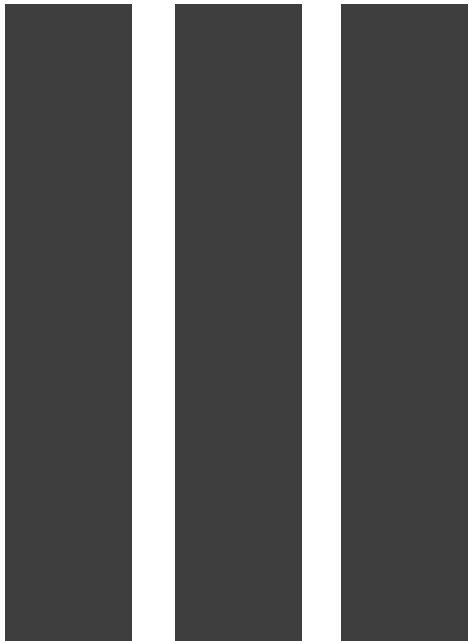
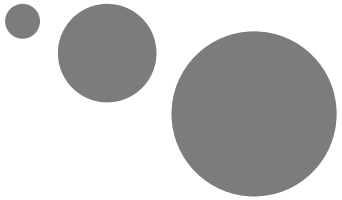
KodeKloud

Module 1: Design for authentication and authorization





Scenario

Vendetta Corp would like to use Azure AD as their identity and access management solution, and they have the following requirements:

- Should be able to collaborate with their external partners without the need to manage username and passwords in their environment
- Their app users should be able to access their e-commerce website using Apple, Google, and Microsoft email IDs
- Access to their corporate apps should be limited to 52.11.11.0/27 network
- Any users access their corporate apps outside the corporate network requires MFA
- They should be able to tackle leaked passwords and compromised accounts trying to access their environment
- All administrators should get a weekly report with the list of role assignments for them to review and verify if the access needs to be persisted.
- They have several HTTPS applications which requires to store SSL certificate, suggest a certificate store for them.
- Several apps uses SQL database as the backend datastore, as of now the credentials are stored in code in an encrypted form. Suggest a better way to store credentials and access the SQL database securely without exposing any keys.

Design for identity and access management

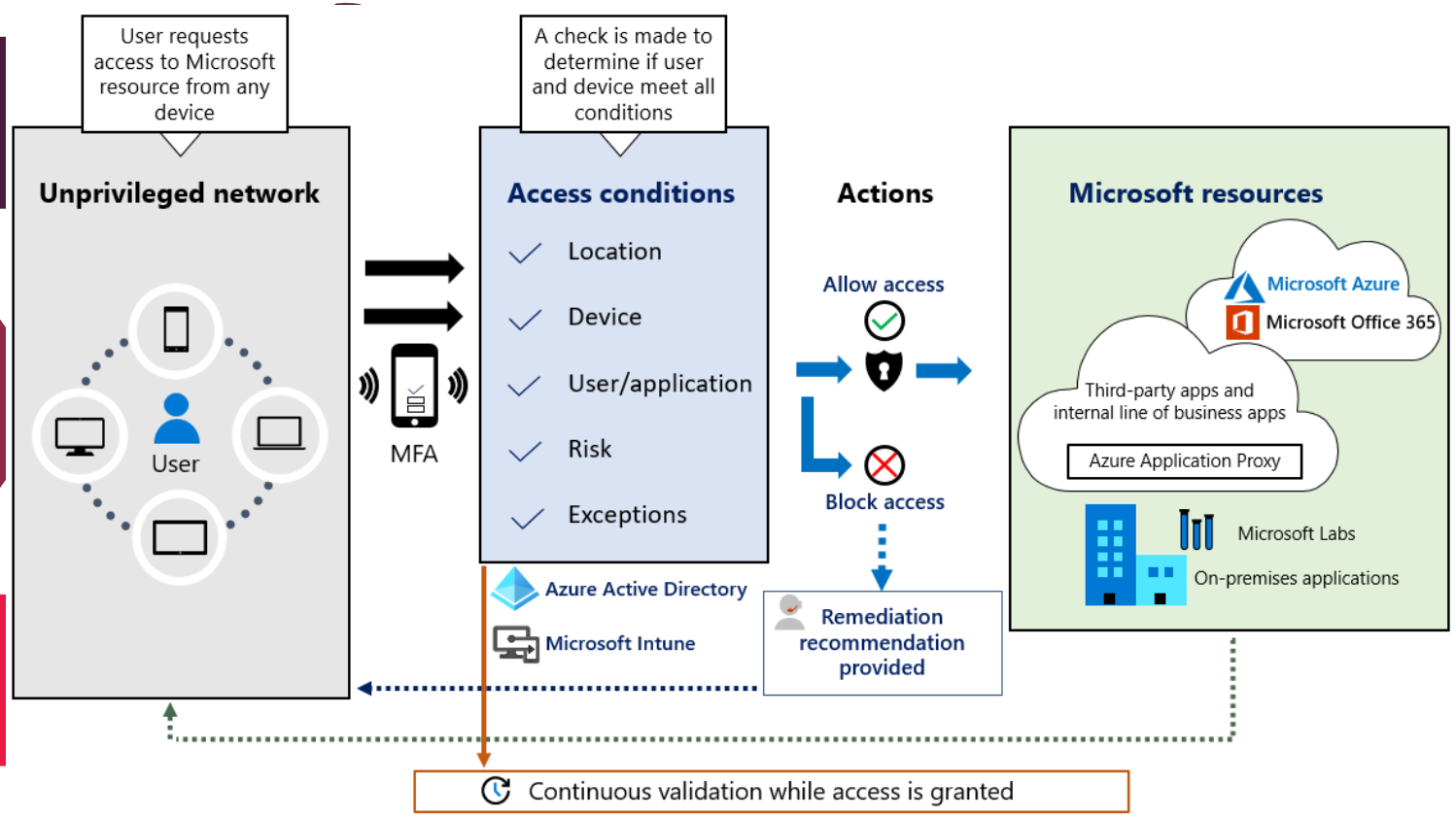
Embrace the Zero Trust Model

Never trust, always verify

Verify explicitly

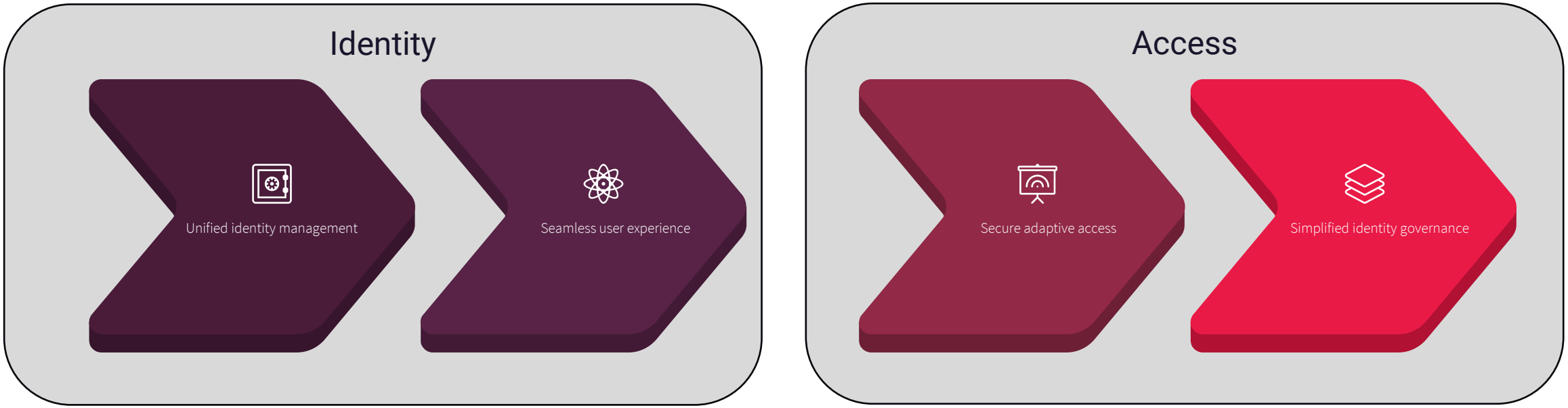
Use least privilege access

Assume breach



Design for identity and access management

Learn how to design an IAM solution as an architect



Unified identity management

Centralized management for all your users, groups, devices and other identities regardless of their location.

Seamless user experience

Seamless, easy and fast user experience while signing in and resetting password

Secure adaptive access

Adaptive policies to secure resources and data using string authentication.

Simplified identity governance

Access management to resources.

Design for identity and access management

Learn how to design an IAM solution as an architect

Scenario

01

You need to provide identity and access management for your employees or on-premises users

Azure AD

Scenario

02

You need to collaborate with external users or guests like partners, vendors etc.

Azure AD B2B

Scenario

03

You need control how you customers can sign in and access your applications.

Azure AD B2C

Design for Azure Active Directory

Design for Azure Active Directory

Learn why should you use Azure Active Directory

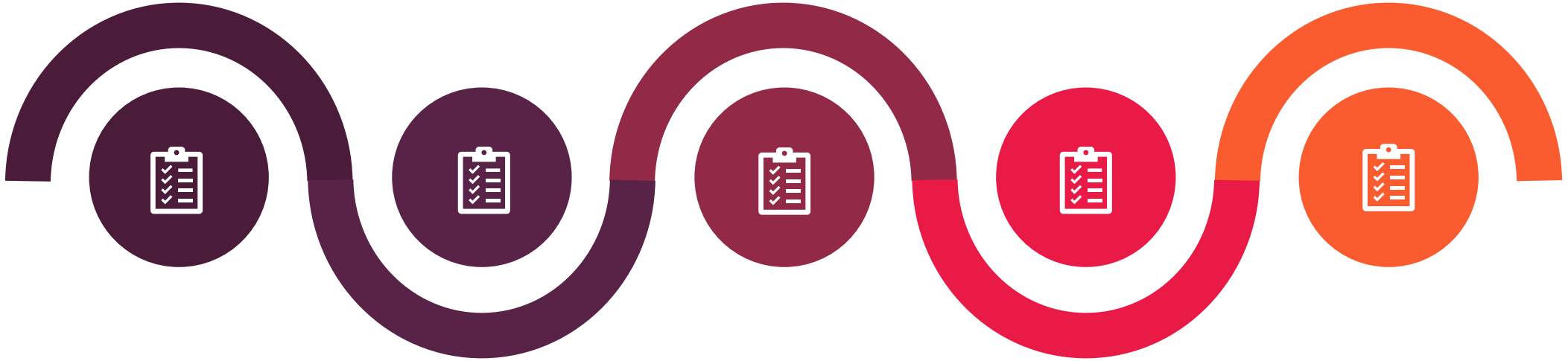
- Cloud only users
- Guest users (B2B)
- Directory synchronized users

Why Azure AD?

- A multitenant, cloud based, centralized identity access management solution.
- Directory services, identity access management, application access management , and identity protection under a single roof.
- If you have an existing Active Directory, you can synchronize that with Azure AD and have hybrid identities.

Best practices for Azure AD

Keep these best practices in mind while you design a solution with Azure AD.



Have a centralized management

If you have a hybrid scenario, it's better you synchronize identities to the cloud and have a single centralized management.

Single tenant approach

Though you can have multiple tenants for your organization, it's recommended that you follow a single tenant approach to avoid complexity.

Don't sync AD privileged accounts

By default, Azure AD connect makes sure that privileged accounts in AD are not synced to Azure AD.

Turn on Password Hash Synchronization

Enable PHS for hybrid identities avoid leaked credentials from being replayed.

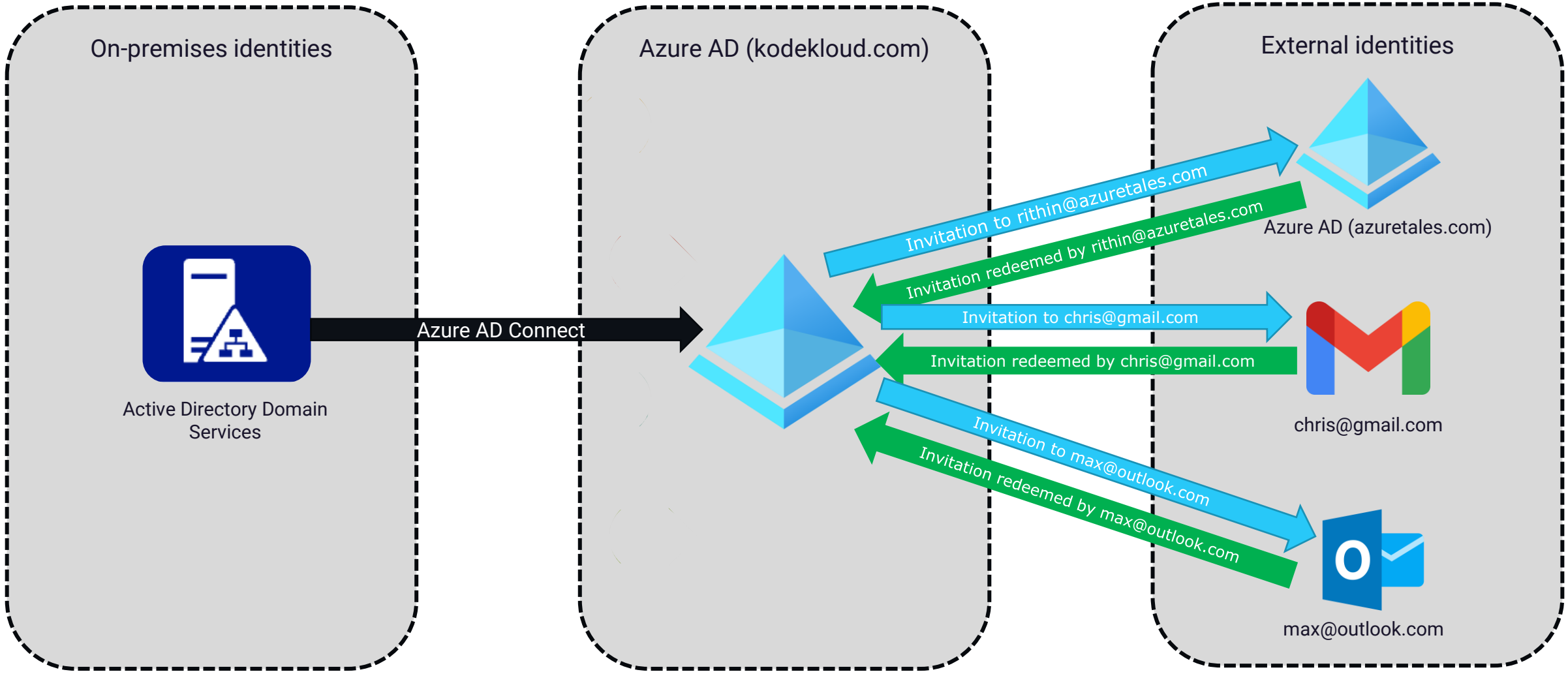
Enable SSO

With SSO, users can sign in without the need for entering the password multiple times

Design for Azure AD B2B

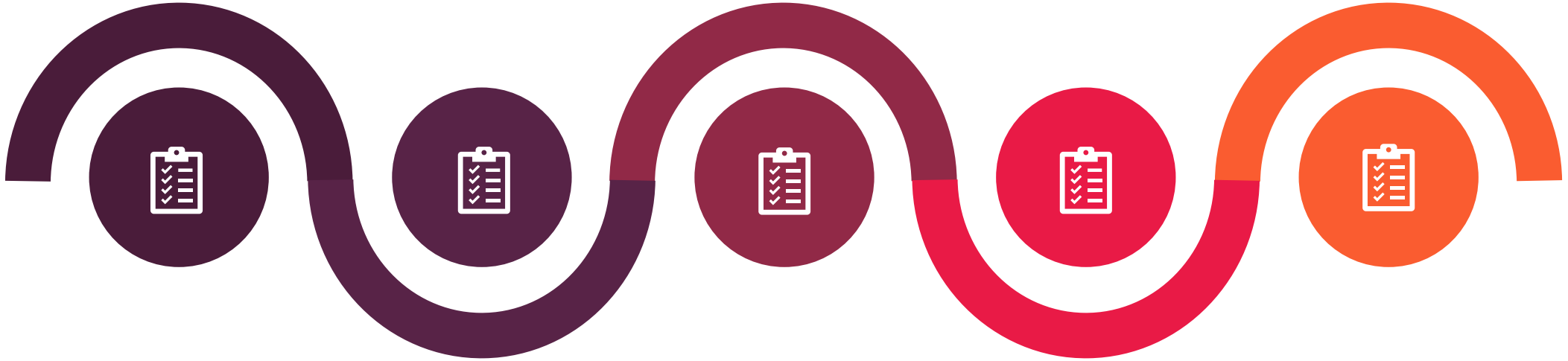
Design for Azure AD B2B

Collaborate with external partners using Azure AD B2B



Best practices for Azure AD B2B

Keep these best practices in mind while you design a solution with Azure AD.



Let application owners manage guest users

Application owners can decide which external users should be given access to the applications.

Use Conditional Access

Make use of conditional access to make decisions on authentication.

Leverage MFA

Combine Conditional Access and let the users sign in MFA only.

Integrate with third-party identity providers

Integrate Azure AD with Facebook, Microsoft, and Facebook accounts which will let the user sign in with their social accounts.

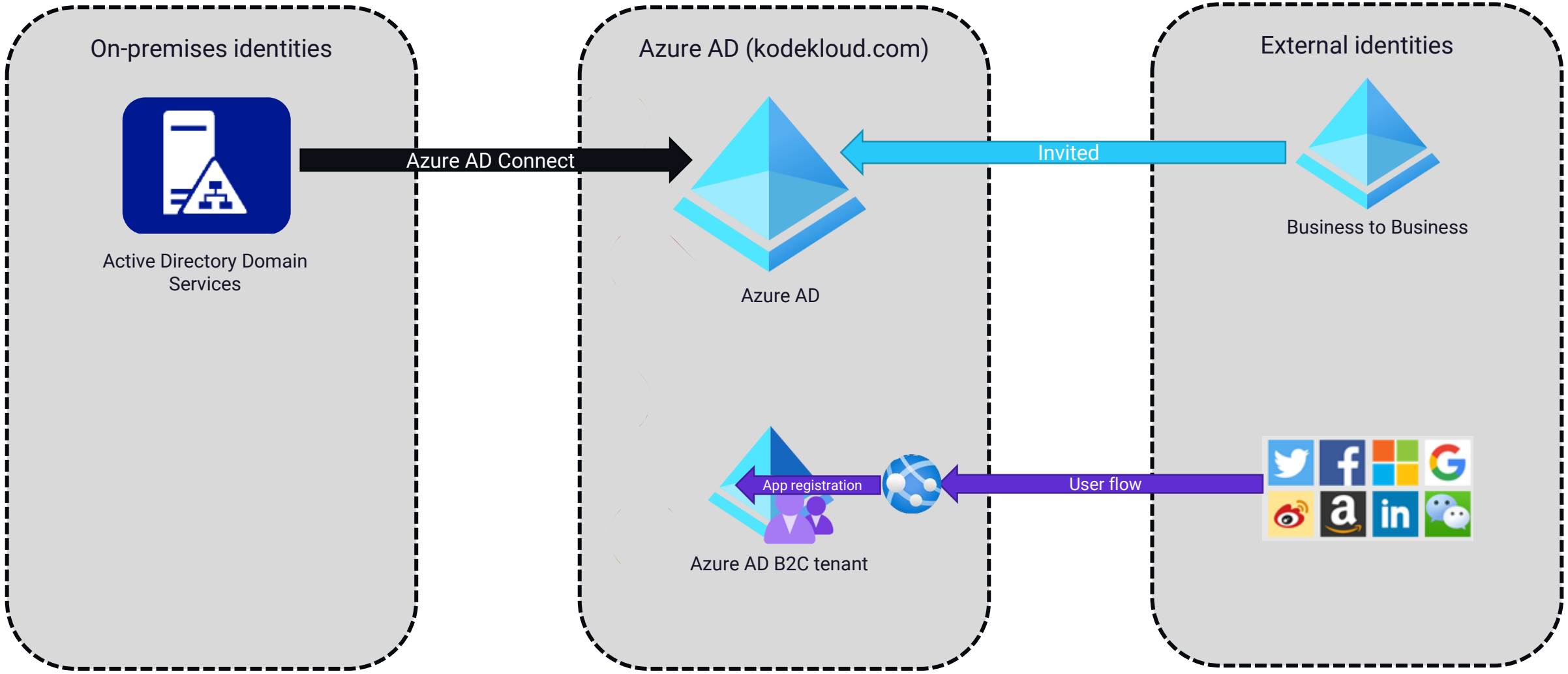
Self-service sign-up user flow

Enable self-service sign-up workflow for your users.

Design for Azure AD B2C

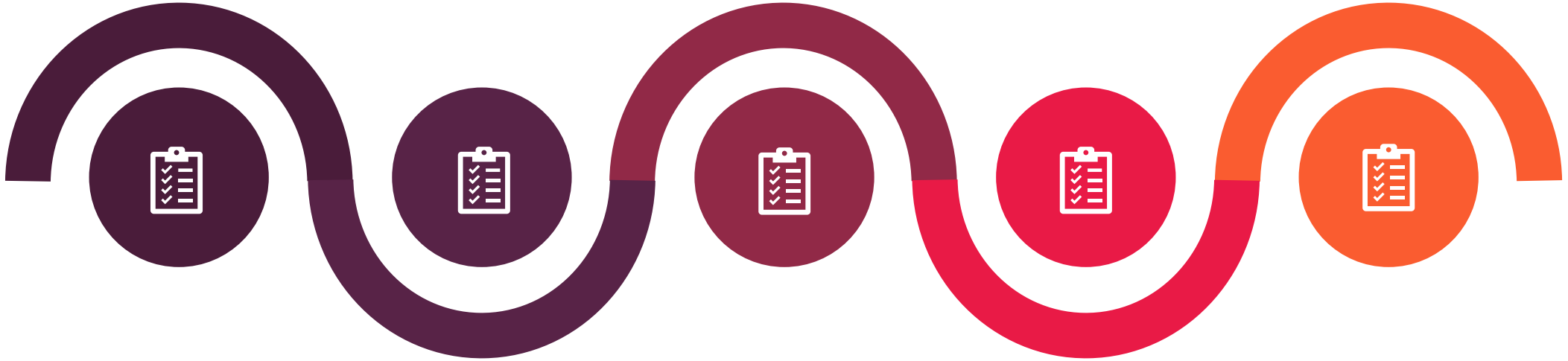
Design for Azure AD B2C

IAM solution to manage your customers



Best practices for Azure AD B2C

Keep these best practices in mind while you design a solution with Azure AD B2C.



Create user flows

Create user flows to manage how your users are signing in.

Choose your IdPs

B2C supports a plethora of identity providers like Amazon, Facebook, Google, Microsoft etc.

Customize user experience

Design your own HTML and CSS templates building your branding or use built-in templates.

Additional attributes and external data sources

You can add 100 custom attributes for your customers and this can be connected to external data sources such as CRM.

Third party verification

You can send the data to third party validation systems for verification.

Comparison between B2B and B2C

Keep these best practices in mind while you design a solution with Azure AD.

- Contains users that belong to the organization, users that are synchronized from on-premises and external users who are invited for collaboration.
- Users are managed using invitation, access review, RBAC etc.
- Users invited can interact with users that are already part of the directory
- Guest users are managed in the same directory as the employees of the organization.
- Organization branding can be done

VS

COMPARISON

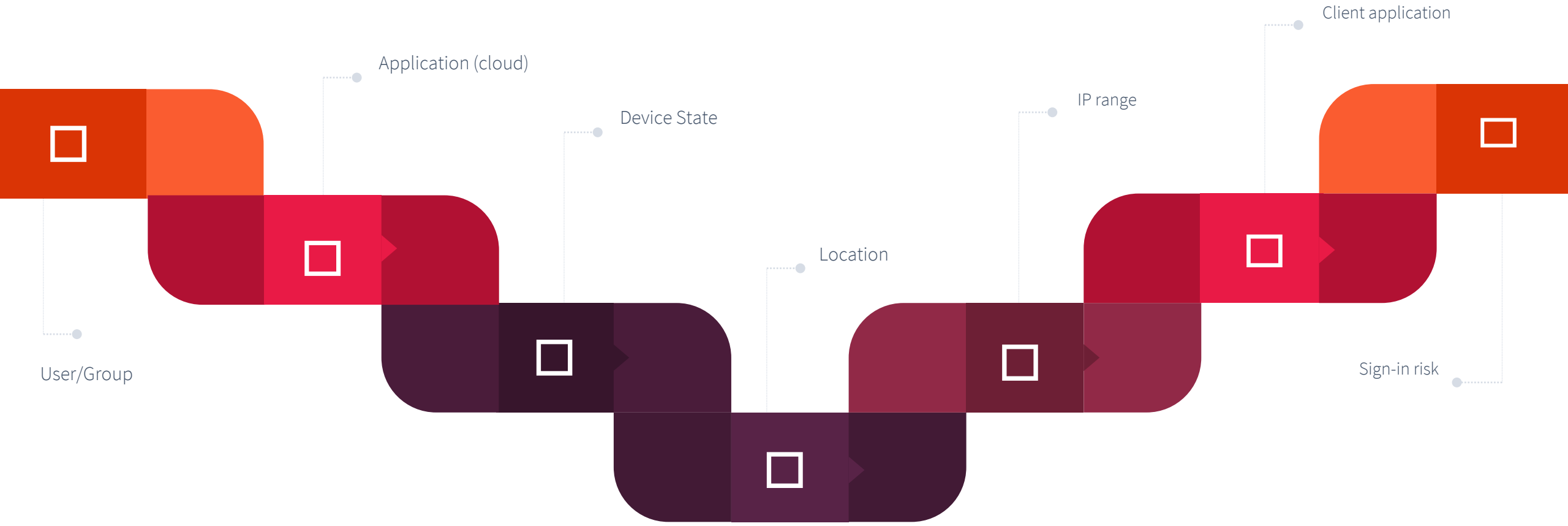
- Customers of your application. These users are managed separately in a B2C tenant. It's is not related to your B2B tenant.
- Users manage their own profiles
- Customers are not visible to other customers
  .
- These users cannot interact with the employees and is managed in separate tenant.
- Fully customizable

Design for Conditional Access

KodeKloud

Conditional Access

Make decision on how users should sign in based on signals.



Allow access

Enforce MFA

Block access

Conditional Access – Best practices

Following are the recommended conditional access policies

Use to enable MFA

Enforce users to use MFA if they are signing in from an unknown location or IP address

Require managed devices

Enforce users to use their organization managed devices to access corporate data and applications

Access only approved client apps

Provide access to certain apps only. Useful when you are managing personal devices of users and want to control the exposure of data.

Exclude countries

Exclude sign in from countries from which you are never expecting a sign in.

Respond to compromised accounts

Combining three policies: Require MFA, Require password change if user is high-risk, and require MFA for medium or high-risk users.

Completely block access

You can block complete access to an application with the help of this policies

Conditional Access – Best practices

Following are the recommended best practices related to conditional access policies

Block legacy authentication protocols

Older protocols are exploited by attackers, ensure that the legacy authentication is blocked.

