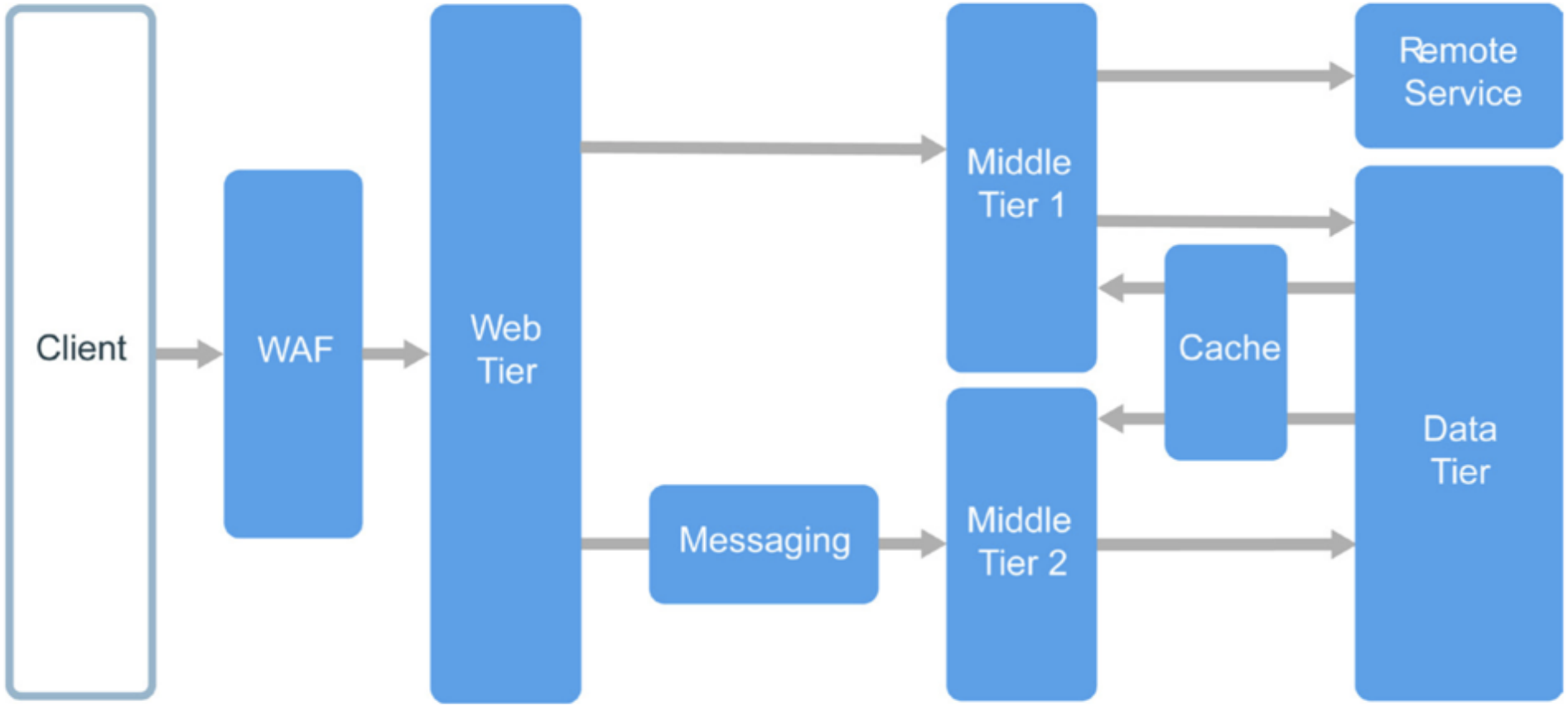
Microsoft

Azure Solutions Architecture (AZ-303)

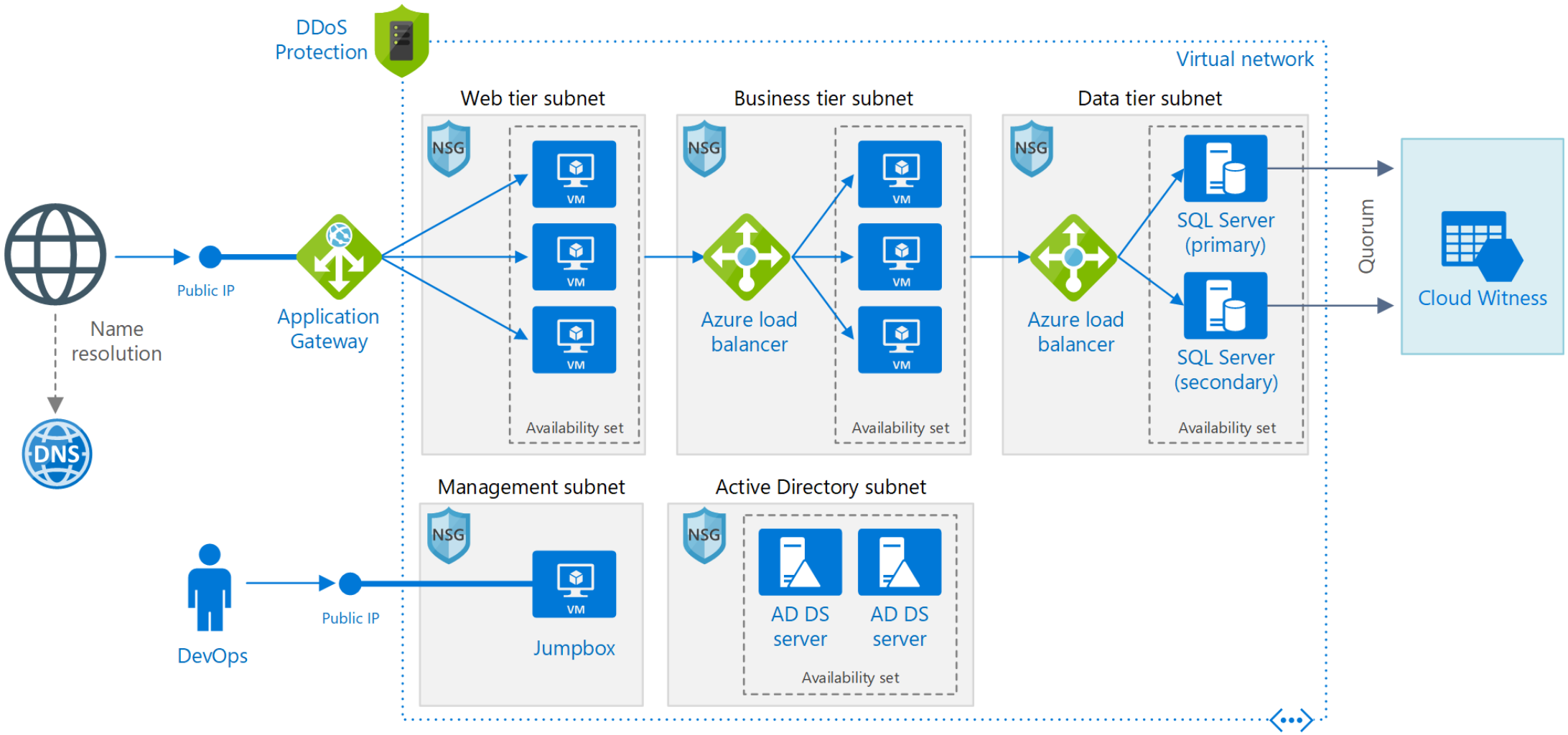
Four questions we always need to be asking ourselves

1. Where are the single points of failure in this architecture?
2. How could I break this thing?
3. How could I do this with the least amount of spend?
4. How can we do this using the least amount of administrative effort

N-tier Application Architecture



N-tier Application Architecture



N-tier Application Architecture

- Consider an N-tier architecture for:
  - Simple web applications
  - Migrating an on-premises application to Azure with minimal refactoring
  - Unified development of on-premises and cloud applications
- N-tier architectures are very common in traditional on-premises applications, so it's a natural fit for migrating existing workloads to Azure

N-tier Application Architecture Benefits

- Portability between cloud and on-premises, and between cloud platforms
- Less learning curve for most developers
- Natural evolution from the traditional application model
- Open to heterogeneous environment (Windows/Linux)

N-tier Application Architecture Challenges

- Monolithic design prevents independent deployment of features.
- Managing an IaaS application is more work than an application that uses only managed services.
- It’s easy to end up with a middle tier that just does CRUD operations on the database, adding extra latency without doing any useful work.

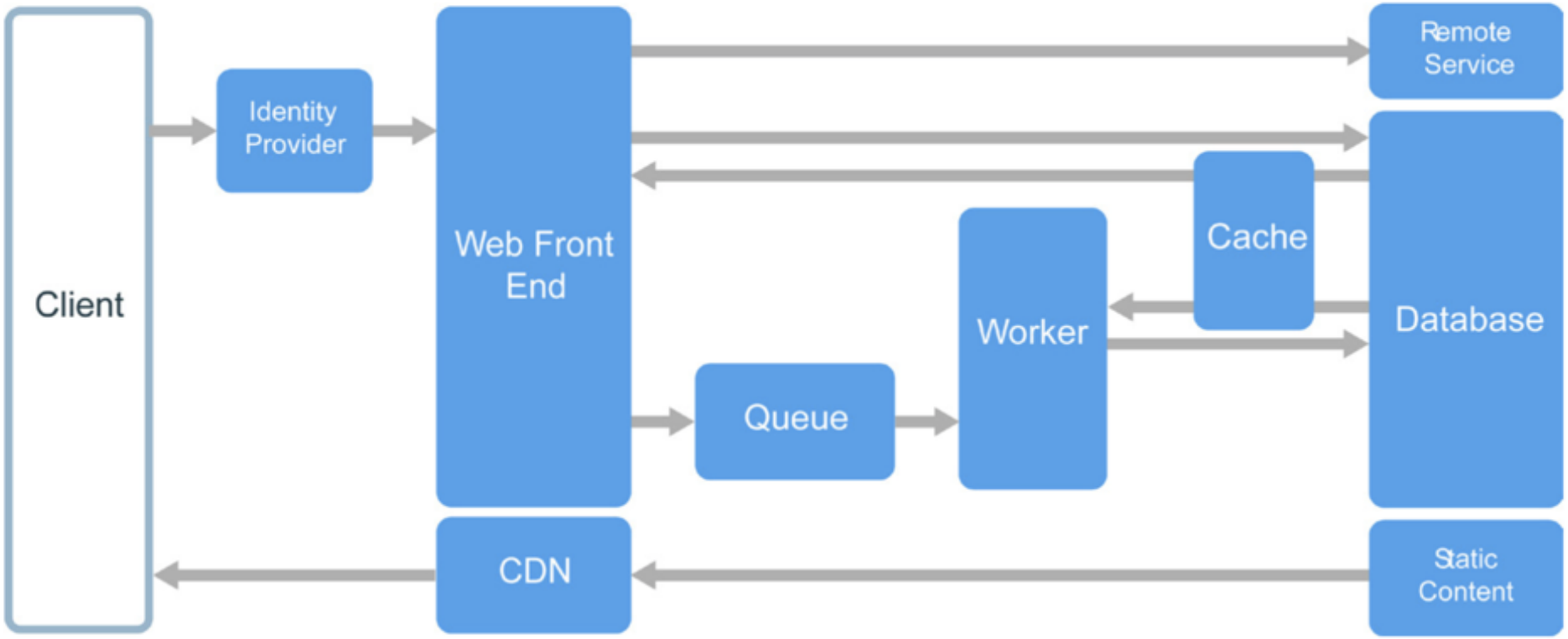
N-tier Application Architecture Best Practices

- Use autoscaling to handle changes in load
- Architect for high availability
- Protect internet facing web apps with web application firewall (WAF)
- Place each tier in its own subnet and use as a security boundary
- Restrict access between the various tiers of the application

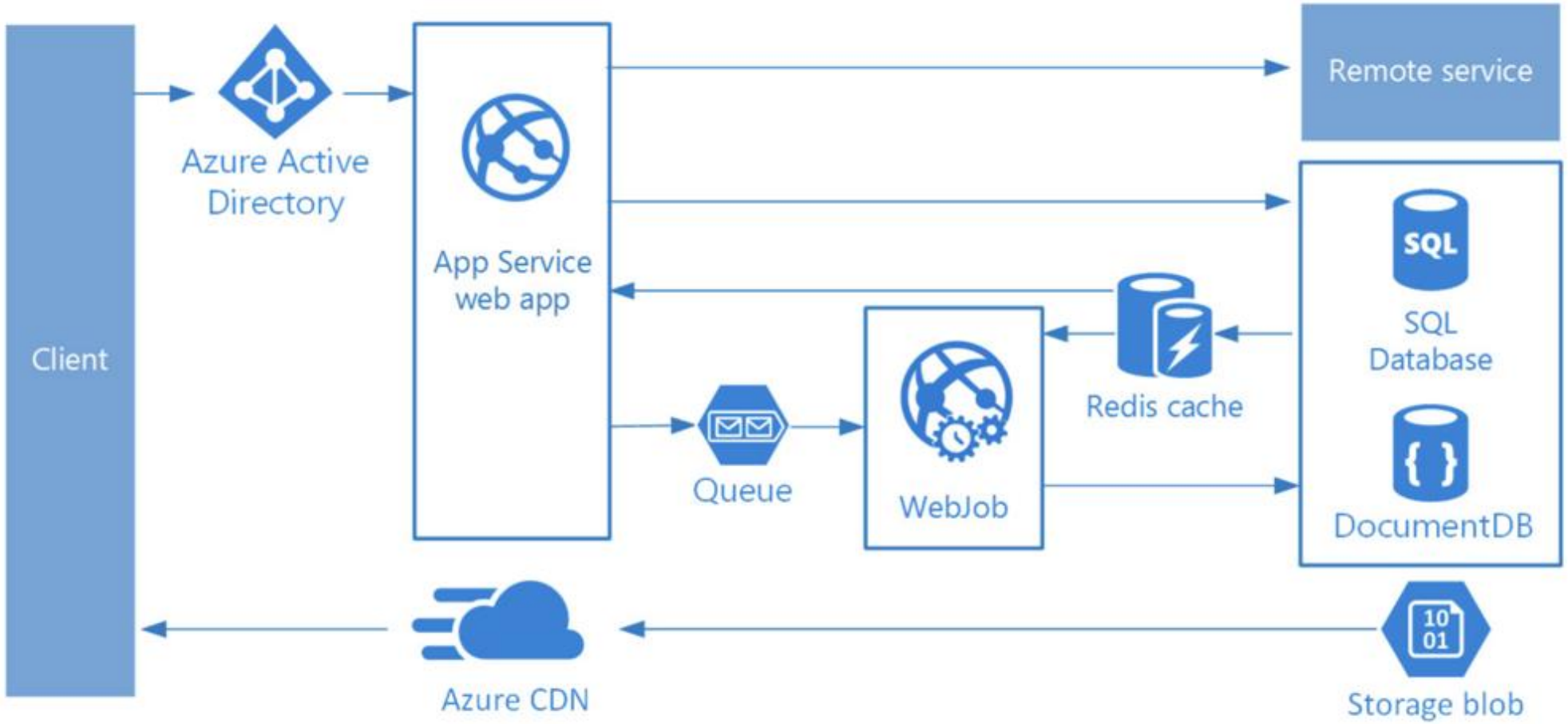
Additional Architecture Best Practices

- Lead with managed services when possible
- To increase security, implement a network DMZ that includes network virtual appliances (NVAs) that implement additional security checks and controls
- Do not allow RDP or SSH from the internet
- Implement multi-region architecture for increased redundancy

Web-Queue-Worker Architecture



Web-Queue-Worker Architecture



Web-Queue-Worker Architecture

- Consider an Web-Queue-Worker architecture for:
  - Applications with some long-running work flows or batch operations
  - When you want to use managed services, rather than infrastructure as a service (IaaS)

Web-Queue-Worker Architecture Benefits

- Relatively simple architecture that is easy to understand
- Easy to deploy and manage
- Clear separation of concerns
- The front end is decoupled from the worker using asynchronous messaging
- The front end and the worker can be scaled independently

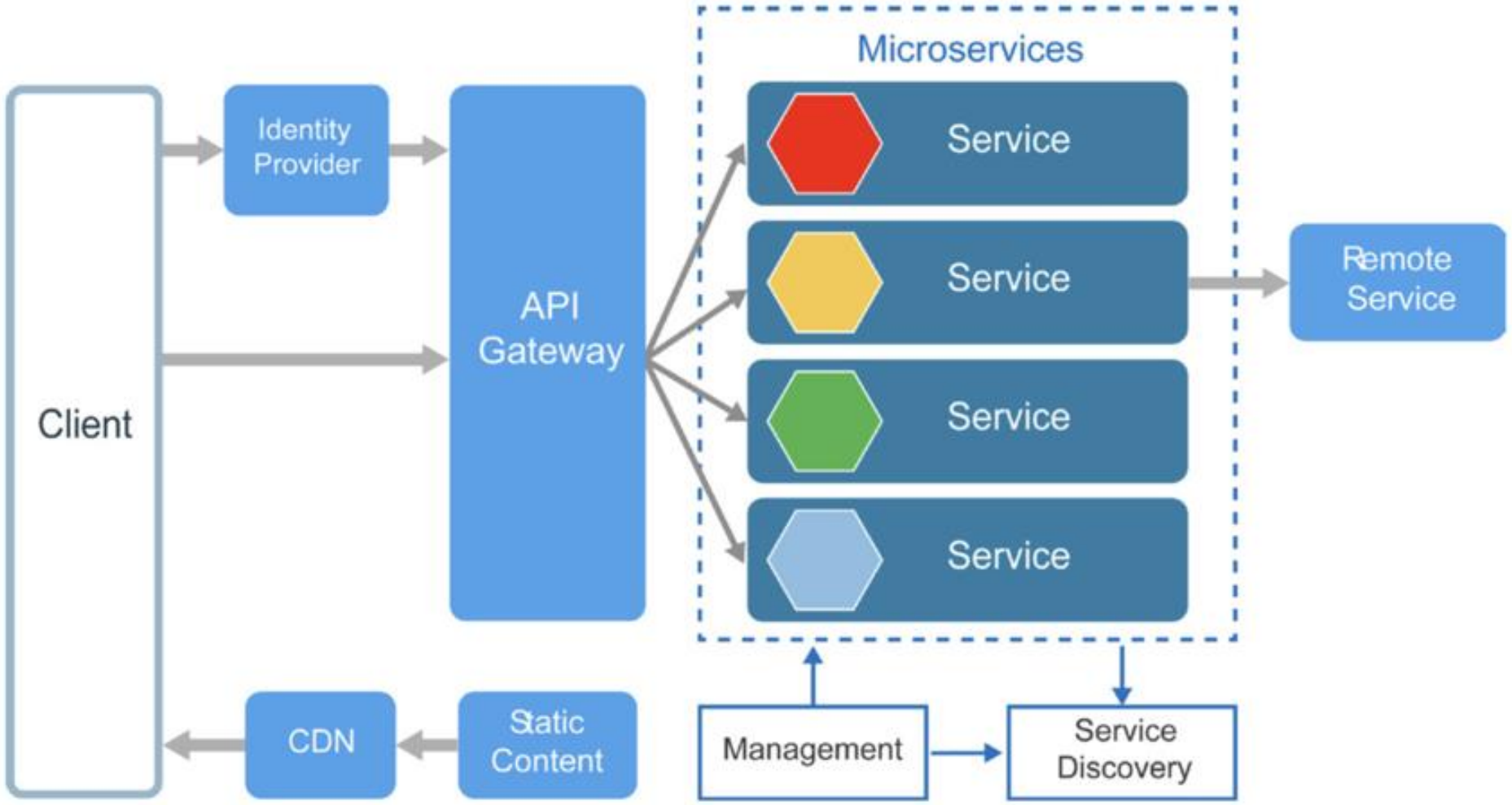
Web-Queue-Worker Architecture Challenges

- Without careful design, the front end and the worker can become large, monolithic components that are di cult to maintain and update.
- There may be hidden dependencies, if the front end and worker share data schemas or code modules.

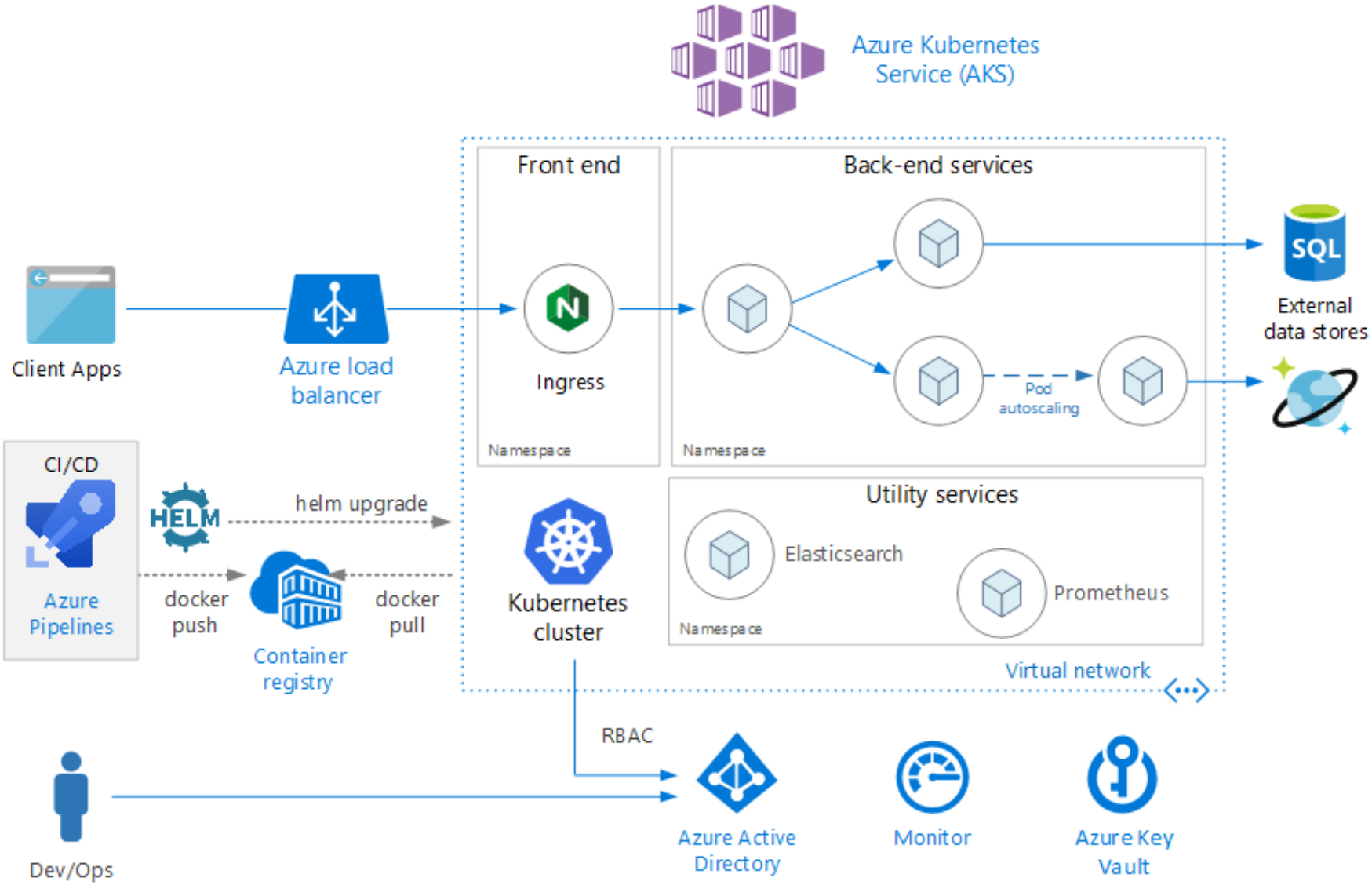
Additional Architecture Best Practices

- Use deployment slots to manage deployments. This lets you to deploy an updated version to a staging slot, then swap over to the new version. It also lets you swap back to the previous version, if there was a problem with the update.
- Use the built-in autoscale feature of App Service to scale out the number of VM instances. If the load on the application follows predictable patterns, use schedule-based autoscale. If the load is unpredictable, use metrics-based autoscaling rules.

