

AZ-301: Azure Architect Design



SKY LINES

ACADEMY

Exam Overview

Exam Tips

40-60 Questions

- Some questions worth more than 1 point
- Answer ALL the questions. There is no penalty.

Plan for 180 minutes

- 150 minutes to answer questions
- 30 mins for various instructions, comments etc.

Types of question

- Multiple choice
- List
- Hot Area
- Active Screen
- Drag and Drop

Case Studies

- Lots of information to absorb
- Focus on the key points
- Skim read first, look at the question and come back to dig in for the requirements

If you took AZ-300...

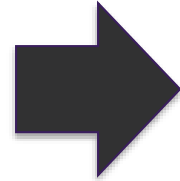


- This exam focuses more on “Design” and “Choice”
- Less hands on...
- Core concepts on compute, storage, networking will be repeated but focus on mapping requirements to your choices this time.

Identifying Requirements

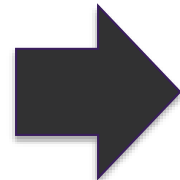
Identifying Requirements

Use Cases



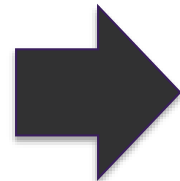
- Business Drivers
- Understand the goals of the business and application teams
- Use to formulate specific requirements

Assumptions



- Any assumptions being made about requirements?
- E.g. Must be able to use existing licenses

Critical Success Factors



- Try to align these to specific business outcomes
- Examples: Application needs to be scalable to xyz or must be able to utilize existing operations team.

Business Needs

Define Business Objectives

- Is this a 24x7 application?
- What RPO/RTO is acceptable?
- Does the application need to be globally available?

Document SLAs

- What is that availability requirement? 99.9? 99.99%?

Functional and Non Functional Requirements

- Functional defines whether the application does the right thing.
- Nonfunction lets you define whether the application does those things well.

Decompose by workload

- Different workloads may have different requirements for availability, scalability, data consistency, and disaster recovery.

Business Needs (cont.)

Plan for Growth

- What are the current expected users and how will you scale beyond that?

Manage Costs

- Ensure you account for all costs in the solution as well as shared cost increases.

Azure Architecture Center

- Be aware of the Azure Architecture Center
- Review example scenarios
- Design Patterns
- Reference Architectures
- Data Architecture Guide

Azure Architecture Center



Azure Application Architecture Guide

A guide to designing scalable, resilient, and highly available applications, based on proven practices that we have learned from customer engagements.



Reference Architectures

A set of recommended architectures for Azure. Each architecture includes best practices, prescriptive steps, and a deployable solution.



Microsoft Cloud Adoption Framework for Azure

A process for creating an organization-wide cloud adoption strategy, focusing on policies, governance, and infrastructure.



Build Microservices on Azure

This design guide takes you through the process of designing and building a microservices architecture on Azure. A reference implementation is included.



Azure Data Architecture Guide

A structured approach to designing data-centric solutions on Microsoft Azure.



High Performance Computing (HPC) on Azure

Design guidance and component information for building High Performance Computing (HPC) applications on Azure.



Cloud Best Practices

Best practices for cloud applications, covering aspects such as auto-scaling, caching, data partitioning, API design, and others.

<https://docs.microsoft.com/en-us/azure/architecture/>

Compliance and Security Requirements

Shared Responsibility Model

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: ■ Cloud Customer, ■ Cloud Provider

- 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

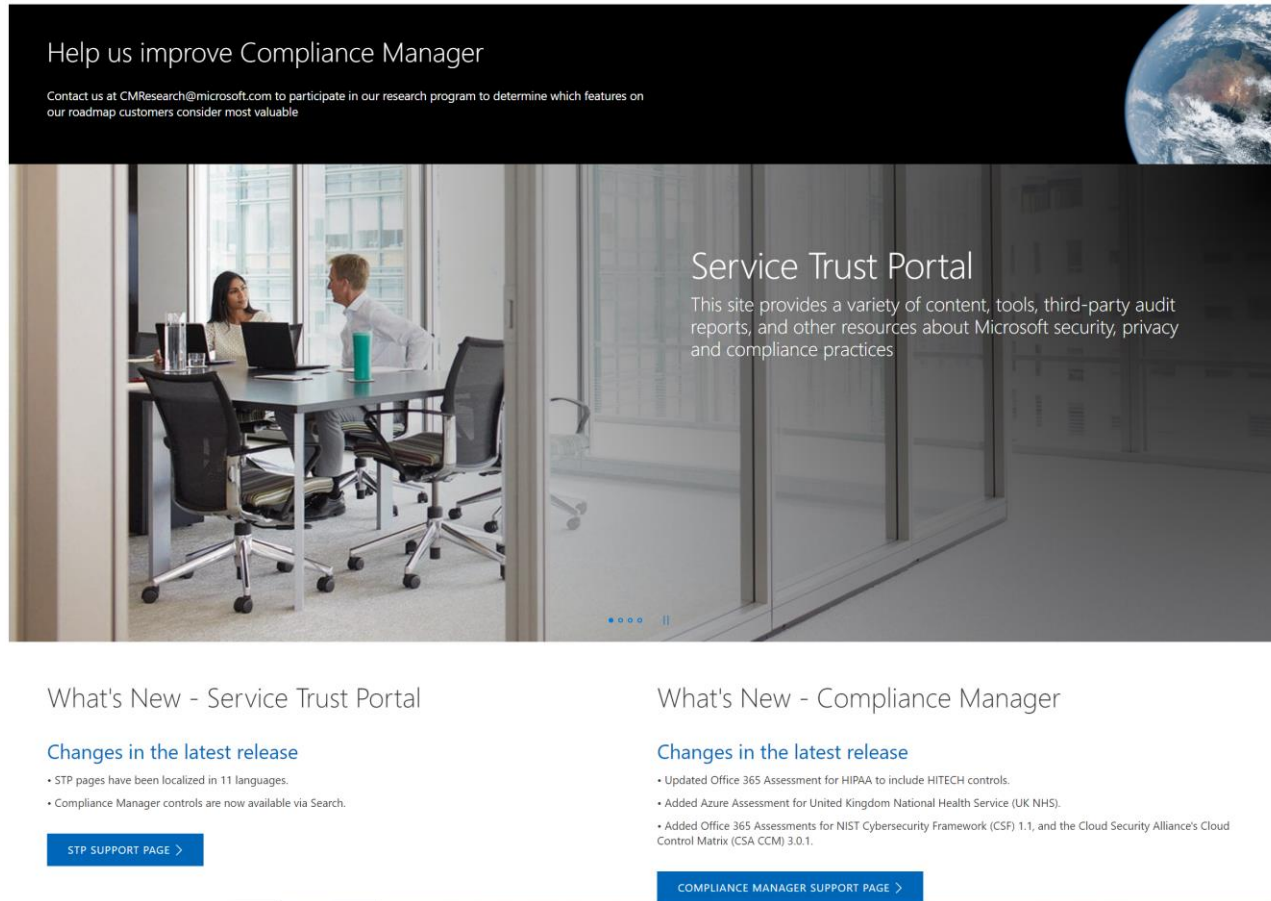
Endpoints

Account

Access
Management

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

Microsoft Trust Center



Help us improve Compliance Manager

Contact us at CMResearch@microsoft.com to participate in our research program to determine which features on our roadmap customers consider most valuable

Service Trust Portal

This site provides a variety of content, tools, third-party audit reports, and other resources about Microsoft security, privacy and compliance practices

What's New - Service Trust Portal

Changes in the latest release

- STP pages have been localized in 11 languages.
- Compliance Manager controls are now available via Search.

[STP SUPPORT PAGE >](#)

What's New - Compliance Manager

Changes in the latest release

- Updated Office 365 Assessment for HIPAA to include HITECH controls.
- Added Azure Assessment for United Kingdom National Health Service (UK NHS).
- Added Office 365 Assessments for NIST Cybersecurity Framework (CSF) 1.1, and the Cloud Security Alliance's Cloud Control Matrix (CSA CCM) 3.0.1.

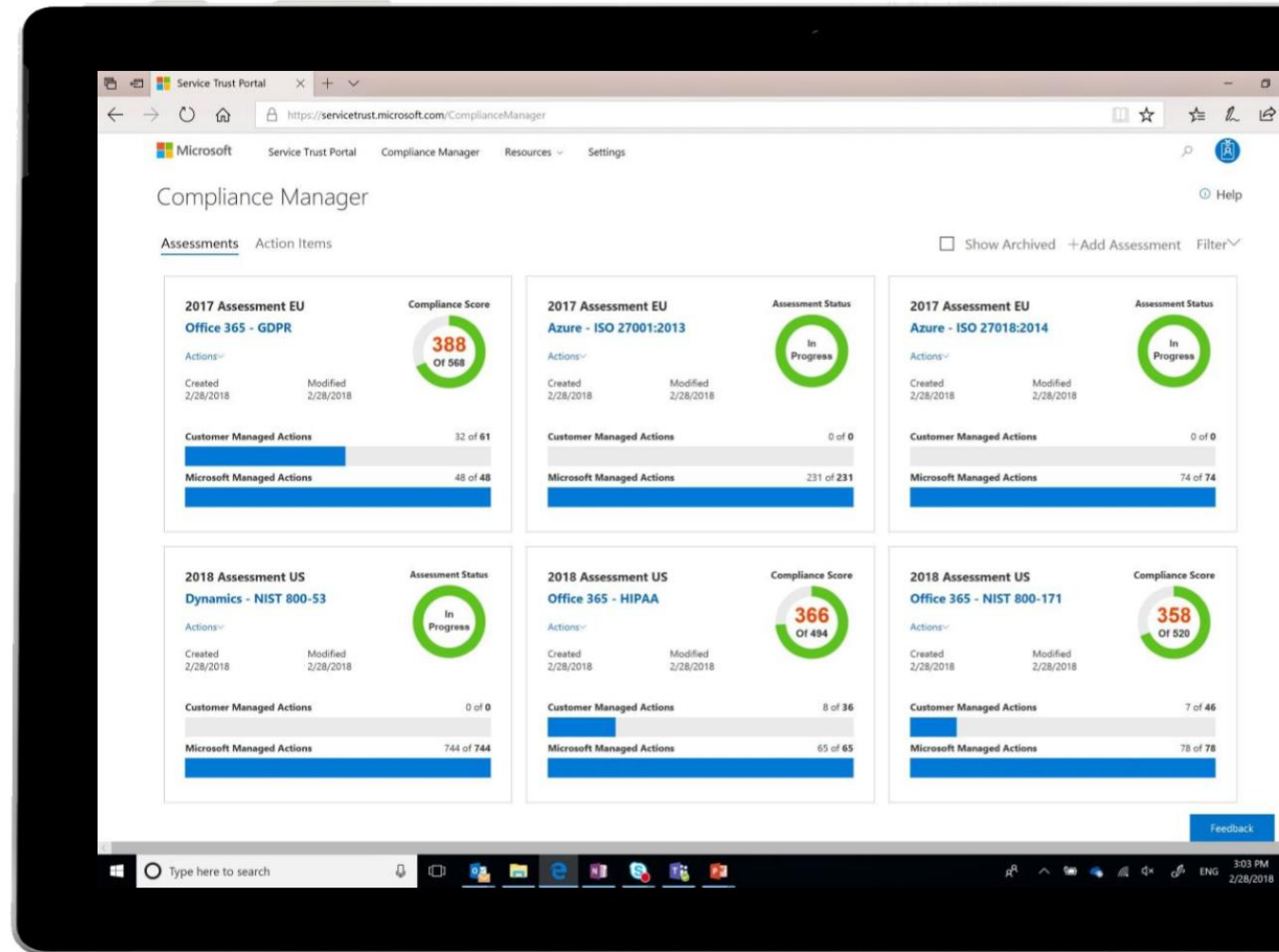
[COMPLIANCE MANAGER SUPPORT PAGE >](#)

- 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

<https://servicetrust.microsoft.com/>

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>

Service Level Agreements (SLAs)

What is an SLA?

“A Service Level Agreement (SLA) is an agreement with the business and application teams on the expected performance and availability of a specific service.”

General SLA Practices

- Define SLA's for each workload

- Dependency mapping

- Make sure to include internal/external dependencies

- Identify single points of failure

- Example – workload requires 99.99% but depends on a service that is only 99.9%

Key Terms

Mean Time To Recovery (MTTR)

- Average time to recover service from an outage

Mean Time Between Failures (MTBF)

- Average time between outages

Recovery Point Objective (RPO)

- Interval of time in which data could be lost during a recovery. E.g. 5 minute RPO means up to 5 minutes of data could be lost.

Recovery Time Objective (RTO)

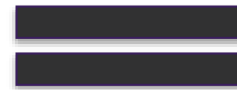
- Time requirement for recovery to be completed in before there is business impact.

Composite SLAs

SQL SLA
99.95%



Web App
99.5%



SLA of 99.94%

Domain Services

Domain Services Overview

Azure AD
(AAD)

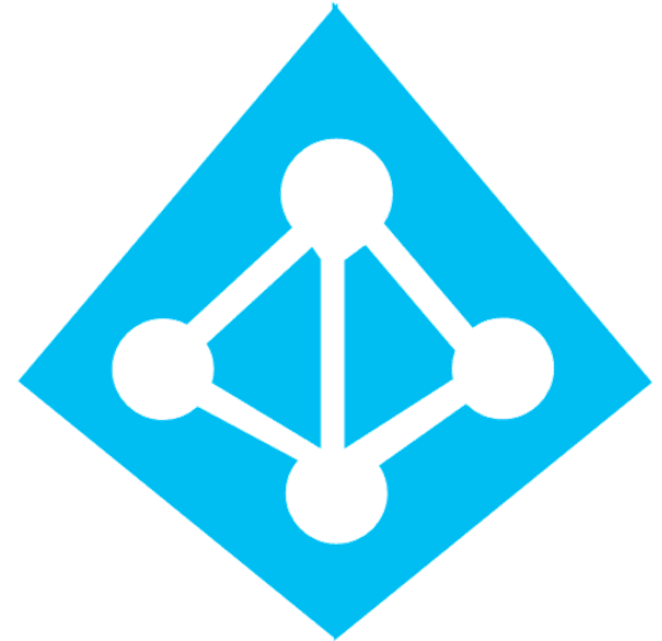
Active Directory
Domain Services
(ADDS)

Azure Active
Directory
Domain Services
(AADDs)

Azure Active Directory

AAD

- Modern AD service built directly for the cloud
- Often the same as O365 directory service
- Can sync with On-premises directory service



Active Directory Domain Services

ADDS

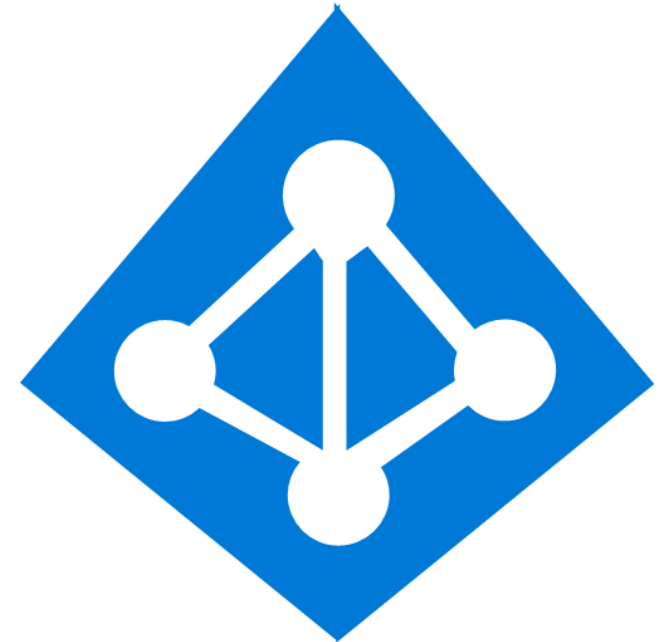
- Legacy Active Directory since Windows 2000
- Traditional Kerberos and LDAP functionality
- Deployed on Windows OS usually on VMs



Azure Active Directory Domain Services

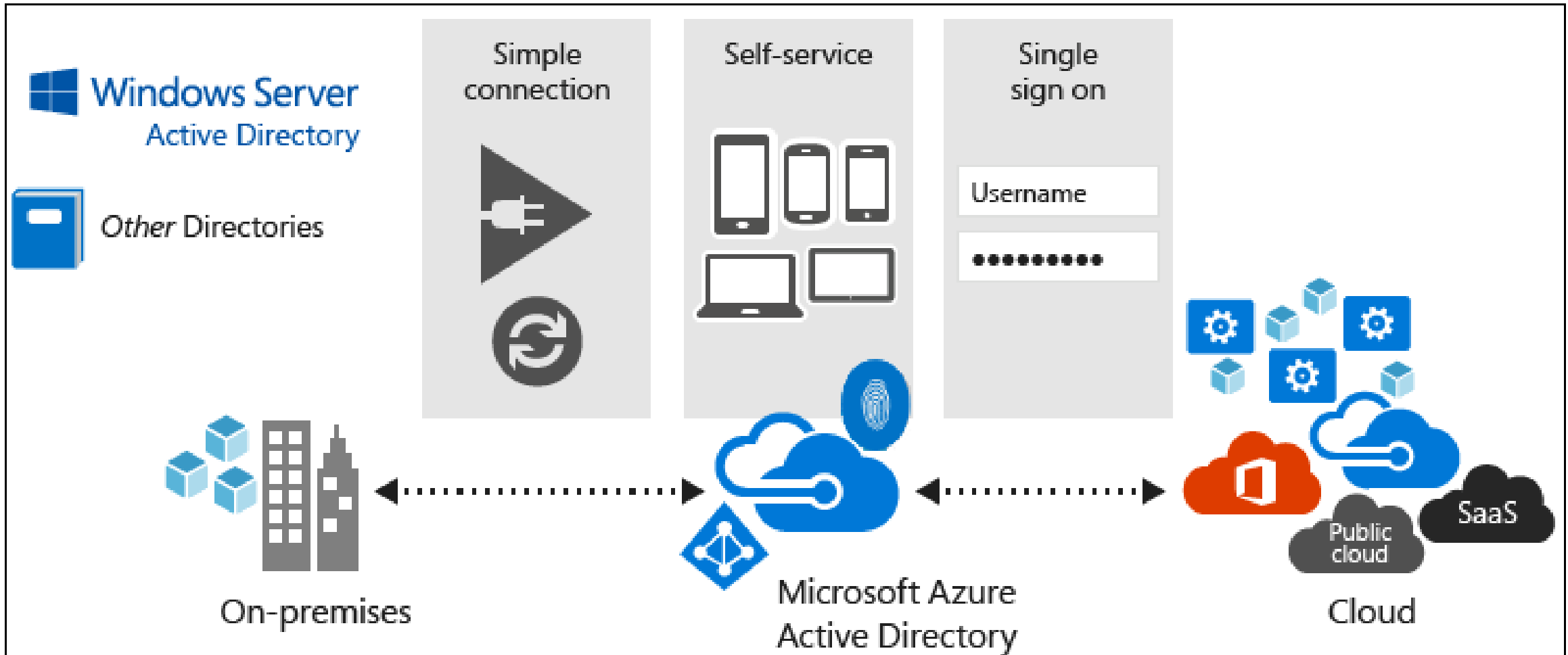
AADDS

- Provides managed domain services
- Allows you to consume domain services without the need to patch and maintain domain controllers on IaaS
- Domain Join, Group Policy, LDAP, Kerberos, NTLM; all supported



Azure AD Overview

Azure AD Overview



<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>

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)

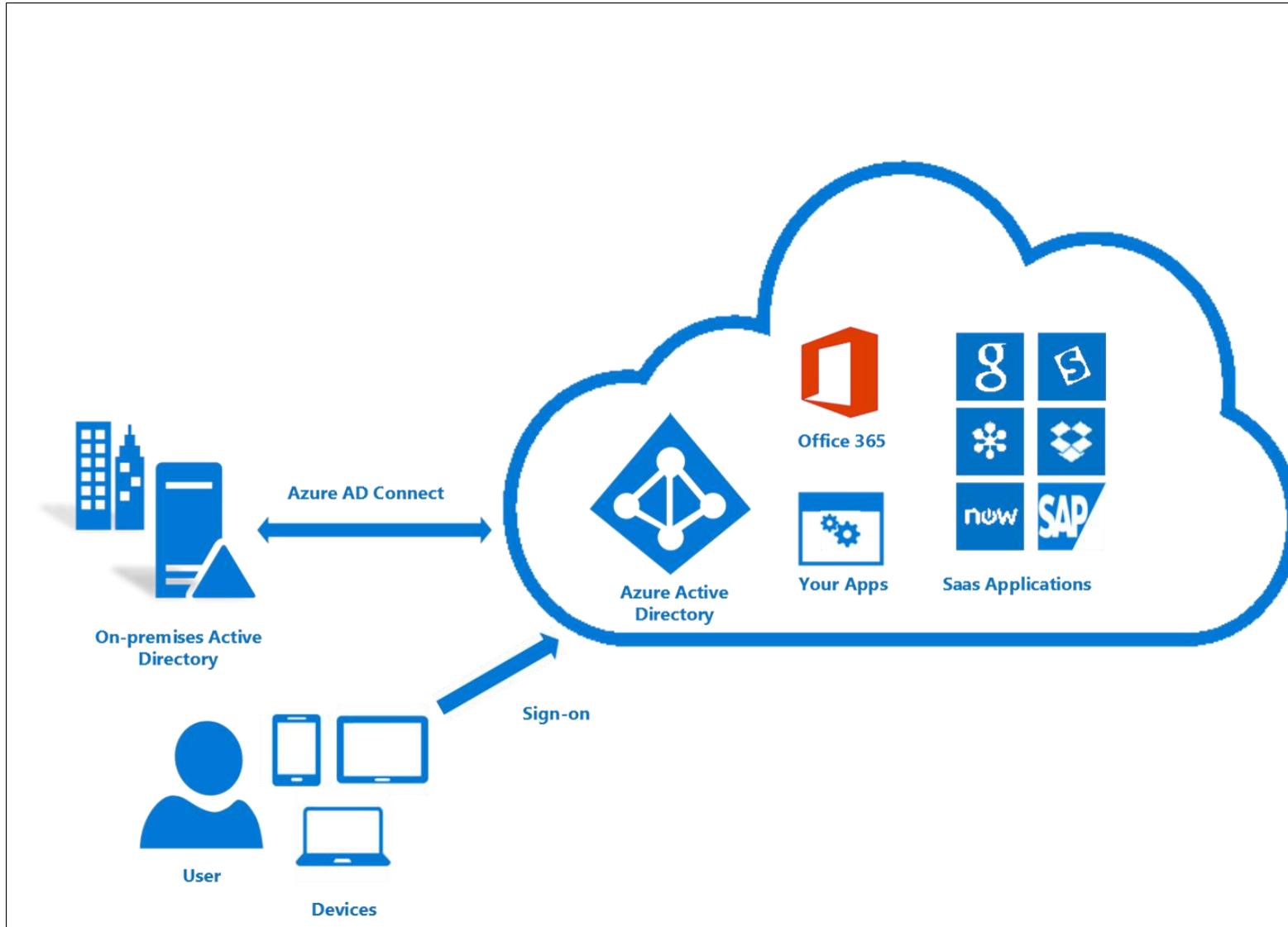
Enhance security with additional factors of authentication.

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

Synchronization
Services

Active Directory
Federation
Services
(optional)

Health
Monitoring

AD Connect Sync Features

Filtering

Password hash
synchronization

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

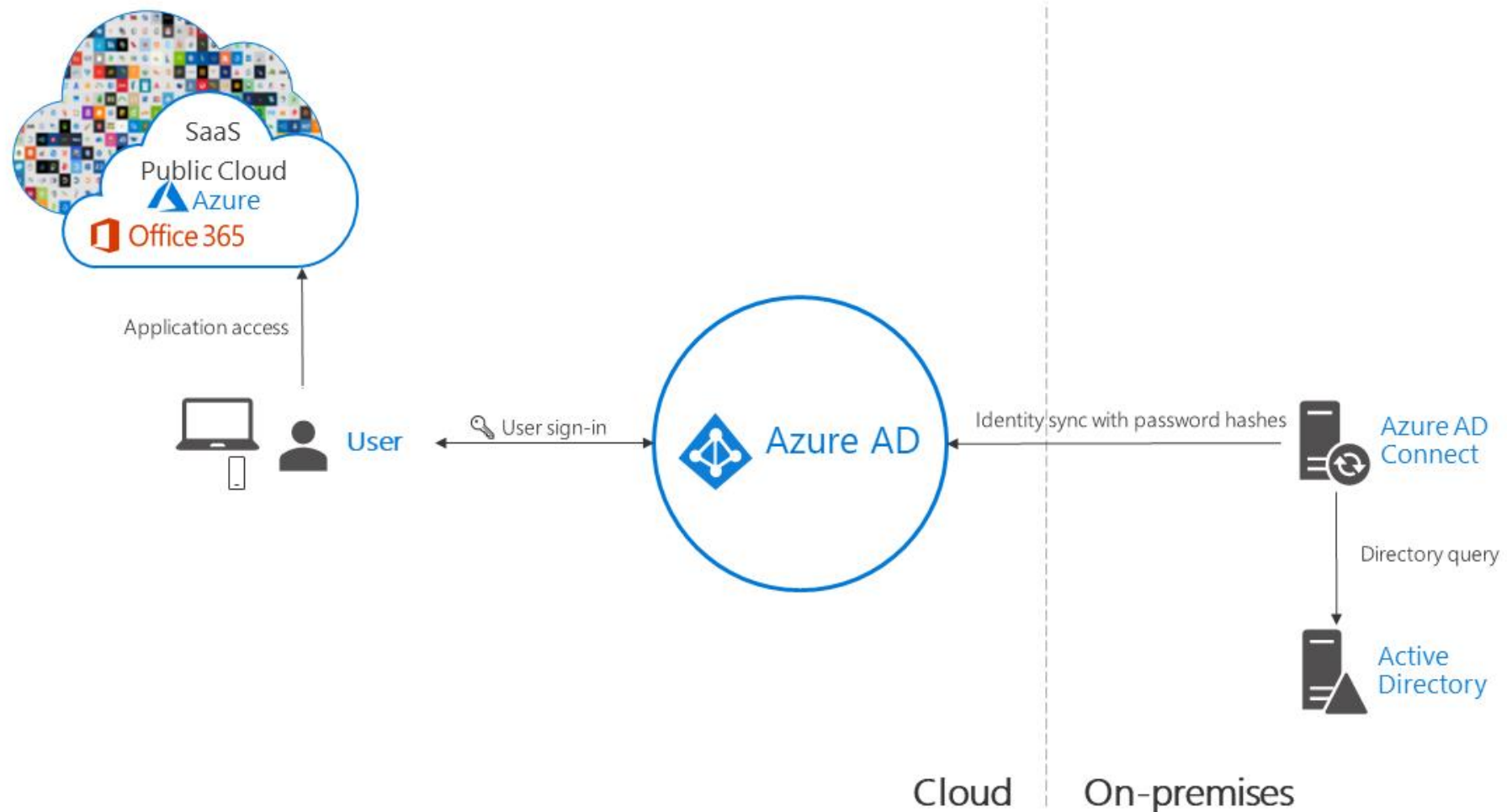
Pass-Through
Authentication +
Seamless SSO

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.

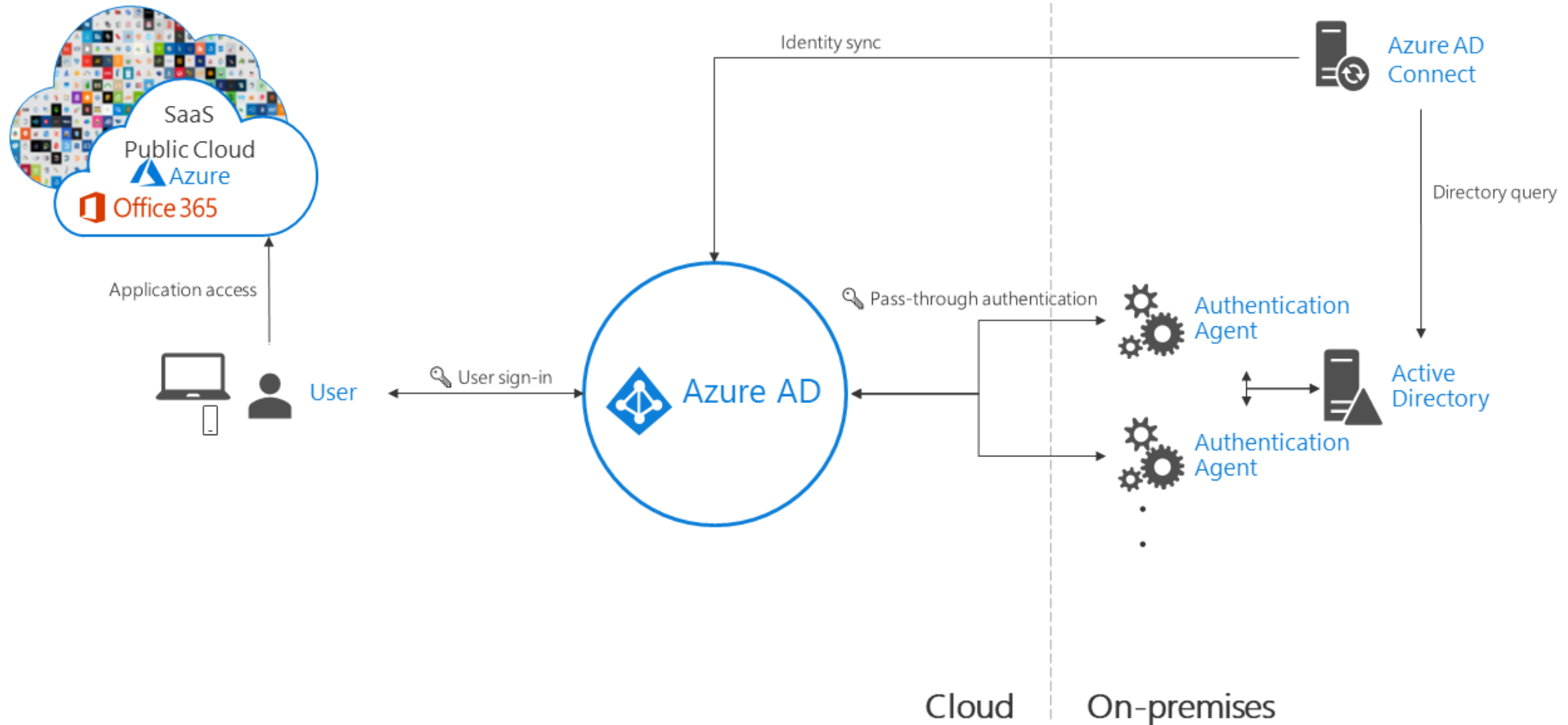
Business Continuity

- 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.

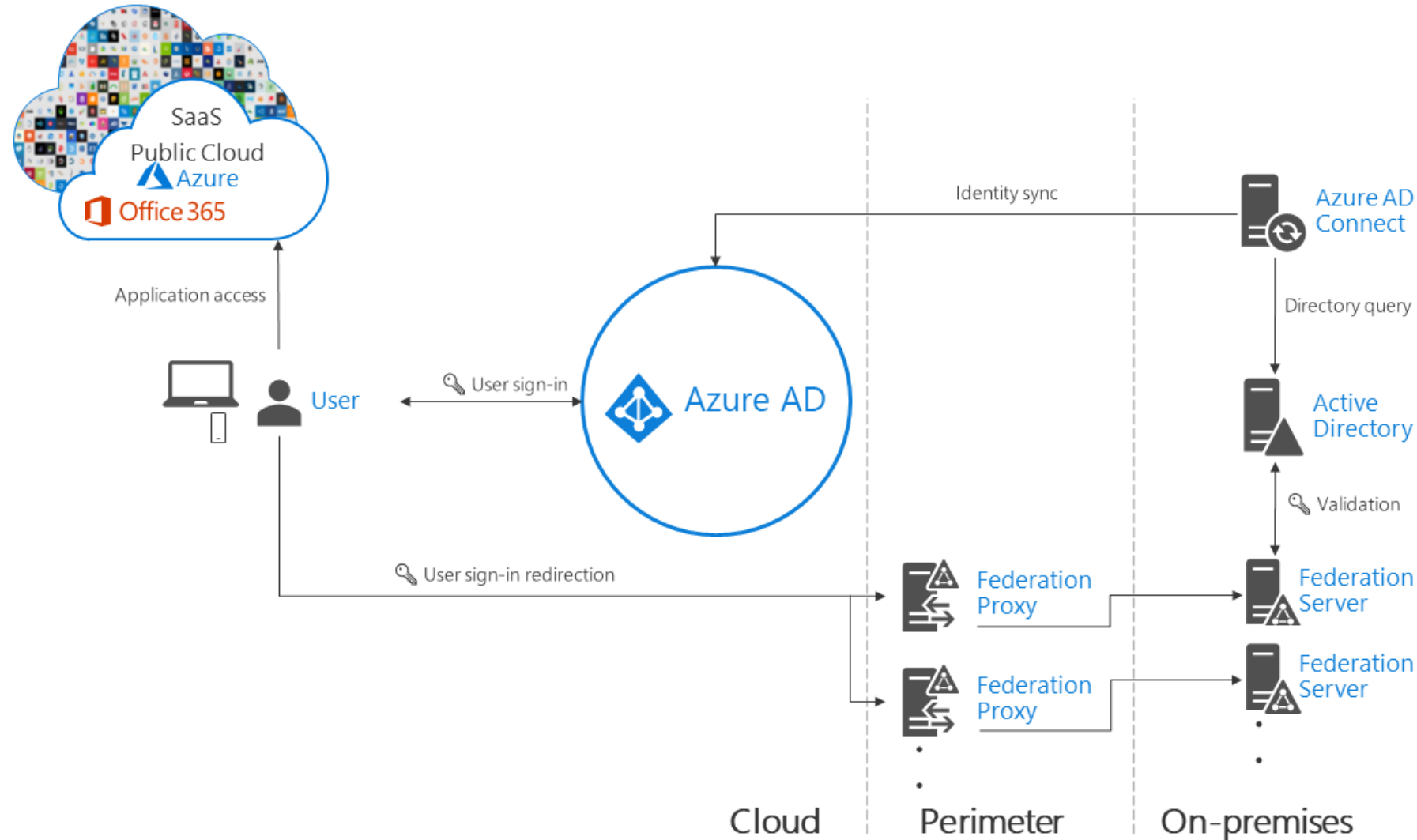
Business Continuity

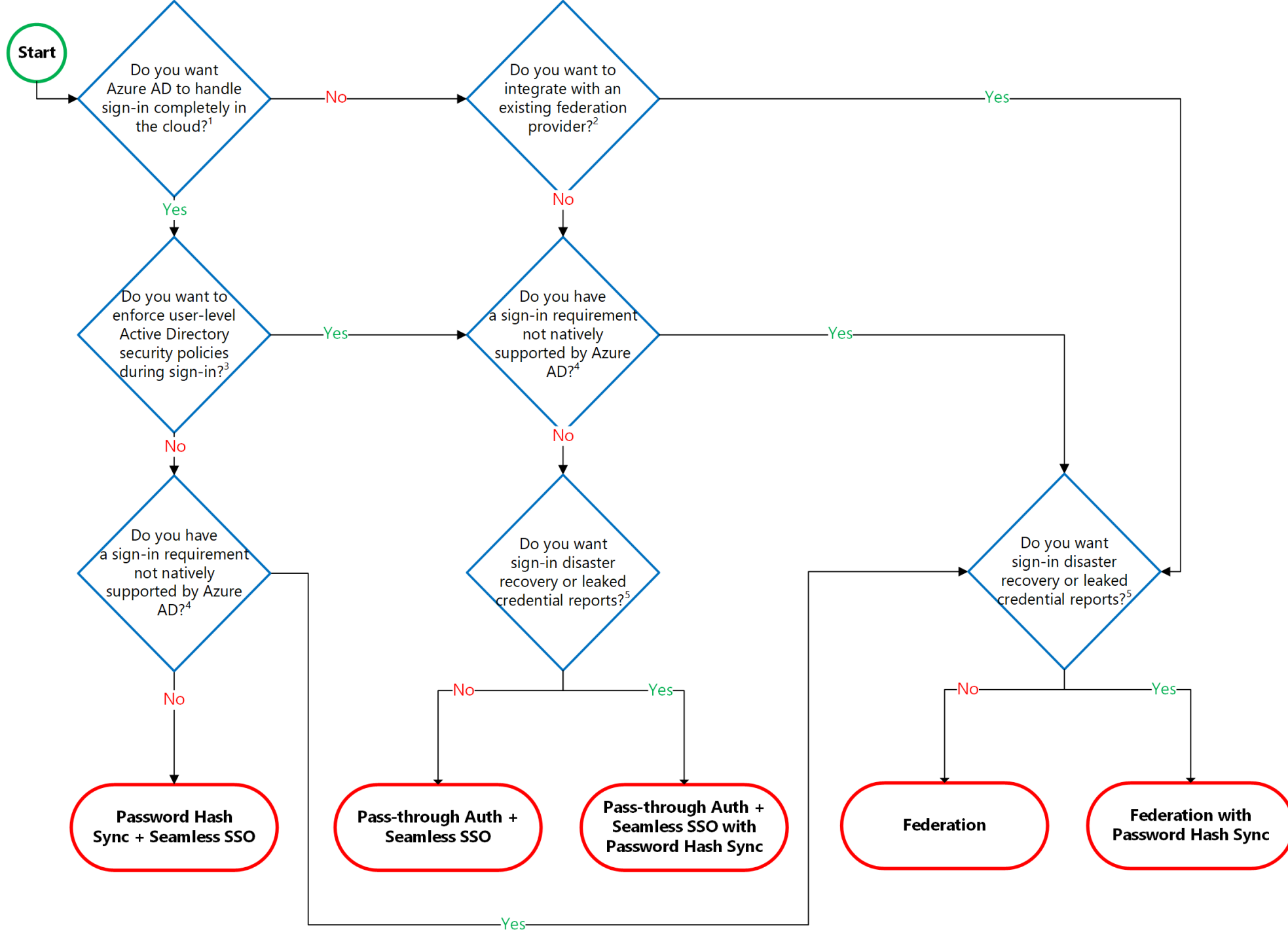
- Recommended to deploy 2 extra pass through agents for redundancy.
- Deploy password hash sync as a backup method.

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.

