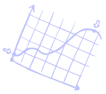
KODEKLOUD

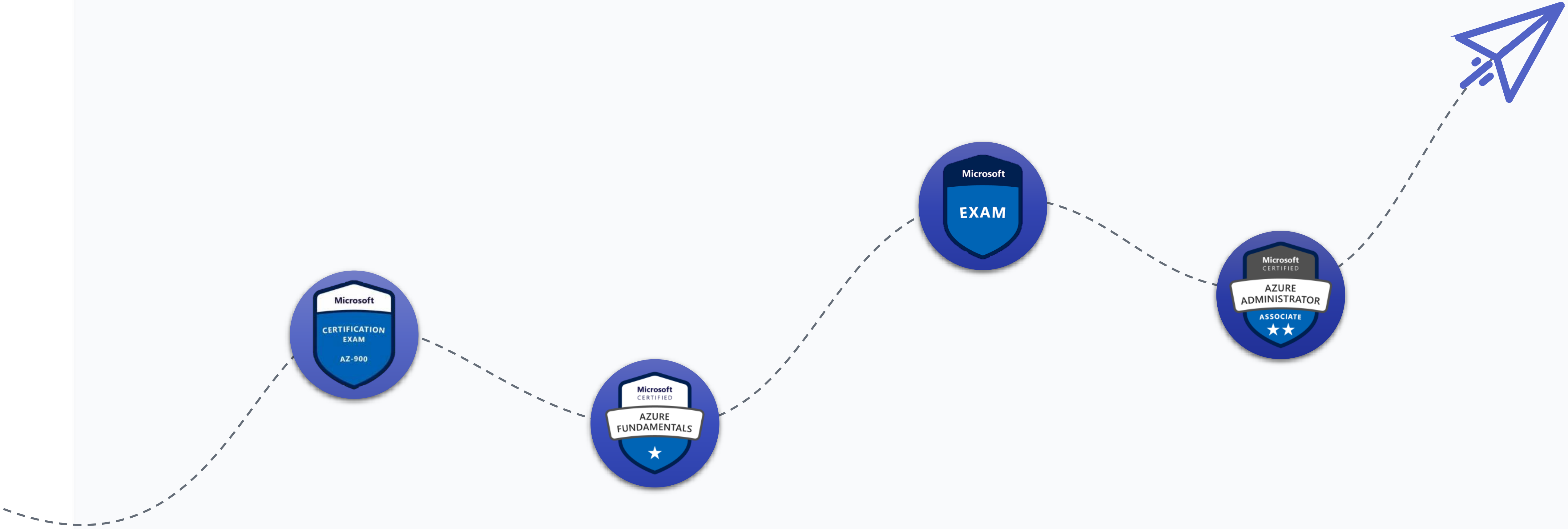
Instructor

Rithin Skaria

Microsoft Certified Trainer



Certification Roadmap



AZ-900 (Azure Fundamentals is optional). Passing score for AZ-104 is 700

Manage identities and governance

15-20%

Implement and manage storage

15-20%

Deploy and manage compute resources

20-25%

Configure and manage virtual networking

25-30%

Monitor and backup resources

10-15%

Exam AZ-104 : Skills Measured

As an administrator, you need to implement, manage and administer compute, network, storage, identity, governance and monitoring. This includes creating, updating, resizing, and deleting resources in cloud infrastructure as needed.

One of the prerequisites for the course is basic knowledge of Azure services and strong knowledge of compute, storage, and network concepts. In large enterprise organizations, you will be a part of a team which focuses on administering one or more Azure services.

Exam AZ-104: Microsoft Azure Administrator

START

MODULE 1

Managing Azure Active Directory

Understand the basics of Azure Active Directory and how it's different from traditional AD. Along with learn user management and group management in Azure AD.

MODULE 2

Subscription and Governance

Managing Azure Subscriptions and implementing governance using Azure Policy, Azure Tags and Role Based Access Control.

MODULE 3

Implementing virtual networking

Learn how to manage Azure Virtual Networks and some of the core networking concepts such as User Defined Routes, Azure DNS, Azure Firewall and Network Security Groups.

MODULE 4

Configure VMs

Start planning and deploy your virtual machines to Azure. Understand how to set up scaling and high availability for Azure VMs.

MODULE 5

Load Balancing

Load Balancing is required to balance the requests between our Azure workloads. Explore different load balancing solutions available in Azure

MODULE 6

Intersite connectivity

Learn how to deploy Azure-to-Azure connectivity and Azure-to-on-premises connectivity.

MODULE 7

Automating deployment and configuration

Start automating resource deployment using ARM templates and configure your VMs with the help of VM Extensions.

MODULE 8

Securing storage

Learn how to secure your Azure Storage Accounts

MODULE 9

Administering Azure Blobs and Azure Files

Understand how to work storage services like Azure Blobs and Azure Files.

MODULE 10

Managing Storage

Get familiarized with tools that can be used to manage Azure Storage. Explore Azure Storage Explorer, AZCopy, and Import/Export service

MODULE 11

Azure App Services

Learn Azure App Service Plans and Azure App Service

MODULE 12

Configuring containers

Explore Azure Container Instances and Azure Kubernetes Service..

MODULE 13

Implement backup and recovery

Learn how to setup backup and disaster recovery in Azure

MODULE 14

Network Monitoring

Set up network monitoring tools to troubleshoot network related issues

MODULE 15

Resource Monitoring

Configure monitoring for Azure resources.

END

Manage identities and governance 15-20%	Implement and manage storage 15-20%	Deploy and manage compute resources 20-25%	Configure and manage virtual networking 25-30%	Monitor and backup resources 10-15%
Managing Azure Active Directory	Securing storage	Configure Virtual Machines	Implementing virtual networking	Implement backup and recovery
Subscription and Governance	Administering Azure Blobs and Azure Files	Automating deployment and configuration	Load Balancing	Network Monitoring
	Managing Storage	Azure App Services	Intersite connectivity	Resource Monitoring
		Configuring containers		

Identity

Learn how to use Azure Active Directory to secure your identities. Also, understand how users and groups are implemented in Azure AD.

Azure Active Directory

Overview of Azure AD and concepts related to Azure AD

Azure AD Join

Joining and registering devices to Azure AD

Self-Service Password Reset

Enabling users to reset their passwords without reaching out to IT helpdesk.

.

User Accounts

Managing users and bulk user operations in Azure AD.

Group Accounts

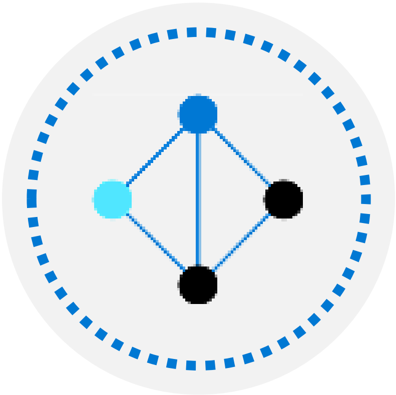
Group Management in Azure AD

Multi-tenant environments

Managing multiple tenants or directories

KODEKLOUD

Managing Azure Active Directory
Section Overview



Identity

Learn how to use Azure Active Directory to secure your identities. Also, understand how users and groups are implemented in Azure AD.

Azure Active Directory

Overview of Azure AD and concepts related to Azure AD

Azure AD Join

Joining and registering devices to Azure AD

Self-Service Password Reset

Enabling users to reset their passwords without reaching out to IT helpdesk.

.

User Accounts

Managing users and bulk user operations in Azure AD.

Group Accounts

Group Management in Azure AD

Multi-tenant environments

Managing multiple tenants or directories

Introduction to Azure AD

Azure Active Directory

Cloud based identity and directory management service enabling access to Azure services and other SaaS solutions like Microsoft 365, DropBox, Concur, Salesforce etc.

Offers self-service options including password reset, authentication, device management, hybrid identities, and single sign-on.

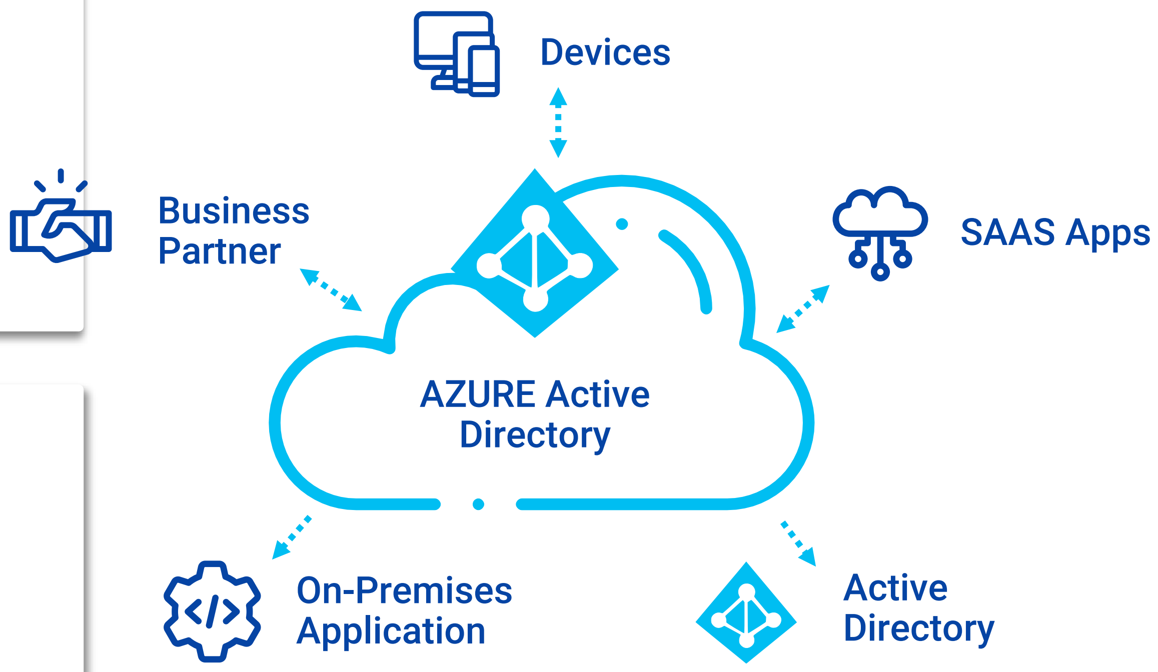


Image source: Microsoft Docs

Azure AD concepts

Azure AD Concepts

Identity

Any object that can be authenticated is considered as an identity. It could be a user, group, managed identity, or service principals.

Account

When we associate data attributes to an identity, we call it an account. For example, a user will have multiple attributes like location, department, manager, phone number etc.

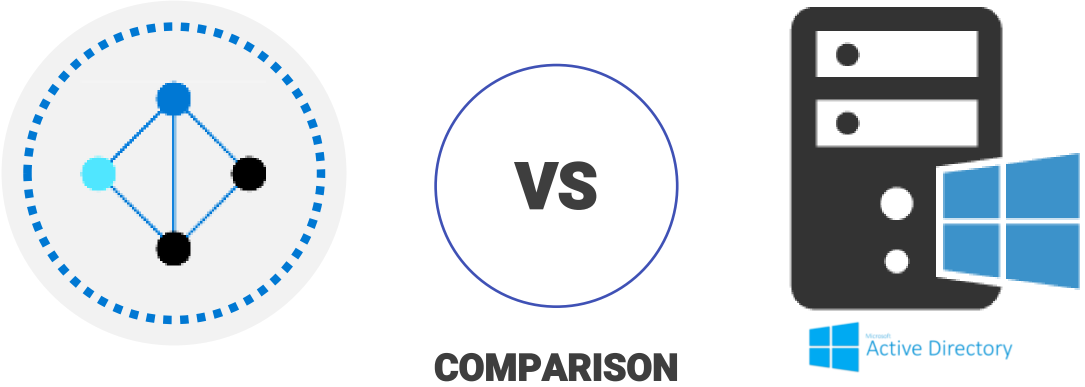
Azure AD Account

Accounts that are created in Azure AD or another Microsoft cloud service is known as Azure AD Account.

Azure AD tenant or directory

Dedicated instance of Azure AD that is created during the sign-up of any Microsoft cloud service subscription. Tenant and directory means the same and you can use interchangeably

Azure AD vs Active Directory Domain Services

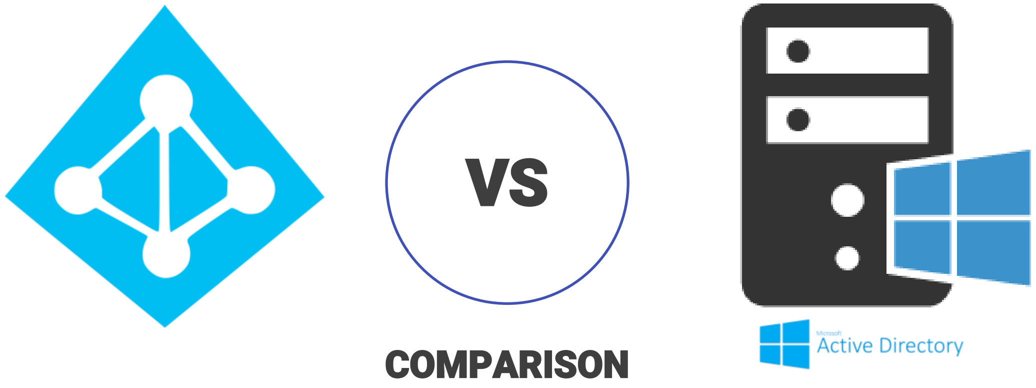


VS

COMPARISON

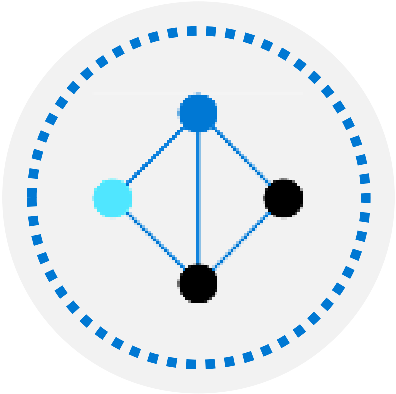
Azure AD vs Active Directory Domain Services

- Queried using HTTP/HTTPS
- Protocols used for authentication includes SAML, WS-Federation, OpenID connect. OAuth is used for authorization
- Federation can be setup with third party providers like Facebook.
- Azure AD is a managed service offering.



- Queried using LDAP
- Kerberos is used AD DS authentication
- Federation is only to other domains; third party services are not supported.
- ADDS will be running on VMs or physical servers.

Azure AD Editions



Azure AD Editions

Premium P2	No directory object limit	Single Sign on & Core IAM	B2B collaboration	O365 Identity & Access	Hybrid identities	Conditional Access	Identity Protection	Identity Governance
Premium P1	No directory object limit	Single Sign on & Core IAM	B2B collaboration	O365 Identity & Access	Hybrid identities	Conditional Access		
M365 Apps	No directory object limit	Single Sign on & Core IAM	B2B collaboration	O365 Identity & Access				
Free	50,000 directory objects	Single Sign on & Core IAM	B2B collaboration					

User Accounts

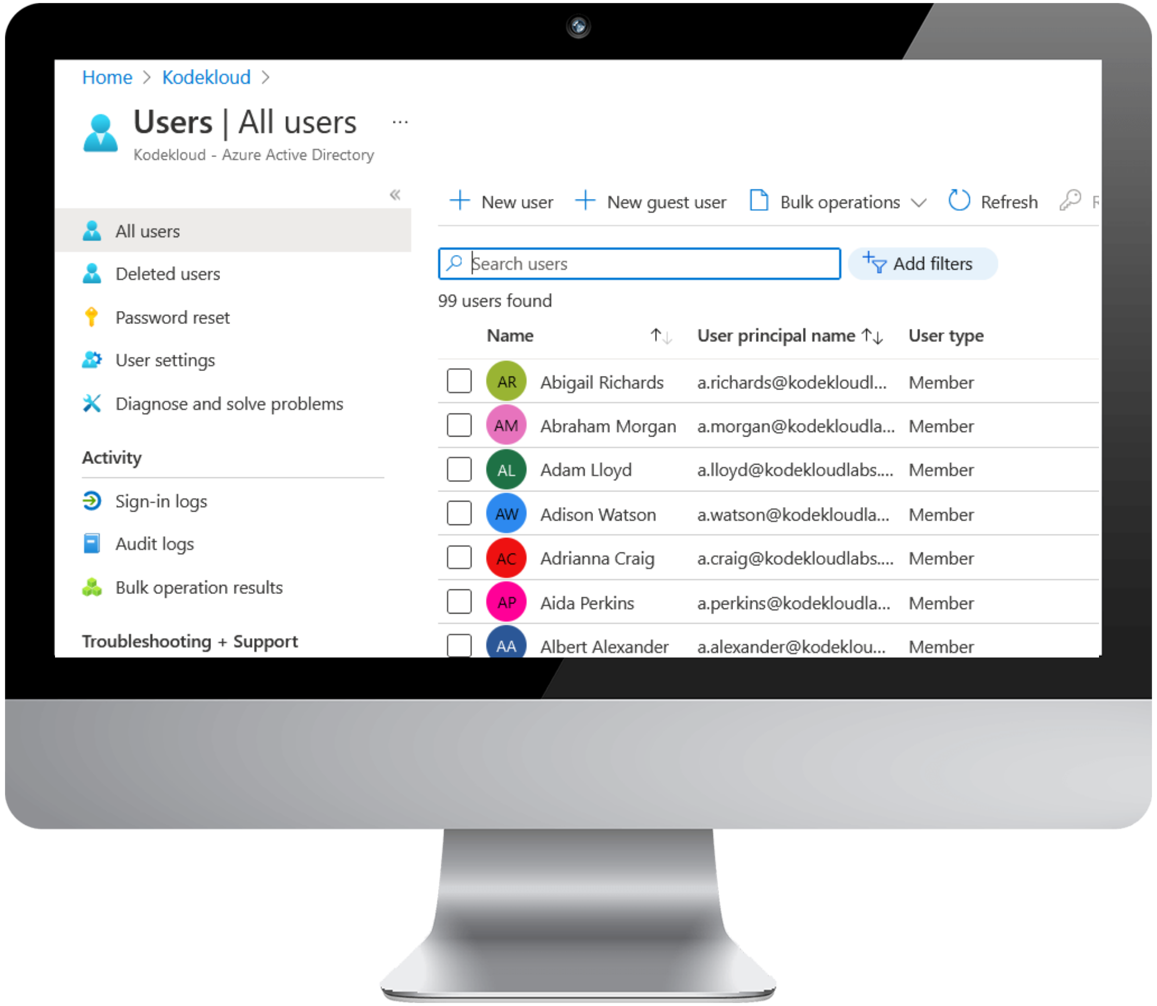
User Accounts

User accounts are used for authentication and authorization, all users must have an account.

Each user account can have optional properties such as address, department etc.

All users can be accessed from Azure Active Directory > Users > All Users.

We can also perform bulk operations like bulk create, bulk invite, and bulk delete.



Home > Kodekloud >

Users | All users ...

Kodekloud - Azure Active Directory

99 users found

	Name ↑↓	User principal name ↑↓	User type
□	AR Abigail Richards	a.richards@kodekloudl...	Member
□	AM Abraham Morgan	a.morgan@kodekloudla...	Member
□	AL Adam Lloyd	a.lloyd@kodekloudlabs....	Member
□	AW Adison Watson	a.watson@kodekloudla...	Member
□	AC Adrianna Craig	a.craig@kodekloudlabs....	Member
□	AP Aida Perkins	a.perkins@kodekloudla...	Member
□	AA Albert Alexander	a.alexander@kodeklou...	Member

Cloud Identities

These are users exist only in azure AD. Can be Azure AD or external Azure AD as well.

Guest Accounts

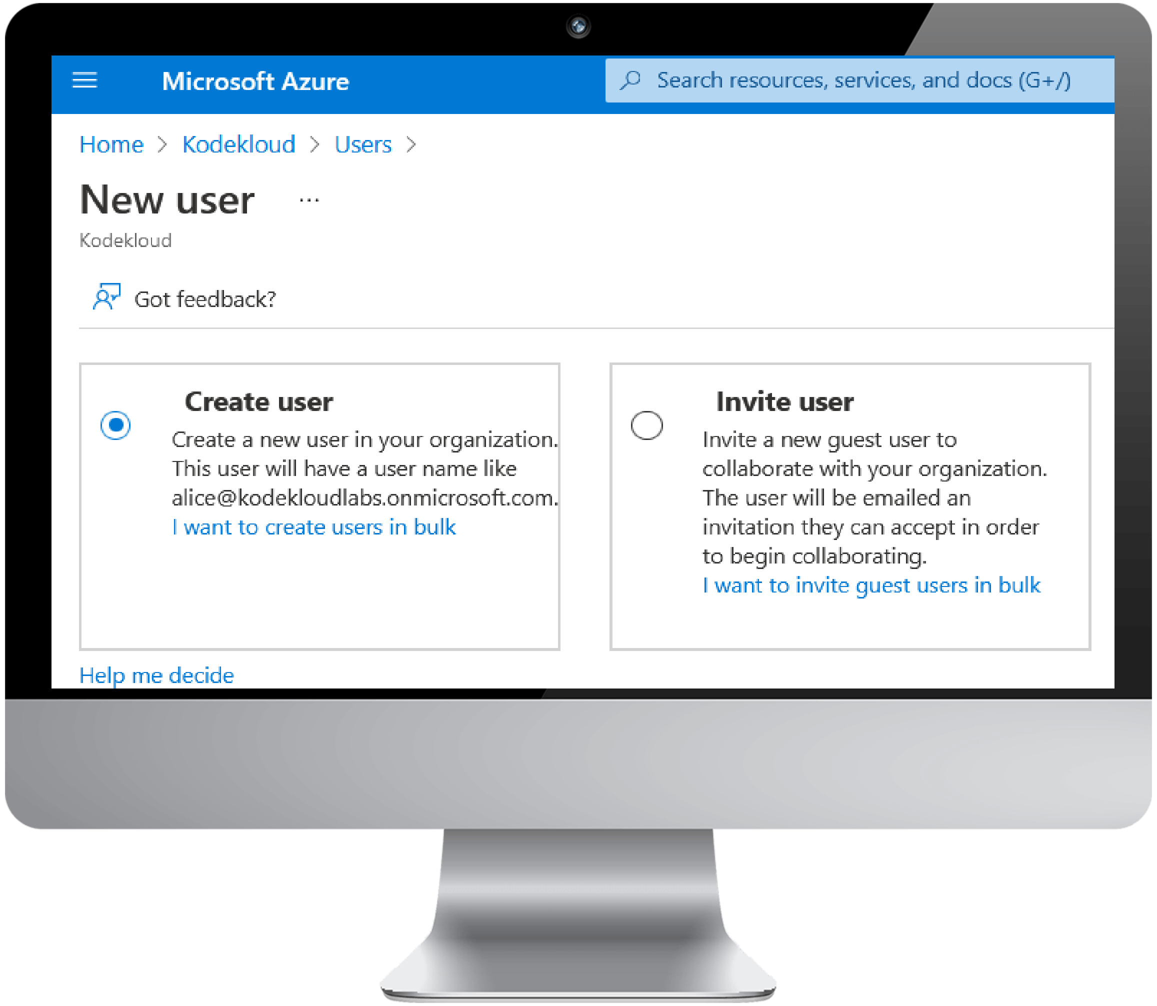
These are users exist outside of Azure and they are invited for collaboration. Microsoft accounts, Live accounts etc.

Directory synchronized users

These users are synchronized from your on-premises Windows AD. We cannot create directory synchronized users; they need to be synchronized.

Managing User Accounts

- **Create a user:** This will create a user in your Azure AD. The identity created as part of this process will have a sign in name from your tenant.
- **Invite a user:** This will help us to invite guest users to collaborate with your organization. An invitation will be triggered to the email address, and they must accept the invitation to start collaborating.
- User can be deleted if needed. Deleted users will be retained for 30 days and can be restored during this window.
- All sign in and audit log can be tracked.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Kodekloud > Users >
Got feedback?
Help me decide

New user ...
Kodekloud

● **Create user**
Create a new user in your organization. This user will have a user name like alice@kodekloudlabs.onmicrosoft.com.
I want to create users in bulk

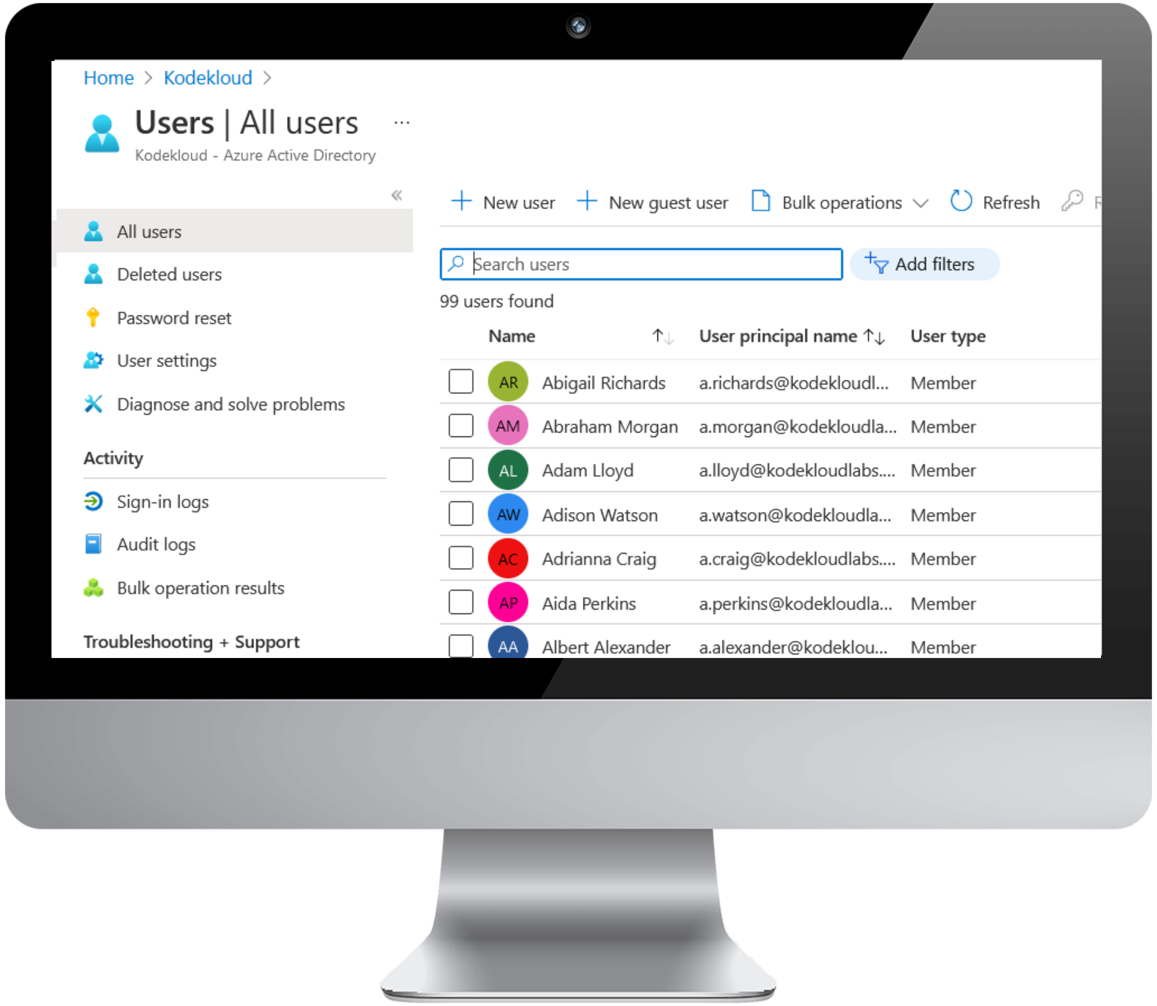
○ **Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
I want to invite guest users in bulk

Bulk Operations

User Accounts – Bulk Operations

Bulk operations will let you download a CSV template where you add users you want to create, delete, or invite. Using bulk operation, we can easily work on these operations rather than doing one by one.

- **Bulk create:** Create users in bulk
- **Bulk invite:** Invite external users for collaboration in bulk.
- **Bulk delete:** Delete existing users in bulk
- **Download users:** Creates export of all users in the directory



Home > Kodekloud >

Users | All users ...

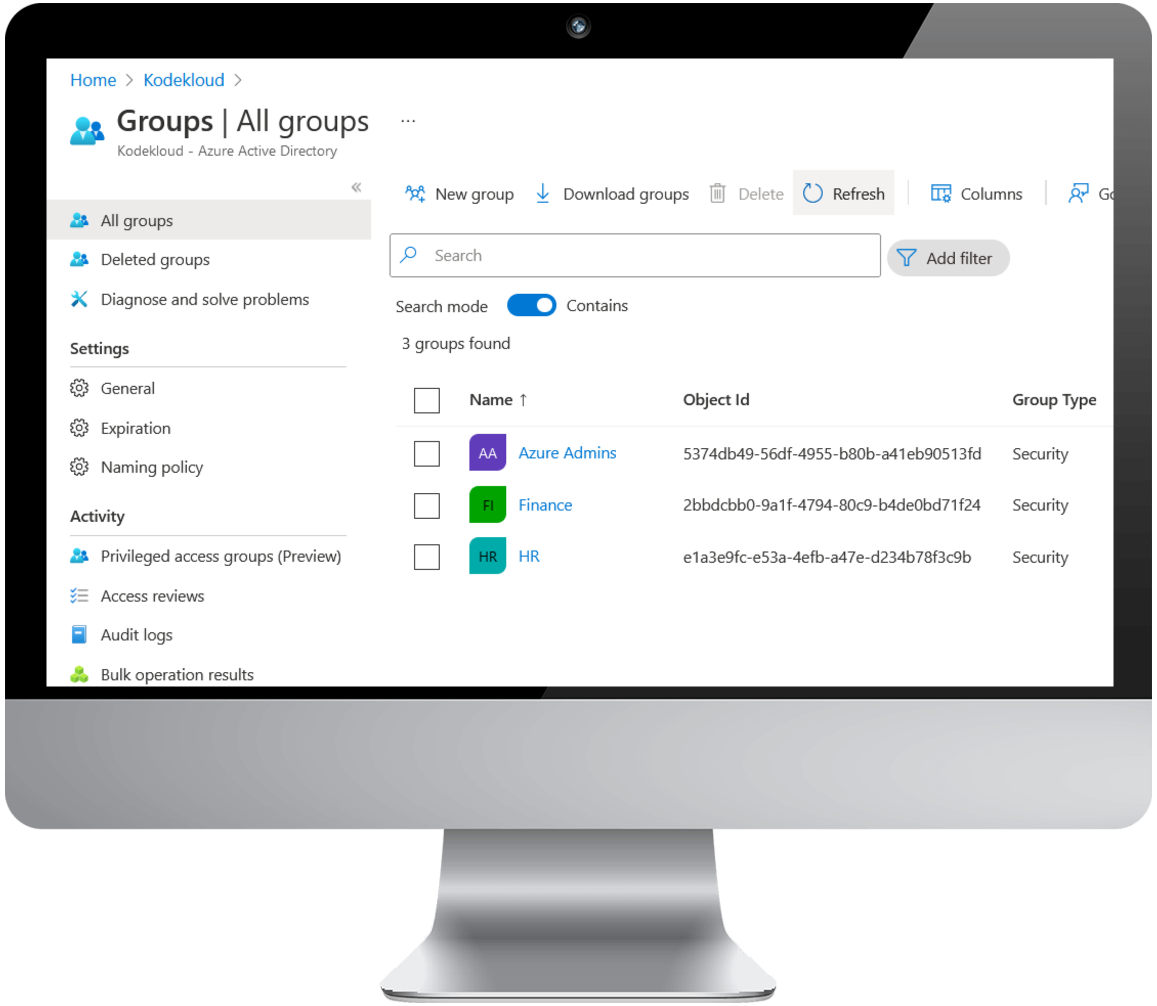
Kodekloud - Azure Active Directory

99 users found

	Name	User principal name	User type
□	AR Abigail Richards	a.richards@kodekloudl...	Member
□	AM Abraham Morgan	a.morgan@kodekloudla...	Member
□	AL Adam Lloyd	a.lloyd@kodekloudlabs....	Member
□	AW Adison Watson	a.watson@kodekloudla...	Member
□	AC Adrianna Craig	a.craig@kodekloudlabs....	Member
□	AP Aida Perkins	a.perkins@kodekloudla...	Member
□	AA Albert Alexander	a.alexander@kodeklou...	Member

Group Account

Group Accounts



Home > Kodekloud >

Groups | All groups ...

Kodekloud - Azure Active Directory

Search mode Contains

3 groups found

□	Name ↑	Object Id	Group Type
□	AA Azure Admins	5374db49-56df-4955-b80b-a41eb90513fd	Security
□	FI Finance	2bbdcbb0-9a1f-4794-80c9-b4de0bd71f24	Security
□	HR HR	e1a3e9fc-e53a-4efb-a47e-d234b78f3c9b	Security

Group Types

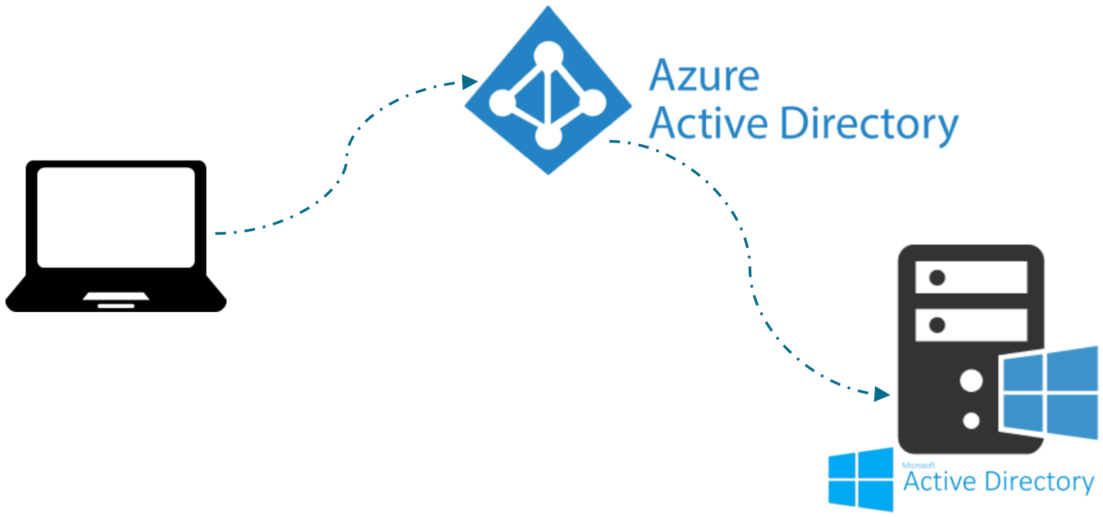
- Security groups
- Microsoft 365 groups

Assignment Types

- Assigned
- Dynamic user
- Dynamic device (only for Security group type)

Azure AD Join

Azure AD Join



Single sign-on

Single sign-on

Enable SSO for your apps, services, and SaaS solutions

Microsoft Store for Business

Access to Microsoft Store for Business

Publish your internal applications to Microsoft Store for Business for internal users.

Enterprise state roaming

Enterprise State Roaming

Synchronize your user settings and configuration across devices

Windows Hello

Windows Hello support

For supported Windows devices, users can use facial or biometric sign in.

Device Management

Device Management

Check device compliance and restrict access to applications

On-premises access

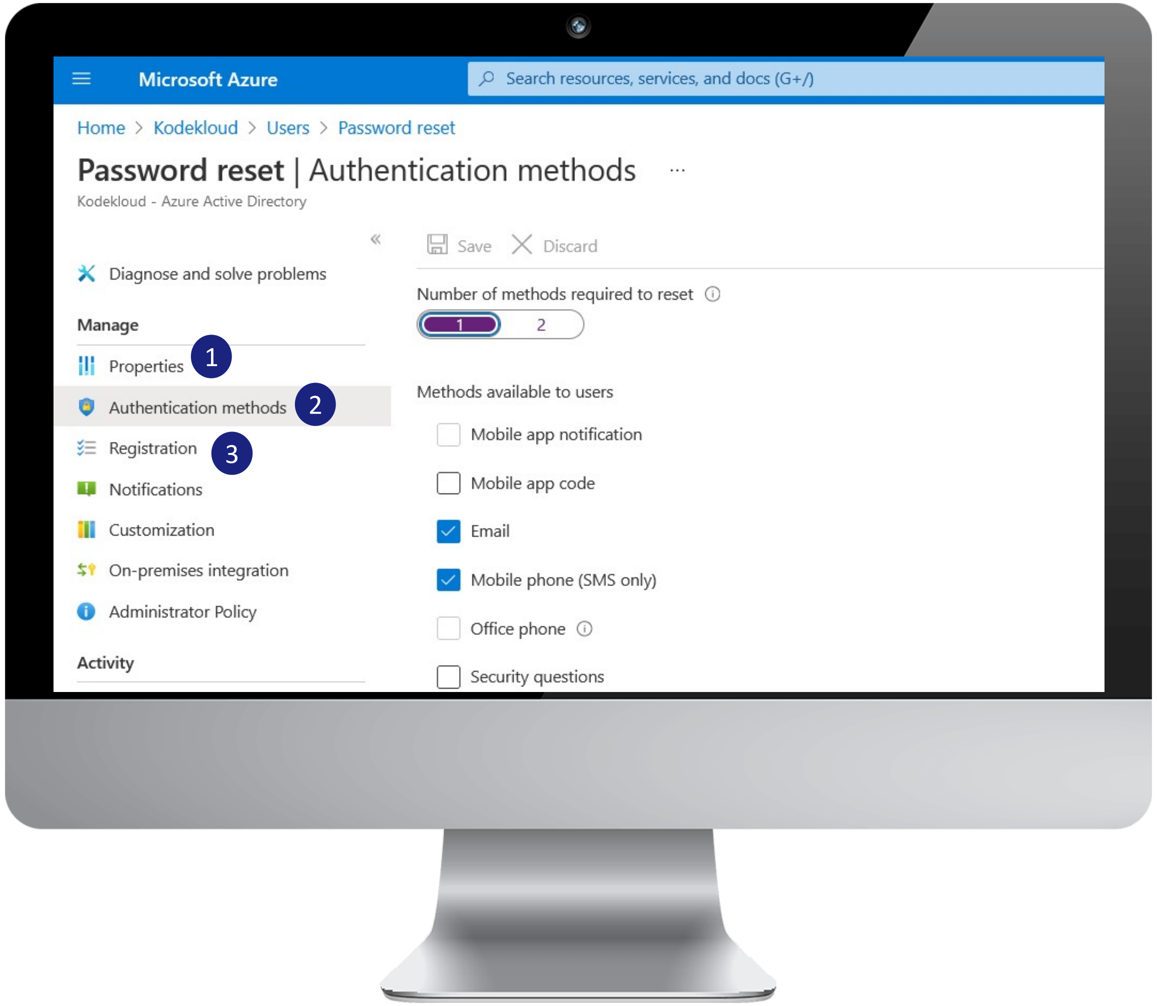
Access to on-prem apps

Enable seamless access to on-premises applications and resources.

Self service password reset (SSPR)

Self service password reset (SSPR)

- Enables users to reset password without the need to call IT helpdesk.
- Setup multiple methods for resetting the password.
- Requires Premium P2 license as this a premium feature.
- Target all users or a group of users and enable SSPR. For admin accounts, SSPR is enabled by default.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Kodekloud > Users > Password reset

Password reset | Authentication methods

Kodekloud - Azure Active Directory

Number of methods required to reset: [✓ 1] 2

Methods available to users

- □ Mobile app notification
- □ Mobile app code
- ☑ Email
- ☑ Mobile phone (SMS only)
- □ Office phone
- □ Security questions

1 **Step 1**

Enable SSPR for all users or for selected groups

2 **Step 2**

Setup the number of authentication methods requires for reset and the available methods

3 **Step 3**

Users will be requested to register for SSPR during next sign in where they can enable their reset method.

Multi tenant environments

Multi tenant environments

Relationship

Each Azure AD organization or tenant is fully independent. There is no parent-child relationship between these tenants. Each tenant will be considered as a separate entity.

Resource Independence

Creation or deletion of a resource in one tenant has no impact on any resource in another tenant.

Administration independence

The level of permissions of the user is only valid within the tenant. If a user is Global Administrator in one tenant and non-admin user in another tenant , that user will not have admin rights in the tenant where the user non-admin.

Synchronization independence

We can setup synchronization of account data for each Azure AD tenant independently.

KODEKLOUD

Managing Subscriptions

Azure Subscriptions

- Logical container that defines the billing boundary for the usage.
- Resources deployed in Azure will be mapped to an Azure subscription
- Subscriptions can also help in setting up environmental boundaries
- Every subscription will have a unique ID and it's called the subscription ID.

- An account can have multiple subscriptions.
- Identities that are part of Azure AD or an identity from any trusted Microsoft cloud service can sign up for a subscription
- There are different types of subscriptions based on the use case scenario.
- Subscription also act as a scope for access management.

Subscription offer types

Enterprise Agreements

Recommended for organizations with 500 or more users or devices that offers the cloud services and software licenses at discounted rates

Pay-as-you-go

Ideal for small organizations, where they don't have the budget to make upfront agreements

Cloud Solution Provider

Subscriptions licensed via Microsoft Partners, ideal for small to medium organizations. Billing is managed by the partner.

Free Trial

$200 credit for 30 days and free limited access for 12 months.

Azure for Students

Students are eligible for $100 credit for 12 months upon verification of student credentials

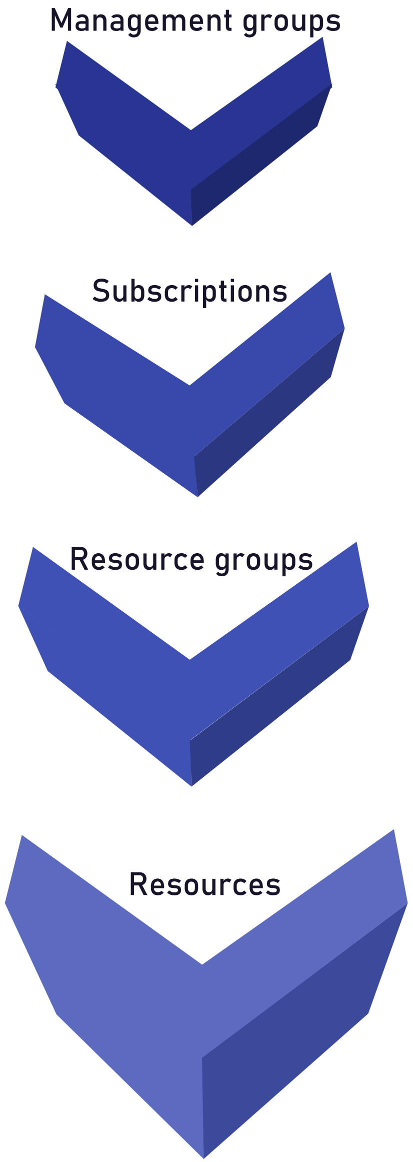
Visual Studio

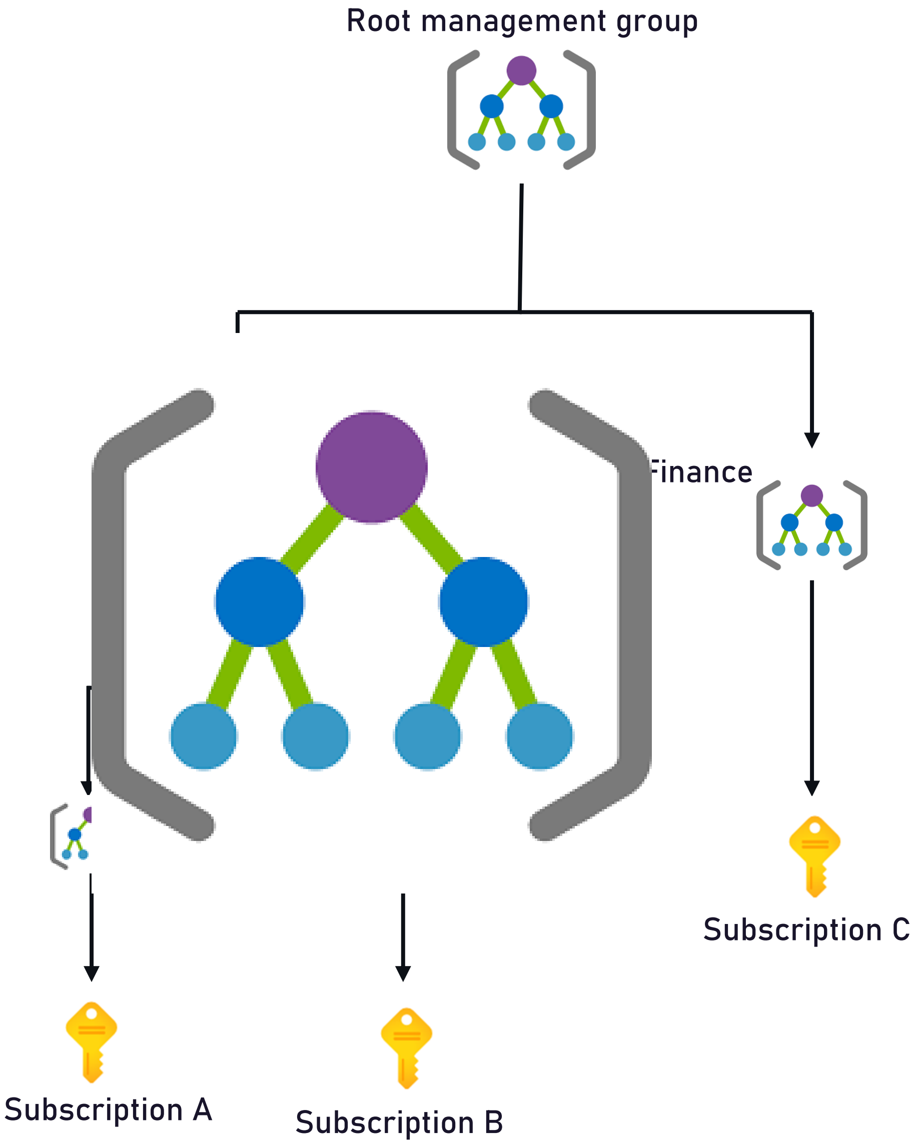
Credit based subscriptions offered to Visual Studio Professional and Enterprise subscribers.

Understanding the hierarchy

Understanding the hierarchy

- Management groups offers a scope above subscriptions by which you will be able to group subscriptions together.
- Root Management group is created by default, and you have up to 6 levels of nested groups excluding the root group.
- Each subscription will contain one or more resources groups for logically grouping resources like virtual machines, databases etc.
- Hierarchy helps in implementing policies, access and cost management

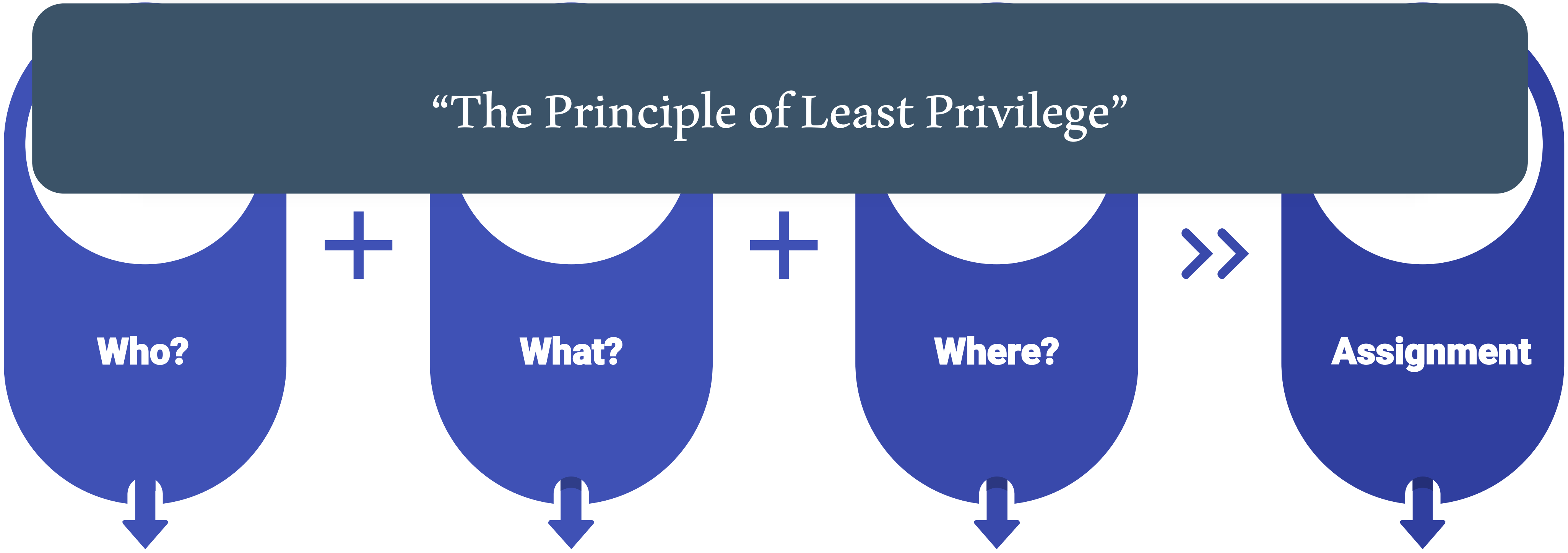




Working with Role Based Access Control

Role Based Access Control

Enables administrators to grant access to Azure resources and to segregate duties within the team.



“The Principle of Least Privilege”

Security Principal

Any identity which is requesting for access. It could be a user, group, service principal or managed identity.

Role Definition

Defines a set of operations that a particular role can perform. Written in JSON format.

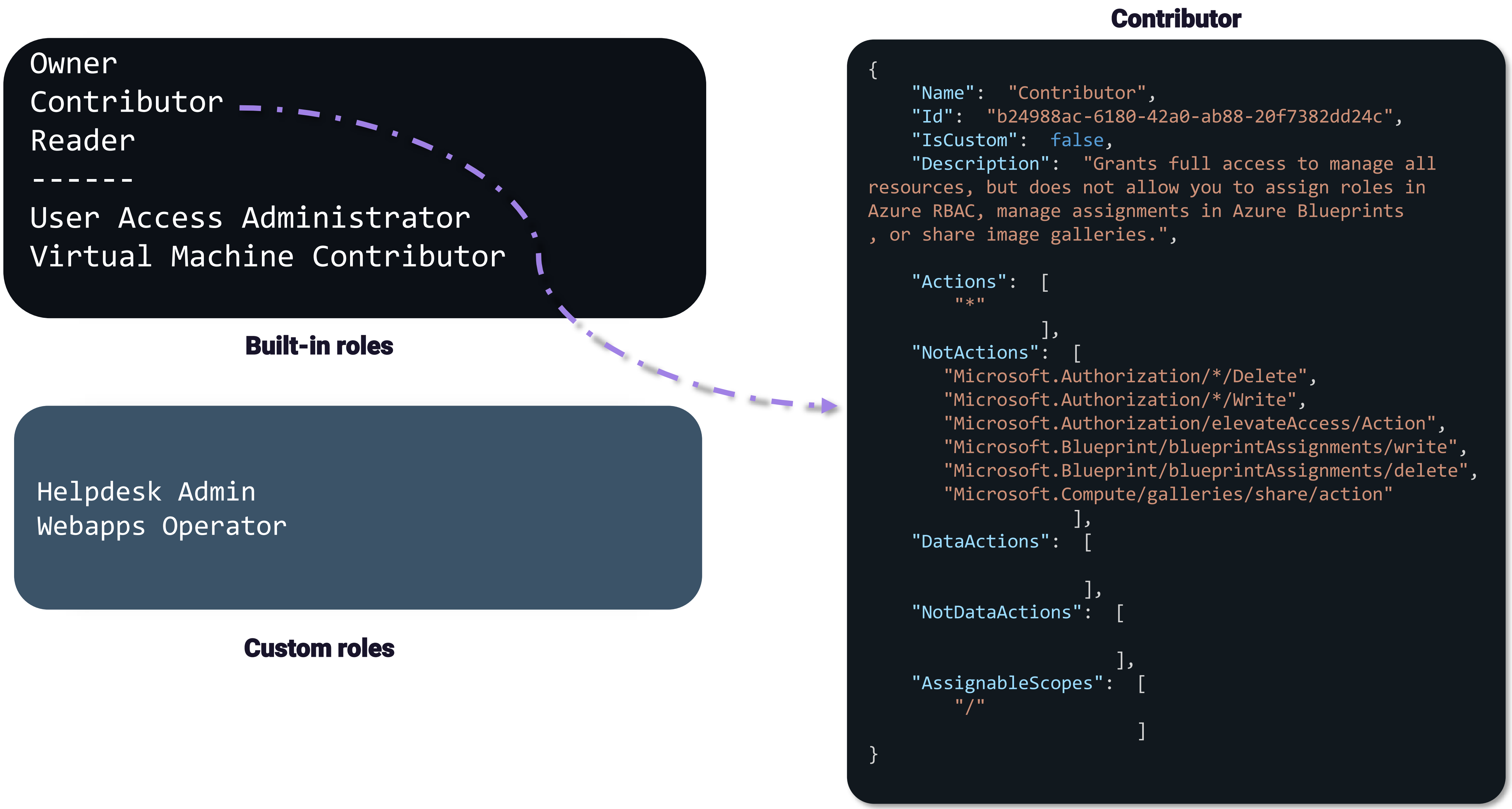
Scope

Limit of access, defines a boundary.

Role Assignment

When we attach a role definition to a service principal at a particular scope, then it becomes a role assignment. Max: 2000 in each subscription.

Role Definition



```
Owner
Contributor
Reader
------
User Access Administrator
Virtual Machine Contributor
```

Built-in roles

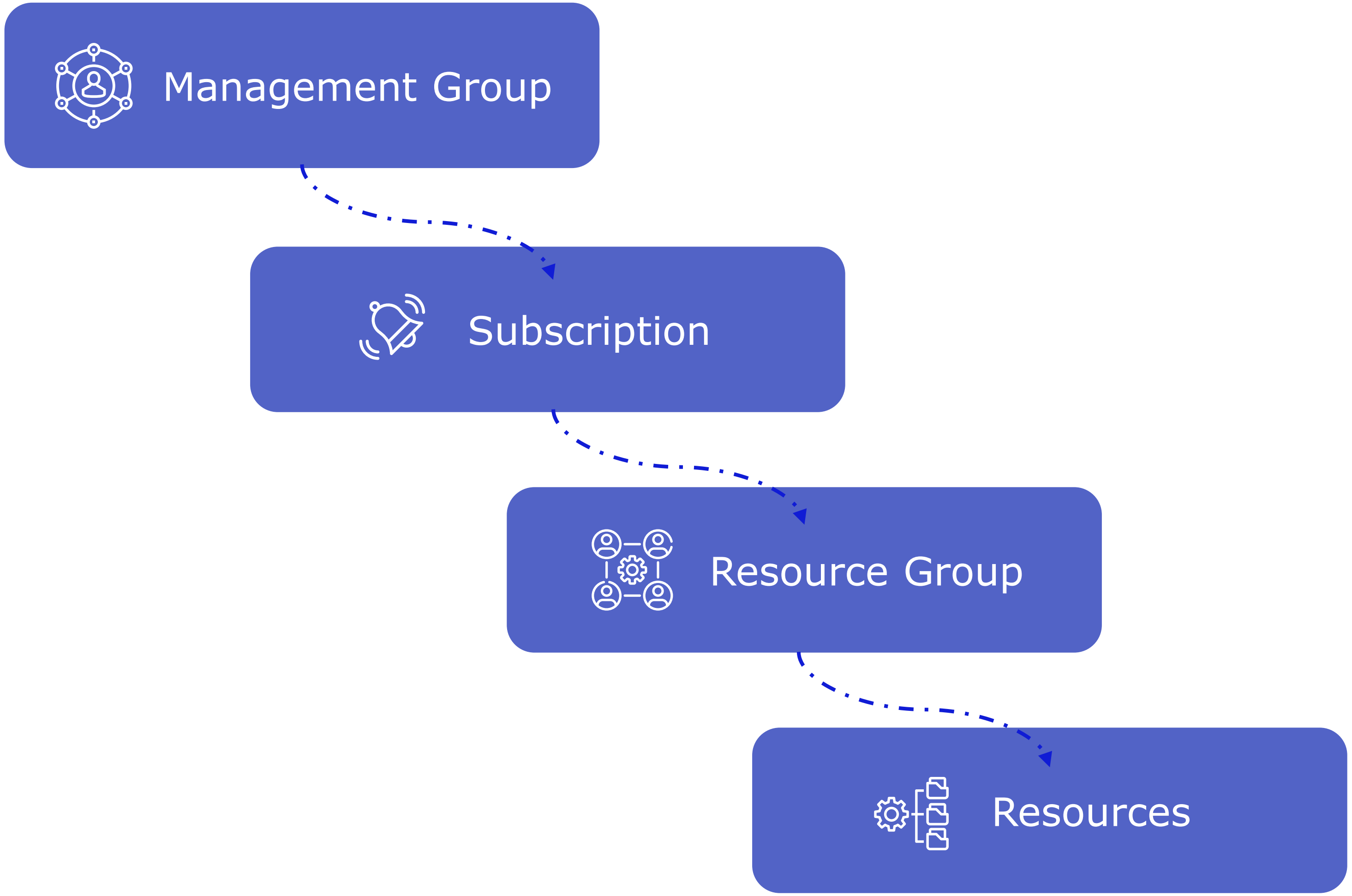
```
Helpdesk Admin
Webapps Operator
```

Custom roles

Contributor

```
{
    "Name":  "Contributor",
    "Id":  "b24988ac-6180-42a0-ab88-20f7382dd24c",
    "IsCustom":  false,
    "Description":  "Grants full access to manage all
resources, but does not allow you to assign roles in
Azure RBAC, manage assignments in Azure Blueprints
, or share image galleries.",

    "Actions":  [
        "*"
                ],
    "NotActions":  [
       "Microsoft.Authorization/*/Delete",
       "Microsoft.Authorization/*/Write",
       "Microsoft.Authorization/elevateAccess/Action",
       "Microsoft.Blueprint/blueprintAssignments/write",
       "Microsoft.Blueprint/blueprintAssignments/delete",
       "Microsoft.Compute/galleries/share/action"
                   ],
    "DataActions":  [

                    ],
    "NotDataActions":  [

                       ],
    "AssignableScopes":  [
        "/"
                         ]
}
```

Scope



Azure RBAC vs Azure AD Roles

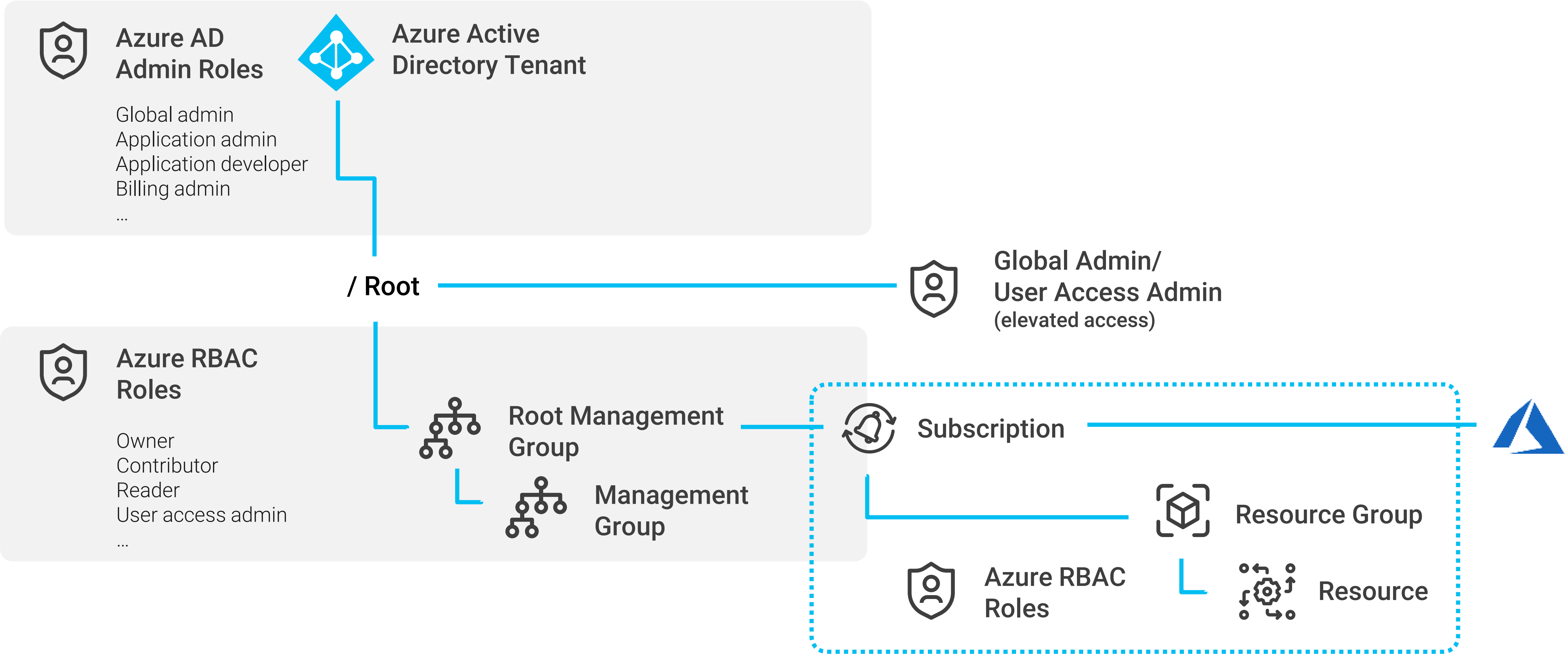
- Used to manage access to Azure resources
- Scopes include Management groups, Subscriptions, Resource Groups, and Resources
- Role assignments can be managed via Azure Portal, Azure PowerShell, Azure CLI, ARM templates, and REST API
- Example roles includes Owner, Contributor, Reader, User Access Administrator etc.

VS

COMPARISON

- Used to manage Azure AD features
- Scope is at the Azure AD tenant level
- Roles can be managed via Azure Portal, M365 Admin Portal, Microsoft Graph API, Azure AD and Graph PS module.
- Example roles includes Global Administrator, Billing Administrator, Global Reader etc.

Azure RBAC vs Azure AD Roles



Azure AD Admin Roles

Global admin
Application admin
Application developer
Billing admin
...

Azure Active Directory Tenant

/ Root

Global Admin/
User Access Admin
(elevated access)

Azure RBAC Roles

Owner
Contributor
Reader
User access admin
...

Root Management Group

Management Group

Subscription

Resource Group

Azure RBAC Roles

Resource

Image source: https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?WT.mc_id=modinfra-28824-socuff

Built-in-roles and Custom Roles

Built-in roles

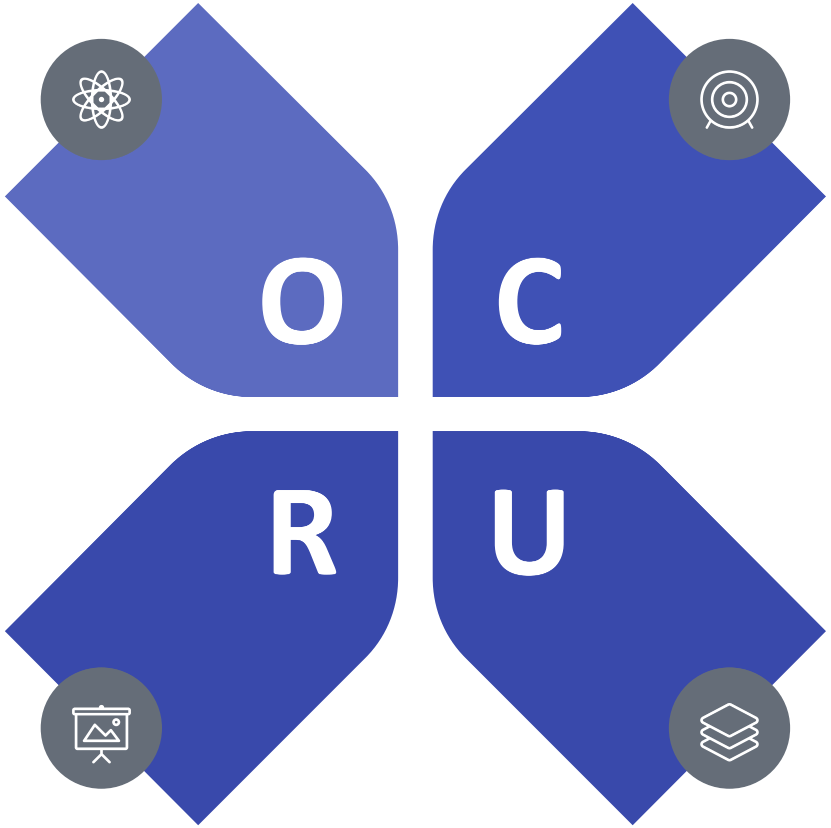
Built-in roles are roles offered by Azure which we can assign to users, groups, service principals, and managed identities. Following are the fundamental roles that you need to be aware of.

Owner

Full access to all resources and can delegate access to other users.

Contributor

Create and manage all types of resources, however, cannot grant access to others.



Reader

Read access to all resources, no permission to make changes to the resources.

User Access Administrator

User access to Azure resources can be managed using this role.

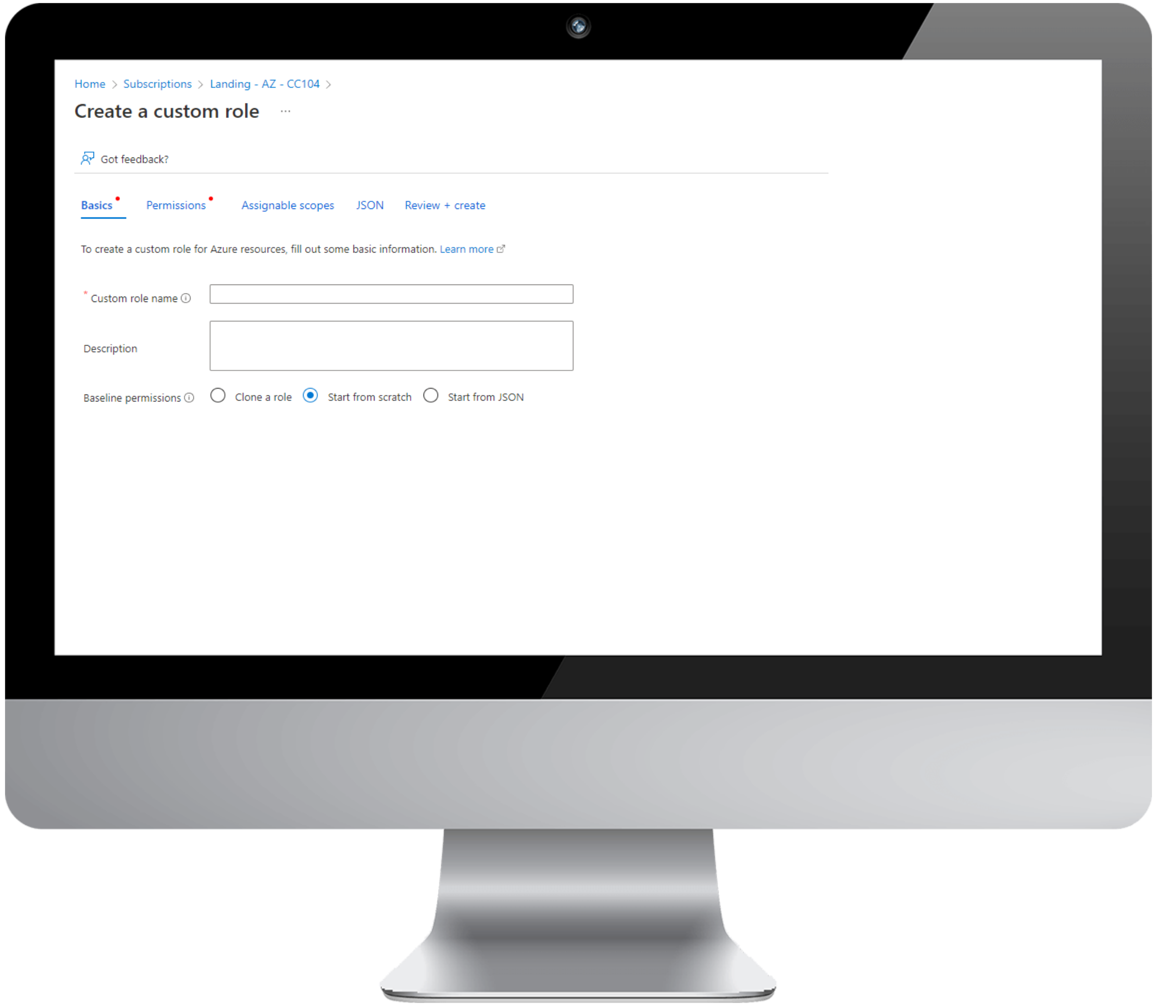
Custom RBAC Roles

Custom RBAC roles can be used to create fine tuned roles for your environment, if the built-in roles doesn't meet your specific needs

Custom roles can be created from Azure Portal, Azure PowerShell, Azure CLI and REST API

Each directory can have up to 5000 custom roles

We can assign custom roles to users, groups, and service principals to any scope; same way we work with built-in roles.



Home > Subscriptions > Landing - AZ - CC104 >

Create a custom role ···

Got feedback?

Basics* | Permissions* | Assignable scopes | JSON | Review + create

To create a custom role for Azure resources, fill out some basic information. Learn more

* Custom role name ⓘ

Description

Baseline permissions ⓘ ○ Clone a role ● Start from scratch ○ Start from JSON

Multi tenant Managing access using Azure Portal

Azure Tags

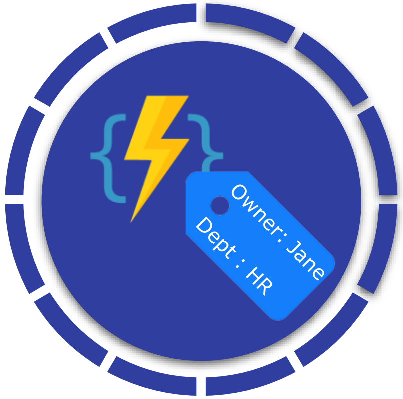
Azure Tags

Adding metadata

Using tags we can add metadata to our subscription, resource groups, and resources

Logical grouping

With tags, we can logically filter our resources for management purposes



Name-value pair

Tags uses a name value pair. Tag name is limited to 512 characters and tag value is limited to 256 character. Maximum number of tags we can assign is limited to 50.

Cost Management

Tags can be used to filter Azure usage and cost management. The tags added to resources will be propagated to Azure Billing system.

⚠ *Tags doesn't follow inheritance by default, we can use Azure Policy to inherit tags from resource group or subscription.*

Resource Locks

Resource Locks

Avoids accidental changes

With the help of resource locks, we can protect our resources from accidental changes or deletion.

Inheritance

Locks can be applied at the subscription, resource group, and resource level. The lock will inherit to the lower scopes.

Read-only locks

Resources with read-only locks cannot be modified and this will prevent any changes to the resource.

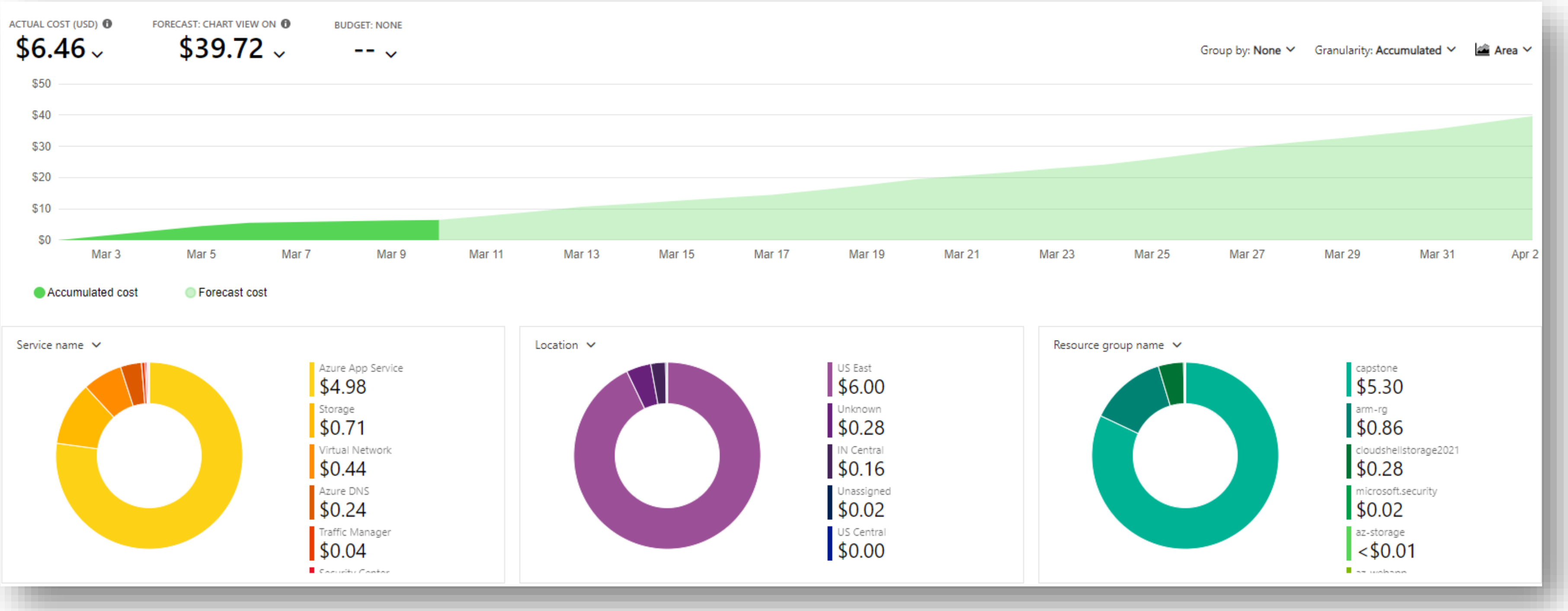
Delete locks

Resources with delete lock can be modified, however, they cannot be deleted. Ideal for resources which you would like to modify and at the same time, prevent accidental deletion.