Use What-if tool

With the help of What-if tool, you can verify the effect of policy. This will help you to plan and troubleshoot policies

Test using “Report-only” mode

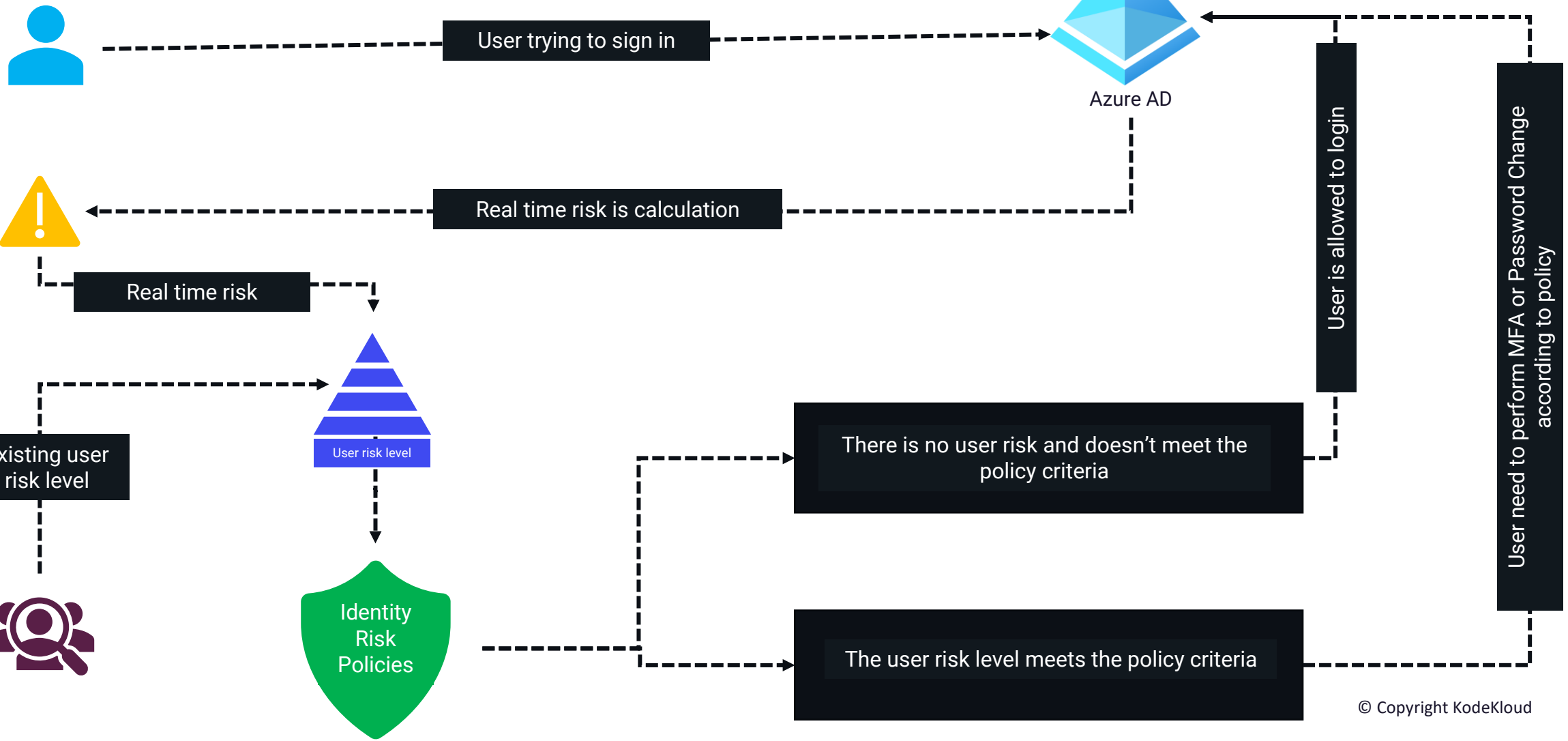
With the help of report-only, the policy will only report if the conditions are matched. This is good for monitoring the policy before you implement it.

Design for Identity Protection

KodeKloud

Azure Identity Protection

Detect and remediate identity-based risks



Identity Protection– Best practices

Following are the recommended while using Identity Protection

Acquire licenses

Identity Protection requires Premium P2 license

Set-up policies

Make sure you setup the policies and is actively reviewing the results

Self-remediation

Set the sign-in risk policy to Medium and above, and ensure that you allow self-remediation options

User risk policy

High is recommended threshold for user risk policy

Exclude users

Make sure you exclude emergency or break glass accounts from the policies

Integration

Send your data from Identity Protection to Conditional Access or SIEM solutions.

Design for access reviews

Access Reviews

Review the current role assignments or memberships and verify if they are needed

Notify resource owners

An email will be triggered to users and resource owners with the list of current role assignments.

Review assignments

Resources owners will be reviewing the current assignments or memberships to verify if they are needed or not

Purge

Remove the stale assignments or memberships that are no longer need. Then the report will be sent to the administrator .

Retention

Resource owners will choose the assignments or memberships they would like to keep

Access Reviews – Best practices

Following are the recommended while using access reviews

Acquire licenses

Identity Protection requires Premium P2 license

Understand the purpose

Purpose of access reviews is to protect, monitor and audit access to your resources.

Decide the reviewers

You can set the reviewers as resource owners, or you can add delegated reviewers.

Decide the self-attest process

Determine which users can self-attest their access to continue accessing the resources.

Decide the resource types

Determine which resources needs to reviewed using access reviews

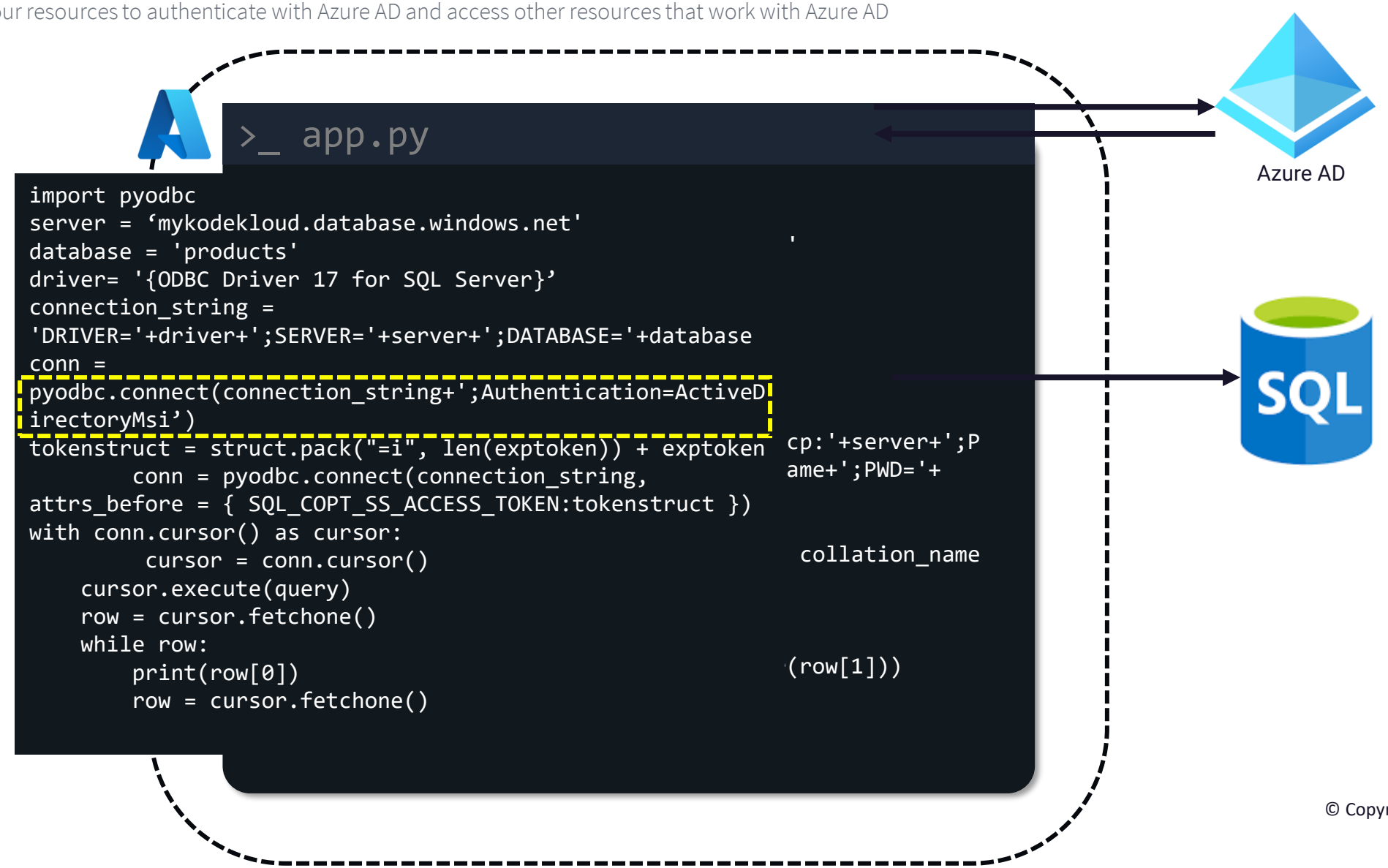
Setup a review plan

Produce a plan which includes the list of reviewers, resources you want to review, frequency of review, remediation plan etc.

Design for managed identities

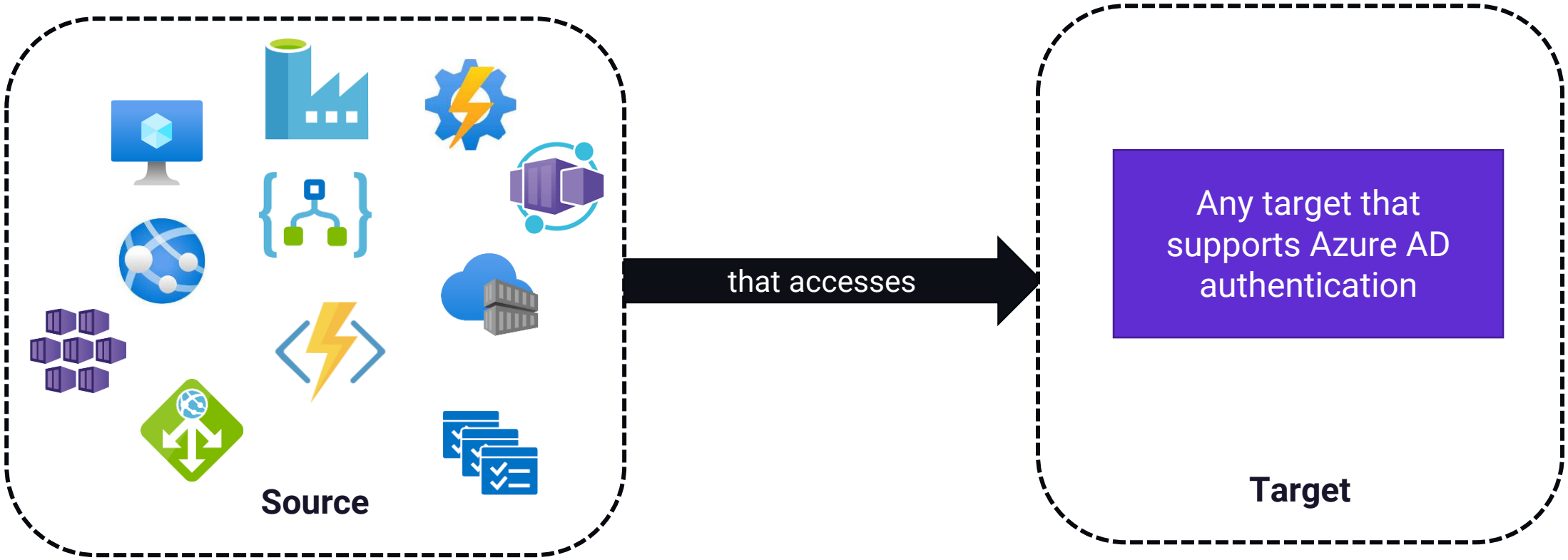
Managed identities

Enable your resources to authenticate with Azure AD and access other resources that work with Azure AD

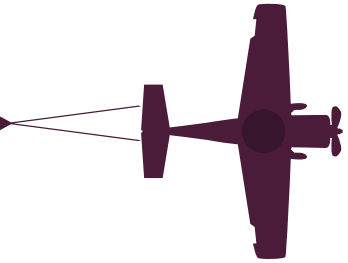


Managed identities

Enable your resources to authenticate with Azure AD and access other resources that work with Azure AD



- Source should be in Azure, and target can be any anything that supports Azure AD and Azure RBAC
- No need to perform credential rotation or certificate management
- No need to store keys in your code



Managed Identities

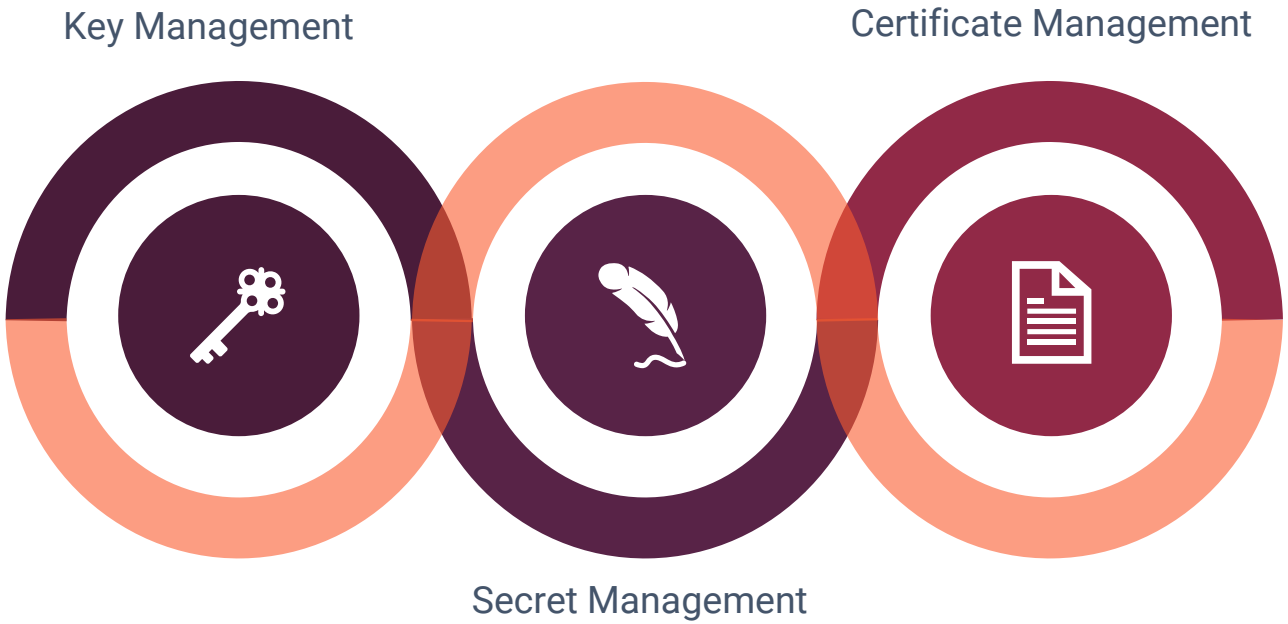
System-assigned managed identity and User-assigned managed identity

Property	System-assigned managed identity	User-assigned managed identity
Alignment	Represents identity of a resource in Azure	Created as a standalone resource in Azure and can be mapped to multiple resources
Lifecycle	Mapped to the resource for which the identity is created	Independent resource in Azure and is not mapped to lifecycle of resource
Sharing	Cannot be shared with other resources (1:1)	Can be shared with multiple resources (1: Many)
Use cases	• Ideal for workloads that are deployed in a single resource • Workloads that require independent identity	• Ideal for workloads that run on multiple instances • Workloads that requires a common identity

Design for Azure Key Vault

Design for Azure Key Vault

Secure storage for keys, secrets, and certificates that are used by your application



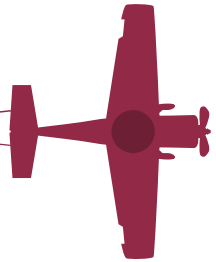
KodeKloud

Why use Azure Key Vault?

Learn why should you use Azure Key Vault for storing credentials

- Separate sensitive information from your code to avoid credential leak
- Leverage access policies to control access and data operations
- Provides a centralized storage for all your keys, secrets and certificates
- All operations are logged and monitored
- You can generate or import keys or certificates

You can have multiple key vaults if required based on whether you need to have different access policies or to improve performance



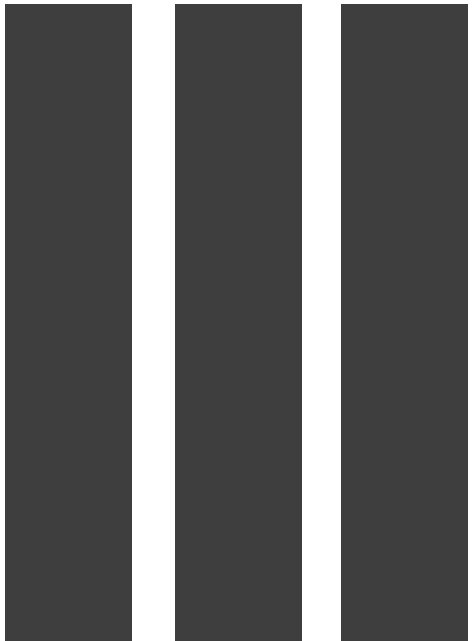
Scenario

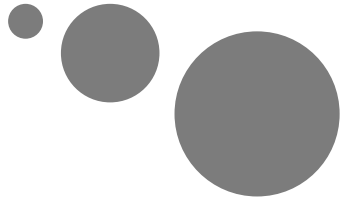
Vendetta Corp would like to use Azure AD as their identity and access management solution, and they have the following requirements:

- Should be able to collaborate with their external partners without the need to manage username and passwords in their environment **Azure AD B2B**
- Their app users should be able to access their e-commerce website using Apple, Google, and Microsoft email IDs **Azure AD B2C**
- Access to their corporate apps should be limited to 52.11.11.0/27 network **Implement CA Policy with IP range**
- Any users access their corporate apps outside the corporate network requires MFA **Implement CA Policy to enforce MFA**
- They should be able to tackle leaked passwords and compromised accounts trying to access their environment **Identity Protection – User Risk Policy**
- All administrators should get a weekly report with the list of role assignments for them to review and verify if the access needs to be persisted. **Access Reviews**
- They have several HTTPS applications which requires to store SSL certificate, suggest a certificate store for them. **AKV**
- Several apps uses SQL database as the backend datastore, as of now the credentials are stored in code in an encrypted form. Suggest a better way to store credentials and access the SQL database securely without exposing any keys. **Use Managed Identities**

KodeKloud

Module 2: Design for governance solution





Scenario

Vendetta Corp would like to implement the following organizational standards:

- Create a hierarchy in Azure with two entities Marketing and HR and host their Production, DR, and Testing environments. There is a separate entity called HUB for hosting shared services used by both Marketing and HR entities. Following subscriptions are there in the environment.

Department	Subscription Name	Environment
Marketing	Marketing_PRD_01	Production
Marketing	Marketing_PRD_02	Production
Marketing	Marketing_STAGE_01	Testing
Marketing	Marketing_DR_01	DR
Marketing	Marketing_DR_02	DR
HR	HR_PRD_01	Production
HR	HR_DR_01	DR
HR	HR_STAGE	Testing
HUB	CENTRAL-HUB	Production
HUB	CENTRAL-HUB-DR	DR

Scenario

Vendetta Corp would like to implement the following organizational standards:

- The organization requires all resources to be deployed in East and West US only regardless of their environment.
- Only VMs in BS, DSv3, DSv4 is allowed in Testing subscriptions
- All production resources should be audited for diagnostic settings
- IT_Helpdesk group users should be able to create Microsoft Support Requests on behalf of any entity in the organization
- IT_Admins group users should e able to manage role assignments and deployments for any subscriptions in the organization
- Marketing_Admins should be to manage their subscriptions and HR_Admins should be able to manage theirs. However, both users should not be able to assign roles. For role assignment they must contact IT_Admins
- All resource groups created in Marketing subscriptions should have tag “Department: Marketing” and that should be inherited to all resources. Similarly for HR with Department as HR.
- Testing should have a template by which they will be able to spin up testing environment where they need two resource groups, role assignments, policy assignments, and Azure resources distributed in the resource groups.

Understanding the hierarchy

Using governance strategies, we can maintain control over the resources we have in Azure

Root Management group is created by default, and

to 6 levels of

ted groups excluding the

Make use of the hierarchy to effectively apply the governance strategies

iption will con

one or more resources groups for logically grouping resources like virtual machines, databases etc.

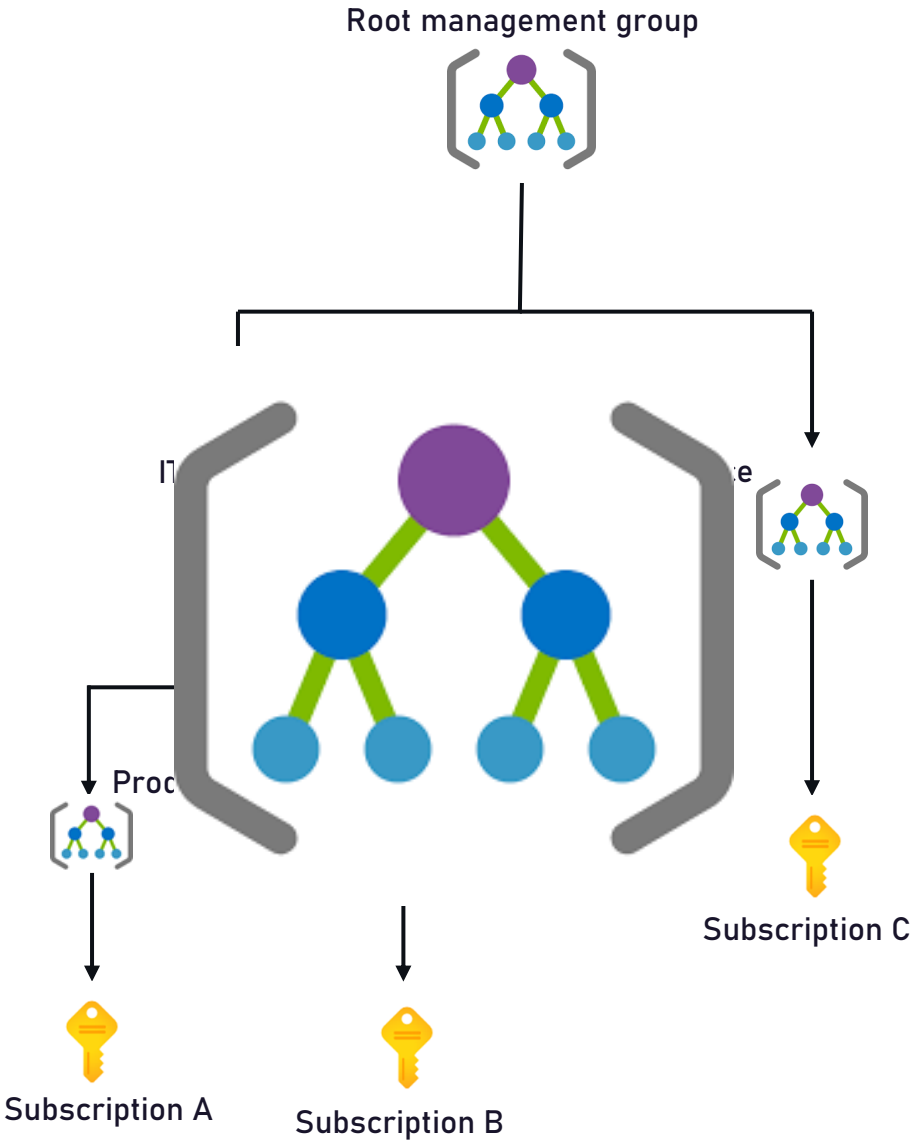
Strategies applied at the higher level will be inherited to the lower levels

Management groups

Subscriptions

Resource groups

Resources



Understanding the hierarchy

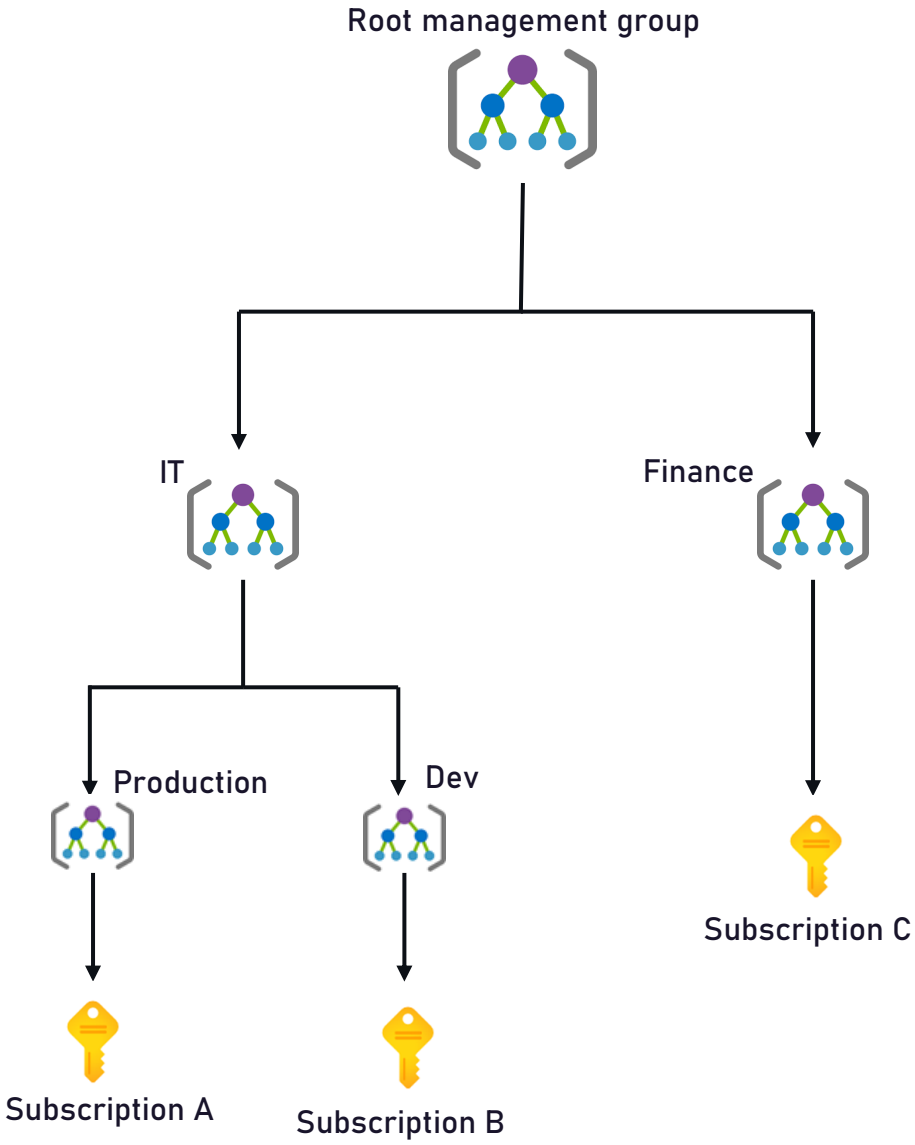
Using governance strategies, we can maintain control over the resources we have in Azure

Root Management group is created by default, and to 6 levels of ted groups excluding the

Make use of the hierarchy to effectively apply the governance strategies

iption will con one or more resources groups for logically grouping resources like virtual machines, databases etc.

Strategies applied at the higher level will be inherited to the lower levels



Design for management groups

KodeKloud

Design for Management Groups

Management groups helps you group your subscriptions together and can be used as a scope to assign roles, policies, and manage compliance

Design a flat hierarchy with governance in mind

Hierarchy with too many levels is not easy to manage and it's better to conclude with no more than four levels. These levels should be designed with governance in mind.

Use the Tenant Root Group as top level and implement a structure

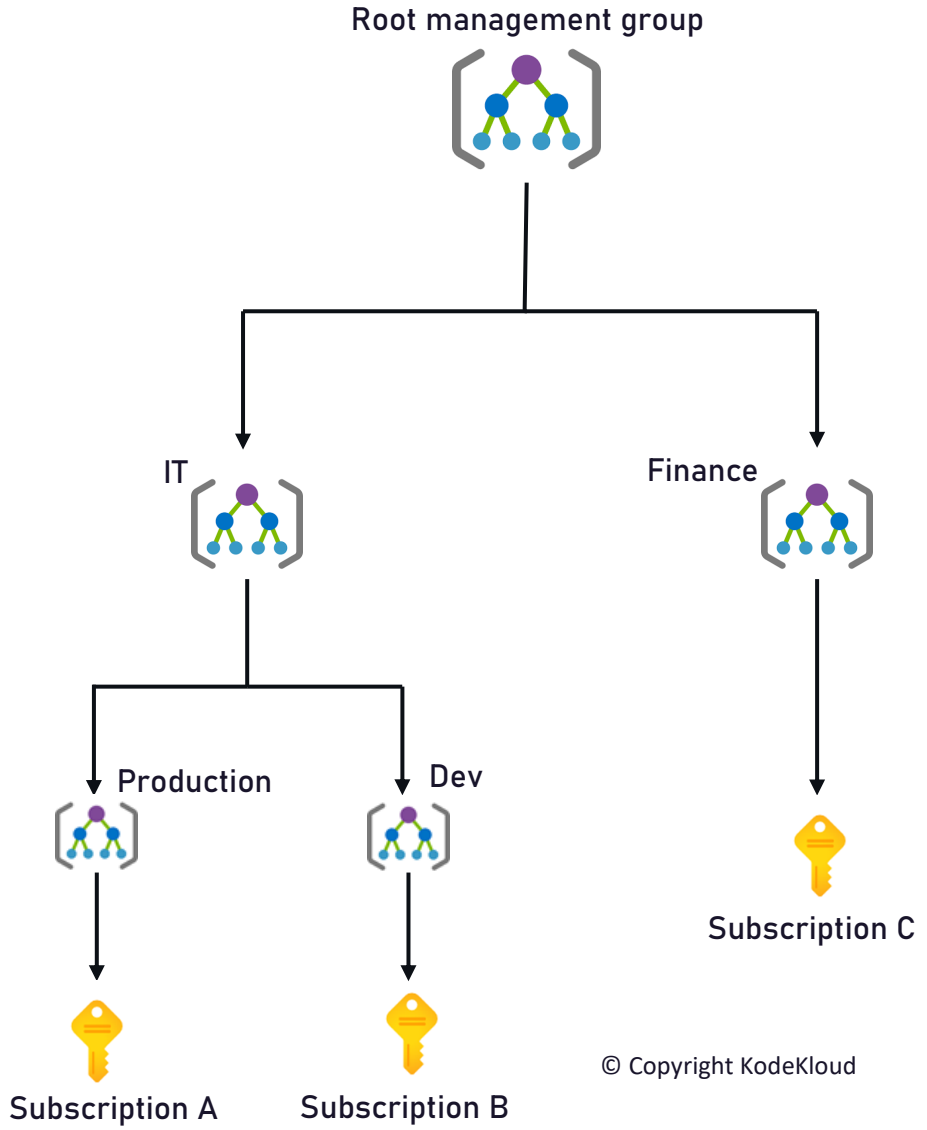
Use organization level policies at the Tenant Root Group and create further levels which represent a business unit or department. Create separate policies for these levels if required.