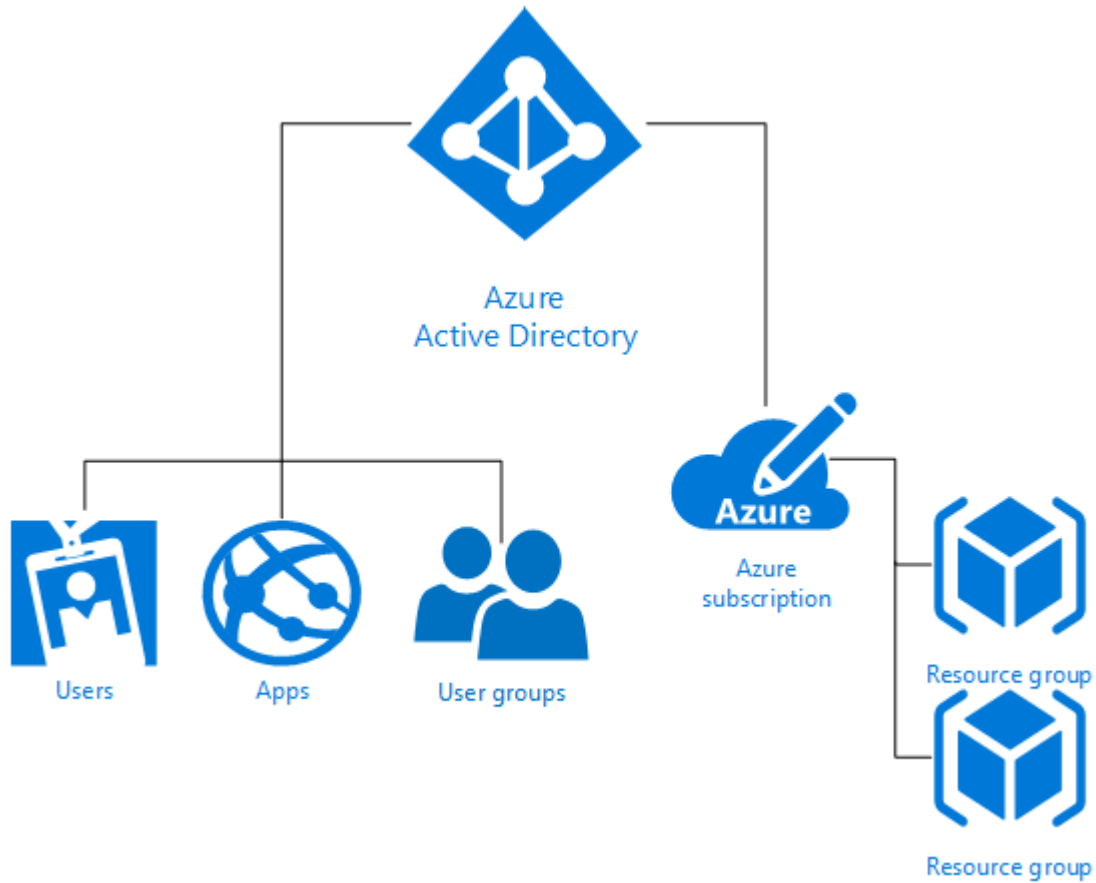
Azure HD Hybrid Identity with Federated authentication





RBAC Overview

RBAC Overview



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

Azure RBAC Built-in Roles

Owner

Full access to all resources, including the right to delegate access to others

Contributor

Can create and manage all types of Azure resources, but cannot grant access to others

Reader

Can view existing Azure resources, but cannot perform any other actions against them

Other Roles

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

Azure RBAC Built-in Roles (continued)

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>

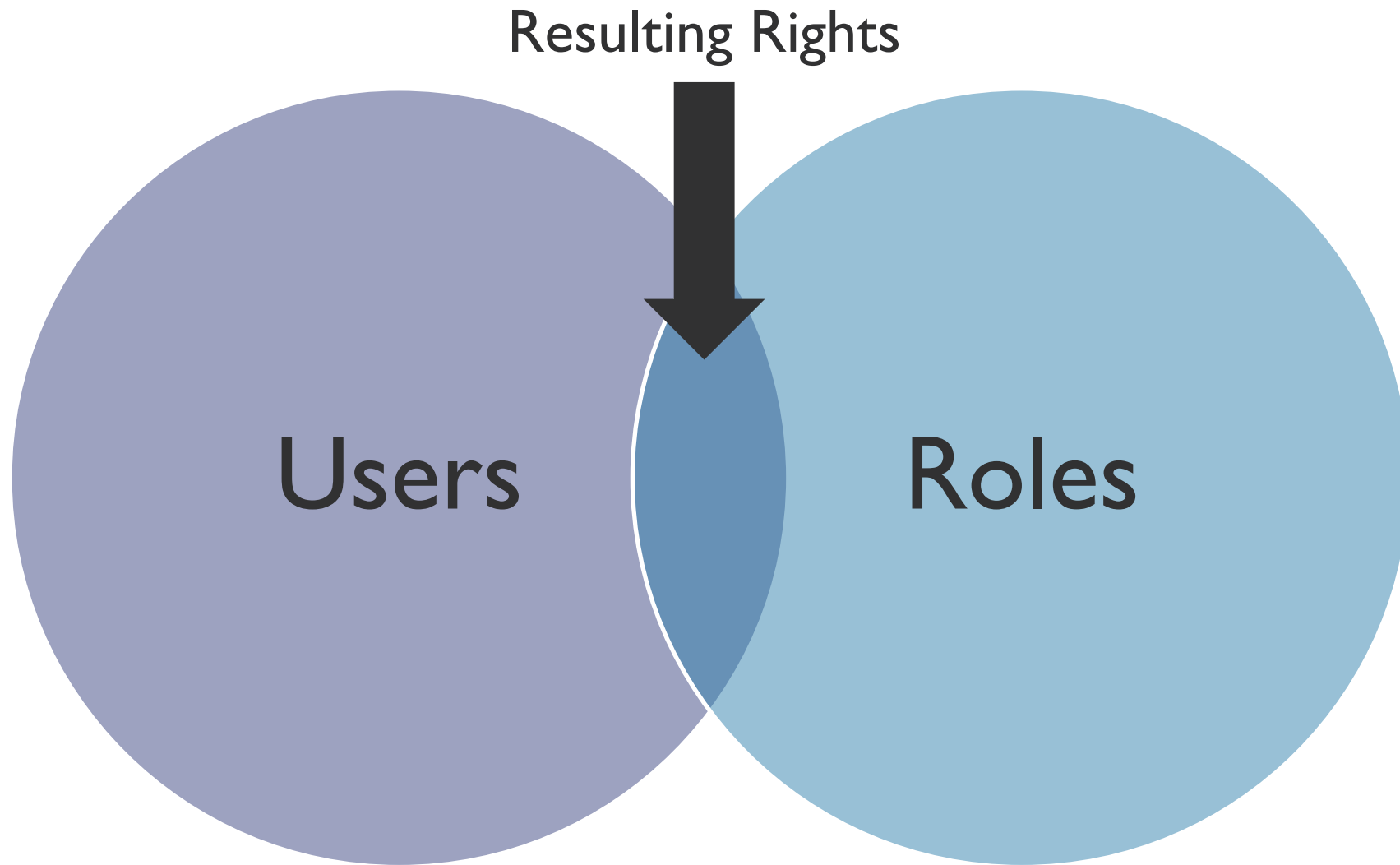
Azure RBAC Built-in Roles (continued)

- 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

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

Each tenant can have to 2000 roles

Use “Actions” and “NotActions”

Assignable scopes:

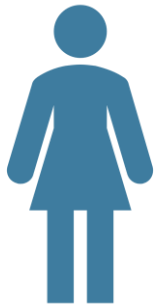
- Subscriptions
- Resource Groups
- Individual Resources

Privileged Identity Management (PIM)

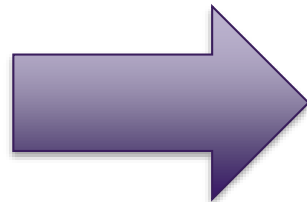
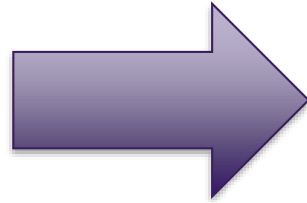
What is Privileged Identity Management (PIM)



Users



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



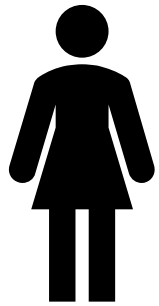
Azure Resources
Azure Active Directory
SaaS Apps
Office 365

Key Features of Azure PIM

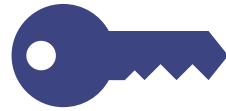
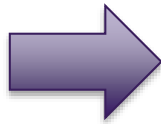
- Visibility into users with privileged access
 - Azure Resources
 - Azure AD
- Enable on-demand administrative access
- View administrator history
- Setup alerts
- Require approvals (via workflows)

PIM Process

Activation Process



User



Additional
authentication
(E.g. MFA)



**ACTIVATED USER
READY TO DO WORK!**



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

PIM Requirements

- Azure AD P2 License

- See: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>

AZExamDemo.onmicrosoft.com

AZExam

Azure AD Free

Sign-ins

To see sign-in data, your organization needs Azure AD Premium P1 or P2.

[Start a free trial](#)



ENTERPRISE MOBILITY + SECURITY E5

Enterprise Mobility + Security E5 is the comprehensive cloud solution to address your consumerization of IT, BYOD, and SaaS challenges. In addition to Azure Active Directory Premium P2 the suite includes Microsoft Intune and Azure Rights Management.

[More information](#)
[Free trial](#)

AZURE AD PREMIUM P2

With Azure Active Directory Premium P2 you can gain access to advanced security features, richer reports and rule based assignments to applications. Your end users will benefit from self-service capabilities and customized branding.

[More information](#)
[Free trial](#)

PIM Roles

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)

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>

Azure Data Services

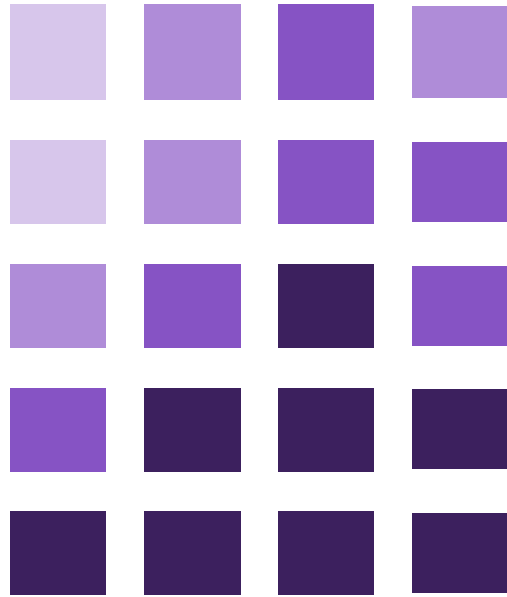
Types of Data

Structured Data

Semi-Structured
Data

Unstructured
Data

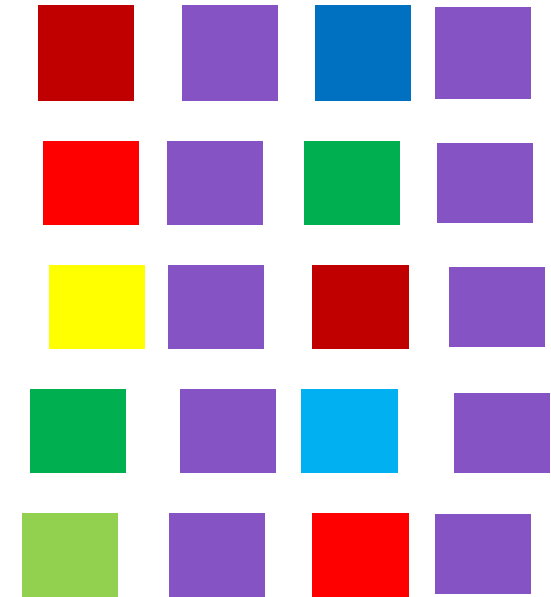
Structured Data



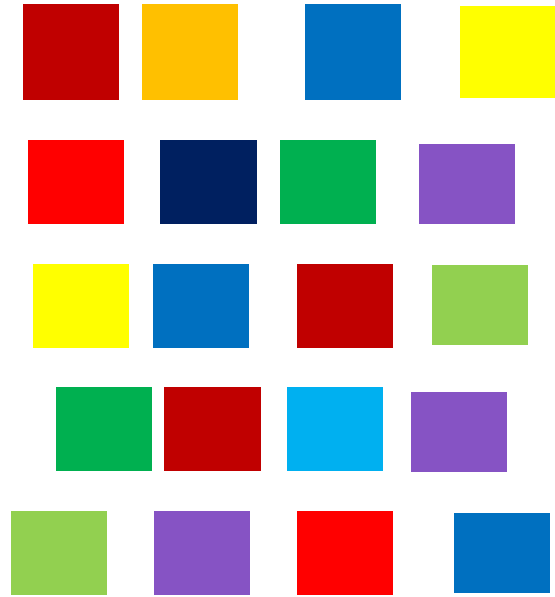
- Adheres to a schema
- All the data has the same field or properties
- Stored in a database table with rows and columns
- Relies on keys to indicate how one row in a table relates to data in another row of another table
- Referred to as “relational data”

Semi-Structured Data

- 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



- 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 SQL Services

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

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

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
<ul style="list-style-type: none">• Small dbs• Single active operation• Dev / Test• Small scale apps• 5 DTU	<ul style="list-style-type: none">• Good option for cloud apps• Multiple operations• Workgroup or web apps• 10-100 DTU	<ul style="list-style-type: none">• 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

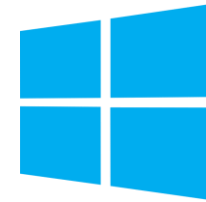
Third-party Databases in Azure – Managed

- 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



Third-party Databases in Azure – Non-managed

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



SQL Pricing Models

vCore Pricing Model

vCore Pricing Model

- Lets you independently scale compute and storage resources
- Match on-premises performance
- Optimize price
- Lets you choose specific generation of hardware

vCore Generations

- **Gen4:** Up to 24 logical CPUs based on Intel E5-2673 v3 (Haswell) 2.4-GHz processors, vCore = 1 PP (physical core), 7 GB per core, attached SSD
- **Gen5:** Up to 80 logical CPUs based on Intel E5-2673 v4 (Broadwell) 2.3-GHz processors, vCore = 1 LP (hyper-thread), 5.1 GB per core, fast eNVM SSD

vCore Pricing Model Tiers

General Purpose

Most business workloads. Offers budget-oriented, balanced, and scalable compute and storage options.

Business Critical

Business applications with high I/O requirements. Offers highest resilience to failures by using several isolated replicas.

Hyperscale

Most business workloads with highly scalable storage and read-scale requirements.

DTU Service Tiers

	Basic	Standard	Premium
Target workload	Development and production	Development and production	Development and production
Uptime SLA	99.99%	99.99%	99.99%
Backup retention	7 days	35 days	35 days
CPU	Low	Low, Medium, High	Medium, High
IO throughput (approximate)	2.5 IOPS per DTU	2.5 IOPS per DTU	48 IOPS per DTU
IO latency (approximate)	5 ms (read), 10 ms (write)	5 ms (read), 10 ms (write)	2 ms (read/write)
Columnstore indexing	N/A	S3 and above	Supported
In-memory OLTP	N/A	N/A	S
Target workload	Development and production	Development and production	Development and production

Single Database DTU and Storage Limits

	Basic	Standard	Premium
Maximum storage size	2 GB	1 TB	4 TB
Maximum DTUs	5	3000	4000

Elastic Pool eDTU, Storage, and Pooled Database Limits

	Basic	Standard	Premium
Maximum storage size per database	2 GB	1 TB	1 TB
Maximum storage size per pool	156 GB	4 TB	4 TB
Maximum eDTUs per database	5	3000	4000
Maximum eDTUs per pool	1600	3000	4000
Maximum number of databases per pool	500	500	100

Single Database DTU and Storage Limits

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-service-tiers-dtu>

SQL Auditing

Auditing for SQL Database and Data Warehouse



- 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

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.



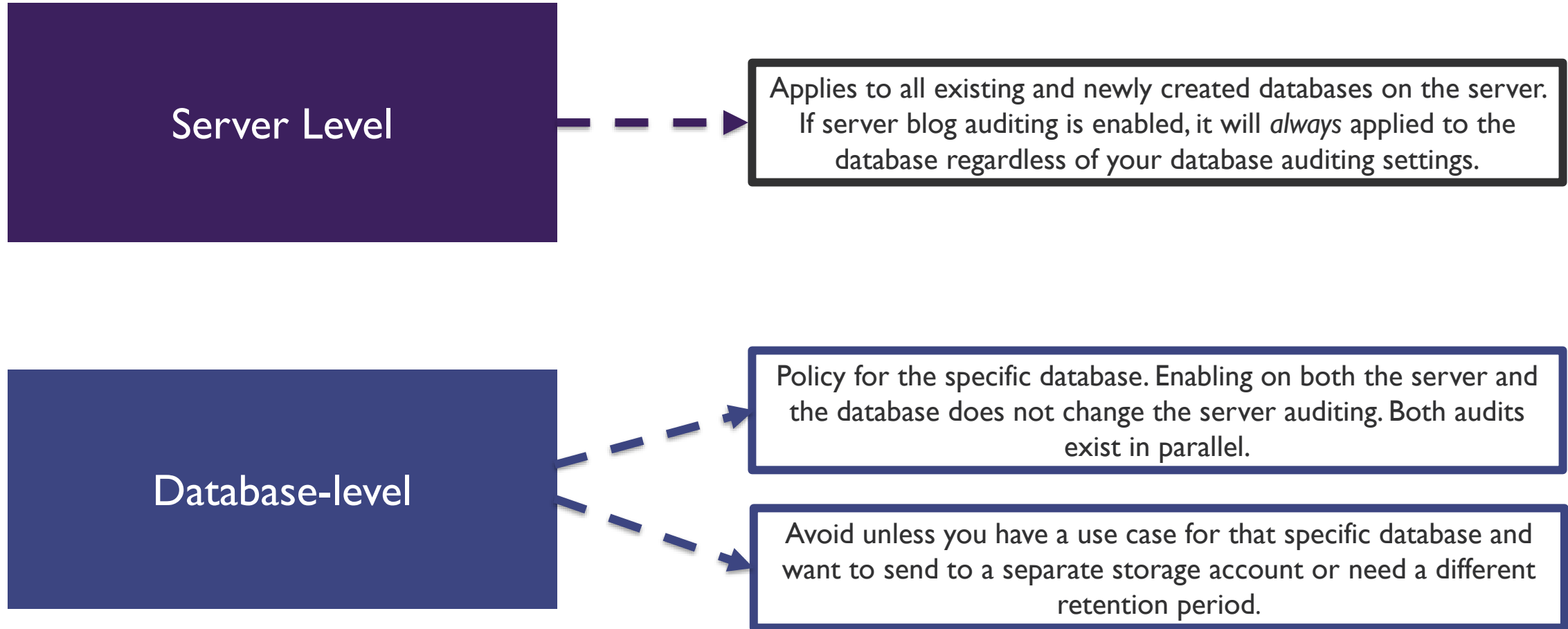
Analyze

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

Azure SQL Database Auditing Overview

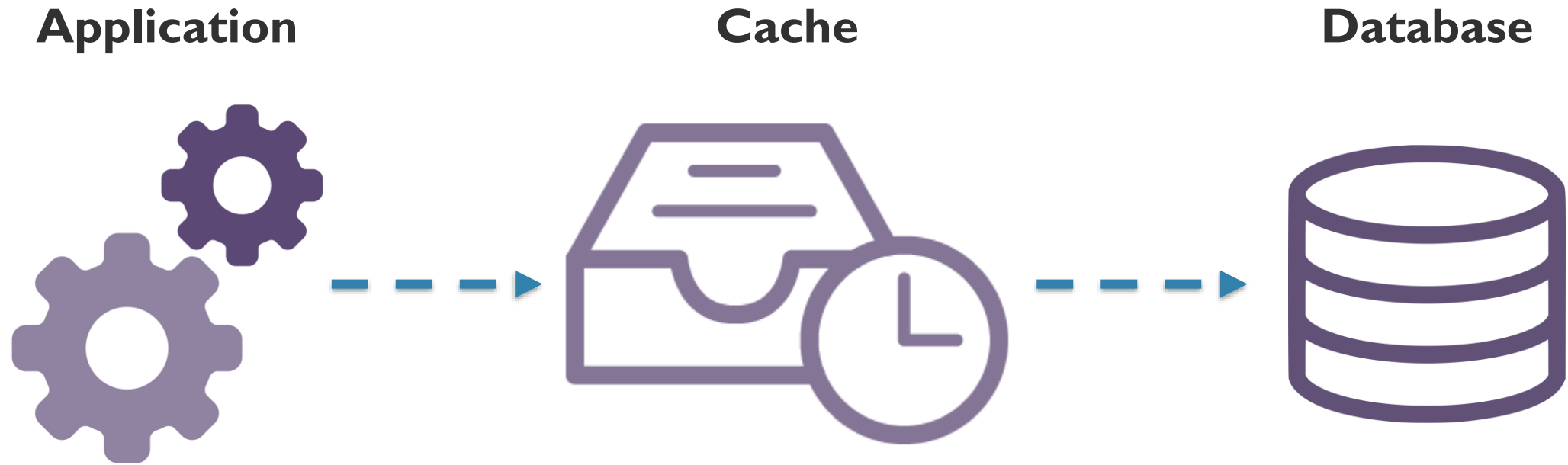
- Audit logs are written to **Append Blobs** in Azure Blob storage on your Azure subscription
- All storage **types (v1, v2, blob) are supported**
- All storage **replication configurations are supported**
- **Premium storage** is currently **not supported**
- **Storage in VNet** is currently **not supported**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

Server-level vs Database-level Auditing Policies



SQL Caching

What is Caching?



Distributed Application Caching

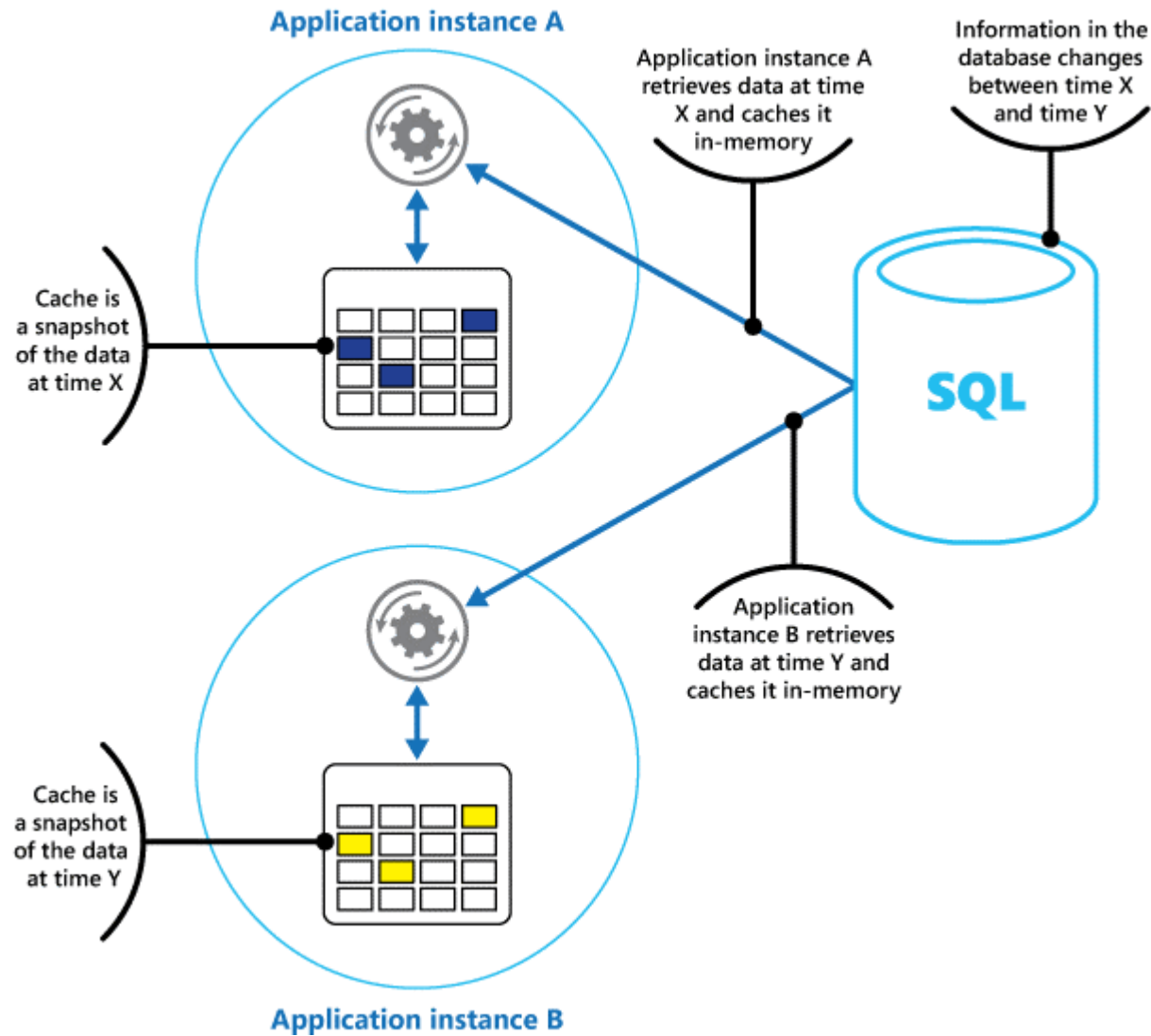
Private Caching

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

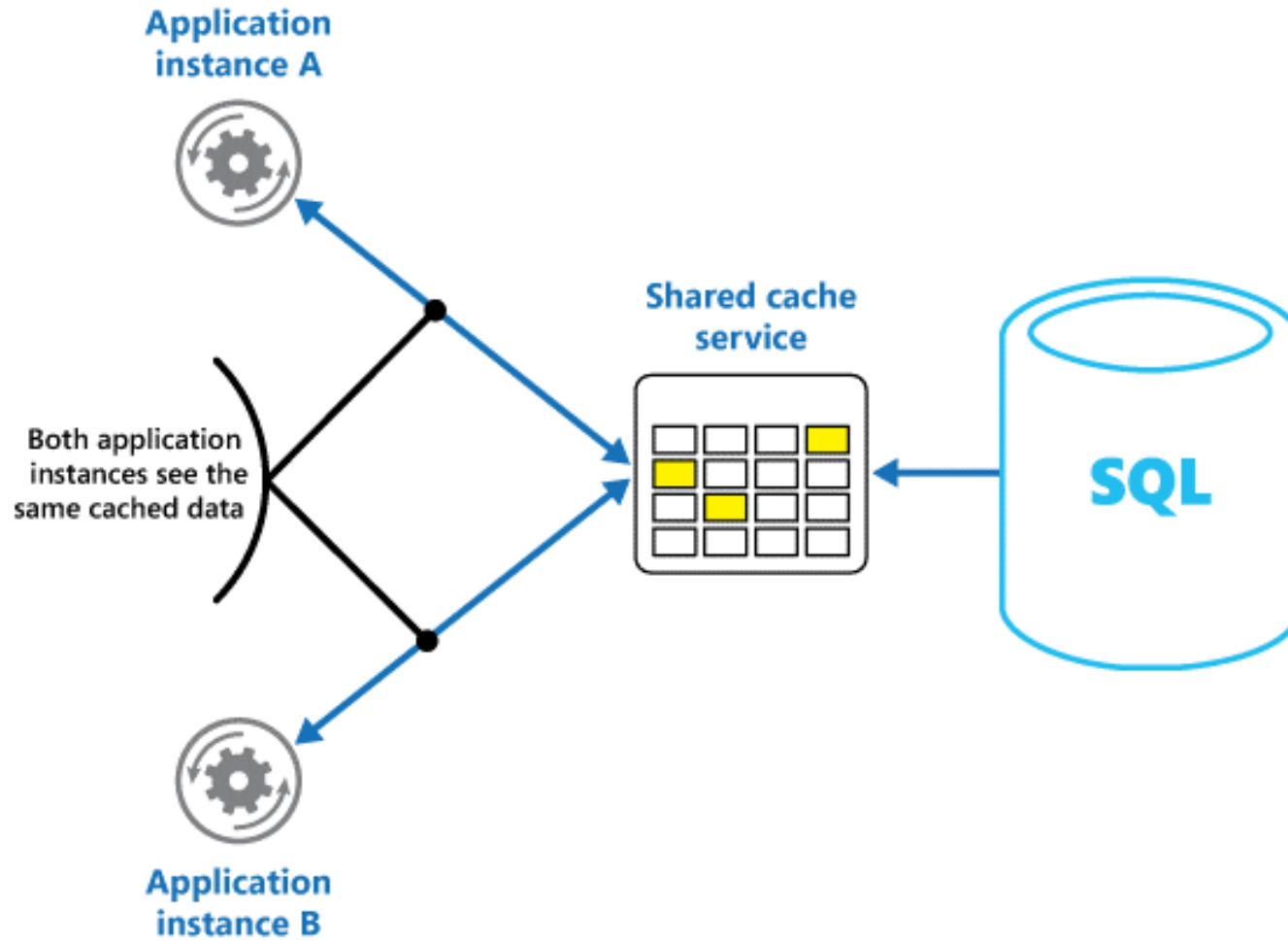
Shared Cache

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

Private Caching



Shared Caching



Caching Considerations

Deciding
WHEN to
cache data

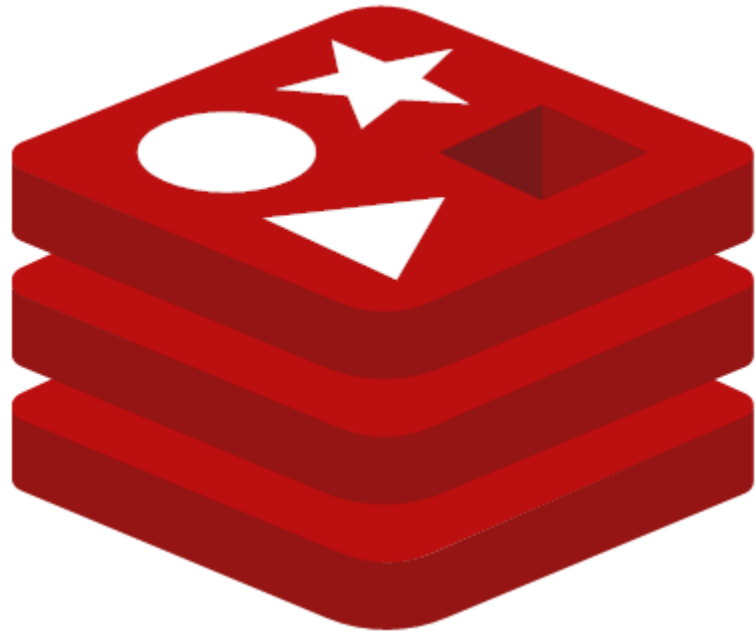
Determine
how to cache
data
effectively

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

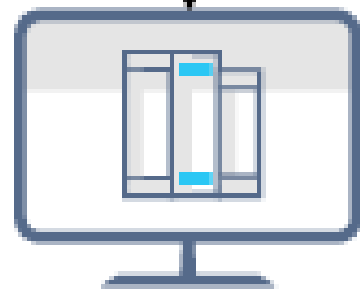
Cosmos DB

Azure Cosmos DB



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

Developer frequently updates the catalog

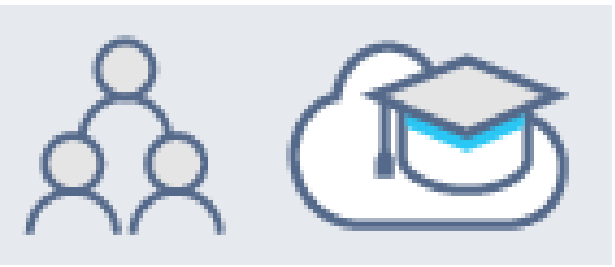


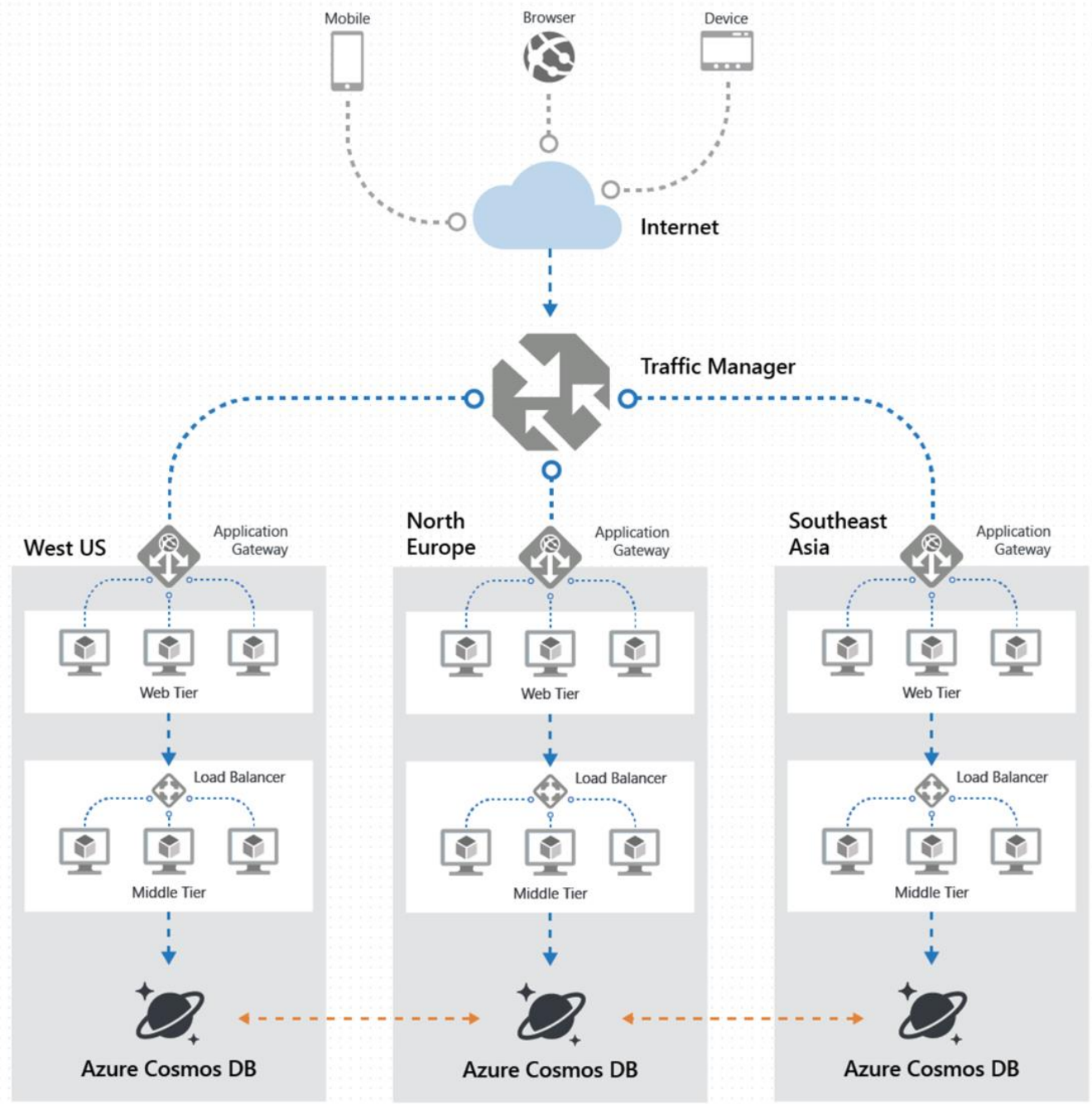
Online course catalog

Azure Cosmos DB database



Global users and training developers





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

Consistency Levels

Strong

Guaranteed write operation only committed and visible on the primary after it has been committed and confirmed by all replicas.

Bounded Staleness

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.

Session

Guarantees that all read and write operations are consistent within a user session.

Consistent Prefix

Ensures changes are read in the order that matches the sequence of the corresponding writes.

Eventual

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

1. Stronger Consistency Level

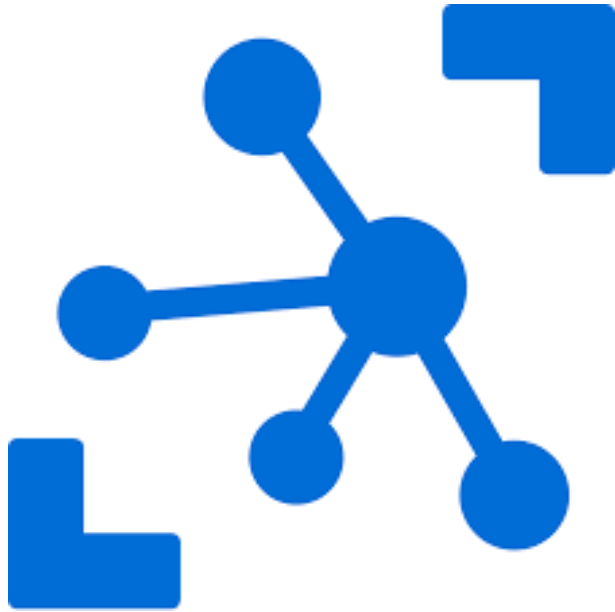
- Ensures documents in replicas do not lag behind the primary
- Recommended for applications that require all replicas to exactly match the primary at any point in time
- Negative affect on the write operations

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

IoT

Azure IoT



- Collection of Microsoft managed cloud services focused on connecting, monitoring and controlling IoT assets
- IoT solutions are made up of 1 or more IoT devices and 1 or more back end services running in the cloud.