.

Analyzing costs

Analyzing costs



ACTUAL COST (USD) $6.46

FORECAST: CHART VIEW ON $39.72

BUDGET: NONE --

Group by: None · Granularity: Accumulated · Area

Service name	
Azure App Service	$4.98
Storage	$0.71
Virtual Network	$0.44
Azure DNS	$0.24
Traffic Manager	$0.04

Location	
US East	$6.00
Unknown	$0.28
IN Central	$0.16
Unassigned	$0.02
US Central	$0.00

Resource group name	
capstone	$5.30
arm-rg	$0.86
cloudshellstorage2021	$0.28
microsoft.security	$0.02
az-storage	<$0.01

Cost Analysis

We can analyze the current spending and see cost forecast. We can also connect our AWS cost to Azure Cost Management

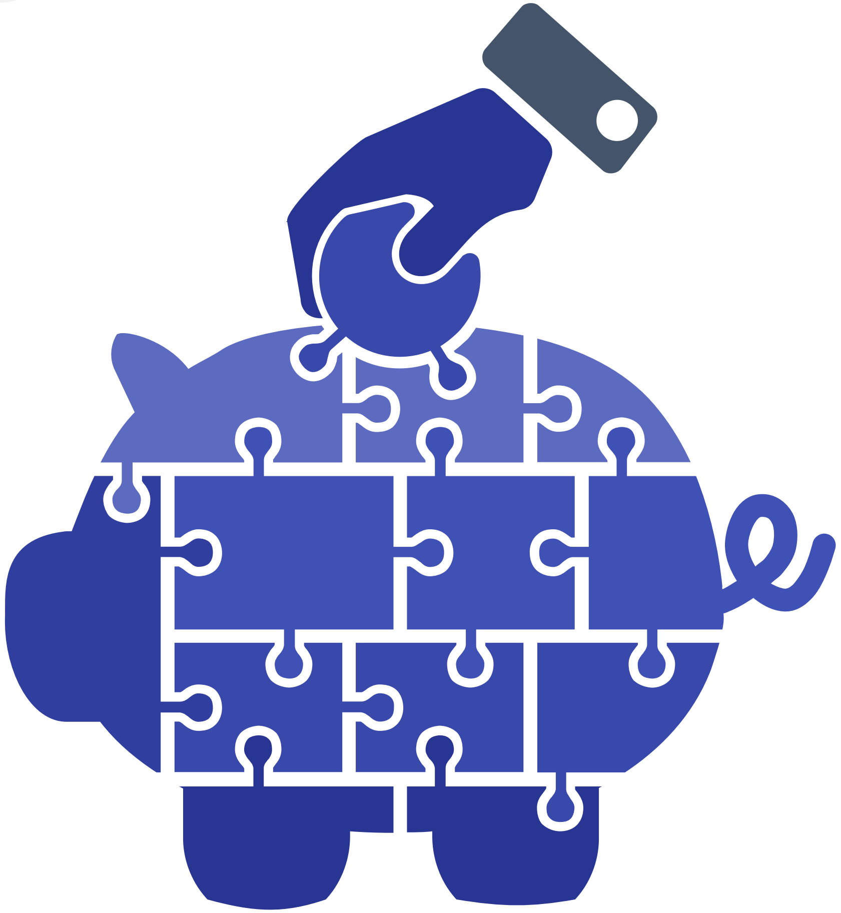
Budgets and Recommendations

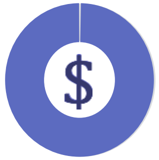
Using Cost Management, we can define fine tuned budgets targeting specific scopes and further narrow it down using filters. We can also generate cost related recommendations.

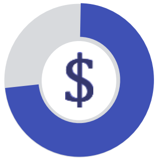
Export data

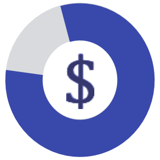
We can export our cost data to a storage account in Azure. The data can be exported as a one-time export or a recurring export which works based on the schedule we define.

Cost savings









✓ Azure Reserved Instances (RI)

For instances that are planned for long term and is running 24x7 can be reserved. Reservations can be purchased for 1 year or 3 year with upfront payment or equated monthly payments.

✓ Azure Hybrid Benefit (AHUB)

You can purchase Windows and SQL licenses from Software Assurance can use with your Azure VMs and PaaS services. AHUB is cheaper than PAYG licensing cost

✓ Credits

Credit based subscriptions such Visual Studio Enterprise, Visual Studio Professional, MPN could provide you monthly credits that can be used for testing and developing solutions on Azure.

✓ Regions

In Azure, every region has a different pricing. When you deploying resources, choose low-cost regions. While selecting low-cost regions, make sure you are not comprising the compliance or performance of your workloads.

Azure Policy

Azure Policy

Helps us to create, manage, and assign policies. Policies can be used to define organizational standards and identify non-compliant resources

Definition

Policy definition is a JSON document which is used to define the policy and its effect. Azure has built-in policies that we can use, or you can write your own custom policies

Assignment

Assignment is the process assigning a policy definition to a scope. Once it's assigned policy enforcement is done.

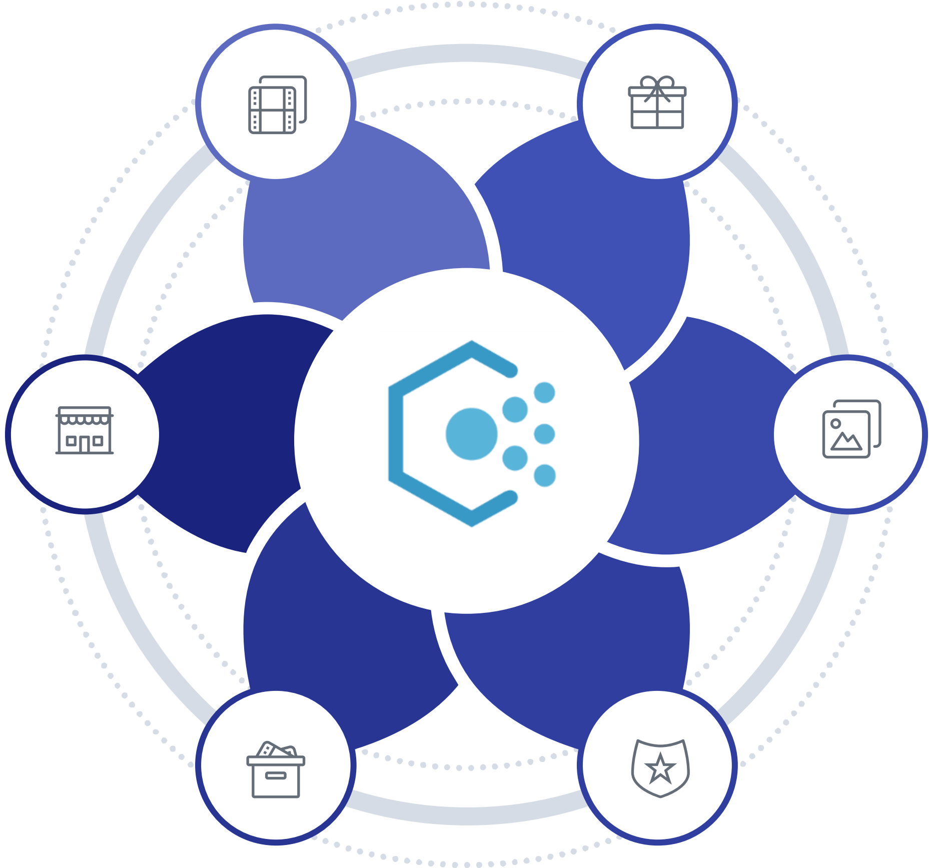
Scope

Like RBAC, we must specify the scope to which we want to enforce the policy. We can scope to management group, subscription, or to resource group.

Compliance

After assigning the policy, we can evaluate the compliance to understand compliant and non-compliant resources.

Azure Policy – Use cases



Allowed resources types
Defines a set of resources that can be created in the selected scope

Allowed virtual machine SKUs
Defines a set of VM SKUs that can be deployed.

Allowed locations
Defines a set of cloud locations where we can deploy resources.

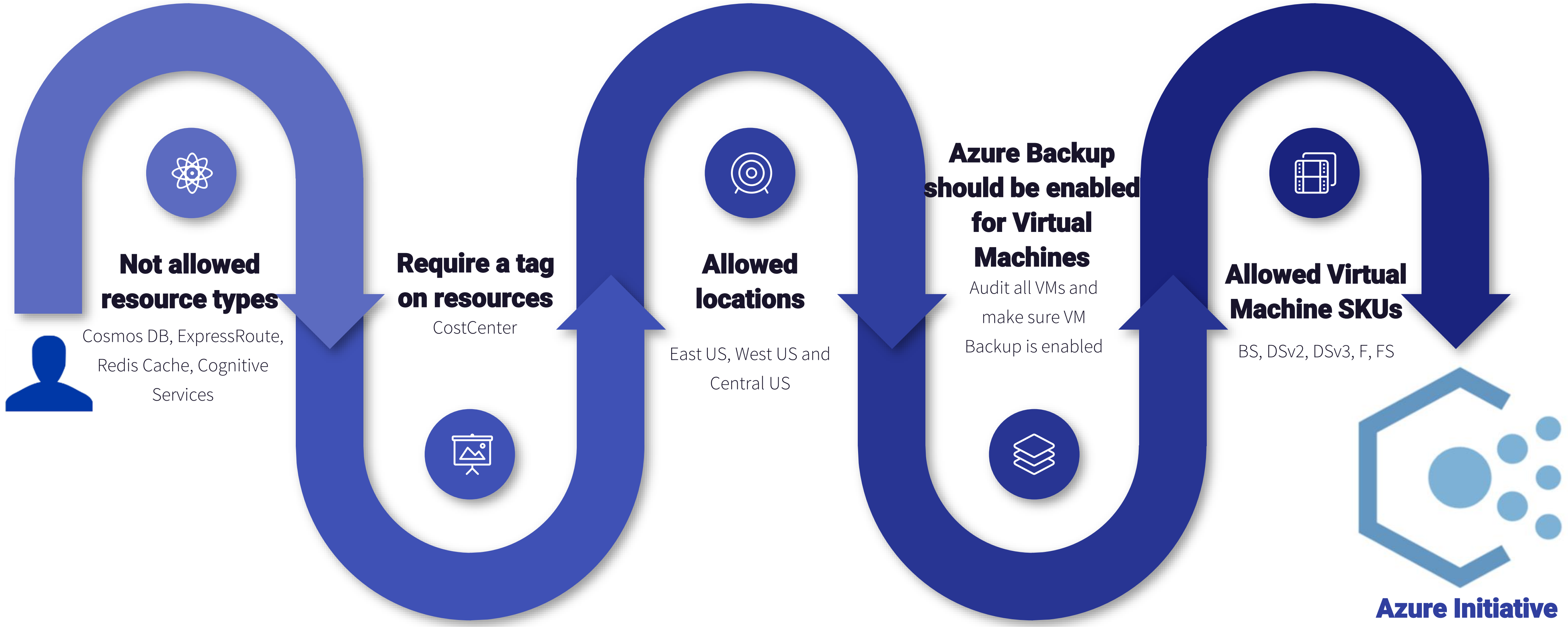
Require tags
Enforce tags that needs to be added to the resources

Inherit tags
Inherit tags from subscription or resource group

Allowed resource group locations
List of locations where you can create resource groups.

Initiative

Chaining policy definitions so that they can assigned as single item and the compliance can be evaluated



Not allowed resource types

Cosmos DB, ExpressRoute, Redis Cache, Cognitive Services

Require a tag on resources

CostCenter

Allowed locations

East US, West US and Central US

Azure Backup should be enabled for Virtual Machines

Audit all VMs and make sure VM Backup is enabled

Allowed Virtual Machine SKUs

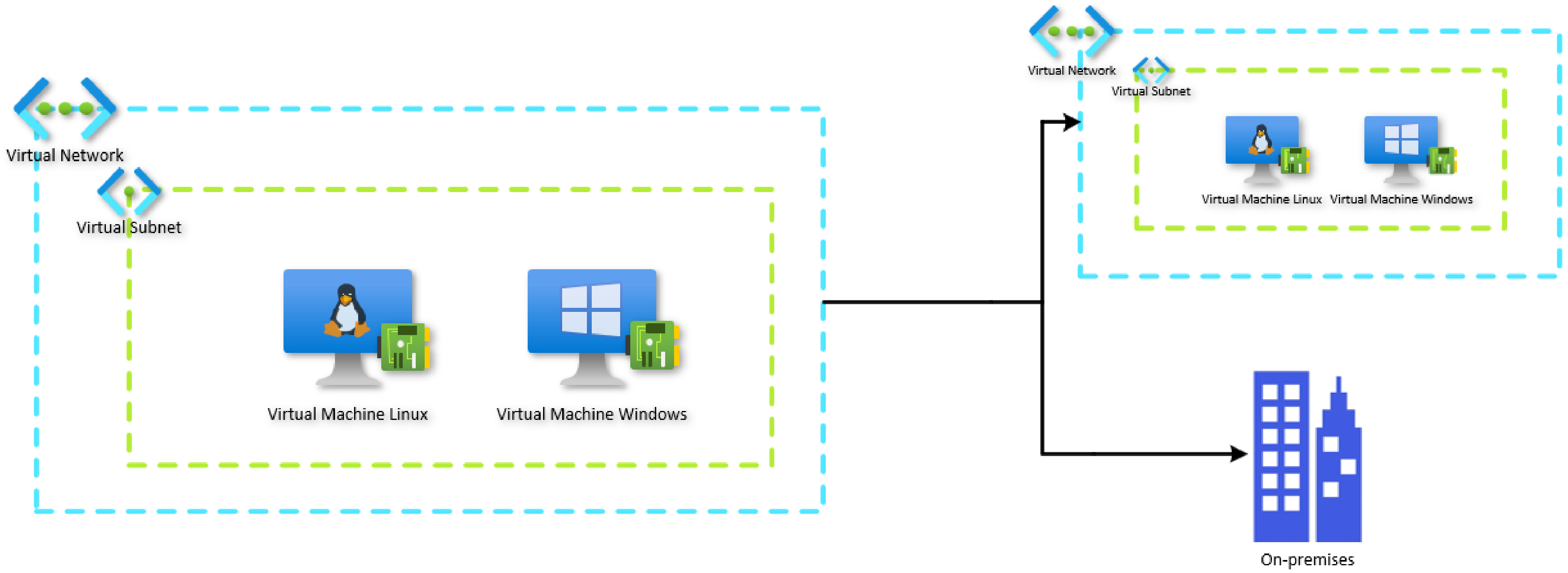
BS, DSv2, DSv3, F, FS

Azure Initiative

KODEKLOUD

Creating and configuring virtual networks

Virtual Networks



Representation of cloud network

Logical representation of your network in the cloud. Azure Virtual Networks (VNets) helps us to create and manage networking in Azure

Dedicated instance

Every VNet instance in Azure is private and dedicated

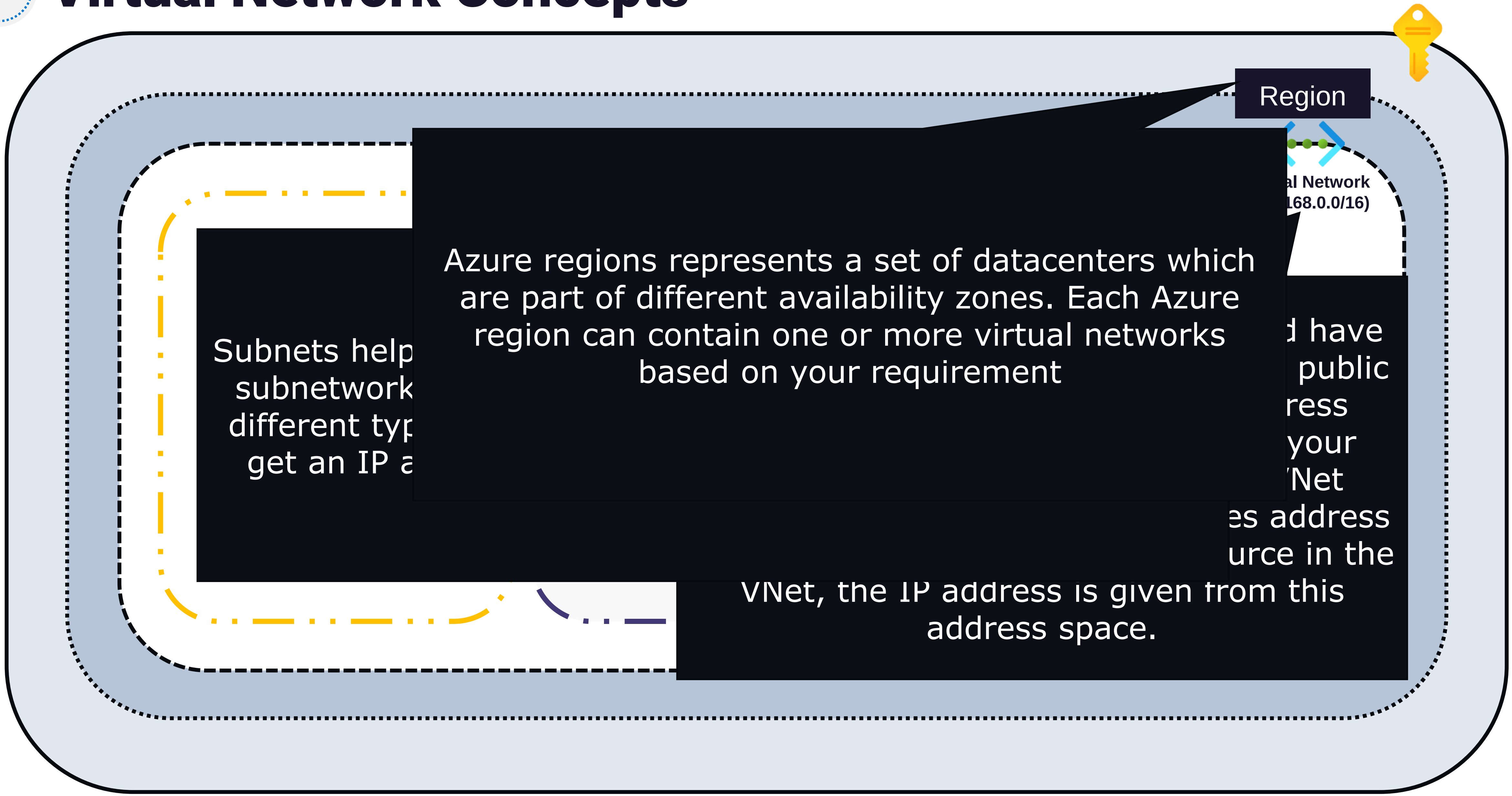
Hybrid scenarios

With the help of VNets, we can extend our communication to on-premises datacenters and other cloud providers securely.

Connectivity between Azure services

Virtual Network is responsible for facilitating connectivity between Azure Virtual Machines and other Azure services. Also, enables Azure VMs to connect to Internet.

Virtual Network Concepts



Region

Azure regions represents a set of datacenters which are part of different availability zones. Each Azure region can contain one or more virtual networks based on your requirement

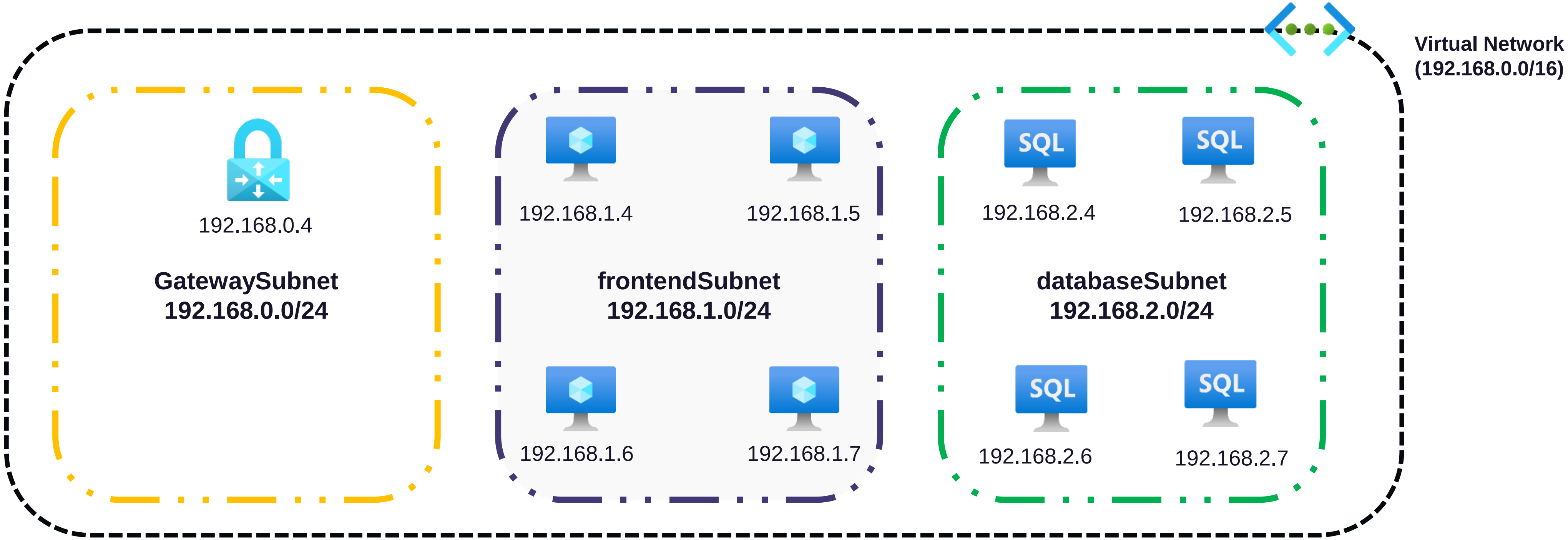
Subnets help
subnetwork
different typ
get an IP a

d have
public
ress
your
'Net
es address
urce in the
VNet, the IP address is given from this
address space.

Private and Public IP addresses

Private IP addresses

Used within Azure Virtual Network, and with hybrid scenarios involving VPN Gateways and ExpressRoute connections



Allocation methods

Static

Helps in setting up static IP address for domain controllers, web servers and DNS servers which do not change even if the servers are rebooted. Also used with services such internal LBs and Application Gateways.

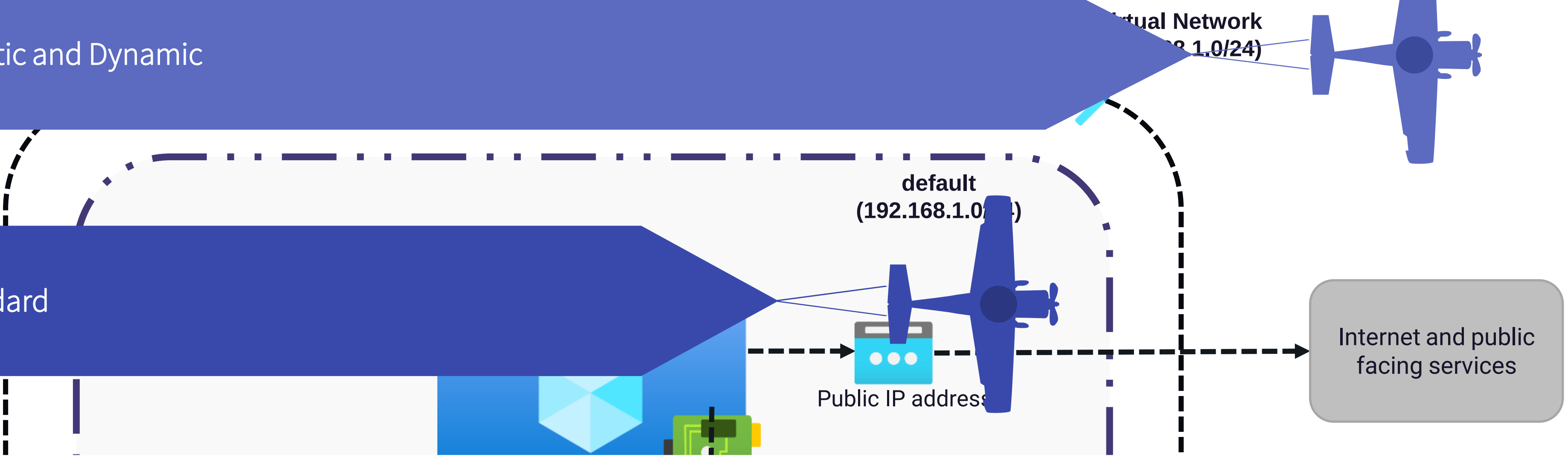
Dynamic

This is the default option, where the IP address is dynamically allocated from the address pool. If you restart a server and if the previous IP address is not available, Azure will assign another available IP address from the address space.

Public IP addresses

Allocation types : Static and Dynamic

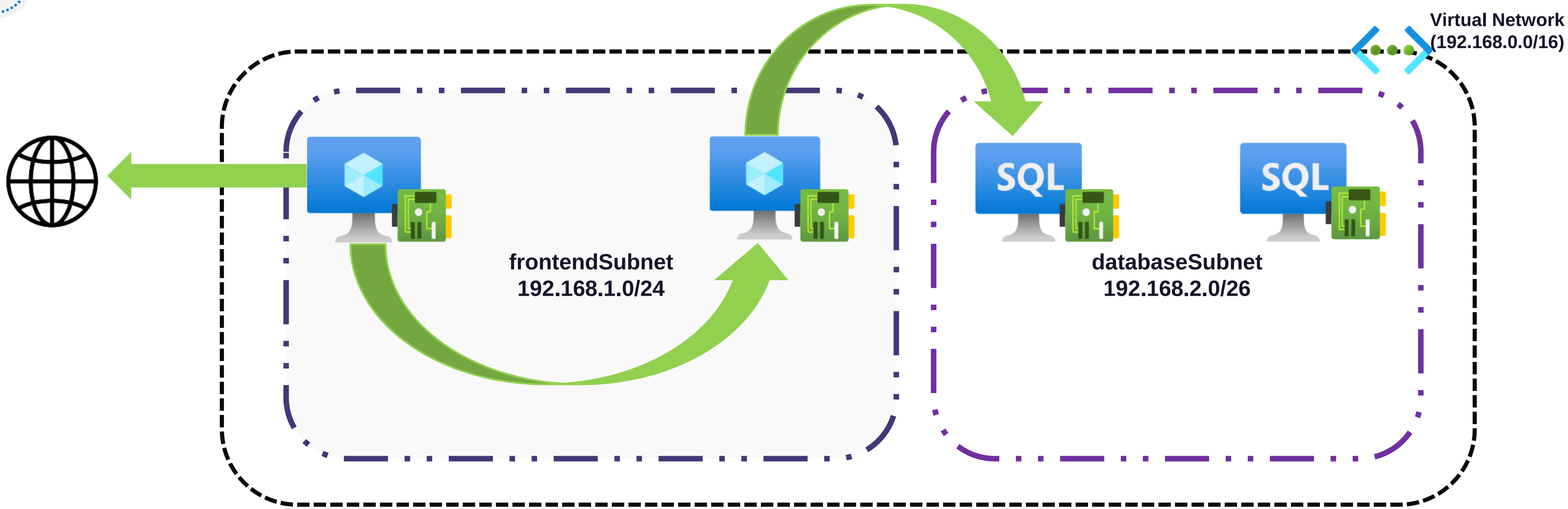
SKU: Basic and Standard



Feature	Basic SKU	Standard SKU
IP Allocation	Static/Dynamic	Static
Security	By default, open	By default, closed
Resources	Virtual Machine NIC, VPN Gateways, Public Load Balancers, Application Gateways	Virtual Machine NIC, Public Load Balancers, Application Gateways
Redundancy	No zone redundancy	Zone redundant

User Defined Routes

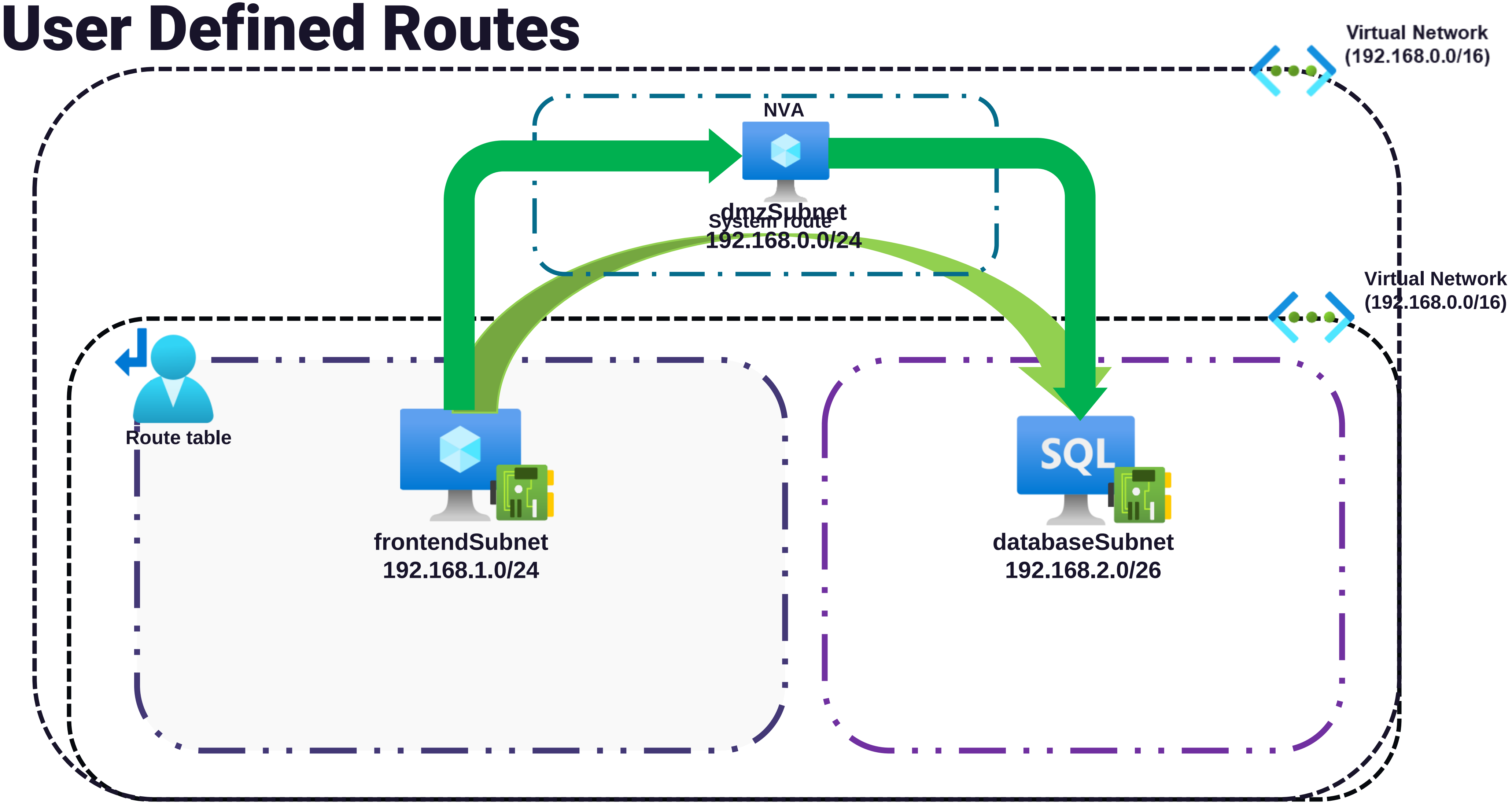
User Defined Routes



System routes

- Communication between VMs in the same subnet
- Communication between VMs in different subnets in the same virtual network.
- Communication from VM to the Internet
- Communication via Site-to-Site and ExpressRoute connection while using VPN gateways

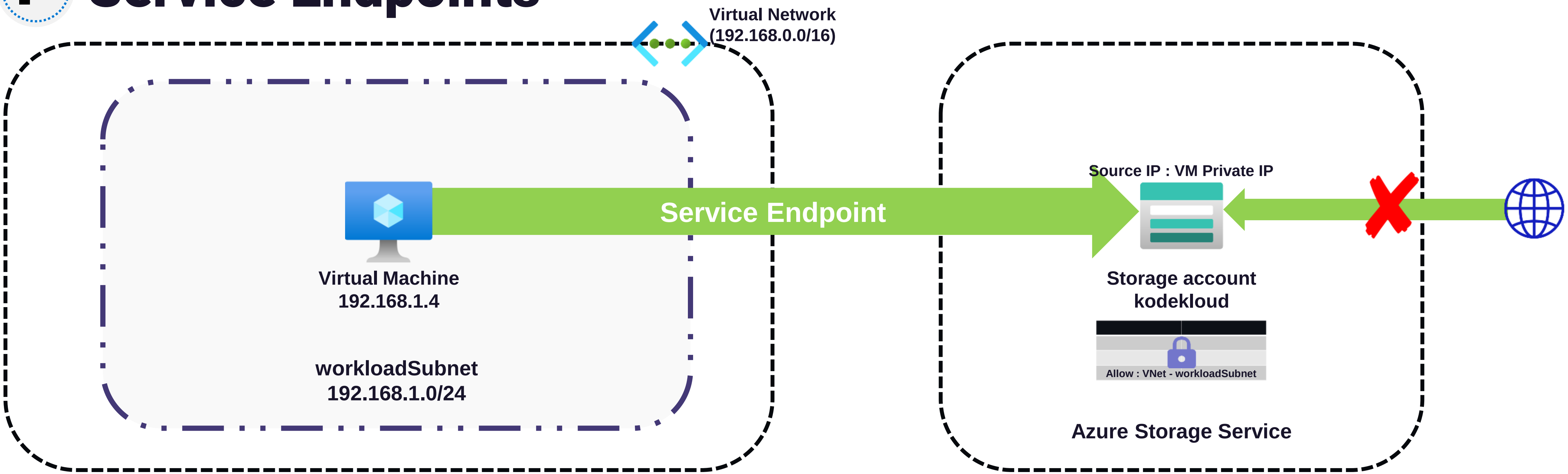
User Defined Routes



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

Service Endpoints

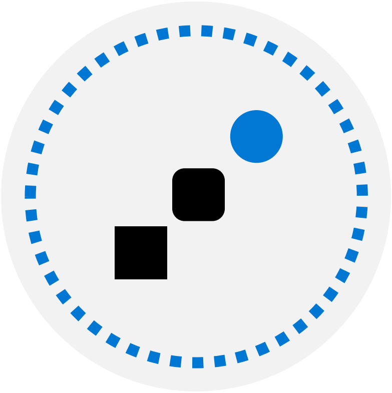
Service Endpoints



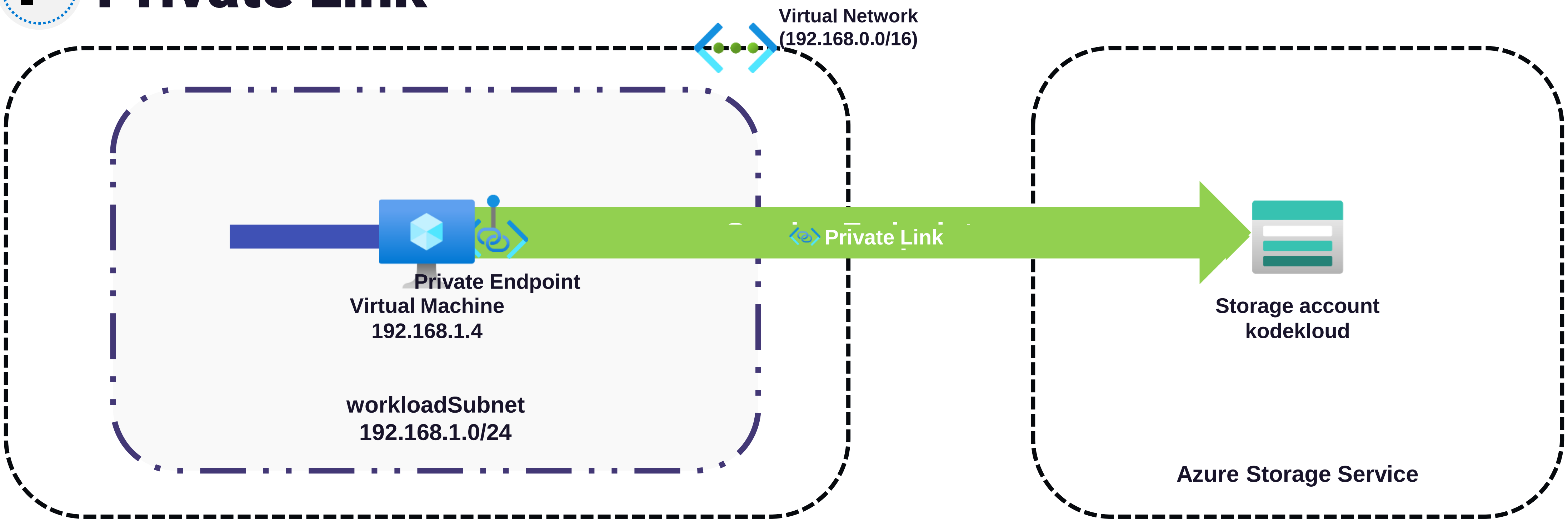
Benefits

- Access Azure services with better security
- Leverages Microsoft backbone network
- Ease of setup and management
- Supported services include Azure Storage, Azure SQL Database, Azure Synapse Analytics, Azure Database for PostgreSQL server, Azure Database for MySQL server, Azure Database for MariaDB server, Azure Cosmos DB, Azure Key Vault, Azure Service Bus, Azure Event Hubs, ADLS Gen1, Azure App Service, Azure Cognitive Services, and Azure Container Registry (preview)

Private Link



Private Link

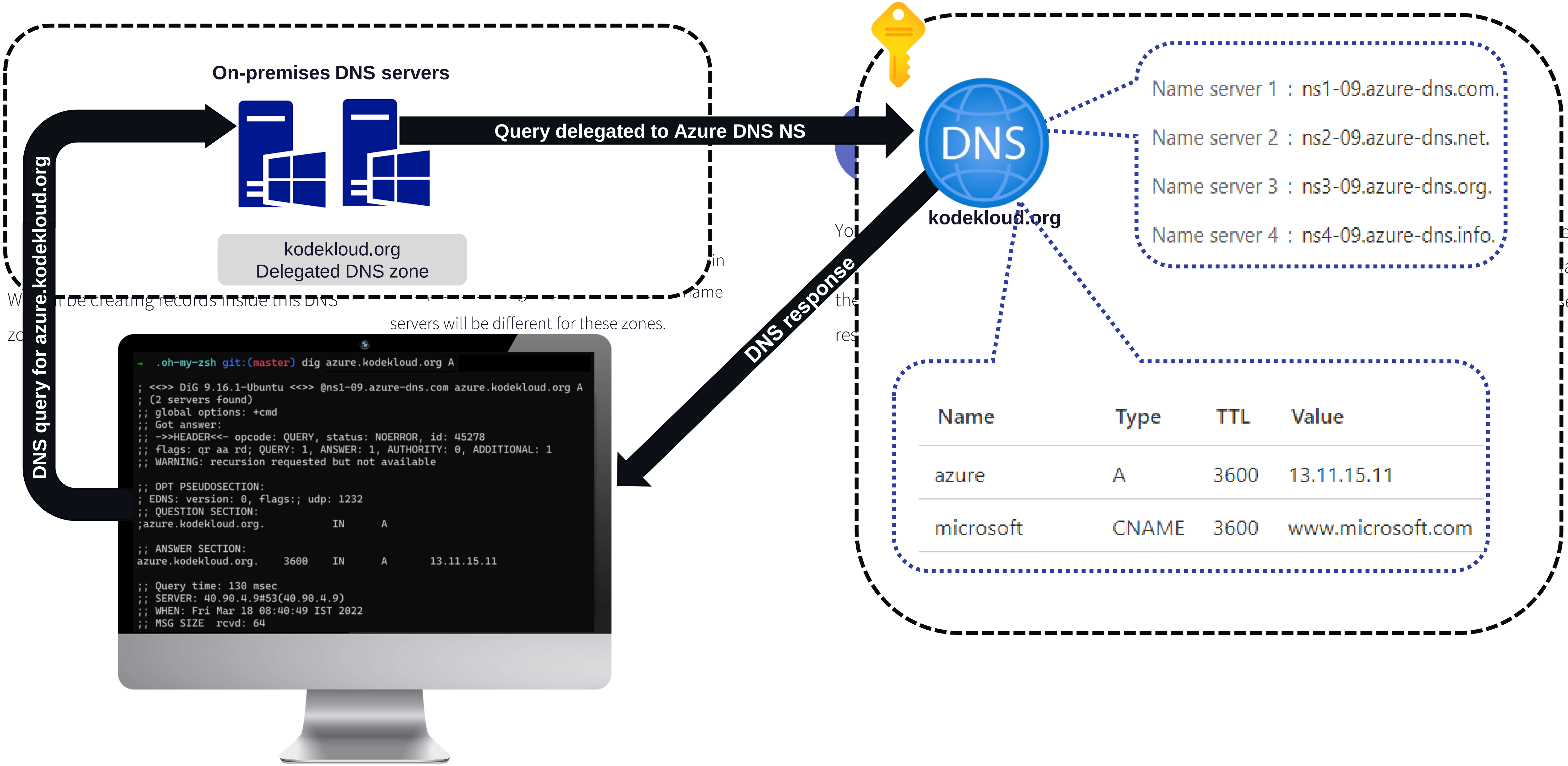


Benefits

- Connect to Azure services via private connection
- Seamless integration with on-premises and peered networks
- Eliminates risk of data exfiltration
- Direct availability in Azure VNets

Azure DNS

Azure DNS


On-premises DNS servers
Query delegated to Azure DNS NS
kodekloud.org
Delegated DNS zone
DNS query for azure.kodekloud.org
DNS response
DNS
kodekloud.org
W   t be creating records inside this DNS
zo
in
name
servers will be different for these zones.
Yo
the
res
e are
aximum
et is 20

Name server 1 : ns1-09.azure-dns.com.

Name server 2 : ns2-09.azure-dns.net.

Name server 3 : ns3-09.azure-dns.org.

Name server 4 : ns4-09.azure-dns.info.

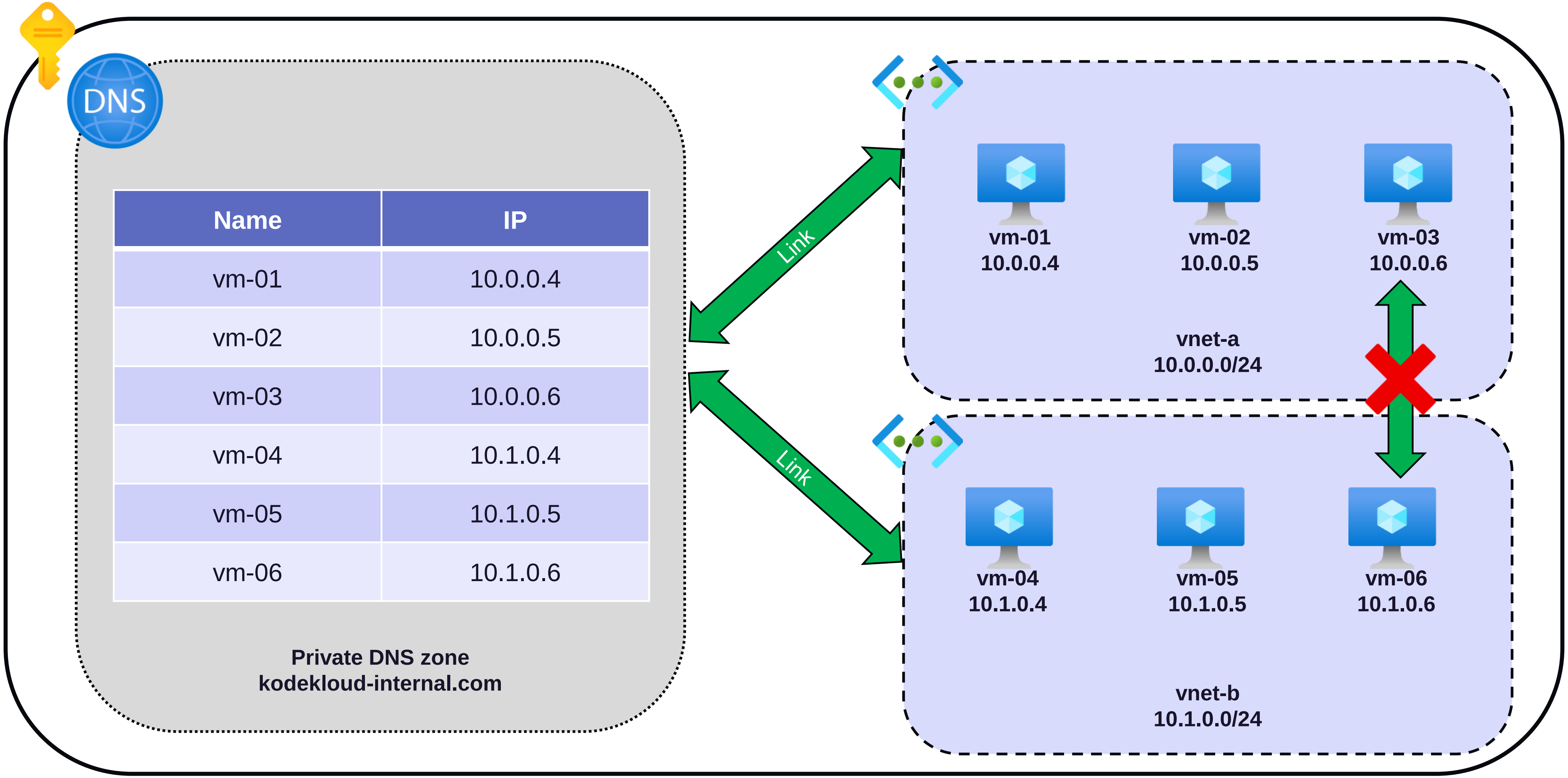
Name	Type	TTL	Value
azure	A	3600	13.11.15.11
microsoft	CNAME	3600	www.microsoft.com

```
→  .oh-my-zsh git:(master) dig azure.kodekloud.org A

; <<>> DiG 9.16.1-Ubuntu <<>> @ns1-09.azure-dns.com azure.kodekloud.org A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45278
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;azure.kodekloud.org.           IN      A

;; ANSWER SECTION:
azure.kodekloud.org.    3600    IN      A       13.11.15.11

;; Query time: 130 msec
;; SERVER: 40.90.4.9#53(40.90.4.9)
;; WHEN: Fri Mar 18 08:40:49 IST 2022
;; MSG SIZE  rcvd: 64
```

Private zones

Private DNS zones

Name resolution for services deployed in Azure Virtual Network



Name	IP
vm-01	10.0.0.4
vm-02	10.0.0.5
vm-03	10.0.0.6
vm-04	10.1.0.4
vm-05	10.1.0.5
vm-06	10.1.0.6

Private DNS zone
kodekloud-internal.com

Link

Link

vm-01
10.0.0.4

vm-02
10.0.0.5

vm-03
10.0.0.6

vnet-a
10.0.0.0/24

vm-04
10.1.0.4

vm-05
10.1.0.5

vm-06
10.1.0.6

vnet-b
10.1.0.0/24

Network Security Groups

Network Security Groups

Filter traffic

NSG operate at layer 4 and allows us to filter the incoming and outgoing traffic from a virtual network

Rule set

NSG comprises a set of priority-based rules that can be used to allow or deny inbound or outbound traffic.

Association

NSGs can be associated to subnets and network interfaces. You can associate multiple subnets and network interfaces to a single NSG.

Evaluation

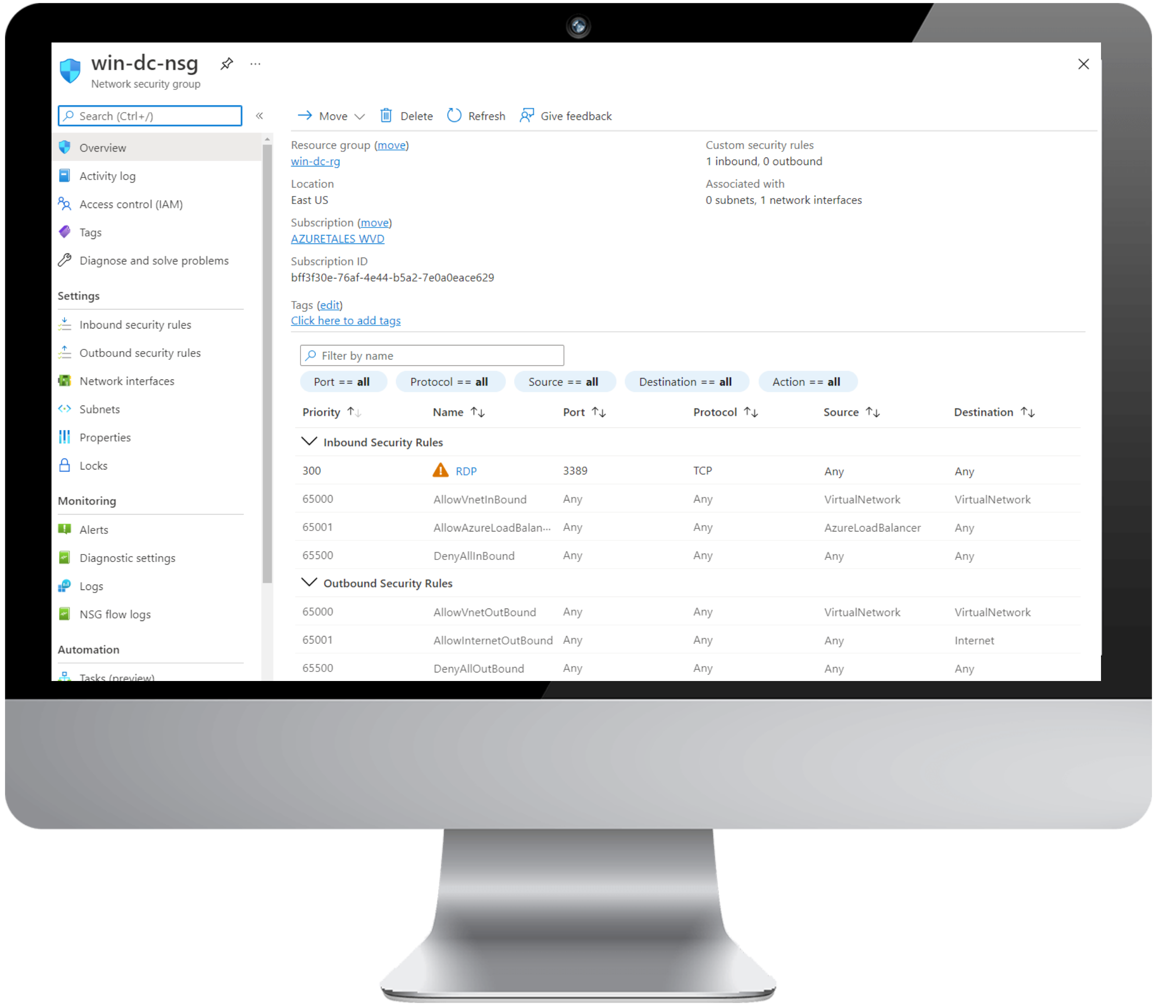
Rules applied at subnet and network interface level is evaluated separately. Traffic requires “allow” rule at both levels to be admitted.

.

Network Security Group Rules

Rules are evaluated based on the priority. There is a set of default rules which cannot be modified or deleted. Nevertheless, we can override these rules by creating rules with higher priority. Rules can be created based on the following attributes besides the IP details:

- Service: You can choose custom or predefined services such as HTTP, HTTPS, RDP, SSH etc to allow the respective ports.
- Port range: You can configure ports or a port range.
- Priority: Lower the number higher the priority. Values range from 100-4096. Values in 65000 range is for default rules.
- Action: Allow or Deny



Resource group (move)
win-dc-rg

Location
East US

Subscription (move)
AZURETALES WVD

Subscription ID
bff3f30e-76af-4e44-b5a2-7e0a0eace629

Tags (edit)
Click here to add tags

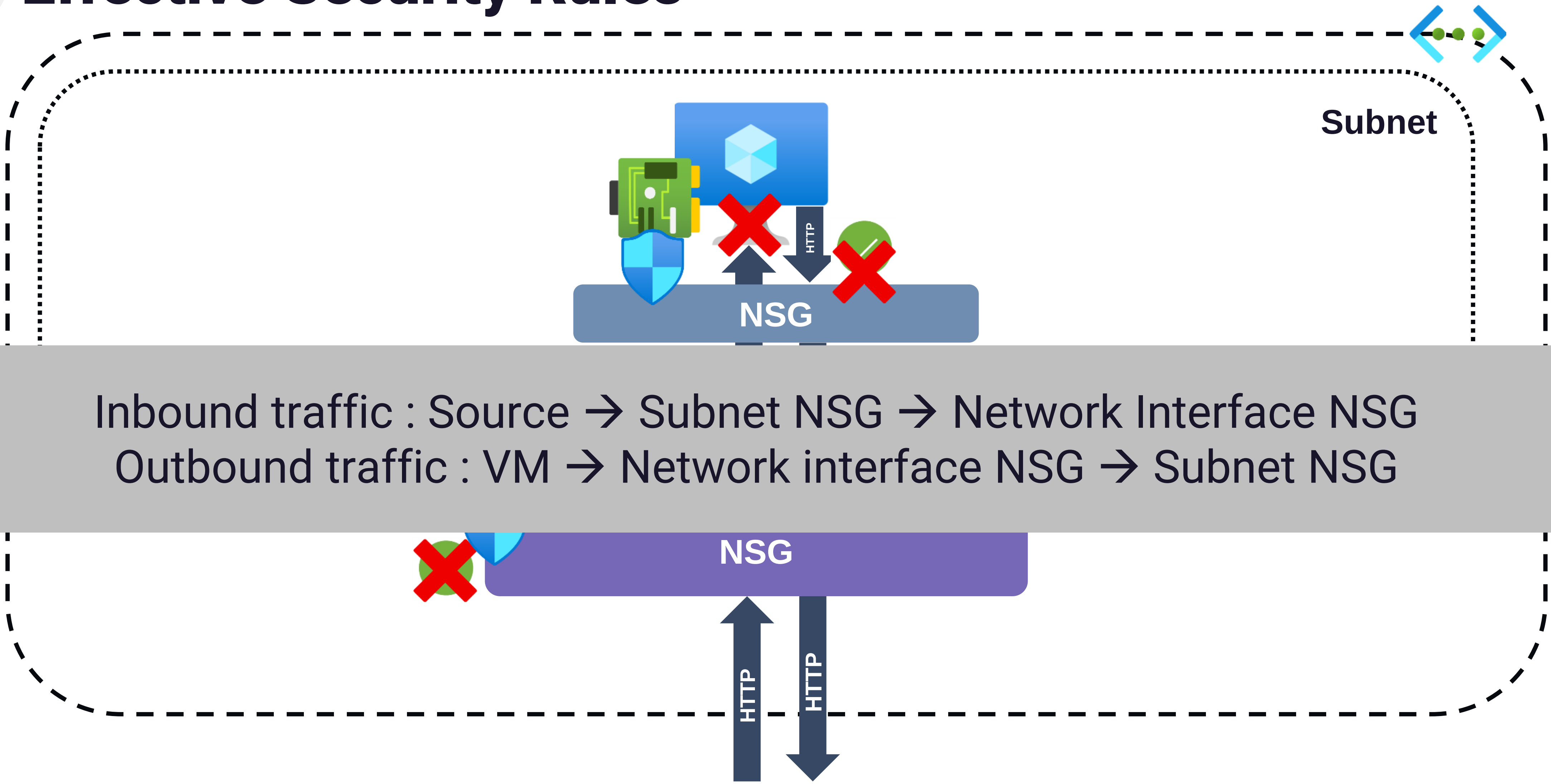
Custom security rules
1 inbound, 0 outbound

Associated with
0 subnets, 1 network interfaces

Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓
Inbound Security Rules					
300	⚠ RDP	3389	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any
Outbound Security Rules					
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any	Internet
65500	DenyAllOutBound	Any	Any	Any	Any

Effective Security Rules



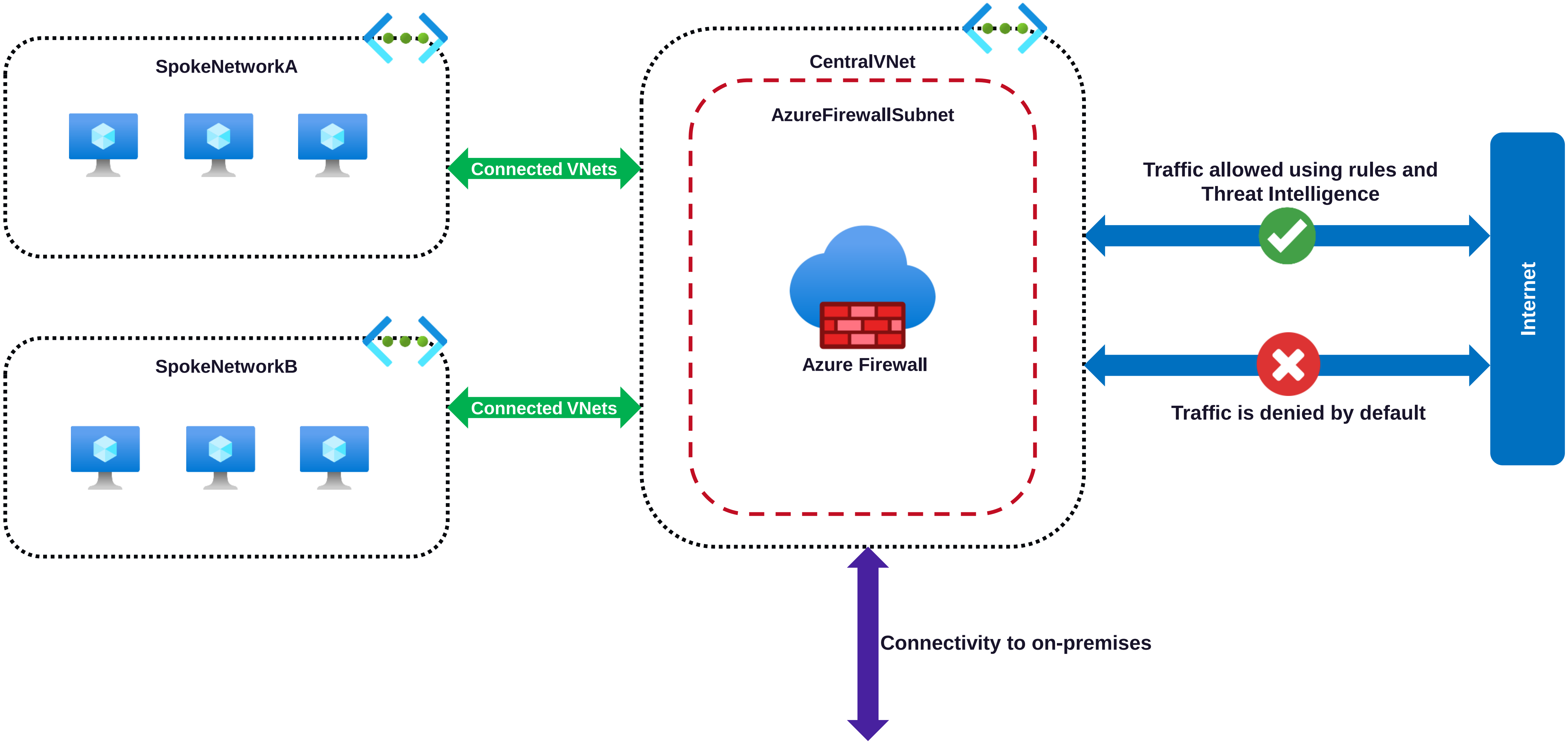
Inbound traffic : Source → Subnet NSG → Network Interface NSG
Outbound traffic : VM → Network interface NSG → Subnet NSG

Azure Firewall

Azure Firewall

- Highly available and scalable
- Redundancy
- Multiple types of rules
- Threat Intelligence
- Public IP support

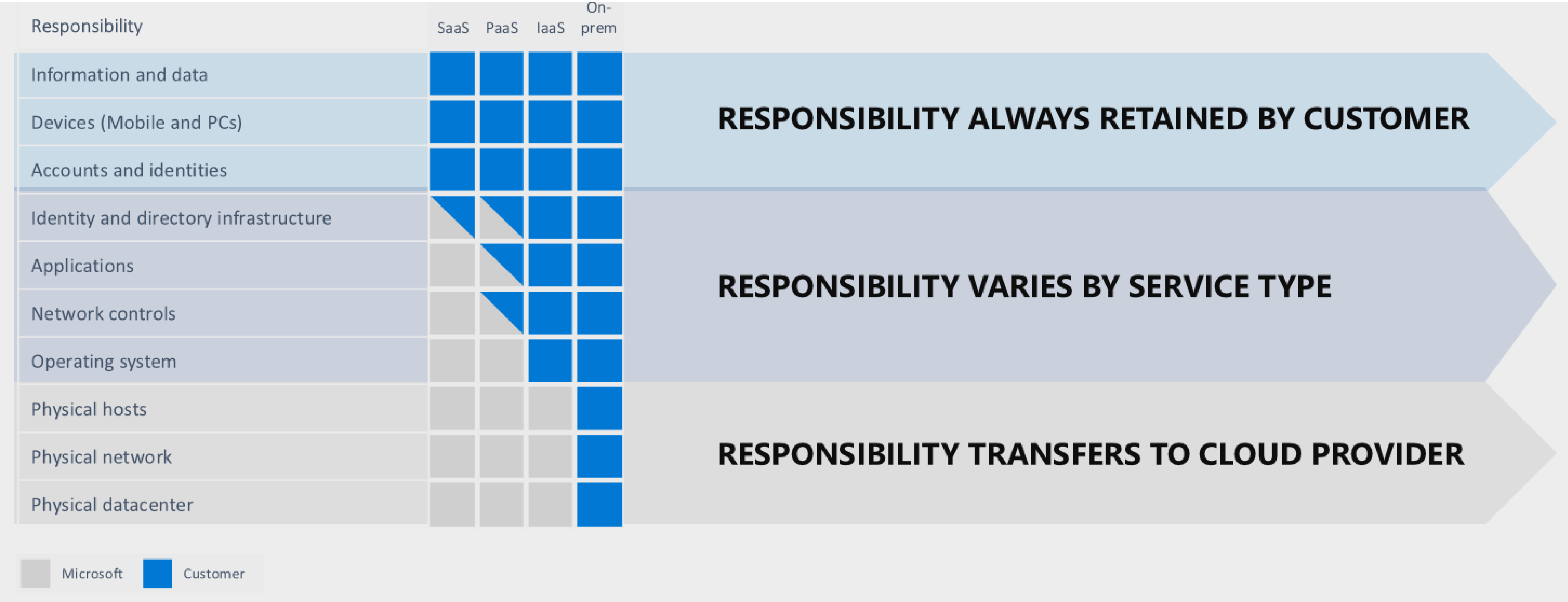
Azure Firewall



KODEKLOUD

Planning VMs

Shared responsibility model



Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◥	◥	🟦	🟦
Applications	⬜	◥	🟦	🟦
Network controls	⬜	◥	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

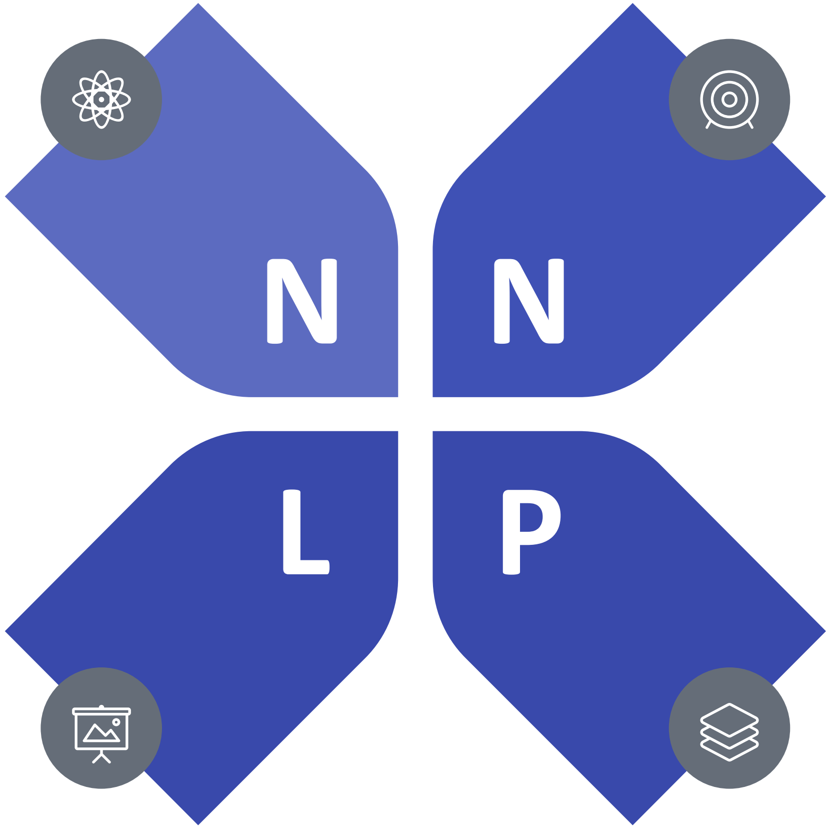
RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

⬜ Microsoft 🟦 Customer

Image source: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Virtual Machine Planning

We need to plan certain aspects before deploying our virtual machines



Networking

We need to plan our networking address spaces based on the number of virtual machines you are planning to create. Also, make sure the network address spaces are not overlapping.

Location

You need to check the availability of VM sizes in Azure regions. Choose low-cost regions if you are flexible with data residency. Also, for production resources choose regions closer to your customers to avoid performance issues. Azure has 60+ regions to choose from.

Naming

Naming convention helps us in recognizing VMs by looking their names. Try adding environment, role, service, and region details to VM names. For example, we could name production webserver in East US as *“web-prod-eus”*

Pricing

Consider pricing models such as Pay-As-You-Go and Reserved Instances. For low priority development workloads choose Spot VMs. Licensing cost can be reduced by using Azure Hybrid Benefit.

Managing VM sizes

Virtual Machine Sizing

Choosing the virtual machine size and family depends on what type of workload you are running. Azure offers different VM families targeting different types of workloads

Type	Sizes	Targeted workloads
General Purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute optimized	F, Fs, Fsv2, FX	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	Esv3, Ev3, Easv4, Eav4, Ebdsv5, Ebsv5, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage optimized	LSv2	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	NC, NCv2, NCv3, NCasT4_v3, ND, NDv2, NV, NVv3, NVv4, NDasrA100_v4, NDm_A100_v4	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
HPC	HB, HBv2, HBv3, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).
Confidential computing	DCsv2, DCsv3, and DCdsv3	Confidential computing allows you to isolate your sensitive data while it's being processed. Ideal for banks and hospitals which handle customer PII.

Microsoft documentation – VM sizes

Virtual Machine Storage

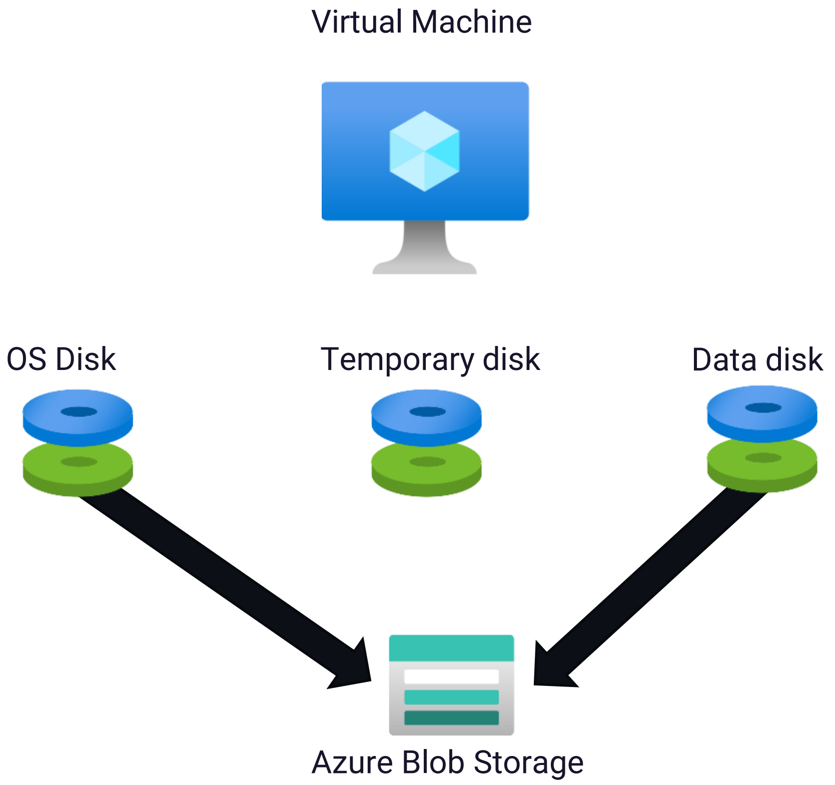
Virtual Machine Storage

Performance tiers

Azure disks can be created in different performance tiers such as Standard HDD, Standard SSD, Premium SSD or Ultra SSD. Based on the tiers the IOPS and performance will vary. Standard HDD is the cheapest option. You can change tier even after creating the disks. Premium SSD is required for IO intensive applications.

Management

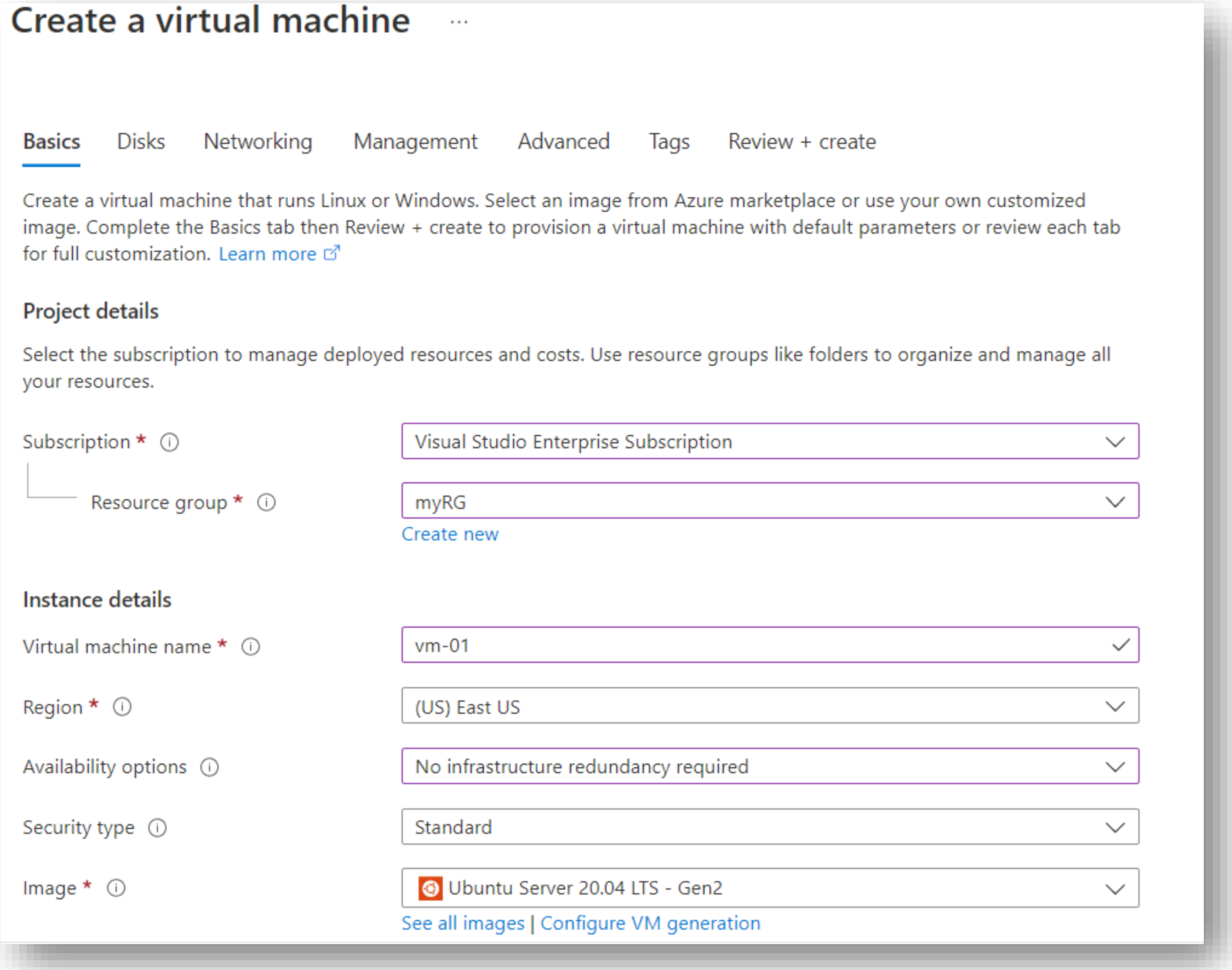
When creating VMs, you can choose between, Managed disks and Unmanaged disks. In Unmanaged disks, customer needs to take care of the underlying storage account which is used to store the VHD file. In case of Managed disks, the underlying storage account will be managed by Microsoft, and you can use the service. Microsoft recommends to use Managed disks.