Microservices Architecture



Microservices Architecture



Microservices Architecture

- Consider Microservices for:
  - Large applications that require a high release velocity
  - Complex applications that need to be highly scalable
  - Applications with rich domains or many subdomains
  - An organization that consists of small development teams

Microservices Architecture Benefits

- Independent deployments. You can update a service without redeploying the entire application, and roll back or roll forward an update if something goes wrong.
- Independent development. A single development team can build, test, and deploy a service. The result is continuous innovation and a faster release cadence.
- Small, focused teams. Teams can focus on one service. The smaller scope of each service makes the code base easier to understand, and it’s easier for new team members to ramp up.

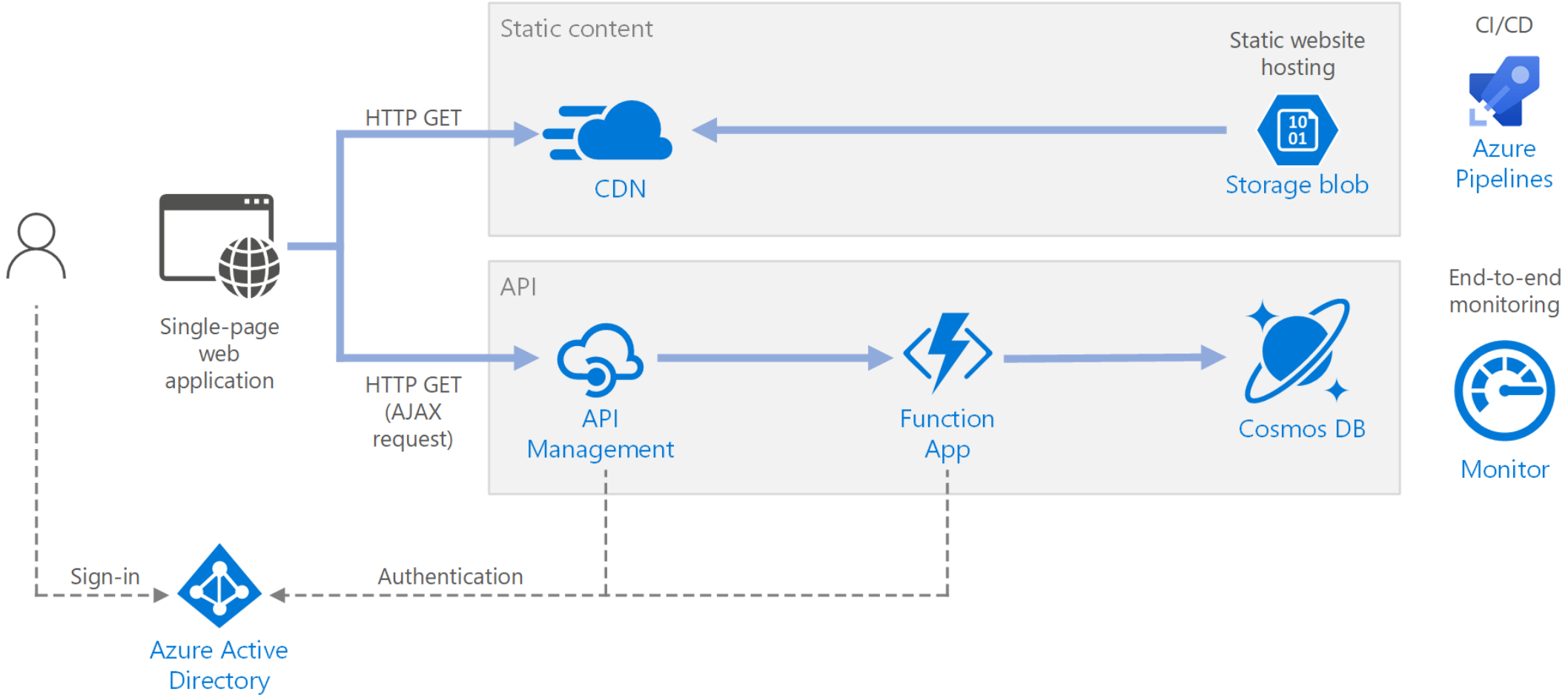
Microservices Architecture Benefits

- Fault isolation. If a service goes down, it won't take out the entire application. However, that doesn't mean you get resiliency for free. You still need to follow resiliency best practices and design patterns. See Designing resilient applications for Azure.
- Mixed technology stacks. Teams can pick the technology that best ts their service.
- Granular scaling. Services can be scaled independently. At the same time, the higher density of services per VM means that VM resources are fully utilized. Using placement constraints, a services can be matched to a VM pro le (high CPU, high memory, and so on).

Microservices Architecture Challenges

- Operational Complexity
- Governance Complexity
- Skillset

Serverless Architecture



Serverless Architecture

- Consider Serverless for:
  - Compute resources are allocated dynamically as needed by the platform.
  - Consumption-based pricing: You are charged only for the compute resources used to execute your code.
  - The compute resources scale on demand based on traffic, without the developer needing to do any configuration.

Serverless Architecture Best Practices

- Enforce HTTPS: CDN, static website hosting, API management
- Lock down function apps
- Protect application secrets (KeyVault)

Sign up for GitHub

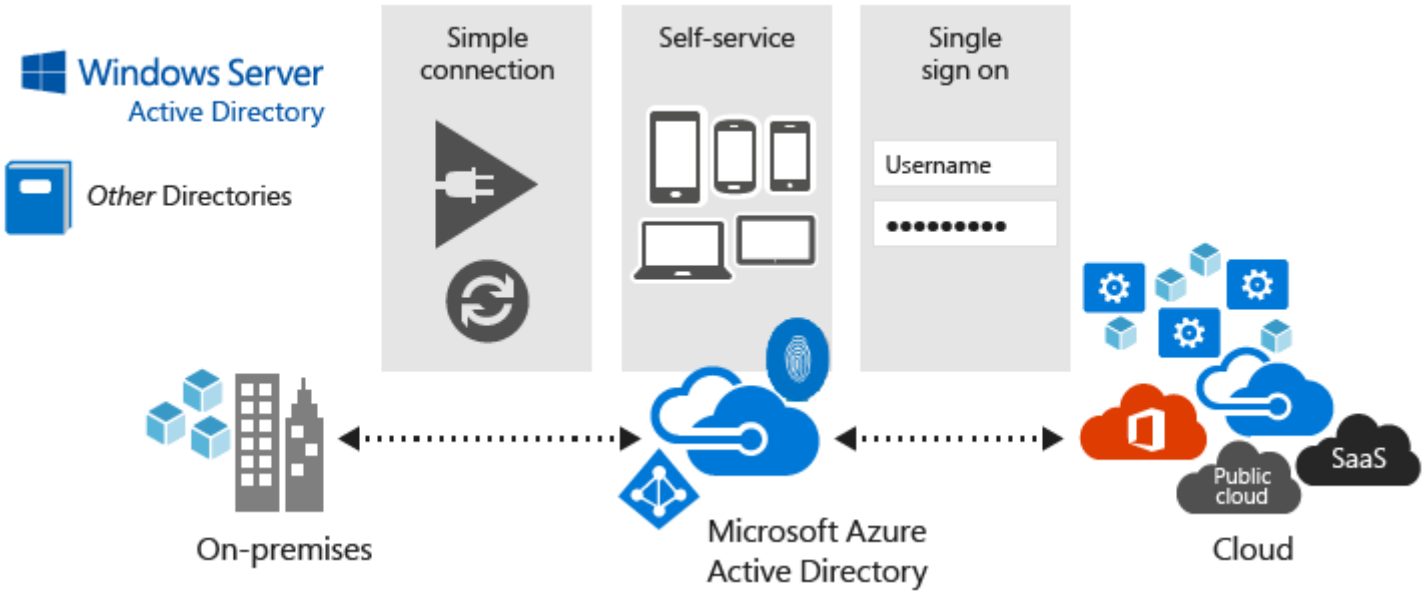
Send me your GitHub username

mike@cloudskills.io

Identity and Security

Azure Active Directory

- multi-tenant cloud-based directory and identity management:
  - **Provides single sign-on access to cloud applications and resources**
  - **Facilitates developing apps with a global scope**
  - **Offers a full suite of identity management capabilities:**
    - **Self-service password and group management**
    - **Privileged account management**
    - **Role-based access control**
    - **App usage monitoring**
    - **Security monitoring**
    - **Device Registration**
    - **Alerting**
    - **MFA**



Azure Active Directory Editions

- **Free offers:**
  - **user/group management, single sign-on, self-service password change, basic reporting**
- **Basic offers (in addition to the Free edition features):**
  - **group-based access management, self-service password reset, Azure Active Directory Application Proxy, 99.9% availability SLA**
- **Premium P1 offers (in addition to the Basic edition features):**
  - **access to hybrid application access, self-service identity and access management, security in the cloud**
- **Premium P2 offers (in addition to the Premium P1 features):**
  - **advanced identity protection and privileged identity management**

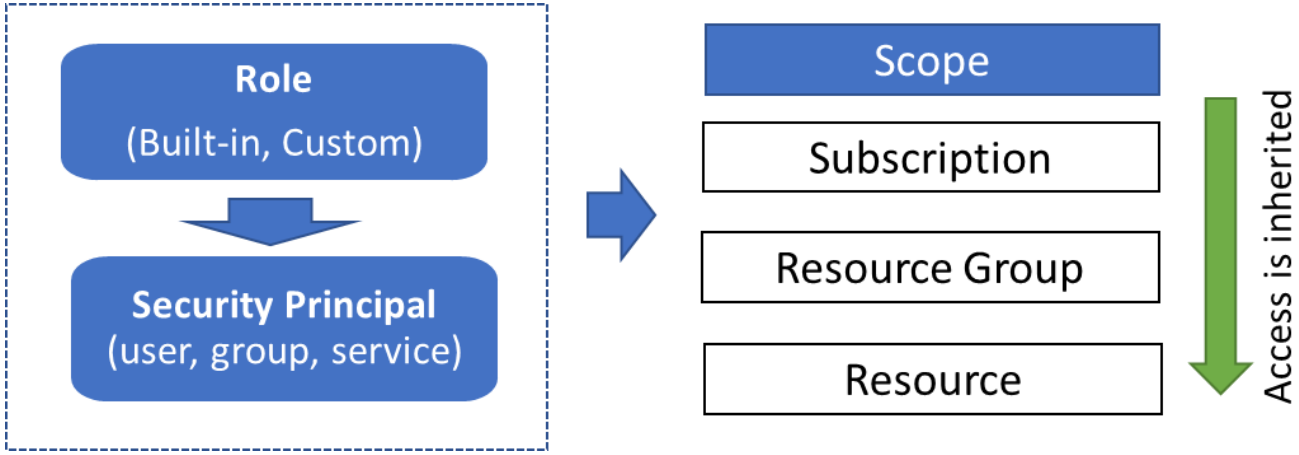
Choosing Between Azure AD and Azure AD DS

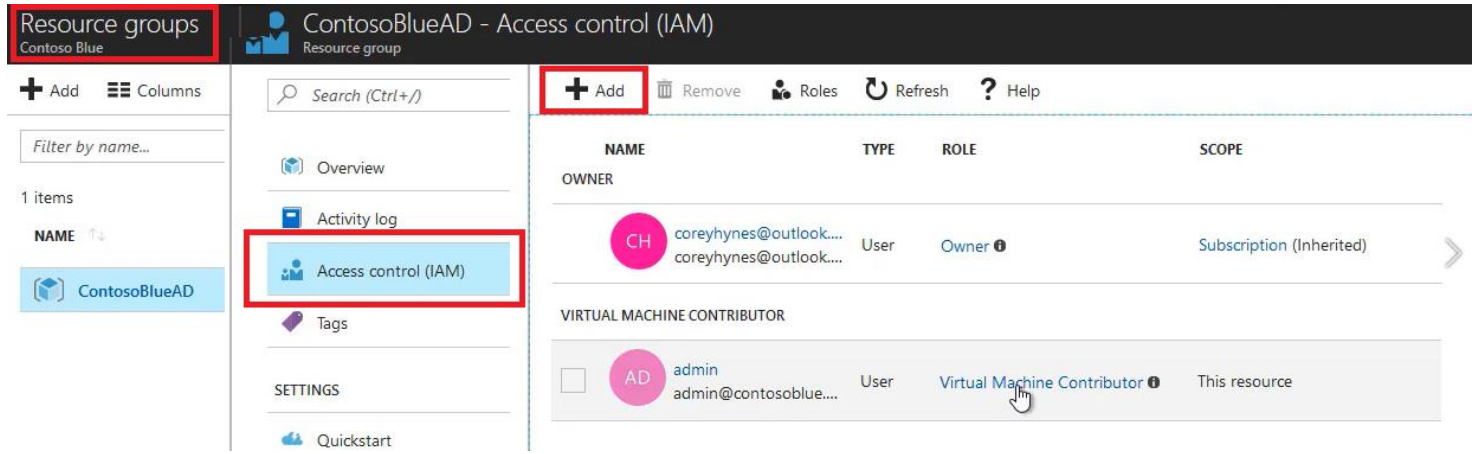
- Azure AD DS is a managed AD DS deployment in an Azure VNet:
  - **Integrates with Azure AD**
  - **Delivers core AD DS features:**
    - **Domain join**
    - **Kerberos and NTLM**
    - **LDAP**
    - **Group Policy**
  - **Intended for:**
    - **Azure VMs that rely on AD DS**
    - **Cloud-based environments**

Aspect	Course Content	Azure AD Domain Services
Device controlled by	Azure AD	Azure AD Domain Services managed domain
Representation in the directory	Device objects in the Azure AD directory.	Computer objects in the AAD-DS managed domain.
Authentication	OAuth/OpenID Connect based protocols	Kerberos, NTLM protocols
Management	Mobile Device Management (MDM) software like Intune	Group Policy
Networking	Works over the internet	Requires machines to be on the same virtual network as the managed domain.
Great for ...	End-user mobile or desktop devices	Server virtual machines deployed in Azure

Role-Based Access Control

- Facilitates granular access to Azure resources:
- Consists of:
  - **Role definition**
  - **Role assignment**
  - **Scope of assignment**
- Can be managed by using:
  - **The Azure portal**
  - **Azure PowerShell**
  - **Azure CLI**
  - **ARM templates**





Built-in Roles

- A role represents a set of permissions to carry out specific actions
- Azure AD provides many built-in roles:
  - **Built-in, not resource specific, including:**
    - **Owner: full access to all resources including the right to delegate access to others.**
    - **Contributor: creating and managing all resources but without the ability to delegate access to others.**
    - **Reader: viewing all resources (except for secrets).**
  - **Built-in, resource specific (e.g. Virtual Machine Contributor)**
- A role is described by a JSON-formatted role definition:
  - **Name, Id, Actions, Not Actions, AssignableScopes**
  - **Can be retrieved by Get-AzureRmRoleDefinition**

```
Get-AzureRmRoleDefinition -Name Owner
Name             : Owner
Id               : 8e3af657-a8ff-443c-a75c-2fe8c4bcb635
IsCustom         : False
Description      : Lets you manage everything, including
                   access to resources.
Actions          : {*}
NotActions       : {}
AssignableScopes : {/}
```

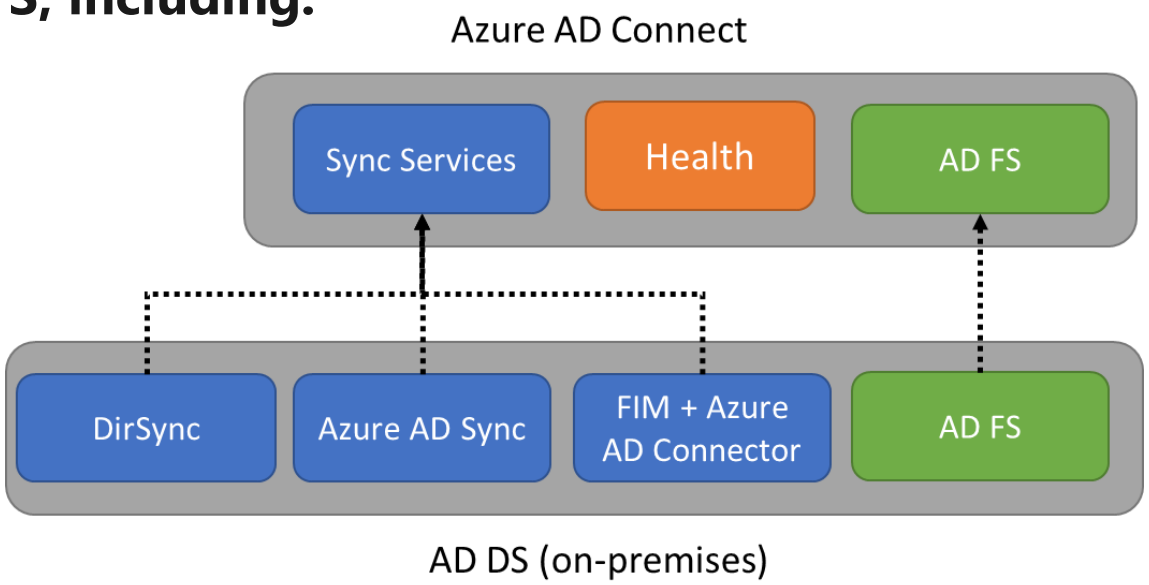
Role Definitions

- Actions and NotActions:
  - **Include or exclude actions associated with the role**
- AssignableScopes:
  - **/subscriptions/[subscription id]**
  - **/subscriptions/[subscription id]/resourceGroups/[resource group name]**
  - **/subscriptions/[subscription id]/resourceGroups/[resource group name]/[resource]**

Built-in Role	Action	NotActions
Owner (allow all actions)	*	
Contributor (allow all actions except writing or deleting role assignment)	*	Microsoft.Authorization/*/Delete, Microsoft.Authorization/*/Write, Microsoft.Authorization/elevateAccess/Action
Reader (allow all read actions)	*/read	

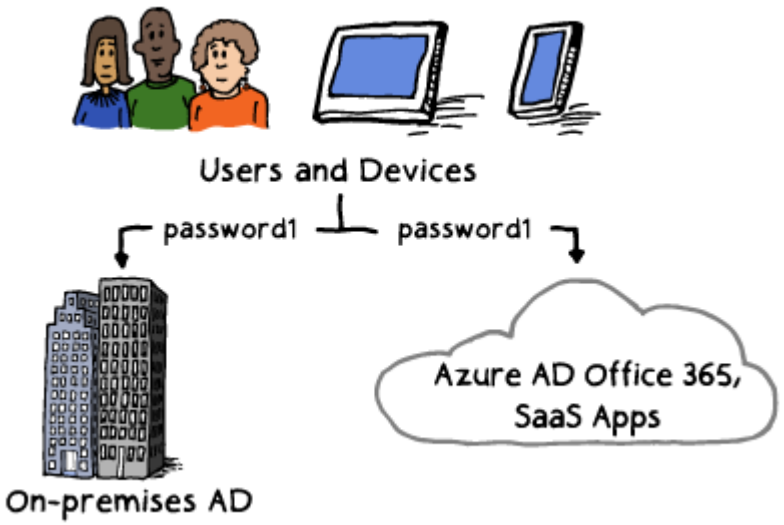
Azure AD Connect

- 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 available from the Azure portal.**
  - **Federation: simplifies configuration of AD FS, including:**
    - **enforcement of AD sign-in policies**
    - **smart card or 3rd party MFA**



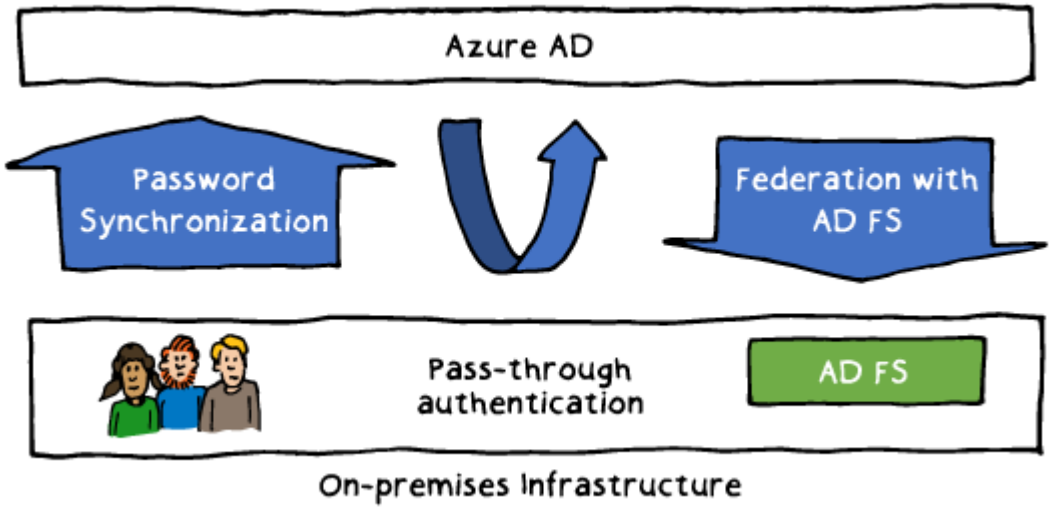
Password Synchronization

- Supported by Azure AD Connect:
  - **Synchronizes user passwords from AD DS to Azure AD**
  - **Allows users to use their AD credentials in order to access:**
    - **Azure resources**
    - **Office 365**
    - **Microsoft Intune**
    - **Dynamics 365**
    - **Azure AD DS**
  - **Improves user productivity**
  - **Reduces helpdesk costs**



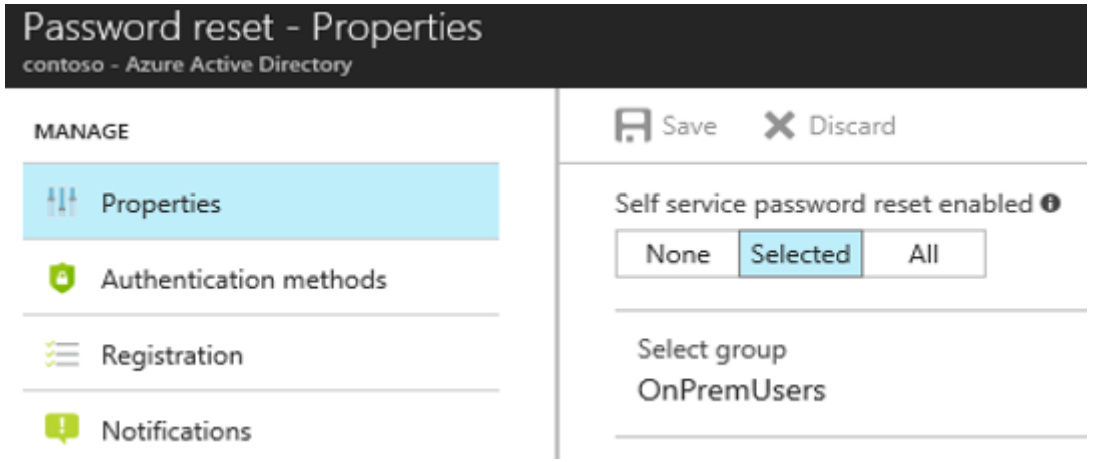
Sign-On Methods

- Available when using Azure AD Connect:
  - **Password Synchronization: synchronizes AD DS user password hashes**
  - **Federation with AD FS: uses federation to redirect authentication requests to AD DS**
  - **Pass-through authentication: redirects authentication requests to AD DS without dependency on a federation service**



