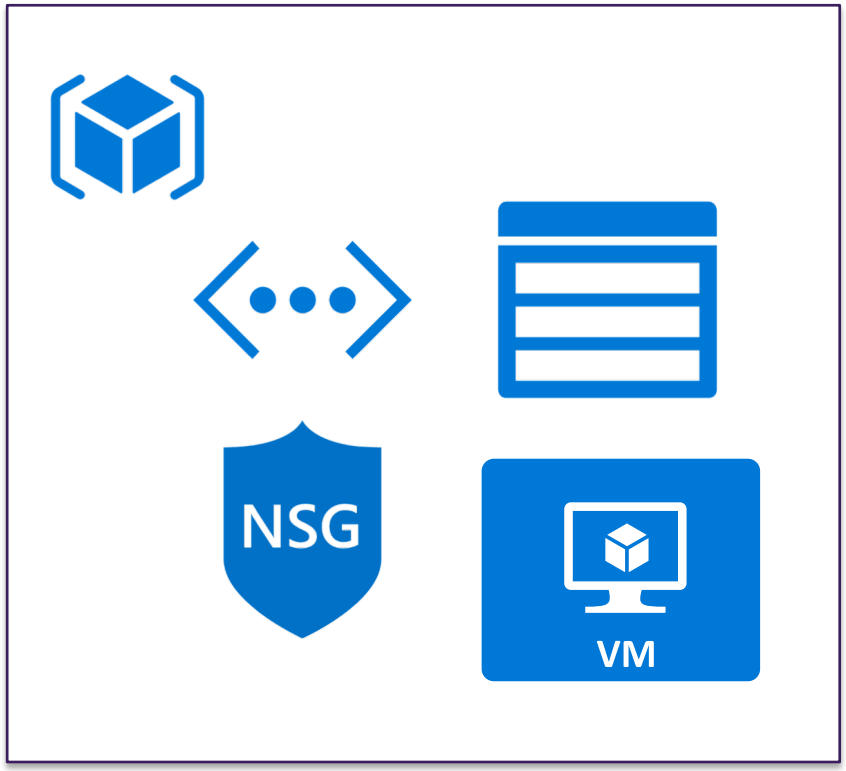
SKYLINES ACADEMY



VM Extensions



Deployment



VM Extensions

DSC | Scripts

Configuration Management

Extensions available in Azure

Configuration Management (continued)

Enterprise-level configuration management for multiple nodes

PowerShell DSC Key Components

SKYLINES ACADEMY

Configurations

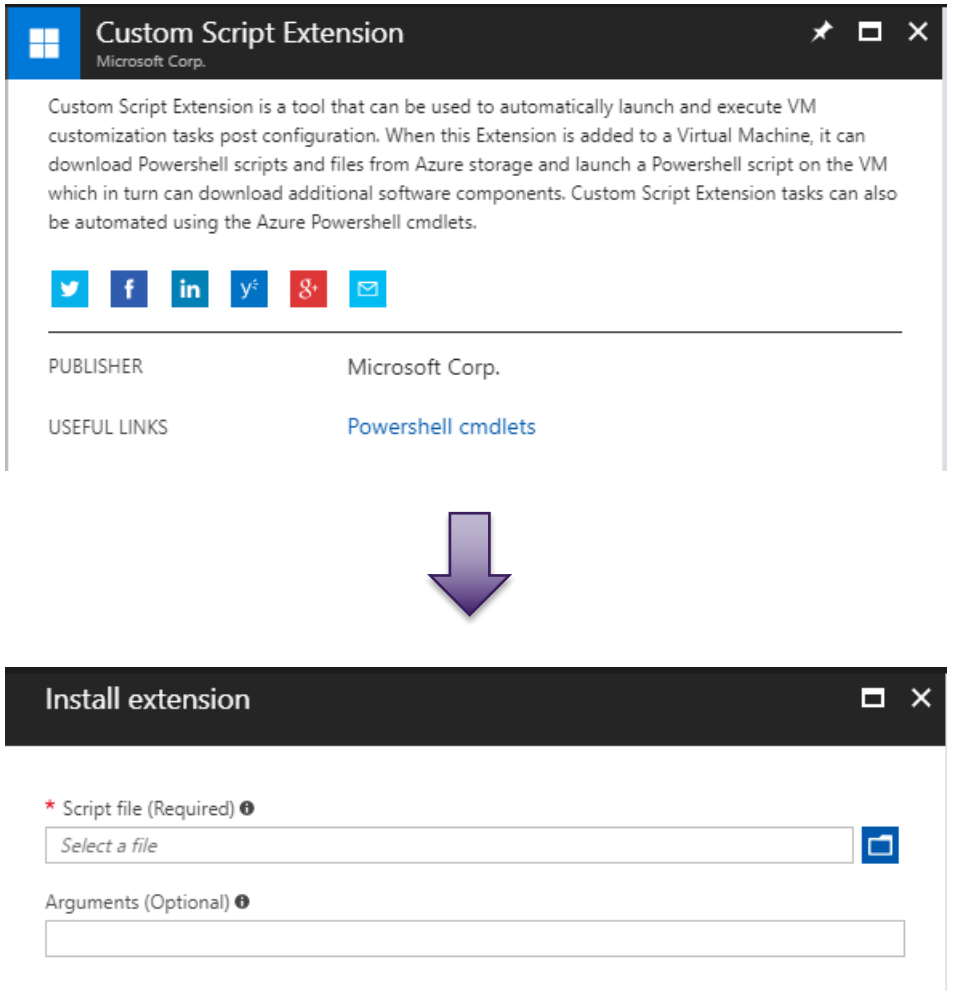
Resources

Logical Configuration Manager

Custom Script Extension

SKYLINES ACADEMY

- 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 (continued)

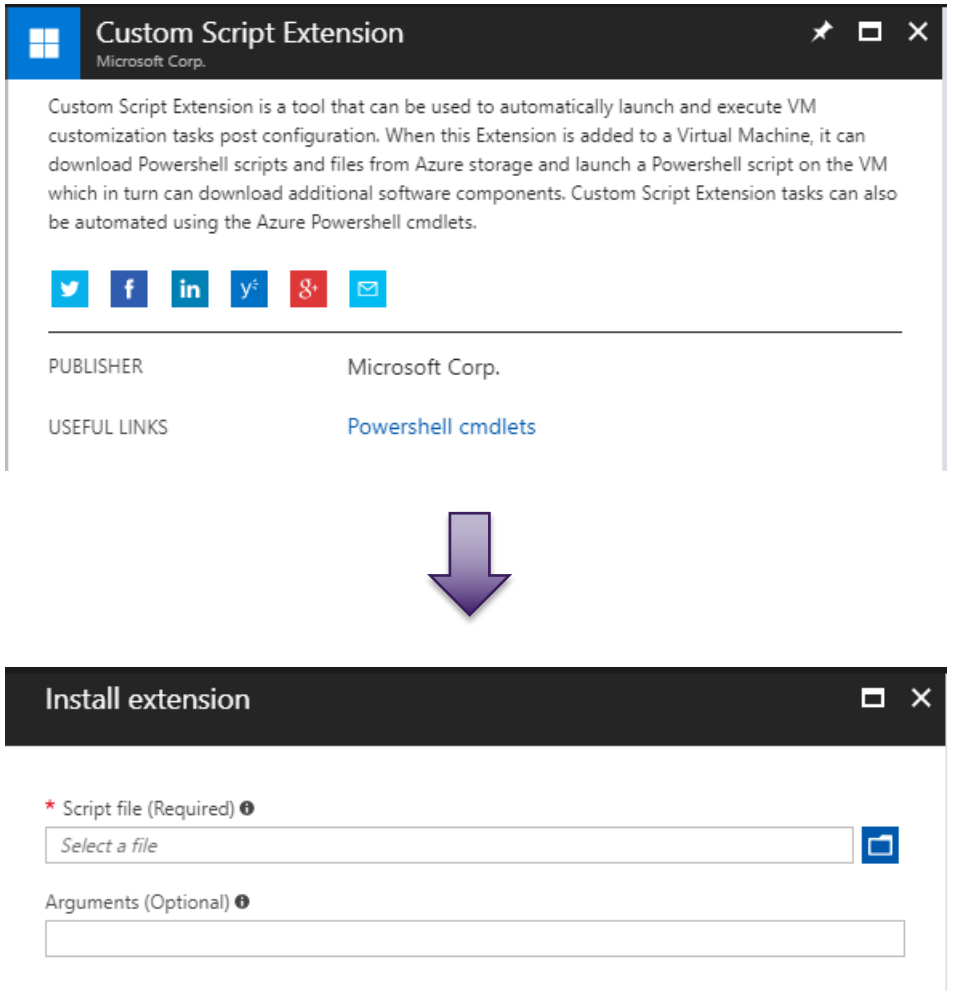
SKYLINES ACADEMY

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



Enabling Remote Debugging

SKYLINES ACADEMY

1. Download and install Remote Tools for Visual Studio

https://www.visualstudio.com/downloads/#remote-tools-for-visual-studio-2017

Remote Tools for Visual Studio 2017

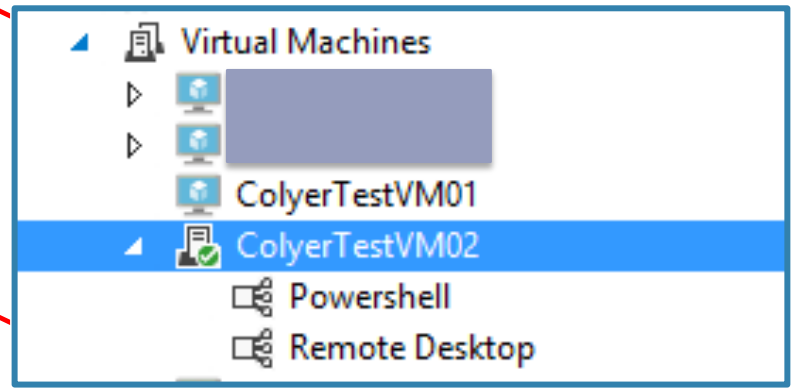
Remote Tools for Visual Studio 2017 enables app deployment, remote debugging, remote testing, performance profiling, and unit testing on computers that do not have Visual Studio installed.

x64
x86

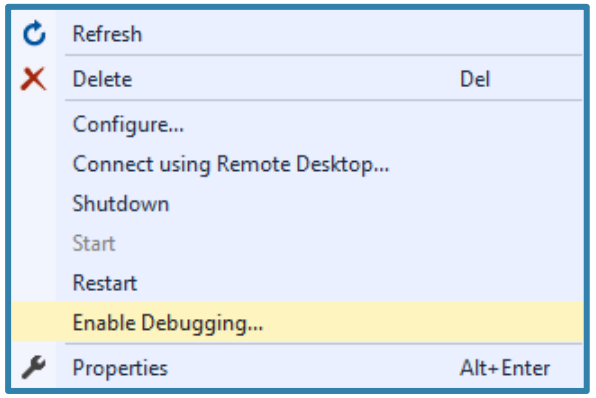
English

Download

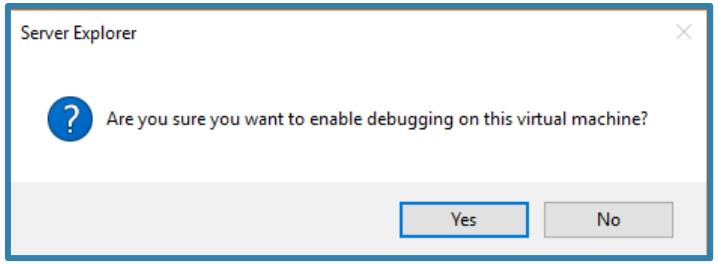
2. Right Click VM in Visual Studio



3. Enable Debugging



4. Confirm



VM Storage Types

SKYLINES ACADEMY

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

SKYLINES ACADEMY

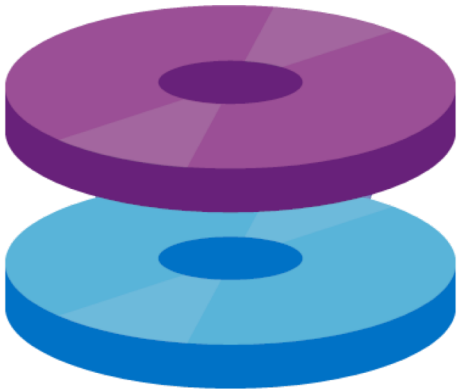
	P4	P6	P10	P15	P20	P30	P40	P50
Disk size (GB)	32	64	128	256	512	1024	2048	4095
Max IOPS	120	240	500	1100	2300	5000	7500	7500
Max through	25 MB/s	50 MB/s	100 MB/s	125 MB/s	150 MB/s	200 MB/s	250 MB/s	250 MB/s

Managed vs. Unmanaged Disks

SKYLINES ACADEMY

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

SKYLINES ACADEMY

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

VM Storage Limits and Capacity Planning

SKYLINES ACADEMY

Resource	Target
Storage Account	500 TiB
Max size of single blob container	500 TiB
Max number of blocks in a block blob or append blob	50,000 blocks
Max size of a block in a block blob	100 MiB
Max size of a block blob	50,000 X 100 MiB (approx. 4.75 TiB)
Max size of a block in an append blob	4 MiB
Max size of an append blob	50,000 x 4 MiB (approx. 195 GiB)
Max size of a page blob	8 TiB
Max number of stored access policies per blob container	5
Target throughput for single blob	Up to 60 MiB per second, or up to 500 requests per second

https://docs.microsoft.com/en-us/azure/storage/common/storage-scalability-targets

Disk Caching

SKYLINES ACADEMY

- 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)

SKYLINES ACADEMY

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

Storage Service Encryption (SSE)

SKYLINES ACADEMY

- Provides encryption-at-rest
- Automatically enabled with Managed Disks
- Enabled at Storage Account level for unmanaged disks
- Only new files added to account will be encrypted

Azure VM Disk Encryption

SKYLINES ACADEMY

- Encryption at rest with industry standard encryption system
  - Windows drives encrypted using Bitlocker
  - Linux drives encrypted using DM-Crypt
- Regulatory requirements met. IaaS VMs all use customer controlled keys and policies allowing auditing of key vault