Creating VMs

Creating Virtual Machine (Portal)

- **Basics (mandatory):** Subscription, Resource group, Region, VM Image, Size, Port rules
- **Disks:** Disk type, size, data disks
- **Networking:** Virtual Network, subnet, NSG, load balancing
- **Management:** Monitoring, Diagnostic Account, Azure AD login, Backup, Auto-shutdown



Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Visual Studio Enterprise Subscription

Resource group * : myRG

Create new

Instance details

Virtual machine name * : vm-01

Region * : (US) East US

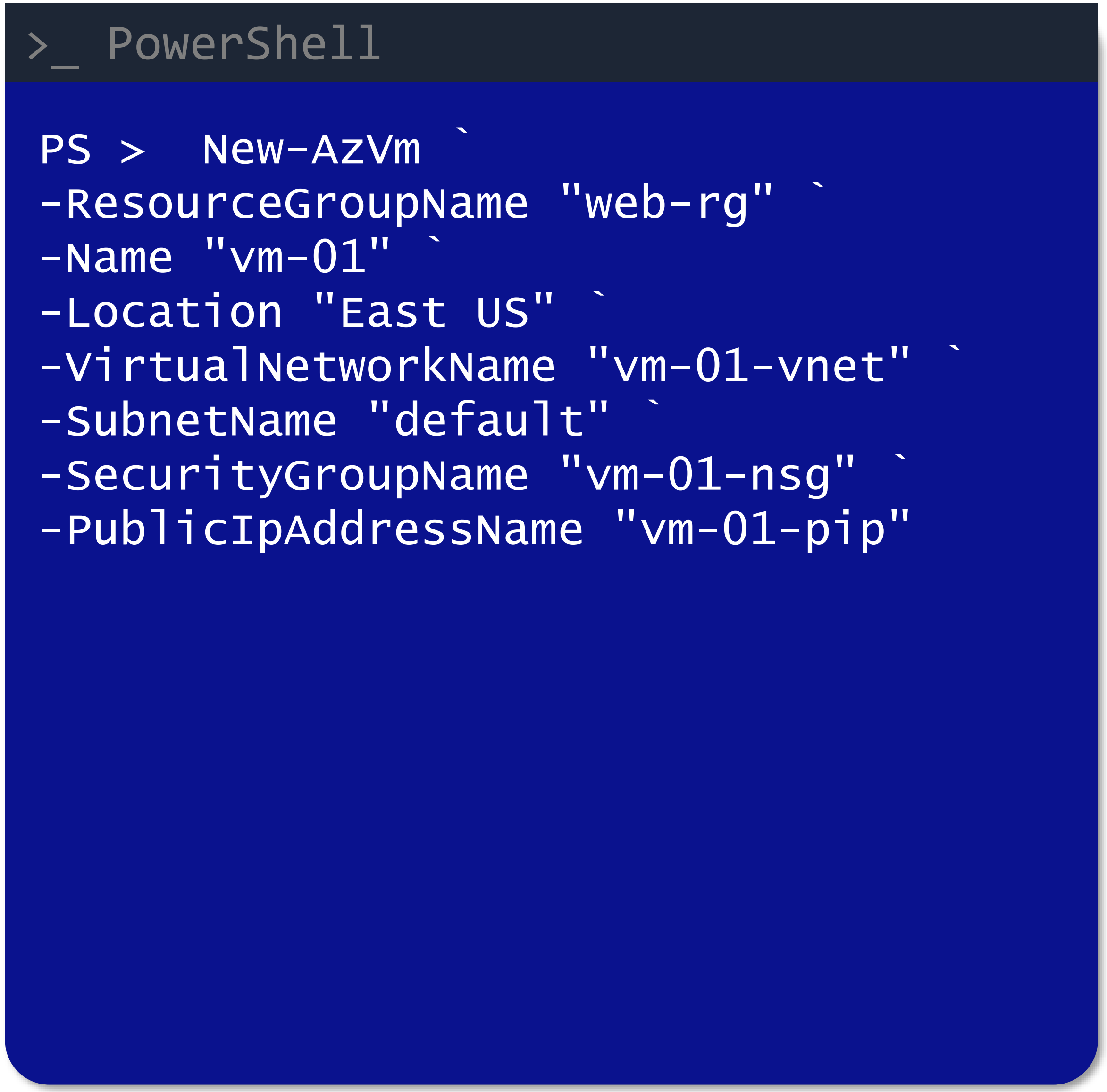
Availability options : No infrastructure redundancy required

Security type : Standard

Image * : Ubuntu Server 20.04 LTS - Gen2

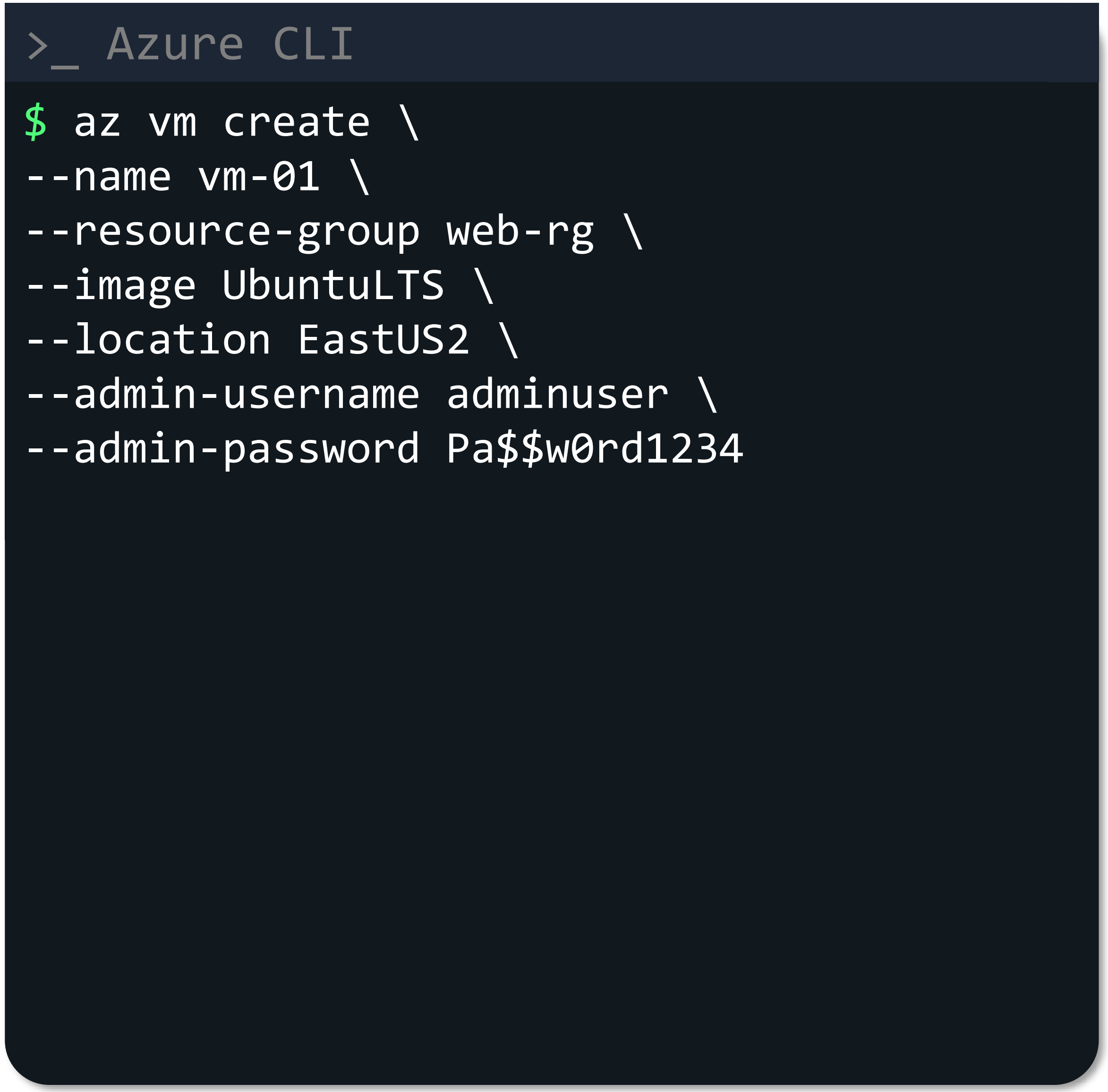
See all images | Configure VM generation

Creating Virtual Machine (PowerShell & Azure CLI)



>_ PowerShell

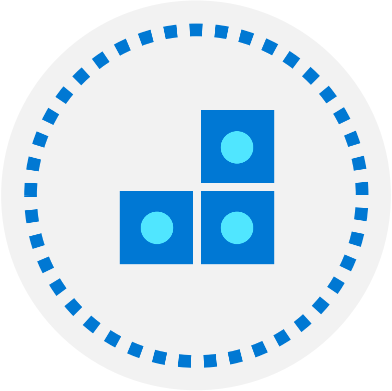
```
PS >  New-AzVm `
-ResourceGroupName "web-rg" `
-Name "vm-01" `
-Location "East US" `
-VirtualNetworkName "vm-01-vnet" `
-SubnetName "default" `
-SecurityGroupName "vm-01-nsg" `
-PublicIpAddressName "vm-01-pip"
```



>_ Azure CLI

```
$ az vm create \
--name vm-01 \
--resource-group web-rg \
--image UbuntuLTS \
--location EastUS2 \
--admin-username adminuser \
--admin-password Pa$$w0rd1234
```

Connecting to VMs

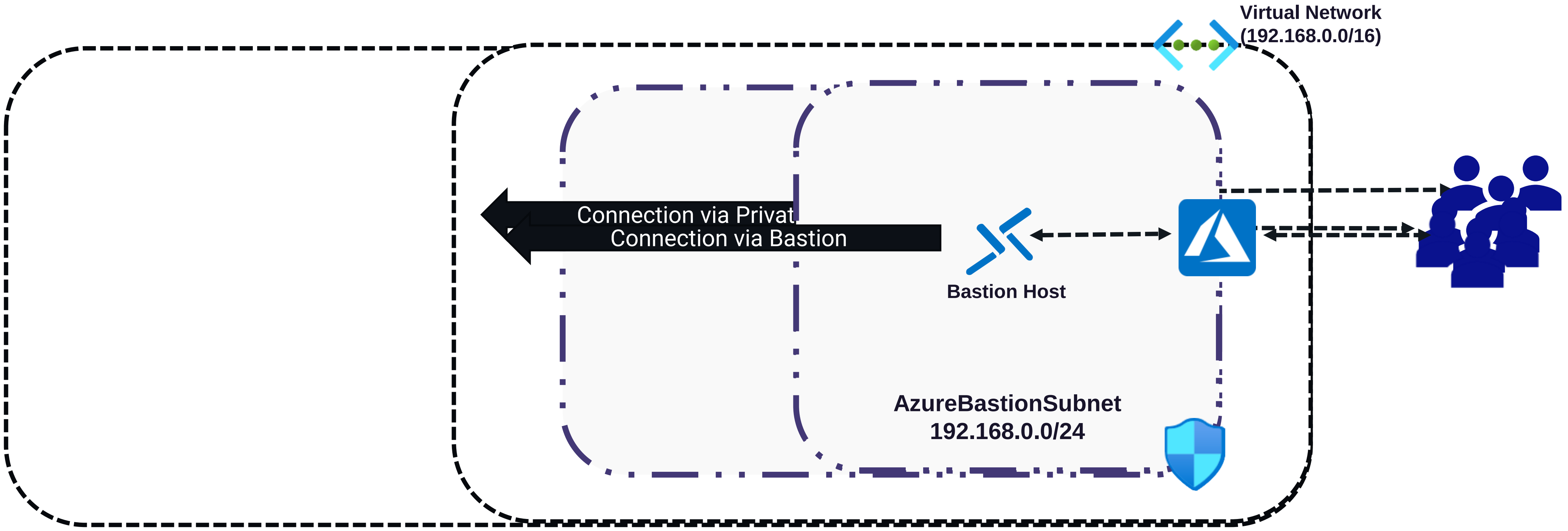


Connecting to Virtual Machines

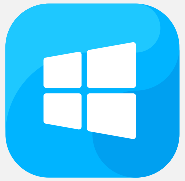
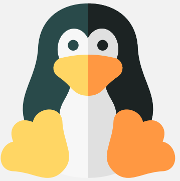
Public IP

Jumpbox

Azure Bastion



Connecting to Virtual Machines

Operating System	Protocol/ Port	Authentication Method
	RDP (TCP/3389) WinRM (TCP5986)	Password Certificates
	SSH (TCP/22)	Password

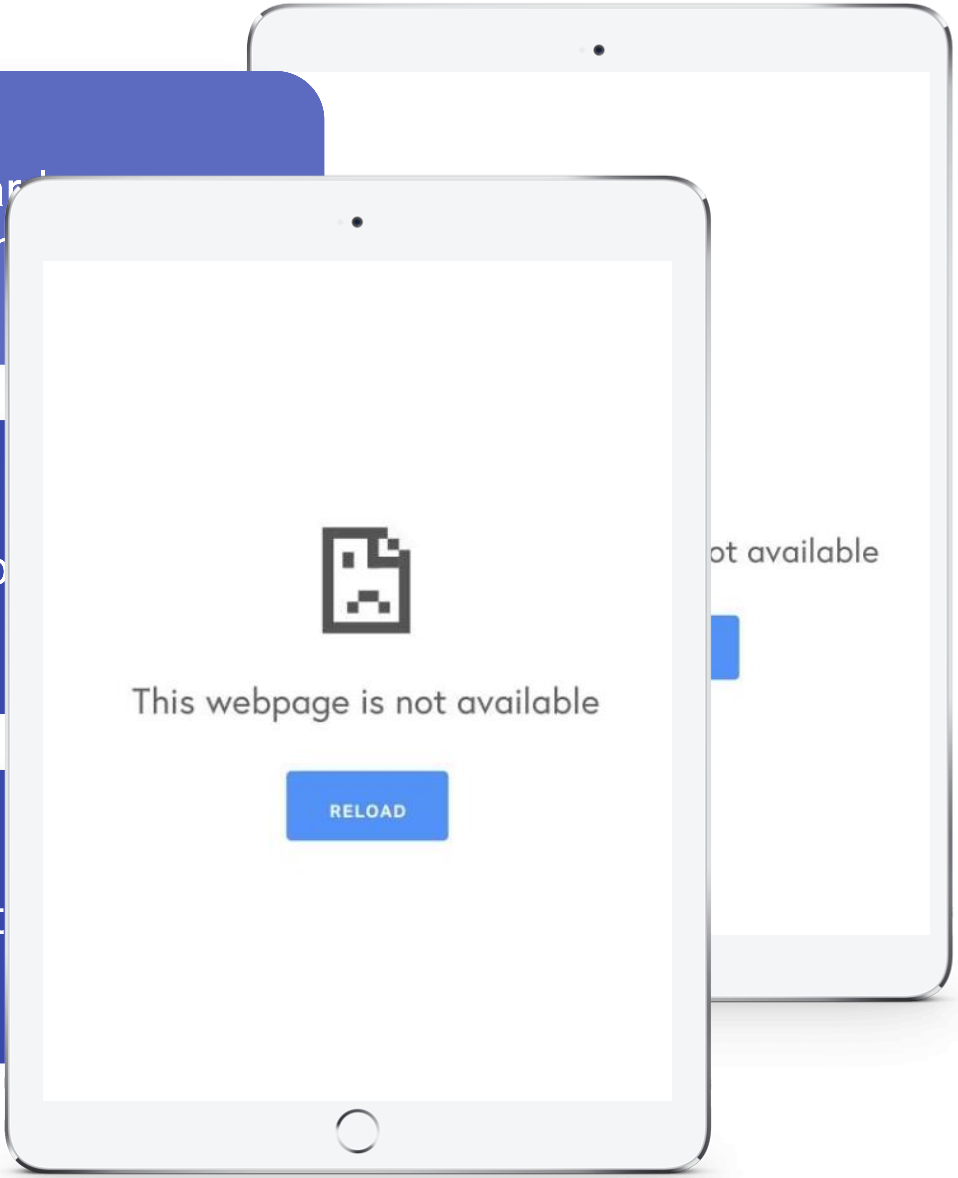
Configuring high availability

Configuring High Availability

Unplanned Har
Maintenar

Unexpected do

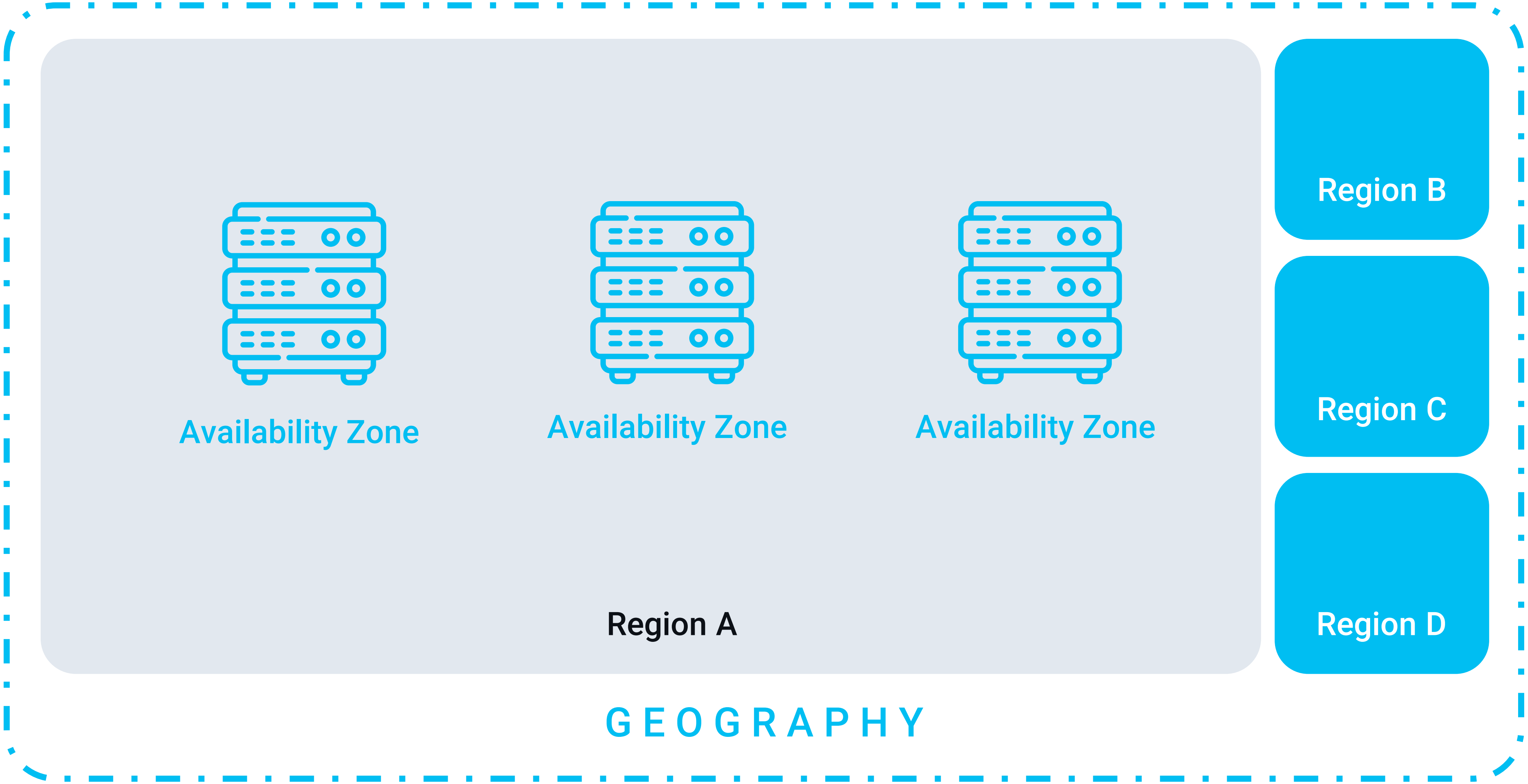
Planned maint



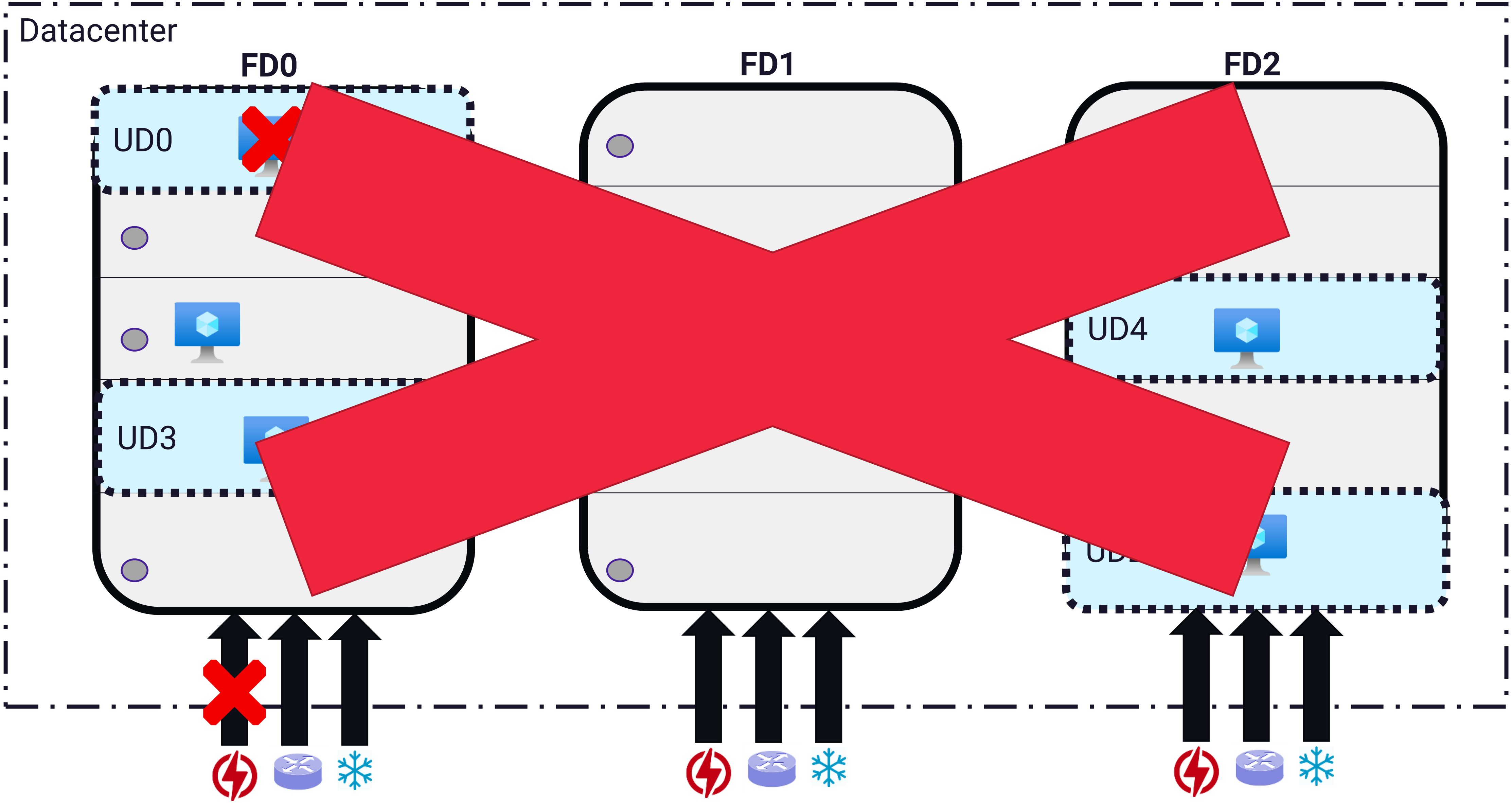
ot available

This webpage is not available

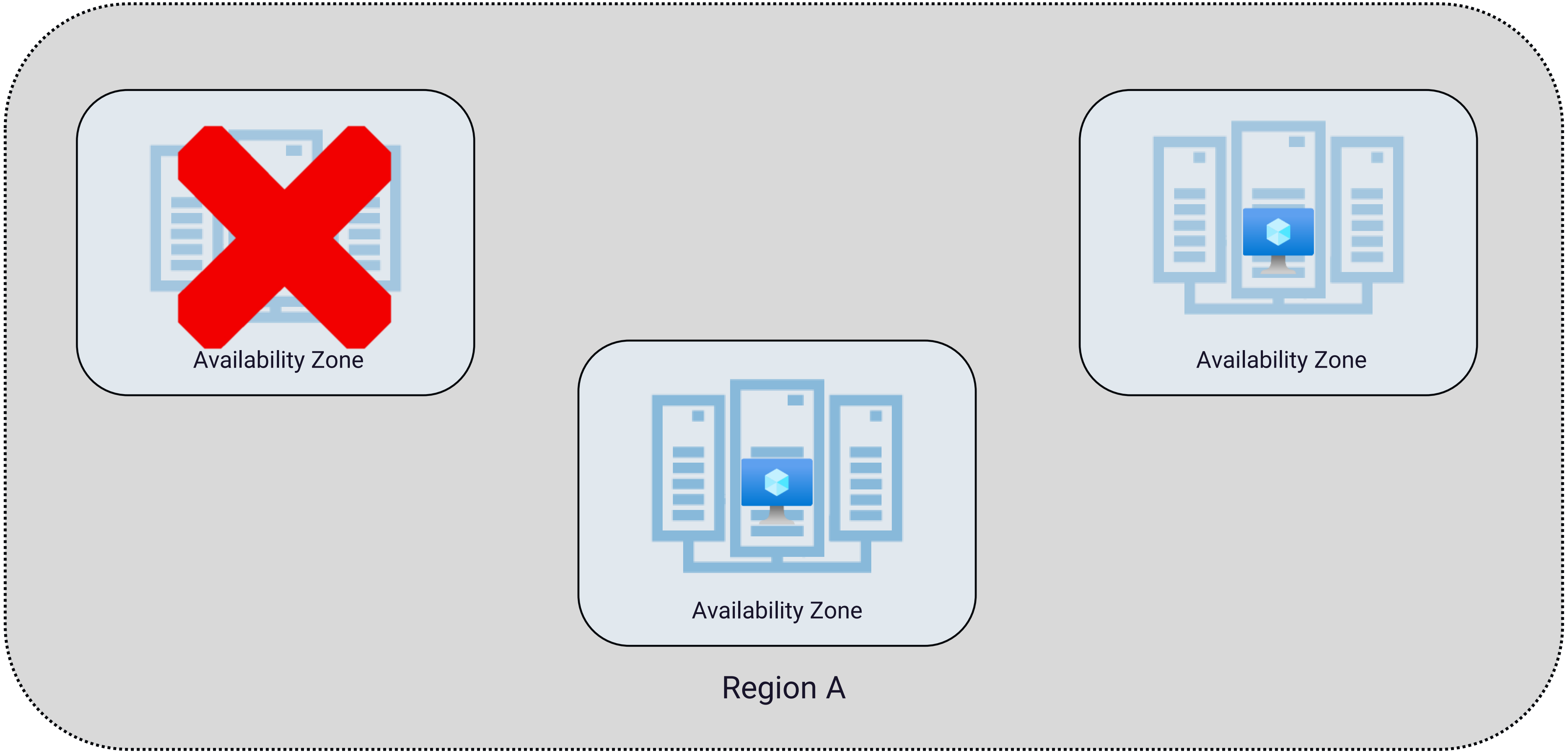
Configuring High Availability



Availability Set



Availability zones



Deploying VM Scale Sets

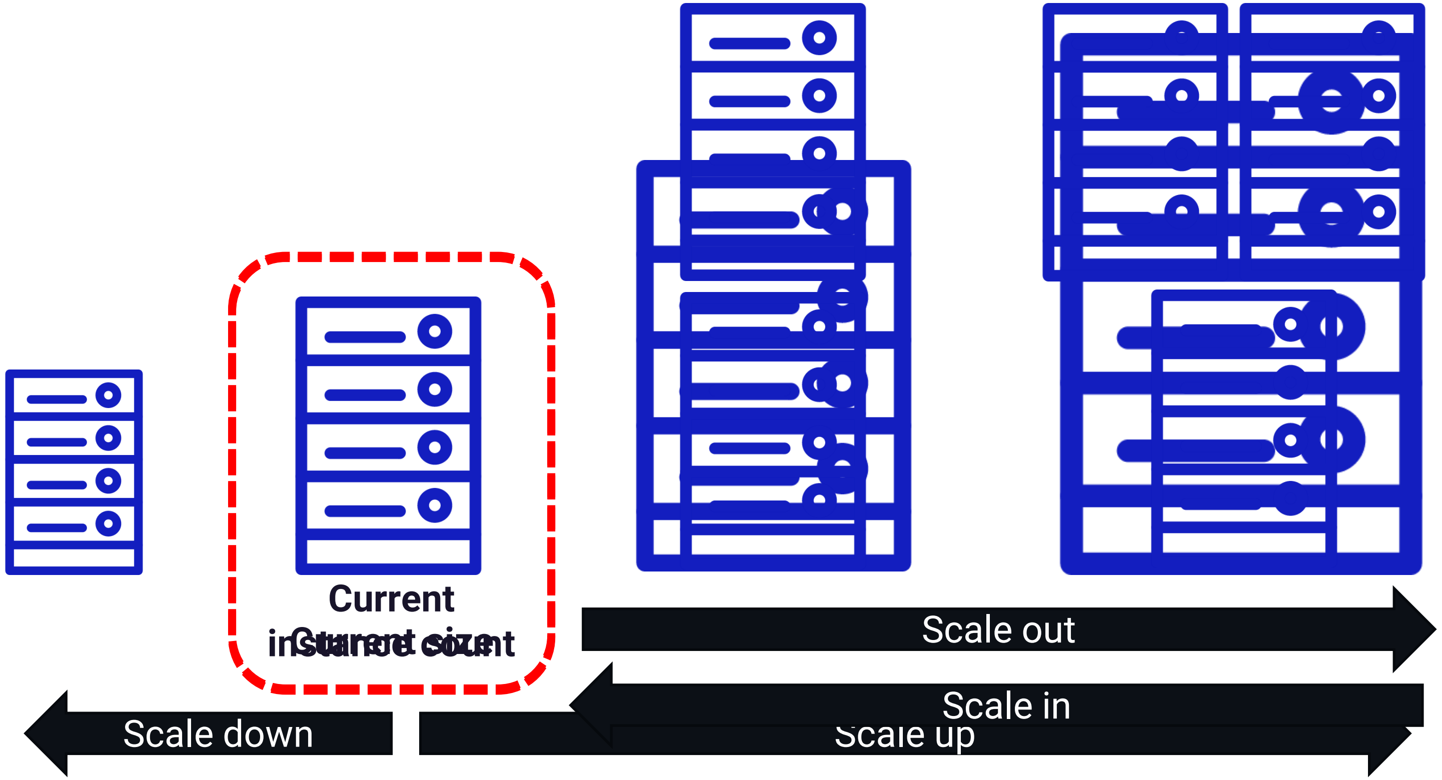
Deploying VM Scale Sets

Vertical Scaling

Adding or removing compute power to an instance is called vertical scaling. Increasing compute power is called scale up and decreasing compute power is called scale down. This process is usually manual.

Horizontal Scaling

Increasing or decreasing number of instances is called horizontal scaling. This is usually automated with the help of some criteria like metrics or schedule; hence it's also called autoscaling. Increasing instances is called scale out and decreasing instances is called scale in.



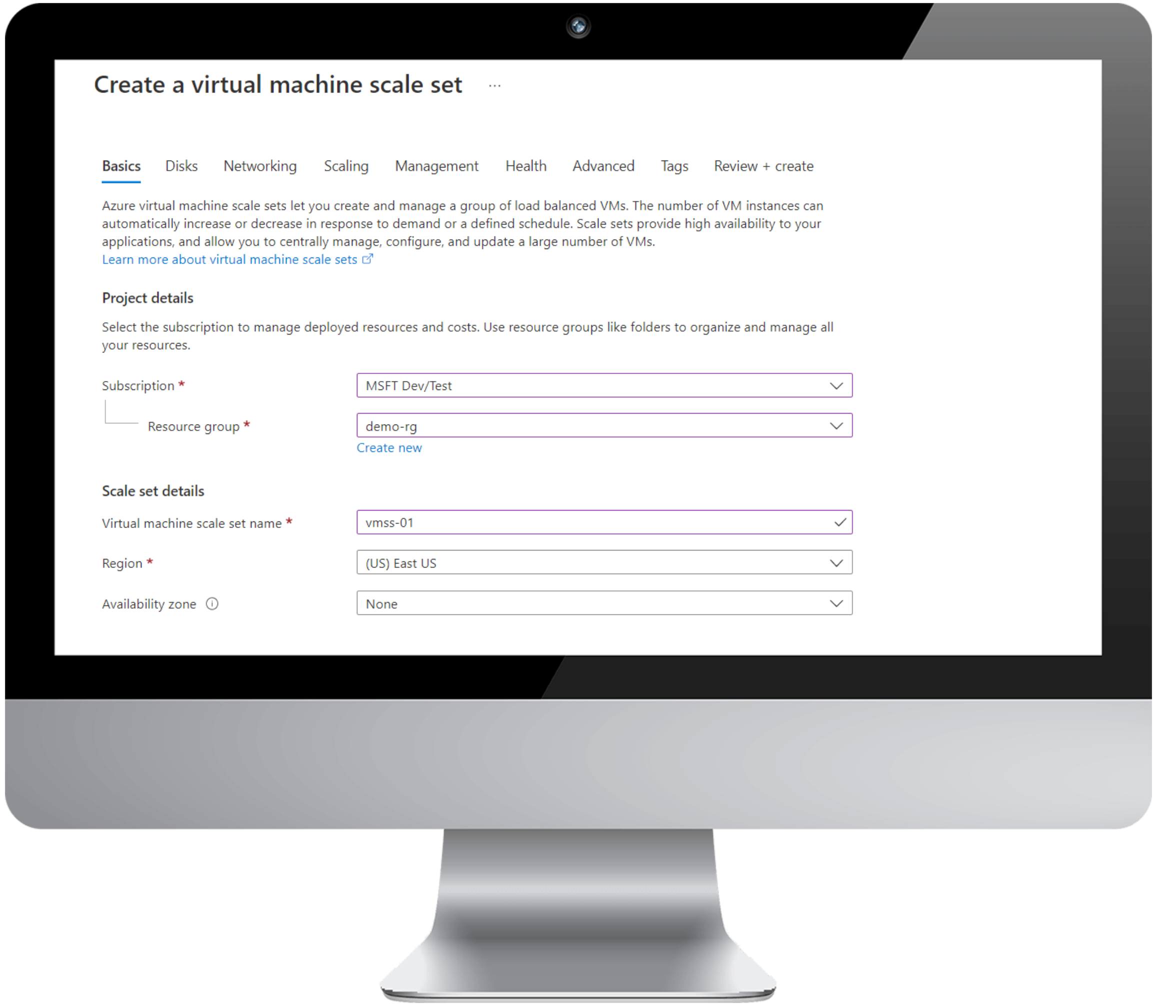
Deploying VM Scale Sets

- Azure Virtual Machine Scale set is used to create a group of load balanced VMs and manage them. VMSS supports use of Azure Load Balancer and Application Gateway

- We can increase or decrease the number of instances based on schedule, metrics, or on demand. All VMs in a scale set are created from the same base OS and configuration.

- We can distribute the VMs in a scale set across availability zones for high availability. If one VM becomes unavailable, customers can access the application via other VMs in the scale set.

- For images from marketplace and custom images, scale set can scale up to 1000 instances. If you create scale set using a managed image, the limit is set to 600.



Create a virtual machine scale set

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs.
Learn more about virtual machine scale sets

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	MSFT Dev/Test
Resource group *	demo-rg Create new

Scale set details

Virtual machine scale set name *	vmss-01
Region *	(US) East US
Availability zone	None

KODEKLOUD

Azure Load Balancer

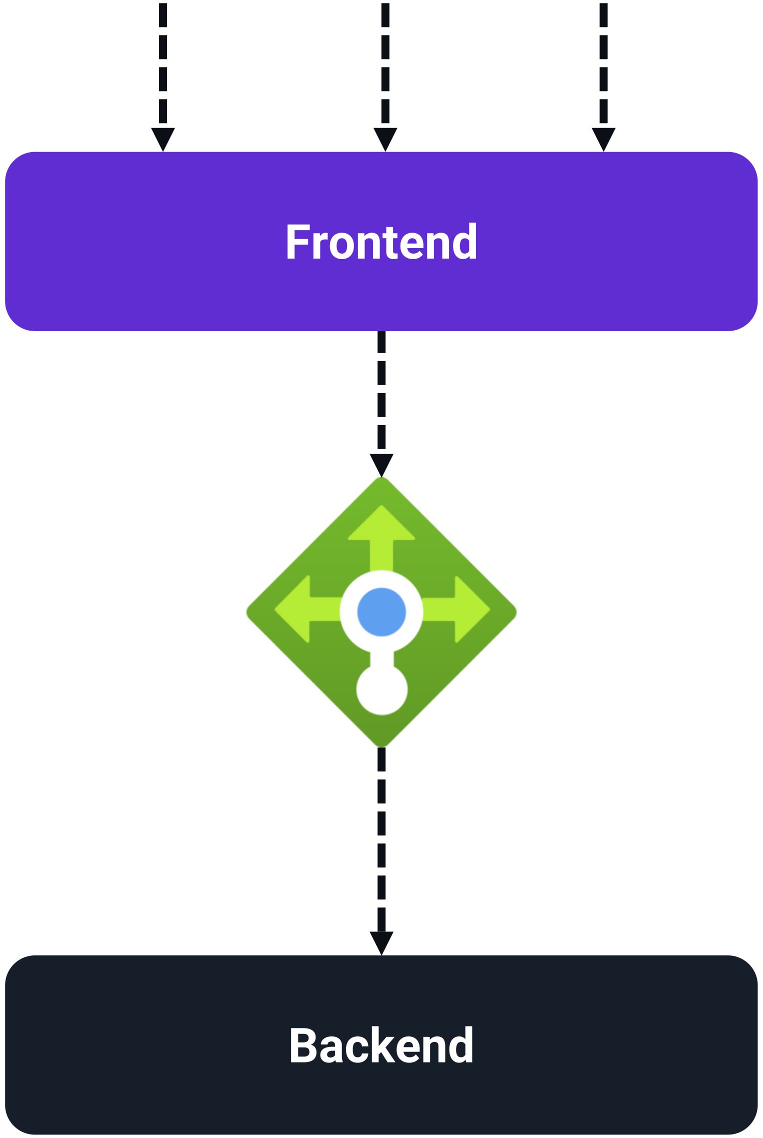
Azure Load Balancer

Azure Load Balancer is a Layer 4 load balancer which supports Azure Virtual Machines and Azure Virtual Machine Scale Sets as backend.

Load Balancer is offered in two SKUs: Standard and Basic SKU

Supports all TCP/UDP protocols

Security is managed with the help of Network Security Groups



Load Balancer SKU

✓ **Basic Load Balancer**

Ideal for testing and development. No SLA offered

✓ **Standard Load Balancer**

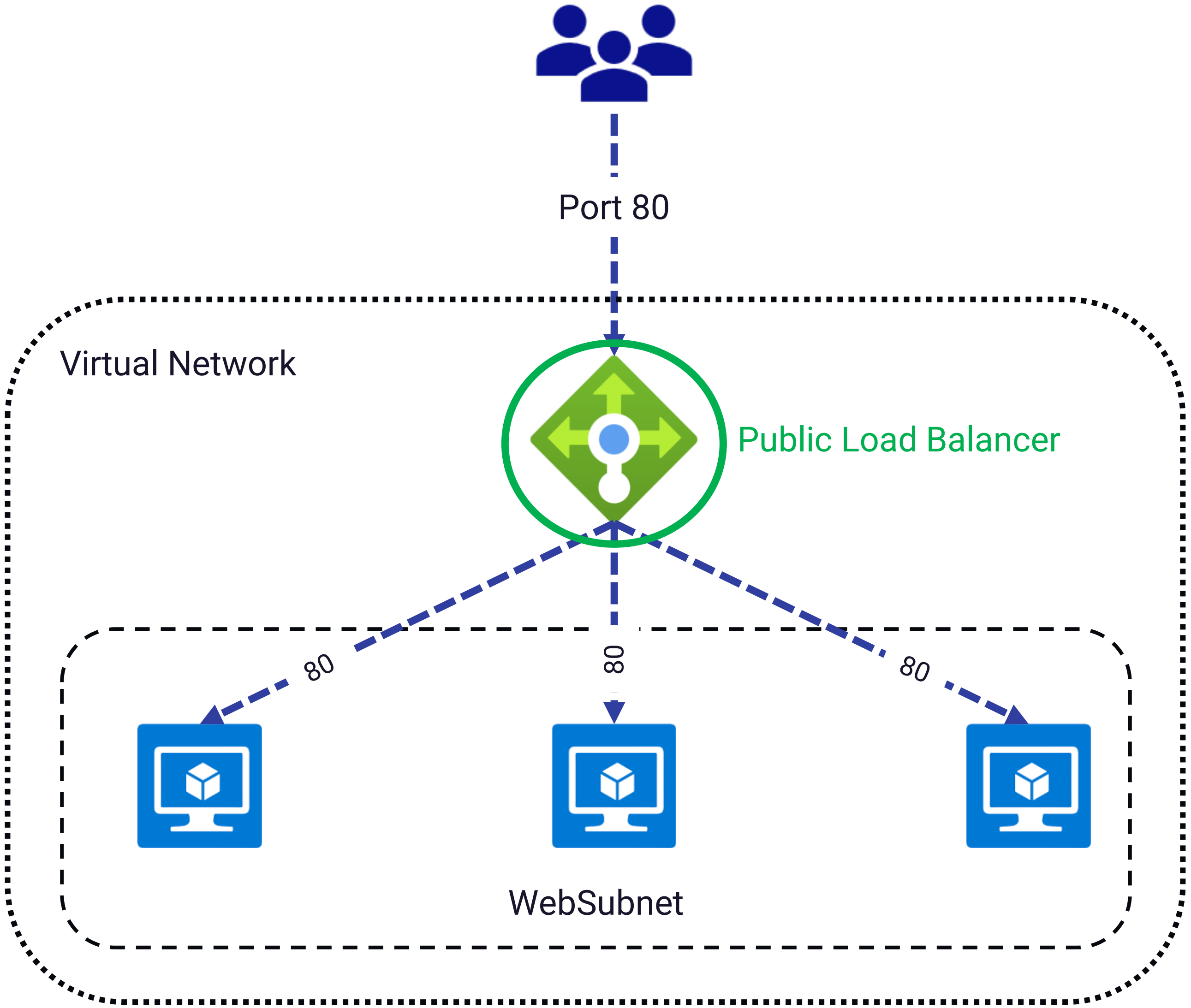
Recommended for production scenarios because of the SLA. Offers HTTPS health probe

Feature	Basic	Standard
Backend pool size	Up to 300 instances	Up to 1000 instances
Health probes	TCP, HTTP	TCP, HTTP, HTTPS
Redundancy	Not available	Zone redundant and zonal redundant
Multiple frontend	Inbound only	Inbound and outbound
Security	Open by default. NSG is optional	Closed, unless traffic is allowed by NSG
SLA	Not applicable	99.99%

Public Load Balancer

Ideal for public facing workloads

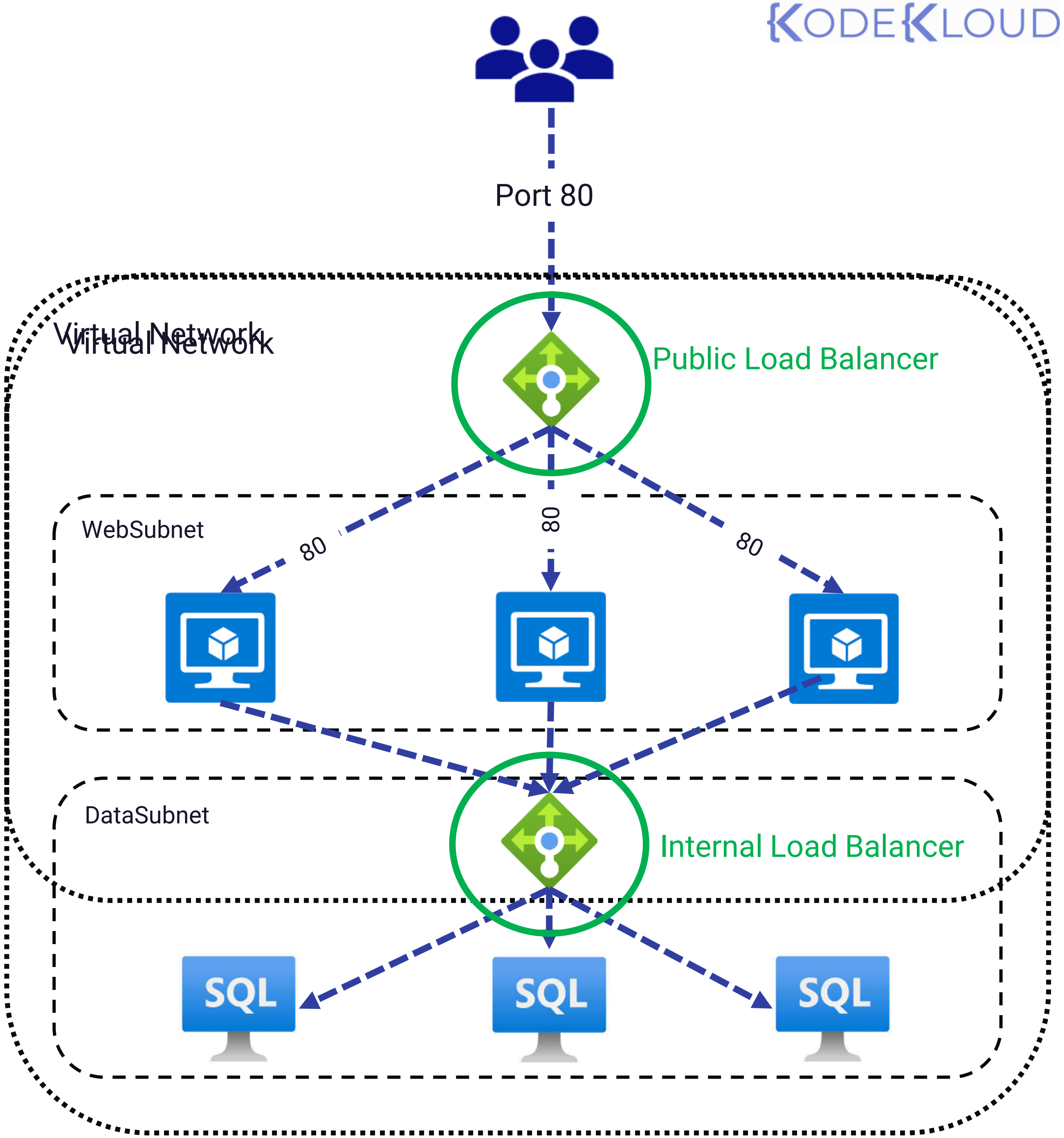
- Public load balancer will have public IP address
- Incoming traffic's public IP address and port number will be mapped to the private IP address and port number of the backend servers.
- With the help of load balancing rules, we can distribute the traffic across backend servers.
- Used in all public facing workloads which require load balancing.



Internal Load Balancer

Ideal for internal workloads

- Internal load balancer doesn't have public IP address as frontend
- Incoming traffic inside the virtual network or from a VPN can be distributed across the backend servers
- This load balancer is never exposed to the internet, so the IP addresses and port numbers are not visible to the internet.
- Used in internal resources that needs to be accessed from Azure or on-premises via VPN connection.



Load Balancer Rules

Load balancing rules

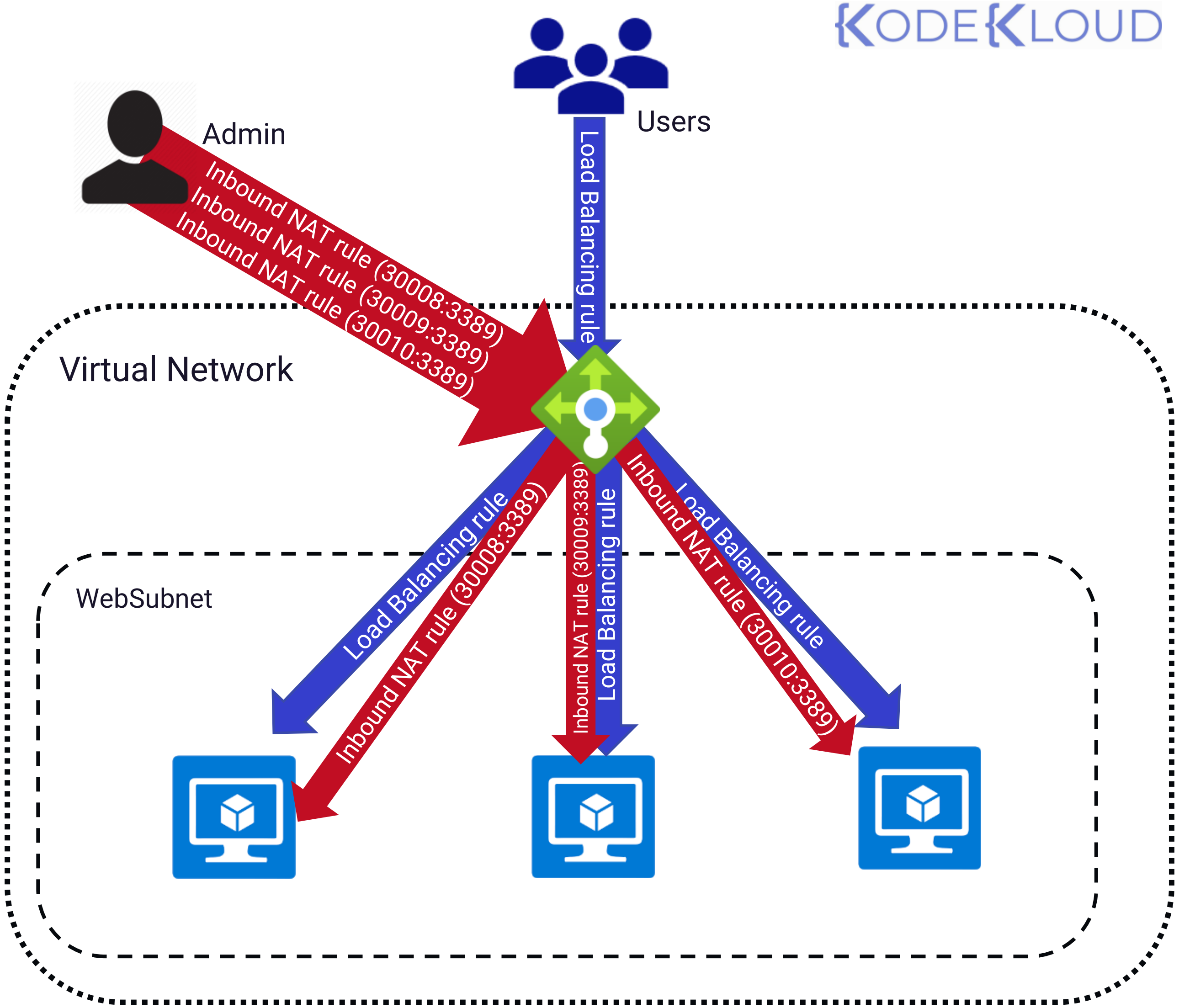
The incoming traffic to backend pools is distributed with the help of load balancing rules. We can create frontend IP to backend IP port mapping and the traffic is distributed accordingly.

Inbound NAT rules

Instead of backend pool, we can target a specific virtual machine and create a NAT rule. Frontend IP and port combination is used to send traffic to IP and port of the designated VM.

Outbound rule

Allows instances in the backend pool to communicate to the Internet and other endpoint.


Admin
Users
Inbound NAT rule (30008:3389)
Inbound NAT rule (30009:3389)
Inbound NAT rule (30010:3389)
Load Balancing rule
Virtual Network
WebSubnet
Load Balancing rule
Inbound NAT rule (30008:3389)
Inbound NAT rule (30009:3389)
Load Balancing rule
Inbound NAT rule (30010:3389)
Load Balancing rule

Session Persistence

None (default)

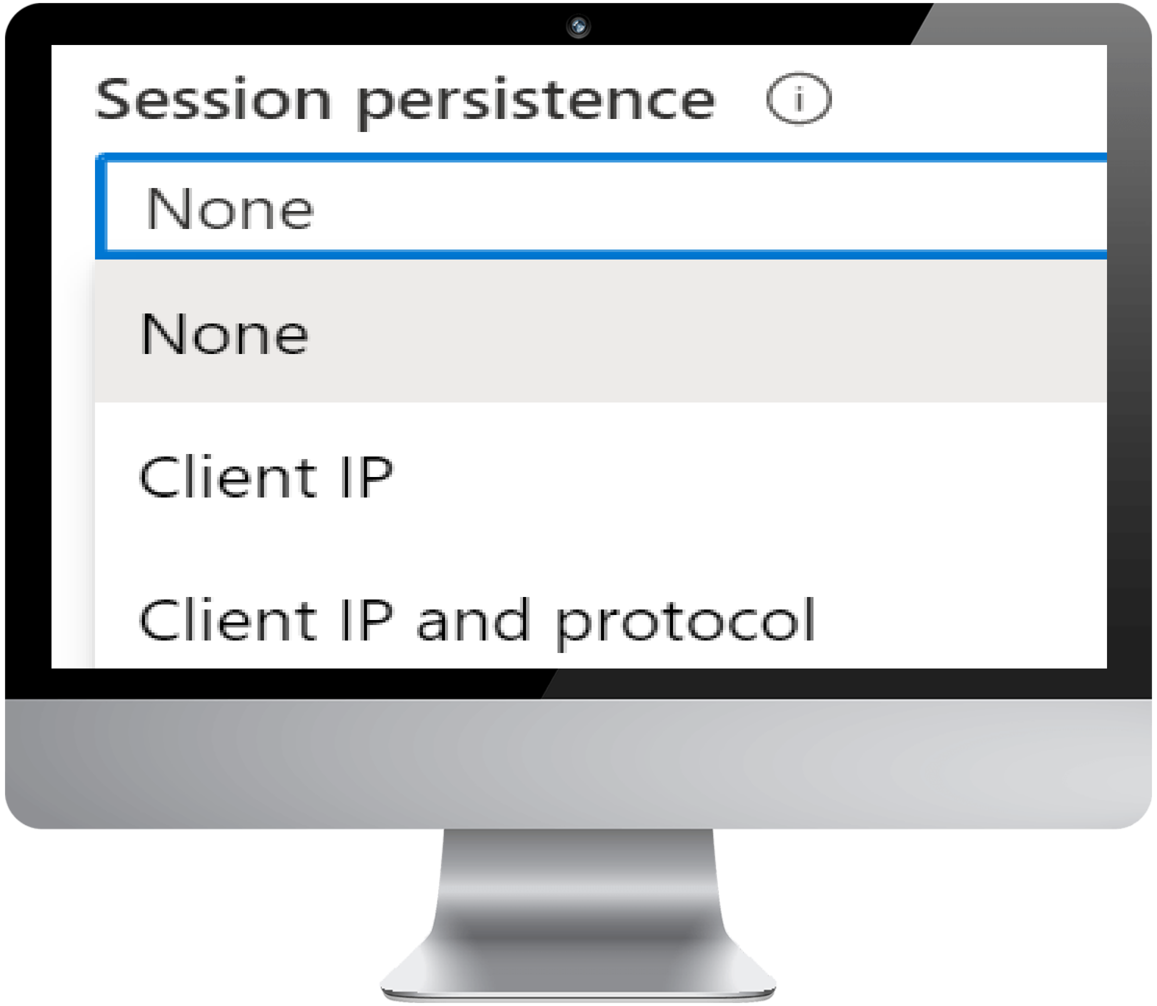
Request will be routed based on a 5-tuple hash. Five tuple comprises of Source IP, Source Port, Destination IP, Destination port, and Protocol. Requests can be handled by any VM and the chances of getting a new VM for every session is very high.

Client IP

Client IP is called two-tuple where the hash of source IP and destination IP is used to route the traffic. Requests will be handled by the same VM if the source IP or destination IP doesn't change.

Client IP and protocol

This is also called as three-tuple hash, where the hash of source IP, destination IP and protocol is used to route the traffic to the VM. Requests coming from same IP and protocol will be handled by the same VM.

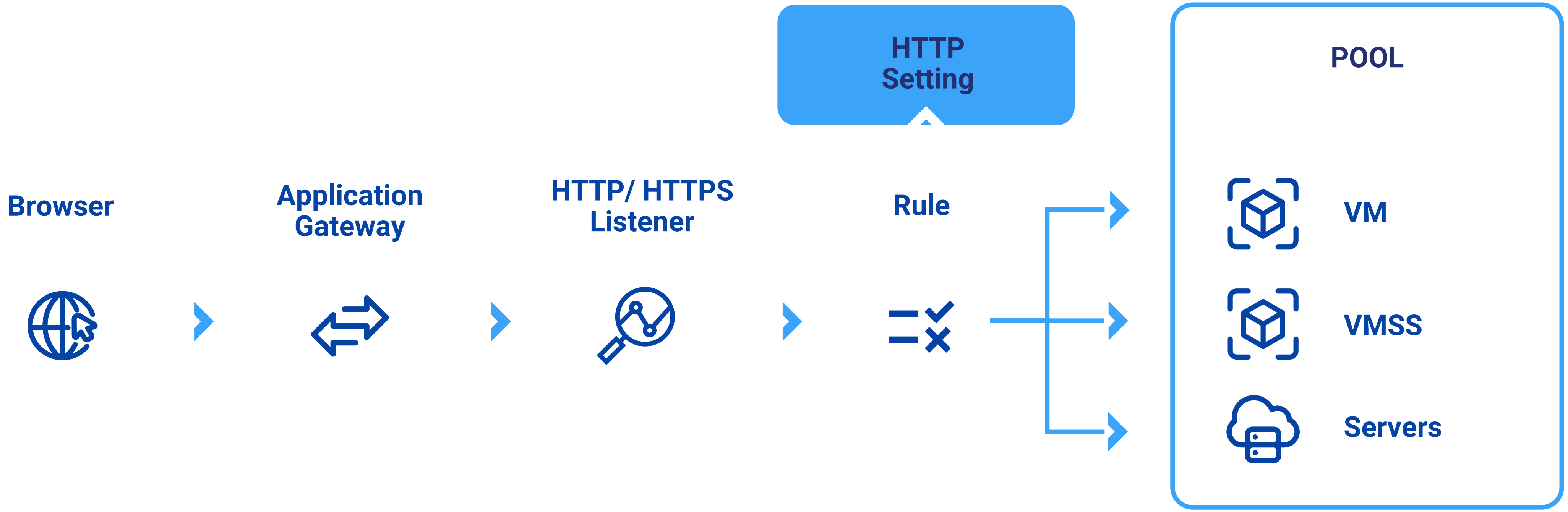


Session persistence ⓘ

None

Azure Application Gateway

Application Gateway



Layer 7 Load Balancer

Manages HTTP, HTTPS, HTTP/2, and WebSocket requests. Requests will be routed to the backend pool. Web Application Firewall can be added to Application Gateway as an option component.

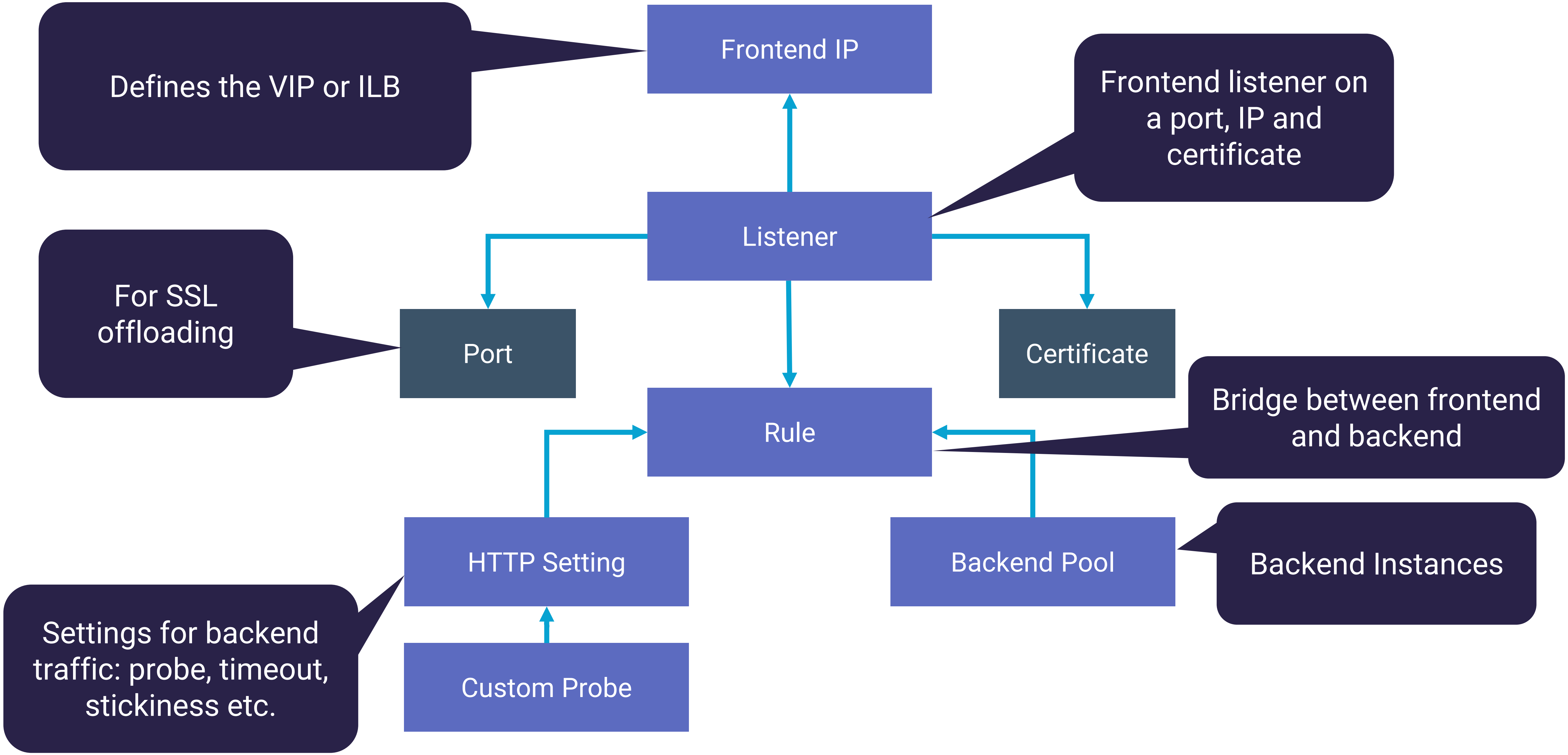
Routing and features

Requests can be routed to the backend pool based on URL also known as path-based routing. Also, we can host multiple sites behind an application gateway. Features includes URL Redirect, SSL termination, Rewrite HTTP headers and Custom error pages.

Backend pools

The web servers can be hosted in Azure Virtual Machines, Azure Virtual Machine Scale Sets, Azure App Services, and even on-premises servers.

Application Gateway - Components



Defines the VIP or ILB

Frontend listener on a port, IP and certificate

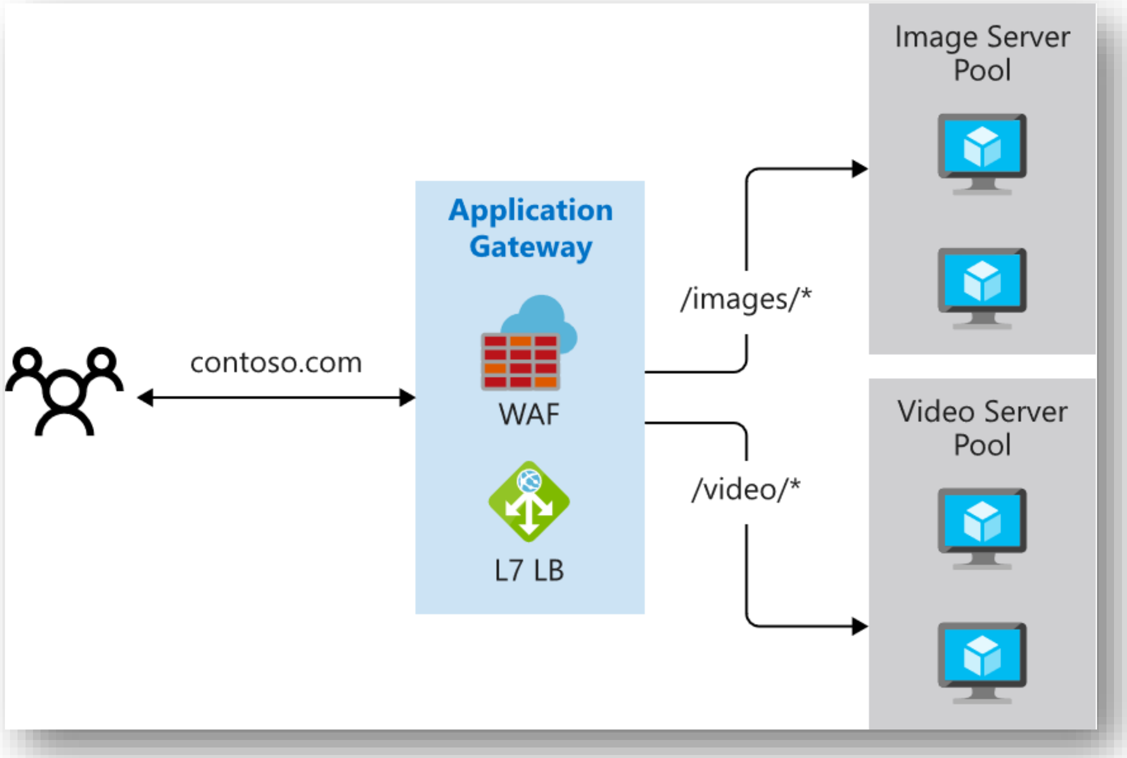
For SSL offloading

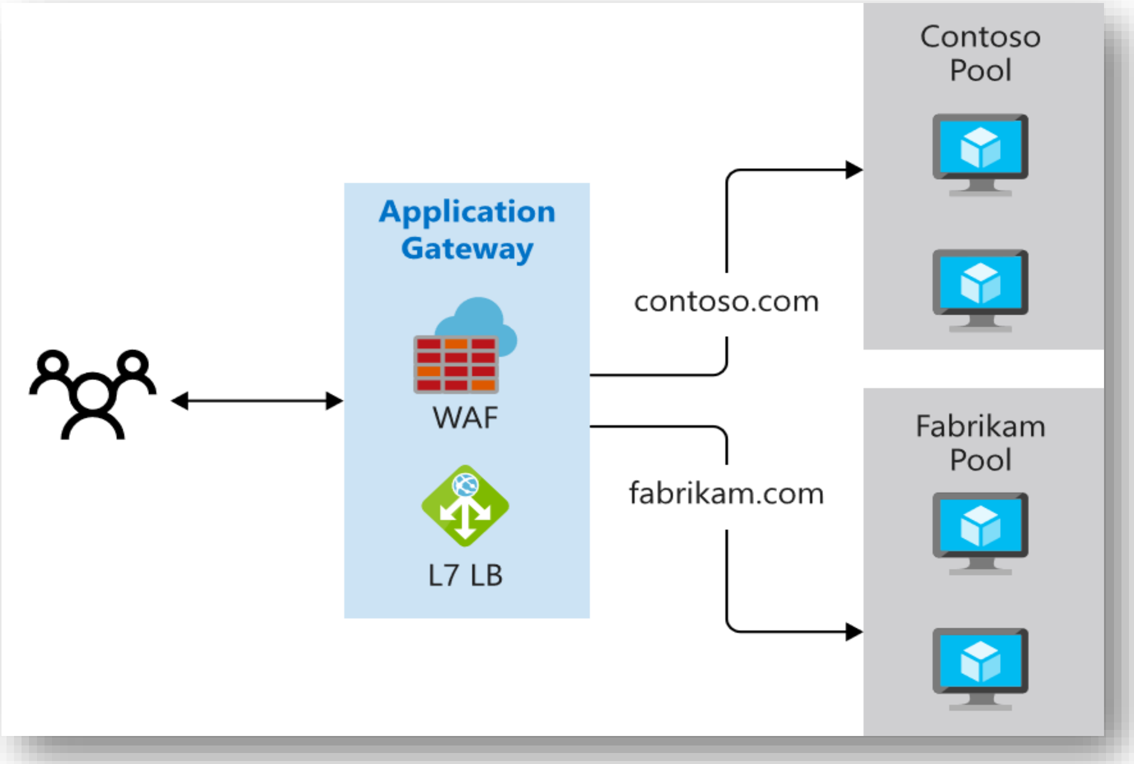
Bridge between frontend and backend

Backend Instances

Settings for backend traffic: probe, timeout, stickiness etc.

Application Gateway – Routing Rules





Path based routing

Based on the path in the URL, we can route the request to different backend pools. Ideal for routing requests to different backend pools optimized for different paths.

Multiple-site routing

Multiple sites can be hosted behind a single application gateway. Based on the domain, the request can be routed to the backend pool hosting the requested domain.

Image source: https://docs.microsoft.com/en-us/learn/modules/configure-azure-application-gateway/3-determine-routing

Other load balancing solutions

Other load balancing solutions

✓ Azure Front Door

Modern CDN solution that provides reliable, fast content delivery . Azure Front Door is a global solution which leverages the Microsoft's global edge network with hundreds of global and local point-of-presence locations. These endpoints are distributed across the globe and closer to your customers.

We can deploy our solutions in multiple regions and load balance using the Azure Front Door. Path based routing and multiple-site routing is available.

Web Application Firewall can be added as an optional component.

✓ Azure Traffic Manager

ATM or Azure Traffic Manager is a DNS based load balancer. Traffic coming to your public facing applications can be distributed across the globe with the help of ATM.

As this is a DNS load balancer, it uses DNS to direct the client request to an endpoint based on the routing rule we configure. Traffic Manager finds the best endpoint for you based on the routing and returns a DNS response with the endpoint name. Client then directly reaches out to the endpoint.

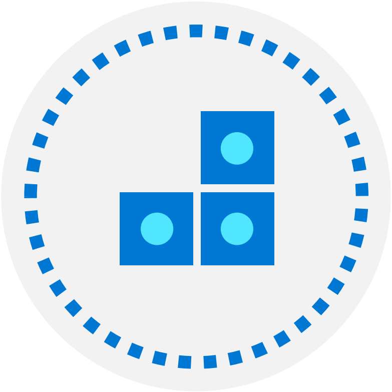
ATM can be used with the public facing services deployed in Azure or non-Azure environments. Routing methods includes Priority, Weighted, Geography, Performance and Nested Profile.