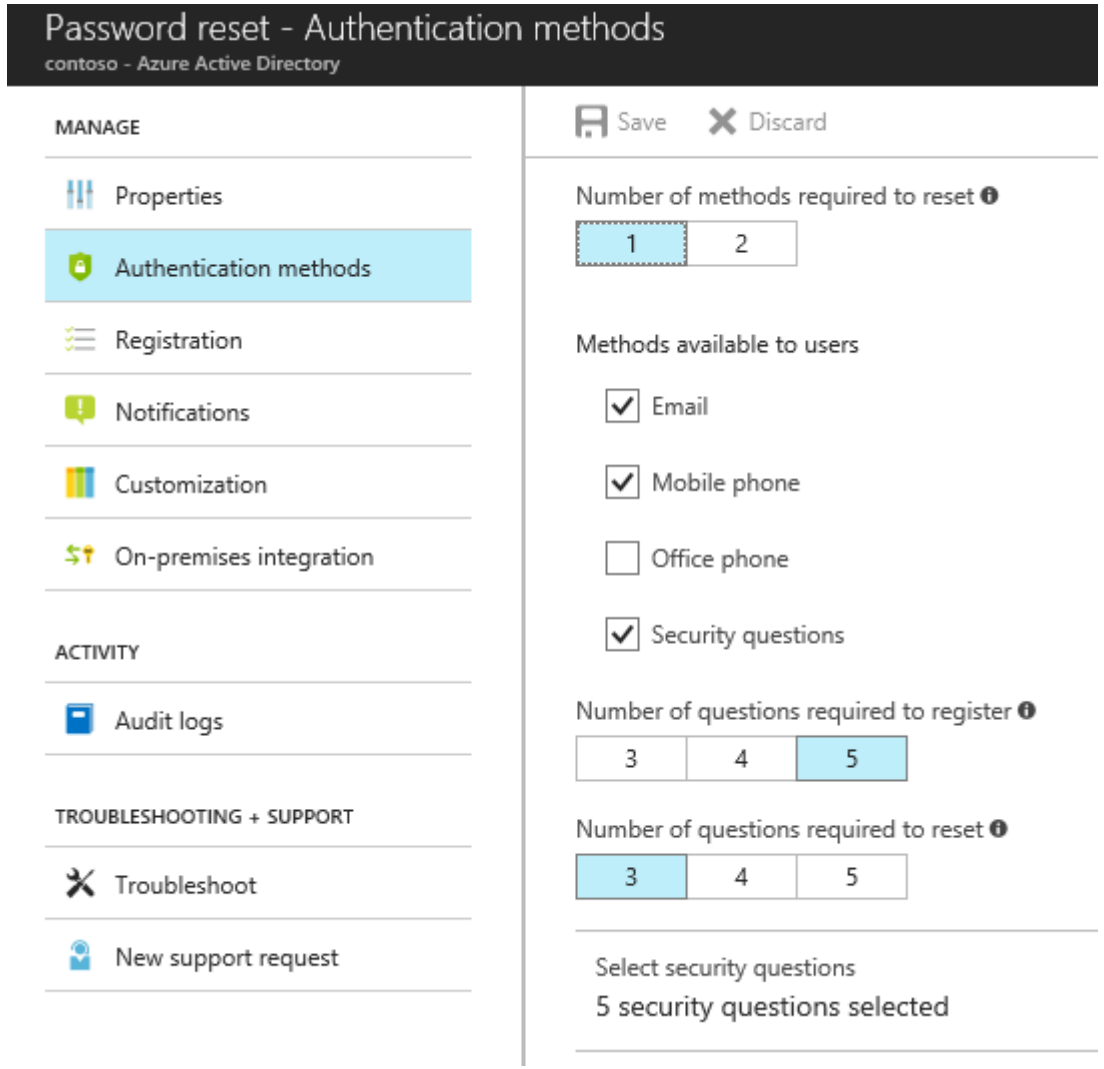
Configuring Self-Service Password Reset

- Available directly from the Azure portal
- Requires designating users in scope:
  - **None**
  - **Selected (limited to specific Azure AD users or groups)**
  - **All**



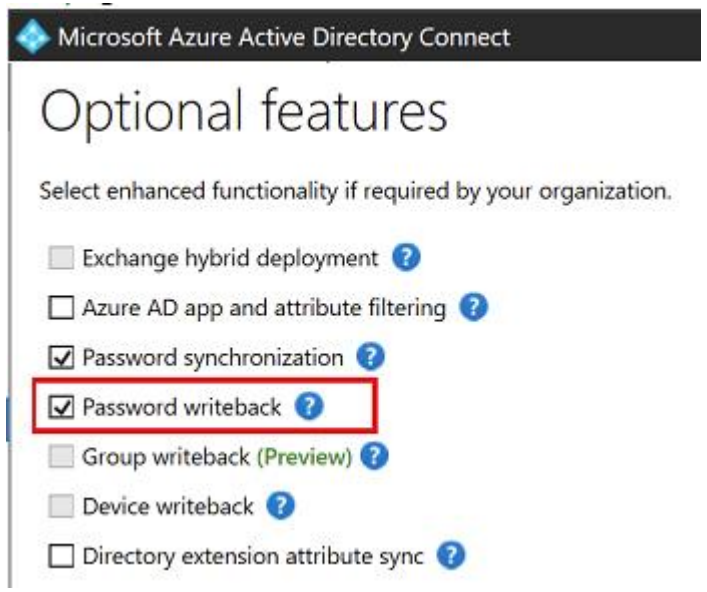
Authentication Methods for Password Reset

- Include (at least one is required):
  - **Email notification**
  - **Text or code sent to the user's mobile device**
  - **Office phone**
  - **A set of security questions**



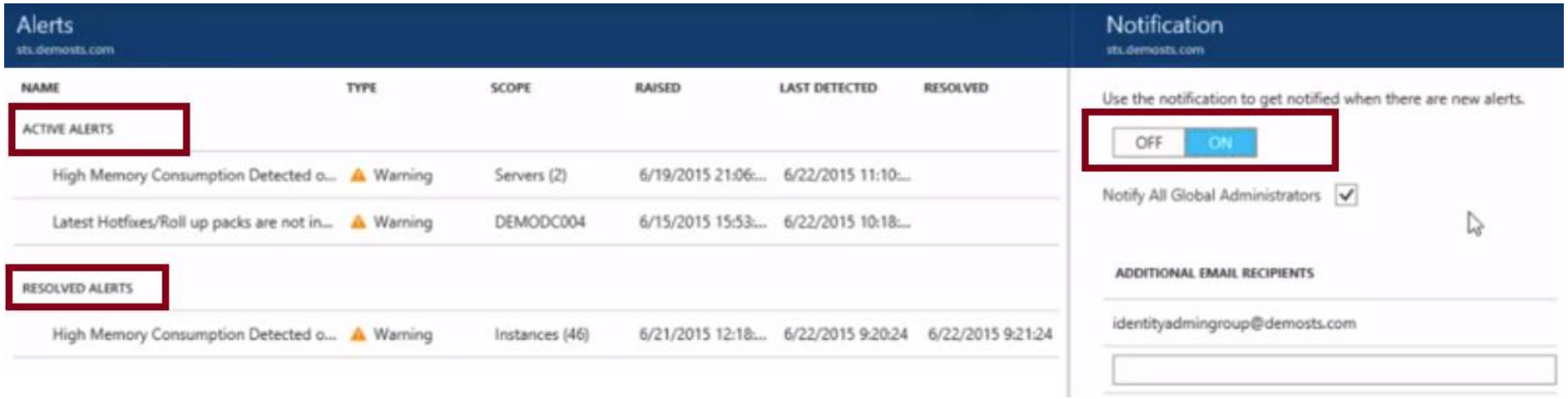
Password Writeback

- Writes Azure AD users' password changes/resets to AD DS
- Eliminates the need for on-premises SSPR solutions
- Requires Azure AD Premium P1 or P2 edition
- Is enabled by using Azure AD Connect:
  - **Start Azure AD Connect Configuration Wizard**
  - **Select Customize synchronization options**
  - **Enable the checkbox on the Optional features page**



Azure AD Connect Health

- Provides monitoring of AD DS and Azure AD integration:
  - **Azure AD Connect and its synchronization engine**
  - **AD DS domain controllers**
  - **AD FS servers**



Device Management

- Azure AD supports device integration by using:
  - **Registering a device in Azure AD:**
    - **Provides the device with an Azure AD identity (a device object) that facilitates device authentication.**
    - **Introduces device object-specific attributes in Azure AD. This facilitates using Azure AD and mobile device management (MDM) solution such as Microsoft Intune to create conditional access rules that allow or block access from devices based on their security and compliance status.**
    - **It supports disabling or enabling the Azure AD identity representing the device.**
  - **Joining a device to Azure AD:**
    - **Constitutes an extension to registering a device**
    - **Provides the benefits of registering a device and, in addition, changes the local state of a device.**
    - **Allows Azure AD users to sign-in to devices using work or school accounts instead of personal accounts.**

Azure Joined Devices

- Hybrid Azure AD joined devices are joined to:
  - **AD**
  - **Azure AD**
- Hybrid Azure AD join facilitates:
  - **Centralized management of all work-owned devices**
  - **Support for user sign-ins with Active Directory accounts**

	Registered Devices	Azure AD Joined Devices	Hybrid AD Joined Devices
Device Type	Personal	Organization owned	Organization owned
Registration	Manual	Manual	Automatic
Operating System	Windows 10	Windows 10	Windows 7, 8, and 10

Career Strategy and Tactics

Career Strategy and Tactics

- Clearly Define Your Target
  - What are you after? Be practical but aim high
  - Most people have weak or non-existent goals
- Build Your Platform
  - LinkedIn, Twitter, and GitHub at a minimum
- Thought Leadership = Leverage
  - This is not about fame…it’s about avoiding the ”commodity" trap
  - How will you share ideas? Text, Audio, or Video?
  - Start with one channel

Career Strategy and Tactics

- Work Ethic is Your Secret Weapon
  - Do what most other people aren’t willing to do
  - Realize there is no end to any of this
- Build Awareness of Your Inner Critic
  - Become hyper aware of your fears, insecurities, judgements, finger pointing and lack ownership
  - Call BS on your inner critic and stay committed to your mission
- Intent
  - If your mission serves a cause outside yourself it will help pull you through the hard times
  - Contribution is the ultimate career (and life) hack

Platform Security

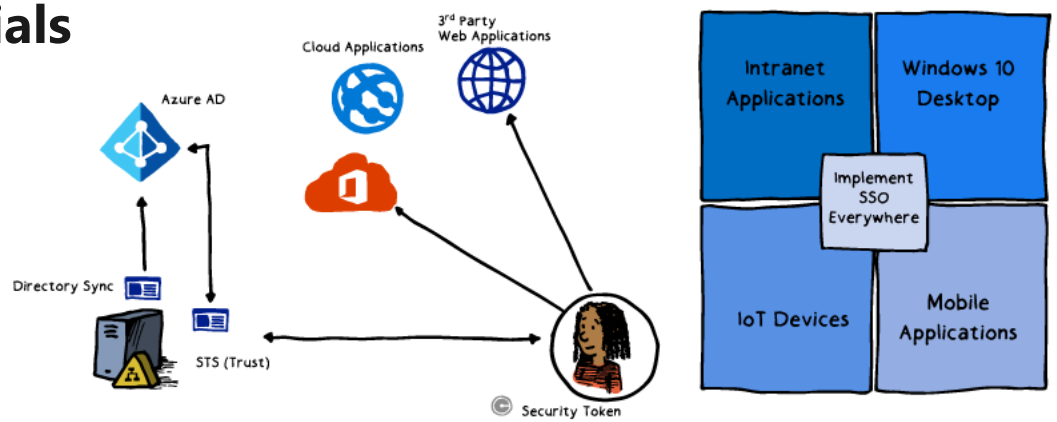
- Azure offers a “shared responsibility” security model:
  - **Microsoft Azure is built with end-to-end security in mind. Microsoft delivers a secure foundation and tooling to control your environment.**
  - **Customers own responsibility of their subscription governance, data, identities, and protection. The level of responsibility varies between IaaS and PaaS-based solutions.**
- Azure is architected for multi-tenancy, with separation based on:
  - **The Azure Fabric Controller (FC) functioning as the kernel of the Azure platform**
  - **The host OS running a hardened installation of Windows Server**
  - **The hypervisor implemented as the Hyper-V server role**
  - **The guest VM OS, which can be Windows Server or an approved Linux distribution**
  - **Storage isolation: hypervisor maps storage blocks to separate storage accounts.**
  - **Network isolation: hypervisor switch blocks inter-tenant communication**

Securing the Azure Platform

- Azure Key Vault is a managed FIPS 140-2 Level 2 HSM-based service:
  - **Safeguards cryptographic keys, secrets, and certificates**
  - **Facilitates RBAC and policy-based delegated administration and usage, including:**
    - **Creating and importing keys and secrets.**
    - **Revoking and deleting keys and secrets.**
    - **Authorizing users or applications to access the key vault.**
    - **Configuring key usage (e.g. for signing or encryption).**
    - **Monitoring key usage.**

Azure AD B2B & B2C

- Azure AD B2B:
  - **Allows granting partner organizations access to local resources and applications**
  - **Allows adding partner organization users to local Azure AD groups**
  - **Supports partner organization user credentials**
  - **Is managed by the host organization:**
    - **Partner lifecycle**
    - **Security policy and compliance**
    - **Branding**



- Azure AD B2C:
  - **Allows granting individual customers access to local resources and applications**
  - **Supports social identities via federation but allows creating new Azure AD accounts**
  - **Requires a separate Azure AD tenant (separately from the host organization's tenant)**
  - **Provides SSO to customer's applications**
  - **Is managed by the host organization with app specific customization**

Azure AD Identity Protection

- Azure AD Identity Protection:
  - **Protects all identities regardless of their privilege level.**
  - **Detects threats based on adaptive machine learning and heuristics.**
  - **Generates reports and alerts to accelerate response and remediation.**
- Privileged Identity Management:
  - **Identifies users with administrative roles in Azure AD.**
  - **Identifies users with privileged roles to manage Azure resources (Preview)**
  - **Enables on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune, and to Azure resources (Preview).**
  - **Tracks history of privilege escalation, including changes to Azure resources (Preview).**
  - **Generates alerts in response to changes in administrator assignments.**
  - **Implements approval-based elevation to Azure AD privileged admin roles (Preview).**
  - **Generates reports identifying members of privileged roles.**

Multi-factor authentication

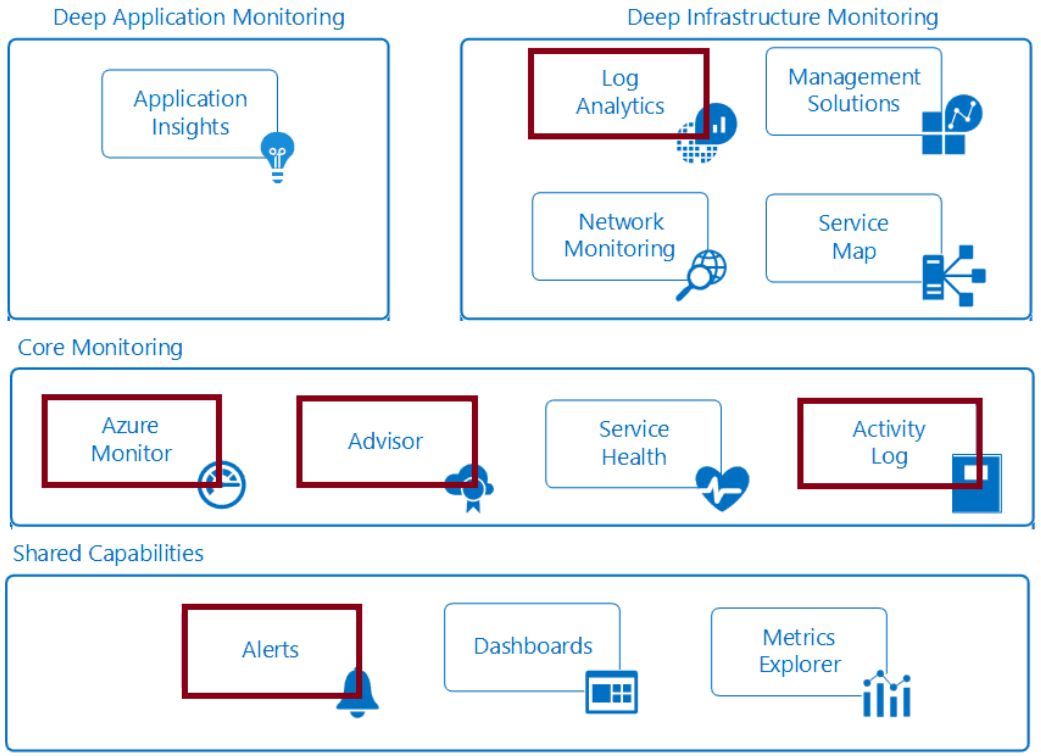
- Enforces two or more factors when authenticating users:
  - **Knowledge: something that only the user knows (security questions, password, or PIN).**
  - **Possession: something that only the user has (corporate badge, mobile device, or security token).**
  - **Inherence: something that only the user is (fingerprint, face, voice, or iris).**

Multi-factor authentication with Azure AD

- Can be enabled by:
  - **Enabling users for MFA to trigger two-step verification each time they sign in:**
    - **Supports exceptions such as sign-ins from a trusted IP addresses or using the remembered devices feature.**
  - **Setting up a conditional access policy requiring two-step verification:**
    - **Relies on the Azure AD Identity Protection risk policy requiring two-step verification based on sign-in risk.**
- Offers several authentication methods:
  - **Call to phone**
  - **Text message to phone**
  - **Notification through mobile app**
  - **Verification code from mobile app (Microsoft Authenticator app)**
- Can be customized by using the Multi-Factor Authentication SDK:
  - **Allows building MFA into the sign-in or transaction processes of applications**
  - **Supports C#, Visual Basic (.NET), Java, Perl, PHP, and Ruby**

Introducing Azure Monitoring Services

- Monitoring: act of collecting and analyzing data to determine performance, health, and availability of your workloads.
- Azure offers a comprehensive monitoring solution that provides:
  - **Core Monitoring**
  - **Deep Infrastructure Monitoring**
  - **Deep Application Monitoring**
  - **Shared Monitoring Capabilities**



Azure Monitor: Key Capabilities

- Azure core monitoring consists of collection of:
  - **Metrics:**
    - **Represent performance statistics of Azure resources**
    - **Include operating system metrics of Azure VMs**
    - **Are available in 1 minute intervals (suitable for critical alerts and notifications)**
  - **Activity logs**
  - **Diagnostic logs**

Monitor & Visualize Metrics

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

Explore Metrics

Query & Analyze Logs

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

Search Logs

Setup Alert & Actions

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

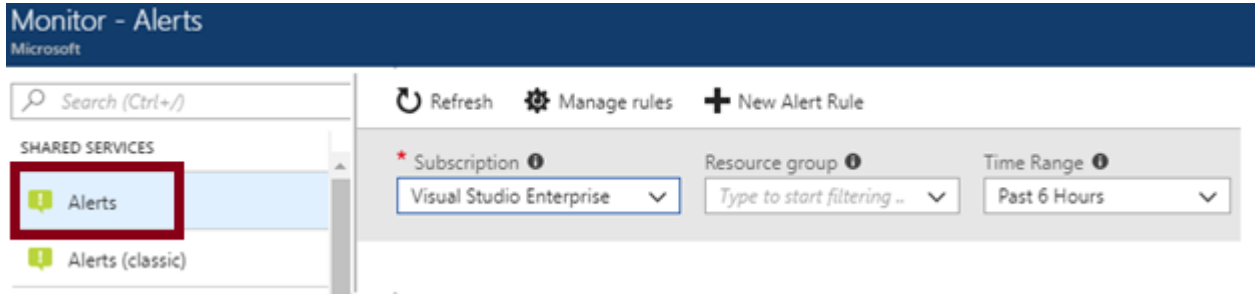
Create Alert

Azure Advisor

- Personalized cloud service for optimizing Azure deployments:
  - **Analyzes resource configuration and usage telemetry**
  - **Offers recommendations grouped in four categories:**
    - **High availability: To ensure and improve the continuity of your business-critical applications.**
    - **Security: To detect threats and vulnerabilities that might lead to security breaches.**
    - **Performance: To improve the speed of your applications.**
    - **Cost: To optimize and reduce your overall Azure spending.**

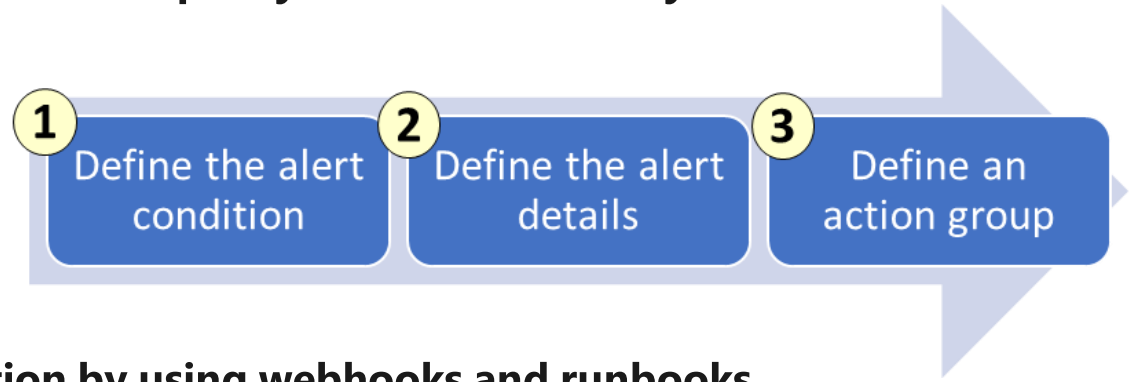
Azure Monitor Alerts

- Azure Monitor supports alerts, including a range of benefits:
  - **Improved notification system through action groups**
  - **Separation of fired alerts and alert rules**
  - **A unified authoring experience**
  - **Enhanced workflow**
  - **Access to Log Analytics alerts directly from the Azure portal**



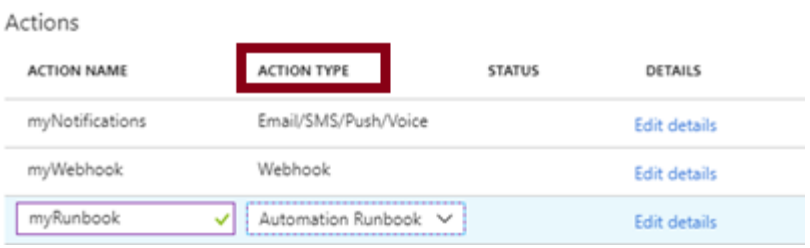
Alert Rules

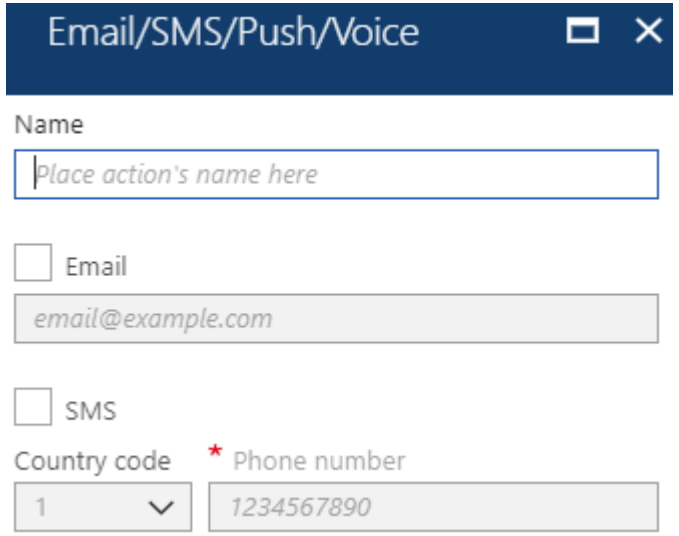
- Creating an alert is a three-step task:
  - **1. Define the alert condition:**
    - **Target selection: e.g. an Azure Storage account.**
    - **Alert criteria: e.g. Used Capacity.**
    - **Alert logic: e.g. over a six-hour period whenever the Used Capacity is over 1000000 bytes.**
  - **2. Define alert details:**
    - **Alert rule name**
    - **Alert rule description**
    - **Alert severity (between 0 and 4).**
  - **3. Define an action group:**
    - **notify via email and text messages, or trigger an action by using webhooks and runbooks**



