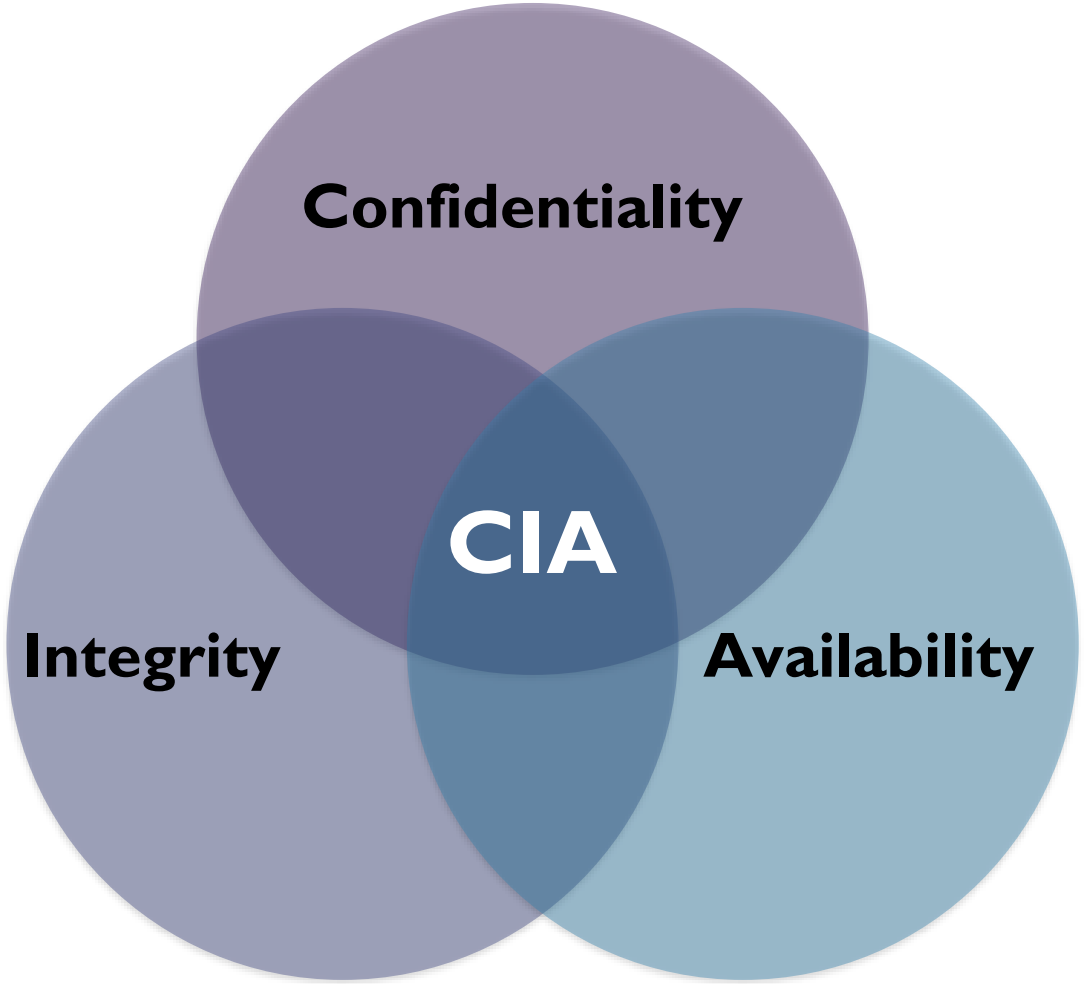
SKYLINES

ACADEMY

Defense in Depth

Defense in Depth



Confidentiality

- Principle of least privilege
- Restricts access to information only to individuals explicitly granted
- Information includes protection of user passwords, remote access certificates, and e-mail content

Integrity

- Prevention of unauthorized changes to information at rest or in transit
- Data Transmission: Sender creates unique fingerprint of the data with a one-way hashing algorithm

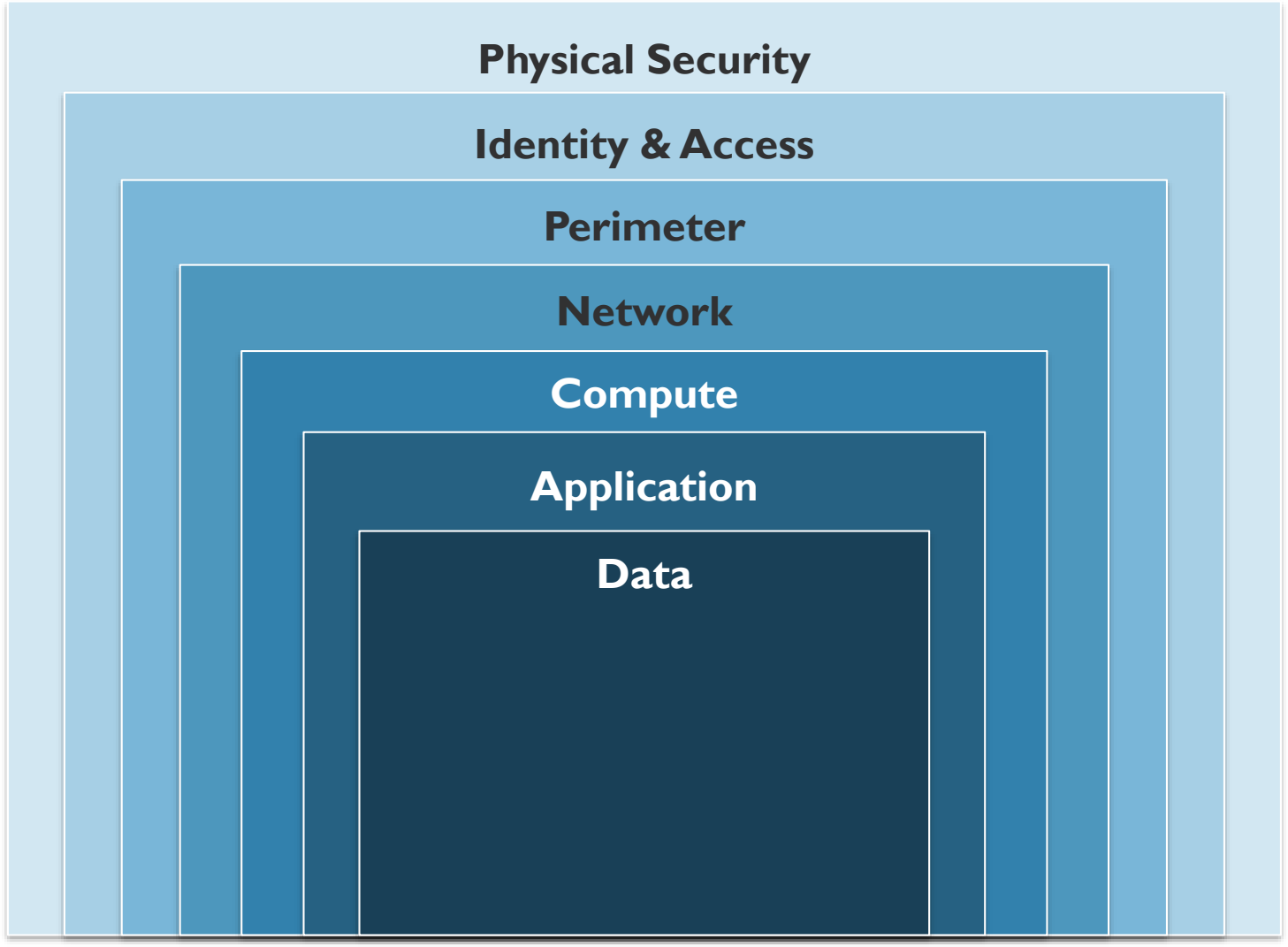
Availability

- Ensure services are available
- Prevent denial of service attacks
- Consider natural disasters
- High availability and disaster recovery

Security Layers

Security Layers

SKYLINES ACADEMY



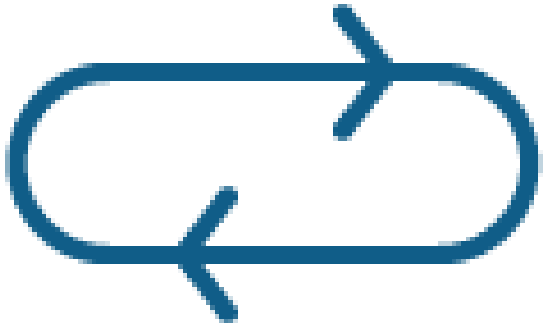
Physical Security

- Physical building security
- Control access to datacenter hardware
- Intent is to provide physical safeguards to ensure other layers are not bypassed

Identity & Access

- Authenticate – Prove who you are
- Authorization – What you are allowed to do
- Control access to infrastructure
- Audit events and changes

Perimeter



- Use DDOS protection to filter large scale attacks
- Firewalls at the perimeter to prevent intrusions
- Goal is to protect your network from attacks against your resources. Identify the attacks, minimize impact, and alert on them

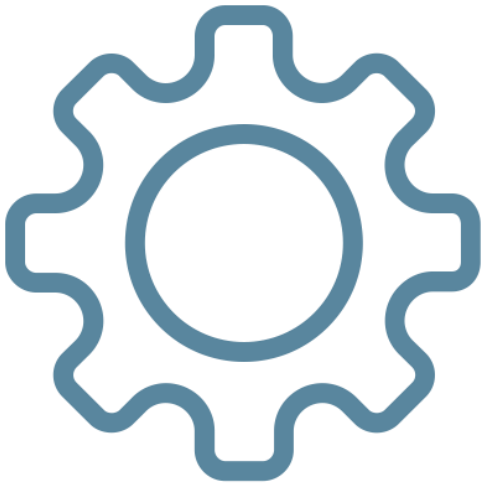
Network

- Limit communication via micro-segmentation and access controls
- Deny by default
- Restrict inbound internet access and limit outbound
- Only allow what is required

Compute

- Harden virtual machines
- Implement endpoint protection
- Control access to operating systems
- Good housekeeping is essential to ensure systems are patched and you aren't exposing the environment to additional risks

Application



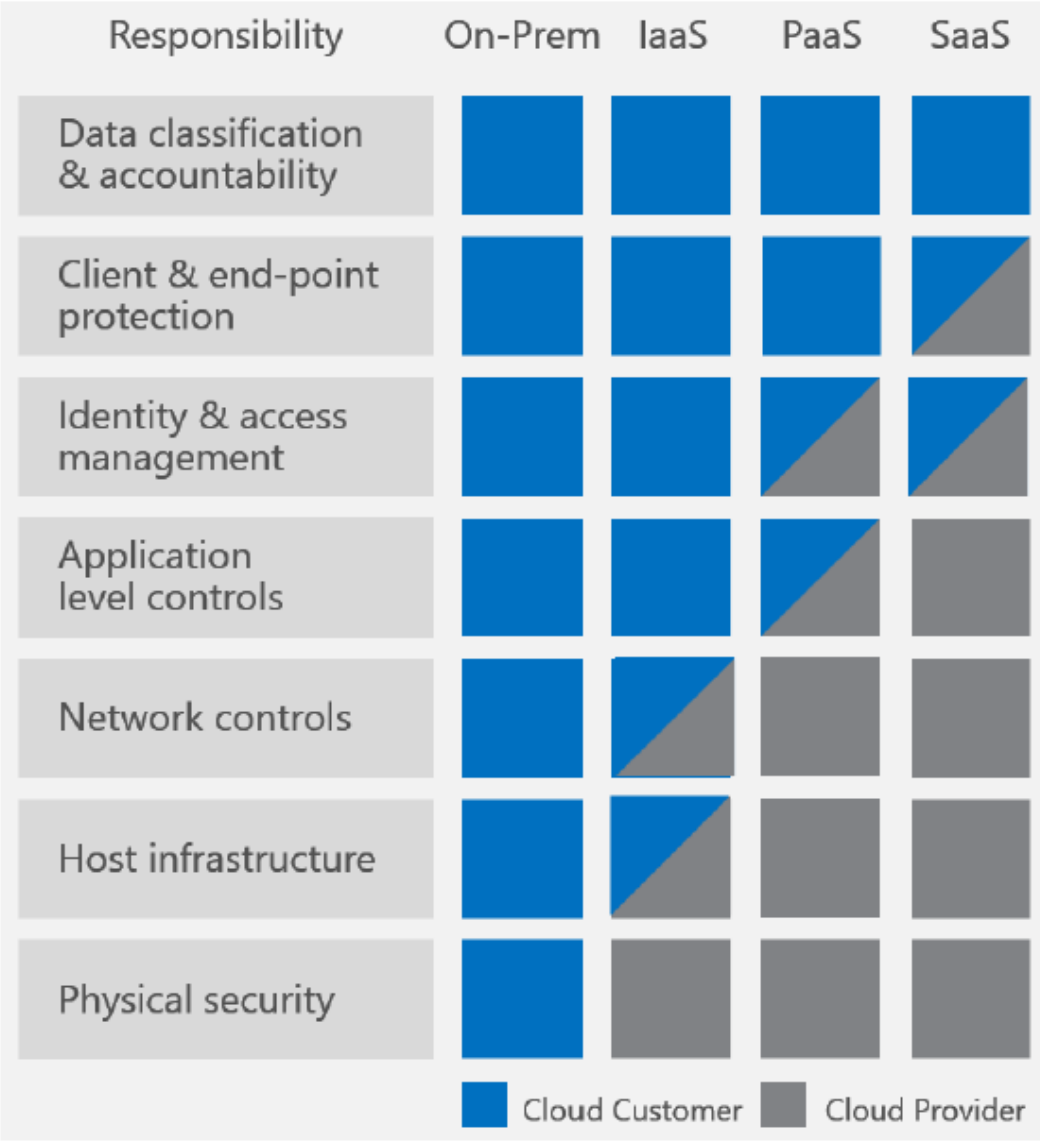
- Ensure applications are secure
- Store sensitive application secrets appropriately
- Make security design a requirement for all new application development

Data

- Almost all attackers are trying to gather data
- Data is stored
  - In databases
  - On disks inside VMs
  - SaaS apps such as O365
  - Cloud storage
- Responsible for ensuring data is properly secured while at rest and in transit

Compliance and Security Requirements

Shared Responsibility Model



- Security is a joint responsibility
- Cloud computing clearly provides many benefits over on-premises
- As you move from IaaS > PaaS > SaaS you can offload more of the controls to Microsoft

You are always responsible for…

Data

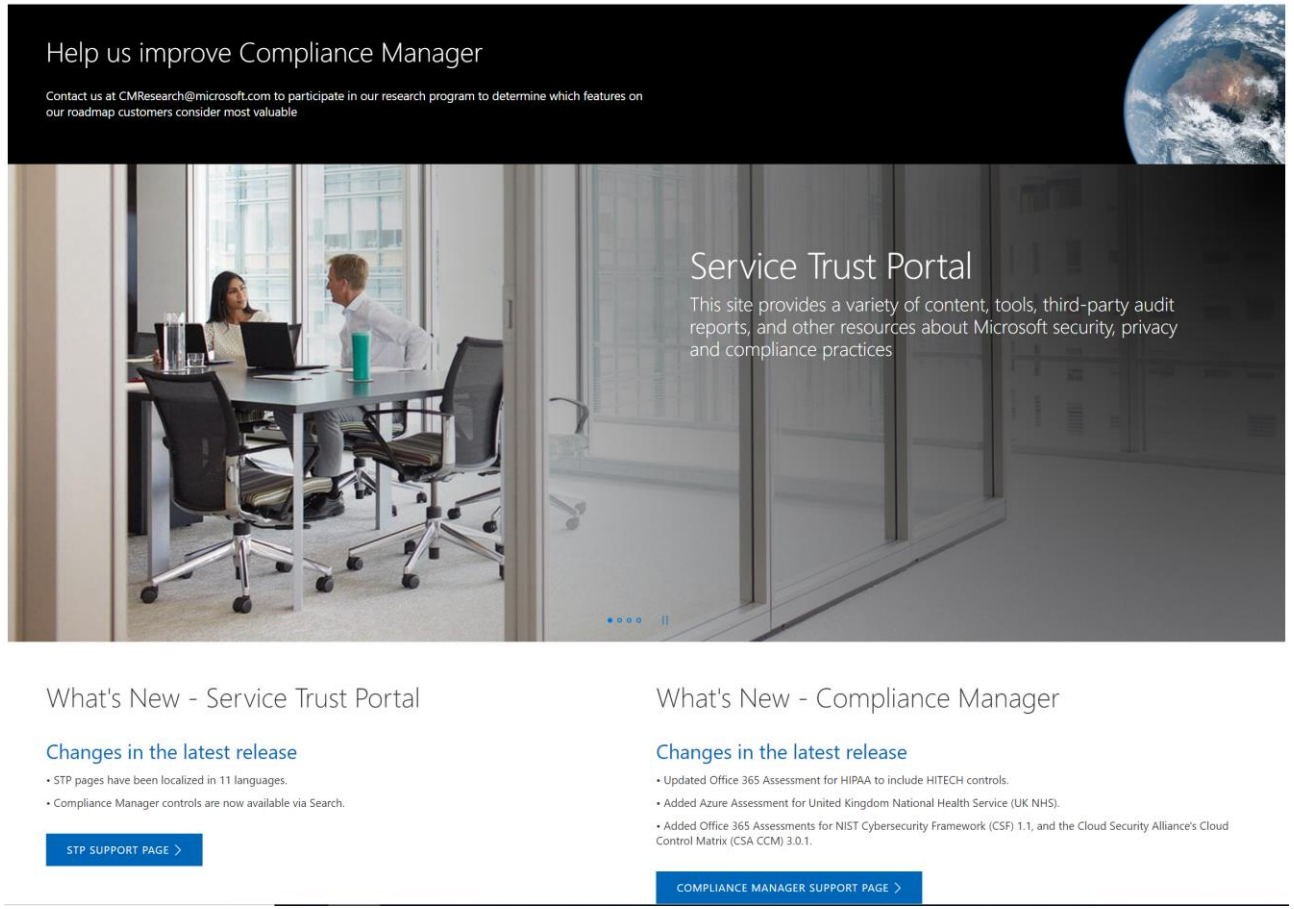
Endpoints

Account

Access Management

https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

Microsoft Trust Center

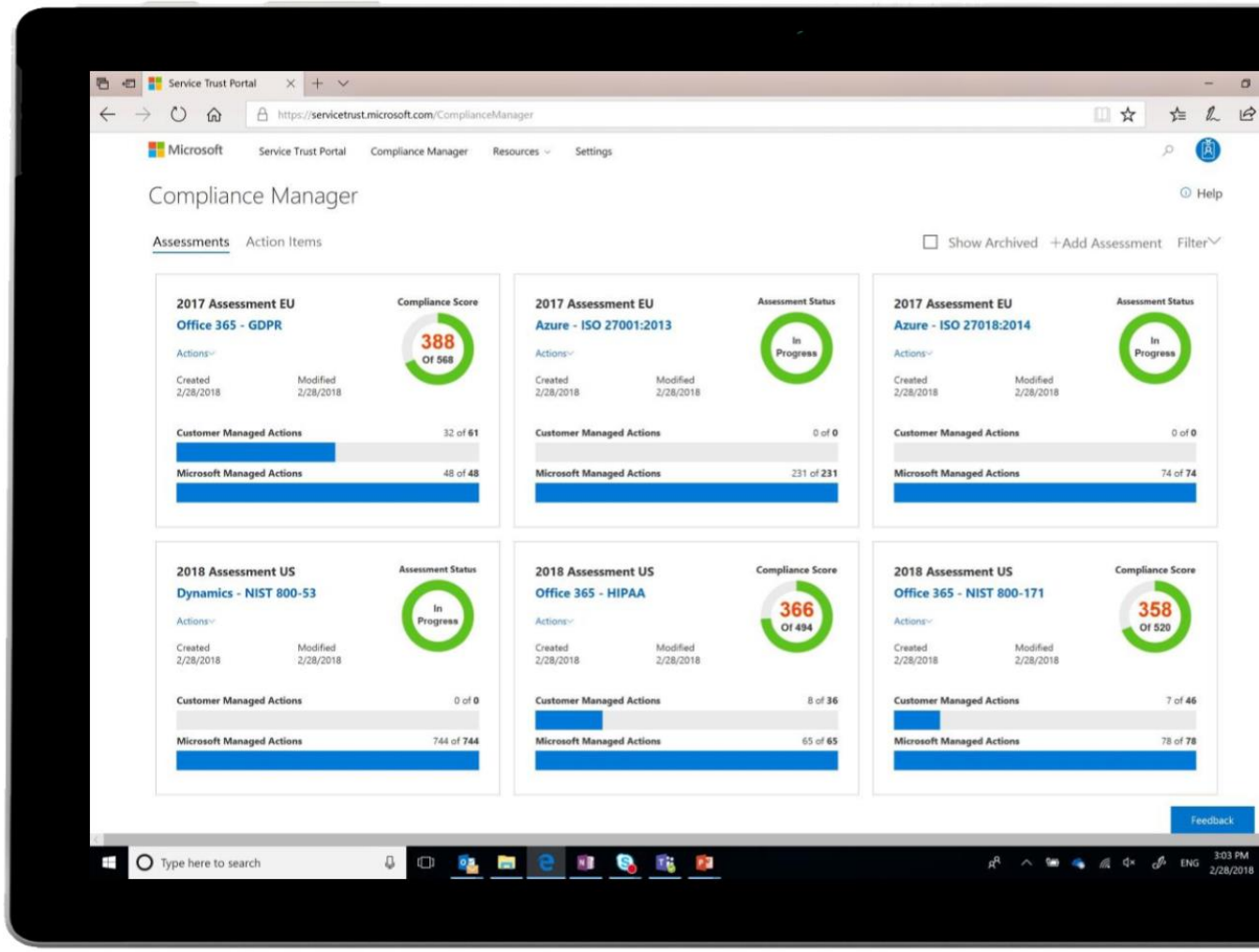


https://servicetrust.microsoft.com/

- In-depth information Access to FedRAMP, ISO, SOC audit reports, data protection white papers, security assessment reports, and more
- Centralized resources around security, compliance, and privacy for all Microsoft Cloud services
- Powerful assessment tools

Compliance Manager

- Manage compliance from a central location
- Proactive risk assessment
- Insights and recommended actions
- Prepare compliance reports for audits



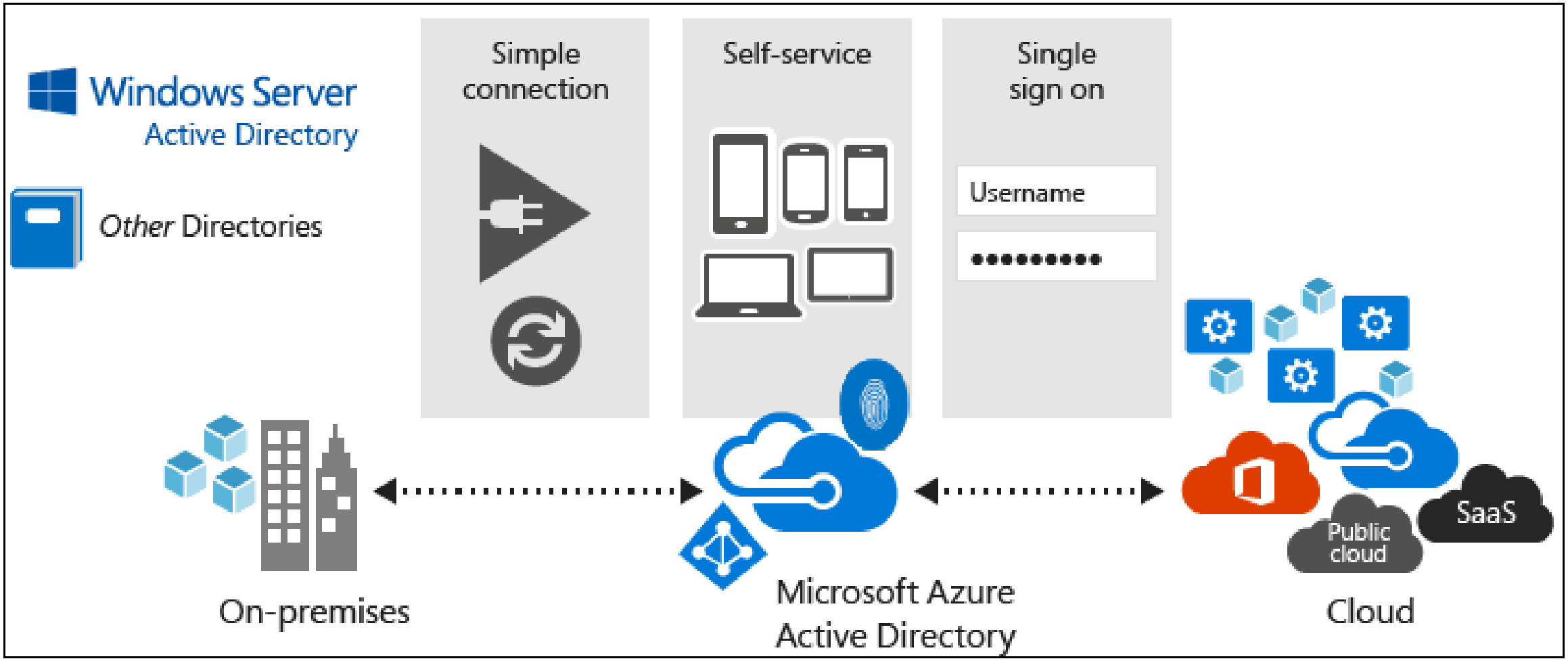
Data Protection Resources

https://servicetrust.microsoft.com/ViewPage/TrustDocuments

Blueprints

https://servicetrust.microsoft.com/ViewPage/BlueprintOverview

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)

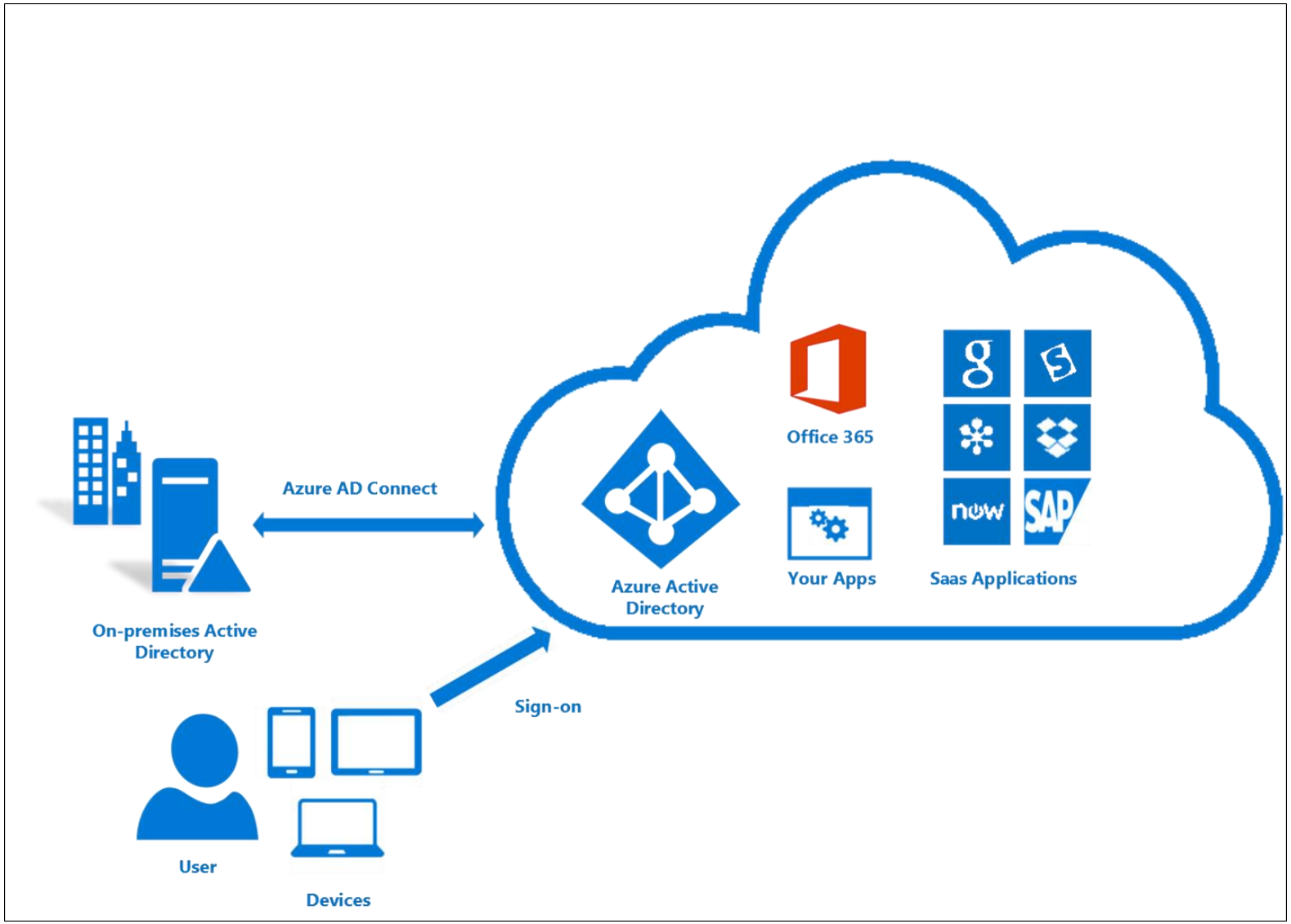
Enhance security with additional factors of authentication.