Comparing Load Balancing Solutions

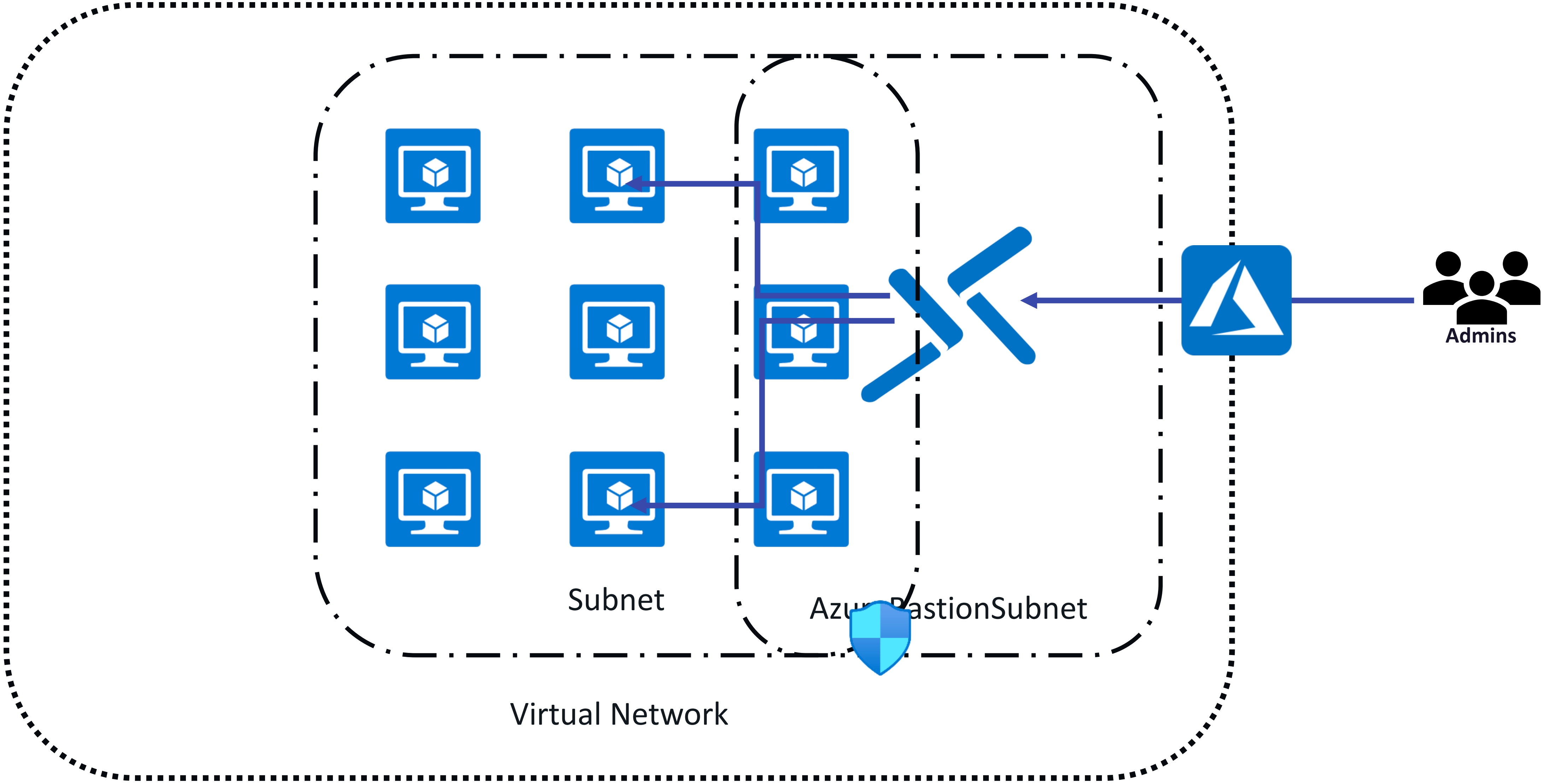
Feature	Application Gateway	Front Door	Load Balancer	Traffic Manager
Usage	Optimize delivery from application server farms while increasing application security with web application firewall.	Scalable, security-enhanced delivery point for global, micro service-based web applications.	Balance inbound and outbound connections and requests to your applications or server endpoints.	Distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.
Protocols	HTTP, HTTPS, HTTP2	HTTP, HTTPS, HTTP2	TCP, UDP	Any
Internal support	Yes		Yes	
Cross Region	No	Yes	Preview	Yes
Environment	Azure, non-Azure cloud, on premises	Azure, non-Azure cloud, on premises	Azure	Azure, non-Azure cloud, on premises
Security	WAF	WAF, NSG	NSG	-

Reference architecture examples

Azure Bastion



Azure Bastion



Azure Bastion

✓ **Direct RDP and SSH in Azure Portal**

No need to deploy or download SSH and RDP clients to your computer, you can RDP/SSH from browser.

✓ **Public IP is not required**

Since we are connecting via Bastion Host, there is no need to main public IP addresses for our virtual machines.

✓ **No need to tweak NSGs**

No need to manage and write complex rules in your NSG as Bastion is connecting to private IP address

✓ **Port scanning protection**

Since we are not exposing any public IPs, attackers cannot perform port scanning.

✓ **Hardening**

Bastion is a platform managed service and hardening in one place only.

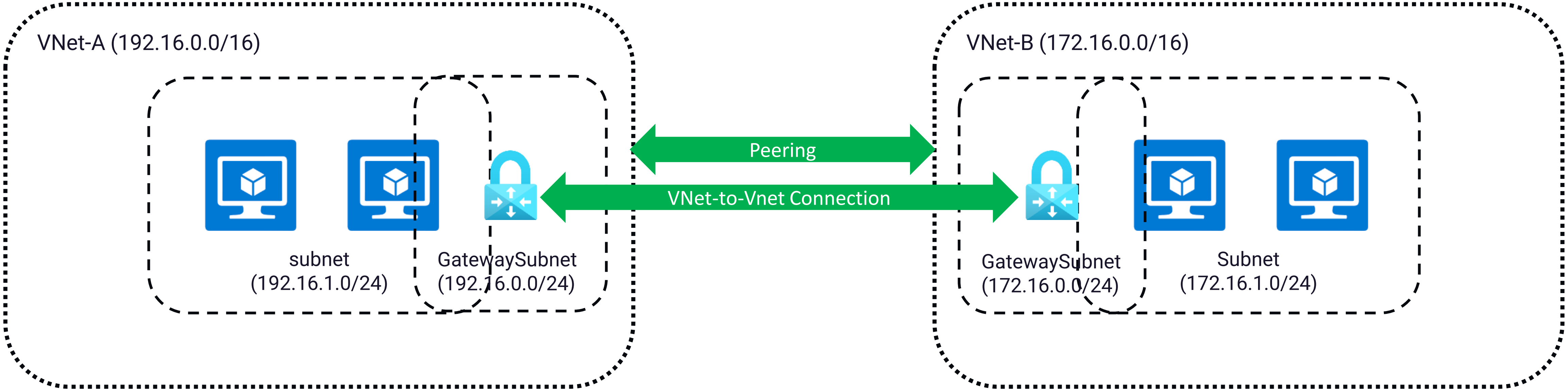
✓ **Basic and Standard SKUs**

Basic SKU provides base functionality as in direct RDP/SSH access. The Standard SKU enables premium features that allow Azure Bastion to manage remote connectivity at a larger scale.

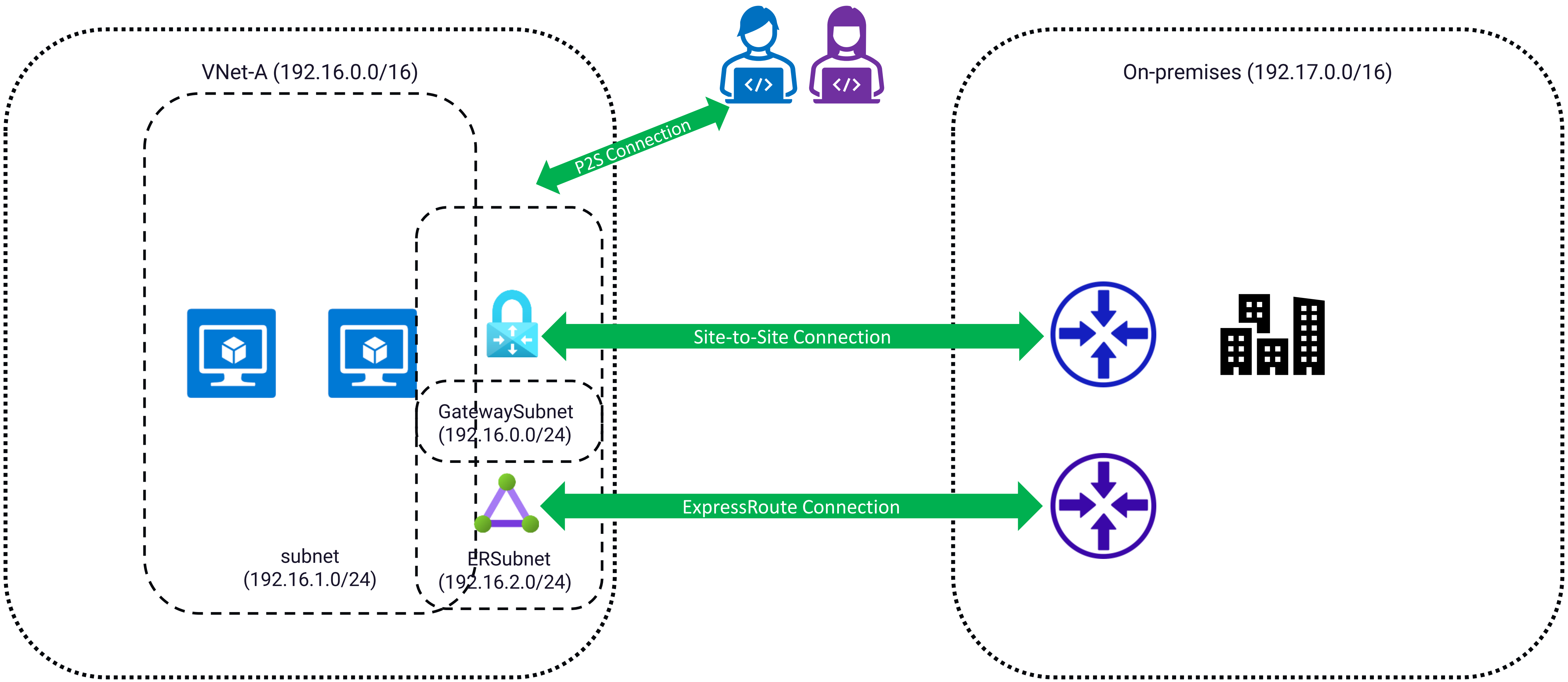
KODEKLOUD

Intersite connectivity

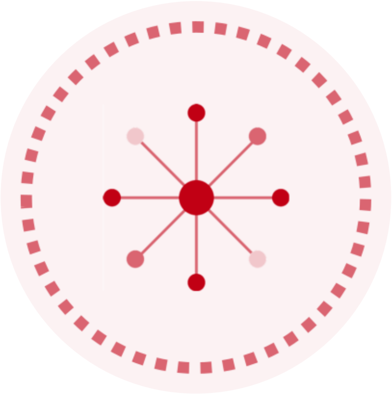
Intersite Connectivity – Azure-to-Azure connectivity



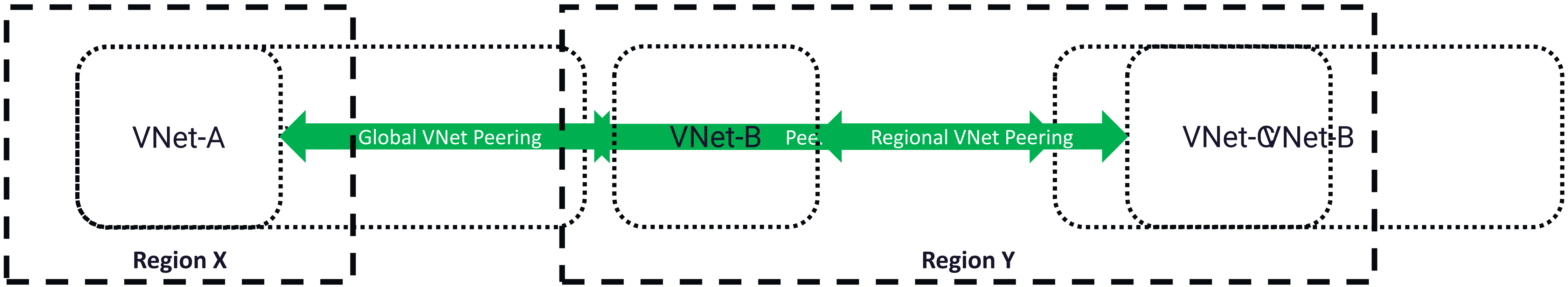
Intersite Connectivity – Azure-to-on premises connectivity



Virtual Network Peering



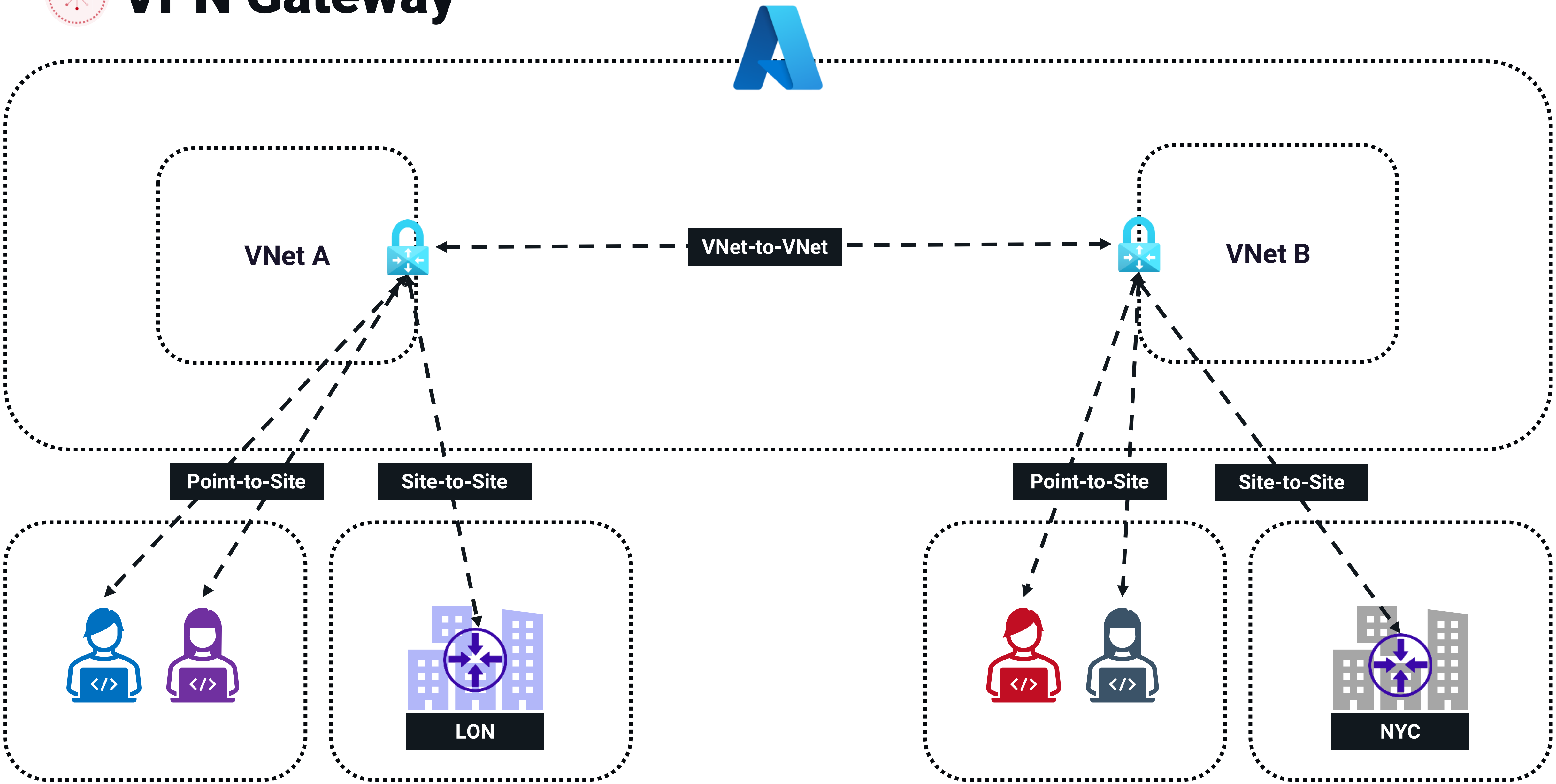
Virtual Network Peering



- Types of peering: Global VNet Peering and Regional VNet Peering.
- Uses Microsoft backbone network for data transfer, so privacy and low latency is offered in peering
- High speed data transfer, easy configuration and great performance
- Provides connectivity between Azure virtual networks. The virtual networks can reside in the same region, different region, same subscription, different subscription, same tenant or different tenant

VPN Gateway

VPN Gateway


VNet A
VNet-to-VNet
VNet B
Point-to-Site
Site-to-Site
Point-to-Site
Site-to-Site
LON
NYC

VPN Gateway SKUs

Gen	SKU	S2S/VNet-to-VNet Tunnels	P2S IKEv2 Connections	Throughput Benchmark
Gen 1	VpnGw1/Az	Max. 30	Max. 250	650 Mbps
Gen 1	VpnGw2/Az	Max. 30	Max. 500	1.0 Gbps
Gen 2	VpnGw2/Az	Max. 30	Max. 500	1.25 Gbps
Gen 1	VpnGw3/Az	Max. 30	Max. 1000	1.25 Gbps
Gen 2	VpnGw3/Az	Max. 30	Max. 1000	2.5 Gbps
Gen 2	VpnGw4/Az	Max. 100	Max. 5000	5.0 Gbps
Gen 2	VpnGw5/Az	Max. 100	Max. 10000	10.0 Gbps

✓ **SKU selection**

SKU is selected based on the number of connections and throughput you require.

✓ **Resizing**

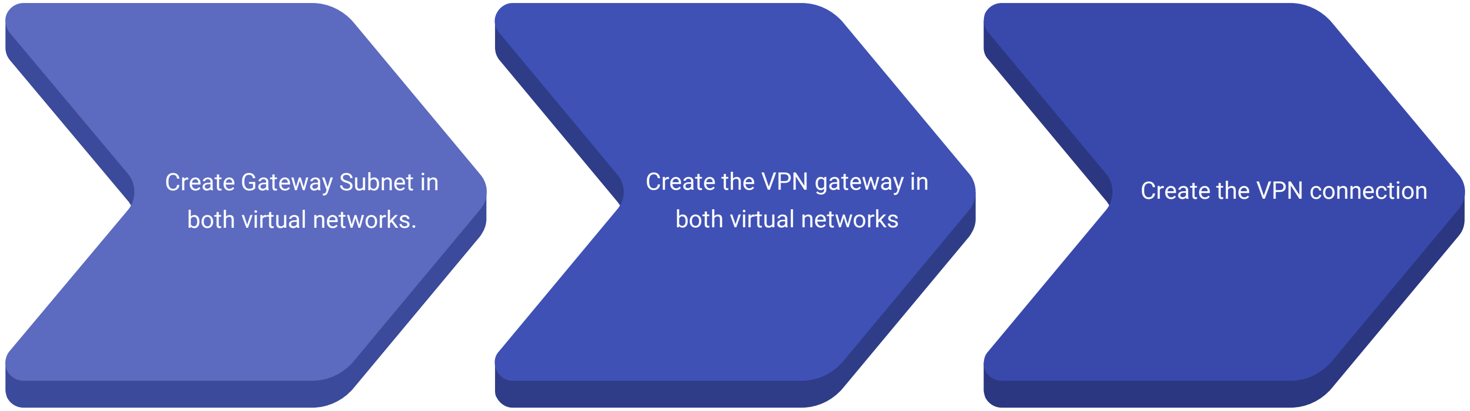
Within generation, we can resize the VPN gateway based on the requirement.

✓ **Basic SKU**

In addition to the above SKUs, we have Basic SKU which is considered as legacy and should not be used.

VNet-to-VNet Connection

Establish VNet-to-VNet connection using VPN gateways


Create Gateway Subnet in both virtual networks.
Create the VPN gateway in both virtual networks
Create the VPN connection

● **Gateway Subnet**

VPN Gateways requires a dedicated subnet to deploy the gateway. First, we need to create Gateway Subnet in both of our virtual networks.

● **VPN Gateway**

Once the Gateway Subnet is created, we will deploy the VPN gateway to the subnet. Creating a VPN gateway would take around approx.: 40 minutes.

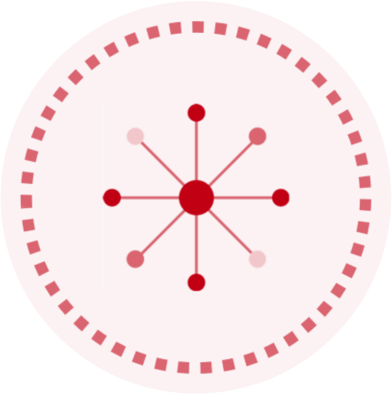
● **VNet-to-VNet connection**

After creating the VPN gateway, then we need to create VNet-to-VNet connection from the VPN Gateway

VNet Peering v/s VNet-to-VNet Connection

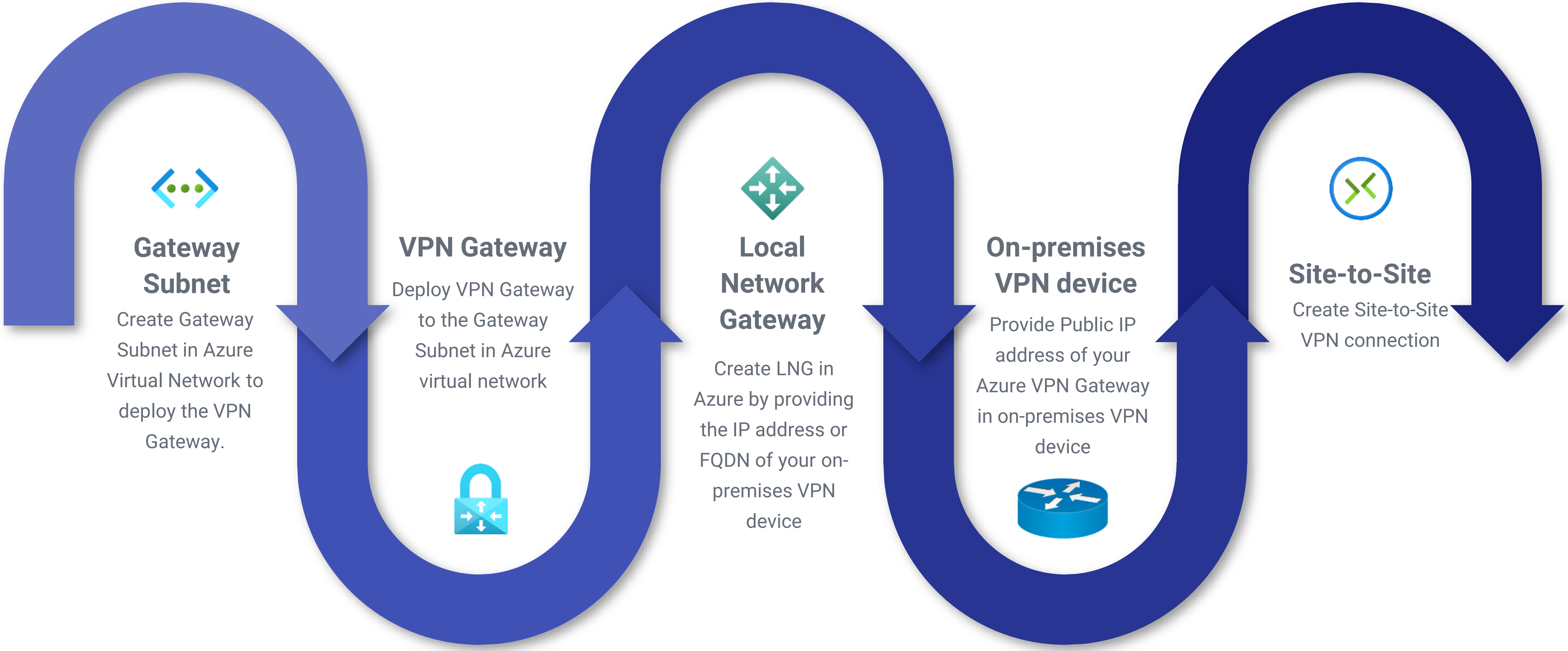
Property	VNet Peering	VNet-to-VNet Connection
Number of connections	Up to 500 VNet peerings per VNet	One VNet can have only VPN Gateway and connection count is SKU dependent
Pricing	Ingress + Egress	Gateway hourly cost + egress
Encryption	No encryption. Software level is recommended.	IPsec/IKE
Bandwidth	No restrictions	SKU dependent
Route	Routed via Microsoft backbone network and is private	Routed via public internet, however encrypted
Public IP	No public IP or internet is used	Public IP is involved
Transitivity	Nontransitive	Transitive (BGP enabled)
Initial setup time	Fast	~ 30-40 minutes
Use cases	Data replication, database failover, and other scenarios needing frequent backups of large data.	Scenarios where encryption is needed and not latency/bandwidth sensitive.

Site-to-Site and Point-to-Site



Site-to-Site connection

Connecting to your virtual network to an on-premises site or non-Azure site.



Gateway Subnet

Create Gateway Subnet in Azure Virtual Network to deploy the VPN Gateway.

VPN Gateway

Deploy VPN Gateway to the Gateway Subnet in Azure virtual network

Local Network Gateway

Create LNG in Azure by providing the IP address or FQDN of your on-premises VPN device

On-premises VPN device

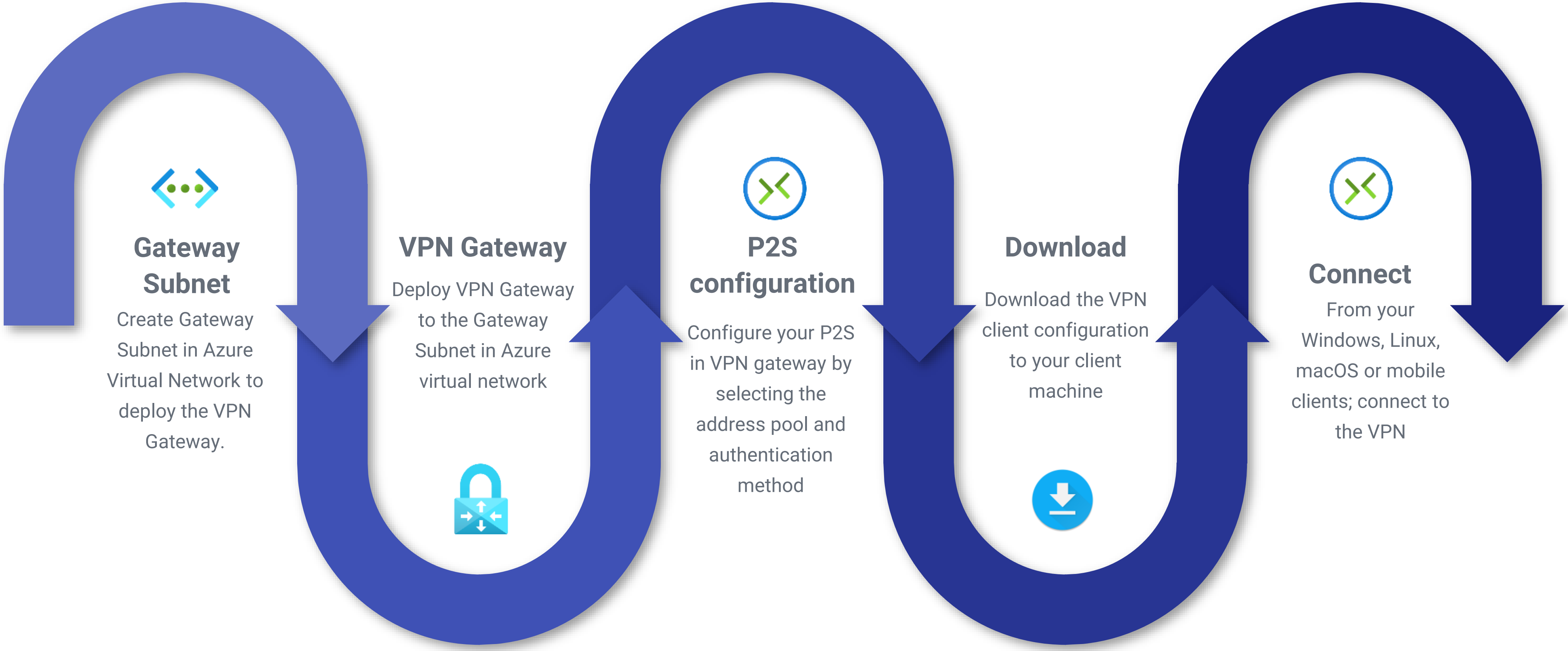
Provide Public IP address of your Azure VPN Gateway in on-premises VPN device

Site-to-Site

Create Site-to-Site VPN connection

Point-to-Site connection

Connecting to your virtual network from a device



Gateway Subnet
Create Gateway Subnet in Azure Virtual Network to deploy the VPN Gateway.

VPN Gateway
Deploy VPN Gateway to the Gateway Subnet in Azure virtual network

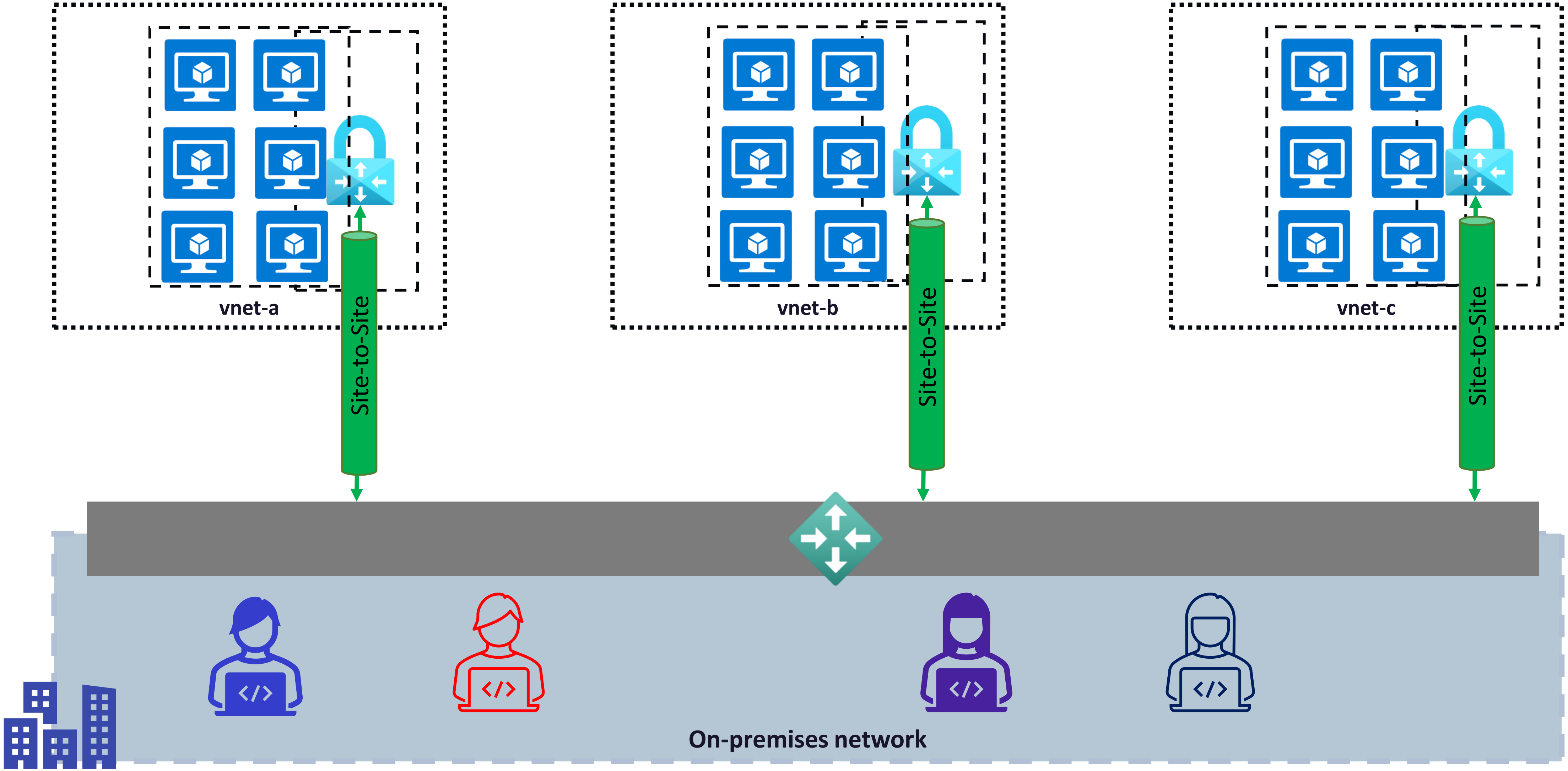
P2S configuration
Configure your P2S in VPN gateway by selecting the address pool and authentication method

Download
Download the VPN client configuration to your client machine

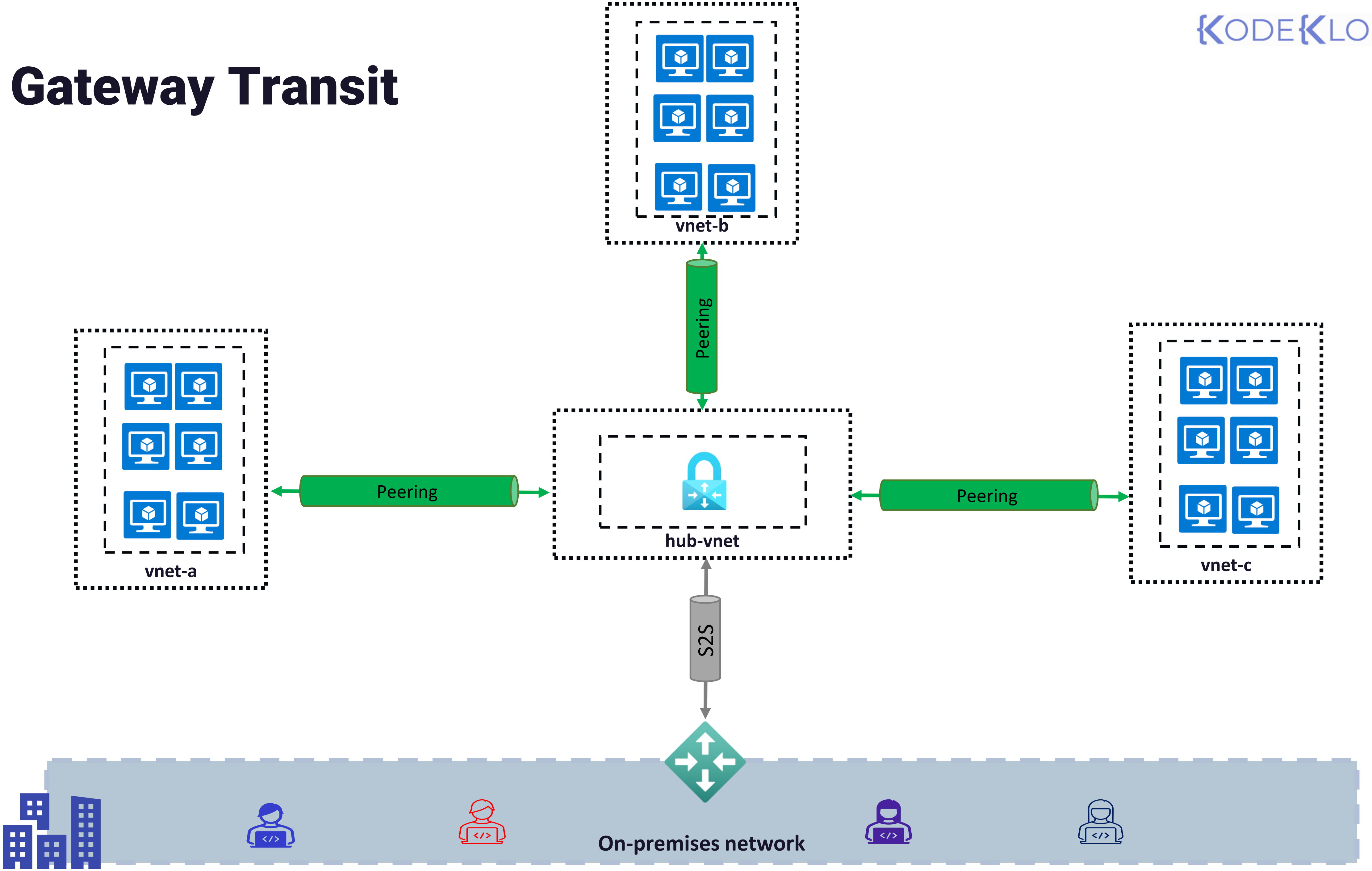
Connect
From your Windows, Linux, macOS or mobile clients; connect to the VPN

Gateway Transit

Gateway Transit

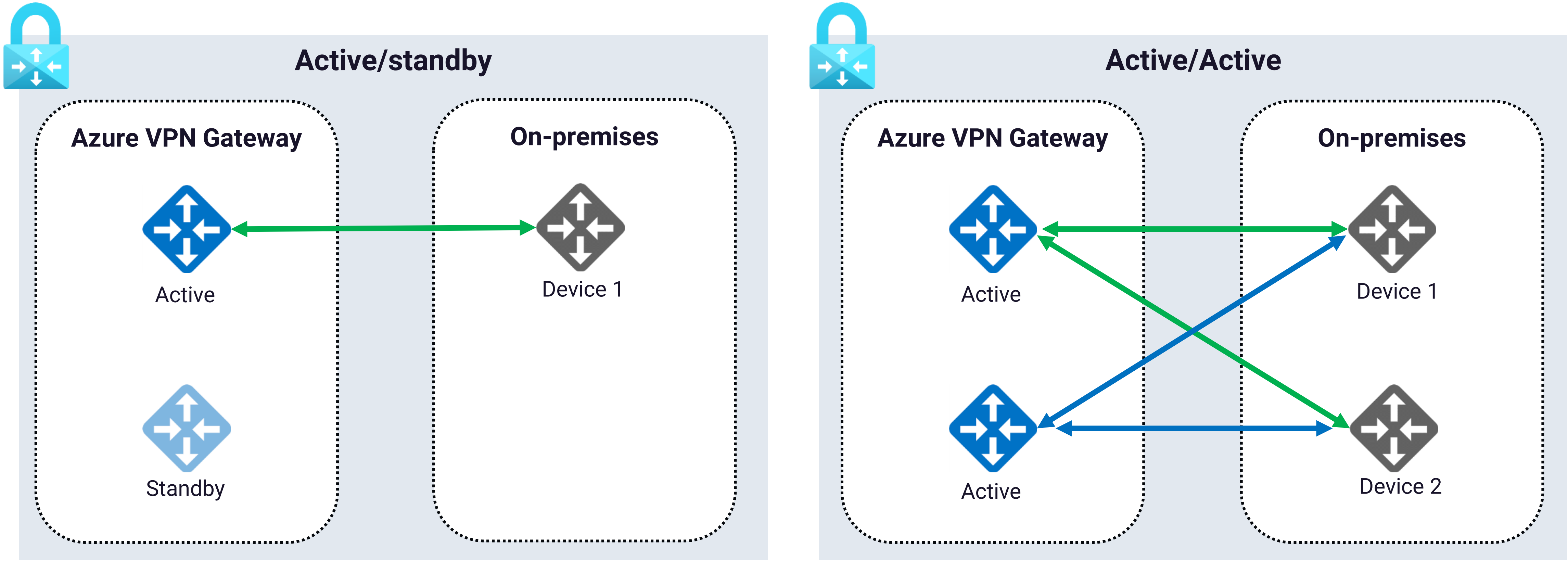


Gateway Transit



High Availability

High Availability



Default count

There will be always two instances of VPN Gateway, default selection is Active/standby

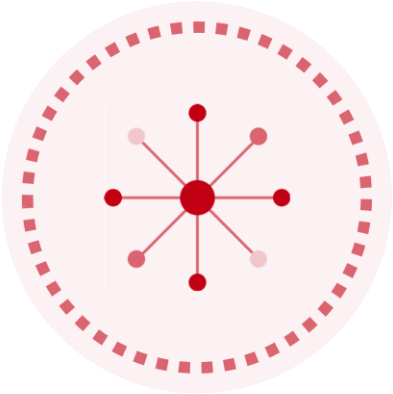
Cost

The cost of the gateway includes the cost of two instances. Regardless of whether it's active/standby or active/active cost will be same.

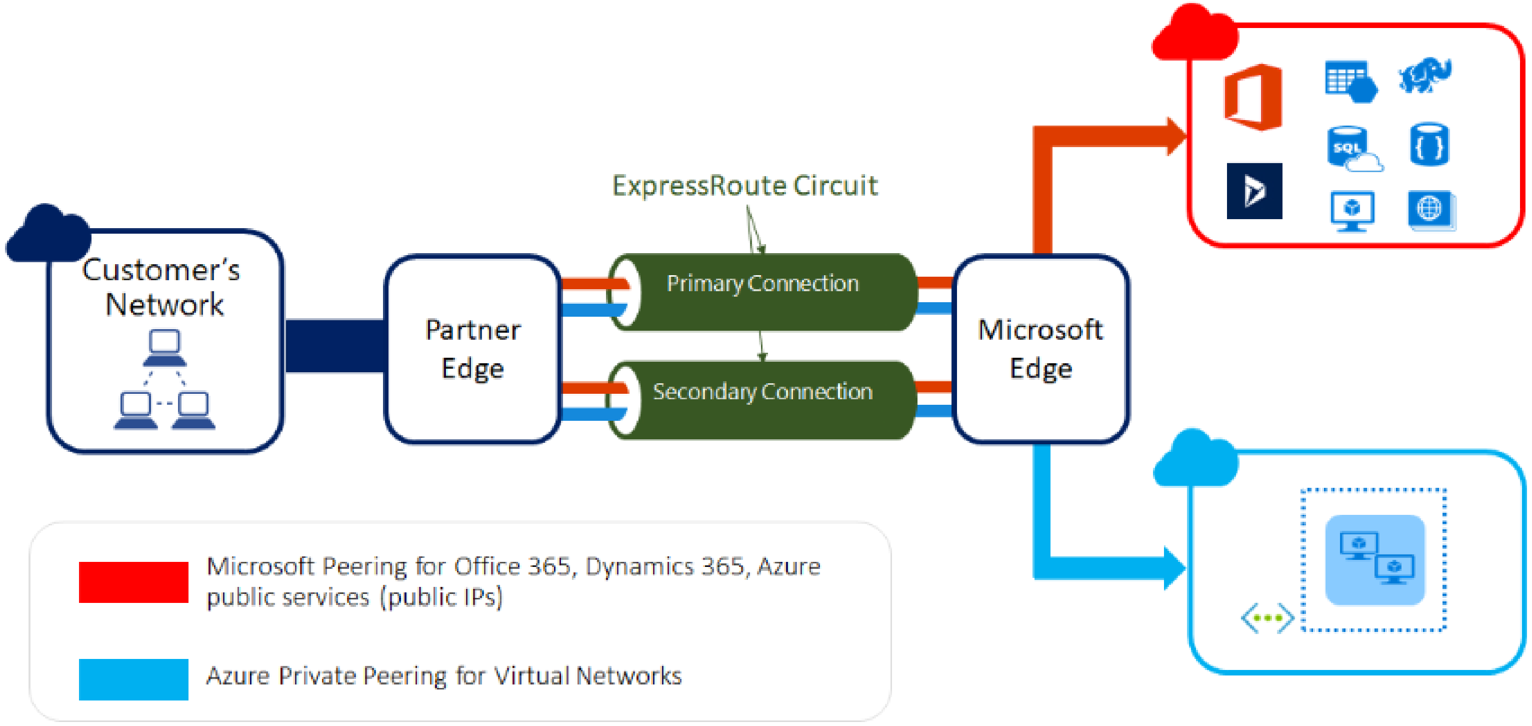
High availability

High availability can be ensured by enabling Active/active configuration. You should make sure that you have similar setup in on-premises.

ExpressRoute



ExpressRoute


ExpressRoute Circuit
Customer's Network
Partner Edge
Primary Connection
Secondary Connection
Microsoft Edge
🟥 Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
🟦 Azure Private Peering for Virtual Networks

Private connectivity

ExpressRoute offers private connectivity between on-premises infrastructure and Microsoft datacenters.

Partner network

Traffic is routed with the help of partner network and public internet is not used.

Features

Reliable, secure, low latency and high-speed connection.

Image source: https://docs.microsoft.com/en-us/learn/modules/configure-expressroute-virtual-wan/2-determine-expressroute-uses

ExpressRoute

- Redundant L3 connectivity
- Within a geography, connectivity is available to all regions
- Bandwidth options vary from 50 Mbps to 100 Gbps
- ExpressRoute circuit is offered in Local, Standard and Premium SKUs
- In Local SKU, you will be charged under the Unlimited plan. In unlimited outbound data transfer is free.
- With Standard and Premium SKU, you can select between a Metered or an Unlimited data plan. In metered, you will be charged for outbound data transfer.
- With the addition of premium add-on, you can get global connectivity.

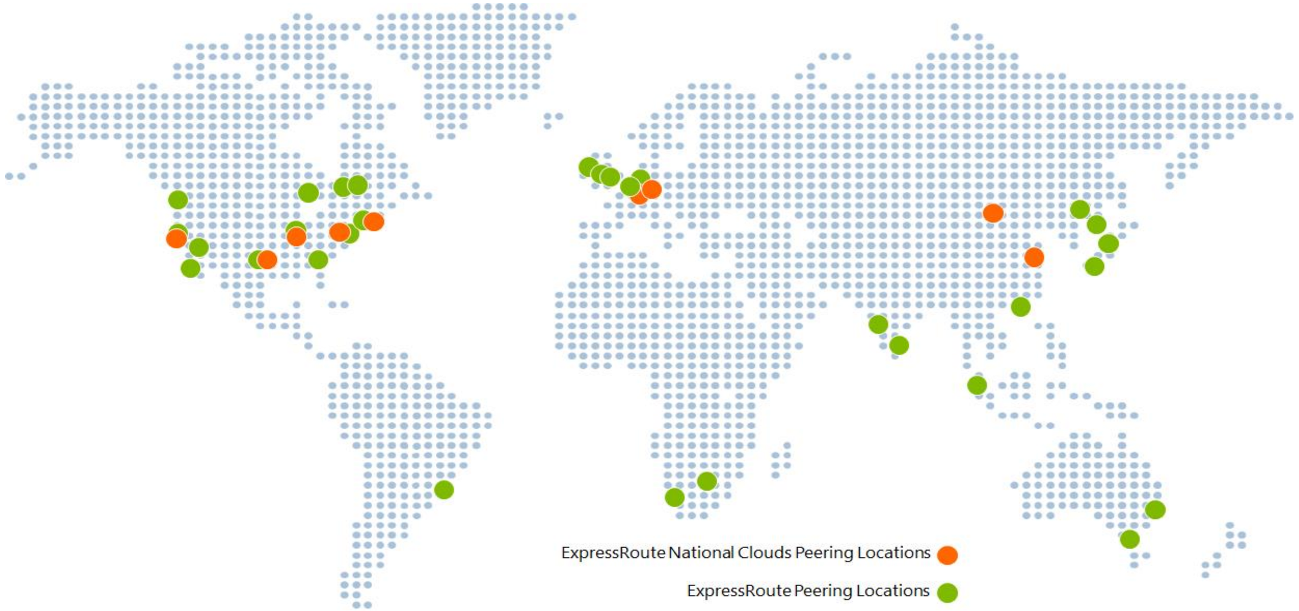

ExpressRoute National Clouds Peering Locations 🟠
ExpressRoute Peering Locations 🟢

Image source: https://docs.microsoft.com/en-us/learn/modules/configure-expressroute-virtual-wan/3-determine-expressroute-capabilities

ExpressRoute connectivity models

Co-located at a cloud exchange

If your facility is already co-located with cloud exchange, then virtual cross connections to Microsoft cloud can be provisioned through the co-location provider's Ethernet exchange. L2 and managed L3 cross connections are supported.

Point-to-Point Ethernet connection

By leveraging point-to-point Ethernet links, you can connect your on-premises network to Microsoft cloud. L2 or managed L3 connections are supported.

Any-to-Any (IPVPN)

With the integration of your WAN to Microsoft cloud, you can make it look like Microsoft cloud is one of your branch offices. Supports managed L3 connectivity.

Direct model

Establish connectivity by directly connecting to Microsoft's global network at a peering location nearby.

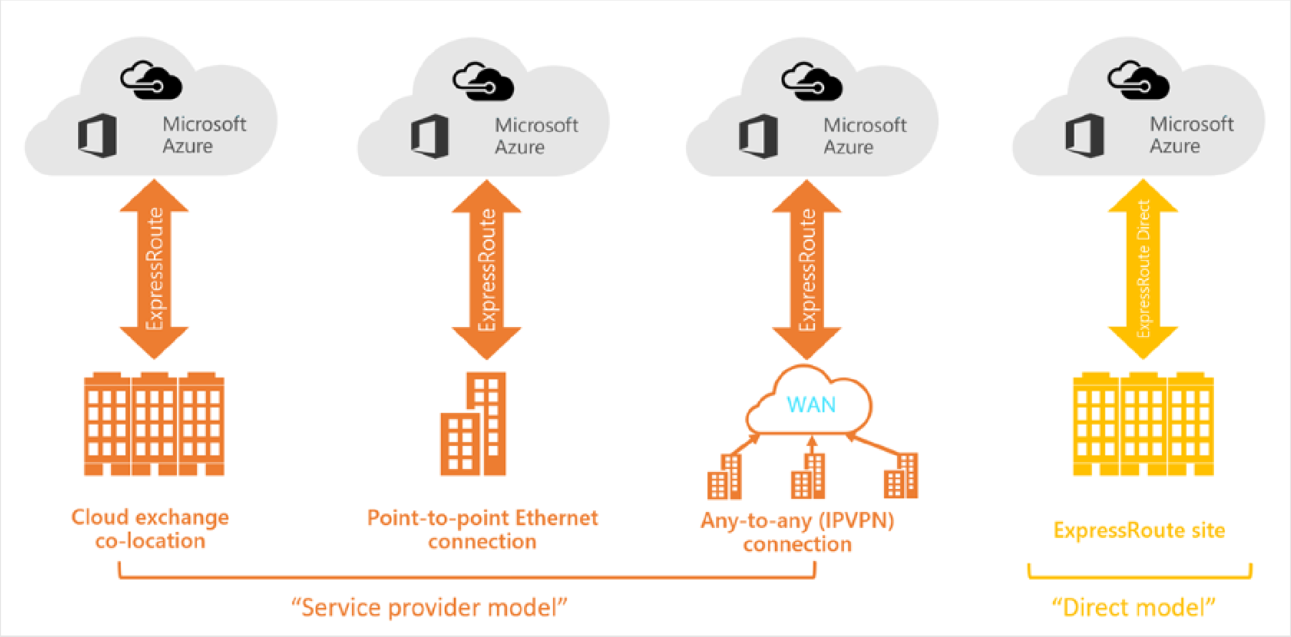
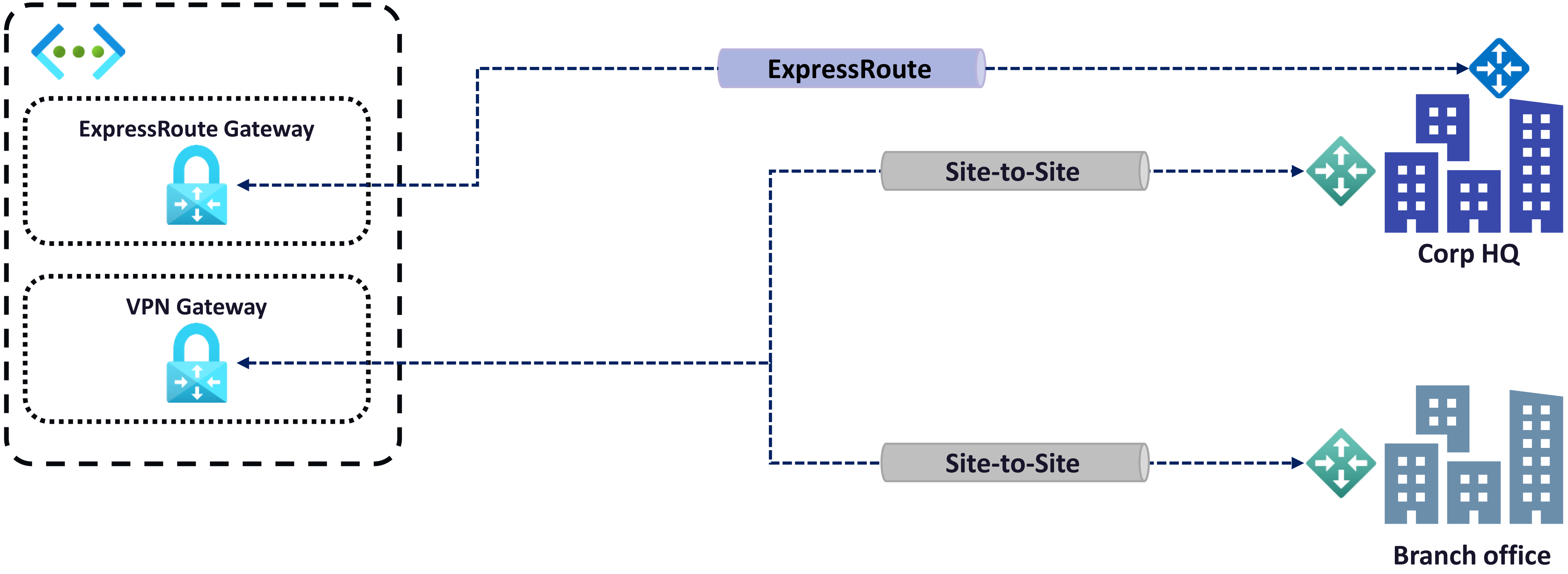


Image source: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models

Co-existing ExpressRoute and Site-to-Site



Failover path

Though ExpressRoute has redundant connection, we can use S2S connection as a failover path for ExpressRoute

Branch office connectivity

We can use S2S connectivity to connect to branch offices or other sites which are not connected to ExpressRoute.

Separate gateways

ExpressRoute and VPN requires separate gateways for communication.

Image source: https://docs.microsoft.com/en-us/learn/modules/configure-expressroute-virtual-wan/4-coexist-site-to-site-expressroute

Virtual WAN

Virtual WAN

Brings together all connections

We can connect Point-to-Site, Site-to-Site, Virtual Network and ExpressRoute connections to VWAN.

Seamless connectivity

Connects Azure virtual networks and resources to the hub seamlessly.

Advanced architecture

With the help VWAN, we can advance our hub-spoke architecture. End-to-end traffic flow can be visualized.

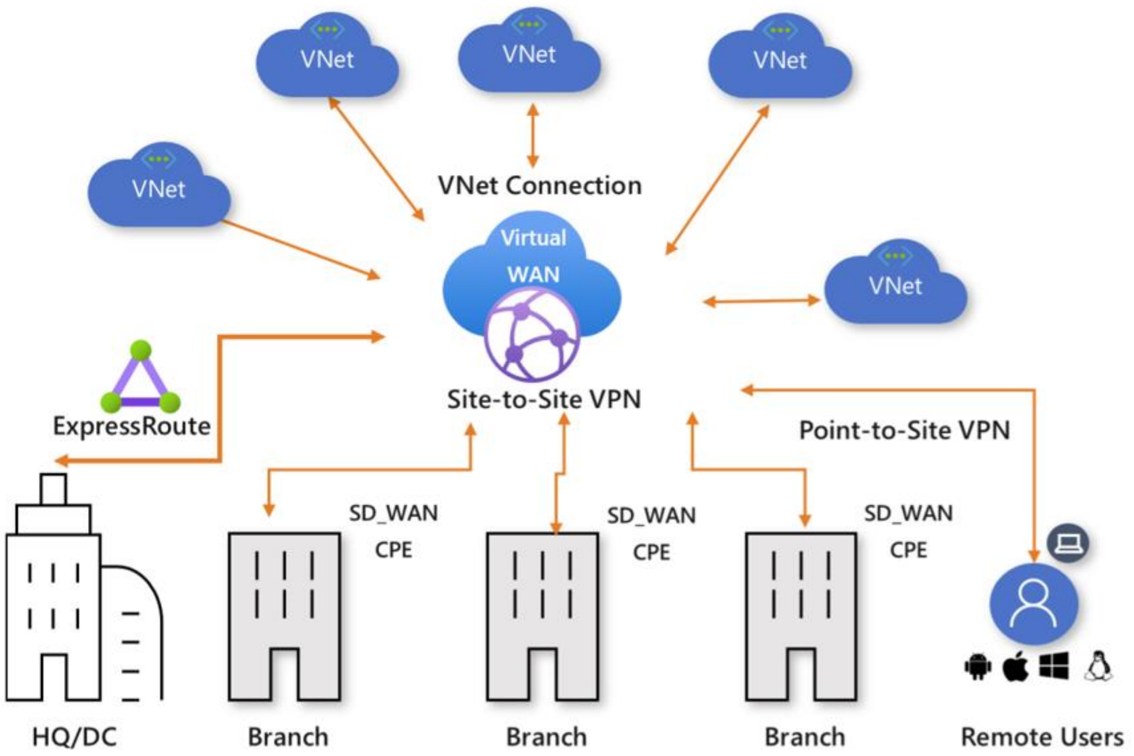
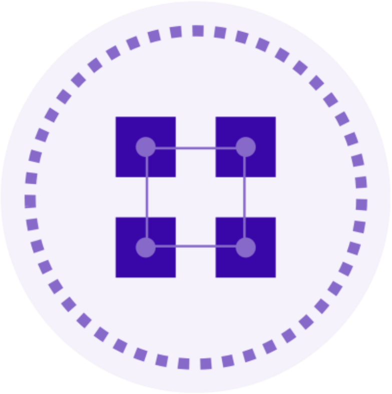


Image source: https://docs.microsoft.com/en-us/learn/modules/configure-expressroute-virtual-wan/6-determine-uses

KODEKLOUD

Creating ARM template



Azure Resource Manager

Management layer

Azure Resource Manager or ARM is the management layer responsible for creating, updating and managing resources.

Way to deploy resources

Regardless of whether you are using Azure Portal, Azure PowerShell, Azure CLI or REST API; Azure Resource Manager offers a way to deploy and manage the resources.

Features

Access Control, Locks, Tags, Resource Groups, and Templates are some of the features offered by ARM, which was not available in the previous model – Azure Service Manager

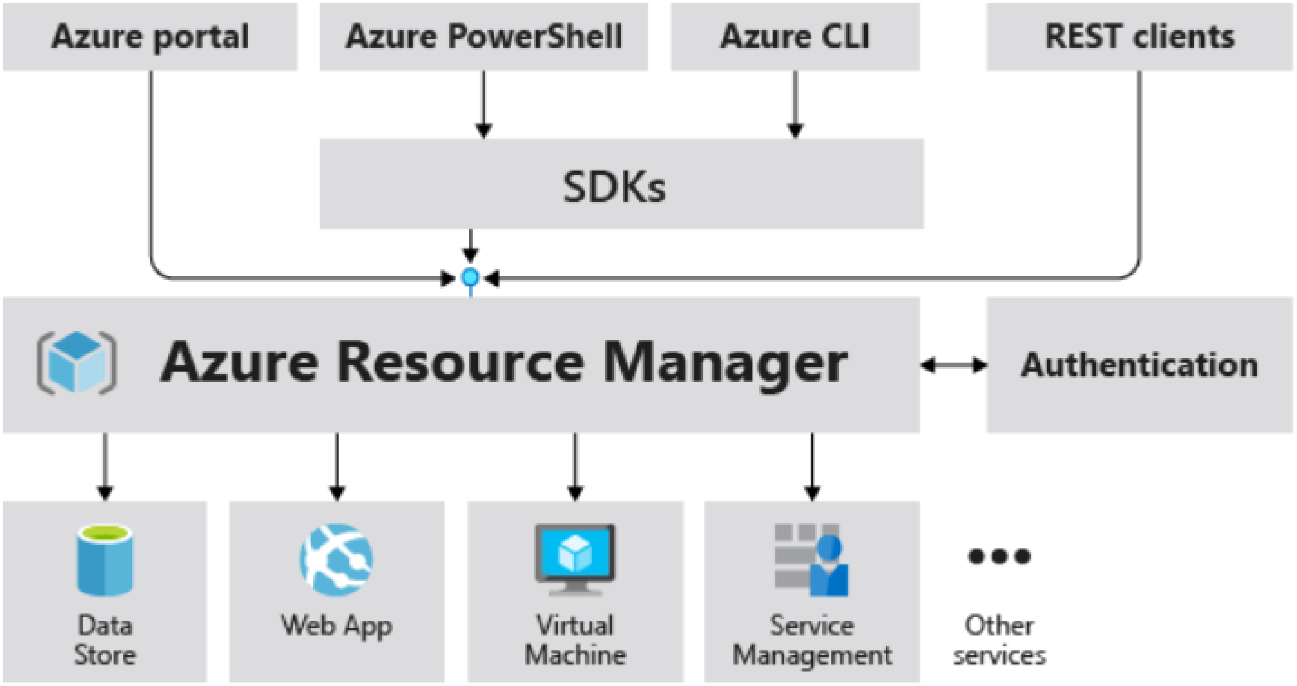


Image source: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview

Azure Resource Manager (ARM) Templates

Declarative automation

ARM templates uses JSON file. In declarative automation, you need to declare the resources but not how to create them. Creating the resources is Resource Manager’s responsibility.

Consistent and reusable

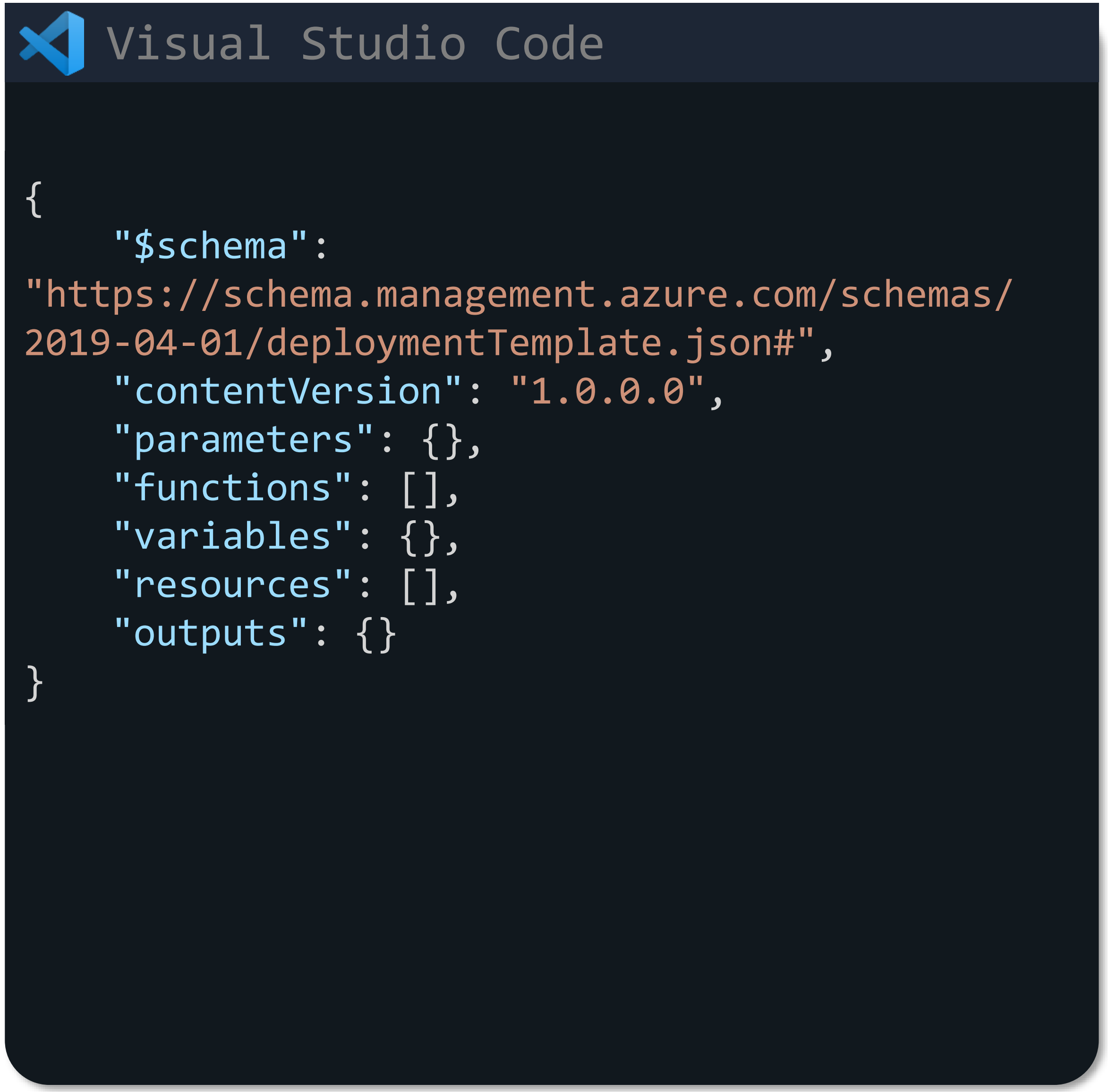
Environments deployed via ARM template will be consistent. With the help of parameters, we can share and reuse the template to create environment from scratch.

Error prone tasks and simplify deployment

If we are creating environment manually chances of human error will be there and with ARM templates, we can deploy all the resources we define in a single operation.

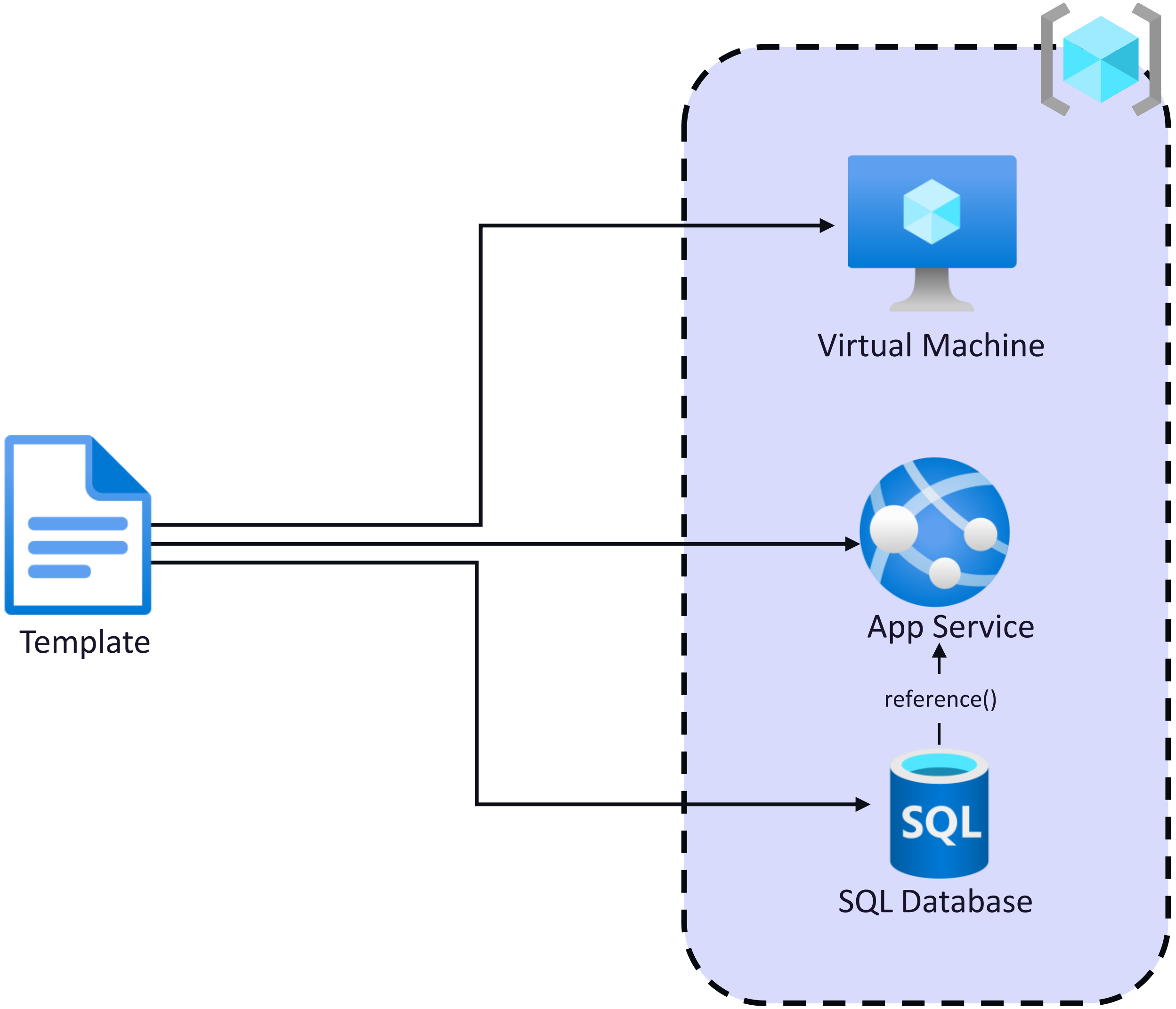
Linkable and helps complex deployment

You can write small ARM templates and link them to a parent template. This helps in managing different parts of the template efficiently. With ARM templates, we can deploy complex environments in the correct dependency order.