Use geographic structure with separate group for production

If you are organization has global presence, it's better to create separate management groups representing the geographies (US, EMEA, APAC etc.) this will help you to enforce regional policies for data residency. Furthermore, you should have separate management group representing the production environment.

Use Sandbox management group and separate management group to isolate sensitive data

Sandbox management group can be used to cover your sandbox environment. Similarly, we need to have separate management group to include sensitive corporate data, this will help you to enforce strict policies for data protection and isolation.



Design for subscriptions

Design for subscriptions

Logical container to deploy Azure resources and pay for the deployed resources

Group subscriptions under Management Groups and consider subscription as a democratized unit of management

Group subscriptions based on your criteria to different management groups and align these subscriptions based on your business priorities and needs.

Consider the subscription quota and limits

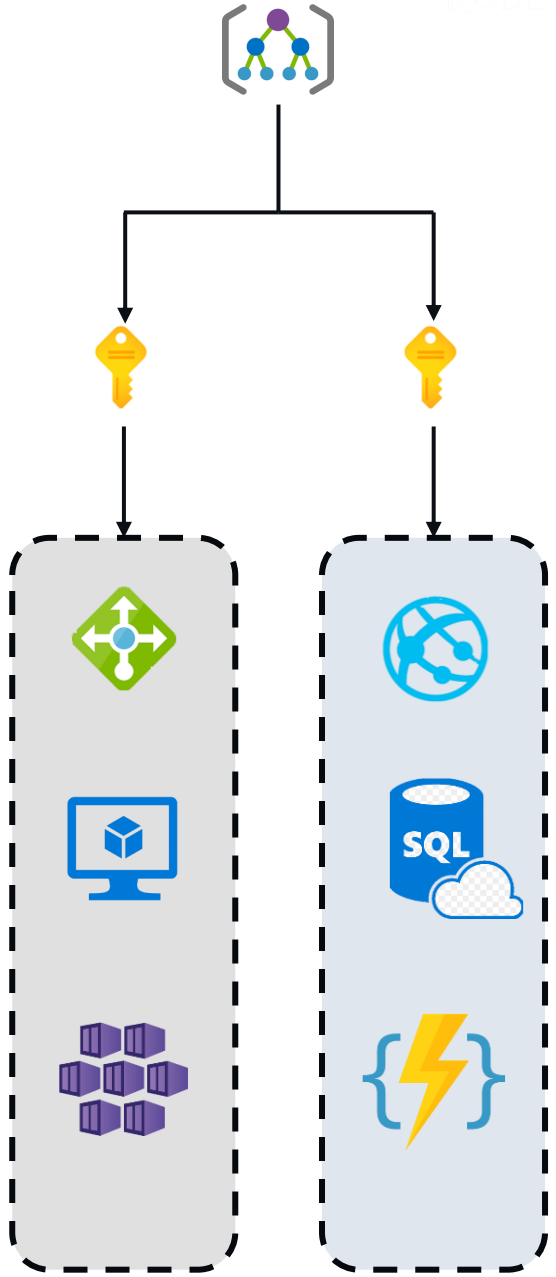
Every subscription has a set of limits defined by Microsoft. Some of these limits are soft limits which can be changed by reaching out to Microsoft support, while others are hard limits.

Consider setting up a subscription to host shared services

Shared services such as firewall, ExpressRoute, VPN gateways, Virtual WAN should be placed in a single subscription. This consideration is further used for the development of Azure Landing Zones.

Consider policy management and access control

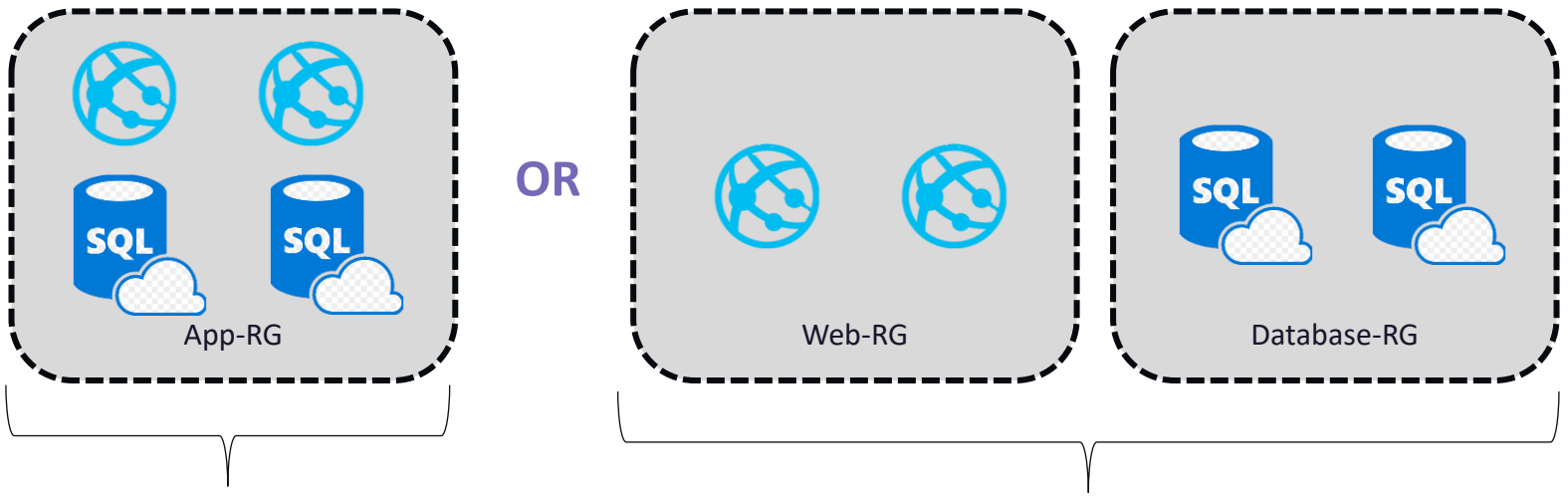
Subscriptions can be used as scope for policy assignment, hence plan how will you will be assigning the policies. Follow the principle of least privilege when assigning roles to users and furthermore leverage Privileged Identity Management



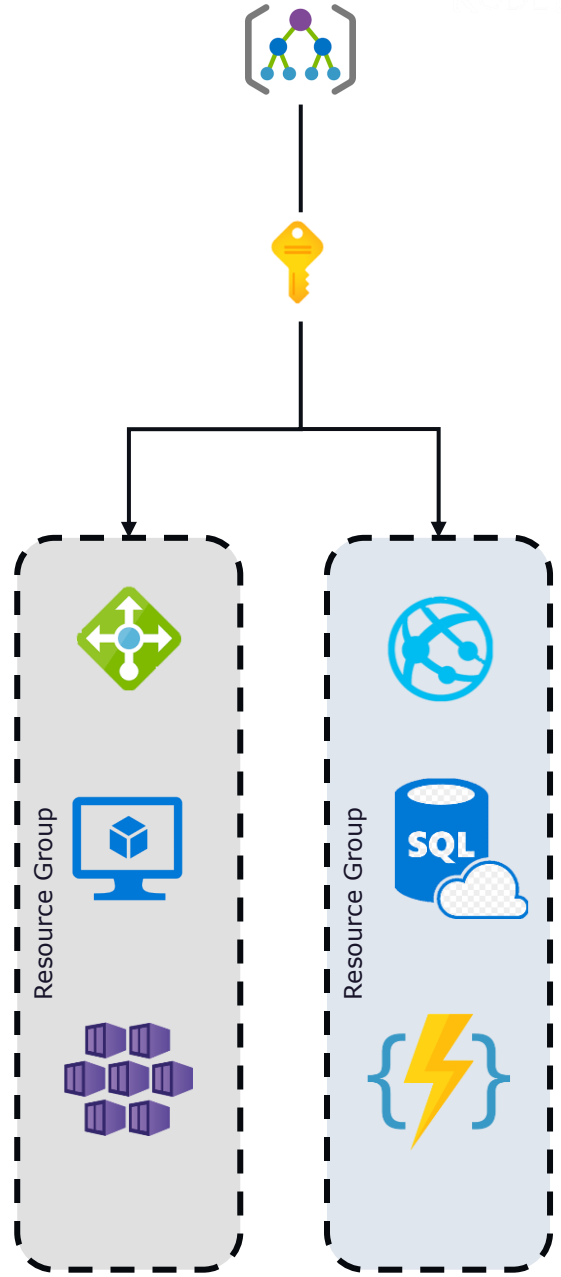
Design for resource groups

Design for resource groups

Logical container within an Azure subscription to group Azure resources



- Group by department or cost center
- Group by region or location
- Group by resource lifecycle
- Consider management overhead
- Consider role-based access controls
- Consider policy and compliance requirements



Design for resource tagging

KodeKloud

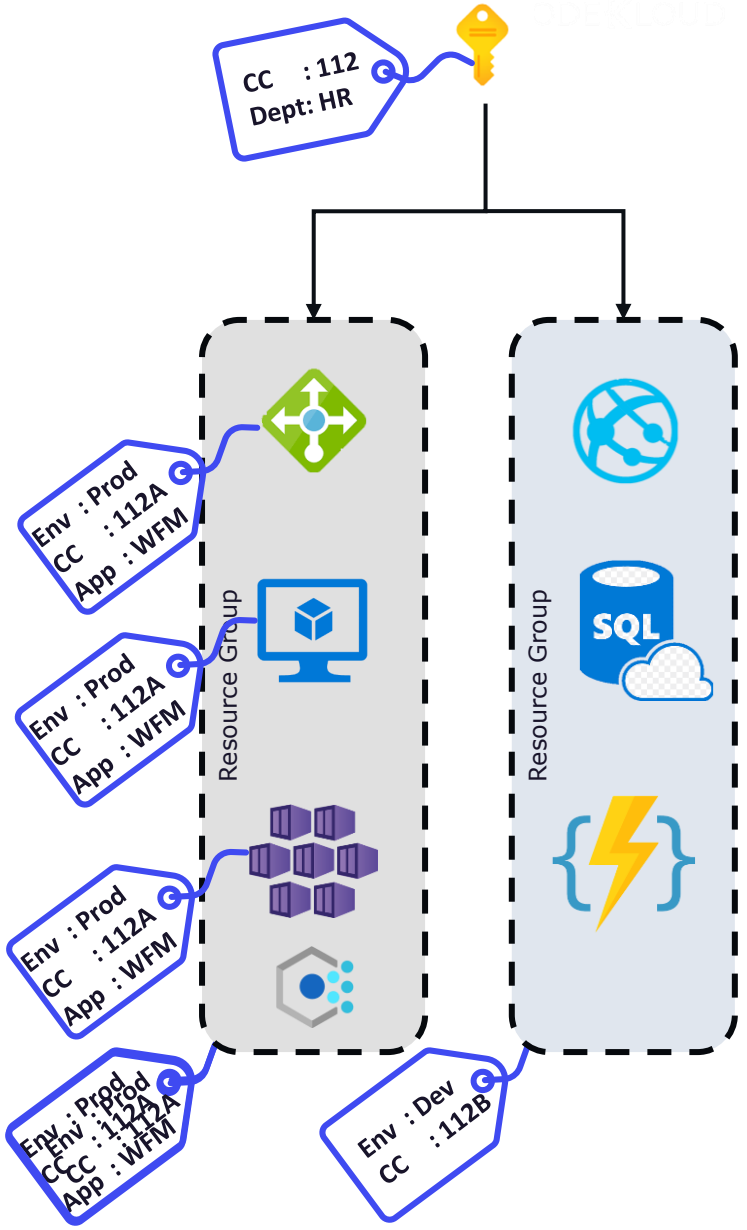
Design for resource tags

Add metadata to your resources to identify or categorize them

- Azure Resource Tags doesn't inherit from the higher level.
- Tags can be applied to subscription, resource group or individual resources
- Tags can be created or modified from Azure Portal, Azure PowerShell, CLI or REST API

- Marketing aligned tag
- Business aligned tags

- Type of tagging required and types of resources you want to tag
- Use Azure policy for tag enforcement



Design for resource tags

Add metadata to your resources to identify or categorize them

Type	Type definition	Examples
Functional	Grouped based on the application role, functionalities, and tiers	App : Payroll Tier : 0 Webserver : IIS Env : Staging
Classification	Confidentiality labels and criticality	Label: Internal SLA : 5h30m
Billing	Grouped based on accounting requirements	Dept : HR CC : 11A Region : WEU
Ownership	Ownership and contact details	Owner: Mark OwnerEmail : mark@xyz.com
Purpose	Impact and business alignment details	Process : HRPortal BusinessImpact : Low RevenueImpact : Low

Design for policy and role-based access control

KodeKloud

Design for policy

Enforcing organizational standards and compliance

Define Management level policies

Apply policy at the highest scope

Applying policy at a higher level will help inheriting the policies to lower levels without any management overhead.

Remediation

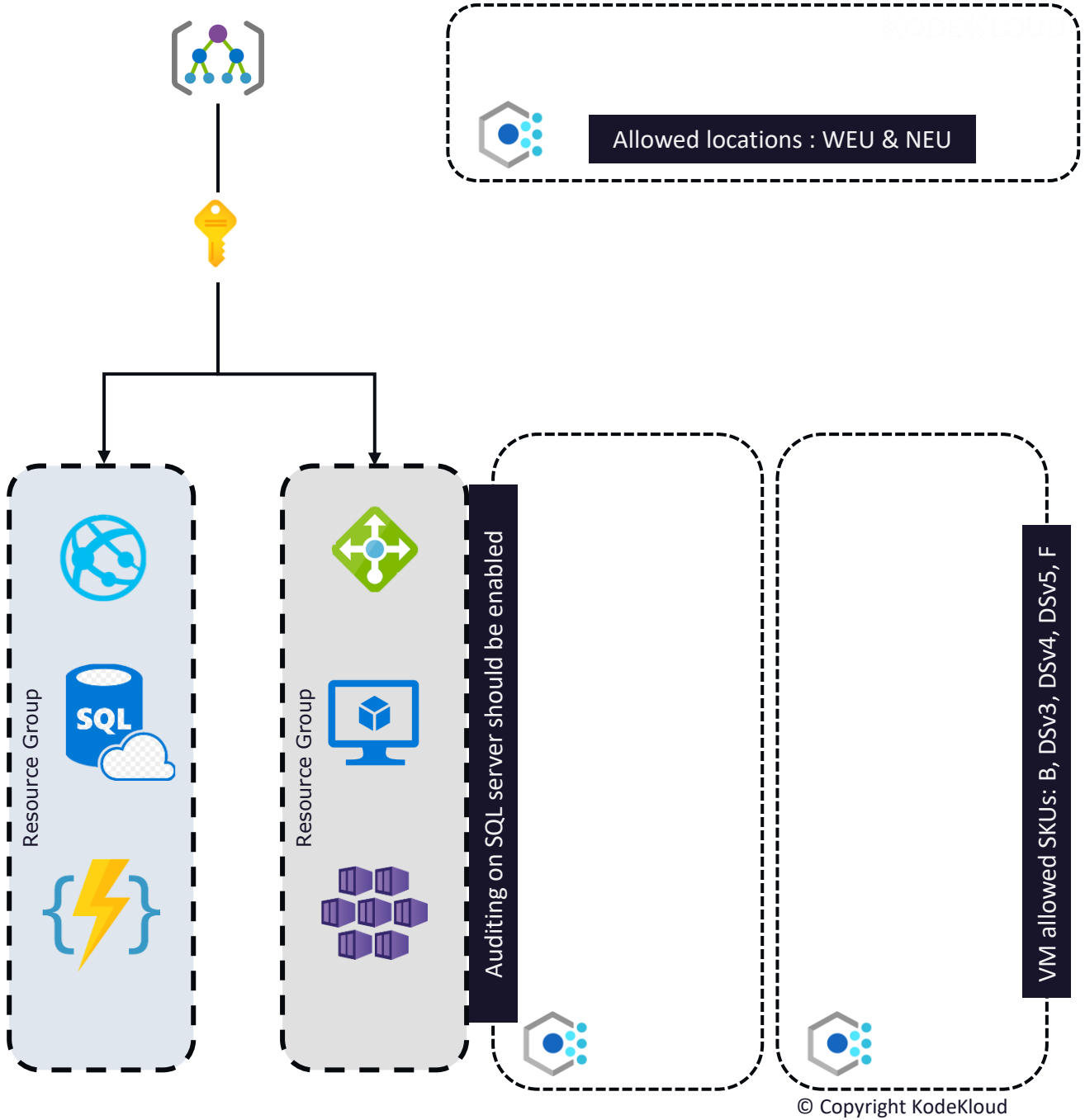
Plan for remediation

Understand what non-compliant resources mean and what should be done in case of non-compliance. Azure Policy supports automated remediation for several policies.

Compliance dashboards

Get bird's eye view of policy assignments and compliance

With the help of compliance dashboards, we can understand the non-compliant resources and how far we have achieved compliance.

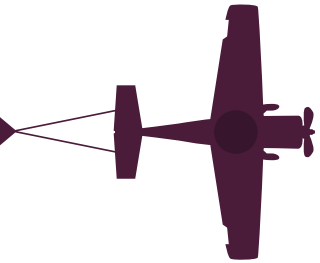


Design for role-based access controls

Manage access to your resources with the help Azure RBAC

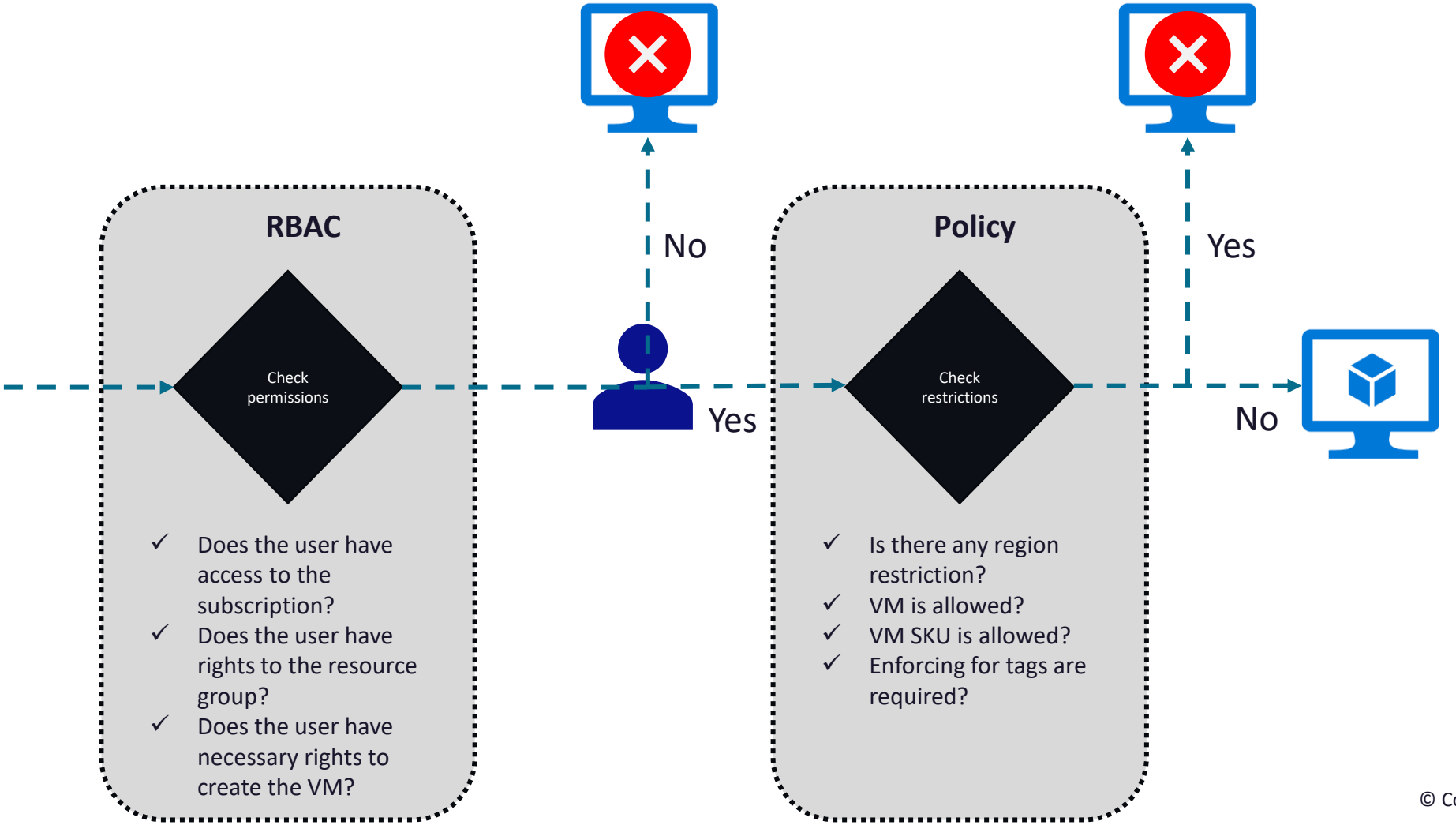
Scope	Reader	Built-in	Custom	Contributor	Owner
Management Groups	Observers Auditors Reviewers	Developers Resource managers Custom roles Resource specific roles			Admins
Subscription					
Resource Group					
Resources	Managed identities for automation or granular access				

- Use the principle of least privilege
- Understand the requirements and assign at highest level
- Consider providing access to groups rather than adding individual users
- Consider role overlapping scenarios and limit number of owners . Furthermore, leverage Azure PIM



Combining policies and role-based access control

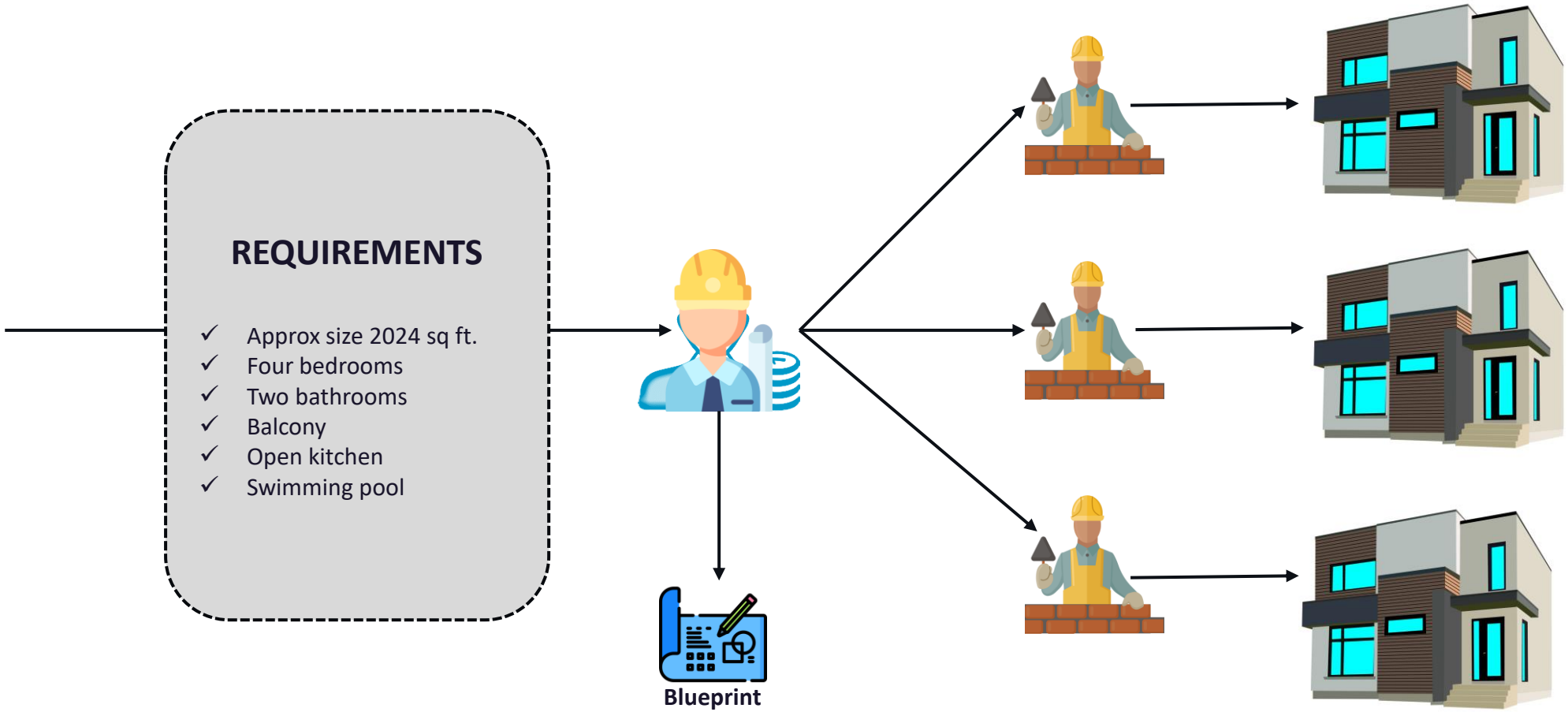
Combine Azure Policies and Azure Role Based Access Control to grant resource access and enforce compliance



Design for Azure Blueprints

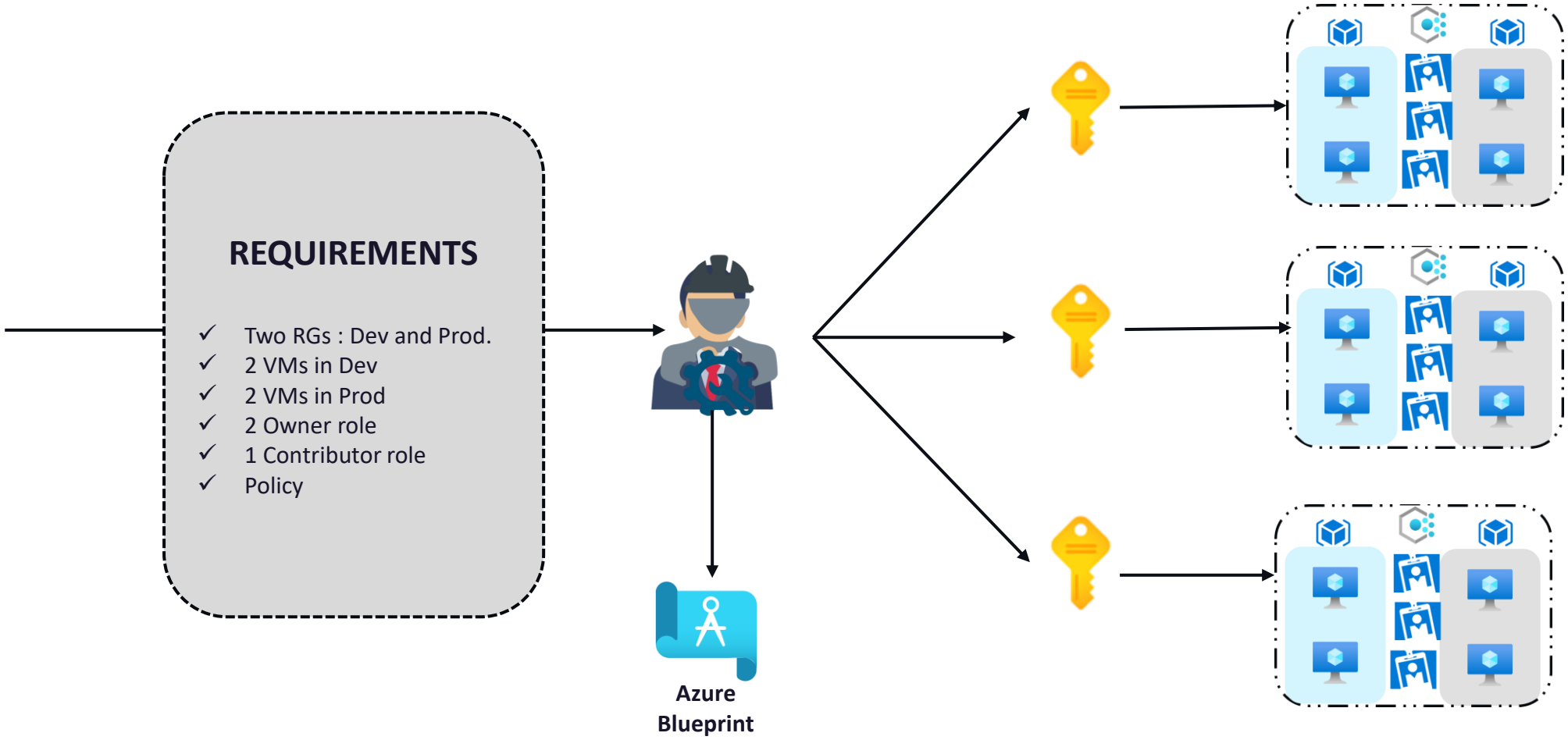
Design for Azure Blueprints

Define a set of repeatable resources and governance tools that you need in your environment