Self Service

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

AD Connect Overview

AD Connect Overview



AD Connect Components

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.

Authentication Options

Design Authentication

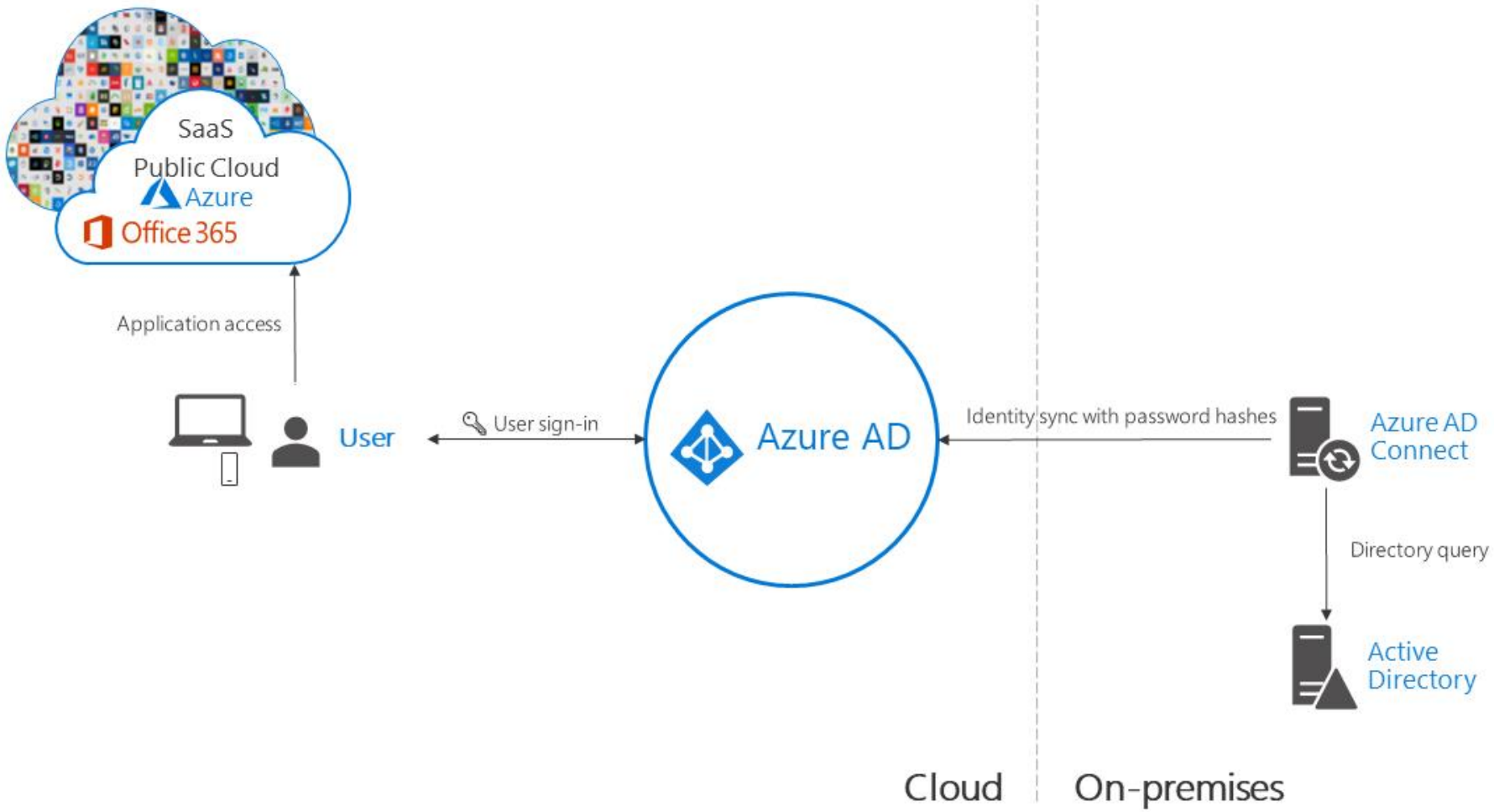
Cloud Authentication

- Cloud-Only
- Password Hash Sync + Seamless SSO
- Pass-Through Authentication + Seamless SSO

Federated Authentication

- AD FS
- 3rd Party Federation Providers

Azure HD Hybrid Identity with Password Hash Sync



Azure HD Hybrid Identity with Password Hash Sync

Effort

- Least effort required
- Part of AD Connect Sync process that runs every 2 minutes.

User Experience

- Deploy seamless SSO eliminating unnecessary prompts after user signs in.

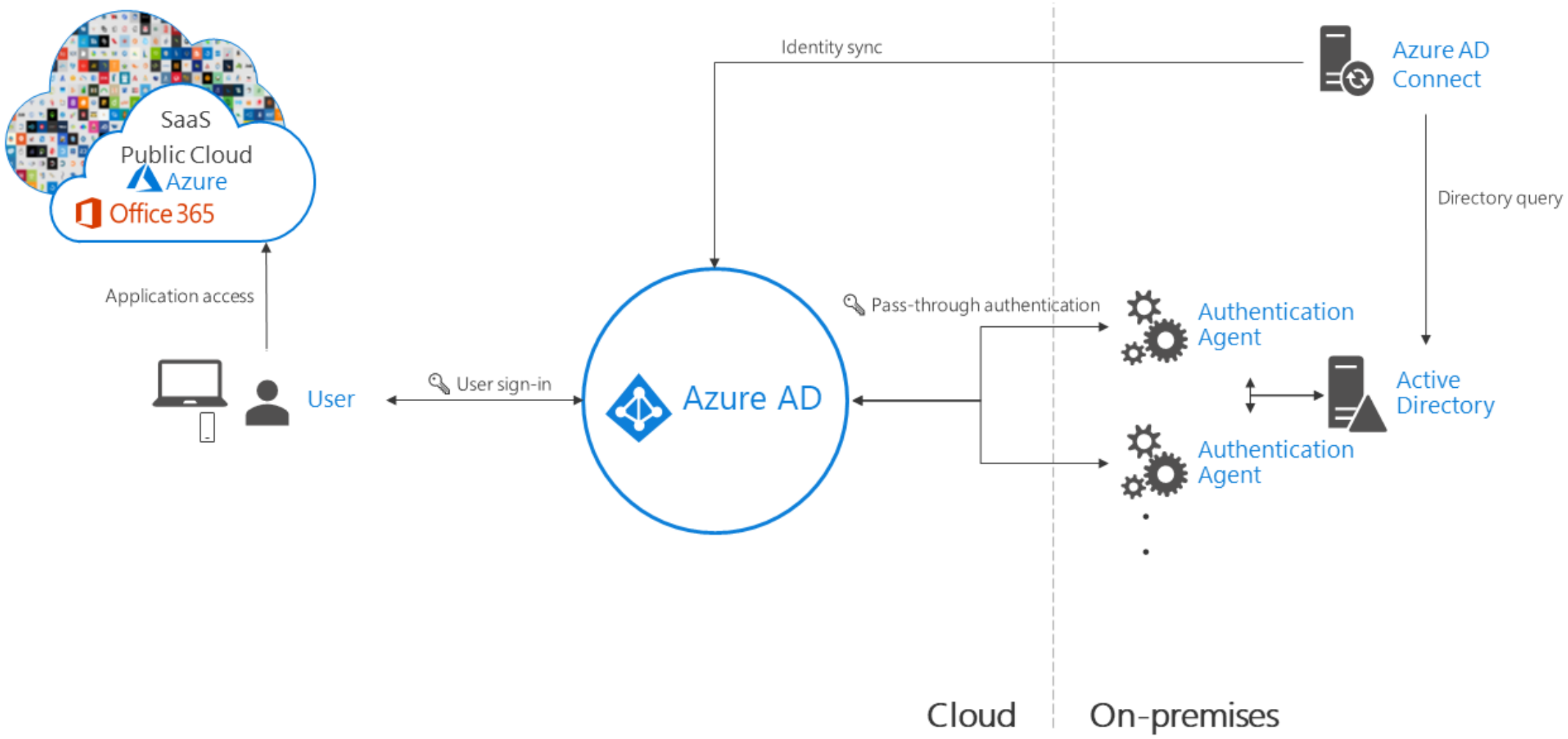
Business Continuity

- Highly available as the cloud service scales with Microsoft datacenters.
- Deploy additional AD Connect server in staging mode in a standby configuration.

Other Considerations

- No immediate enforcement in on-premises account state changes. Consider running an immediate sync after bulk updates.

Azure HD Hybrid Identity with Pass-through authentication



Azure HD Hybrid Identity with Pass-through authentication

Effort

- Need 1 or more (recommend 3) agents installed on existing servers.
- Must have access to on-premises AD controllers.
- Need outbound access to internet

User Experience

- Deploy seamless SSO eliminating unnecessary prompts after user signs in.

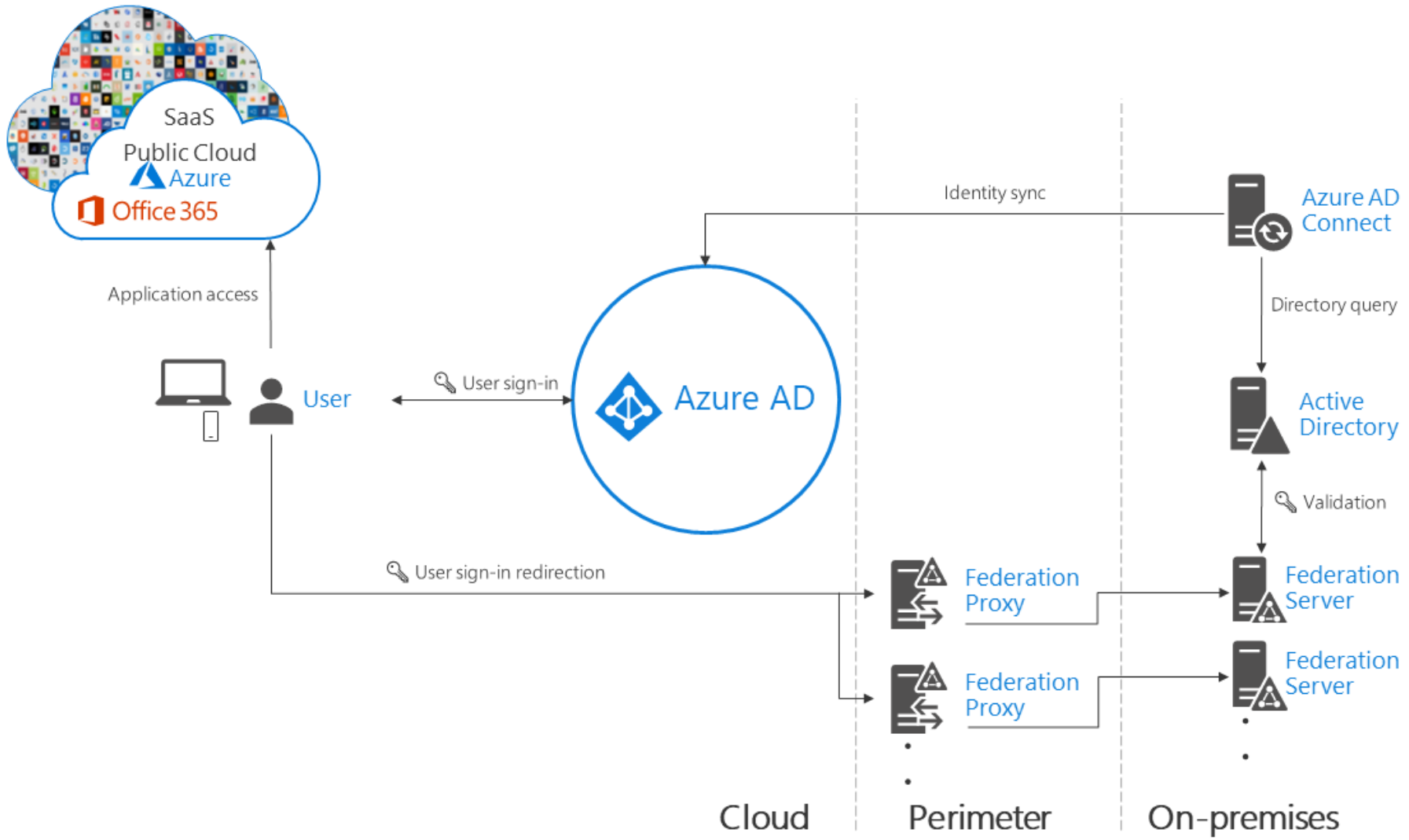
Business Continuity

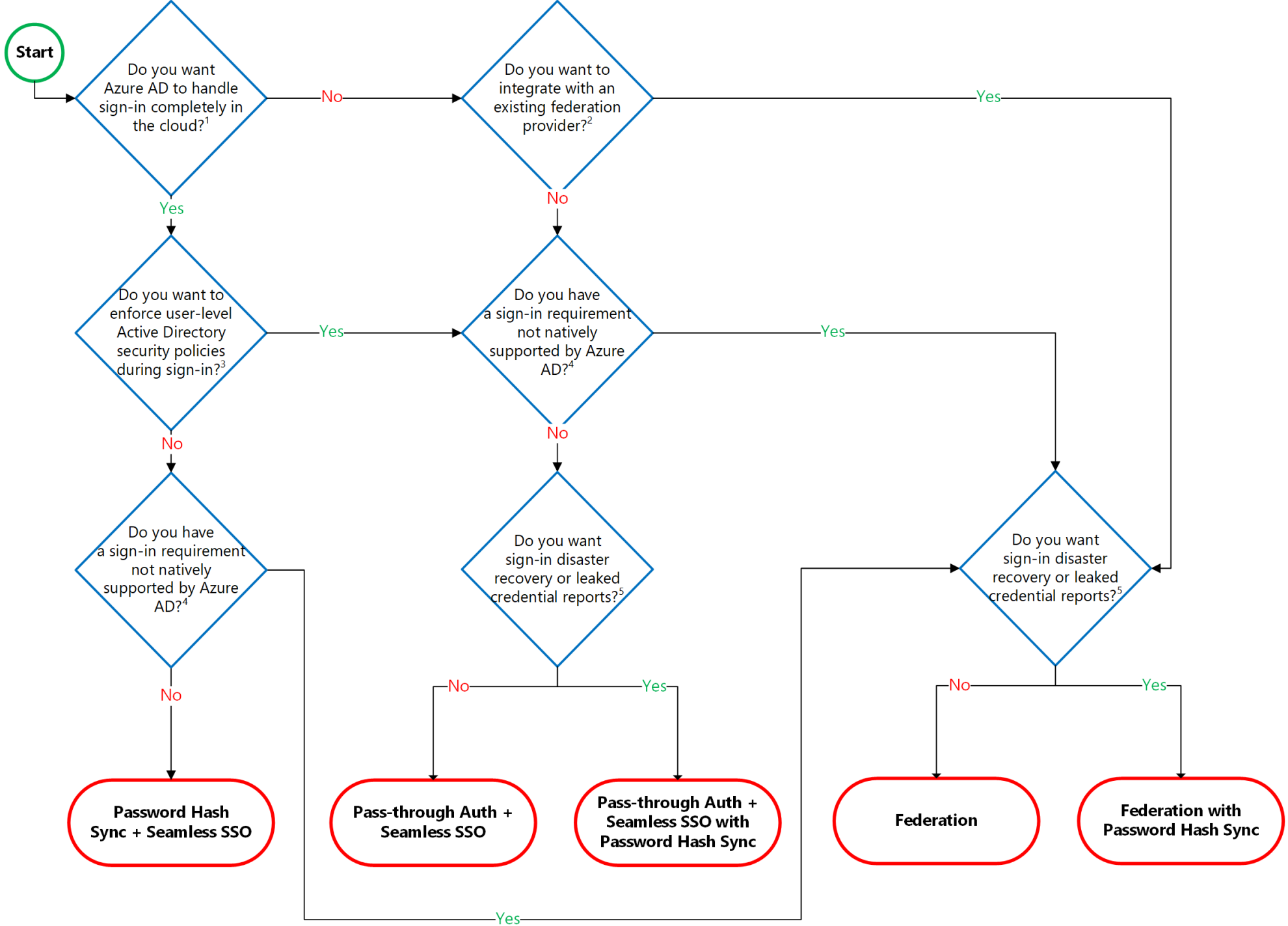
- Recommended to deploy 2 extra pass through agents for redundancy.
- Deploy password hash sync as a backup method.

Other Considerations

- Consider password hash sync as a backup method.
- Remember pass-through auth enforces on the on-premises account policy at the time of sign in.

Azure HD Hybrid Identity with Federated authentication




Start
Do you want Azure AD to handle sign-in completely in the cloud?[1]
No
Do you want to integrate with an existing federation provider?[2]
Yes
Yes
No
Do you want to enforce user-level Active Directory security policies during sign-in?[3]
Yes
Do you have a sign-in requirement not natively supported by Azure AD?[4]
Yes
No
No
Do you have a sign-in requirement not natively supported by Azure AD?[4]
Do you want sign-in disaster recovery or leaked credential reports?[5]
Do you want sign-in disaster recovery or leaked credential reports?[5]
No
Yes
No
Yes
No
Yes
Password Hash Sync + Seamless SSO
Pass-through Auth + Seamless SSO
Pass-through Auth + Seamless SSO with Password Hash Sync
Federation
Federation with Password Hash Sync
Yes

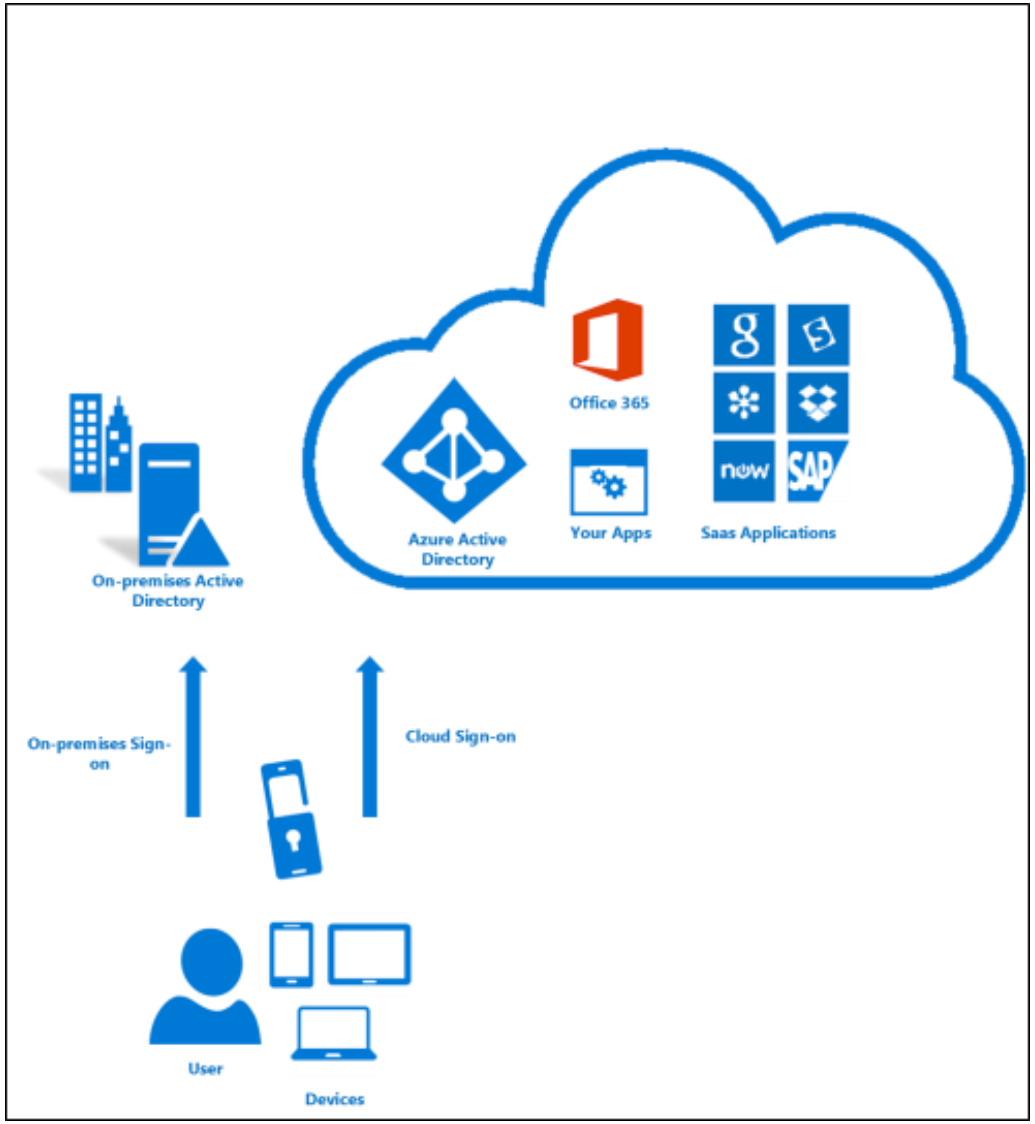
SSO & MFA

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)

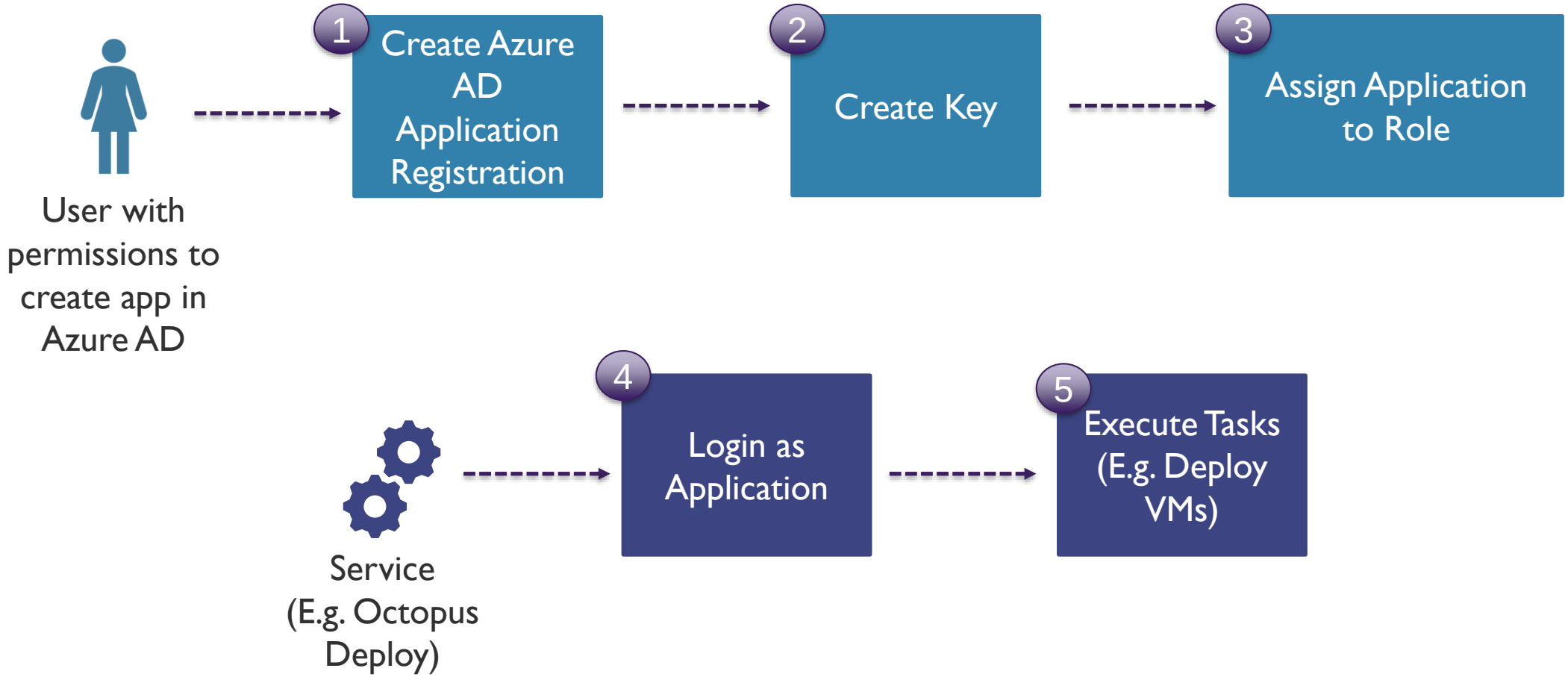
- Works by requiring 2 or more of the following verification methods:
  - Something you know (Password)
  - Something you have (e.g. Cellphone)
  - Something you are (Biometrics)



Multifactor Authentication (MFA)

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.