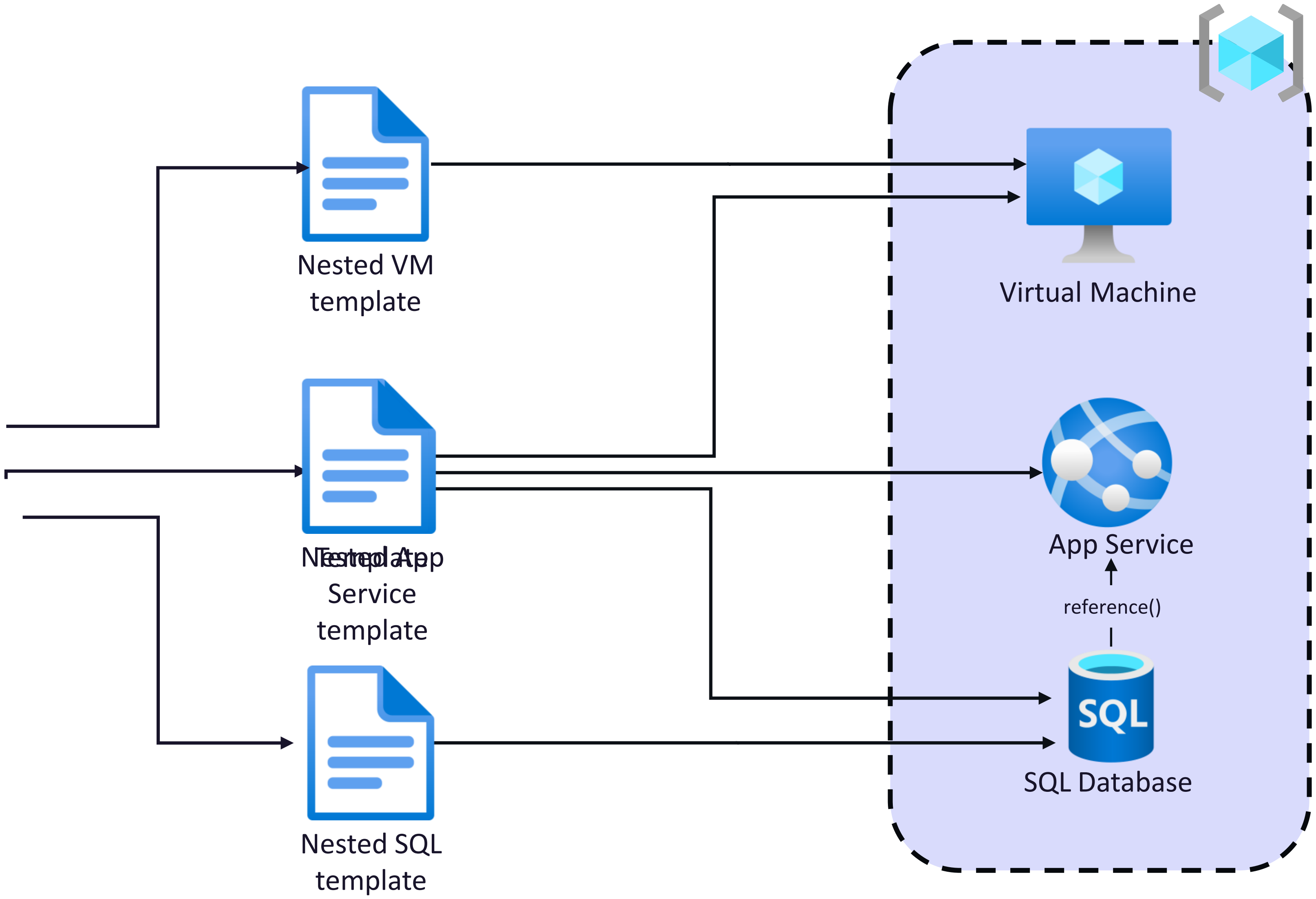


```
{
    "$schema":
"https://schema.management.azure.com/schemas/
2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {},
    "functions": [],
    "variables": {},
    "resources": [],
    "outputs": {}
}
```

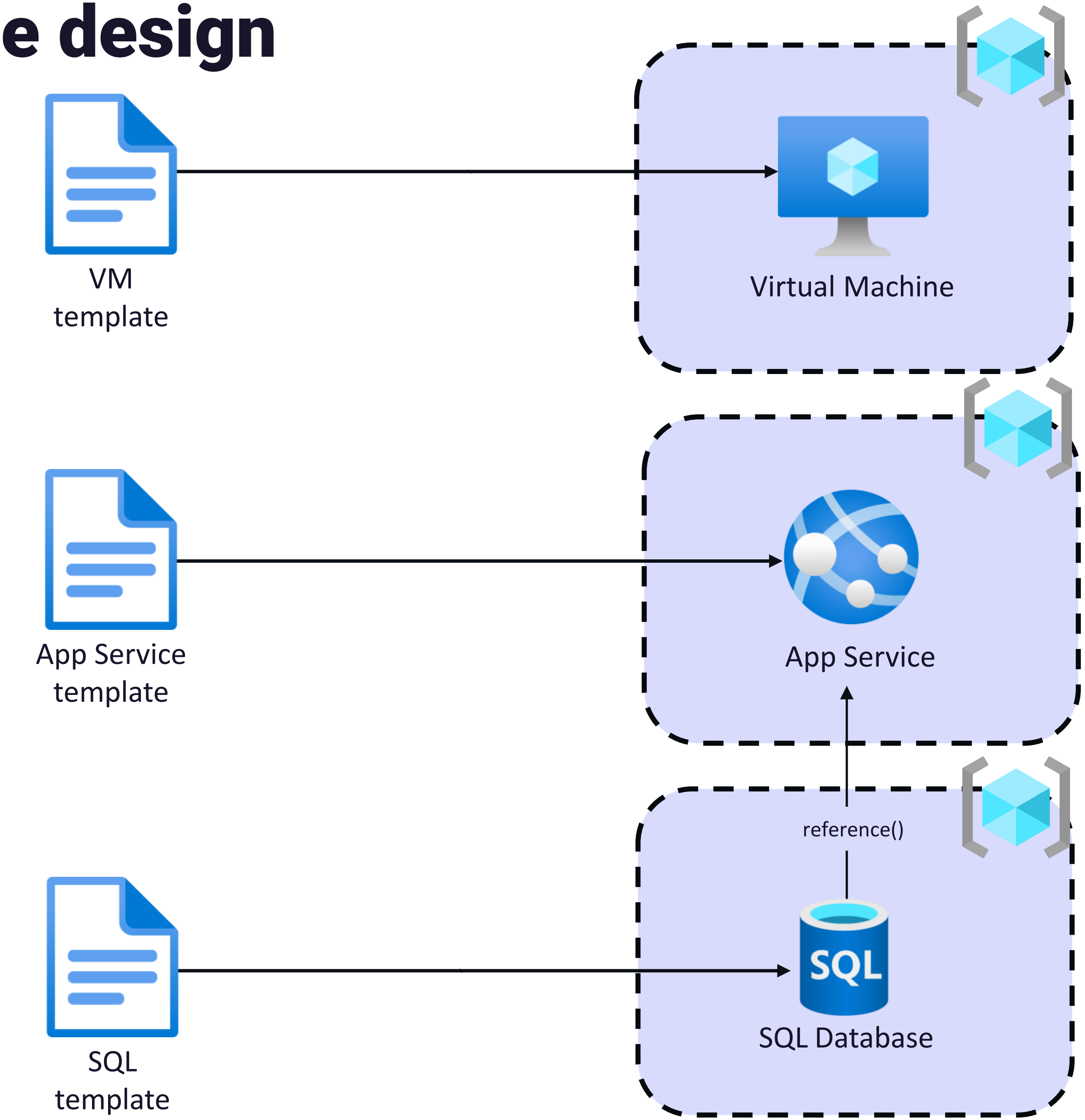
ARM template design



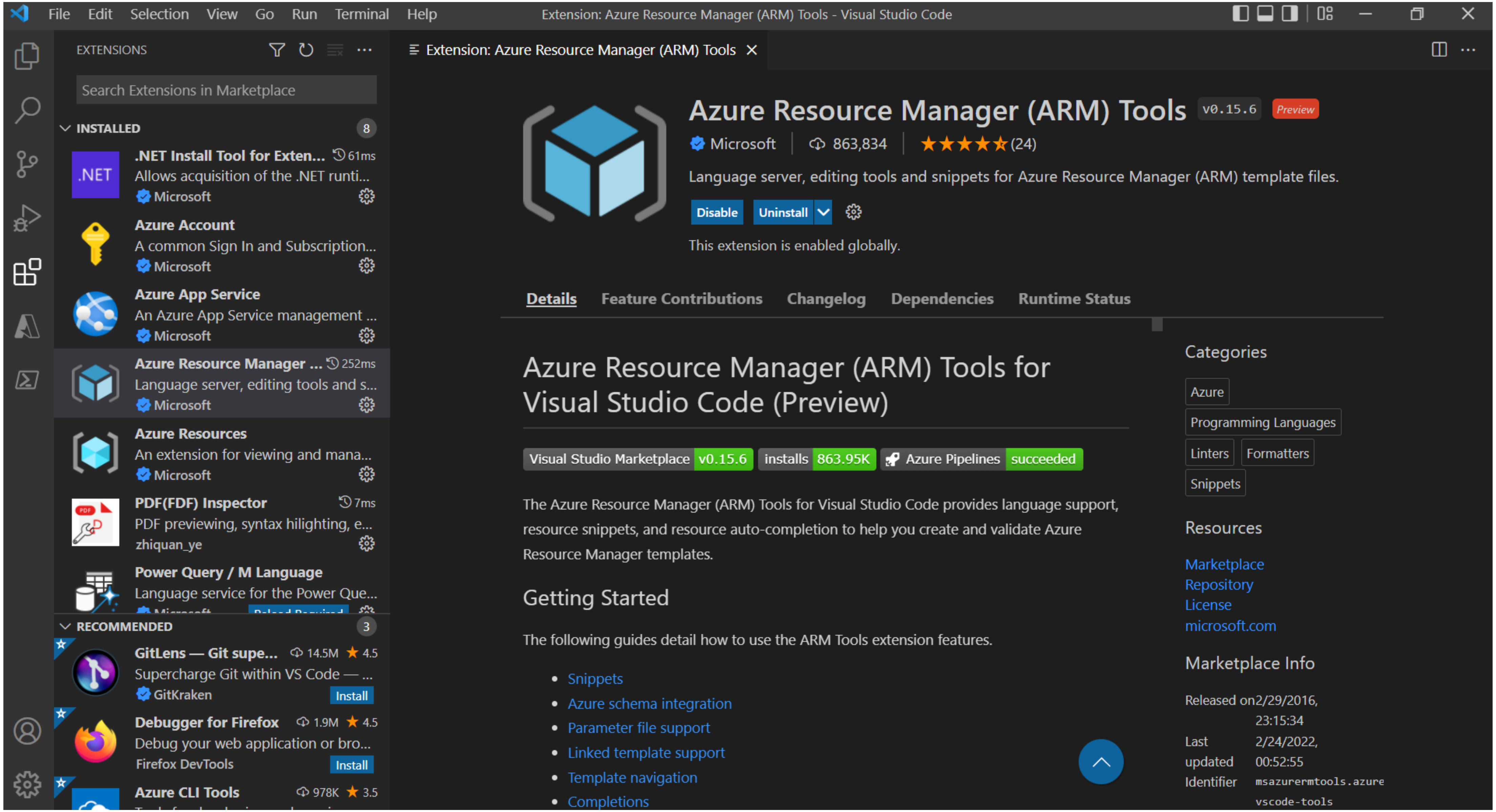
ARM template design



ARM template design



ARM Extension for VS Code (optional)


File
Edit
Selection
View
Go
Run
Terminal
Help
Extension: Azure Resource Manager (ARM) Tools - Visual Studio Code
EXTENSIONS
Search Extensions in Marketplace
Extension: Azure Resource Manager (ARM) Tools

INSTALLED 8

.NET Install Tool for Exten... 61ms
Allows acquisition of the .NET runti...
Microsoft

Azure Account
A common Sign In and Subscription...
Microsoft

Azure App Service
An Azure App Service management ...
Microsoft

Azure Resource Manager ... 252ms
Language server, editing tools and s...
Microsoft

Azure Resources
An extension for viewing and mana...
Microsoft

PDF(FDF) Inspector 7ms
PDF previewing, syntax hilighting, e...
zhiquan_ye

Power Query / M Language
Language service for the Power Que...
Microsoft Reload Required

RECOMMENDED 3

GitLens — Git supe... 14.5M ★ 4.5
Supercharge Git within VS Code — ...
GitKraken Install

Debugger for Firefox 1.9M ★ 4.5
Debug your web application or bro...
Firefox DevTools Install

Azure CLI Tools 978K ★ 3.5

Azure Resource Manager (ARM) Tools v0.15.6 Preview

Microsoft | 863,834 | ★★★★★ (24)

Language server, editing tools and snippets for Azure Resource Manager (ARM) template files.

Disable | Uninstall

This extension is enabled globally.

Details | Feature Contributions | Changelog | Dependencies | Runtime Status

Azure Resource Manager (ARM) Tools for Visual Studio Code (Preview)

Visual Studio Marketplace v0.15.6 | installs 863.95K | Azure Pipelines succeeded

The Azure Resource Manager (ARM) Tools for Visual Studio Code provides language support, resource snippets, and resource auto-completion to help you create and validate Azure Resource Manager templates.

Getting Started

The following guides detail how to use the ARM Tools extension features.

- Snippets
- Azure schema integration
- Parameter file support
- Linked template support
- Template navigation
- Completions

Categories

Azure
Programming Languages
Linters
Formatters
Snippets

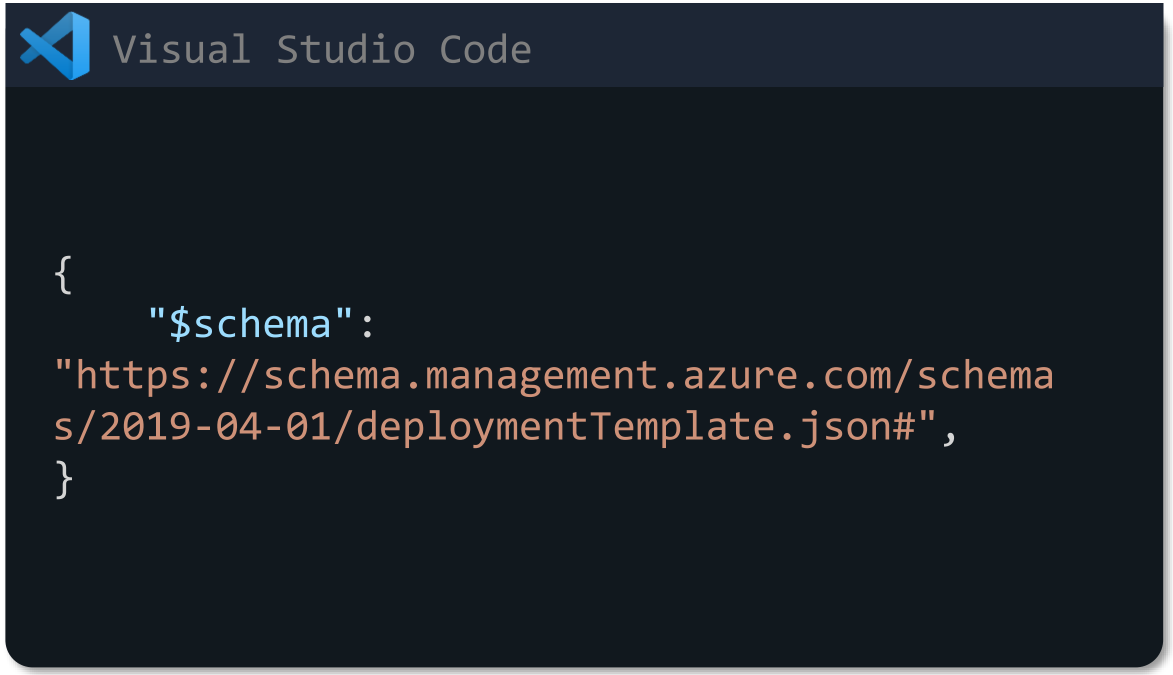
Resources

Marketplace
Repository
License
microsoft.com

Marketplace Info

Released on2/29/2016, 23:15:34
Last updated 2/24/2022, 00:52:55
Identifier msazurermtools.azurevscode-tools

ARM Template structure

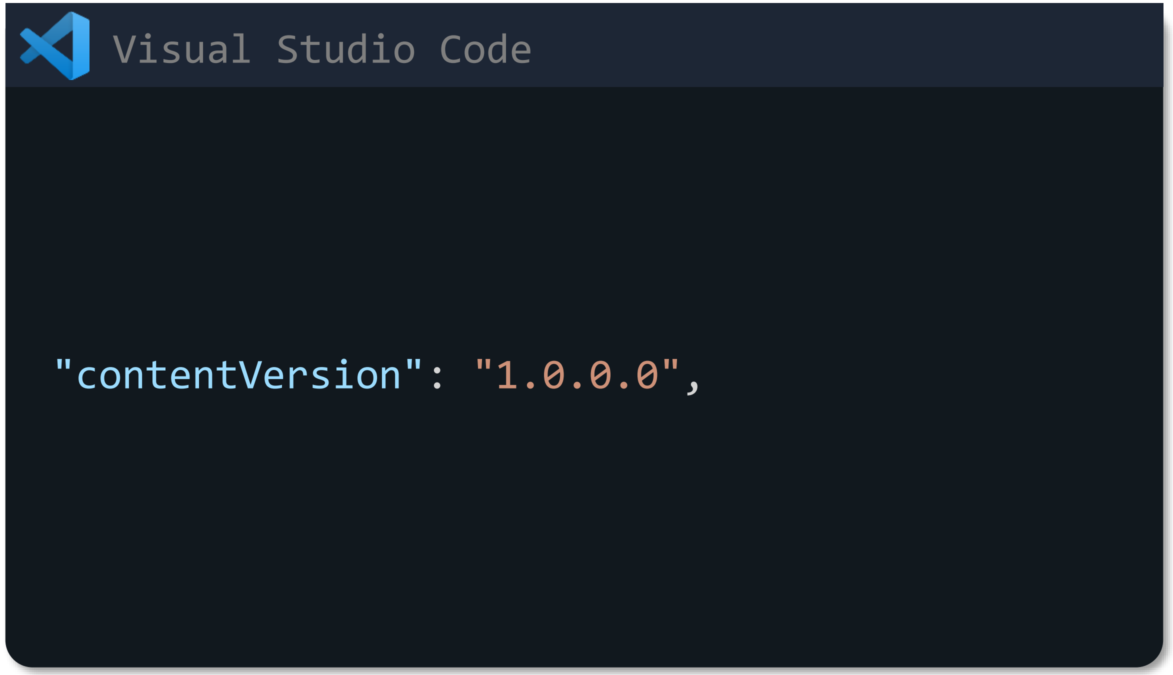


```
{
    "$schema":
"https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
}
```

$schema*

References the location of the JSON file schema that describes the version of the template language. We can deploy ARM templates to different scopes like tenant, management groups, subscriptions; based on the scope that we are selecting the schema will change.

ARM Template structure

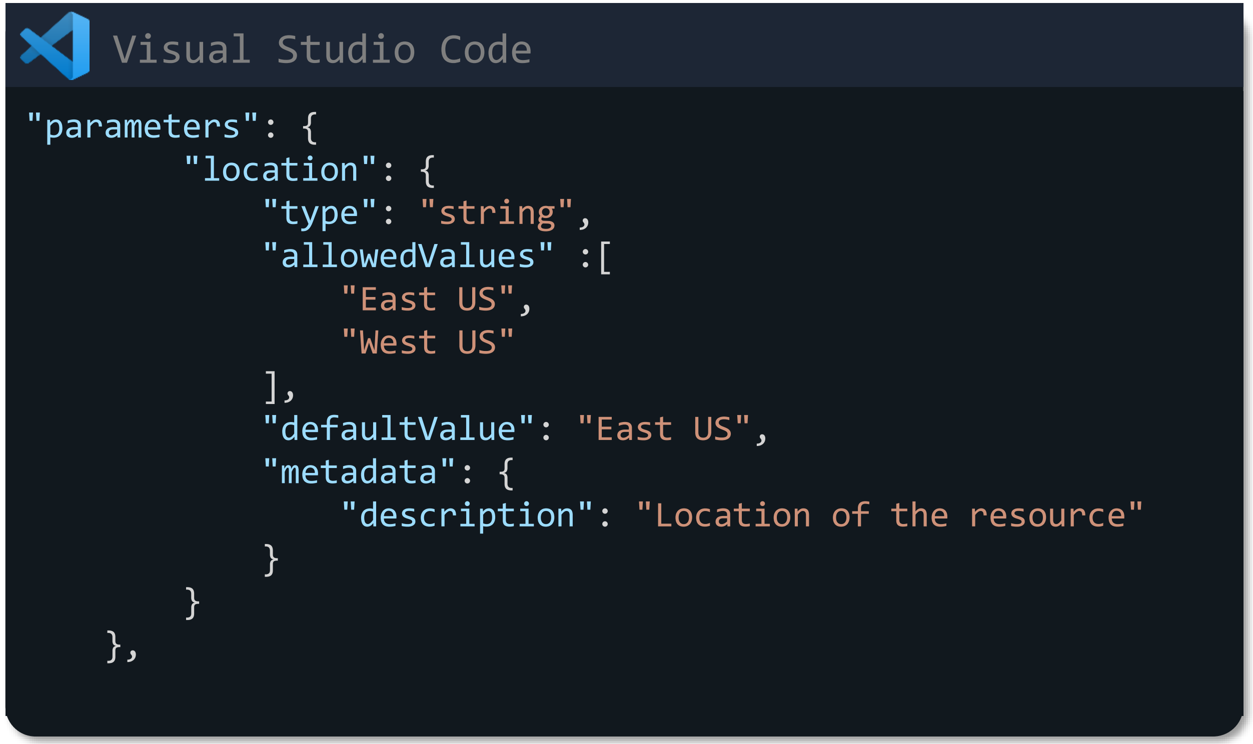


```
"contentVersion": "1.0.0.0",
```

contentVersion*

Used to version the template, the default value is 1.0.0.0. Any value can be given to this element. Content version is useful if you are storing your templates in a source control and would like to keep the changes tracked in different versions. Proper versioning will help users to pick the latest version of your template.

ARM Template structure

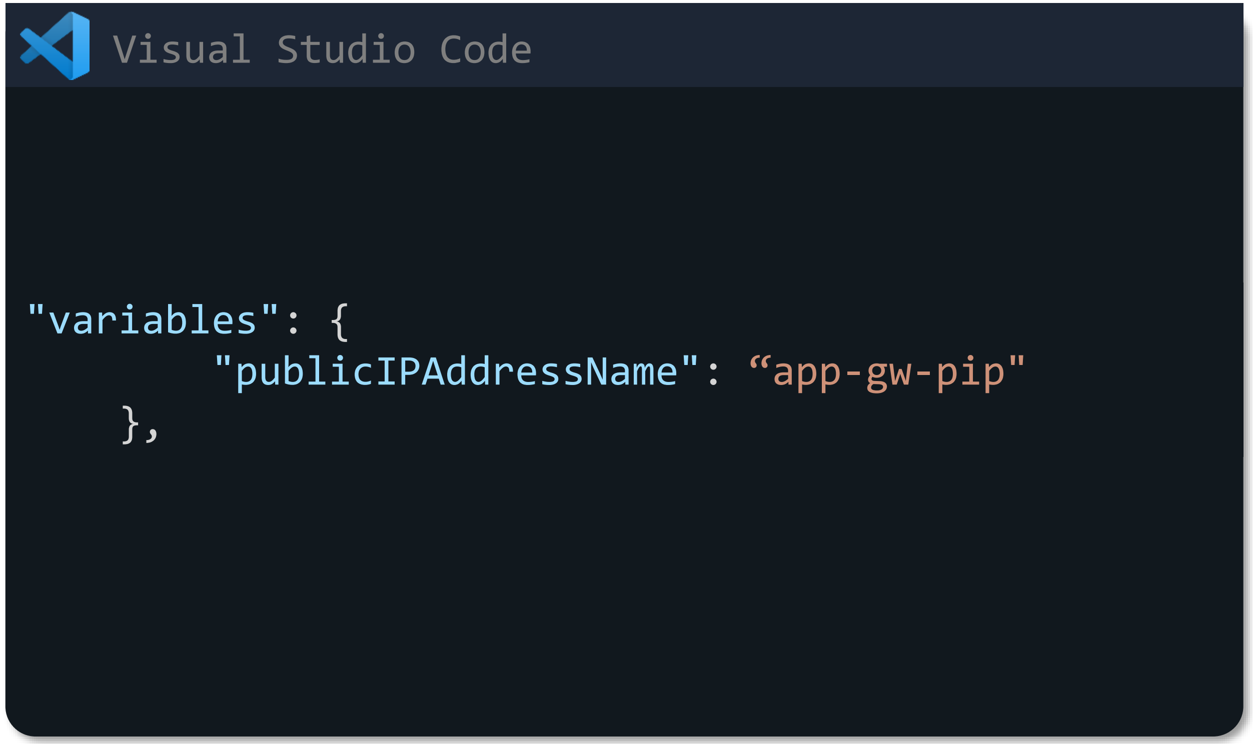


```
"parameters": {
        "location": {
            "type": "string",
            "allowedValues" :[
                "East US",
                "West US"
            ],
            "defaultValue": "East US",
            "metadata": {
                "description": "Location of the resource"
            }
        }
    },
```

parameters

During resource deployment, the parameter value can be provided as an input to the template. Parameters helps making the templates reusable, where users can supply different values during execution without the need to modify the template.

ARM Template structure

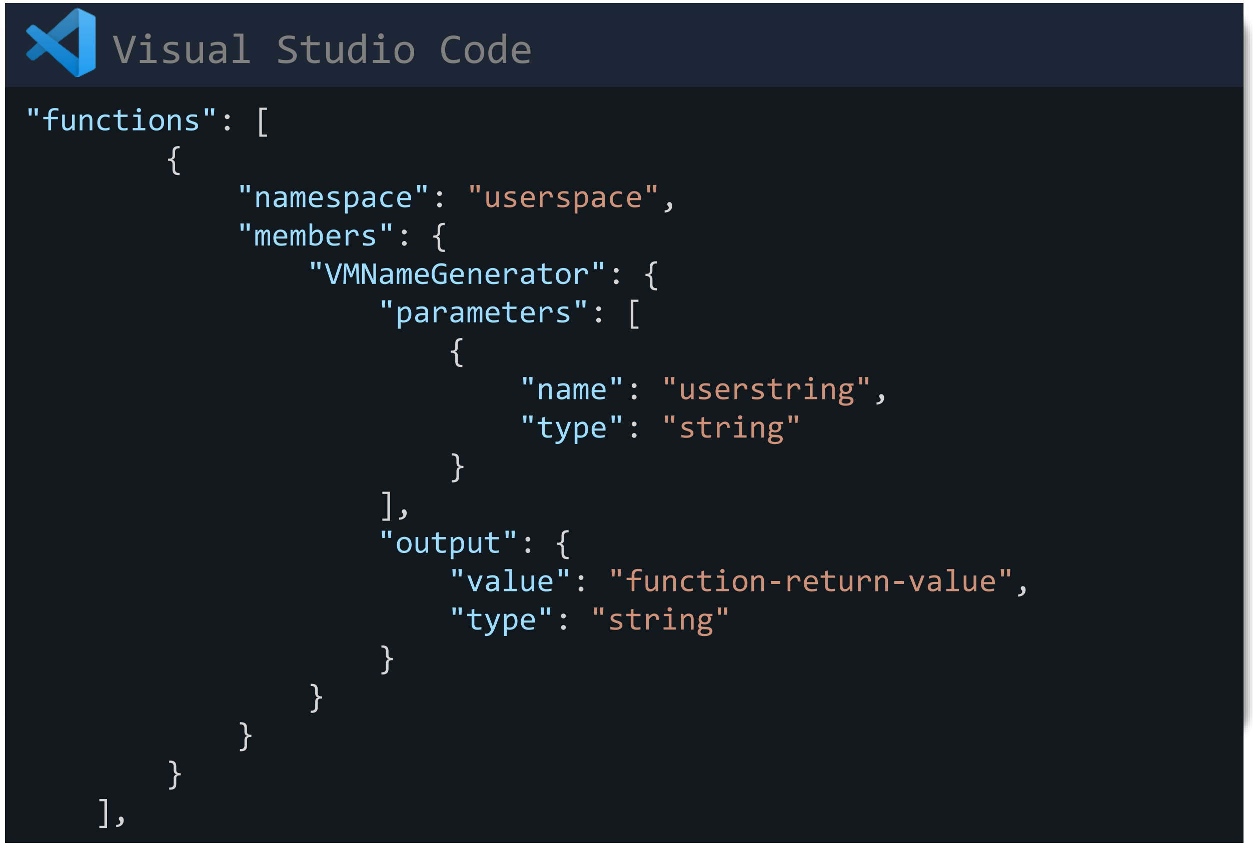


```
"variables": {
        "publicIPAddressName": “app-gw-pip"
    },
```

variables

Variables can be used to hardcode value to the templates. If you are referencing a value with the help of variables and if that value needs to be modified; instead of updating all occurrences, you just need to update the value of the variable.

ARM Template structure

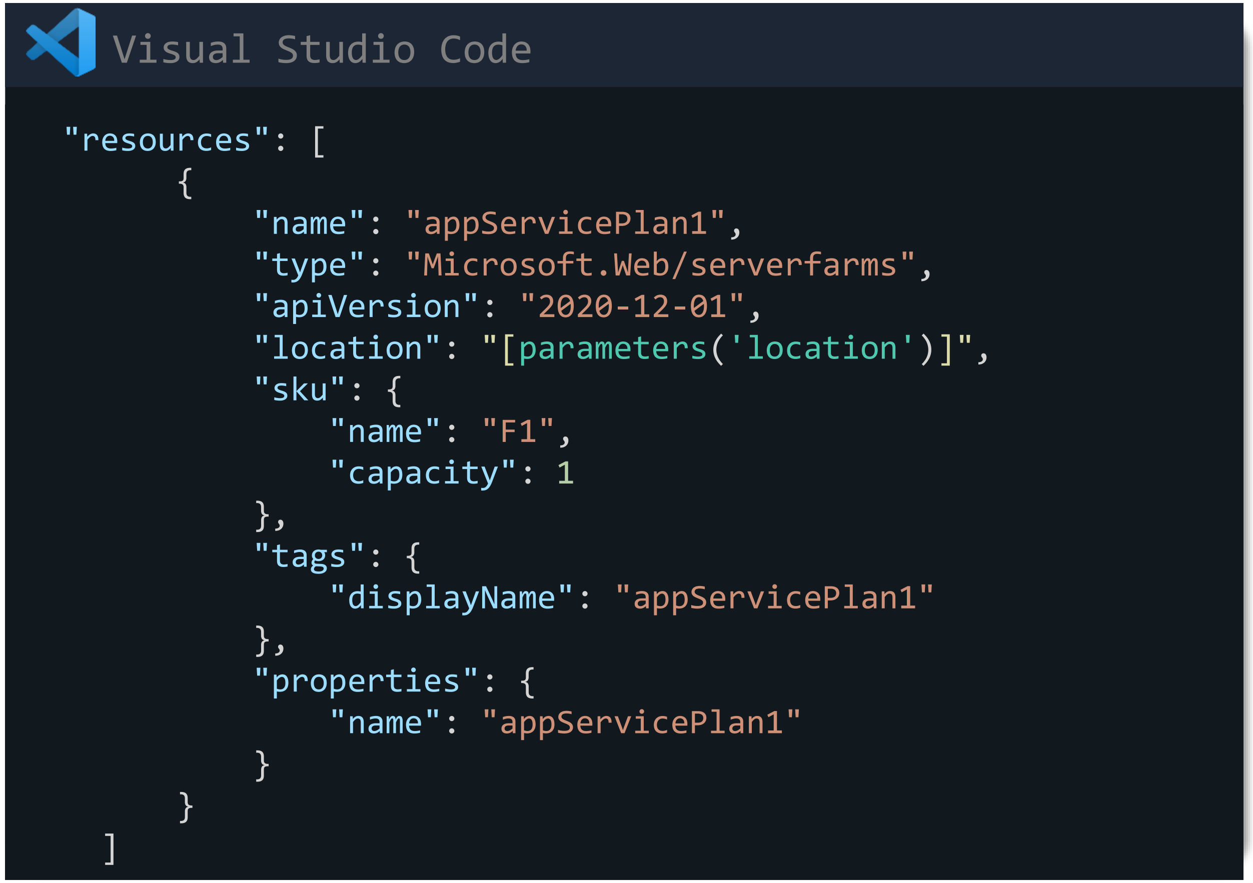


```
"functions": [
        {
            "namespace": "userspace",
            "members": {
                "VMNameGenerator": {
                    "parameters": [
                        {
                            "name": "userstring",
                            "type": "string"
                        }
                    ],
                    "output": {
                        "value": "function-return-value",
                        "type": "string"
                    }
                }
            }
        }
    ],
```

functions

We can create user defined functions in ARM templates that can be used to replace repeated code blocks.

ARM Template structure

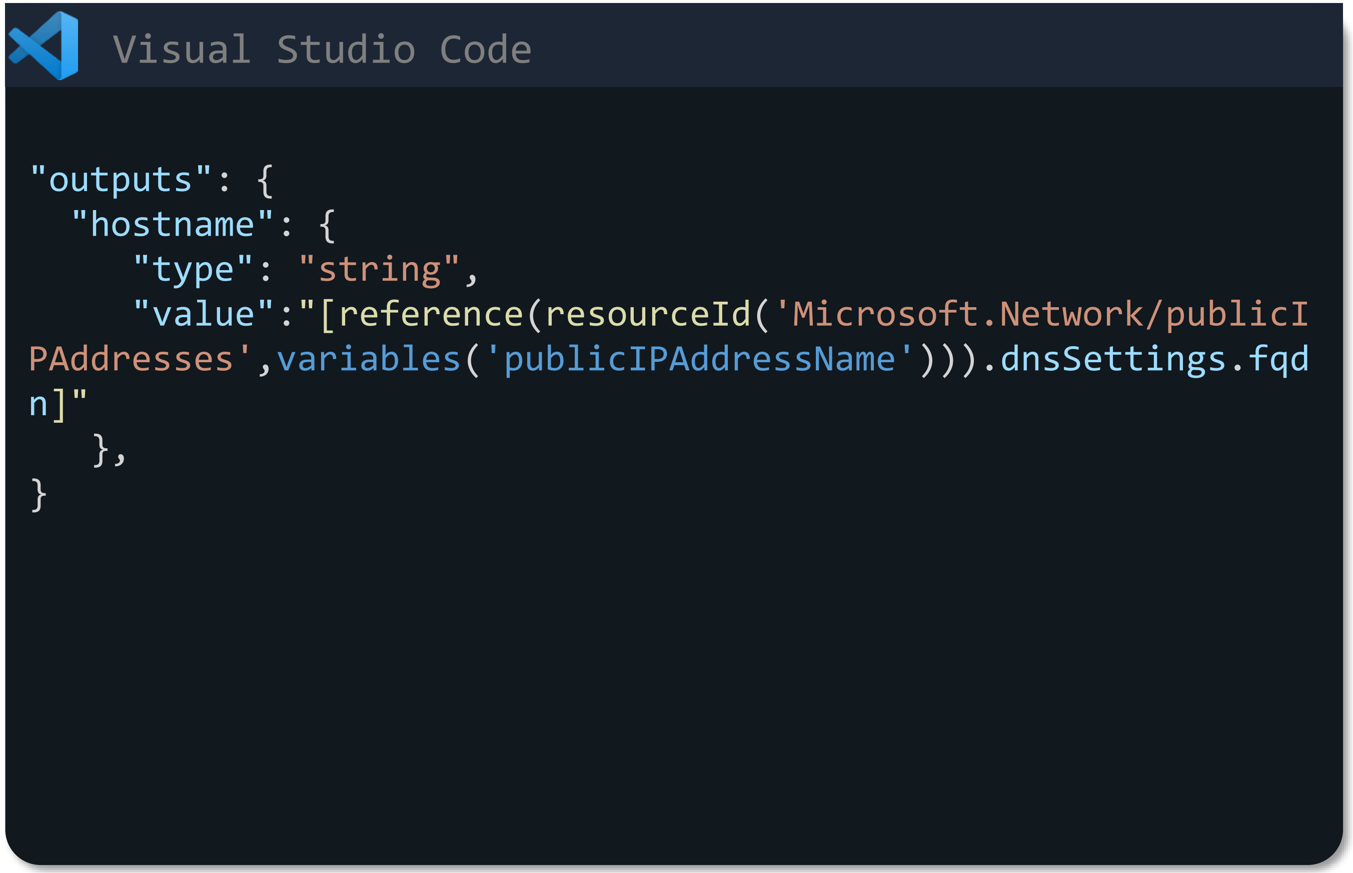


```
"resources": [
   {
     "name": "appServicePlan1",
     "type": "Microsoft.Web/serverfarms",
     "apiVersion": "2020-12-01",
     "location": "[parameters('location')]",
     "sku": {
       "name": "F1",
       "capacity": 1
     },
     "tags": {
       "displayName": "appServicePlan1"
     },
     "properties": {
       "name": "appServicePlan1"
     }
   }
 ]
```

resources*

Resources we intend to create, or update will be declared inside this element. Here, we can reference the parameters, variables, and functions we created earlier.

ARM Template structure

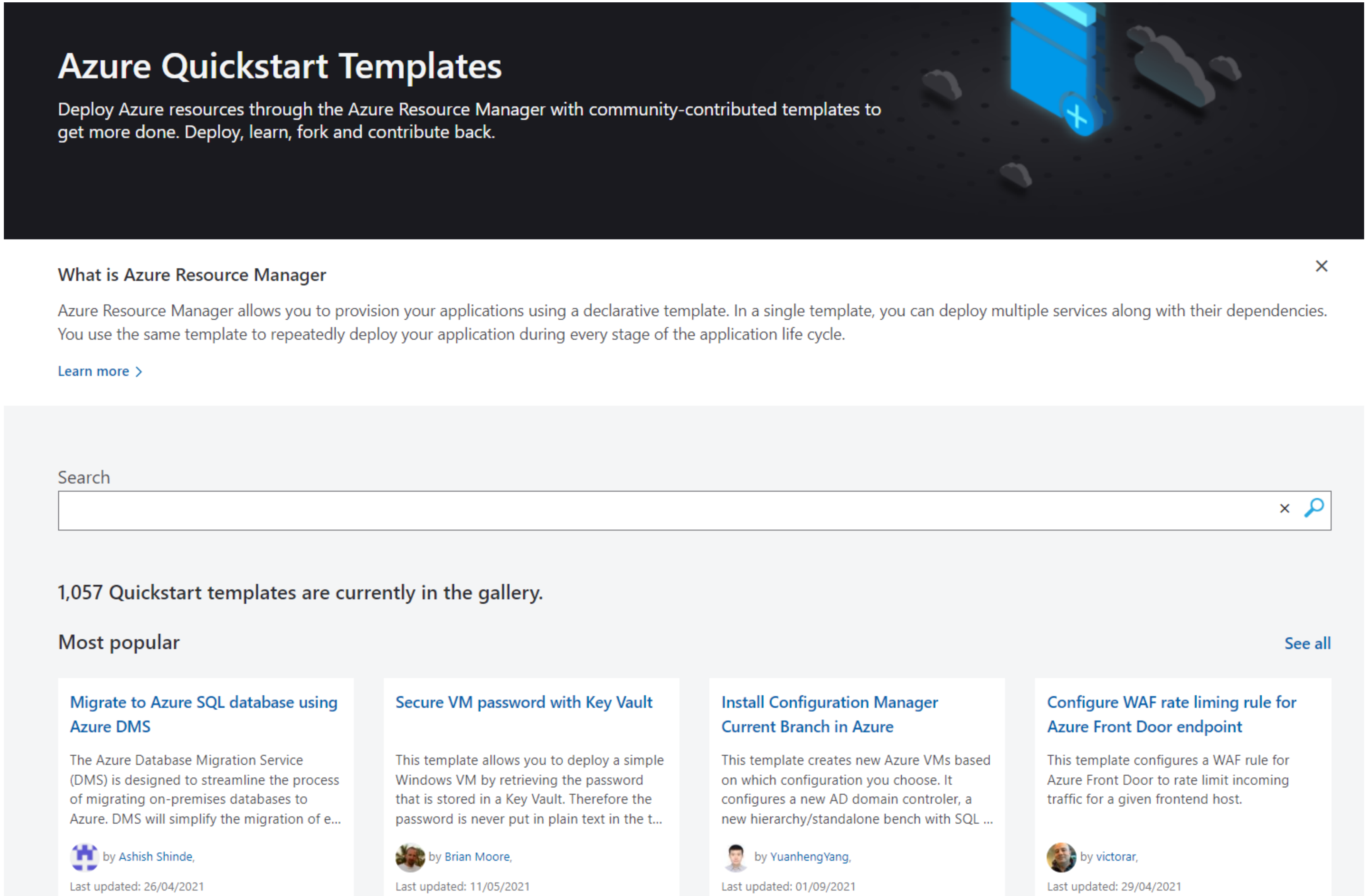


```
"outputs": {
  "hostname": {
     "type": "string",
     "value":"[reference(resourceId('Microsoft.Network/publicIPAddresses',variables('publicIPAddressName'))).dnsSettings.fqdn]"
   },
}
```

outputs

Display values that are returned after deployment.

Azure Quickstart Templates



Azure Quickstart Templates

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

What is Azure Resource Manager

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

Learn more >

Search

1,057 Quickstart templates are currently in the gallery.

Most popular

See all

Migrate to Azure SQL database using Azure DMS

The Azure Database Migration Service (DMS) is designed to streamline the process of migrating on-premises databases to Azure. DMS will simplify the migration of e...

by Ashish Shinde,

Last updated: 26/04/2021

Secure VM password with Key Vault

This template allows you to deploy a simple Windows VM by retrieving the password that is stored in a Key Vault. Therefore the password is never put in plain text in the t...

by Brian Moore,

Last updated: 11/05/2021

Install Configuration Manager Current Branch in Azure

This template creates new Azure VMs based on which configuration you choose. It configures a new AD domain controler, a new hierarchy/standalone bench with SQL ...

by YuanhengYang,

Last updated: 01/09/2021

Configure WAF rate liming rule for Azure Front Door endpoint

This template configures a WAF rule for Azure Front Door to rate limit incoming traffic for a given frontend host.

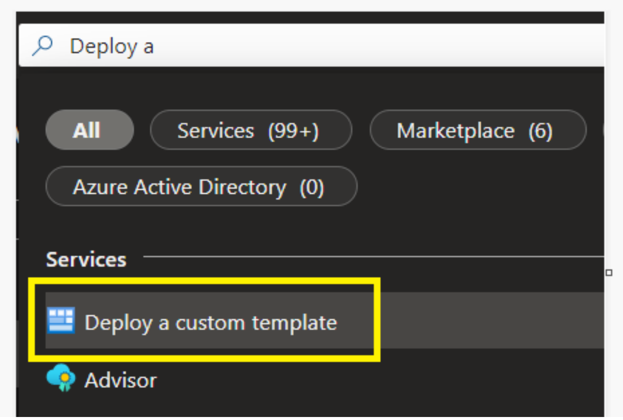
by victorar,

Last updated: 29/04/2021

Deploy ARM template

Deploy ARM template

Azure Portal



Deploy a

Azure CLI

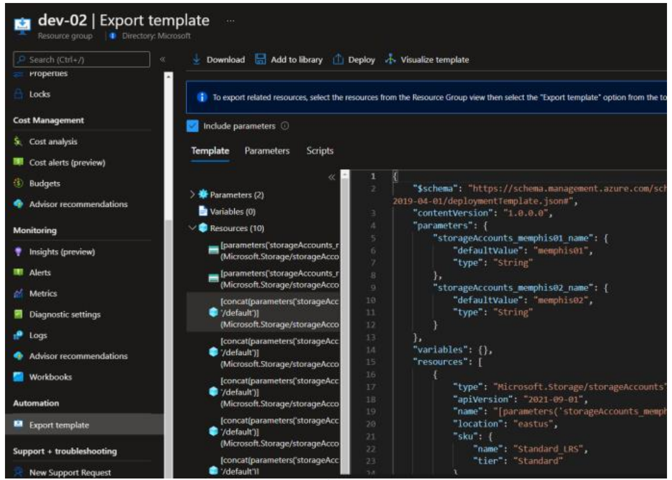
```
>_ Azure CLI

$ az group deployment create \
-g <resource-group-name>
--template-file <path-to-file>
```

Azure PowerShell

```
>_ Azure PowerShell

$ New-AzResourceGroupDeployment `
-ResourceGroupName <resourcegroup> `
-TemplateFile <path-to-file>
```

Exporting deployments as ARM template

Exporting deployments as ARM template



To export related resources, select the resources from the Resource Group view then select the "Export template" option from the to

☑ Include parameters

[parameters('storageAccounts_r
(Microsoft.Storage/storageAcco

[parameters('storageAccounts_r
(Microsoft.Storage/storageAcco

[concat(parameters('storageAcc
'/default')]
(Microsoft.Storage/storageAcco

[concat(parameters('storageAcc
'/default')]
(Microsoft.Storage/storageAcco

[concat(parameters('storageAcc
'/default')]
(Microsoft.Storage/storageAcco

[concat(parameters('storageAcc
'/default')]
(Microsoft.Storage/storageAcco

[concat(parameters('storageAcc
'/default')]

```
{
    "$schema": "https://schema.management.azure.com/sch
2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "storageAccounts_memphis01_name": {
            "defaultValue": "memphis01",
            "type": "String"
        },
        "storageAccounts_memphis02_name": {
            "defaultValue": "memphis02",
            "type": "String"
        }
    },
    "variables": {},
    "resources": [
        {
            "type": "Microsoft.Storage/storageAccounts"
            "apiVersion": "2021-09-01",
            "name": "[parameters('storageAccounts_memph
            "location": "eastus",
            "sku": {
                "name": "Standard_LRS",
                "tier": "Standard"
```

Azure Portal

Azure CLI

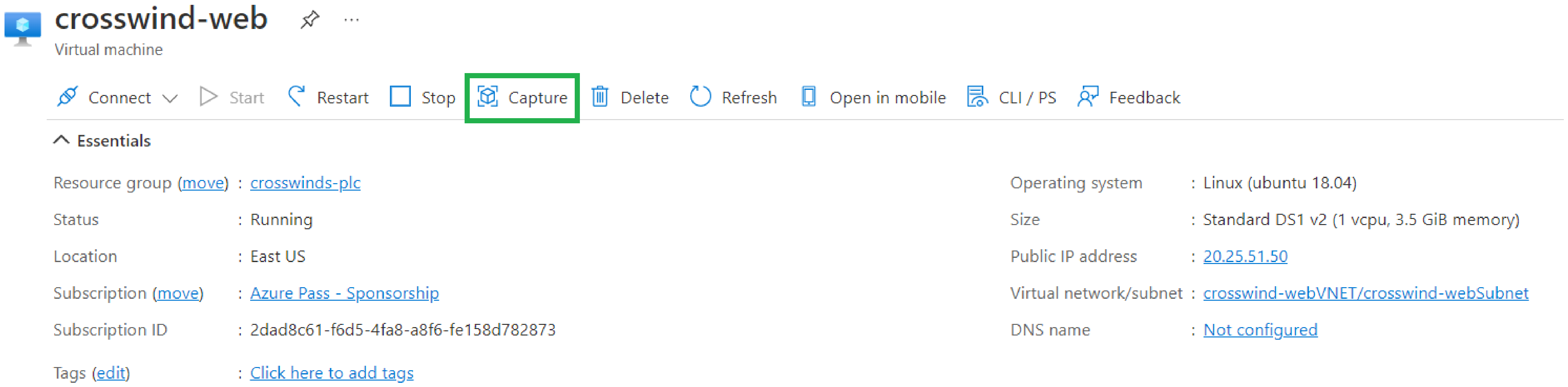
Azure PowerShell

```
>_ Azure PowerShell

$ Export-AzResourceGroup `
-ResourceGroupName <resource-group>
```

```
>_ Azure CLI

$ az group export \
--name <resource-group-name>
```

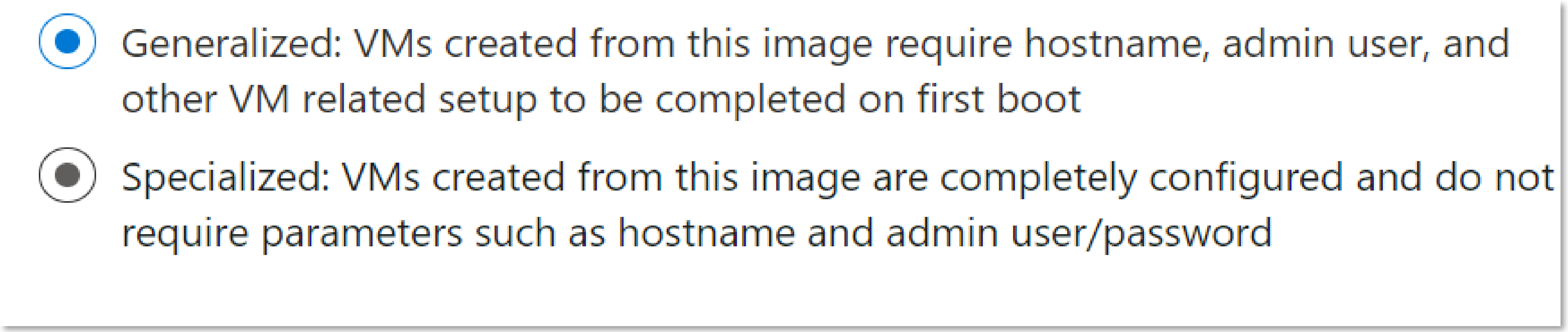
Creating VHD Templates

Creating VHD Templates



crosswind-web
Virtual machine

Resource group (move)	: crosswinds-plc	Operating system	: Linux (ubuntu 18.04)
Status	: Running	Size	: Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Location	: East US	Public IP address	: 20.25.51.50
Subscription (move)	: Azure Pass - Sponsorship	Virtual network/subnet	: crosswind-webVNET/crosswind-webSubnet
Subscription ID	: 2dad8c61-f6d5-4fa8-a8f6-fe158d782873	DNS name	: Not configured
Tags (edit)	: Click here to add tags		



● Generalized: VMs created from this image require hostname, admin user, and other VM related setup to be completed on first boot

○ Specialized: VMs created from this image are completely configured and do not require parameters such as hostname and admin user/password

Operating System State

Virtual Machine Extensions

Virtual Machine Extensions

Small applications

Automation tasks and post deployment configuration can be done with the help of extension.

Management

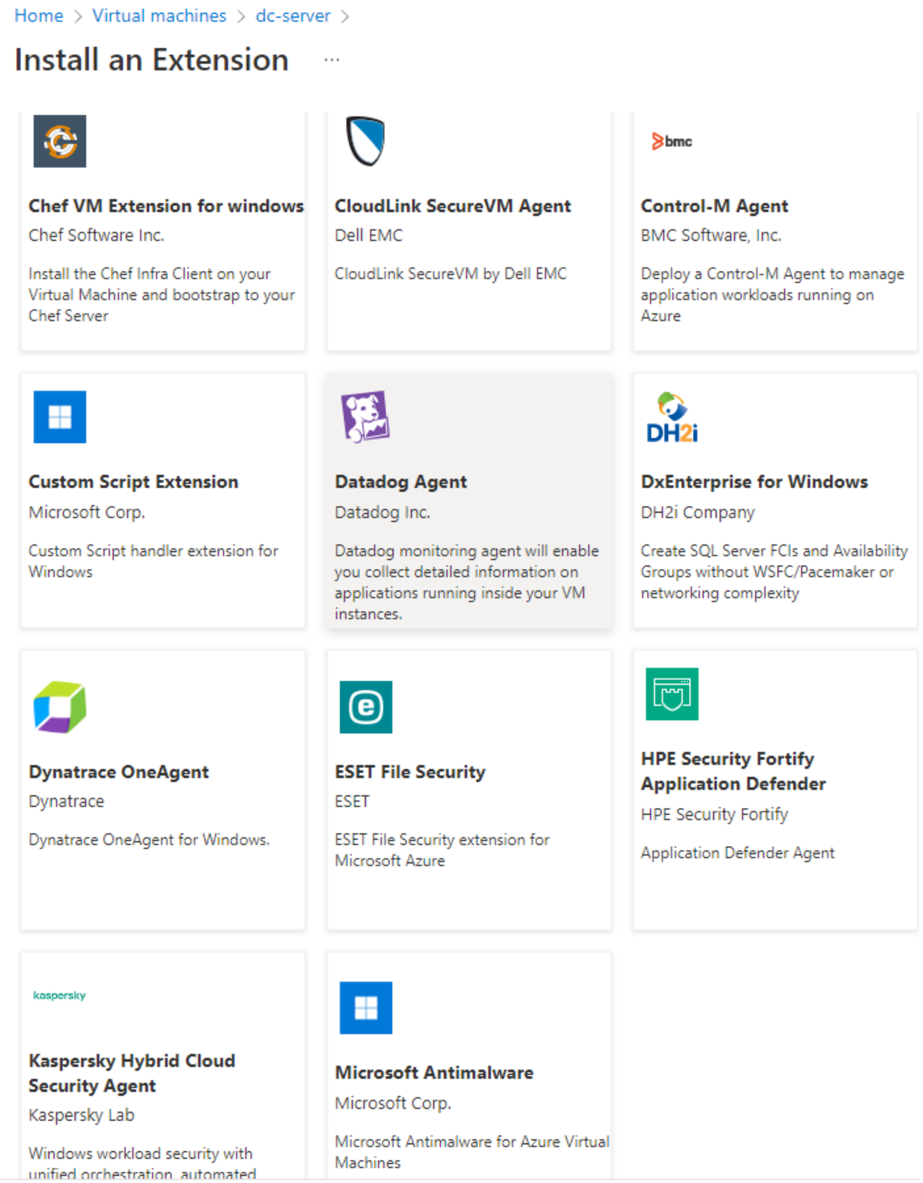
Extensions can be managed with Azure Portal, Azure PowerShell, Azure CLI and ARM templates..

Scope

Extensions can be used for post-deployment configuration during the VM deployment or on existing VMs.

Platform

Extensions and their availability will vary based on the operating system. We have different extensions available for Windows and Linux VMs.



Home > Virtual machines > dc-server >

Install an Extension ...

Chef VM Extension for windows
Chef Software Inc.
Install the Chef Infra Client on your Virtual Machine and bootstrap to your Chef Server

CloudLink SecureVM Agent
Dell EMC
CloudLink SecureVM by Dell EMC

Control-M Agent
BMC Software, Inc.
Deploy a Control-M Agent to manage application workloads running on Azure

Custom Script Extension
Microsoft Corp.
Custom Script handler extension for Windows

Datadog Agent
Datadog Inc.
Datadog monitoring agent will enable you collect detailed information on applications running inside your VM instances.

DxEnterprise for Windows
DH2i Company
Create SQL Server FCIs and Availability Groups without WSFC/Pacemaker or networking complexity

Dynatrace OneAgent
Dynatrace
Dynatrace OneAgent for Windows.

ESET File Security
ESET
ESET File Security extension for Microsoft Azure

HPE Security Fortify Application Defender
HPE Security Fortify
Application Defender Agent

Kaspersky Hybrid Cloud Security Agent
Kaspersky Lab
Windows workload security with unified orchestration, automated

Microsoft Antimalware
Microsoft Corp.
Microsoft Antimalware for Azure Virtual Machines

Custom Script Extension

Supported scenarios

Custom Script extension can be used for simple and complex scripts. Scripts will not continue execution if the workflow includes reboot. PowerShell scripts can be selected and optionally arguments can be passed.

Duration

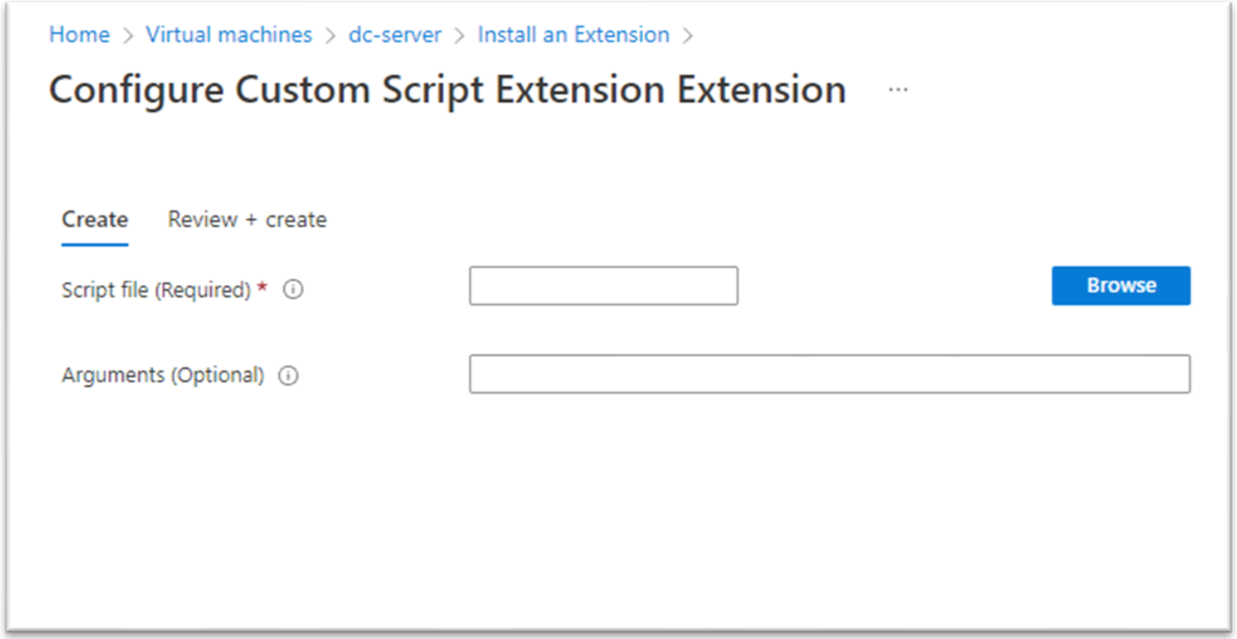
Script can run up to 90 minutes, if the script takes more than 90 minutes to execute, then it will be a timed-out operation. Also, the VM should be in running state to execute the script.

Dependency access

Storage and network access is required by the extension. For successful execution of the script, we need to make sure that the content is available.

Error handling and data sensitivity

Plan for error handling and how to handle sensitive data such as passwords, connection strings, storage account keys etc.



Home > Virtual machines > dc-server > Install an Extension >

Configure Custom Script Extension Extension ...

Script file (Required) *

Arguments (Optional)

Desired State Configuration

Supported scenarios

DSC uses PowerShell DSC which will help you to carry out complex deployments which includes reboot as well. DSC will ensure that the state is achieved.

Configuration

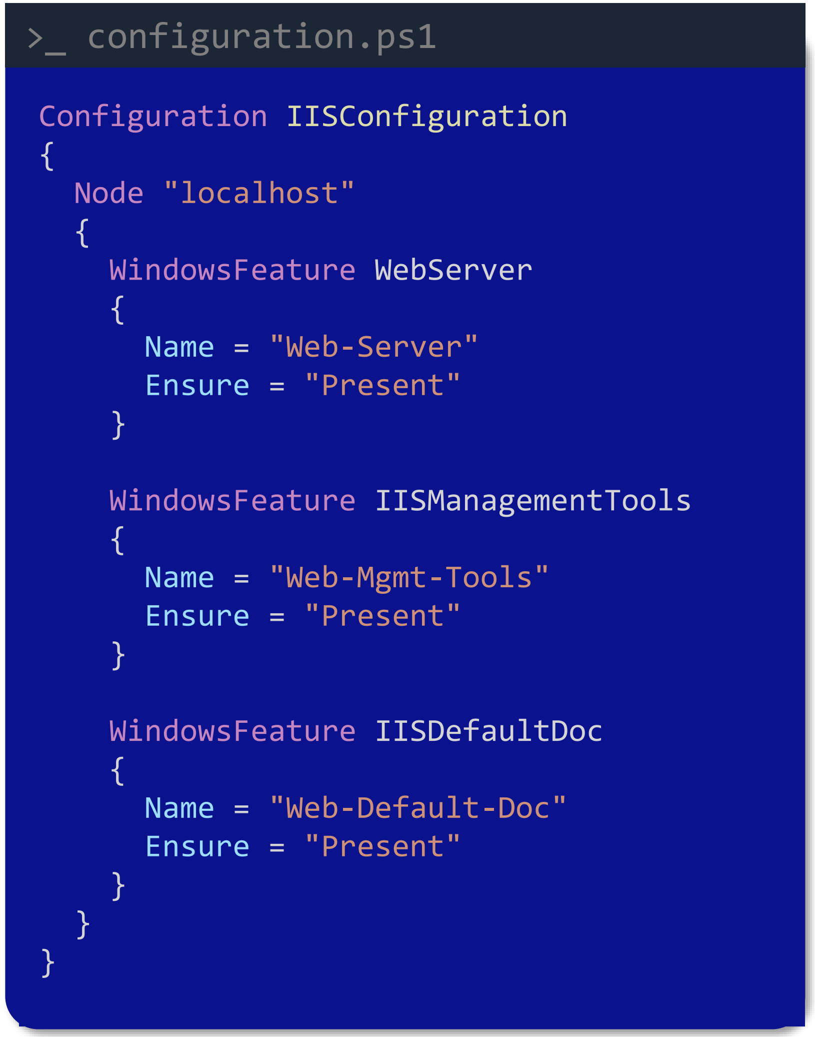
Easy to read scripts called configuration is created in a declarative way. Configuration is saved in PS1 format.

When to use DSC?

If your post deployment configuration includes complex steps such as reboots, then CSE is not the right choice. Choose DSC in all complex scenarios where CSE is not supported.

Blocks

Configuration block is the outermost script block, we will give a name to the configuration define the script. Node block defines the computers that are under the scope of the configuration. Each node block has one or more resource where we define the configuration.



>_ configuration.ps1

```
Configuration IISConfiguration
{
  Node "localhost"
  {
    WindowsFeature WebServer
    {
      Name = "Web-Server"
      Ensure = "Present"
    }

    WindowsFeature IISManagementTools
    {
      Name = "Web-Mgmt-Tools"
      Ensure = "Present"
    }

    WindowsFeature IISDefaultDoc
    {
      Name = "Web-Default-Doc"
      Ensure = "Present"
    }
  }
}
```

KODEKLOUD

Storage accounts

Storage accounts

Microsoft Azure's storage solution for object storage, file storage, message queue and a NoSQL store for meeting modern application requirements.

High availability and durability

Storage account comes with different redundancies to fulfill your durability requirements. Data stored in the storage account can be replicated to different datacenters and even across regions ensuring high availability for the data.

Security

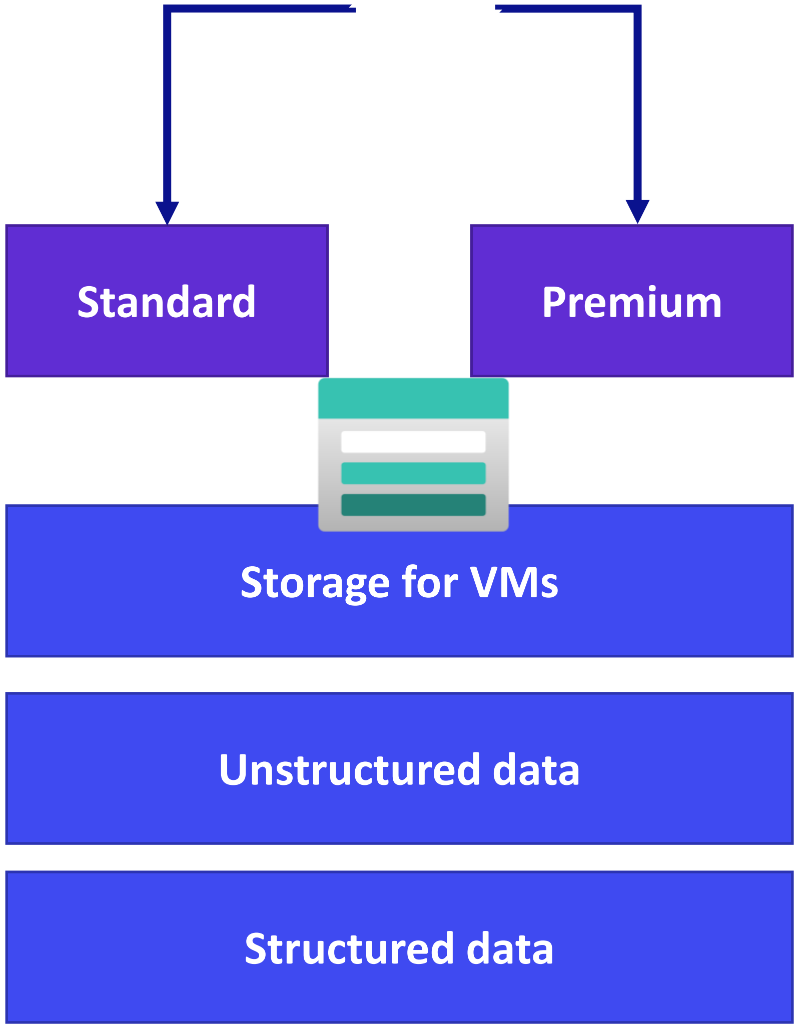
By default, all data written to the storage account is encrypted by Storage Encryption Service. To access the data storage accounts, provide different authorization methods such as storage keys, shared access signature, and Azure AD.

Scalability and Managed

Azure Storage is a platform managed service, depending upon the requirement it will automatically scale the storage and performance.

Access

HTTP or HTTPS can be used to access the data that is stored in Azure Storage. With the help SDKs provided by Microsoft, developers can easily integrate Azure Storage with their code. Azure Storage also supports Azure PowerShell, Azure CLI and REST API.



Standard

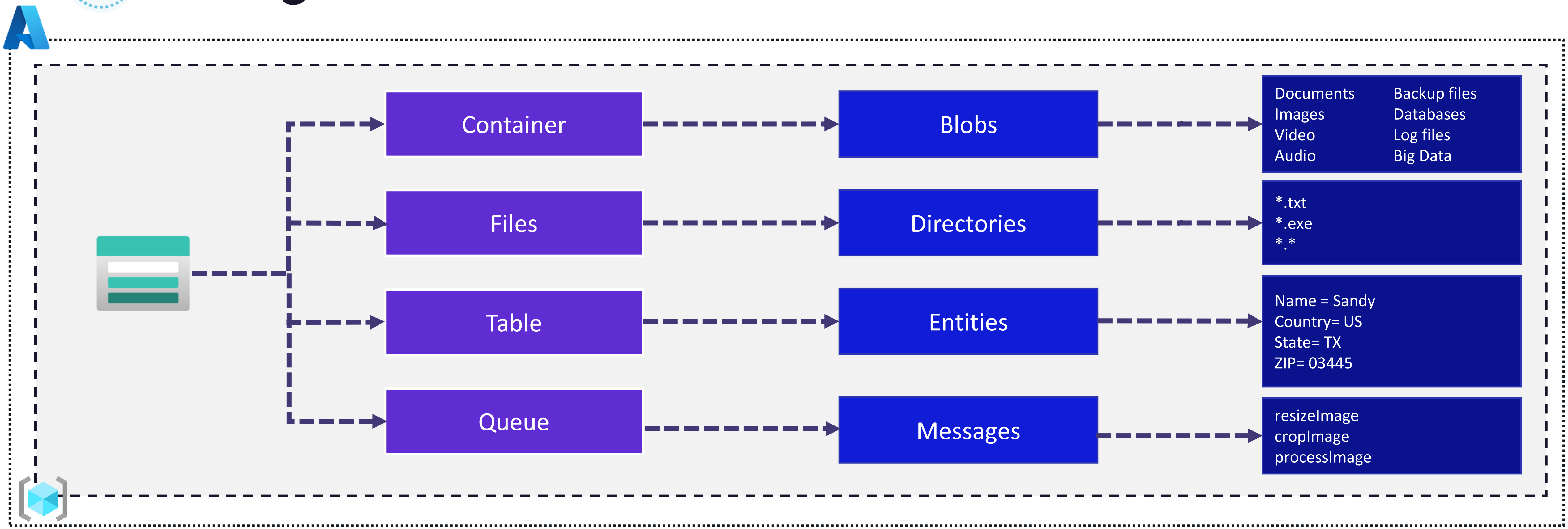
Premium

Storage for VMs

Unstructured data

Structured data

Storage services



Azure Containers

An object store with immense scaling capability.

Ideal for storing unstructured data such as text or binary data.

Azure Files

Managed file share

Used to provision highly available file shares in cloud that can be mounted to cloud and on-premises machines.

Azure Tables

NoSQL datastore

Ideal for storing structured non-relational data

Azure Queues

Messaging store

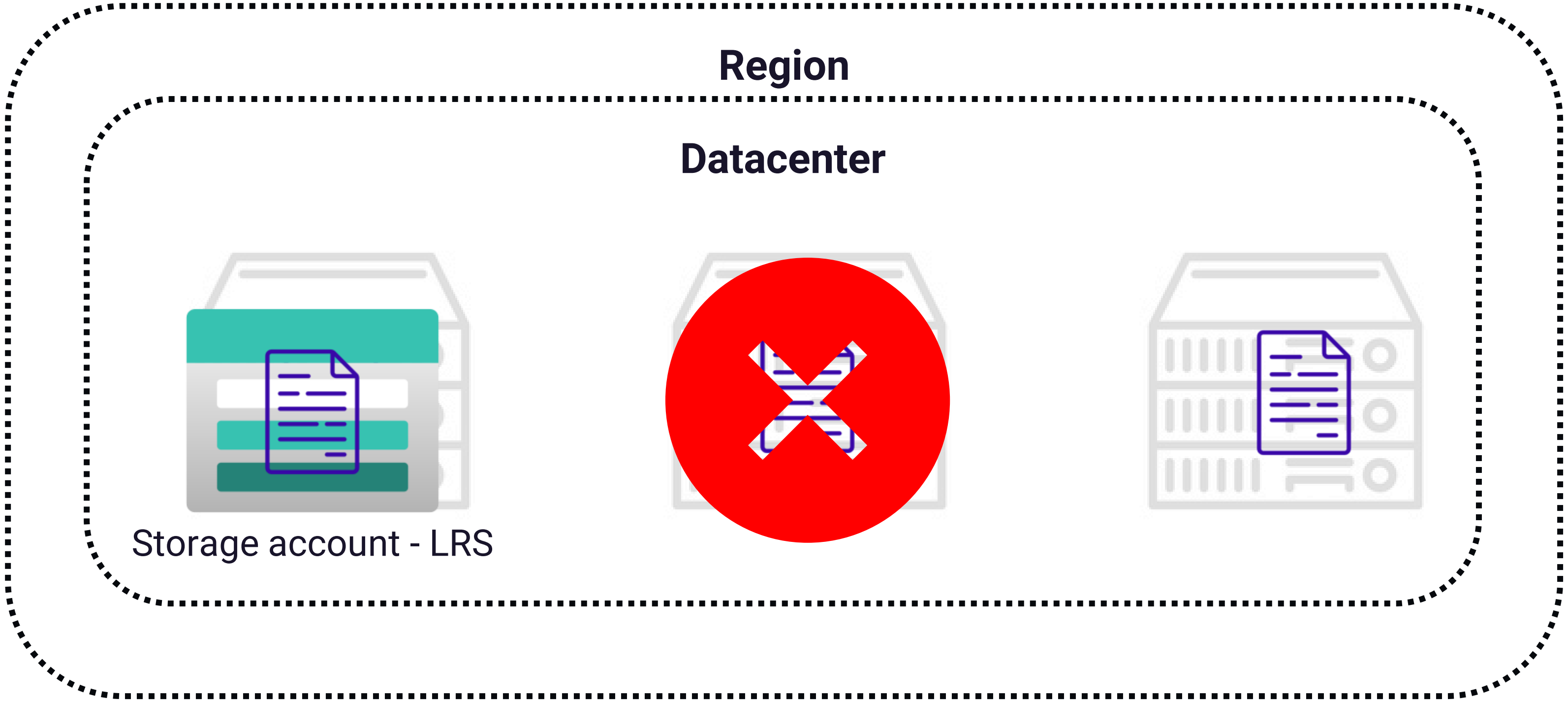
Used to store messages and retrieve messages between application components that needs to be processed asynchronously.

Storage account types

Type	Services	Performance tiers	Replication options
Blob storage	Blob	Standard	LRS, GRS, RA-GRS
General Purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
General Purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, ZRS, GRS, RA-GRS, GZRS, RA-GZRS
Block blob storage	Blob	Premium	LRS, ZRS
File storage	Files	Premium	LRS, ZRS

Storage redundancy

Storage replication – Locally Redundant Storage



Replication

Data is replicated and will retain three copies of data across fault domain within a single datacenter. Since the data is replicated only within a single data center, LRS is the cheapest option.

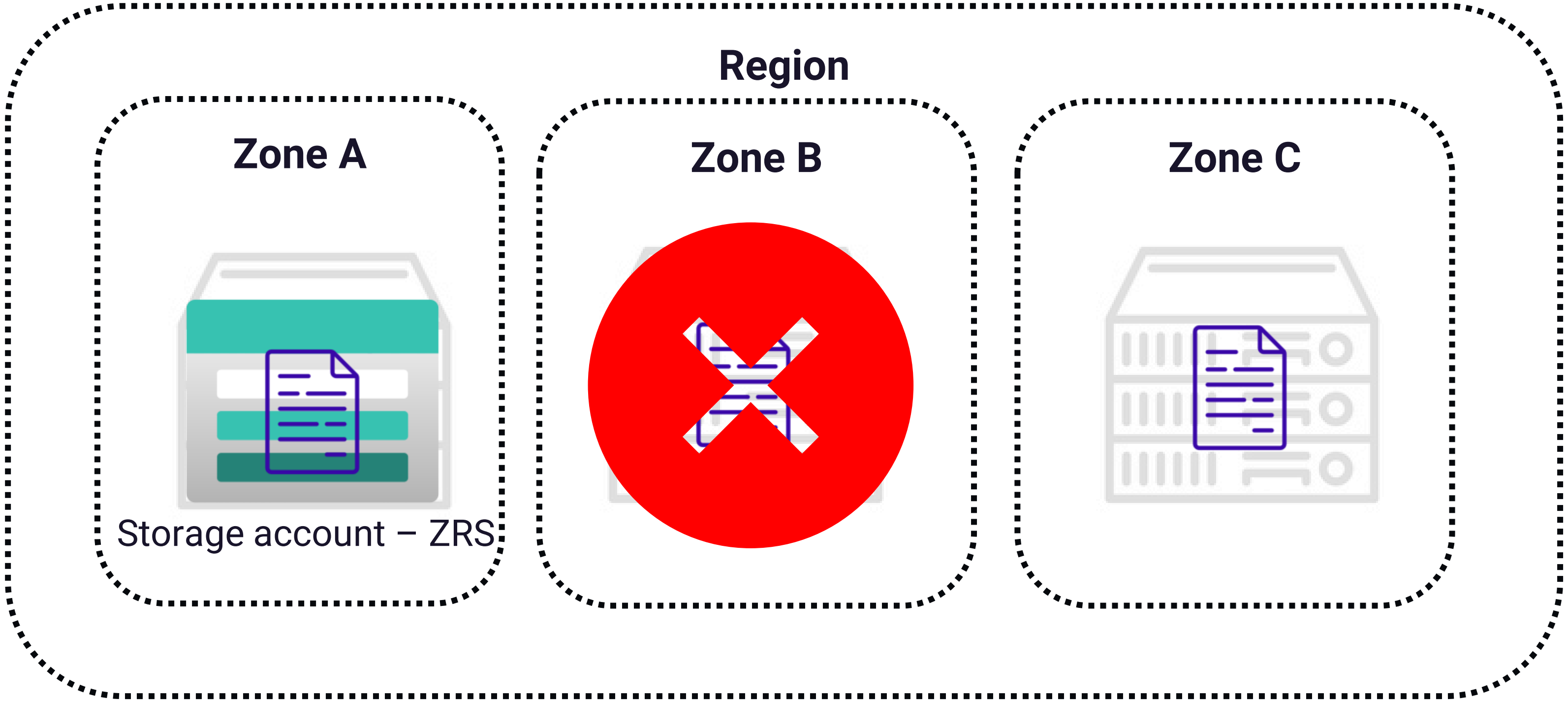
Durability

LRS offers 99.99999999999 (11 9's) of durability. Data stored in LRS is protected from hardware failures as the data is stored in different fault domains.

Chances of failure

As the replicated copies are stored within a single datacenter, if the entire datacenter is down, then the data will not be available

Storage replication – Zone Redundant Storage



Replication

Data is replicated and will retain three copies of data across availability zones within a single region.

