

Azure AZ-300 Prep

AZ-300 - Microsoft Azure Architect Technologies

Jordan Radkov

Cloud Solution Architect



Week 1

Deploy and Configure Infrastructure
(25-30%)

Series Agenda

1	Kickoff
2	Deploy and Configure Infrastructure (25-30%)
3	Implement Workloads and Security (20-25%)
4	Create and Deploy Apps (5-10%)

5	Implement Authentication and Secure Data (5-10%)
6	Develop for the Cloud (20-25%)

Series Agenda

1	Kickoff
2	Deploy and Configure Infrastructure (25-30%)
3	Implement Workloads and Security (20-25%)
4	Create and Deploy Apps (5-10%)

5	Implement Authentication and Secure Data (5-10%)
6	Develop for the Cloud (20-25%)

Jordan Radkov

- Cloud Solution Architect based in the Munich
- 10+years in the industry in infrastructure administration , automation and now cloud
- Constant learner - Ancora Imparo



Ignite - https://www.youtube.com/watch?v=u1myyD_cGVQ

Exam basics



40-60 questions

- Some questions worth more than 1 point
- Answer all the questions
 - *No penalty for guessing*
 - *Some questions cannot be skipped!*
- Mark items for review if you're not sure of your answer



Plan for 180 minutes

- 150 minutes to answer questions
- 30 minutes for instructions, comments, score reporting, etc.



More than just multiple-choice questions!

- Build list, hot area, active screen, drag and drop, etc.
- *Performance based coming soon!*



Case Studies

- Detailed information on business and technical requirements; existing environment and other background you need to solve problems
- Requires you to understand and integrate information across multiple sources, determine what's important, and make the best decision

Tips and Tricks Slide

DO

Exam questions are typically action-based

Understand the technology from the Azure Portal, PowerShell Modules, and Azure CLI

For example – Don't just create storage account from the portal – use other methods and understand the parameters to grasp how the feature works

READ

Not easy to deploy and test all features

Use **docs.microsoft.com** to your advantage – All exam questions have some type of authoritative supporting information – typically documentation

Objective Review - Deploy and Configure Infrastructure (25-30%)

Analyze resource utilization and consumption

- *May include but not limited to:* Configure diagnostic settings on resources; create baseline for resources; create and rest alerts; analyze alerts across subscription; analyze metrics across subscription; create action groups; monitor for unused resources; monitor spend; report on spend; utilize Log Search query functions; view alerts in Log Analytics.

Create and configure storage accounts

- *May include but not limited to:* Configure network access to the storage account; create and configure storage account; generate shared access signature; install and use Azure Storage Explorer; manage access keys; monitor activity log by using Log Analytics; implement Azure storage replication

Create and configure a Virtual Machine (VM) for Windows and Linux

- *May include but not limited to:* Configure high availability; configure monitoring, networking, storage, and virtual machine size; deploy and configure scale sets

Objective Review - Deploy and Configure Infrastructure (25-30%) – cont'd

Automate deployment of Virtual Machines (VMs)

- *May include but not limited to:* Modify Azure Resource Manager (ARM) template; configure location of new VMs; configure VHD template; deploy from template; save a deployment as an ARM template; deploy Windows and Linux VMs

Create connectivity between virtual networks

- *May include but not limited to:* Create and configure VNET peering; create and configure VNET to VNET; verify virtual network connectivity; create virtual network gateway

Implement and manage virtual networking

- *May include but not limited to:* Configure private and public IP addresses, network routes, network interface, subnets, and virtual network

Manage Azure Active Directory (AD)

- *May include but not limited to:* Add custom domains; configure Azure AD Identity Protection, Azure AD Join, and Enterprise State Roaming; configure self-service password reset; implement conditional access policies; manage multiple directories; perform an access review

Implement and manage hybrid identities

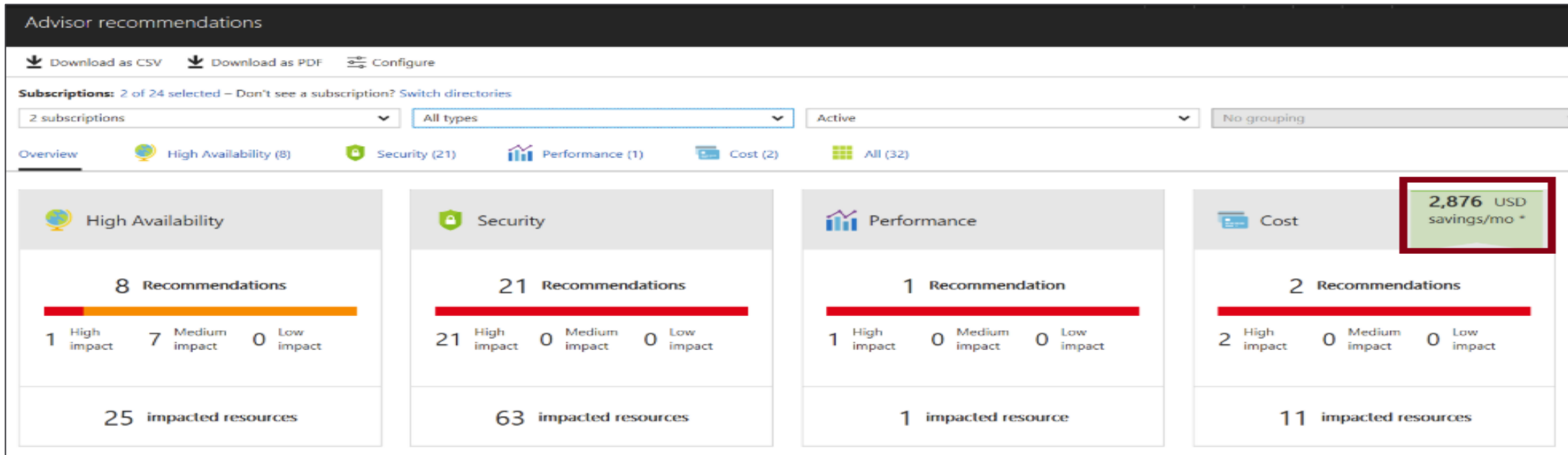
- *May include but not limited to:* Install and configure Azure AD Connect; configure federation and single sign-on; manage Azure AD Connect; manage password sync and writeback

Objective Review - #1

Analyze resource utilization and consumption

- Configure diagnostic settings on resource
- Create baseline for resources
- Create and rest alert
- Analyze alerts across subscription
- Analyze metrics across subscription
- Create action groups
- Monitor for unused resources
- Monitor spend
- Report on spend
- Utilize Log Search query functions
- View alerts in Log Analytics

Azure Advisor

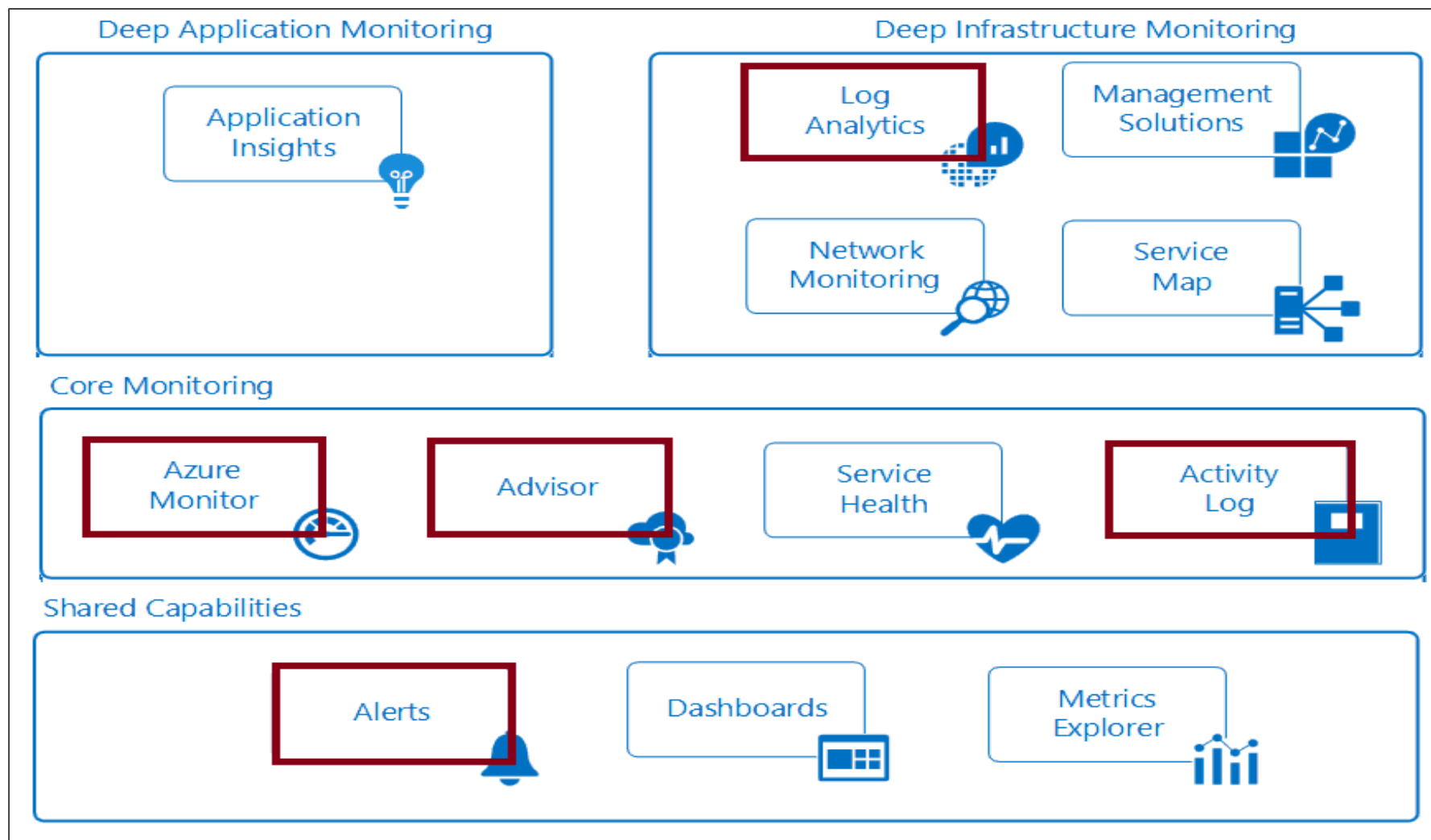


Personalized cloud consultant

Analyzes your configuration and recommends solutions

Four areas: High Availability, Security, Performance, and Cost

Introducing Azure Monitor Service





Azure Monitor

Application

Operating System

Azure Resources

Azure Subscription

Azure Tenant

Custom Sources



Insights



Application



Container



VM



Monitoring
Solutions

Visualize



Dashboards



Views



Power BI



Workbooks

Analyze



Metric Analytics



Log Analytics

Respond



Alerts



Autoscale

Integrate



Event Hubs

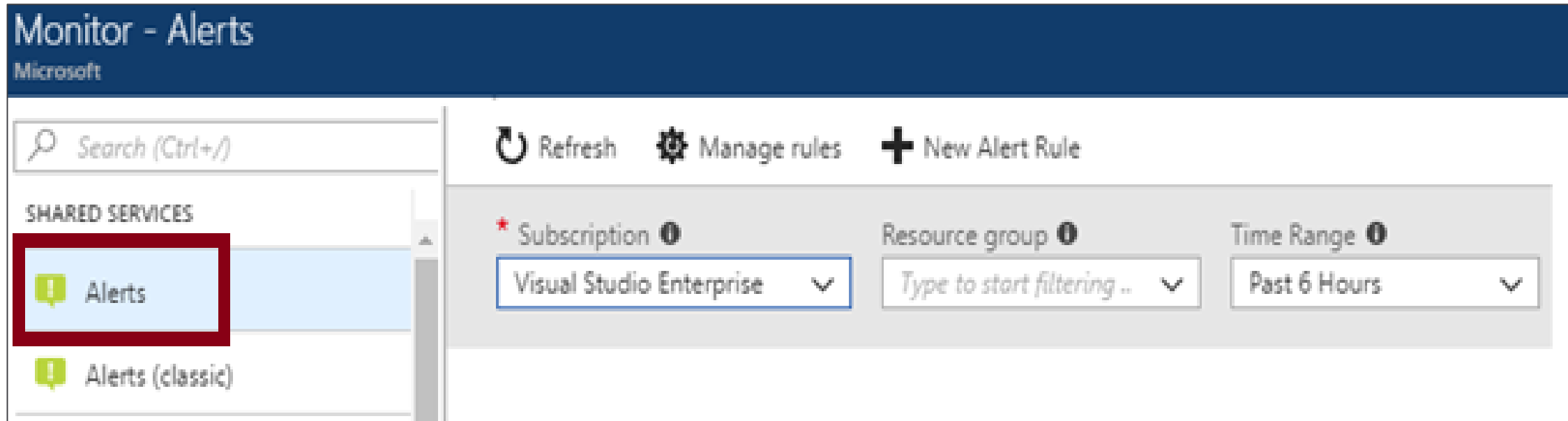


Logic Apps



Ingest &
Export APIs

Azure Monitor Alerts



A unified authoring experience

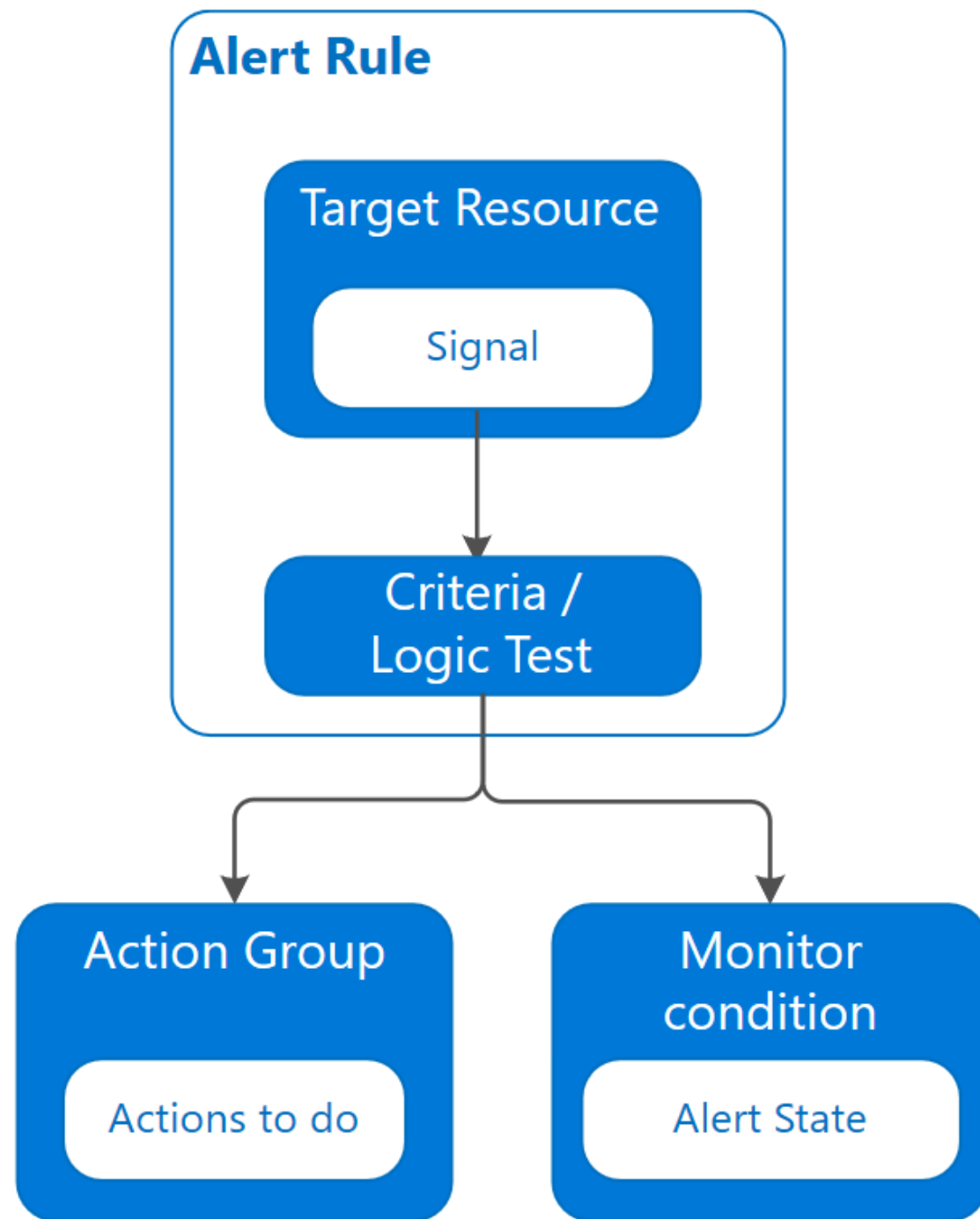
Better creation workflow and fired alert notification

Consolidation into one view

Creating Alert Rules



1. Define the alert condition with target, criteria, and logic
2. Define the alert details like rule name, description, and severity
3. Define the action group for notifications



Action Groups

The diagram illustrates the process of configuring an action. On the left, a table titled 'Actions' lists various actions. The 'ACTION TYPE' column is highlighted with a red box. An arrow points from the 'Email/SMS/Push/Voice' action in this table to a configuration form on the right.