Availability Sets

SKYLINES ACADEMY

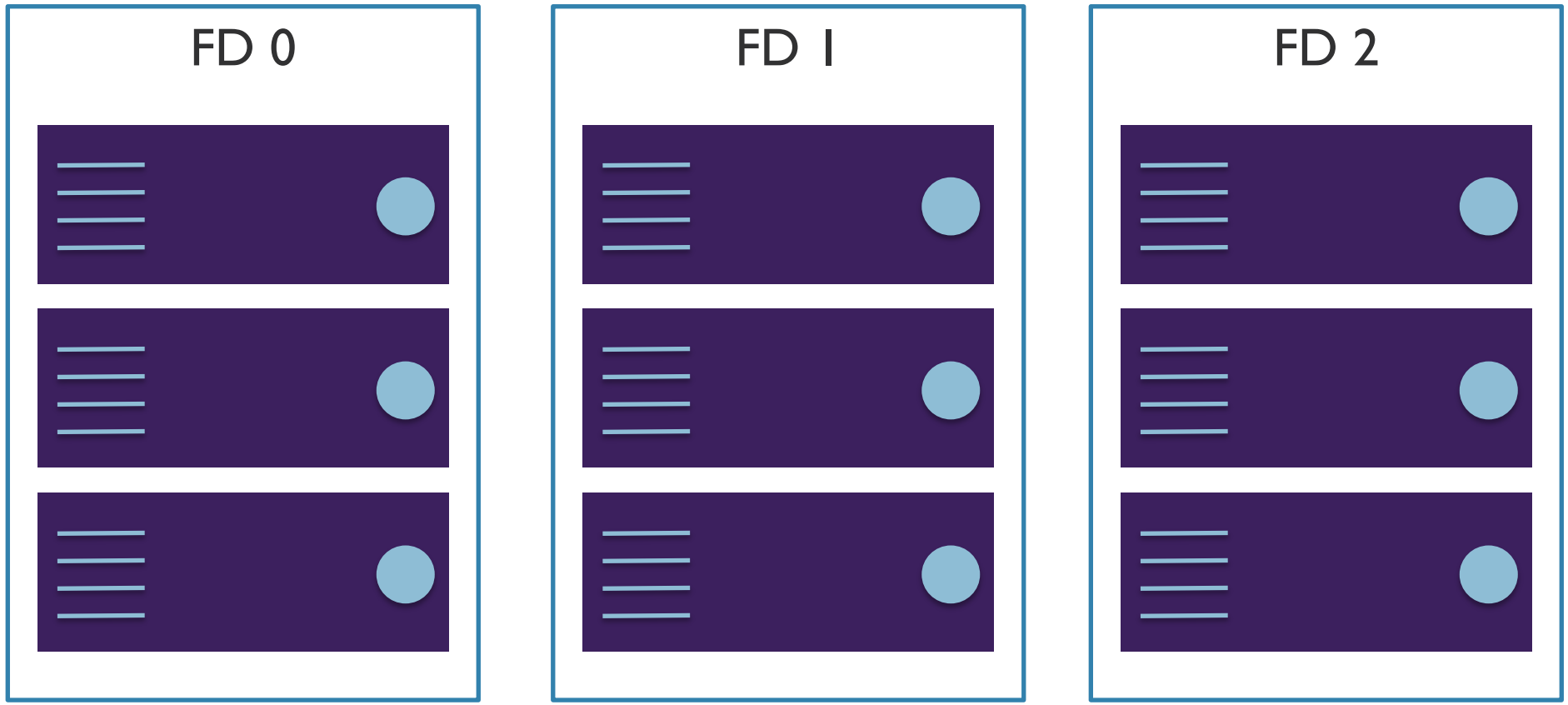
Potential for VM Impact

- Planned maintenance
- Unplanned hardware maintenance
- Unexpected downtime

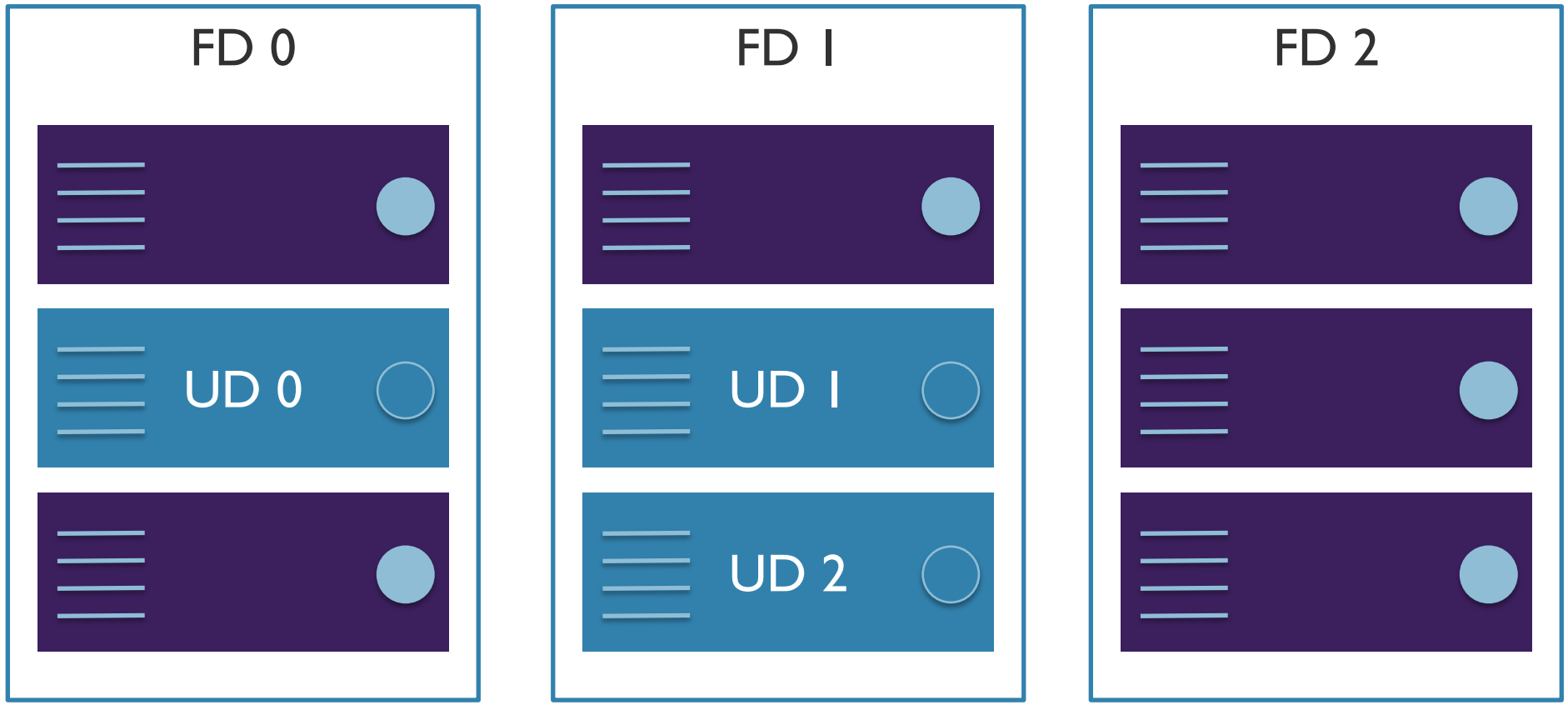
Availability Sets

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

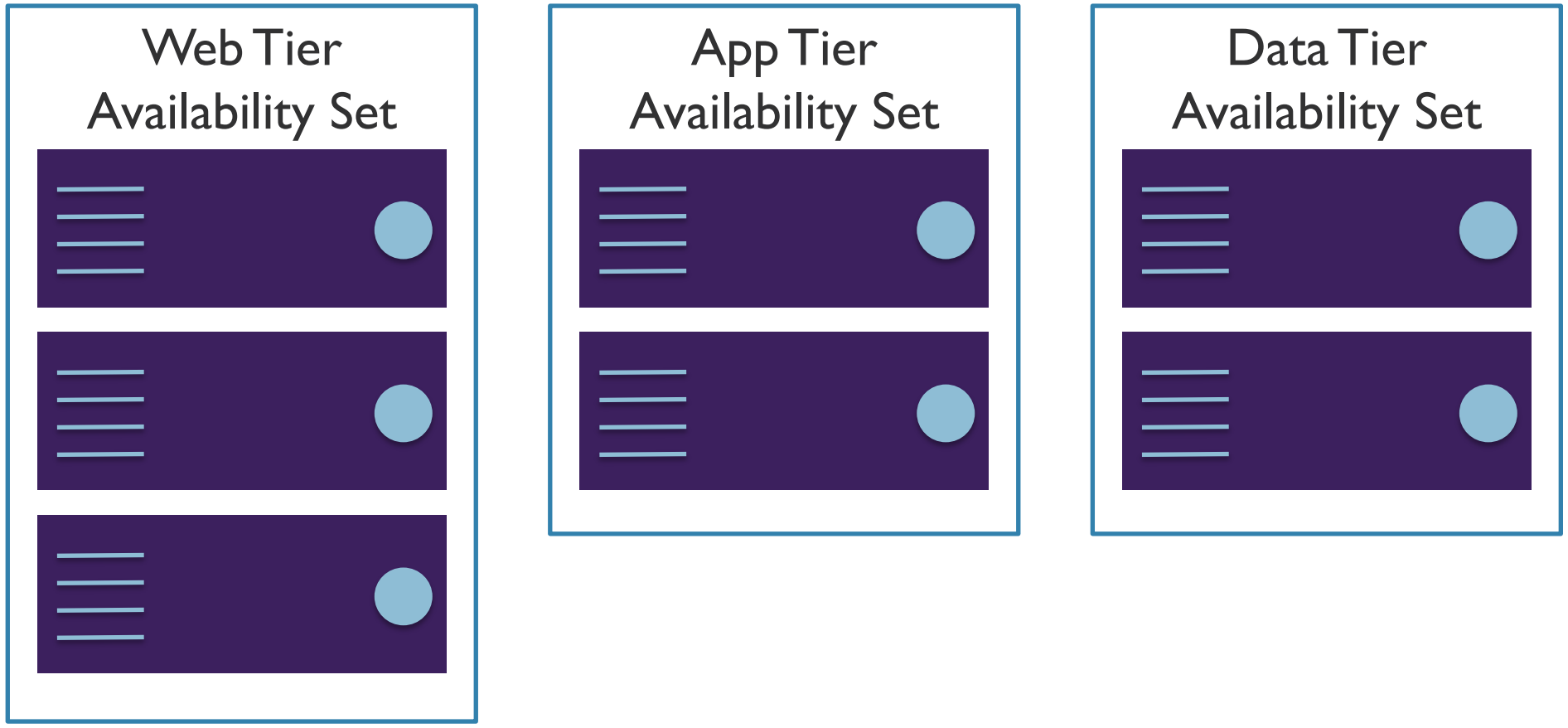
Fault Domains and Update Domains



Fault Domains and Update Domains



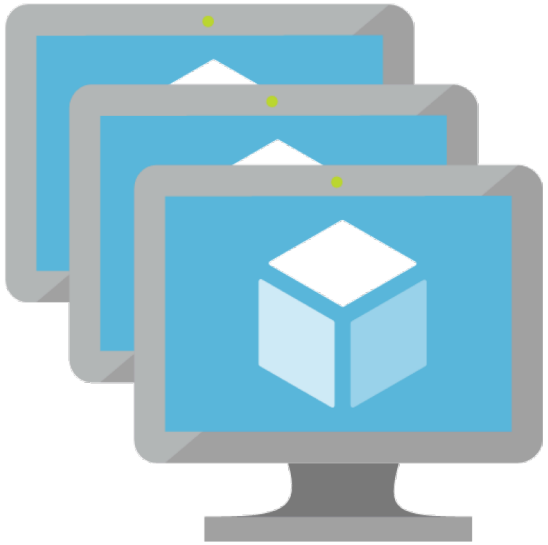
Planning for Availability



Scale Sets

SKYLINES ACADEMY

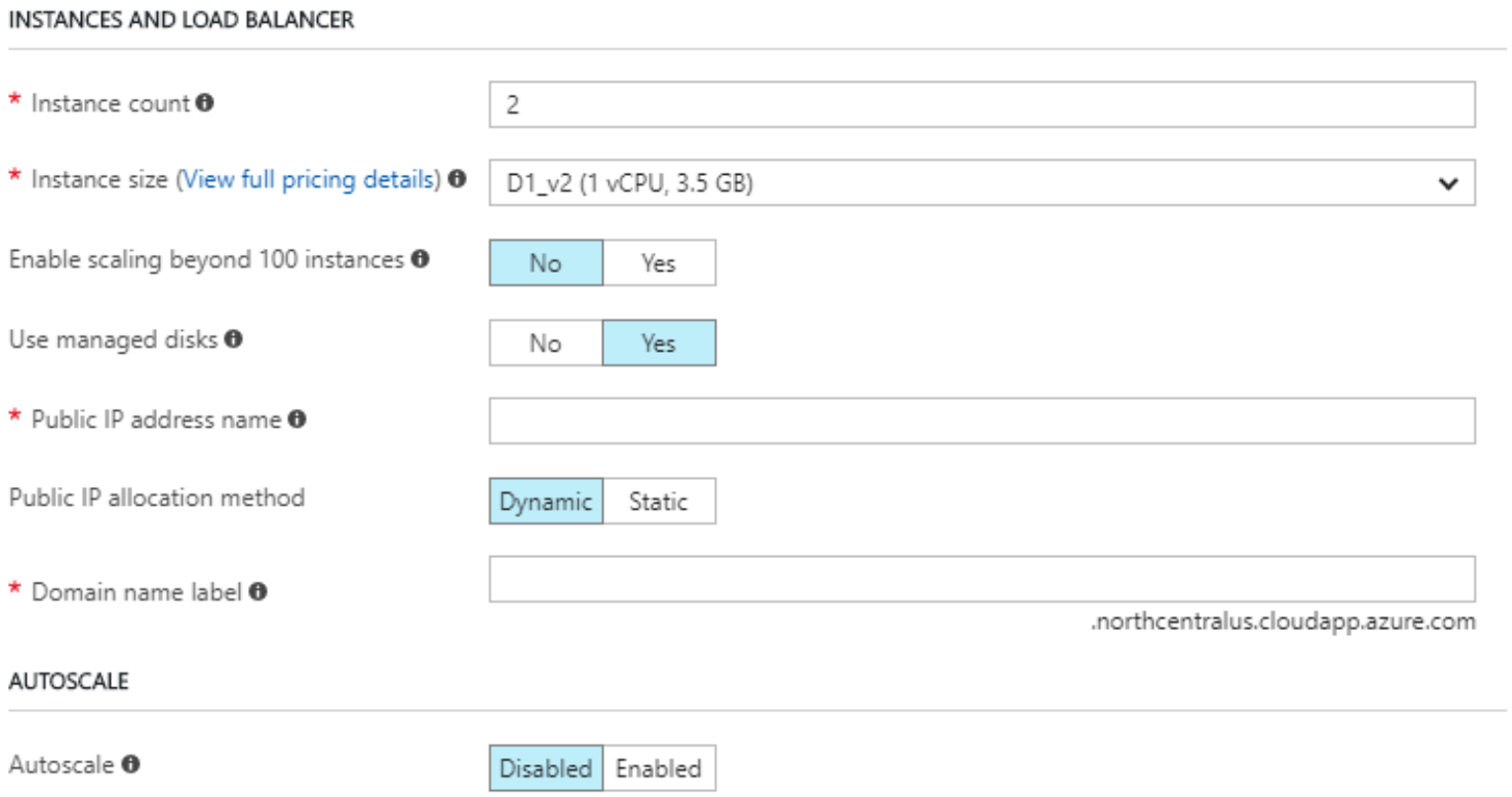
VS.



Define Virtual Machine Scale Set (VMSS)

SKYLINES ACADEMY

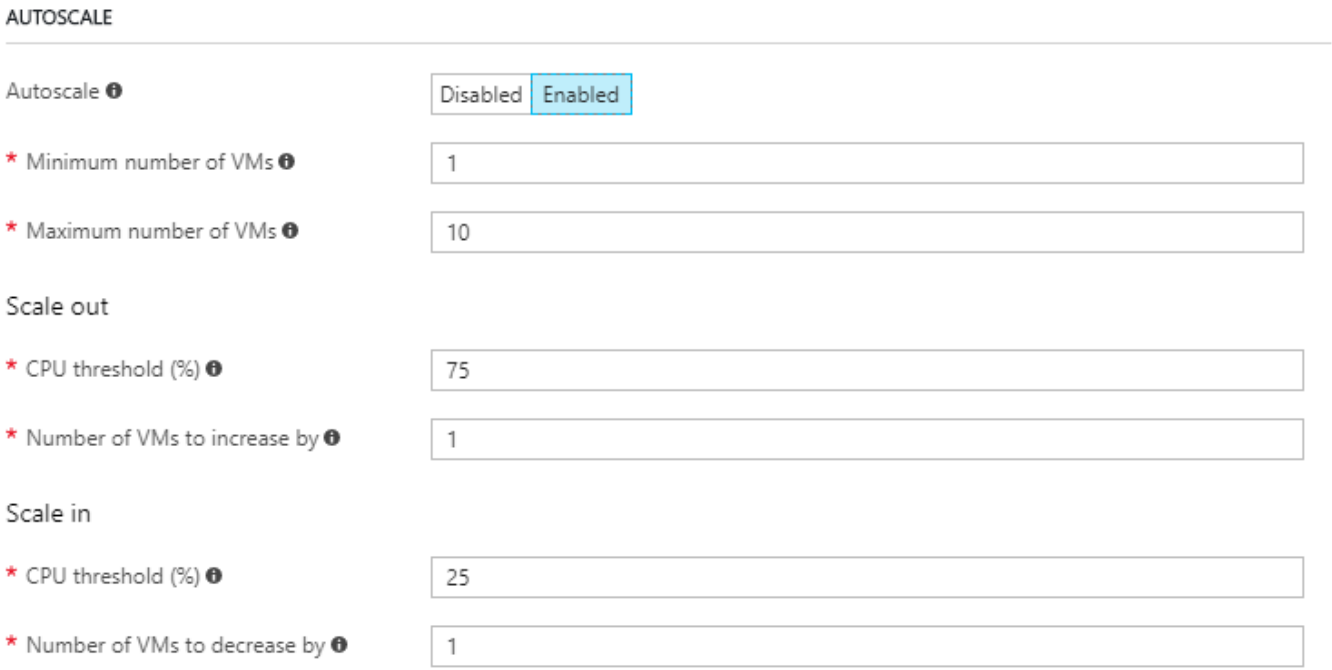
- Use Portal, PowerShell or API
- Number of instances you wish to run, instance size, etc.
- Determine if you want to auto-scale