IoT Device Examples



- Water sensors for farming
- Pressure sensors on a remote oil pump
- Temperature and humidity sensors in an air-conditioning unit

IoT Services in Azure

IoT Central

SaaS solution to help you connect and manage your devices

IoT Hub

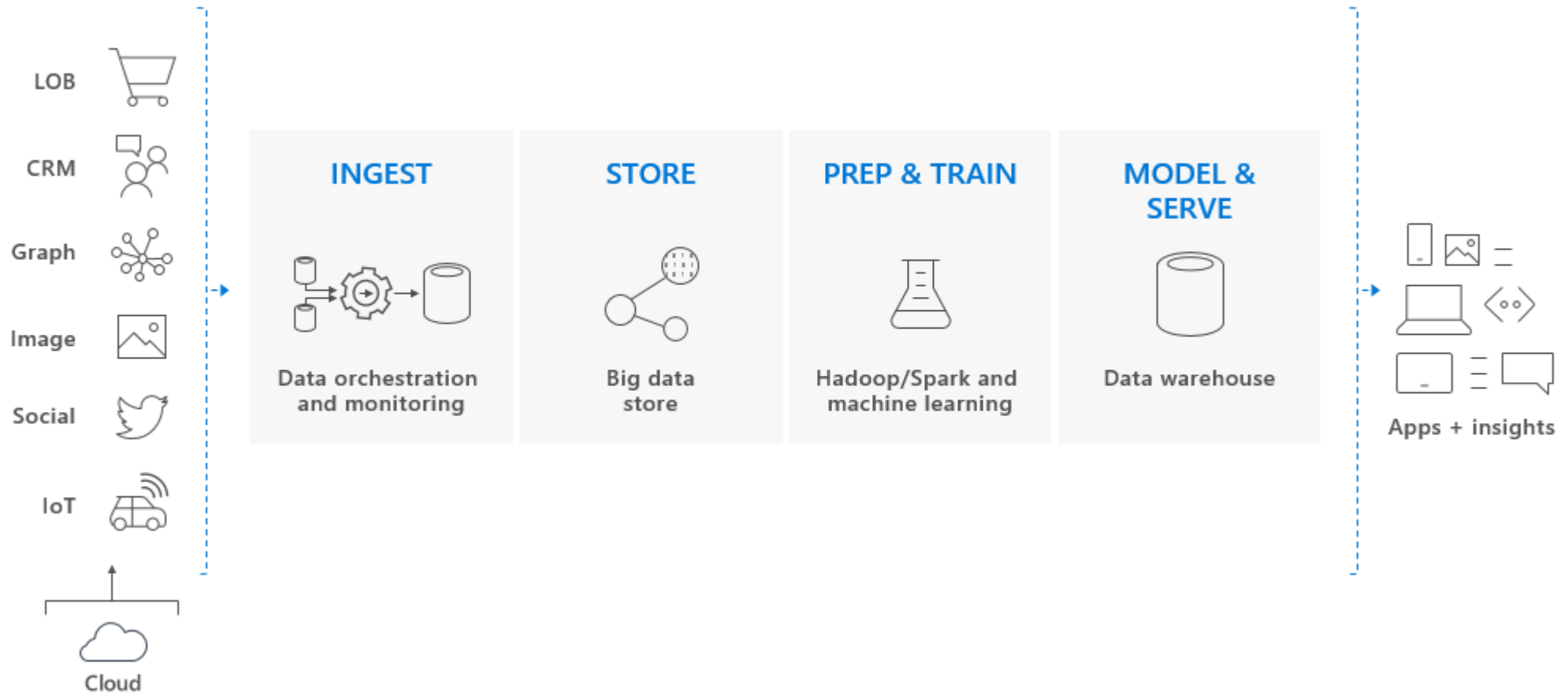
Underlying service needed to facilitate messages between your IoT application and devices

IoT Solution Accelerators

Complete ready to deploy solutions that implement common IoT scenarios

Big Data Solutions

Big Data Solution



SQL Data Warehouse



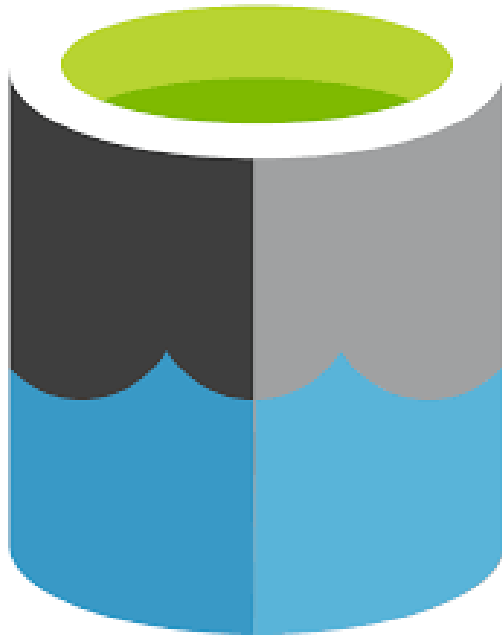
- Key component of a Big Data solution
- Cloud based Enterprise Data Warehouse (EDW) that uses Massive Parallel Processing (MPP) to run complex queries across petabytes of data.
- Stores data in relational tables reducing storage costs and improves performance

HD Insight



- Fully managed open-source analytics service for enterprises
- Use the most popular frameworks like Hadoop, Spark, Hive etc.
- Scenarios:
 - Batch Processing (ETL)
 - Data Warehousing

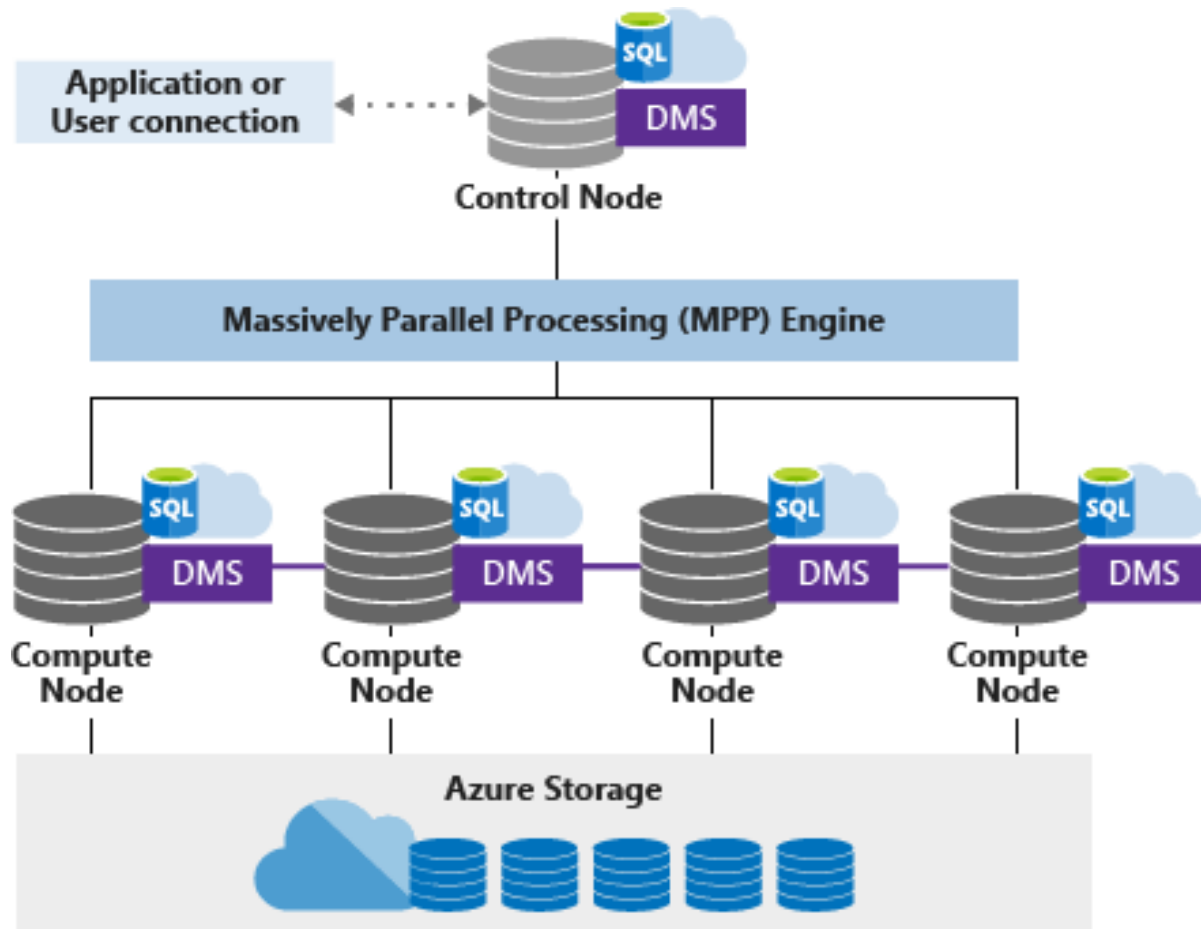
Data Lake Analytics



- On-Demand job service that simplifies big data
- Pay only for your job when it is running
- You write queries to transform your data and extract insights

SQL DW Architecture

SQL DW Architecture



Control Node

Compute Node

DMS – Data Movement Service

Azure Storage

Data Storage and Integration Options

Data Integration with Azure Data Factory



- Manage exact-transform-load (ETL) and data integration service
- Facilitates data-drive workflows (pipelines) that carry out tasks:
 - Connect and collect
 - Transform and enrich
 - Publish
 - Monitor

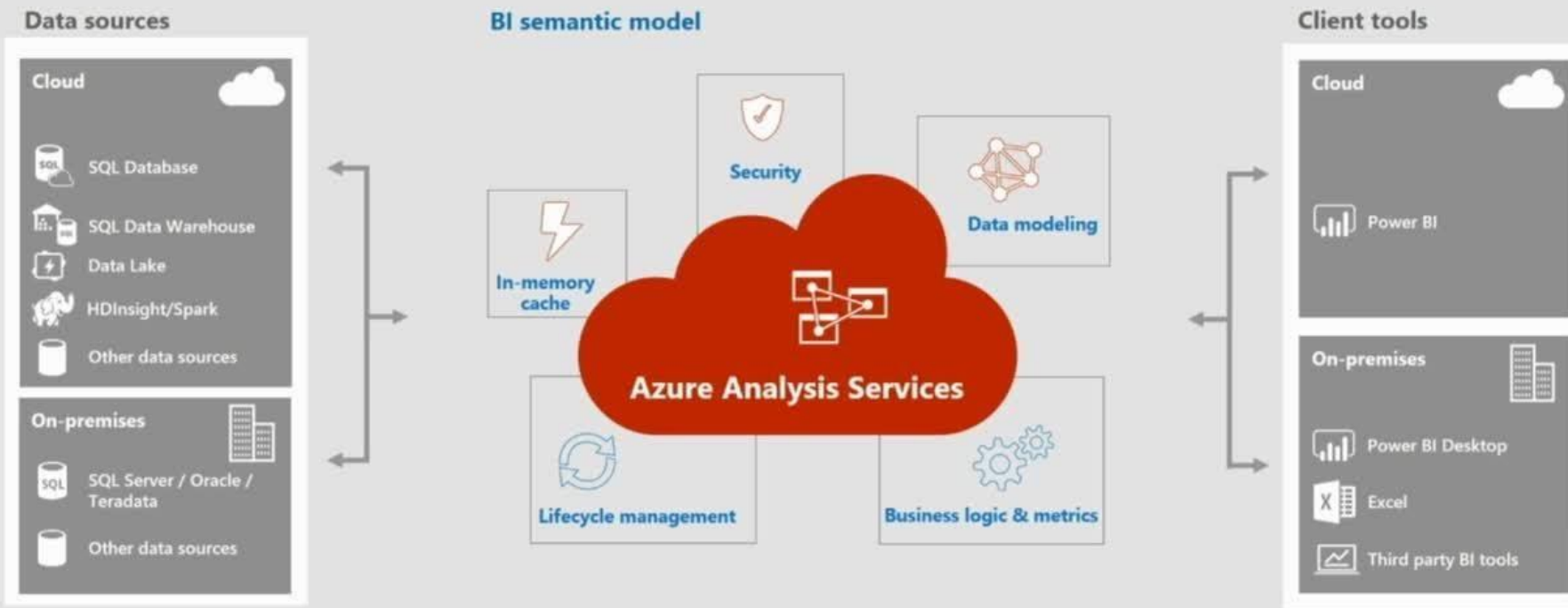
Data Integration with Azure Data Factory



Data Analysis Options

Azure Analysis Services

Azure Analysis Services is based on SQL Server technology



Database Choices

Database Choices

IF YOU WANT...	USE THIS
A globally distributed multi-model database, with support for NoSQL choices, with industry-leading performance and SLAs	Azure Cosmos DB
A fully managed relational database that provisions quickly, scales on the fly, and includes built-in intelligence and security	SQL Database
A fully managed, scalable MySQL relational database with high availability and security built in at no extra cost	Azure Database for MySQL
A fully managed, scalable PostgreSQL relational database with high availability and security built in at no extra cost	Azure Database for PostgreSQL
To host enterprise SQL Server apps in the cloud	SQL Server on Virtual Machines

Database Choices

IF YOU WANT...	USE THIS
A fully managed, elastic data warehouse with security at every level of scale at no extra cost	SQL Data Warehouse
Help migrating your databases to the cloud with no application code changes	Azure Database Migration Service
High throughput and consistent low-latency data access to power fast, scalable applications	Azure Cache for Redis
A NoSQL key-value store for rapid development using massive semi-structured datasets	Table storage
Fast and highly scalable data exploration service	Azure Data Explorer
A fully managed, scalable MariaDB relational database with high availability and security built in at no extra cost	Azure Database for MariaDB

Azure Storage Services

Azure Blob Storage



- Unstructured storage for storing objects
- Store images, video, and files of any type
- Use cases:
 - Streaming video and images direct to user
 - Backup/DR of data
 - Archiving

SMB File Storage – Azure File Services

Benefits

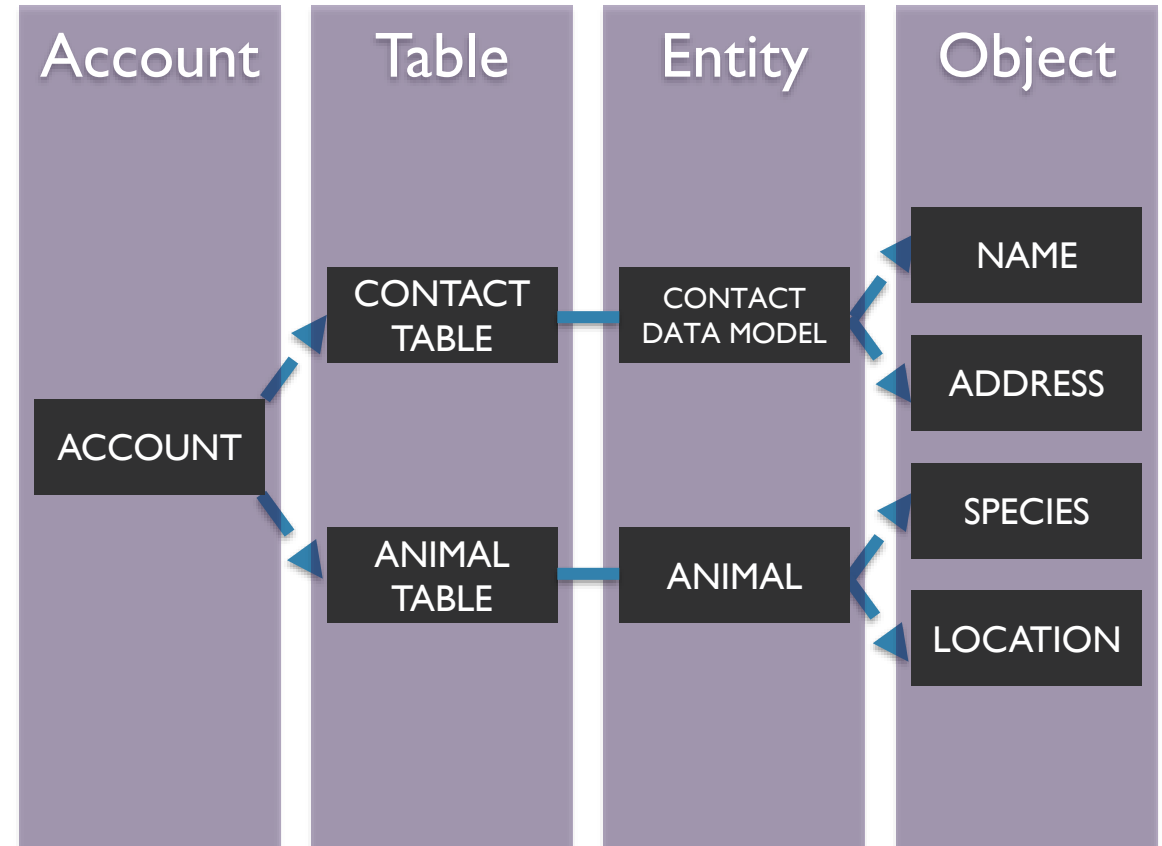
- Easy way to create file shares
- Supports SMB 2.1 (unsecured) and 3.0 (secured)
- Mount on Windows, Linux, or Mac
- Azure File Sync can be utilized to sync file servers on-premises with Azure Files



Azure Table Storage

Table Storage

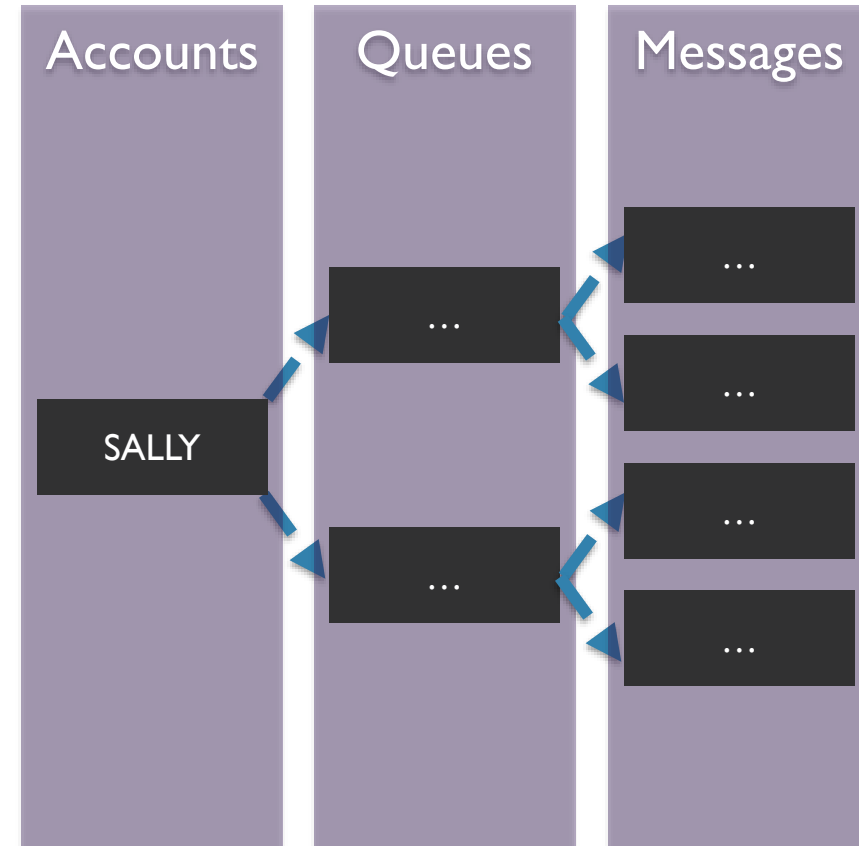
- A NoSQL key-value store
- Schemaless design
- Structured or Unstructured Data
- Access using the Odata protocol and LINQ queries
WCF Data Service .NET Libraries



Azure Queue Storage

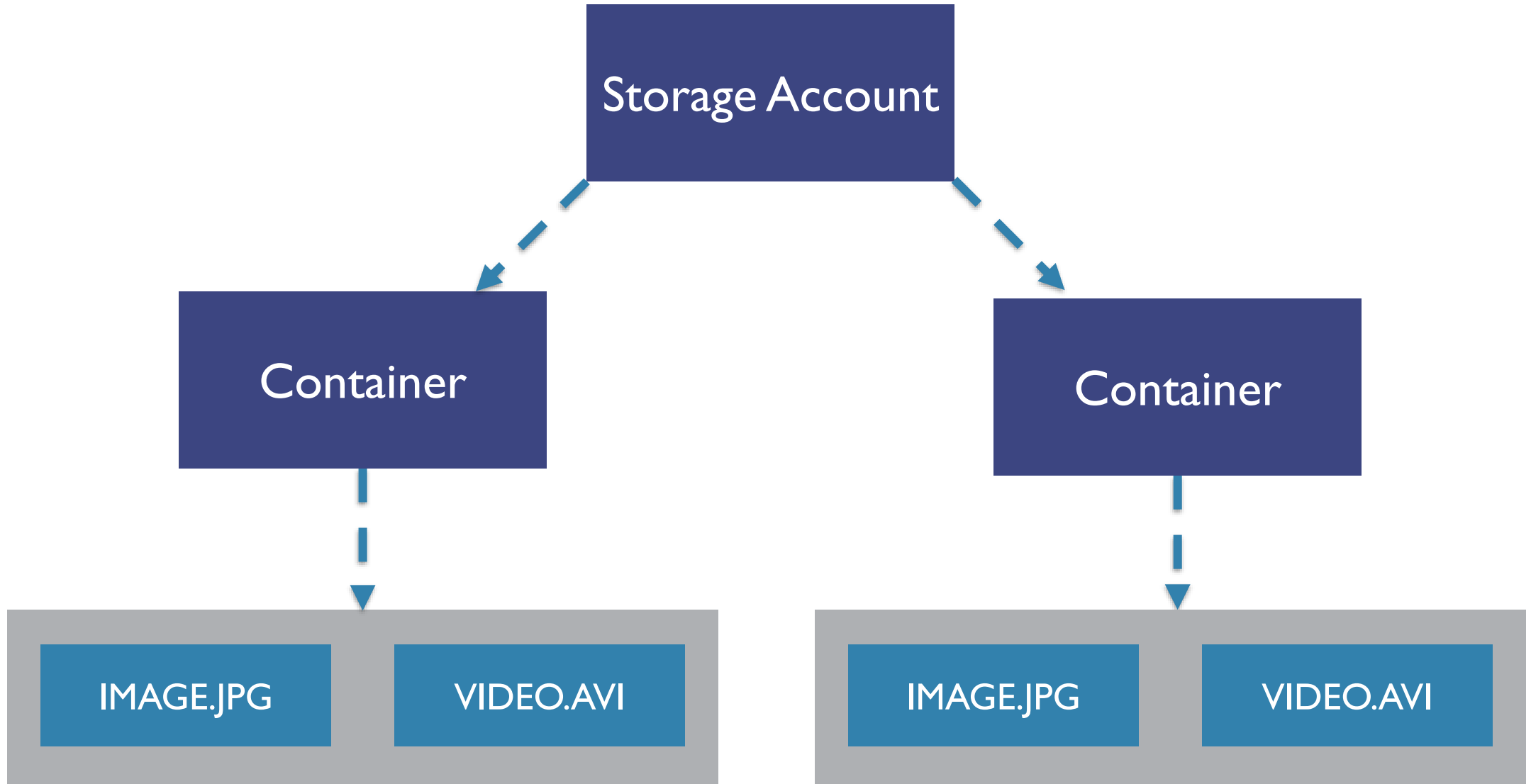
Queue Storage

- 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



Storage Account Overview

Azure Blob Storage Overview



Storage Account Types

General Purpose
v1
(GPV1)

Blob Account

General Purpose
v2
(GPV2)

Block Blobs vs. Page Blobs

Block Blob

- Ideal for storing text or binary files
- A single block blob can contain up to 50,000 blocks of up to 100 MB each, for a total size of 4.75 TB
- Append blobs are optimized for append operations (e.g. logging)

Page Blob

- Efficient for read/write operations
- Used by Azure VMs
- Up to 8 TB in size

Storage Tiers

Hot

- Higher storage costs
- Lower access costs

Cold

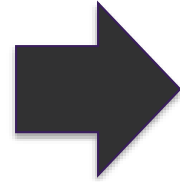
- Lower storage costs
- Higher access costs
- Intended for data that will remain cool for 30 days or more

Archive

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

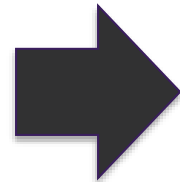
Choosing Between Blobs, Files, and Disks

Blobs



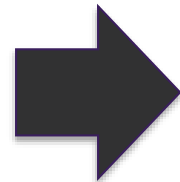
- Access application data from anywhere
- Large amount of objects to store, images, videos etc.

Files



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

Disks



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

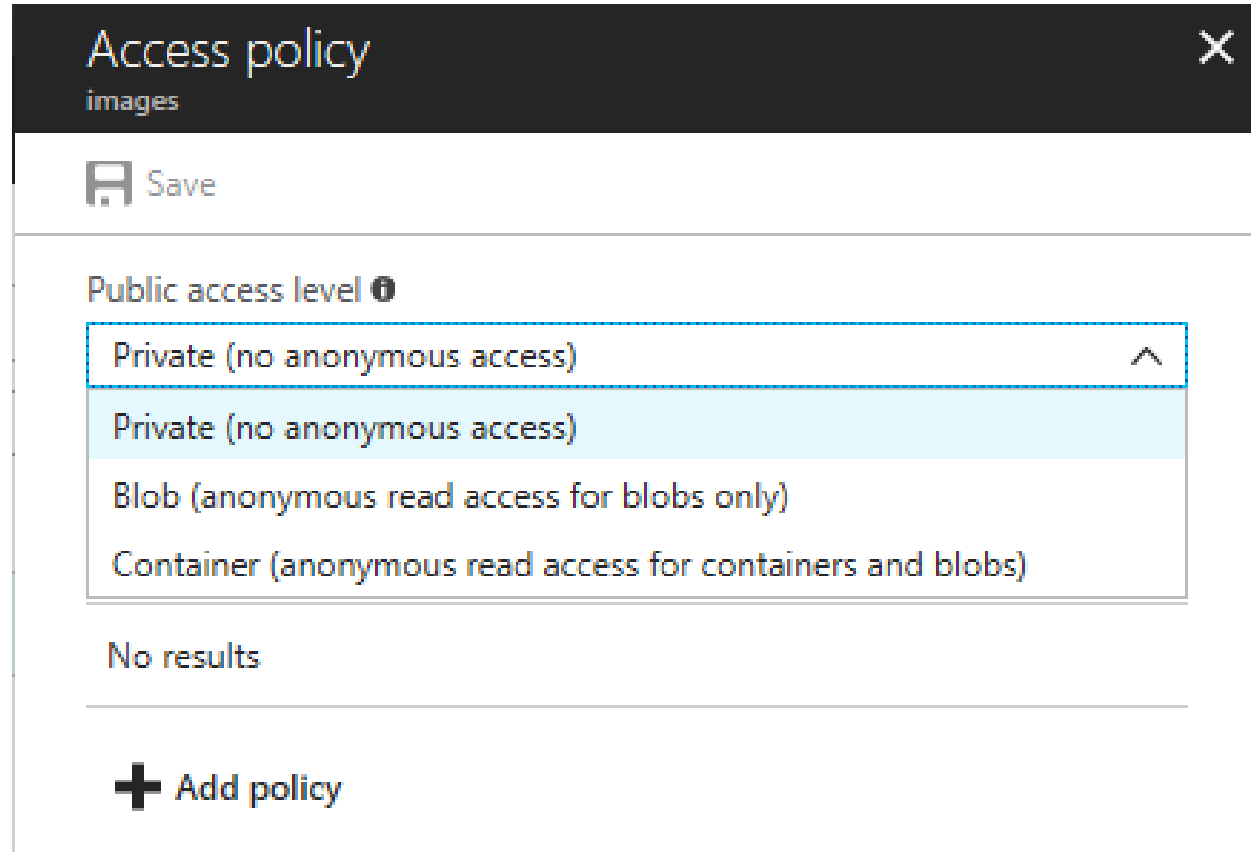
Manage Permissions

Manage Access: Container Permissions

Private
(No Anonymous Access)

Blob
(Anonymous read access for
blobs only)

Container
(Anonymous read access for
containers and blobs)



The screenshot shows the 'Access policy' dialog for a storage container named 'images'. At the top, there is a 'Save' button with a floppy disk icon. Below that, the 'Public access level' is displayed with an information icon. A dropdown menu is open, showing four options: 'Private (no anonymous access)' (selected and highlighted in light blue), 'Private (no anonymous access)', 'Blob (anonymous read access for blobs only)', and 'Container (anonymous read access for containers and blobs)'. Below the dropdown, the text 'No results' is visible. At the bottom, there is a '+ Add policy' button.

Managing Access: SAS Overview

Shared Access Signature (SAS)

- It is a query string that we add on to the URL of a storage resource.
- The string informs Azure what access should be granted.

Account SAS Tokens

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

Service SAS Tokens

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

Encrypted

- Utilizes hash-based message authentication

SAS Breakdown

Storage Resource URI

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

SAS Token

?sv=2017-07-29&ss=bfqt&srt=sco&sp=rwdlacup&se=2018-02-24T01:21:26Z&st=2018-02-23T17:21:26Z&spr=https&sig=dctAWsi39LncBNCIZRn%2FQMjMMA5CPByLzagfsF7MVYc%3D

SAS Breakdown (continued)

- <https://salsdemo.blob.core.windows.net/images/image.jpg>
- sv=2017-07-29
- ss=bfqt
- srt=sco
- sp=rwdlacup
- se=2018-02-24T01:21:26Z&st=2018-02-23T17:21:26Z
- spr=https
- sig=dctAWsi39LncBNCIZRn%2FQMjMMA5CPByLzagfsF7MVYc%3D

The Blob

Storage Service Version

Signed Services

Signed Resource Types

Signed Permission

Signed Expiry & Start

Signed Protocol

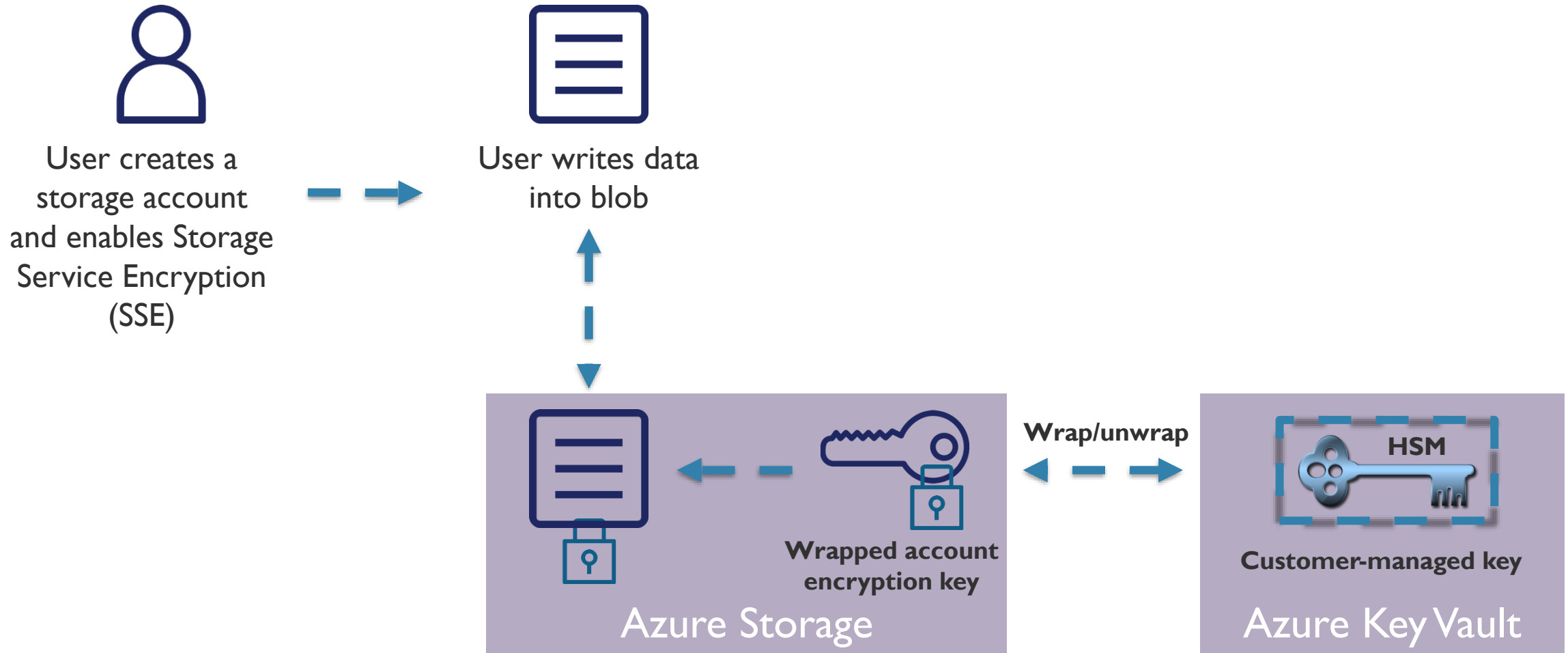
Signature

Stored Access Policies

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

Storage Keys

Encryption Keys and Key Vault



Custom Domains

Custom Domains

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

Custom Domain Mapping

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

1. Your domain

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

2. The "asverify" subdomain

- Such as asverify.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.

Business Continuity and Recovery Overview

DR Considerations

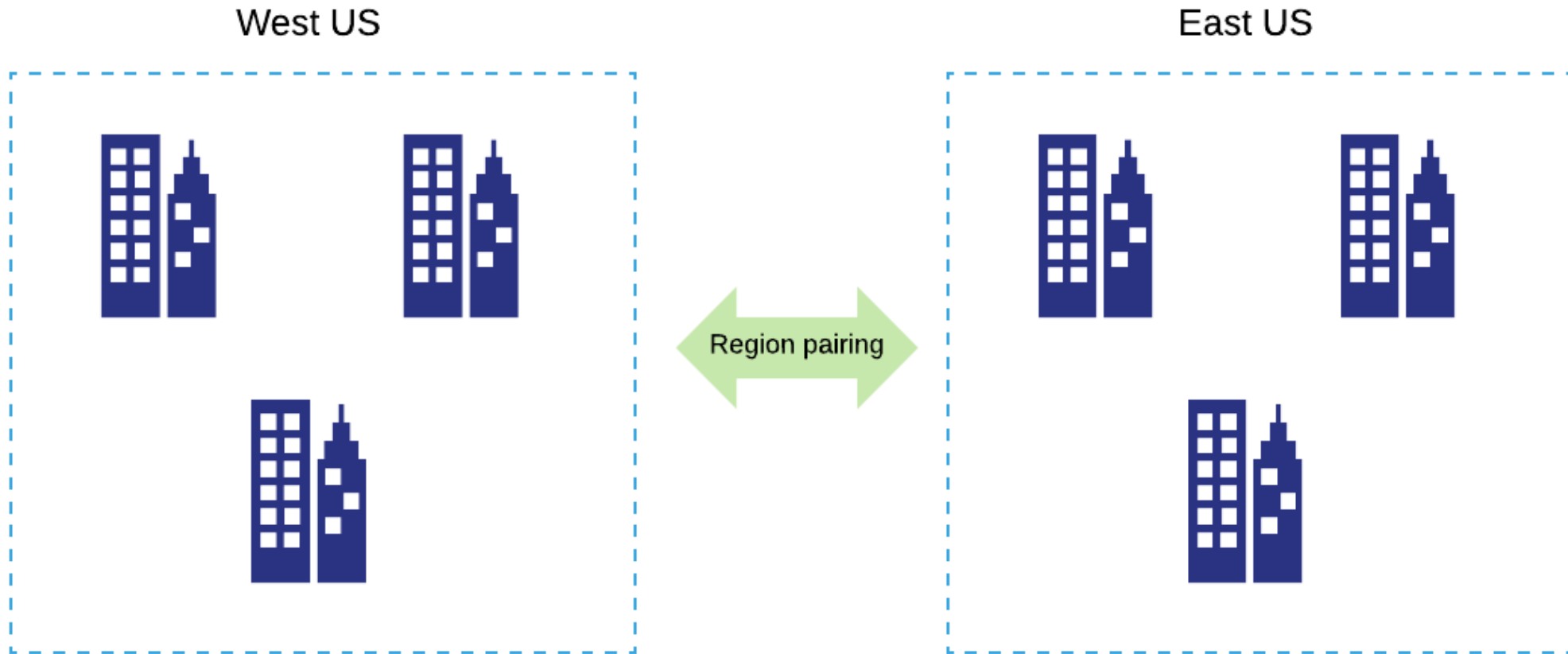
Azure Regional
Outage

Azure Service
Outage

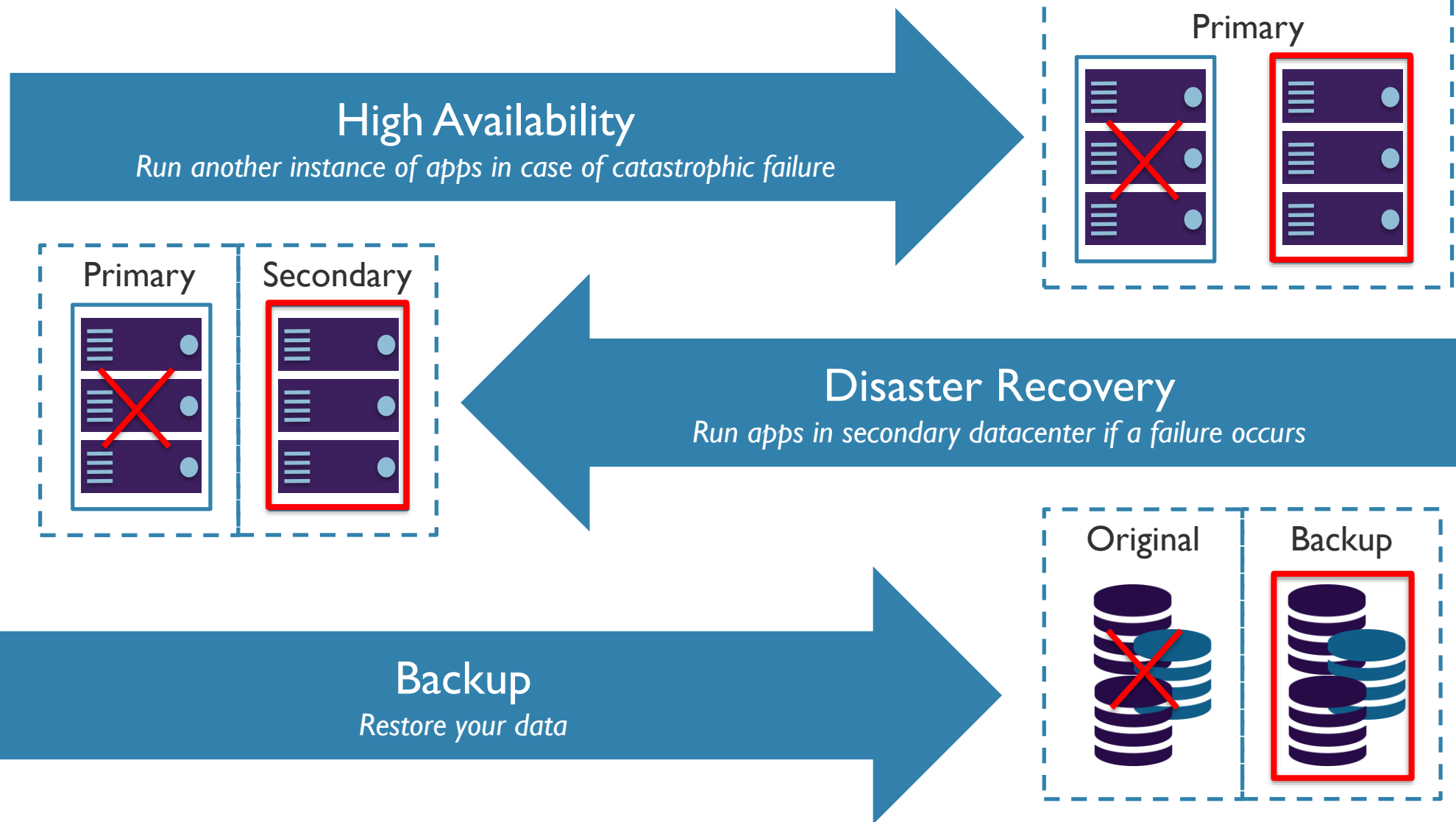
Azure-wide
Outage

Individual
workload issue

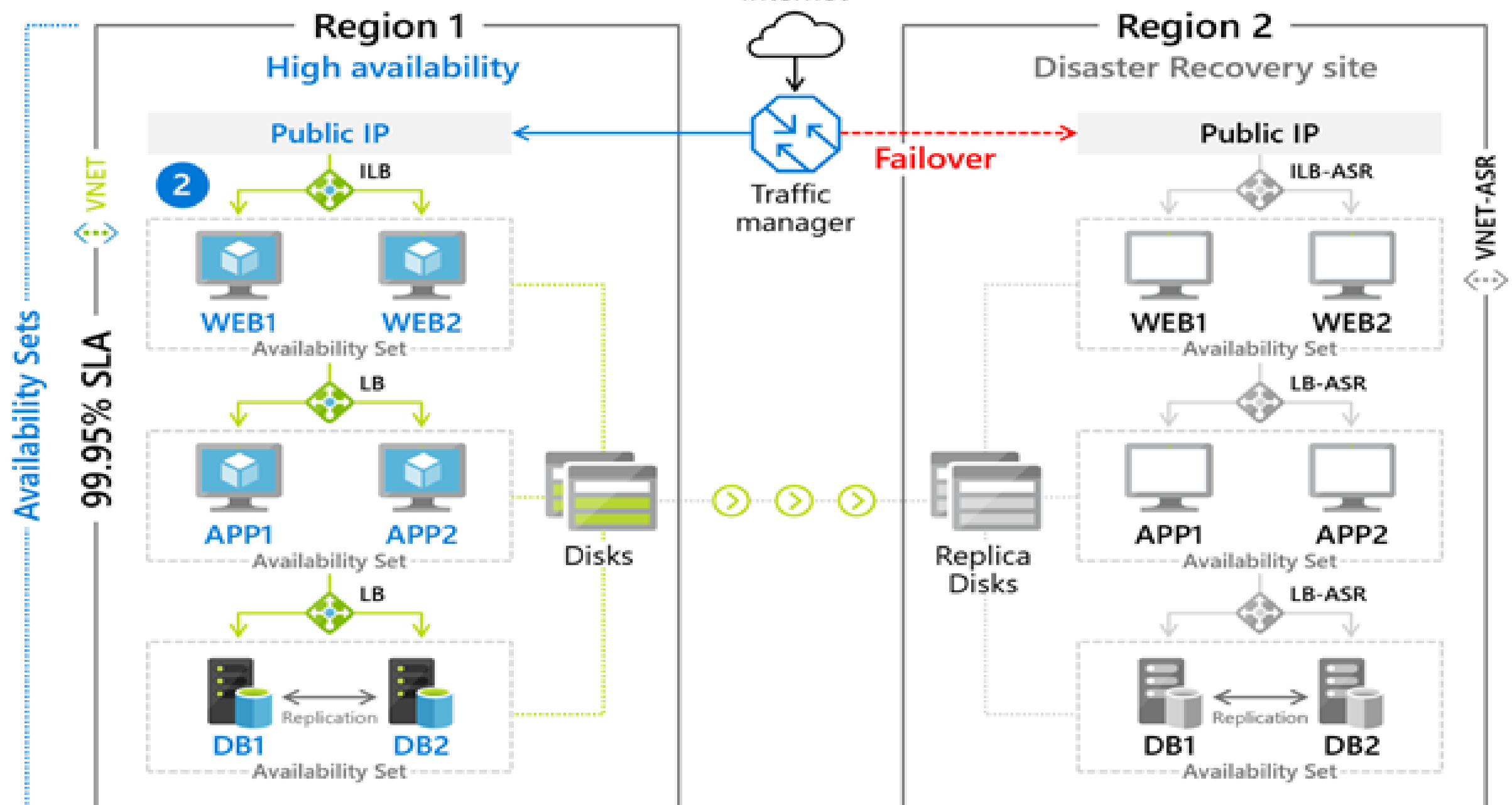
Region Pairs



Business Continuity Strategies

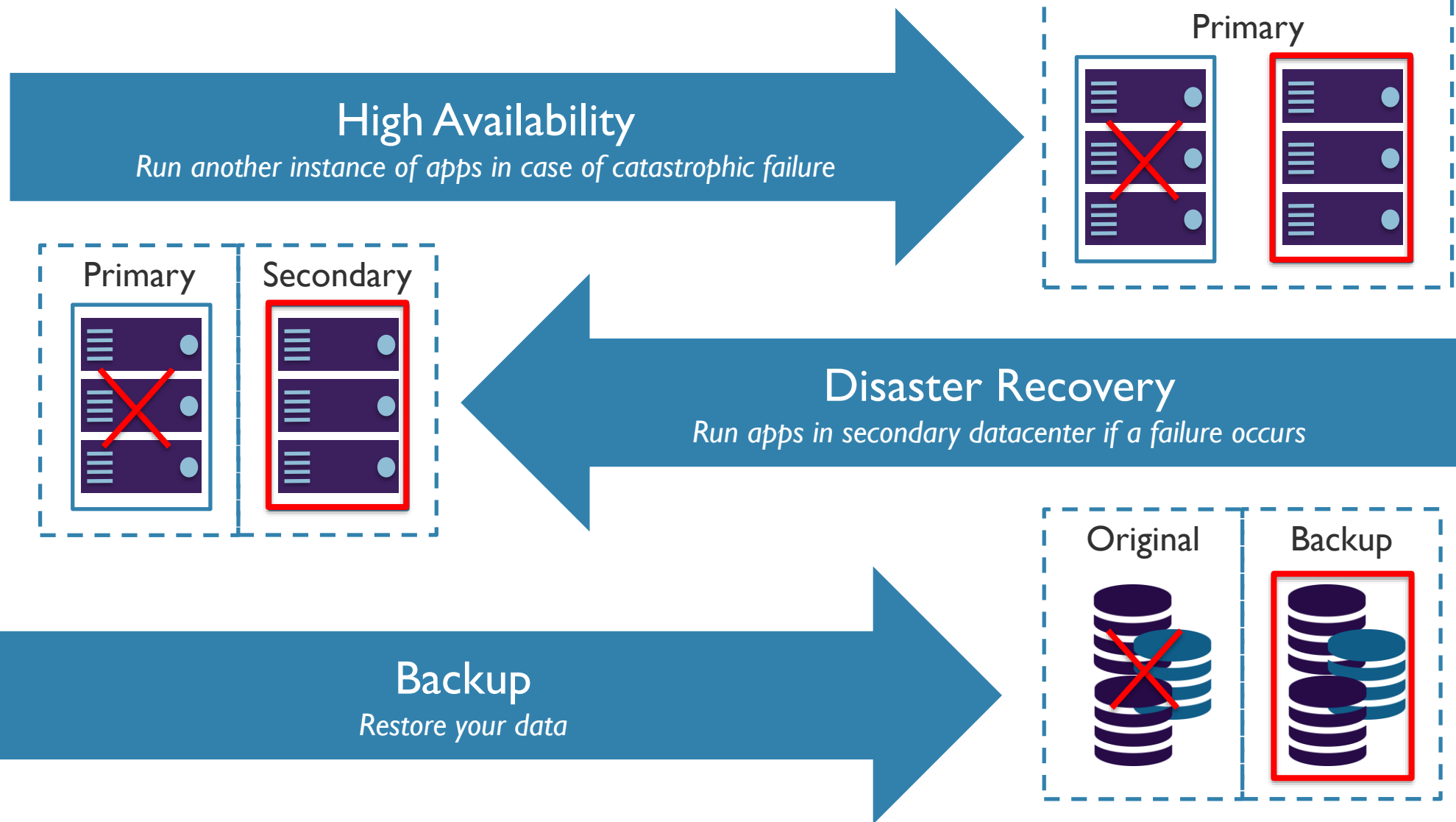


Azure Site Recovery



Azure Site Recovery

Business Continuity Strategies



Azure Site Recovery Overview

On-Premises to Azure Recovery

On-Premises Vmware and Hyper-V to Azure Replication

Azure to Azure Recovery

Recover workloads from your Primary Region in a Secondary target region

Automation and Orchestration

Set up recovery plans to customize the order in which services are restored, as well as any subsequent scripts etc. that need to be run.