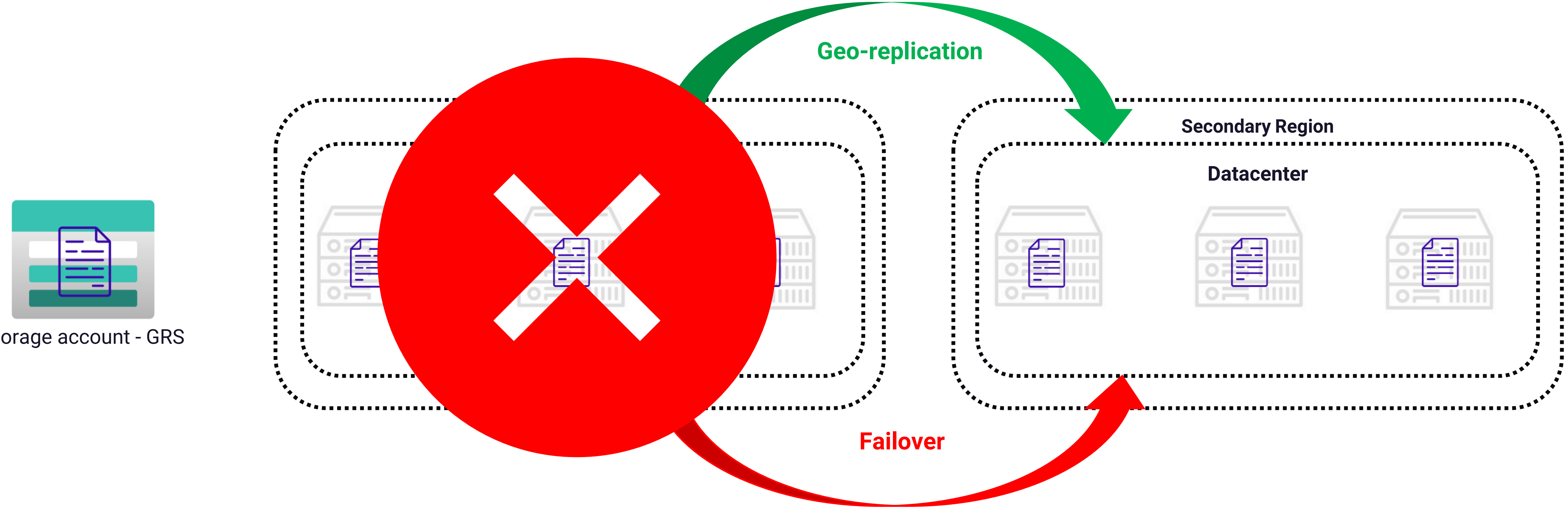
Durability

ZRS offers 99.999999999999 (12 9's) of durability. Data stored in ZRS is protected from datacenter failures as each zone where the datacenter resides is physically separated from each other.

Chances of failure

As the replicated copies are stored within a single region, if the entire region goes down, then the data will not be available

Storage replication – Geo Redundant Storage



Replication

Data is replicated across three fault domains in a datacenter which is part of the primary region and is asynchronously replicated to secondary region where we will have three copies across fault domains.

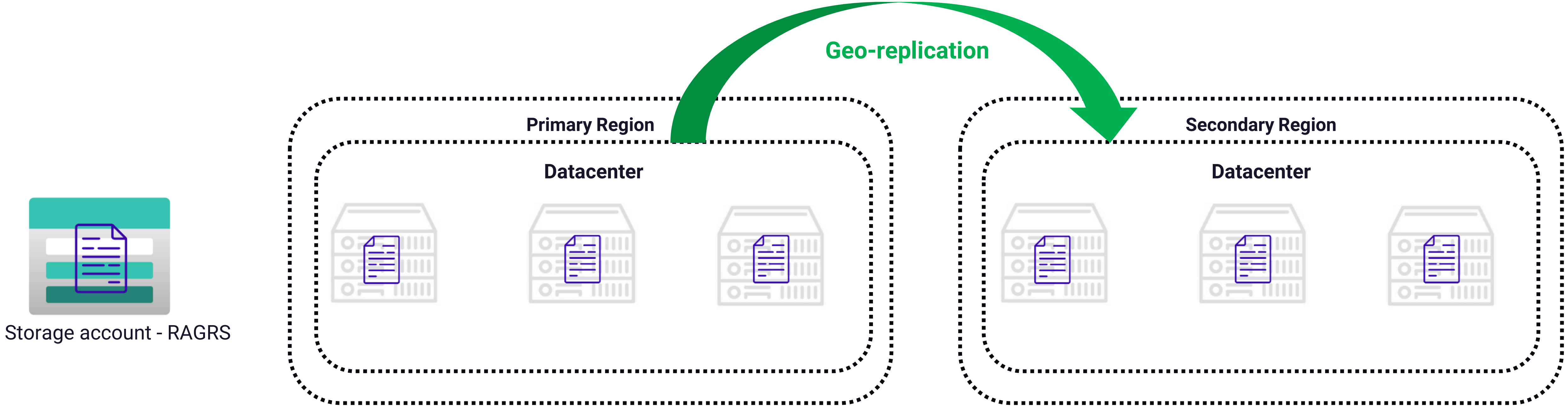
Durability

GRS offers 99.99999999999999 (16 9's) of durability. If the primary region goes down, a failover will happen, and secondary region will become available for read requests.

Considerations

The primary region will be available for all operations and secondary will be only available after failover. The failover can be Microsoft initiated or customer initiated.

Storage replication – Read access Geo Redundant Storage



Replication

Data is replicated across three fault domains in a datacenter which is part of the primary region and is asynchronously replicated to secondary region where we will have three copies across fault domains.

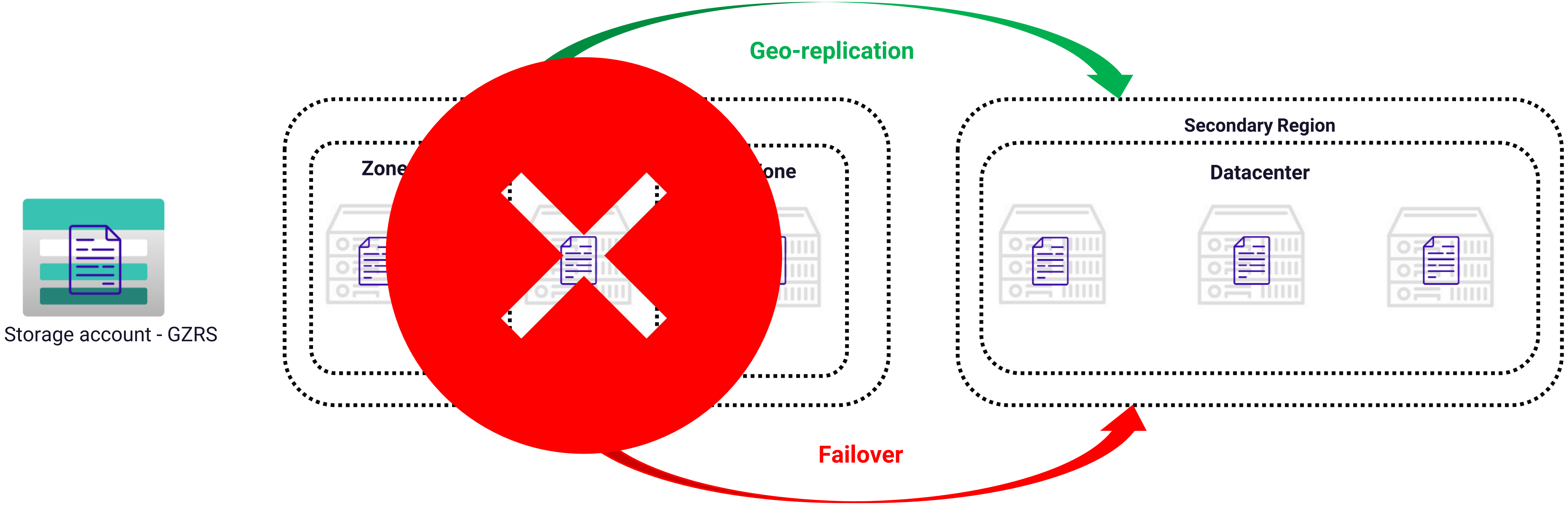
Durability

RAGRS offers 99.9999999999999999 (16 9’s) of durability.

Considerations

The secondary region will be always available for reach operations regardless whether there is a failover or not.

Storage replication –Geo Zone Redundant Storage



Replication

Three copies will be spread across availability zones within the primary region and is asynchronously replicated to secondary region where we will have three copies across fault domains.

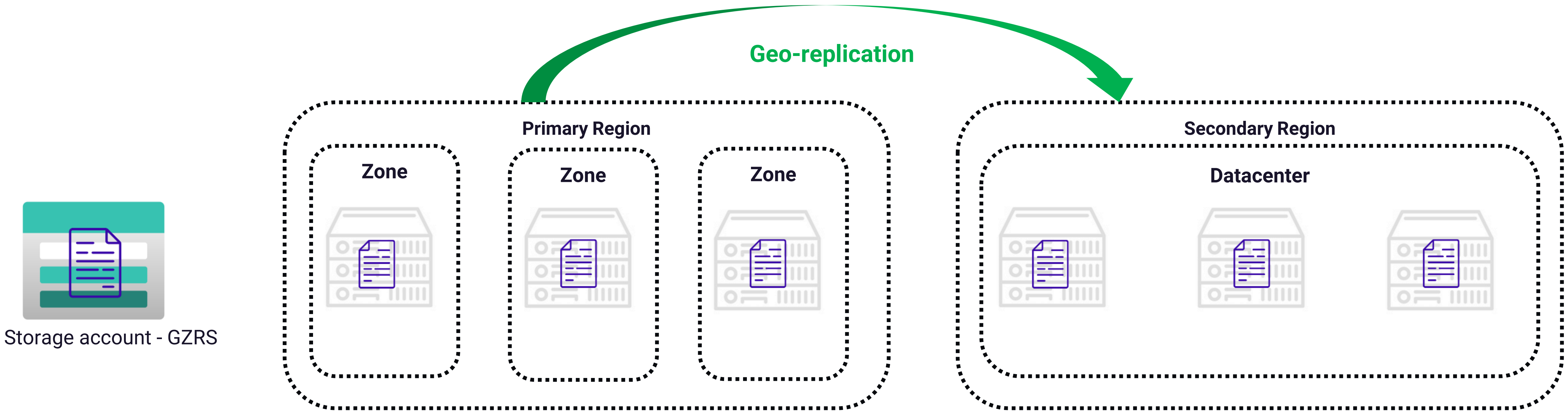
Durability

GZRS offers 99.99999999999999 (16 9's) of durability. If the primary region goes down, a failover will happen, and secondary region will become available for read requests.

Considerations

As we saw in the case of GRS, the primary region will be available for all operations and secondary will be only available after failover. The failover can be Microsoft initiated or customer initiated

Storage replication –Read Access Geo Zone Redundant Storage



Replication

Three copies will be spread across availability zones within the primary region and is asynchronously replicated to secondary region where we will have three copies across fault domains.

Durability

GZRS offers 99.99999999999999 (16 9's) of durability

Considerations

Here secondary region will be always available regardless of whether there is a failover or not.

Accessing storage endpoints

Based on the storage account name and the service, every service has its own unique endpoint

```
<protocol>://<storage account name>.<service>.core.windows.net
```

http, https — Your storage account name — blob, queue, file, table

For a storage account named "kodekloud", the endpoints will be:

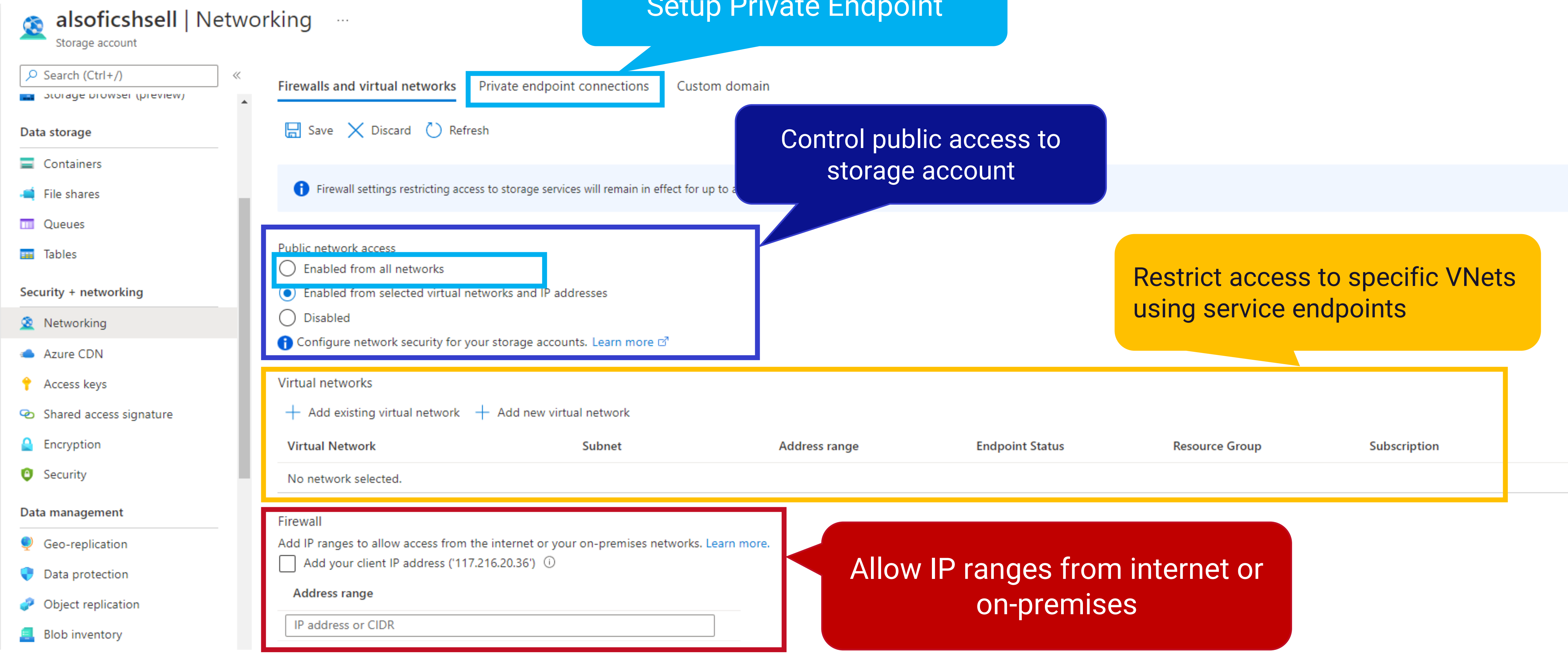
Service	Endpoint
Container service	https://kodekloud.blob.core.windows.net
Queue service	https://kodekloud.queue.core.windows.net
File service	https://kodekloud.file.core.windows.net
Table service	https://kodekloud.table.core.windows.net

If needed, we can use our own custom domain with CNAME mapping

DNS CNAME entry	Alias
blobs.kodekloud.com	kodekloud.blob.core.windows.net

Securing storage endpoints

Securing storage endpoints



alsoficshsell | Networking ...

Storage account

Firewall settings restricting access to storage services will remain in effect for up to a

Public network access

○ Enabled from all networks

● Enabled from selected virtual networks and IP addresses

○ Disabled

Configure network security for your storage accounts. Learn more

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

□ Add your client IP address ('117.216.20.36')

Address range

IP address or CIDR

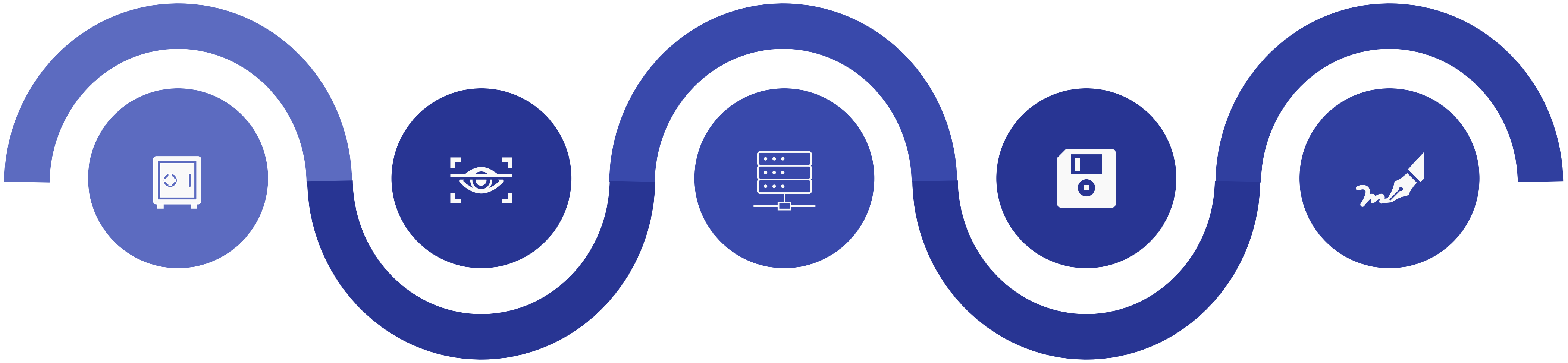
Setup Private Endpoint

Control public access to storage account

Restrict access to specific VNets using service endpoints

Allow IP ranges from internet or on-premises

Storage security capabilities



● **Encryption**

By default, without any additional configuration, all data written to the storage account is encrypted by Storage Service Encryption (SSE)

● **Authentication**

With help of Azure AD and RBAC, we can authenticate and requests and provide authorization to storage services.

● **Data in transit**

Client-side encryption, HTTPS, and SMB 3.0 is used to secure data in transit.

● **Disk encryption**

OS and Data disks of Linux and Windows VMs can be encrypted using Azure Disk Encryption (ADE).

● **Shared access signature**

Fine tuned granular access can be given to storage services with the help of SAS.

Storage Service Encryption (SSE) and Azure Disk Encryption (ADE)

Storage Service Encryption (SSE)

Protection

Data at rest is protected using SSE. All data written to Azure Disks, Blob, File, Queue, and Table is encrypted using SSE and is decrypted when the data is retrieved.

Compliance

Organizations doesn't need develop in-house encryption methods to encrypt data stored in Azure storage. Using SSE organizations can meet their compliance and security requirements.

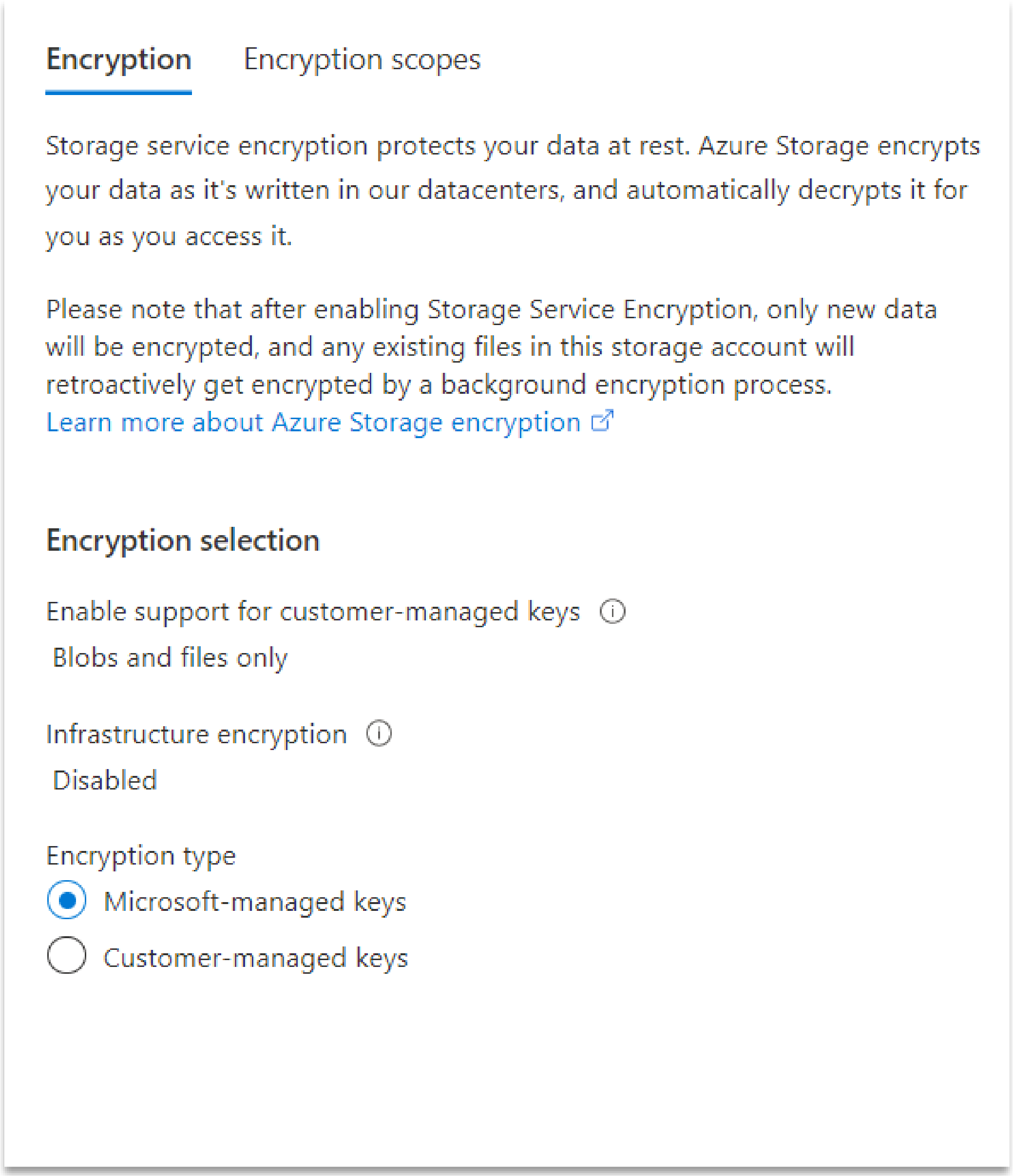
Strong cipher

SSE uses 256-bit AES encryption to encrypt the data. The encryption, decryption, data management and key management is done by storage service. SSE cannot be disabled.

.

Bring your own keys

If you would like to control the encryption keys and their rotation, you replace Microsoft managed keys with Customer Managed Keys. You need to create an Azure Key Vault to store the key and the storage service will retrieve the key from Key Vault for encryption and decryption.



Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.
Learn more about Azure Storage encryption

Encryption selection

Enable support for customer-managed keys ⓘ
Blobs and files only

Infrastructure encryption ⓘ
Disabled

Encryption type
● Microsoft-managed keys
○ Customer-managed keys

Azure Disk Encryption (ADE)

Encrypt disks

Using ADE, we can encrypt OS and Data Disks of Windows and Linux virtual machines. ADE uses BitLocker for Windows and DM-Crypt for Linux to encrypting the disks. Encryption keys are stored in Azure Key Vault.

Restrict access

Since the disk is encrypted, only the VM owner will be able to retrieve the data stored in the VM. If anyone downloads the VHD and attaches to another VM, without the keys, they will not be able to read the data.

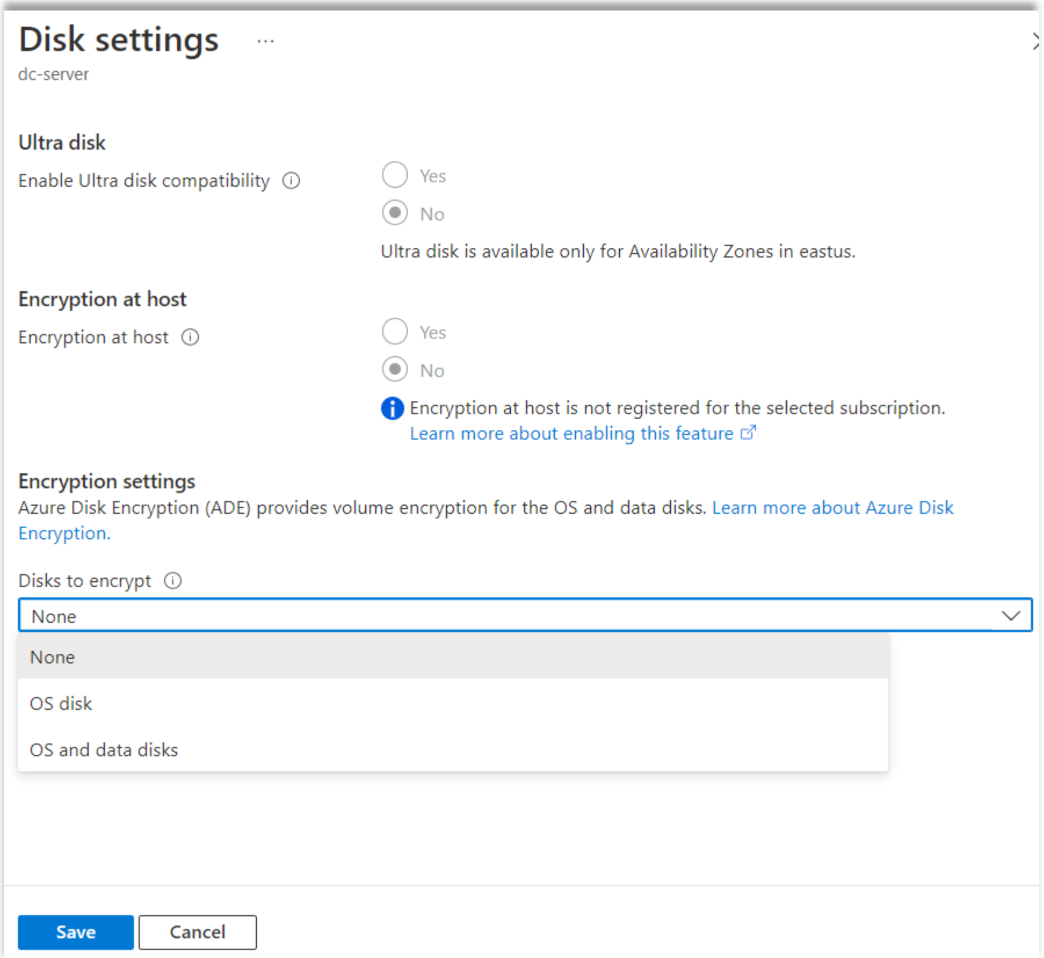
Encrypted backup

When you are using Azure Backup, the encryption keys are backed up to the recovery service vault. Also, the backups are encrypted. ASE uses AES 256-bit encryption.

.

Considerations

If you are encrypting both OS and Data disk, there will be a small performance impact due to the encryption and decryption activity. The impact is very minimal, however, if your application is CPU intensive then you can skip the OS disk and encrypt data disk only to enhance performance.



Disk settings ...

dc-server

Ultra disk

Enable Ultra disk compatibility ⓘ ○ Yes ● No

Ultra disk is available only for Availability Zones in eastus.

Encryption at host

Encryption at host ⓘ ○ Yes ● No

ⓘ Encryption at host is not registered for the selected subscription. Learn more about enabling this feature

Encryption settings

Azure Disk Encryption (ADE) provides volume encryption for the OS and data disks. Learn more about Azure Disk Encryption.

Disks to encrypt ⓘ

None

Storage security - Authorization

Storage security - Authorization

Storage Account Keys

Two 512-bit keys will be generated for every storage account, and this can be rotated. Account keys are like root passwords, and we need to secure them to avoid unauthorized access.

Shared access signature

Delegate access to storage at a very granular level. SAS are generated using account keys but with fine tuned access.

Azure AD

Using Azure AD and RBAC we can authenticate and authorize requests from users. Currently Azure AD authentication is supported by Blobs, Queues, and Tables only. For Files, SMB access can be given with the help of AAD Domain Services.

Anonymous

We can enable anonymous access to our blobs and containers. As the request is anonymous, we don't need pass any authorization header.

Storage Account Keys

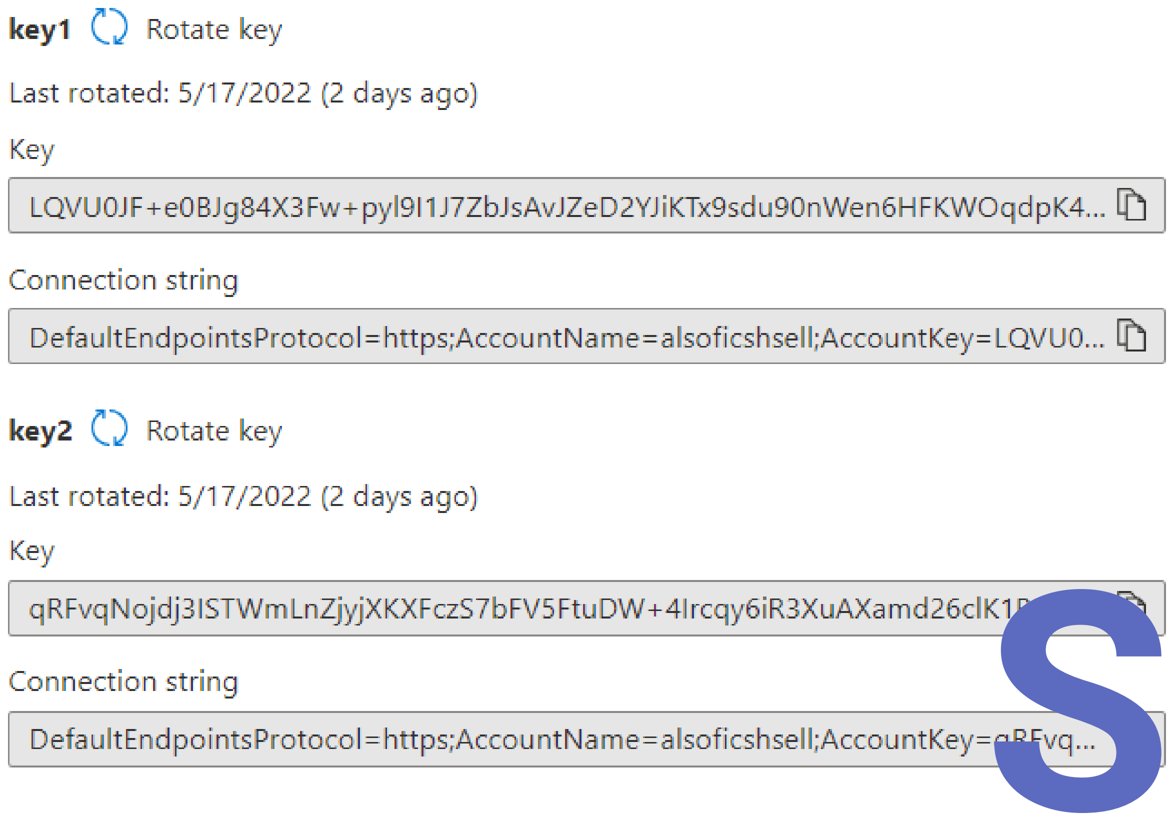
Storage Account Keys

○ **Be cautious with the account key!**

Account key is like the root password, the user possessing the account keys can perform any action against the storage account. Microsoft recommends to save the key to Azure Key Vault and regularly rotate them.

○ **Two keys**

Azure provides two 512-bit keys for every storage account. You can either one of these in your API calls in your authorization header. Users with permission to Microsoft.Storage/storageAccounts/listkeys/action can view, read or copy the key via Azure Portal, Azure CLI, and Azure PowerShell.



key1 Rotate key

Last rotated: 5/17/2022 (2 days ago)

Key

LQVU0JF+e0BJg84X3Fw+pyl9I1J7ZbJsAvJZeD2YJiKTx9sdu90nWen6HFKWOqdpK4...

Connection string

DefaultEndpointsProtocol=https;AccountName=alsoficshsell;AccountKey=LQVU0...

key2 Rotate key

Last rotated: 5/17/2022 (2 days ago)

Key

qRFvqNojdj3ISTWmLnZjyjXKXFczS7bFV5FtuDW+4Ircqy6iR3XuAXamd26clK1

Connection string

DefaultEndpointsProtocol=https;AccountName=alsoficshsell;AccountKey=qRFvq...

Shared Access Signature

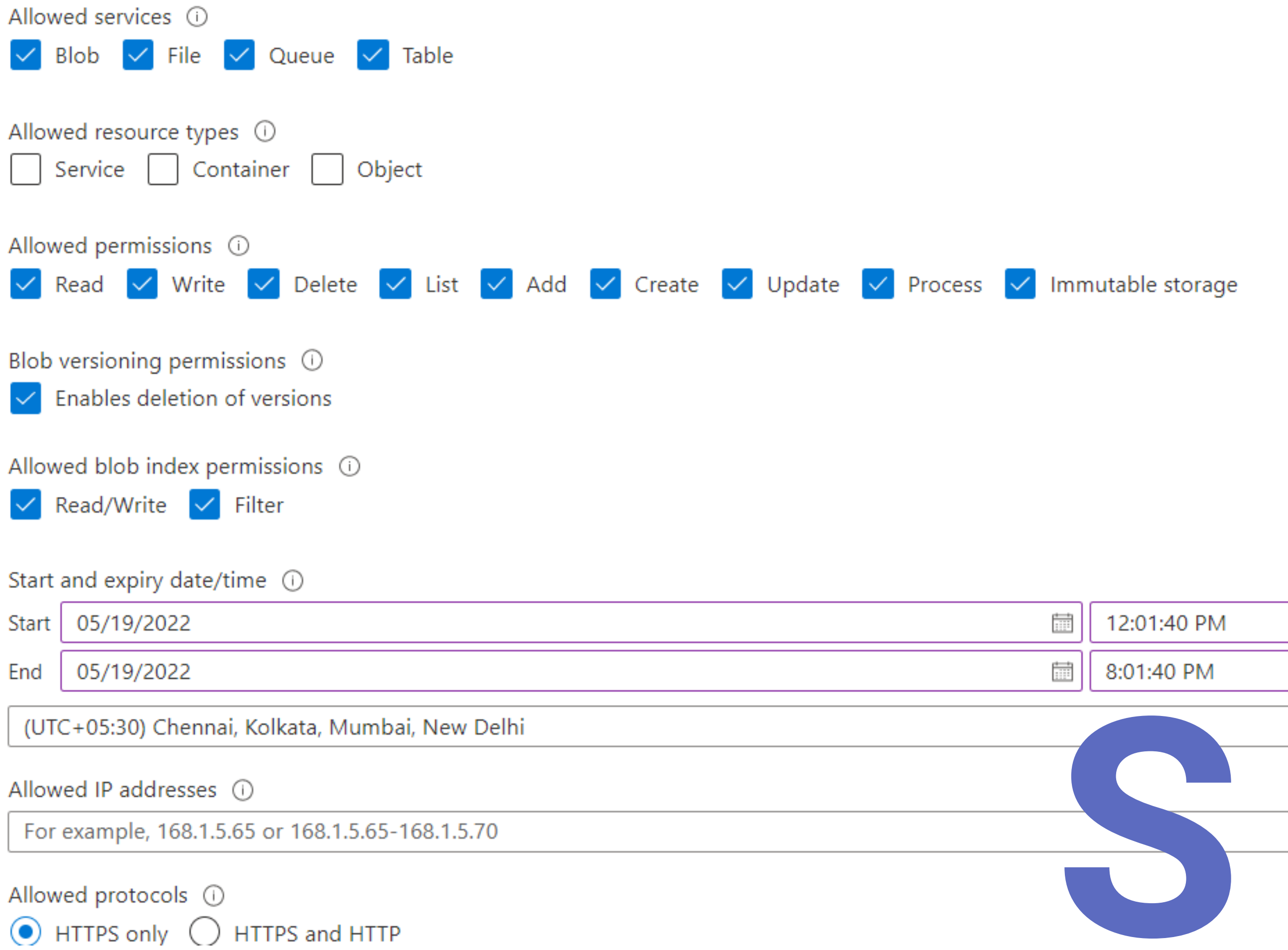
Shared Access Signature

Fine tuned access

Instead of giving full access via account keys we can fine tune the access via SAS. We can control the allowed services, allowed resource types, permissions, start time, end time, IP address and protocol using SAS

Three types of SAS keys

- ✓ User delegation SAS
- ✓ Service SAS
- ✓ Account SAS



Allowed services ⓘ
☑ Blob ☑ File ☑ Queue ☑ Table

Allowed resource types ⓘ
☐ Service ☐ Container ☐ Object

Allowed permissions ⓘ
☑ Read ☑ Write ☑ Delete ☑ List ☑ Add ☑ Create ☑ Update ☑ Process ☑ Immutable storage

Blob versioning permissions ⓘ
☑ Enables deletion of versions

Allowed blob index permissions ⓘ
☑ Read/Write ☑ Filter

Start and expiry date/time ⓘ
Start 05/19/2022 12:01:40 PM
End 05/19/2022 8:01:40 PM
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

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

Shared Access Signature

Name	Excerpt	Explanation
Resource URI	https://kodekloud.blob.core.windo	Blob endpoint
Permissions	sp=rwdlacup	Supports read, write, delete, list, add, create, and update
Start time	st=2022-05-19T06:31:40Z	Start date and time in UTC
End time	se=2022-05-19T14:31:40Z	End date and time in UTC
IP address range	sip=168.11.12.13-168.11.12.19	Allowed IP range
Protocol	spr=https	Only HTTPS requests are allowed
Signature	sig=66iXqzZSakarJO5J210%2ByoPRVXTeT%2FTJcHHSEkUjHr0%3D	Unique signature which is HMAC computed over a string to sign and key using SHA256, then Base64 encoding on top of that.

https://kodekloud.blob.core.windows.net?sv=2020-08-04&ss=bfqt&srt=sc&sp=rwdlacup&se=2022-05-19T14:31:40Z&st=2022-05-19T06:31:40Z&sip=168.11.12.13-168.11.12.19&spr=https&sig=66iXqzZSakarJO5J210%2ByoPRVXTeT%2FTJcHHSEkUjHr0%3D

Azure AD Authentication

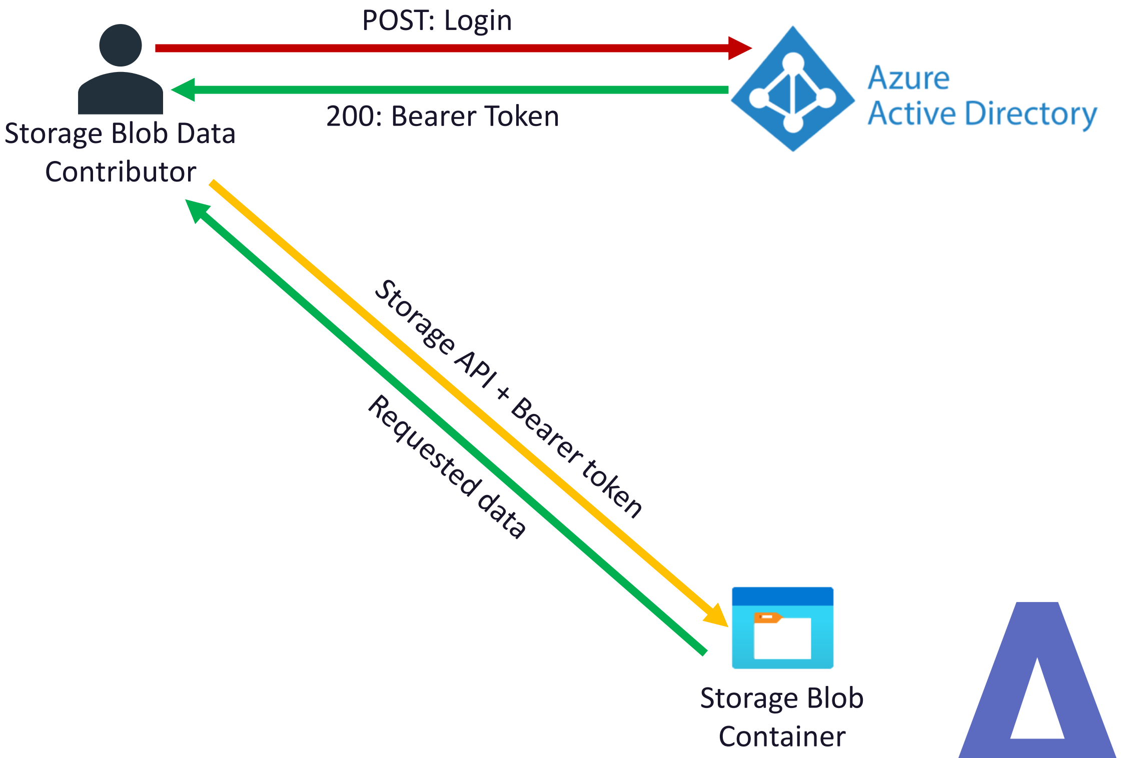
Azure AD Authentication

Secure way of authenticating

Microsoft recommends using Azure AD authentication for accessing Blobs, Queues and Tables. Azure AD integrates features such as MFA, Conditional Access to enhance the request to access storage.

Requires dedicated RBAC roles

Even if you are the Owner or Contributor of the subscription, you would still require storage specific RBAC to authorize storage access requests. These RBAC can be assigned to any scope and the access will be inherited. Example: Storage Blob Data Owner, Storage Queue Data Contributor.



Anonymous access to blobs

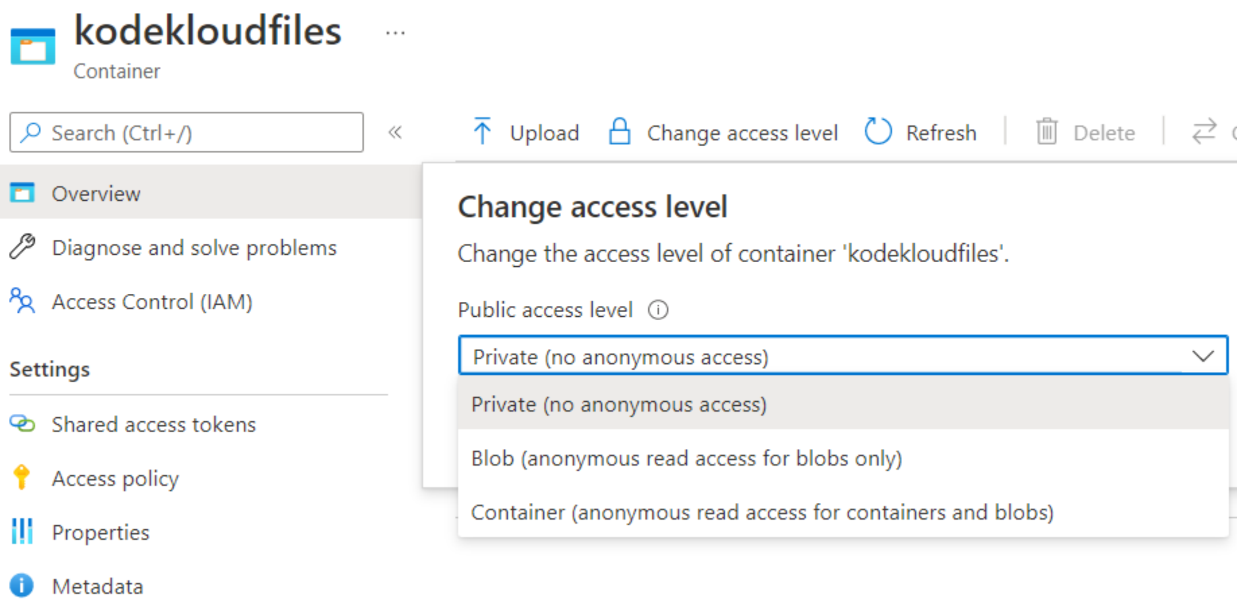
Anonymous access

Public access without authorization

Anonymous access can be granted to blobs and containers. Read request to blobs and containers with anonymous access enabled, doesn't require any sort of authorization.

Ideal for public facing content

Used to share documents, images, or any unstructured data stored in blob storage to public.



Change access level

Change the access level of container 'kodekloudfiles'.

Public access level: Private (no anonymous access)

- Private (no anonymous access)
- Blob (anonymous read access for blobs only)
- Container (anonymous read access for containers and blobs)

KODEKLOUD

Creating Azure File share

Creating Azure File Share

Enterprise grade file share

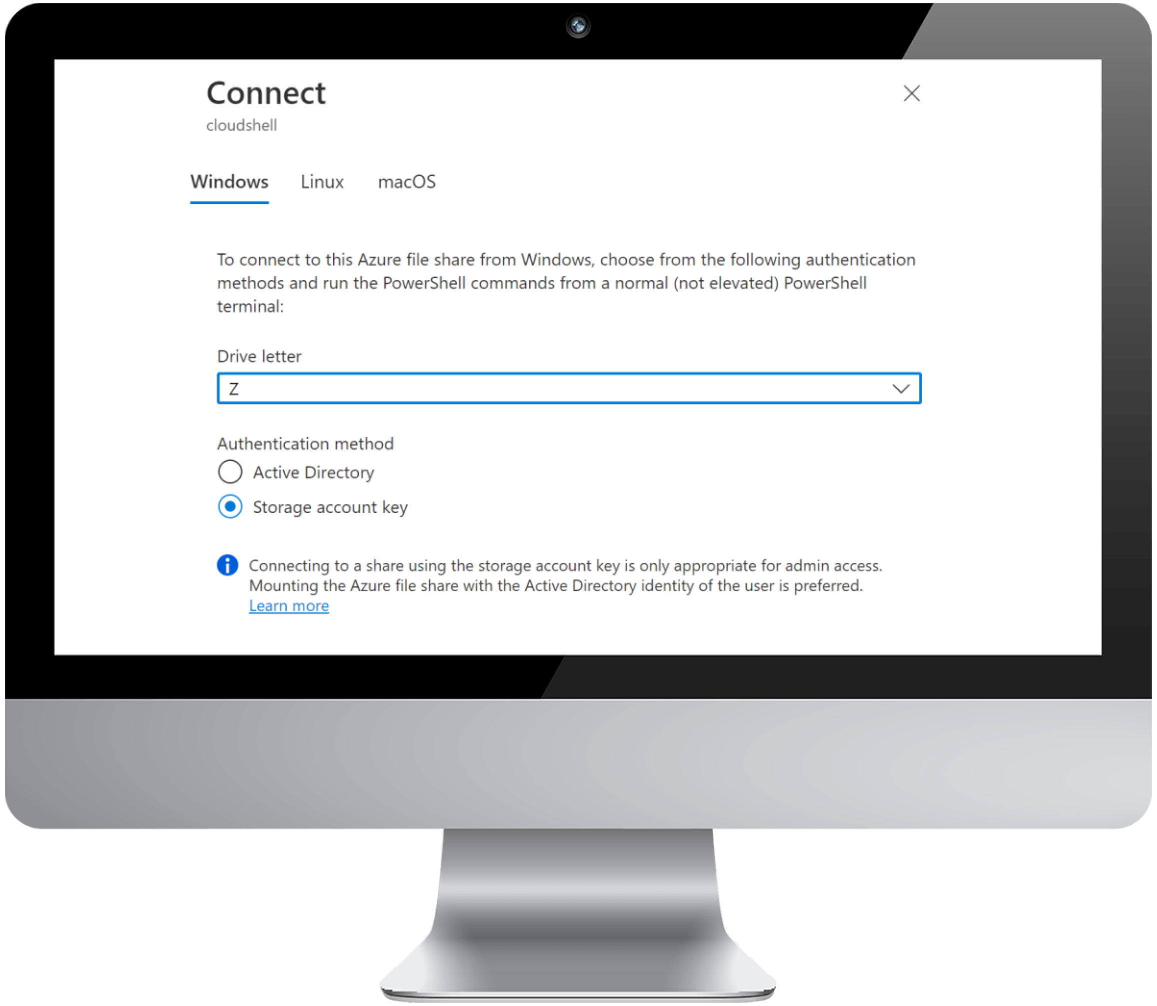
With file shares, we can share files across virtual machines and non-Azure workloads. Any number of Azure or non-Azure virtual machines can mount and work on the file share simultaneously. Also supports backup and snapshot for data recovery.

Supports Windows, Linux and macOS

Azure provides easy to use scripts to mount the file share to Windows, Linux and macOS computers. Computers can interact with Azure file share as they work with on-premises file shares. Port 445 needs to be open for SMB traffic.

Use cases

Firstly, we can decommission on-premises file share and migrate to Azure Files. It can be used for storing diagnostic data, tool and utilities which needs to be shared with teams.



Connect

cloudshell

To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:

Drive letter: Z

Authentication method

○ Active Directory

● Storage account key

Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory identity of the user is preferred. Learn more

Configuring Azure File Sync service

Azure File Sync

Without losing the flexibility, performance, and compatibility for your on-premises file servers, extend and centralize your file shares in Azure Files using Azure File Sync. Use SMB, NFS, and FTPS to connect with your file shares.

Lift and shift

Centralize your file share and provide access to file shares across Windows Servers and Azure Files. Helps to share files across multiple sites at ease.

Adding new offices

You can easily onboard new branch offices and share files with them.

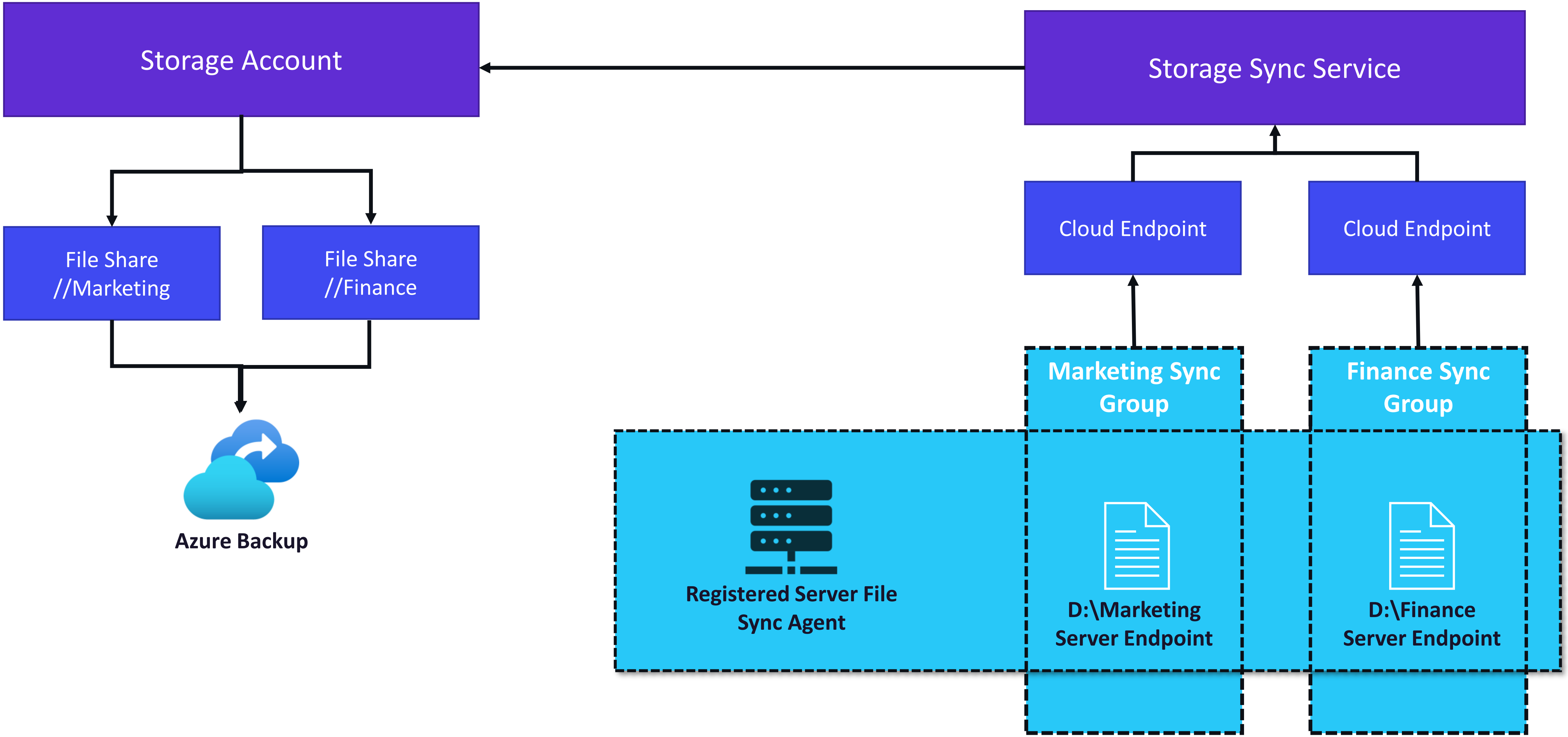
BCDR

Azure Backup will backup your on-premises data once the sync is established. Restoring data after a catastrophic failure will be quick.

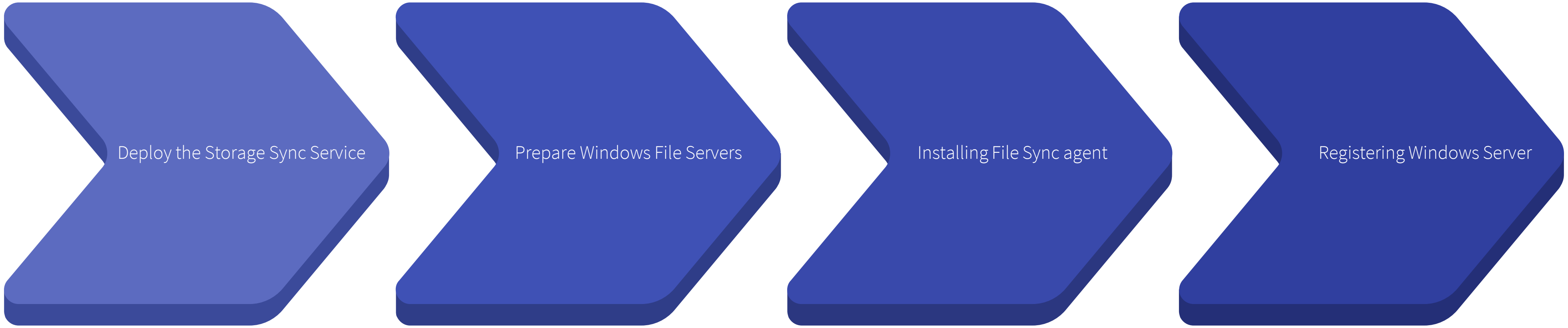
Archiving

File Sync caches data that has been used recently. Data which is not in consumption will be stored in Azure Files and is retrieved only upon request. You can control this using the cloud tiering feature.

Azure File Sync - Components



Azure File Sync - Implementation


Deploy the Storage Sync Service
Prepare Windows File Servers
Installing File Sync agent
Registering Windows Server

- **Deploy the Storage Sync Service**

  In the Azure Portal, we need to create a Storage Sync Service. This will be deployed to a resource group like the storage account

- **Prepare Windows File Servers**

  All servers we are planning to register requires preparation. Some prerequisites include disabling IE Enhanced Security and installing latest version of PowerShell

- **Installing File Sync Agent**

  File Sync Agent needs to be installed on the prepared Windows Server. Agent is responsible for the sync to Azure file share.

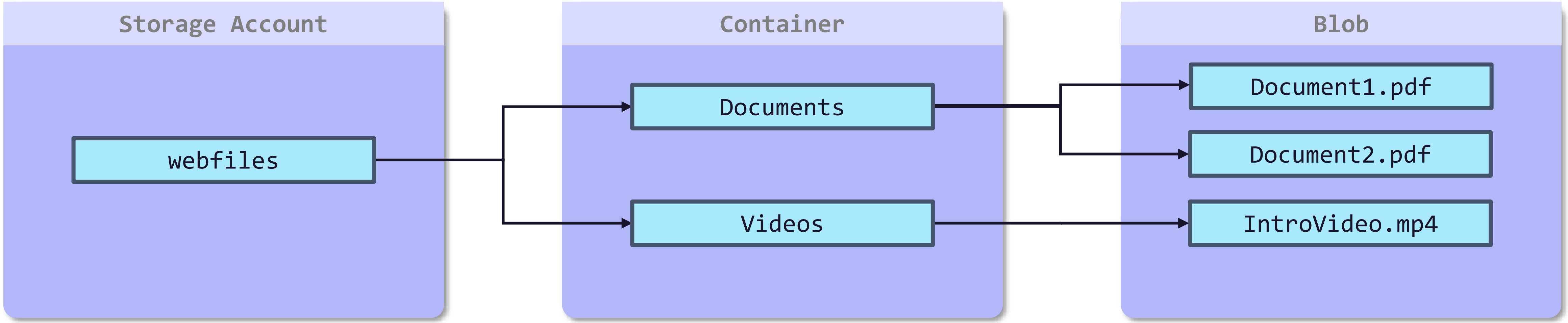
- **Register Windows Server**

  Once the agent is installed, you will be redirected to the server registration window. Registration is required to establish trust with the Storage Sync Service.

Configuring Azure Blob Storage

Azure Containers (Blob Storage)

Provides storage for storing unstructured data as in any type of text or binary data. Blob Storage is referred to as “object storage”

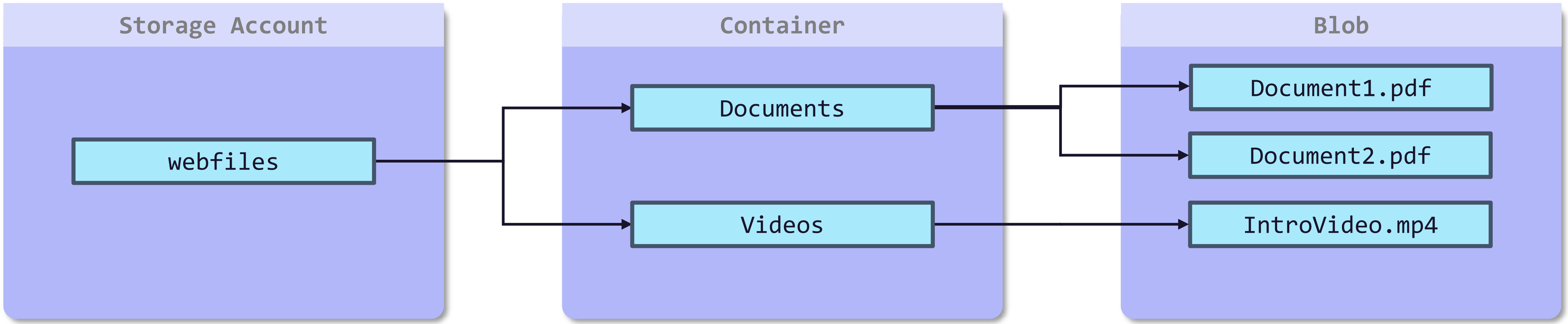


- Embed images or documents in webpages
- Strong files for distribution for example installation packages on websites
- Backup, recovery and archiving
- Stream video and audio directly to browser
- Act as a disaster recovery site for your on-premises site
- Store data for analysis which can be accessed by tools like Power BI

Creating Containers

All objects or blobs we upload should be in a container. A storage account can have unlimited number of containers and each container can have unlimited blobs.

Containers provides logical grouping of blobs, acts as a scope of assign RBAC and public access level



Storage Account

webfiles

Container

Documents

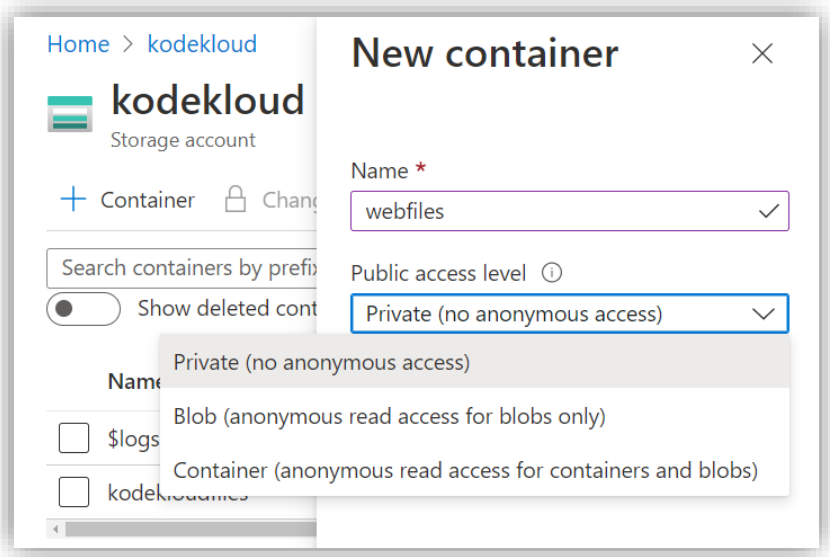
Videos

Blob

Document1.pdf

Document2.pdf

IntroVideo.mp4



Home > kodekloud

kodekloud

Storage account

New container

Name *

webfiles

Public access level ⓘ

Private (no anonymous access)

- Private (no anonymous access)
- Blob (anonymous read access for blobs only)
- Container (anonymous read access for containers and blobs)

○ **Private**

No anonymous access to data stored in the container

○ **Blob**

Anonymous read access to blobs only

○ **Container**

Permission to read and list entire container, which includes all the blobs

Storage Tiers

Blob Access Tiers

Based on the frequency of access, we can optimize storage cost using access tiers.

○ **Hot**

Ideal for storing data that is frequently accessed.

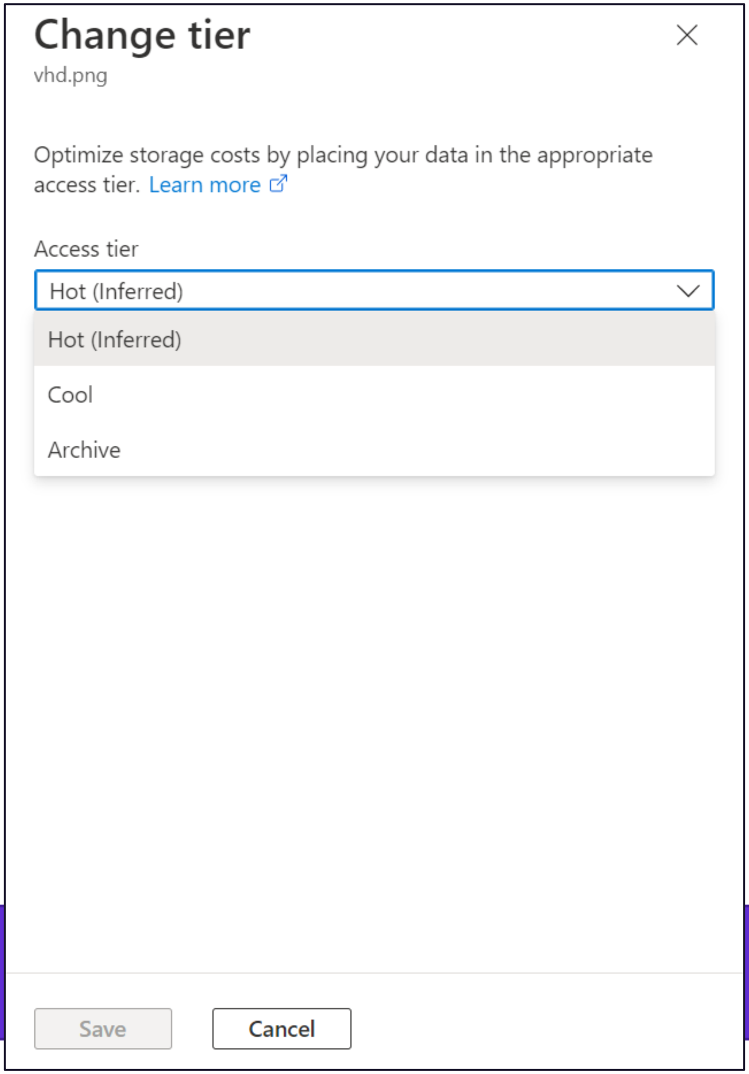
○ **Cool**

Ideal for storing large amounts data that is not accessed frequently and is stored for at least 30 days.

○ **Archive**

Ideal for that can tolerate several hours of retrieval latency and will remain the archive tier for at least 180 days.

Tier	Storage Cost	Access Cost
Hot	$$$	$
Cool	$$	$$
Archive	$	$$$



Change tier

vhd.png

Optimize storage costs by placing your data in the appropriate access tier. Learn more

Access tier: Hot (Inferred)

Access tiers can be switched any time as required

Lifecycle Management

Blob Lifecycle Management

Policy based transition

We can transition blobs to cooler tiers automatically based on the last modified date.

Delete blobs and snapshots

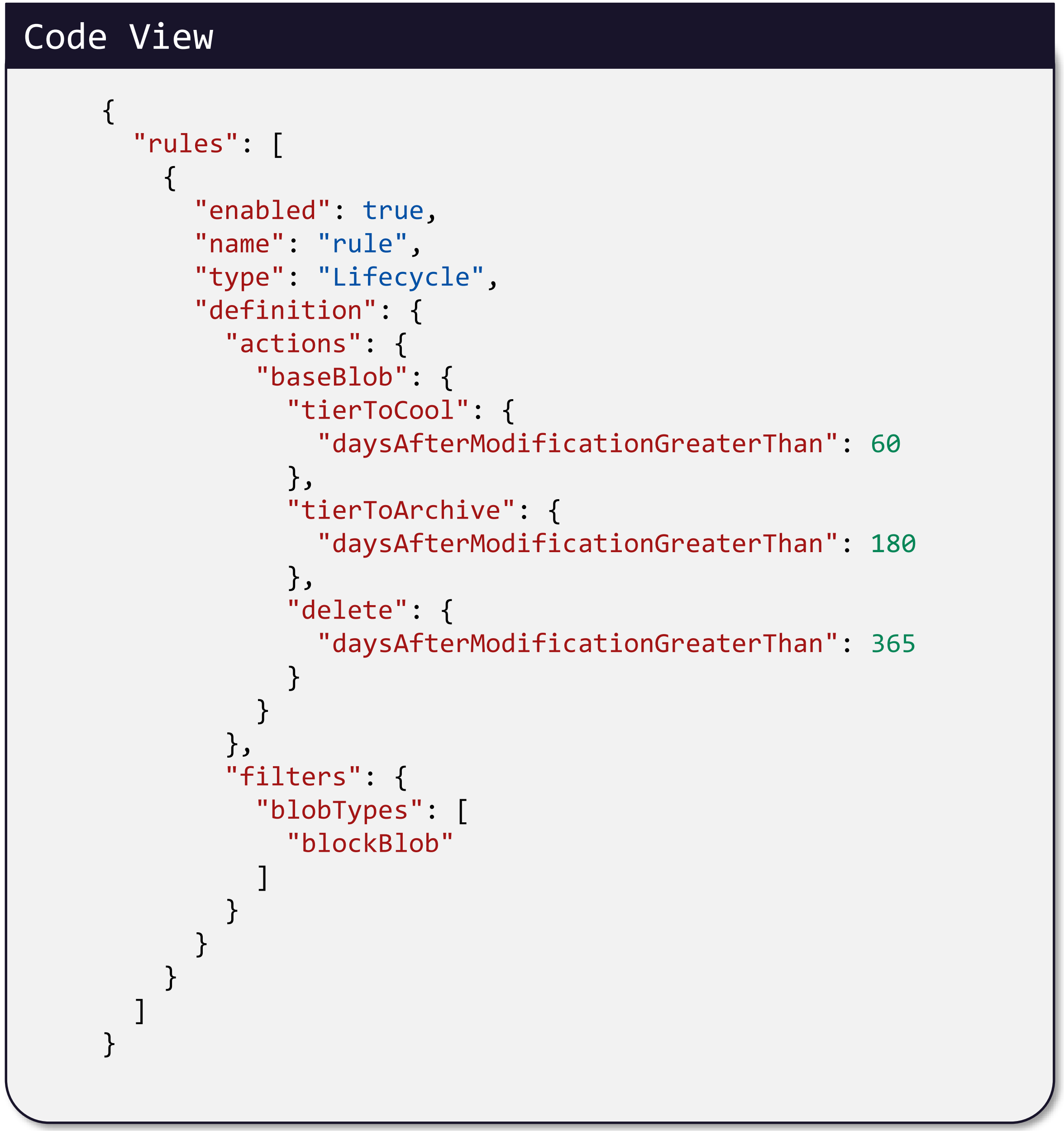
Besides transitioning to cooler tiers, LCM can be used to delete blobs and blob snapshots after X number of days if they are not modified.

Filtering option

We can apply the policy to all the blobs in the storage or limit blobs with filters

Target different types

LCM can target block blobs and append blobs and further apply to sub types such as base blobs, versions and snapshots.



Code View

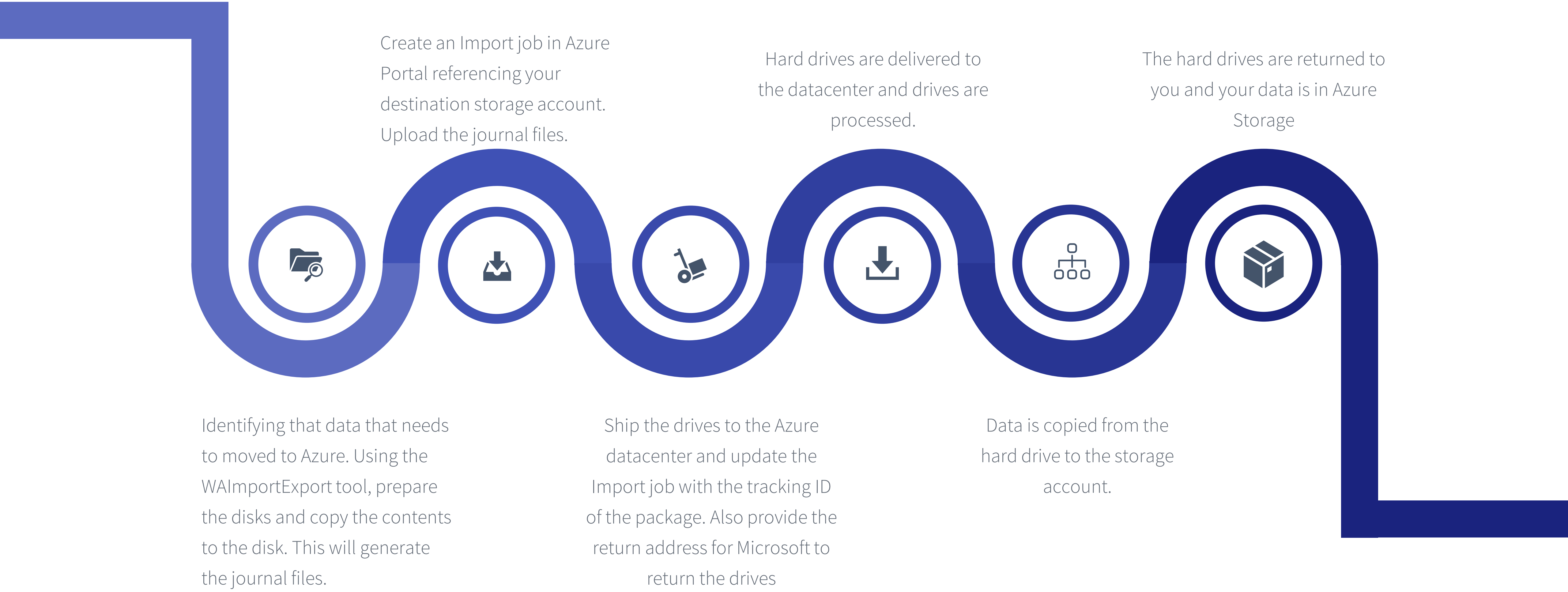
```
{
  "rules": [
    {
      "enabled": true,
      "name": "rule",
      "type": "Lifecycle",
      "definition": {
        "actions": {
          "baseBlob": {
            "tierToCool": {
              "daysAfterModificationGreaterThan": 60
            },
            "tierToArchive": {
              "daysAfterModificationGreaterThan": 180
            },
            "delete": {
              "daysAfterModificationGreaterThan": 365
            }
          }
        },
        "filters": {
          "blobTypes": [
            "blockBlob"
          ]
        }
      }
    }
  ]
}
```

KODEKLOUD

Import/Export Service

Import/Export Service

Import workflow



Identifying that data that needs to moved to Azure. Using the WAImportExport tool, prepare the disks and copy the contents to the disk. This will generate the journal files.

Create an Import job in Azure Portal referencing your destination storage account. Upload the journal files.

Ship the drives to the Azure datacenter and update the Import job with the tracking ID of the package. Also provide the return address for Microsoft to return the drives

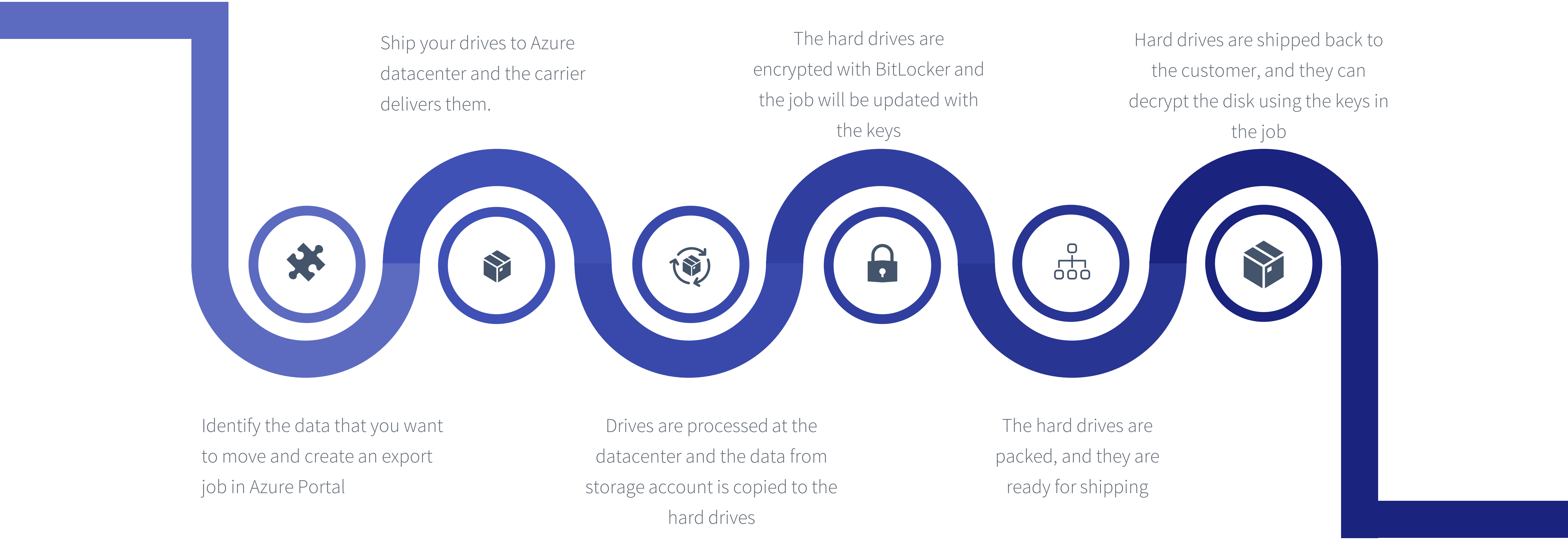
Hard drives are delivered to the datacenter and drives are processed.