Configure Autoscale Rules

SKYLINES ACADEMY

- 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



Scaling Up

SKYLINES ACADEMY

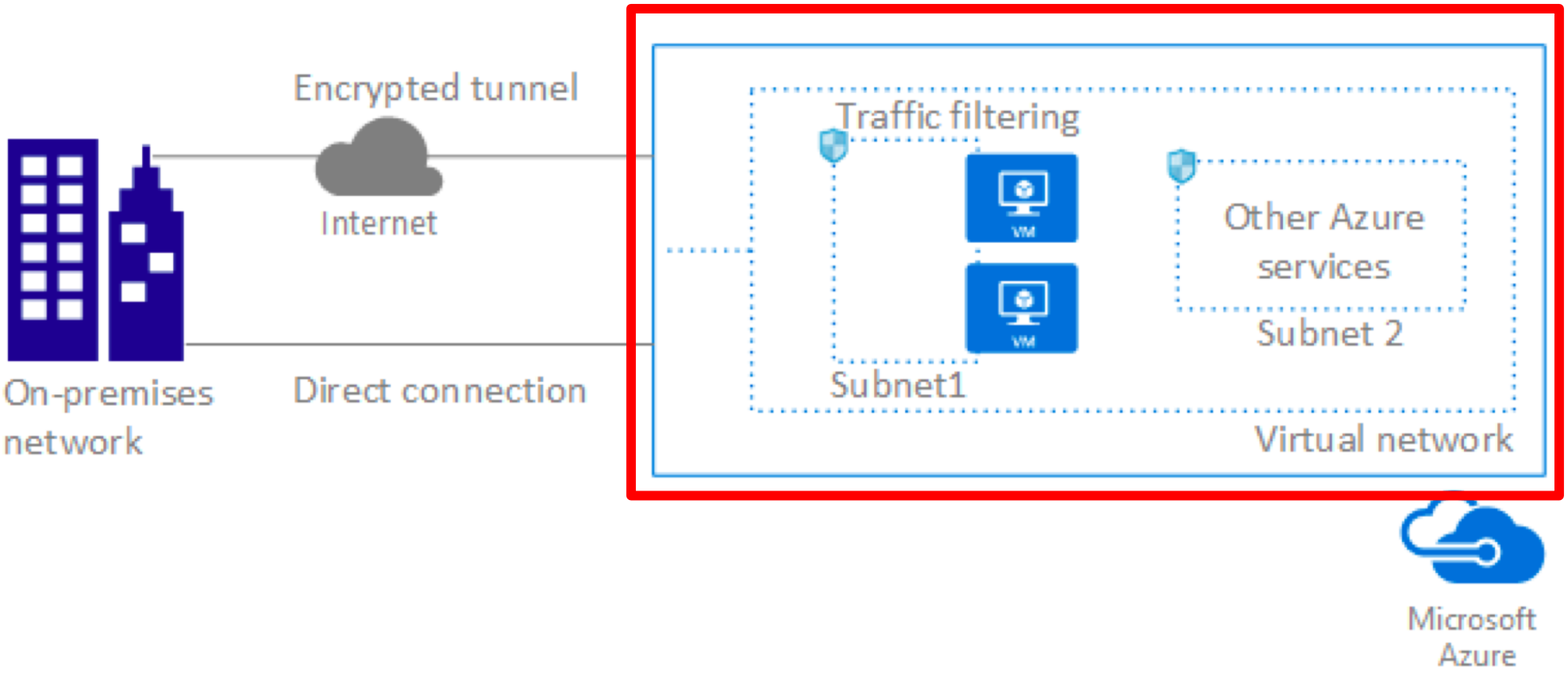
Scaling Up Pairs Supported by Azure Automation

From	To
Standard_A0	Standard_A11
Standard_D1	Standard_D14
Standard_DS1	Standard_DS14
Standard_D1v2	Standard_D15v2
Standard_G1	Standard_G5
Standard_GS1	Standard_GS5

Module: Networking

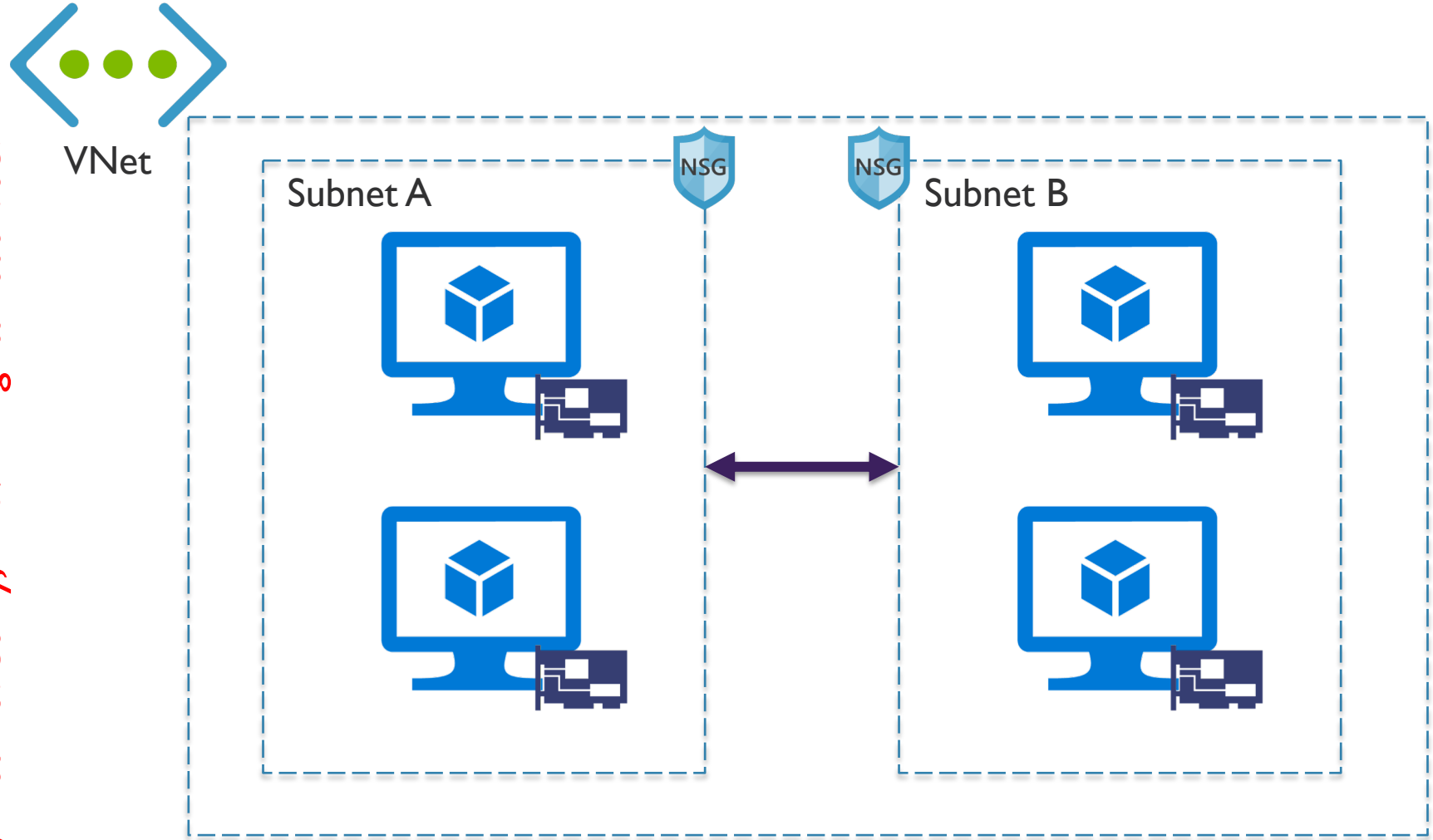
SKYLINES ACADEMY

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

SKYLINES ACADEMY

- 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)

SKYLINES ACADEMY

- 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

Internet Access

SKYLINES ACADEMY

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

SKYLINES ACADEMY

Azure-provided DNS

Customer DNS Server

IaaS Server with DNS

Infoblox Virtual Appliance

DNS Scenarios and Recommendations

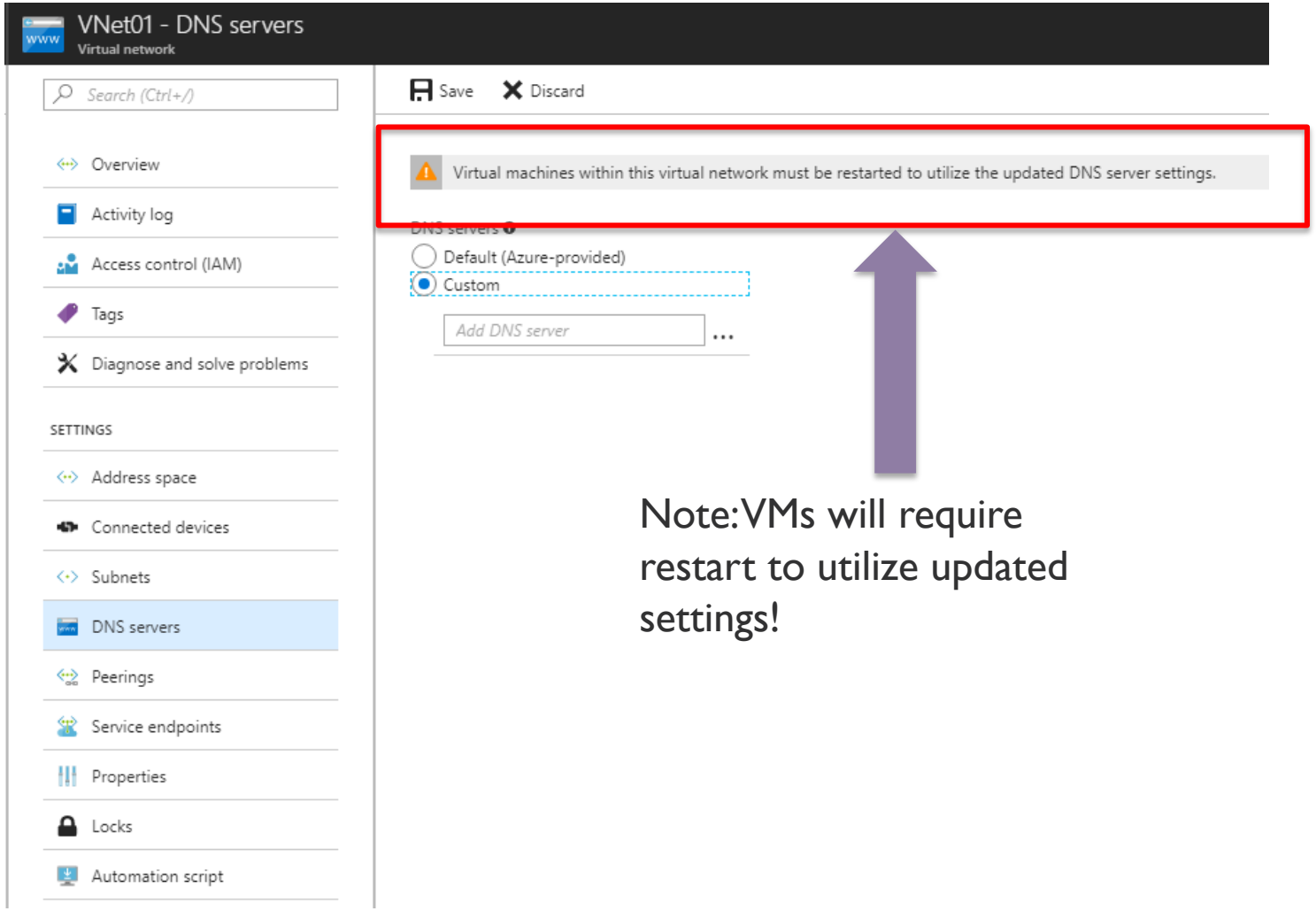
SKYLINES ACADEMY

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

SKYLINES ACADEMY

- **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!

System Routes

SKYLINES ACADEMY

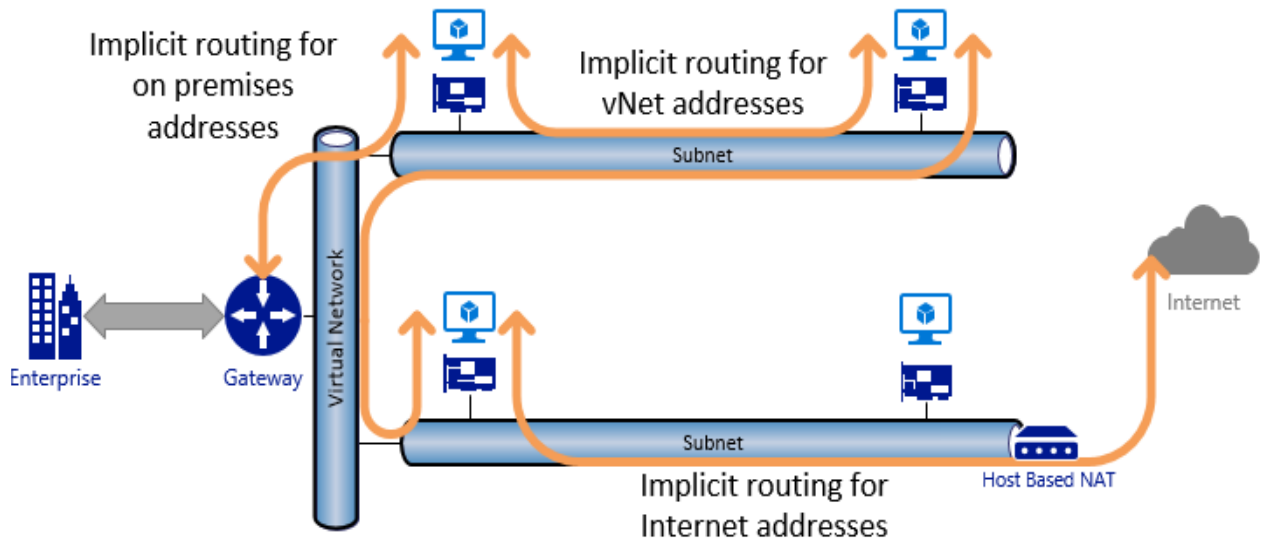
Every subnet has a route table that contains the following minimum routes:

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)