ACTION NAME	ACTION TYPE	STATUS	DETAILS
myNotifications	Email/SMS/Push/Voice		Edit details
myWebhook	Webhook		Edit details
myRunbook	Automation Runbook	✓	Edit details

The configuration form on the right is titled 'Email/SMS/Push/Voice'. It contains the following fields:

- Name:** A text input field with the placeholder text 'Place action's name here'.
- Email:** A checkbox labeled 'Email' followed by a text input field containing 'email@example.com'.
- SMS:** A checkbox labeled 'SMS'.
- Country code:** A dropdown menu showing '1'.
- Phone number:** A text input field with a red asterisk indicating it is required, containing '1234567890'.

Configure a list of actions to take when the alert is triggered

Ensures the same actions are taken each time an alert is triggered

Action types: Email/[SMS](#)/Push/Voice, [Logic App](#), [Webhook](#), [IT Service Management](#), or Automation Runbook

Signal Types and Metrics

Improved latency

Support for multi-dimensional metrics

More control over metric conditions

Combined monitoring of multiple metrics

Metrics from Logs

Configure signal logic

Define your alert criteria by choosing a signal below and defining your alert condition on the next screen.

SIGNAL NAME	SIGNAL TYPE	MONITOR SERVICE
Used capacity	Metric	Platform
Transactions	Metric	Platform
All Administrative operations	Activity Log	Administrative
List Storage Account Keys (storageAccounts)	Activity Log	Administrative
Regenerate Storage Account Keys (storageAcc...	Activity Log	Administrative
Delete Storage Account (storageAccounts)	Activity Log	Administrative

Practice: Alerts

Audit and receive notifications about important actions in your Azure subscription

Create a network security group

Browse the Activity Log in the portal

Browse an event in the Activity log

Create an Activity log alert

Test the Activity log alert

Overview of [Activity Log](#) - [Video](#): Activity Log

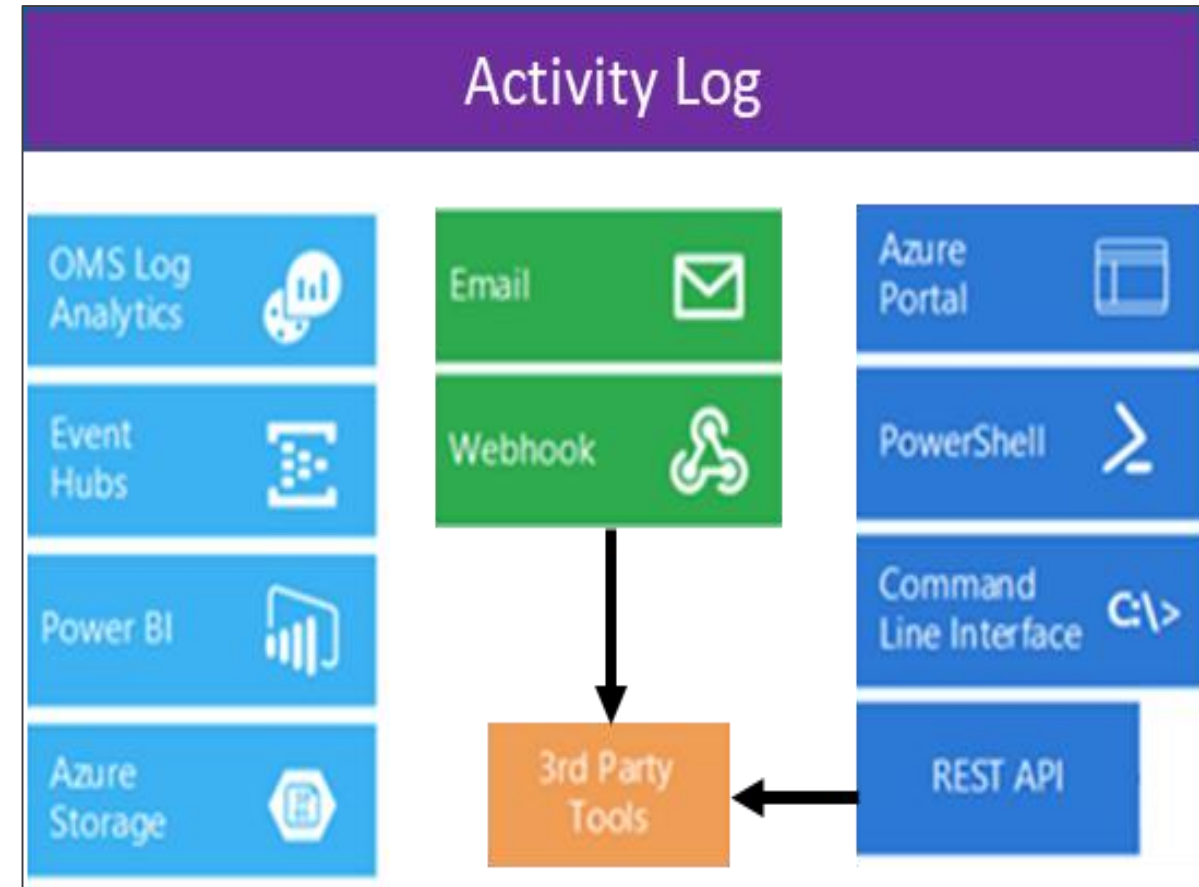
Send data to Log Analytics for advanced search and alerts

Query or manage events in the Portal, PowerShell, CLI, and REST API

Stream information to Event Hub

Archive data to a storage account

Analyze data with Power BI



Query the Activity Log

Activity log

Columns

Export

Log Analytics

Select query ...

Insights (Last 24 hours): 0 failed deployments | 0 role assignments | 0 errors | 0 alerts fired | 2 outage notifications

* Subscription ⓘ

Visual Studio Enterprise

Resource group ⓘ

All resource groups

Resource ⓘ

All resources

Resource type ⓘ

All resource types

Operation ⓘ

0 selected

Timespan ⓘ

Last 24 hours

Event category ⓘ

Service Health

* Event severity ⓘ

4 selected

Event initiated by ⓘ

Email or name or service principal name

Search ⓘ

Apply

Reset

Filter by: Subscription, Resource group, Resource (name), Resource type, Operation name, Timespan, Category, Severity, and Event initiated by

Event Categories

- Administrative events
- Service health events with status
- Alert events
- Autoscale events
- Usage recommendations
- Security events
- Policy and Resource Health (reserved)

Resource group ⓘ

All resource groups ▾

Event category ⓘ

Service Health ▴

All categories

Administrative

Security

Service Health

Alert

Recommendation

Policy

Autoscale

Resource Health

Activity Log and Log Analytics

The screenshot displays the Microsoft Azure Log Analytics interface. The left sidebar shows the 'Log Analytics' workspace with a list of subscriptions. One subscription, 'bandersa...', is highlighted with a red box. The main pane shows the 'Azure Activity log' workspace. A red box highlights the 'Azure Activity log' option in the 'WORKSPACE DATA SOURCES' list. The right pane shows a table of OMS connections. The 'ASC DEMO' connection is highlighted with a red box.

SUBSCRIPTION	OMS CONNECTION
Advisor Analytics Capacity Dev	Not connected
Advisor Analytics TechEd Demo	Not connected
ASC DEMO	Not connected
OMS Ecosystem Production	Not connected
Visual Studio Enterprise	Connected

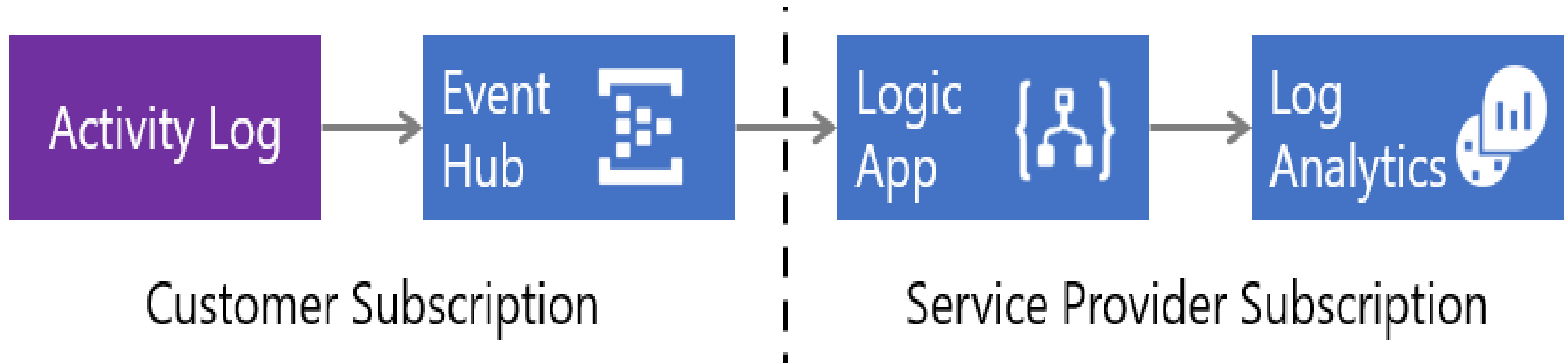
Analyze the activity logs with pre-defined views

Analyze and search activity logs from multiple Azure subscriptions

See operational activities aggregated by status

View trends of activities happening on each of your Azure services

Collect Across Subscriptions



Low latency and minimal coding

Azure Activity Log sends events to an [Event Hub](#) where a [Logic App](#) sends them to your Log Analytics workspace

Practice: Activity Log

Configure activity logs in the Azure portal

Create an activity log alert

View the Activity Log in the Azure portal

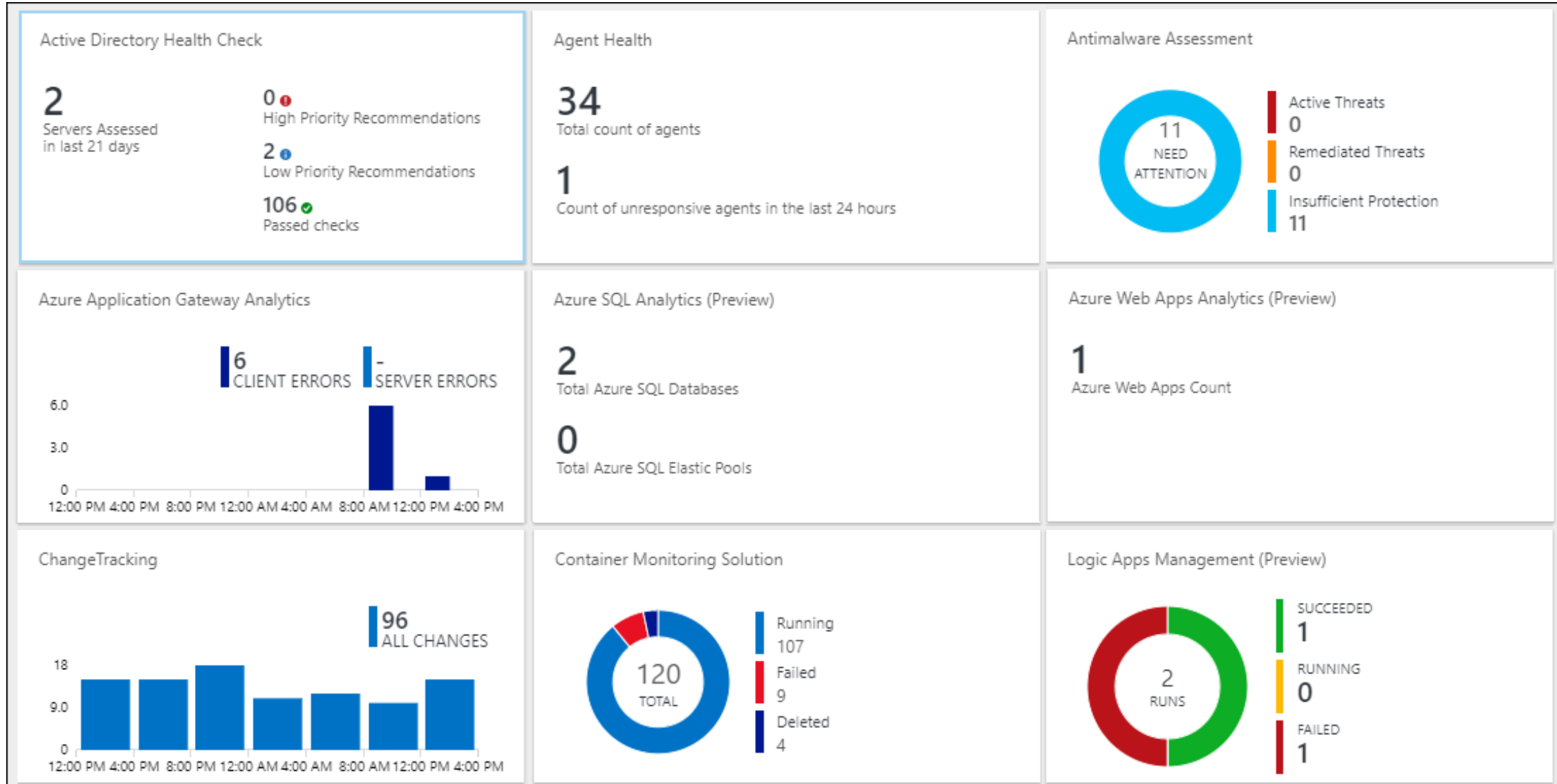
Configure log profiles using the Azure portal

Enable streaming of the Activity Log

Archive the Activity Log using the portal

Configure the Activity Log Analytics solution for your workspaces

Video: Log Analytics



Log Analytics Scenarios

Example 1 - Assessing updates

- IT Administrators assess systems update requirements
- Must be able to accurately schedule updates
- OMS/Log Analytics collects data from all customers performing updates
- Uses "Crowd-sourced" data to provide an average time to help meet strict SLAs

Example 2 - Change tracking

- Troubleshooting operational incidents is a complex process
- OMS/Log Analytics let you perform analysis from multiple angles, using a variety of sources
- Everything correlated through a single interface
- Track issues such as unexpected system reboots or shutdowns

Practice: Collect and Analyze Data

Part 1

Collect data about virtual machines

Create a workspace

Enable Log Analytics on virtual machines

Collect event and performance data

View the data collected

Part 2

View or analyze data collected with Log Analytics search

Search, modify, and filter event data

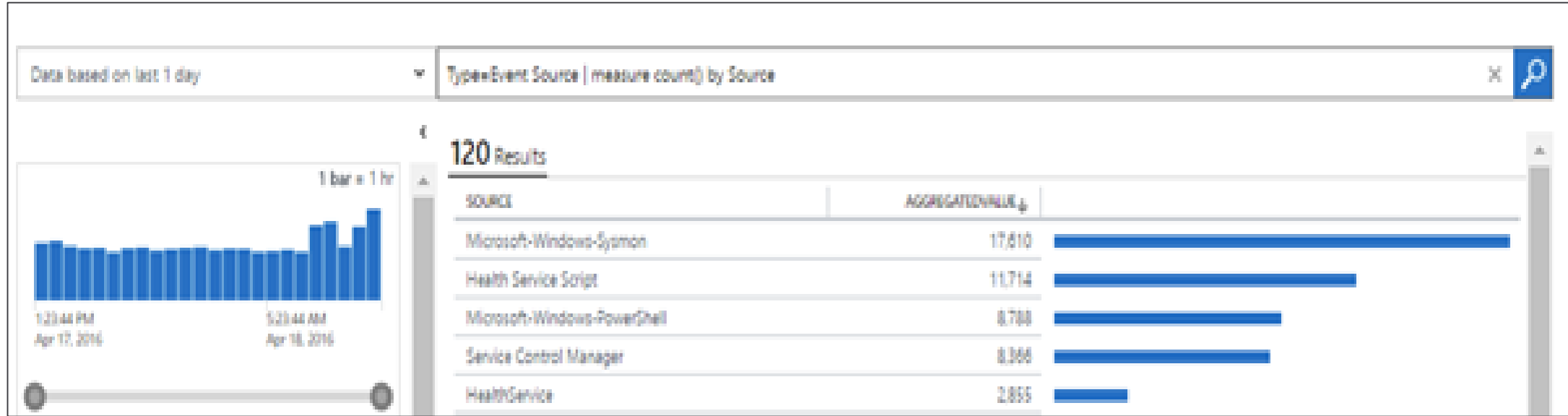
Work with performance data

Practice: Analysis with Log Analytics

Microsoft Online Labs has a self-paced **Deep Analysis with Microsoft Azure Log Analytics** exercise.