Rich integration into Azure Automation for additional automation requirements.

RTO and RPO Targets

Continuous replication for Azure and VMware and Hyper-V

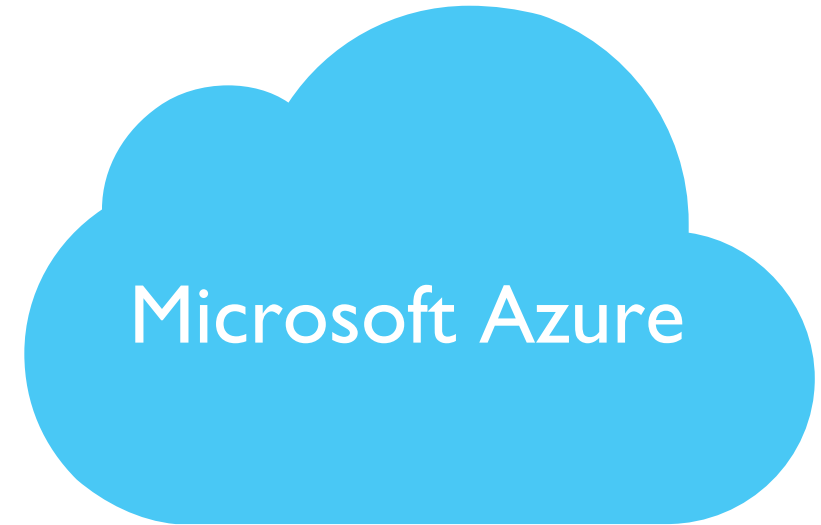
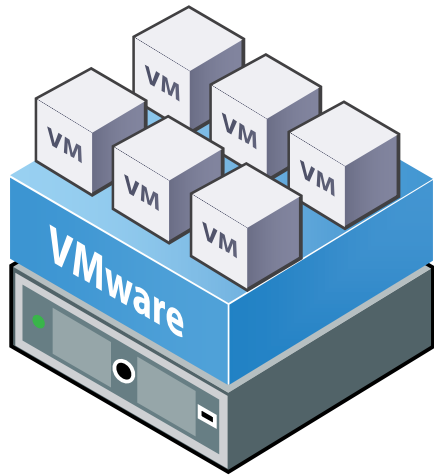
ASR Replication Frequency

30 seconds

5 minutes

15 minutes

VMware to Azure Recovery



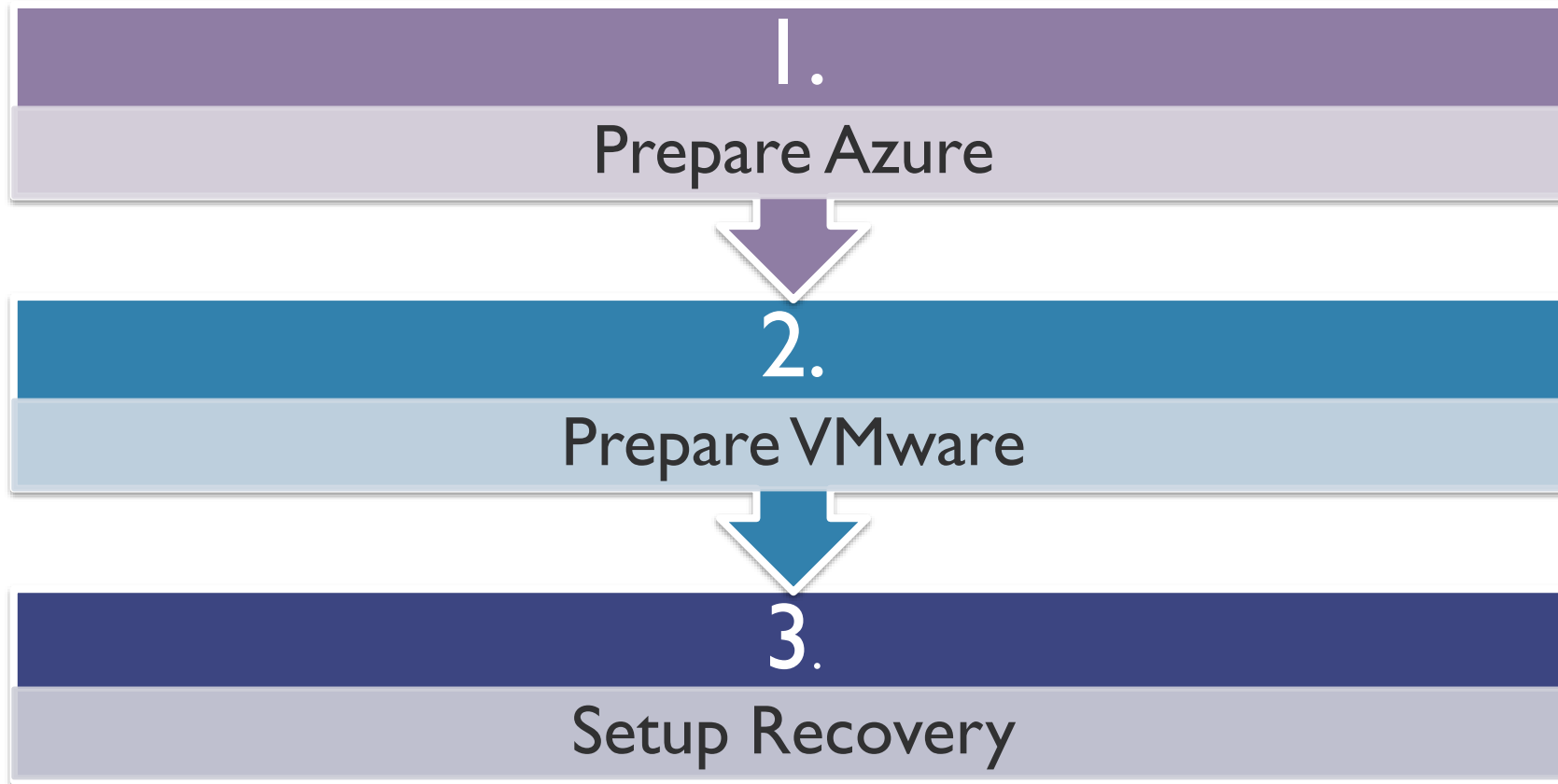
ASR Process

Converts VM to
VHD

Uploads to Azure

Migration
completed from
recovery vault

VMware Migration



Prepare Azure

Verify Account
Permissions

Create Storage
Account

Create Recovery
Services Vault

Setup an Azure
Network

- Create a VM in a Resource Group
- Create a VM in selected Network
- Write to the selected Storage Account

Prepare VMware

VMware
Permissions

Prepare an
account for
Mobility service
installation

Verify
compatibility

Prepare
connectivity to
Azure VMs

- VMware Support Matrix
- Linux VMs: Check file system requirements
- Verify Networking and Storage
- Check post failover configuration support
- Validate Azure VM requirements

<https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-tutorial-prepare-on-premises>

VMware Account Permission Requirements

Task	Role/Permissions	Details
VM discovery	<p>At least a read-only user</p> <p>Data Center object → Propagate to Child Object, role=Read-only</p>	<p>User assigned at datacenter level, and has access to all the objects in the datacenter.</p> <p>To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, VMs and networks).</p>
Full replication, failover, failback	<p>Create a role (Azure_Site_Recovery) with the required permissions, and then assign the role to a VMware user or group</p> <p>Data Center object → Propagate to Child Object, role=Azure_Site_Recovery</p> <p>Datastore → Allocate space, browse datastore, low-level file operations, remove file, update virtual machine files</p> <p>Network → Network assign</p> <p>Resource → Assign VM to resource pool, migrate powered off VM, migrate powered on VM</p> <p>Tasks → Create task, update task</p> <p>Virtual machine → Configuration</p> <p>Virtual machine → Interact → answer question, device connection, configure CD media, configure floppy media, power off, power on, VMware tools install</p> <p>Virtual machine → Inventory → Create, register, unregister</p> <p>Virtual machine → Provisioning → Allow virtual machine download, allow virtual machine files upload</p> <p>Virtual machine → Snapshots → Remove snapshots</p>	<p>User assigned at datacenter level, and has access to all the objects in the datacenter.</p> <p>To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, VMs and networks).</p> <p>https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-tutorial-prepare-on-premises</p>

Azure Backup

Azure Backup Overview



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

Other Recovery Options

Snapshot Recovery

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

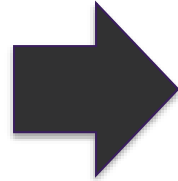
Geo-Replication

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

Recovery Options Overview

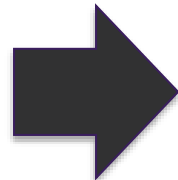
Recovery Options Review

VMs available in event of region outage



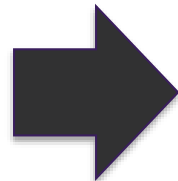
- Azure Site Recovery
- GRS storage

Individual recovery of data for specific service



- Azure Backup
- 3rd Party Backup Technologies

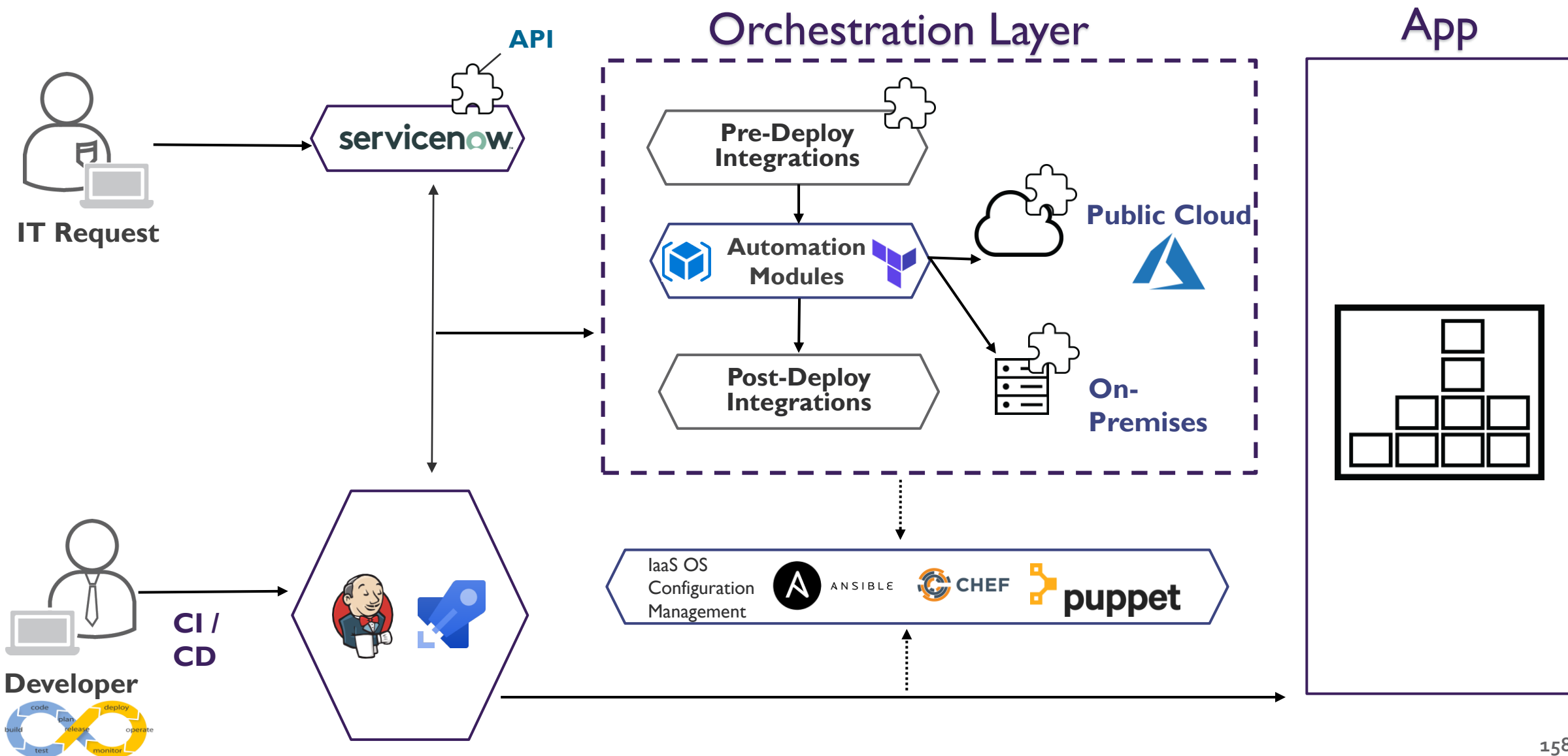
Highly available application across regions



- Traffic Manager
- Load Balancers in each region
- Availability Sets/Zones in each region

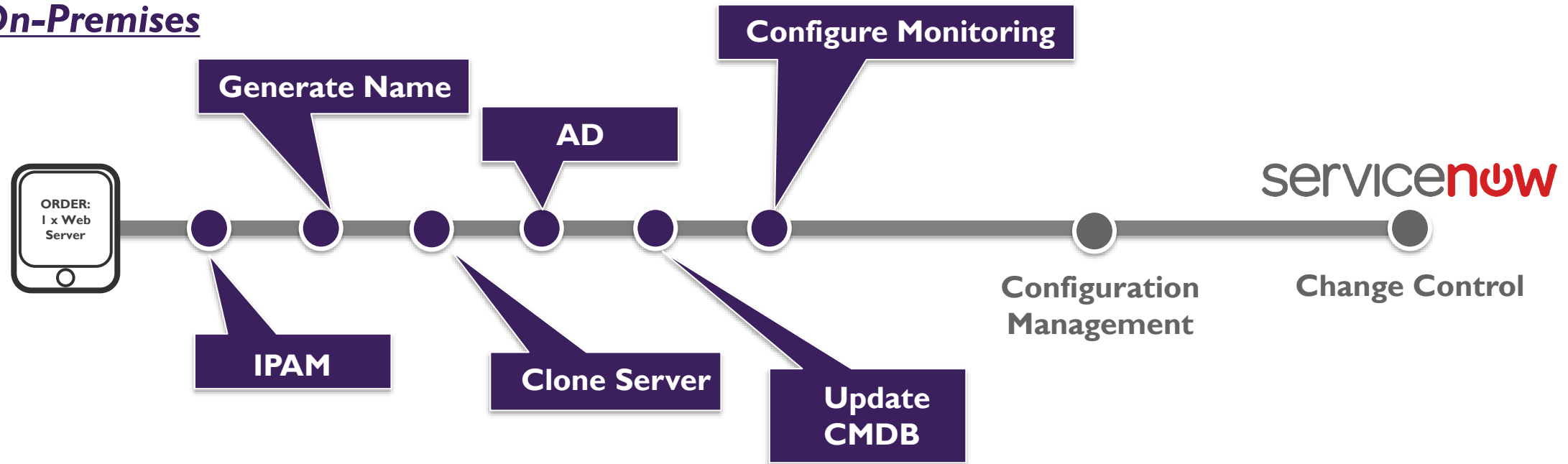
Design Deployment

AUTOMATION ARCHITECTURE



IaaS Automated Service Delivery

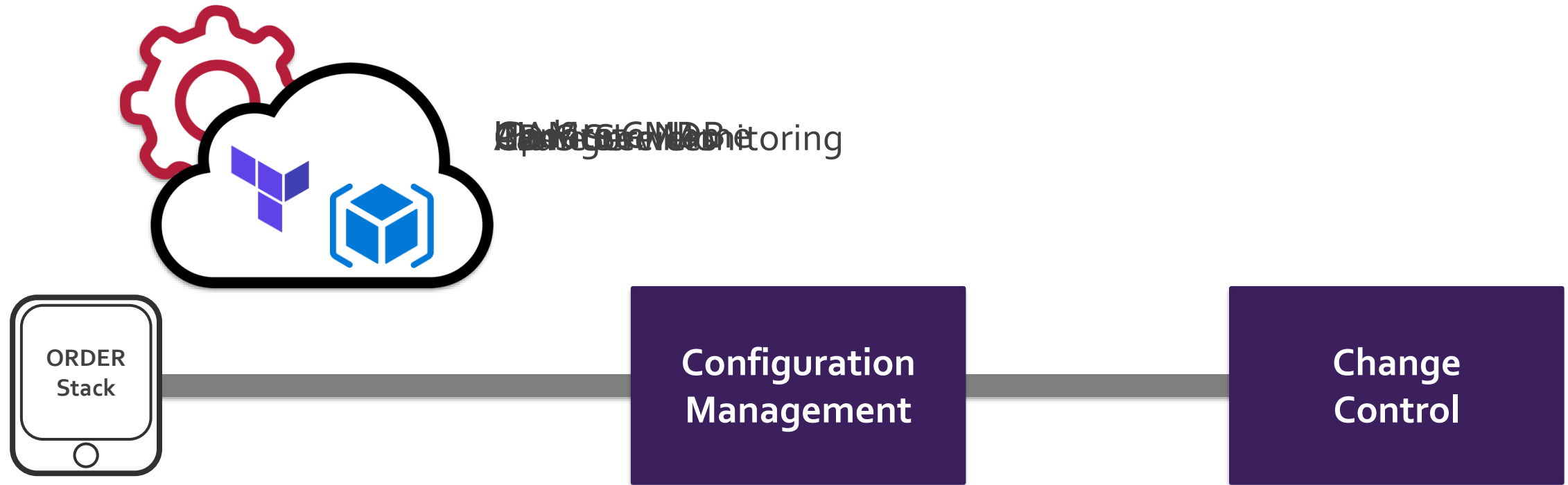
On-Premises



Public Cloud



Public Cloud – Enterprise PaaS



Configuration Management

Modules



WINDOWS
(BASE OS)



LINUX
(BASE OS)



SQL



SECURITY



APACHE
WEB SERVER



IIS
WEB SERVER

Compose Application Stacks

Role: IIS Server

Module:

Azure Resource Manager (ARM)

ARM Templates Overview

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



Resource
(E.g. Storage Account)

- Apply Infrastructure as Code
- Download templates from Azure Portal
- Author new templates
- Use Quickstart templates, provided by Microsoft

Quickstart Templates

Microsoft Azure

SALES 1-800-867-1389 MY ACCOUNT PORTAL Search

Why Azure Solutions Products Documentation Pricing Training Marketplace Partners Blog Resources Support FREE ACCOUNT

Azure Quickstart Templates

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

What is Azure Resource Manager

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

Learn more >

641 Quickstart templates are currently in the gallery.

Most popular See All

- Create VM from existing VHDs and connect it to existing VNET**
This template creates a VM from VHDs (OS + data disk) and let you connect it to an existing VNET that can reside in another Resource Group then the virt...
by Mickaël Mottet, Last updated: 11/25/2016
- Create an Azure VM with a new AD Forest**
This template creates a new Azure VM, it configures the VM to be an AD DC for a new Forest
by Simon Davies, Last updated: 4/21/2017
- Blockchain Template**
Deploy a VM with blockchain software.
by Neil Sant Gat, Last updated: 10/11/2016
- Blockchain - Ethereum Private Consortium Network**
This template fully automates the provisioning of necessary Azure resources like VMs, storage, network settings etc. as well as the configurati...
by Christine Avanesians, Last updated: 9/20/2016
- Create a V2 data factory**
- Basic RDS farm deployment**
- Create a new AD Domain with 2 Domain Controllers**
- Join a VM to an existing domain**

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

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

ARM File Types

ARM Template
File

Describe the configuration
of your infrastructure via a
JSON file

ARM Template
Parameter File

Separate your parameters
(optional)

Deployment
Scripts

E.g. PowerShell for
Deployment

ARM Template Constructs

Parameters

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

Variables

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

Resources

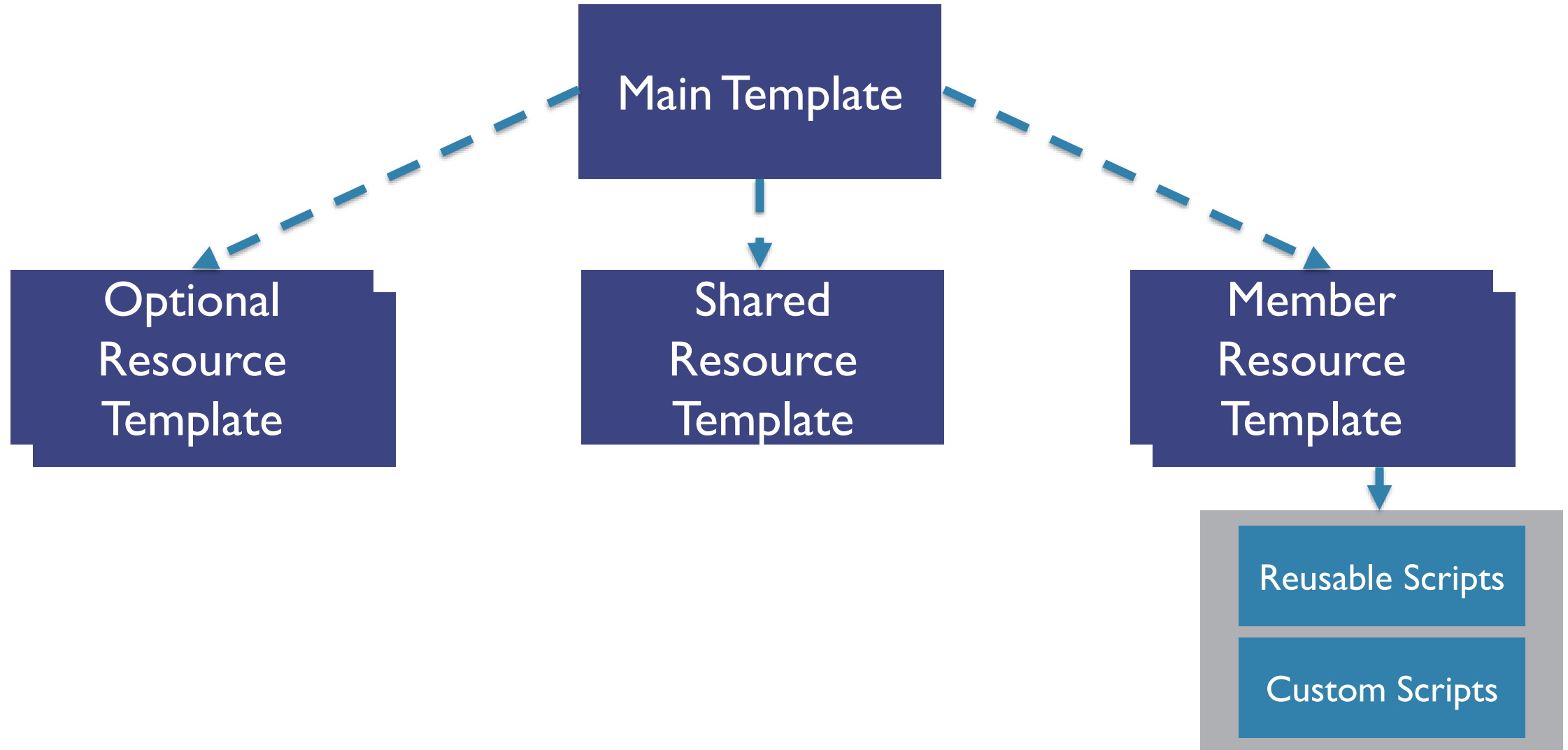
Define the resources you wish to deploy or update.

Outputs

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

Linking Templates

Linking Templates



Linking Templates (continued)

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

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

Inline Example

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

New Template
created in the
body of the
current ARM
template



External Example

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



Template and parameters linked inside current ARM templates

Key ARM Functions

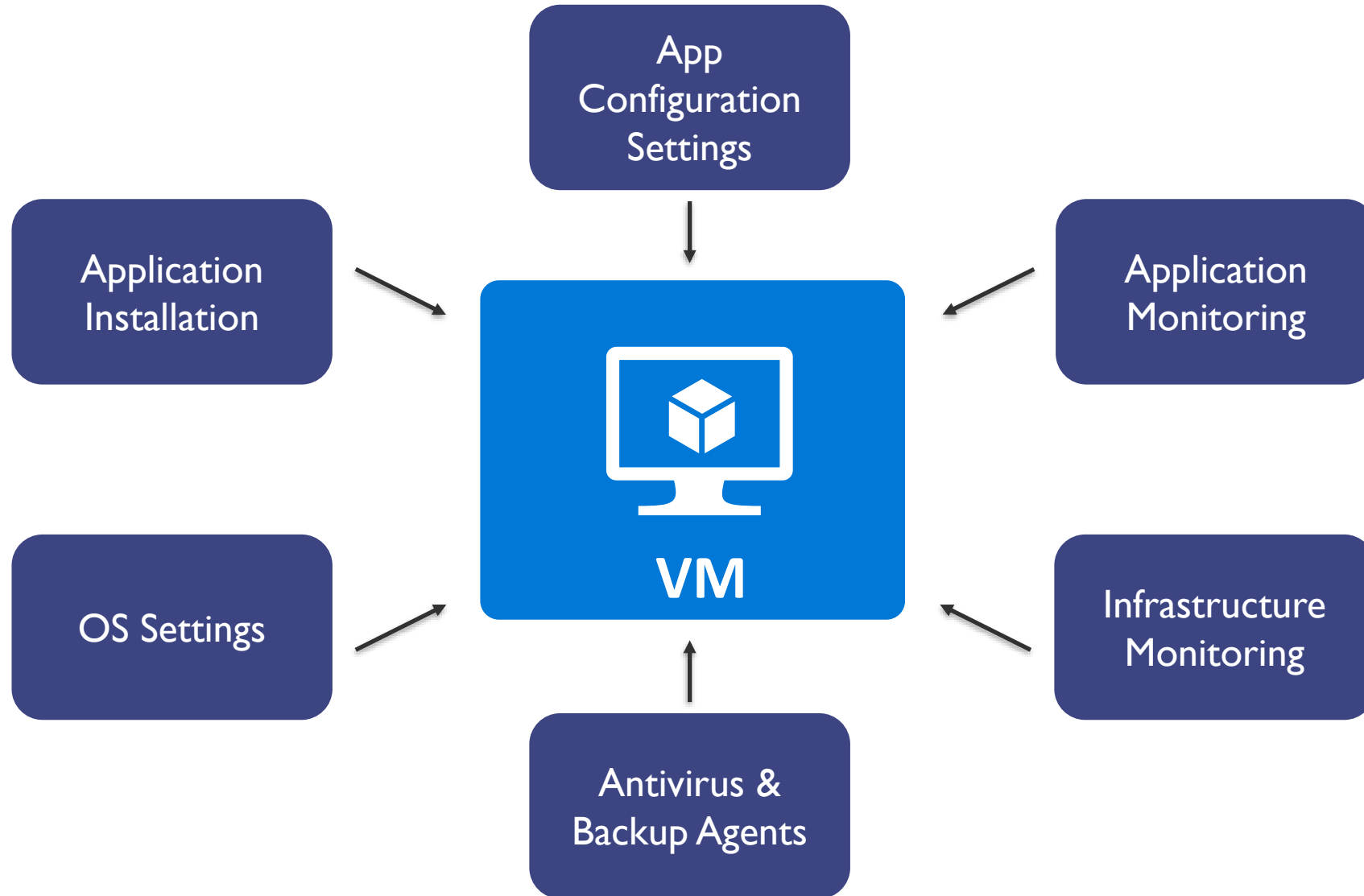
Copy

copyIndex()

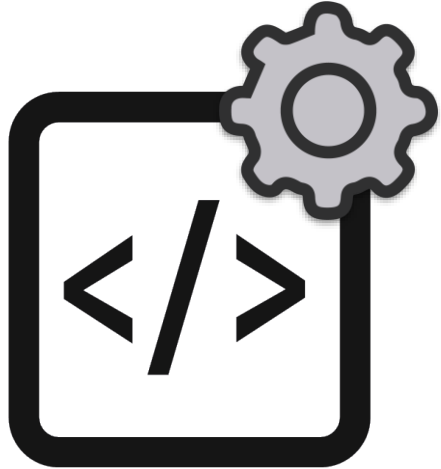
dependsOn

PowerShell DSC

Introduction to Configuration Management



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

Configurations

Resources

Logical
Configuration
Manager

PowerShell DSC Example

```
Configuration SkylineWebSite
```

```
{
```

```
  Node 'localhost'
```

```
  {
```

```
    #Install IIS - Enabled via Windows  
feature
```

```
  WindowsFeature IIS
```

```
  {
```

```
    Ensure = "Present"
```

```
    Name = "Web-Server"
```

```
  }
```

```
  #Install ASP.NET 4.5
```

```
  WindowsFeature ASP
```

```
  {
```

```
    Ensure = "Present"
```

```
    Name = "Web-Asp-Net45"
```

```
  }
```

```
}
```

```
}
```

← The name of the configuration.

← Specifies which targets the configuration applies to.

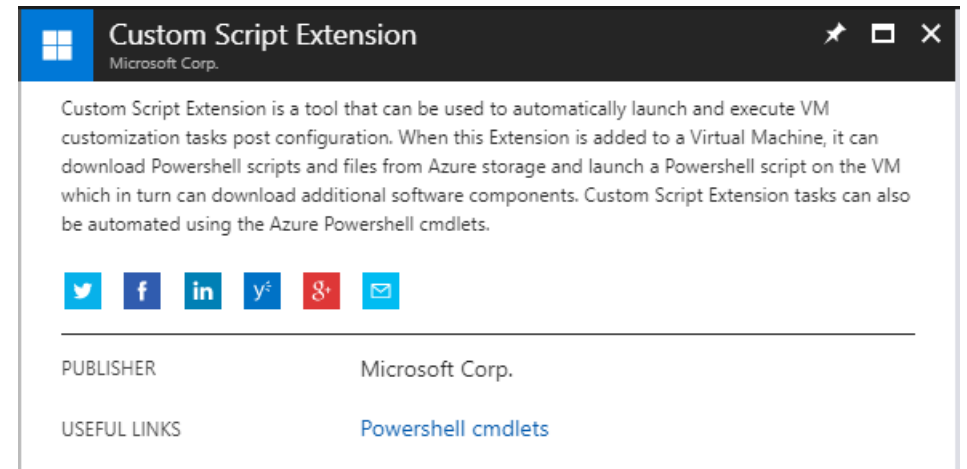
← Declarative statement about what we are configuring. In this case, we want IIS installed.

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



Custom Script Extension

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



Custom Script Extension

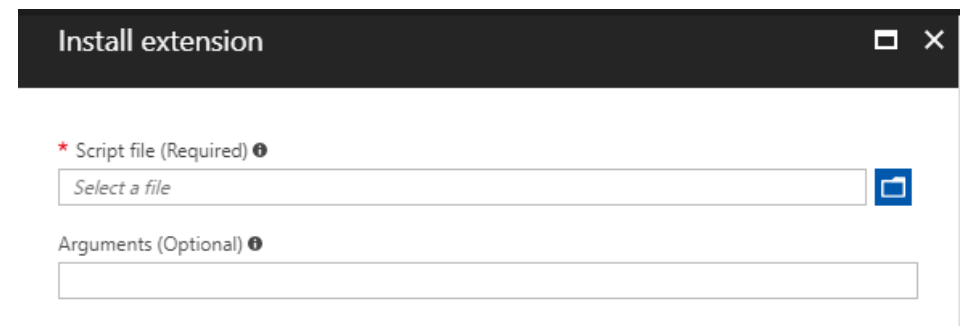
Microsoft Corp.

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

[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#) [Email](#)


PUBLISHER: Microsoft Corp.

USEFUL LINKS: [Powershell cmdlets](#)



Install extension

* Script file (Required) ⓘ

Select a file 

Arguments (Optional) ⓘ

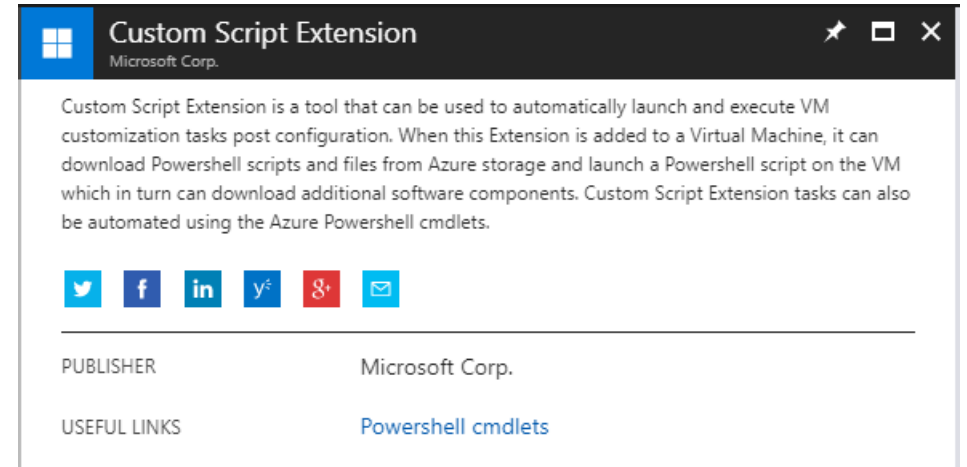
Custom Script Extension (continued)

Benefits

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

Drawbacks

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



Custom Script Extension

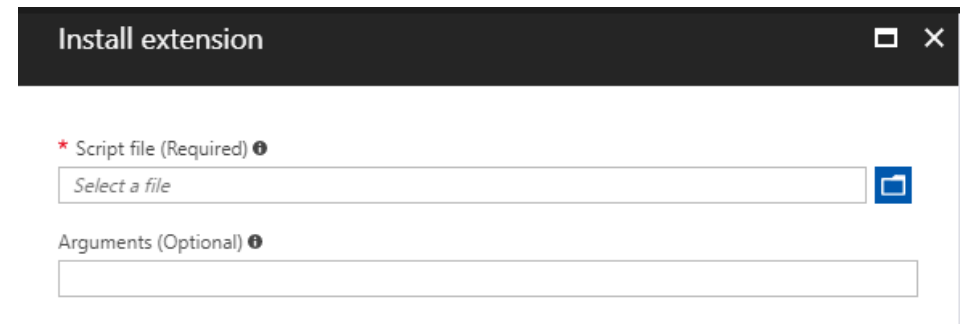
Microsoft Corp.

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

[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#) [Email](#)


PUBLISHER Microsoft Corp.