Data is copied from the hard drive to the storage account.

The hard drives are returned to you and your data is in Azure Storage

Import/Export Service

Export workflow



Identify the data that you want to move and create an export job in Azure Portal

Ship your drives to Azure datacenter and the carrier delivers them.

Drives are processed at the datacenter and the data from storage account is copied to the hard drives

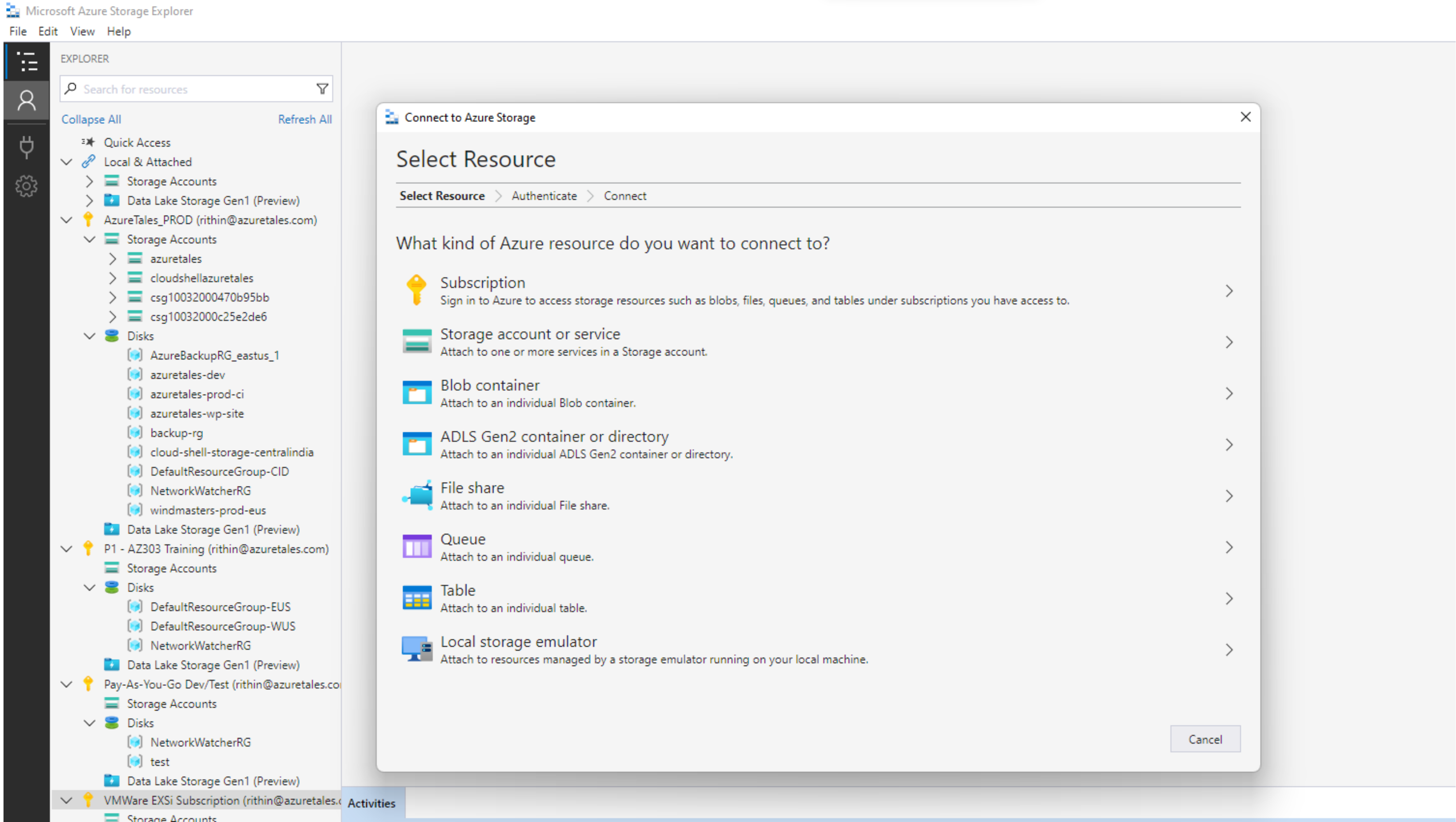
The hard drives are encrypted with BitLocker and the job will be updated with the keys

The hard drives are packed, and they are ready for shipping

Hard drives are shipped back to the customer, and they can decrypt the disk using the keys in the job

Azure Storage Explorer

Azure Storage Explorer



What kind of Azure resource do you want to connect to?

Subscription
Sign in to Azure to access storage resources such as blobs, files, queues, and tables under subscriptions you have access to.

Storage account or service
Attach to one or more services in a Storage account.

Blob container
Attach to an individual Blob container.

ADLS Gen2 container or directory
Attach to an individual ADLS Gen2 container or directory.

File share
Attach to an individual File share.

Queue
Attach to an individual queue.

Table
Attach to an individual table.

Local storage emulator
Attach to resources managed by a storage emulator running on your local machine.

AzCopy

AzCopy

Supports multiple scenarios

AzCopy can be used as a multi-cloud datar transfer tool. It supports Azure Blobs, Azure Files, Amazon S3, GCP, ADLS Gen2 APIs etc. Data movement between these and on—premises is supported by azcopy.

Enhanced resiliency

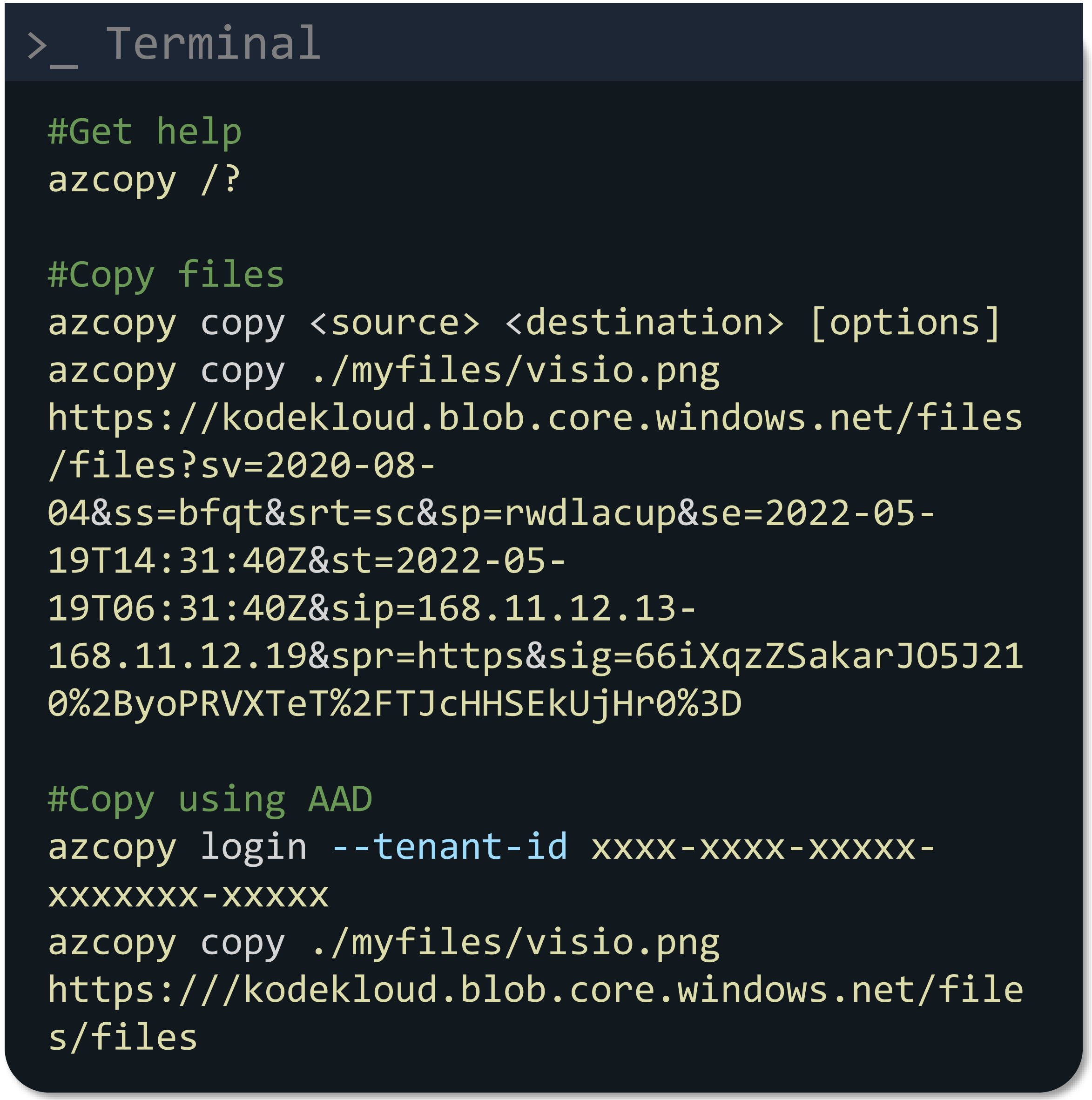
Every instance will create a job ID and related log file. If your job is getting failed, you can restart or review the logs to understand what went wrong.

Supports include, exclude, wildcards and recursive

We can use include or exclude flags along with wildcard patterns. Recursive can be used to copy all files within a folder. We can also list or remove blobs in a given path.

Authentication and suppport

AzCopy can be authenticated using SAS tokens or Azure Active Directory. AzCopy can be installed on Windows, Linux or macOS computers.



```
#Get help
azcopy /?

#Copy files
azcopy copy <source> <destination> [options]
azcopy copy ./myfiles/visio.png
https://kodekloud.blob.core.windows.net/files
/files?sv=2020-08-
04&ss=bfqt&srt=sc&sp=rwdlacup&se=2022-05-
19T14:31:40Z&st=2022-05-
19T06:31:40Z&sip=168.11.12.13-
168.11.12.19&spr=https&sig=66iXqzZSakarJO5J21
0%2ByoPRVXTeT%2FTJcHHSEkUjHr0%3D

#Copy using AAD
azcopy login --tenant-id xxxx-xxxx-xxxxx-
xxxxxxx-xxxxx
azcopy copy ./myfiles/visio.png
https:///kodekloud.blob.core.windows.net/file
s/files
```

KODEKLOUD

Creating an App Service

App Service Plans

Compute

App Service Plan defines a set of compute resources required to run our App Service.

Performance tier

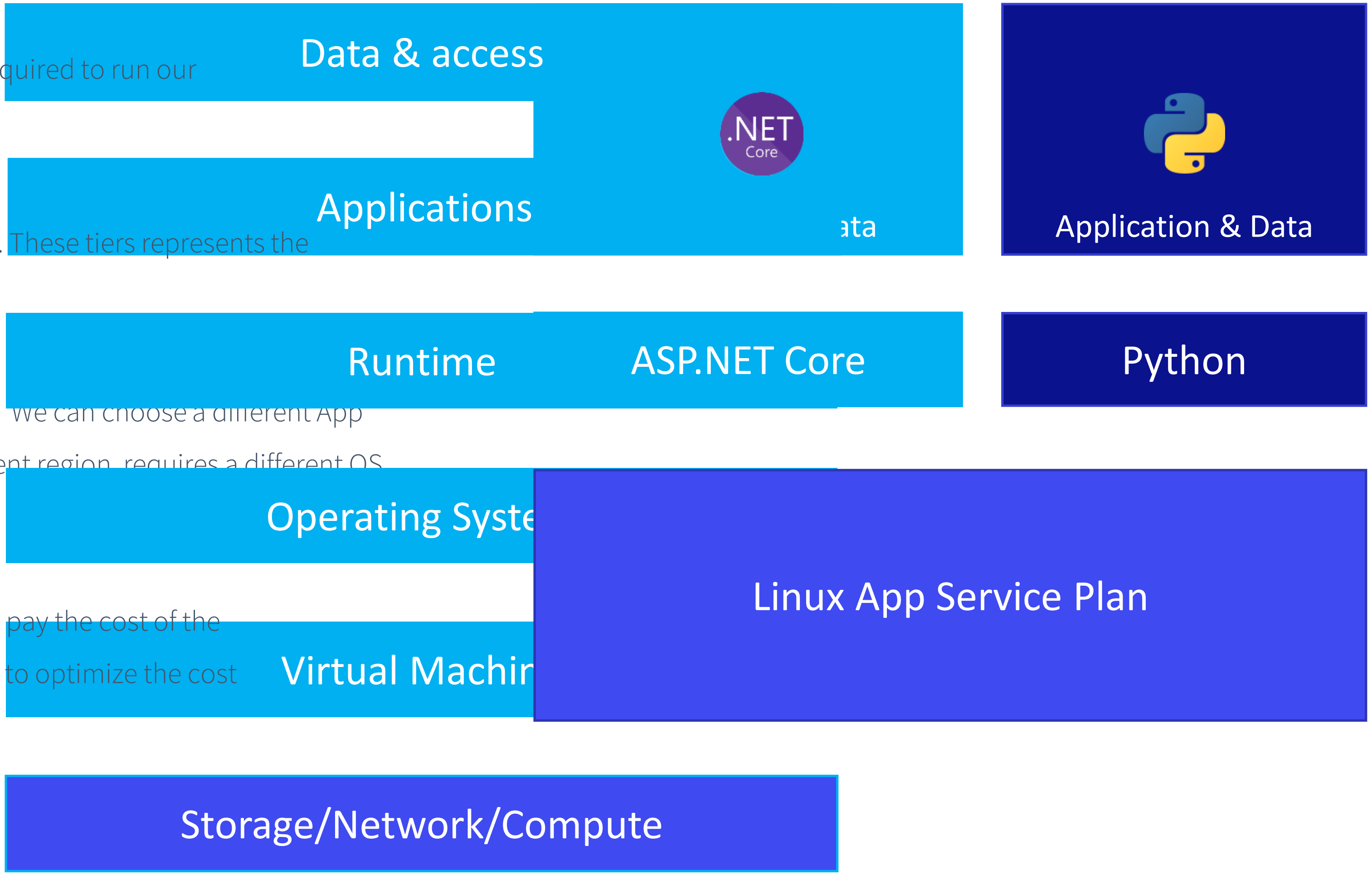
Like VMs, App Service Plans also come in different tiers. These tiers represents the performance, features, size and the price you pay.

Host multiple apps

We can run multiple apps on a single App Service Plan. We can choose a different App Service Plan if you need to deploy your apps in a different region, requires a different OS or higher performance.

Considerations

Regardless of the number of apps you run, you have to pay the cost of the App Service Plans. We need to choose the plans wisely to optimize the cost



App Service Plans

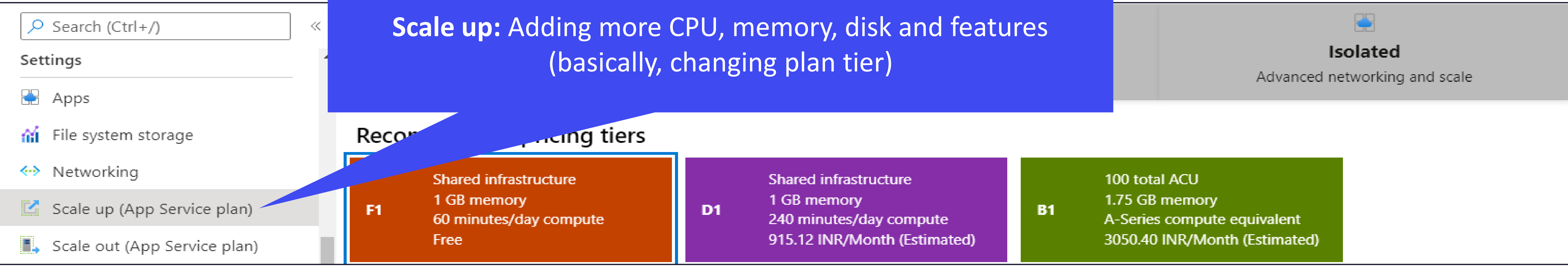
Selected Features	Free	Shared	Basic	Standard	Premium	Isolated
Web, mobile, or API apps	10	100	Unlimited	Unlimited	Unlimited	Unlimited
Disk space	1 GB	1 GB	10 GB	50 GB	250 GB	1 TB
Auto Scale	–	–	–	Supported	Supported	Supported
Deployment Slots	0	0	0	5	20	20
Max Instances	–	–	Up to 3	Up to 10	Up to 30	Up to 100

Shared Compute (Free & Shared): Run apps on the shared Azure VM infrastructure where your app will be placed along with other apps.

Dedicated Compute (Basic, Standard, and Premium): Dedicated VMs will be provisioned, and your apps will be running on that

Isolated: Dedicated VMs will be provisioned in dedicated virtual networks.

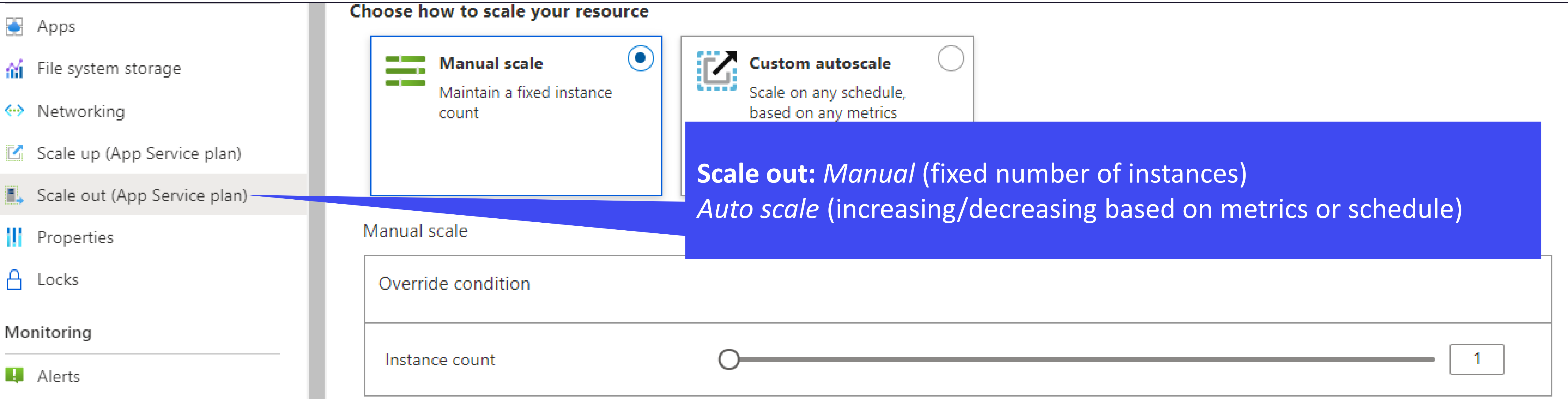
App Service Plans


Search (Ctrl+/)
Settings
Apps
File system storage
Networking
Scale up (App Service plan)
Scale out (App Service plan)
Isolated
Advanced networking and scale

Scale up: Adding more CPU, memory, disk and features (basically, changing plan tier)

Recon… …ricing tiers

F1	Shared infrastructure 1 GB memory 60 minutes/day compute Free
D1	Shared infrastructure 1 GB memory 240 minutes/day compute 915.12 INR/Month (Estimated)
B1	100 total ACU 1.75 GB memory A-Series compute equivalent 3050.40 INR/Month (Estimated)



Choose how to scale your resource

● **Manual scale** Maintain a fixed instance count

○ **Custom autoscale** Scale on any schedule, based on any metrics

Manual scale

Override condition

Instance count: 1

Scale out: *Manual* (fixed number of instances)
Auto scale (increasing/decreasing based on metrics or schedule)

App Service

Single plan

Using App Service Plan, we can host web apps, API apps, mobile apps, and serverless apps.

Fully managed PaaS solution

Developers can focus on enhancing their code, while Microsoft will take care of the underlying virtual machines and infrastructure

CI/CD and Visual Studio Integration

Support CI/CD from source control and we can directly publish our code from Visual Studio.

API and mobile features

Features like CORS support, offline data sync, push notifications making it best candidate for hosting mobile apps.

Support multiple languages

Developer can run .NET, .NET core, Node.js, PHP, Java, Python, and even containerized applications on App Service.

Security and Compliance

Enterprise compliance standards such as ISO, SOC, and PCI is there for App Service. Also, we can setup authentication with Azure AD or social login.

Marketplace templates

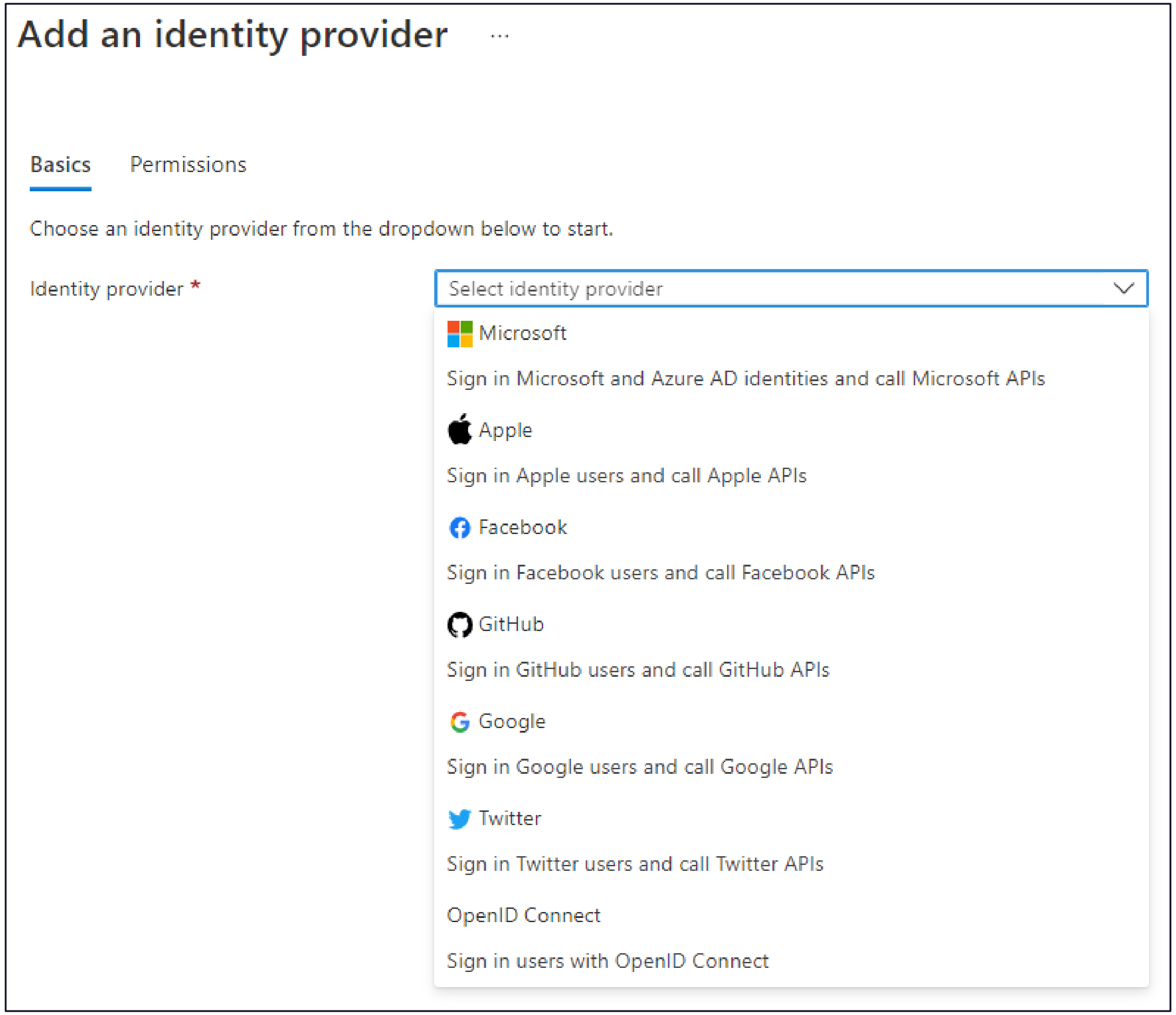
We can use templates like WordPress, Drupal etc. from Azure Marketplace with App Service, making our deployments easier.

Run Function apps

Functions can be run on your existing app service plan without the need to provision additional infrastructure.

Securing an App Service

Securing App Service



Add an identity provider ···

Basics Permissions

Choose an identity provider from the dropdown below to start.

Identity provider * Select identity provider

Microsoft
Sign in Microsoft and Azure AD identities and call Microsoft APIs

Apple
Sign in Apple users and call Apple APIs

Facebook
Sign in Facebook users and call Facebook APIs

GitHub
Sign in GitHub users and call GitHub APIs

Google
Sign in Google users and call Google APIs

Twitter
Sign in Twitter users and call Twitter APIs

OpenID Connect
Sign in users with OpenID Connect

Authentication

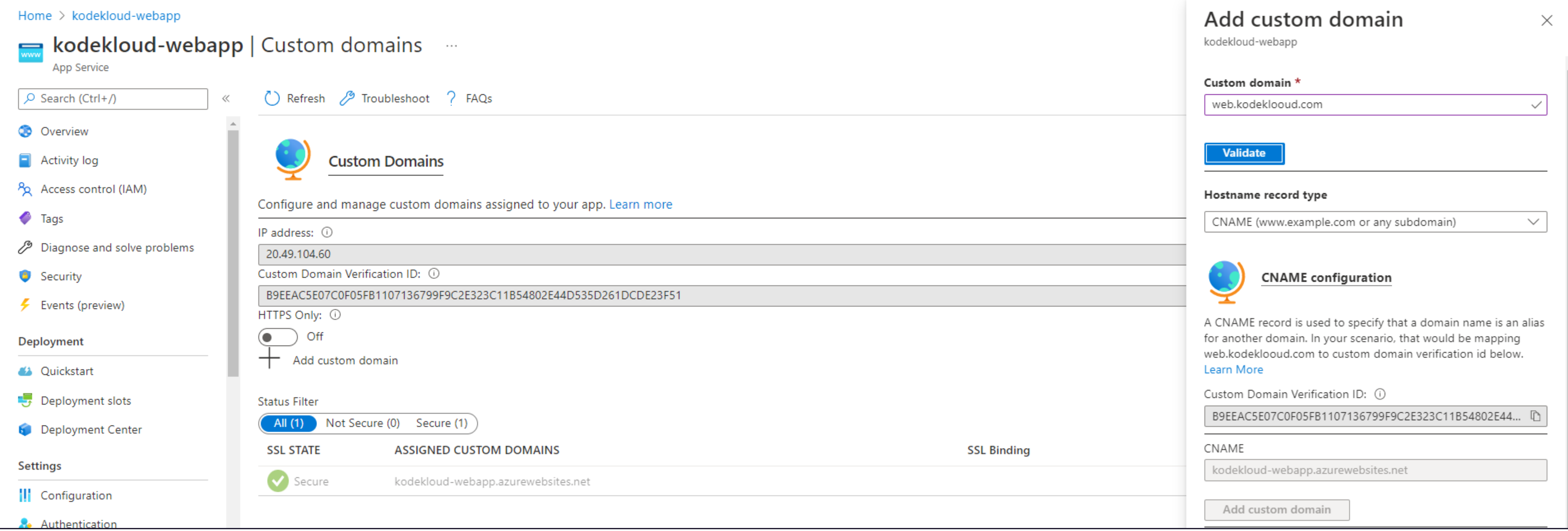
Enable authentication for Azure App Service. Supports Microsoft, Apple, Facebook, GitHub, Google, Twitter, or any service that's using OpenID Connect. Default selection will be anonymous, where users can access the app without presenting any credentials.

Security

- SSL certificates
- Diagnostic settings for troubleshooting
- Network ACL
- Integrate keys with Azure Key Vault

Custom Domains

Custom Domains in App Service



Home > kodekloud-webapp

kodekloud-webapp | Custom domains ...

App Service

Custom Domains

Configure and manage custom domains assigned to your app. Learn more

IP address: 20.49.104.60

Custom Domain Verification ID: B9EEAC5E07C0F05FB1107136799F9C2E323C11B54802E44D535D261DCDE23F51

HTTPS Only: Off

+ Add custom domain

Status Filter: All (1) | Not Secure (0) | Secure (1)

SSL STATE	ASSIGNED CUSTOM DOMAINS	SSL Binding
Secure	kodekloud-webapp.azurewebsites.net	

Add custom domain

kodekloud-webapp

Custom domain *: web.kodeklooud.com

Validate

Hostname record type: CNAME (www.example.com or any subdomain)

CNAME configuration

A CNAME record is used to specify that a domain name is an alias for another domain. In your scenario, that would be mapping web.kodeklooud.com to custom domain verification id below. Learn More

Custom Domain Verification ID: B9EEAC5E07C0F05FB1107136799F9C2E323C11B54802E44...

CNAME: kodekloud-webapp.azurewebsites.net

Add custom domain

Branding

By default, Azure creates an entry in azurewebsites.net domain. You can bring in your own domain and add to your app service. You need to validate the domain, before you could add to the App Service

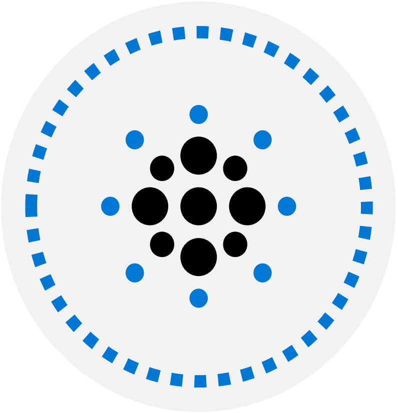
Supports A or CNAME mapping

Requires to create TXT record to prove domain ownership. Once that's done, you can add an A record or CNAME record to map the custom domain to App Service.

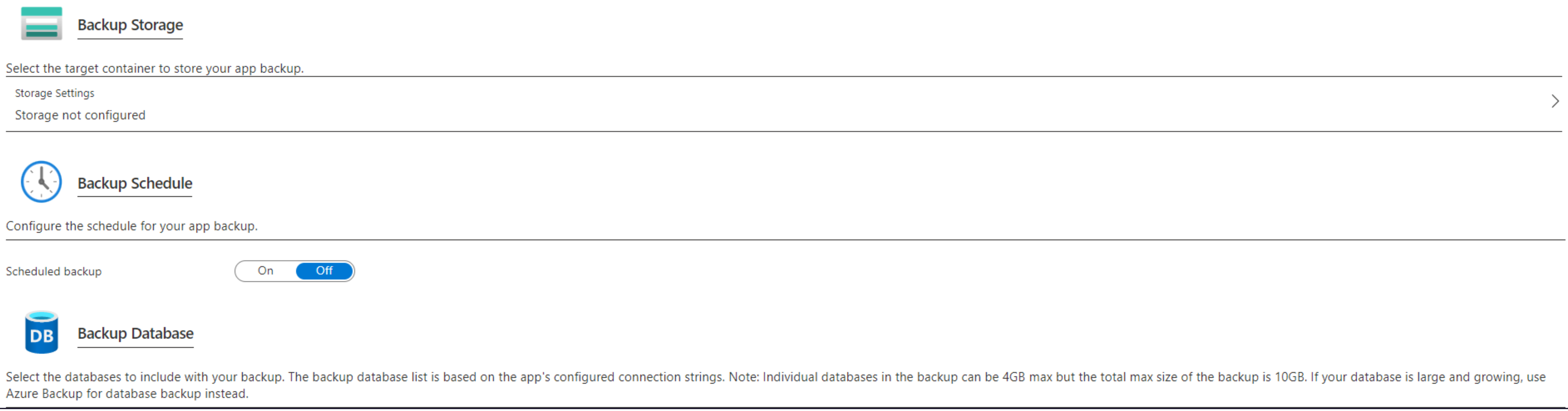
Plan dependent

Custom domains are supported from Basic plan onwards.

Backup App Service



Backup App Service



Backup Storage

Select the target container to store your app backup.

Storage Settings

Storage not configured

Backup Schedule

Configure the schedule for your app backup.

Scheduled backup ○ On [✓ Off]

Backup Database

Select the databases to include with your backup. The backup database list is based on the app's configured connection strings. Note: Individual databases in the backup can be 4GB max but the total max size of the backup is 10GB. If your database is large and growing, use Azure Backup for database backup instead.

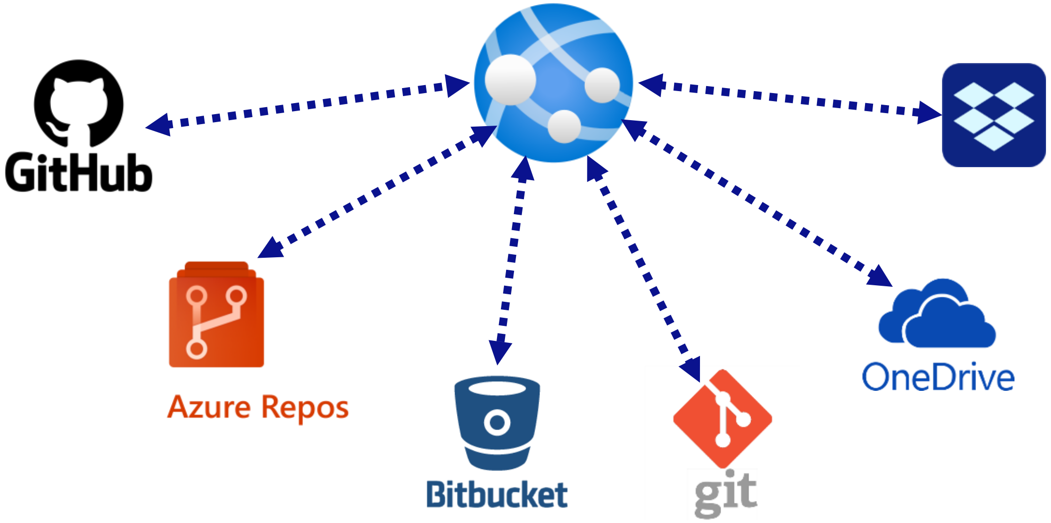
- **Manual and scheduled backups**
  Backup supports manual or scheduled backup which includes the backup of configuration, file contents, and the connected database.

- **Filters and multiple restore options**
  Backup can be up to 10 GB of app and database. Full and partial backups can be configured. We can restore the app to a previous restore point or create a new app altogether.

- **Plan dependent**
  Backup requires Standard or Premium plan

CI/CD and Deployment slots

CI/CD



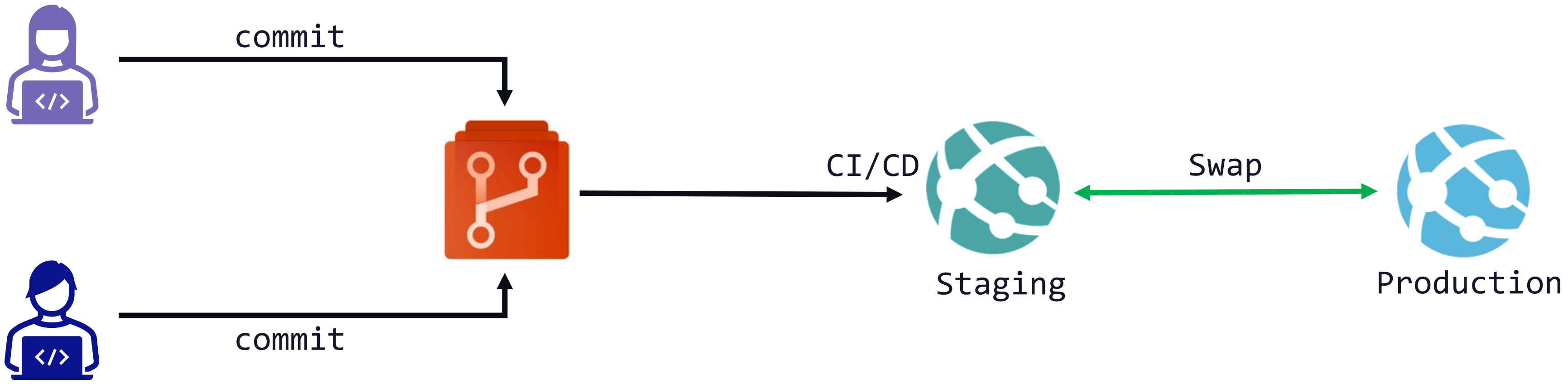
Automated Deployment

Automated deployment (CI/CD) is where developers will be push new code which includes features, patches and bug fixed with minimal impact to end users. These features will be immediately updated in Azure App Service. We can integrate App Services with GitHub, Bitbucket, Local Git and Azure Repos

Manual Deployment

Manual Deployment is where developers can store their code in a remote cloud storage like OneDrive/Dropbox or to an external git. In manual deployment, developers need to manually push the code to the location for the App Service to update.

Deployment slots



Slots representing different environments
With the help of deployment slots, we can run different versions of our application like prod, qa, dev etc.

Unique URLs
Deployments slots will have their own unique URL like your App Service

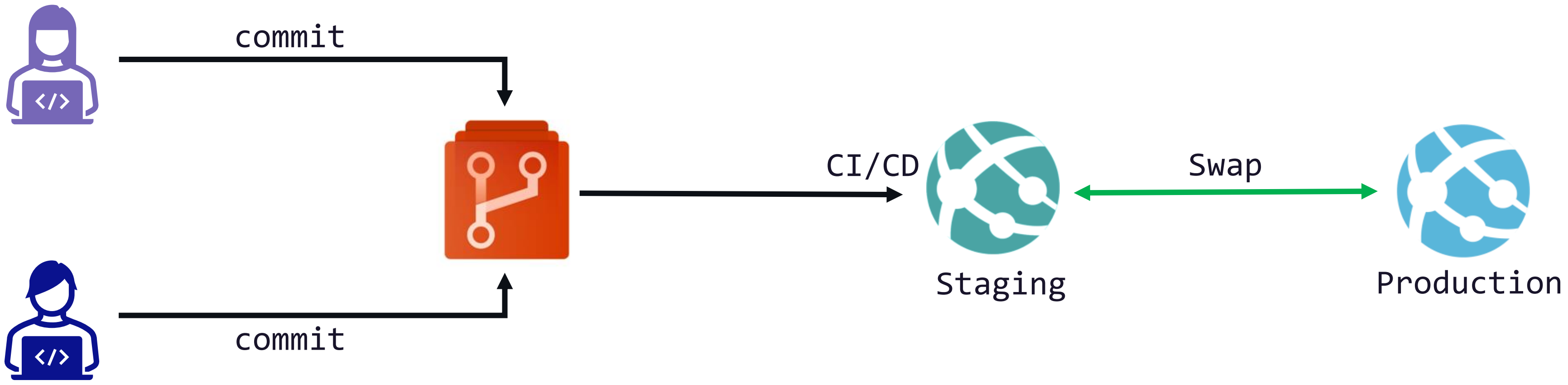
Reduces downtime and rollback strategy
As we are swapping, deployment slots avoids cold start and hence eliminate service disruption. Since this is a swap, we can always swap and roll back to the last known good configuration.

Test before swapping
Developers get a chance to test and validate their code in App Service before pushing to production.

Auto swap
We can configure auto-swap in scenarios where validation is not needed.

Plan dependent
Number of slots supported depends on the service plan. Free, Shared, and Basic plan doesn't support deployment slots. Standard supports up to 5, Premium supports up to 20 and Isolated supports up to 20 slots.

Deployment slots - considerations



Decision

Decide whether you want to clone an app configuration, clone from another deployment slot or do no copy anything.

Understand what will be swapped or not

Understand the list of settings that can be swapped and cannot be swapped.

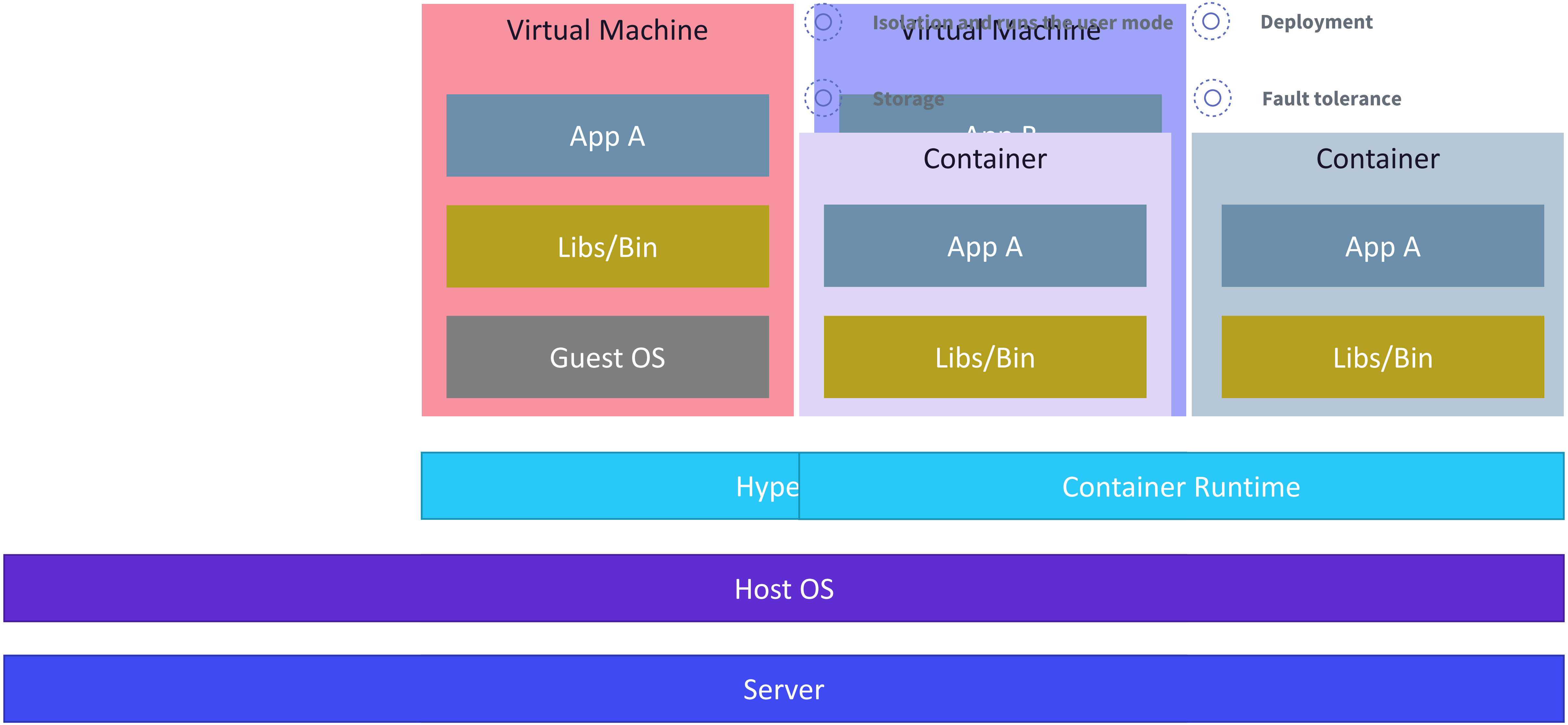
Settings that can be swapped	
General settings	WebJobs contents
App Settings & Path mappings	Hybrid connections*
Connection strings	Service Endpoints*
Handler mappings	Azure CDN*

Settings that aren't swapped		
Publishing endpoints	Scale settings	CORS
Custom domain names	IP restrictions	VNet integration
Non-public certificates	Always On	Managed identities
TLS/SSL settings	Diagnostic settings	Settings that end with _EXTENSION_VERSION suffix

KODEKLOUD

Azure Container Instances

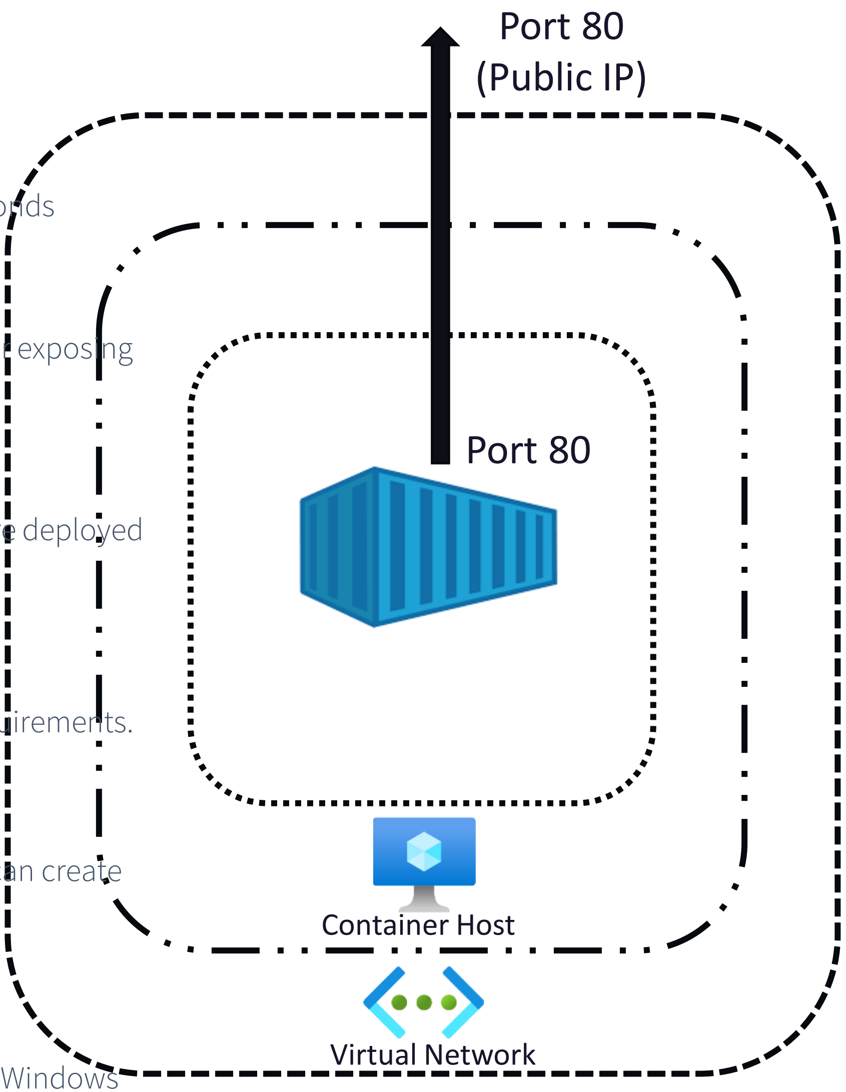
Virtual Machines v/s Containers



- Isolation and runs the user mode
- Storage
- Deployment
- Fault tolerance

Azure Container Instances

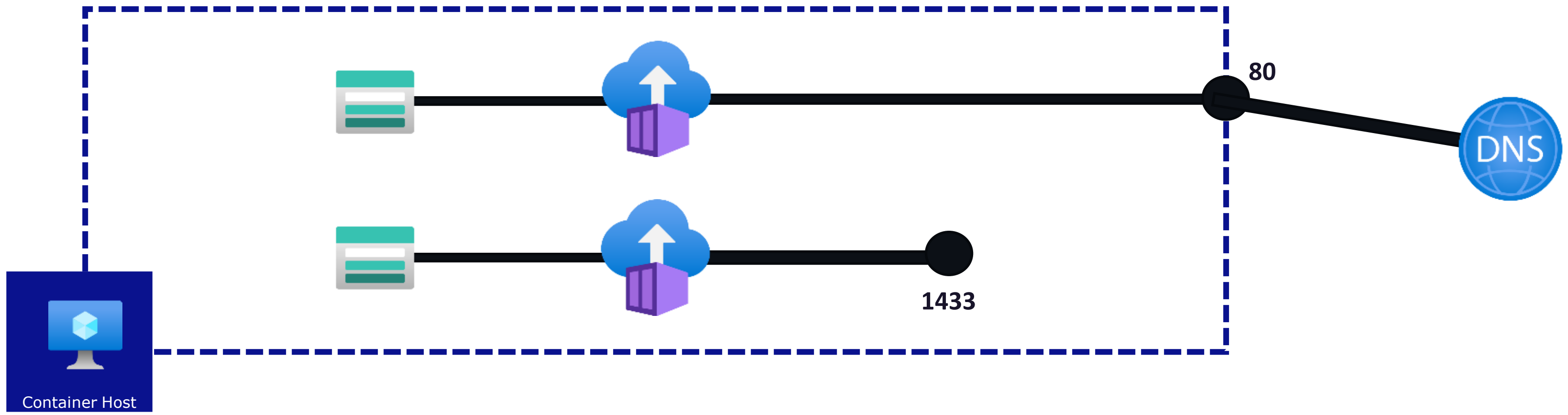
- **Faster startup**
  Unlike Virtual Machines, containers can startup in seconds
- **Host internet facing applications**
  ACI supports Public IP and DNS name which is ideal for exposing your container apps to the internet.
- **Isolation**
  Containers are isolated from each other even if they are deployed on the same container host.
- **Scalability**
  You can choose custom sizes as per your resource requirements.
- **Persistent storage**
  Container storage is ephemeral, using Azure Files we can create persistent storage for ACI.
- **OS and VNet**
  ACI can be directly deployed to virtual networks. Both Windows and Linux containers are supported by ACI.



Container Groups

Container groups

Collection of containers that get scheduled on the same container host machine they share resources, lifecycle, local network, and storage volumes.



Deployment options

Container Groups can be deployed using ARM templates or YAML file. If your container group includes Azure resources like a file share, then ARM template is the better option.

Resource allocation

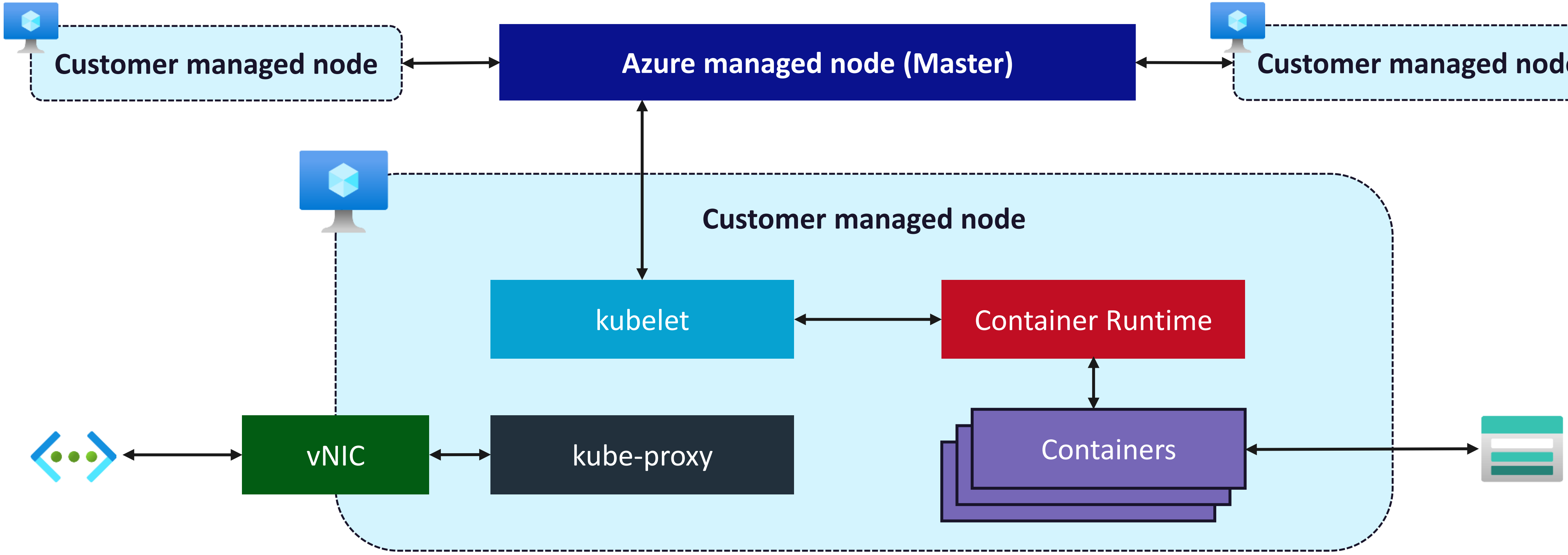
Resource requests of the container group is calculated by summing up resource request of individual containers that's part of the container group.

Shared networking

Public IP address, one or more ports, and DNS label can be shared within container group. In order to reach the containers from internet, we need to expose the port to the internet.

Azure Kubernetes Service

Azure Kubernetes Services



Azure managed node

This node is created automatically when you create an AKS cluster.

This node is not visible to the end user and run Kubernetes master node services

Customer managed nodes

These nodes run your containerized applications and services. You only pay for the number of nodes.

kubelet

Receives requests from Azure managed node for scheduling containers

kube-proxy

Routes traffic and manages IP addresses of pods and services

Container Runtime

Allows containers to be created and interact with networking and storage components

AKS Terminology

Pools

Logical grouping of nodes with identical configuration

Nodes

VMs that are running containerized application. Nodes are managed by Kubernetes master node which is not visible to the end user.

Pods

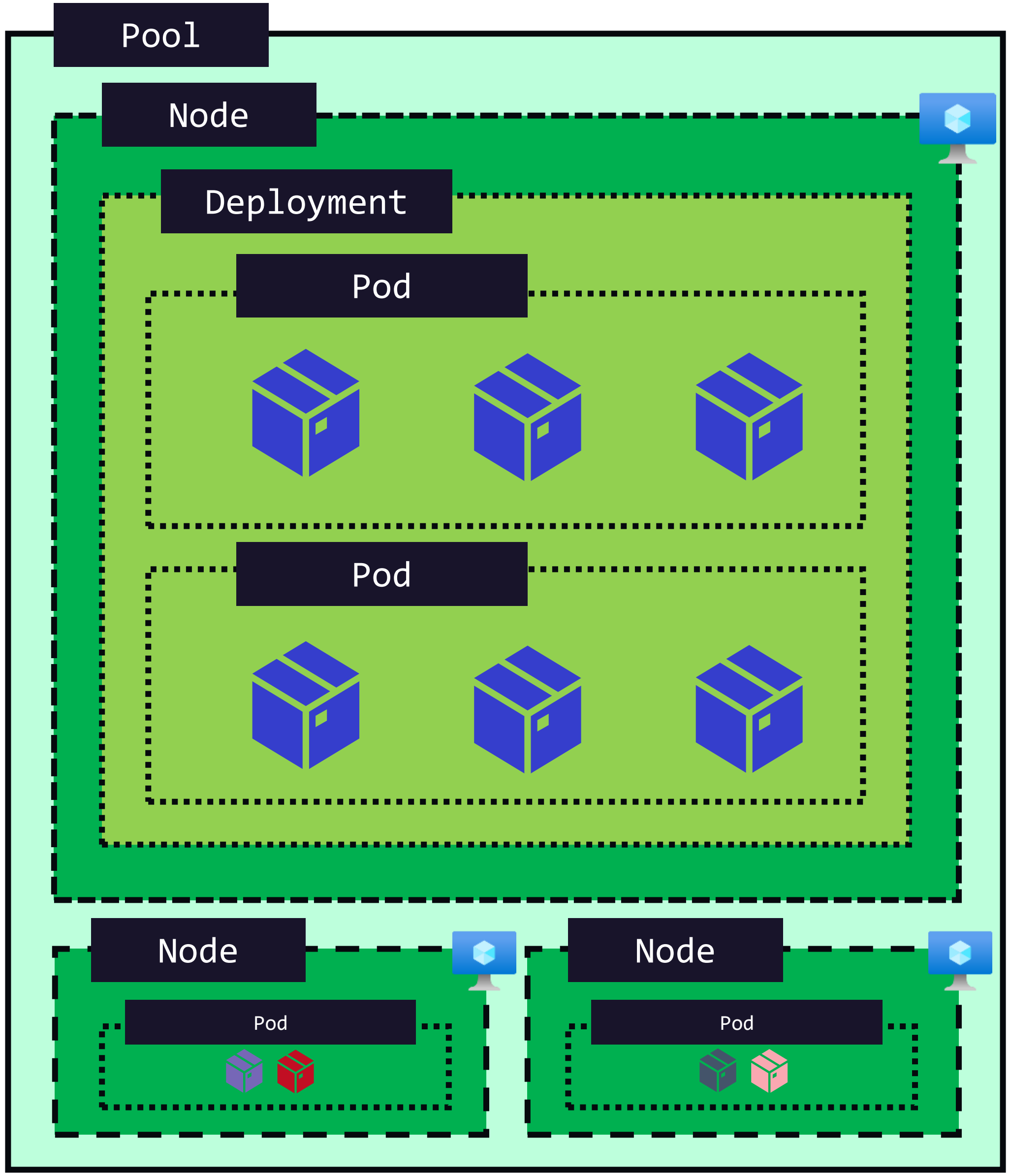
Smallest unit of deployment which is a collection of one or more containers representing a single instance of your application.

Deployment

Creates one or more identical replicas of your pod

Manifest

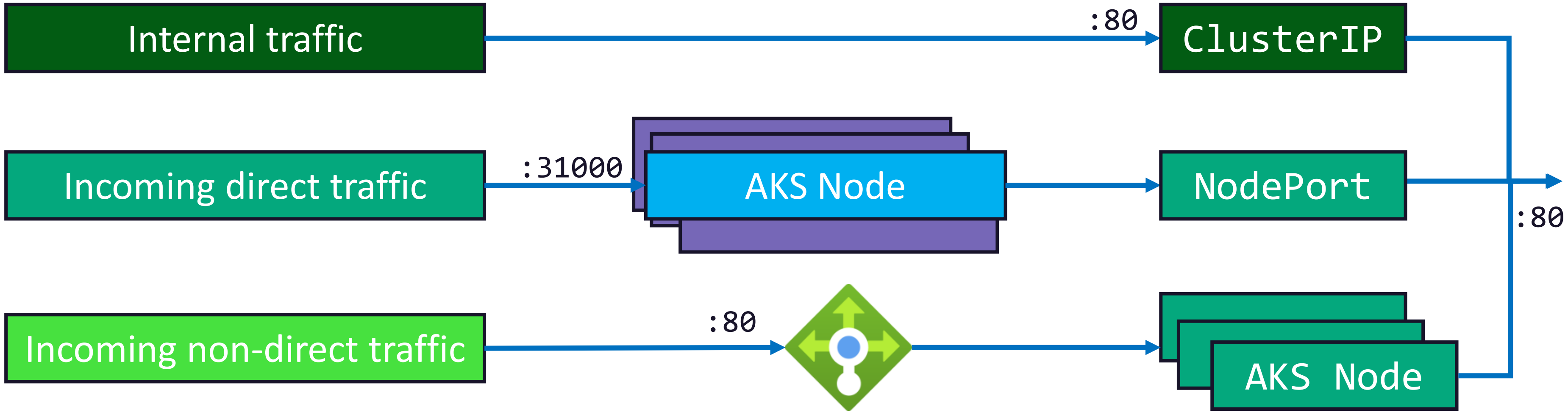
YAML or JSON file used for deployment



AKS Networking

AKS Networking

Services in Kubernetes provide internal and external network connectivity to pods



ClusterIP

Facilitates internal communication with other apps in your cluster. There is no external access. ClusterIP is the default Kubernetes service

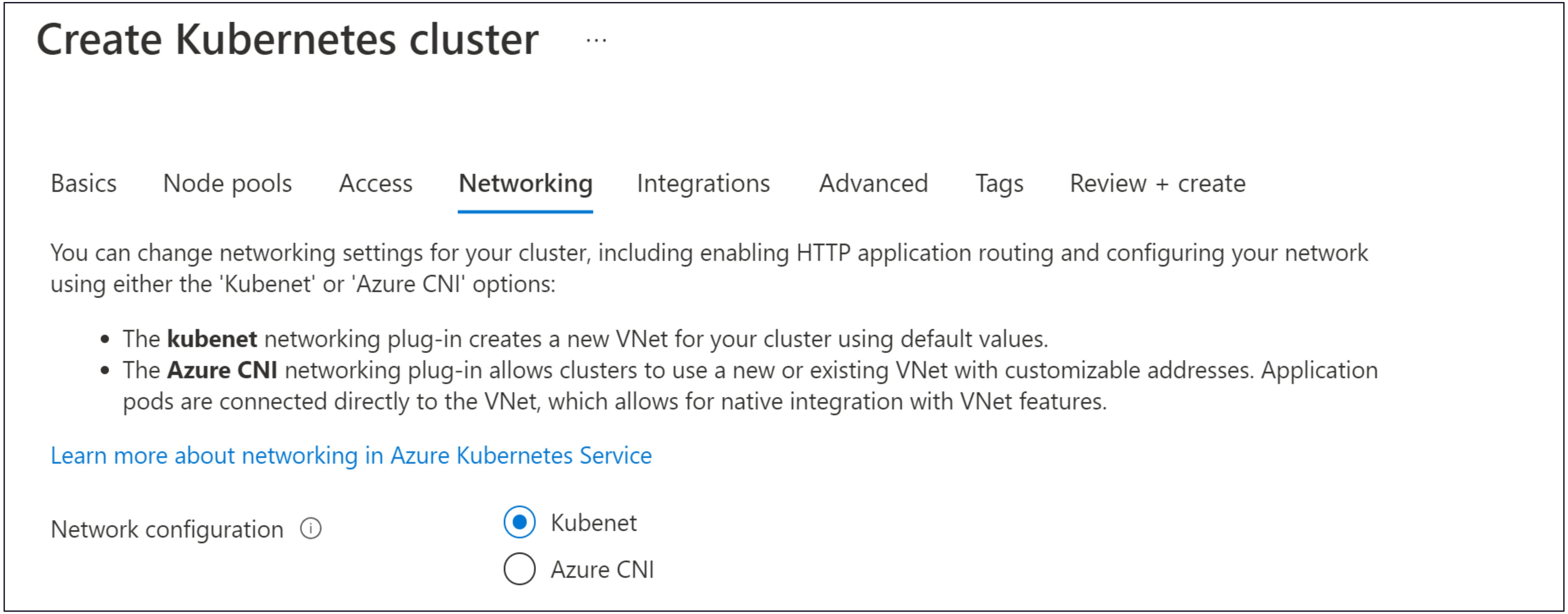
NodePort

Open a specific port on the node and forward traffic to pod via the service. You can choose port numbers 30000-32767 and number of services is limited to one service per port

LoadBalancer

Creates an Azure Load Balancer which will route the traffic from external to the service. This is the standard way to expose your applications to the internet.

AKS Networking



Create Kubernetes cluster ...

You can change networking settings for your cluster, including enabling HTTP application routing and configuring your network using either the 'Kubenet' or 'Azure CNI' options:

- The **kubenet** networking plug-in creates a new VNet for your cluster using default values.
- The **Azure CNI** networking plug-in allows clusters to use a new or existing VNet with customizable addresses. Application pods are connected directly to the VNet, which allows for native integration with VNet features.

Learn more about networking in Azure Kubernetes Service

Network configuration ⓘ ● Kubenet ○ Azure CNI

AKS Storage

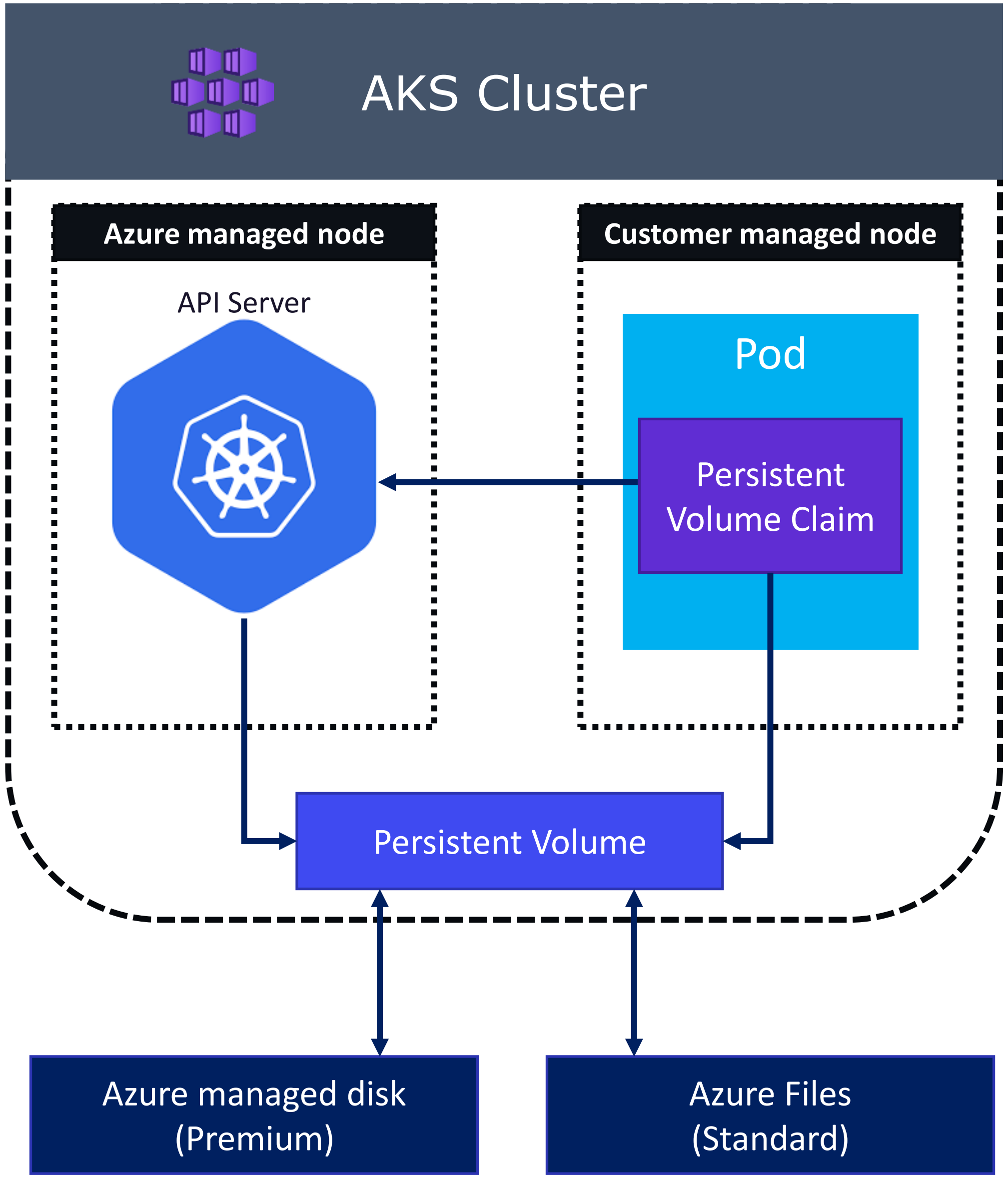
AKS Storage

Volumes
Volumes can be used to store, retrieve, and persist data. Local storage is fast and easy to use, on the other hand, Kubernetes treats pods as ephemeral. If needed, we can create persistent volume using Azure Files or Azure Managed Disk.

Persistent Volumes
Volume created along with pod is deleted when the pod is deleted. With the help of persistent volume (PV) we can persist the storage even after deleting the pod.

Storage class
While creating storage, we can use StorageClasses to define the tier of the storage required. You can select Premium or Standard. With the help of reclaimPolicy parameter, we can define if the storage needs to be persisted or not.

Persistent Volume Claims
Using PVC, we can request Azure Managed Disk or Azure File for a specific tier (via StorageClass), access mode and size.



AKS Scaling

AKS Scaling

Manual scale

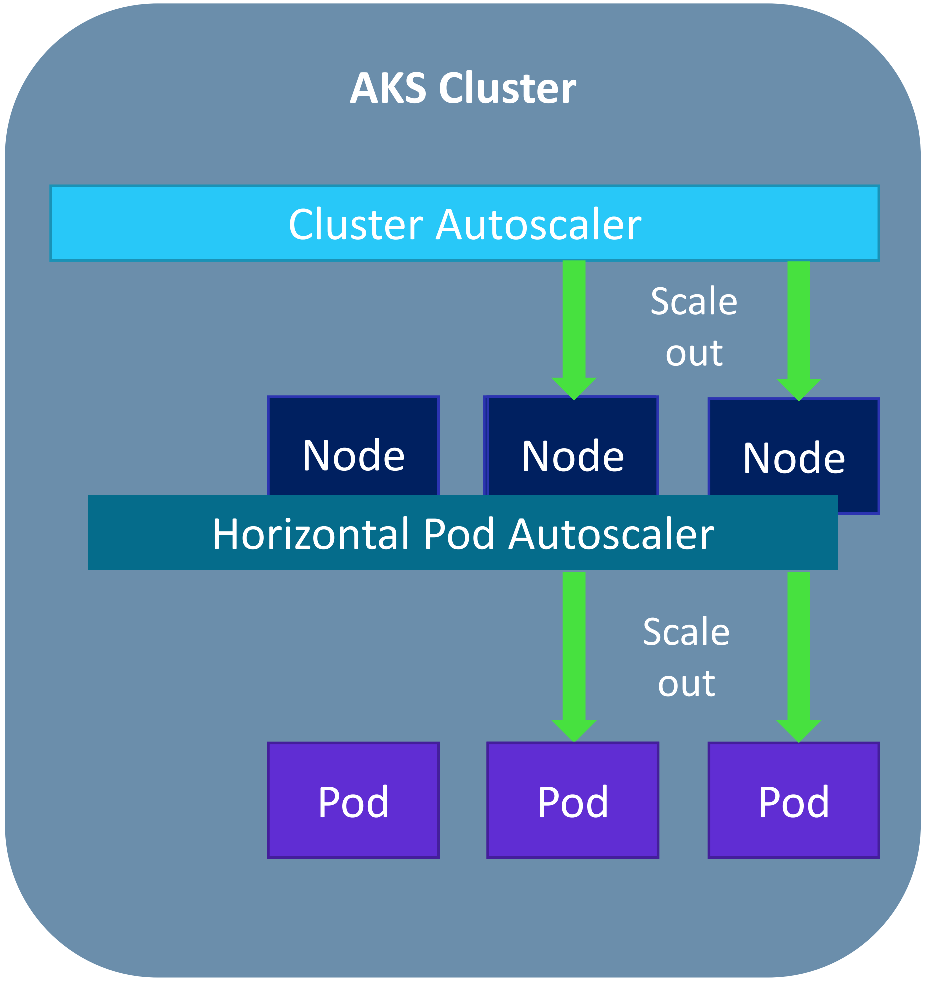
Based on the requirement, you can independently increase the number of pods replicas or increase the number of nodes.

Cluster autoscaler

Cluster autoscaler can increase the number of nodes in the cluster automatically based on demand. API server checks every 10 seconds for validate if there are any changes required on the node count.

Horizontal Pod Autoscaler

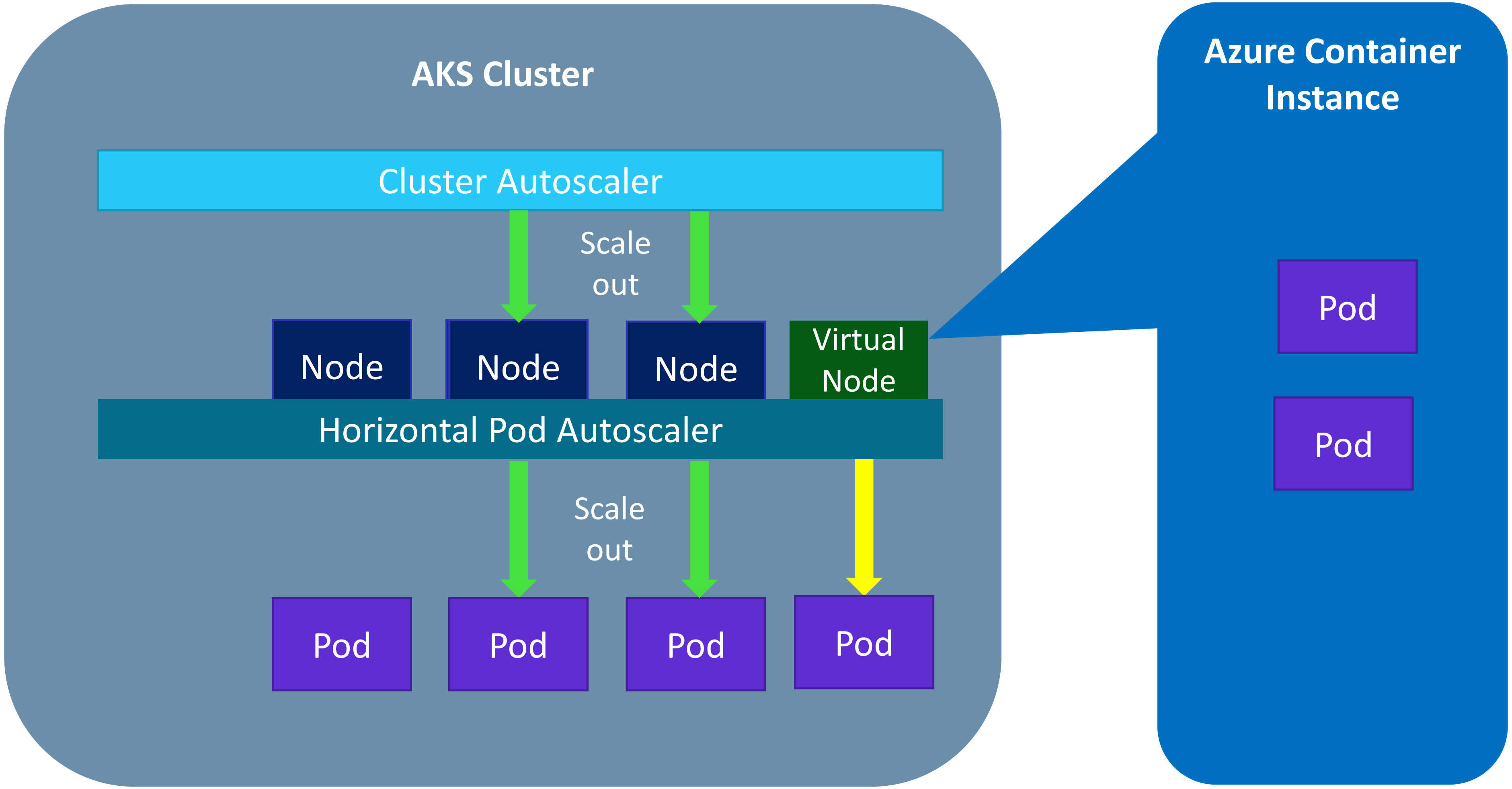
Based on the demand, HPA will automatically increase the number of pod replicas. Metrics API checks every 30 seconds to see if there any changes required on the replica count.