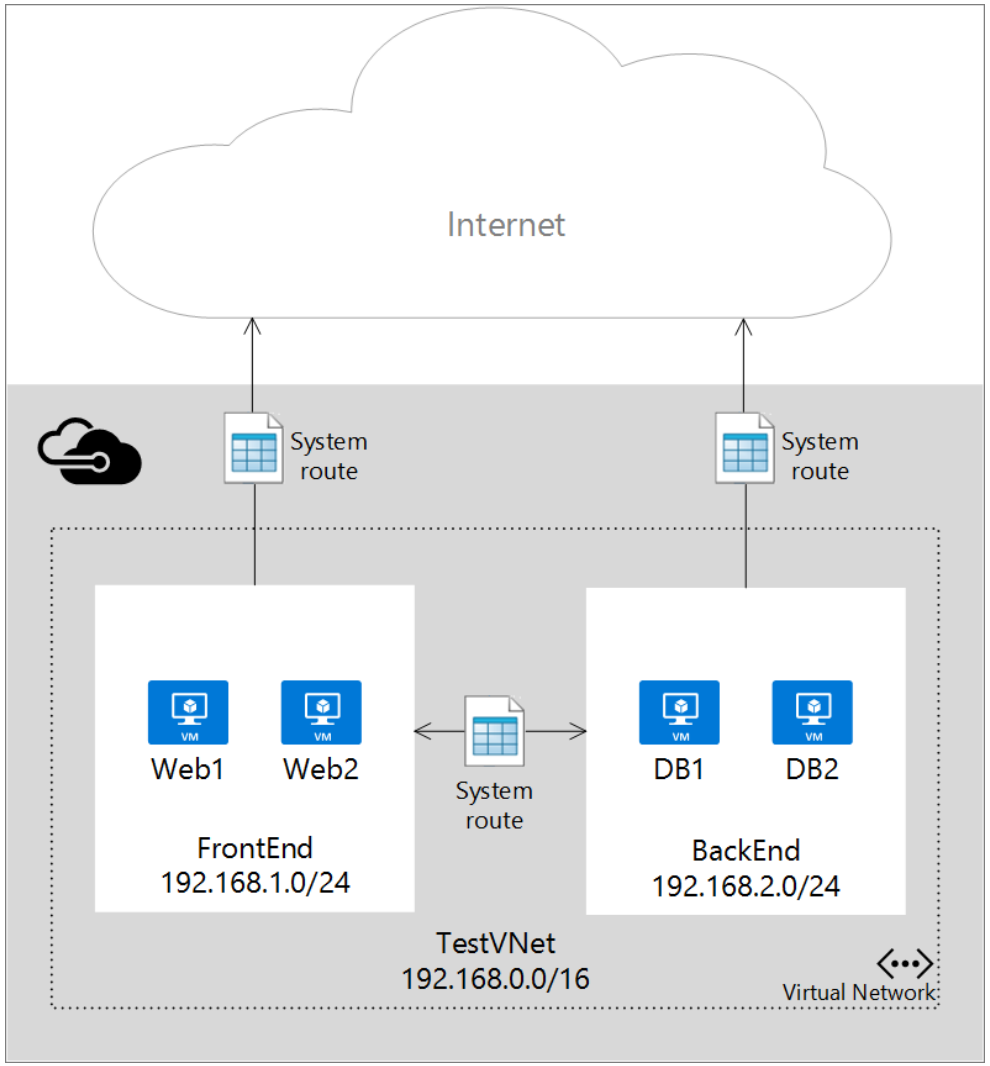
Default Routing in a Subnet

SKYLINES ACADEMY

- 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*

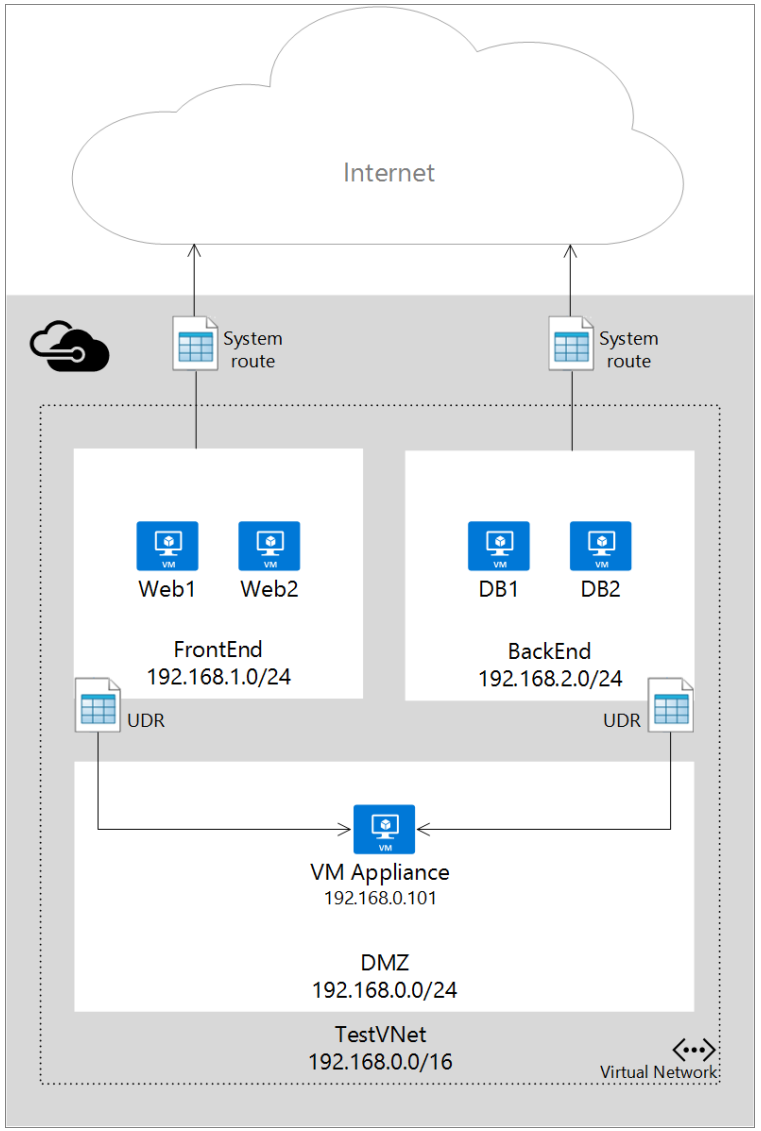


User-Defined Routes

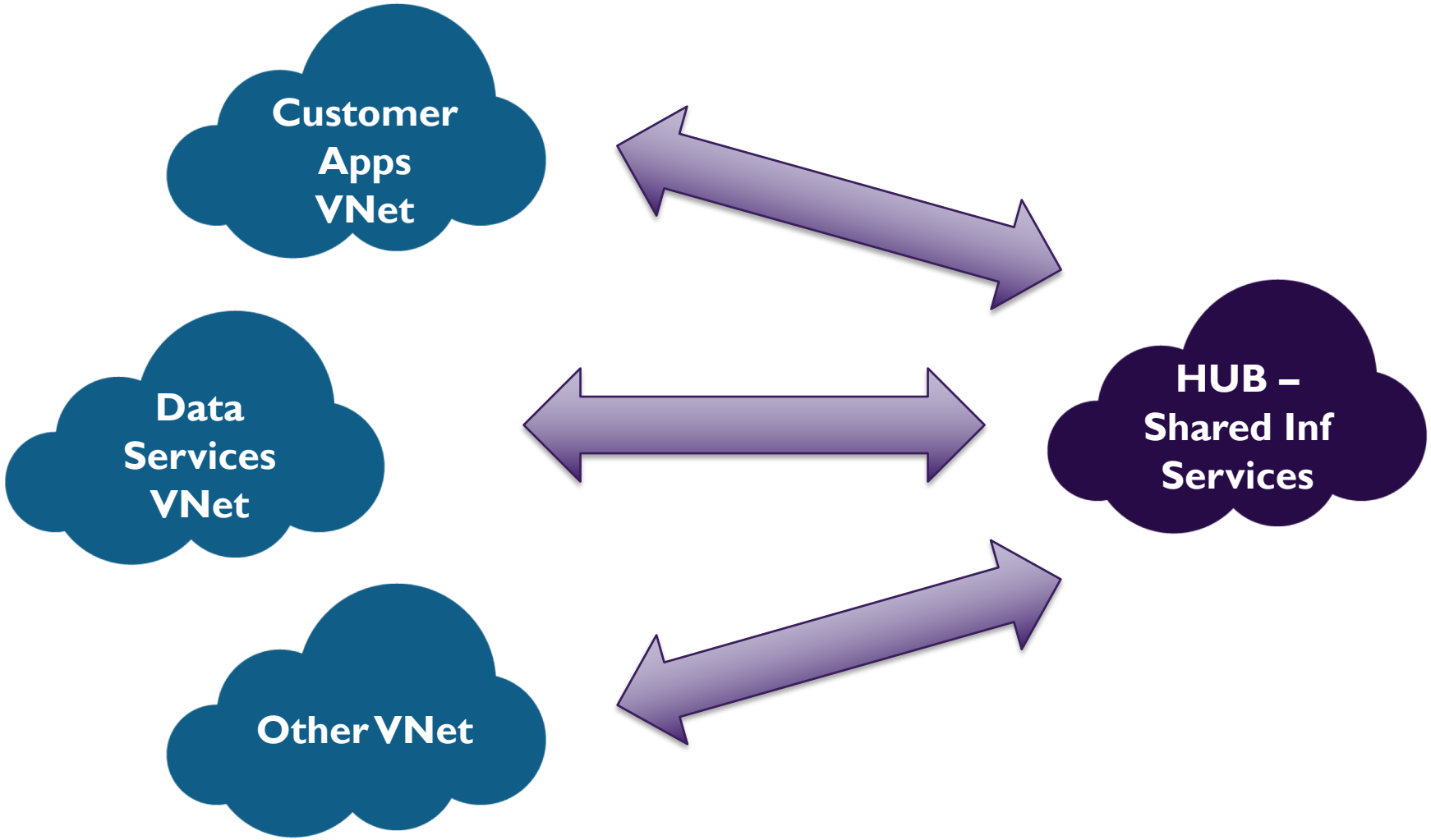


https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

User-Defined Routes (continued)



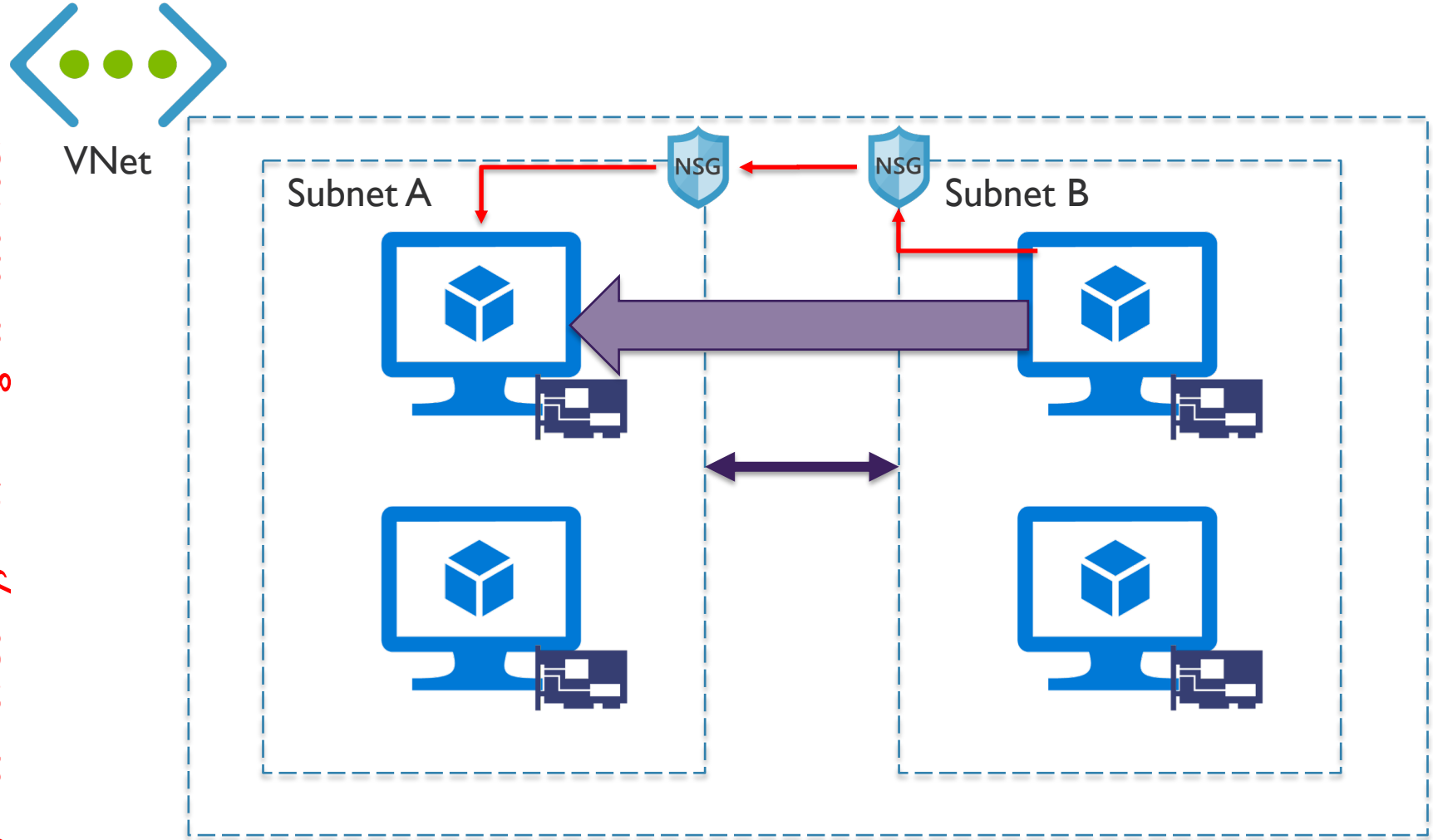
VNet Peering



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

SKYLINES ACADEMY

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

SKYLINES ACADEMY

System-provided to identify groups of IP addresses

Virtual network

Azure Load Balancer

Internet

NSG Default Rules

SKYLINES ACADEMY

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

SKYLINES ACADEMY

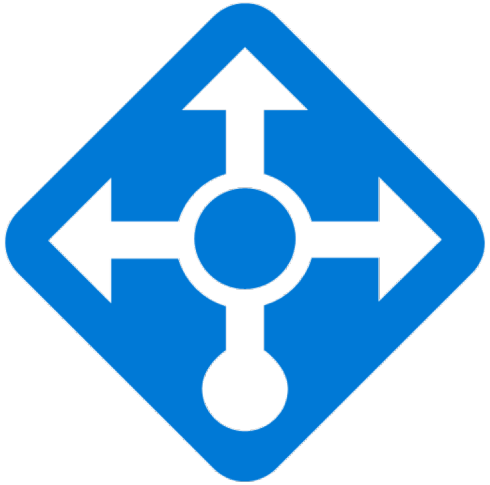
The following limits apply only for networking resources managed through ARM per region per subscription:

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

Azure Load Balancing Services

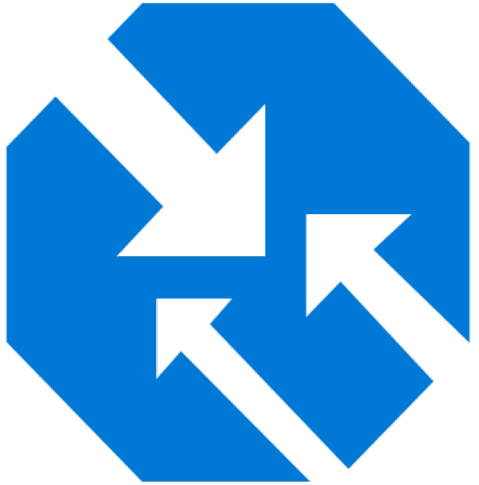
SKYLINES ACADEMY

Load Balancer



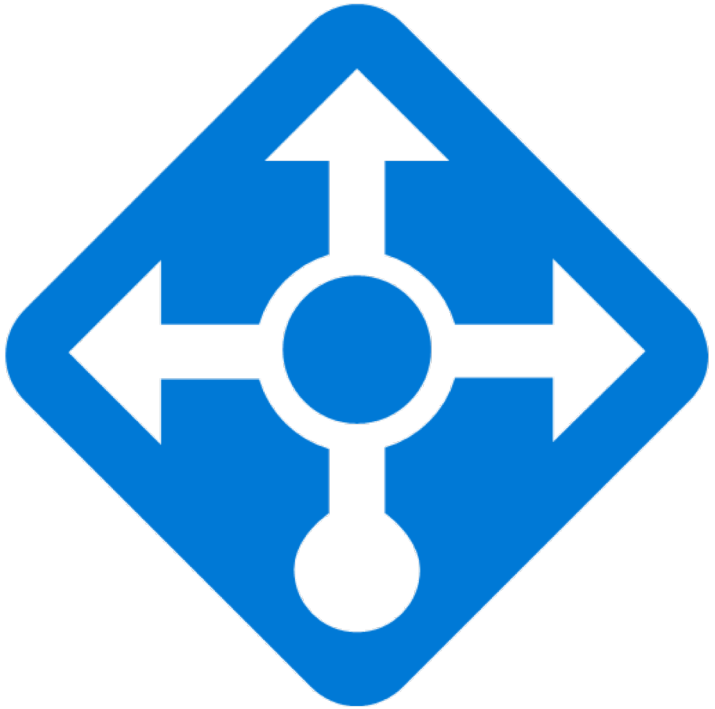
Application Gateway

Traffic Manager



Azure Load Balancer

SKYLINES ACADEMY

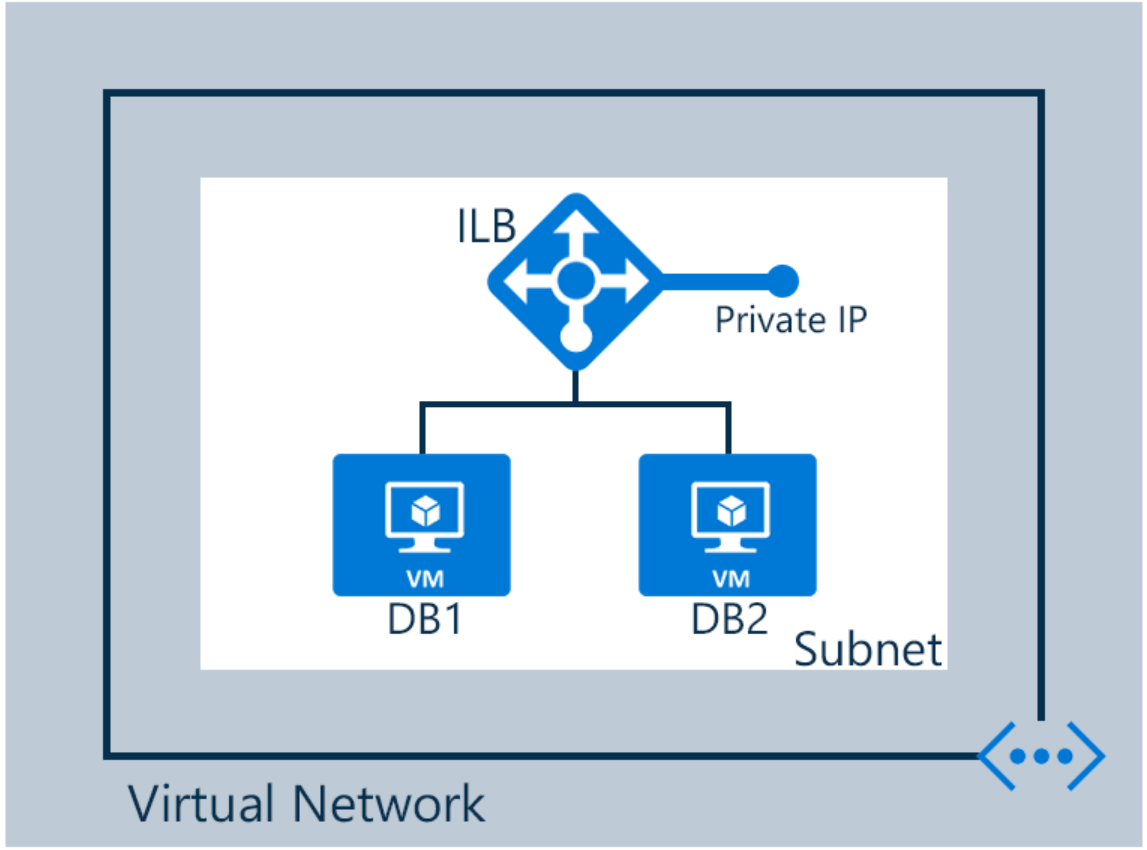


Key Features:

- Layer 4
- Basic and standard (preview) SKUs
- Service monitoring
- Automated reconfiguration
- Hash-based distribution
- Internal and public options

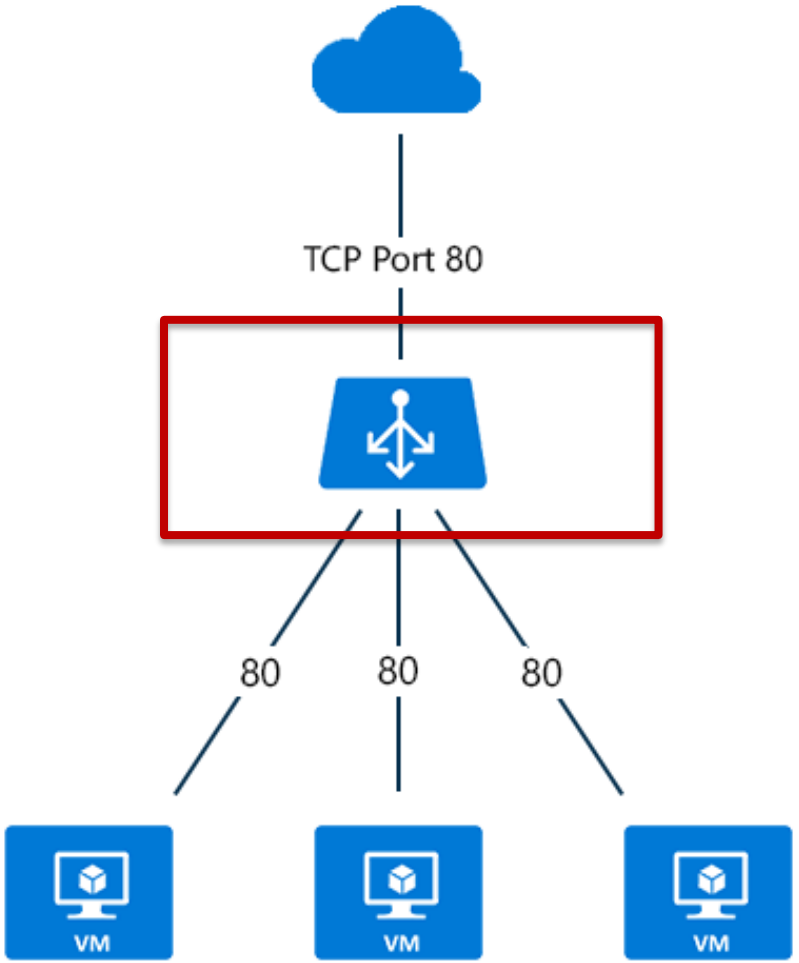
Azure Load Balancer: Internal Example

SKYLINES ACADEMY

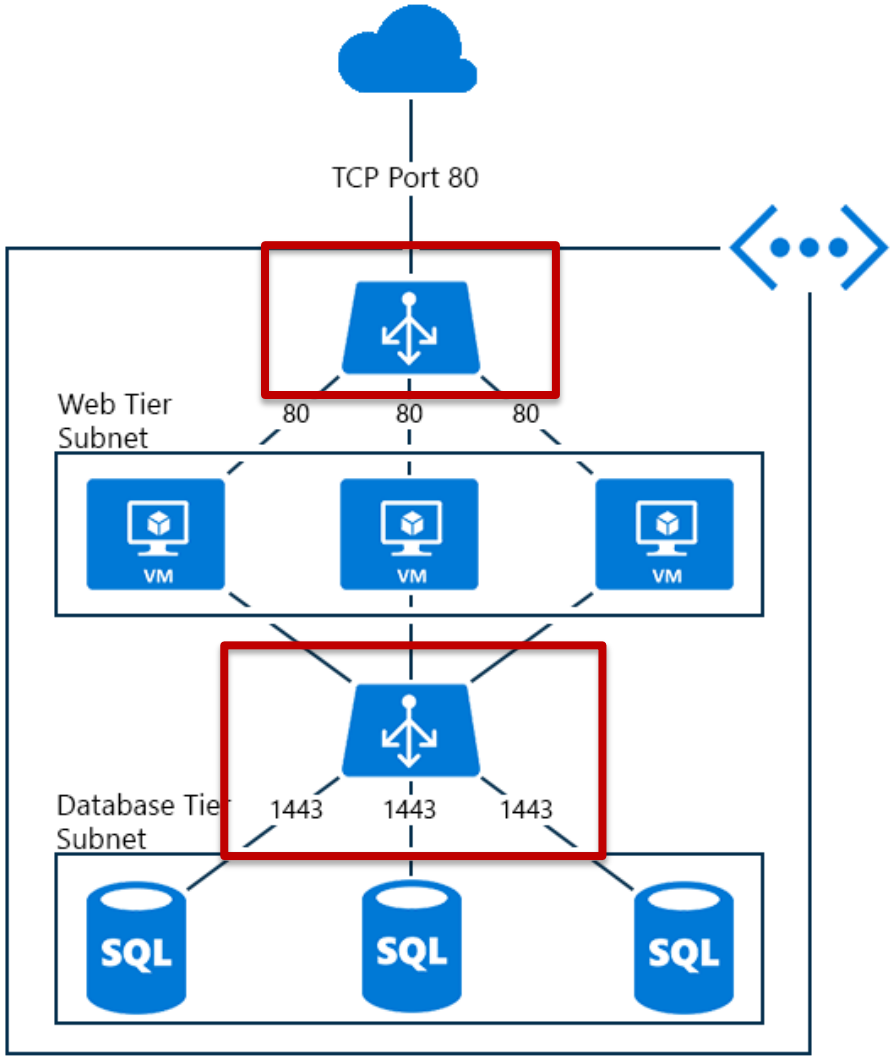


Azure Load Balancer: Public Example

SKYLINES ACADEMY



Azure Load Balancer: Multi-Tier Example



Load Balancing: App Gateway

Key Features:

- Layer 7 application load balancing
- Cookie-based session affinity
- SSL offload
- End-to-end SSL
- Web application firewall
- URL-based content routing
- Requires its own subnet

App Gateway Sizes

SKYLINES ACADEMY

Page Response	Small	Medium	Large
6K	7.5 Mbps	13 Mbps	50 Mbps
100K	35 Mbps	100 Mbps	200 Mbp

Load Balancer Comparison

SKYLINES ACADEMY

Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport level (Layer 4)	Application level (Layer 7)	DNS-level
Application Protocols Supported	Any	HTTP, HTTPS, and WebSockets	Any (An HTTP endpoint is required for endpoint monitoring)
Endpoints	Azure VMs and Cloud Services role instances	Any Azure internal IP address, public internet IP address, Azure VM, or Azure Cloud Service	Azure VMs, Cloud Services, Azure Web Apps, and external endpoints
VNet support	Can be used for both Internet- facing and internal (VNet) applications	Can be used for both Internet-facing and internal (VNet) applications	Only supports Internet-facing applications
Endpoint Monitoring	Supported via probes	Supported via probes	Supported via HTTP/HTTPS GET

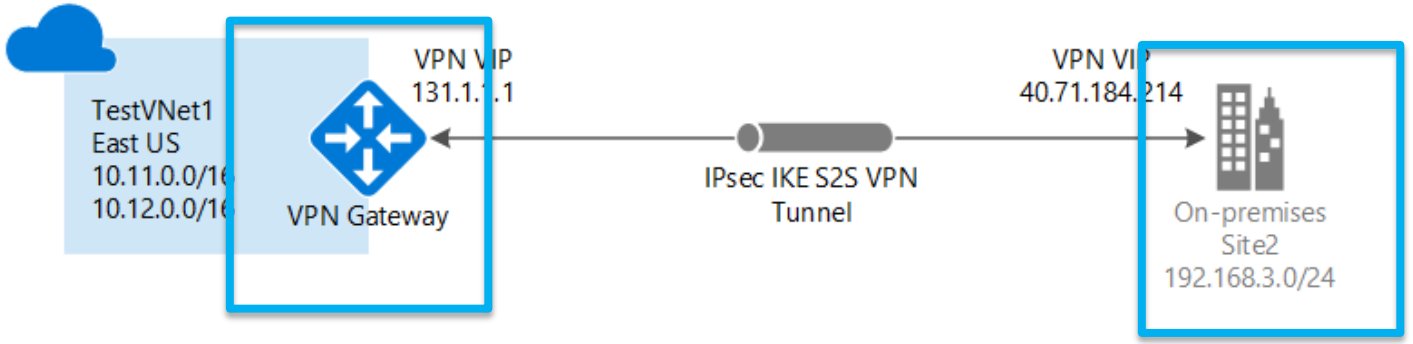
Hybrid Connectivity Options

SKYLINES ACADEMY

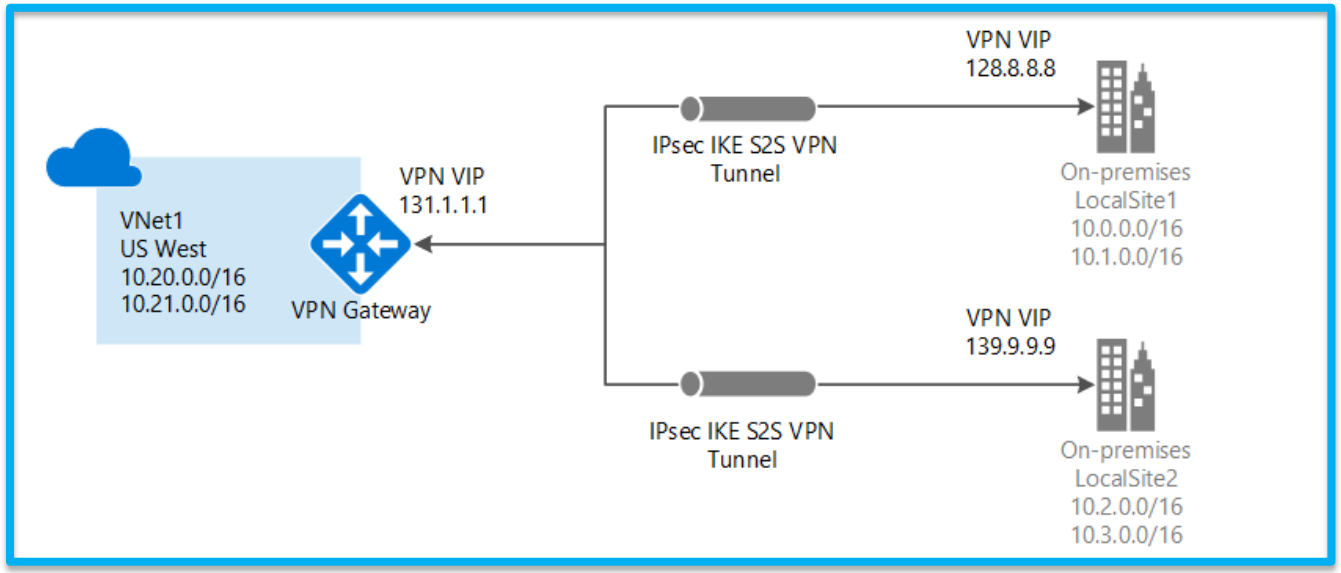
- Site-to-Site (S2S)
- ExpressRoute
- Point-to-Site (P2S)

S2S

S2S



Multi-Site



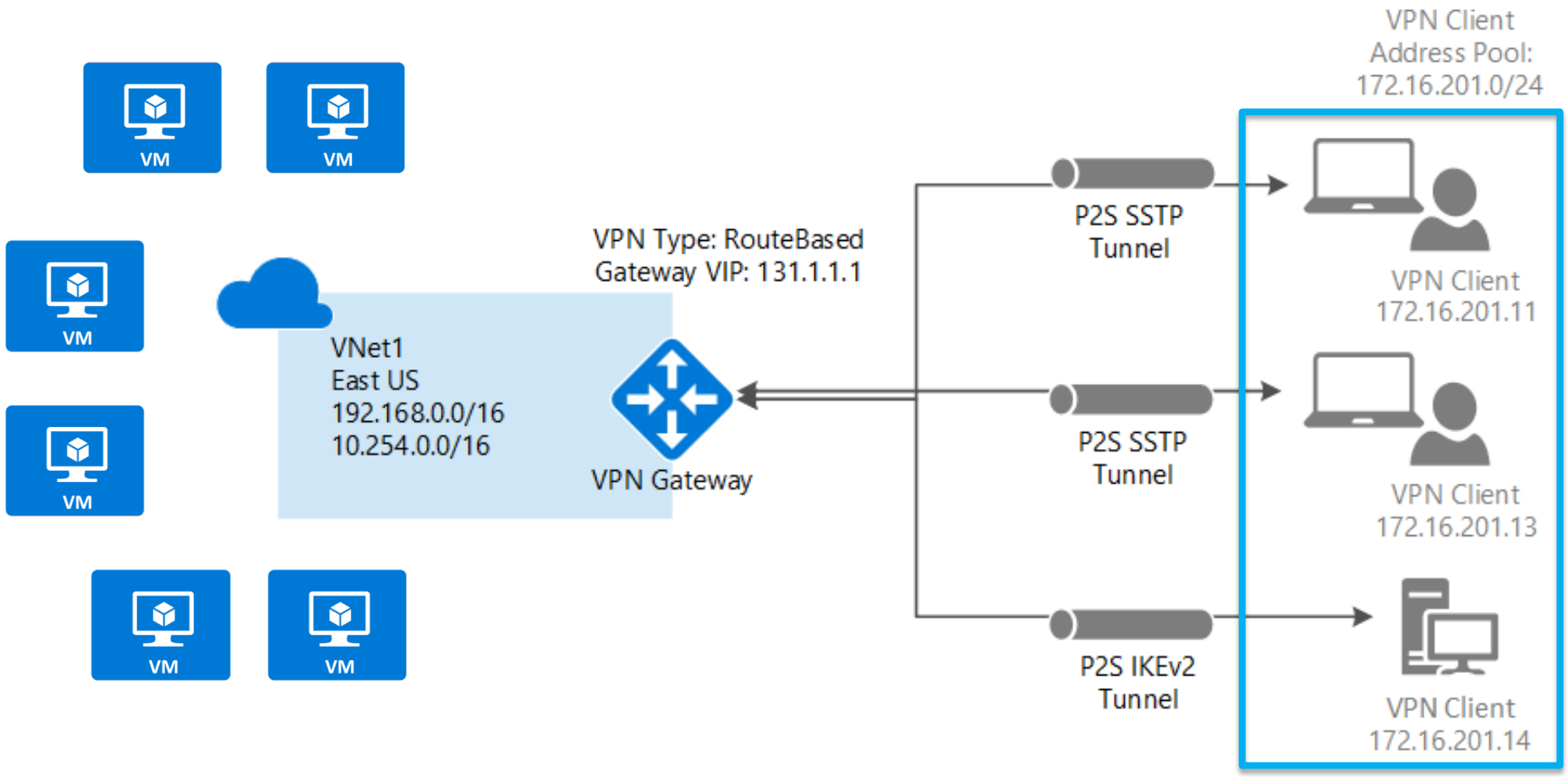
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

S2S (continued)

SKYLINES ACADEMY

- S2S VPN gateway connection is a connection over **IPsec/IKE** (IKEv1 or IKEv2) VPN tunnel
- Requires a VPN device in enterprise datacenter that has a public IP address assigned to it
- Must **not** be located behind a NAT
- S2S connections can be used for cross-premises and hybrid configurations

P2S



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

P2S (continued)

SKYLINES ACADEMY

- Secure connection from an individual computer. Great for remote worker situations.
- No need for a VPN device or public IP. Connect wherever user has internet connection.
- OS Support: Windows 7, 8, 8.1 (32 and 64bit), Windows 10, Windows Server 2008 R2, 2012, 2012 R2 64-bit.
- Throughput up to 100 Mbps (unpredictable due to internet).
- Doesn't scale easily, so only useful for a few workstations.