Service Principal Overview



Identity Protection

SKYLINES
ACADEMY

Azure AD Identity Protection

- Majority of attacks take place when a user account is compromised
- It is essential to protect all identities regardless of access level and prevent compromised identities from being abused
- Identity protection generates reports alerts based on adaptive machine learning algorithms

Identity Protection Capabilities

SKYLINES ACADEMY

Detect vulnerabilities and risky accounts

- Providing custom recommendations to improve overall security posture by highlighting vulnerabilities
- Calculating sign-in risk levels
- Calculating user risk levels

Investigating risk events

- Sending notifications for risk events
- Investigating risk events using relevant and contextual information
- Providing basic workflows to track investigations
- Remediation actions

Risk-based conditional access policies

- Policy to mitigate risky sign-ins
- Policy to block or secure risky user accounts
- Policy to require users to register for multi-factor authentication

Identity Protection Roles

SKYLINES ACADEMY

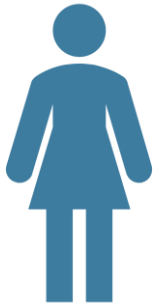
Role	Can do	Cannot do
Global administrator	Full access to Identity Protection, Onboard Identity Protection	
Security administrator	Full access to Identity Protection	Onboard Identity Protection, reset passwords for a user
Security reader	Read-only access to Identity Protection	Onboard Identity Protection, remediate users, configure policies, reset passwords

Privileged Identity Management (PIM)

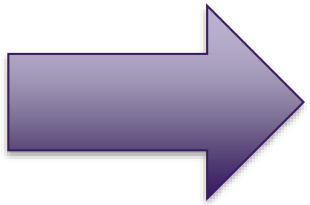
SKYLINES
ACADEMY

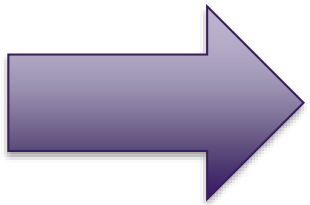
What is Privileged Identity Management (PIM)

Users



Privileged User
(E.g. Subscription Owner,
AAD Global Admin)





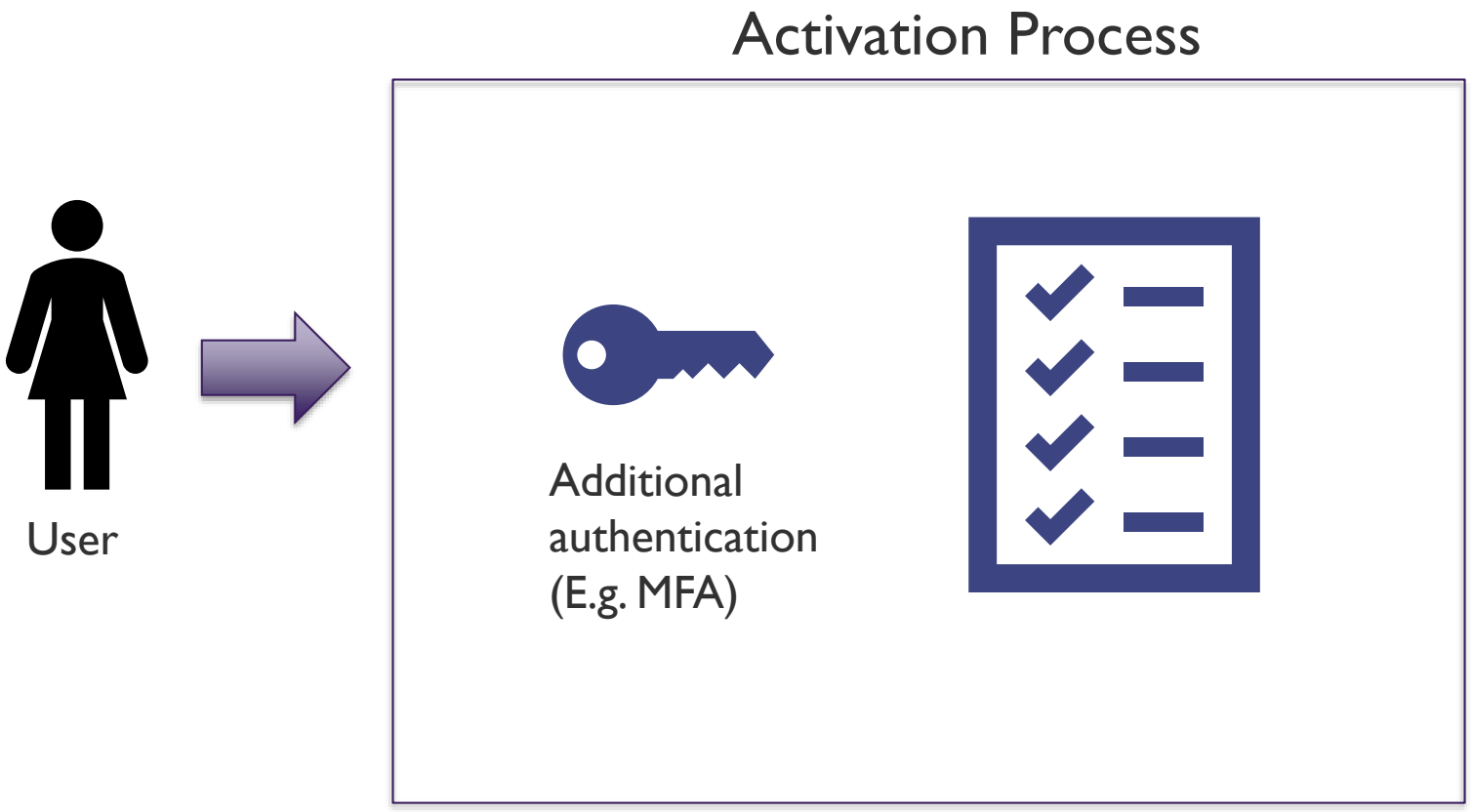
Azure Resources
Azure Active Directory
SaaS Apps
Office 365

Key Features of Azure PIM

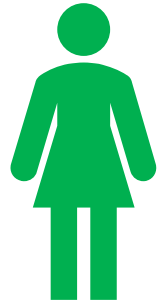
SKYLINES ACADEMY

- Visibility into users with privileged access
  - Azure Resources
  - Azure AD
- Enable on-demand administrative access
- View administrator history
- Setup alerts
- Require approvals (via workflows)

PIM Process



ACTIVATED USER READY TO DO WORK!

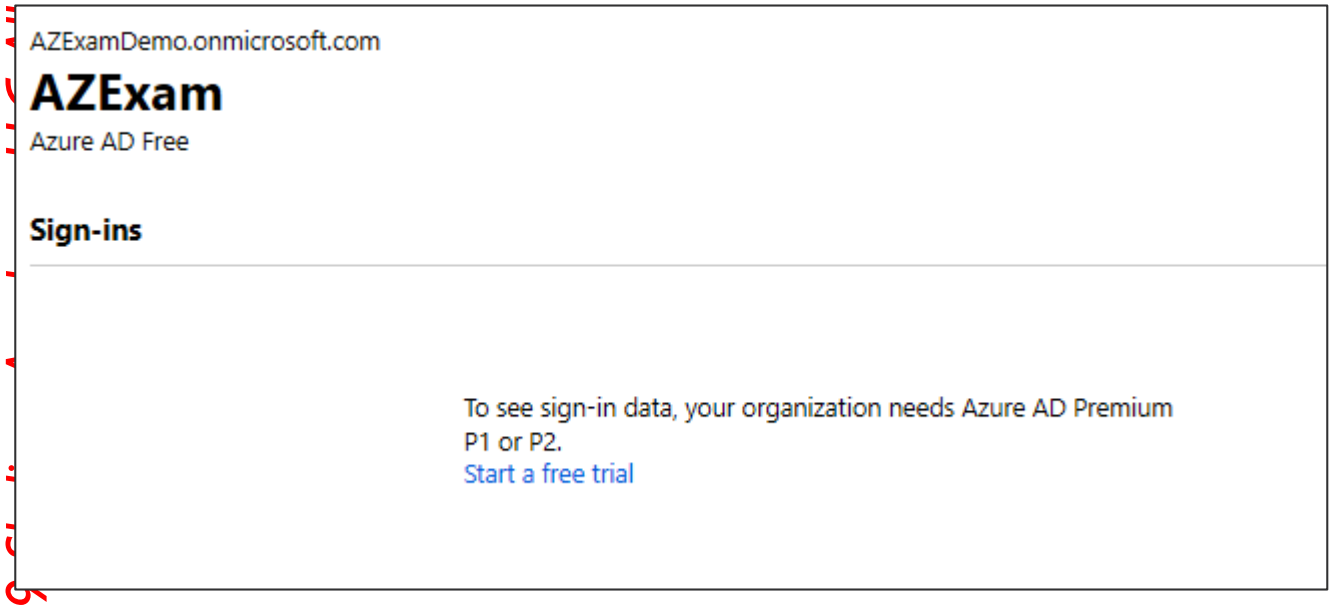


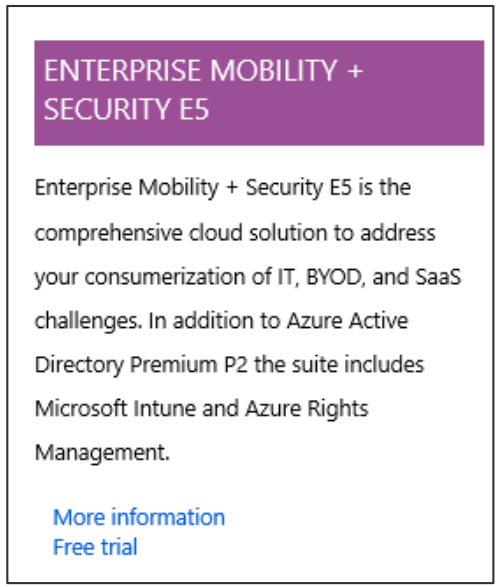
- Azure RBAC
  E.g. Contributor)
- AAD Global Admin

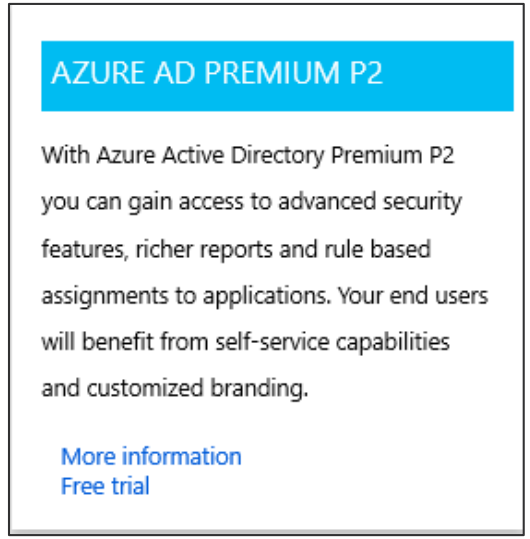
PIM Requirements

SKYLINES ACADEMY

- Azure AD P2 License
  - See: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis







PIM Roles

SKYLINES ACADEMY

Role	Description
Privileged Role Administrator	Can manage role assignments in Azure AD, and all aspects of Privileged Identity Management.
Security Administrator	Can read security information and reports, and manage configuration in Azure AD and Office 365.

- First person to use PIM is assigned the Security Administrator and Privileged Role Administrator roles.
- Only Privileged Role Administrators can manage Azure AD directory role assignment of users.

Assigned Roles (Directory vs Resource)

SKYLINES ACADEMY

Directory Roles

- Azure AD Roles
- E.g. Global Admin etc.
- Roles can be "eligible" or "permanent"

Resource Roles

- Use Azure RBAC
- Built-in or custom roles
- E.g. Subscription Admin etc.

Microsoft Recommended Process

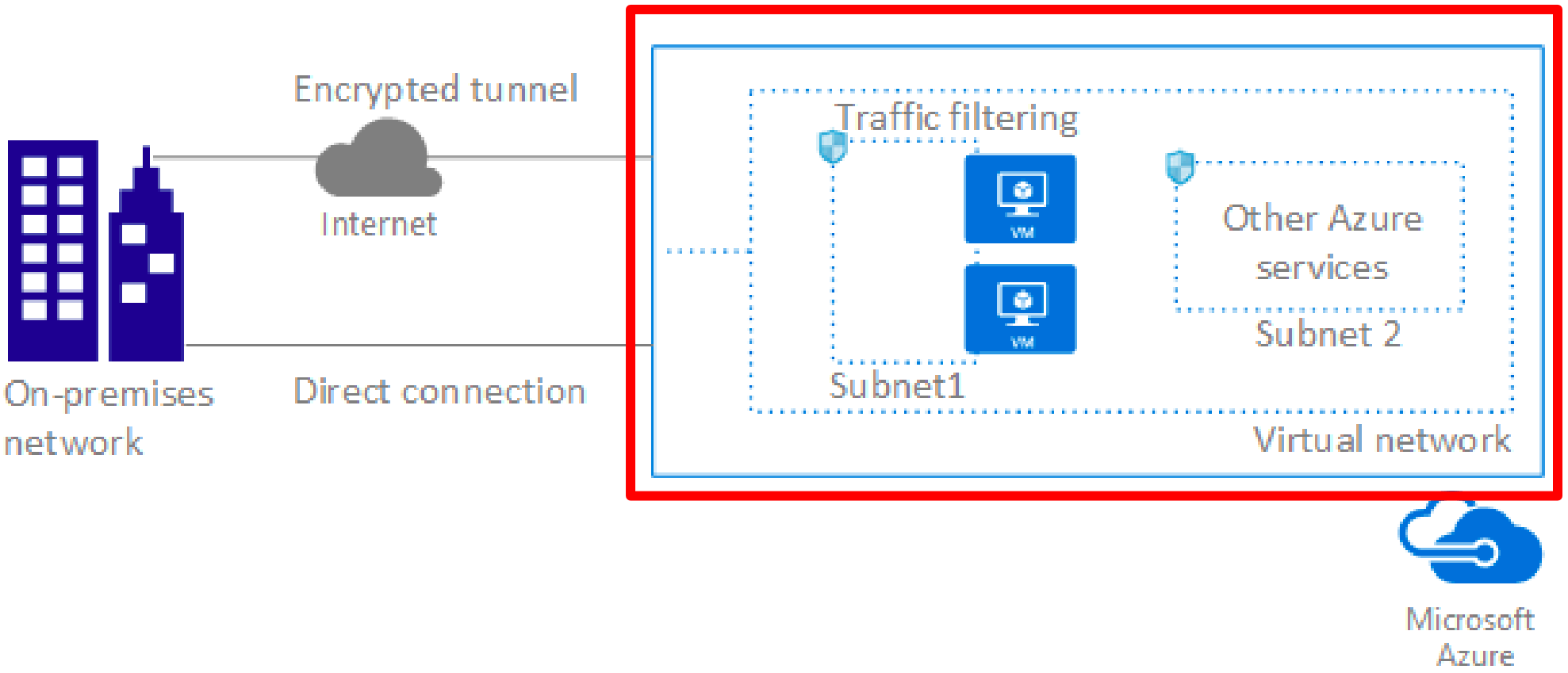
- Stage 1 (24-48 hours): Critical items that we recommend you do right away
- Stage 2 (2-4 weeks): Mitigate the most frequently used attack techniques
- Stage 3 (1-3 months): Build visibility and build full control of admin activity
- Stage 4 (six months and beyond): Continue building defenses to further harden your security platform

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin-roles-secure

Networking Overview

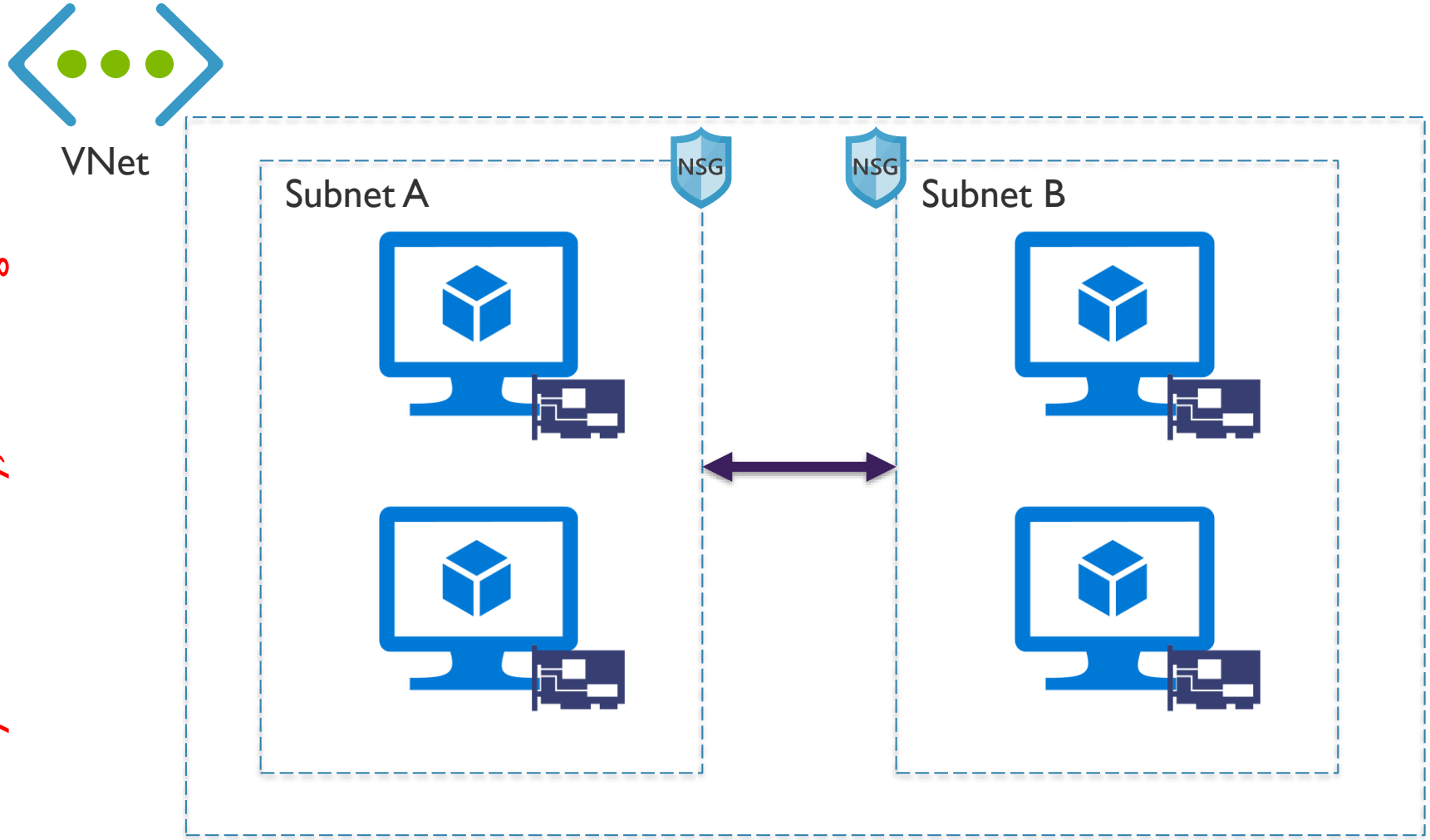
SKYLINES
ACADEMY

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

Network Security Overview

Network Security Overview

SKYLINES ACADEMY

- Network Access Control
- Firewall
- Secure remote access and cross-premises connectivity
- Availability
- Name Resolution
- Global Traffic Routing
- DDoS
- Monitoring and Threat Detection
- Logging and Auditing

Network Access Control

Network Layer Control

Secure deployments through Network Security Groups (NSGs), Azure Security Center (ASC), and Service Endpoints.

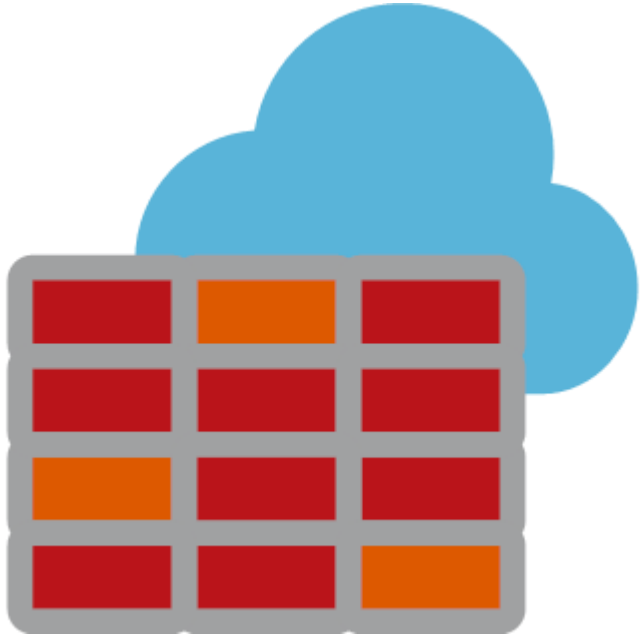
Resource Control and Forced Tunneling

Control routing behavior on VNets with custom behavior and shut down devices initiating connections to the internet via Forced Tunneling.

Virtual Network Security Appliances

Enable security a level higher than the network for extra protection.

Azure Firewall



- What is Azure Firewall?
  - Cloud-based network security service to protect Azure Virtual Network resources
  - Fully stateful firewall service
- Why do I need one?
  - When an NSG just isn't enough…
  - Compliance reasons

Secure Remote and Cross-Premises Connectivity

SKYLINES ACADEMY

Connect individual workstations to a VNET (P2S)	Connect on-premises network to a VNET with a VPN (S2S)	Connect on-premises network to a VNET with a dedicated WAN link	Connect virtual networks to each other
xyz	xyz.	xyz	xyz

Availability

SKYLINES ACADEMY

HTTP Load Balancing (App Gateway)

Network Load Balancing (Azure Load Balancer)

Global Load Balancing (Traffic Manager)

Increase Availability
Increase Performance

Other Network Security Factors

SKYLINES ACADEMY

DNS

Global Traffic Routing (Front Door)

Monitoring and Threat Detection

Logging and Auditing

Network Security Overview

SKYLINES ACADEMY

- Network Access Control
- Firewall
- Secure remote access and cross-premises connectivity
- Availability
- Name Resolution
- Global Traffic Routing
- DDoS
- Monitoring and Threat Detection
- Logging and Auditing

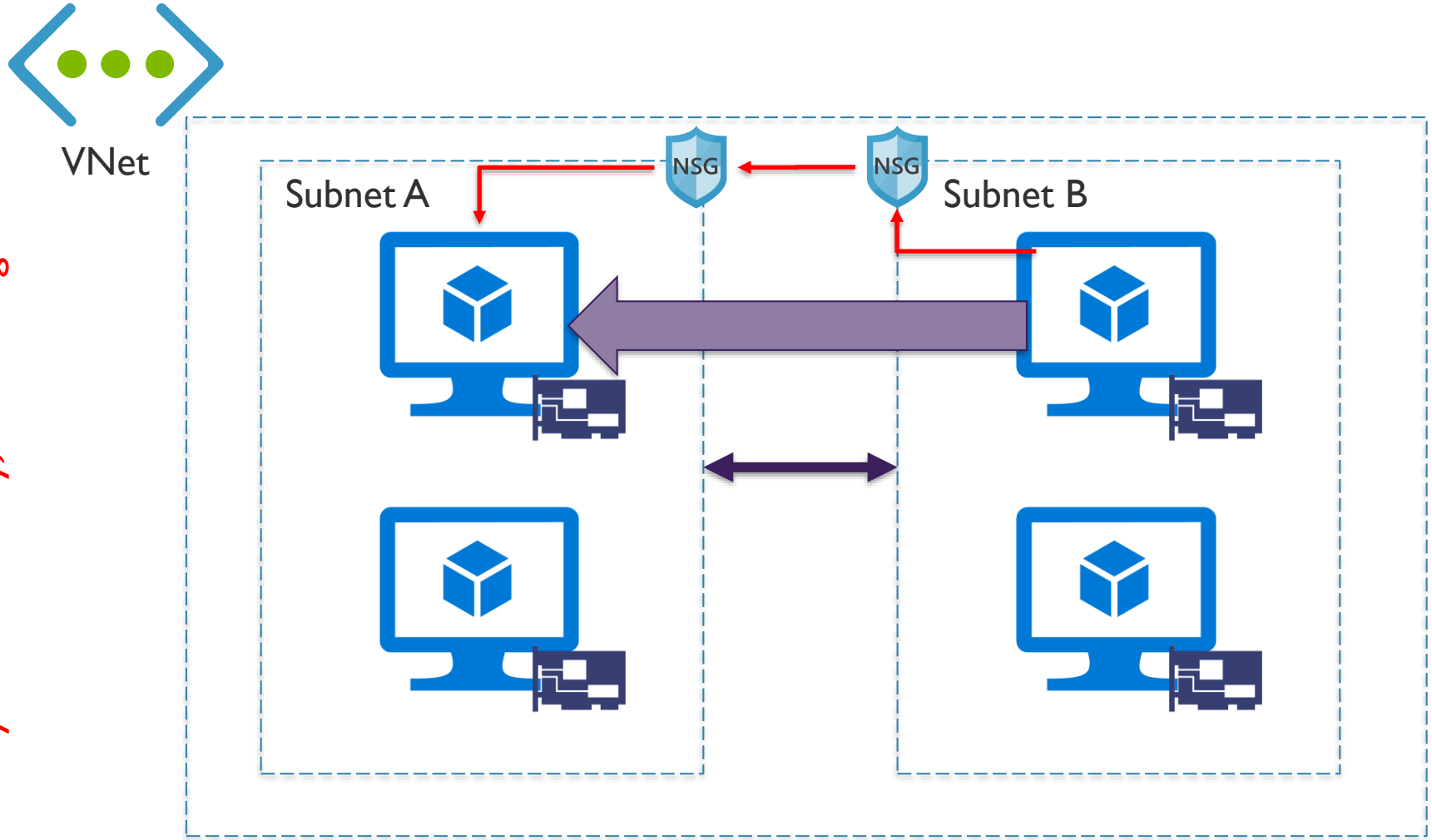
Network Security Groups (NSGs)

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

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:

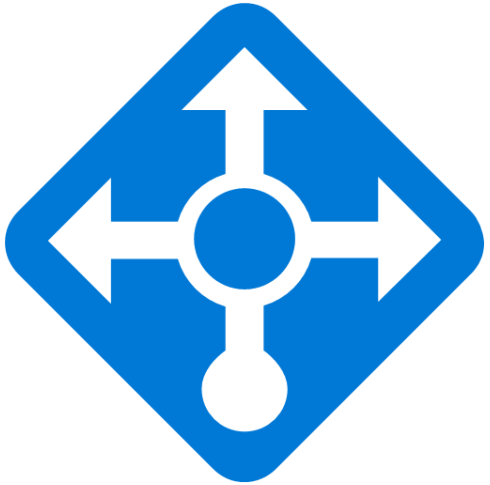
Resource	Default Limit	Maximum Limit
Virtual networks per subscription	50	500
DNS Servers per virtual network	9	25
Virtual machines and role instances per virtual network	2048	2048
Concurrent TCP connections for a virtual machine or role instance	500k	500k
Network Interfaces (NIC)	300	1000
Network Security 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

Azure Load Balancing Services

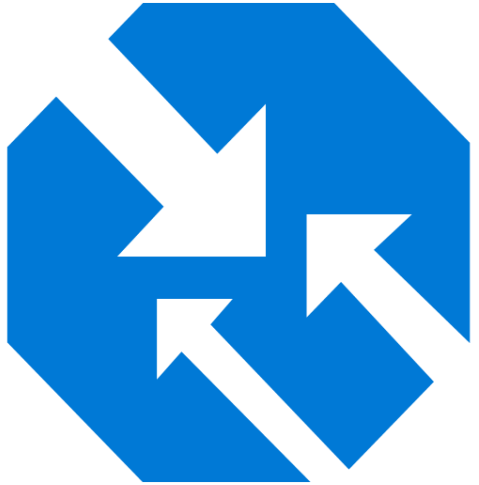
SKYLINES ACADEMY

Load Balancer (Basic and Standard)