USEFUL LINKS [Powershell cmdlets](#)



Install extension

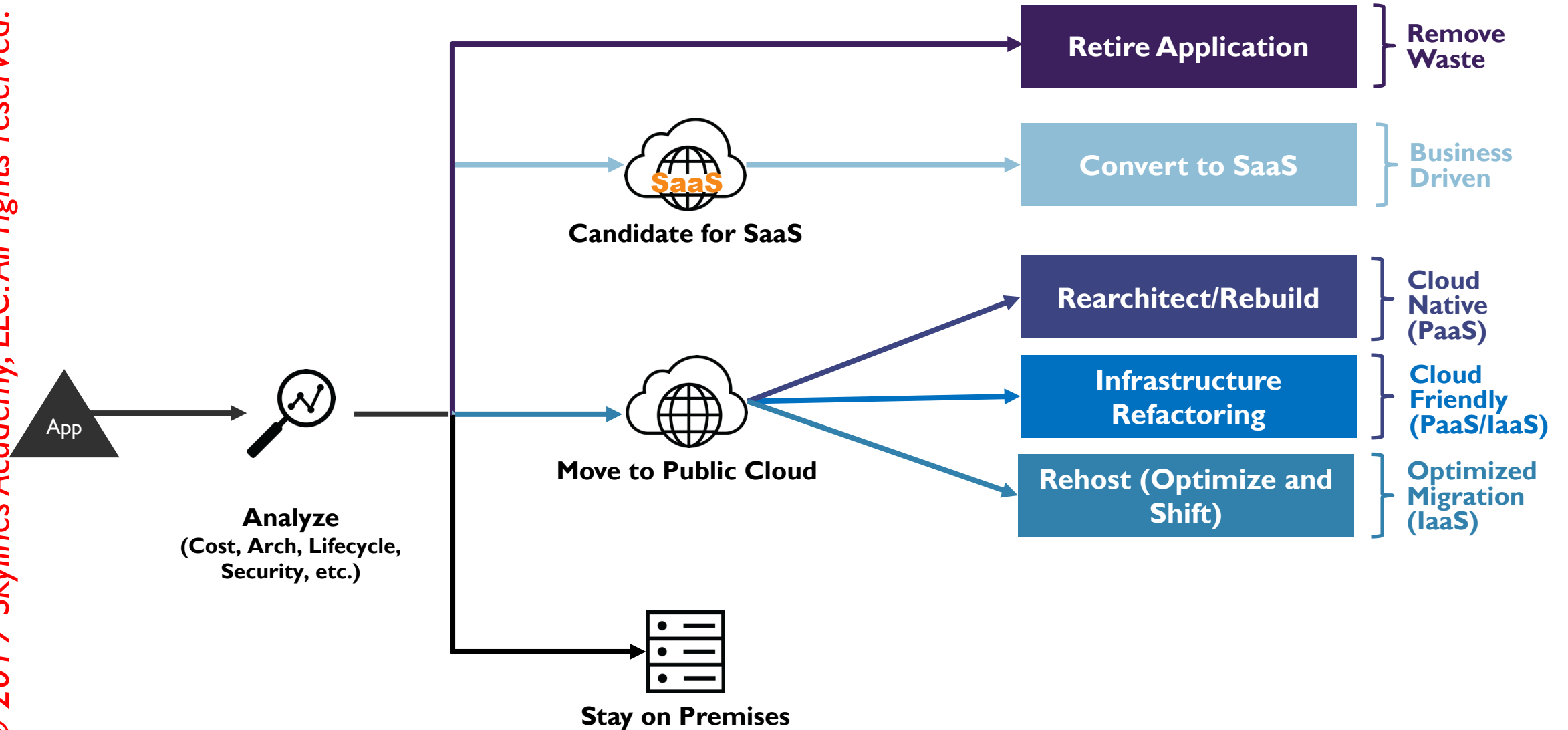
* Script file (Required) ⓘ

Select a file 

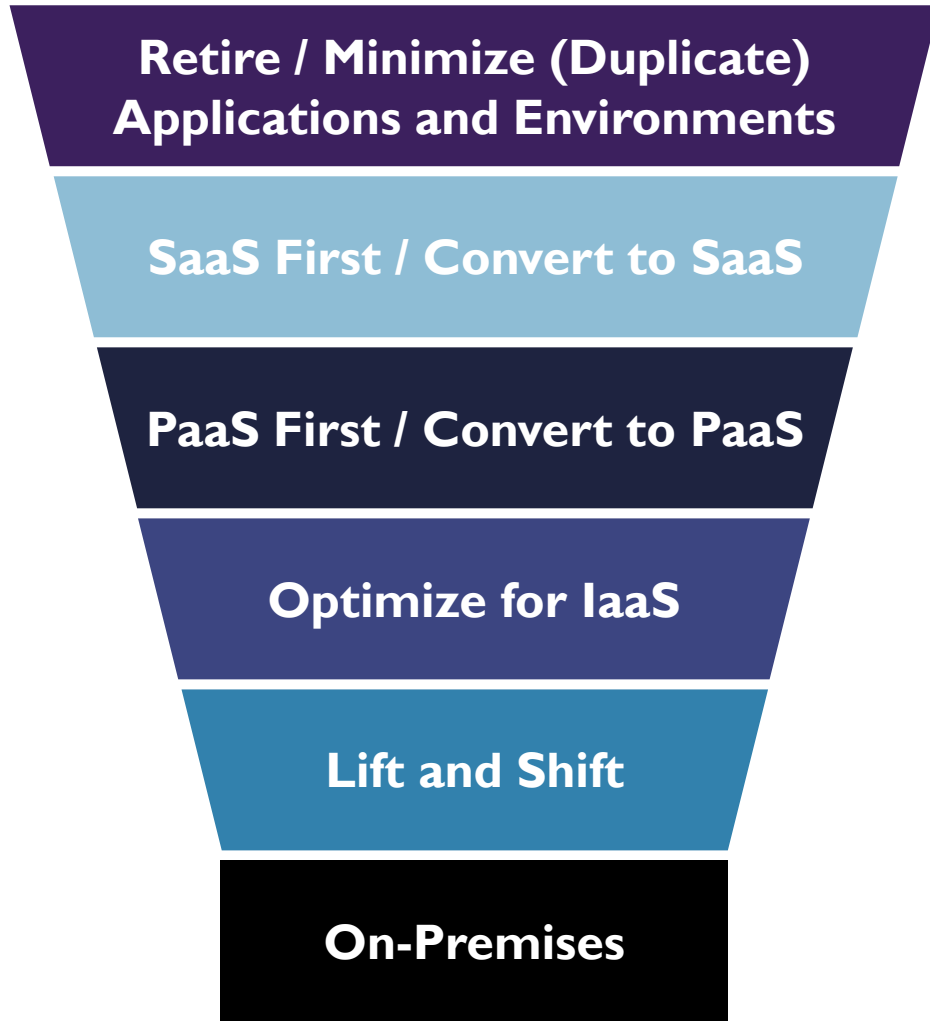
Arguments (Optional) ⓘ

Migration

Migration Options



Enterprise Cloud Strategy



BEFORE		AFTER
Exchange	➔	Office 365
Sharepoint	➔	Sharepoint Online
NAS HomeDir	➔	OneDrive

FOUNDATIONAL SPRINTS	PHASE 1	PHASE 2	PHASE 3
Foundation Sprint	Web Apps	Databases	Legacy Systems
Security & Operations Sprint	New Apps		



Azure Migrate Assessment

Azure Migrate Overview

Assess Azure Readiness

Are my machines capable of running in Azure? Are there any specific compatibility issues that need to be addressed?

Sizing

Get approximate sizing recommendations based on historic performance.

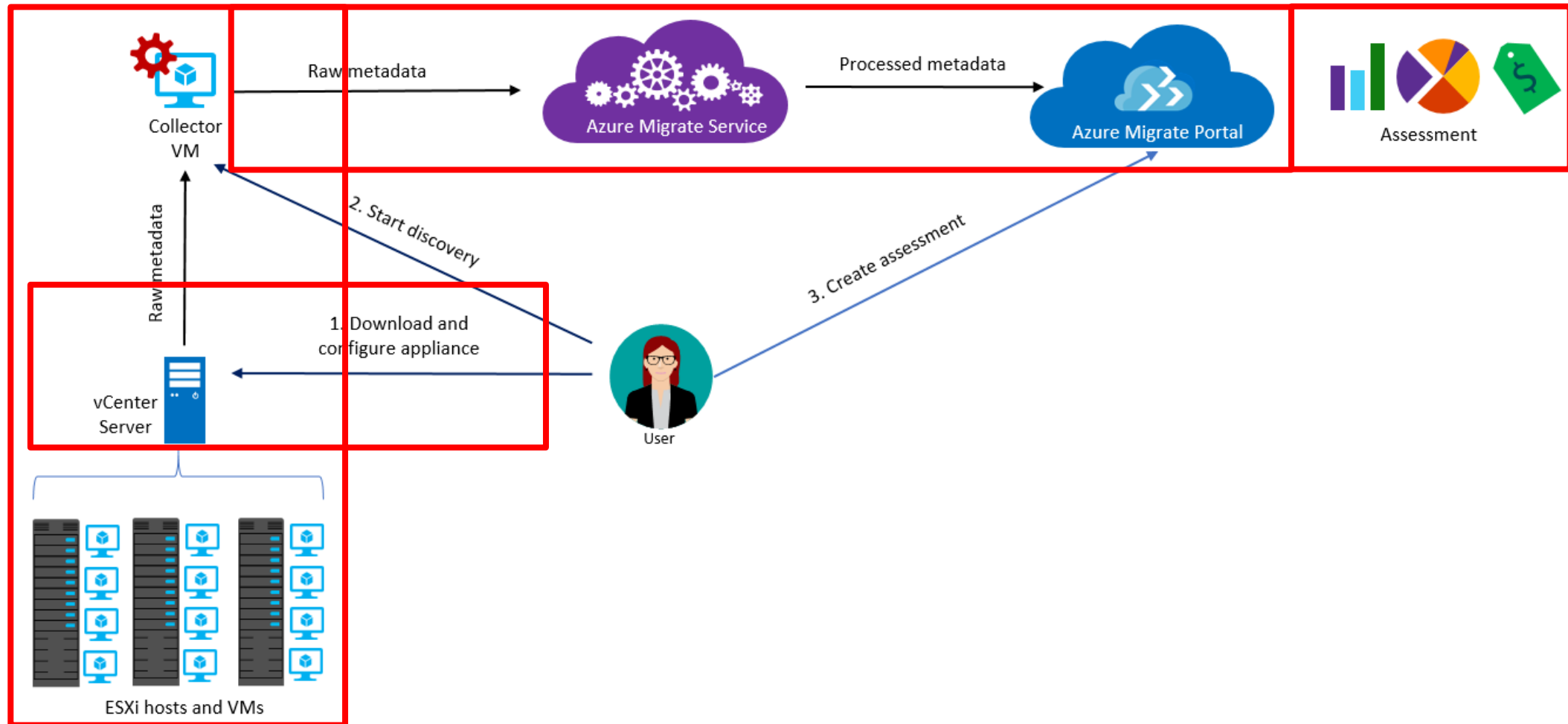
Cost Estimation

Based on the sizes selected, how much is it going to cost me?

Dependency Mapping

Visualize dependencies in order to plan waves of workloads for migration appropriately.

How it Works



Azure Migration Limitations

- VMware assessment only (for Hyper-V use ASR deployment planner).
- Up to 1500 VMs in a single discovery and project.
- For larger environments, split the discovery into multiple assessments. You can execute up to 20 projects per a subscription.
- Projects can only be created in the US regions. Metadata is stored in West Central US, or East US

What goes into an Assessment?

Target location	Target region. Currently Azure supports up to 30 regions.
Storage type	Determines whether to use Standard or Premium disks. For performance-based sizing, the disk sizing recommendation is automatically done based on the performance data of the VMs.
Sizing criterion	Sizing can be based on performance history of the on-premises VMs, or as on-premises (the default), without considering performance history.
Azure Hybrid Benefit	Determine whether you have licensing you are able to utilize in order to reduce costs using Azure Hybrid Benefit.
Reserved Instances	Determine whether to utilize Reserved Instances to further reduce costs.
VM uptime	The duration for which VMs will run in Azure. Useful for VMs that only need to run during business hours to further reduce costs.
Pricing tier	Pricing Tier of the VMs chosen. E.g. Basic or Standard.
Performance history	By default, Azure Migrate evaluates the performance of on-premises machines using performance history for the last day , with a 95% percentile value.
VM series	Choose the VM Series types you want to include.

<https://docs.microsoft.com/en-us/azure/migrate/migrate-overview>

Comfort Factor

Azure Migrate considers a buffer (comfort factor) during assessment. This buffer is applied on top of machine utilization data for VMs (CPU, memory, disk, and network). The comfort factor accounts for issues such as seasonal usage, short performance history, and likely increases in future usage.

For example, a 10-core VM with 20% utilization normally results in a 2-core VM. However, with a comfort factor of 2.0x, the result is a 4-core VM instead. The default comfort setting is 1.3x.

Comfort Factor Examples

Source Machine CPU	Utilization	Recommended CPU	Comfort Factor	Resulting Recommendation
10 Cores	20%	2 Cores	2.0x	4 Cores (2 x 2)
10 Cores	50%	5 Cores	1.3x (Default)	6.5 Cores (5 x 1.3) Recommendation = 8 You can't have a half core and no 7 core VMs exist
10 Cores	20%	2 Cores	1.3x	2.6 Cores (2 x 1.3) Recommendation = 4 You can't have a half core and no 3 core VMs exist

Port Requirements

Component	Communicates With	Details
Collector	Azure Migrate service	443
Collector	vCenter Server	Default: 443 This can be changed to a different port if required by your vCenter.
On-premises VM	Log Analytics Workspace	443

Import/Export Service

Azure Import/Export Use Cases

Data Migration to Cloud

Move large amounts of data to Azure quickly.

e.g. Large migration from your datacenter.

Content Distribution

Sending data to customer sites.

Backup

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

Data Recovery

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

Import/Export Components

Import/Export Service

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

Import/Export Components

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

Import/Export Components

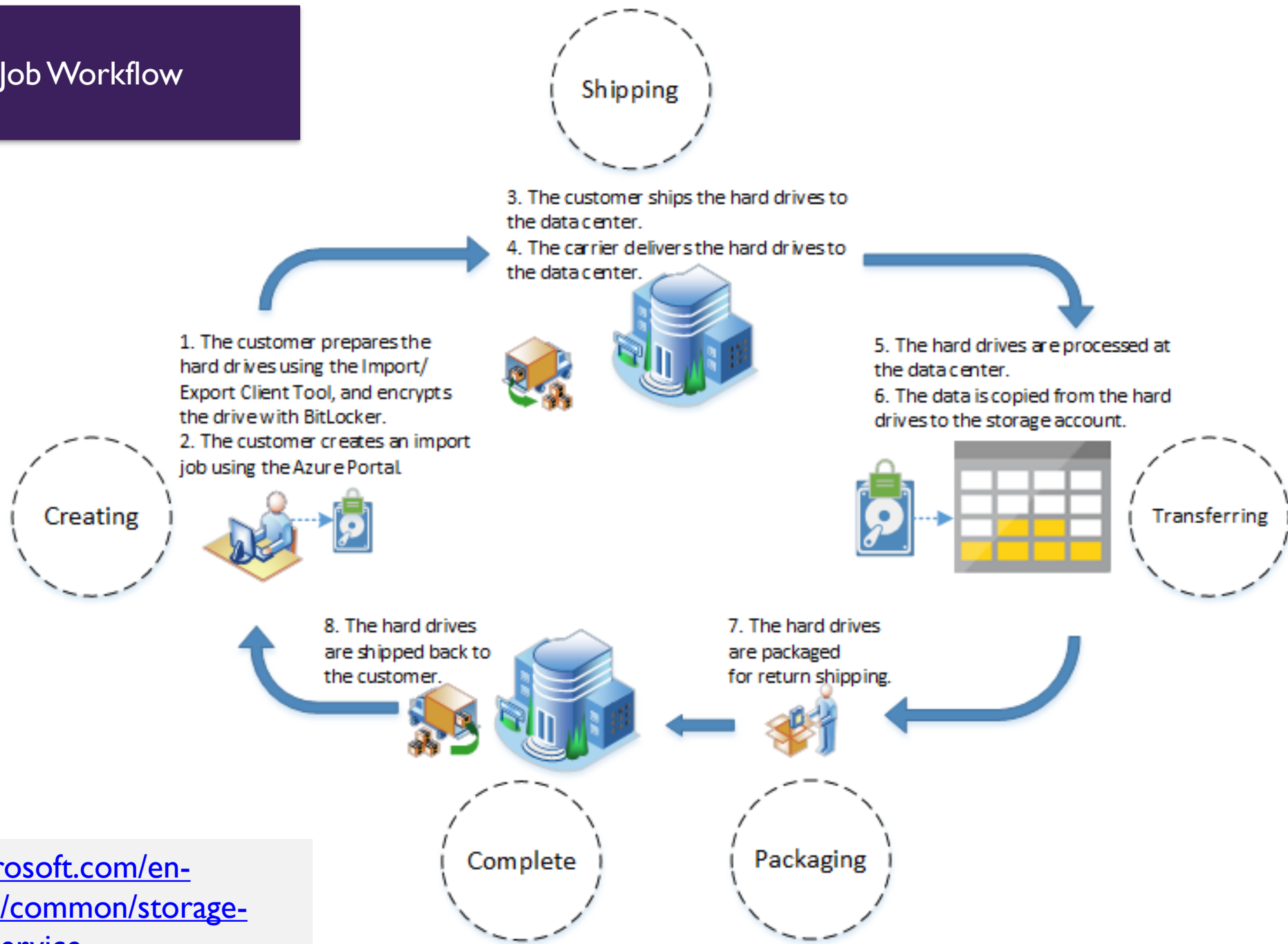
Disk Drives

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

Supported Disks:

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

Import Job Workflow



Skylines Academy, LLC. All rights reserved.

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

Design Infrastructure

Design Infrastructure

Compute

Network

Data

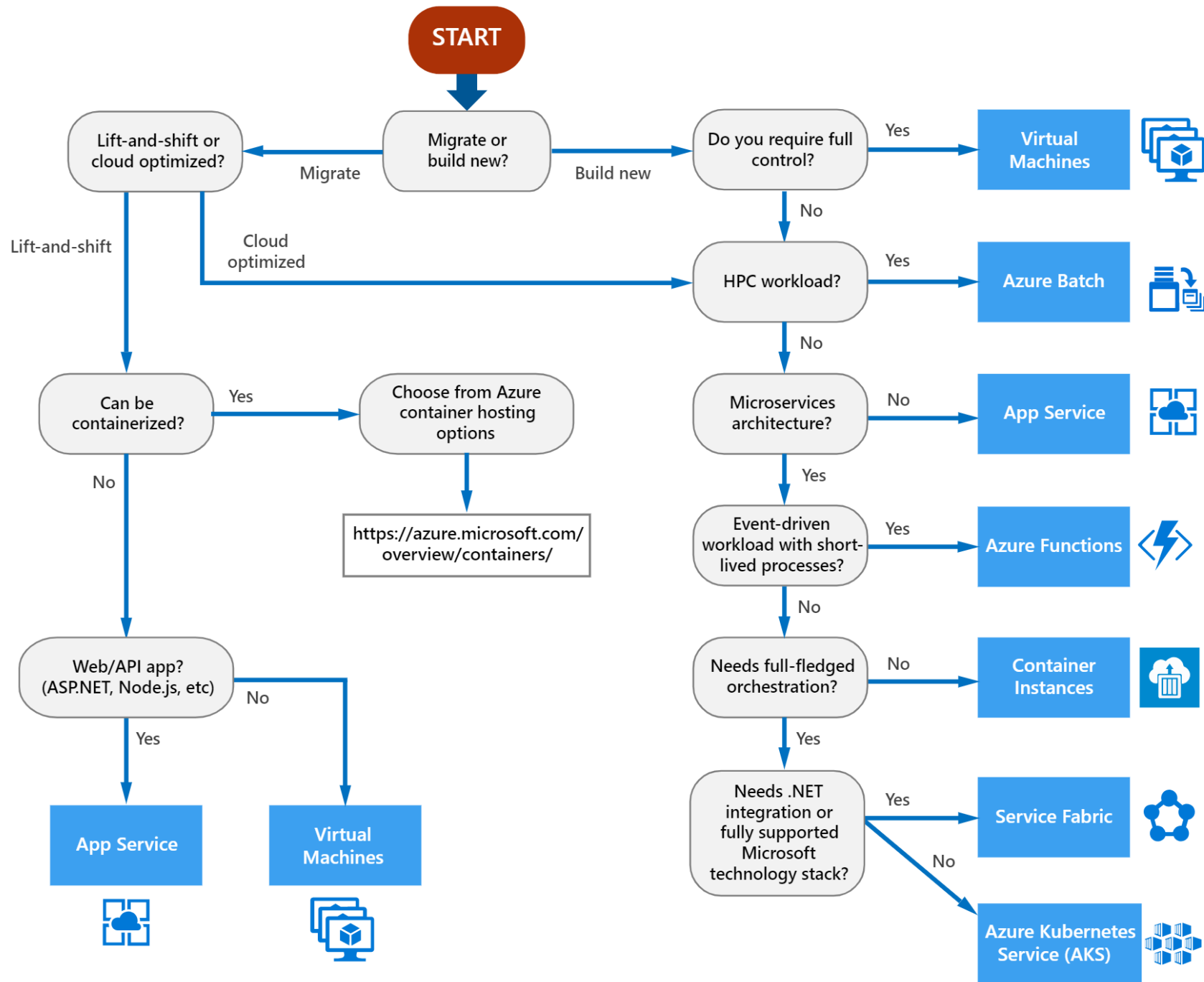
Operations

Compute Services

Compute Options (High Level)

- **Virtual Machines** – IaaS service allowing you to deploy and manage VMs inside a virtual network
- **App Service** – Managed PaaS service for hosting web apps, mobile apps, APIs or Logic Apps
- **Service Fabric** – Distributed systems platform that can run in many environments. Orchestrates microservices across its clusters
- **Azure Container Service** – Create and configure clusters of VMs that are preconfigured to run containerized apps
- **Azure Kubernetes Service** – Managed Kubernetes service for running containers via Kubernetes
- **Azure Functions** – FaaS Service
- **Azure Batch** – Managed service for running large-scale parallel and high performance computing (HPC) applications.

Decision Tree for Compute

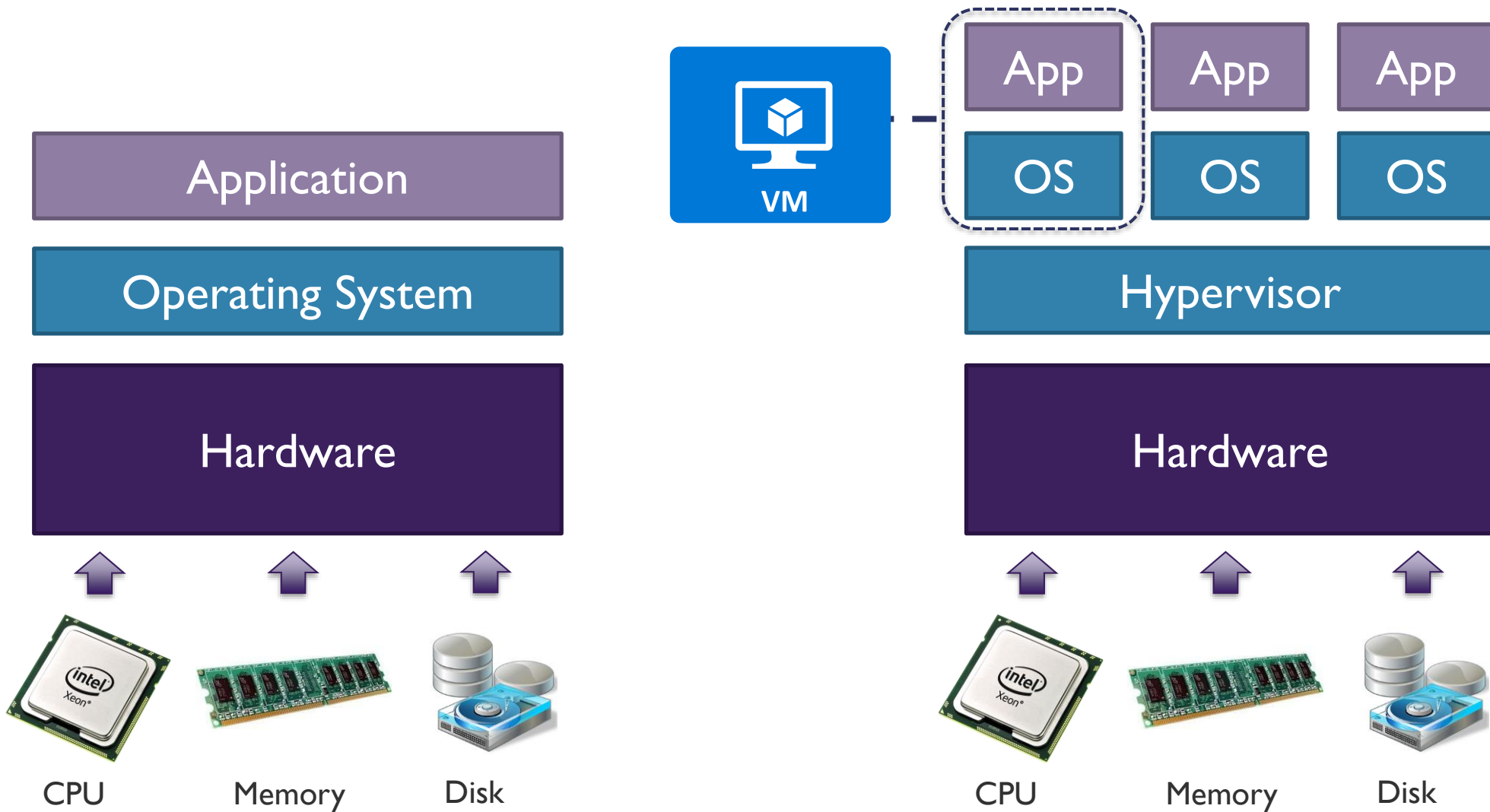


Compute Comparison

<https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/compute-comparison>

VMs Overview Part I

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

VMs Overview Part 2

Azure Compute Units (ACUs)

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

Microsoft-
created
performance
benchmark

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

OS Reference Documentation

Windows Virtual Machines

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



Linux Virtual Machines

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



VMs Overview Part 3

Windows Server Support

OS	Key Points
Pre-Windows 2008 R2 (e.g. Windows Server 2003)	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Supported.• Specific support matrix for server roles.
Windows Server 2012	<ul style="list-style-type: none">• Supported – Datacenter version in marketplace.
Windows Server 2016	<ul style="list-style-type: none">• Supported – Datacenter and nano versions in marketplace.
Desktop OS	<ul style="list-style-type: none">• Windows 10 Pro and Enterprise in marketplace.

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

VMs Overview Part 4

Regional Limitations

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

Restricted Usernames

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

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

VM Storage

VM Storage Types

Standard Storage

Backed by traditional
HDD

Most cost effective

Max throughput –
60MB/S per disk

Max IOPS –
500 IOPS per disk

Premium Storage

Backed by SSD drives

Higher performance

Max throughput –
250MB/S per disk

Max IOPS –
7500 IOPS per disk

Managed Disk – Standard Storage Sizes

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



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

Managed Disk – Premium Storage Sizes

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

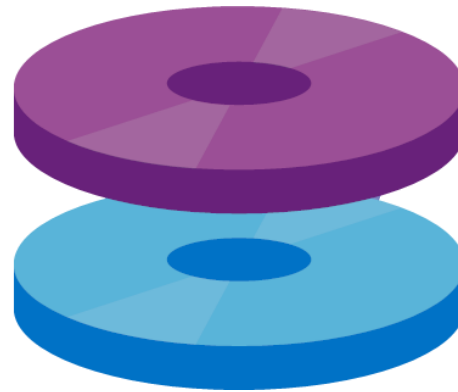
Managed vs. Unmanaged Disks

Unmanaged Disks

DIY option

Management overhead
(20000 IOPS per storage
account limit)

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



Managed Disks

Simplest option

Lower management
overhead as Azure manages
the storage accounts

Only LRS replication mode
currently available

Replication Options

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 durable even in the event of a complete region outage.

Read Only Geographically Replicated Storage (RA-GRS)

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

Replication Strategies

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

VM Availability

Availability Sets

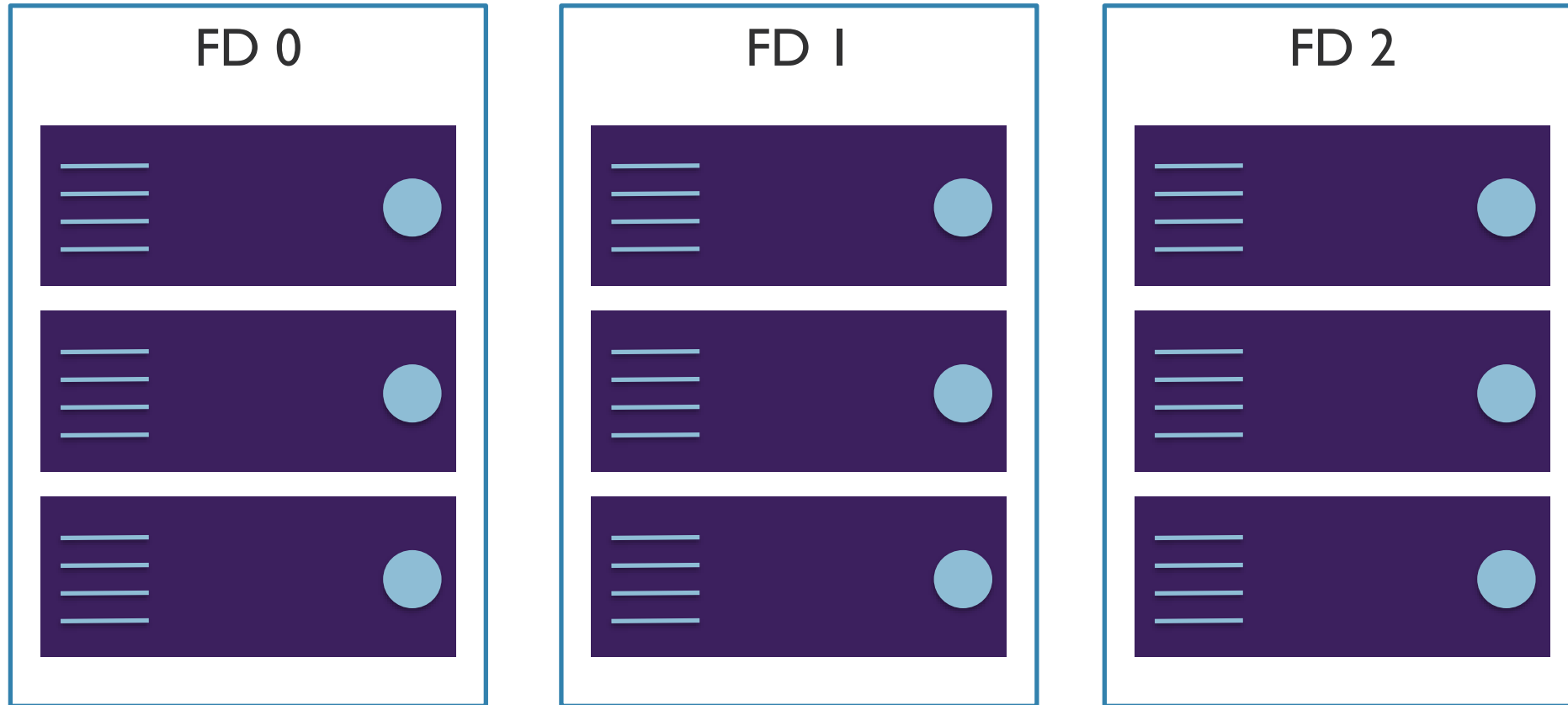
Potential for VM Impact

- Planned maintenance
- Unplanned hardware maintenance
- Unexpected downtime

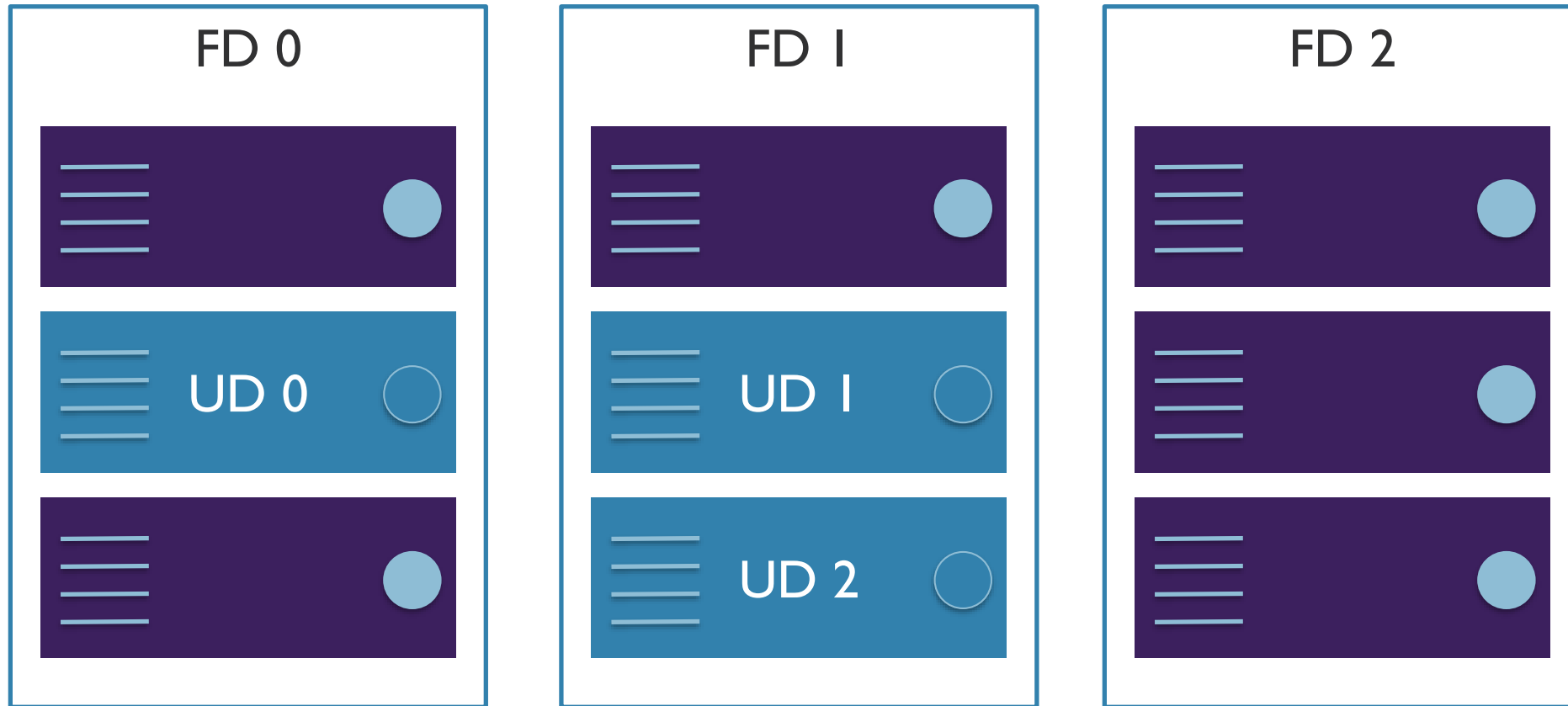
Availability Sets

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

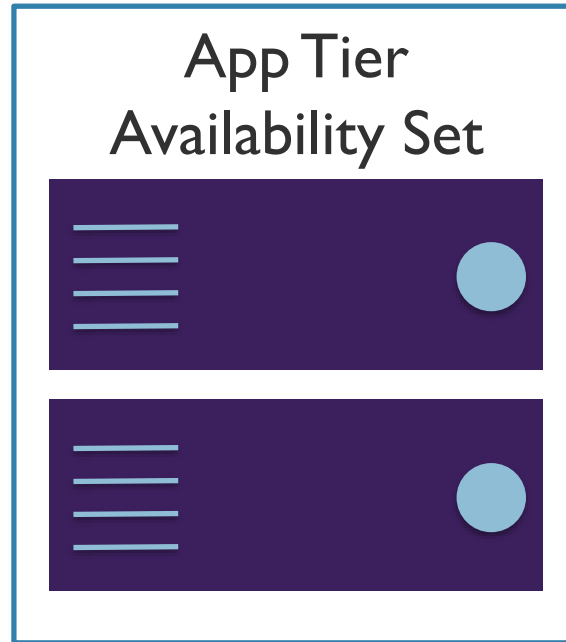
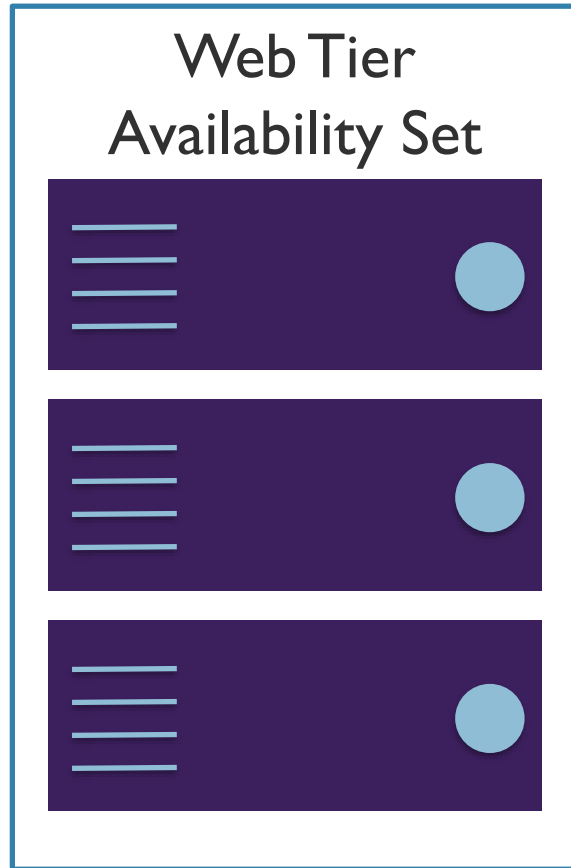
Fault Domains and Update Domains



Fault Domains and Update Domains

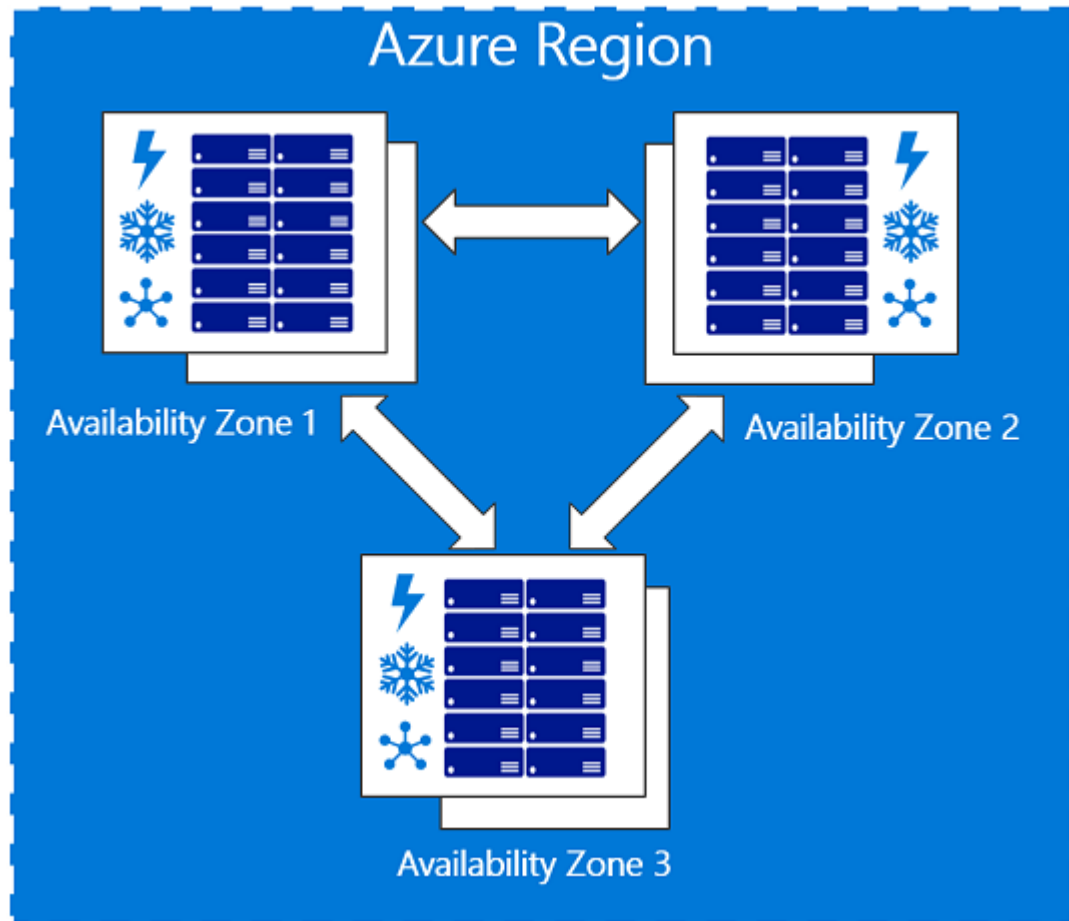


Planning for Availability



VM Availability Zones

Availability Zones



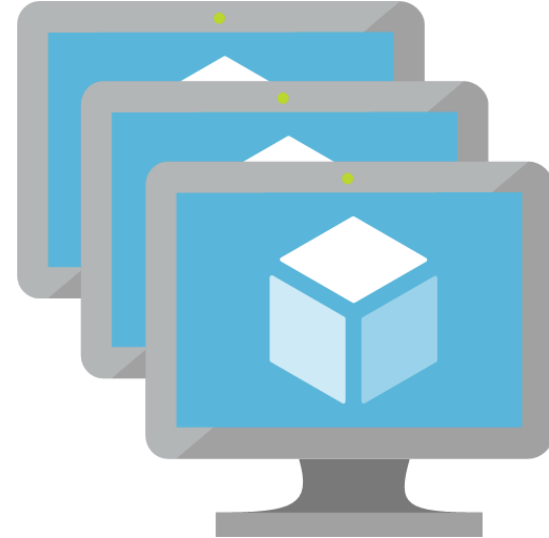
- Offer 99.99% availability
- Minimize impact of planned and unplanned downtime
- Enforce them like Availability Sets, but now you choose your specific zone in Azure

VM Scaling

Scale Sets



VS.