- Focus on the basics of Azure Insight and Analytics
- Explore Log Analytics, log searches, analysis of Service Map and Network Performance Monitor solutions

Log Analytics Querying



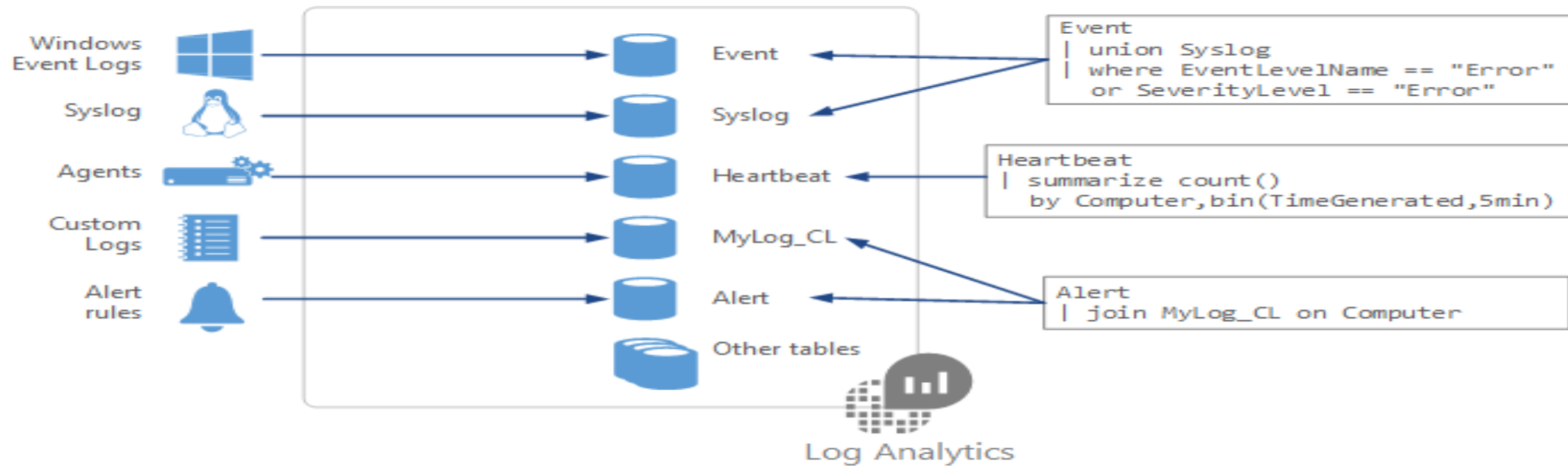
Log Analytics provides a query syntax

Quickly retrieve and consolidate data in the repository

Save or have log searches run automatically to create an alert

Export the data to Power BI or Excel

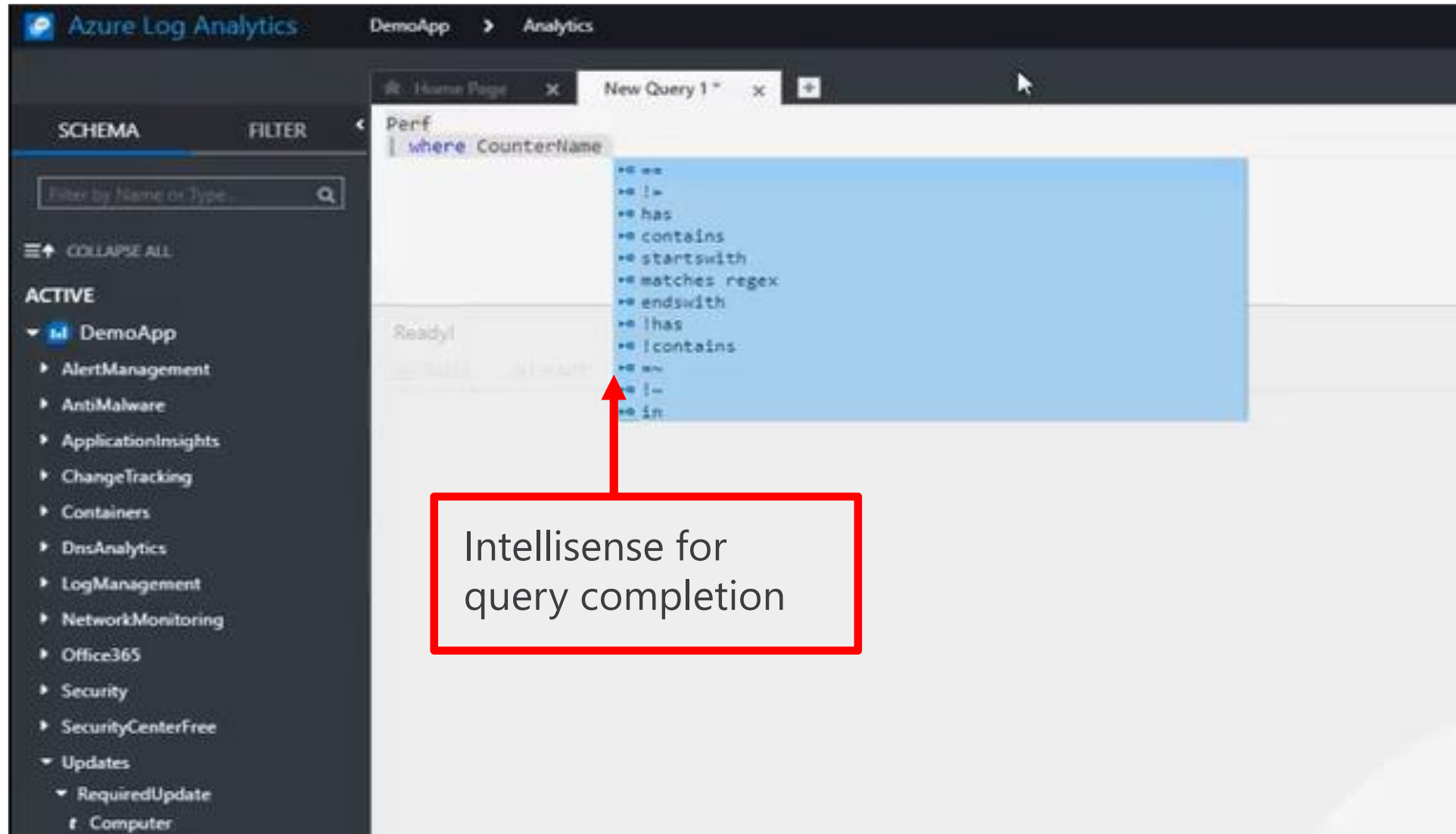
Query Language Syntax



Event

```
| where (EventLevelName == "Error")  
| where (TimeGenerated > ago(1days))  
| summarize ErrorCount = count() by Computer  
| top 10 by ErrorCount desc
```

Demonstration: [Log Analytics Querying](#)



Practice: Log Analytics Query

Access the live [Log Analytics Querying Demonstration](#) workspace where you can run and test queries

Some of the testing queries are

See the volume of data collected in the last 24 hours in intervals of 30 minutes

Chart the distribution of billable data by type, over the last 24 hours

Find out which computers were alive in the past 2 days but haven't sent any data in the last 6 hours

Network Watcher

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.

Monitor communication between a virtual machine and an endpoint

Connection monitor provides the minimum, average, and maximum latency observed over time

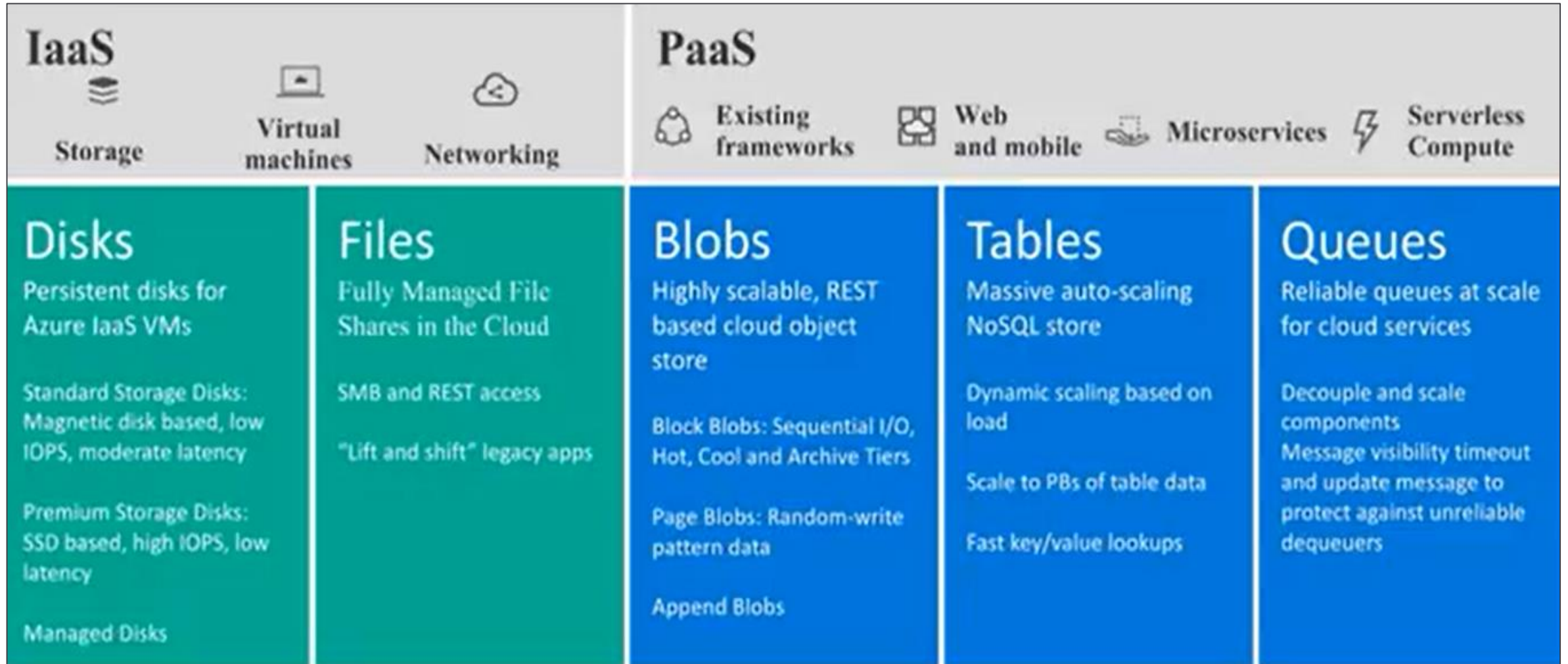
Network performance monitor

Objective Review - #2

Create and configure storage accounts

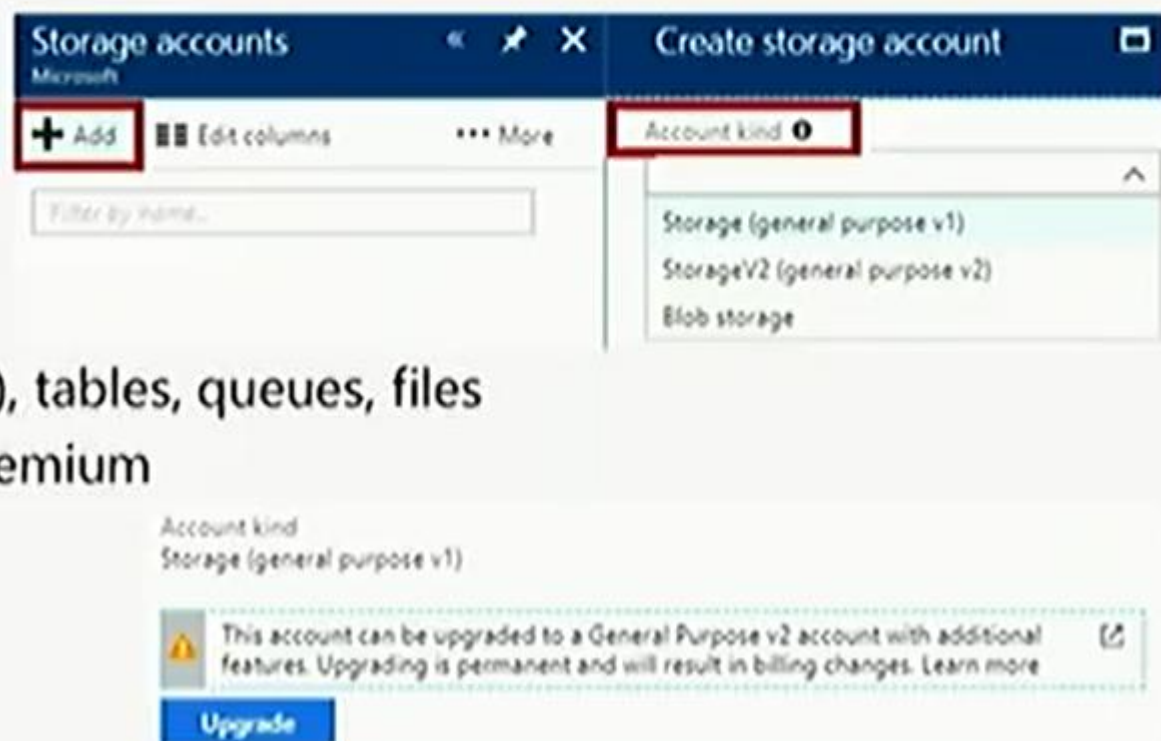
- Configure network access to the storage account
- Create and configure storage account
- Generate shared access signature
- Install and use Azure Storage Explorer
- Manage access keys
- Monitor activity log by using Log Analytics
- Implement Azure storage replication

Introduction to Azure Storage



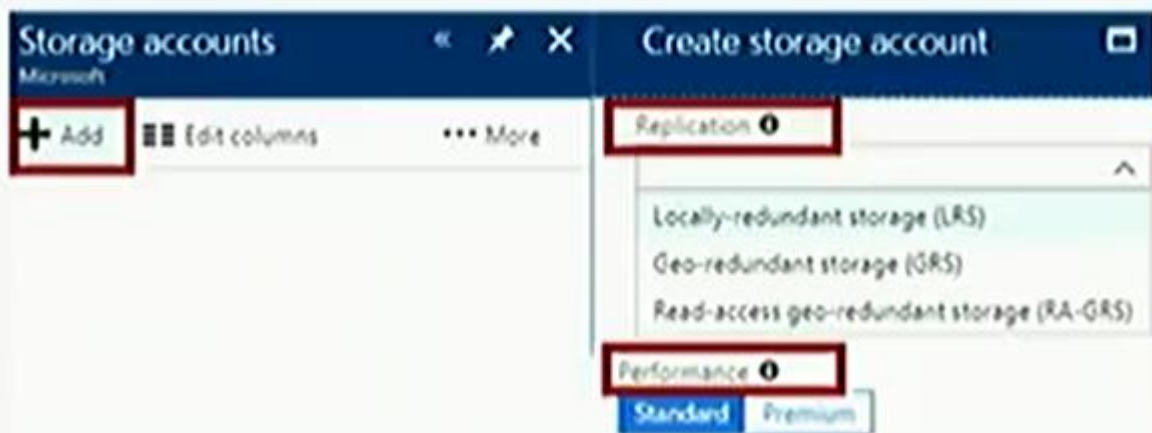
Azure Storage Accounts

- Storage (general purpose v1):
 - Can contain blobs (including Azure VM disks), tables, queues, files
 - Supports performance tiers: Standard and Premium
- Blob storage:
 - Can contain blobs only
 - Supports access tiers: hot, cool, archive
- Storage V2 (general purpose v2):
 - Can contain blobs (including Azure VM disks), tables, queues, files
 - Supports performance tiers: Standard and Premium
 - Supports access tiers: hot, cool, archive