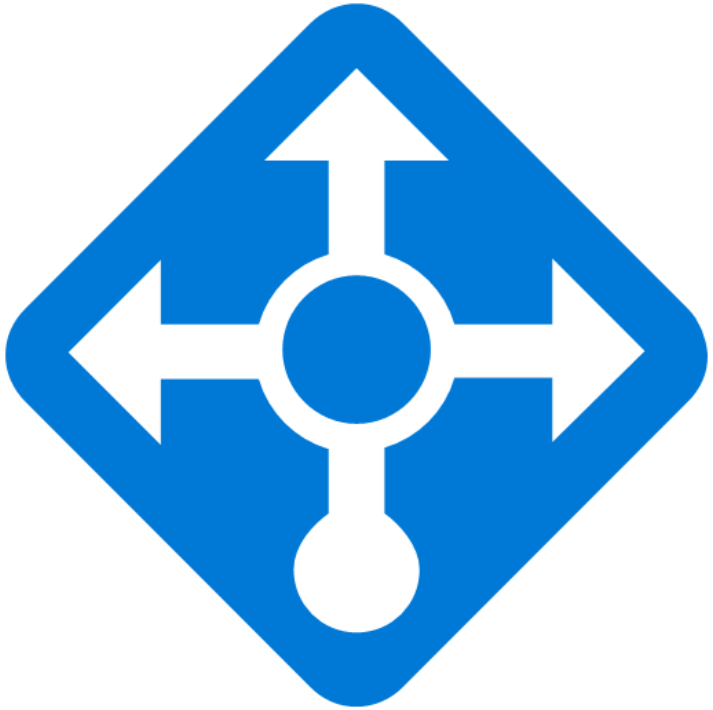
Application Gateway

Traffic Manager



Azure Basic Load Balancer

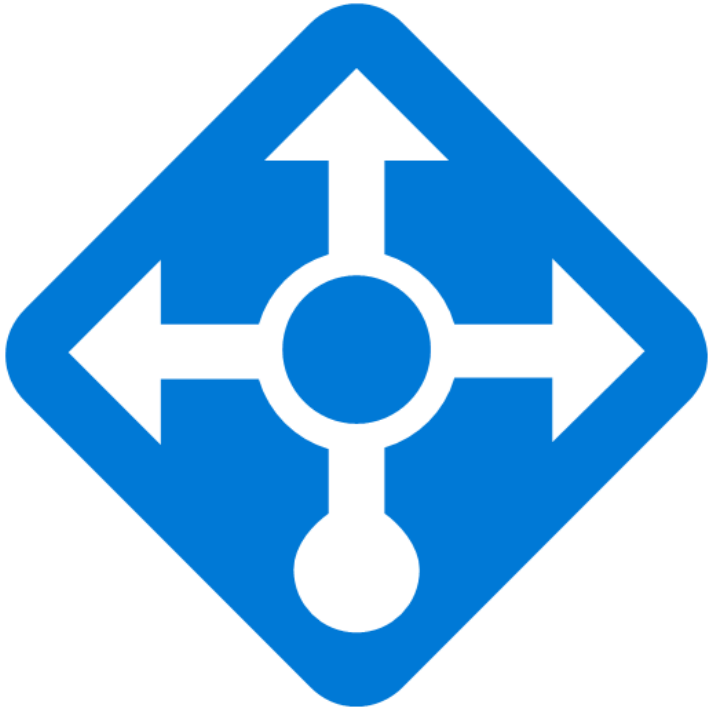
SKYLINES ACADEMY



Key Features:

- Layer 4
- Supports up to 100 instances
- Service monitoring
- Automated reconfiguration
- Hash-based distribution
- Internal and public options

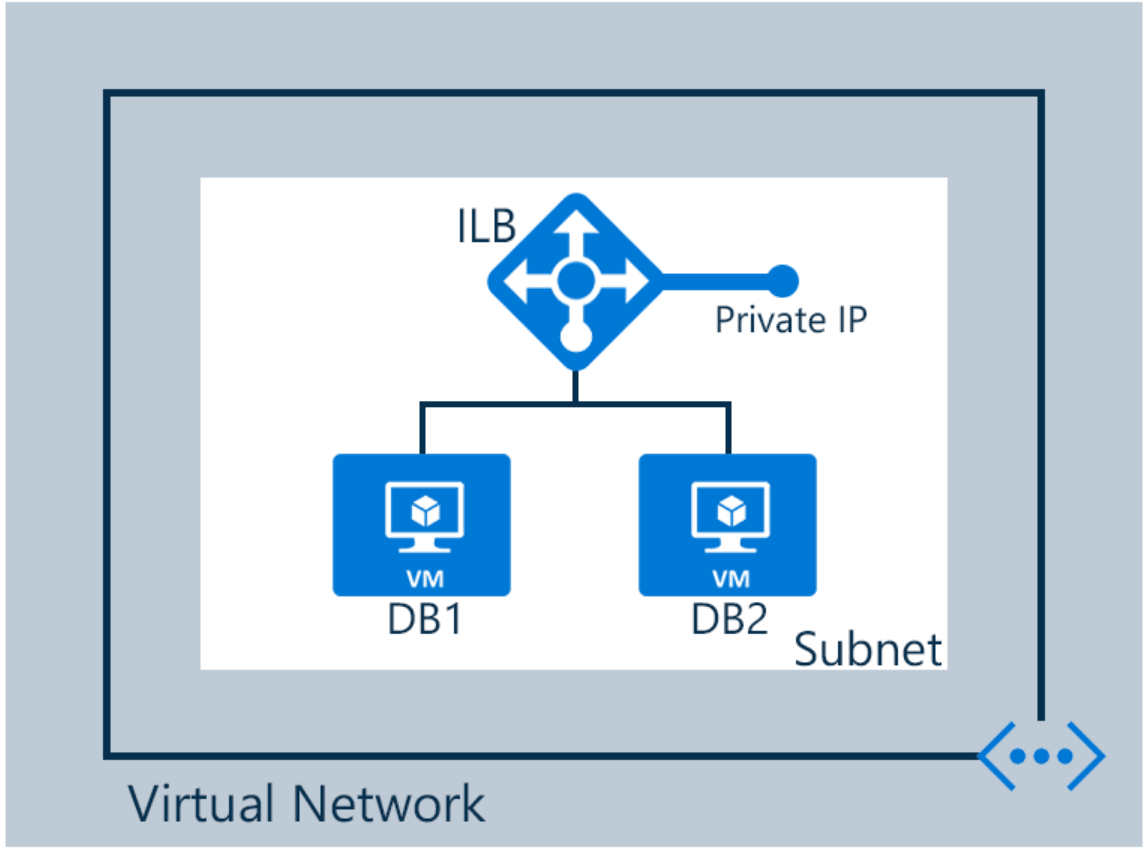
Azure Standard Load Balancer



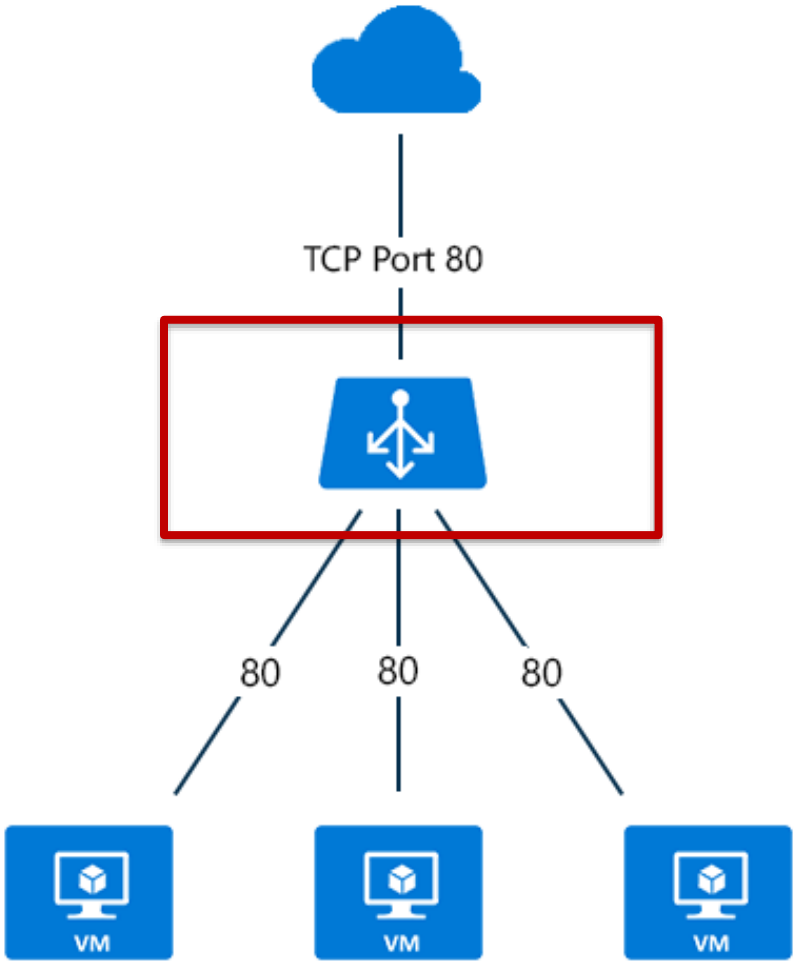
Key Features:

- Layer 4
- Supports up to 1000 instances
- Service monitoring
- Automated reconfiguration
- Hash-based distribution
- Internal and public options

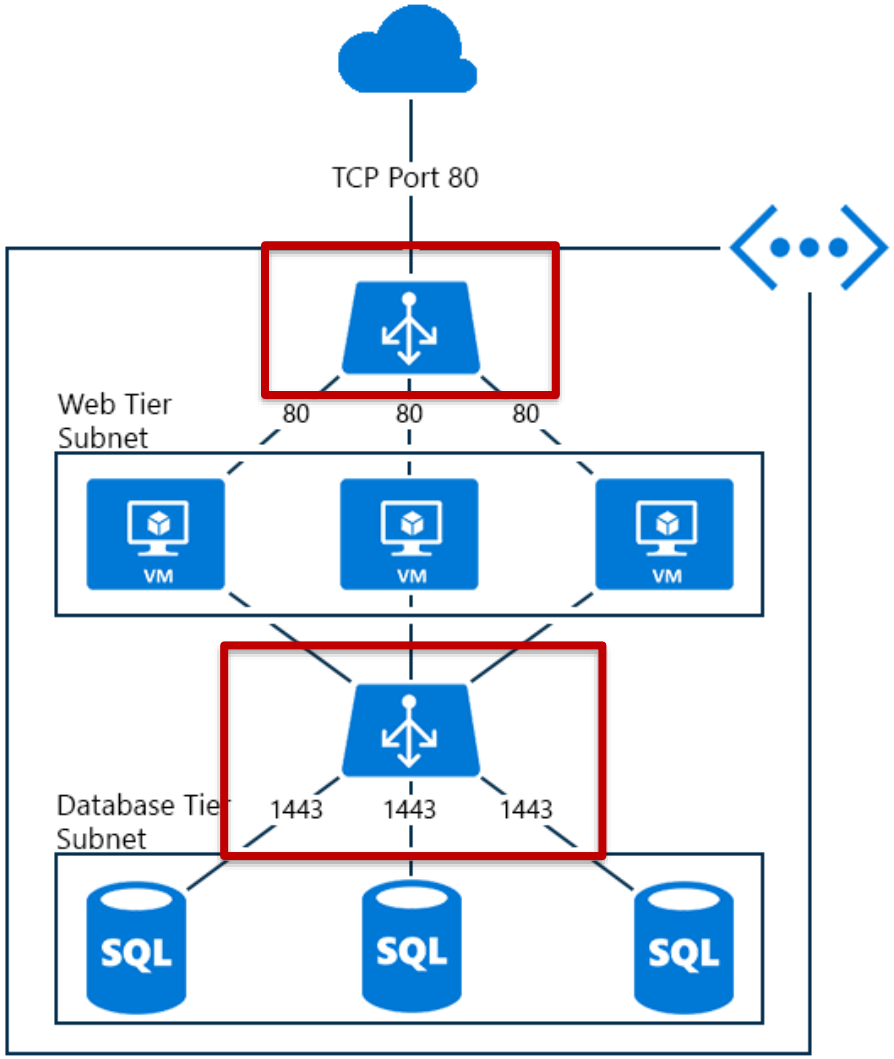
Azure Load Balancer: Internal Example



Azure Load Balancer: Public Example



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

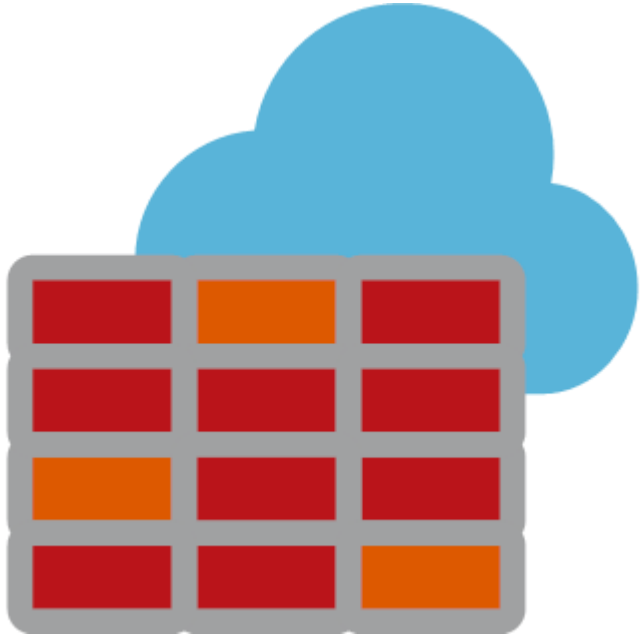
Load Balancer Comparison

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

Azure Firewall

Azure Firewall



- What is Azure Firewall?
  - Cloud-based network security service to protect Azure Virtual Network resources
  - Fully stateful firewall service
- Why do I need one?
  - When an NSG just isn't enough…
  - Compliance reasons

Key Features

SKYLINES ACADEMY

Built-in HA

No need to configure load balancers. HA is managed for you.

Availability Zone Support

Can span availability zones which increases SLA to 99.99%.
Standard SLA 99.95% for single zone

Application FQDN Filtering Rules

You can limit outbound HTTP/S traffic or Azure SQL traffic (preview) to a specified list of fully qualified domain names (FQDN) including wild cards.

Network Traffic Filtering Rules

You can centrally create allow or deny netw ork filtering rules by source and destination IP address, port, and protocol. Azure.

Key Features (cont.)

SKYLINES ACADEMY

FQDN Tags

Allow well known traffic (e.g. Windows Update) through your firewall. You create the App rule and include the Tag.

Service Tags

Microsoft managed groupings of services.

Threat Intelligence

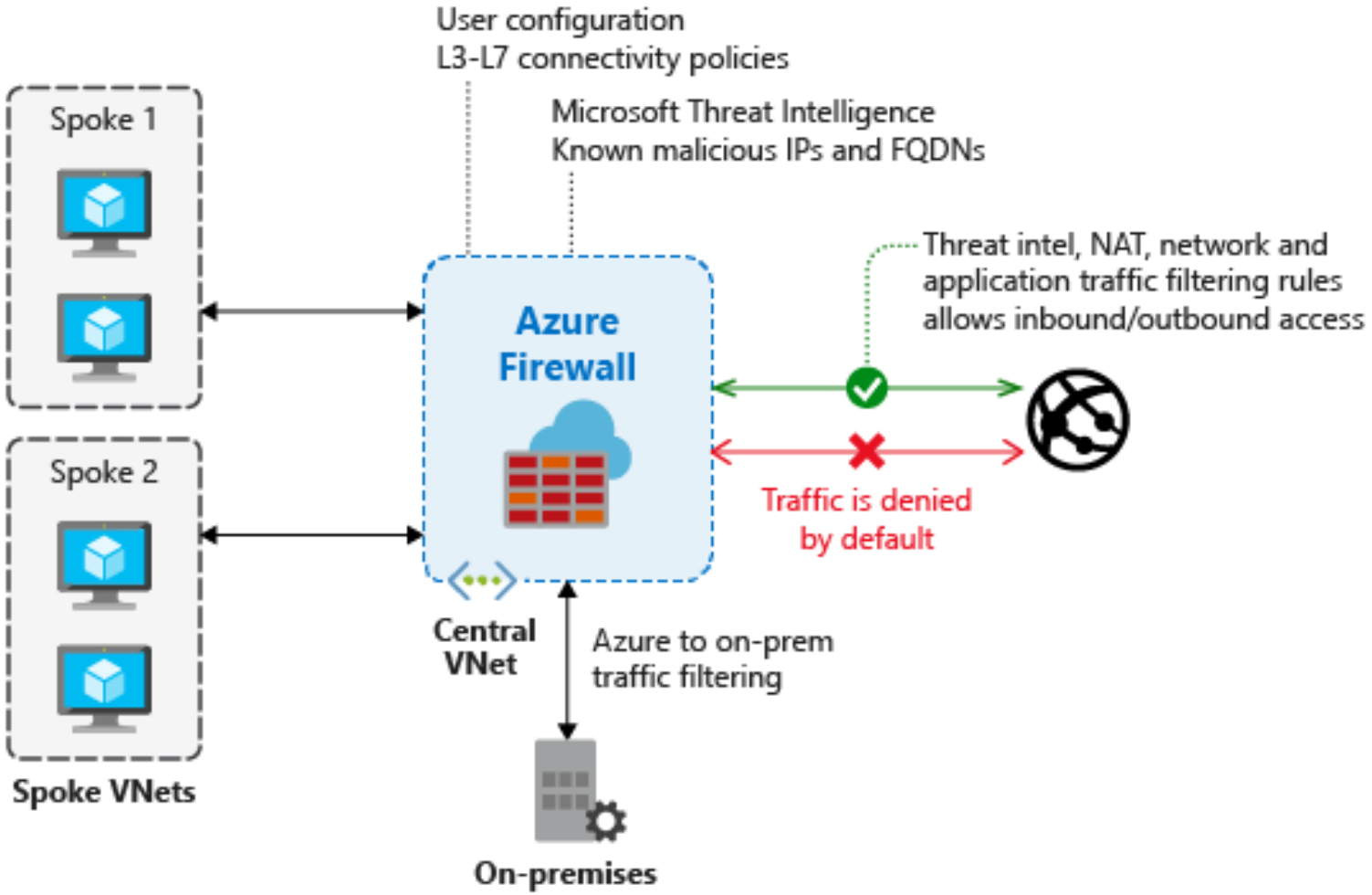
Filter traffic based on Microsoft Threat intelligence feed.

SNAT/DNAT Support

Outbound SNAT Support.

Inbound DNAT support.

Architecture Example



DDoS

Configure Azure DDoS Protection

SKYLINES ACADEMY

- The goal of a DoS attack is to prevent access to services or systems
- Botnets are collections of internet-connected systems that an individual controls and uses without their owners' knowledge
- A Distributed DoS (DDoS) is a collection of attack types aimed at disrupting the availability of a target
- DDoS involves many systems sending traffic to targets as part of a botnet

Configure Azure DDoS Protection (cont.)

- Azure DDoS Protection, combined with application design best practices, provides defense against DDoS attacks
- DDoS Protection provides the following service tiers:
  - Basic: Automatically enabled as part of the Azure platform
  - Standard: Provides additional mitigation capabilities over the Basic service tier that are tuned specifically to Azure Virtual Network resources
- DDoS Protection Standard can mitigate the following types of attacks:
  - Volumetric attacks
  - Protocol attacks
  - Resource (application) layer attacks

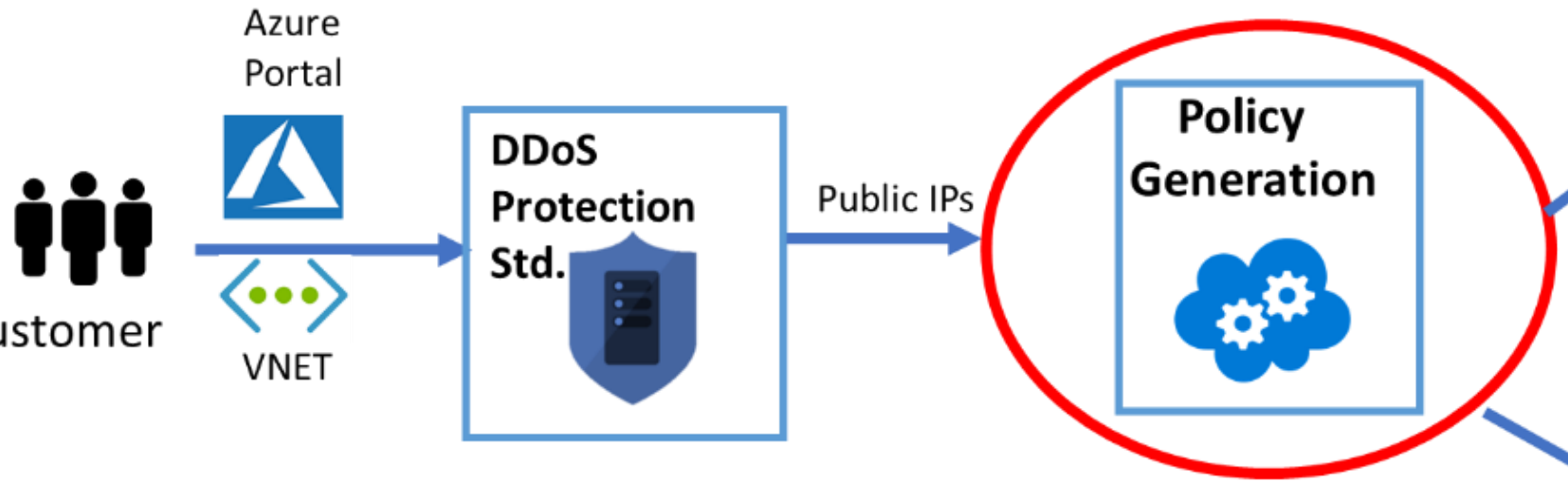
DDOS Standard Features

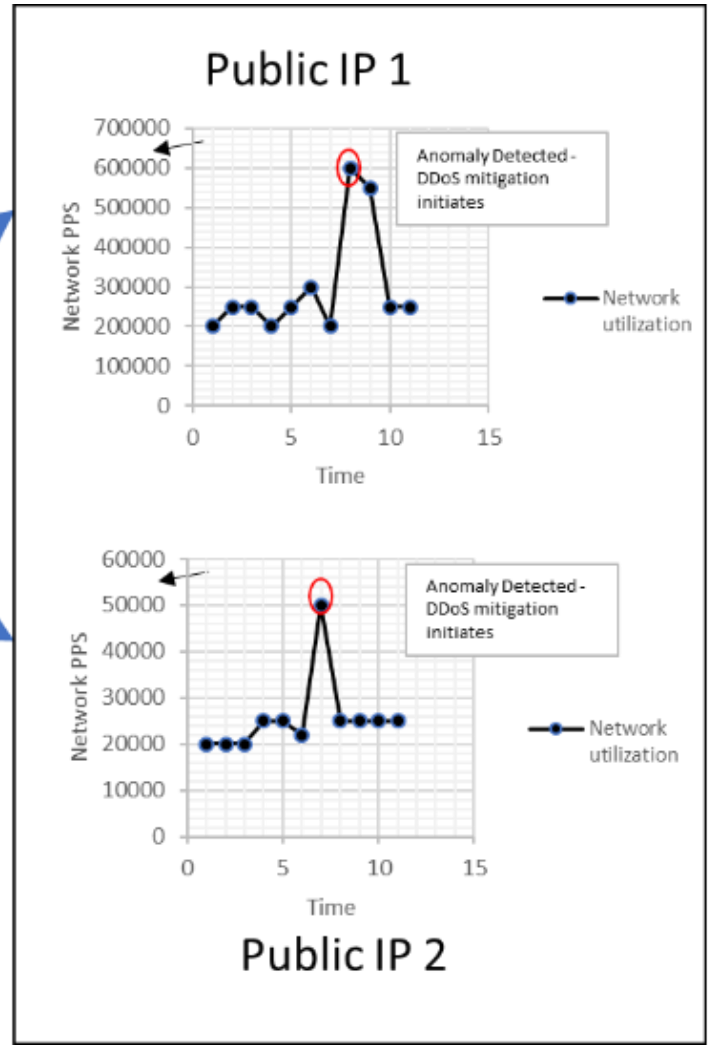
SKYLINES ACADEMY

Feature	Details
Native platform integration	Natively integrated into Azure. Includes configuration through the Azure portal. DDoS Protection Standard understands your resources and resource configuration.
Turn-key protection	Simplified configuration immediately protects all resources on a virtual network as soon as DDoS Protection Standard is enabled. No intervention or user definition is required. DDoS Protection Standard instantly and automatically mitigates the attack, once it is detected.
Always-on traffic monitoring	Your application traffic patterns are monitored 24 hour a day, 7 days a week, looking for indicators of DDoS attacks. Mitigation is performed when protection policies are exceeded.
Attack Mitigation Reports	Attack Mitigation Reports use aggregated network flow data to provide detailed information about attacks targeted at your resources.
Attack Mitigation Flow Logs	Attack Mitigation Flow Logs allow you to review the dropped traffic, forwarded traffic and other attack data in near real-time during an active DDoS attack.
Adaptive tuning	Intelligent traffic profiling learns your application's traffic over time and selects and updates the profile that is the most suitable for your service. The profile adjusts as traffic changes over time. Layer 3 to layer 7 protection: Provides full stack DDoS protection, when used with a web application firewall.
Extensive mitigation scale	Over 60 different attack types can be mitigated, with global capacity, to protect against the largest known DDoS attacks.
Attack metrics	Summarized metrics from each attack are accessible through Azure Monitor.
Attack alerting	Alerts can be configured at the start and stop of an attack, and over the attack's duration, using built-in attack metrics. Alerts integrate into your operational software like Microsoft Azure Monitor logs, Splunk, Azure Storage, Email, and the Azure portal.
Cost guarantee	Data-transfer and application scale-out service credits for documented DDoS attacks.
DDoS Rapid responsive	DDoS Protection Standard customers now have access to Rapid Response team during an active attack. DRR can help with attack investigation, custom mitigations during an attack and post-attack analysis.