Define Virtual Machine Scale Set (VMSS)

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

INSTANCES AND LOAD BALANCER

* Instance count ⓘ	<input type="text" value="2"/>
* Instance size (View full pricing details) ⓘ	<input type="text" value="D1_v2 (1 vCPU, 3.5 GB)"/>
Enable scaling beyond 100 instances ⓘ	<input checked="" type="radio"/> No <input type="radio"/> Yes
Use managed disks ⓘ	<input type="radio"/> No <input checked="" type="radio"/> Yes
* Public IP address name ⓘ	<input type="text"/>
Public IP allocation method	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static
* Domain name label ⓘ	<input type="text" value=""/> .northcentralus.cloudapp.azure.com

AUTOSCALE

Autoscale ⓘ	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
-------------	---

Configure Autoscale Rules

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

AUTOSCALE

Autoscale ⓘ

Disabled Enabled

* Minimum number of VMs ⓘ

1

* Maximum number of VMs ⓘ

10

Scale out

* CPU threshold (%) ⓘ

75

* Number of VMs to increase by ⓘ

1

Scale in

* CPU threshold (%) ⓘ

25

* Number of VMs to decrease by ⓘ

1

VM Security Best Practices

Reference Documentation

Security best practices for IaaS workloads in Azure

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

VM Security: Control Access

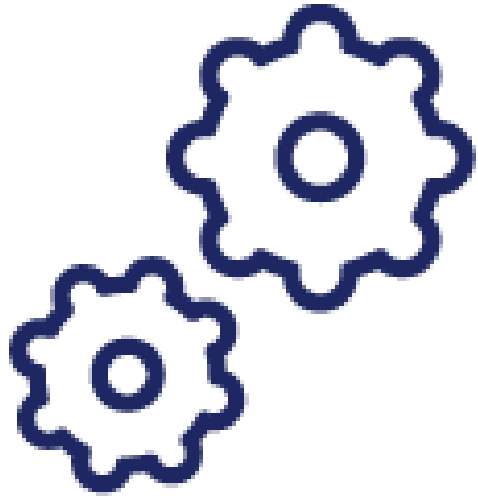


Best practice: Control VM access.

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

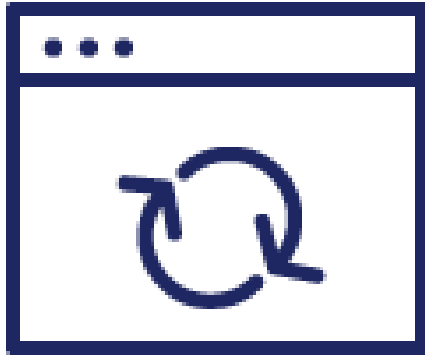


Best practice: Keep your VMs current.

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.

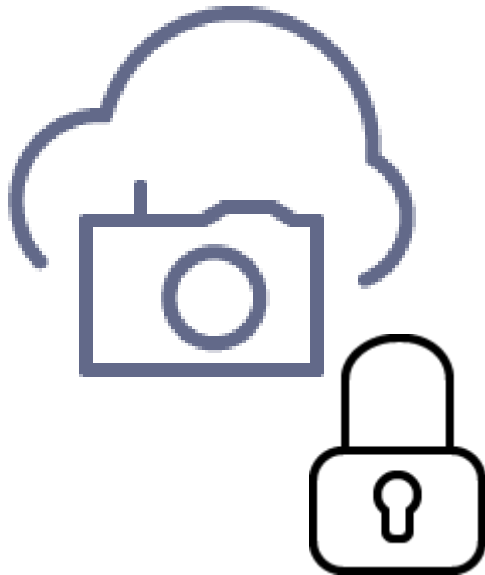
VM Security: Backup



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

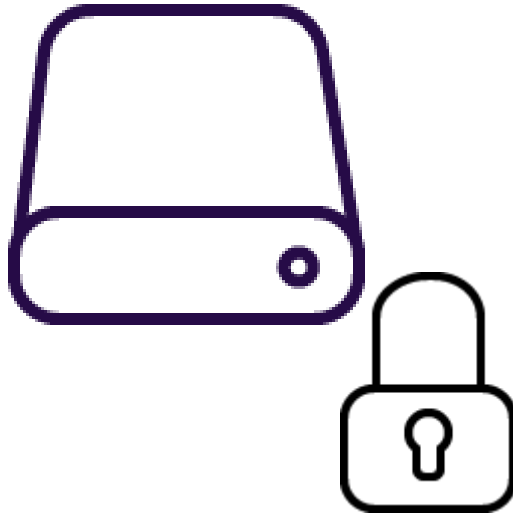


Best practice: Monitor your VM performance

Details:

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

VM Security: Disk Encryption

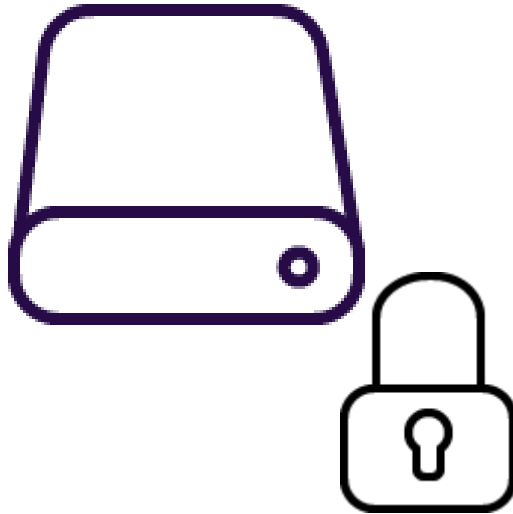


Best practice: Enable encryption on VMs.

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

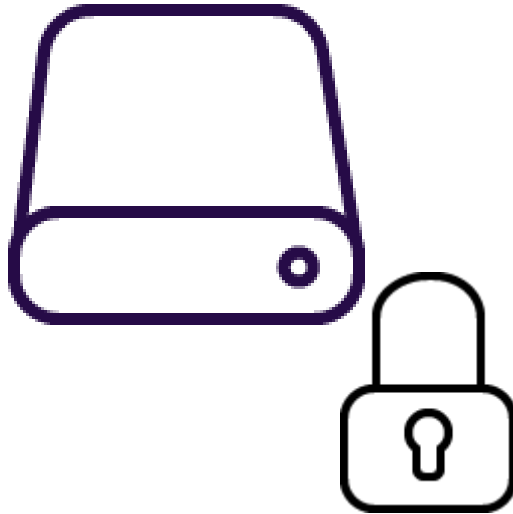


Best practice: Use a key encryption key (KEK) for an additional layer of security for encryption keys. Add a KEK to your key vault.

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: 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.

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

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)

- ✓ 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

- × 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

Supported VM Sizes

Not Available on A-Series
Check Minimum Memory Requirements

Supported OS

Windows 8 and Later
Windows Server 2008 R2
and Later
See Linux Table

Networking

Connectivity to Azure AD
Connect to KeyVault
Azure Storage

Key Vault

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>

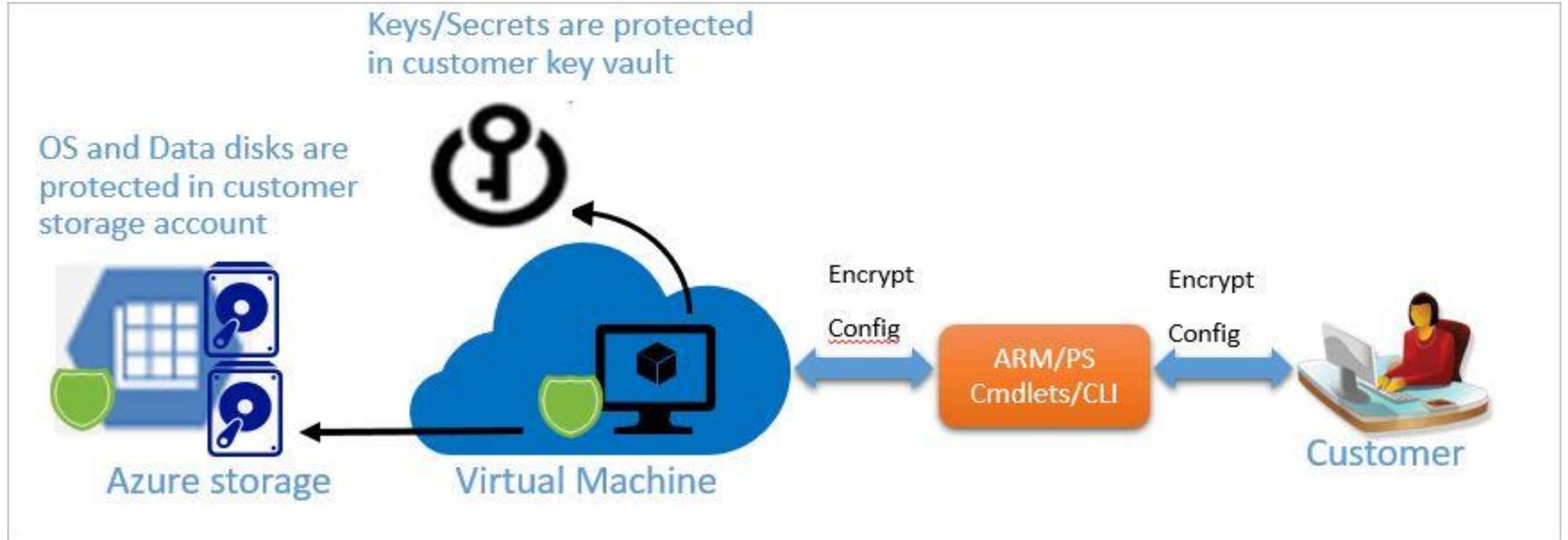
Configuration Methods

PowerShell

Azure CLI

ARM Templates

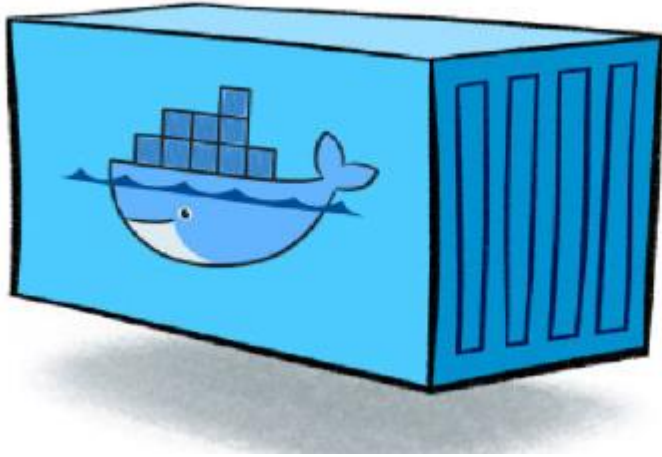
Azure Disk Encryption Elements



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

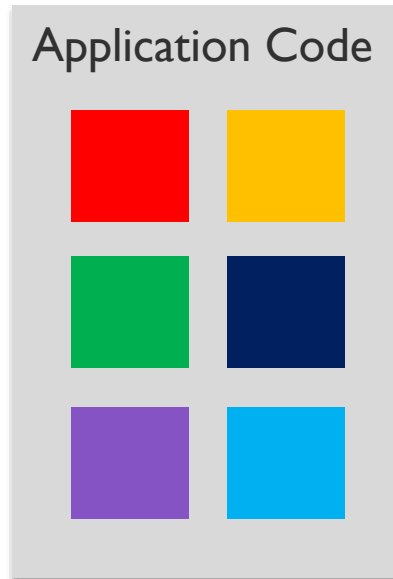
Containers

What is a Docker Container?



- Standardized packaging for software and dependencies
- A way to isolate apps from each other
- Works with Linux and Windows Servers
- Allows separate apps to share the same OS kernel

Application Modernization



Monolithic App Issues:

- Minor code requires full recompile and testing
- Application becomes a single point of failure
- Application is difficult and often expensive to scale

Application Modernization

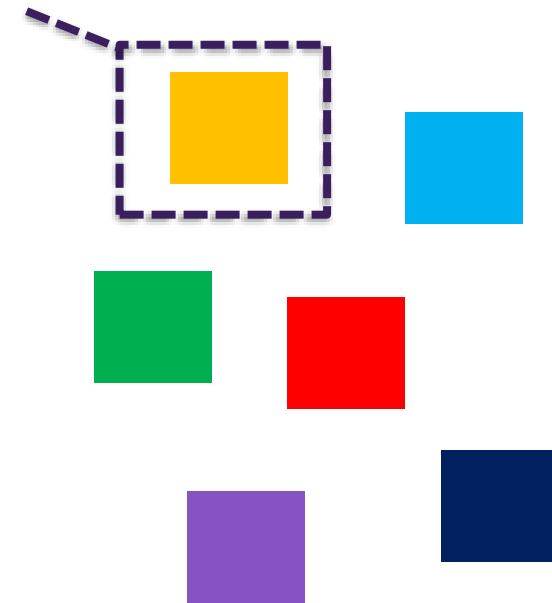
Microservices:

- Break application out into separate services

12-Factor Apps:

- Make the app independently scalable, stateless, highly available design.

Individual service



Comparing Monolithic and Microservices

Monolithic

Simple deployments
Inter-module refactoring
Vertical scaling
Technology monoculture

Microservices

Partial deployments
Strong module boundaries
Horizontal scaling
Technology diversity

Three Keys to Microservices

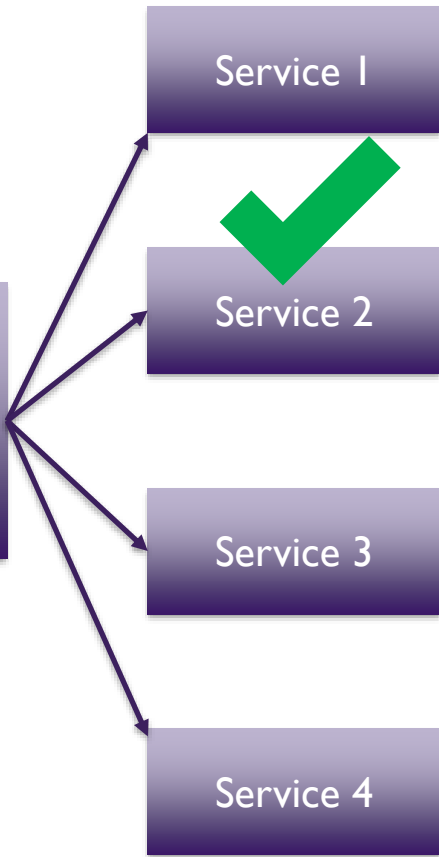
1. Functional Decomposition

This...

Becomes This

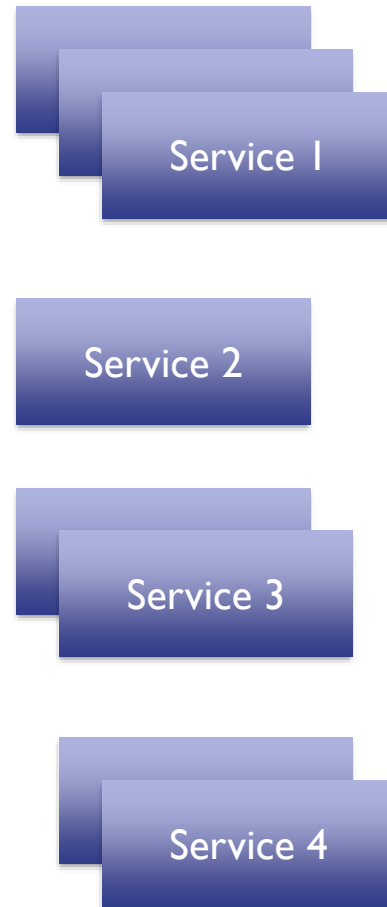


All services tightly coupled and error prone



2. Horizontal Scale

Scale what you need to, not what you don't

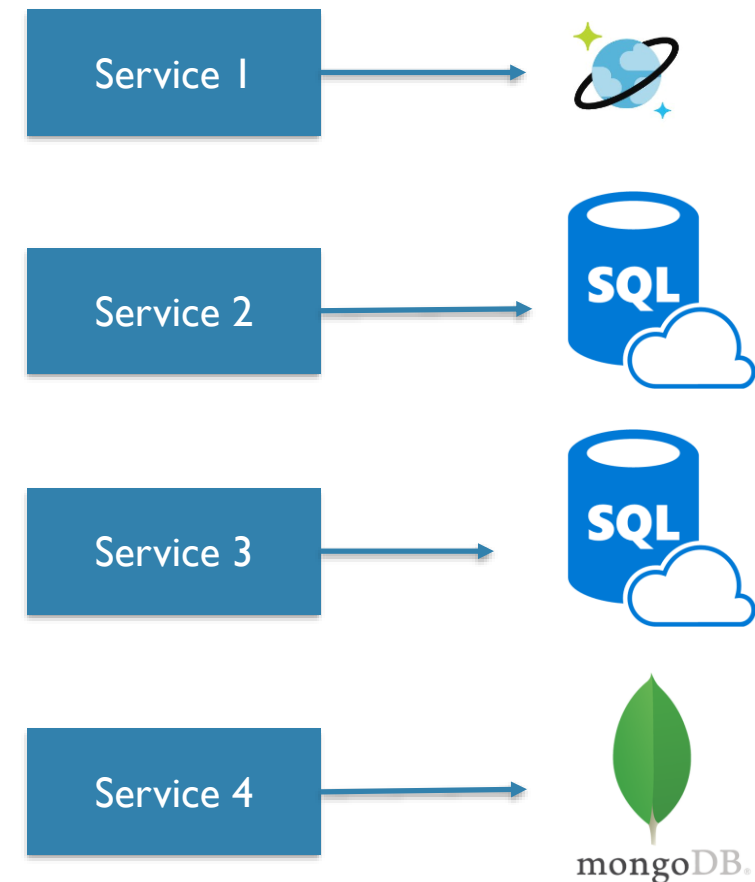


Scaling Options

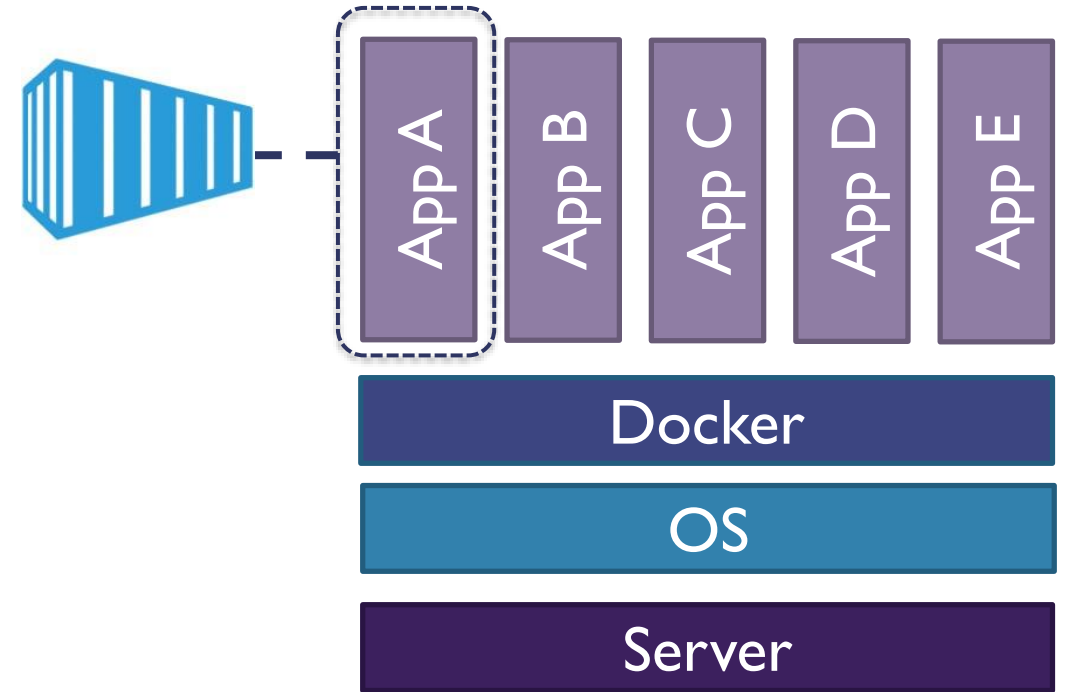
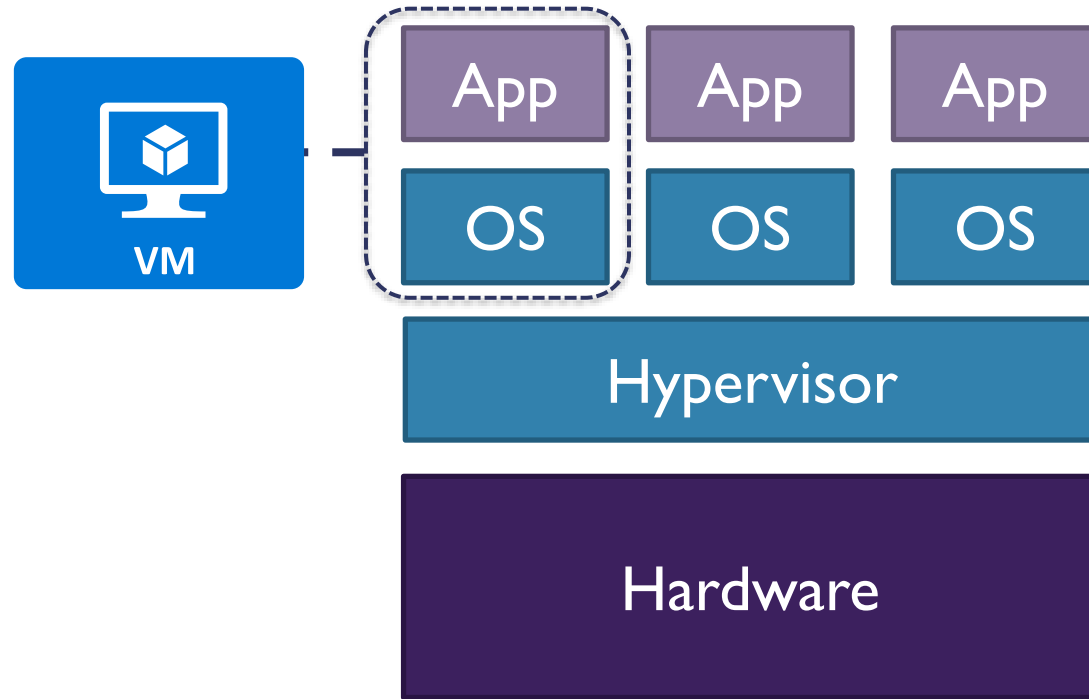


3. Data Decoupling

Now I can pick the best database for the service



Containers vs. Virtual Machines



Docker Container Benefits

Speed

No OS to boot =
application online in
seconds

Portability

Less dependencies
between process layers =
ability to move between
infrastructure

Efficiency

Less OS overhead
Improved VM density

Docker Basics

Image	The basis of a Docker container. The content is at rest
Container	The image when it is 'running'. The standard unit for the app service.
Engine	The software that executes commands for containers. Networking and volumes are part of the Engine. Can be clustered together.
Registry	Stores, distributes and manages Docker containers.
Control Plane	Management plane for container and cluster orchestration.

Container Security: AKS

AKS Security

Container Security
(Customer)

Node Security
(Customer)

Master Security
(Microsoft)

AKS Security: Best Practices

Secure Access
to AKS

Secure
Container
Access

Update AKS
Nodes

App Services Overview

Introduction to Web Apps

Azure App Services consist of the following:

Web Apps

Mobile Apps

Logic Apps

API Apps

Web Apps

- Formerly "Websites"
- Build and host apps with various programming languages
- Auto-scalable
- Highly-available
- DevOps features



Mobile Apps

- Build a mobile device backend
- Highly-scalable
- Highly-available
- Build native apps for iOS, Android, Windows, cross-core platform apps
- **BENEFIT:** Share same App Service deployment to reduce run rates



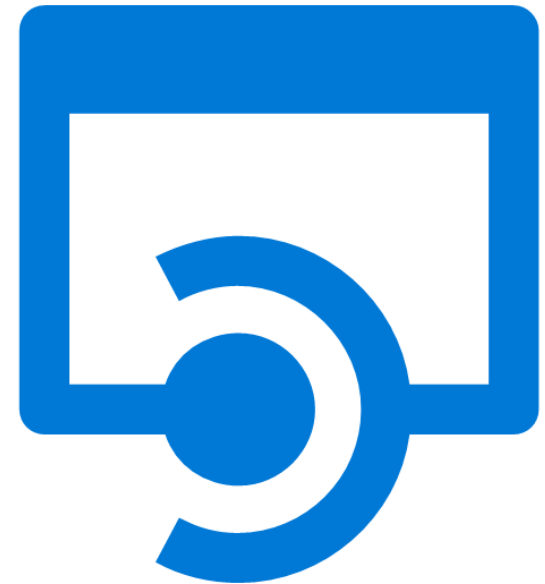
Logic Apps

- Automate business processes and workflows
- Use the orchestration engine to build a solution
- Examples:
 - Every time your app calls an API do some task
 - Routinely ingest data from a storage blob or external SaaS- based service
 - Regularly check Tweets or #SLACK messages from a specific account



API Apps

- Allow us to easily create, consume, and call APIs
- Option to use APIs you create
- Could also be from external API services



Security Features

- Features run on isolated VM
- ISO, SOC, and PCI compliant
- Fully-integrated Azure Active Directory
- Managed service identity (currently in preview)
- Support custom domains, SSL/TLS, including custom certificates using wildcard or subject alternate name
- Supports multiple authentication protocols: OAuth, OpenID, and Microsoft Active Directory
- Integrates with Web Application Firewall (WAF)

DevOps Features

CI/CD Support

IDE Tool
Integration

Deployment Slots

App Service Plans Overview

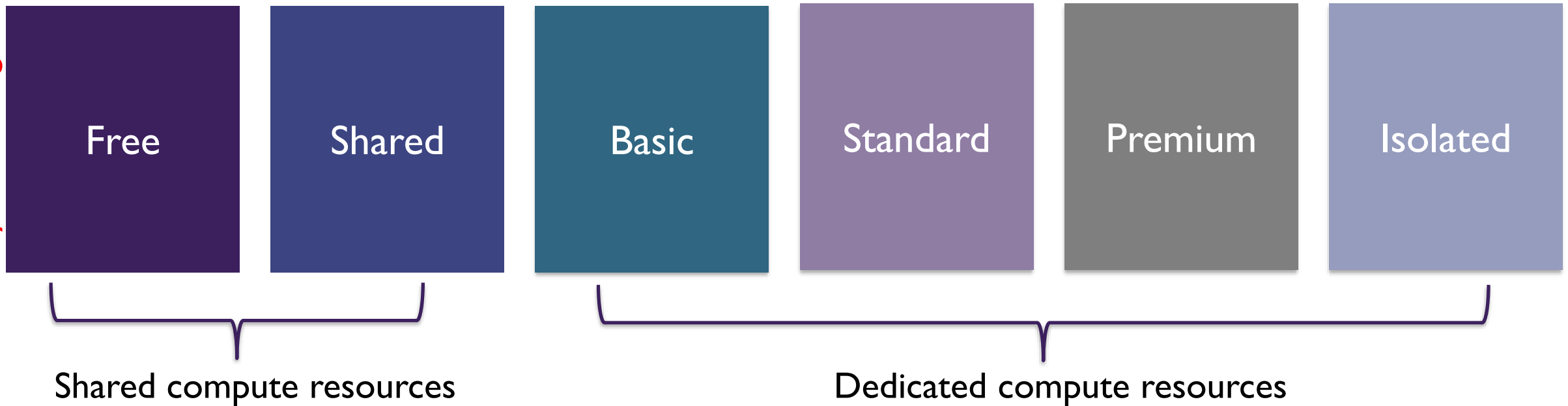
First define the following:

- Subscription the plan belongs to
- Location (e.g. North Central US, etc.)
- Pricing tier (Free, Shared, Basic, Standard Premium, Isolated)
- Instance size (Small, Medium, Large)

Then configure settings:

- Scale count (1,2, 3 instances, etc.)
- Scale rules – Allow for auto scaling if the plan supports it
- Scale up – increasing the resources associated with the App Service Plan (this is essentially how you switch the plan you defined at the start)

App Service Plan Pricing Tiers



<https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits>

App Service Plans – General Guidelines



- Create for specific applications
- Deploy app services to support the application
- Do not use a single plan for every web app
- Combine app services vs. mass VM creation
- Combine other services in the same resource group

App Service Environments (ASEs)

- Fully isolated environment
- For high-performing apps – high CPU and/or memory
- Individual or multiple services plans
- 2 ways to deploy: *Internal* or *External*
- Created in a subnet of a VNet, which achieves isolation
- *Note:* May take a few hours to spin up

App Services

App Services can support the following:

Web Apps

Mobile Apps

Logic Apps

API Apps

App Service Plans Overview

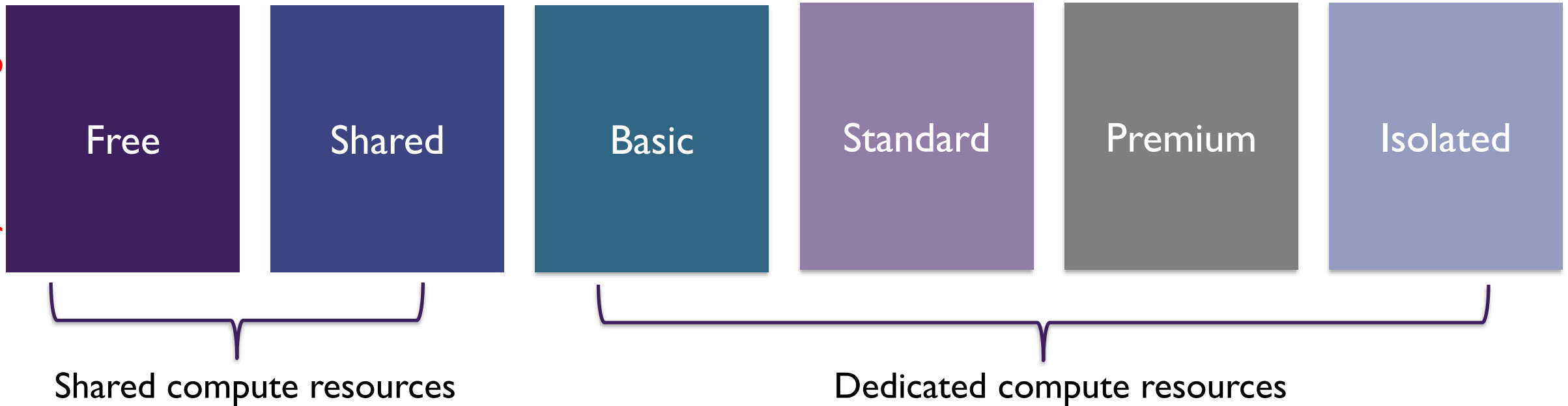
First define the following:

- Subscription the plan belongs to
- Location (e.g. North Central US, etc.)
- Pricing tier (Free, Shared, Basic, Standard Premium, Isolated)
- Instance size (Small, Medium, Large)

Then configure settings:

- Scale count (1,2, 3 instances, etc.)
- Scale rules – Allow for auto scaling if the plan supports it
- Scale up – increasing the resources associated with the App Service Plan (this is essentially how you switch the plan you defined at the start)

App Service Plan Pricing Tiers



<https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits>

App Service Plans – General Guidelines



- Create for specific applications
- Deploy app services to support the application
- Do not use a single plan for every web app
- Combine app services vs. mass VM creation
- Combine other services in the same resource group

App Service Environments (ASEs)

- Fully isolated environment
- For high-performing apps – high CPU and/or memory
- Individual or multiple services plans
- 2 ways to deploy: *Internal* or *External*
- Created in a subnet of a VNet, which achieves isolation
- *Note:* May take a few hours to spin up

App Service Monitoring

Management Tools

Management
Portal

Kudu

Visual Studio

PowerShell

CLI

App Service Plan Metrics

Component	Description
CPU Percentage	The average CPU used across all instances of the plan.
Memory Percentage	The average memory used across all instances of the plan.
Data In	The average incoming bandwidth used across all instances of the plan.
Data Out	The average outgoing bandwidth used across all instances of the plan.
Disk Queue Length	The average number of both read and write requests that were queued on storage. A high disk queue length is an indication of an application that might be slowing down due to excessive disk I/O.
HTTP Queue Length	The average number of HTTP requests that had to sit on the queue before being fulfilled. A high or increasing HTTP Queue length is a symptom of a plan under heavy load.

Free and Shared App Quotas

Component	Description
CPU (Short)	Amount of CPU allowed for this application in a 5-minute interval. This quota resets every 5 minutes.
CPU (Day)	Total amount of CPU allowed for this application in a day. This quota resets every 24 hours at midnight UTC.
Memory	Total amount of memory allowed for this application.
Bandwidth	Total amount of outgoing bandwidth allowed for this application in a day. This quota resets every 24 hours at midnight UTC.
Filesystem	Total amount of storage allowed.

Results of Exceeding Quota

Component	Result of Exceeding Quota
CPU	Exceeding either CPU (short) or the CPU (day) quota will result in the application being stopped until the quota resets. During this time, all incoming requests result in a HTTP 403.
Memory	The application is restarted.
Bandwidth	Application is stopped until the quota resets. During this time, all incoming requests result in a HTTP 403.
Filesystem	Write operations including writes to logs, will fail.

Azure Web App Diagnostic Logs

1. Application

- Error
- Warning
- Information
- Verbose

2. Web Server

- Web Server Logging
- Detailed Error Message
- Failed Request Tracing

Diagnostic Logs and Locations

Type	Location- /LogFiles/
Application Logs	Application/
Failed Request Traces	W3SVC#####/
Detailed Error Logs	DetailedErrors/
Web Server Logs	http/RawLogs
Deployment Logs	/Git

Creating Alerts in Application Insights

Alert Type	Description
Metric	A metric crosses a metric threshold for a period of time.
Web Tests	A site is not available or is responding slowly.
Proactive Diagnostics	Triggered when something out of the ordinary occurs.

Application Settings

Connection Strings

Characteristics

- Configuring connection strings will allow us to specify database servers that can be utilized per slot
- The connection string is a *variable* instead of a configuration file
- It is secure because it doesn't store information as a file

Variable Prefixes

SQL Server: `SQLCONNSTR_`

MySQL: `MYSQLCONNSTR_`

SQL Database: `SQLAZURECONNSTR_`

Custom: `CUSTOMCONNSTR_`

Handler Mappings

Extension

The file extension to be handled e.g. *.py, *.php, etc.

Processor Path

The absolute path of the script processor

Additional Arguments (Optional)

Additional command-line arguments for your script processor

Handler mappings

No results

Extension

Processor path

Additional arguments

...

Virtual Applications and Directories

Virtual Directory
Path users will take to access the application

Physical Path
Path to the physical directory or application

Application
Virtual directory by default; must select for web app

Virtual applications and directories			
/	site\wwwroot	<input checked="" type="checkbox"/> Application	...
<input type="text" value="Virtual directory"/>	<input type="text" value="Physical path relative to site root"/>	<input type="checkbox"/> Application	...