Replication Options

- Locally-redundant storage (LRS):
 - The only replication option when using Premium performance tier
- Zone-redundant storage (ZRS):
- Geo-redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)



Azure Storage

A service that you can use to store files, messages, tables, and other types of information


Three categories of Azure storage:


Storage for virtual machines – Disks and File Shares


Unstructured data – Blobs and Data Lake Store


Structured data - Tables, Cosmos DB, and Azure SQL DB

Services

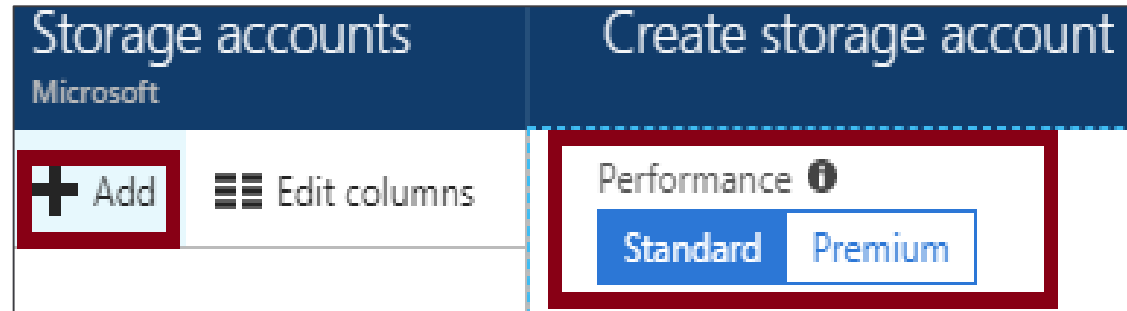
**Blobs**
REST-based object storage for unstructured data
[Learn more](#)

**Files**
File shares that use the standard SMB 3.0 protocol
[Learn more](#)

**Tables**
Tabular data storage
[Learn more](#)

**Queues**
Effectively scale apps according to traffic
[Learn more](#)

Azure Storage Accounts - Standard and Premium Storage Accounts



Standard:

Backed by magnetic drives (HDD)

Lowest cost per GB

Premium:

Backed by solid state drives (SSD)

Can only be used with Azure VM disks

99.99% SLA

Storage Account Endpoints

Every object has a unique URL address

The storage account name forms the subdomain of that address

The subdomain and domain name forms an *endpoint*

Blob service: <http://mystorageaccount.blob.core.windows.net>

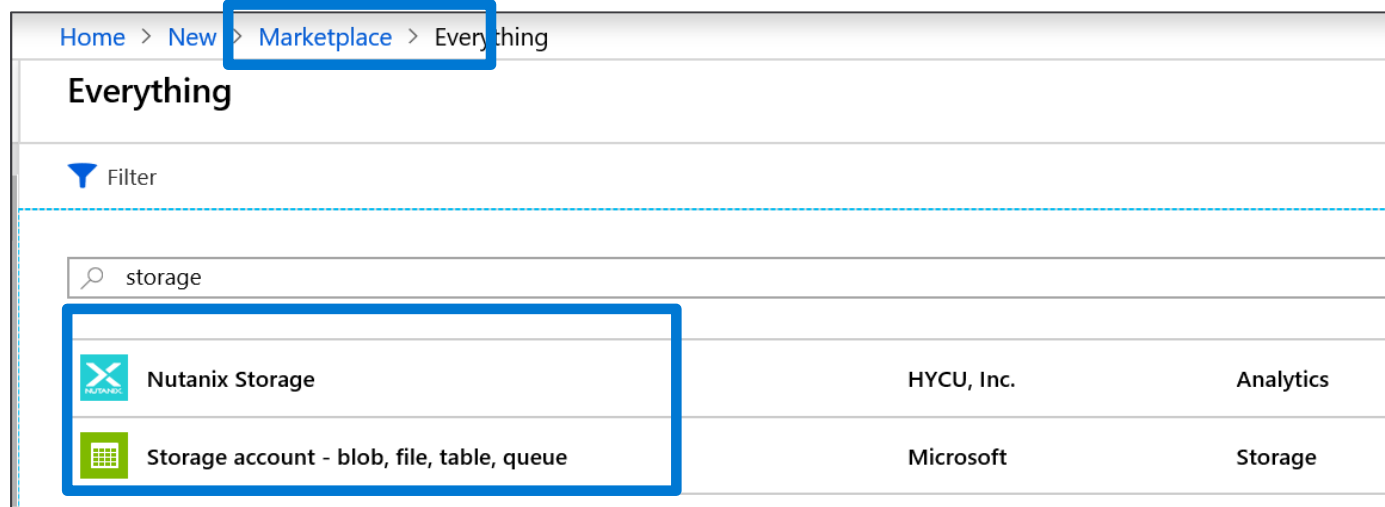
Table service: <http://mystorageaccount.table.core.windows.net>

Queue service: <http://mystorageaccount.queue.core.windows.net>

File service: <http://mystorageaccount.file.core.windows.net>

Demonstration: Creating Storage Accounts

Create a storage account using Azure Marketplace (Portal)



- PowerShell
 - # Create new storage account
New-AzureRMStorageAccount -ResourceName storage -Name storage2test
-SkuName Standard LRS -Location 'west us'

Practice: Storage Accounts

Microsoft Online Labs has a self-paced **Assessing on-premises VMware environments with Azure Migrate** lab

- Understand and deploy storage accounts
- Explore key storage concepts and resources

Practice: Storage Account Management

[How to create a GPv2 storage account](#)

[How to convert a GPv1 or Blob storage account to a GPv2 storage account](#)

[How to set the account in a GPv2 storage account](#)

[How to set a blob tier in a Blob storage or GPv2 storage account](#)

Storage Explorer & Manage Access Key

Storage Explorer - Reminder to install and use it

Manage Access Key

Storage Account roles:

- Owner
- Contributor
- Reader
- Storage Account Contributor
- User Access Administrator
- VM Contributor

Least privilege

Video: Storage Security Overview

Storage service encryption

Encryption in transit

Storage firewall - limit IP addresses through network security groups

Limit user access to storage accounts using RBAC

Analyze metrics and logs with Azure Monitor and Log Analytics

Storage keys

More granular security with Shared Access Signatures

Policy based signatures

Shared Access Signature (SAS)



Provides delegated access to resources

Grants access to clients without sharing your storage account keys

The account SAS delegates access to resources in one or more of the storage services: Blob, Queue, Table, or File service

The service SAS delegates access to a resource in just one of the storage services

Configuring SAS Parameters

Allowed services ⓘ

☒ Blob ☒ File ☒ Queue ☒ Table

Allowed resource types ⓘ


☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ


☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☒ Update ☒ Process

Start and expiry date/time ⓘ

Start

2018-05-31  10:12:46 AM

End

2018-05-31  6:12:46 PM

(UTC-07:00) --- Current Timezone ---


Allowed IP addresses ⓘ

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Signing key ⓘ

key1 

Account level SAS, full permissions

New-AzureStorageAccountSASToken

-Service Blob,File,Table,Queue

-ResourceType Service,Container,Object

-Permission "racwdlup"

Blob level SAS, full permissions

New-AzureStorageBlobSASToken

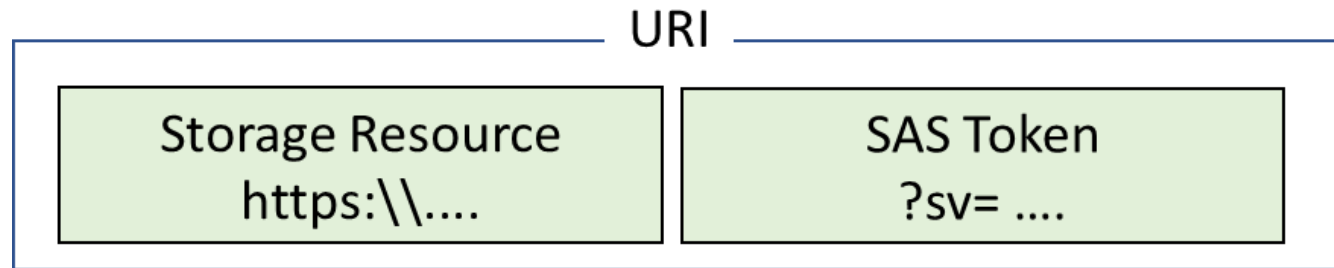
-Container "ContainerName"

-Blob "BlobName"

-Permission rwd

URI and SAS Parameters

A SAS is a signed URI that points to one or more storage resources
Consists of a storage resource URI and the SAS token



- Includes parameters for resource URI, storage services version, services, resource types, start time, expiry time, resource, permissions, IP range, protocol, signature

Demonstration: Storage Encryption

Enable encryption either at REST or in transit

Secure transfer required option will require HTTPS for any connections that come into the storage account

Practice: Shared Access Signatures

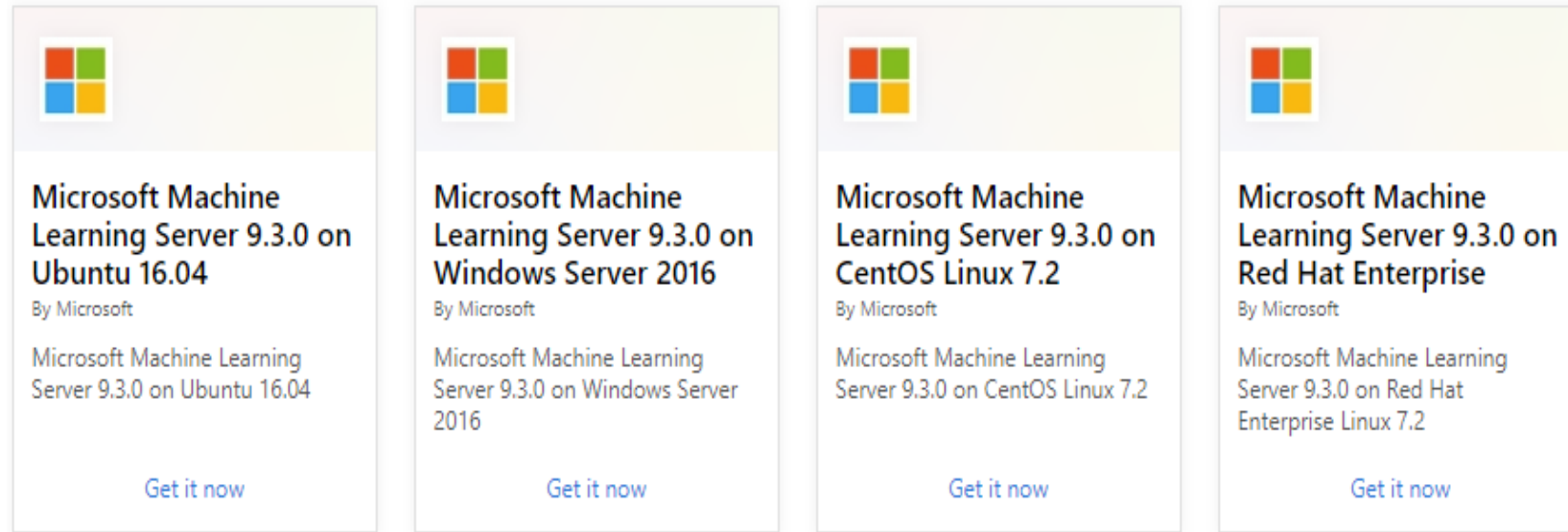
1. Generate an SAS in the Azure Portal
2. Use SAS to connect to your storage account through Storage Explorer
3. Configure additional SAS strings to work with different resources

Objective Review - #3

Create and configure a Virtual Machine (VM) for Windows and Linux

- Configure high availability
- Configure monitoring, networking, storage, and virtual machine size
- Deploy and configure scale sets

Supported Operating Systems



Windows Server includes many common products, requires a license, doesn't support OS upgrades

Linux distributions are supported, upgrade of the OS is supported

Demonstration: Deploying Linux Virtual Machines

Add an Ubuntu server from the Azure Marketplace

Configure settings in the Azure portal and create

Allow inbound rule SSH (TCP/22)

Connect to the running instance of the Linux VM through an SSH session

Connecting to Linux VMs

* Authentication type

SSH public key

Password

* SSH public key ⓘ

Provide an RSA public key in the single-line format (starting with "ssh-rsa") or the multi-line PEM format. You can generate SSH keys using ssh-keygen on Linux and OS X, or PuTTYGen on Windows.

Authenticate with a SSH public key or password

SSH is an encrypted connection protocol that allows secure logins over unsecured connections

[Video](#): Creating SSH Keys

Create SSH keys with ssh-keygen

If you can run a command shell such as Bash for Windows or GitBash (or Bash in Azure Cloud Shell), create an SSH key pair using the ssh-keygen command.

Create SSH keys with PuTTYgen

If you prefer to use a GUI-based tool to create SSH keys, you can use the PuTTYgen key generator. The steps to use PuTTYgen are shown in this video.

Practice: Advanced Azure Virtual Machine and Compute

Configure a virtual machine scale set

Administer a download and install PowerShell on an Ubuntu server using Git Bash

Create and upload an automation script from an ARM template

Video: Virtual Machine Storage

- Disks are how virtual machines store their VHD files
- Premium or Standard storage
- Managed or unmanaged
- Virtual Machine disk types
 - Operating System disks – SATA, C:
 - Temporary disk – short term storage
 - Data disks – depend on VM Type



Move a VM from on premises to Azure with Site Recovery

- Create Recovery Services Vault
- Select replication goal
- Set up source environment
- Set up Target environment
- Set up Replication policy
- Enable Replication

Demonstration: Virtual Machine Storage

Several ways to implement virtual machine storage

Storage configuration can be either managed or unmanaged

For VMs using unmanaged disks, you must manage the storage accounts

For VMs using managed disks, the storage account is set automatically

Premium Storage

Delivers high-performance, low-latency SSD disk support

Use for virtual machines with input/output (I/O)-intensive workloads

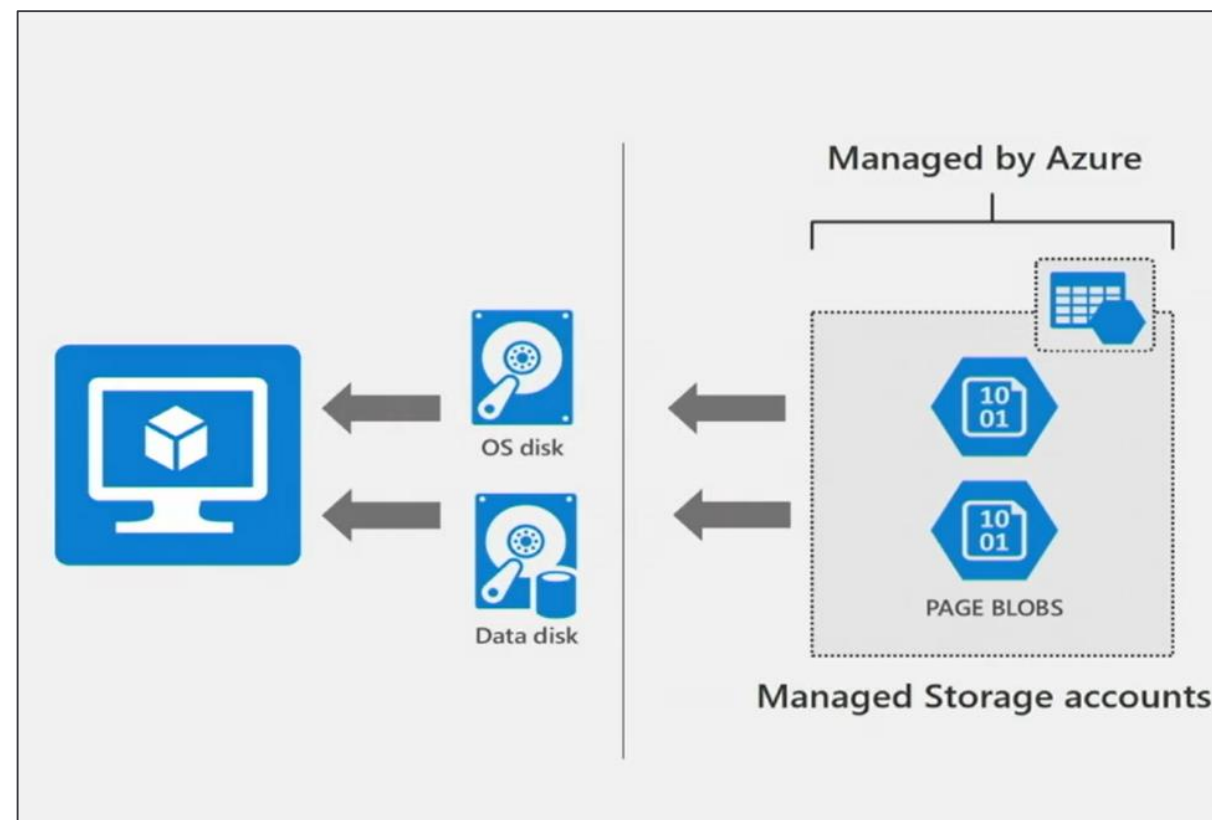
Two types of disks: Unmanaged and Managed