DDOS Standard Mitigation

SKYLINES ACADEMY

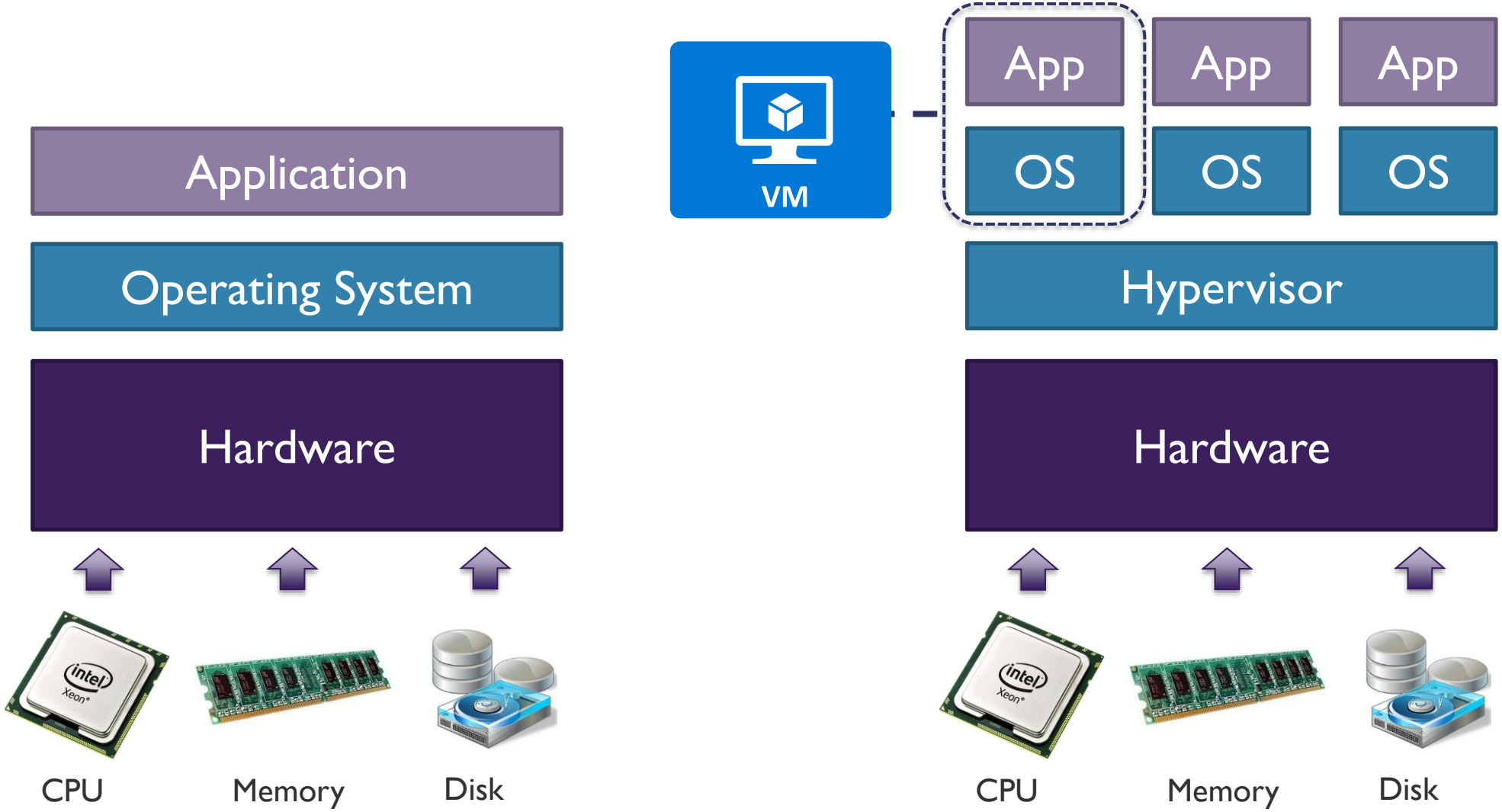




Azure Virtual Machines

SKYLINES
ACADEMY

Introduction to Virtual Machines



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/

Azure Disk Encryption

Azure Disk Encryption

Key Features:

- Protect and safeguards your data by encrypting the OS volumes and data disks attached to your VM
- Uses Bit-Locker for Windows and DM-Crpyt for Linux
- Integrates with KeyVault for customer management of encryption keys

Azure Disk Encryption Scenarios

SKYLINES ACADEMY

Enabling and disabling on encryption…

- ✓ on new VMs created from the supported Azure Gallery images
- ✓ on existing VMs that run in Azure
- ✓ on new Windows VMs created from pre-encrypted VHD and encryption keys
- ✓ on Windows virtual machine scale sets
- ✓ on data drives for Linux virtual machine scale sets
- ✓ of managed disk VMs

Azure Disk Encryption Scenarios (continued)

SKYLINES ACADEMY

- ✓ Updating encryption settings of an existing encrypted Premium and non-Premium Storage VM
- ✓ Backing up and restoring encrypted VMs
- ✓ Bring your own encryption (BYOE) and bring your own key (BYOK) scenarios, in which the customers use their own encryption keys and store them in an Azure Key Vault

Non-supported Scenarios

SKYLINES ACADEMY

- × Encrypting basic tier VM or VMs created through the classic VM creation method.
- × Disabling encryption on an OS drive or data drive of a Linux VM when the OS drive is encrypted.
- × Encrypting OS drive for Linux virtual machine scale sets.
- × Encrypting Windows VMs configured with software-based RAID systems.
- × Encrypting custom images on Linux VMs.
- × Integration with an on-premises key management system.
- × Azure Files (shared file system).
- × Network File System (NFS).
- × Dynamic volumes.
- × Ephemeral OS disks.

Disk Encryption Pre-Requisites

SKYLINES ACADEMY

Supported VM Sizes	Supported OS	Networking	Key Vault
Not Available on A-Series Check Minimum Memory Requirements	Windows 8 and Later Windows Server 2008 R2 and Later See Linux Table	Connectivity to Azure AD Connect to KeyVault Azure Storage	Enable for Encryption Enable for Deployment (if required) Enable for template Deployment (if required)

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisite

Configuration Methods

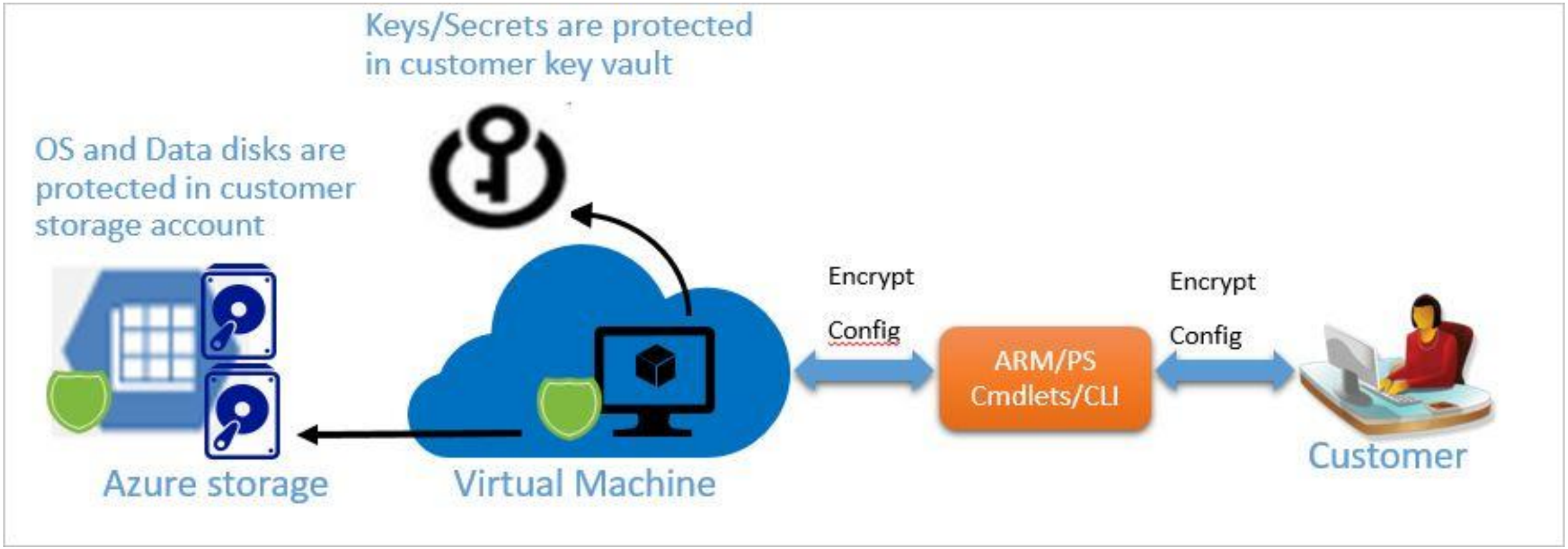
SKYLINES ACADEMY

PowerShell

Azure CLI

ARM Templates

Azure Disk Encryption Elements



https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

VM Security Best Practices

SKYLINES
ACADEMY

Reference Documentation

SKYLINES ACADEMY

Security best practices for IaaS workloads in Azure

https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

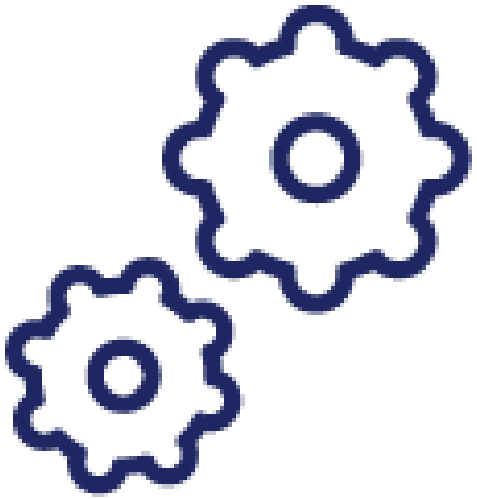
VM Security: Control Access

Best practice: Control VM access.

Detail:

- Use Azure policies to establish conventions for resources in your organization and create customized policies.
- Apply these policies to resources, such as resource groups. VMs that belong to a resource group inherit its policies.

VM Security: ARM Templates



Best practice: Reduce variability in your setup and deployment of VMs.

Detail: Use Azure Resource Manager templates to strengthen your deployment choices and make it easier to understand and inventory the VMs in your environment.

VM Security: Secure Access

Best practice: Secure privileged access.

Detail:

- Use a least privilege approach and built-in Azure roles to enable users to access and set up VMs:
- Virtual Machine Contributor: Can manage VMs, but not the virtual network or storage account to which they are connected.
- Classic Virtual Machine Contributor: Can manage VMs created by using the classic deployment model, but not the virtual network or storage account to which the VMs are connected.
- Security Admin: In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.
- DevTest Labs User: Can view everything and connect, start, restart, and shut down VMs.

VM Security: Availability

Best practice: Deploy VMs with uptime in mind

Detail: Use Availability Sets and Availability Zones to meet SLA requirements.

VM Security: Malware Protection

Best practice: Use Endpoint Protection

Detail: Prevent viruses and other malware by installing Microsoft or 3rd Party Endpoint Protection

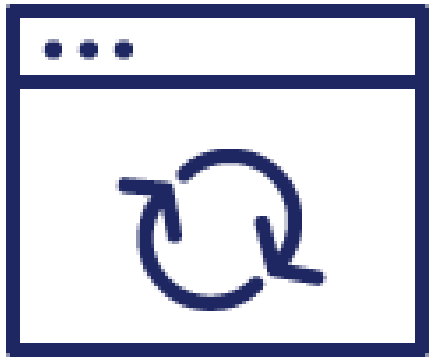
VM Security: System Updates

Best practice: Keep your VMs current.

Detail:

- Use the Update Management solution in Azure Automation to manage operating system updates for your Windows and Linux computers that are deployed in Azure, in on-premises environments, or in other cloud providers.
- You can quickly assess the status of available updates on all agent computers and manage the process of installing required updates for servers.

VM Security: System Updates



Best practice: Ensure at deployment that images you built include the most recent round of Windows updates.

Detail:

- Check for and install all Windows updates as a first step of every deployment.
- This measure is especially important to apply when you deploy images that come from either you or your own library.
- Although images from the Azure Marketplace are updated automatically by default, there can be a lag time (up to a few weeks) after a public release.

VM Security: Backup

Best practice: Deploy and test a backup solution.

Detail: A backup needs to be handled the same way that you handle any other operation. This is true of systems that are part of your production environment extending to the cloud.

VM Security: Monitor your Security Posture

Best practice: Monitor your VM Security Posture

Details:

- Apply OS security settings with recommended configuration rules.
- Identify and download system security and critical updates that might be missing.
- Deploy recommendations for endpoint antimalware protection.
- Validate disk encryption.
- Assess and remediate vulnerabilities.
- Detect threats.

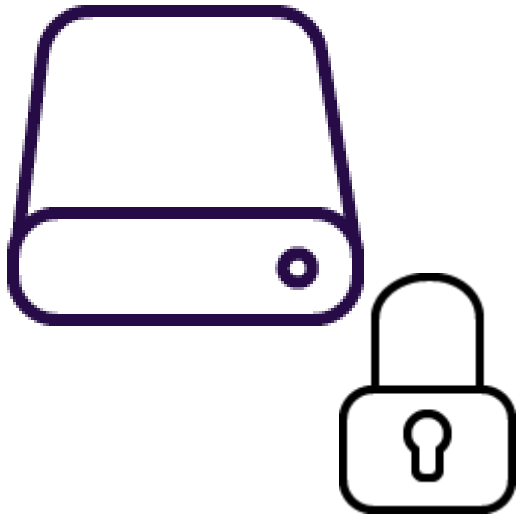
VM Security: Monitor Performance

Best practice: Monitor your VM performance

Details:

- Create alerts and enforce logging for your Virtual Machines.
- Routinely exam VMs that have activity which is not "normal."

VM Security: Disk Encryption

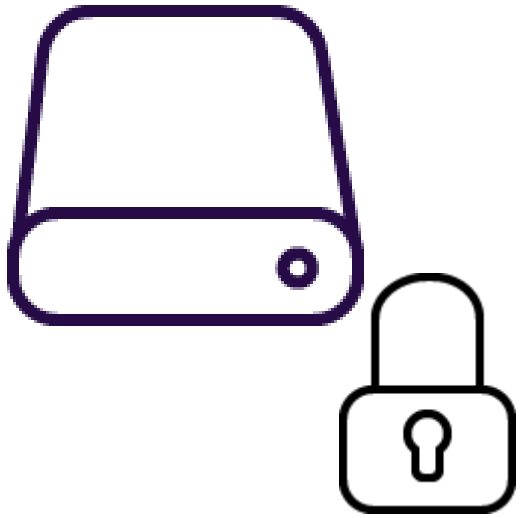


Best practice: Enable encryption on VMs.

Detail:

- Azure Disk Encryption generates and writes the encryption keys to your key vault. Managing encryption keys in your key vault requires Azure AD authentication.
- Create an Azure AD application for this purpose. For authentication purposes, you can use either client secret-based authentication or client certificate-based Azure AD authentication.

VM Security: Disk Encryption

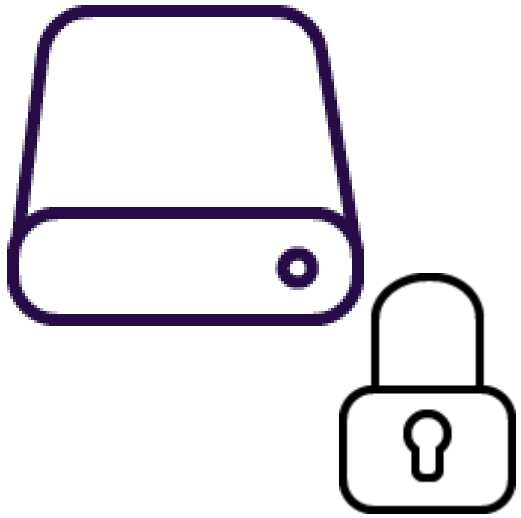


Best practice: Use a key encryption key (KEK) for an additional layer of security for encryption keys. Add a KEK to your key vault.

Detail:

- Use the Add-AzKeyVaultKey cmdlet to create a key encryption key in the key vault.
- You can also import a KEK from your on-premises hardware security module (HSM) for key management. For more information, see the Key Vault documentation.
- When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to Key Vault. Keeping an escrow copy of this key in an on-premises key management HSM offers additional protection against accidental deletion of keys.

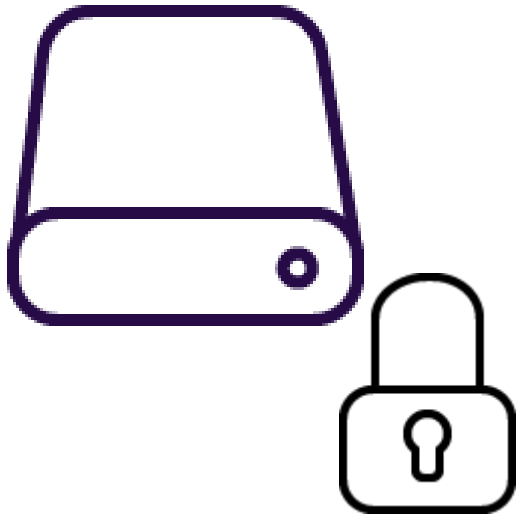
VM Security: Disk Encryption



Best practice: Take a snapshot and/or backup before disks are encrypted. Backups provide a recovery option if an unexpected failure happens during encryption.

Detail: VMs with managed disks require a backup before encryption occurs. After a backup is made, you can use the **Set-AzVMDiskEncryptionExtension** cmdlet to encrypt managed disks by specifying the *-skipVmBackup* parameter. For more information about how to back up and restore encrypted VMs, see the Azure Backup article.

VM Security: Disk Encryption



Best practice: To make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the key vault and the VMs to be located in the same region.

Detail: Create and use a key vault that is in the same region as the VM to be encrypted.

VM Security: Network Connectivity

Best practice: Prevent inadvertent exposure to network routing and security.

Detail: Use RBAC to ensure that only the central networking group has permission to networking resources.

.

VM Security: Network Connectivity

Best practice: Identify and remediate exposed VMs that allow access from "any" source IP address.

Detail:

- Use Azure Security Center.
- Security Center will recommend that you restrict access through internet-facing endpoints if any of your network security groups has one or more inbound rules that allow access from "any" source IP address.
- Security Center will recommend that you edit these inbound rules to restrict access to source IP addresses that actually need access.

VM Security: Network Connectivity

Best practice: Restrict management ports (RDP, SSH).

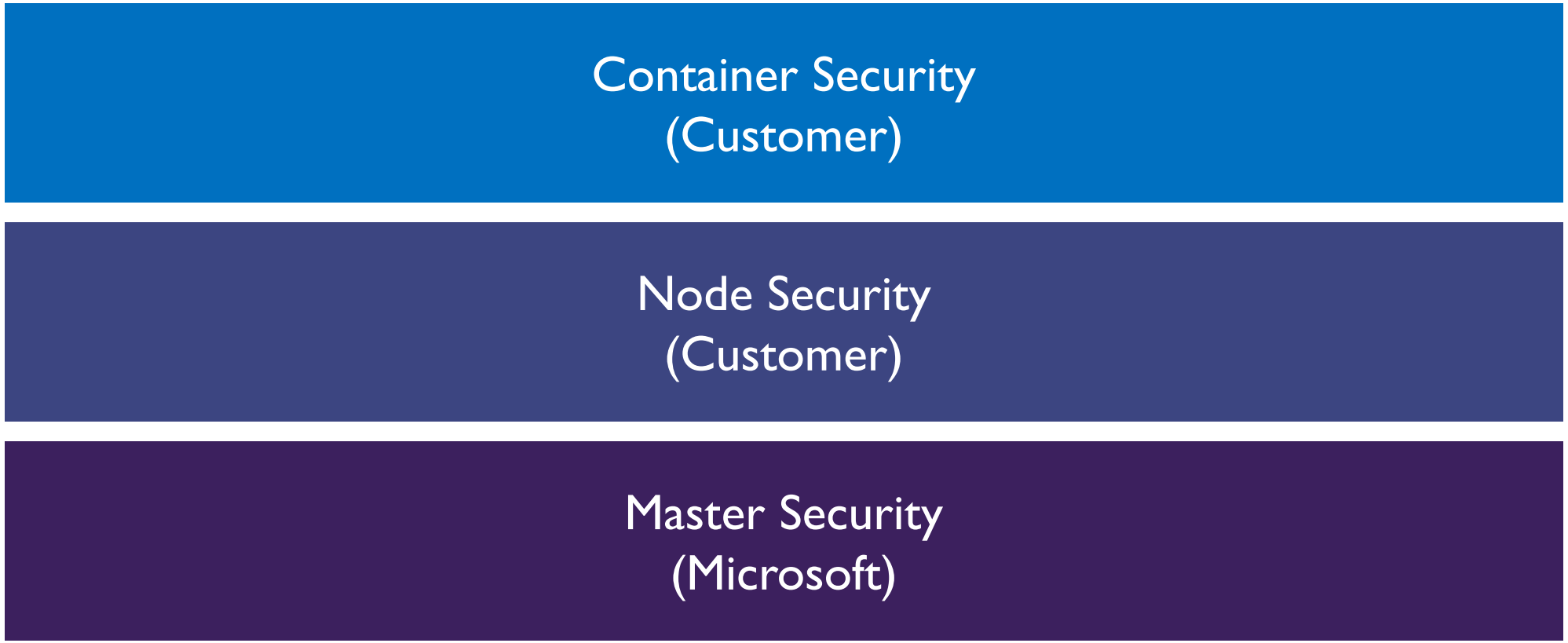
Detail:

- Just-in-time (JIT) VM access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
- When JIT is enabled, Security Center locks down inbound traffic to your Azure VMs by creating a network security group rule.
- You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the JIT solution.

Container Security: AKS

AKS Security

SKYLINES ACADEMY



AKS Security: Best Practices

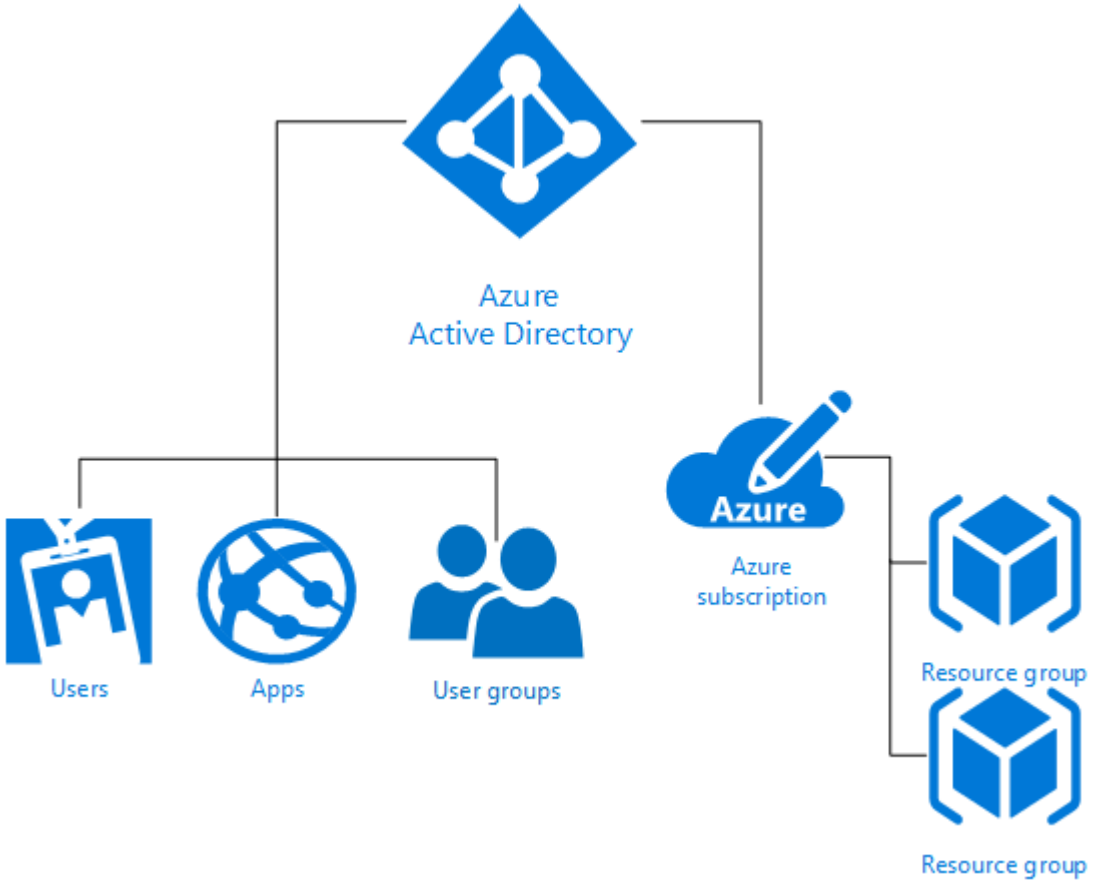
SKYLINES ACADEMY

- Secure Access to AKS
- Secure Container Access
- Update AKS Nodes

Role Based Access Control (RBAC)

SKYLINES
ACADEMY

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

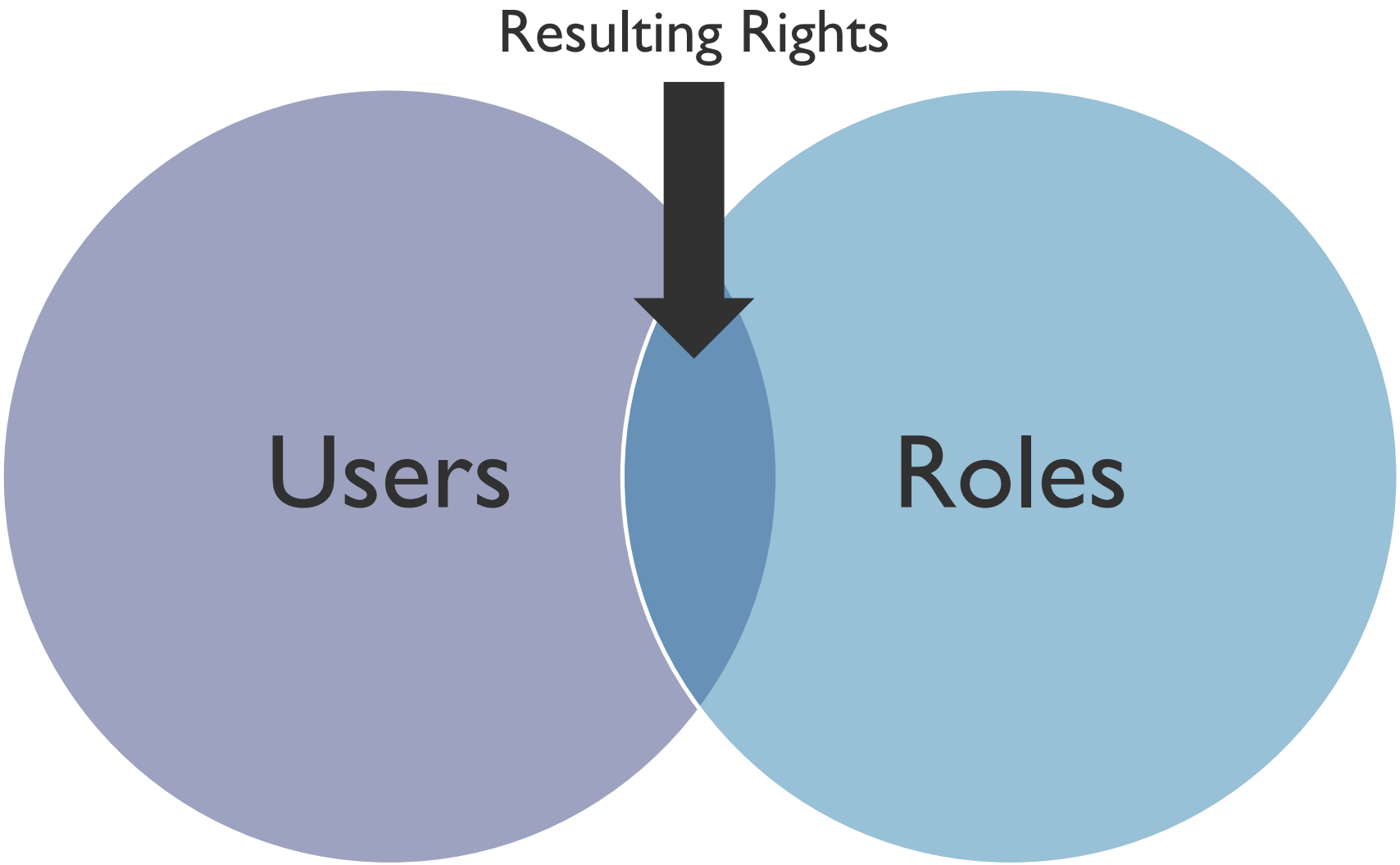
Azure RBAC Built-in Roles (continued)