Design for Azure Blueprints

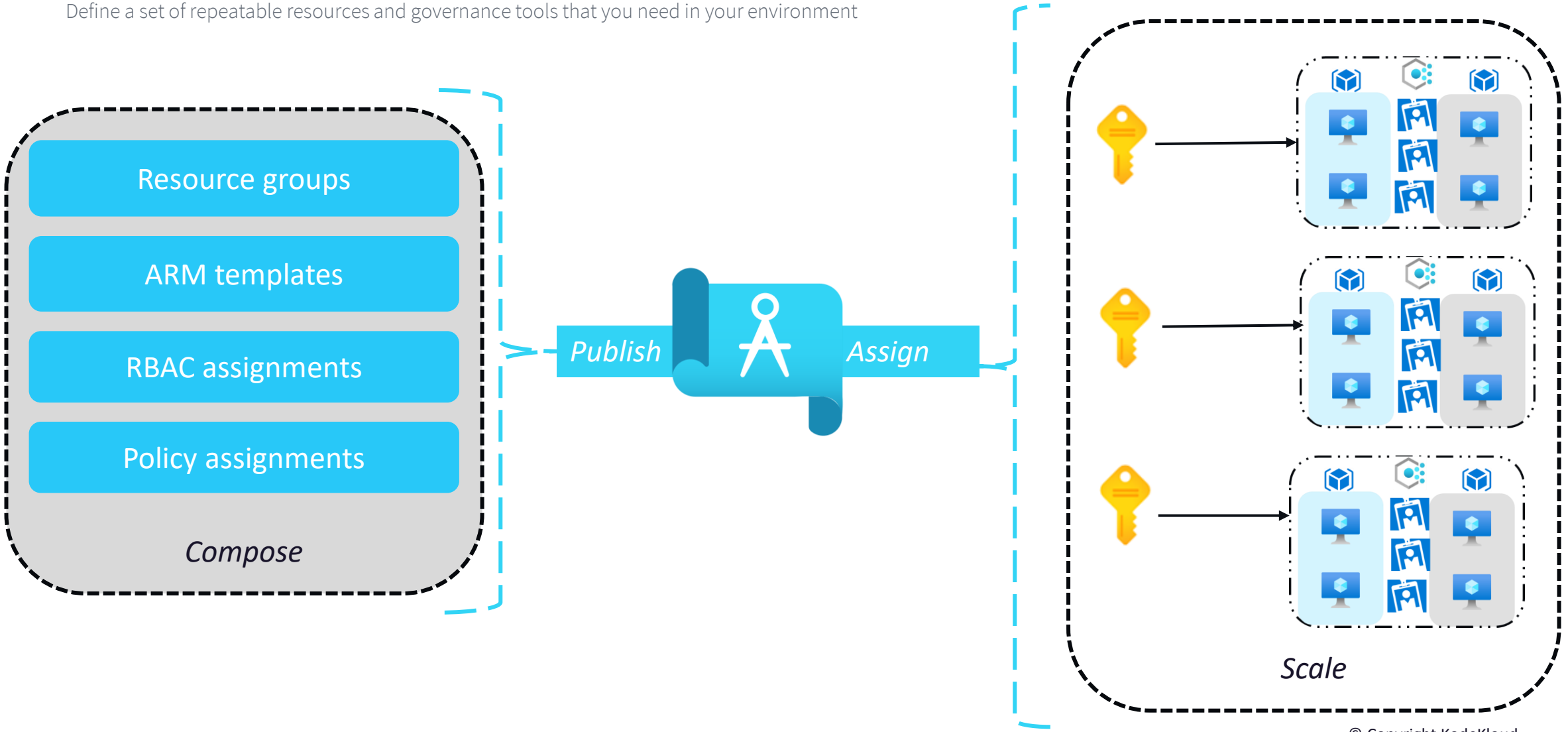
Define a set of repeatable resources and governance tools that you need in your environment



KodeKloud

Design for Azure Blueprints

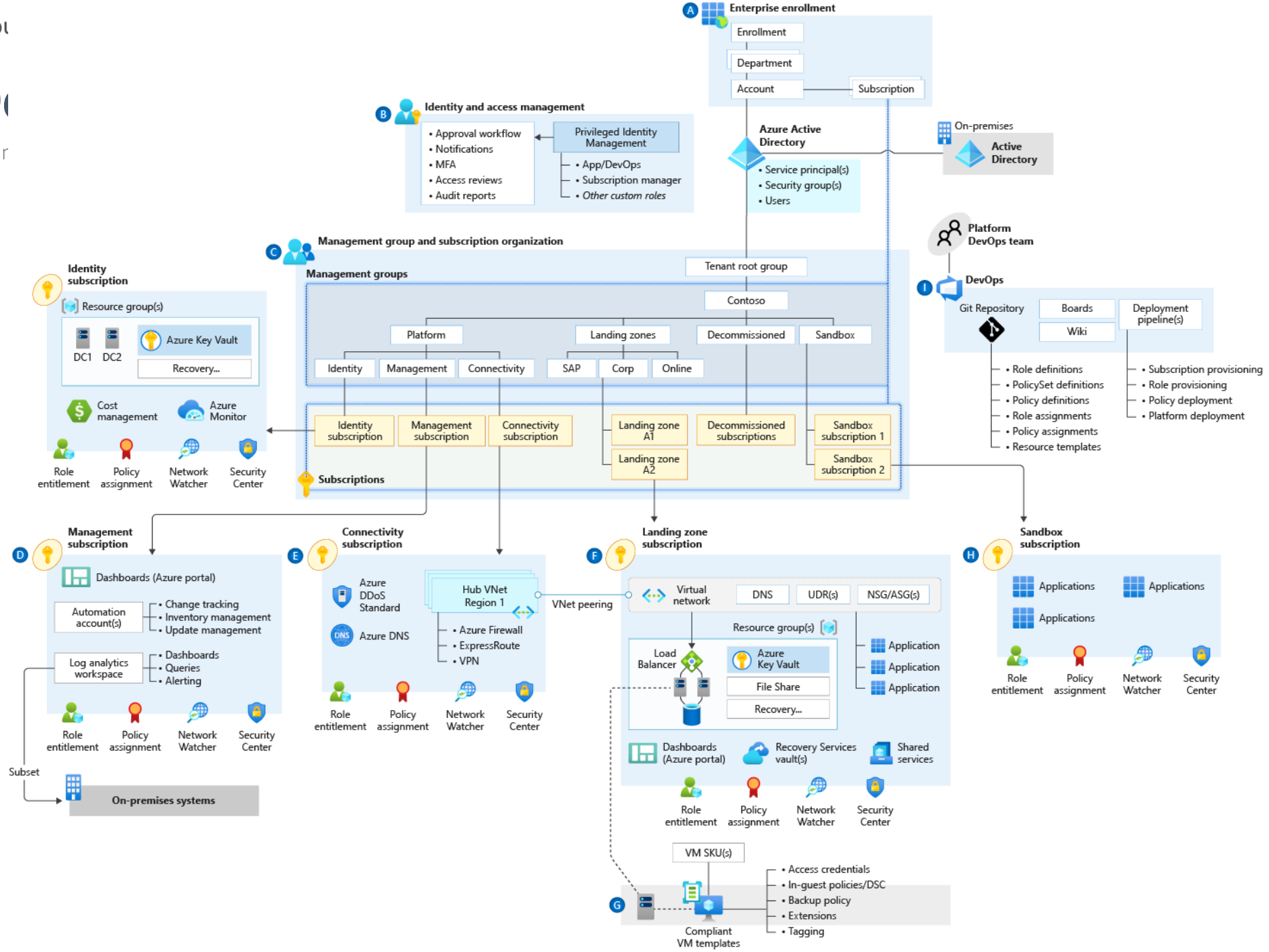
Define a set of repeatable resources and governance tools that you need in your environment



KodeKloud

D

Defir



Scenario

Vendetta Corp would like to implement the following organizational standards:

- Create a hierarchy in Azure with two entities Marketing and HR and host their Production, DR, and Testing environments. There is a separate entity called HUB for hosting shared services used by both Marketing and HR entities. Following subscriptions are there in the environment.

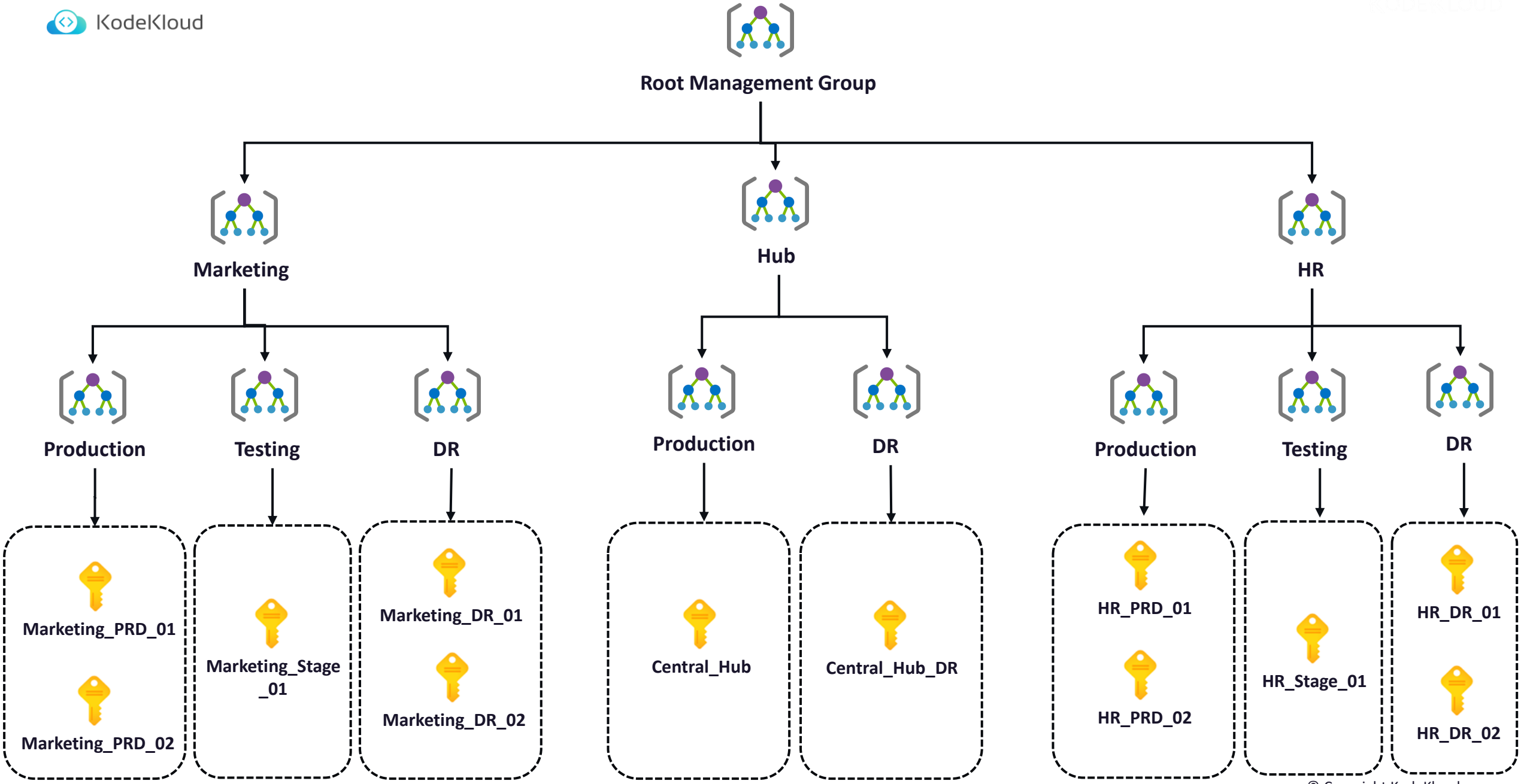
Department	Subscription Name	Environment
Marketing	Marketing_PRD_01	Production
Marketing	Marketing_PRD_02	Production
Marketing	Marketing_STAGE_01	Testing
Marketing	Marketing_DR_01	DR
Marketing	Marketing_DR_02	DR
HR	HR_PRD_01	Production
HR	HR_DR_01	DR
HR	HR_STAGE	Testing
HUB	CENTRAL-HUB	Production
HUB	CENTRAL-HUB-DR	DR

Scenario

Vendetta Corp would like to implement the following organizational standards:

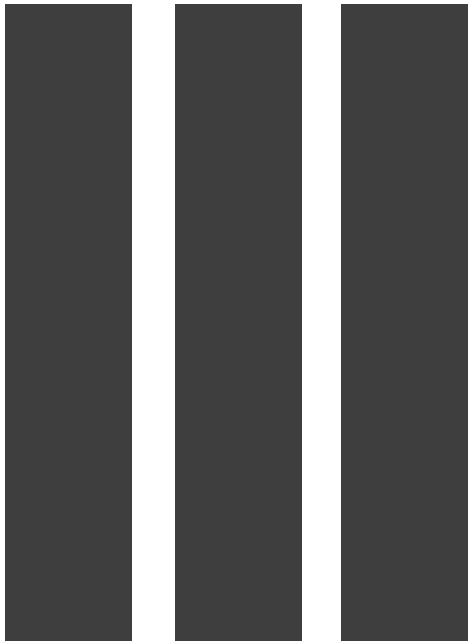
- The organization requires all resources to be deployed in East and West US only regardless of their environment.
- Only VMs in BS, DSv3, DSv4 is allowed in Testing subscriptions
- All production resources should be audited for diagnostic settings
- IT_Helpdesk group users should be able to create Microsoft Support Requests on behalf of any entity in the organization
- IT_Admins group users should e able to manage role assignments and deployments for any subscriptions in the organization
- Marketing_Admins should be to manage their subscriptions and HR_Admins should be able to manage theirs. However, both users should not be able to assign roles. For role assignment they must contact IT_Admins
- All resource groups created in Marketing subscriptions should have tag “Department: Marketing” and that should be inherited to all resources. Similarly for HR with Department as HR.
- Testing should have a template by which they will be able to spin up testing environment where they need two resource groups, role assignments, policy assignments, and Azure resources distributed in the resource groups.

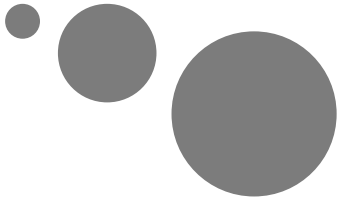
KodeKloud



KodeKloud

Module 3: Design a network architecture





Scenario

Vendetta Corp has following requirements:

- They need to connect their on-premises environment using a private connection to Azure
- If the private connection goes down, they need to have a failover path
- They need a central virtual network with following requirements:
    - All traffic to and from their Azure environment from on-premises should be inspected before they are routed to the Azure.
    - Users should be able to RDP/SSH without the need to manage IaaS servers or public IPs.
    - Should have two spoke that will host a three-tier application in WEU and WUS.
- The 3-tier application has following requirements:
    - All web requests should be inspected and need to be routed to the business logic
    - The business logic requests should be load balanced to the VMs on port 8080.
    - Requests from business logic VMs will be routed to SQL PaaS Database over a private connection
    - Users should be routed to their nearest deployment region based on the latency to WEU and WUS.
    - All traffic from FrontendSubnet should be denied on the databaseSubnet

Design for virtual networks

KodeKloud

Design for virtual networks

Plan your virtual network deployment using the following design principles

Naming

Develop a naming convention for your virtual network to ensure that the name of the virtual network is unique in the resource group

Regions

Virtual Networks are created at the regional scope, and in order to associate a resource to the virtual network then the resource also need to reside in the same region.

Subscriptions

You can deploy as many virtual networks as possible in each subscription, however, take a note of the subscription limits

Subnets

Segmentation of the address space is required to isolate the workloads and assign NSG and UDRs. Plan dedicated subnets for Application Gateway, Azure Firewall, Azure Bastion etc.

Security

Use traffic filtering options such as Azure Firewall, NVA, NSG, etc to filter the traffic to the virtual network. All traffic can be forced to these firewalls using custom route tables

Connectivity

Plan connectivity across virtual networks using Vnet Peering or VPN Gateway. Further consider hybrid connectivity options including ER, S2S, P2S etc.

Permissions

Leverage Azure RBAC to control access to the virtual network with the help of built-in virtual network specific roles. If required, we can develop custom roles

Policy

Azure Policy has built in policies that can audit and enforce standards such as DDoS Protection, Flow logs etc.

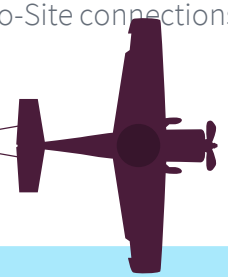
Design for on-premises connectivity to Azure

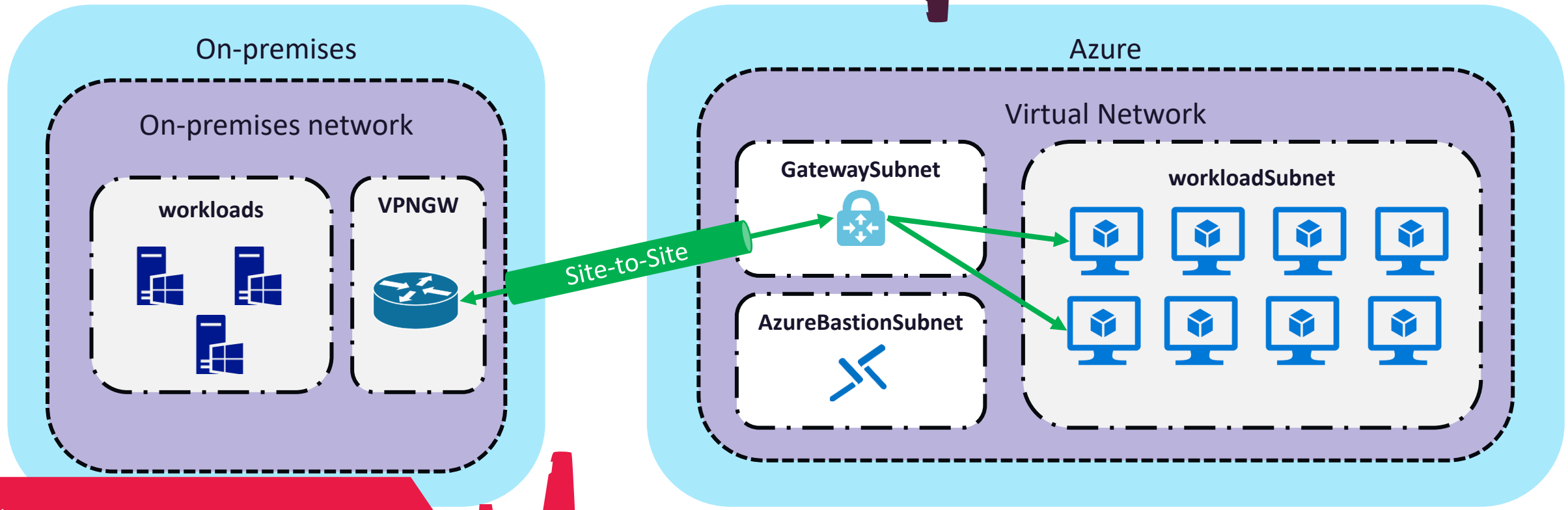
KodeKloud

VPN Connection

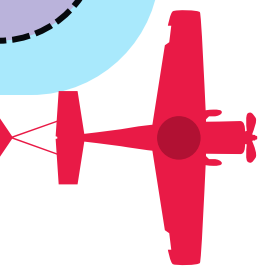
Establish encrypted connectivity to on-premises via internet using Site-to-Site and Point-to-Site connections.

Pros:
- Simple to set up connection
- Throughput supported up to 10 Gbps (SKU dependent)





Cons:
- Requires on-premises VPN device
- Deployment time for the gateway is ~30 minutes

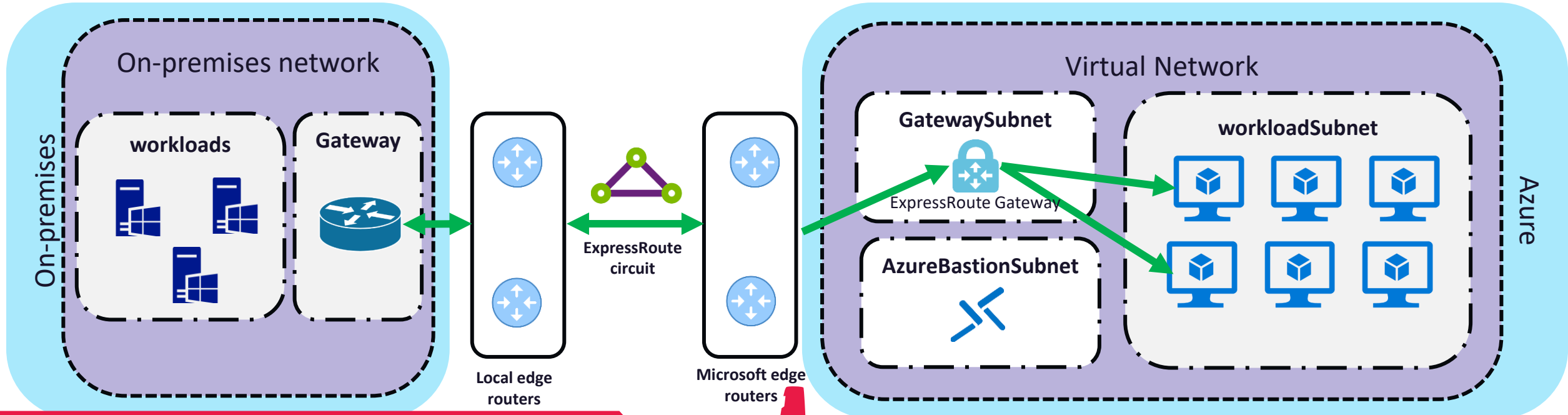


KodeKloud

ExpressRoute Connection

Establish connection to on-premises using dedicated private connection.

Pros:
- Higher throughput than VPN Gateway and the connection is dedicated.
- Dynamic bandwidth scaling is there for cost optimization (provider dependent)
- Support s direct connection using ER Direct (provider dependent)

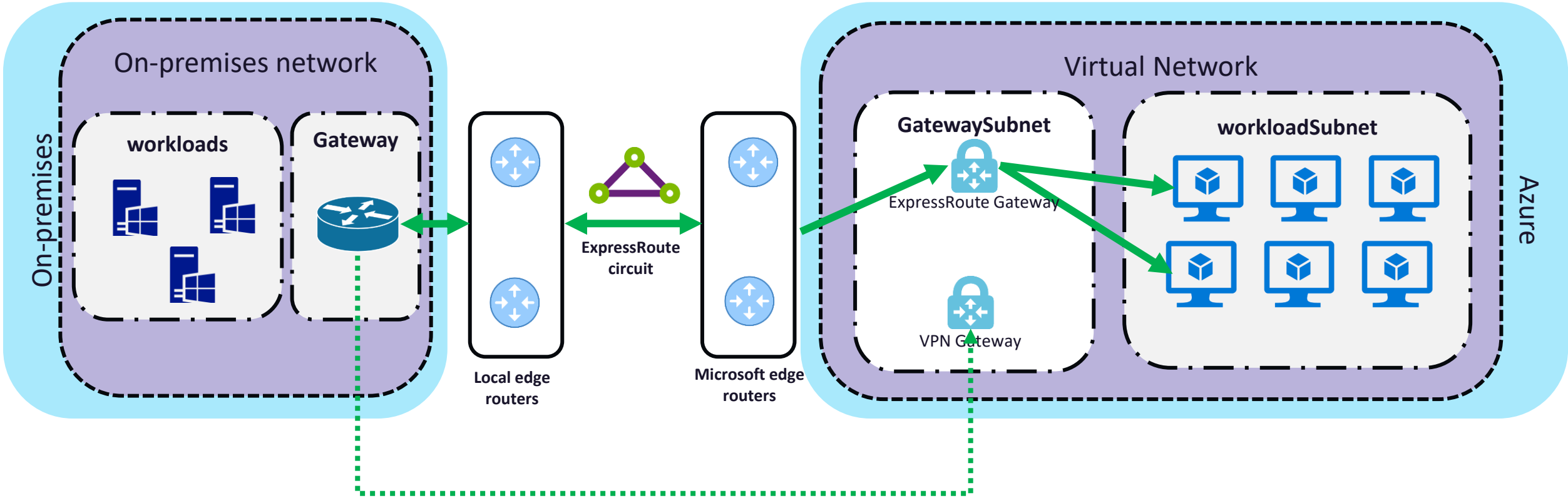


Cons:
- Requires assistance from third party provider and the configuration is complex
- Requires high bandwidth VPN device on-premises

KodeKloud

ExpressRoute with VPN failover

Establish connection to on-premises using dedicated private connection.

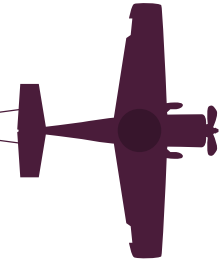


KodeKloud

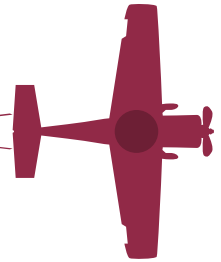
ExpressRoute with VPN failover

Establish connection to on-premises using dedicated private connection.

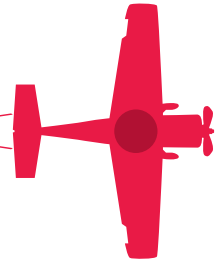
Benefit is we will have a highly available connection to our on-premises environment. One thing to keep in mind is, VPN gateway offers lesser throughput compared to what you get from ExpressRoute



Since this architecture requires both VPN and ER, you need to set up both the connections on your on-premises device. Also, you need to deploy two gateways in Azure.