Unmanaged disks require you to manage the storage accounts and VHDs

Managed disks are maintained by Azure (recommended)

Video: Resiliency with Managed Disks

- Managed disks – abstract storage accounts from customers
- Granular access control – apply Azure RBAC
- Better performance - storage account limits do not apply
- Scale – thousands of disks per region per subscription



Demonstration: Attach and Detach Disks

Attach additional data disks to existing VMS

Number of data disks determined by the class or type of VM you deploy

Understand your workload and how many disks you think you'll need

Helps in sizing and choosing the correct size of VM when you deploy it

Demonstration: Upload Custom Disks

Upload and attach a local VHD file on the local system to a VM running in Azure
Create a storage account and a container to upload the VHD file
To upload the VHD, use PowerShell (**Add-AzureRMVhd**)
Create the new managed disk based on the uploaded VHD

Demonstration: Migrating from Managed Disks

Convert an unmanaged disk to a managed disk

Need to power off the virtual machine during the operation

Consider downtime and availability of applications

Virtual Machine Storage

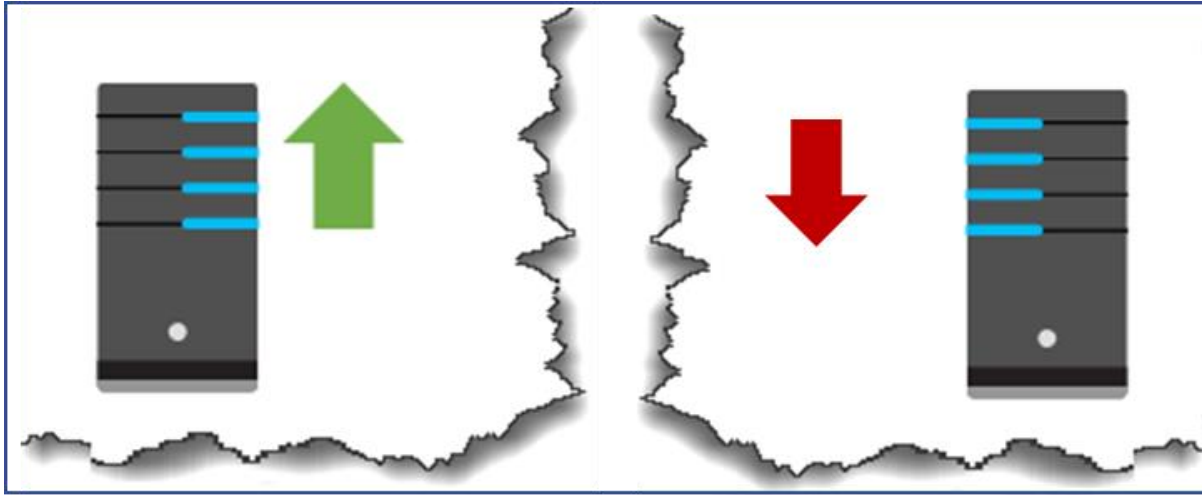
[Attach a data disk to a Windows VM using PowerShell](#)

[Detach a data disk from a Windows virtual machine](#)

[Convert Azure managed disks storage from standard to premium, and vice versa](#)

[Convert a Windows virtual machine from unmanaged disks to managed disks.](#)

Availability Sets



Two or more instances in
a set, 99.95% uptime

- Configure multiple virtual machines in an Availability Set
- Configure each application tier into separate Availability Sets
- Combine a Load Balancer with Availability Sets
- Use managed disks with the virtual machines

Update and Fault Domains

NAME	STATUS	FAULT DOMAIN	UPDATE DOMAIN
myVM0	Stopped (deallocated)	0	0
myVM1	Stopped (deallocated)	1	1

Update domains lets Azure to perform incremental or rolling upgrades across a deployment. During planned maintenance, only one update domain is rebooted at a time.

Fault Domains are a group of virtual machines that share a common set of hardware, switches, that share a single point of failure. VMs in an availability set are placed in at least two fault domains

Demonstration: Creating Availability Sets

End to end highly available solution

Redundancy at every level

Always specify an availability set when creating more than one virtual machine for the same purpose

Practice: Deploying a Highly Available VM

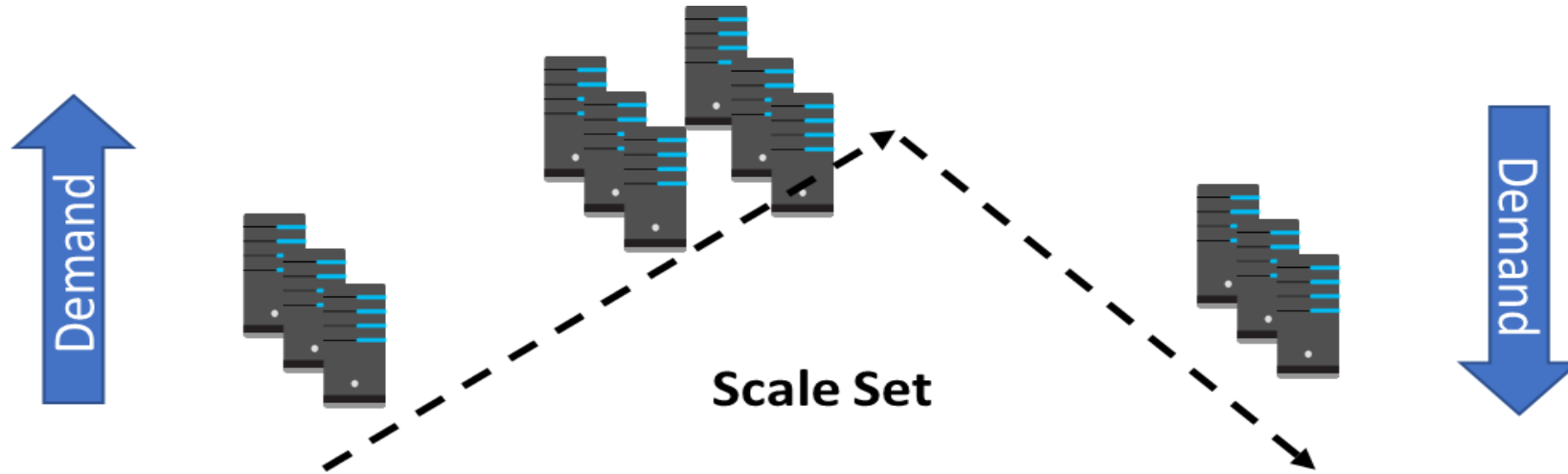
Create an Azure availability group

Deploy a Windows Server 2016 virtual machine into the availability set

Configure networking and storage for the virtual machine

You can also try [Tutorial: Create and deploy highly available virtual machines with Azure PowerShell](#)

Scale Sets



Scale sets deploy a set of identical VMs

No pre-provisioning of VMs is required

As demand goes up VMs are added, as demand goes down VM are removed

The process can be manual, automated, or a combination of both

Autoscale



Define rules to automatically adjust capacity

Scale out (increase) the number of VMs in the set

Scale in (reduce) the number of VMs in the set

Schedule events to increase or decrease at a fixed time

Reduces monitoring and optimizes performance

Implementing Autoscale

Define a minimum, maximum, and default number of VM instances

- Create simple scale sets with scale out and scale in parameters

INSTANCES

*

Instance count ⓘ

2

*

Instance size [\(View full pricing details\)](#) ⓘ

DS1_v2 (1 vCPU, 3.5 GB) ▼

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

Demonstration: Creating Scale Sets

Use Scale sets to reliably deploy and update at large scale

Deploy a group of virtual machines with the same configuration

Allow Azure to bring additional machines online or remove them

Based on the load or other criteria you have established

Practice: Scale Sets

Create a virtual machine scale set.
Connect to a VM in the scale set.

Practice: Autoscale

Create a rule to automatically scale out.

Create a rule to automatically scale in.

Define autoscale instance limits.

Monitor number of instances in a scale set.

Autoscale based on a schedule

Objective Review - #4

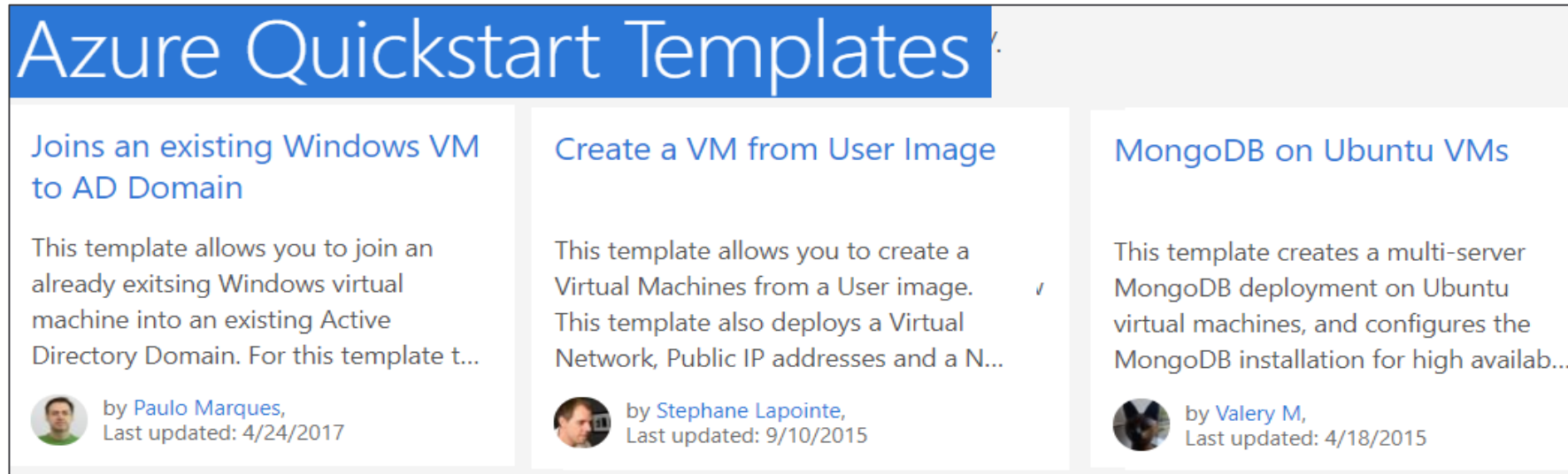
Automate deployment of Virtual Machines (VMs)

- Modify Azure Resource Manager (ARM) template
- Configure location of new VMs
- Configure VHD template
- Deploy from template
- Save a deployment as an ARM template
- Deploy Windows and Linux VMs

Resource Manager Templates

Element name	Required	Description
\$schema	Yes	Location of the JSON schema file that describes the version of the template language. Use the URL shown in the preceding example.
contentVersion	Yes	Version of the template (such as 1.0.0.0). You can provide any value for this element. Use this value to document significant changes in your template. When deploying resources using the template, this value can be used to make sure that the right template is being used.
parameters	No	Values that are provided when deployment is executed to customize resource deployment.
variables	No	Values that are used as JSON fragments in the template to simplify template language expressions.
functions	No	User-defined functions that are available within the template.
resources	Yes	Resource types that are deployed or updated in a resource group.
outputs	No	Values that are returned after deployment.

ARM Process



1. Azure provides many QuickStart templates. As much as possible, you should make use of these templates.
2. Values for the ARM template are provided in a JSON parameters file. You can standardize and reuse the templates.
3. Use the Portal, PowerShell, or the CLI to deploy the template.

Demonstration: Create a VM using ARM

Create a template file (JSON) to deploy required resources

Deployment options

Quickstart template on GitHub – allows you to take any JSON file, correctly structured and syntactically correct and feed it into the portal

Azure Marketplace – in reality, a wizard for JSON-based deployments

Deploy ARM templates directly from Visual Studio code

Supply a parameters file that contains the parameter values to the template

Practice: Creating Virtual Machines (Template)

Create template

Deploy template

Save a deployment as an ARM template

Export template – duplicate of original template

- Deployed in portal

- Readily usable

Template representing current state

- snapshot/backup of Resource Group

- Hard coded values

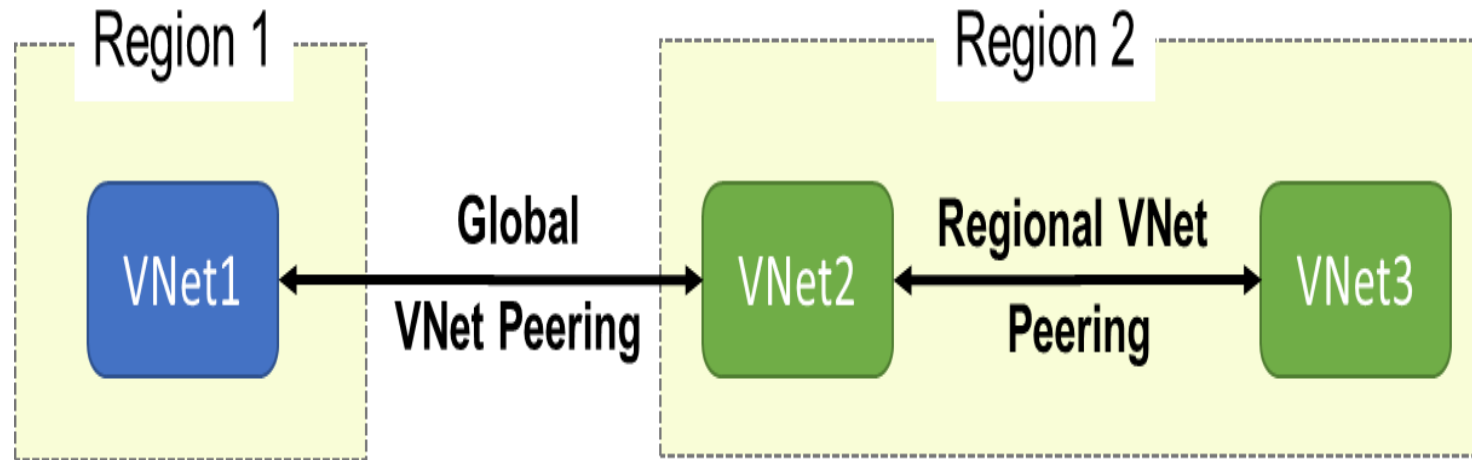
- If use for another resource group, may have to significantly modify

Objective Review - #5

Create connectivity between virtual networks

- Create and configure VNET peering
- Create and configure VNET to VNET
- Verify virtual network connectivity
- Create virtual network gateway

VNet Peering



VNet peering connects two Azure virtual networks (not transient)

Two types of peering: Regional and Global

Peered networks use the Azure backbone for privacy and isolation

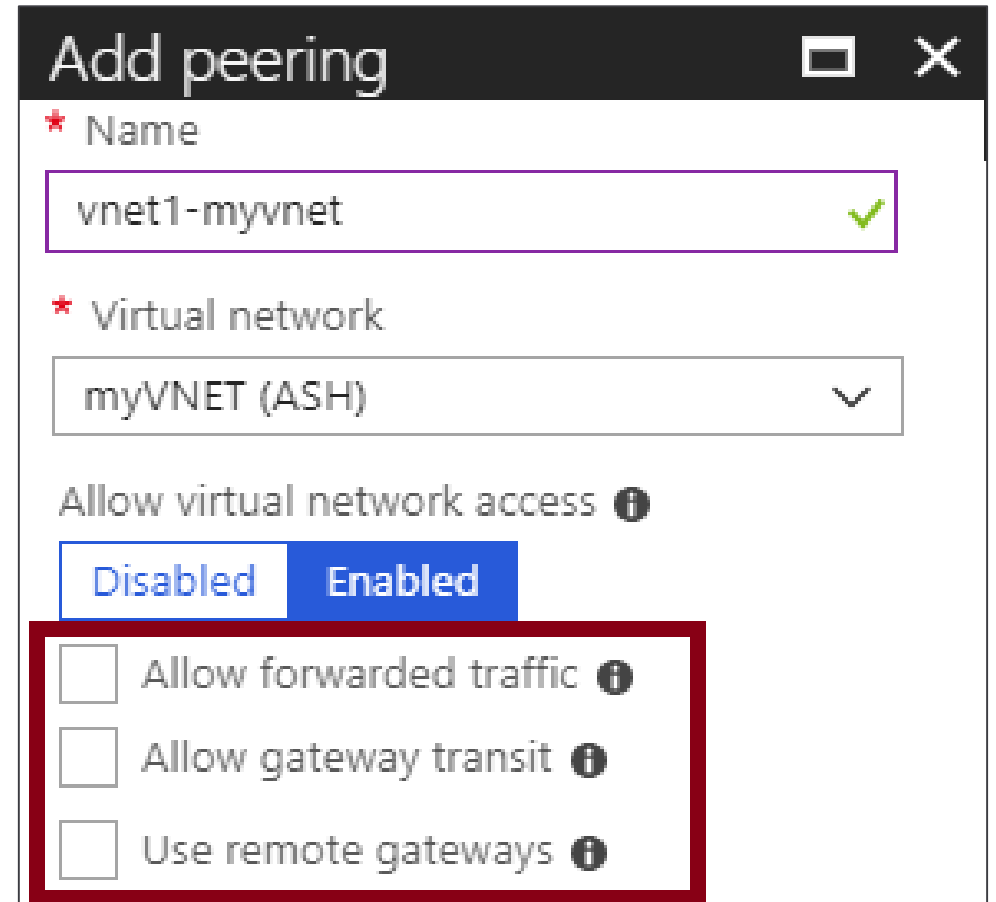
Easy to setup, seamless data transfer, and great performance

Regional VNet Peering

Allow forwarded traffic from within the peer virtual network into your virtual network.