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

Azure Policy

SKYLINES
ACADEMY

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

Azure Log Analytics

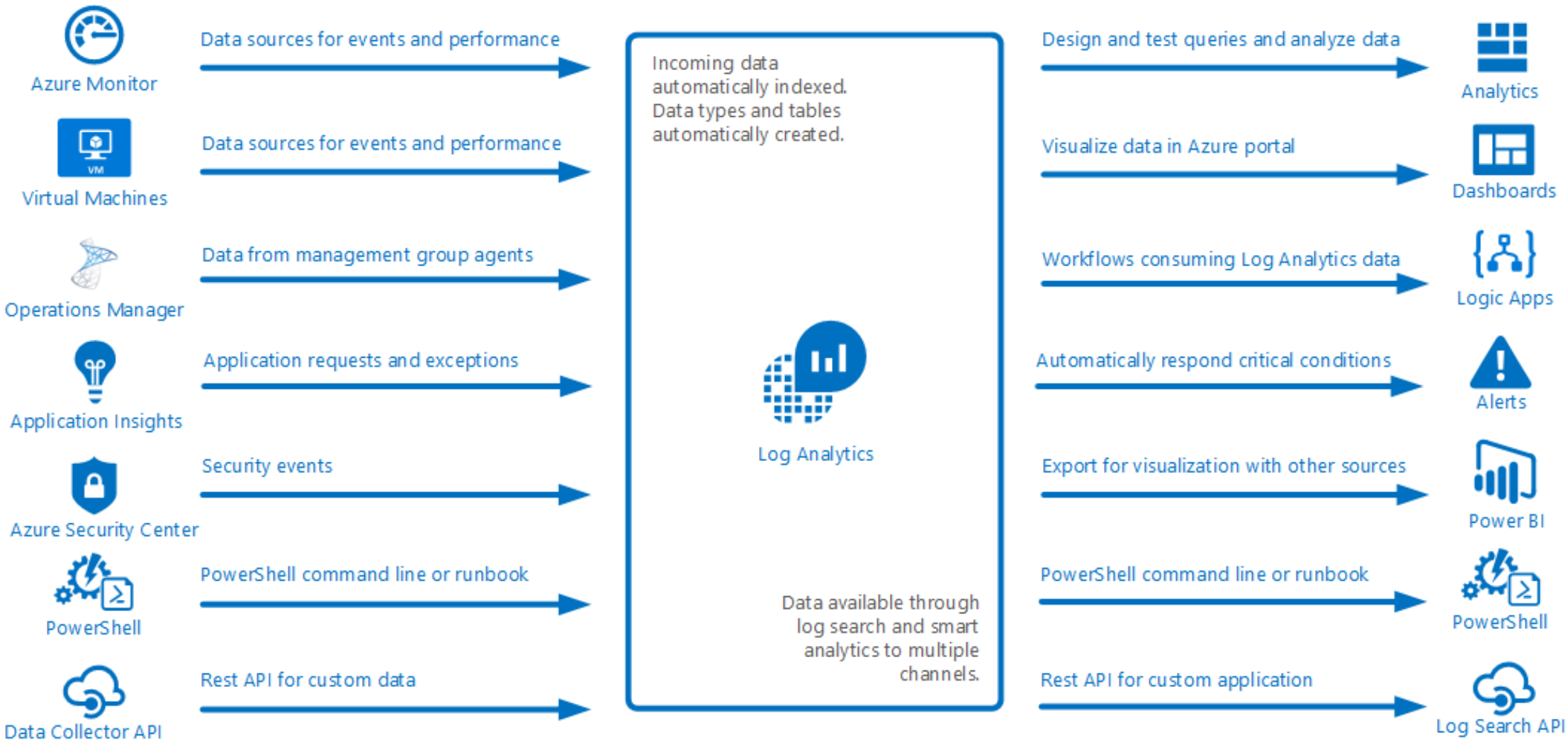
SKYLINES
ACADEMY

Log Analytics Key Features

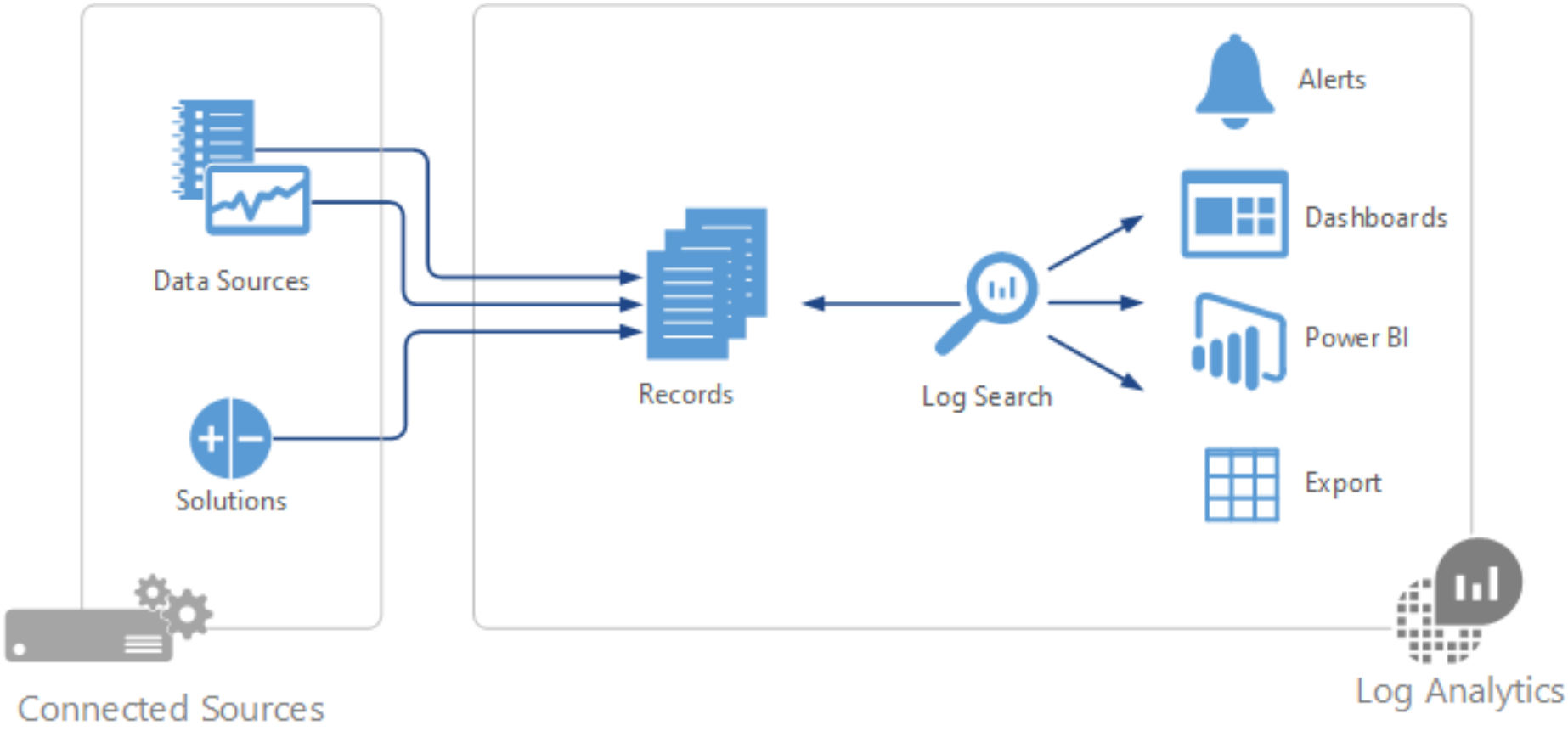
SKYLINES ACADEMY

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

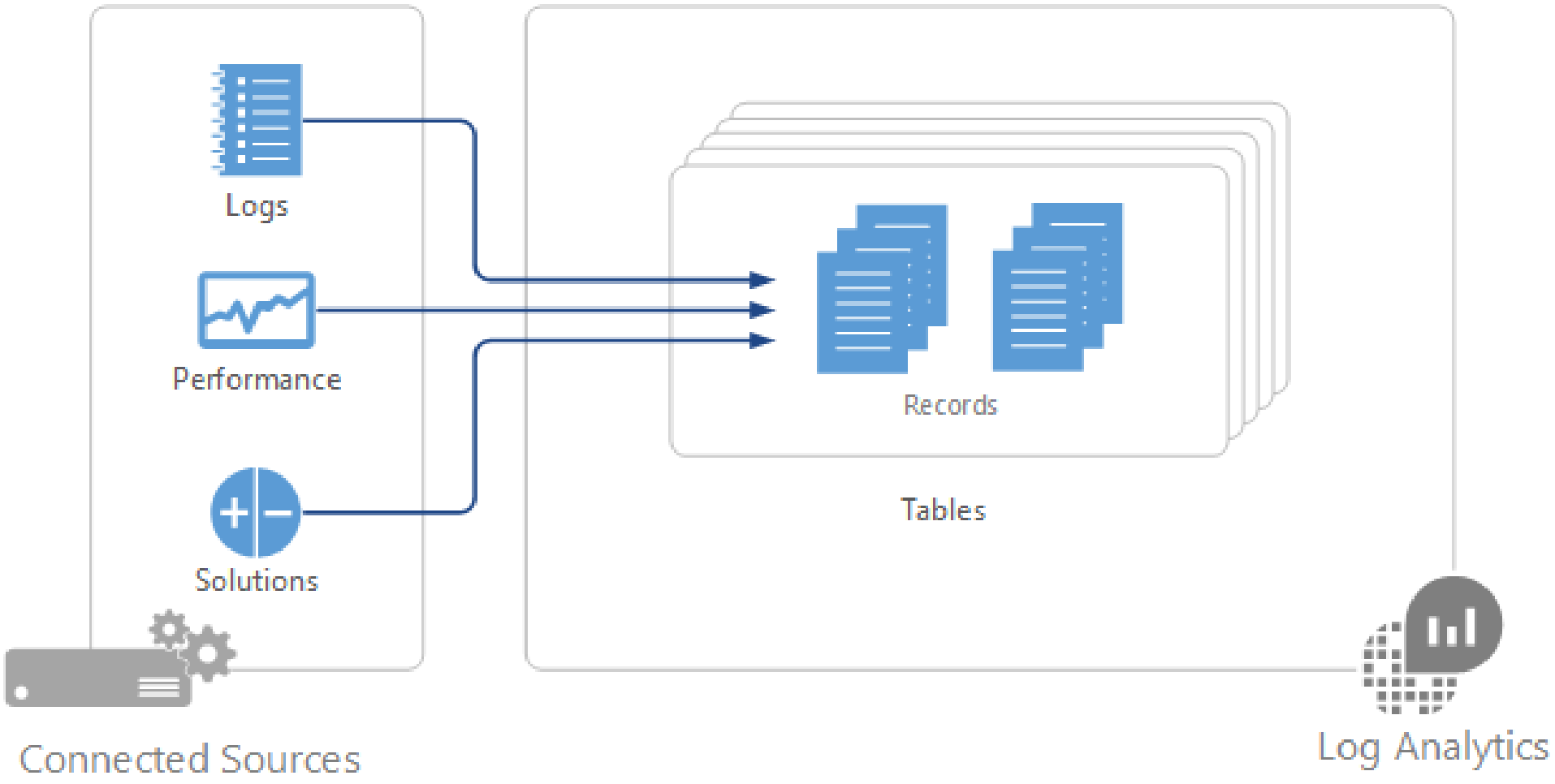
Log Search Use Cases



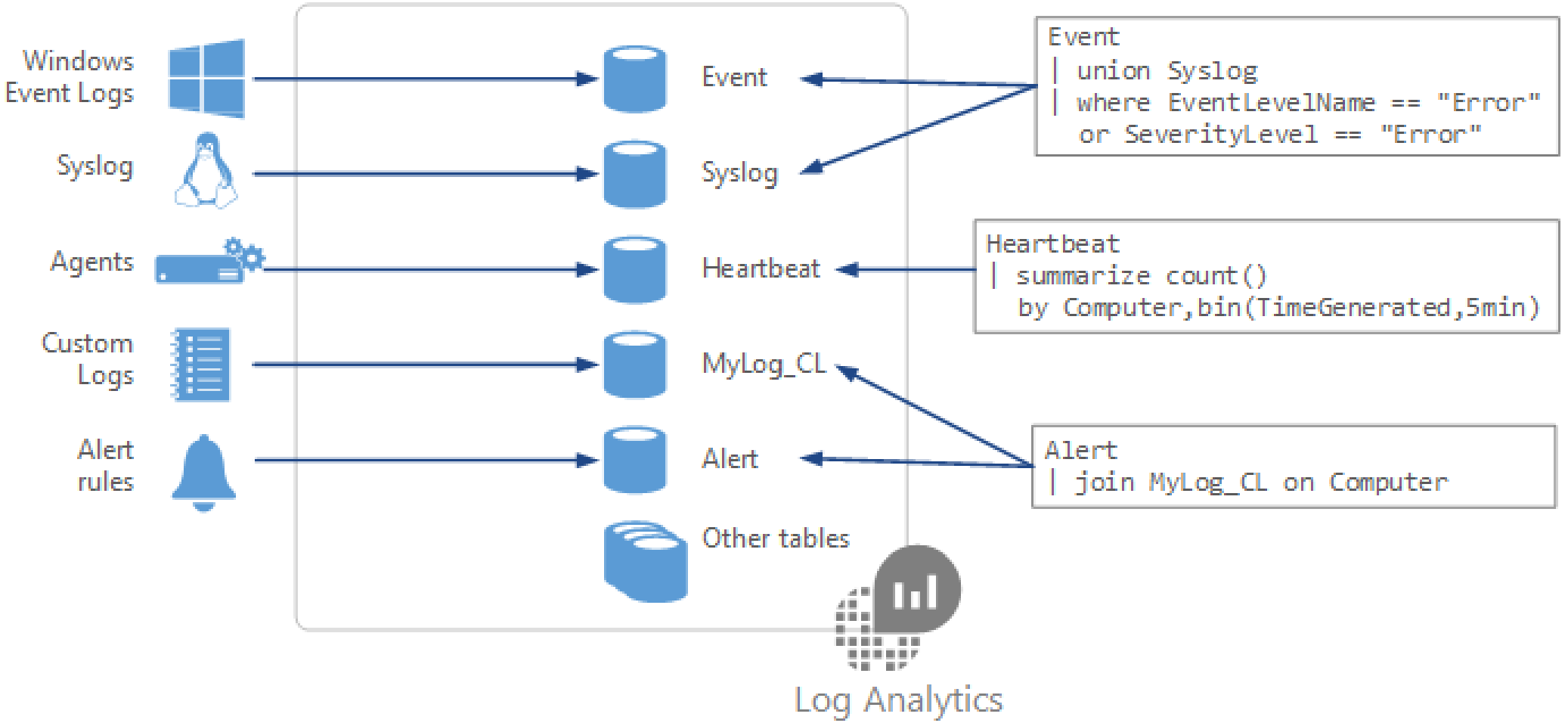
Log Analytics Architecture



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

Azure Security Center Overview

SKYLINES
ACADEMY

Azure Security Center Overview

SKYLINES ACADEMY

- Centralized Policy Management
- Continuous Security Assessment
- Actionable Recommendations
- Advanced Cloud Defenses
- Prioritized Alerts and Incidents
- Integrated Security Solutions

Security Center Pricing Tiers

SKYLINES ACADEMY

Free (Azure Resources Only)	Standard
• Security assessment • Security recommendations • Basic security policy • Connected partner solutions	• All features in free tier plus • Just in time VM access • Network threat detection • VM threat detection

Azure SQL

SKYLINES
ACADEMY

Azure SQL

- Relational database-as-a-service
- Uses latest stable version of Microsoft SQL
- Create NEW or…
- Migrate Existing databases using the Microsoft Data Migration Assistant

Azure SQL Database – Key Features

SKYLINES ACADEMY

Predictable Performance

Measured in database throughput units (DTUs)

High Compatibility

Supporting existing SQL client applications via tubular database stream (TDS) endpoint

Simplified Management

This includes SQL Server-specific Azure tools

Azure SQL Database Tiers

SKYLINES ACADEMY

Basic	Standard	Premium
Small database with single concurrent user	**Medium-sized database that must support multiple concurrent connections**	**Large databases that must support a large number of concurrent connections and operations**
• Small dbs • Single active operation • Dev / Test • Small scale apps • 5 DTU	• Good option for cloud apps • Multiple operations • Workgroup or web apps • 10-100 DTU	• High transaction volumes • Large number of users • Multiple operations • Mission critical apps • 100-800 DTU

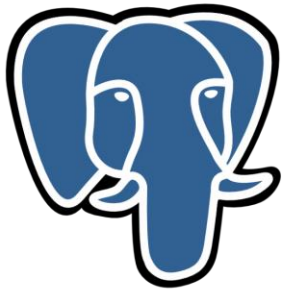
NEW – Azure SQL Managed Instances

- Managed SQL Servers
- More compatible with legacy workloads

Third-party Databases in Azure – Managed

SKYLINES ACADEMY

- Managed database options:
  - Build-in HA at no additional cost
  - Predictable performance
  - Pay-as-you-go
  - Auto-scaling
  - Encryption at-rest and in-transit
  - Automatic backups with point-in-time-restore for up to 35 days
  - Enterprise-grade security and compliance



PostgreSQL

Third-party Databases in Azure – Non-managed

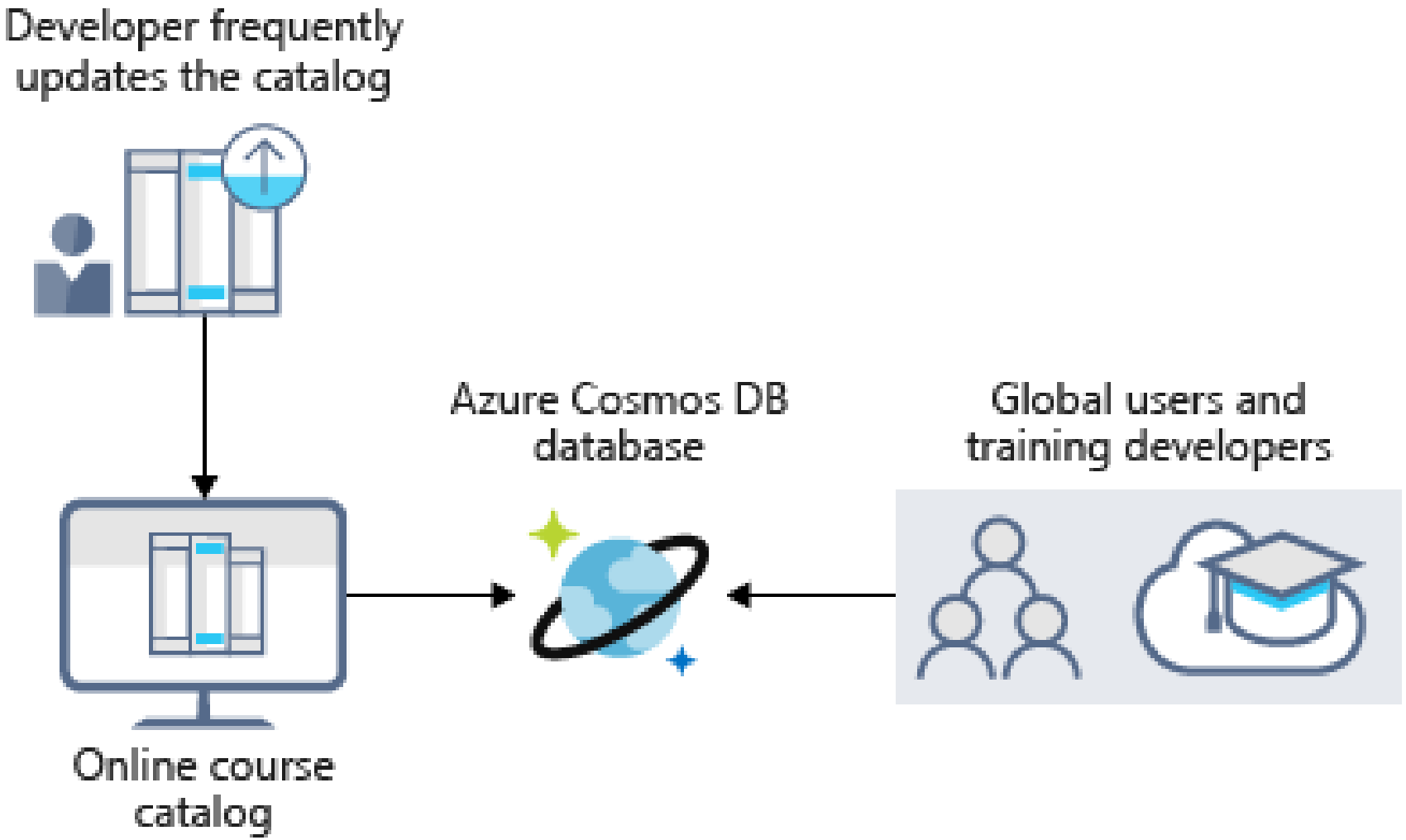
SKYLINES ACADEMY

- Non-managed database options:
  - Windows Azure VMs hosting MySQL installations
  - Linux Azure VMs hosting MySQL installations
  - ClearDB offering managed MySQL instance

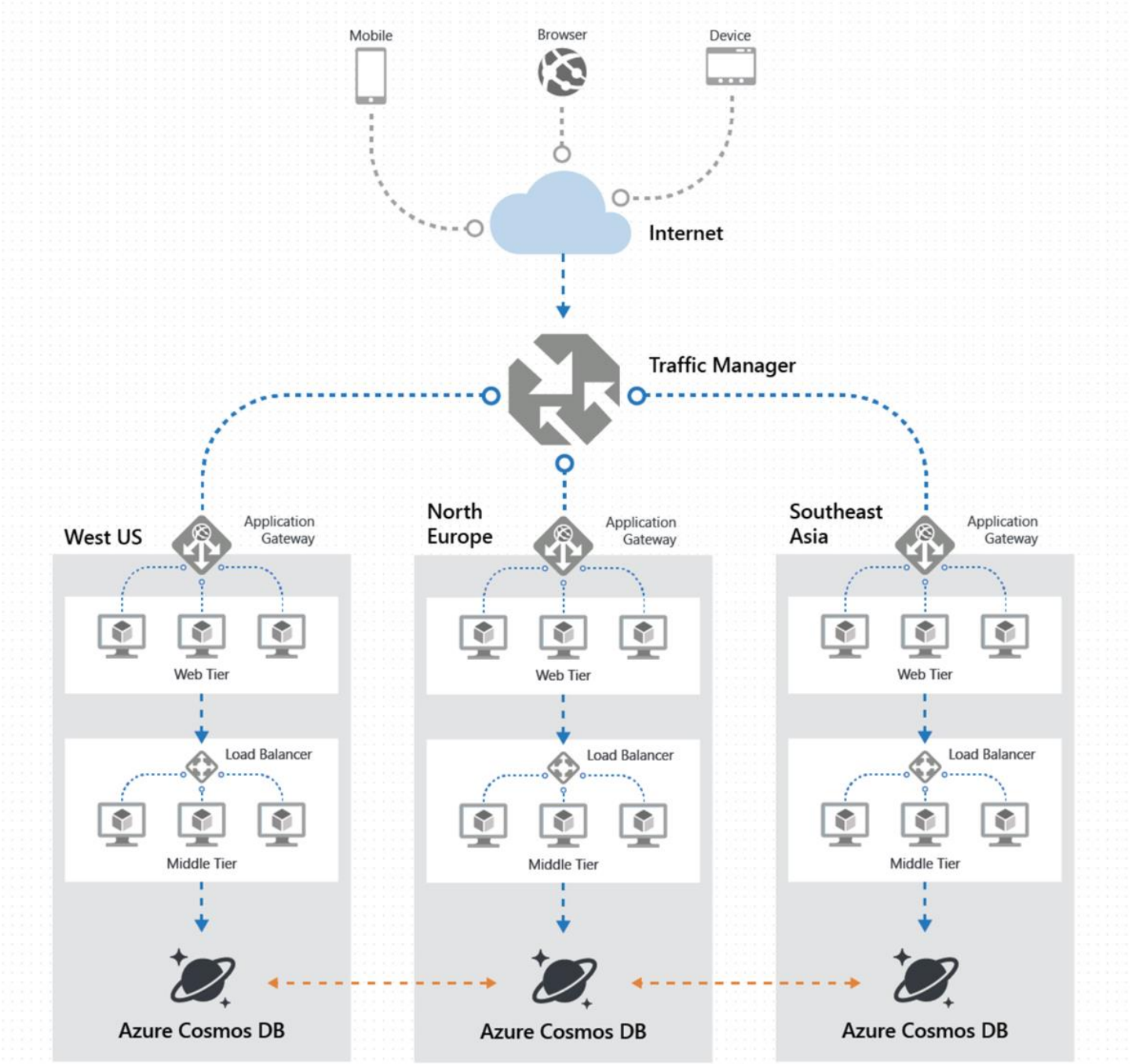
CLEARDB™

Azure Cosmos DB

- Globally Distributed Database Service
- Supports schema-less data
- Used to build highly responsive Always On applications with constantly changing data



SKYLINES ACADEMY



SKYLINES ACADEMY

Azure Cosmos DB APIs

- Accessible via various APIs e.g:
  - Document DB (SQL) API
  - MongoDB API
  - Graph (Gremlin) API
  - Tables (Key/Value) API
- Automatically partitioned for:
  - Performance
  - Storage capacity

Design Auditing and Caching Strategies

SKYLINES
ACADEMY

Auditing

Auditing for SQL Database and Data Warehouse

SKYLINES ACADEMY

- Why Audit?
  - Maintain regulatory compliance
  - Understand DB activity
  - Gain deeper insights
- What it does?
  - Tracks DB events and writes them to an audit log
  - Utilize OMS workspace, Storage Account, or Event Hubs

Azure SQL Database Auditing Overview

SKYLINES ACADEMY

You can use SQL database auditing to:

Retain

An audit trail of selected events. You can define categories of database actions to be audited.

Report

Report on database activity using pre-configured reports and a dashboard to quickly get started.

Analyze

Analyze reports, find unusual activity, suspicious events and trends.

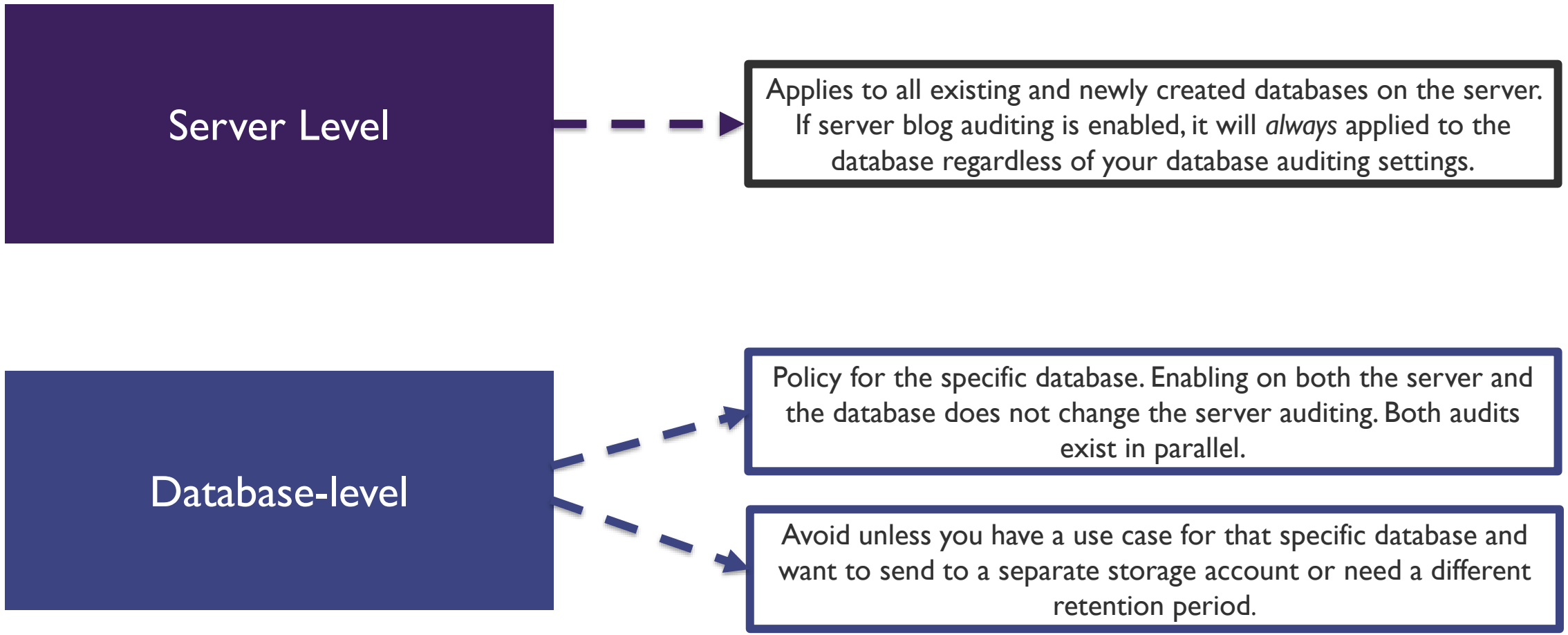
Azure SQL Database Auditing Overview

SKYLINES ACADEMY

- Audit logs are written to **Append Blobs** in Azure Blob storage on your Azure subscription
- All storage **types (v1, v2, blob) are supported**
- All storage **replication configurations are supported**
- **Premium storage** is currently ***not*** **supported**
- **Storage in VNet** is currently ***not*** **supported**
- **Storage behind a Firewall** is currently ***not*** **supported**

Server-level vs Database-level Auditing Policies

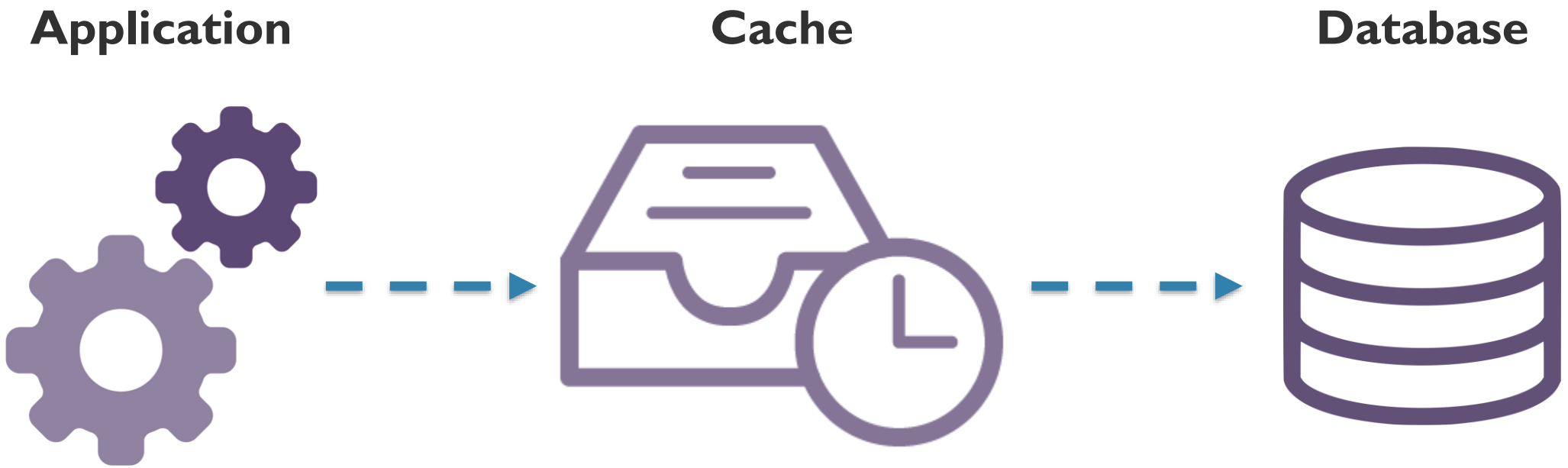
SKYLINES ACADEMY



Caching

What is Caching?