Custom Domains for Web Apps

SETTINGS



Application settings



Authentication / Authorization



Managed service identity



Backups



Custom domains



SSL certificates



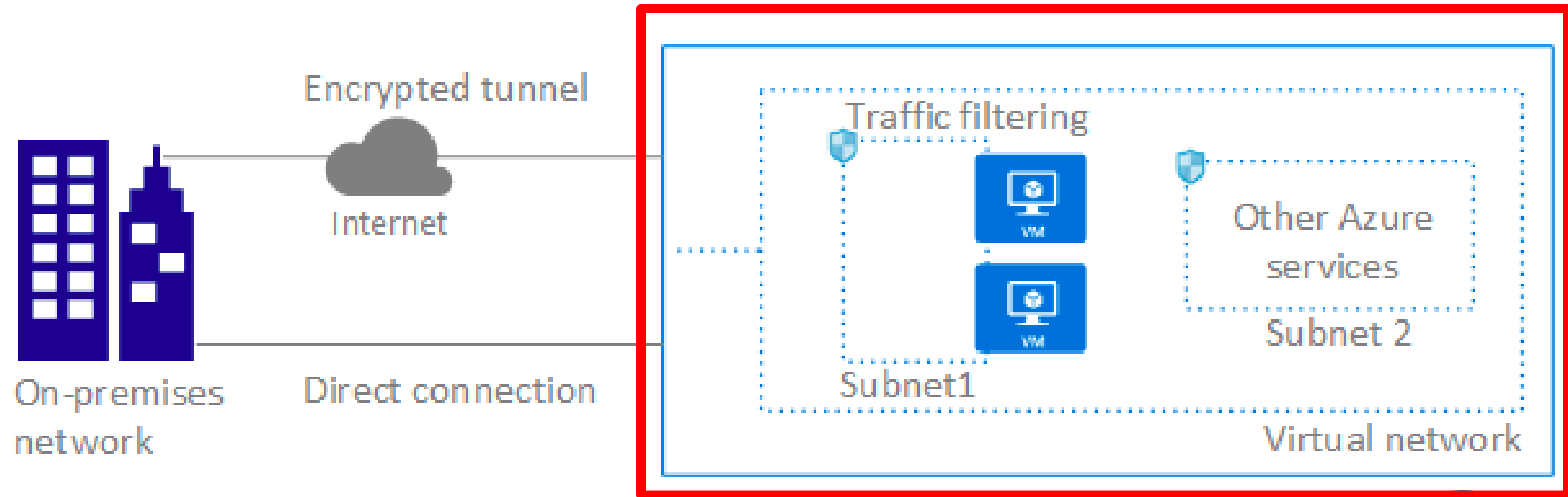
Networking

Steps:

1. Select custom name from registrar
2. Add DNS record
3. Associate with web app

Network Overview

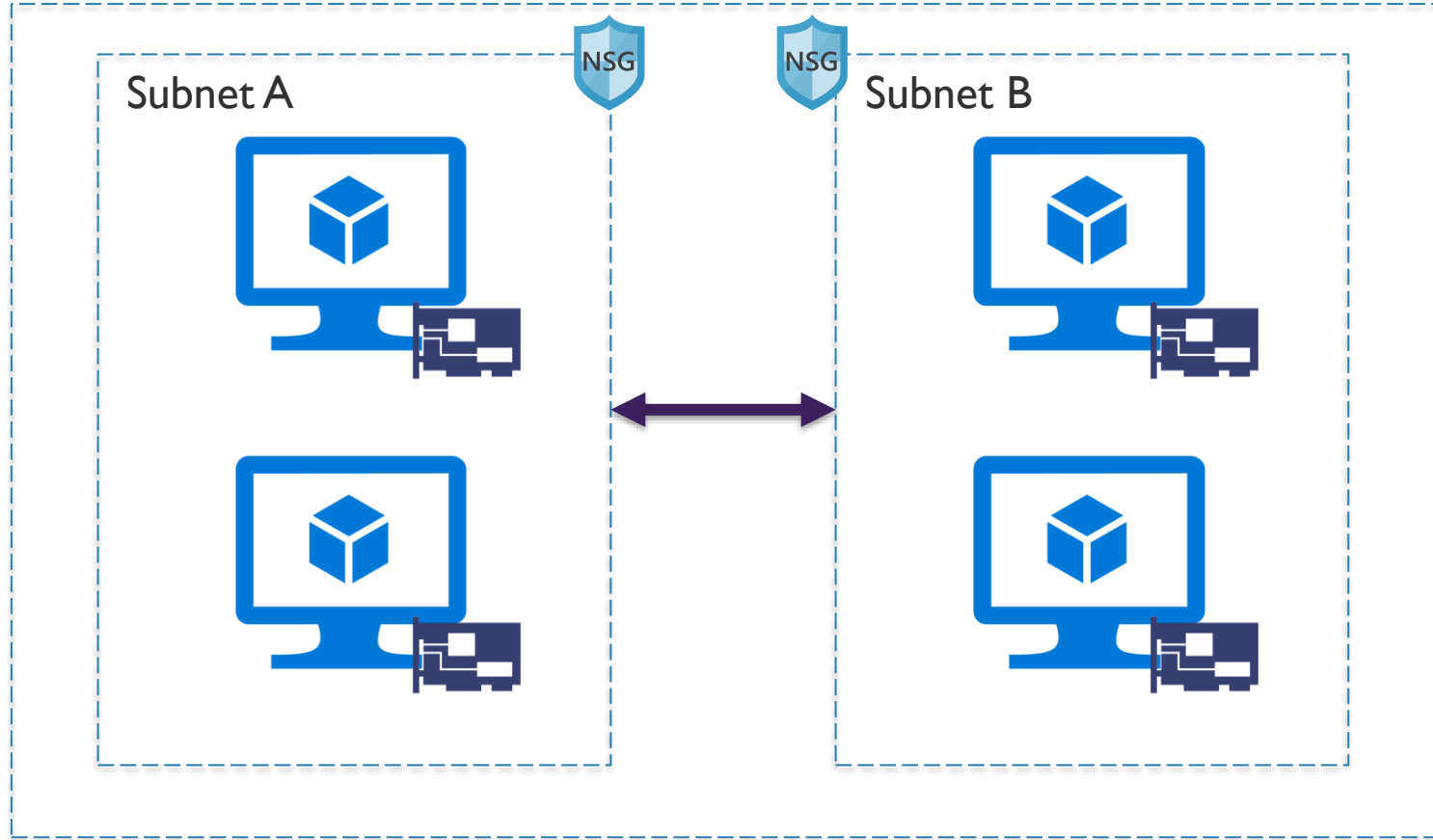
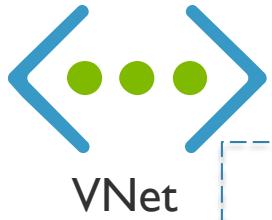
Networking Overview



Microsoft
Azure

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

- 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

Routing and Peering

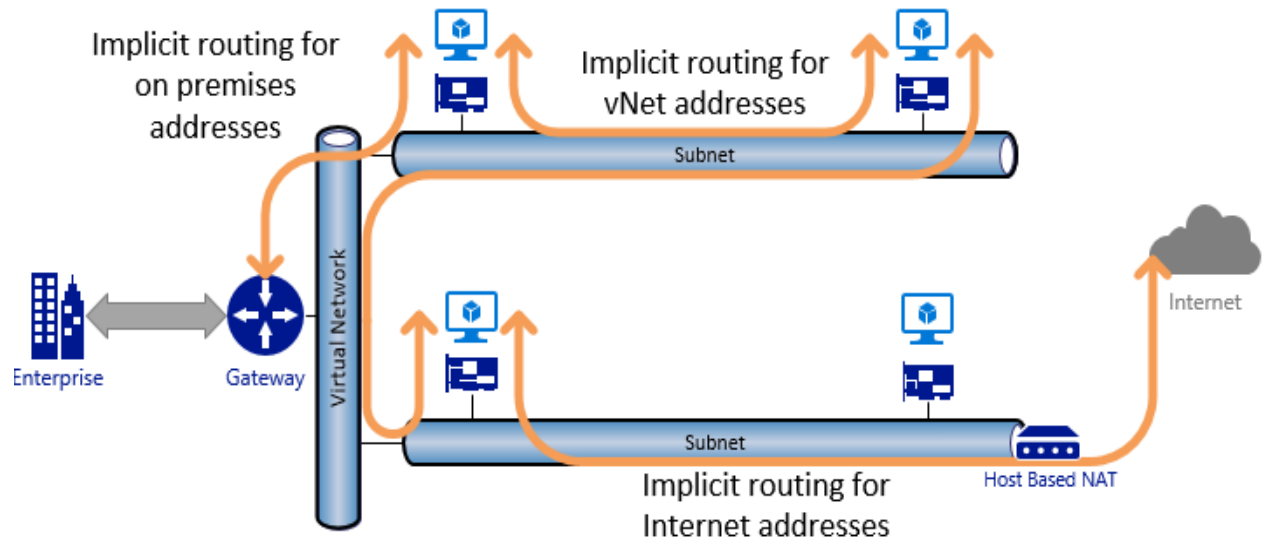
System Routes

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

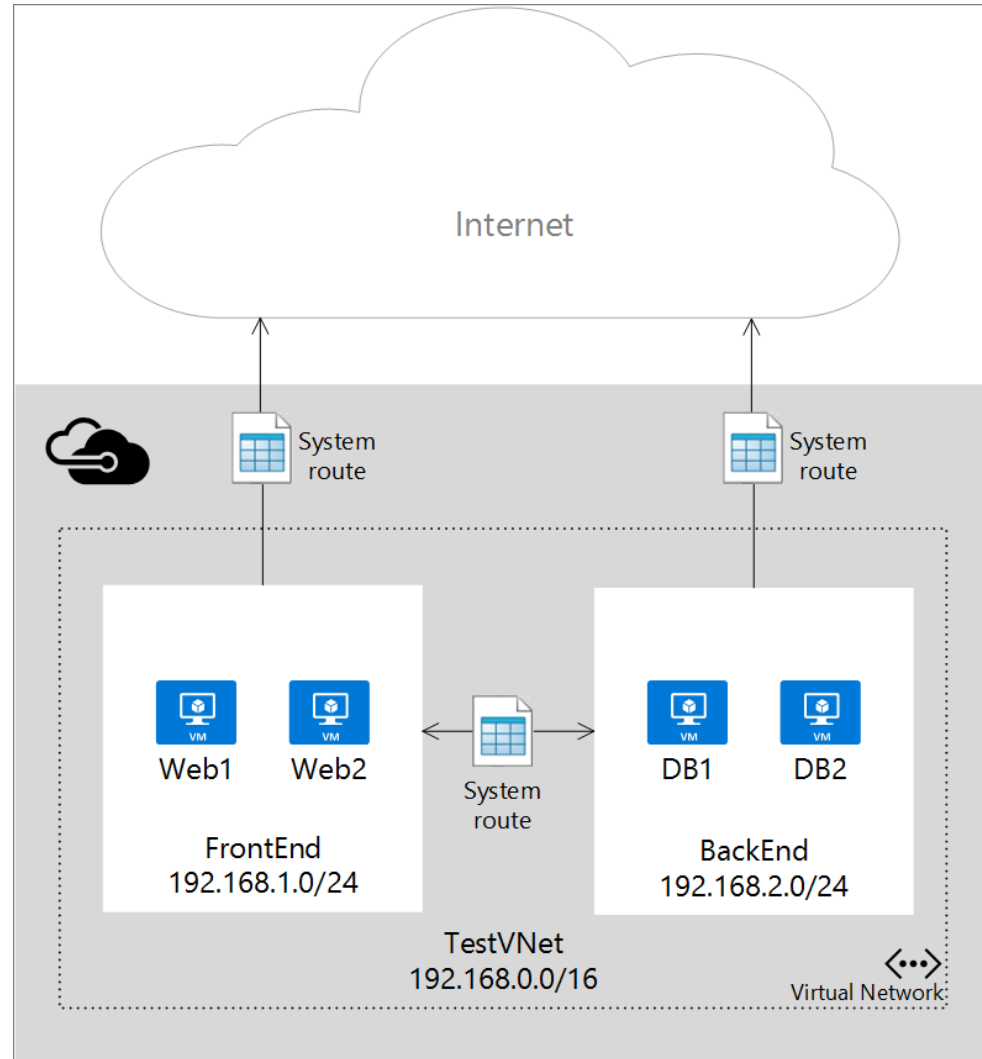
Route	Description
Local VNet	Route for local addresses (no next-hop value)
On-Premises	Route for defined on-premises address space (VNet gateway is next-hop address)
Internet	Route for all traffic destined to the Internet (Internet Gateway is the next-hop address)

Default Routing in a Subnet

- If address is within the VNet address prefix – *route to local VNet*
- If the address is within the on-premises address prefixes or BGP published routes (BGP or Local Site Network (LSN) for S2S) – *route to gateway*
- If the address is not part of the VNet or the BGP or LSN routes – *route to internet via NAT*
- If destination is an Azure datacenter address and ER public peering is enabled – *it is routed to the gateway*
- If the destination is an Azure datacenter with S2S or an ER without public peering enabled, *it is routed to the Host NAT for internet path, but it never leaves the datacenter*

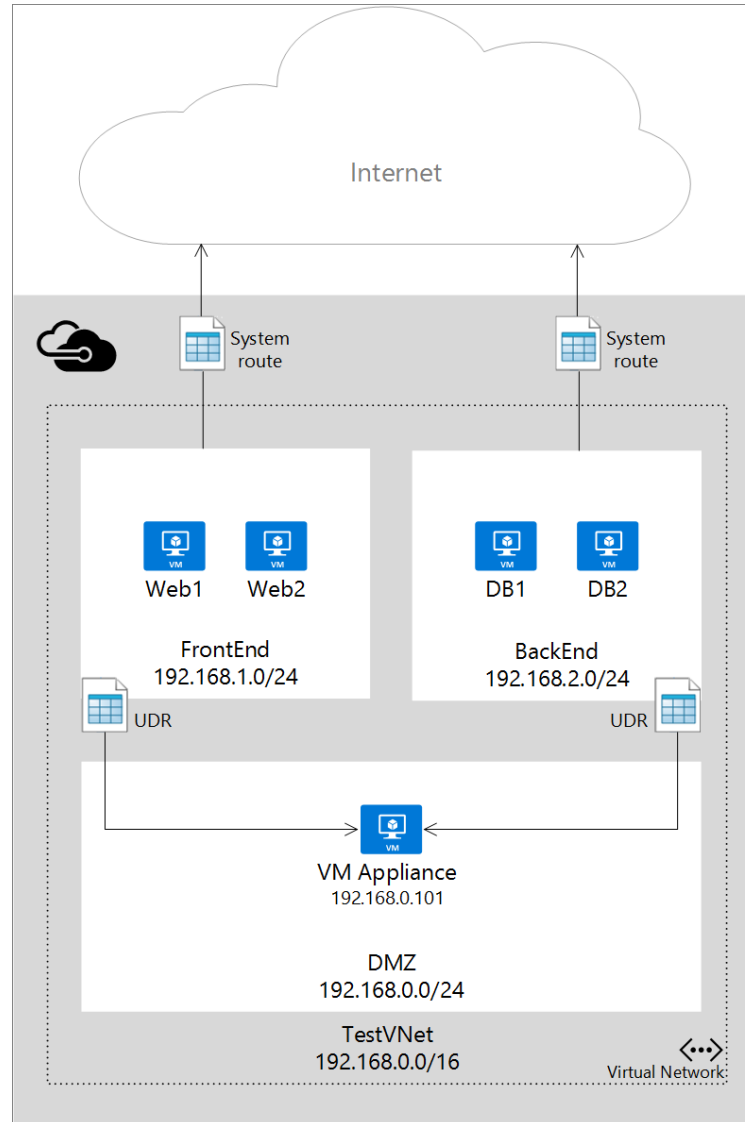


User-Defined Routes

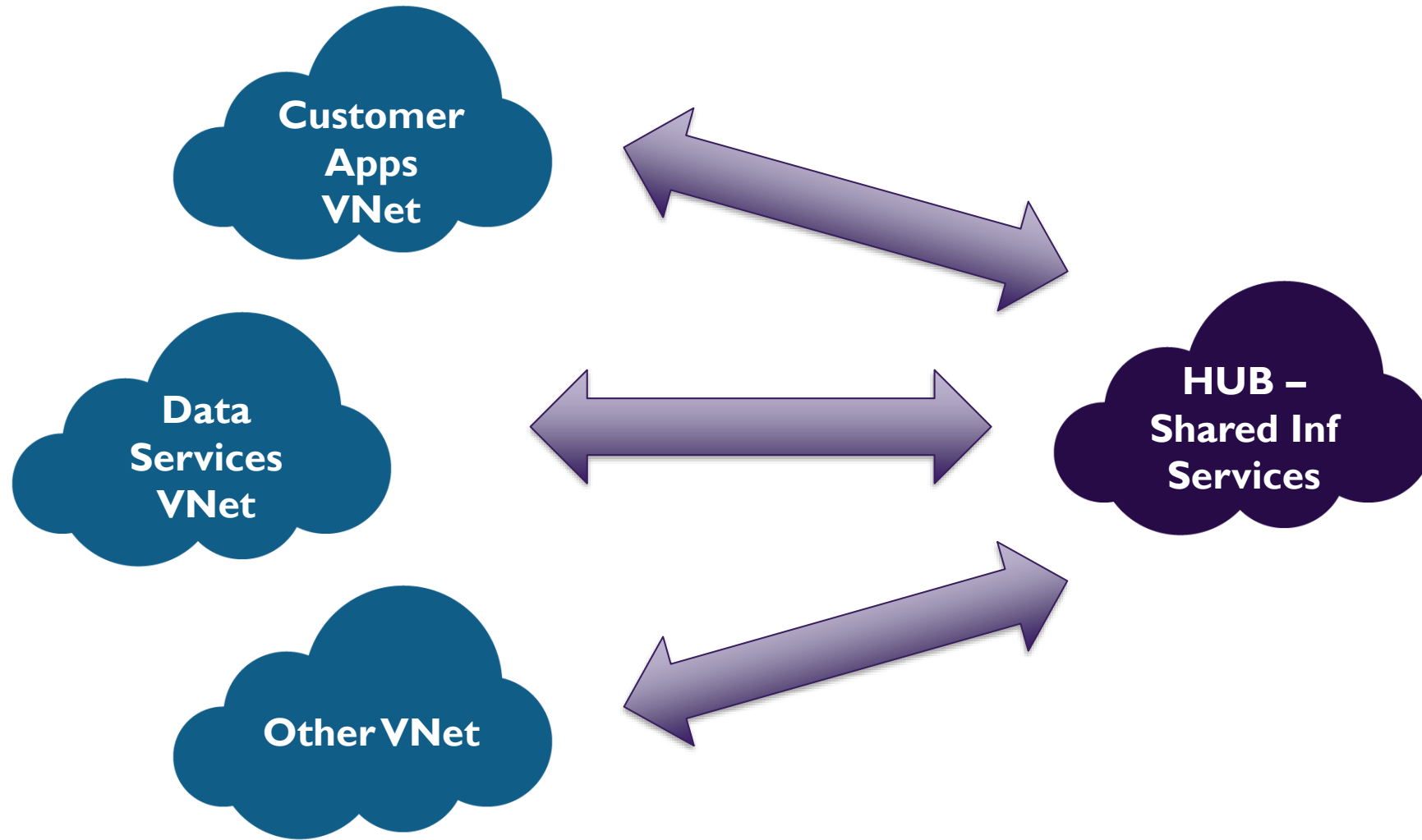


<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

User-Defined Routes (continued)



VNet Peering



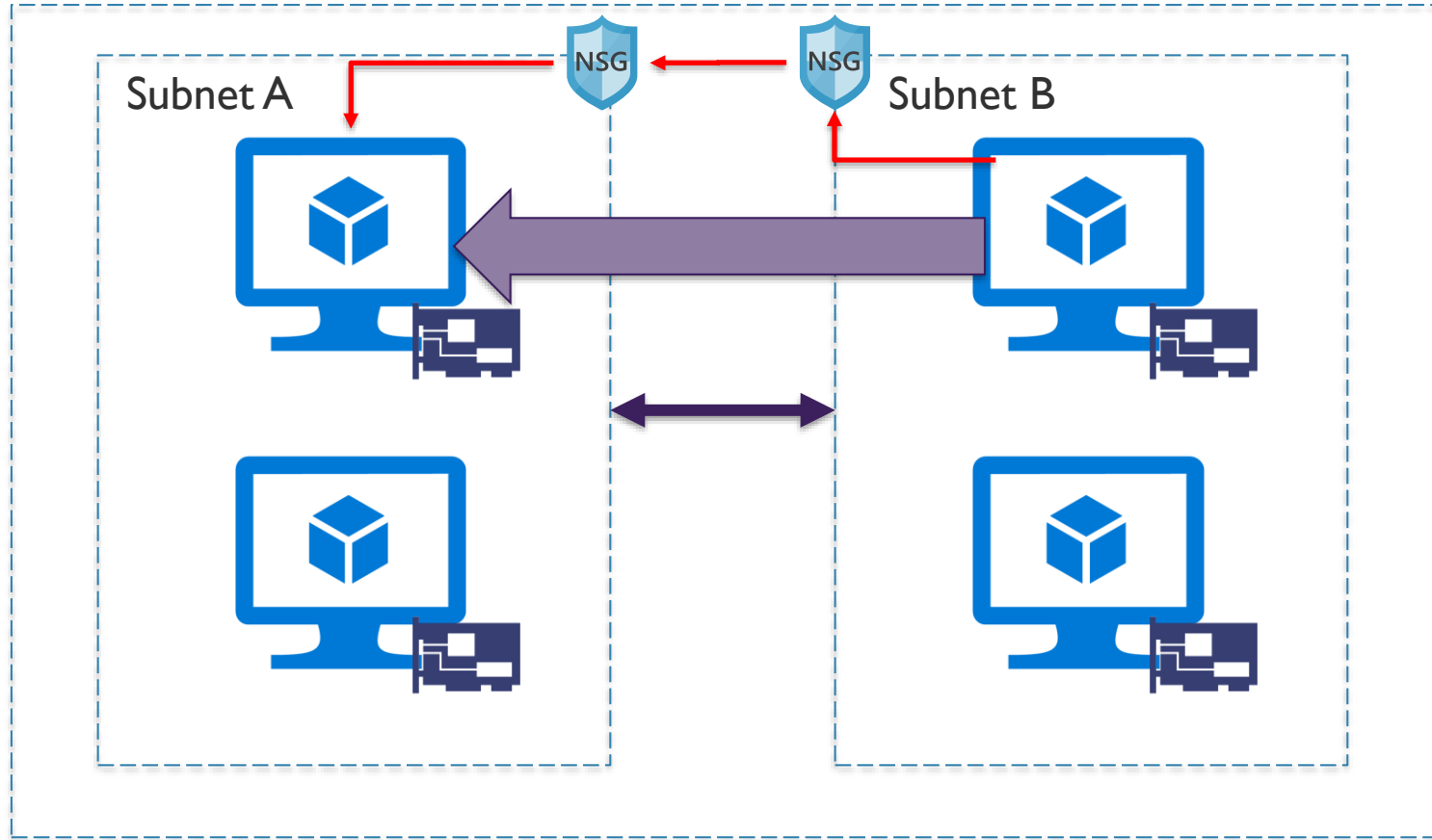
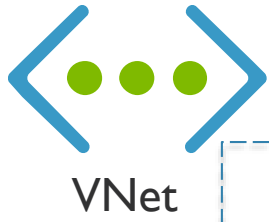
Network Security Groups

Network Security Groups (NSGs)



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

NSGs (continued)



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

NSG Properties

Protocol
(e.g. TCP, UDP)

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

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

Direction
(inbound or
outbound)

Priority

Access
(allow/deny)

NSG Rule Priority

Rules are enforced based on priority

Range from 100 to 4096

Lower numbers have higher priority

NSG Default Tags

System-provided
to identify groups
of IP addresses

Virtual network

Azure Load
Balancer

Internet

NSG Default Rules

INBOUND

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

OUTBOUND

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

Networking Limits

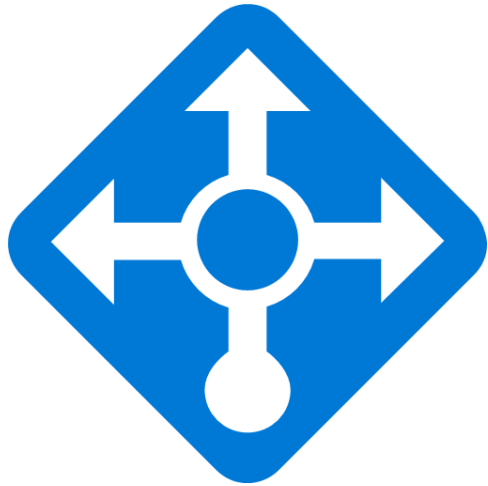
The following limits apply only for networking resources managed through ARM per region per subscription:

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

Load Balancing

Azure Load Balancing Services

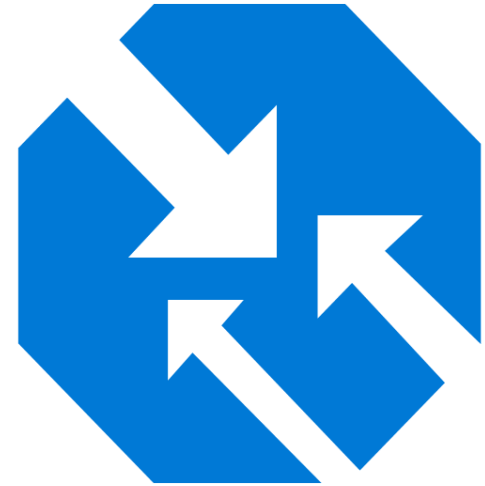
**Load
Balancer**



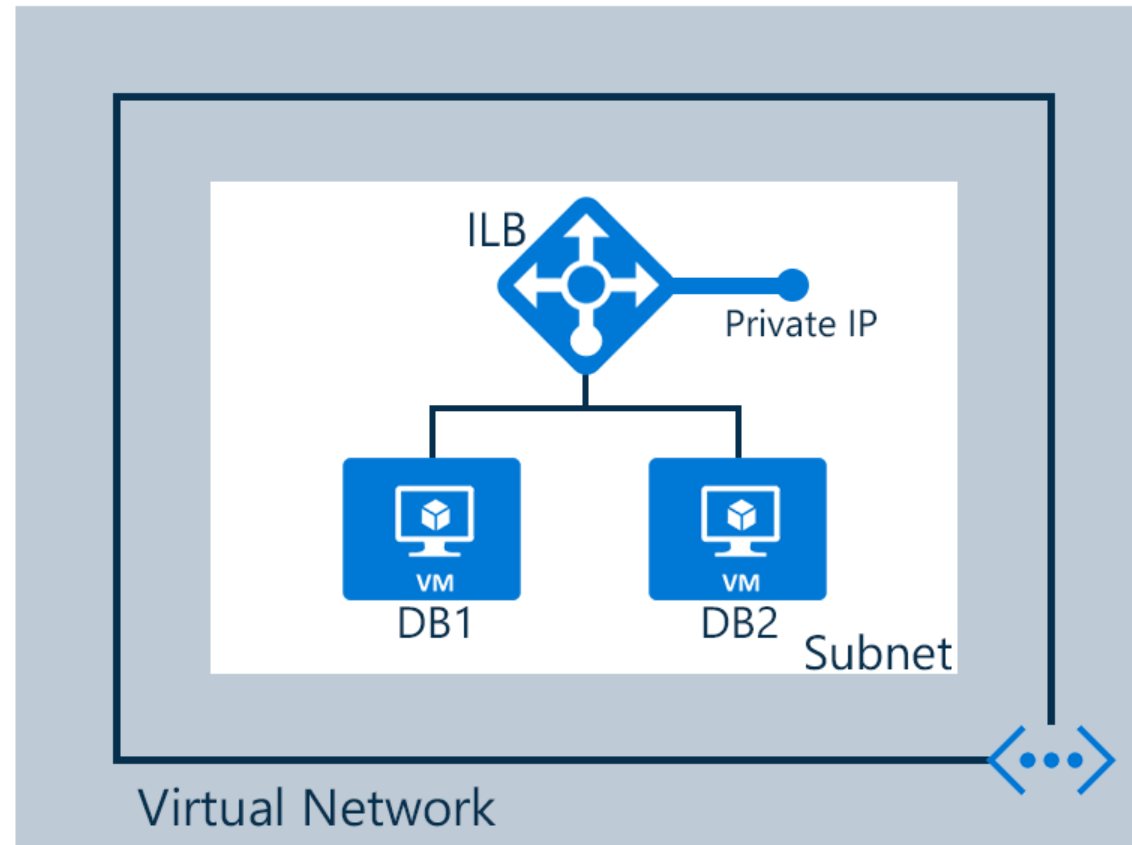
**Application
Gateway**



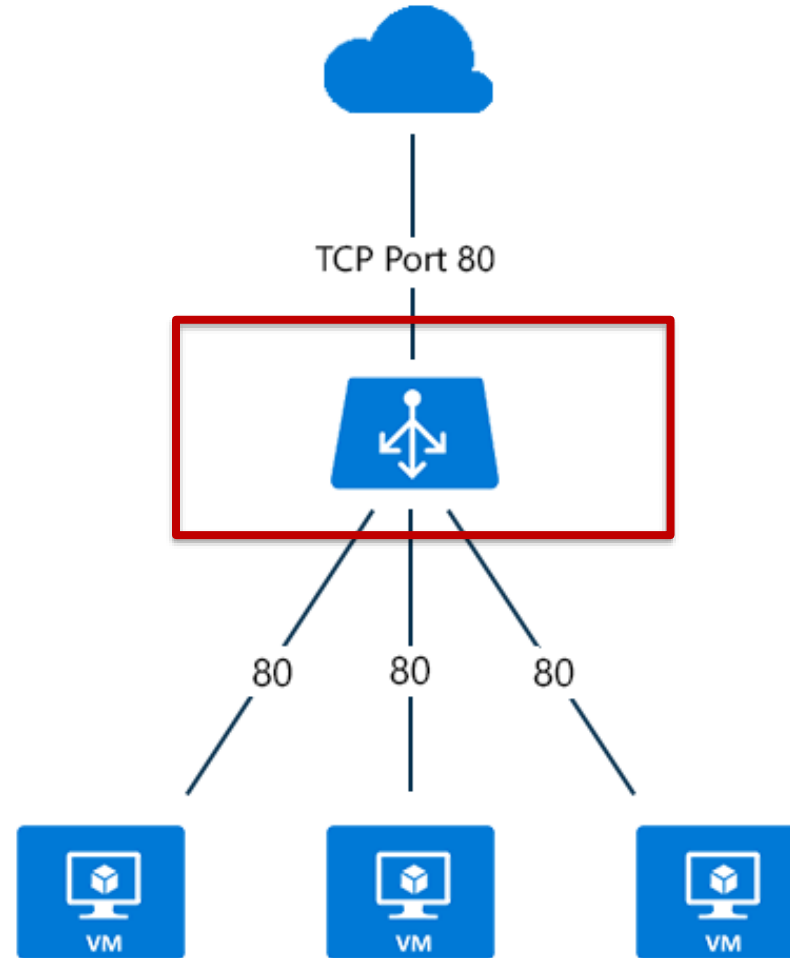
**Traffic
Manager**



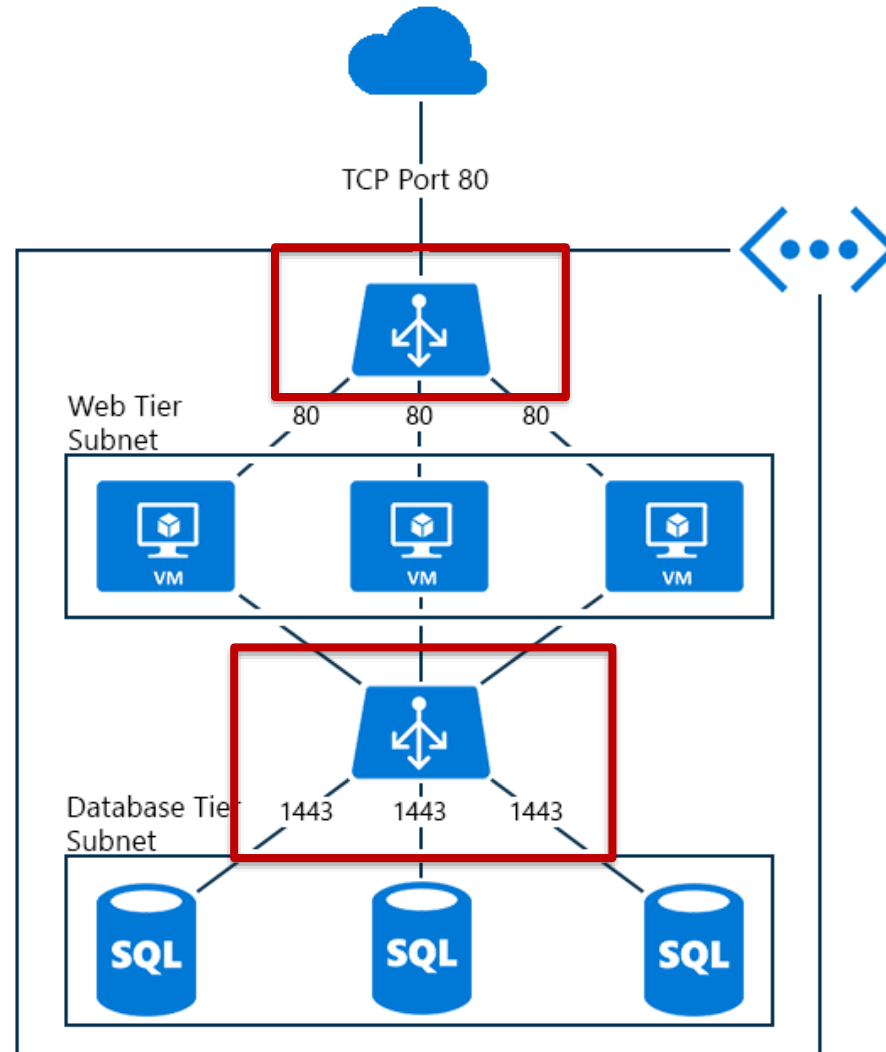
Azure Load Balancer: Internal Example



Azure Load Balancer: Public Example



Azure Load Balancer: Multi-Tier Example



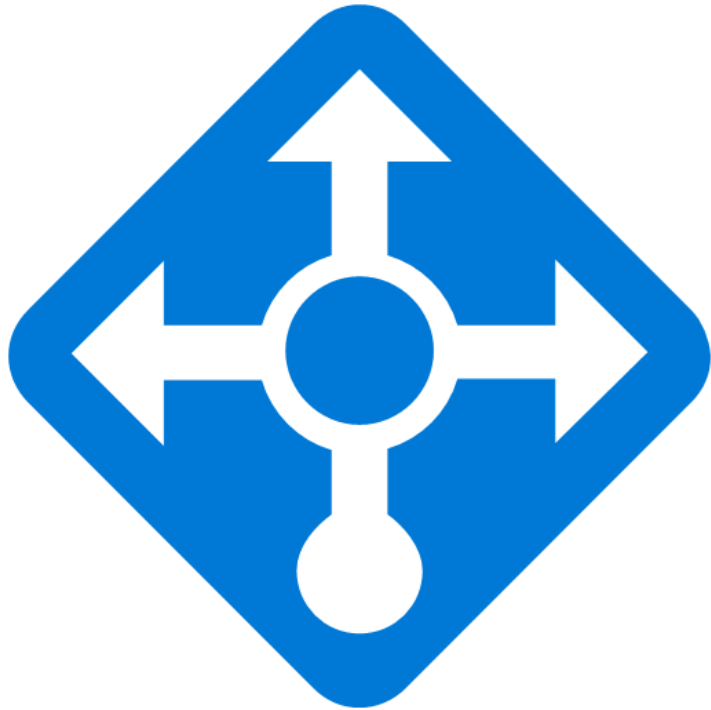
Load Balancing: App Gateway



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

Azure Load Balancer



Key Features:

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

App Gateway Sizes

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

Load Balancer Comparison

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

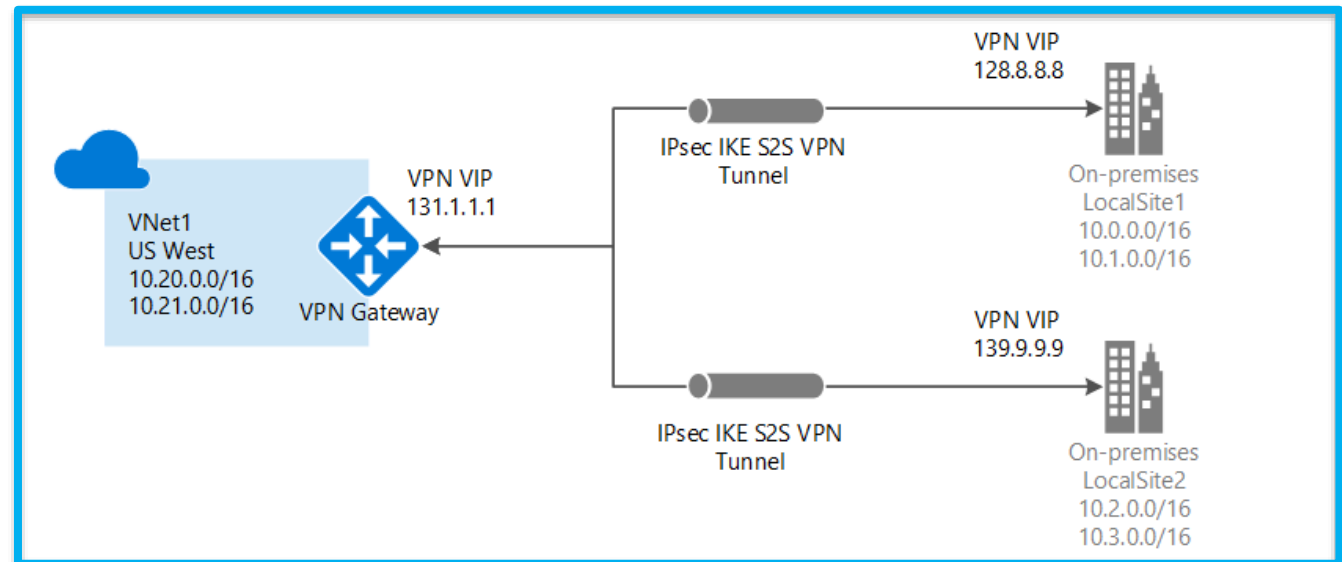
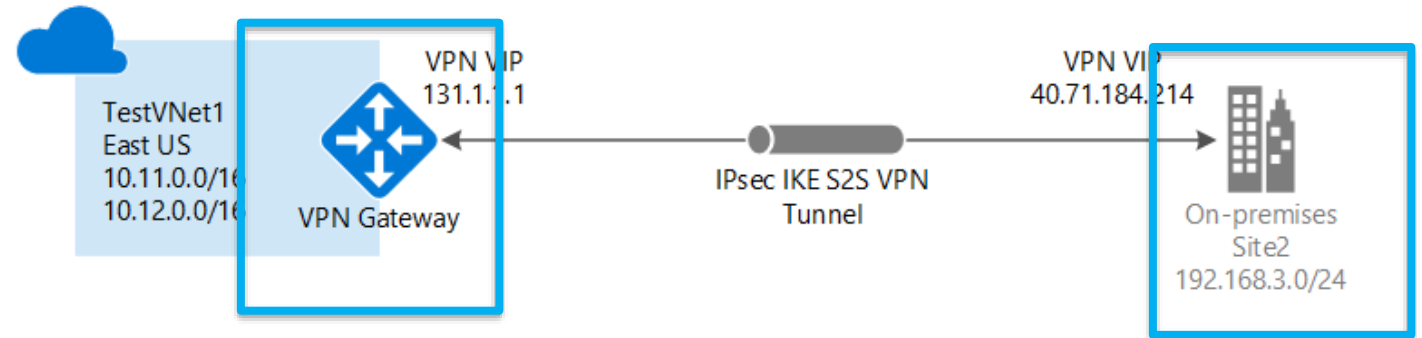
Hybrid Connectivity Options

Site-to-Site (S2S)