Action Groups

- Action groups facilitate configuring actions in response to an alert:
  - **Email/SMS/Push/Voice**
  - **Logic App**
  - **Webhook**
  - **Automation Runbook**
  - **IT Service Management**





Signal Types and Metrics

- Signals are emitted by target resources and include:
  - **Metrics**
  - **Activity log**
  - **Application Insights**
  - **Logs**
- The latest metrics alerts offer:
  - **Improved latency**
  - **Support for multi-dimensional metrics**
  - **More control over metrics conditions**
  - **Combined monitoring of multiple metrics**
  - **Metrics from Logs (limited public preview)**

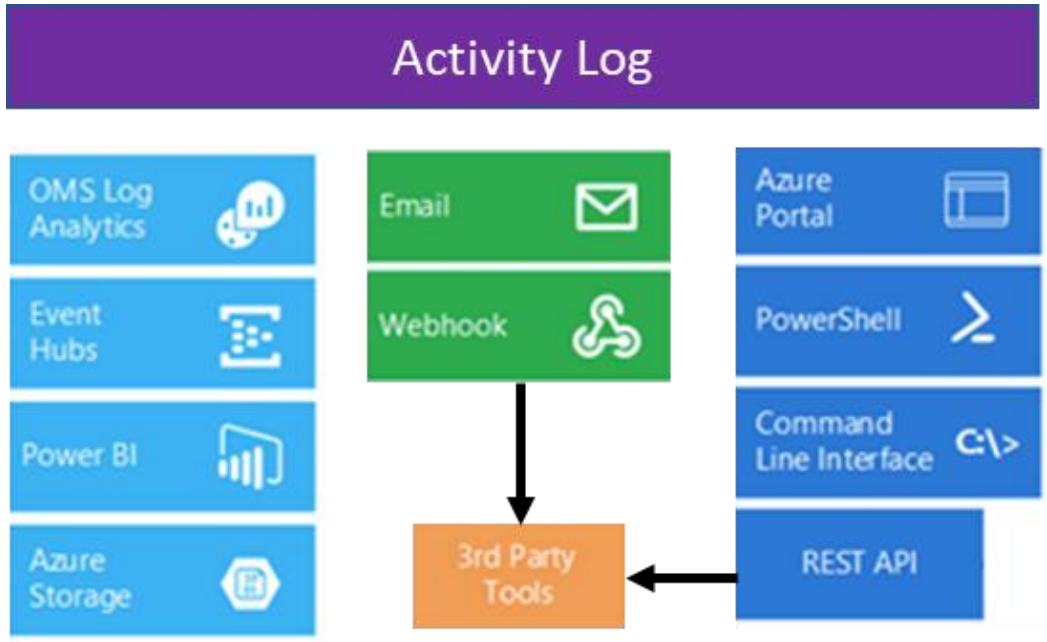
Configure signal logic

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

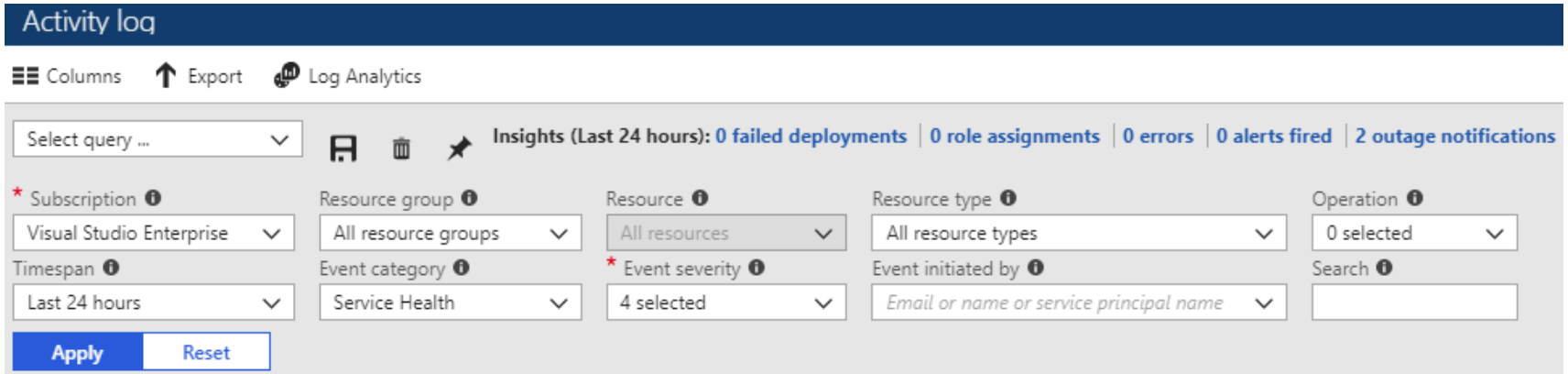
Overview of Activity Log

- A subscription-level log that captures:
  - **Azure Resource Manager operational data (control plane)**
  - **Service Health events**
- Includes audit trail of all write/change operations:
  - **Helps determine "what, who, and when"**
  - **Provides the status of each operation**
- Its content can be:
  - **Streamed to Event Hub.**
  - **Analyzed with Power BI.**
  - **Viewed in the Azure portal.**
  - **Forwarded to Log Analytics.**
  - **Archived in an Azure Storage account.**
  - **Processed with PowerShell, CLI, and REST API.**



Query the Activity Log

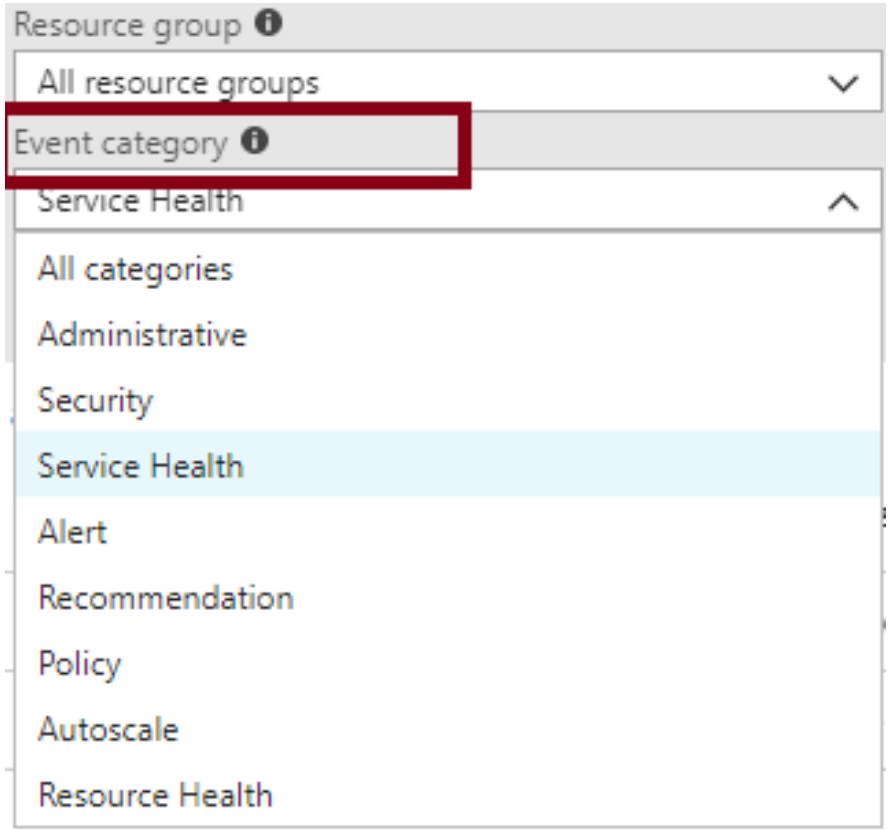
- Available directly from the Azure portal, with filtering based on:
  - **Subscription**
  - **Resource group**
  - **Resource (name)**
  - **Resource type**
  - **Operation (type)**
  - **Timespan**
  - **Event category**
  - **Event severity**
  - **Event initiated by**



- Filter selection can be saved
- Queries can be pinned to the Azure portal dashboard

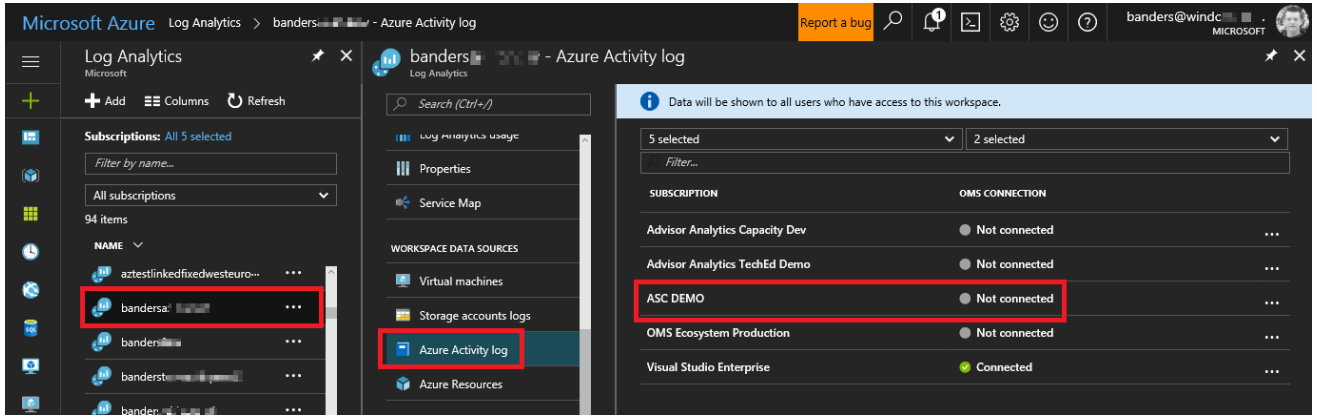
Event Categories

- Administrative
- Security
- Service Health
- Alert
- Recommendation
- Policy
- Autoscale
- Resource Health



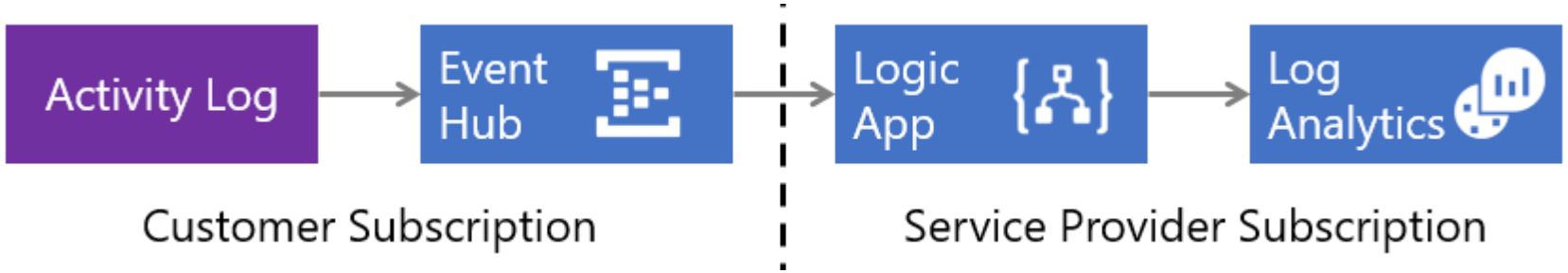
Activity Log and Log Analytics

- Activity log can be added to Azure Log Analytics workspace:
  - **Can be in the same or a different subscription (if it has the same Azure AD tenant)**
  - **Provides the ability to:**
    - **Correlate user activities, auto-scale operations, authorization changes, and service health to other logs or metrics from your environment.**
    - **Correlate activity logs with other Azure services and application data.**
    - **Analyze and search activity logs from multiple Azure subscriptions.**
    - **Keep activity logs for longer than the default of 90 days.**
    - **View operational activities aggregated by status.**
    - **Analyze activity logs with pre-defined views.**
    - **Identify outage or service health issues.**
    - **Report on authorization changes.**
    - **View trends of activities.**



Collect Across Subscriptions

- You can collect Azure Activity Logs into a Log Analytics workspace using the Azure Log Analytics Data Collector connector for Logic Apps
  - **This facilitates using a workspace in a subscription that has a different Azure AD tenant**
  - **It offers a number of advantages, including:**
    - **Low latency, since the Azure Activity Log is streamed into the Event Hub**
    - **Serverless services, with no infrastructure components to deploy**
    - **Minimal custom code**

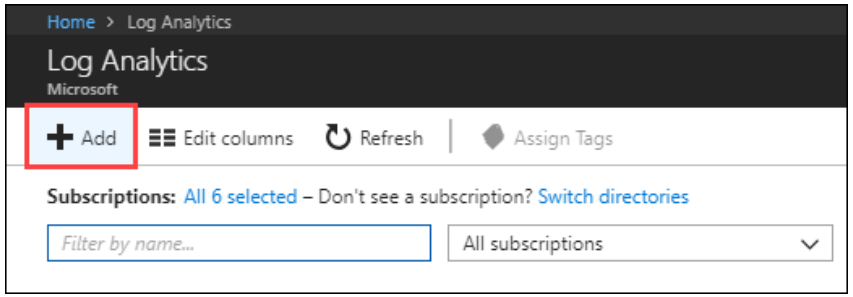


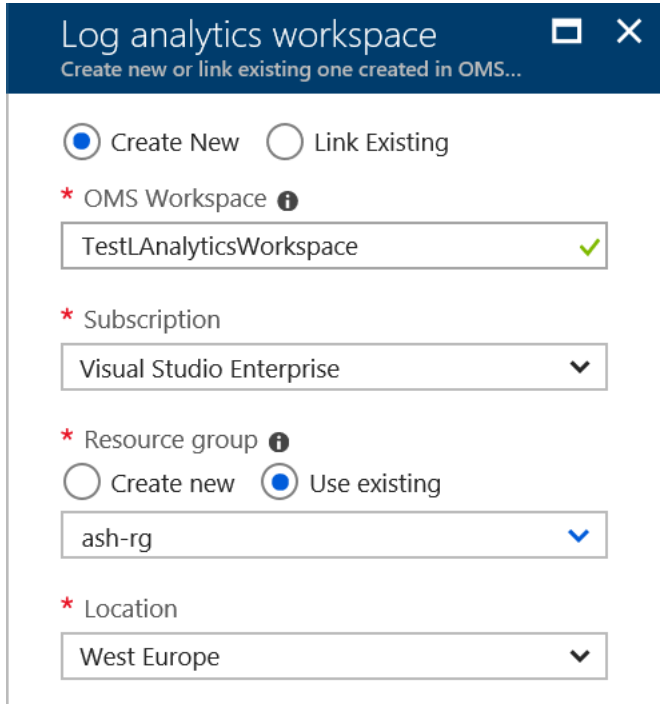
Log Analytics Scenarios

- Scenario 1 – Assessing updates:
  - **Core functionality:**
    - **Identifying system update requirements**
    - **Planning update deployment**
  - **Extra benefits:**
    - **Log Analytics collects customer data globally and provides an average duration of deployment**
- Scenario 2 – Change tracking:
  - **Base functionality:**
    - **Tracking operational changes**
  - **Extra benefits:**
    - **Simplified troubleshooting of operational incidents**
    - **Evidence of security breaches**
    - **Correlation of changes in loosely coupled applications**
    - **Help with detection of unusual behavior, such as installations of unapproved software or unexpected system reboots or shutdowns**

Create a Workspace

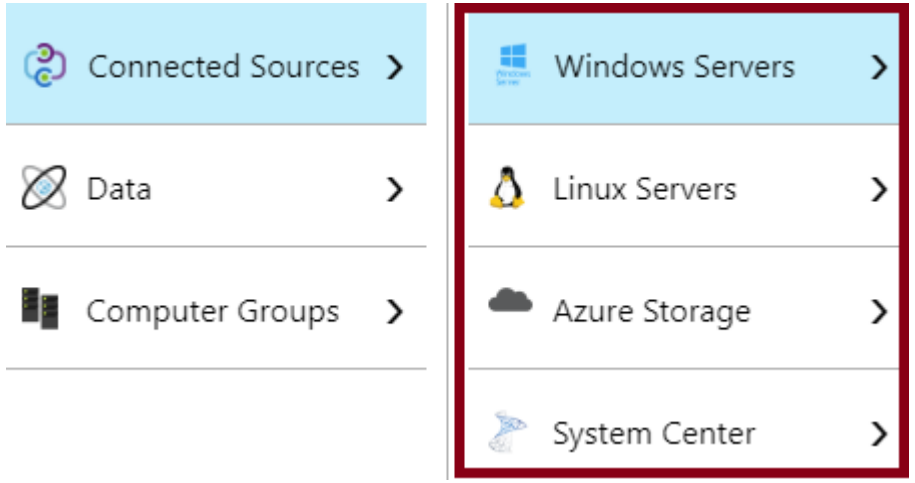
- Start by creating a Log Analytics workspace

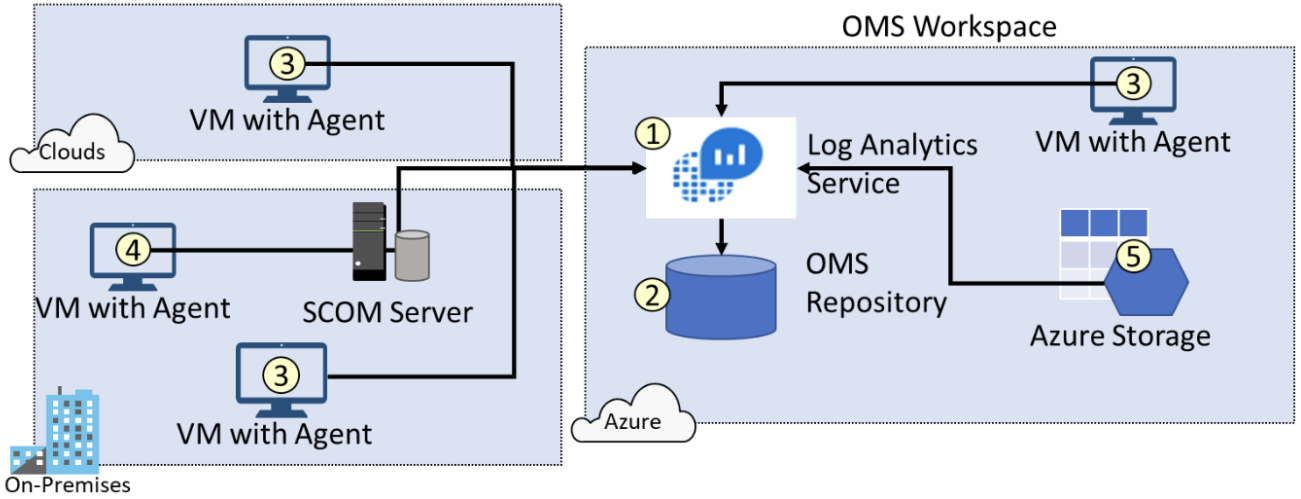




Connected Sources

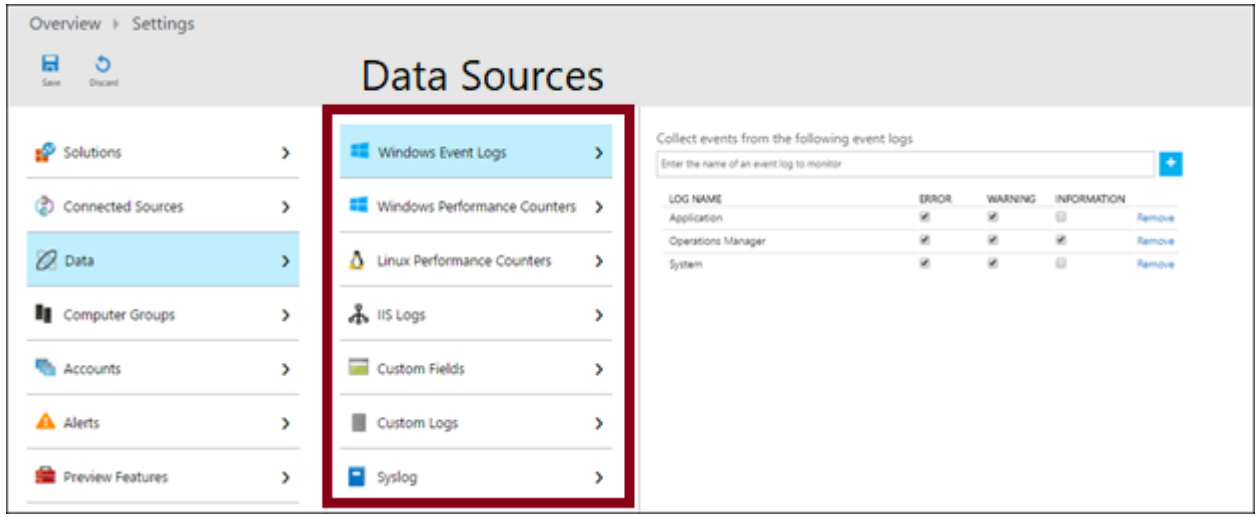
- Include:
  - **Windows and Linux servers:**
    - **Connected directly by installing Log Analytics agent**
    - **Connected as members of a SCOM management group**
  - **Azure Storage**
- Generate data flow:
  - **1. Log Analytics agent collects data**
  - **2. Data is stored in OMS Repository**
  - **3. Agents run on Windows and Linux on-premises and in public clouds**
  - **4. Adding SCOM management group to Log Analytics automatically adds to the workspace all of their computers**
  - **5. Log Analytics collects storage logs**

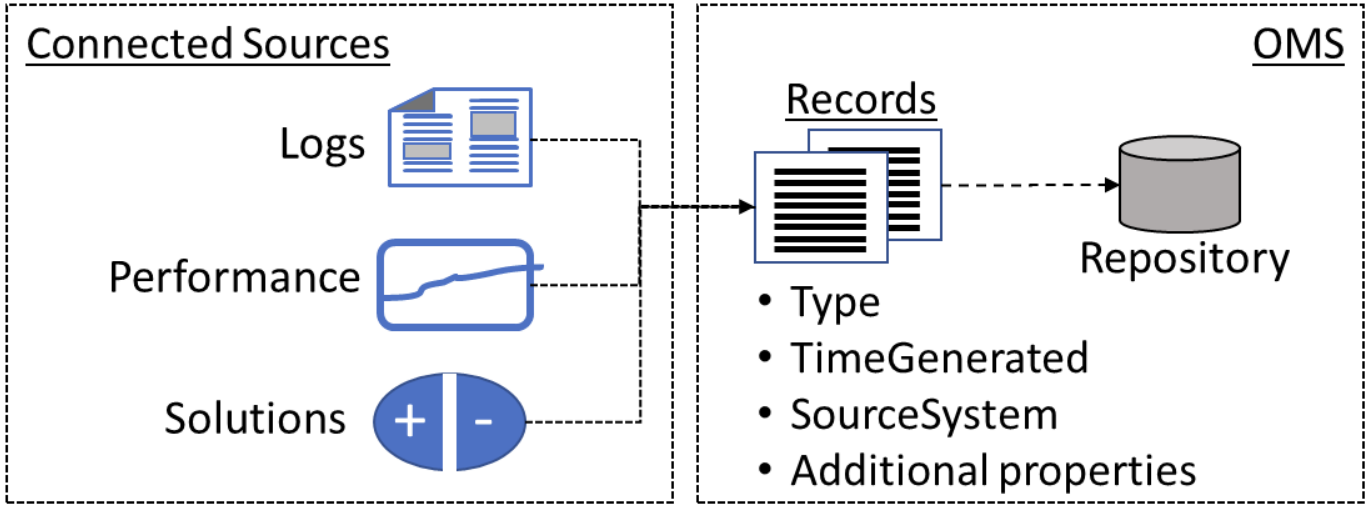




Data Sources

- Types of collected data:
  - **Windows Event Logs**
    - **Error**
    - **Warning**
    - **Informational**
  - **Windows Performance Counters**
  - **Linux Performance Counters**
  - **IIS logs**
  - **Custom fields**
  - **Custom logs**
  - **Syslog**
- You select a data source:
  - **Connected source-specific**
  - **Data collection is automatic**