VPN Gateway SKUs

SKYLINES ACADEMY

SKU	S2S/VNet-to-VNet Tunnels	P2S Connections	Aggregate Throughput Benchmark
VpnGw1	Max. 30	Max. 128	650 Mbps
VpnGw2	Max. 30	Max. 128	1 Gbps
VpnGw3	Max. 30	Max. 128	1.25 Gbps
Basic	Max. 10	Max. 128	100 Mbps

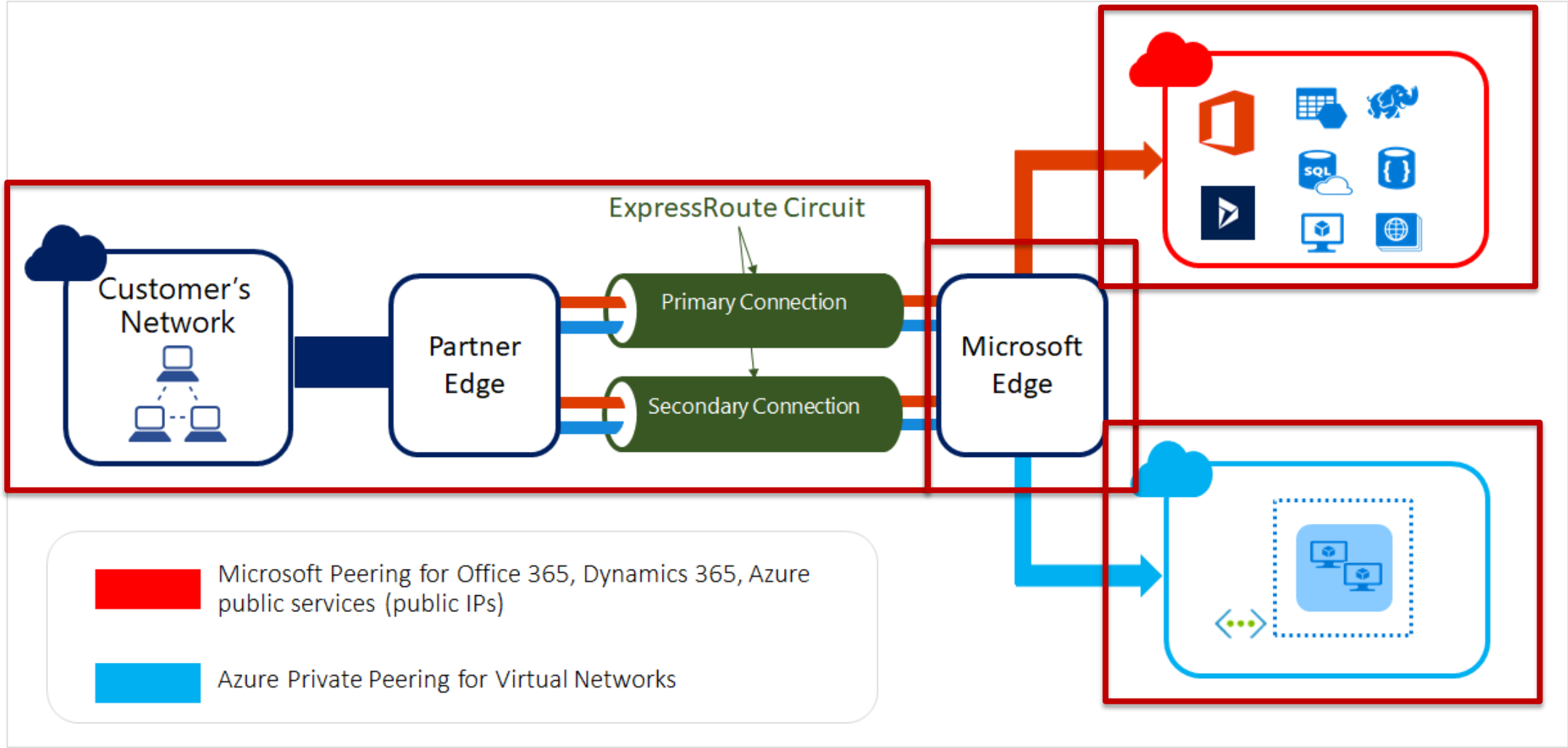
Gateway Recommendations

SKYLINES ACADEMY

Workload	SKUs
Production, critical workloads	VpnGw1, VpnGw2, VpnGw3
Dev-test or proof of concept	Basic

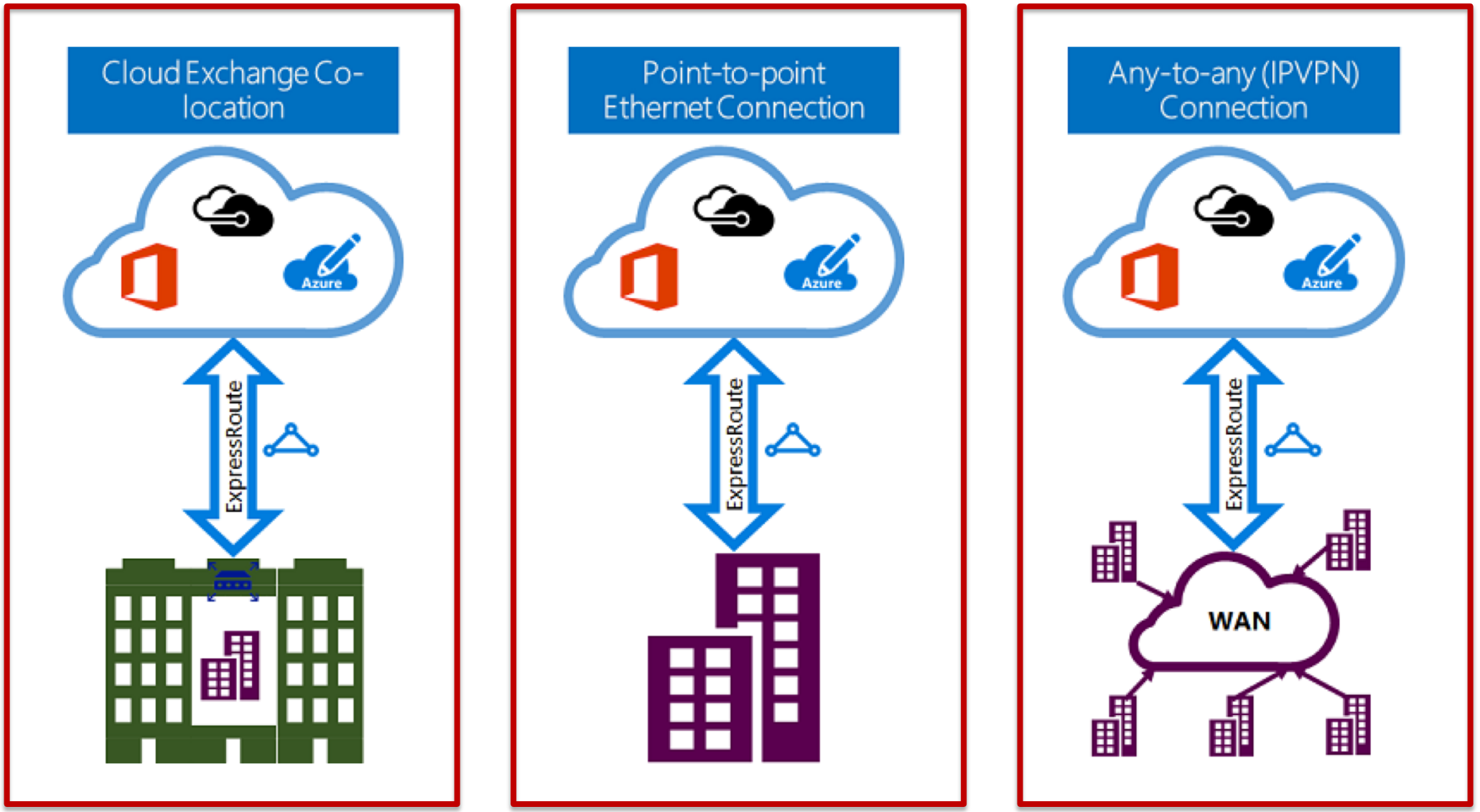
SKU	Features
Basic	**Route-based VPN**: 10 tunnels with P2S; no RADIUS authentication for P2S; no IKEv2 for P2S **Policy-based VPN**: (IKEv1): 1 tunnel; no P2S
VpnGw1, VpnGw2, and VpnGw3	**Route-based VPN**: up to 30 tunnels (*), P2S, BGP, active-active, custom IPsec/IKE policy, ExpressRoute/VPN co-existence

ExpressRoute



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

ExpressRoute Connectivity Models



ExpressRoute Key Benefits

SKYLINES ACADEMY

Layer 3 Connectivity

Between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.

Connectivity in all Regions

To Microsoft cloud services across all regions in the geopolitical region.

Global Connectivity

To Microsoft services across all regions with ExpressRoute premium add-on.

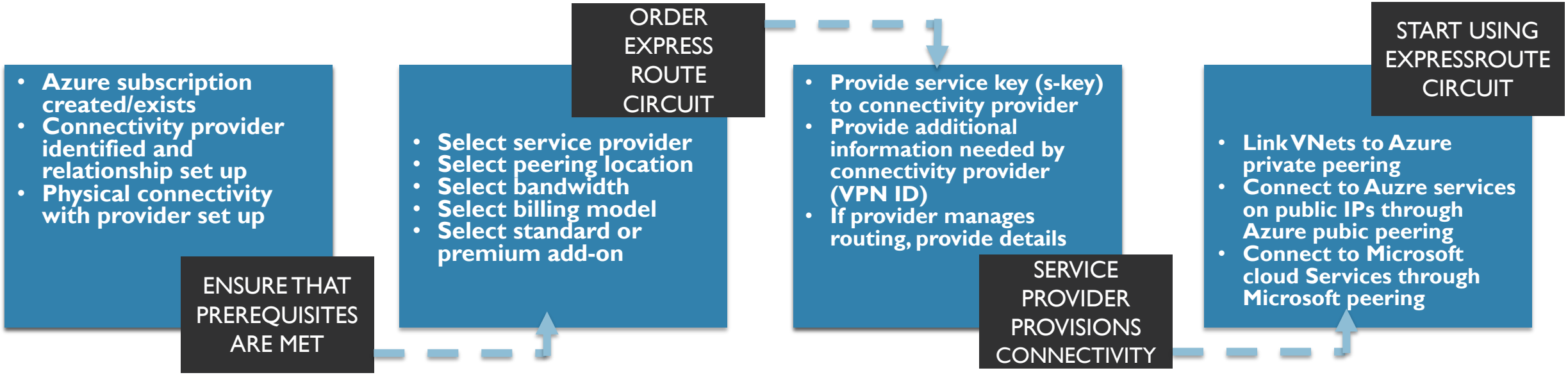
Dynamic Routing

Between your network and Microsoft over industry standard protocols (BGP).

Built-In Redundancy

In every peering location for higher reliability

ExpressRoute Provisioning



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

Peering – Data to Collect

SKYLINES ACADEMY

Azure Private Peering

- Peering subnet for path 1 (/30)
- Peering subnet for path 2 (/30)
- VLAN ID for peering
- ASN for peering
- ExpressRoute ASN = 12076
- MD5 Hash (optional)

Azure Public Peering

- Peering subnet for path 1 (/30) – must be public IP
- Peering subnet for path 2 (/30) – must be public IP
- VLAN ID for peering
- ASN for peering
- ExpressRoute ASN = 12076
- MD5 Hash (optional)

Microsoft Peering

- Peering subnet for path 1 (/30) – must be public IP
- Peering subnet for path 2 (/30) – must be public IP
- VLAN ID for peering
- ASN for peering
- Advertised prefixes – must be public IP prefixes
- Customer ASN (optional if different from peering ASN)
- RIR/IRR for IP and ASN validation
- ExpressRoute ASN = 12076
- MD5 Hash (optional)

Unlimited versus Metered

SKYLINES ACADEMY

Unlimited

- Speeds from 50 Mbps to 10 Gbps
- Unlimited Inbound data transfer
- Unlimited Outbound data transfer
- Higher monthly fee

Metered

- Speeds from 50 Mbps to 10 Gbps
- Unlimited Inbound data transfer
- Outbound data transfer charged at a predetermined rate per GB
- Lower monthly fee

ExpressRoute Considerations

SKYLINES ACADEMY

Understand the models

- Differences between Unlimited Data and Metered Data
- Understand what model you are using today to accelerate adoption
- Understand the differences in available port speeds, locations and approach
- Understand the limits that drive additional circuits

Understand the providers

- Each offer a different experience based on ecosystem and capabilities
- Some provide complete solutions and management

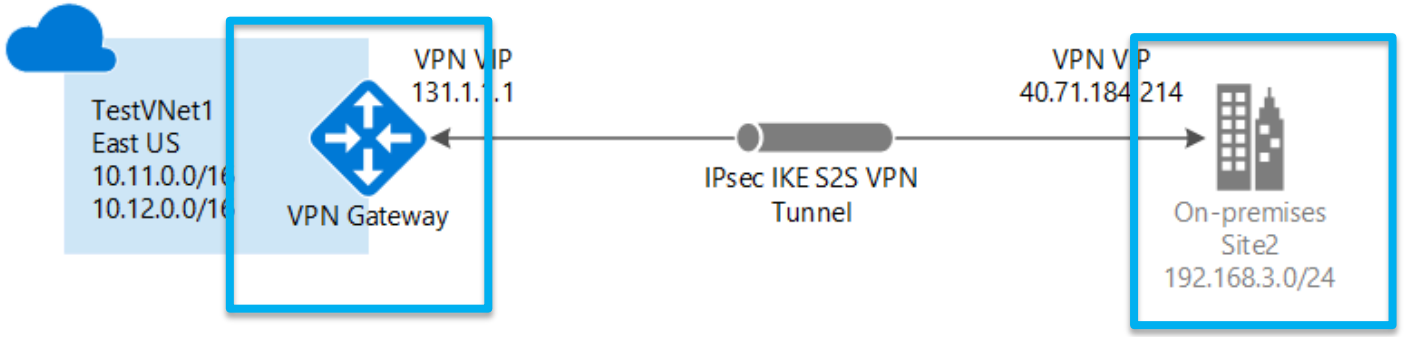
Understand the costs

- Connection costs can be broken out by the service connection costs (Azure) and the authorized carrier costs (telco partner)
- Unlike other Azure services, look beyond the Azure pricing calculator