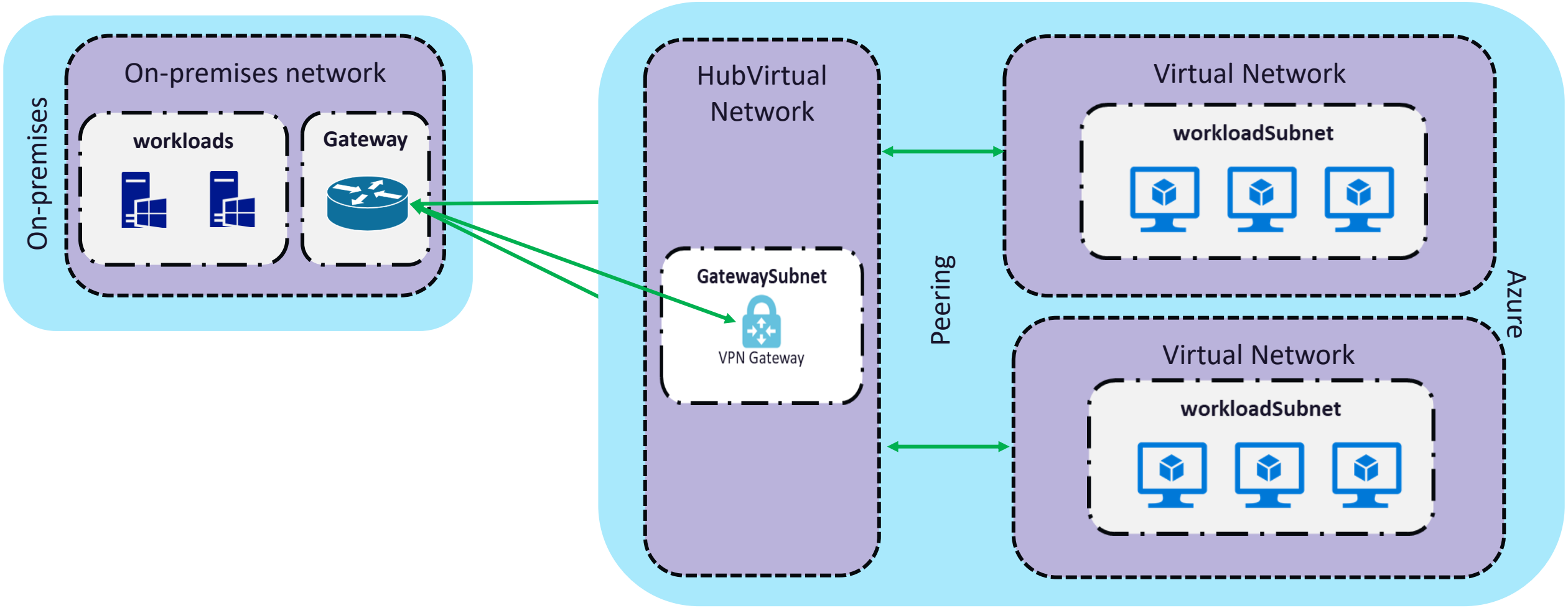
On-premises we need to set up redundant VPN appliances. Also, your Azure cost will be higher because of the two gateways



KodeKloud

Hub-Spoke architecture

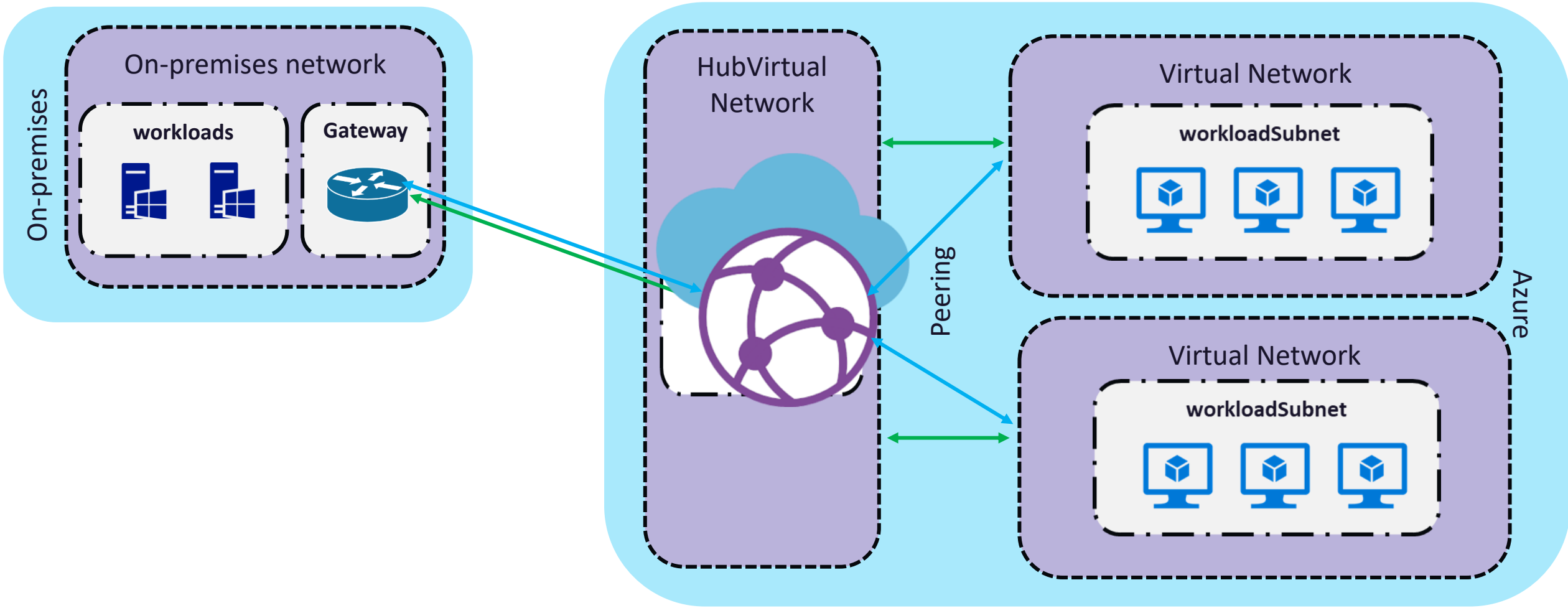
Define a central connectivity network which acts like a hub to your on-premises and Azure virtual networks



KodeKloud

Hub-Spoke architecture using VWAN

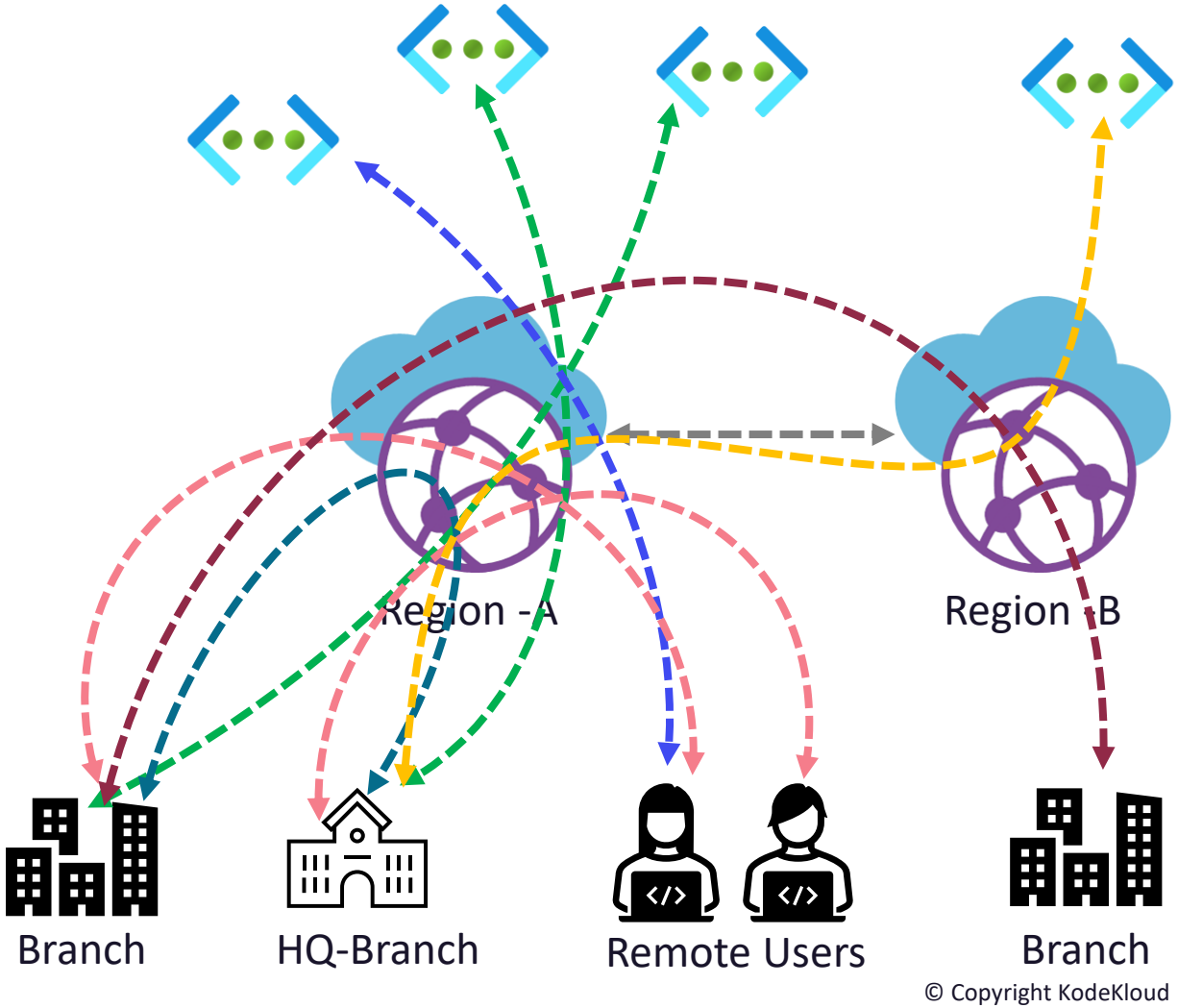
Define a central connectivity network which acts like a hub to your on-premises and Azure virtual networks



Hub-Spoke architecture using VWAN

Define a central connectivity service which acts like a hub to your on-premises and Azure virtual networks

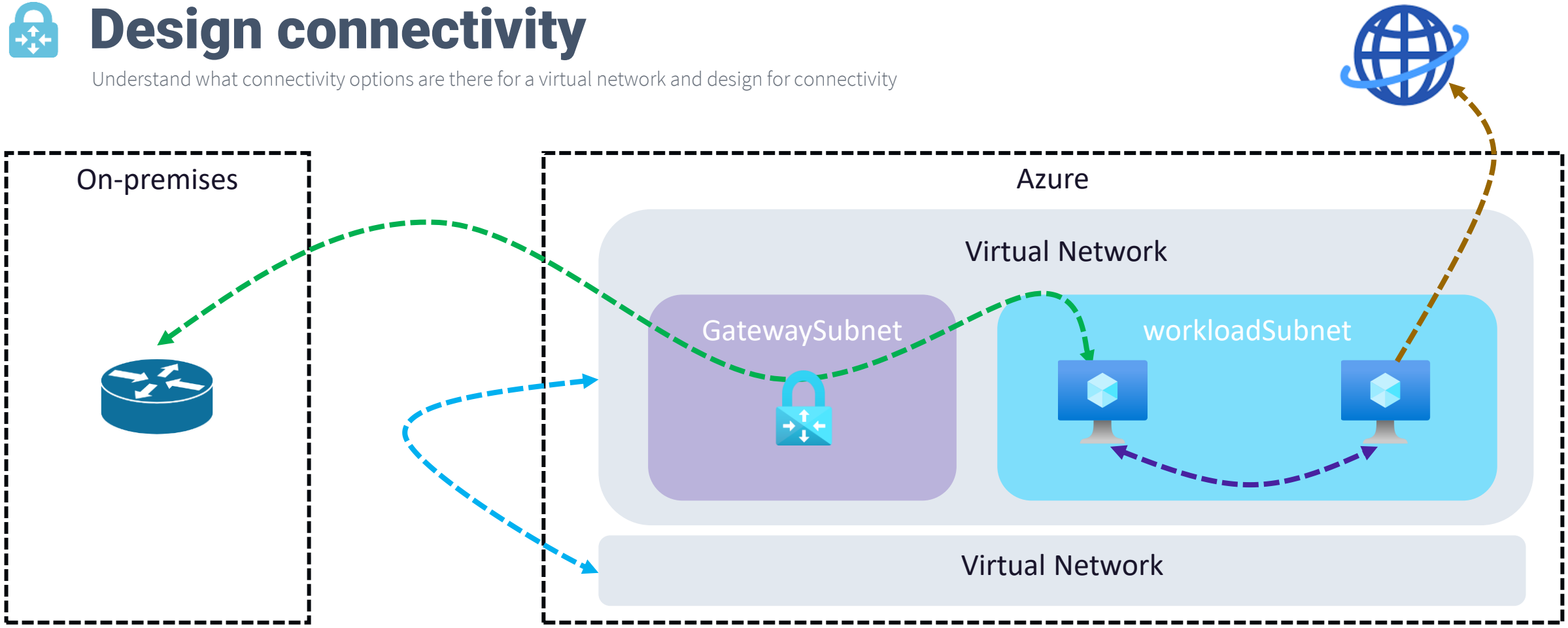
- **Branch-to-VNet**
- **Branch-to-Branch**
- **Remote users-to-VNet**
- **Remote users-to-Branch**
- **Branch-to-hub-to-hub-to-Branch**
- **Branch-to-hub-to-hub-to-VNet**



Design for network connectivity

Design connectivity

Understand what connectivity options are there for a virtual network and design for connectivity



- Connectivity between Azure resources in virtual network
- Connectivity to resources in other virtual networks
- Connectivity to on-premises
- Outbound connectivity to Internet

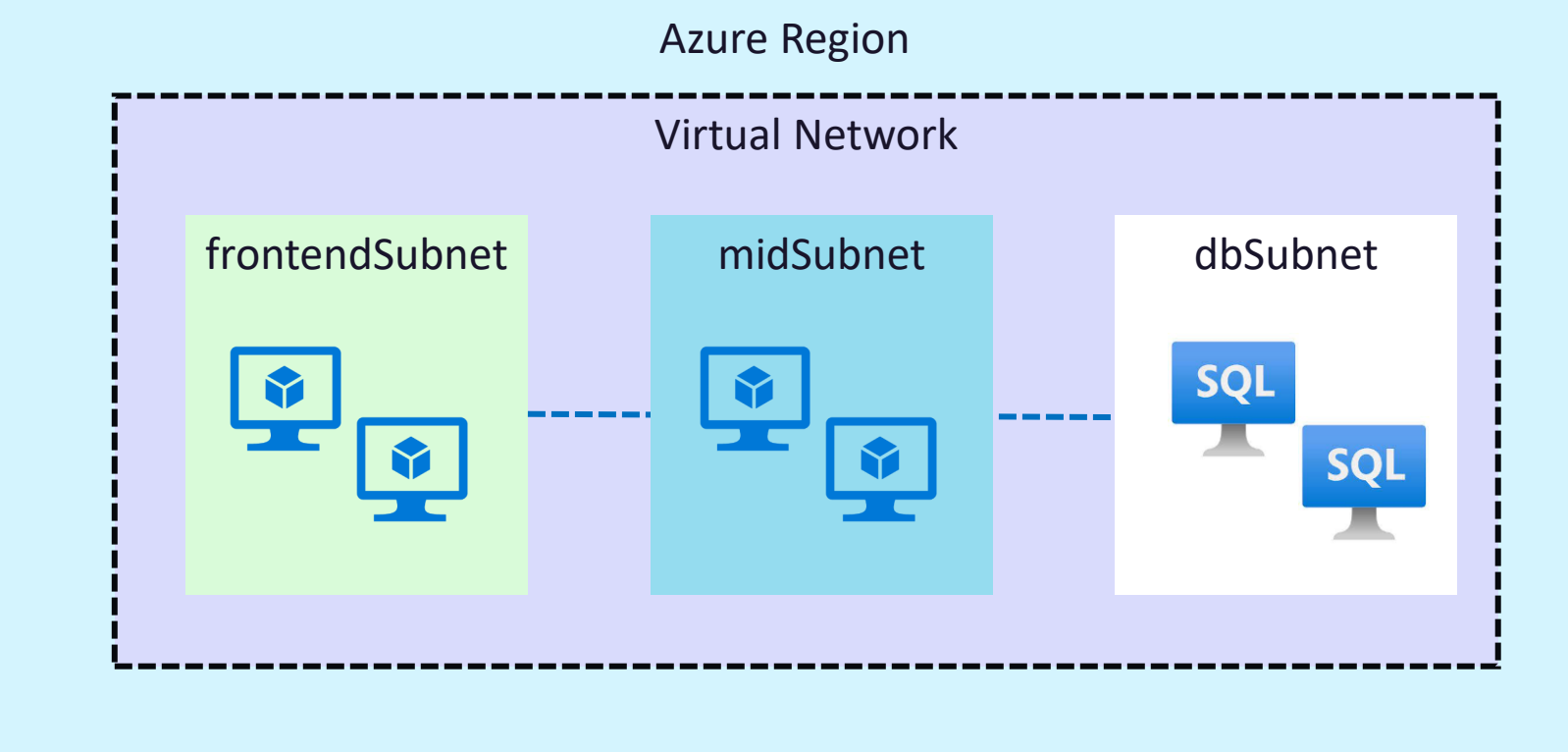
Design topology

Learn the patterns for developing network topology

01

Single network approach

All resources are deployed to single virtual network and segmentation is done using subnets



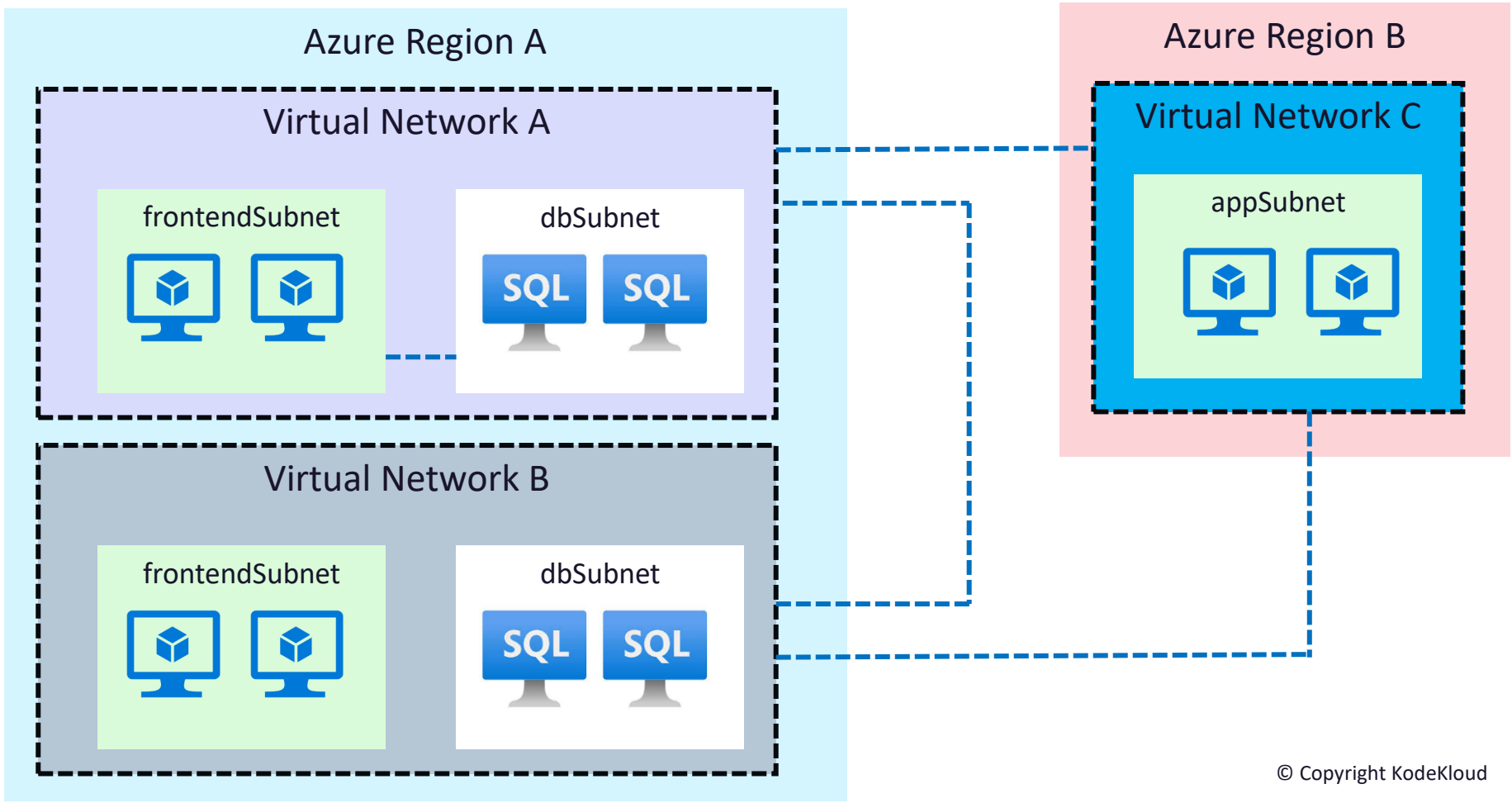
Design topology

Learn the patterns for developing network topology

02

Multiple peered networks

Deploy workloads across multiple virtual networks and connectivity between them is established with the help of Virtual Network Peering



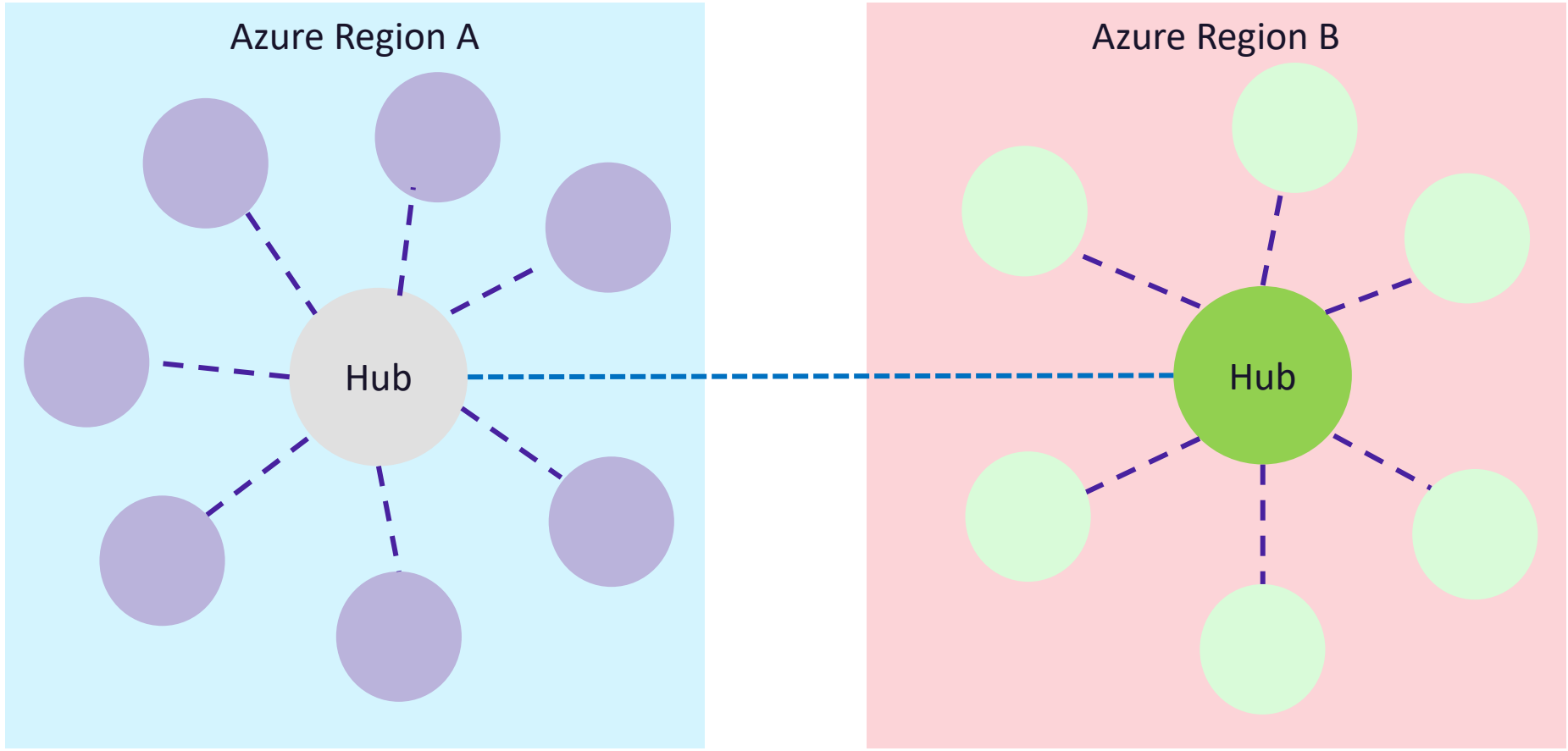
Design topology

Learn the patterns for developing network topology

03

Hub spoke architecture

Deploy workloads across spoke subscriptions which is peered to centralized hub network which hosts shared services, this hub is further peered with hubs in other regions.



Design outbound connectivity

Understand options to control the outbound connectivity from resources in virtual network

01

Azure Firewall

All outbound traffic from virtual network can be forced to the firewall with the help of UDRs..

02

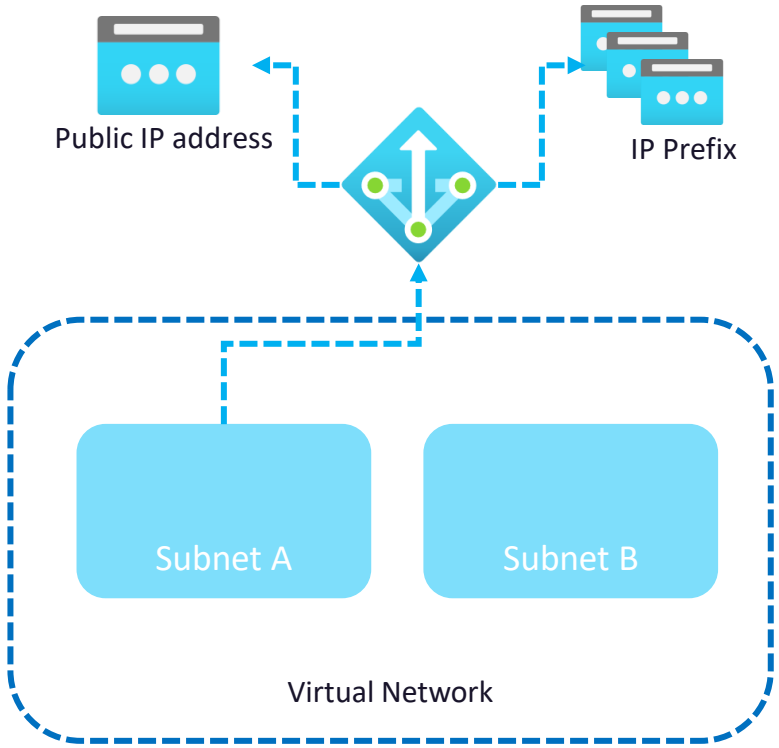
Azure Load Balancer

Outbound traffic from virtual network can be routed via Azure Load Balancer with the help of outbound rules.

03

NAT Gateway

By defining a set of Public IPs in the NAT gateway, all outbound traffic can be NAT'd via the gateway



Design outbound connectivity

Understand options to control the outbound connectivity from resources in virtual network

Security

Since the outbound traffic is routed via the NAT Gateway, there is no need to have public IP for the resources in the virtual network.

Resiliency

NAT Gateway is a fully platform managed distributed service. Since this is software defined networking, NAT gateway is not dependent on a single VM or a single physical gateway.

Scalability

Being a SDN service, Azure manages the scaling of the services and there are multiple instances of the gateway spread across multiple fault domains.

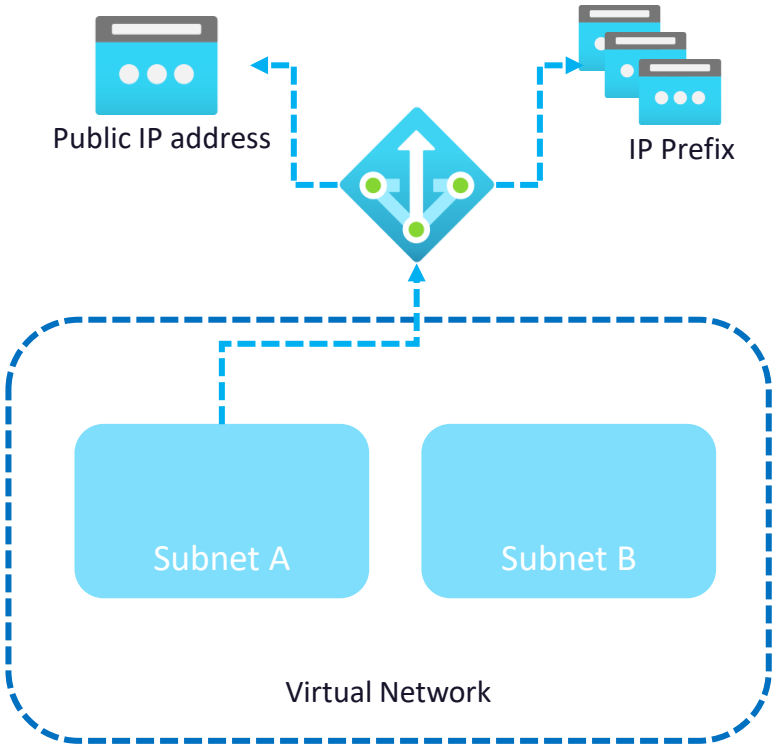
Performance

NAT gateway won't affect the network bandwidth of your compute resources.