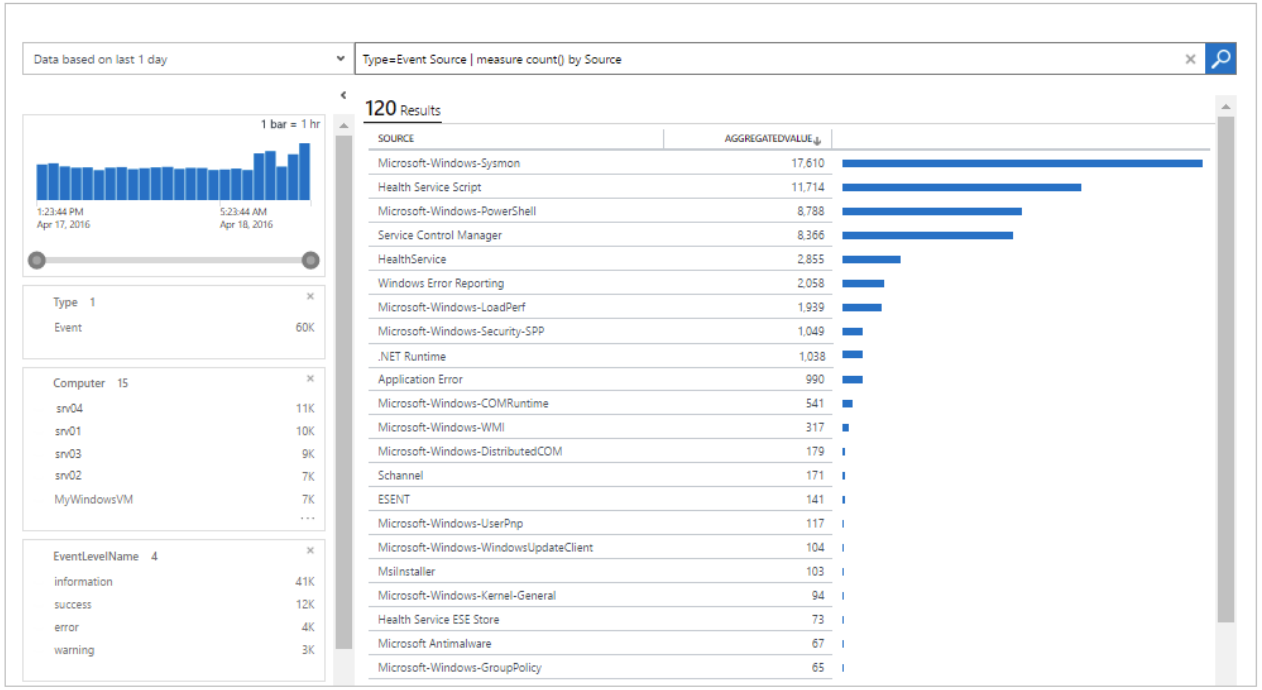


Analyzing Log Analytics Data

- The OMS portal:
  - **Legacy interface**
  - **To be deprecated**
- The Azure portal:
  - **Current interface**
  - **Includes OMS capabilities:**
    - **Log searches**
    - **Dashboards**
    - **Solutions**

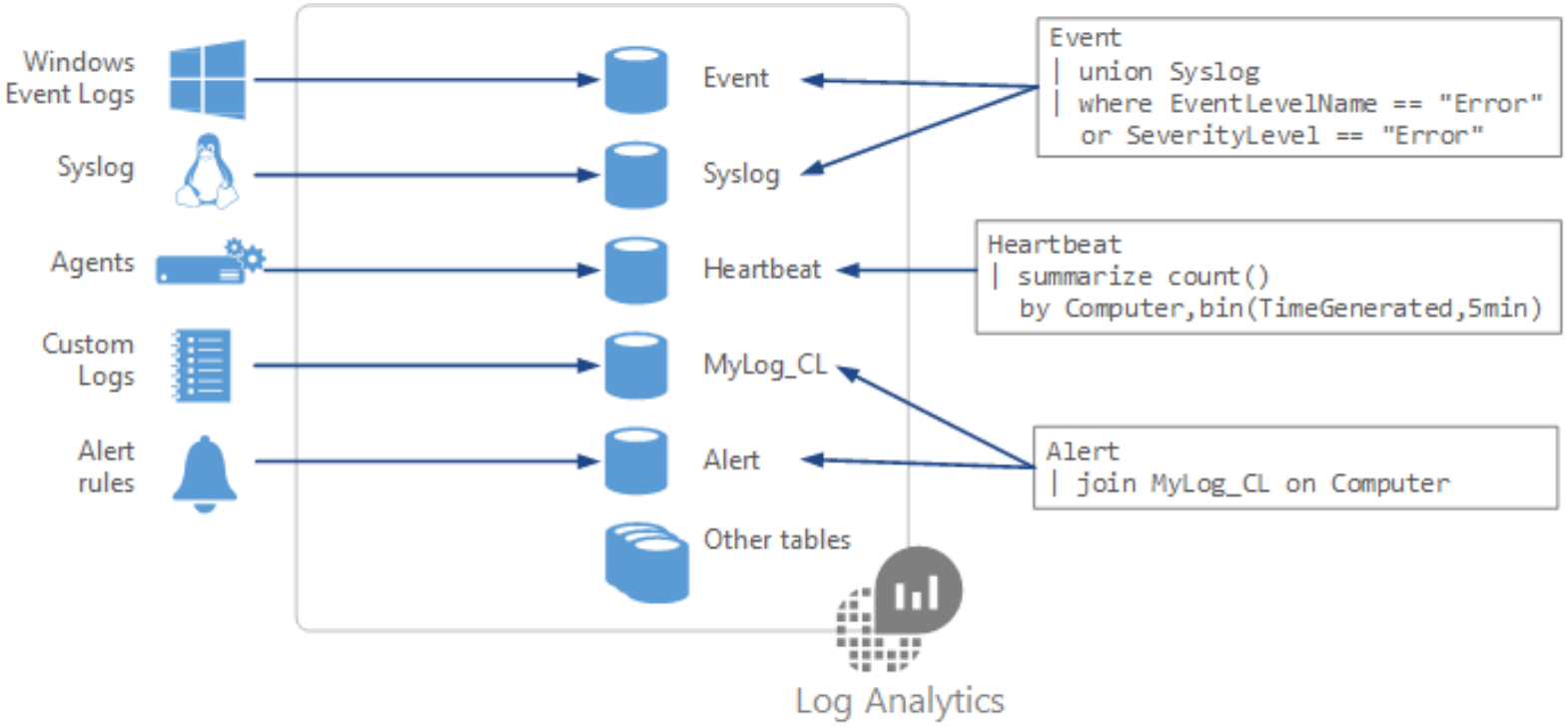
Log Analytics Querying

- Log Analytics queries:
  - **Facilitate data retrieval, aggregation, and analysis**
  - **Can be saved and used to populate dashboards**
  - **Generate data sets for exporting to external tools:**
    - **Power BI**
    - **Excel**
  - **Can be used to generate alerts**
  - **Are available via Log Search API**



Querying Language Syntax

- Each data source and solution stores data in dedicated tables in the Log Analytics workspace.
- The primary query tables are:
  - **Event**
  - **Syslog**
  - **Heartbeat**
  - **Alert**
- Query syntax includes:
  - **A source table**
  - **A series of operators**
  - **Pipe characters**



Scale and auto-scale

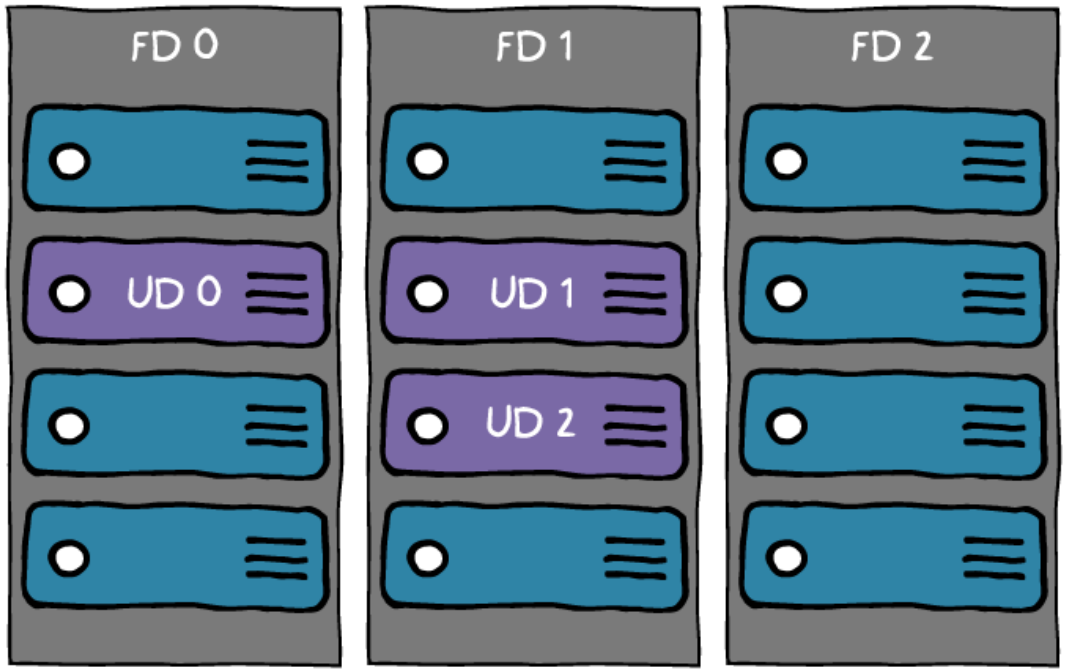
- Cloud offers elastic scaling by using its practically unlimited resources
- Auto-scaling is the ability to monitor workload usage and automatically scale according to changes in usage levels
- Many Azure services support manual and automatic scaling:
  - **infrastructure services such as Azure Virtual Machine Scale Sets**
  - **application services such as Azure App Service**

Azure Availability

- Availability of Azure VMs can be impacted by:
  - **An unexpected downtime**
  - **Planned maintenance events**
  - **Emergency maintenance events**
- To optimize availability of Azure VMs:
  - **Deploy two or more identically configured Azure VMs into the same availability set or different availability zones.**
  - **Use managed disks for Azure VMs deployed into availability sets and availability zones.**
  - **Keep track of Azure Scheduled Events to respond proactively to planned downtime.**
  - **Place each tier of multi-tier applications in a separate availability set or zone.**
  - **Use a load balancer in combination with availability sets and availability zones.**
  - **For individual VMs running critical workloads, use exclusively Premium Storage disks.**

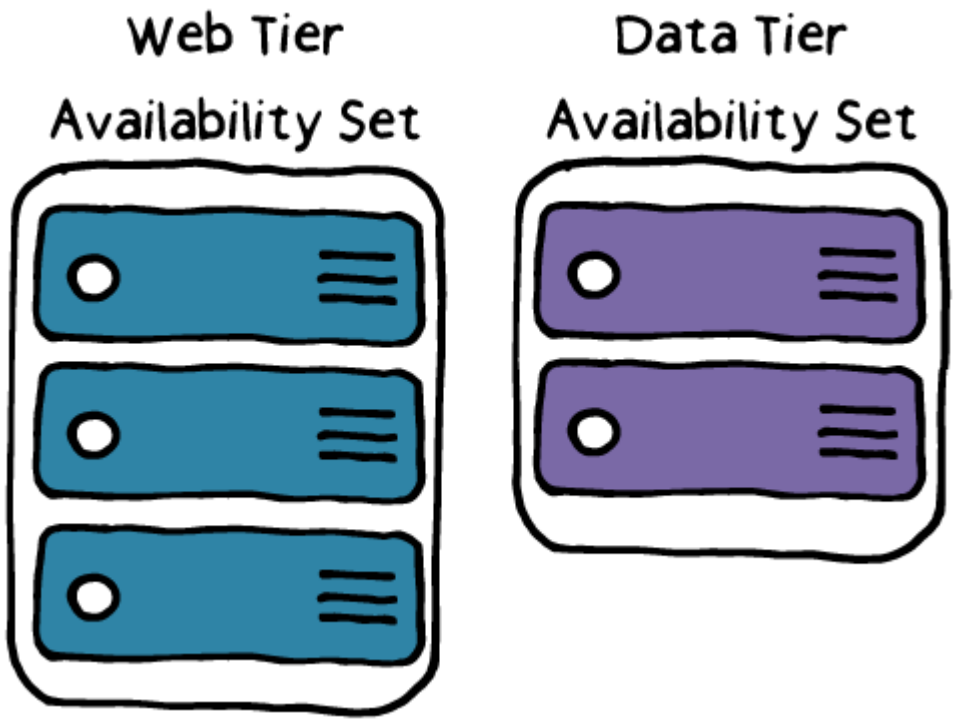
Availability Sets

- Offer 99.95% availability for workloads running on two or more VMs.
- Minimize impact of planned and unplanned downtime.
- Enforce placement of Azure VMs across separate racks in the same datacenter.
- Comprise of:
  - **Fault domains**
  - **Update domains**



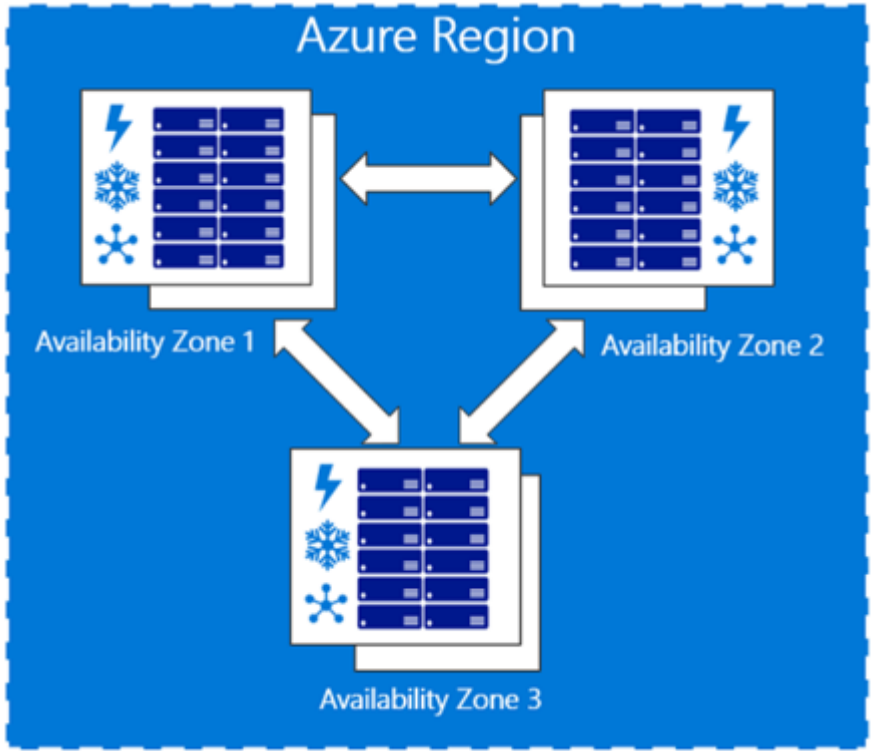
Multiple Availability Sets

- In a multi-tier solution, place each tier in a separate availability set:
  - **The solution remains functional in case of downtime of individual VMs (one per tier)**
  - **For example:**
    - **Web tier availability set**
    - **Data tier availability set**



Availability Zones

- Offer 99.99% availability for workloads running on two or more VMs.
- Minimize impact of planned and unplanned downtime
- Enforce placement of Azure VMs across separate datacenters (zones) in the same Azure region.
- Implicitly comprise of:
  - **Fault domains**
  - **Update domains**

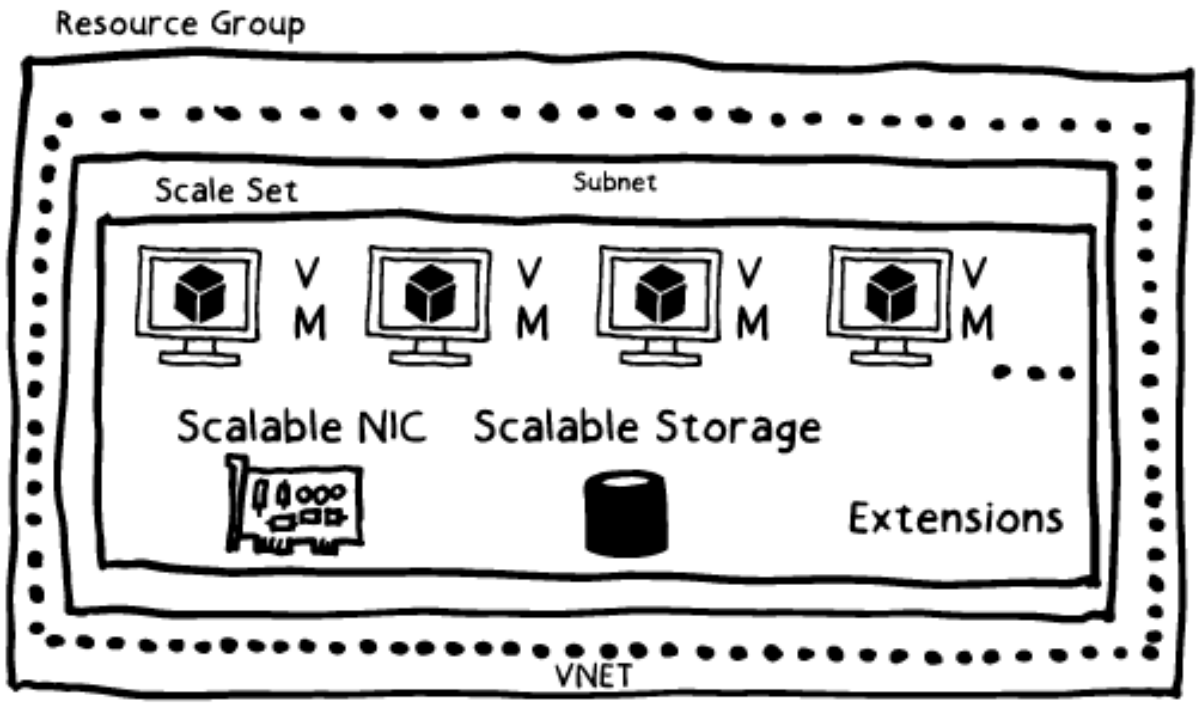


Templated Infrastructure

- Azure VM Scale Sets:
  - **Offer high degree of control of resources**
  - **Auto-scale up to 1,000s of Azure VM instances**
  - **Are optimized for template-based deployments**
  - **Are suitable for hosting big compute and big data workloads**
  - **Automatically provision necessary storage, compute, and network resources**

Virtual Machines Scale Sets (VMSS)

- Deploy into a subnet of a virtual network
- Provide access to individual VMs via NAT
- Scale for up to 1,000 VMs

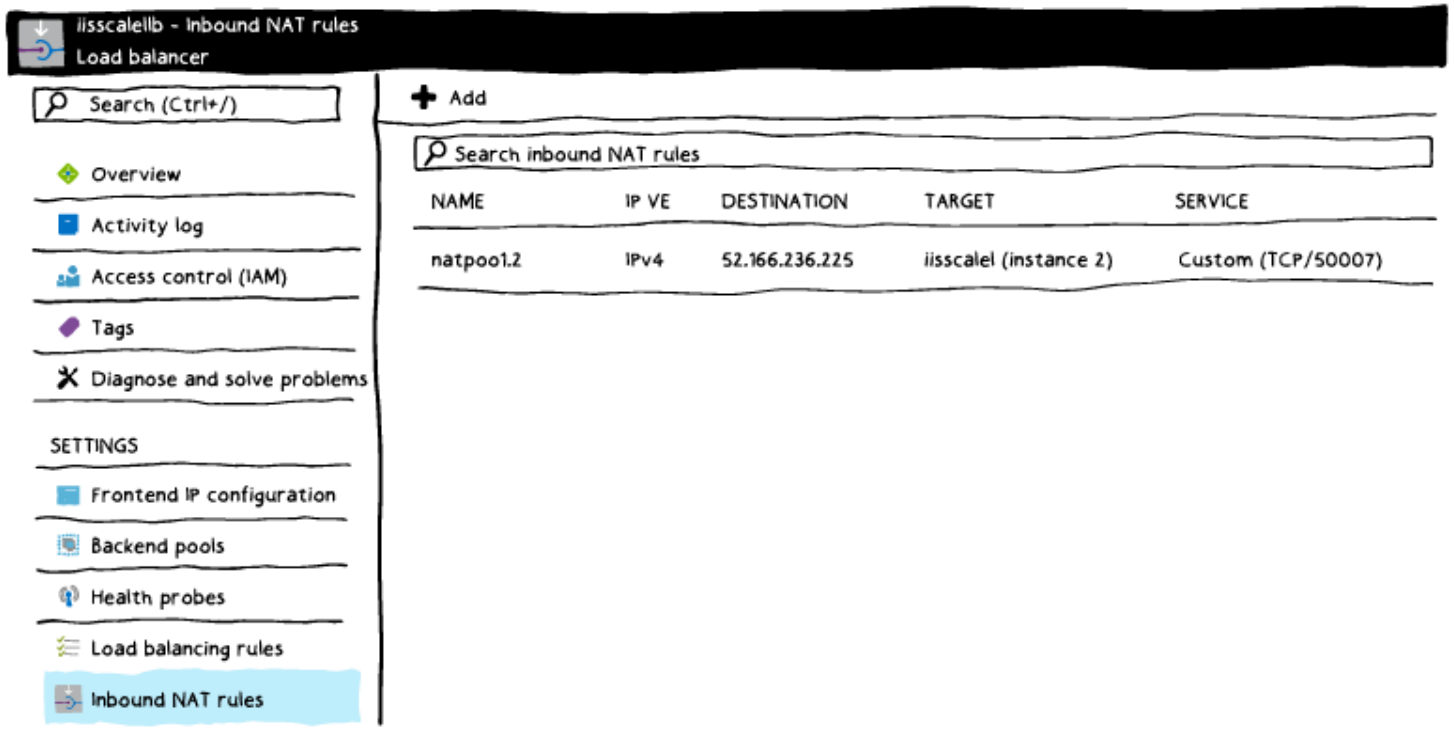


Virtual Machines vs. Virtual Machine Scale Sets

- Azure VM Scale Sets:
  - **Support auto-scaling.**
  - **Offer overprovisioning to accelerate the speed of deployment and scaling out.**
  - **Offer customizable policy controlling upgrade of all VMs in a scale set.**
  - **Support attaching new data disks to all VMs in a scale set (but not individual ones).**
  - **Do not support snapshots or image capture.**
  - **Do not support conversion from unmanaged disks to managed disks.**
  - **Do not support IPv6.**
- Azure VMs:
  - **Support custom configuration, including new or existing data disks.**
  - **Support snapshots and image capture.**
  - **Support conversion of unmanaged disks to managed disks.**
  - **Support IPv6.**