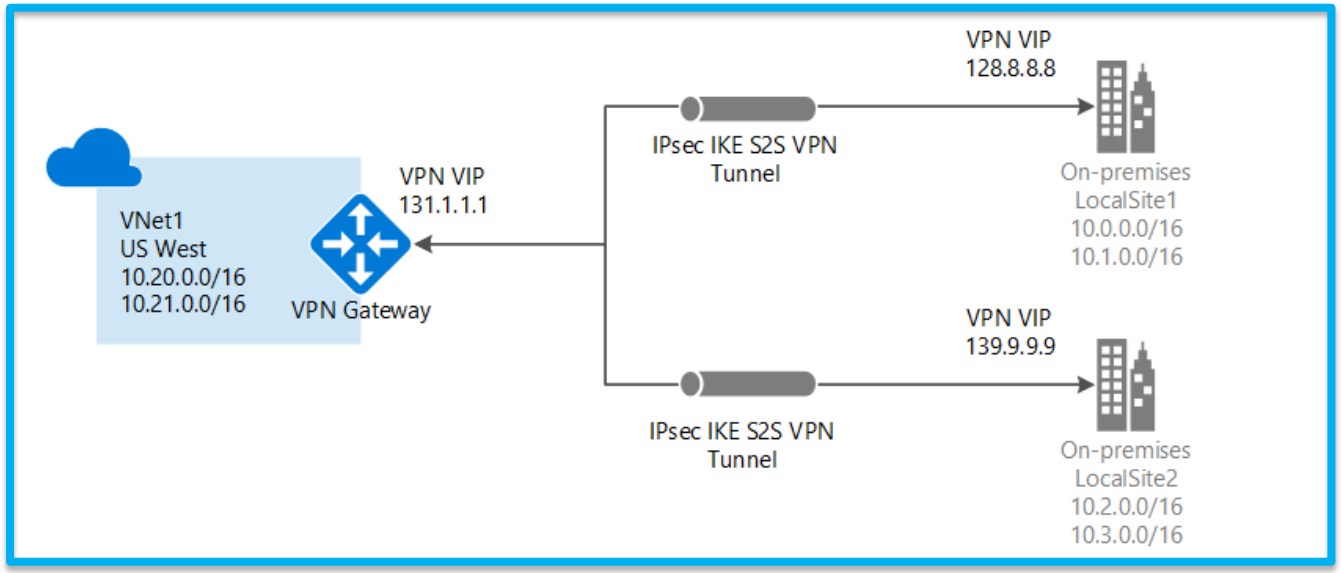
Connectivity Recap

SKYLINES ACADEMY

S2S

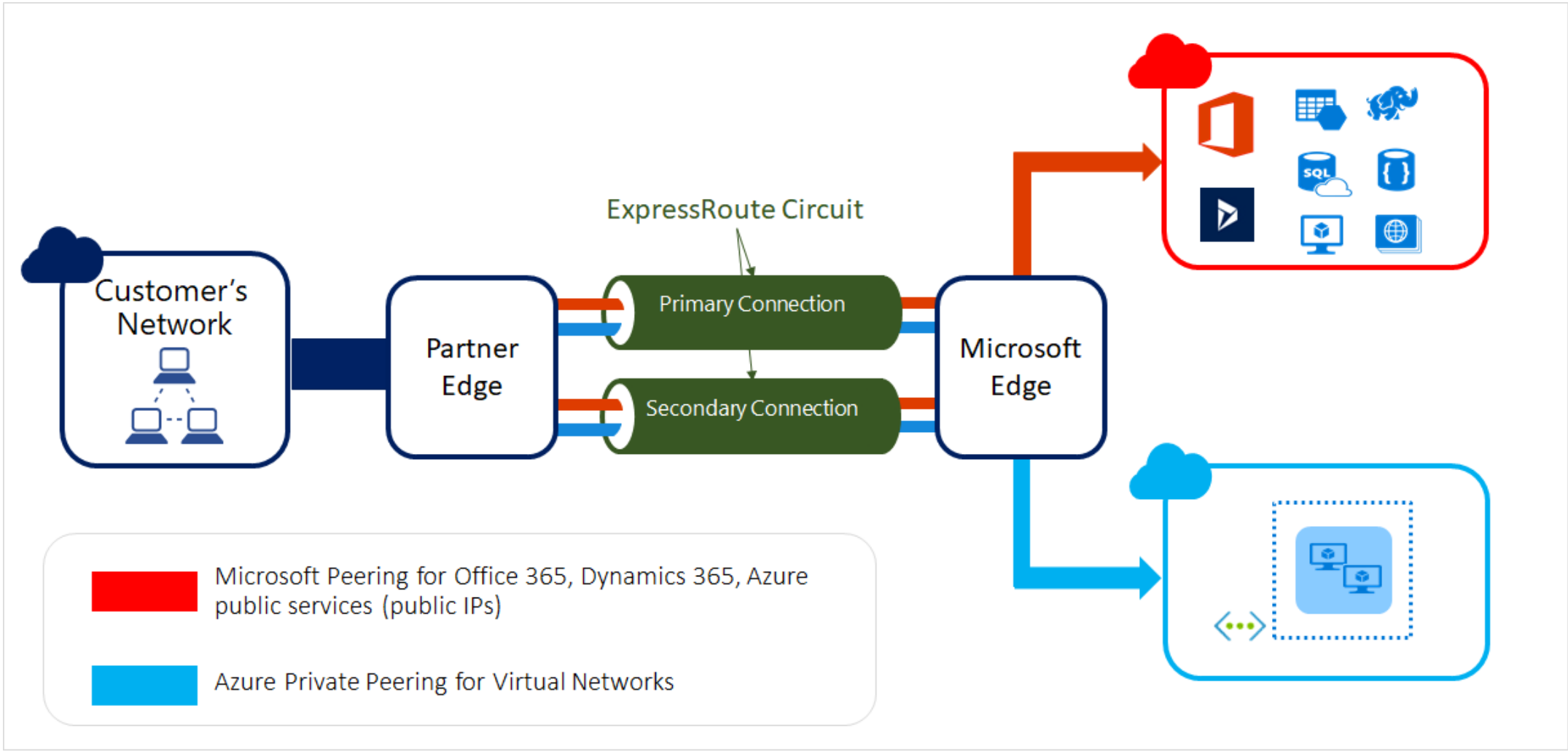


Multi-Site



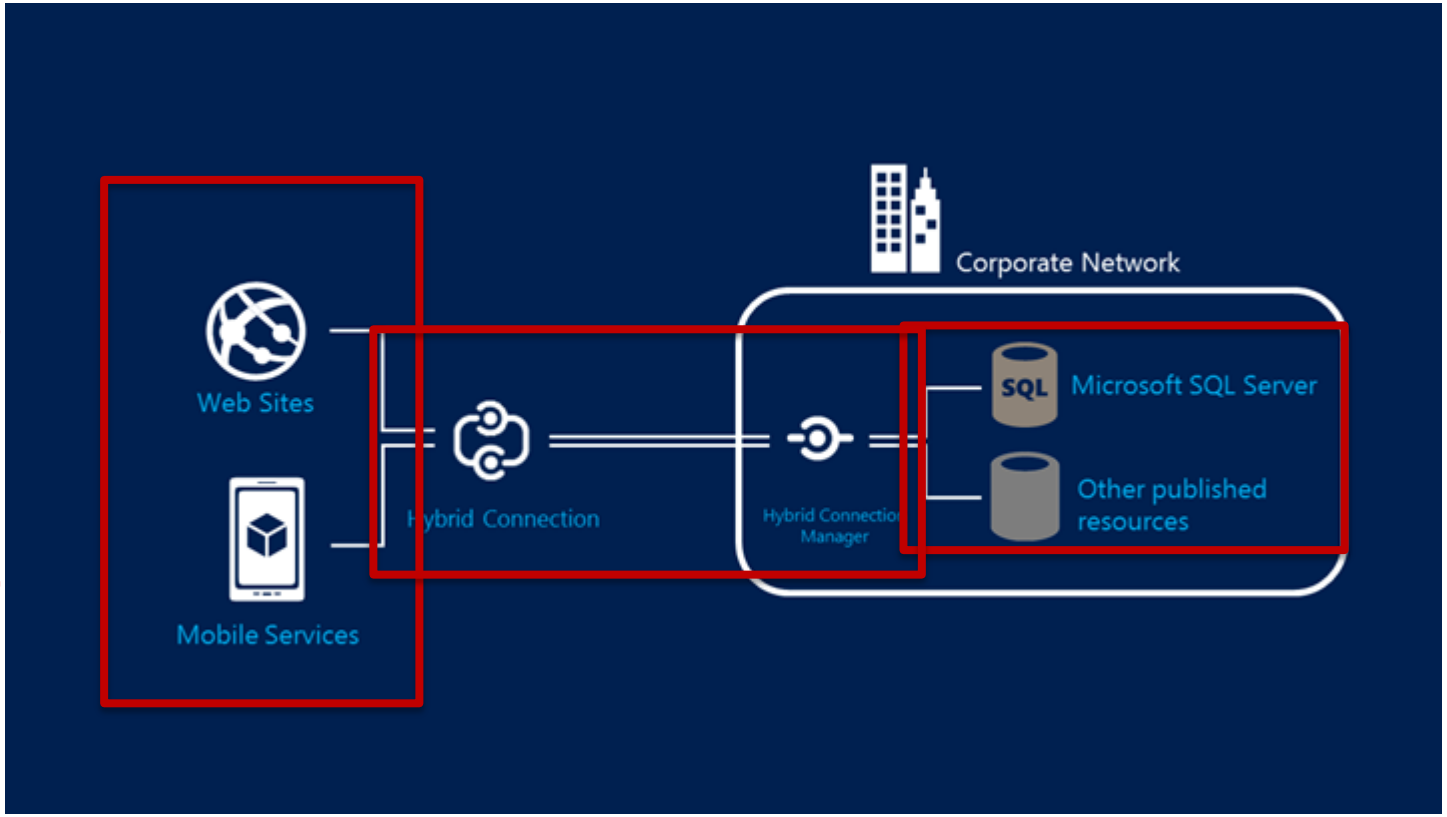
ExpressRoute Recap

SKYLINES ACADEMY



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

SKYLINES ACADEMY

.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

SKYLINES ACADEMY

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)

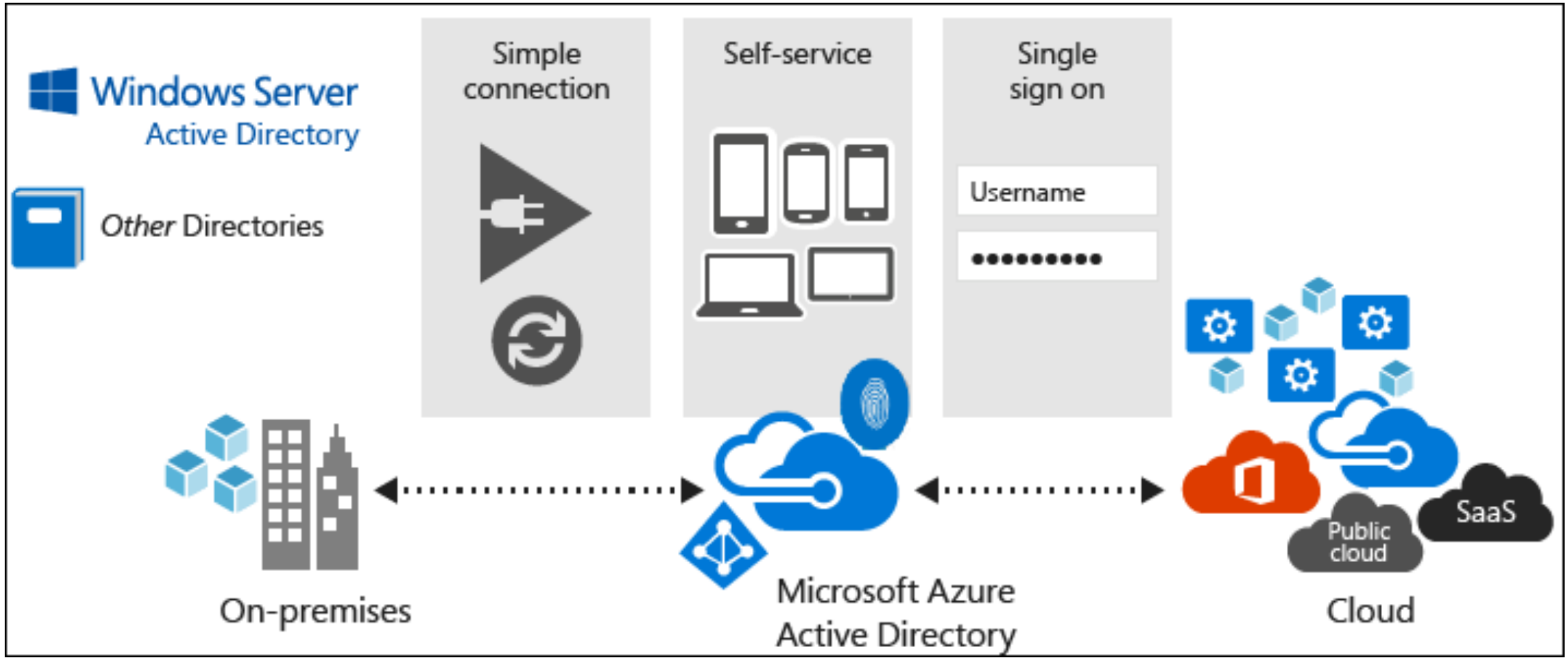
- Windows Server 2012 (Windows Management Framework 4.0+ required)

- Windows Server 2012 R2

Module:
Manage Identities

SKYLINES
ACADEMY

Azure AD Overview



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

Azure AD Features

SKYLINES ACADEMY

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.