Allow gateway transit. Allows the peer virtual network to use your virtual network gateway. (upcoming topic)

Use remote gateways. Only one virtual network can have this enabled



Add peering

* Name
vnet1-myvnet ✓

* Virtual network
myVNET (ASH) ▼

Allow virtual network access ⓘ



Disabled Enabled

☐ Allow forwarded traffic ⓘ

☐ Allow gateway transit ⓘ

☐ Use remote gateways ⓘ

Global VNet Peering

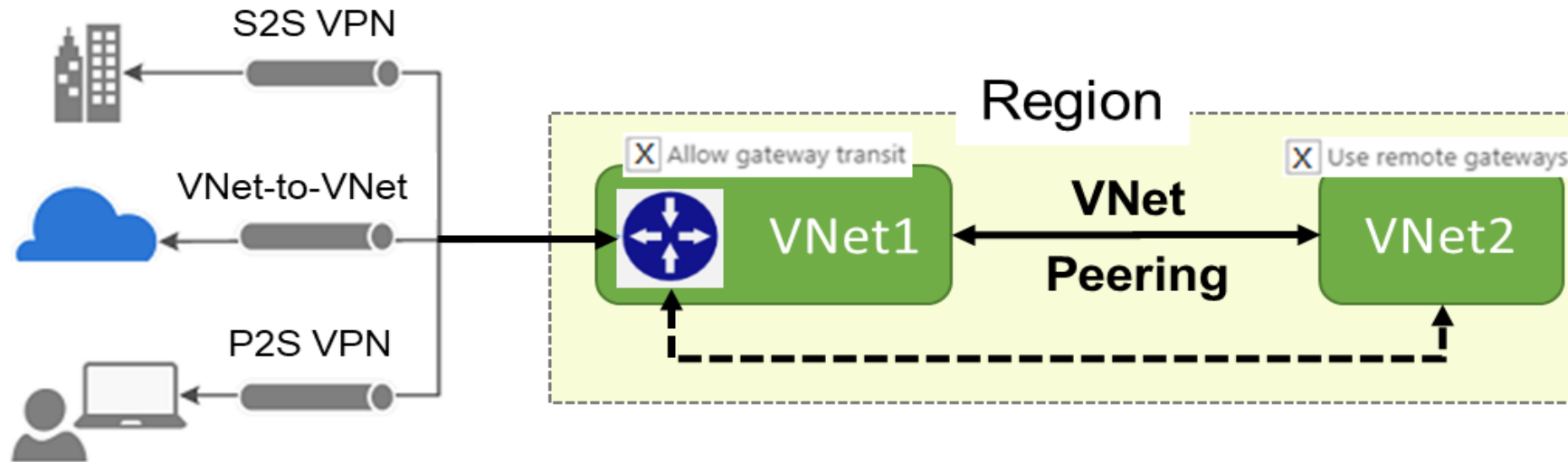
SETTINGS		NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
 DNS servers		myVirtualNetwork1-myVirtualNetwork2	Initiated	myVirtualNetwork2	Disabled
 Peerings					

Global VNet peering connects virtual networks across regions

Status will be Initiated or Connected

Special requirements: public clouds only, virtual network resource limitations, no gateway transit, no transitivity, and limitations on high performance virtual machines.

Gateway Transit



Gateway transit allows peered virtual networks to share the gateway and get access to resources.

This means you do not need to deploy a VPN gateway in the peer virtual network.

Objective Review - #6

Implement and manage virtual networking

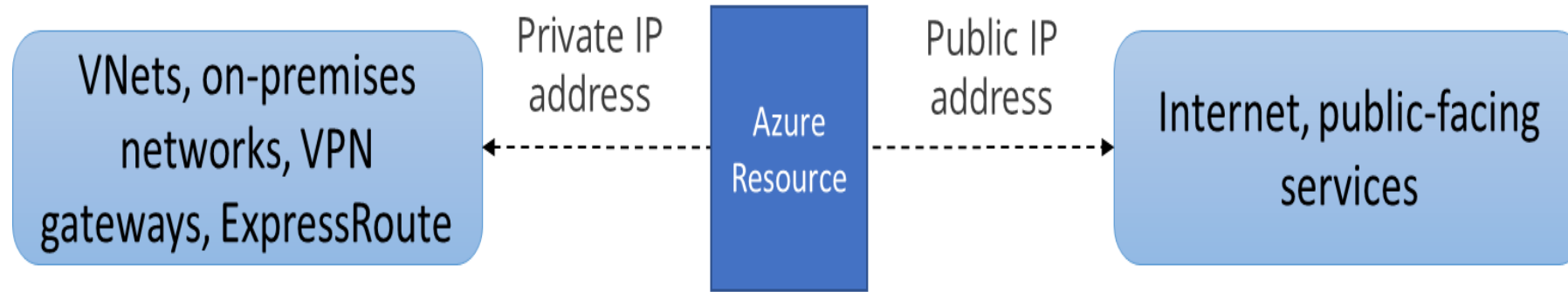
- Configure private and public IP addresses, network routes, network interface, subnets, and virtual network

Video: IP Addressing

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load balancer	Front end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	No
Application Gateway	Front end configuration	Yes	No

Private IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load balancer	Front end configuration	Yes	Yes
Application gateway	Front end configuration	Yes	Yes

Private and Public IP Addresses



Private IP addresses are used for communication within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure.

Public IP addresses is used for communication with the Internet, including Azure public-facing services.

System Routes

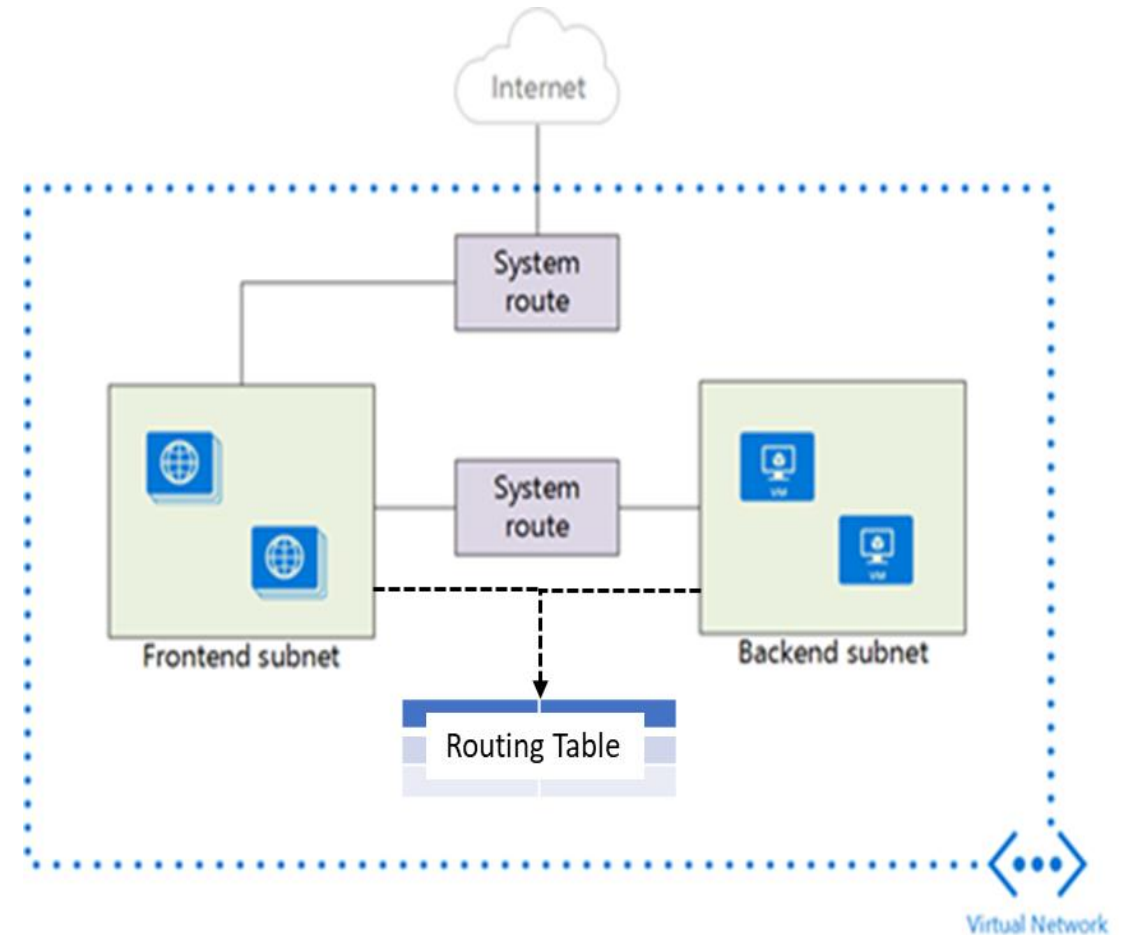
System routes direct network traffic between virtual machines, on-premises networks, and the Internet

Traffic between VMs in the same subnet
Between VMs in different subnets in the same virtual network

Data flow from VMs to the Internet

Communication between VMs using a
VNet-to-VNet VPN

Site-to-Site and ExpressRoute
communication through the VPN gateway

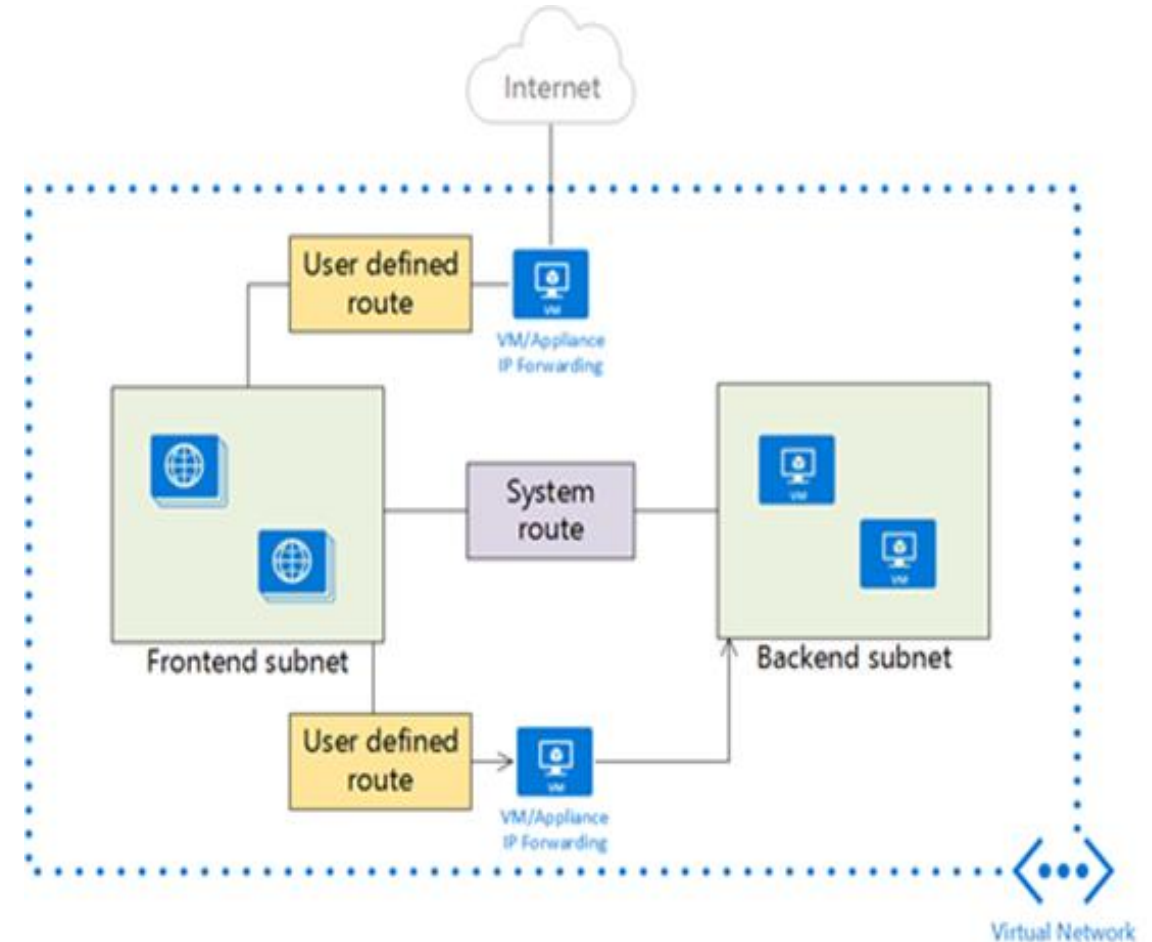


User Defined Routes

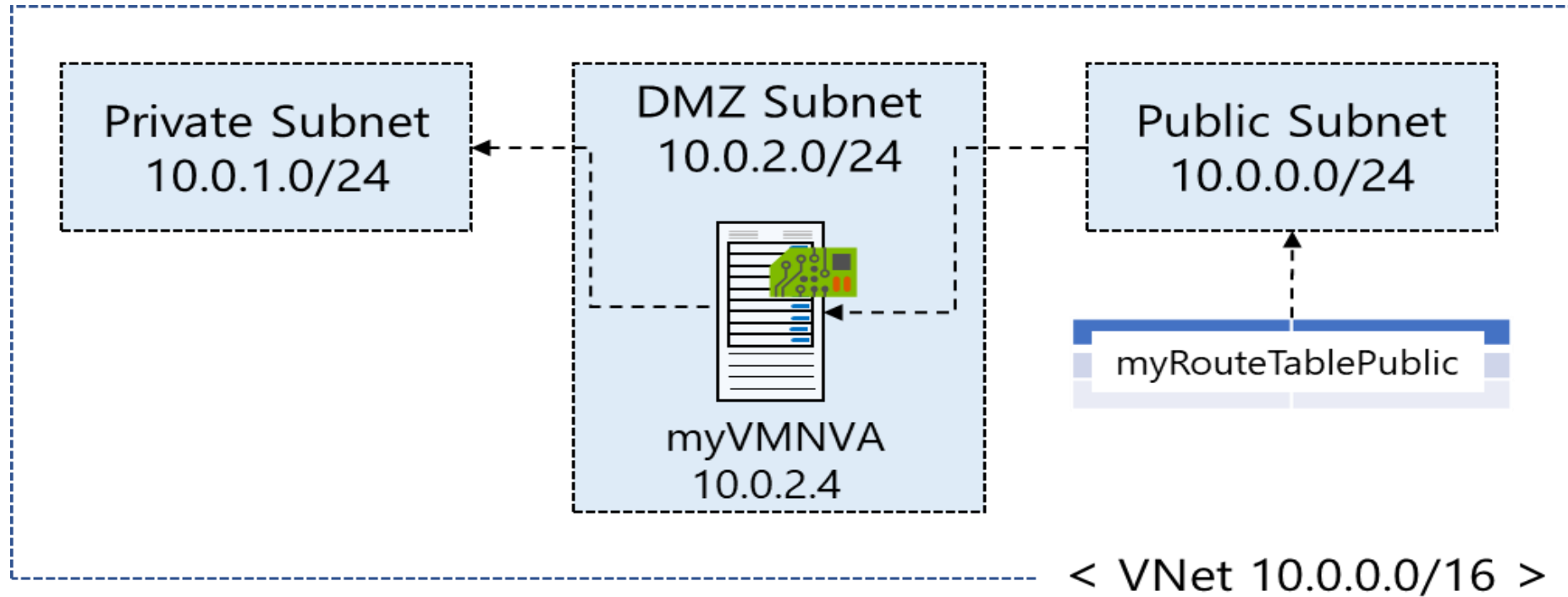
A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network