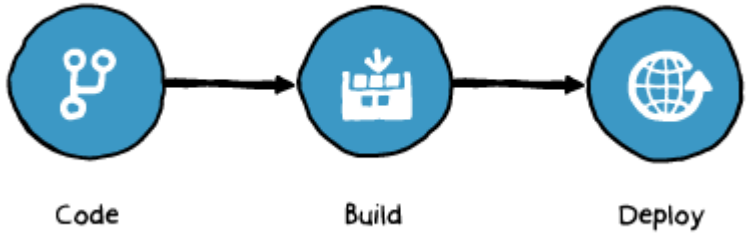
Virtual Machine Scale Set Considerations

- To connect to a VM Scale Set instance VM form Internet:
  - **Use inbound NAT rules of an Internet-facing load balancer in front of the VM Scale Set**
  - **e.g. RDP access via 52.166.236.225:50007**



Continuous Delivery in VMSS

- Use continuous integration/continuous delivery pipelines in Visual Studio Team Services to update an application running in a VMSS:
  - **Code update triggers a new build**
  - **The new built triggers VMSS update:**
    - **By creating and redeploying an updated OS image**
    - **By updating the application (via a VM extension)**
  - **Image based updates offer some benefits:**
    - **Predictability**
    - **Easy roll-back**
    - **Better scaling (no code to install on each VM as it is deployed)**

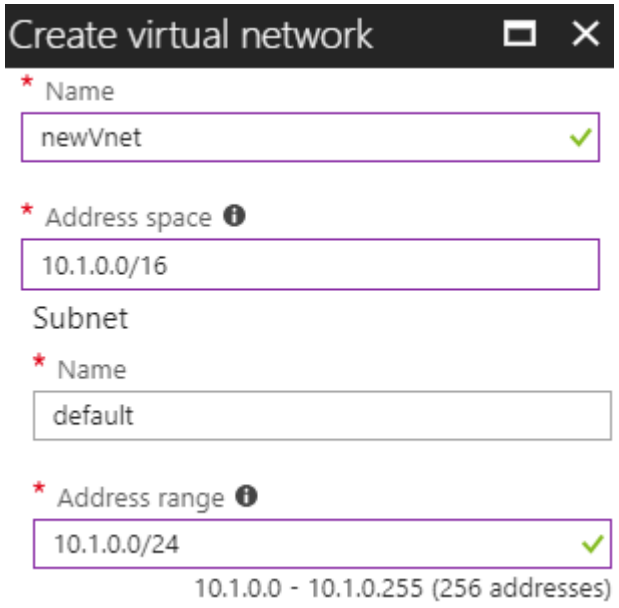


Large VM Scale Sets

- VM Scale Sets with 100+ VMs:
  - **Require the singlePlacementGroup property set to false**
  - **Require the use of managed disks.**
  - **Scale up to 1,000 VMs when based on Azure Marketplace images.**
  - **Scale up to 300 VMs when based on custom images.**
  - **Require the use of Azure Load Balancer Standard SKU for layer-4 load balancing.**
  - **Support Azure Application Gateway for layer-7 load balancing.**
  - **Require sufficiently sized IP subnet (all VMs in the same VMSS are deployed into the same IP subnet)**
  - **Might require an increase in vCPU subscription level quotas.**

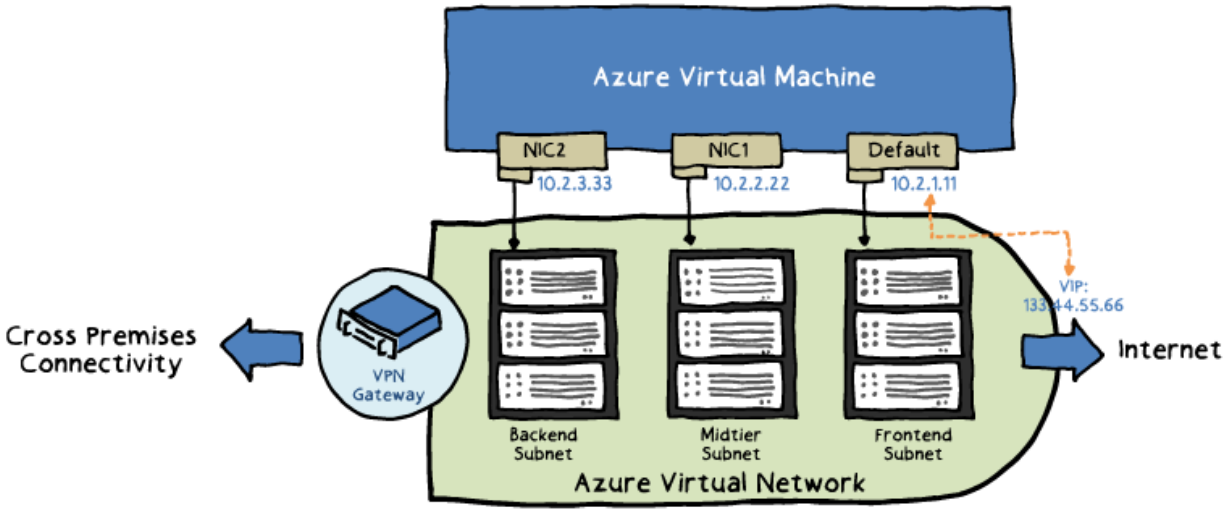
Implementing Virtual Networks

- Implementation includes:
  - **Defining an IP address space**
    - **Consider a non-overlapping address space**
  - **Creation of subnets**



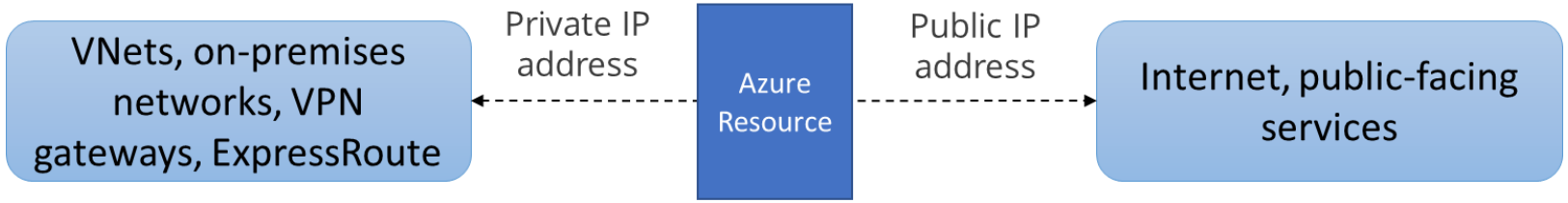
Multiple NICs in Virtual Machines

- A common requirement for network virtual appliances:
  - **Application delivery**
  - **WAN optimization**
- Common scenarios:
  - **isolation of front-end and back-end traffic**
  - **separation of data and control plane**
- Considerations:
  - **The order of NICs inside the OS of a VM is random and can change**
  - **IP addresses and MACs of NICs remain the same for the VM lifetime**
  - **The VM size determines the maximum number of NICs**



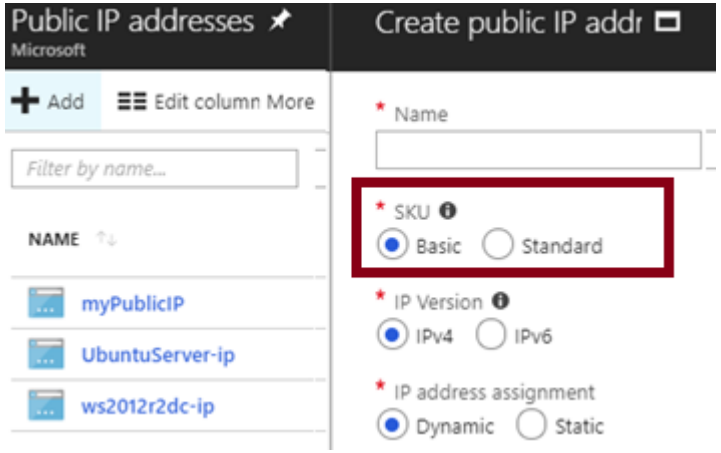
Overview of IP Addressing

- Azure networking supports two types of IP addresses:
  - **Private IP addresses: 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: Used for communication with the Internet, including Azure public-facing services.**
- Azure networking supports two types of IP address assignments:
  - **Static: common in scenarios that involve:**
    - **IP address-based security models which require apps or services to have a static IP address.**
    - **Azure VMs serving such roles as Active Directory Domain Controllers and DNS servers.**
    - **Firewall rules that allow or deny traffic using IP address ranges.**
  - **Dynamic**



Public IP Addresses

- Can be assigned to:
  - **VM NICs**
  - **Internet-facing load balancers**
  - **VPN gateways**
  - **Application gateways**
- Support two SKUs:
  - **Basic and Standard**



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

Feature	Basic SKU	Standard SKU
IP assignment	Static or dynamic	Static
Security	Open by default	Are secure by default and closed to inbound traffic
Resources	Network interfaces, VPN Gateways, Application Gateways, and Internet-facing load balancers	Network interfaces or public standard load balancers
Redundancy	Not zone redundant	Zone redundant by default

Private IP Addresses

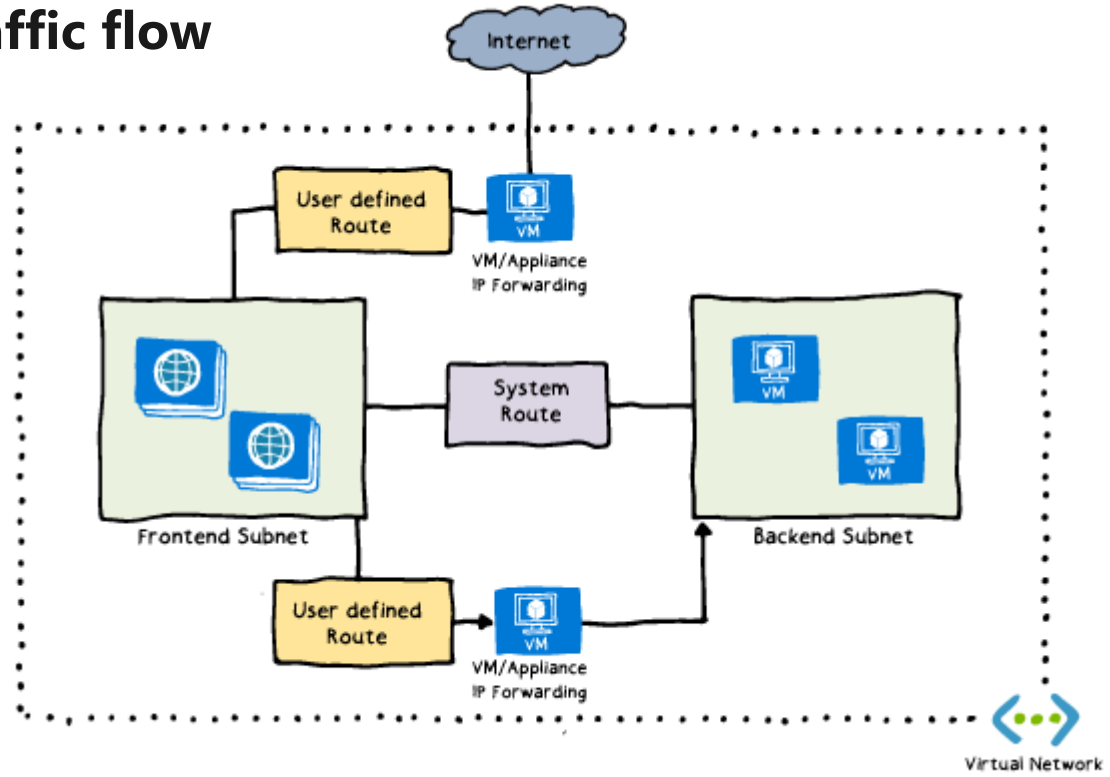
- Can be assigned to:
  - **VM NICs**
  - **Internal load balancers**
  - **Application gateways**

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

- Support two assignment methods:
  - **Static: You select and assign any available IP address in the subnet's address range.**
  - **Dynamic (default): Azure assigns the next available IP address in the subnet's address range.**

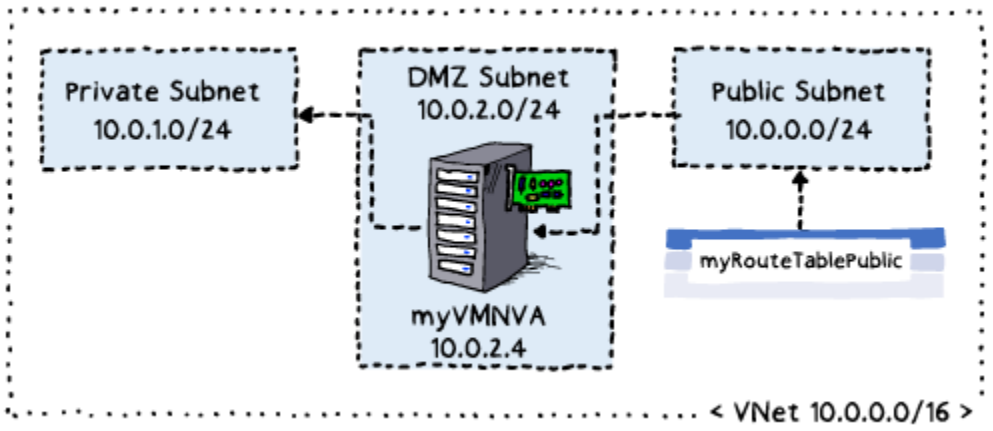
User Defined Routes

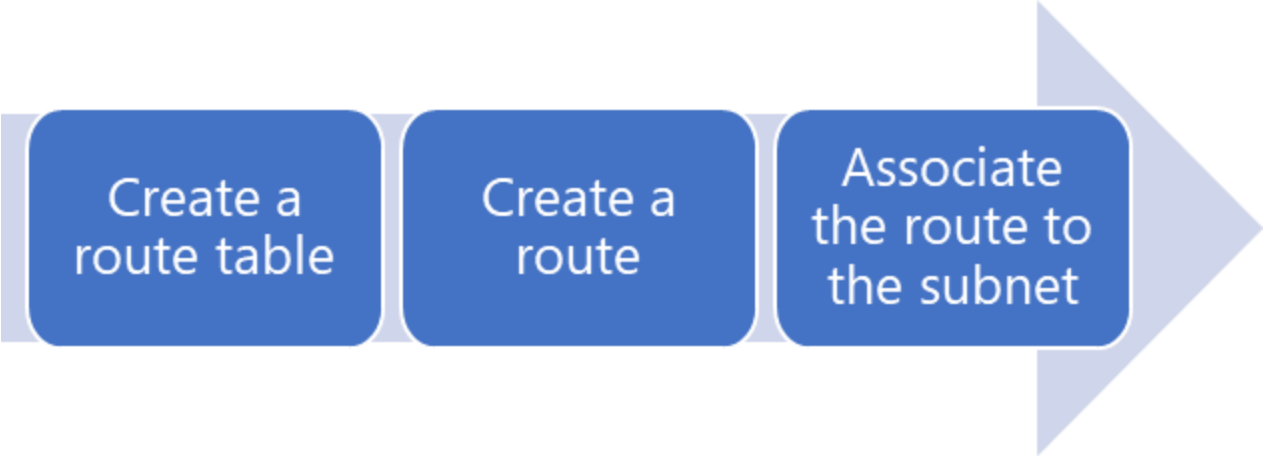
- Alter default system routes:
  - **Direct traffic to a designated virtual appliance**
  - **Facilitate routing, firewalling, or WAN optimization**
  - **Typically specify the next hop of the traffic flow**
- Implementation involves:
  - **Grouping routes into route tables**
  - **Associating route tables to subnets**



Routing Example

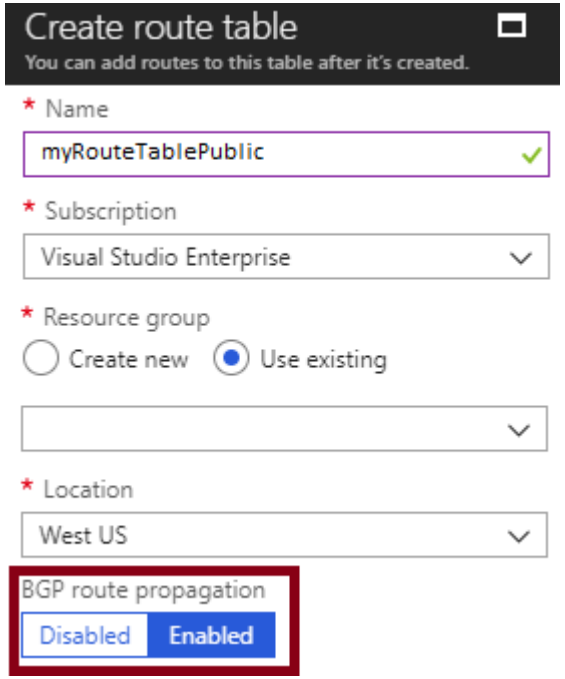
- A sample environment:
  - **Private subnet**
  - **DMZ subnet: hosting an NVA**
  - **Public subnet**
- Requirements:
  - **Traffic from the public subnet must route via NVA**
- Implementation:
  - **Create a route table**
    - **myRouteTablePublic**
  - **Add a route to the table**
    - **with NVA as the next hop**
  - **Associate the table to the Public subnet**





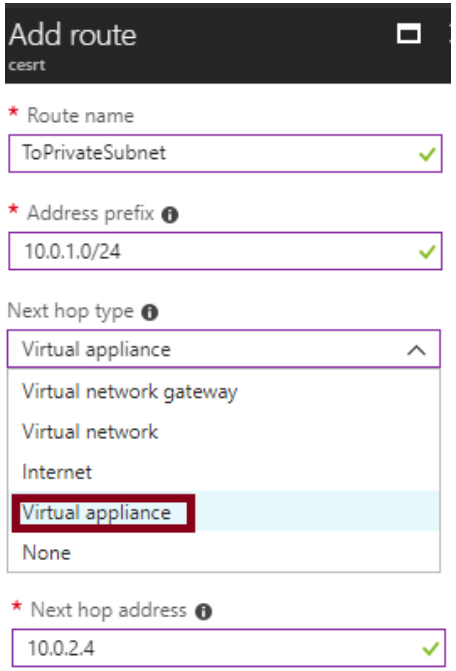
Create Route Table

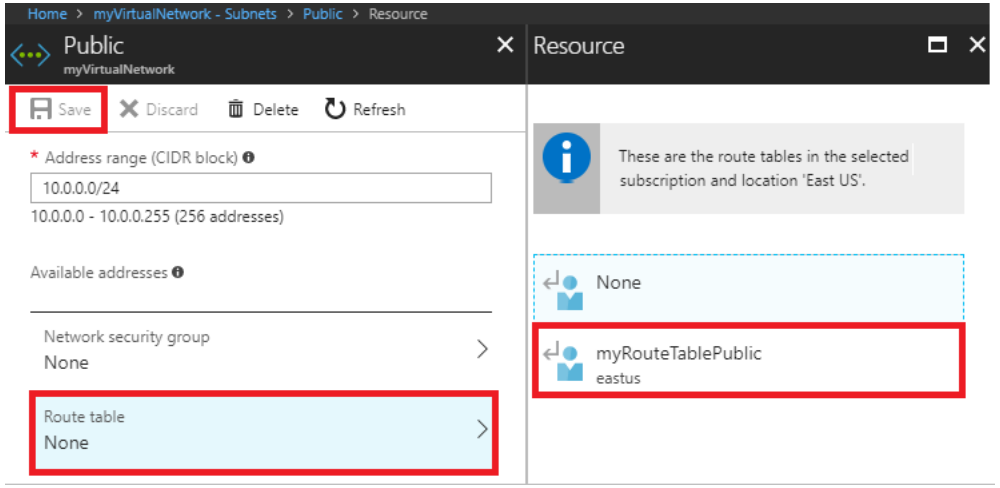
- Azure networking supports route propagation via BGP:
  - **This facilitates exchange routing and reachability information between networks**
  - **It is common in ExpressRoute scenarios**



Create and Associate the Route

- Add route to a route table:
  - **Specify the prefix**
  - **Select the next hop type:**
    - **Virtual network gateway**
    - **Virtual network**
    - **Internet**
    - **Virtual appliance**
    - **None**
  - **Specify the next hop address:**
    - **When using virtual appliance**
- Associate the route table to subnet





Routing Algorithms

- Route selection algorithms:
  - **Longest prefix match**

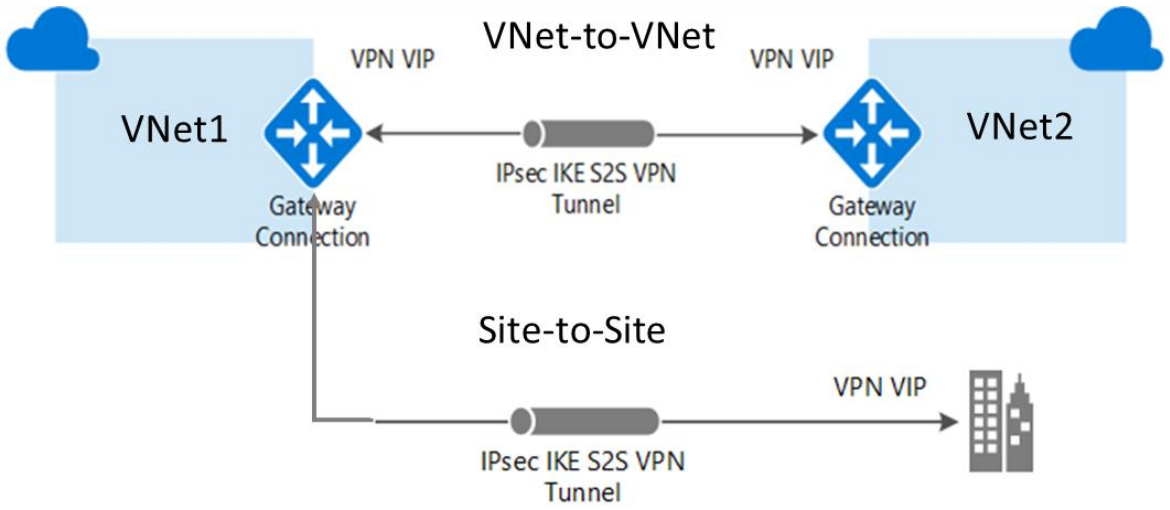
Source	Address prefixes	Next hop type
System	10.0.0.0/24	Internet (selected)
System	10.0.0.0/16	Virtual network gateway

  - **Route priorities:**
    - **1. User-defined route**
    - **2. BGP route**
    - **3. System route**

Source	Address prefixes	Next hop type
User	10.0.0.0/16	Internet (selected)
System	10.0.0.0/16	Virtual network gateway