03

NAT Gateway

By defining a set of Public IPs in the NAT gateway, all outbound traffic can be NAT'd via the gateway



KodeKloud

Design routing

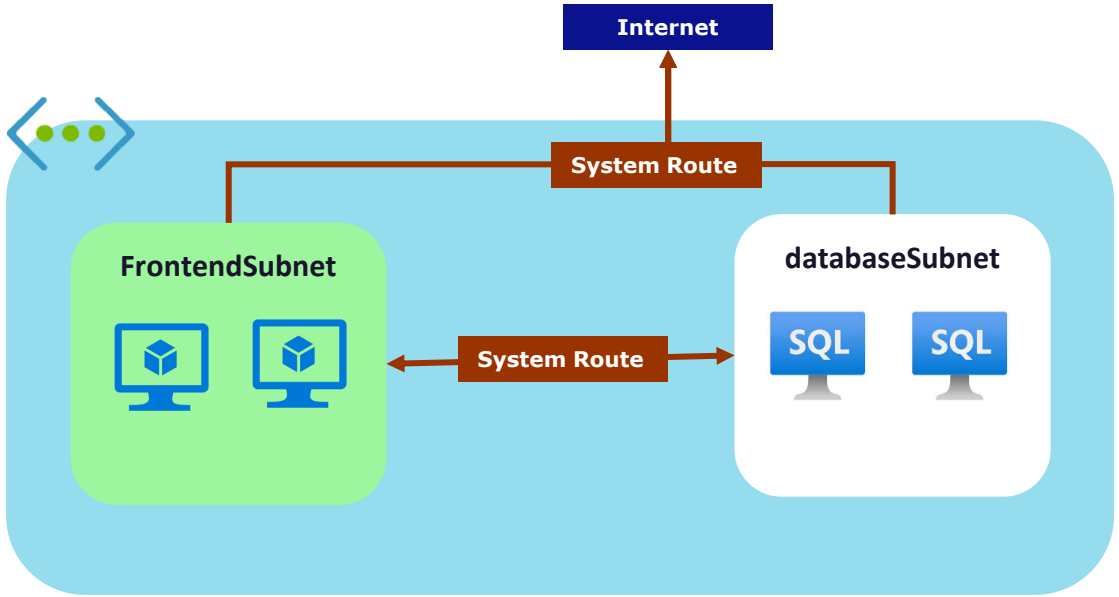
Define how the traffic is routed in your virtual network using route tables

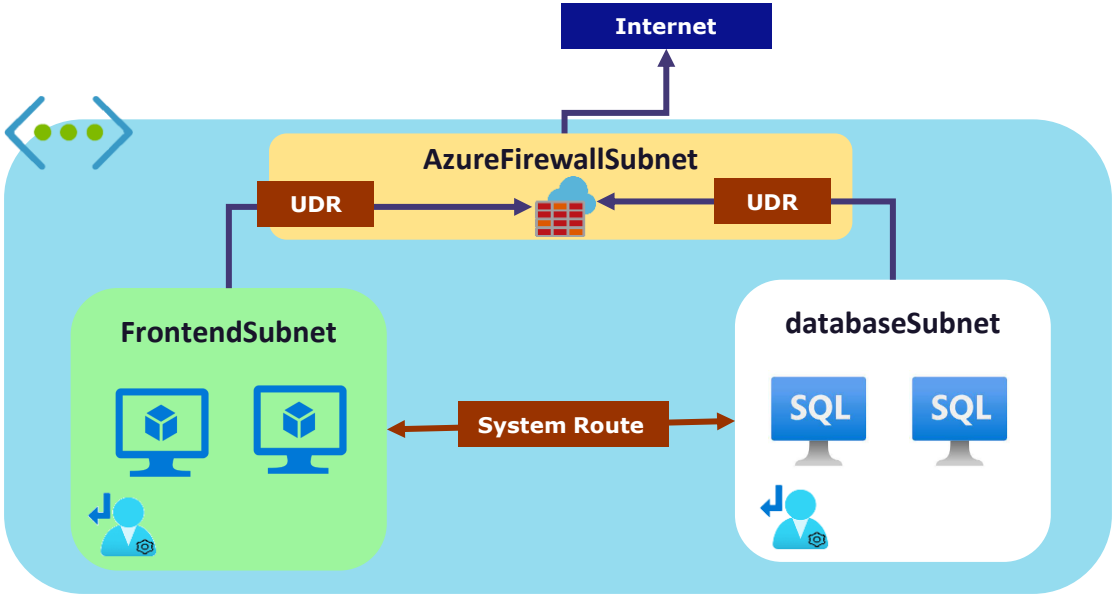
System Route

- When you create a virtual network, Azure will be adding the system routes to the VNet. This route table will help the resources within the same virtual network to communicate with each other without any additional configuration.
- Furthermore, system route enables resources in the network to communicate to the internet.
- If you peer your virtual network to another virtual network, then the address space of the peered network will be added to the route table.

User defined route

- We can override the system route by associating a route table with user defined routes.
- The next hop can be defined, and Azure will route the traffic to that.





Design for application delivery

Choosing a load balancing solution

There are multiple load balancing solutions available in Azure for different requirements, pay attention to the decision criteria and flowchart to find the right solution

Azure Load Balancer	Application Gateway	Azure Front Door	Traffic Manager

01

Type of traffic

Application using HTTP/HTTPS?
Internal or external facing?

02

Coverage

Regional or deployed in multiple regions?

03

Availability

SLA of the application?

04

Cost

Operational cost of the load balancing solution

05

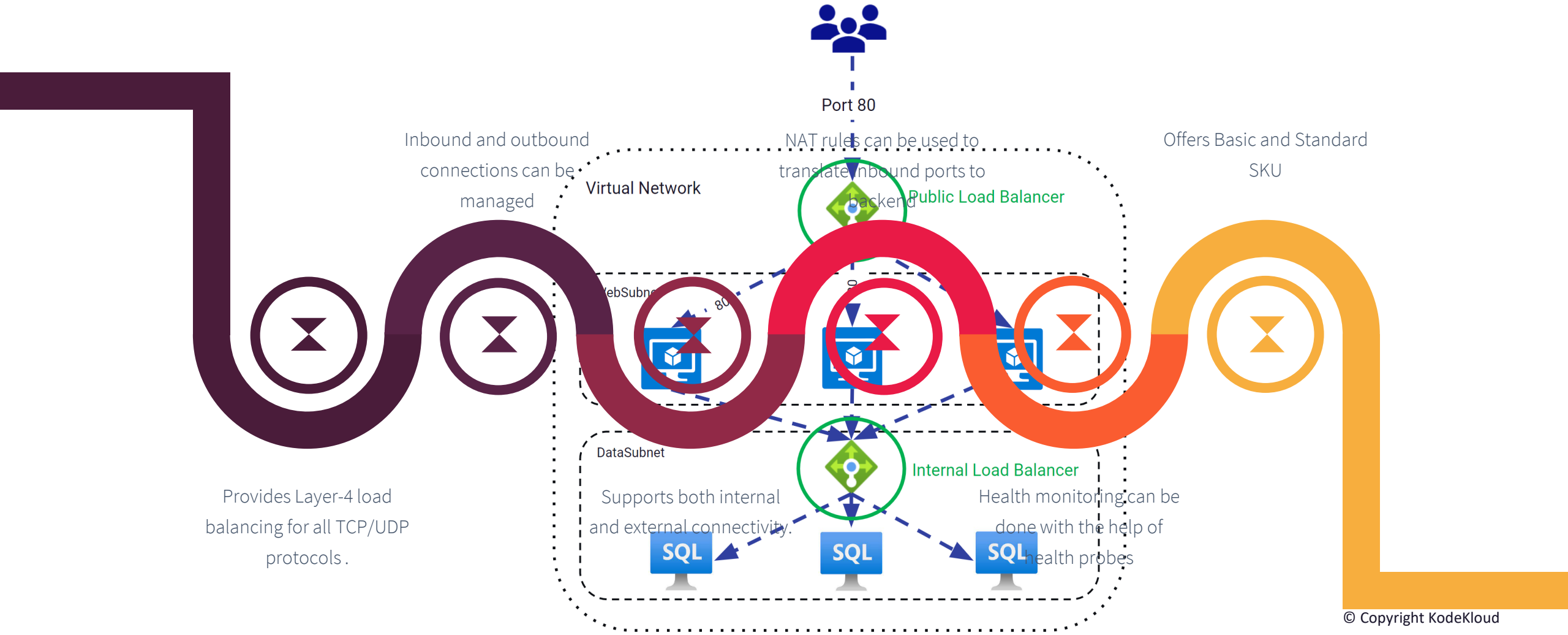
Limits and features

Limitations of the solution and service limits defined by Microsoft

KodeKloud

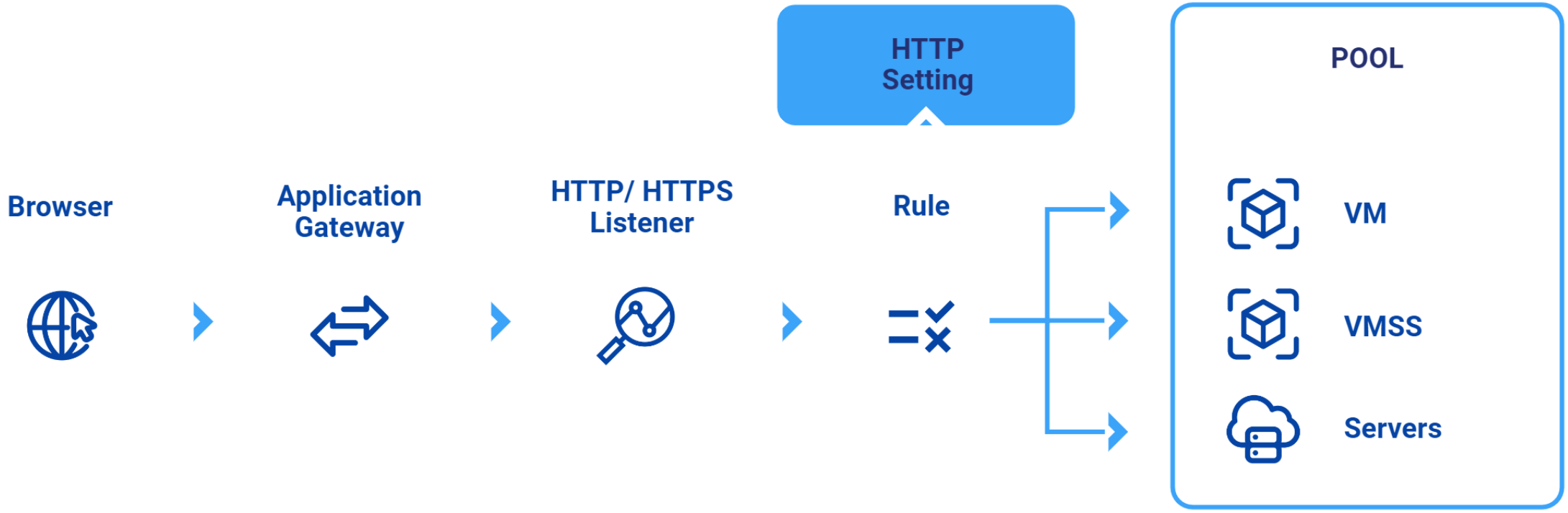
Azure Load Balancer

Load Balances the request from clients for all TCP/UDP traffic to backend pool which consists of VMs or VMSS



Azure Application Gateway

Load balance web request to your application with support for VMs, VMSS, App Services, and non-Azure endpoints as backend

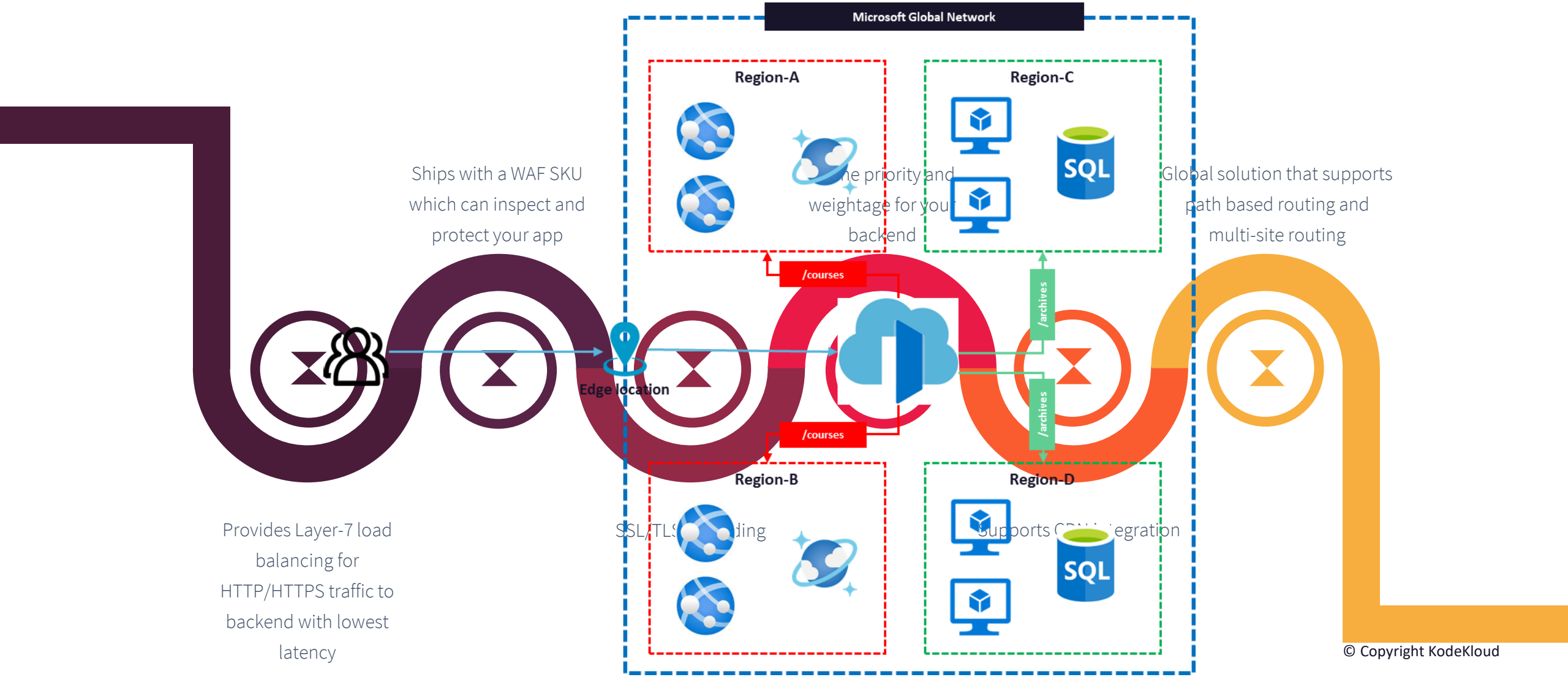


HTTP/HTTPS traffic.

KodeKloud

Azure Front Door

Global solution to distribute your traffic to region with the lowest latency



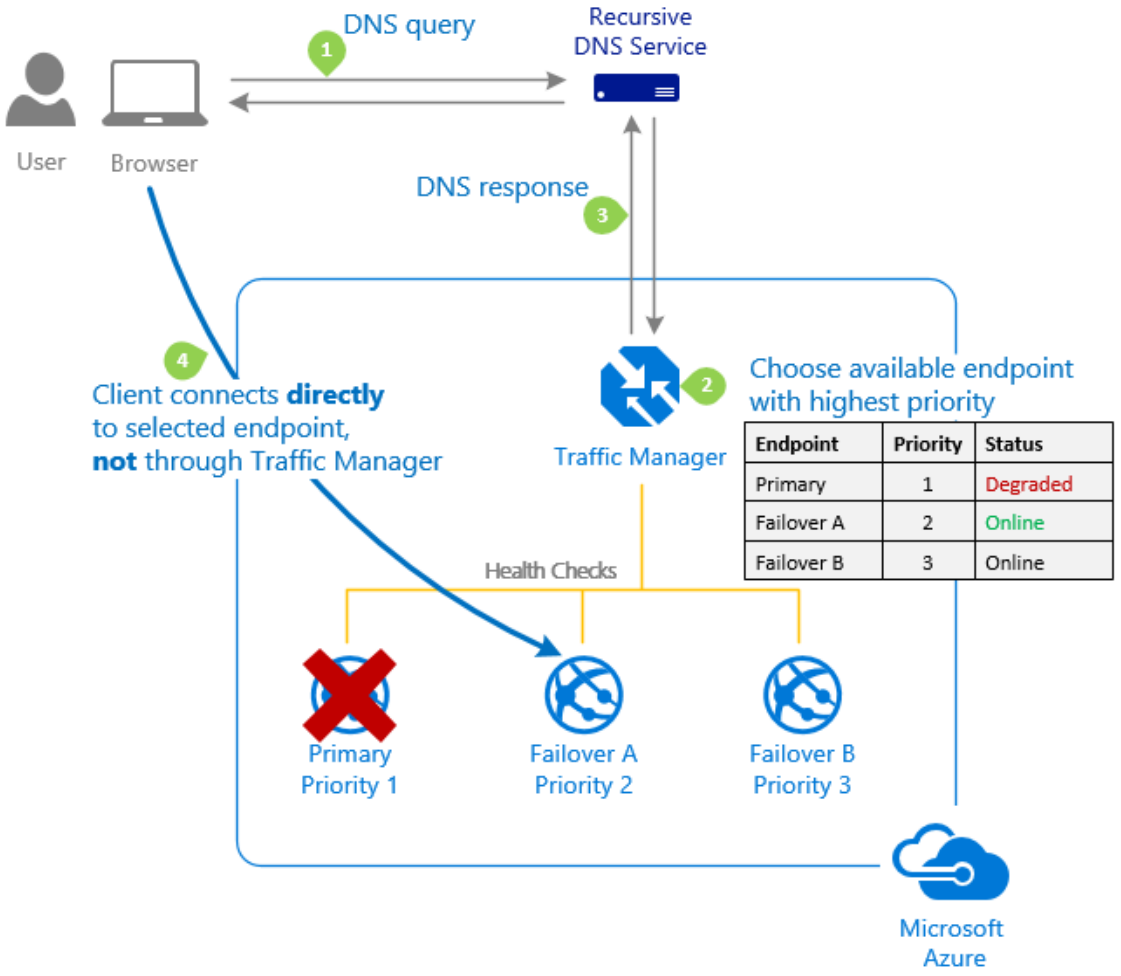
Azure Traffic Manager

DNS Load Balancing solution that supports priority, weighted, performance and geographic routing methods.

W

s

Increase applicatio
availability with the h
of routing method

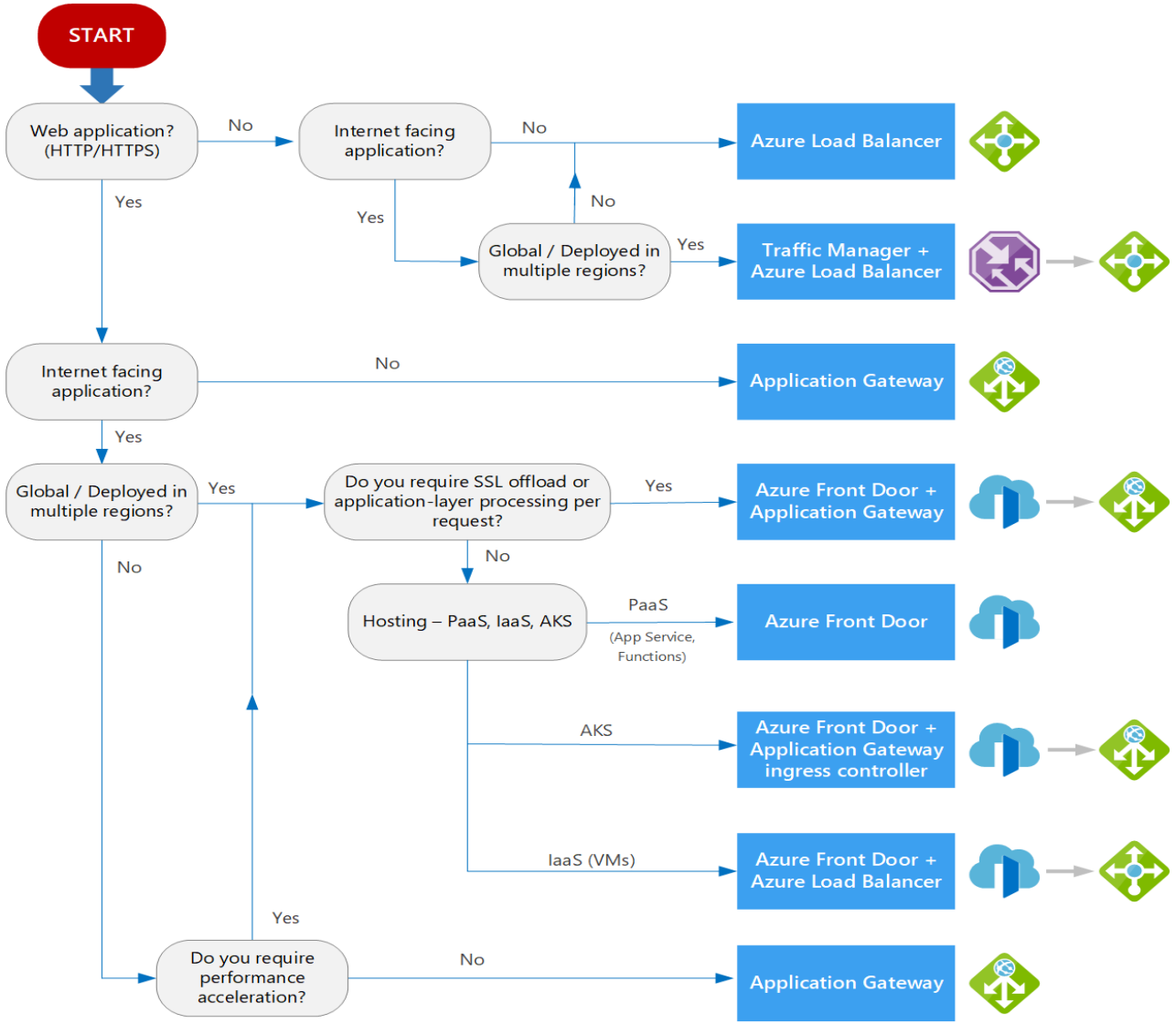


Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online

ternal apps are not
supported

Choosing a load balancing solution

There are multiple load balancing solutions available in Azure for different requirements, pay attention to the decision criteria and flowchart to find the right solution



Source: [Microsoft documentation]

KodeKloud

Content Delivery Network

Improve content delivery performance by caching content to edge locations across the globe.

01

Global Presence

Bring content closer to your customers by caching to edge locations across the globe. Cached content will be delivered from the nearest edge location regardless of the origin location of the content

02

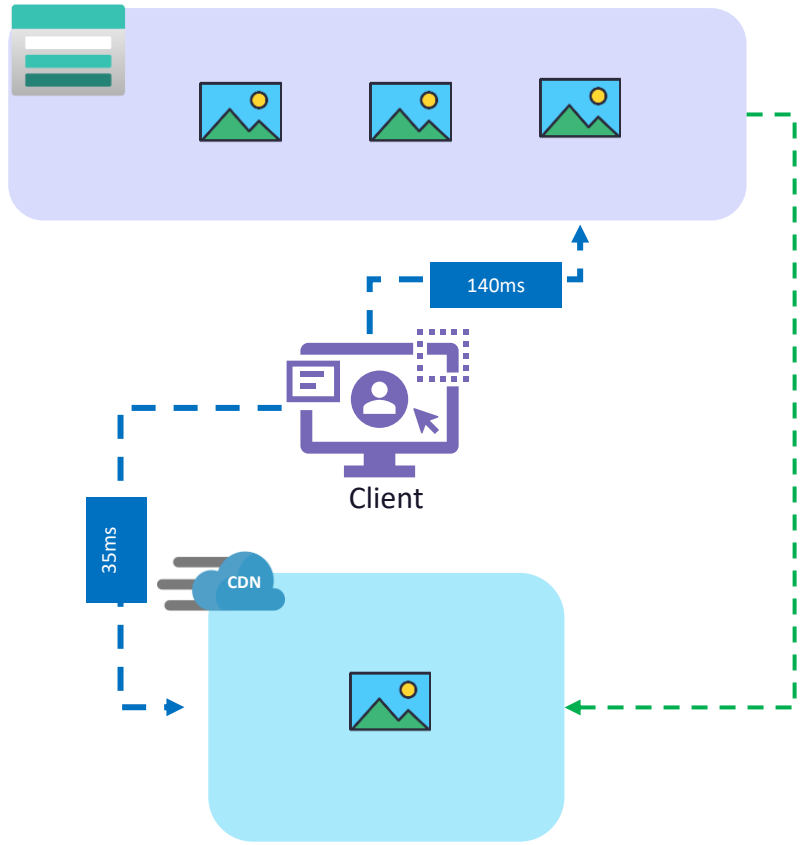
Reduce latency

Latency can be reduced as the content is delivered from the closest edge location.

03

Custom domains

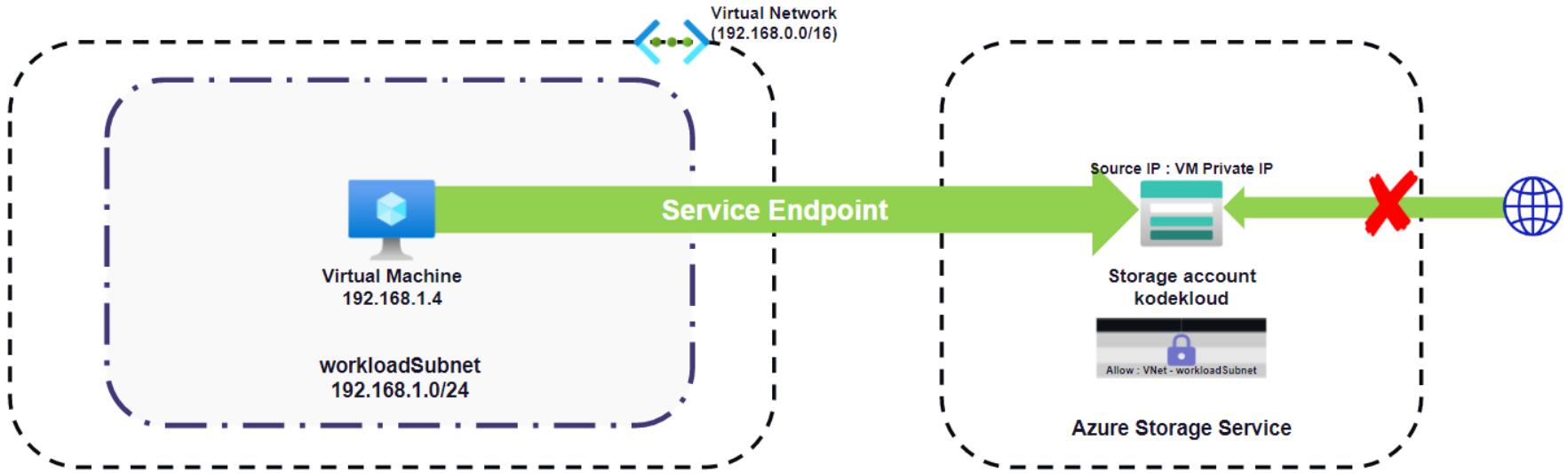
We can associate custom domain to the CDN endpoints. Furthermore, we can add file compression and geo filtering



Design for network security and application protection

Service Endpoint

Direct and secured connection to Azure services from virtual network over Microsoft backbone network



01

Security

Access Azure services with enhanced security. No need to assign or manage Public IP for virtual network resources.

02

Routing

Microsoft uses its backbone network and ensures that optimal routing is selected for communication

03

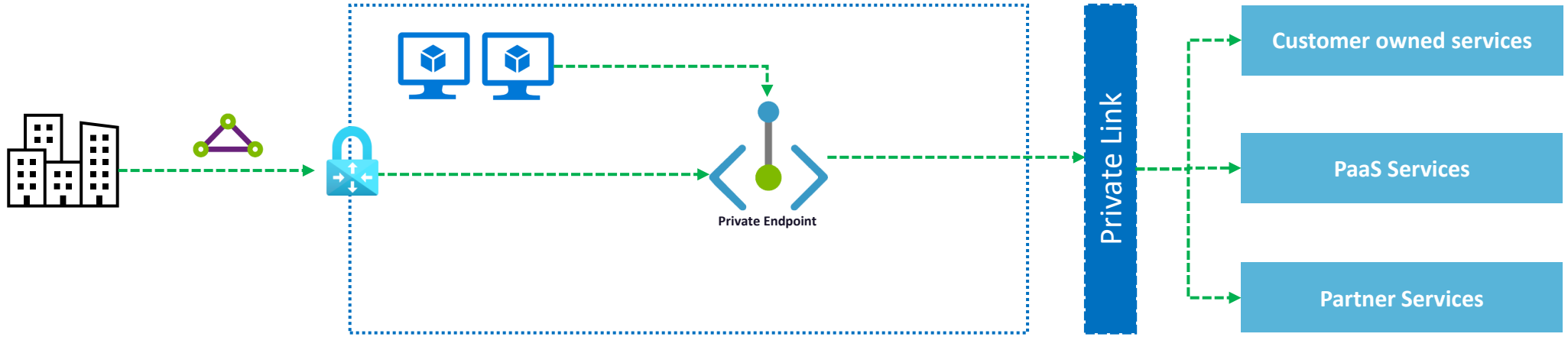
Ease of set up

Service endpoints can be configured from supported resources to virtual network without any complex configuration.

KodeKloud

Private Link

Private connectivity to supported PaaS services using private IP address from the virtual network



01

Private connectivity

The service will obtain an IP address from the virtual network making it look like part of the virtual network

02

Connectivity from on-premises

With the help of ER/VPN we can connect to the supported services using private endpoint

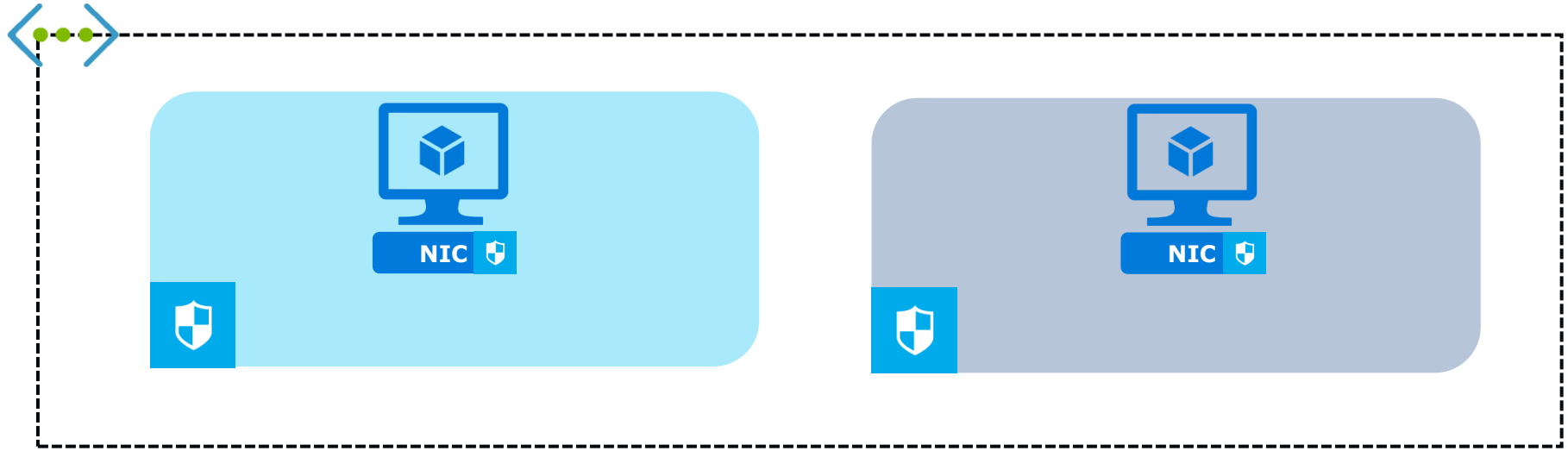
03

Eliminate public internet

Since all communication is happening via private IP address from virtual network, public internet access is not required..