User-defined routes are custom routes that control network traffic by defining routes that specify the next hop of the traffic flow

The next hop can be a virtual network gateway, virtual network, internet, or virtual appliance



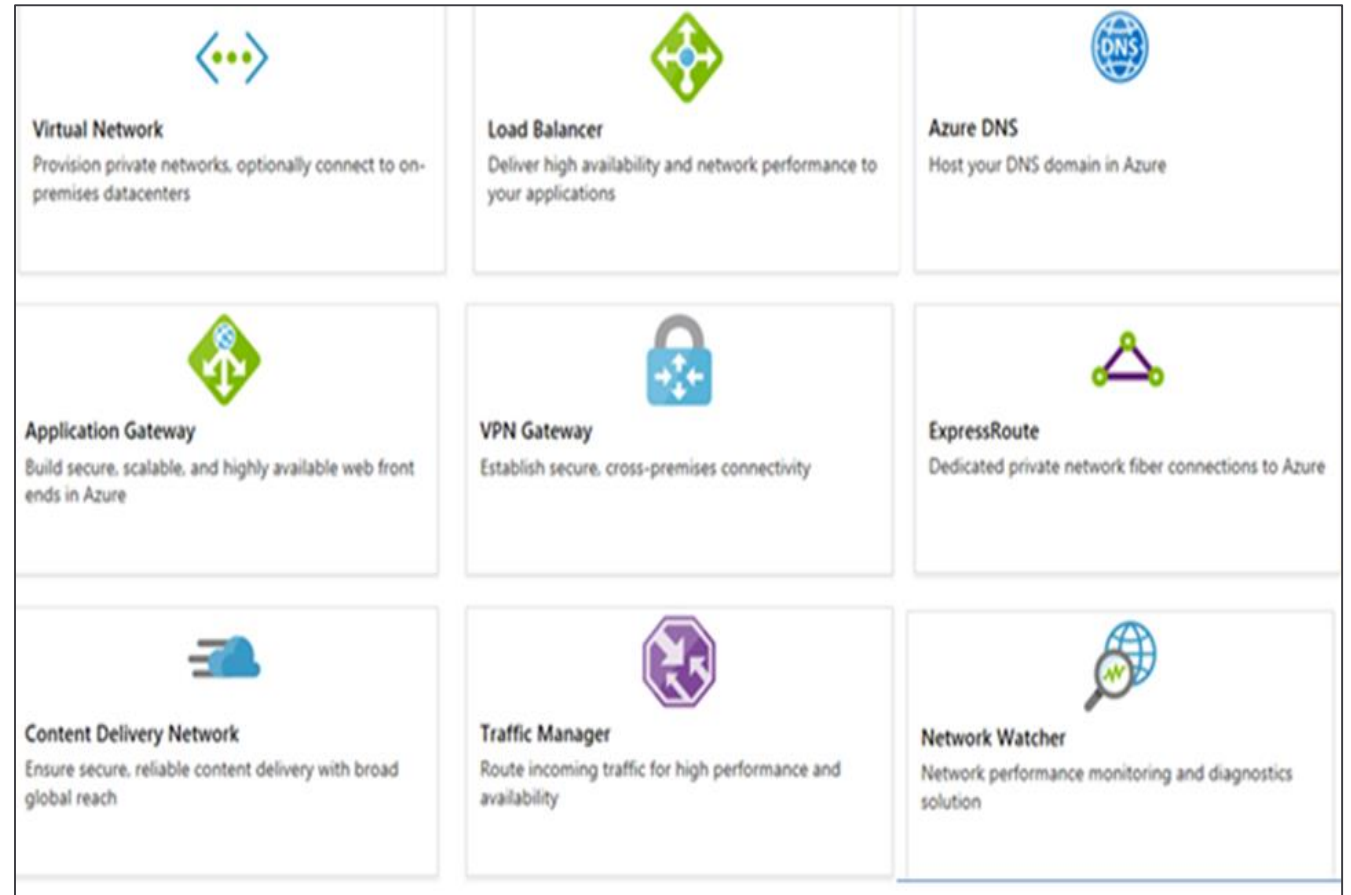
Routing Example



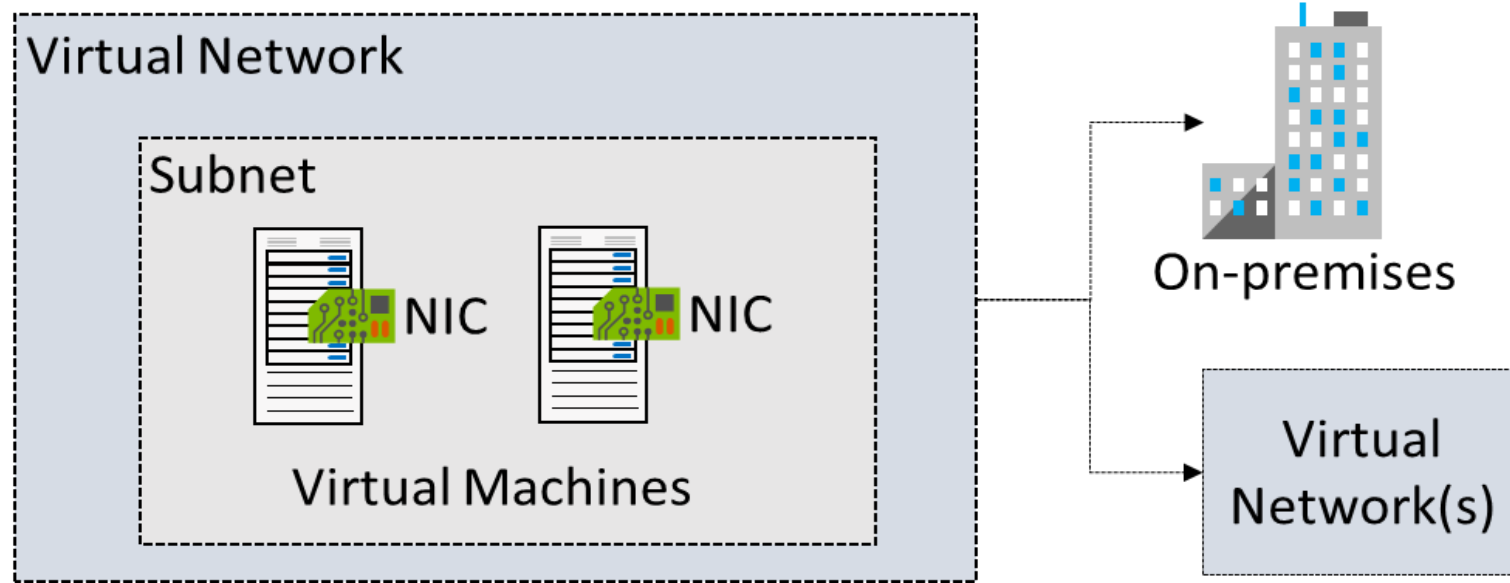
1. Create the route table
2. Create the route
3. Associate the route to the subnet

Introduction to Azure Networking Components

Adopting cloud solutions can save time and simplify operations
Azure requires the same types of networking functionality as on-premises infrastructure
Azure networking offers a wide range of services and products

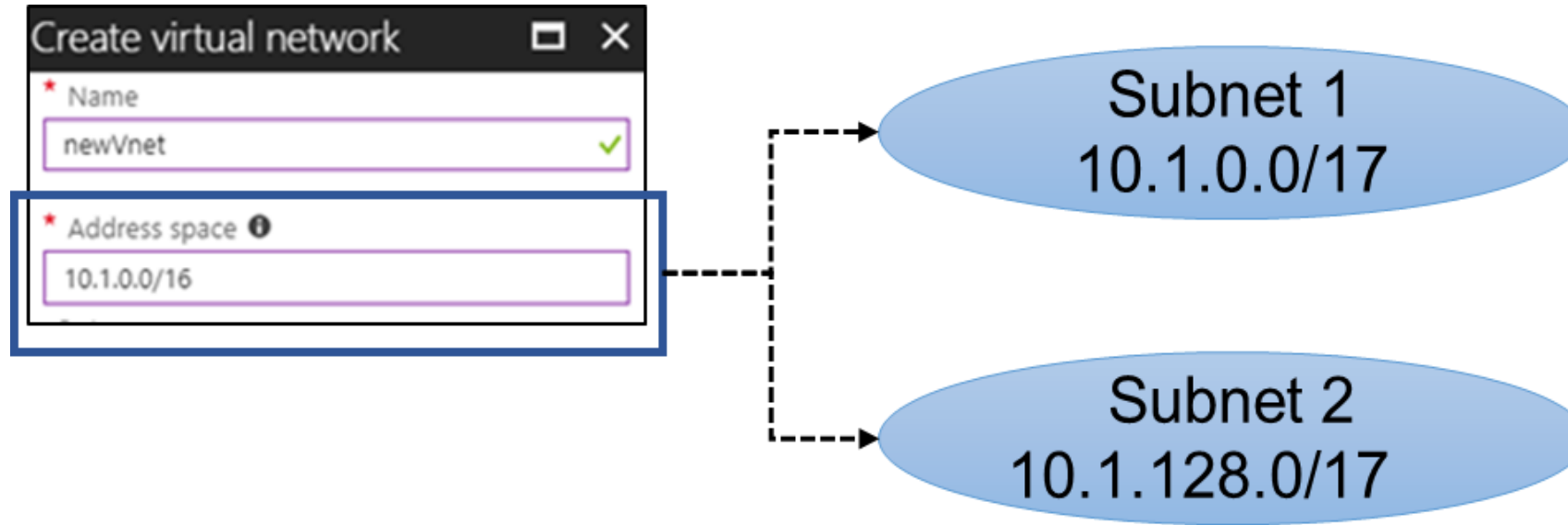


Virtual Networks



Logical representation of your own network
Create a dedicated private cloud-only VNet
Securely extend your datacenter With VNets
Enable hybrid cloud scenarios

Subnets



A virtual network can be segmented into one or more subnets

Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

Video: Managing Virtual Networks (Common Tasks)

Creating a virtual network

Viewing virtual networks and settings

Adding and removing address spaces

Adding and changing a DNS server

Deleting a virtual network

Practice: Virtual Networks

Create a virtual network

Create virtual machines

Connect to a VM from the internet

Communicate between VMs

Objective Review - #7

Manage Azure Active Directory (AD)

- Add custom domains
- Configure Azure AD Identity Protection, Azure AD Join, and Enterprise State Roaming
- Configure self-service password reset
- Implement conditional access policies
- Manage multiple directories
- Perform an access review

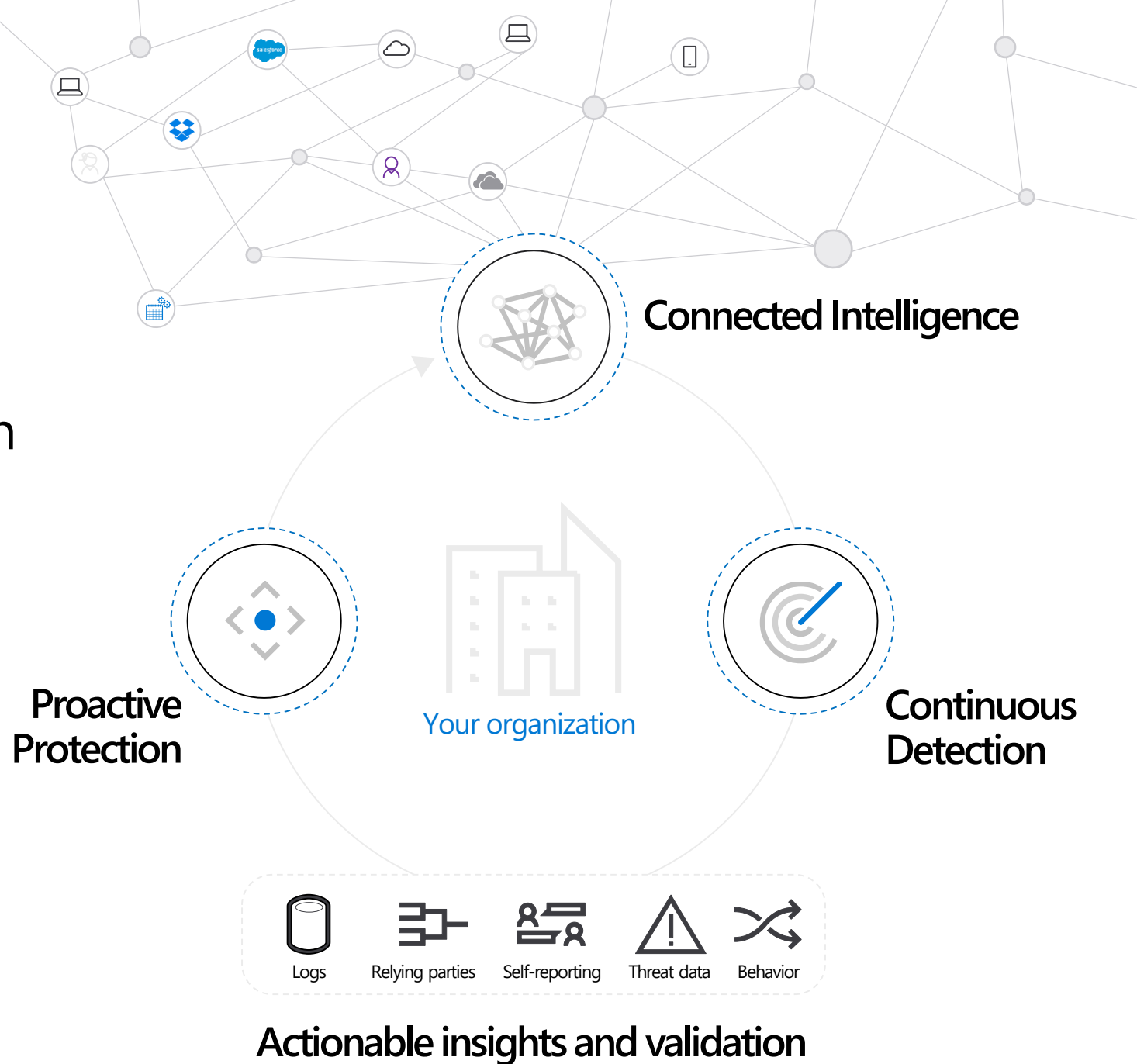
AD Custom Domain

- Create your domain name with a domain registrar
- Create your directory in Azure AD
- Add your custom domain name to Azure AD
- Add your DNS information to the domain registrar
- Verify your custom domain name

Azure Active Directory Identity Protection

Delivering intelligent security
requires a cloud-powered solution

- Proactive, AI-enhanced protection
- Automatic, real-time remediation
- Machine learning at a massive scale
- Detect potential vulnerabilities
- Configure automated responses
- Ability to:
 - Consolidated view of flagged users and risk events
 - Set risk-based Conditional Access policies to automatically protect your users
 - Improve security posture



Azure AD Join

- Ability for users to have a self-service experience to join their devices to the company network
- No need to join on-premises AD
- Enterprise and at-scale ready

Enterprise State Roaming

Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device/synchronizing user and app settings data to the cloud.

Similar to consumer settings sync that was first introduced in Windows as well as:

- Separation of corporate and consumer data
- Enhanced security
- Better management and monitoring

Objective Review - #8

Implement and manage hybrid identities

- Install and configure Azure AD Connect
- Configure federation and single sign-on
- Manage Azure AD Connect
- Manage password sync and writeback

Azure AD Connect

Integrates AD DS with Azure AD:

Implements a common identity for your users across Azure, Office 365, and SaaS apps

Provides support for:

Sync Services: synchronize AD DS objects, such as users and groups.