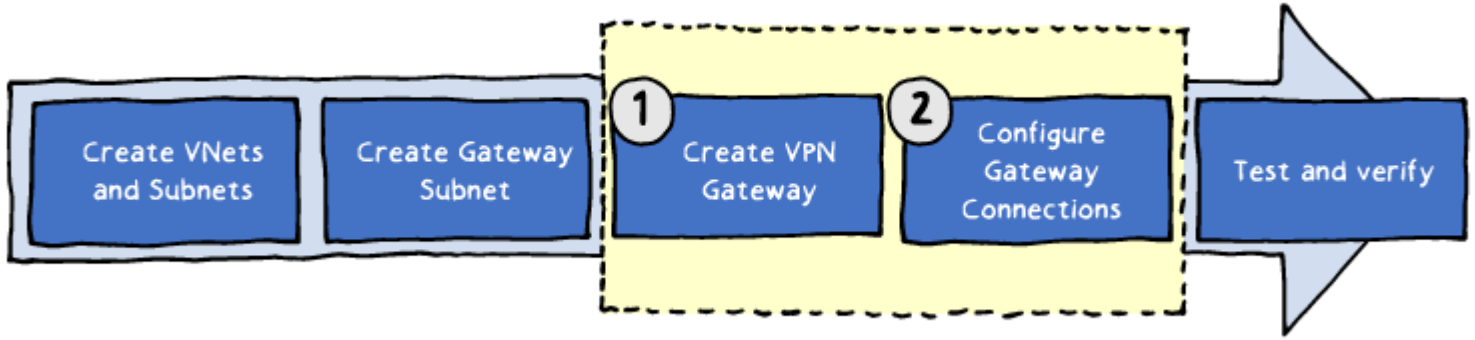
VNet-to-VNet Connections

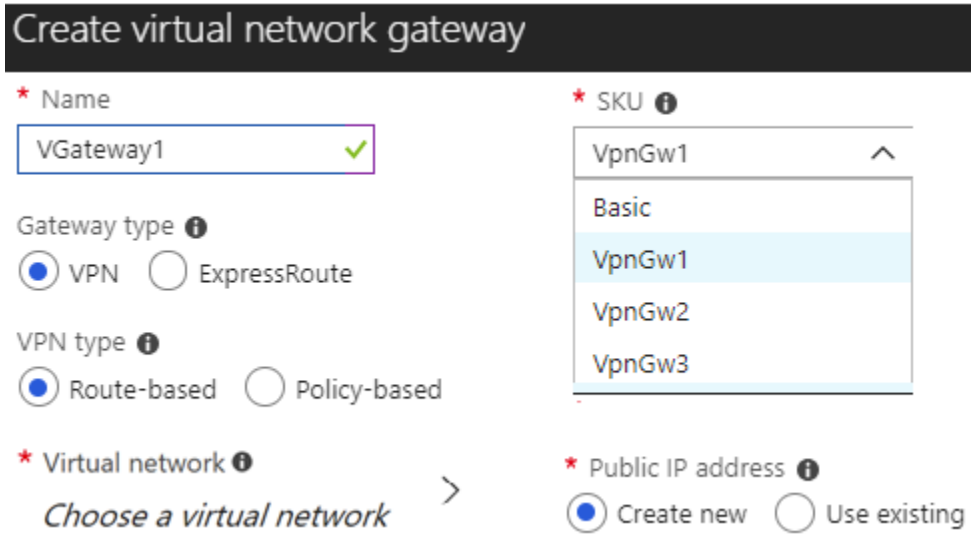
- Rely on VPN connectivity:
  - **Require VPN gateways for each VNet**
  - **Equivalent to Site-to-Site VPN in hybrid scenarios**
- Support connecting:
  - **VNets in the same or different regions.**
  - **VNets in the same or different subscriptions.**
  - **VNets and on-premises networks.**
  - **ARM VNets and classic VNets.**



Implementing VNet-to-VNet VPN

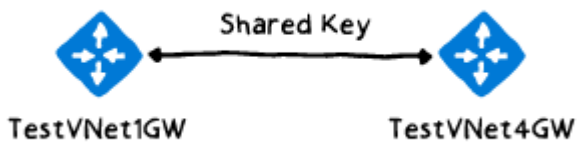
- In each VNet:
  - **Create the Gateway subnet**
  - **Create a VPN gateway:**
    - **Name and Gateway Type**
    - **VPN Type**
    - **SKU**
    - **Virtual Networks**
    - **IP Address**

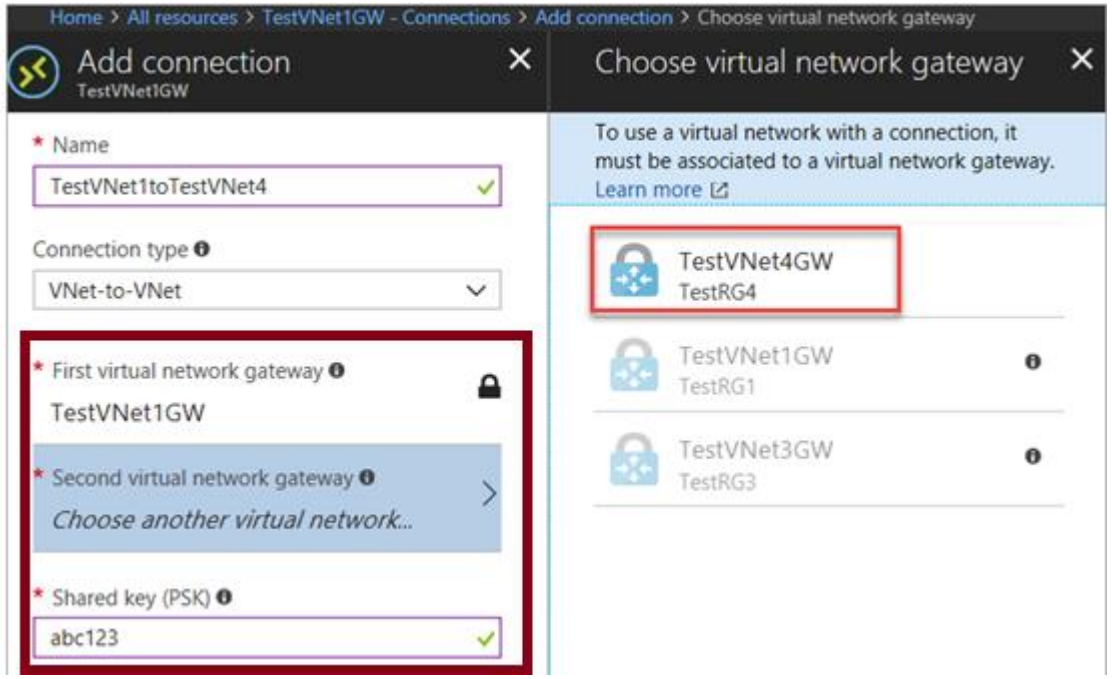




Configuring Gateway Connections

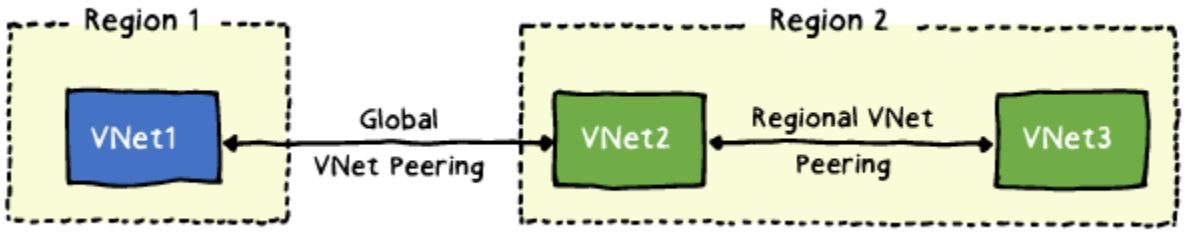
- The next step after provisioning of VPN gateways is completed
- Initial authentication is based on a shared key
- Implementation via:
  - **Azure PowerShell:**
    - **For VNets in the same or different subscriptions**
  - **The Azure portal:**
    - **For VNets in the same subscription**





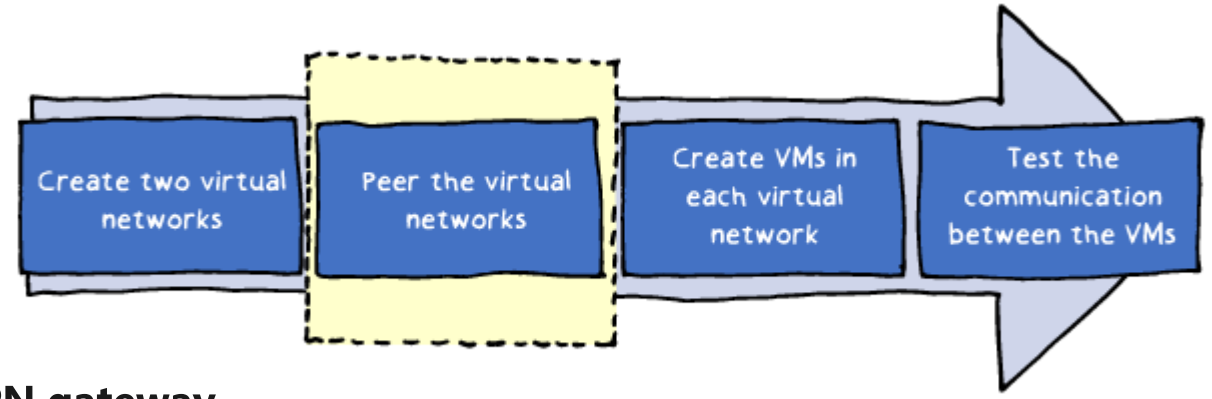
Overview of VNet Peering

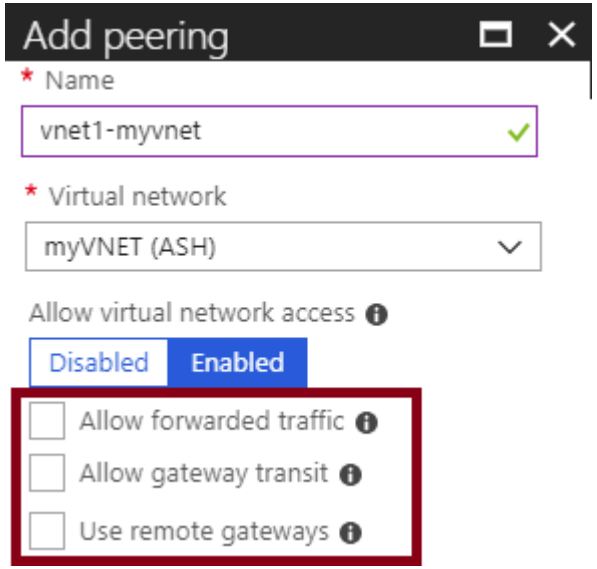
- Seamlessly connect virtual networks:
  - **Regional VNet peering: VNets in the same Azure region**
  - **Global VNet peering: VNets in different Azure regions**
- Offers a range of benefits:
  - **Security**
  - **Performance**
  - **Simplicity**
  - **Efficient**



Regional VNet Peering

- Configuration is required for each virtual network:
  - **Allow virtual network access:**
    - **Must be set to Enabled**
  - **Allow forwarded traffic:**
    - **Allows traffic routing via peered network**
  - **Allow gateway transit:**
    - **Allows the peered network to route to the local VPN gateway**
  - **Use remote gateways:**
    - **Allows the use of the VPN gateway on the peered network**



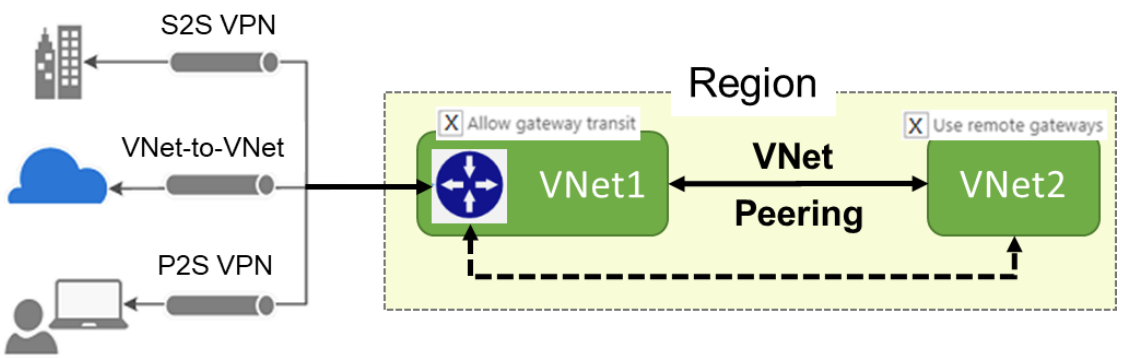


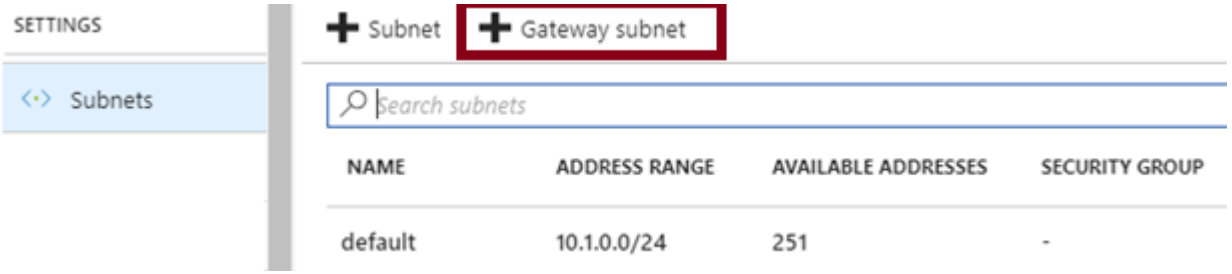
Global VNet Peering

- Provides peering across Azure regions:
  - **When implementing, peering status changes from Initiated to Connected**
- Requirements and constraints:
  - **No support for remote gateways and gateway transit**
  - **No peering between public clouds and national clouds**
  - **No access to front-end IP addresses of Azure internal load balancers in peered networks**
  - **No support for transitivity (for both regional and global peering)**

Gateway Transit

- Provides routing by using a VPN Gateway in a peered VNet to:
  - **an on-premises network (via site-to-site VPN)**
  - **another virtual network (via VNet-to-Vnet)**
  - **a remote VPN client (via point-to-site VPN)**
- Facilitates hub-spoke topology
- Requires Gateway subnet:
  - **hosting the Gateway only (no VMs)**



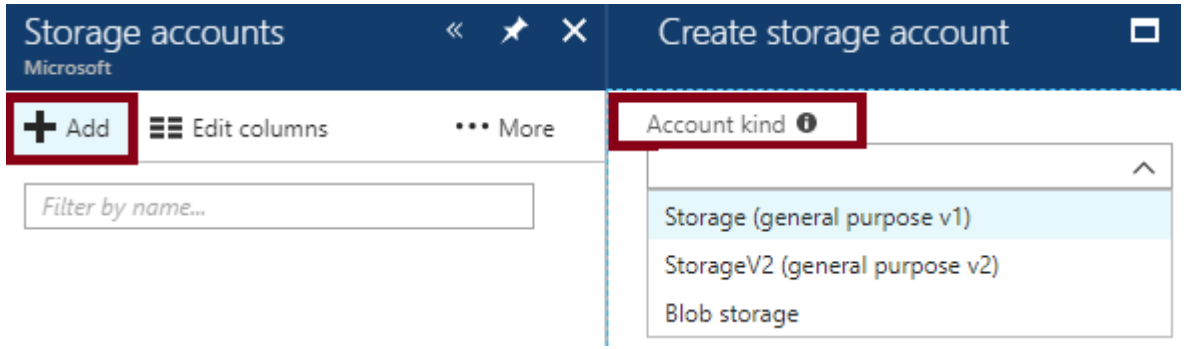


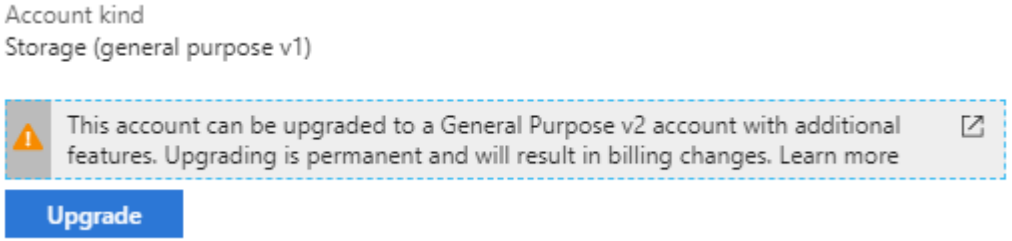
Azure Storage

- Azure Storage serves as:
  - **Storage for Azure VMs:**
    - **operating system and data disks**
    - **file storage**
  - **Store for unstructured data:**
    - **Blobs**
    - **Queues**
    - **Data Lake Store**
  - **Store for structured data:**
    - **Tables**
    - **Cosmos DB**
    - **Azure SQL Database**

Azure Storage Accounts

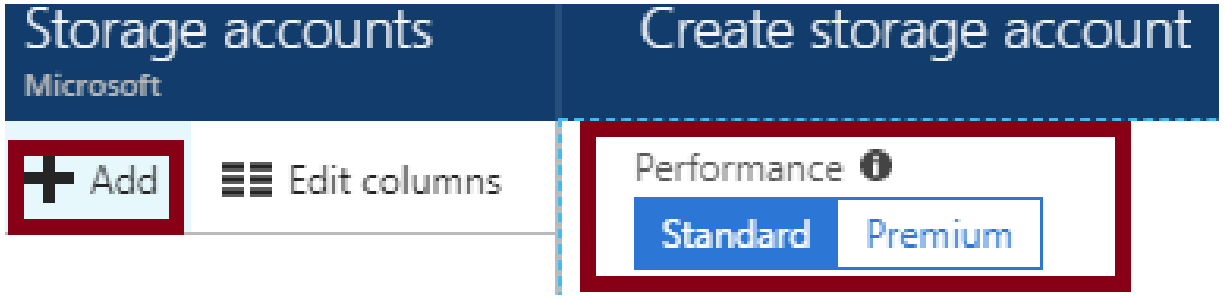
- Storage (general purpose v1):
  - **Can contain blobs (including Azure VM disks), tables, queues, files**
  - **Supports performance tiers: Standard and Premium**
- Blob storage:
  - **Can contain blobs only**
  - **Supports access tiers: hot, cool, archive**
- Storage V2 (general purpose v2):
  -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





Standard and Premium Storage Accounts

- Performance tiers:
  - **Standard:**
    - **Best for workloads that do not require high performance I/O**
    - **Offer the lowest cost per GB**
    - **Backed by magnetic drives (HDD)**
  - **Premium (available exclusively for provisioning Azure VM disks):**
    - **Best for I/O-intensive workloads, such as databases.**
    - **Offer consistent low-latency, high throughput/IOPS**
    - **Backed by solid state drives (SSD)**

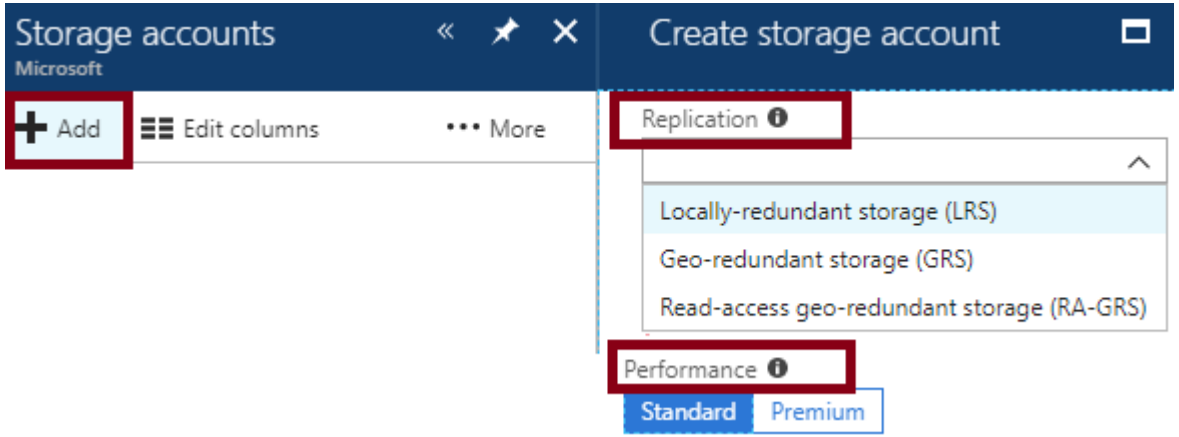


Storage Account Endpoints

- 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

Replication Options

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



Locally Redundant Storage

- Copies:
  - **3 in the same Azure facility**
- Strategy:
  - **Data replicated synchronously across 3 replicas in the same Azure facility**
- Protection:
  - **Localized hardware failures**
- Additional considerations:
  - **LRS is an economical option if your data can be easily reconstructed**
  - **LRS is the only available option if you use the Premium performance tier**
  - **When using LRS, you should plan for an alternative recovery strategy**

Geo-Redundant Storage

- Copies:
  - **Total of 6, with 3 per Azure region.**
- Strategy:
  - **Data replicated synchronously across 3 replicas in the same Azure facility**
  - **Data replicated synchronously within each region and asynchronously across regions.**
- Protection:
  - **Localized hardware failures and region-wide disasters**
- Additional considerations:
  - **With GRS, data in the secondary region becomes available for reads and writes (via the primary endpoint) only after Microsoft initiates a failover from the primary region.**
  - **With RA-GRS, data in the secondary region is always available for reads (via the secondary endpoint). It becomes available for writes (via the primary endpoint) only after Microsoft initiates a failover from the primary region.**

Zone Redundant Storage

- Copies:
  - **3 across different Azure facilities in separate zones in the same region.**
- Strategy:
  - **Data replicated synchronously across 3 replicas in separate zones in the same region.**
- Protection:
  - **Localized hardware failures and failures of individual facilities**
- Additional considerations:
  - **ZRS is not yet available in all regions.**
  - **ZRS may not protect your data against a regional disaster where multiple zones are permanently affected.**
  - **ZRS does not support Azure VM disk files**

Replication Option Comparison

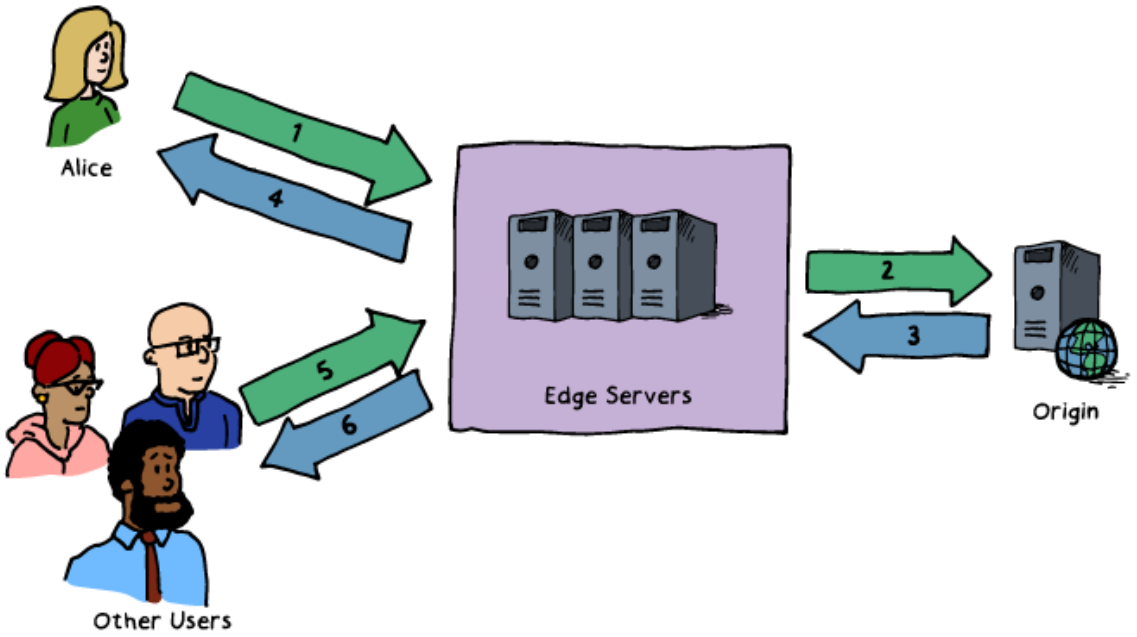
Replication Option	LRS	ZRS	GRS	RA-GRS
Node unavailability within a data center	Yes	Yes	Yes	Yes
An entire data center (zonal or non-zonal) becomes unavailable	No	Yes	Yes	Yes
A region-wide outage	No	No	Yes	Yes
Read access to your data (in a remote, geo-replicated region) in the event of region-wide unavailability	No	No	No	Yes
Available in storage account types	GPv1, GPv2, Blob	Standard,GPv2	GPv1, GPv2, Blob	GPv1, GPv2, Blob