SKYLINES ACADEMY



Distributed Application Caching

SKYLINES ACADEMY

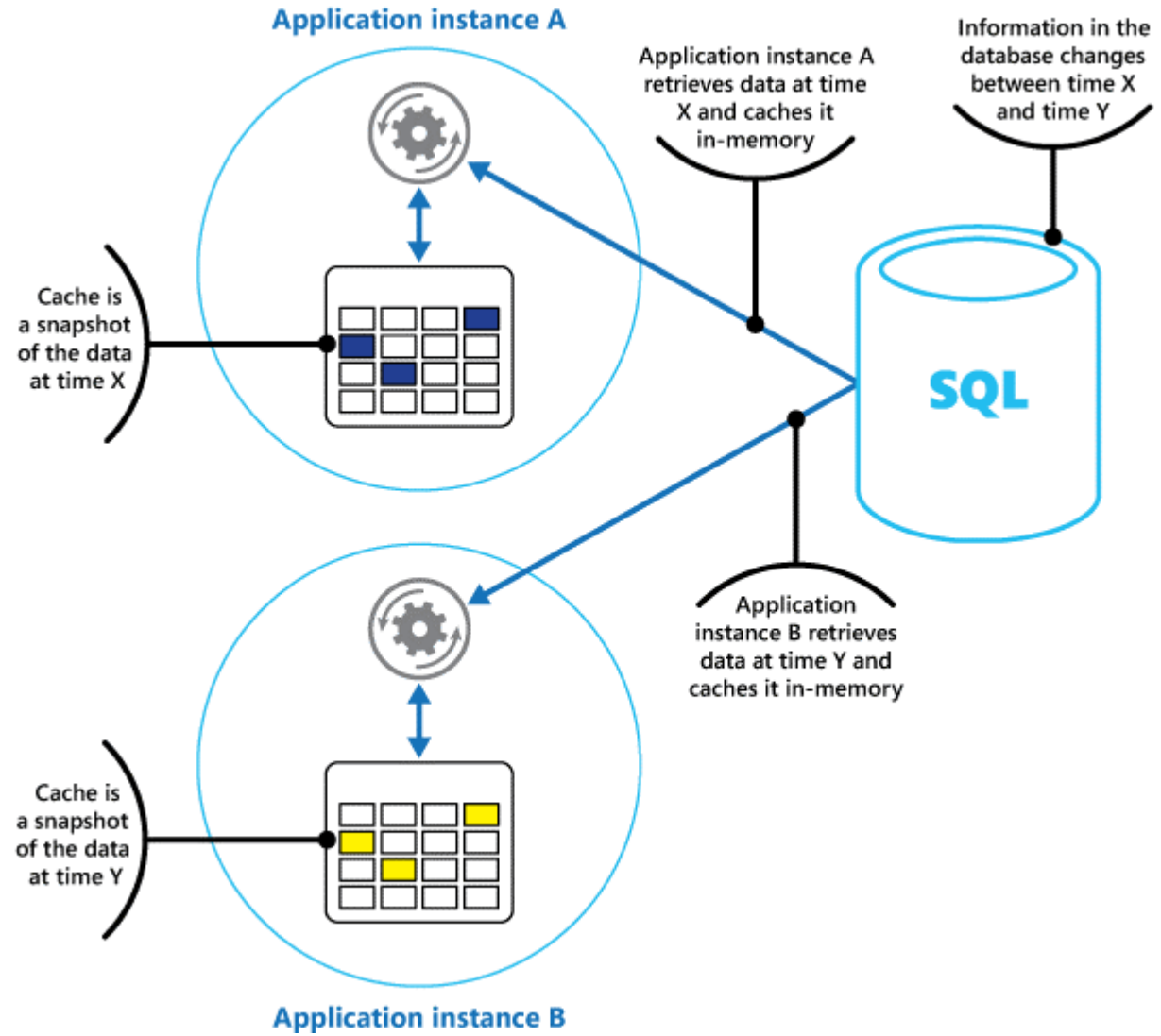
Private Caching

Used when data is held locally on the instance that is running the application or service

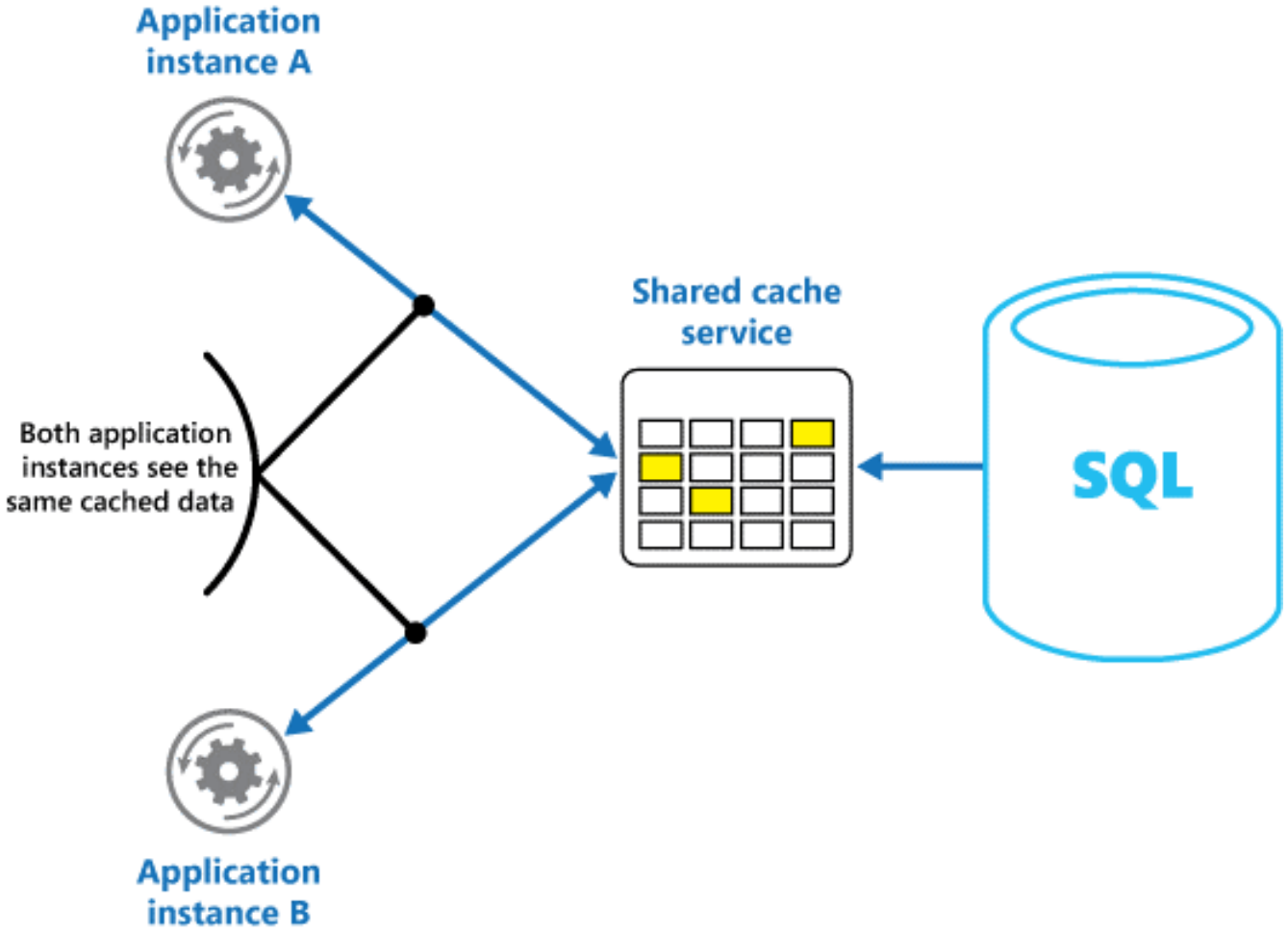
Shared Cache

Common source that can be access by multiple application processes and/or machines

Private Caching



Shared Caching

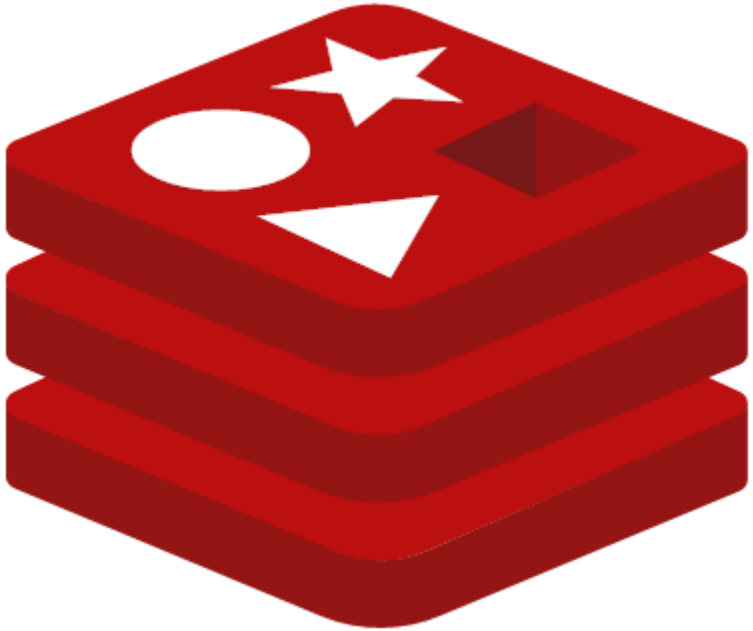


Caching Considerations

SKYLINES ACADEMY

- Deciding WHEN to cache data
- Determine how to cache data effectively
- Highly Dynamic Data
- Data Expiration
- Invalidate data in a client-side cache

Azure Redis Cache



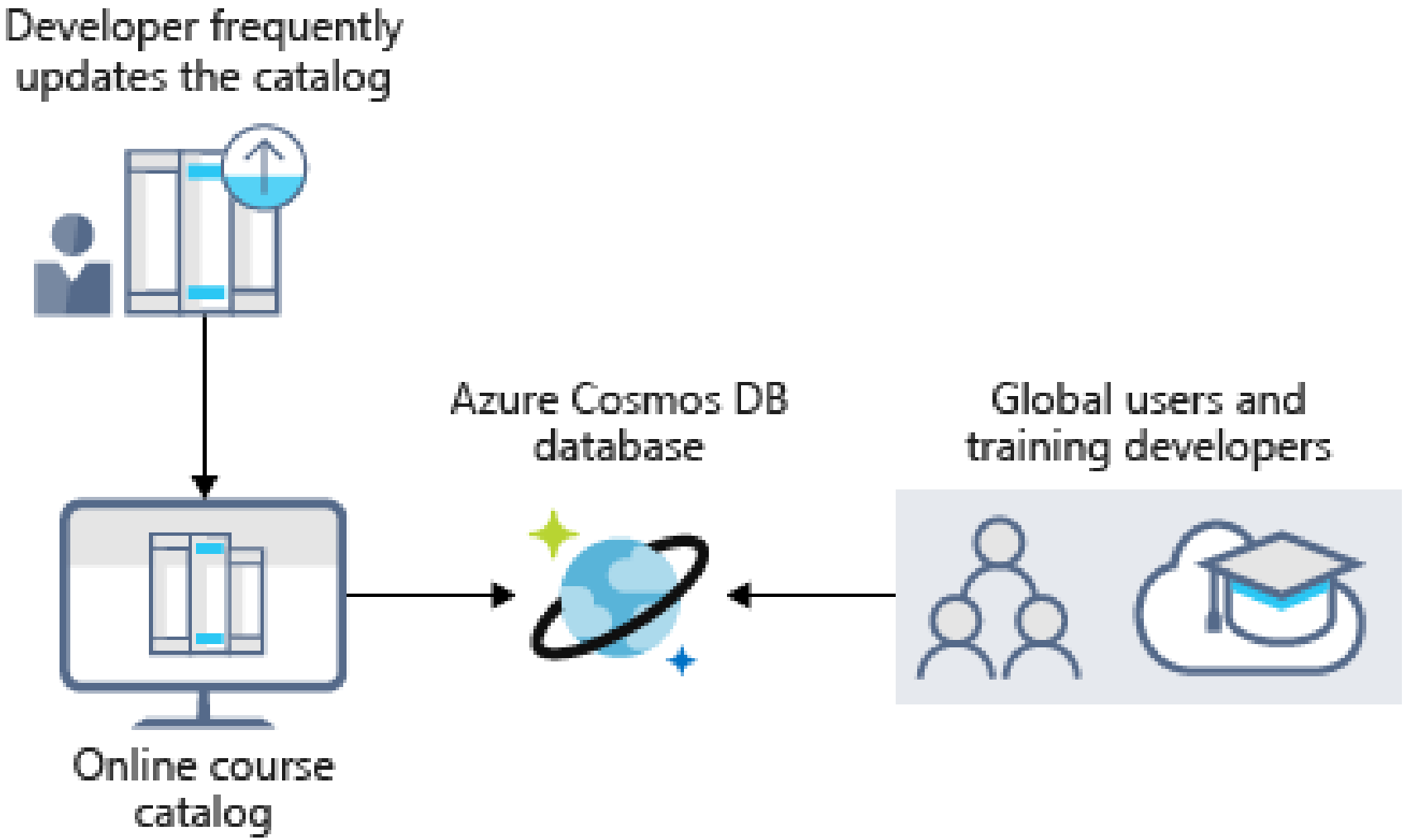
- Implementation of the open source Redis cache that runs as a service in Azure
- Provides caching service for cloud services or websites inside VMs
- Can be shared by client applications that have the access key

Cosmos DB

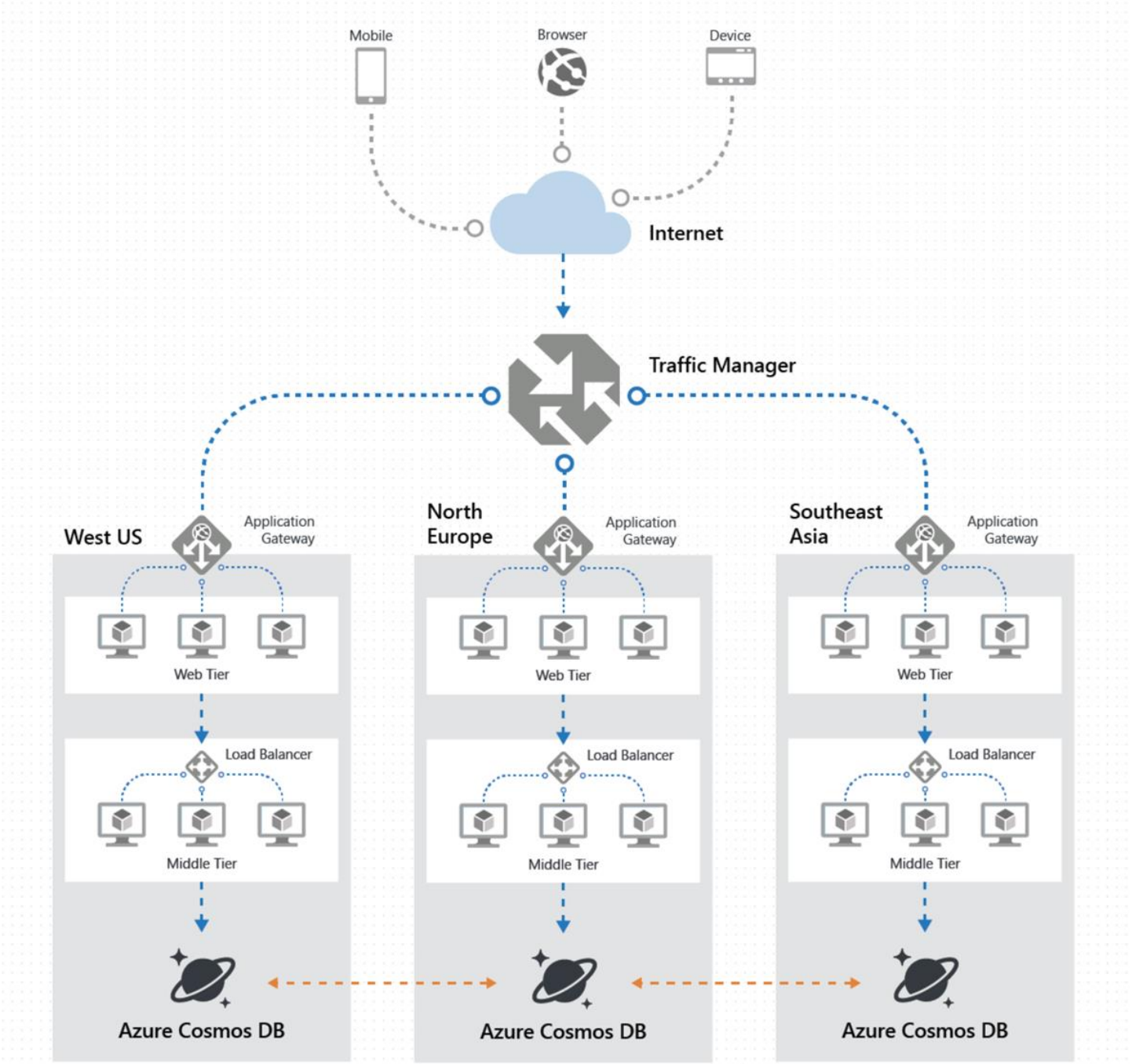
SKYLINES
ACADEMY

Azure Cosmos DB

- Globally Distributed Database Service
- Supports schema-less data
- Used to build highly responsive Always On applications with constantly changing data



SKYLINES ACADEMY



SKYLINES ACADEMY

Azure Cosmos DB APIs

- Accessible via various APIs e.g:
  - Document DB (SQL) API
  - MongoDB API
  - Graph (Gremlin) API
  - Tables (Key/Value) API
- Automatically partitioned for:
  - Performance
  - Storage capacity

Cosmos DB Consistency Levels

SKYLINES
ACADEMY

Consistency Levels

SKYLINES ACADEMY

Strong	Bounded Staleness	Session	Consistent Prefix	Eventual
Guaranteed write operation only committed and visible on the primary after it has been committed and confirmed by all replicas.	Allows to configure how stale docs can be within replicas; staleness means the quantity or version count a replica document can be behind a primary document.	Guarantees that all read and write operations are consistent within a user session.	Ensures changes are read in the order that matches the sequence of the corresponding writes.	Offers looser consistency and commits and write operations against the primary immediately. Replica transactions are asynchronously handled and will eventually be consistent with the primary.

Choose a Consistency Strategy

SKYLINES ACADEMY

1. Stronger Consistency Level

- Ensures documents in replicas do not lag behind the primary
- Recommended for applications that require all replicas to exactly match the primary at any point in time
- Negative affect on the write operations

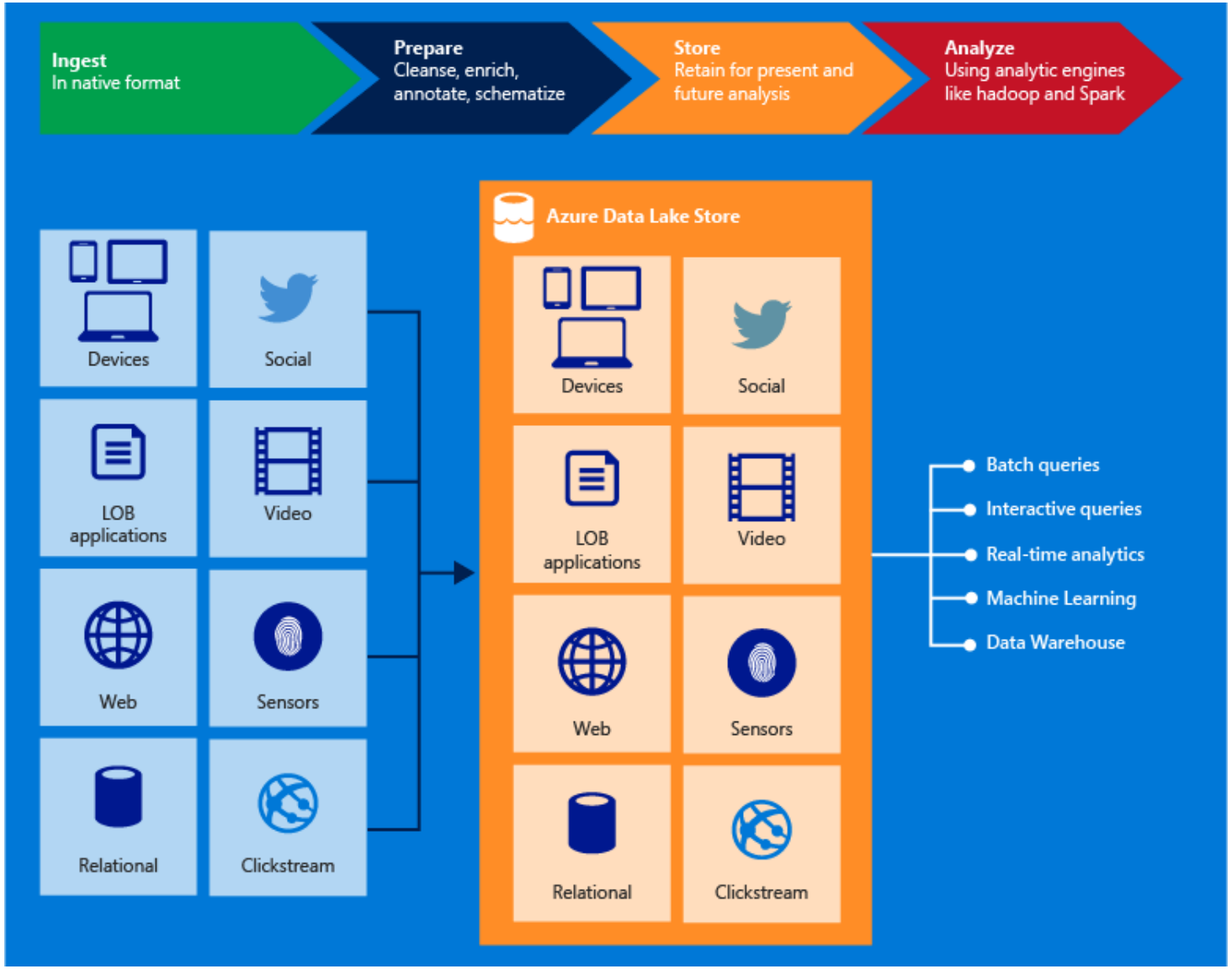
2. Weaker Consistency Level

- Ensures the database operates at peak efficiency
- Recommended for all apps that require high performance
- Read operations against a replica can return stale data

Azure Data Lake Store

SKYLINES
ACADEMY

Azure Data Lake Store Overview



Securing Data in Azure Data Lake Store

SKYLINES ACADEMY

Authentication

- Integrated with Azure Active Directory

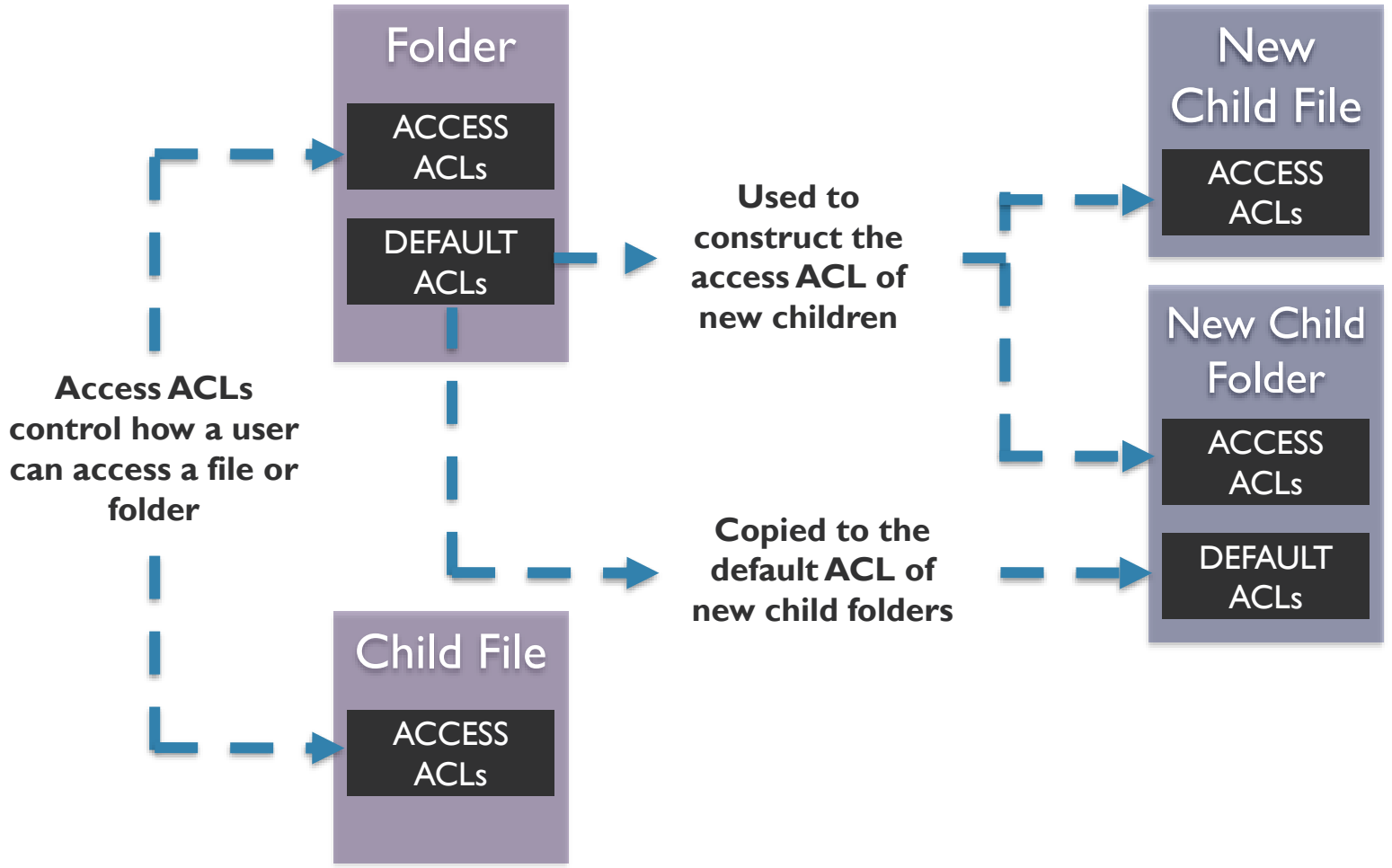
Access Control

- ACLs can be enabled on the root folder, on subfolders, and on individual files.