Health Monitoring: offers centralized monitoring

Federation: simplifies configuration of AD FS

Filtering of synchronization scope

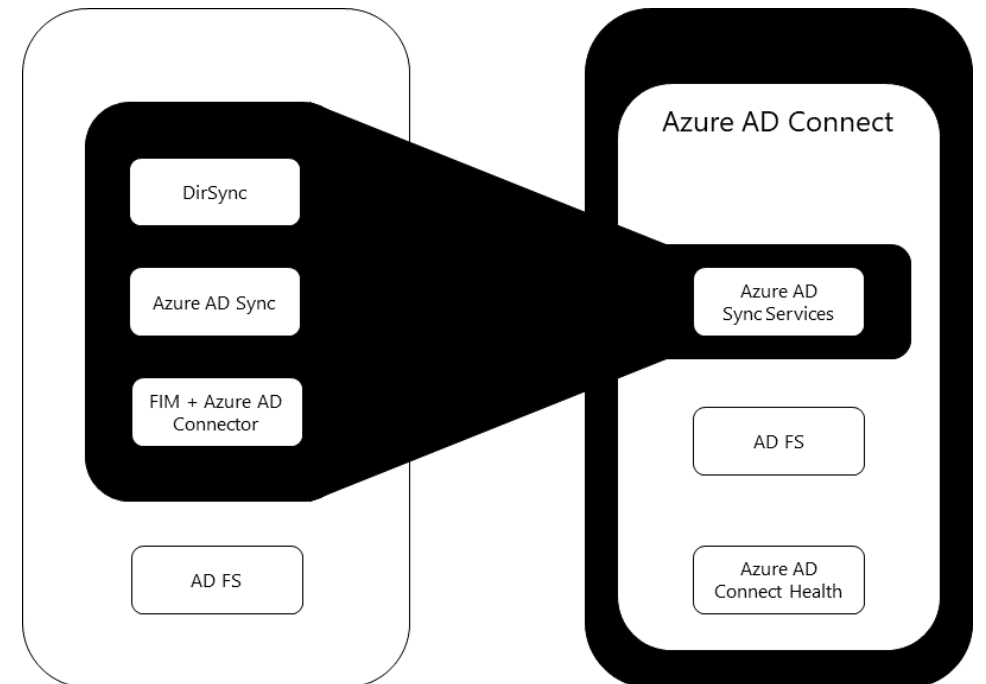
Password hash synchronization

Protection against accidental deletes

Password writeback

Device writeback

Automatic upgrades



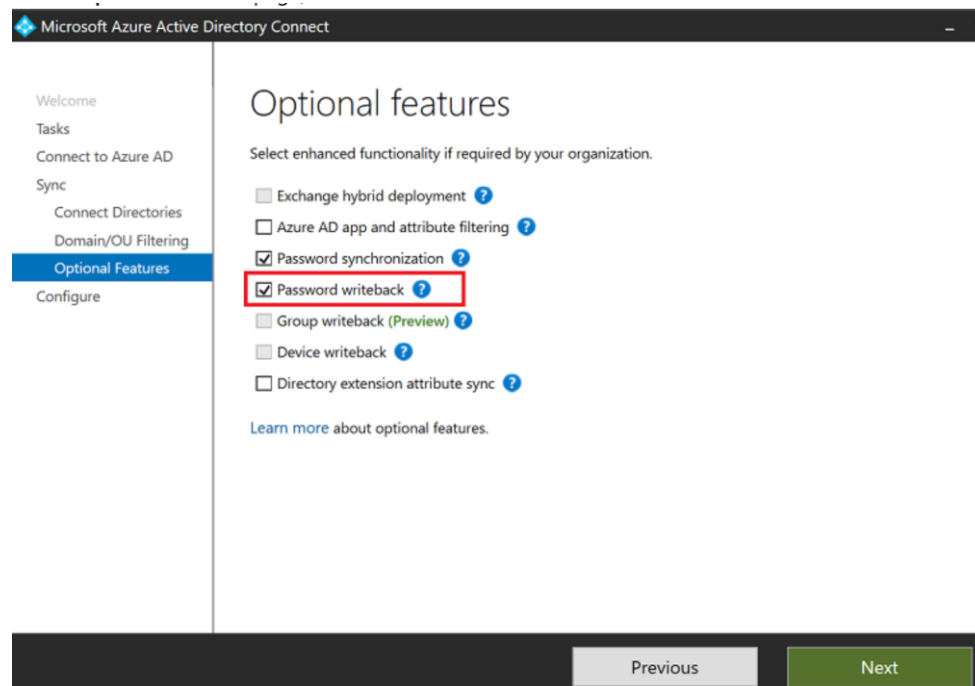
Active Directory Connect

Staging Mode

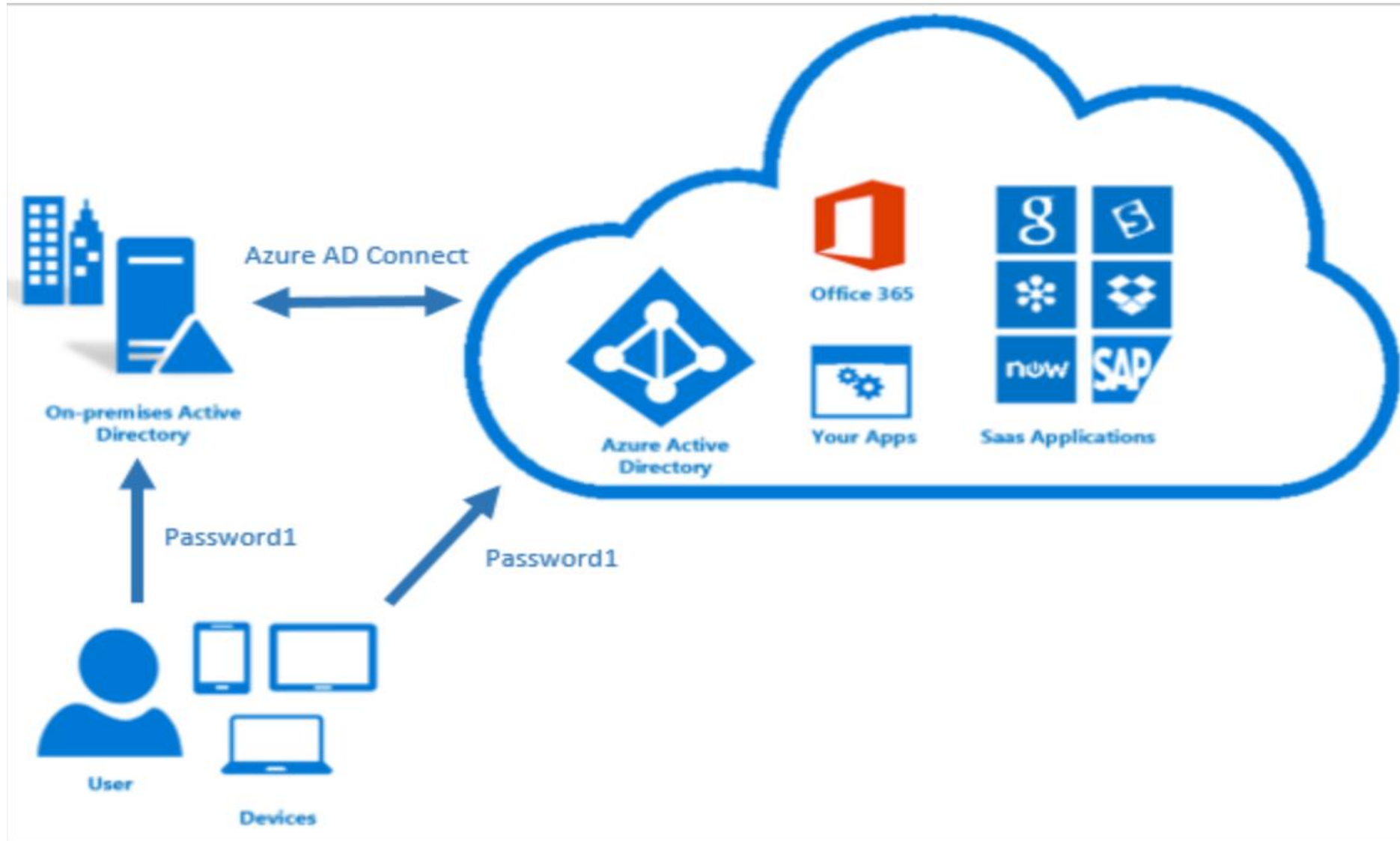
- High availability
- Test and deploy new configuration changes
- Introduce a new server and decommission the old

Active Directory Connect Writeback

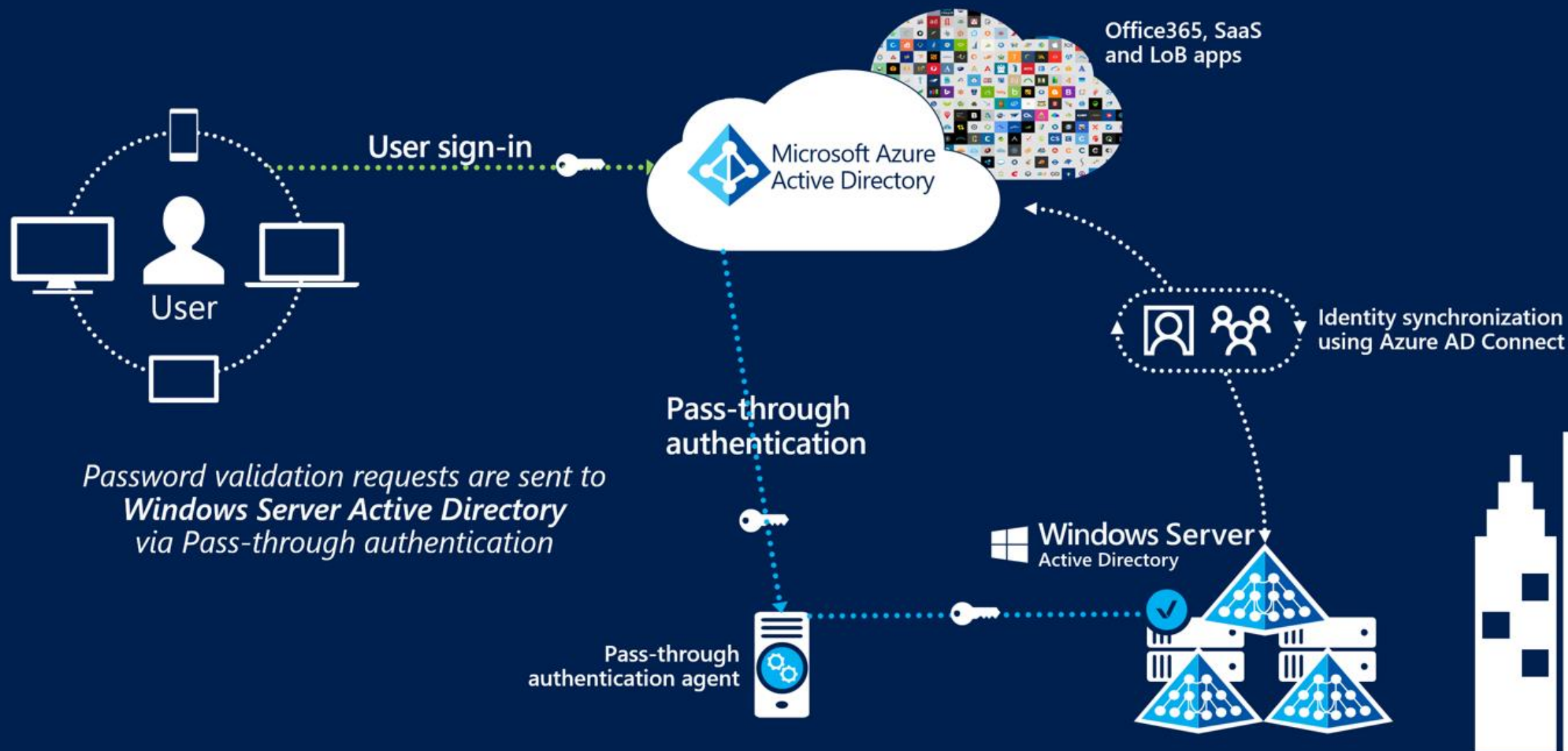
- Subscription to Azure AD Premium is required for device writeback
- Used to enable conditional access based on devices to ADFS (2012 R2 or higher) protected applications (relying party trusts)



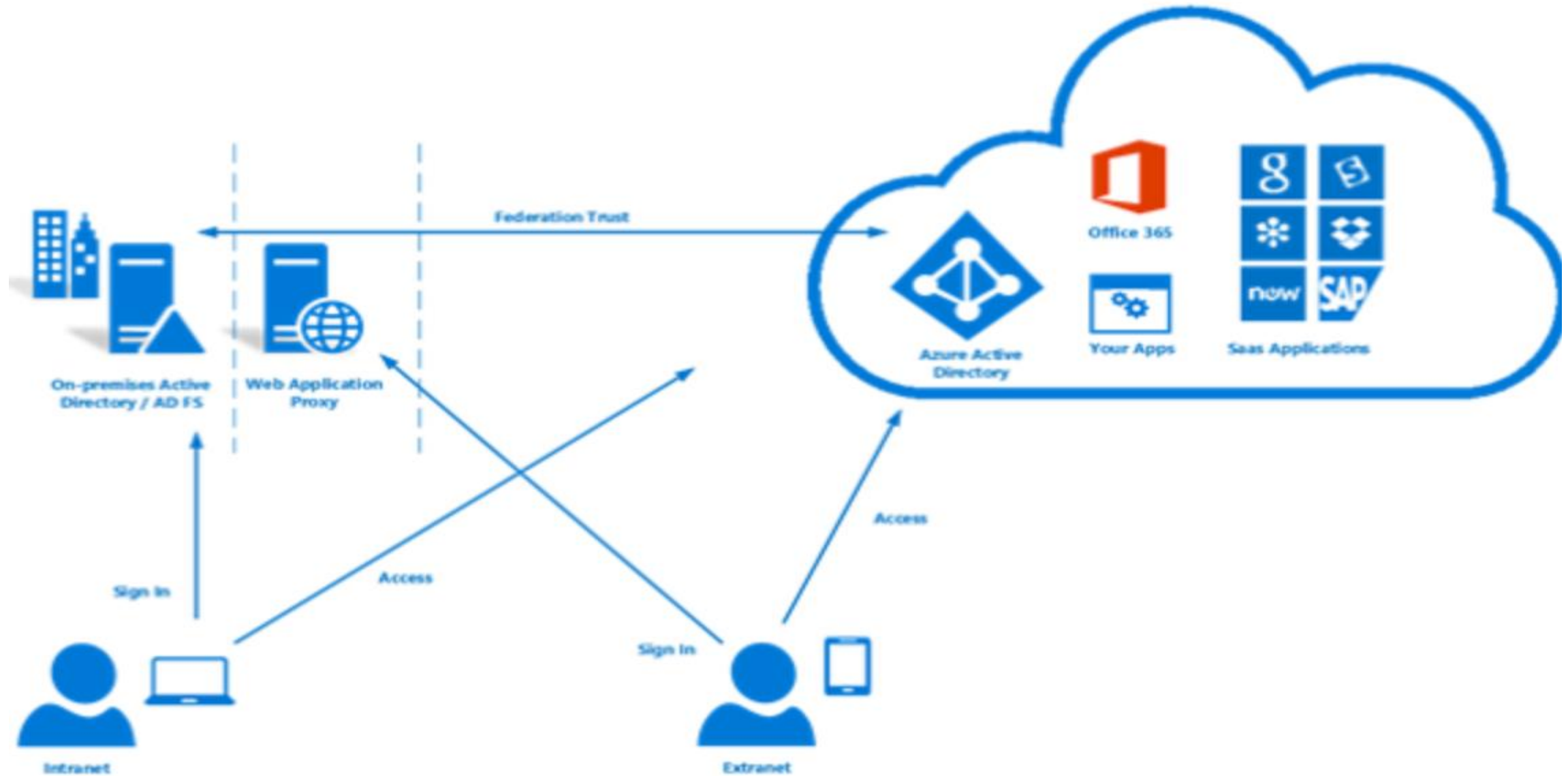
Password hash synchronization with AD



Azure AD Pass-Through Synchronization (alternative to Password Sync)



Federation



Hybrid Identity

[Password hash synchronization \(PHS\)](#)

[Pass-through authentication \(PTA\)](#)

[Federation](#)

Provides single-sign on

Questions?