Import and Export Service

- Transfers very large amounts of data between on-premises and Azure:
  - **Import. Securely transfers data to Azure Blob storage (block and page blobs) and Azure Files. You ship hard drives containing your data to an Azure data center.**
  - **Export. Securely transfers data from Azure Blob storage (block, page, and append blobs) to your location. You ship empty hard drives to an Azure data center.**
- Scenarios:
  - **Migrating data to the cloud**
  - **Content distribution**
  - **Backup and data recovery**

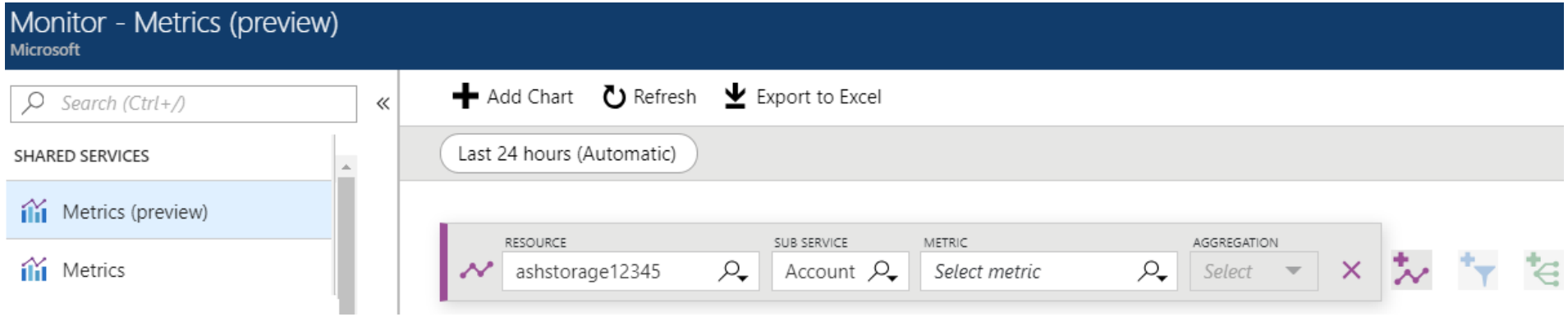
How CDN Works

- Azure content caching service:
  - **Designed to expedite delivery of audio, video, images, etc. hosted by Azure services**
  - **Utilizes the following data flow:**
    - **1. Alice requests a file using a URL pointing to a CDN location. DNS routes the request to the optimal POP**
    - **2. If edge servers do not have the file cached, they requests it from the origin.**
    - **3. The origin returns the file, including its TTL.**
    - **4. The server caches the file and returns it to Alice. The file remains cached until the TTL expires.**
    - **5. Subsequent requests are served from the cache.**



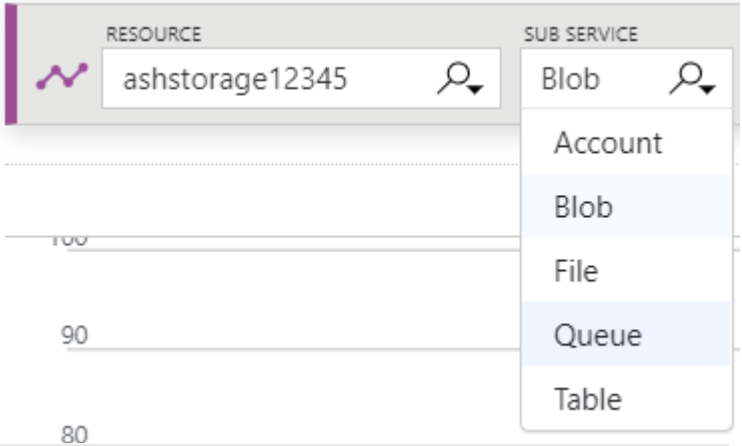
Monitor Metrics

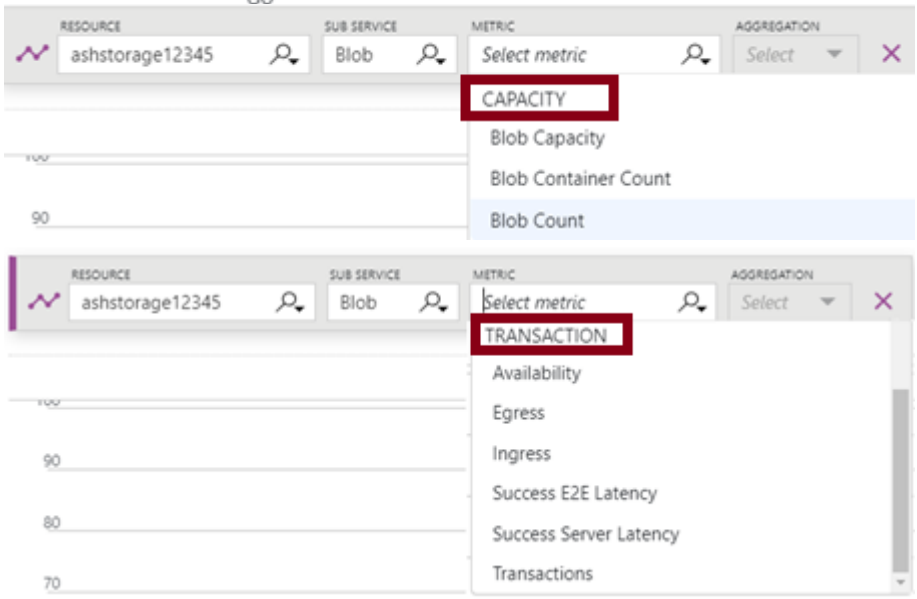
- Azure Monitor provides unified interface for monitoring Azure services
  - **Includes Azure Storage monitoring**
  - **Offers access via the Azure portal and Monitor API (REST and .NET)**
  - **Integrates with Log Analytics and Event Hubs**
  - **Stores metrics for 30 days and allows long term retention in Azure Storage**
  - **Supports consistent metrics filtering (resource, subservice) and aggregation criteria.**



Capacity and Transaction Metrics

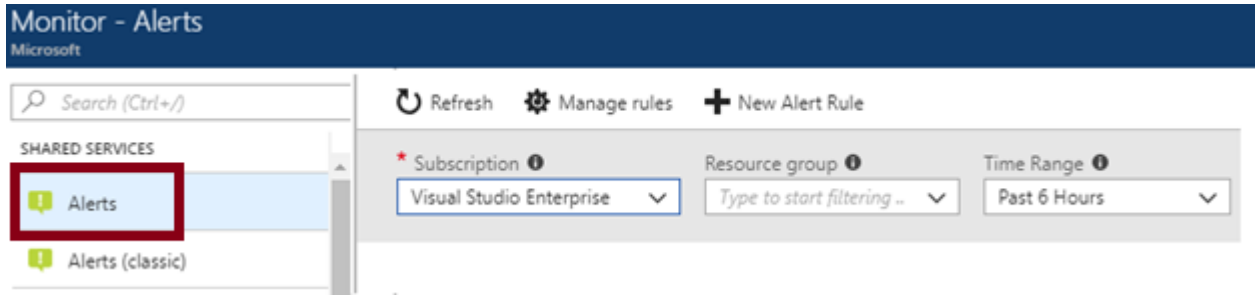
- Available from the Azure portal:
  - **Select a Storage Account resource**
  - **Select a sub-service: Account, Blob, File, Queue, or Table**
  - **The sub-service selection determines Capacity metrics:**
    - **For example, for Blob sub-service, Capacity metrics include:**
      - **Blob Capacity**
      - **Blob Container Count**
      - **Blob Count**
  - **Transaction metrics are available at:**
    - **account level**
    - **service level:**
      - **Blob storage**
      - **Table storage**
      - **Queue storage**
      - **Azure Files**





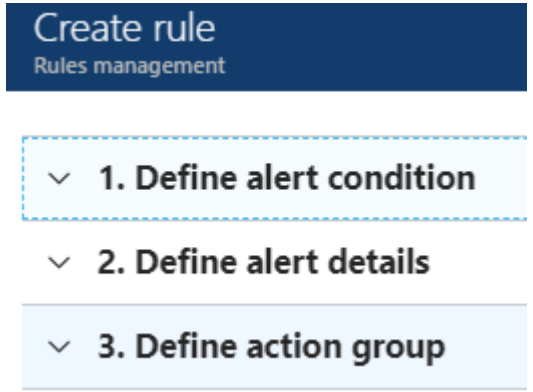
Azure Monitor Alerts

- New experience – comparing with Alerts (Classic):
  - **Better notification system**
  - **A unified authoring experience**
  - **Access to Log Analytics alerts from the Azure portal**
  - **Separation of Fired Alerts and Alert Rules**
  - **Better workflow**



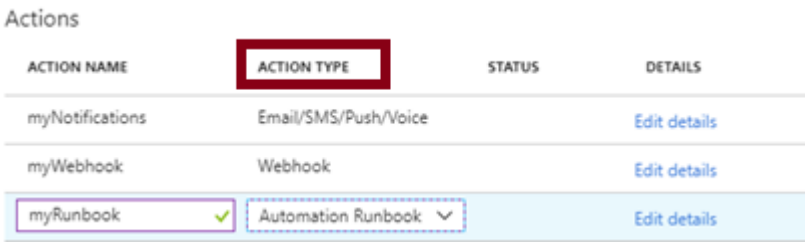
Alert Rules

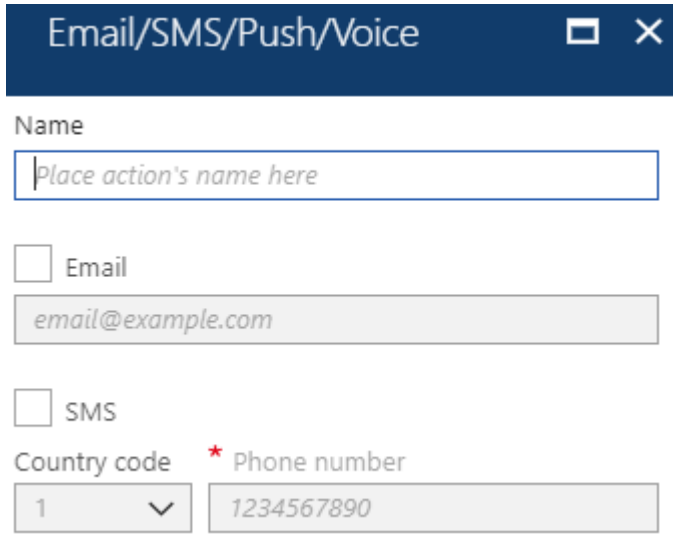
- Part of the new experience:
  - **alerts authoring is consistent regardless of the monitoring service or signal type**
  - **all alerts fired and related details are available on a single page**
- Authoring is a three-step process:
  - **1. Define alert condition, including:**
    - **Target selection. For example, a storage account.**
    - **Alert criteria. For example, Used Capacity.**
    - **Alert logic. For example, over a six-hour period whenever the Used Capacity is over 1000000 bytes.**
  - **2. Define alert details, including:**
    - **Alert rule name, description, and severity. There are five severity levels, Severity 0 to Severity 4.**
  - **3. Define an action group to notify your team via email and text messages or automate actions using webhooks and runbooks.**



Action Groups

- Action groups facilitate configuring actions in response to an alert:
  - **Email/SMS/Push/Voice**
  - **Logic App**
  - **Webhook**
  - **Automation Runbook**
  - **IT Service Management**





Signal Types and Metrics

- Signals are emitted by target resources and include:
  - **Metrics**
  - **Activity log**
  - **Application Insights**
  - **Logs**
- The latest metrics alerts offer:
  - **Improved latency**
  - **Support for multi-dimensional metrics**
  - **More control over metrics conditions**
  - **Combined monitoring of multiple metrics**
  - **Metrics from Logs (limited public preview)**

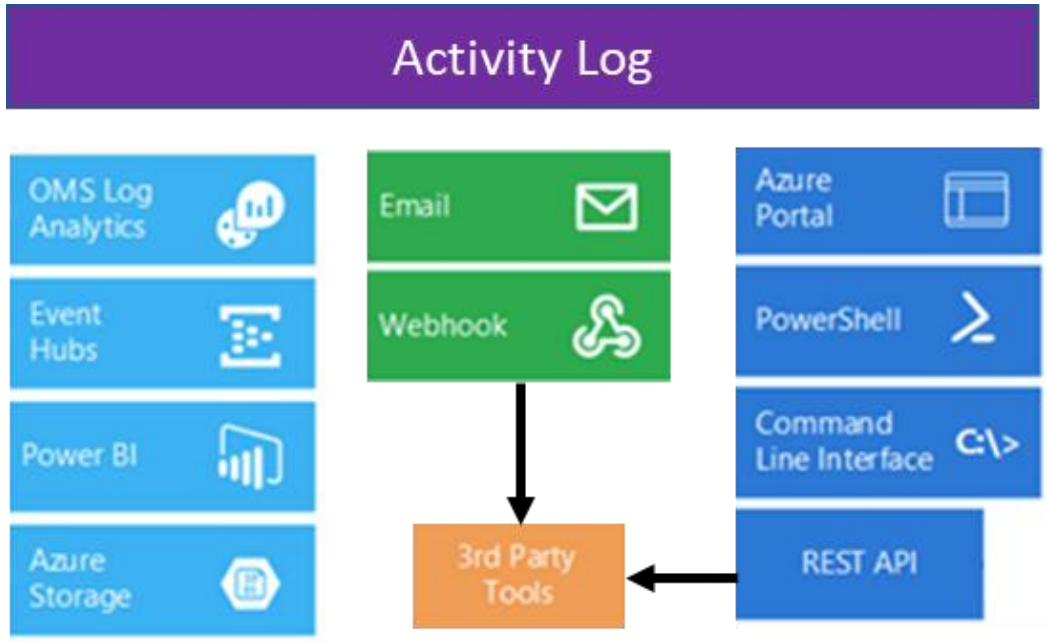
Configure signal logic

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

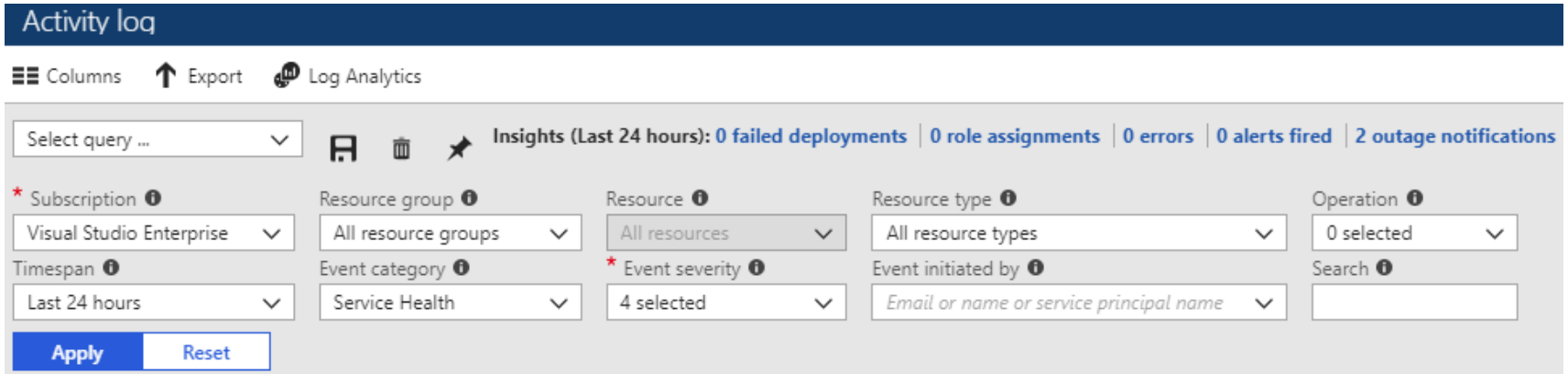
Activity Log

- A subscription-level log that captures:
  - **Azure Resource Manager operational data (control plane)**
  - **Service Health events**
- Includes audit trail of all write/change operations:
  - **Helps determine "what, who, and when"**
  - **Provides the status of each operation**
- Its content can be:
  - **Streamed to Event Hub.**
  - **Analyzed with Power BI.**
  - **Viewed in the Azure portal.**
  - **Forwarded to Log Analytics.**
  - **Archived in an Azure Storage account.**
  - **Processed with PowerShell, CLI, and REST API.**



Query the Activity Log

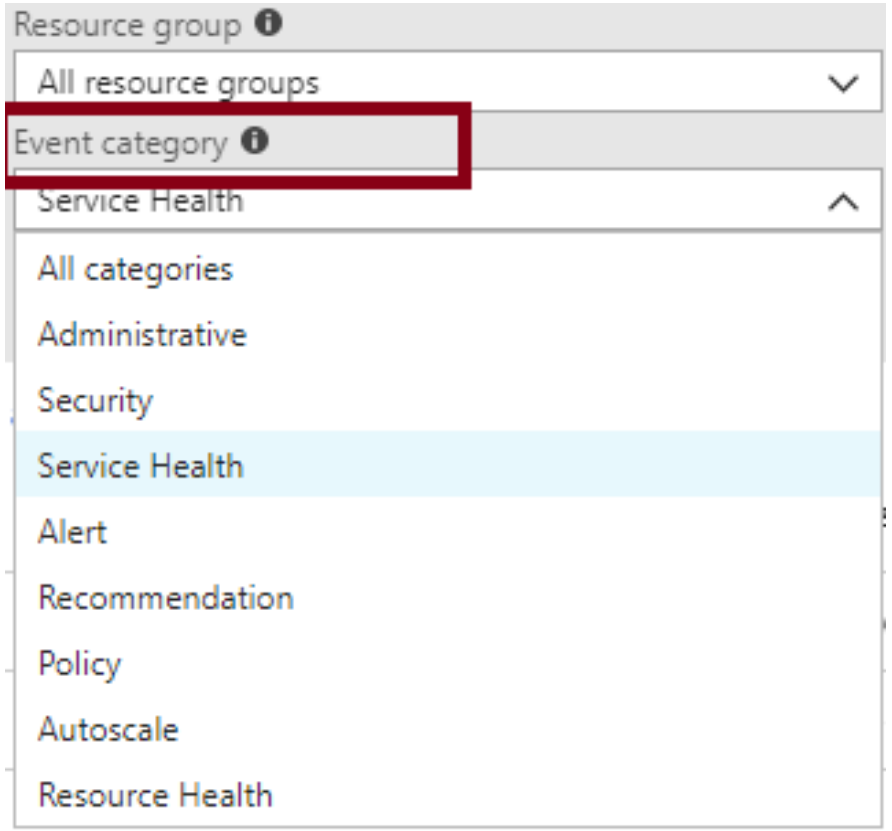
- Available directly from the Azure portal, with filtering based on:
  - **Subscription**
  - **Resource group**
  - **Resource (name)**
  - **Resource type**
  - **Operation (type)**
  - **Timespan**
  - **Event category**
  - **Event severity**
  - **Event initiated by**



- Filter selection can be saved
- Queries can be pinned to the Azure portal dashboard

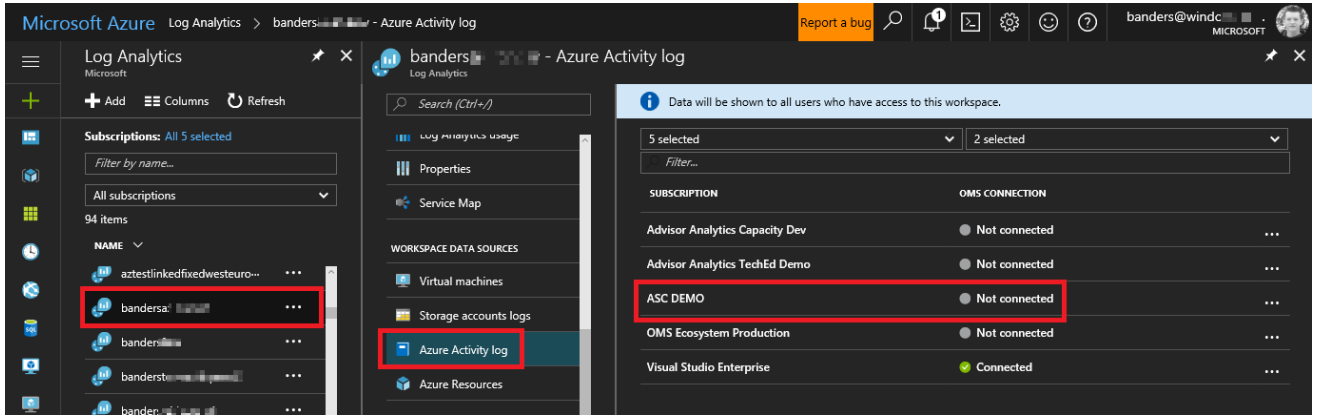
Event Categories

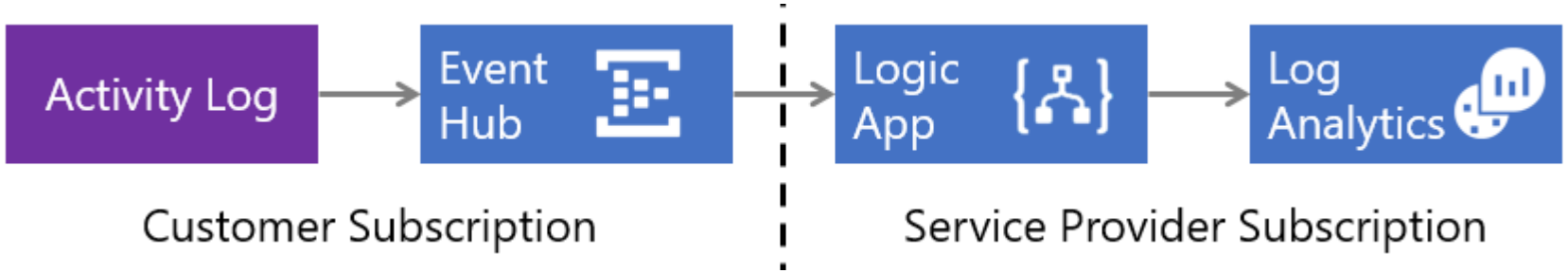
- Administrative
- Security
- Service Health
- Alert
- Recommendation
- Policy
- Autoscale
- Resource Health



Activity Log and Log Analytics

- Activity log can be added to Azure Log Analytics workspace:
  - **Can be in the same or a different subscription (if it has the same Azure AD tenant)**
  - **Provides the ability to:**
    - **Correlate user activities, auto-scale operations, authorization changes, and service health to other logs or metrics from your environment.**
    - **Correlate activity logs with other Azure services and application data.**
    - **Analyze and search activity logs from multiple Azure subscriptions.**
    - **Keep activity logs for longer than the default of 90 days.**
    - **View operational activities aggregated by status.**
    - **Analyze activity logs with pre-defined views.**
    - **Identify outage or service health issues.**
    - **Report on authorization changes.**
    - **View trends of activities.**



Collect Across Subscriptions

- You can collect Azure Activity Logs into a Log Analytics workspace using the Azure Log Analytics Data Collector connector for Logic Apps
  - **This facilitates using a workspace in a subscription that has a different Azure AD tenant**
  - **It offers a number of advantages, including:**
    - **Low latency, since the Azure Activity Log is streamed into the Event Hub**
    - **Serverless services, with no infrastructure components to deploy**
    - **Minimal custom code**