ExpressRoute

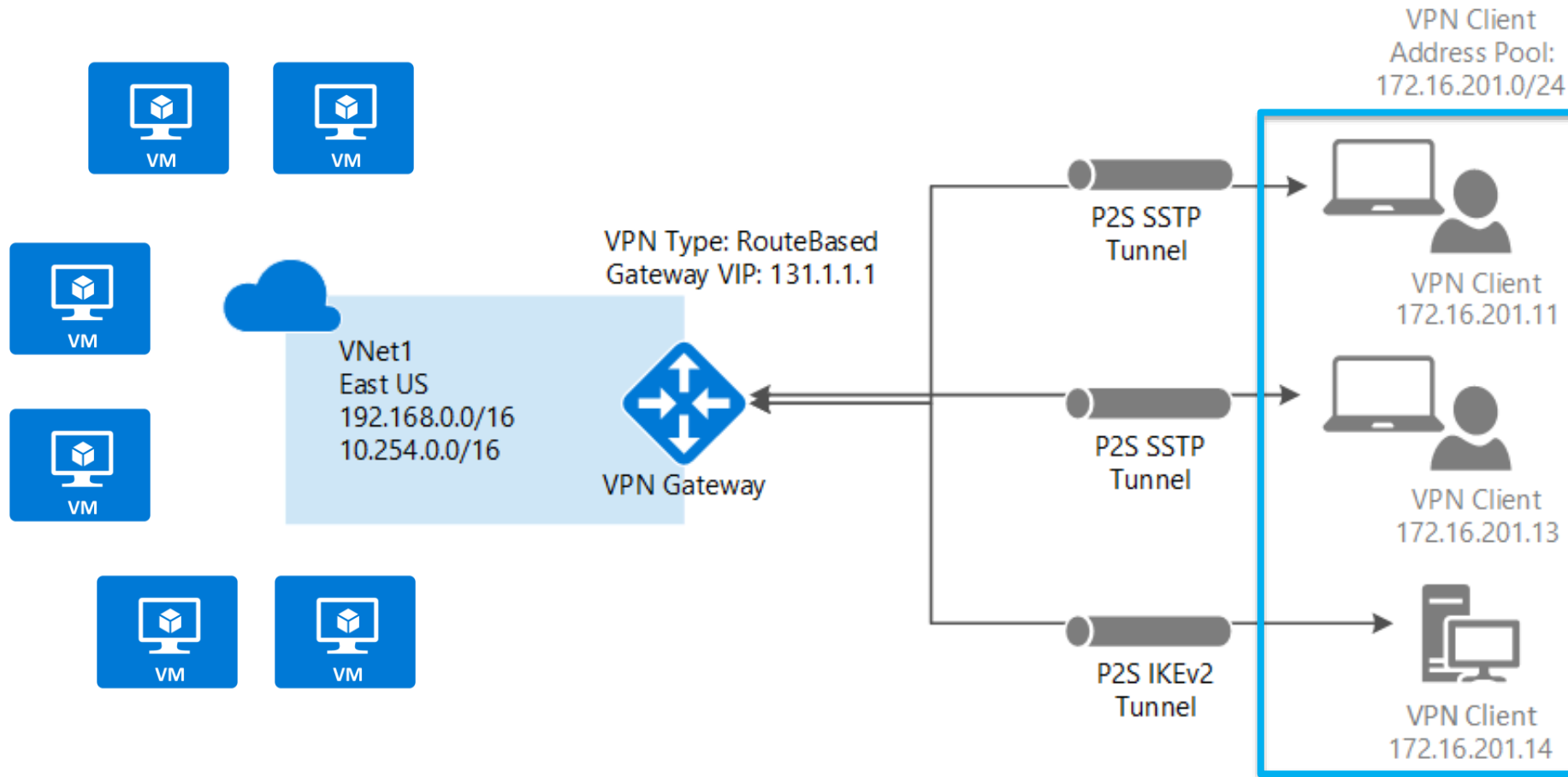
Point-to-Site
(P2S)

S2S



- 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



- 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

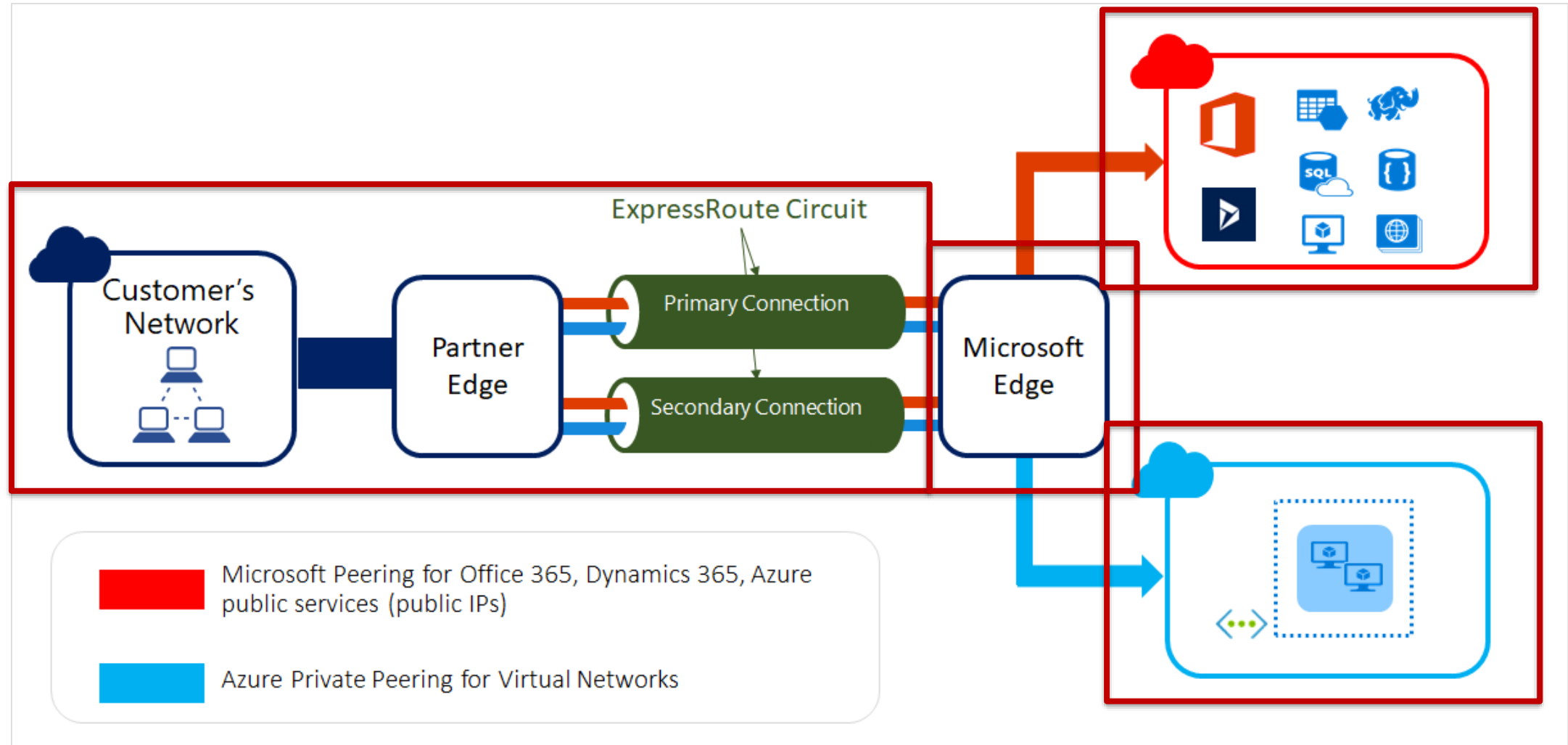
SKU	S2S/VNet-to-VNet Tunnels	P2S Connections	Aggregate Throughput Benchmark
VpnGw1	Max. 30	Max. 128	650 Mbps
VpnGw2	Max. 30	Max. 128	1 Gbps
VpnGw3	Max. 30	Max. 128	1.25 Gbps
Basic	Max. 10	Max. 128	100 Mbps

Gateway Recommendations

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 Key Benefits

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.

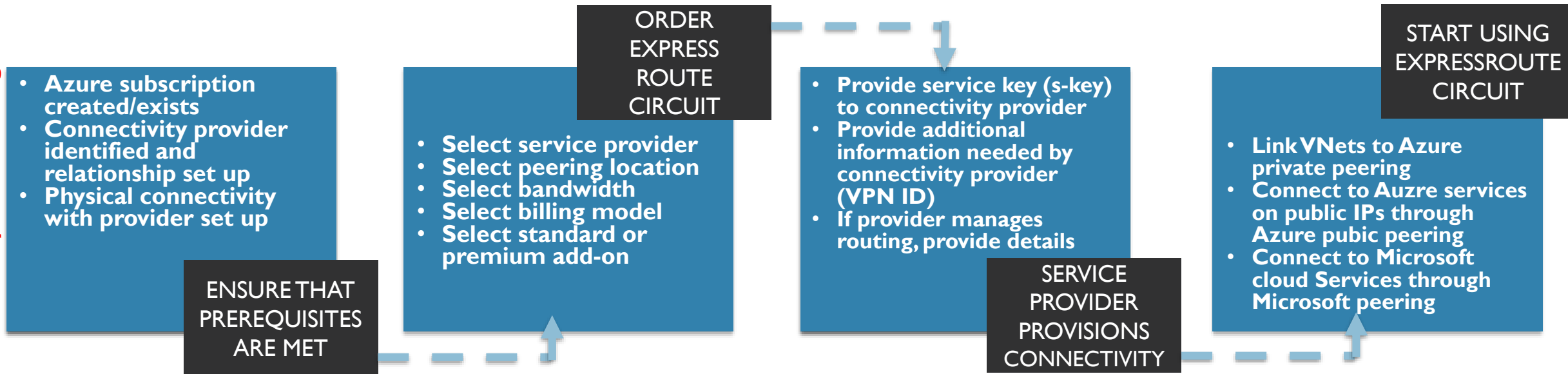
Dynamic Routing

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

Built-In Redundancy

In every peering location for higher reliability

ExpressRoute Provisioning



Peering – Data to Collect

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

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

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

Azure Monitoring Overview

Azure Monitoring Overview



Monitor & Visualize Metrics

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



Query and Analyze Logs

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



Setup & Alert Actions

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

Log Analytics

Azure Monitoring Overview



Monitor & Visualize Metrics

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



Query and Analyze Logs

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



Setup & Alert Actions

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

Log Analytics Key Features

Central Role in
Monitoring

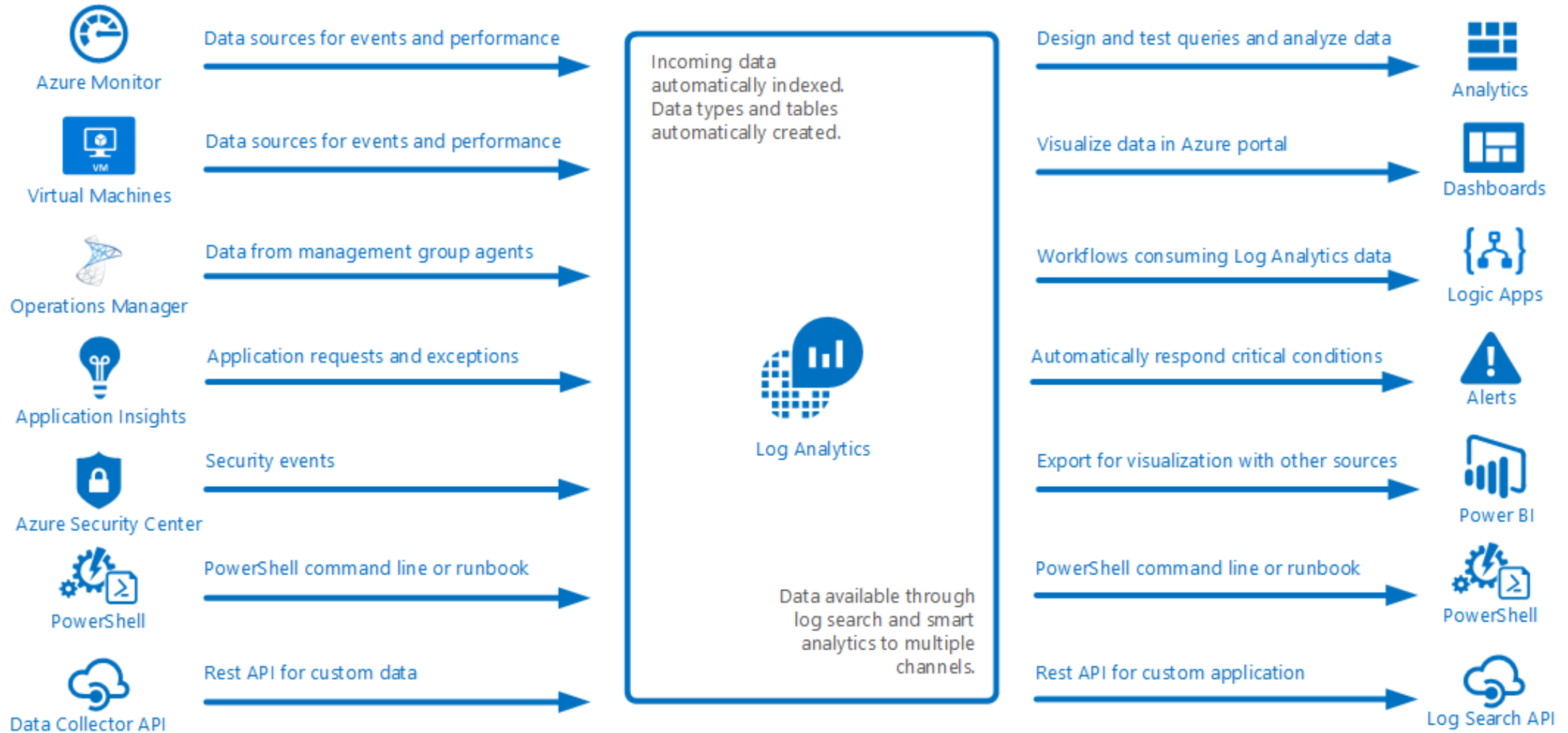
Data Sources

Other Log
Analytics Sources
(Security Center
and App Insights)

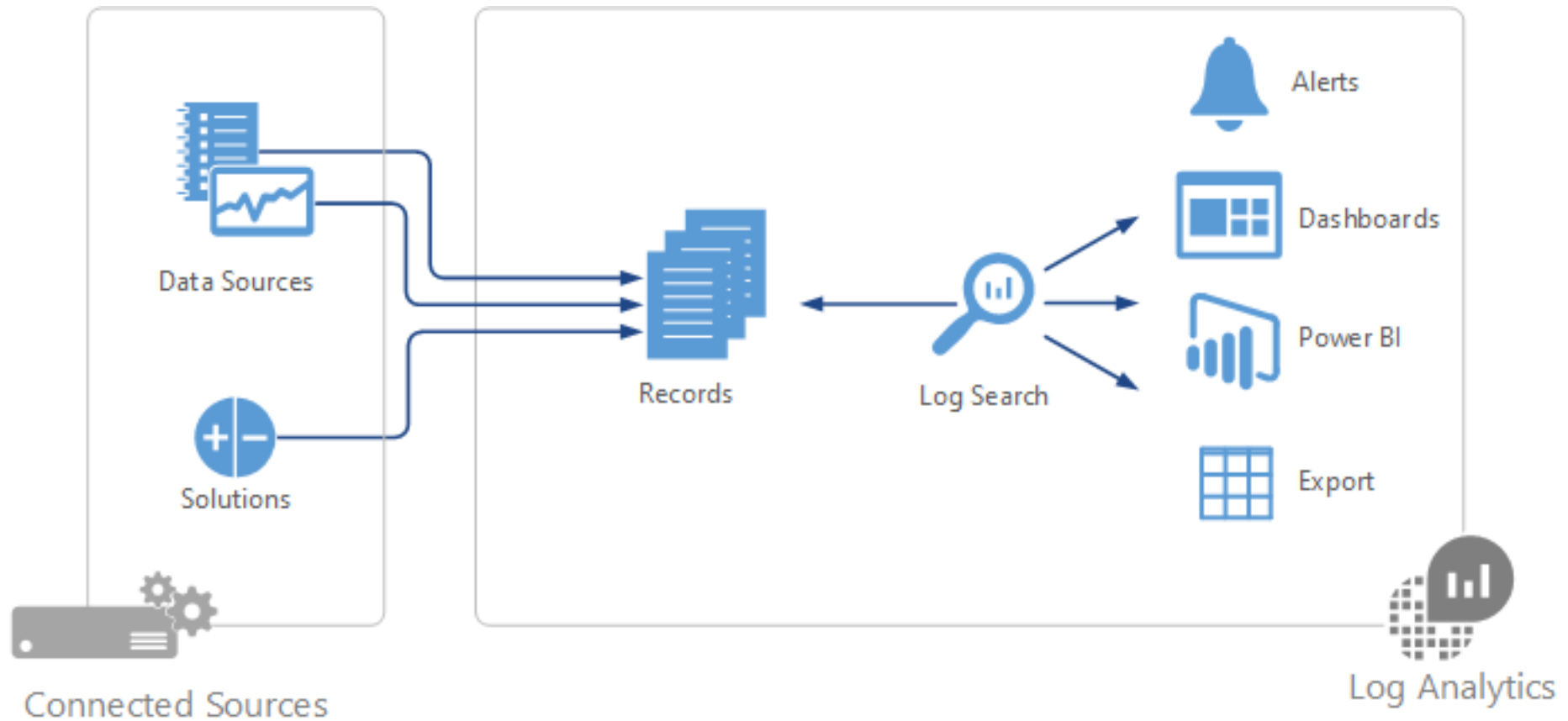
Search Queries

Output Options

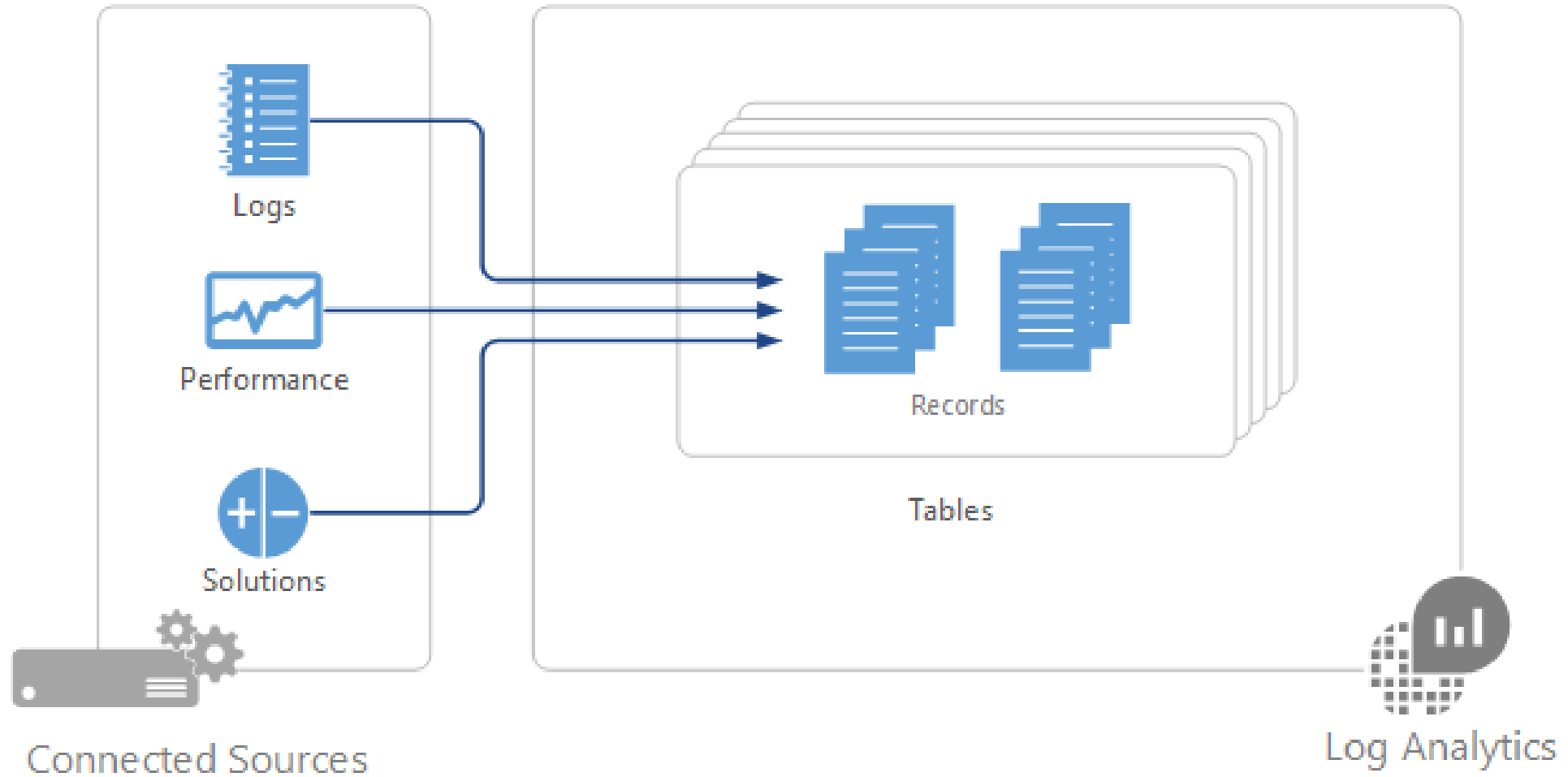
Log Search Use Cases



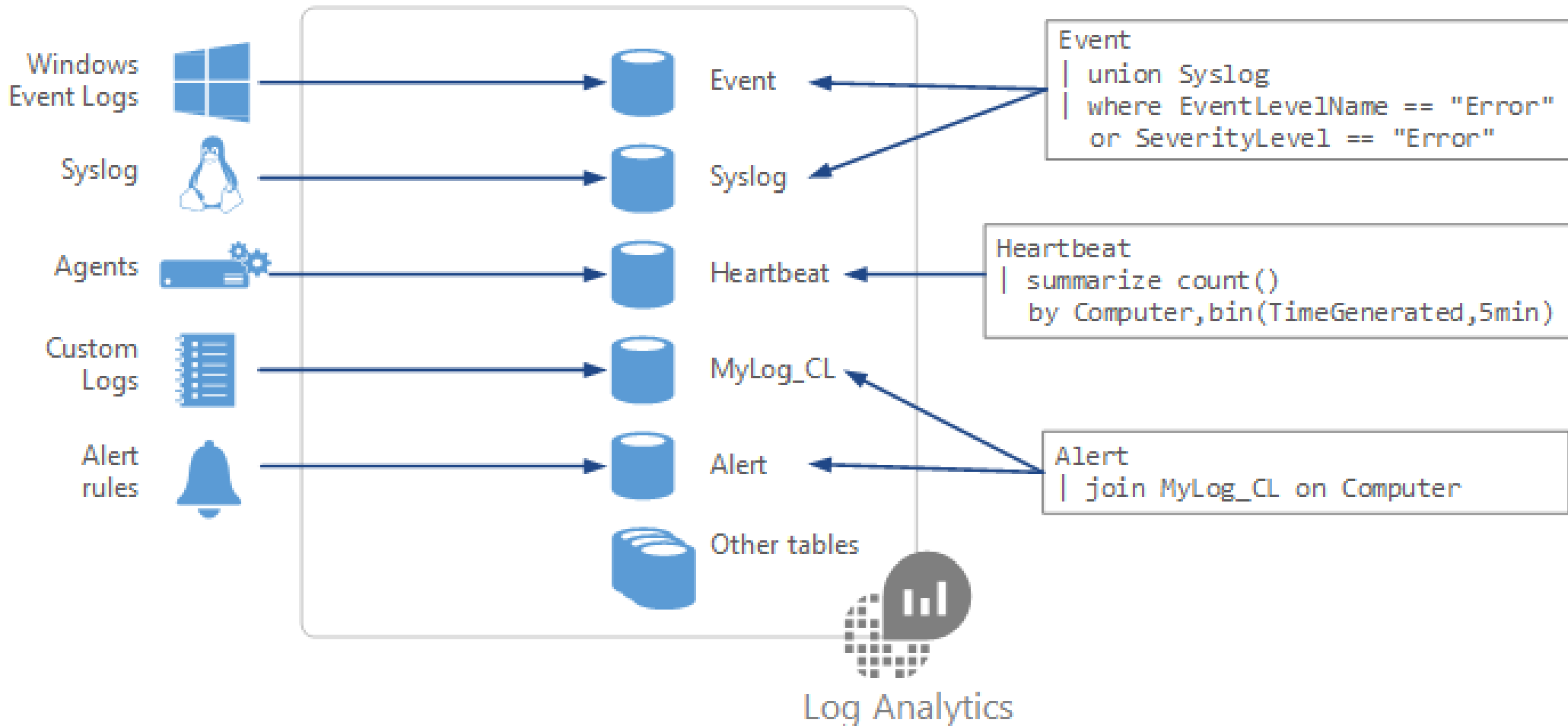
Log Analytics Architecture



Data Sources



Data Organization



Summary Data Sources

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 log on Windows computers.
Windows Performance counters	Perf	Performance counters collected from Windows computers.
Linux Performance counters	Perf	Performance counters collected from Linux computers.
IIS logs	W3CIISLog	Internet Information Services logs in W3C format.
Syslog	Syslog	Syslog events on Windows or Linux computers.

Search Query Fundamentals

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

Azure Policy

Azure Policies

Enforce
Governance

Built-in or
Custom Code

Assigned to
Subscriptions or
Resource Groups

Create > Assign

Resource Locks

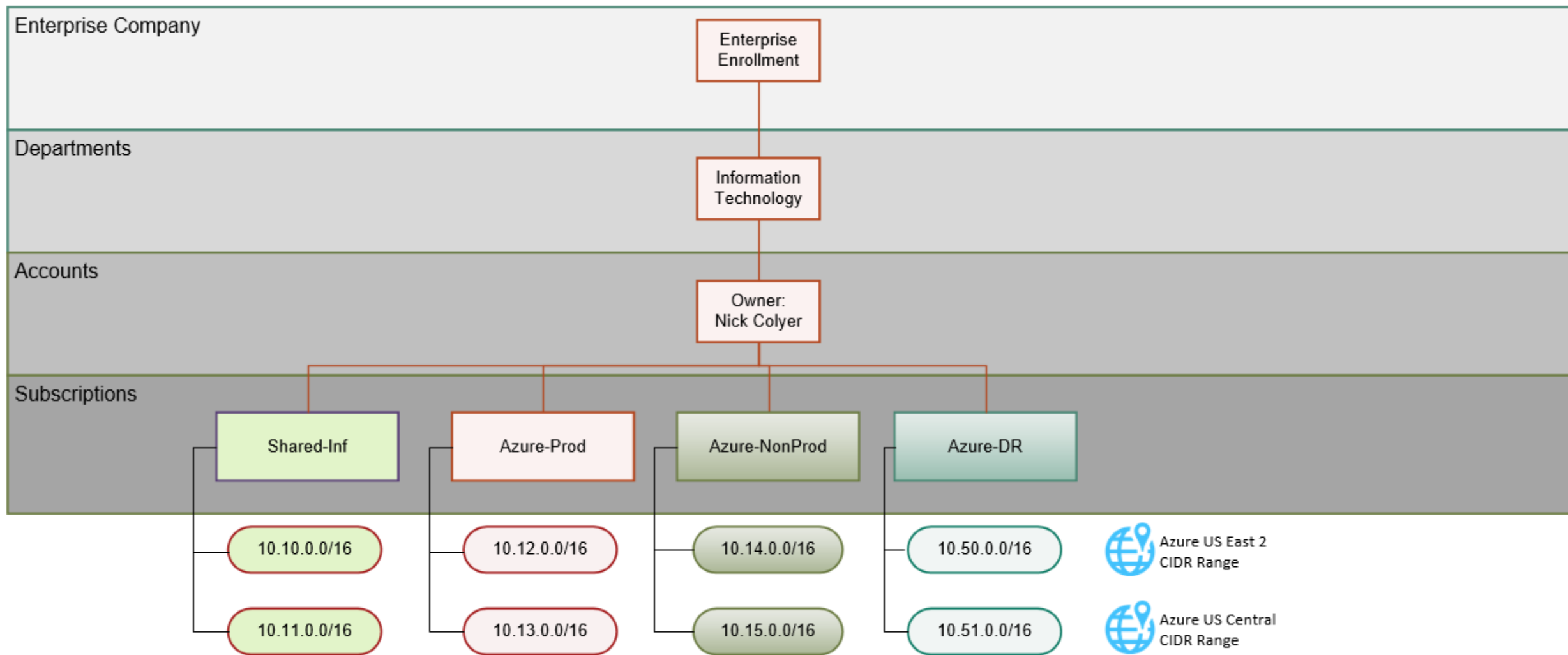
Azure Resource Locks

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

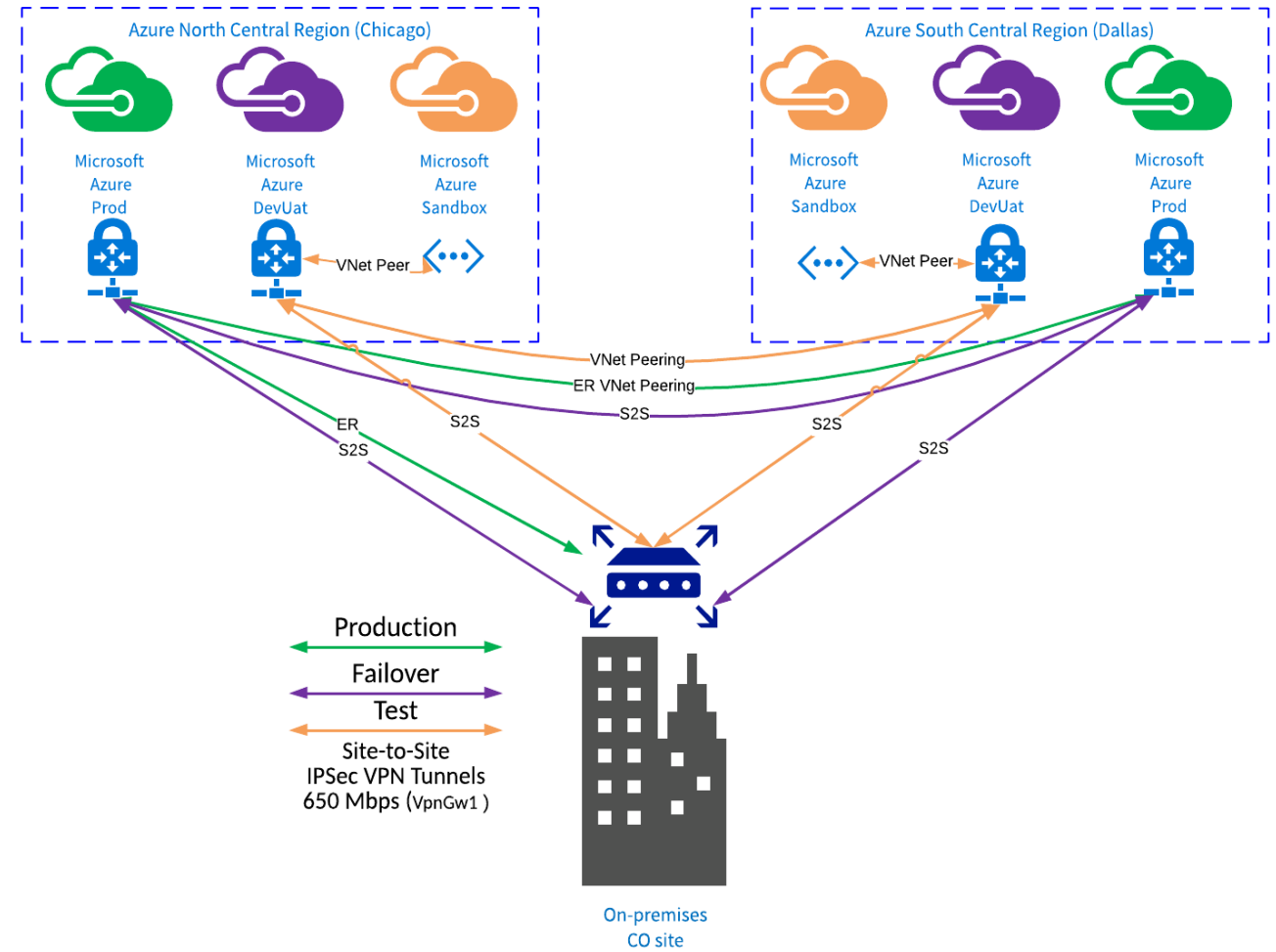


Design Examples

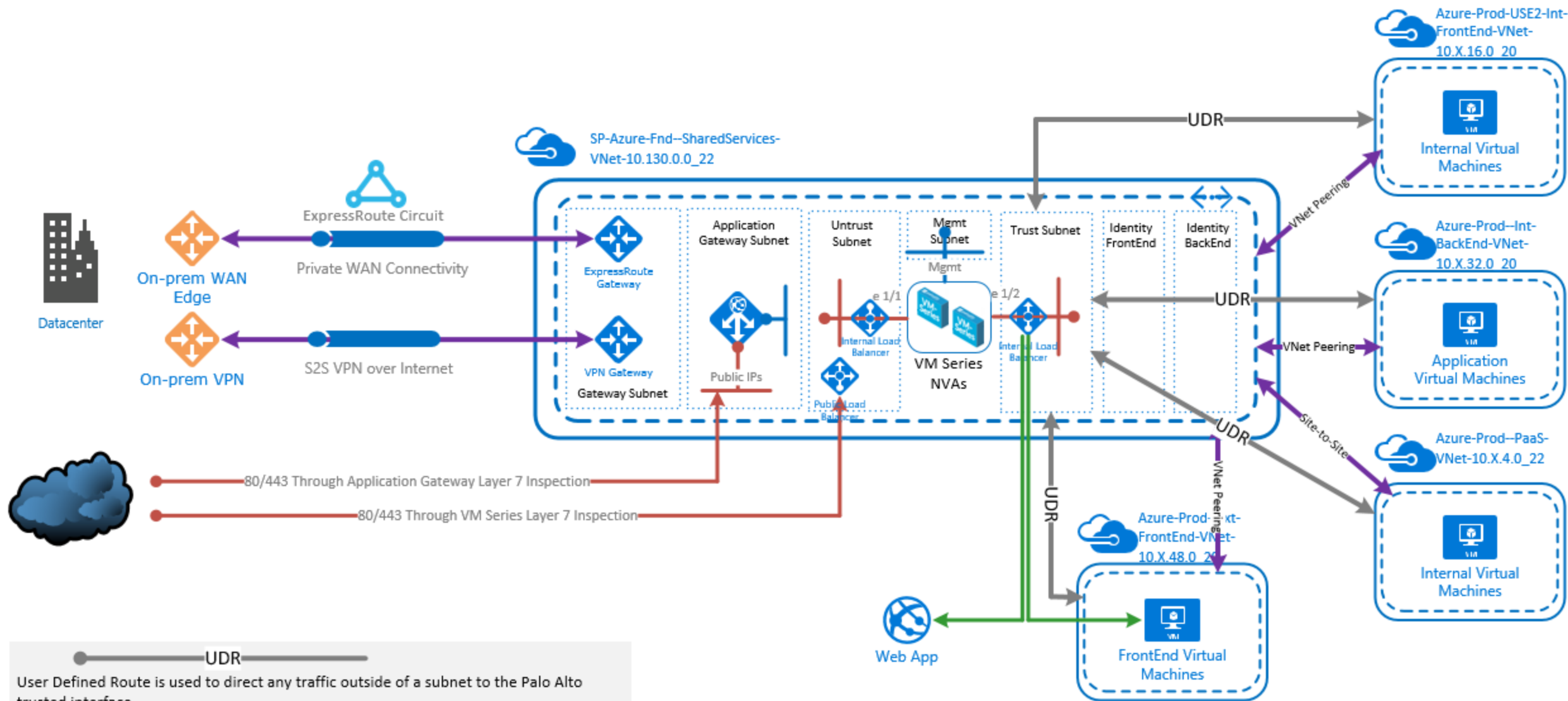
Subscription Design




- [Client] will use S2S VPN Tunnels and an Express Route to connect on-premise site to Azure [Region 1] and Azure [Region 2] Regions.
- There will be a dedicated VPN Gateway for the Prod and DevUat subscription in each Azure Region.
- [Client] will use 650Mbps Gateway speed at the starting point.
- [Client] will add an Express Route to connect CO to Azure
- There will be four (4) total gateways and five (5) total VPN tunnels.




Secure Hybrid Connectivity





UDR

User Defined Route is used to direct any traffic outside of a subnet to the Palo Alto trusted interface.

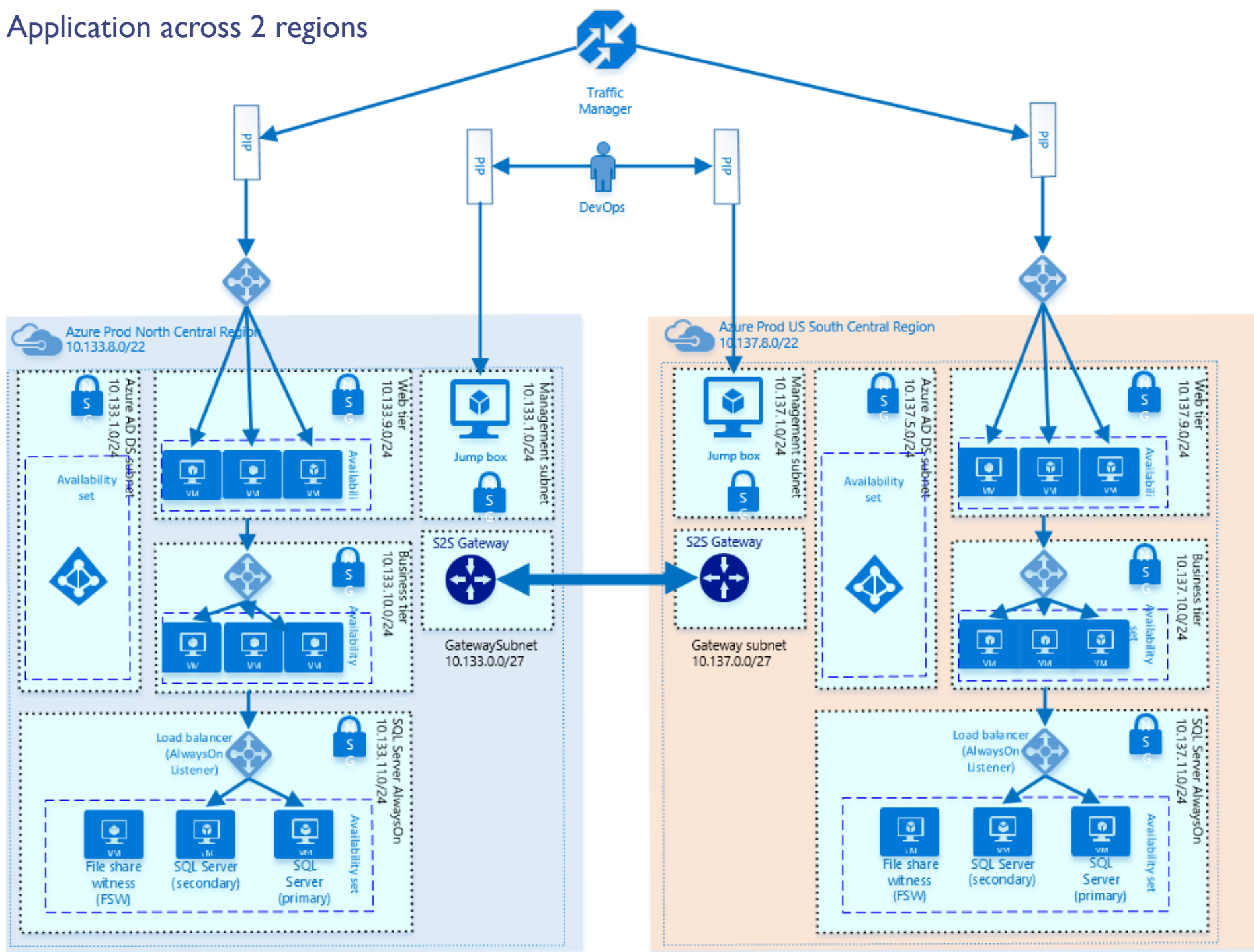

80/443 Through Application Gateway Layer 7 Inspection

Internet → 80/443 → App3 → AGW1 → Untrust Internal LB → Trust LB → WebApp
 Internet → 80/443 → App4 → AGW1 → Untrust Internal LB → Trust LB → External VM


80/443 Through P/A Layer 7 Inspection

Internet → 80/443 → App1 → Public LB → Untrust Internal LB → Trust LB → WebApp
 Internet → 80/443 → App2 → Public LB → Untrust Internal LB → Trust LB → External VM

Highly Available Application across 2 regions





SKY LINES

ACADEMY