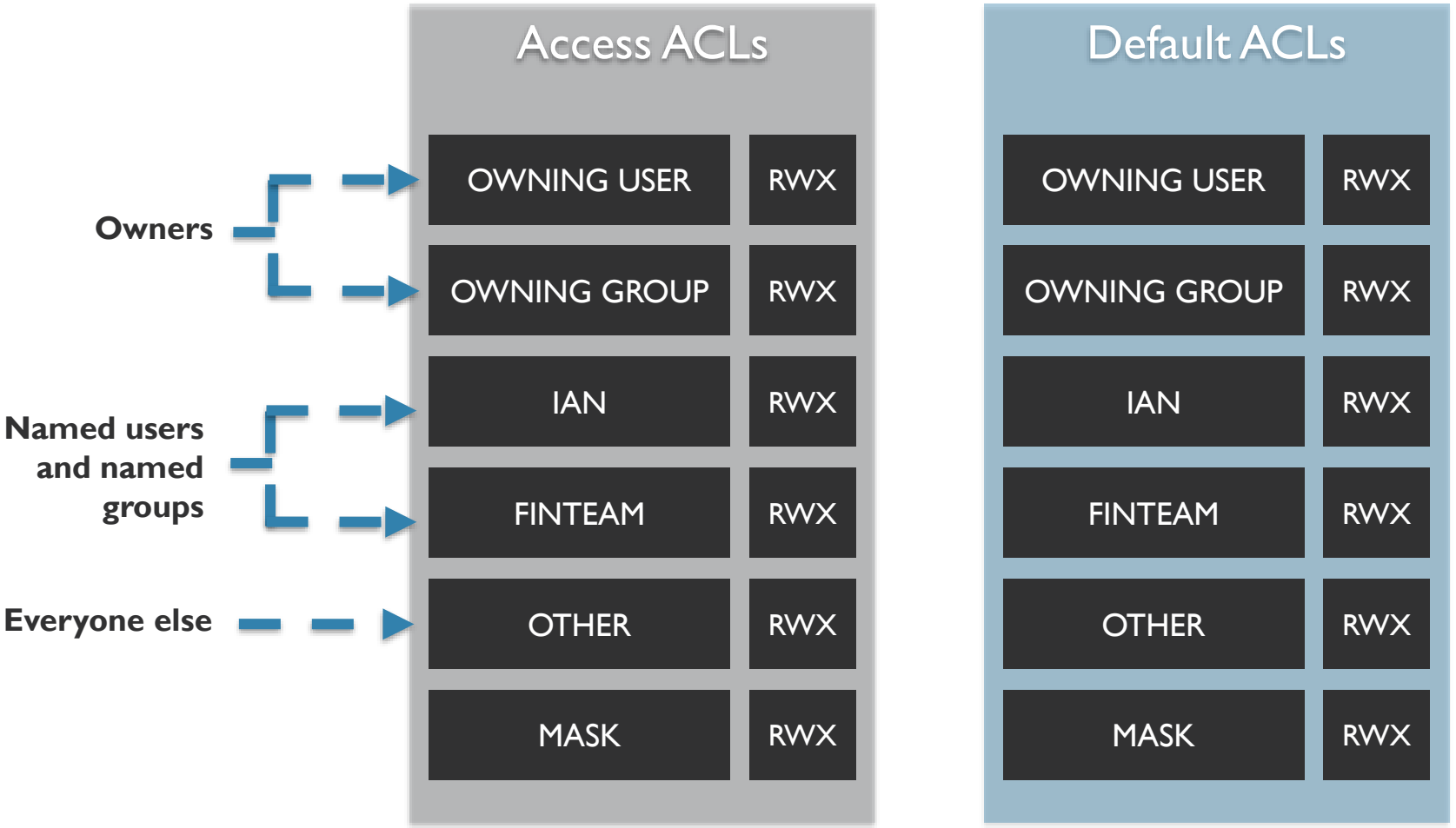
Encryption

- Data Lake Store also provides encryption for data that is stored in the account.
- Specify the encryption settings while creating a Data Lake Store account
- Chose to have your data encrypted or opt for no encryption.

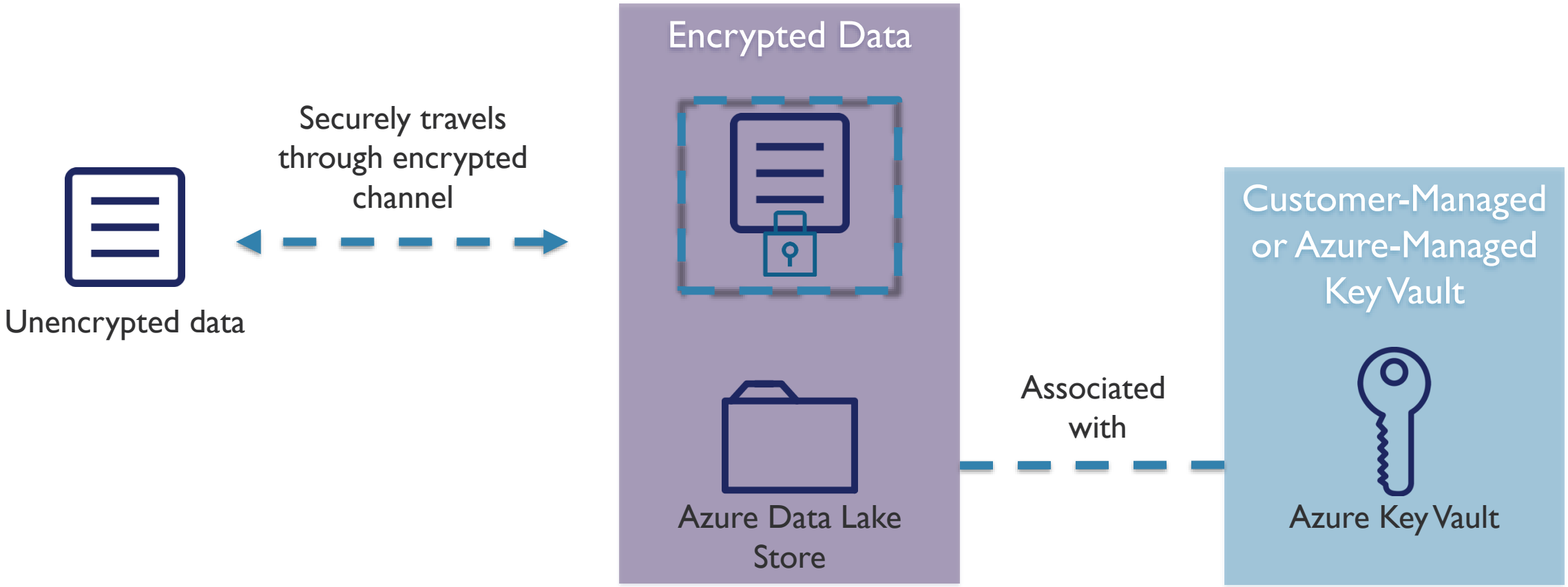
Azure Data Lake Store Access Control



Access Control Structure



Azure Data Lake Store Encryption



Differences in Key Management

SKYLINES ACADEMY

	Service-Managed Keys	Customer-Managed Keys
How is data stored?	Always encrypted prior to being stored	Always encrypted prior to being stored
Where is the Master Encryption Key stored?	Key Vault	Key Vault
Are any encryption keys stored in the clear outside of Key Vault?	No	No
Can the MEK be retrieved by Key Vault?	No.	No
Who owns the Key Vault instance and the MEK?	The Data Lake Store service	You own the Key Vault instance, which belongs in your own Azure subscription
Can you revoke access to the MEK for the Data Lake Store service?	No	Yes
Can you permanently delete the MEK?	No	Yes

Types of Data

SKYLINES
ACADEMY

Types of Data

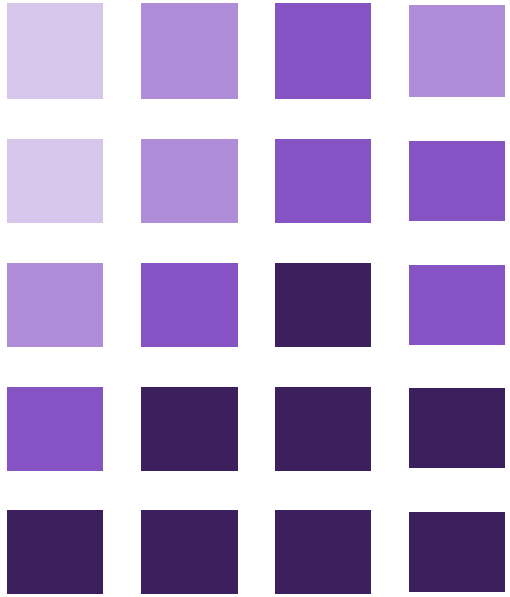
SKYLINES ACADEMY

Structured Data

Semi-Structured Data

Unstructured Data

Structured Data

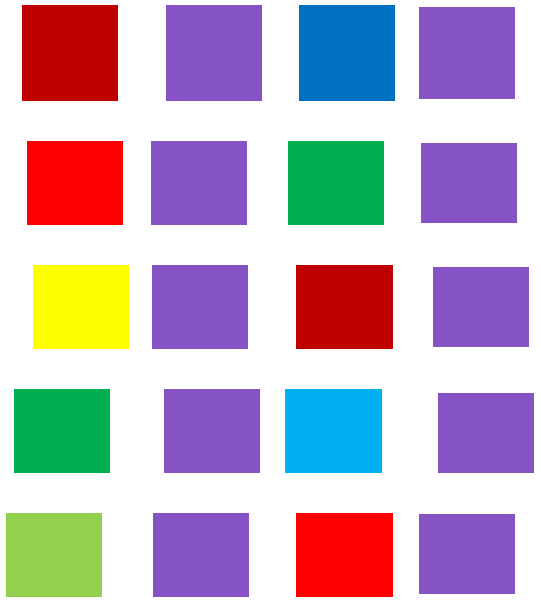


- Adheres to a schema
- All the data has the same field or properties
- Stored in a database table with rows and columns
- Relies on keys to indicate how one row in a table relates to data in another row of another table
- Referred to as “relational data”

Semi-Structured Data

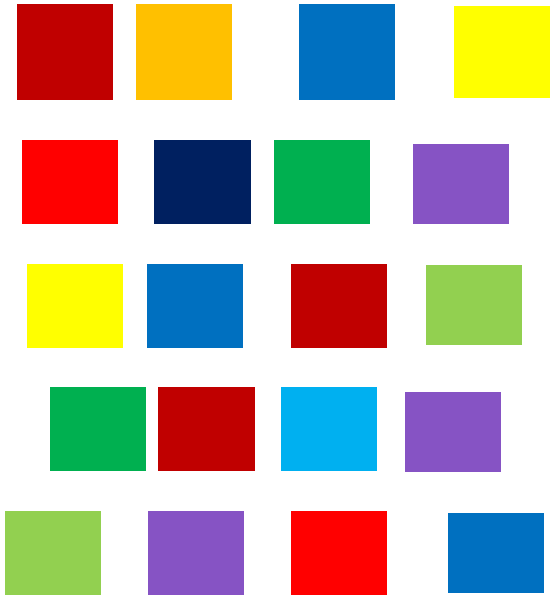
SKYLINES ACADEMY

- Doesn't fit neatly into tables, rows and columns.
- Uses tags or keys to organize and provide a hierarchy for the data.
- Often referred to as NoSQL or non-relational data



Unstructured Data

SKYLINES ACADEMY

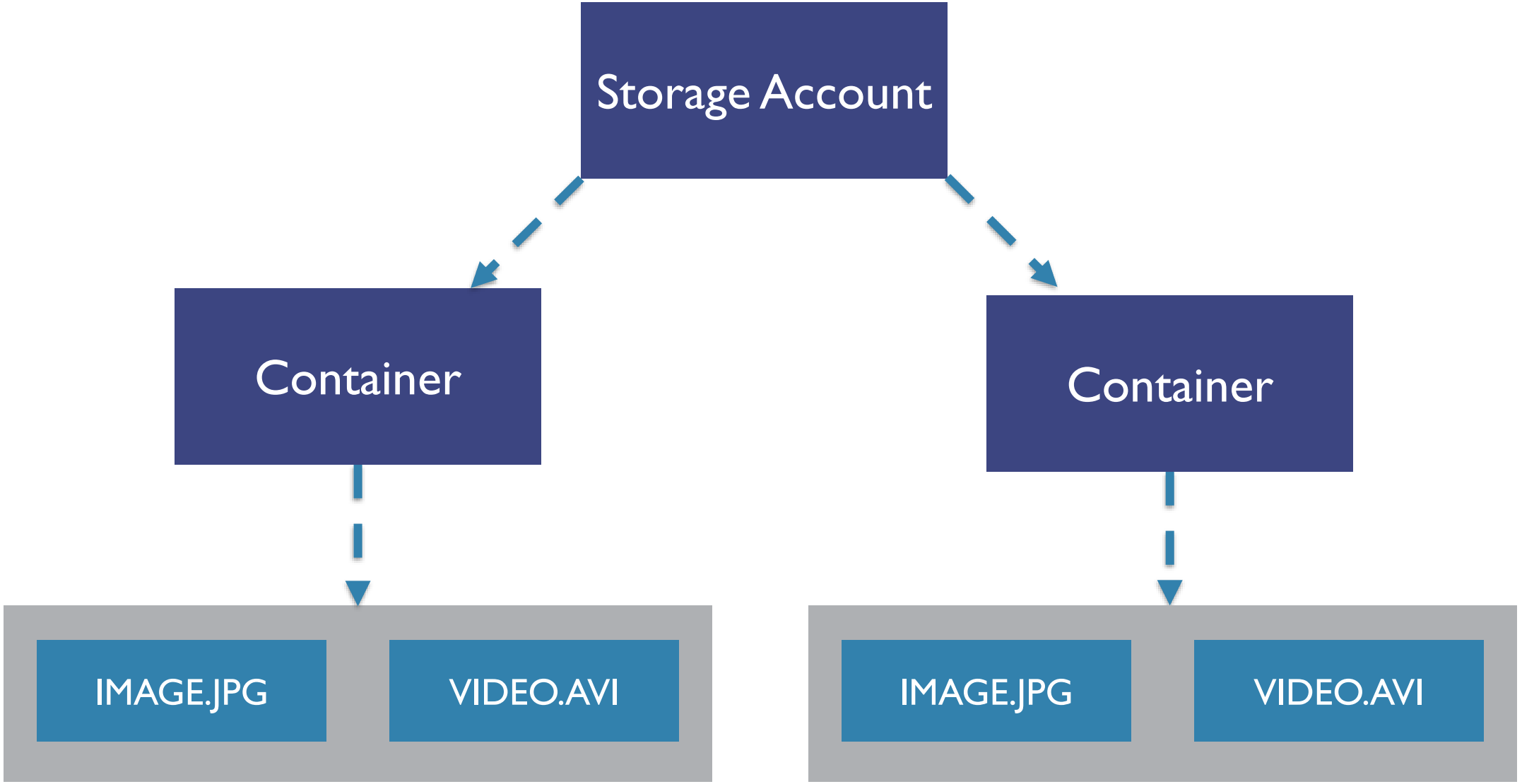


- No designated structure
- No restrictions on the kinds of data it can hold
- Example a blob can hold a PDF, JPEG, JSON, videos etc.
- Enterprises are struggling to manage and tap into the insights from their unstructured data

Azure Storage Account Overview

SKYLINES
ACADEMY

Azure Blob Storage Overview



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

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

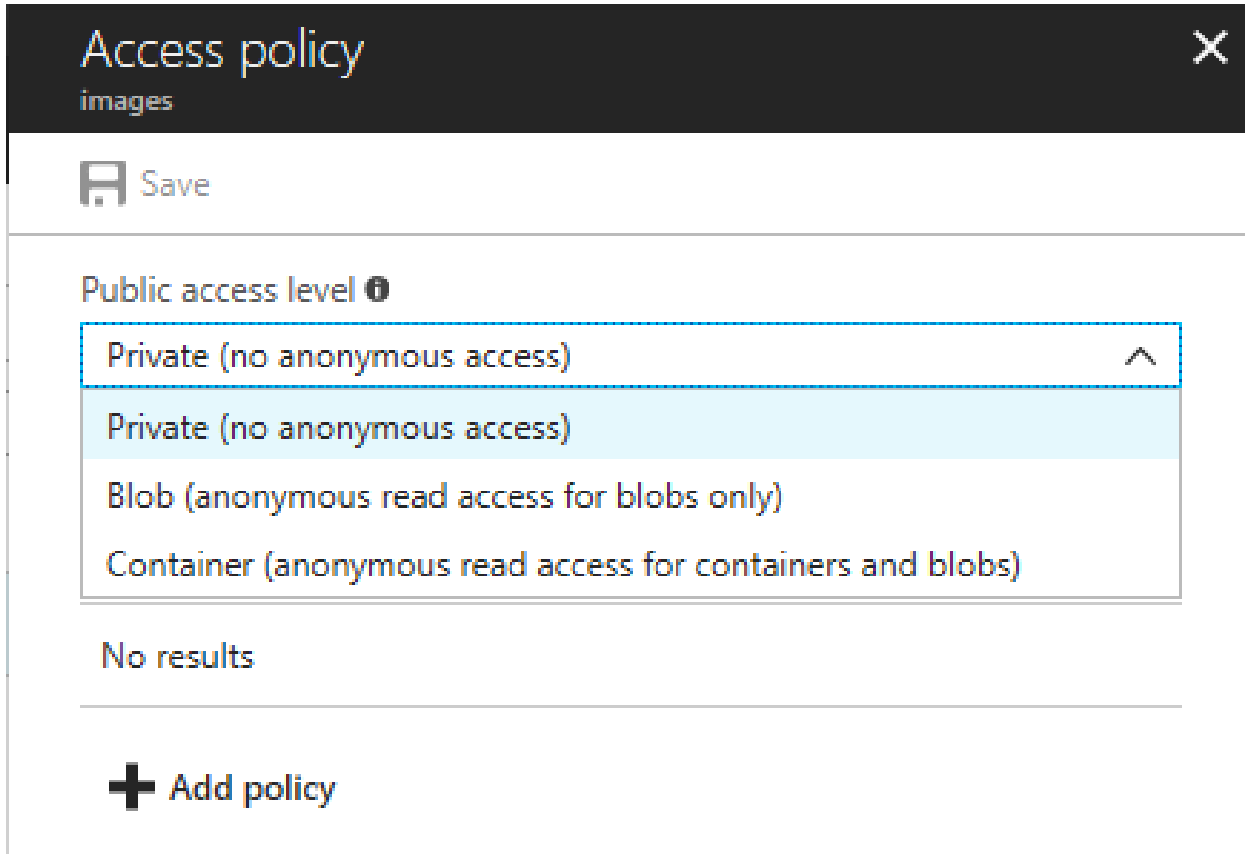
Container Permissions

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)

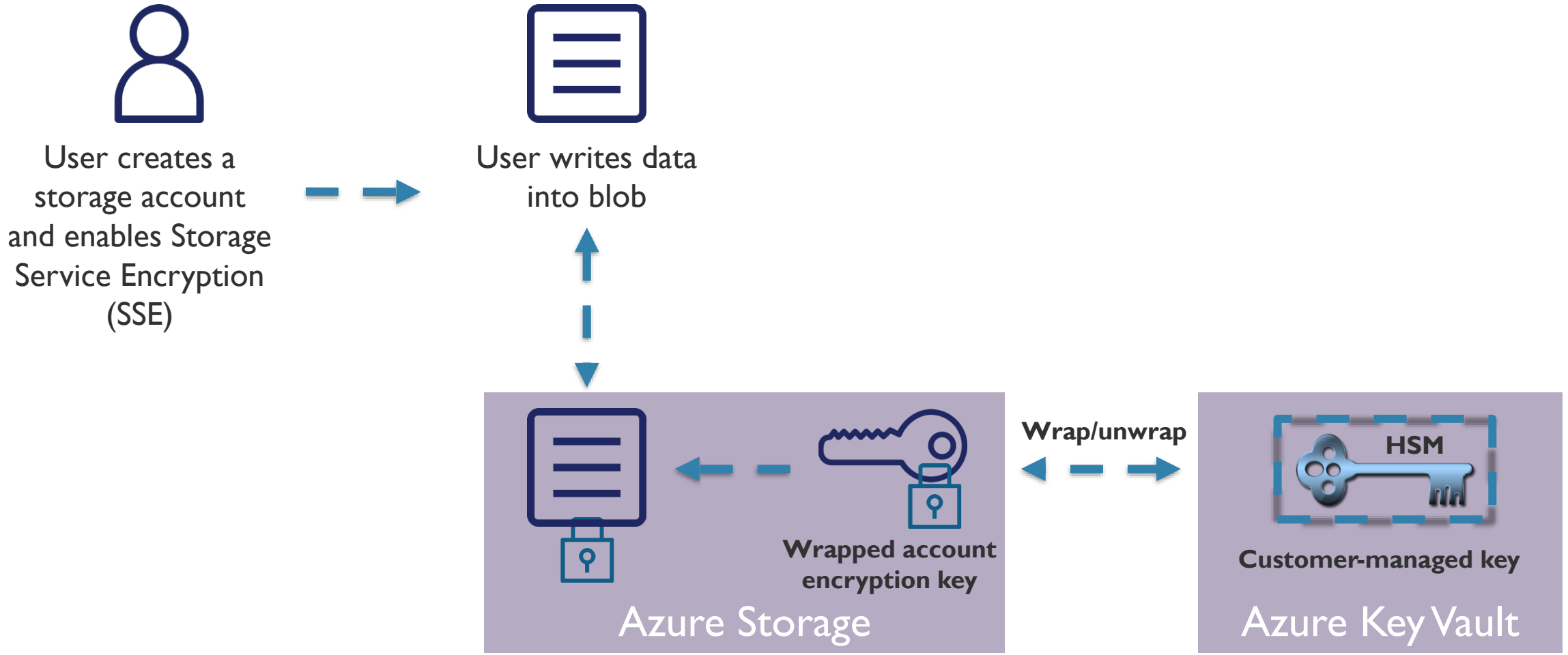
SKYLINES ACADEMY

- 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

Encryption Keys & Key Vault

Encryption Keys and Key Vault

SKYLINES ACADEMY



Key Vault Overview

SKYLINES
ACADEMY

Key Vault Overview

SKYLINES ACADEMY

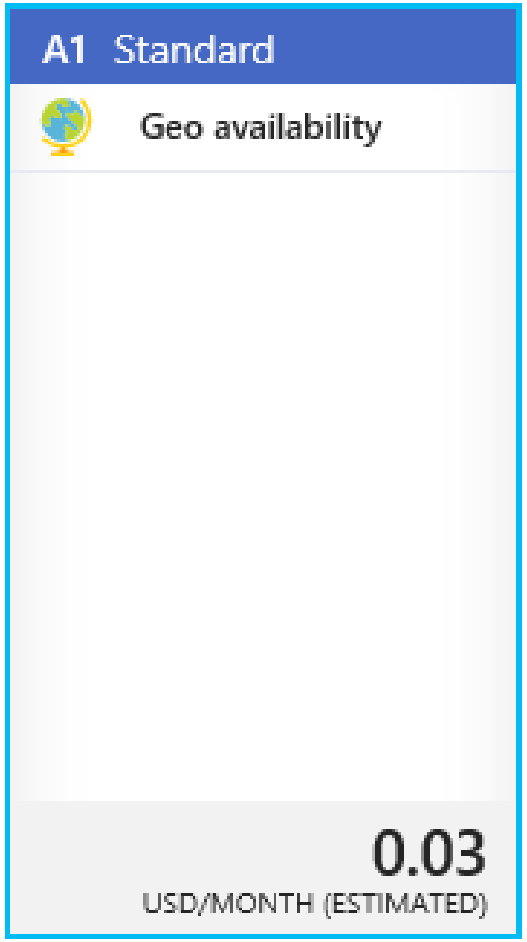
- Service in Azure for safeguarding keys and secrets
- Uses keys that are protected by hardware security modules (HSMs)
- Can import or create new keys
- Can be accessed by AAD-authenticated requests

Key Vault Use Cases

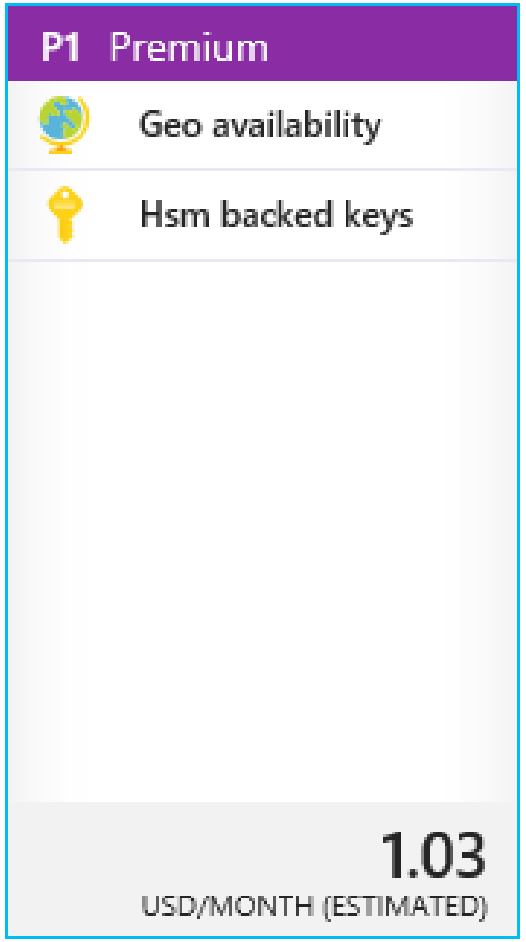
SKYLINES ACADEMY

- Developers:
  - Keeping keys external from applications
  - Allowing customers to bring their own keys for Software-as-a-Service (SaaS) apps
- Azure Admins:
  - Storing passwords in Key Vault which can be referenced during ARM deployments
  - Bring your own storage keys

Key Vault SKUs



OR



Key Management Tasks

SKYLINES ACADEMY

- Create or import a key or secret
- Revoke or delete a key or secret
- Authorize users to access the key vault
- Configure and monitor key usage

SKYLINES

ACADEMY