Module:
ARM and Automation

SKYLINES
ACADEMY

Resource Manager Overview

SKYLINES ACADEMY

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

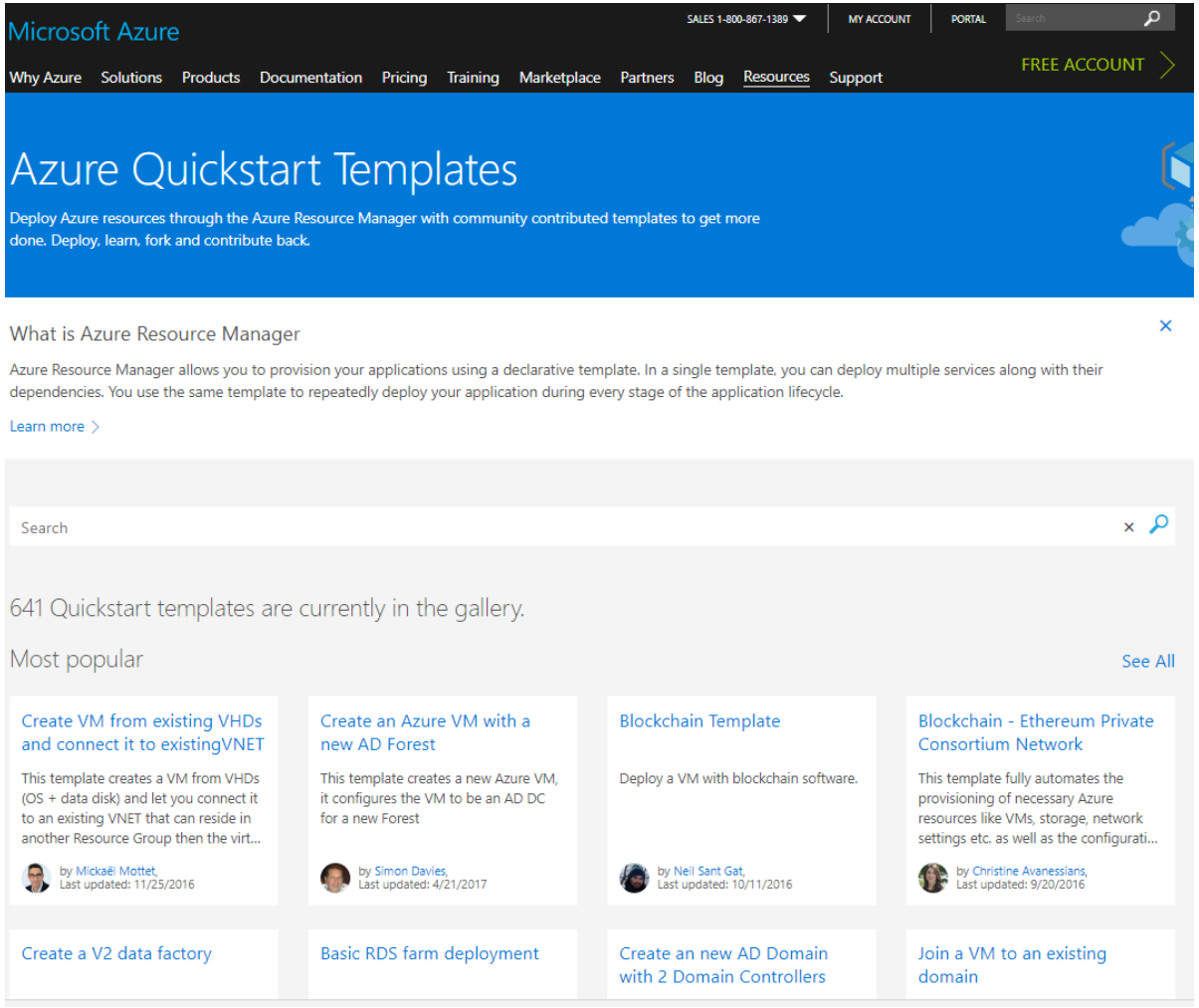
SKYLINES ACADEMY

```
{
  "$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



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

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

ARM File Types

SKYLINES ACADEMY

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

SKYLINES ACADEMY

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.

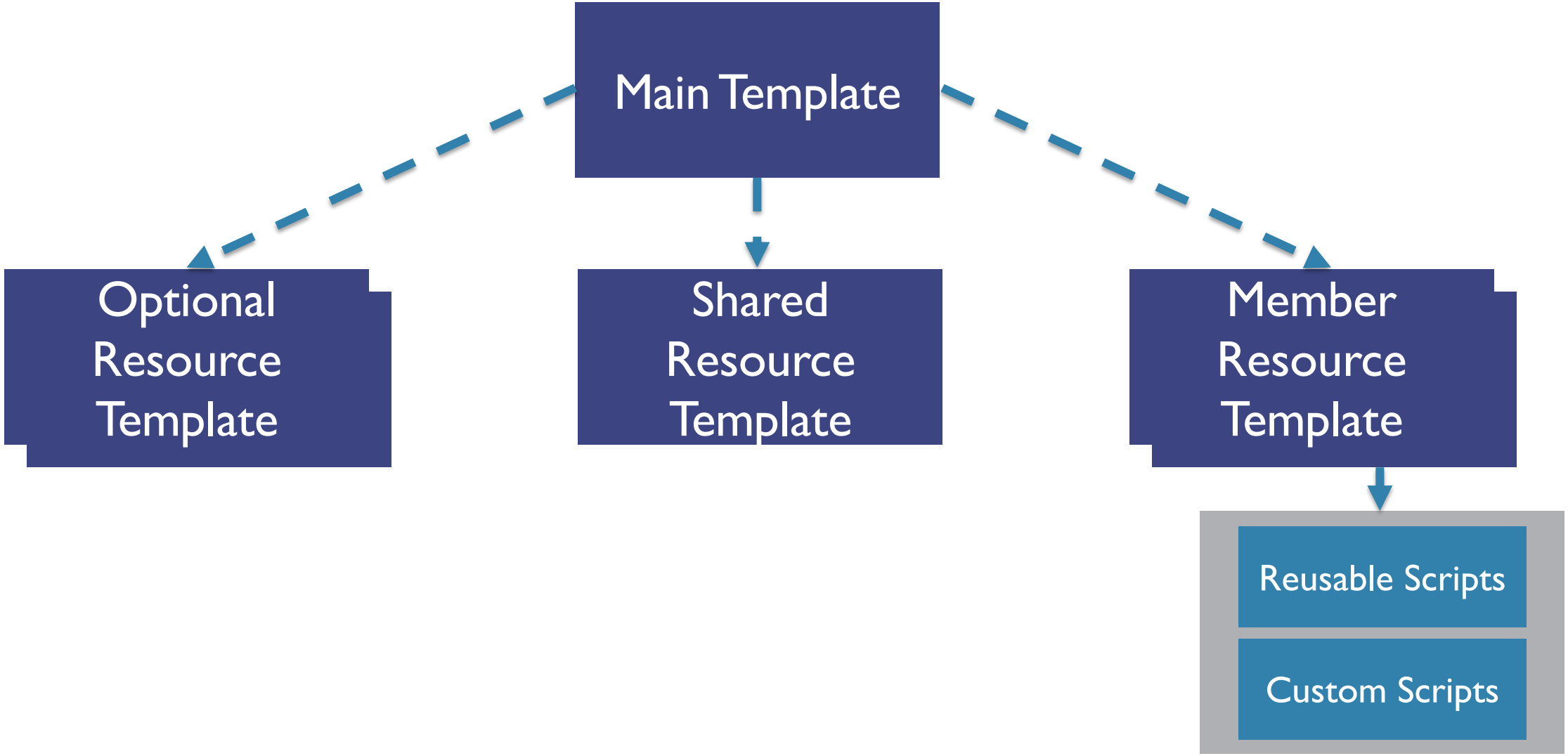
Resources

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

SKYLINES ACADEMY

```
"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

SKYLINES ACADEMY

```
"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

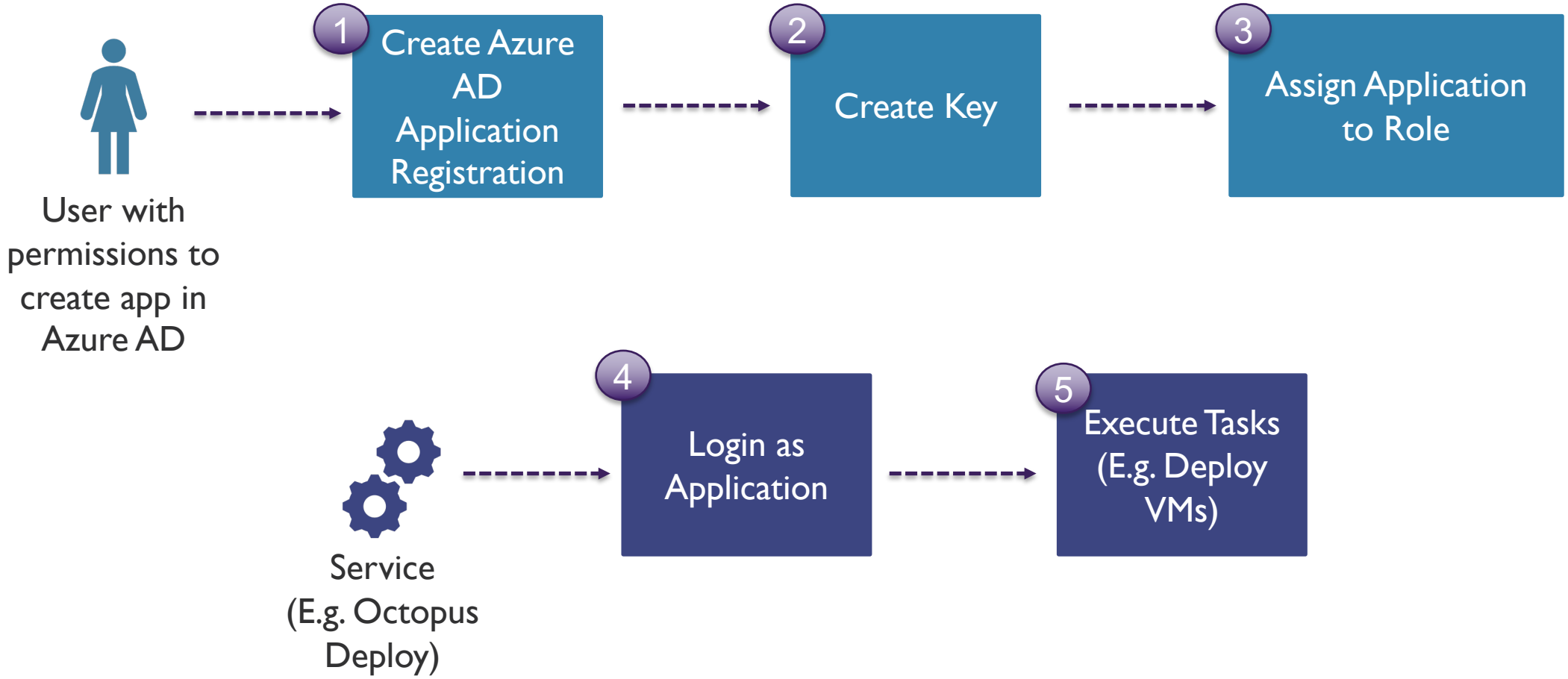
SKYLINES ACADEMY

Copy

copyIndex()

dependsOn

Process for Creating a Service Principal



Azure Policies

SKYLINES ACADEMY

Enforce Governance

Built-in or Custom Code

Assigned to Subscriptions or Resource Groups

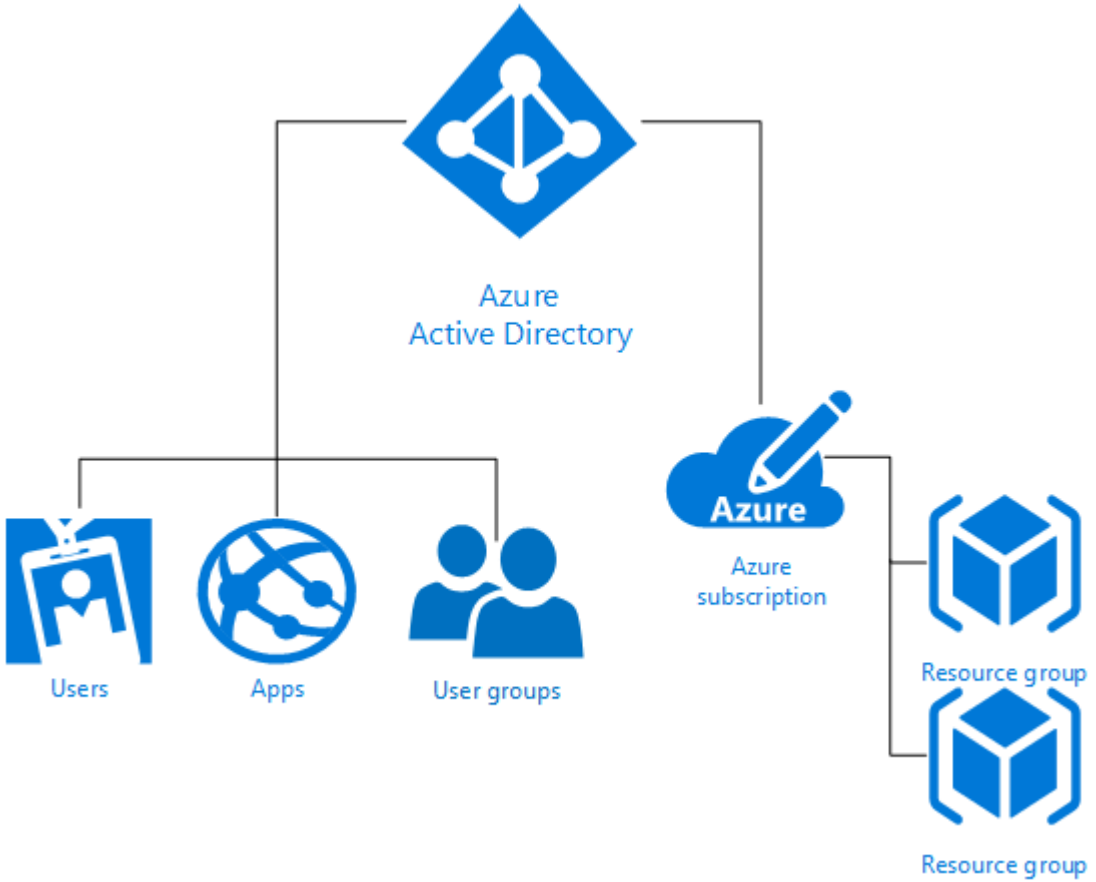
Create > Assign

Azure Resource Locks

SKYLINES ACADEMY

- 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

RBAC Overview



- Create Users, Apps, Groups
- Assign them to objects in Azure with a specific Role

Azure RBAC Built-in Roles

SKYLINES ACADEMY

Owner	Contributor	Reader	Other Roles
Full access to all resources, including the right to delegate access to others	Can create and manage all types of Azure resources, but cannot grant access to others	Can view existing Azure resources, but cannot perform any other actions against them	https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles

Azure RBAC Built-in Roles (continued)

SKYLINES ACADEMY

Role Name	Description
API Management Service Contributor	Can manage API Management service and the APIs
API Management Service Operator Role	Can manage API Management service, but not the APIs themselves
API Management Service Reader Role	Read-only access to API Management service and APIs
Application Insights Component Contributor	Can manage Application Insights components
Automation Operator	Able to start, stop, suspend, and resume jobs
Backup Contributor	Can manage backup in Recovery Services vault
Backup Operator	Can manage backup except moving backup in Recovery Services vault
Backup Reader	Can view all backup management services

https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles

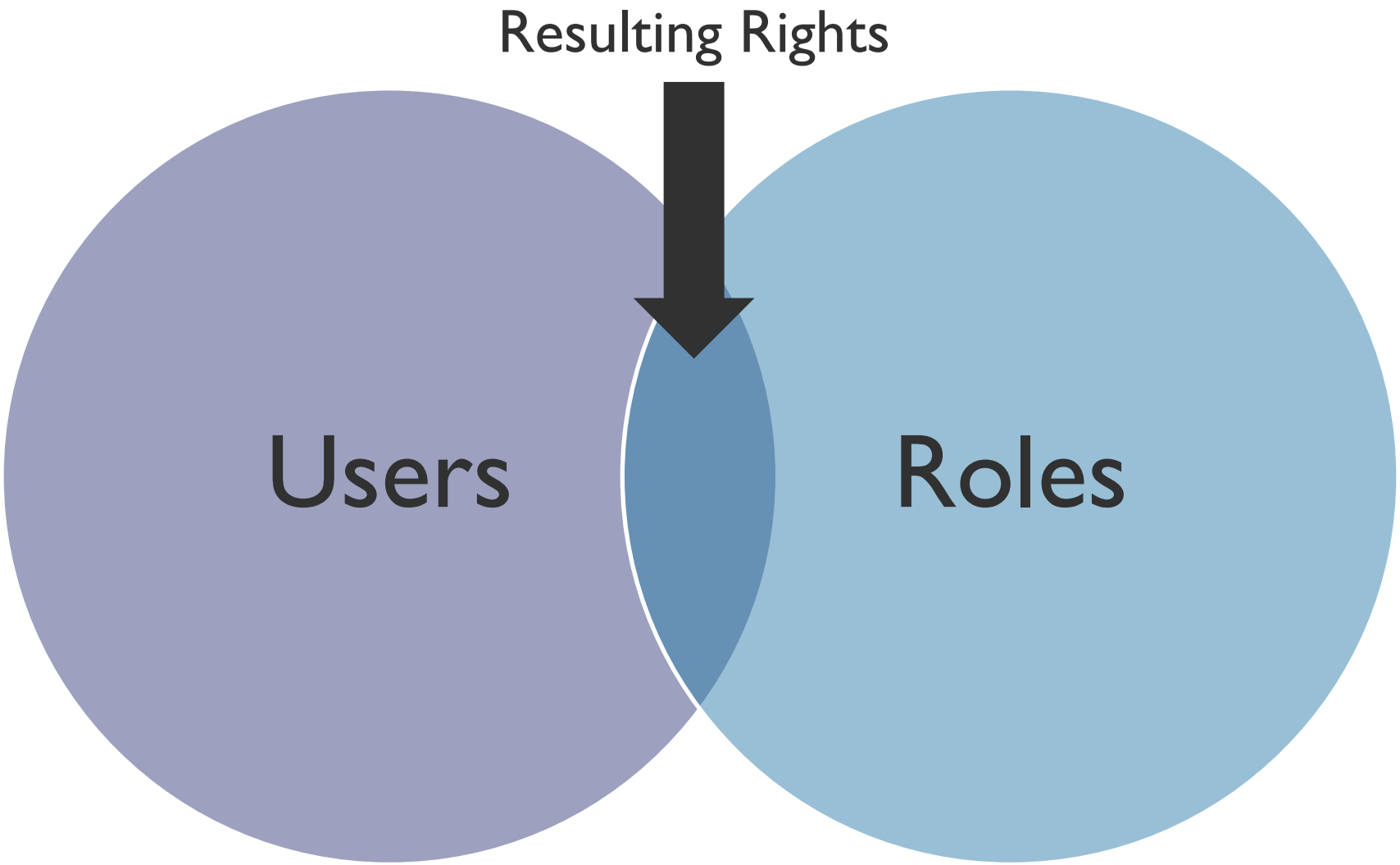
Azure RBAC Built-in Roles (continued)

SKYLINES ACADEMY

- Roles include various actions
- Action defines what type of operations you can perform on a given resource type
  - Write enables you to perform PUT, POST, PATCH, and DELETE operations
  - Read enables you to perform GET operations
- Use PowerShell to get latest roles

Get latest roles	Get-AzureRMRoleDefinition

User Rights



RBAC Custom Roles

SKYLINES ACADEMY

Create if none of the built-in roles work for you

Each tenant can have to 2000 roles

Use "Actions" and "NotActions"

Assignable scopes:
- Subscriptions
- Resource Groups
- Individual Resources