Network Security Groups

Enables traffic filtering at the subnet level or network interface



01

Traffic filtering

Allow or deny traffic based on the port, protocol, and direction of traffic.

02

Applicable for inbound and outbound traffic

Both inbound and outbound traffic can be filtered using the NSG, these rules are evaluated based on the priority.

03

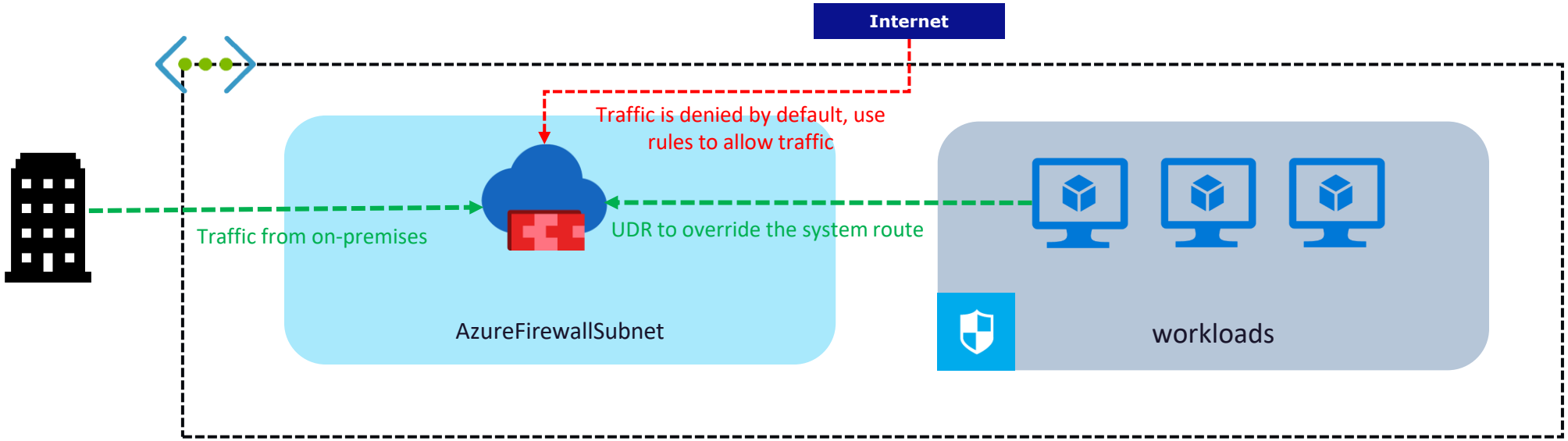
Scopes

Can be applied to subnet or NIC of the VM. NSG applied to subnet will inherit the rules to all interfaces in the subnet.

KodeKloud

Azure Firewall

Protect resources deployed in your virtual network



01

Network protection

Eliminates network infiltration by providing inbound protection for non-web traffic and outbound traffic

02

Rules and policies

By default, all traffic is denied, and incoming and outgoing traffic is monitored. With the help of firewall rules, we can allow traffic.

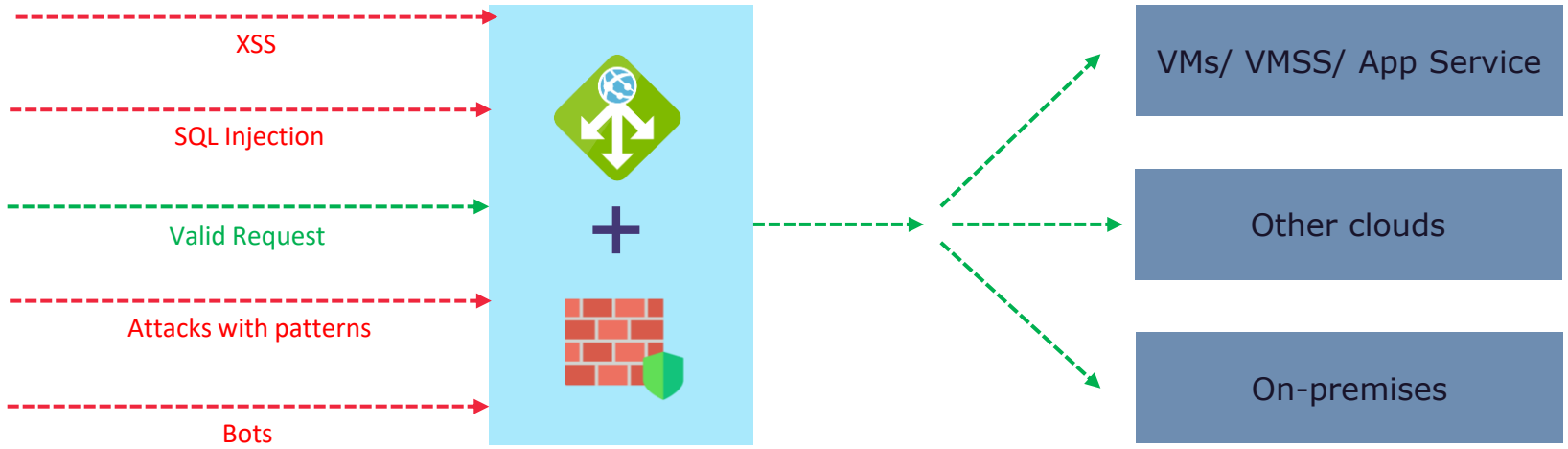
03

Deployment and availability

Ideally firewall is deployed to the hub virtual network to monitor all traffic and route to the spokes based on rules. Azure Firewall is a platform managed service, and the scaling availability of the service is managed by Microsoft.

Web Application Firewall (WAF)

Protect your web applications from known attacks and vulnerabilities



01

Protection Modes

Prevention and Detection mode. In Prevention, all attacks will be prevented by WAF and detection the attack will be detected however, WAF will allow the traffic after logging it.

02

Central Management

WAF policies can be centrally managed and can be associated with multiple apps

03

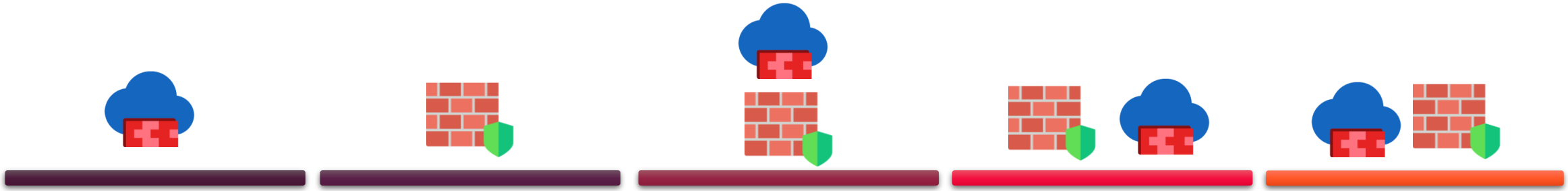
Support

WAF is supported by Application Gateway, Content Delivery Network, and Azure Front Door.

KodeKloud

Azure Firewall v/s WAF - Scenarios

Learn when you use Azure Firewall, WAF or the combination of both



01

Azure Firewall alone

Ideal when you have no web applications in your network, and you want to protect non-HTTP workloads.

02

WAF alone

When there are web-application in your network. For rest of the traffic, we can use NSG for filtering

03

In parallel

Common implementation where the web-based attacks are covered by WAF, and rest of the traffic is filtered using Firewall.

04

WAF in the front

WAF in the front will protect the web application, then the packet will be further inspected by the Azure Firewall. This is appropriate in scenarios where you need to know the client IP address.

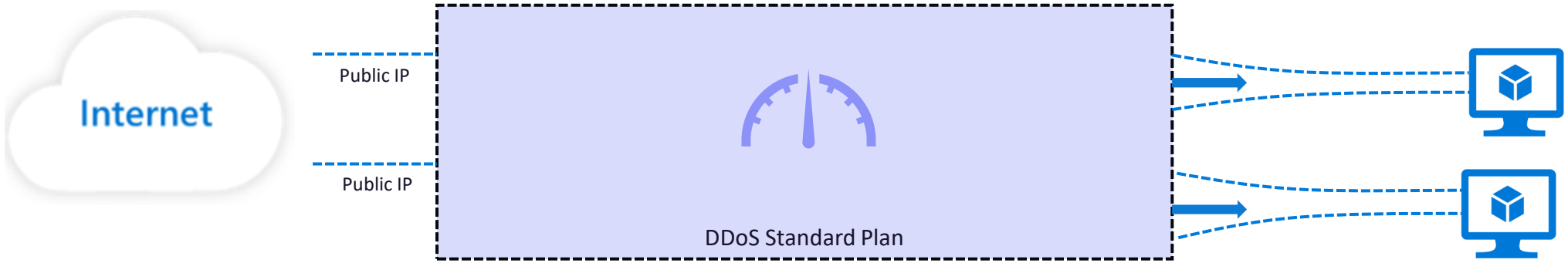
05

Azure Firewall in the front

All traffic will be inspected by Azure Firewall before it is forwarded to the WAF.

DDoS Protection

Enable DDoS mitigation capabilities for your application and resources in the virtual network



01

Always on monitoring

Monitoring always on and is ready to find any DDoS attacks. With the help of adaptive tuning, it can help mitigating the attacks.

02

Multi later protection and alerting

Can be deployed to implement the defense in depth strategy. DDoS Protection plan offers advanced attack analytics and alerts for users.

03

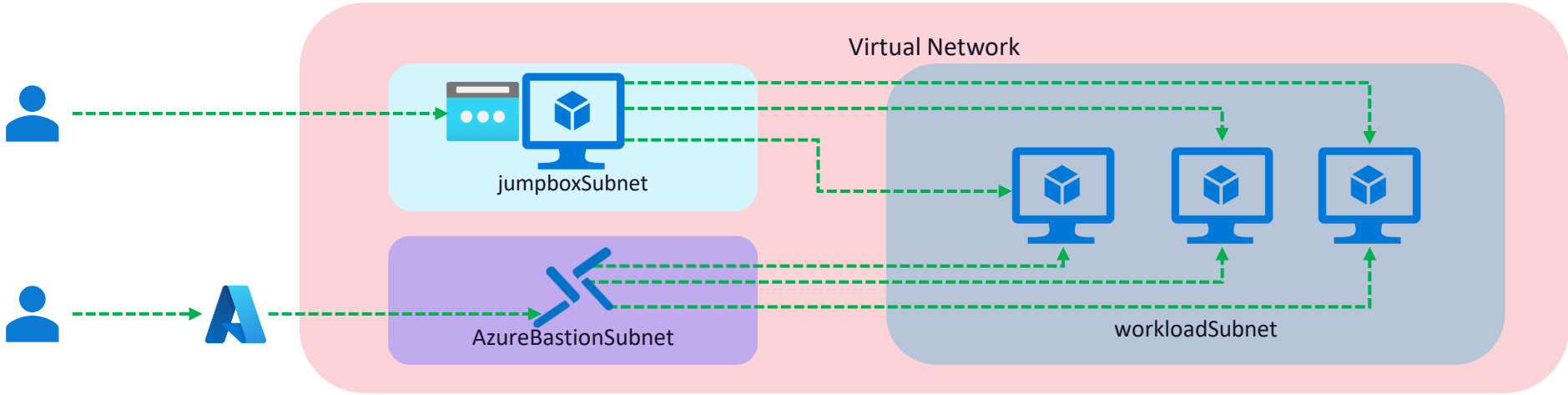
Plan

By default Basic plan is enabled for all virtual networks. It's recommended to go with the standard plan for all production workloads for advanced protection and mitigation capabilities.

KodeKloud

Azure Bastion

Securely access your VMs over a TLS/SSL connection without public IP address



01

Secure connections

As we are not using Public IPs to access the VMs, the connection is more secure than jump host approach

02

Eliminate port exposure

As we are accessing the VMs from the Azure Portal using Bastion, there is no need to expose RDP/SSH ports to the internet.

03

Centralization

With the capability to use across peered networks, we can deploy the Bastion host to the hub network and can be used to access any VMs in the peered networks securely.

KodeKloud

JIT access

Get just in time access to your VMs

01

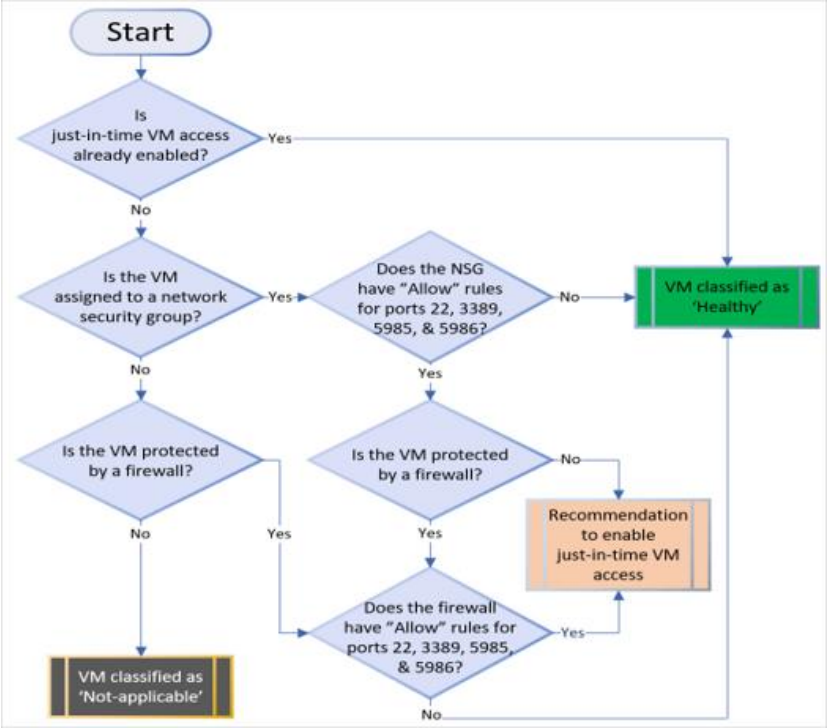
Lock inbound traffic

When you enable JIT, Microsoft Defender for Cloud will check if “deny all traffic” exist for the ports you selected. With the help of this rule, we are blocking access to the VM over the management ports to defend against attacks

02

Access when required

When you request access to the VM, the deny rule will be void for the selected period on the selected management ports. After the timeframe, the rules will be placed back, and access is restricted.



03

Plan

Requires you to purchase the Standard plan of Microsoft Defender for Cloud to use this feature.

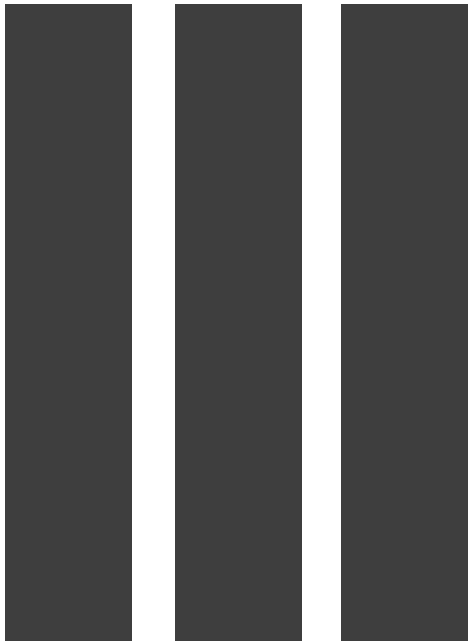
Scenario

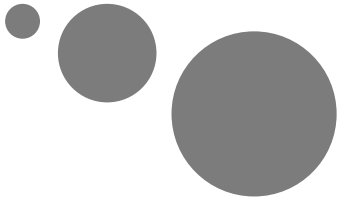
Vendetta Corp has following requirements:

- They need to connect their on-premises environment using a private connection to Azure
- If the private connection goes down, they need to have a failover path
- They need a central virtual network with following requirements:
  - All traffic to and from their Azure environment should be inspected before they are routed to the destination.
  - Users should be able to RDP/SSH without the need to manage IaaS servers or public IPs.
  - Should have two spoke that will host a three-tier application in WEU and WUS.
- The 3-tier application has following requirements:
  - All web requests should be inspected and need to be routed to the business logic
  - The business logic requests should be load balanced to the VMs on port 8080.
  - Requests from business logic VMs will be routed to SQL PaaS Database over a private connection
  - Users should be routed to their nearest deployment region based on the latency to WEU and WUS.
  - All traffic from FrontendSubnet should be denied on the databaseSubnet

KodeKloud

Module 4: Design a compute solution





Scenario

Vendetta Corp would like to use Azure AD as their identity and access management solution, and they have the following requirements:

Choose a compute solution

Virtual Machines

Infrastructure-as-a-service solution which will help you to create computers in the cloud.

App Service

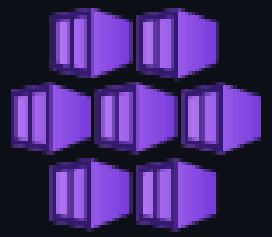
Platform-as-a-solution which is fully managed by Microsoft for hosting web applications, REST APIs, and mobile app backends.

Azure Batch

Compute solution for large scale parallel and HPC batch jobs

Container Instances

Easiest way to deploy containers in Azure without the need to manage VMs or container runtime

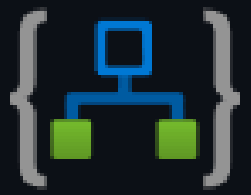


Kubernetes service

Fully managed Kubernetes cluster which can be used for container orchestration in Azure

Azure Functions

Small chunks of code which we call as functions can be triggered when there is an event

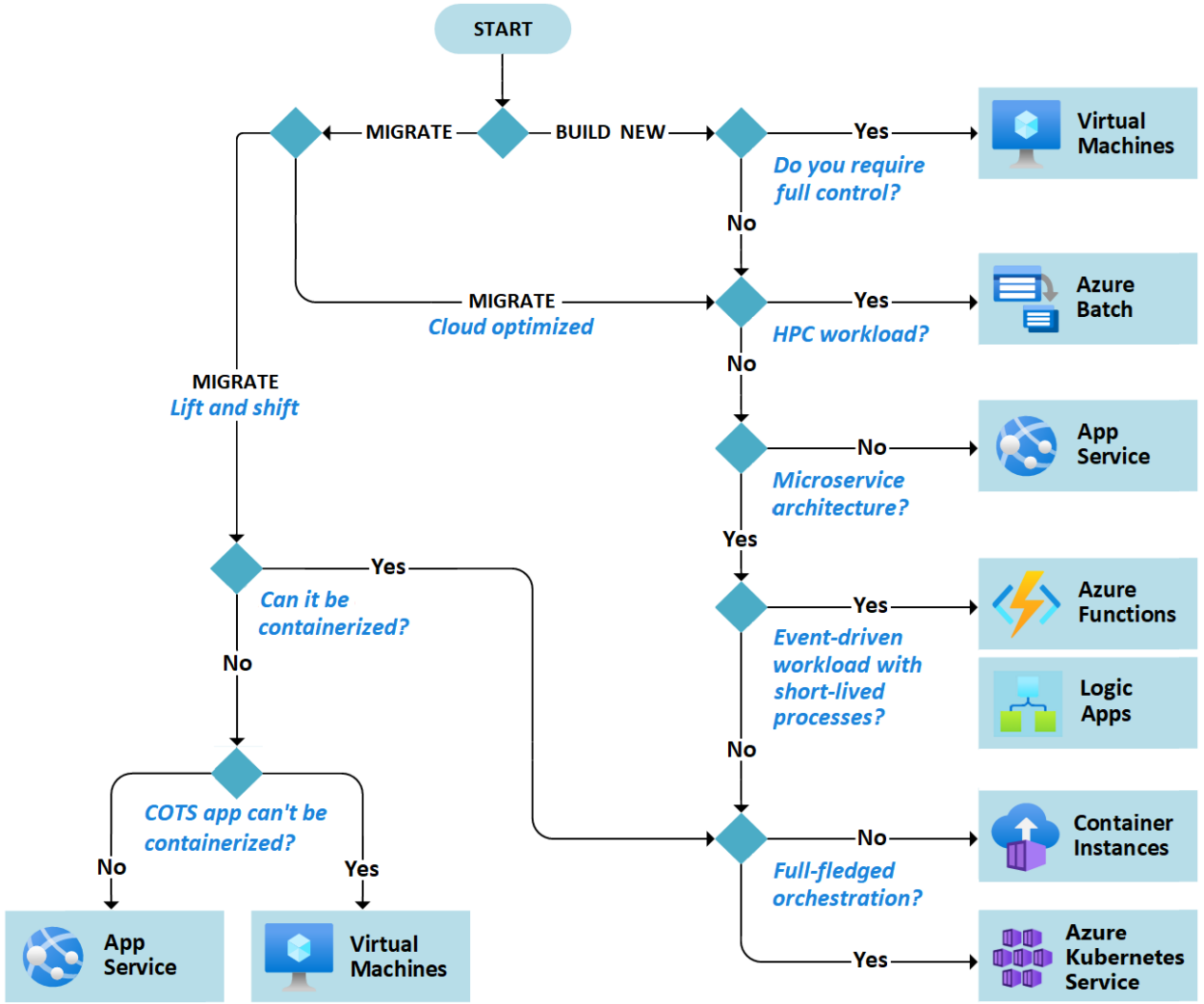


Logic Apps

Create and run cloud-based workflows

Choose a compute solution

Use the following flowchart as a starting point for choosing the compute solution for your application

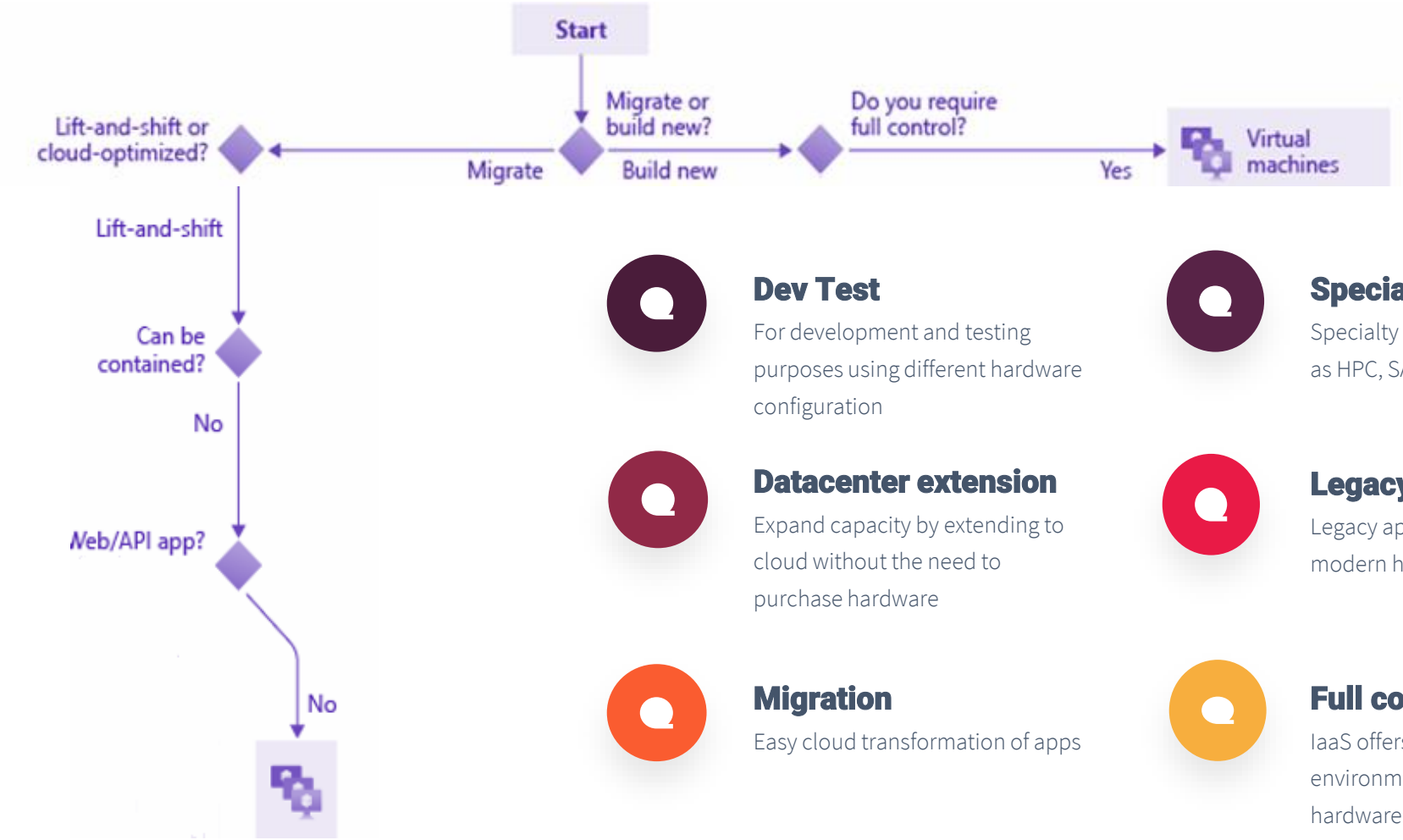


Source: *Microsoft documentation*

Design for virtual machines

When to select virtual machines?

Decide when to select virtual machine as the compute solution to host your application



Dev Test

For development and testing purposes using different hardware configuration

Specialty workloads

Specialty workload hosting such as HPC, SAP etc.

Datacenter extension

Expand capacity by extending to cloud without the need to purchase hardware

Legacy apps

Legacy apps can be run on modern hardware

Migration

Easy cloud transformation of apps

Full control

IaaS offers full control over the environment except the physical hardware owned by the cloud provider

Plan for virtual machines

Consider the following decision criteria when you plan to deploy virtual machines

- Start with network
- Location of the VM
- Operating system of the VM
- Pricing of the VM

- Naming convention for the VM
- Storage performance of the VM.
- Update and patch management
- Monitoring

Plan for virtual machine family

Based on the type of workload you are hosting; you need to pick the VM family that you need to deploy

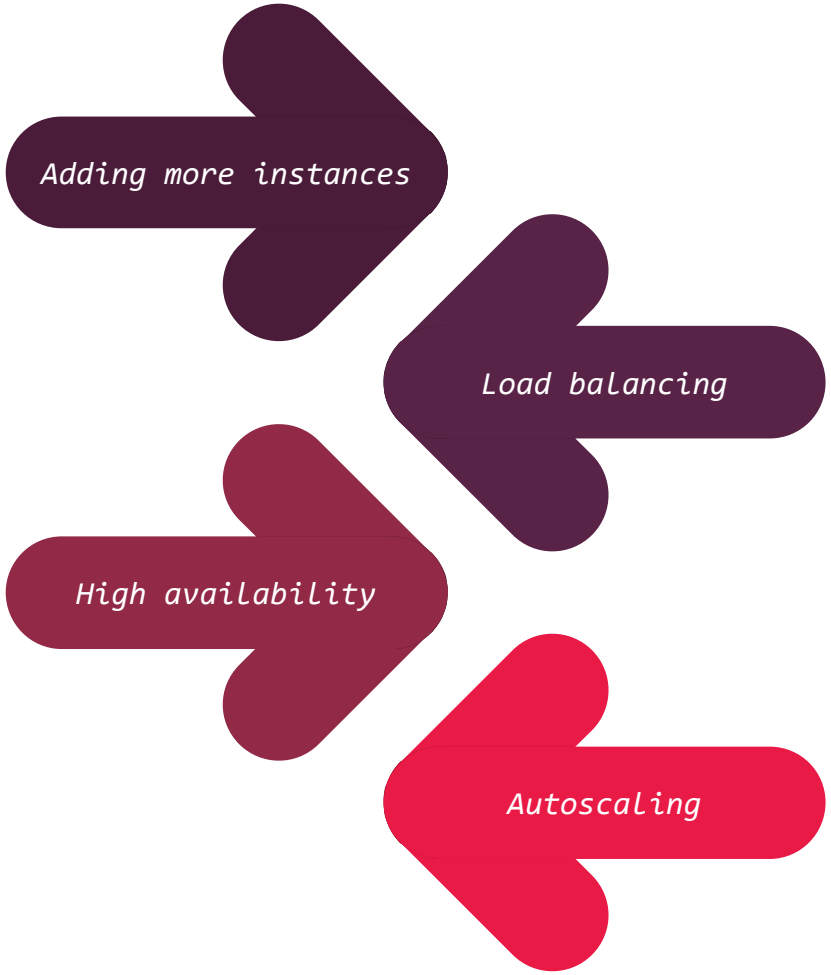
Type	Sizes	Targeted workloads
General Purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute optimized	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

Choose between VM and VMSS

Select whether you need to deploy your application in VMs or VMSS

- In VMs, we need to manually create and configure VMs.
- Manual process to add VMs as backend to load balancer
- Requires to create availability set or availability zones
- Autoscaling is not possible

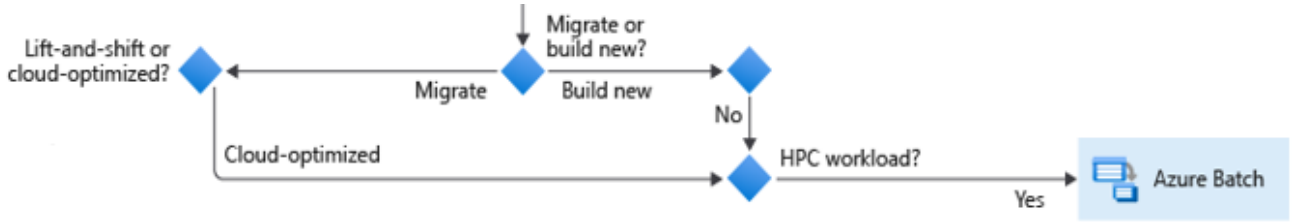


- VMSS relies on a central configuration and all instances will have same configuration
- Instances in VMSS are added to load balancer in a single configuration
- Instances can be automatically spread across availability zones or fault domains.
- Autoscaling can be done based on metrics or schedule

Design for Azure Batch

When to select Azure Batch solution?