For best scaling, we need to use both cluster autoscaler and HP

AKS Bursting

AKS Bursting



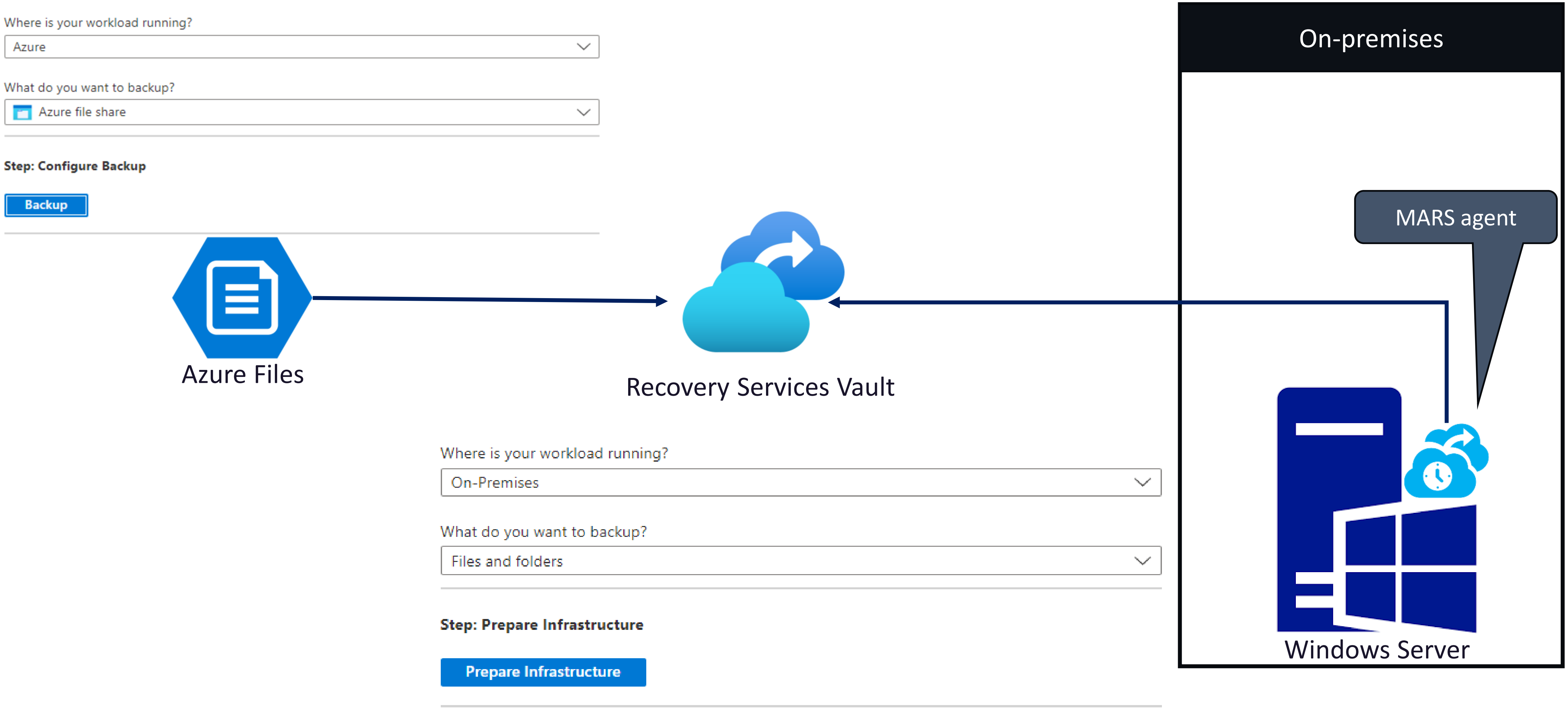
We can use ACI as a virtual node to rapidly scale AKS cluster

Azure Demonstration

KODEKLOUD

File and Folder Backup

File and Folder Backup



Where is your workload running?

Azure

What do you want to backup?

Azure file share

Step: Configure Backup

Backup

Where is your workload running?

On-Premises

What do you want to backup?

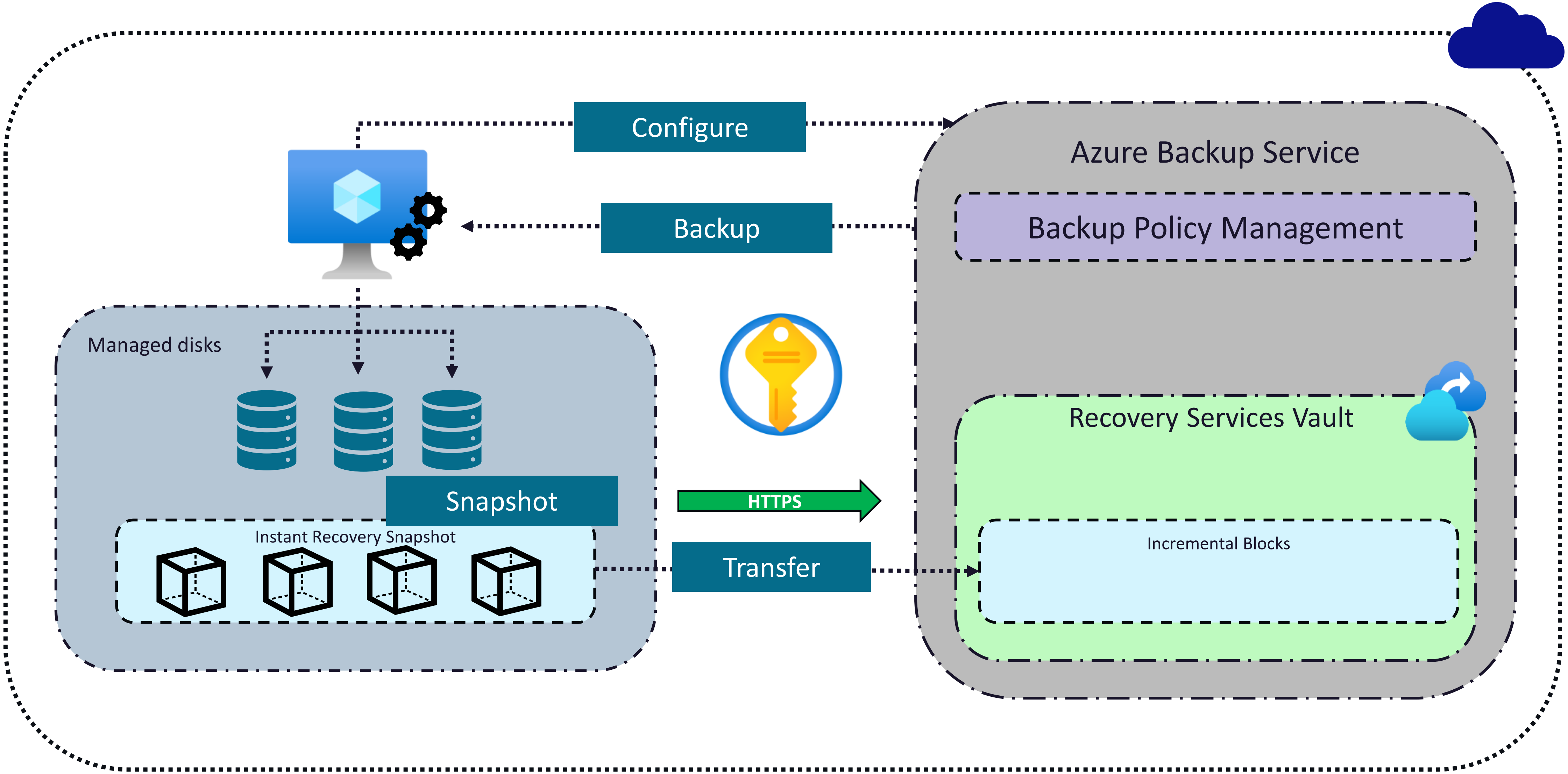
Files and folders

Step: Prepare Infrastructure

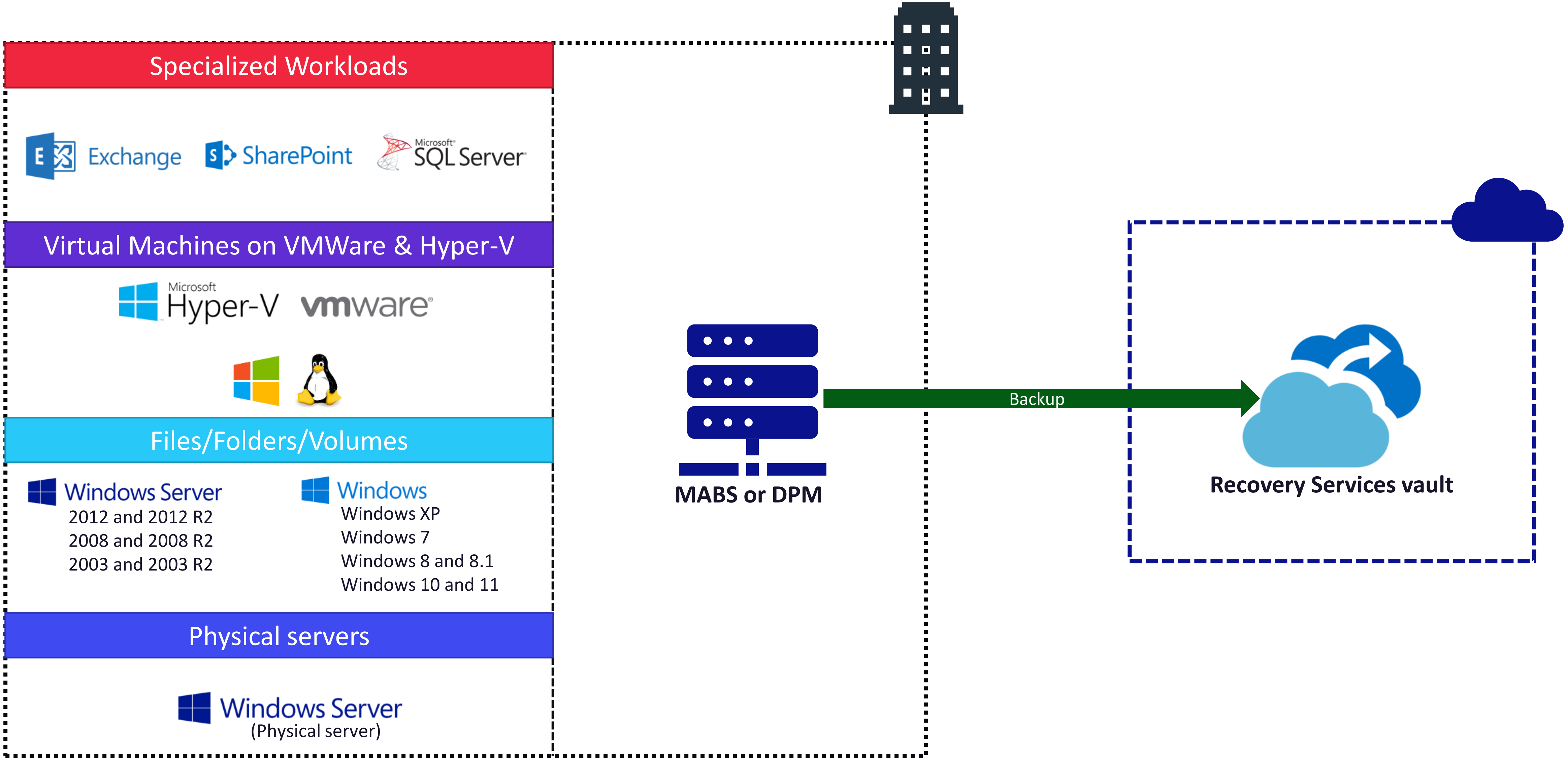
Prepare Infrastructure

Virtual Machine Backup

Virtual Machine Backup – Azure VMs



Virtual Machine Backup – On-premises VMs



Specialized Workloads

Exchange SharePoint Microsoft SQL Server

Virtual Machines on VMWare & Hyper-V

Microsoft Hyper-V vmware

Files/Folders/Volumes

Windows Server
2012 and 2012 R2
2008 and 2008 R2
2003 and 2003 R2

Windows
Windows XP
Windows 7
Windows 8 and 8.1
Windows 10 and 11

Physical servers

Windows Server
(Physical server)

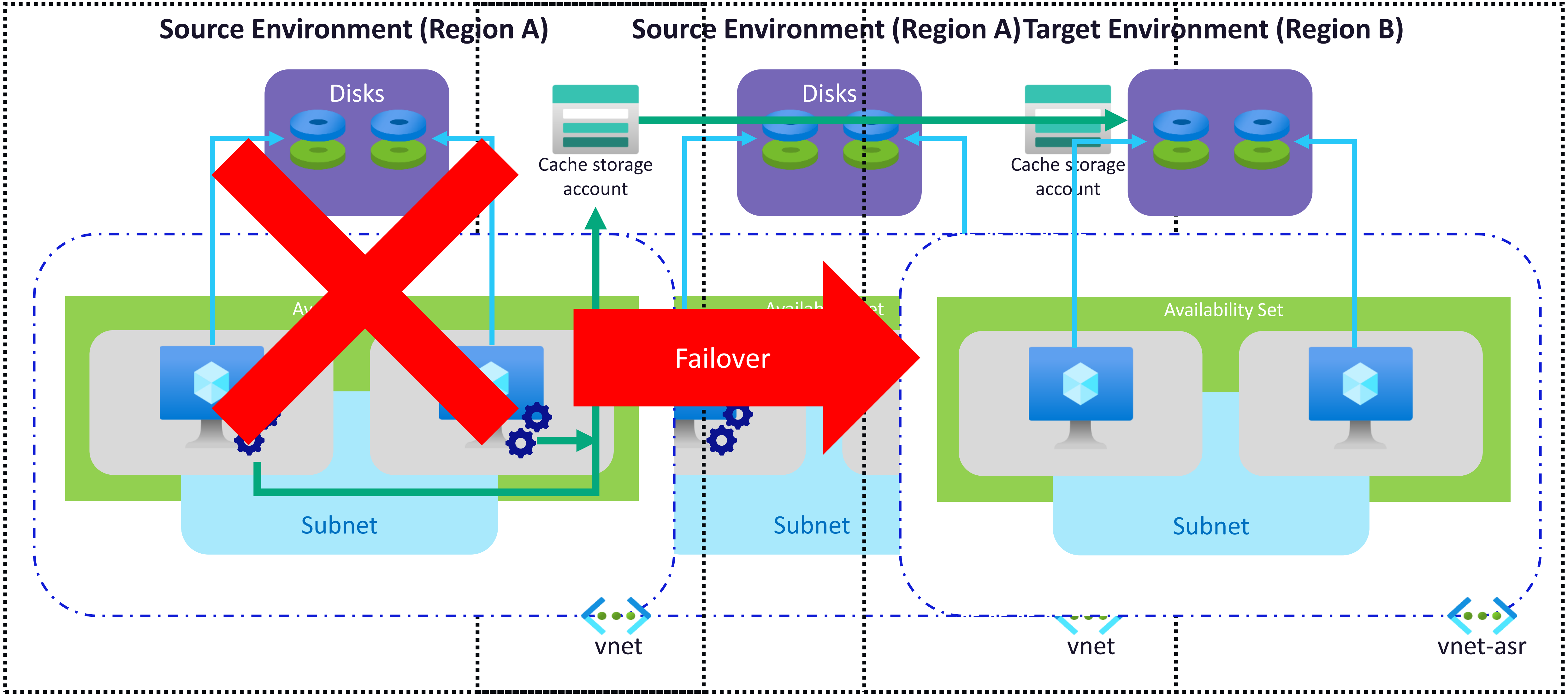
MABS or DPM

Backup

Recovery Services vault

Azure Site Recovery

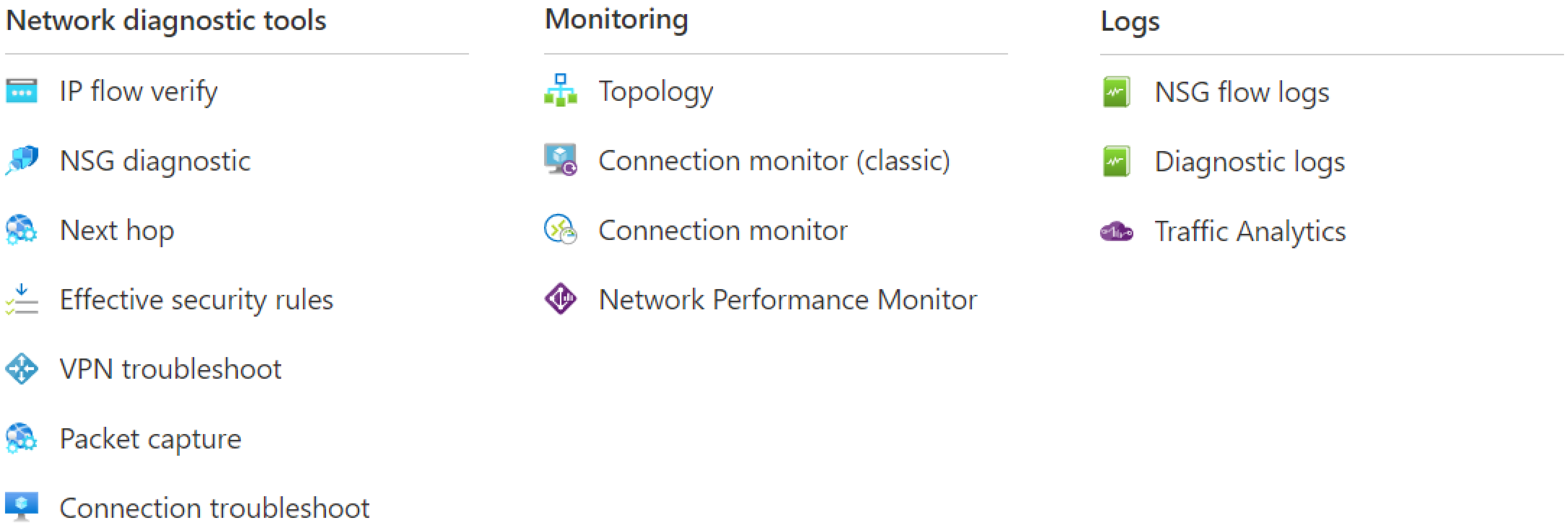
Azure Site Recovery



KODEKLOUD

Network Watcher

Network Watcher



Network diagnostic tools

- IP flow verify
- NSG diagnostic
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Monitoring

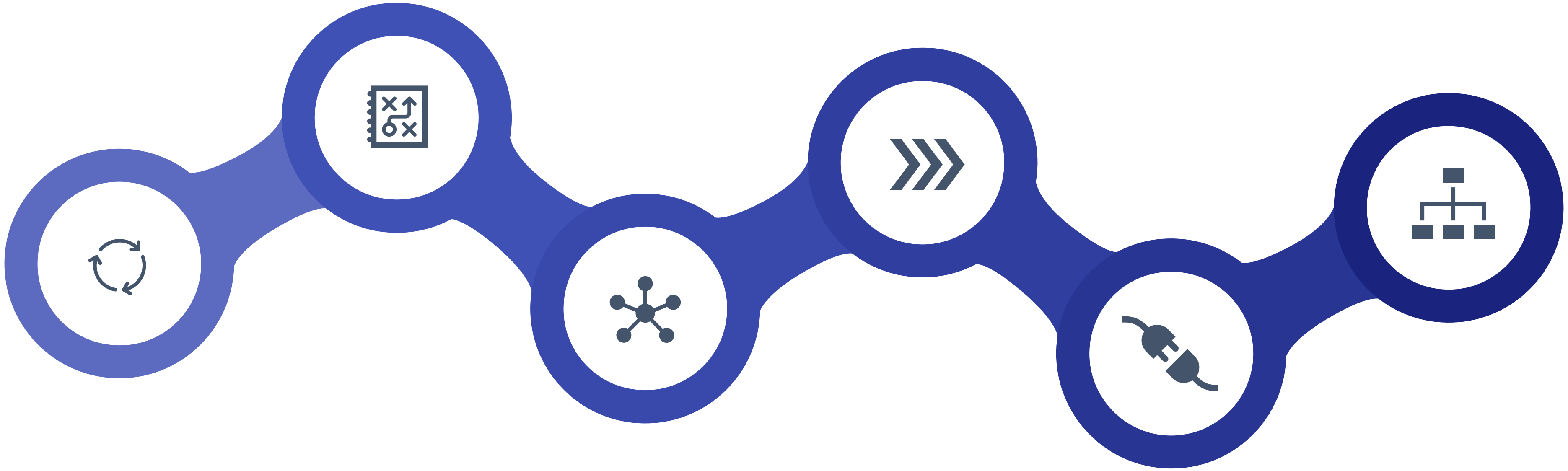
- Topology
- Connection monitor (classic)
- Connection monitor
- Network Performance Monitor

Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

Network Watcher is a regional service that can be used to diagnose, monitor, and setup logging for resources that are deployed in Azure Virtual Network

Network Watcher



IP Flow verify is used to verify inbound and outbound connectivity from or to a VM from a remote IP address

Next hop is used to identify the next destination the traffic will be routed to.

VPN diagnostics will help you diagnose VPN connectivity issues and troubleshoot them.

NSG Flow Logs will store the details of the traffic through an NSG in a storage account.

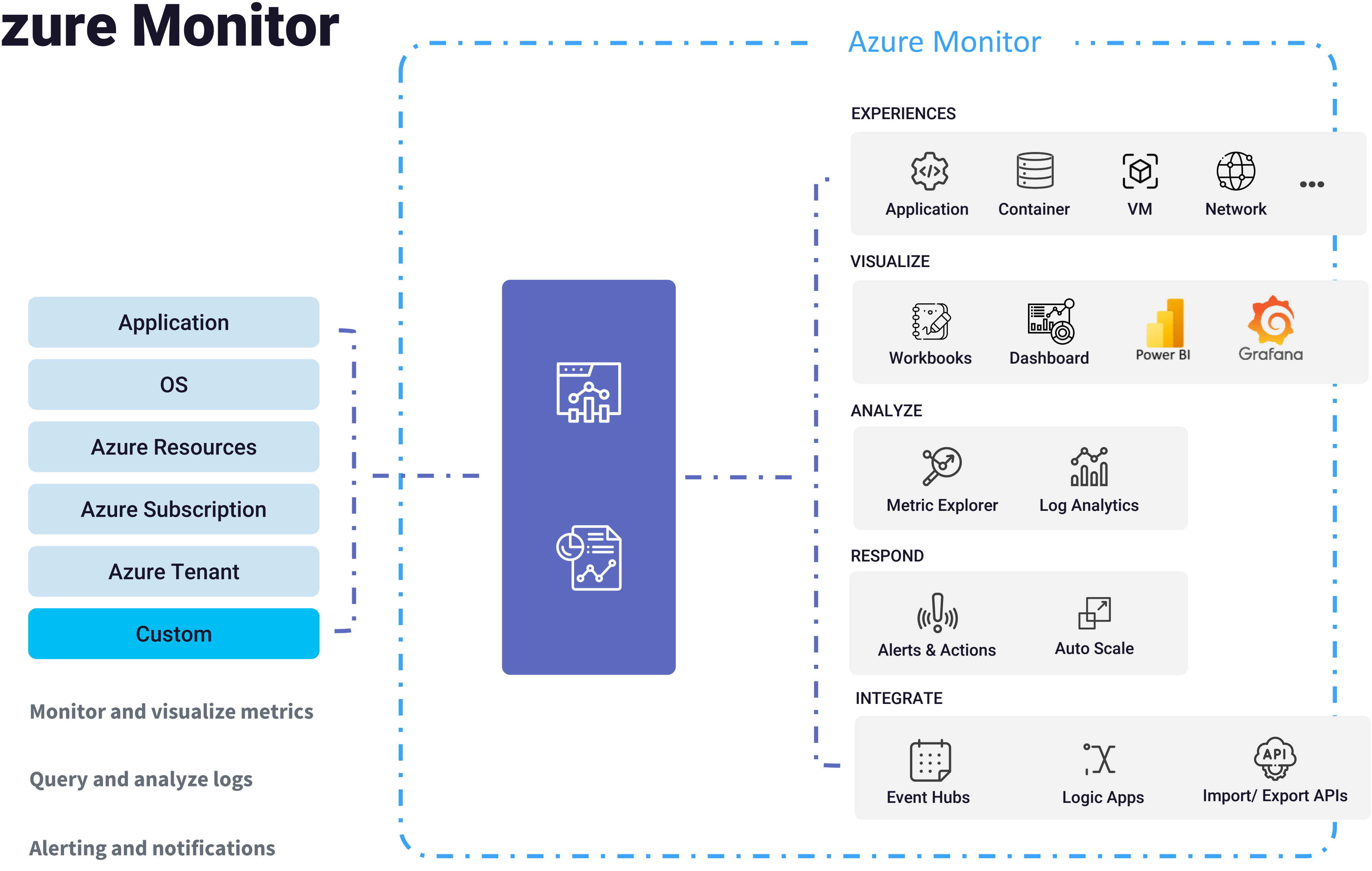
Connectionn troubleshoot can be used to identify network performance and connectivity issues

Topology can be used to see the topology of your Azure infrastructure.

KODEKLOUD

Azure Monitor

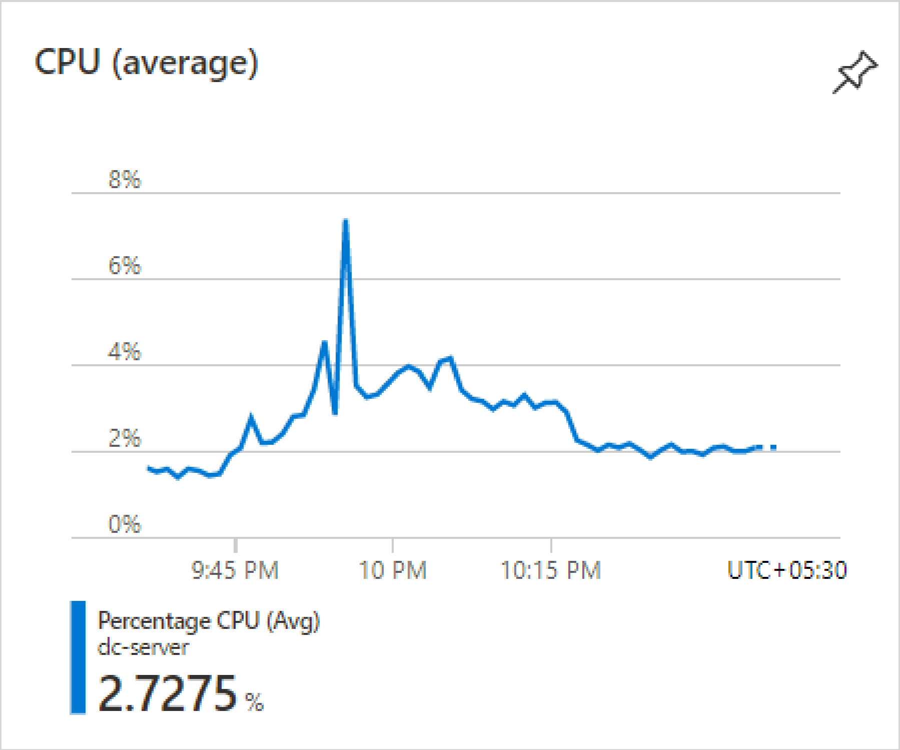
Azure Monitor

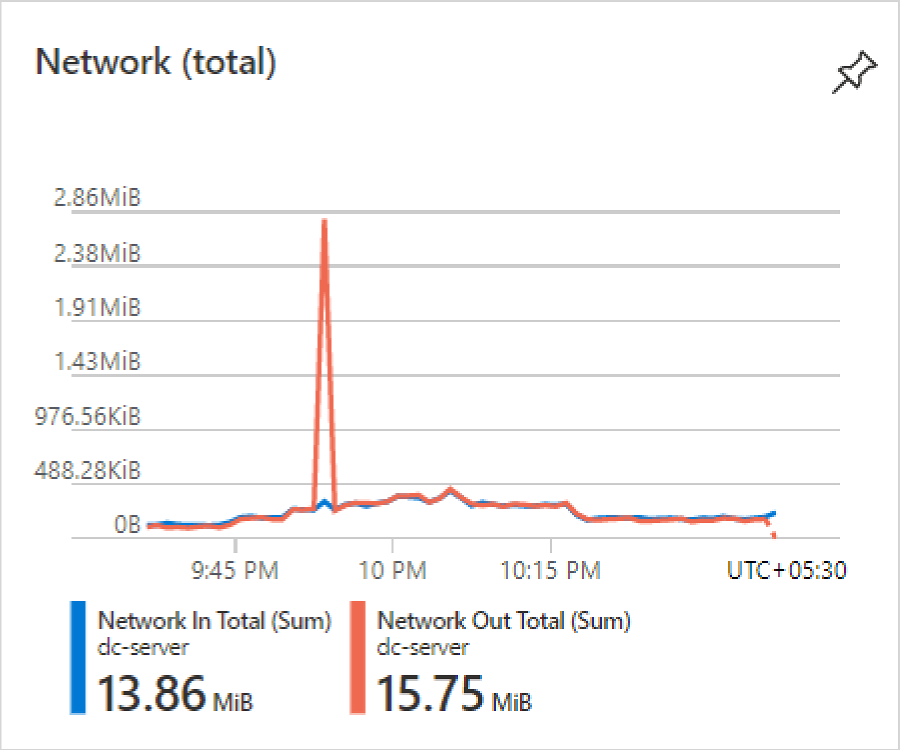


- Monitor and visualize metrics
- Query and analyze logs
- Alerting and notifications

Image source: https://docs.microsoft.com/en-us/azure/azure-monitor/data-platform

Metrics





Zero configuration required

Metrics are collected from Azure resources without any additional configuration. Thus, collected data is displayed in the Overview blade of the resource and we can analyze further with the help of Metrics Explorer.

Time series

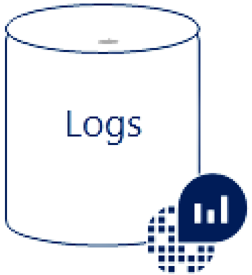
Metrics are plotted on a time axis to represent the state of a system at a point in time.

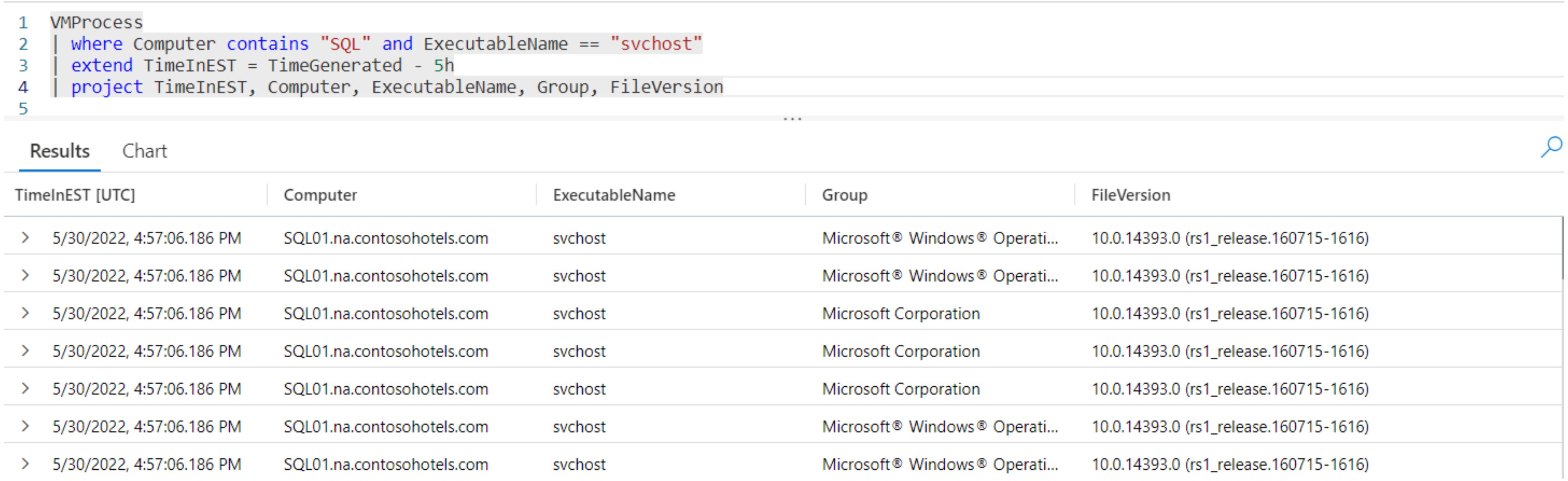
Near real time data

As Metrics can visualize real time data which represents the state of our system, it’s easy to monitor and troubleshoot issues.

Azure Monitor

Logs





```
VMProcess
| where Computer contains "SQL" and ExecutableName == "svchost"
| extend TimeInEST = TimeGenerated - 5h
| project TimeInEST, Computer, ExecutableName, Group, FileVersion
```

TimeInEST [UTC]	Computer	ExecutableName	Group	FileVersion
5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)
5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)
5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft Corporation	10.0.14393.0 (rs1_release.160715-1616)
5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft Corporation	10.0.14393.0 (rs1_release.160715-1616)
5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft Corporation	10.0.14393.0 (rs1_release.160715-1616)
5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)
5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)

Organized as records

Logs represent data that are organized into different records. Each record represents an event or information

Requires additional configuration

Logs collected are stored in Log Analytics and this collection requires agents to be configured on the source.

Rich query language

Log Analytics supports Kusto Query Language (KQL) for querying the data stored in the repository. KQL supports simple queries and complex queries where you can perform joins, aggregations, and analytics.

Data Sources

Application

- Instrumentation Packa
- Availability Test

OS

- Azure Monitor
- Azure diagnost

Azure Resources

- Metrics
- Resource Logs

Azure Subscription

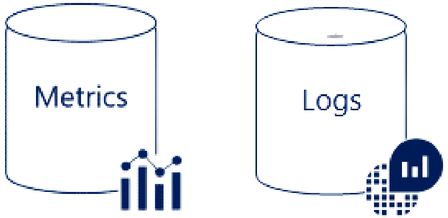
- Service Health
- Activity Log

Azure Tenant

- Ac

Custom

- Instrumentation Package
- Application



Azure Activity Log

Subscription level logging

All subscription level events will be logged in Azure Activity Logs. The ingested data includes all ARM operations and service health events.

Auditing

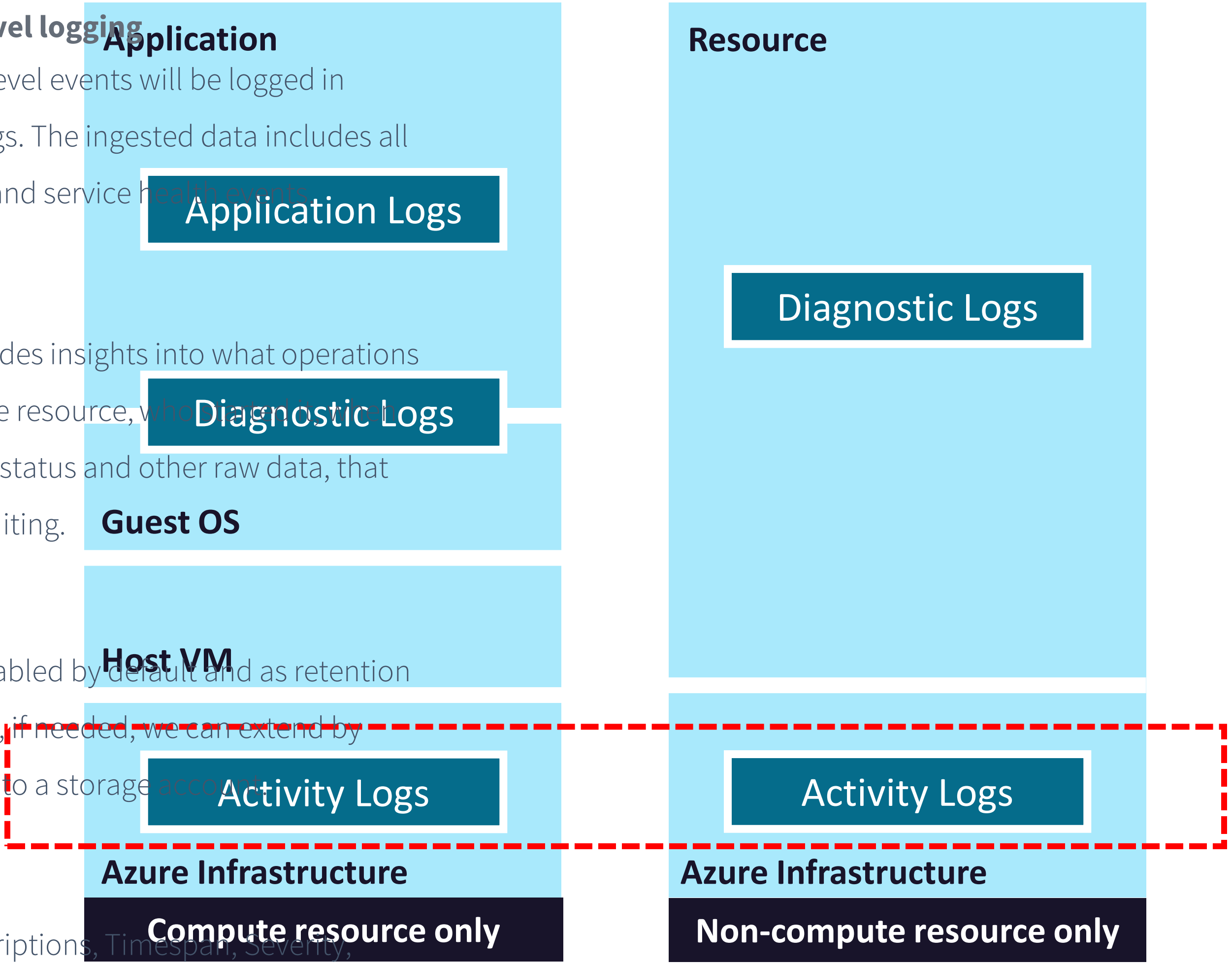
Activity Log provides insights into what operations were taken on the resource, who started it, when did that happen, status and other raw data, that could help in auditing.

Retention

Activity Log is enabled by default and as retention period of 90 days, if needed, we can extend by sending the data to a storage account.

Querying data

Filters like Subscriptions, Timespan, Severity, Resource group, Resource, Operation, Event initiated by, and Search for keywords



Azure Activity Log – Event Categories

Administrative

All Resource Manager create, update, delete, and action operations are categorized under Administrative

Security

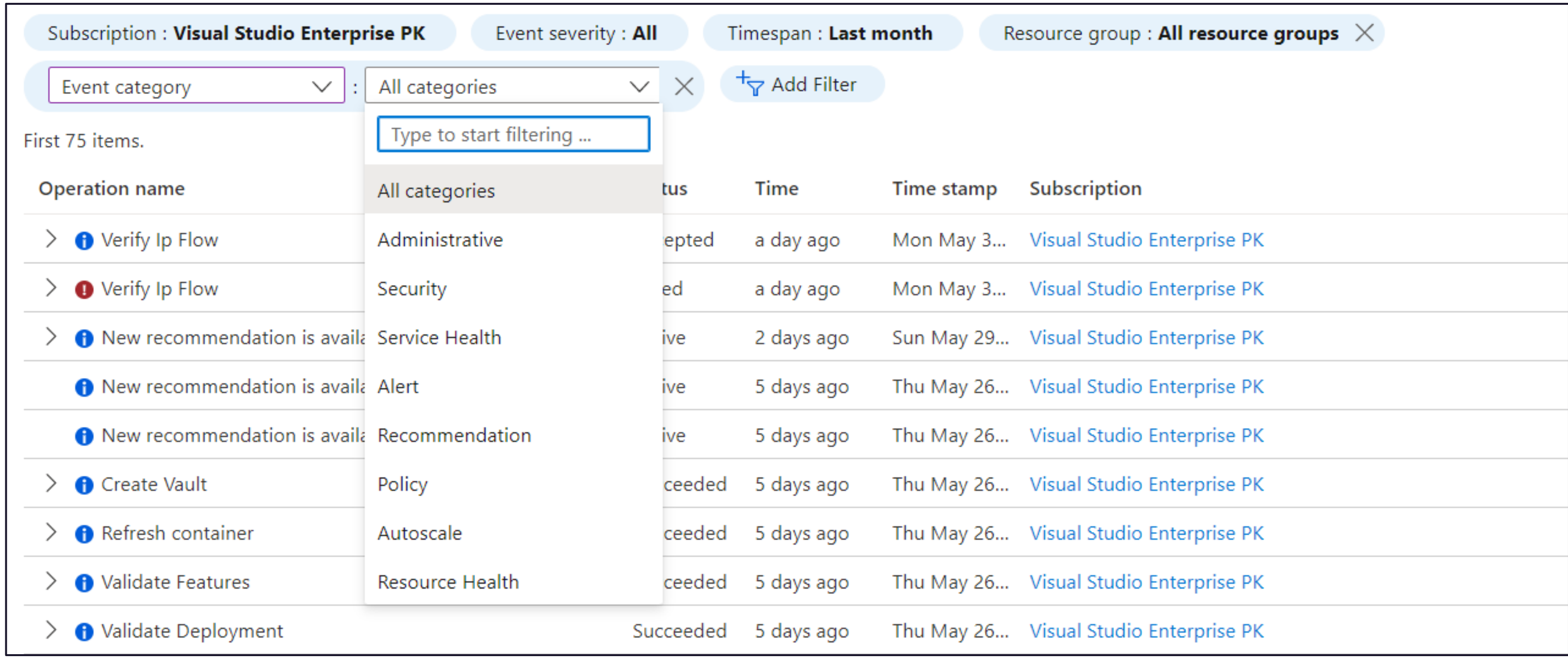
All security alerts generated by Microsoft Defender for cloud will be mapped under this category.

Service Health

Any service health incidents happened to Azure Resources, this may or not may not include your resources.

Alert

Any alerts triggered in Azure Alerts.



Subscription : **Visual Studio Enterprise PK** | Event severity : **All** | Timespan : **Last month** | Resource group : **All resource groups** ✕

Event category ⌄ : All categories ⌄ ✕ | Add Filter

Type to start filtering ...

First 75 items.

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

Operation name	tus	Time	Time stamp	Subscription
Verify Ip Flow	epted	a day ago	Mon May 3...	Visual Studio Enterprise PK
Verify Ip Flow	ed	a day ago	Mon May 3...	Visual Studio Enterprise PK
New recommendation is availa	ive	2 days ago	Sun May 29...	Visual Studio Enterprise PK
New recommendation is availa	ive	5 days ago	Thu May 26...	Visual Studio Enterprise PK
New recommendation is availa	ive	5 days ago	Thu May 26...	Visual Studio Enterprise PK
Create Vault	ceeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK
Refresh container	ceeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK
Validate Features	ceeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK
Validate Deployment	Succeeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK

Recommendation

All recommendations generated in Azure Advisor

Policy

All policy effects will be mapped to this category.

Autoscale

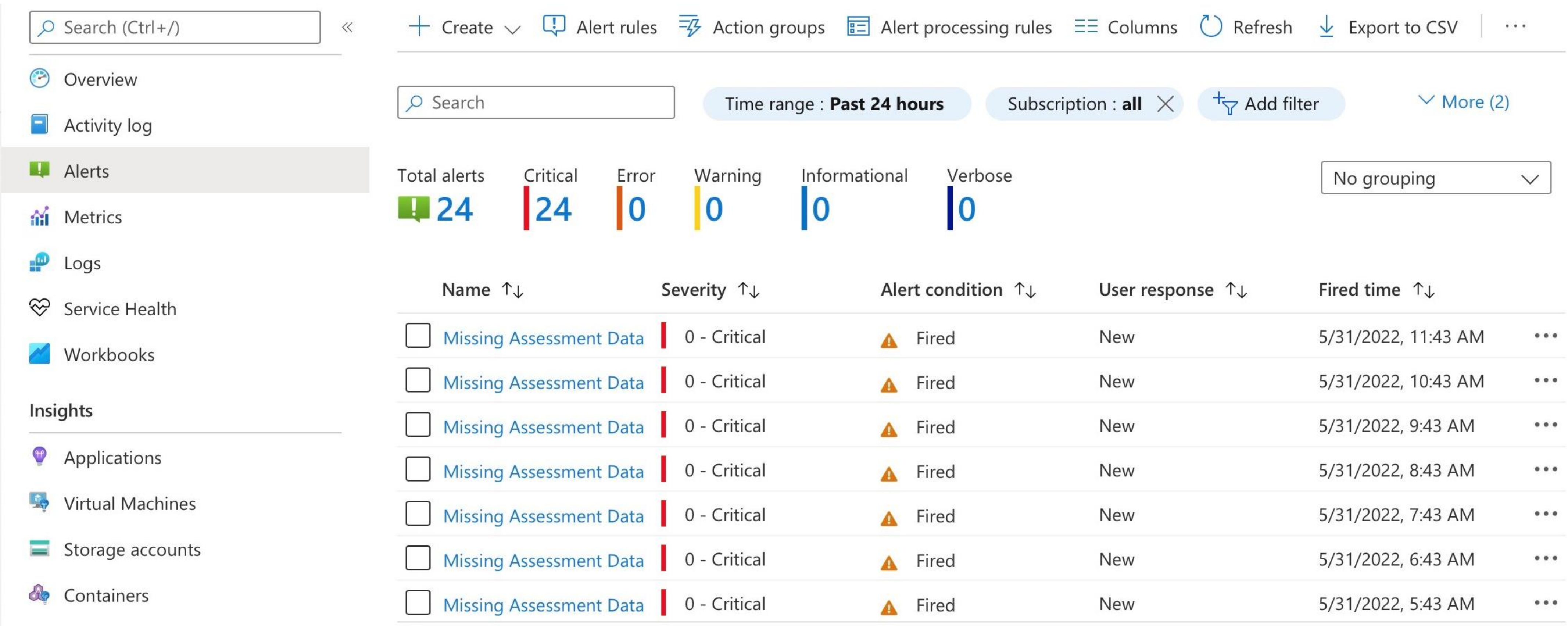
This category contains all scale in and out events

Resource Health

Health events associated your Azure resources.

Azure Alerts

Azure Monitor Alerts



Time range : **Past 24 hours** | Subscription : **all** | No grouping

Total alerts	Critical	Error	Warning	Informational	Verbose
24	24	0	0	0	0

	Name	Severity	Alert condition	User response	Fired time
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 11:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 10:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 9:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 8:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 7:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 6:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 5:43 AM

Unified Authoring Experience

We can create alerts for Activity Logs, Service Health Events, Log Analytics, Metrics etc. In all these scenarios the authoring experience is same.

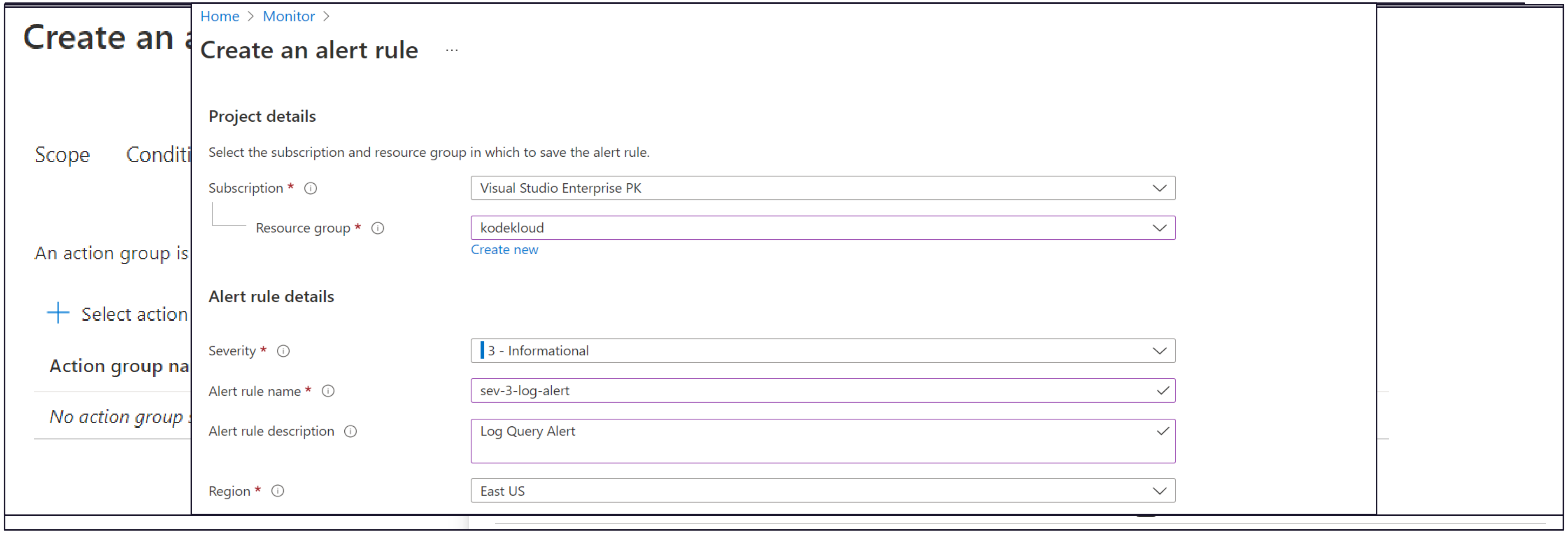
Classify based on severity and response

Azure Alerts supports severity (0-4), so you easily prioritize the alerts. Secondly, we can categorize by user response New, Acknowledged or Closed.

Integrate with Action Groups

Define your notification and automation preferences with the help of Action Groups.

Azure Monitor Alerts



Home > Monitor >

Create an alert rule ...

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription *	Visual Studio Enterprise PK
Resource group *	kodekloud

Create new

Alert rule details

Severity *	3 - Informational
Alert rule name *	sev-3-log-alert
Alert rule description	Log Query Alert
Region *	East US

Scope

Defines the scope for alert

Condition

Helps you to define the signal and criteria for alert

Actions

Integrate alerts with Action Groups

Rule details

Specify name, severity, region, resource group and subscription for the alert.

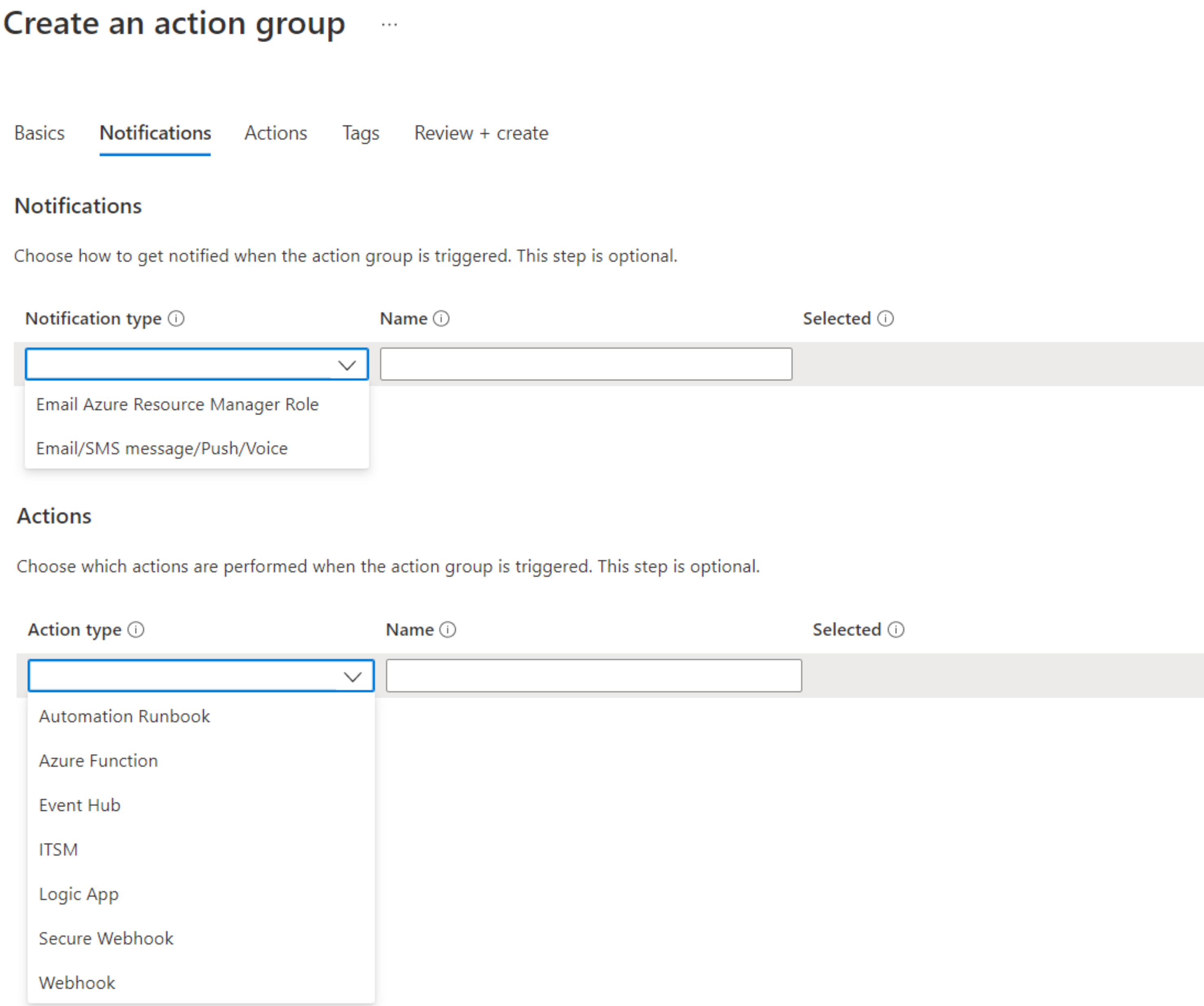
Action Groups

Notification

- Email Azure Resource Manager Role (Owner/ Contributor/ Reader/ Monitoring Contributor/ Monitoring Reader)
- Email/ SMS/ Push/ Voice

Actions

- Automation Runbook
- Azure Function
- Event Hub
- ITSM
- Logic App
- Secure Webhook
- Webhook



Create an action group ···

Basics | Notifications | Actions | Tags | Review + create

Notifications

Choose how to get notified when the action group is triggered. This step is optional.

Notification type ⓘ	Name ⓘ	Selected ⓘ
∨		

Email Azure Resource Manager Role
Email/SMS message/Push/Voice

Actions

Choose which actions are performed when the action group is triggered. This step is optional.

Action type ⓘ	Name ⓘ	Selected ⓘ
∨		

Automation Runbook
Azure Function
Event Hub
ITSM
Logic App
Secure Webhook
Webhook

Log Analytics

Log Analytics

Data collection

Data generated from resources in cloud and on-premises can be collected to Azure Log Analytics workspace.

Reporting and visualization

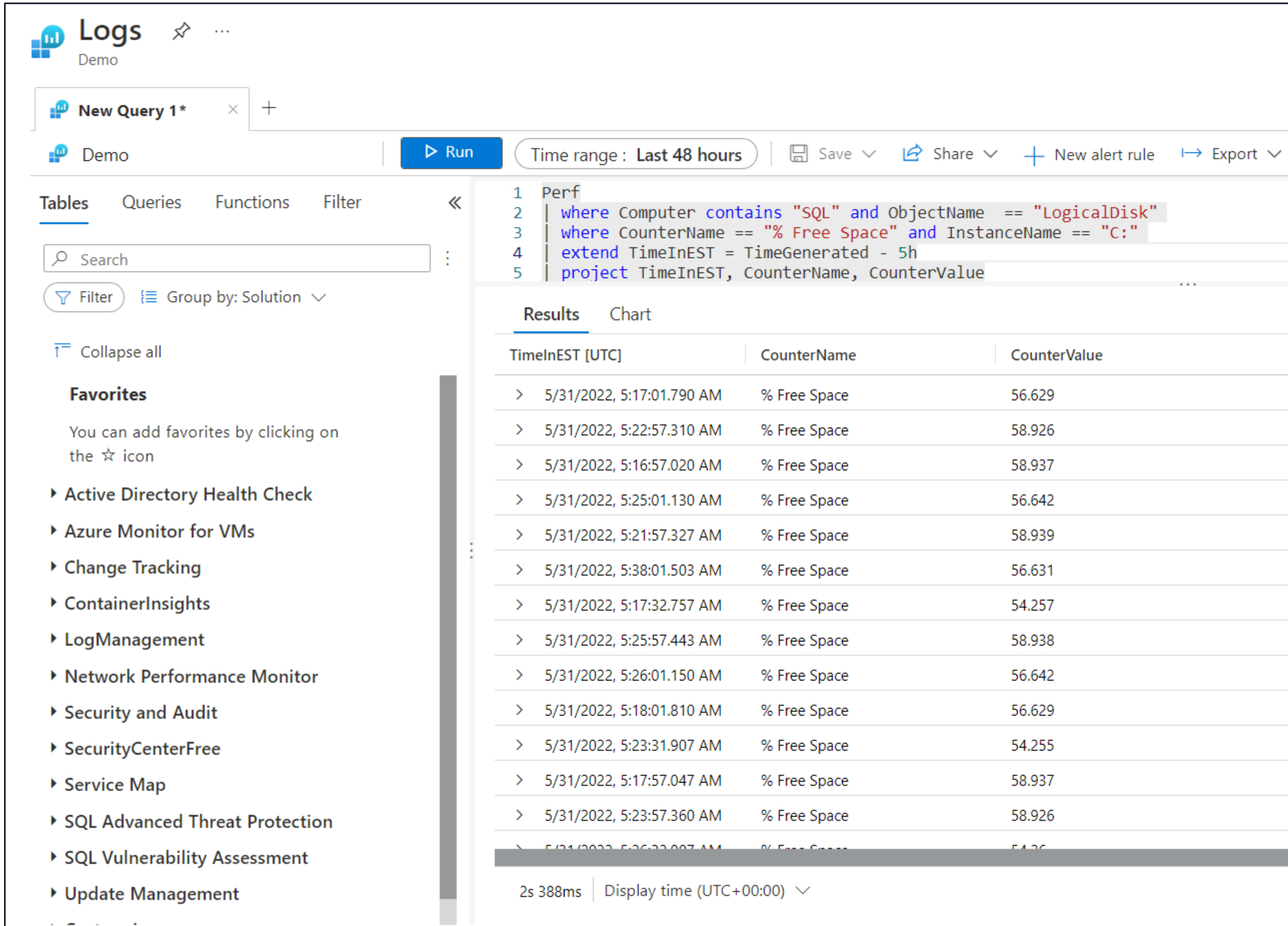
Use KQL to create rich reports and visualization

Workspace

A workspace should be created for data ingestion. You can create one or more workspaces in different regions as per your requirement.

Pricing

Cost is for data ingestion (GB) and data retention (days). Log Analytics offers 30 days of cost-free data retention.



```
Perf
| where Computer contains "SQL" and ObjectName  == "LogicalDisk"
| where CounterName == "% Free Space" and InstanceName == "C:"
| extend TimeInEST = TimeGenerated - 5h
| project TimeInEST, CounterName, CounterValue
```

TimeInEST [UTC]	CounterName	CounterValue
5/31/2022, 5:17:01.790 AM	% Free Space	56.629
5/31/2022, 5:22:57.310 AM	% Free Space	58.926
5/31/2022, 5:16:57.020 AM	% Free Space	58.937
5/31/2022, 5:25:01.130 AM	% Free Space	56.642
5/31/2022, 5:21:57.327 AM	% Free Space	58.939
5/31/2022, 5:38:01.503 AM	% Free Space	56.631
5/31/2022, 5:17:32.757 AM	% Free Space	54.257
5/31/2022, 5:25:57.443 AM	% Free Space	58.938
5/31/2022, 5:26:01.150 AM	% Free Space	56.642
5/31/2022, 5:18:01.810 AM	% Free Space	56.629
5/31/2022, 5:23:31.907 AM	% Free Space	54.255
5/31/2022, 5:17:57.047 AM	% Free Space	58.937
5/31/2022, 5:23:57.360 AM	% Free Space	58.926

2s 388ms | Display time (UTC+00:00)

Log Analytics Workspace

Workspace

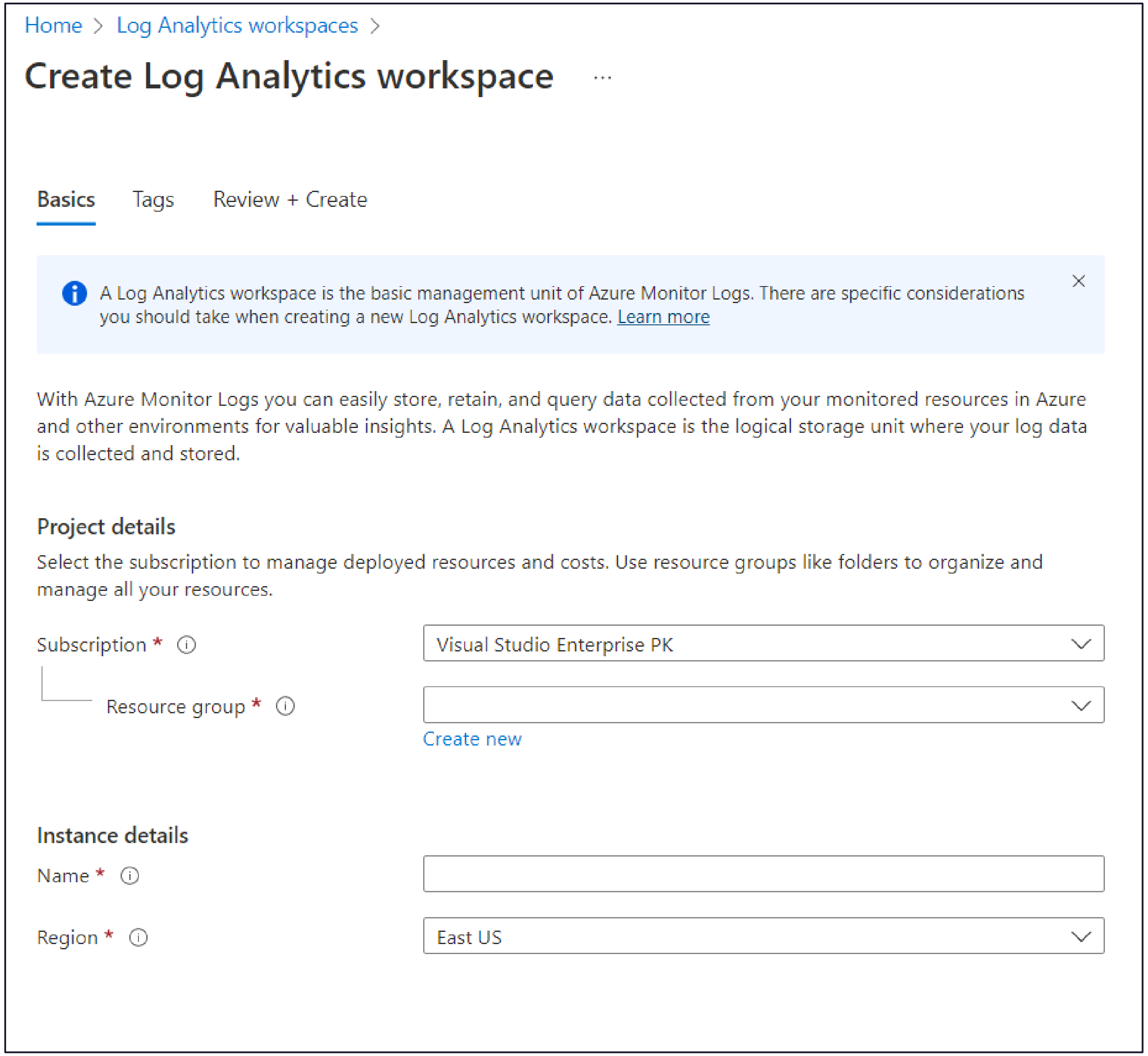
Resource created in Azure to collect, analyze, aggregate, and visualize the data from onboarded resources.

Data isolation

You can create workspaces in different regions to meet compliance and data residency requirements.

Stores Insights and Sentinel data

Data ingested by other services like Application Insights and Sentinel use Log Analytics Workspace to store data.



Home > Log Analytics workspaces >

Create Log Analytics workspace ...

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Visual Studio Enterprise PK

Resource group * :

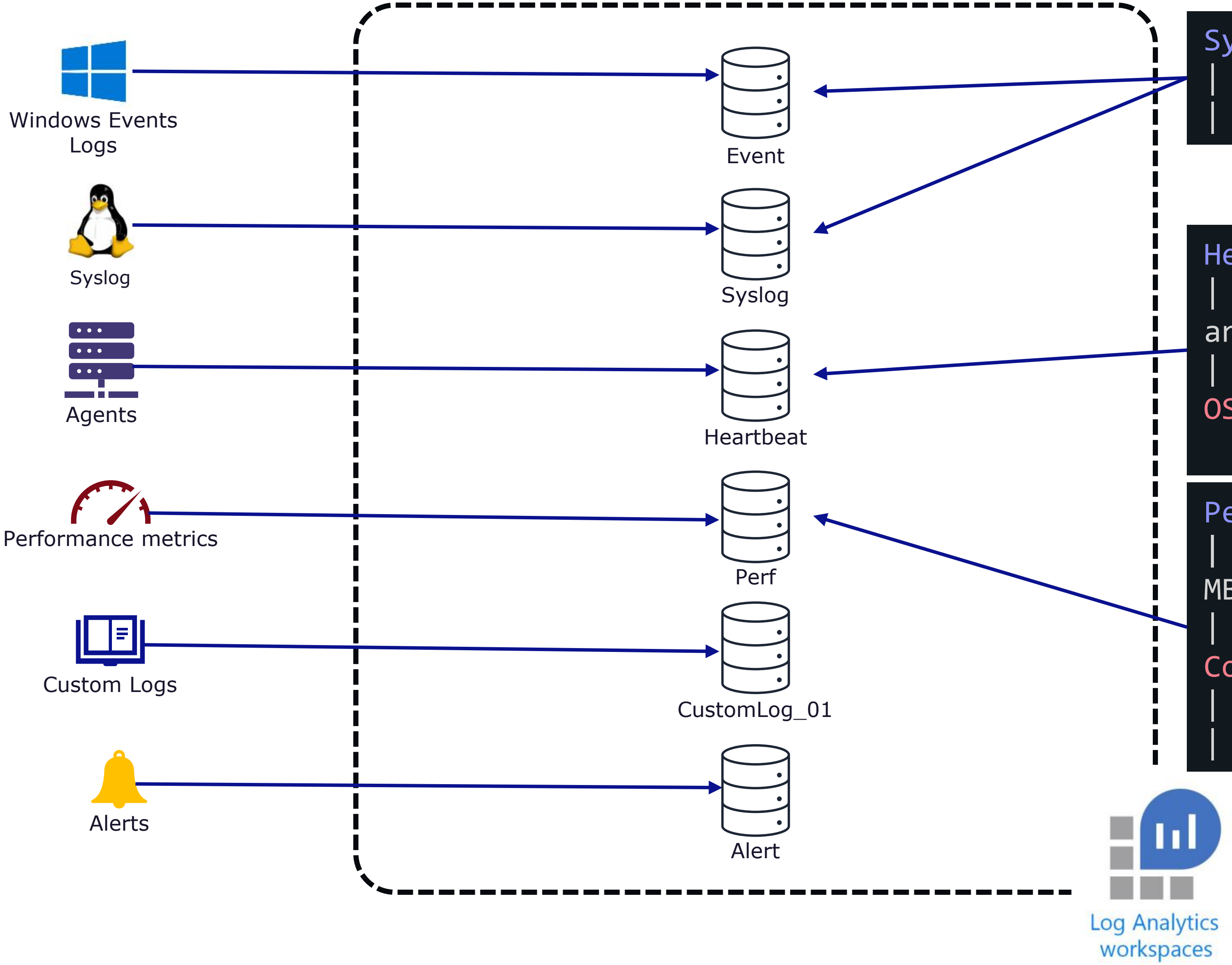
Create new

Instance details

Name * :

Region * : East US

Querying Log Analytics Workspace

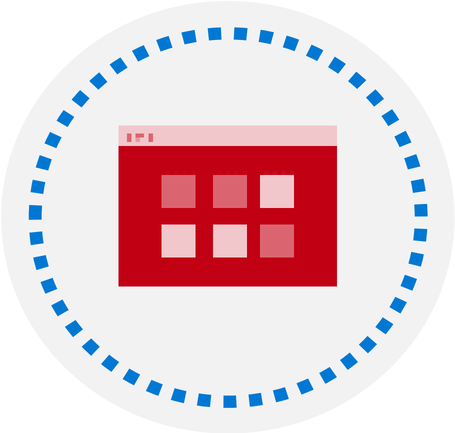


```
Syslog
| union Event
| where SeverityLevel == “Error”
```

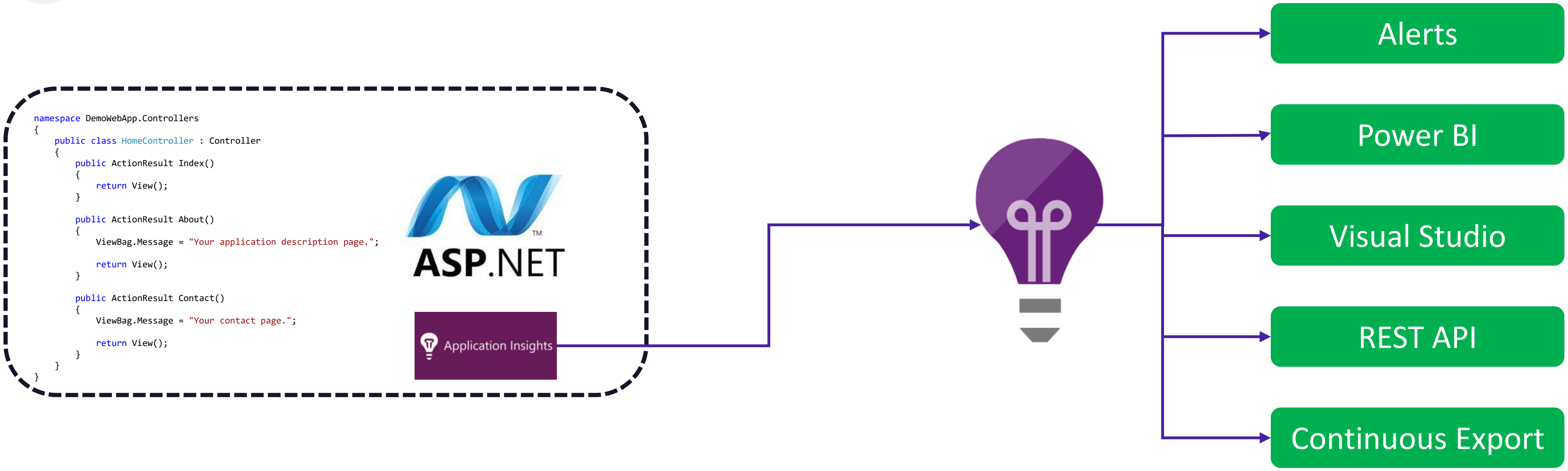
```
Heartbeat
| where ComputerIP startswith "52"
and Computer startswith "DC"
| where OSType == "Windows" and
OSName contains "2016"
```

```
Perf
| where CounterName == "Available
MBytes" and Computer == "JBOX00"
| project TimeGenerated,
CounterValue
| sort by TimeGenerated asc
| render timechart
```

Application Insights



Application Insights



```
namespace DemoWebApp.Controllers
{
    public class HomeController : Controller
    {
        public ActionResult Index()
        {
            return View();
        }

        public ActionResult About()
        {
            ViewBag.Message = "Your application description page.";

            return View();
        }

        public ActionResult Contact()
        {
            ViewBag.Message = "Your contact page.";

            return View();
        }
    }
}
```

Continuous Monitoring

Ability to monitor failures and unavailability of our applications continuously.

Availability test

Ability to perform availability test from different geographic regions to observe latency and performance.

Supports Azure and non-Azure applications

We can install the instrumentation package on Azure and non-Azure environment to monitor our applications.

KODEKLOUD