Decide when to select Azure Batch as your compute solution



HPC scenarios

Any scenarios where we need to accomplish compute intensive tasks without the need to manage the infrastructure, we go for Azure Batch

Managing jobs

Jobs are the tasks that you are feeding to the Batch solution. We can create different pools of compute nodes based on the intensity of the task

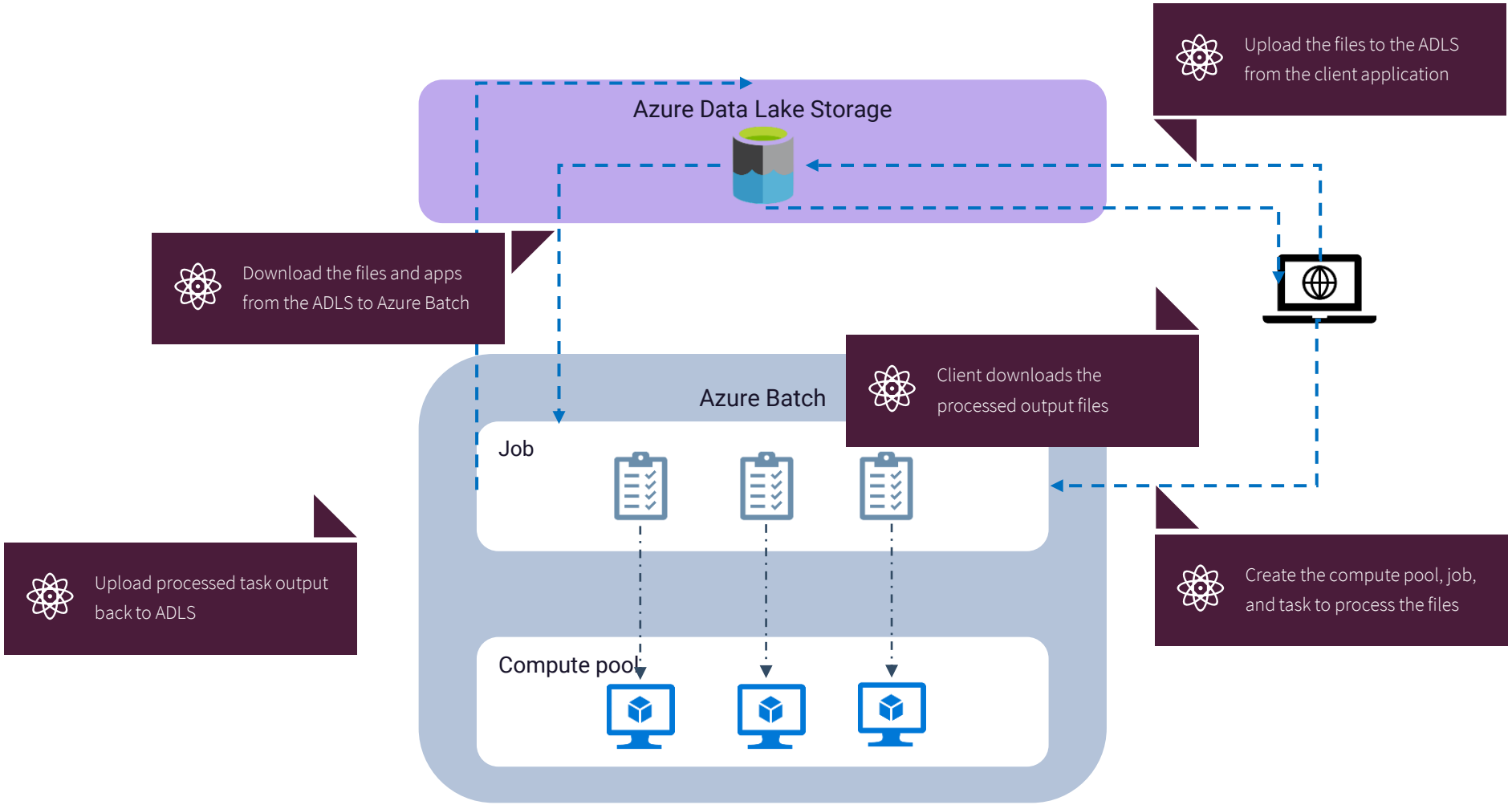
Install application

On Azure Batch we can install your own application and schedule your jobs to process on the provisioned compute nodes

KodeKloud

Working of Azure Batch

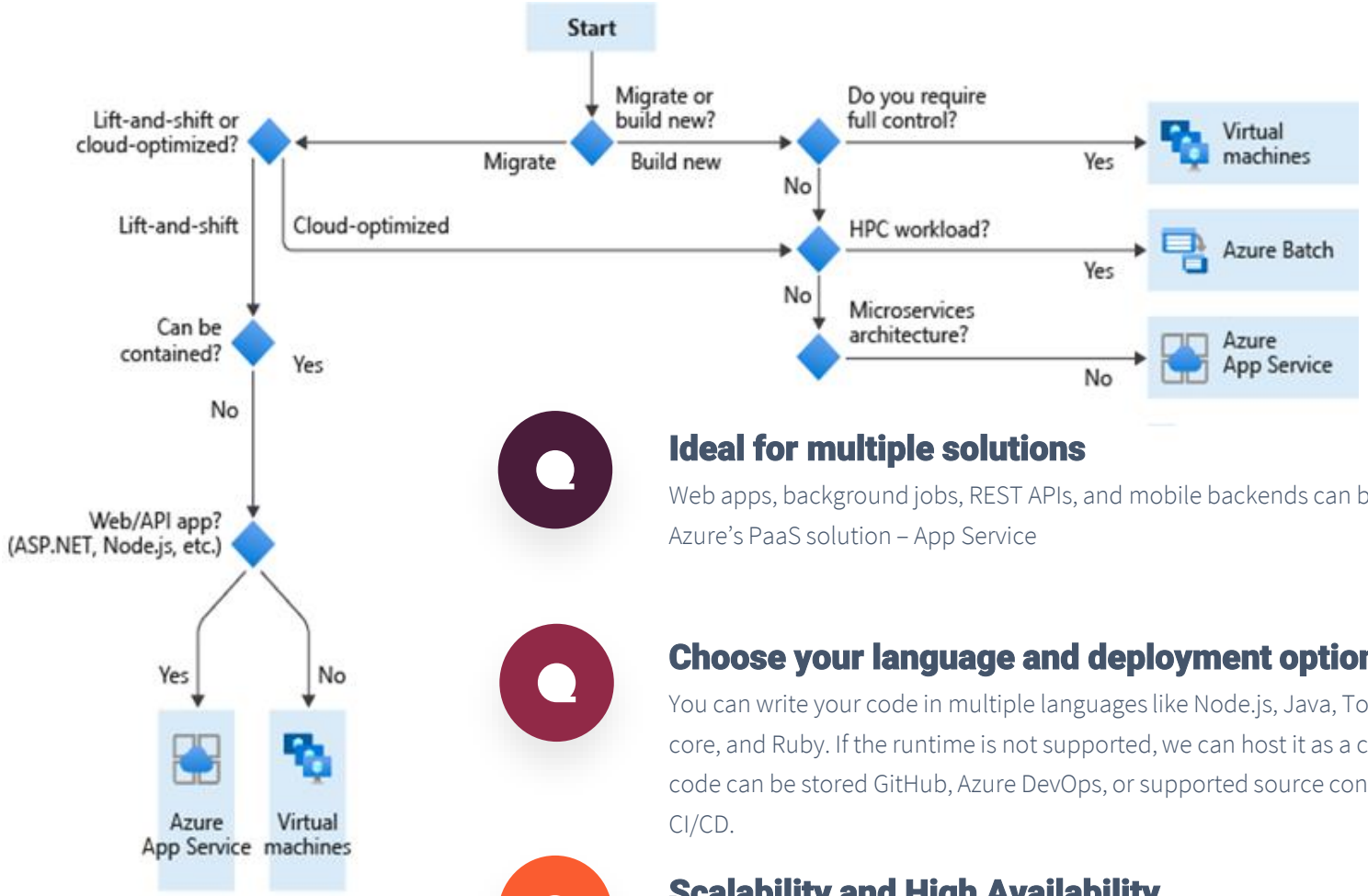
Learn how the data processing is done in Azure Batch



Design for Azure App Service solutions

When to select Azure App Service solution?

Decide when to select Azure App Service as your compute solution



Ideal for multiple solutions

Web apps, background jobs, REST APIs, and mobile backends can be hosted in Azure's PaaS solution – App Service

Choose your language and deployment options

You can write your code in multiple languages like Node.js, Java, Tomcat, PHP, .NET core, and Ruby. If the runtime is not supported, we can host it as a container. This code can be stored GitHub, Azure DevOps, or supported source control to set up CI/CD.

Scalability and High Availability

As this is a PaaS solution, infra management is done by Microsoft. Auto scaling is supported in Standard, Premium and Isolated tiers of App Service Plan.

Considerations

Keep these considerations in mind when you decide to use App Service as your compute solution

Sizing

Determine the correct App Service Plan tier which will help you understand the cost, scaling and features.

Support for built-in authentication

Integrate application with Microsoft, Google, Facebook and other social identities without the need to develop additional solution.

Use deployment slots

Deployment slot helps in promoting your tested staging code to production and roll back if needed easily.

Decide the type of app

If you are hosting backend for iOS or Android apps then use mobile backend. WebJobs can be used to run background jobs.

CI/CD

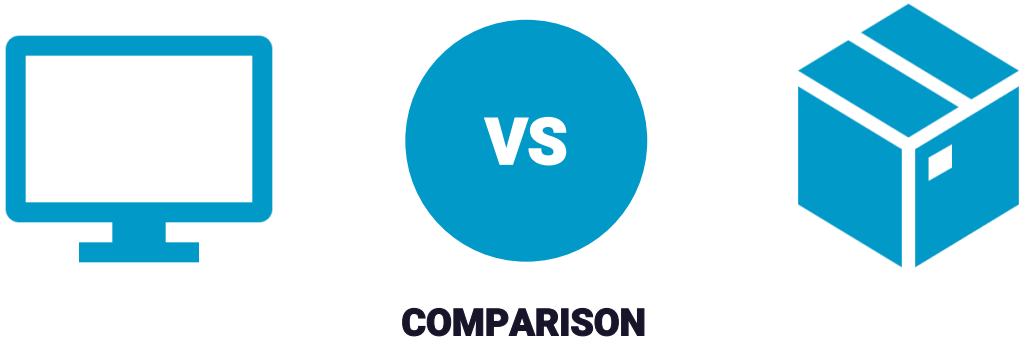
Integrate with your code repository to enable CI/CD

Design for Azure Container Instances solutions

Comparison of VM and containers

Understand the key differences between VM and containers

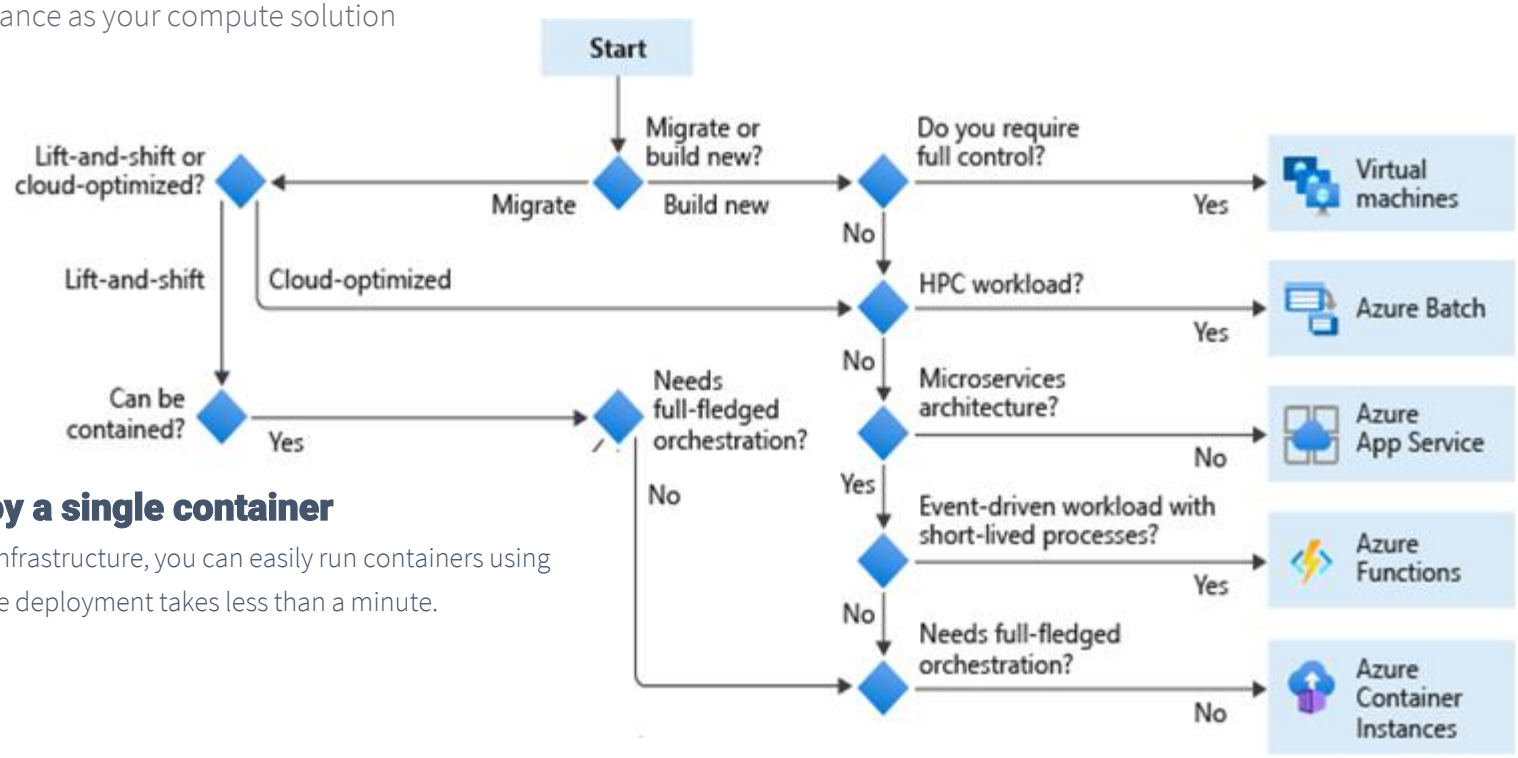
- Full isolation, deployed VMs are separated from other VMs on the host.
- Hosts a full-fledged operating system
- Deployed in cloud or on-premises using different deployment tools
- Virtual Hard disk is provisioned to store data
- VMs failover to another server or redeployed on a different host



- Lightweight isolation from other containers on the host and from the host itself
- Operating system's user mode portion is used
- Deployed using Docker
- Azure Disks or file share is used as persistent storage
- Orchestrators are used to recreate the containers

When to select Azure Container Instances solution?

Decide when to select Azure Container Instance as your compute solution



Easiest way to deploy a single container

Without the need to manage infrastructure, you can easily run containers using Azure Container Instances. The deployment takes less than a minute.

Container images

ACI supports Docker images, and these can be pulled from Docker Hub, Private Docker Hub, Private image registry, or integrate with Azure's native solution for storing images : Azure Container Registry.

Container groups

Container groups help you to deploy set of related containers on the same underlying host. This helps in lifecycle management and easy integration with other Azure services.

Considerations

Keep these considerations in mind while you design a solution with ACI

Pace of deployment

ACI fast, easy, and very convenient when you plan to run a container in Azure

Development and testing scenarios

Development teams can pack their container images and can easily test the image in ACI

Short lived processes

ACI is also ideal for short lived processes that are part of a workflow

Virtual Node

Due to the faster deployment time than VMs, ACI can be used as a virtual node in AKS bursting

Limitations

ACI doesn't offer any built-in load balancing like App Services or scalability. Also, this is not designed for microservices

Design for Azure Kubernetes Service

KodeKloud

Understand the basics of AKS

Let's quickly recap the basics we studied earlier

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

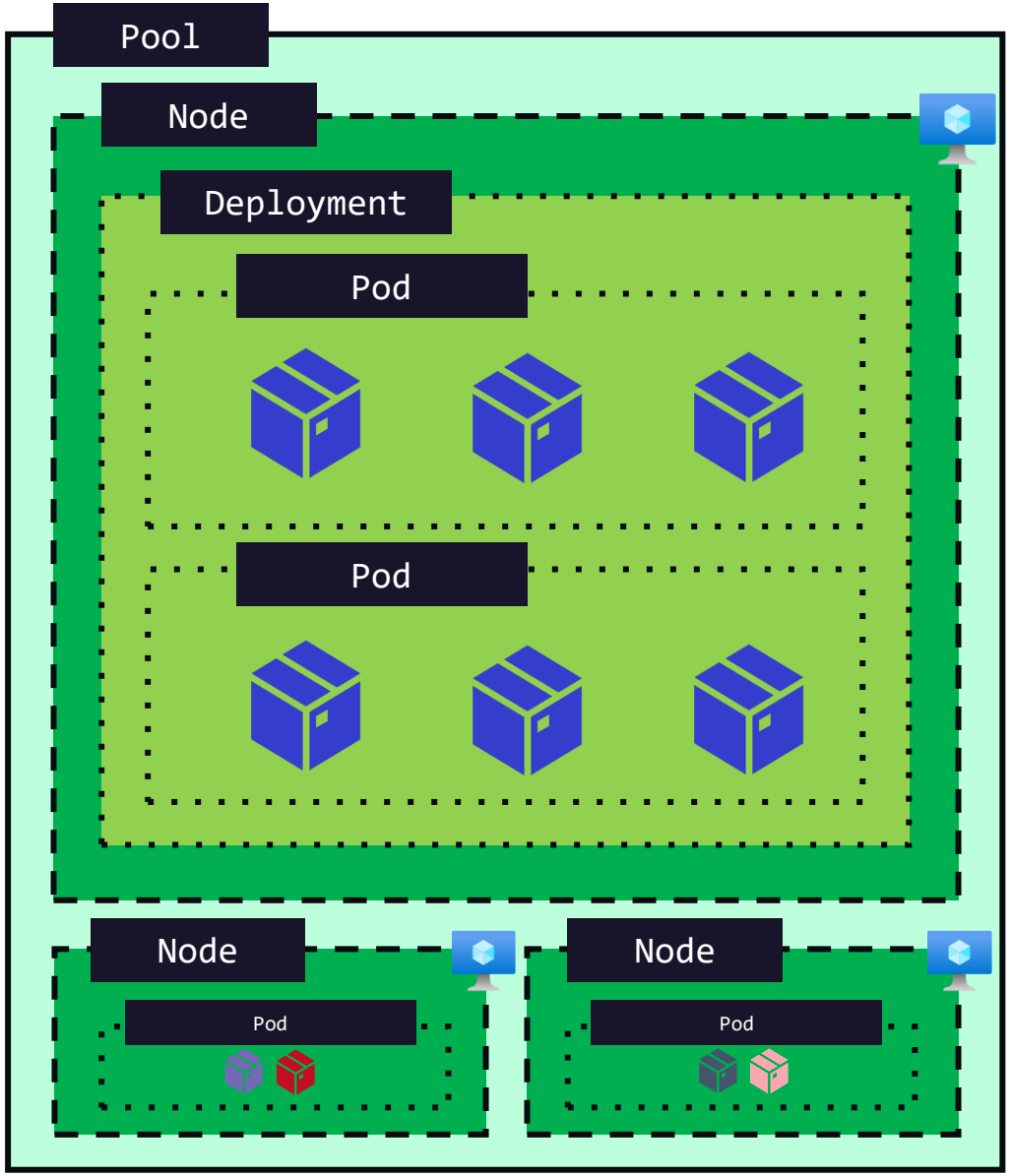
Smallest unit of deployment which is a collection of one or more containers representing a single instance of your application.

Deployment

Creates one or more identical replicas of your pod

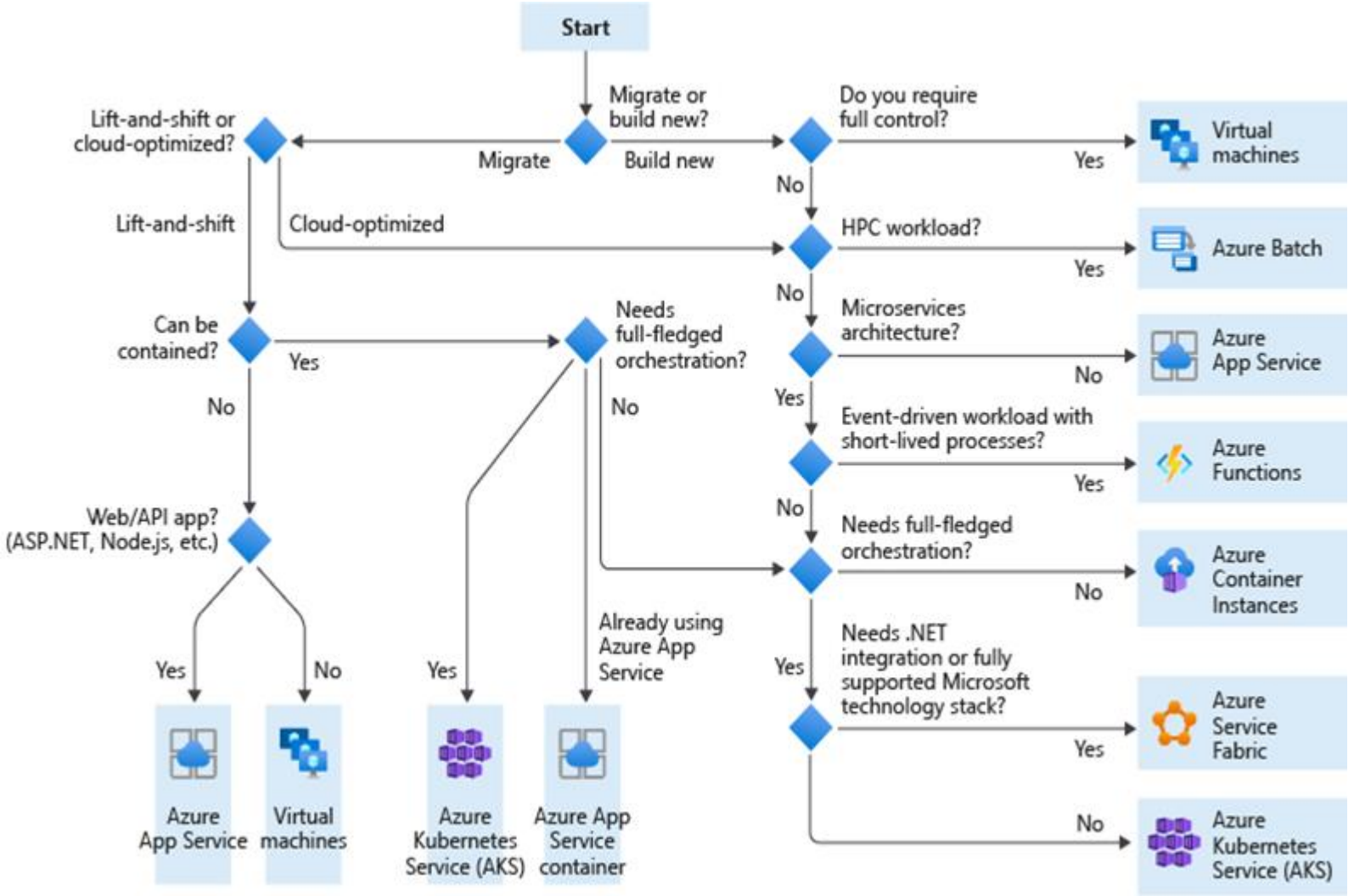
Manifest

YAML or JSON file used for deployment



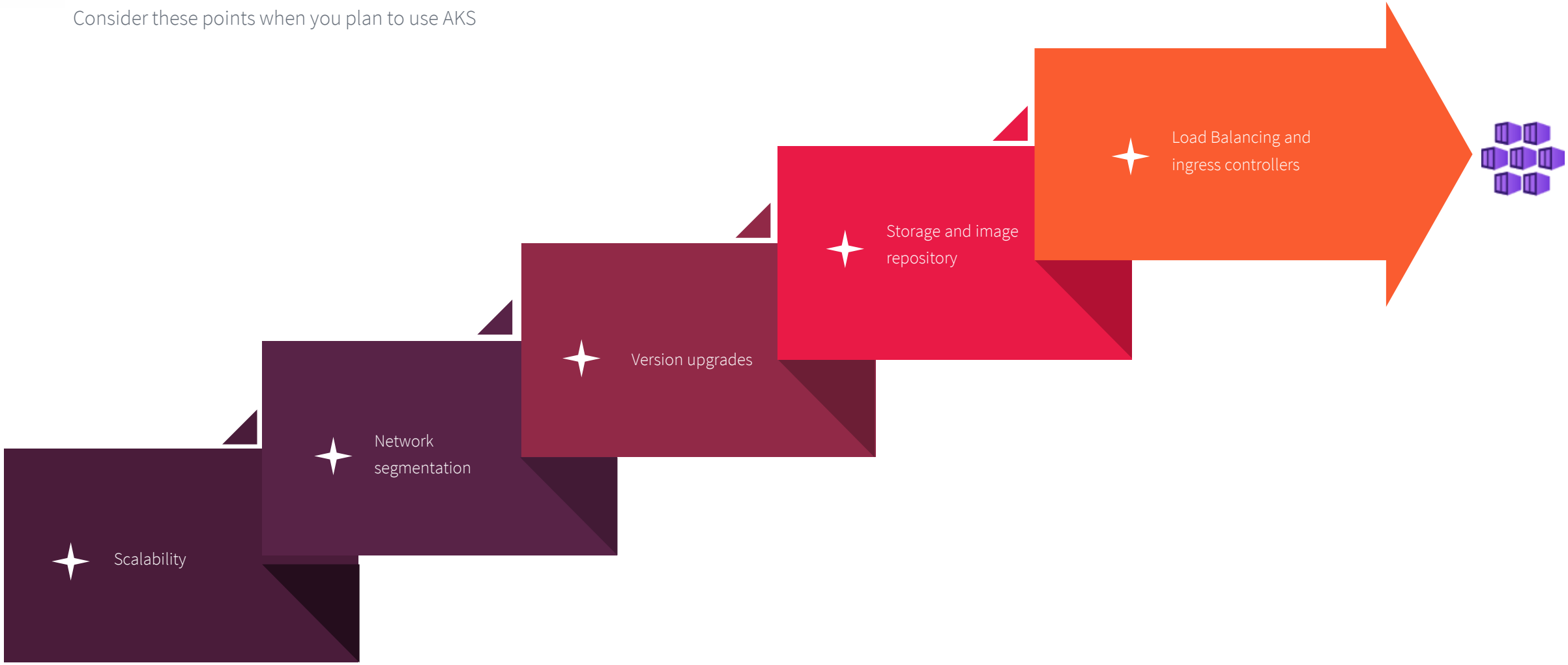
When to use AKS?

Review the flowchart and understand when should we use AKS



Considerations

Consider these points when you plan to use AKS

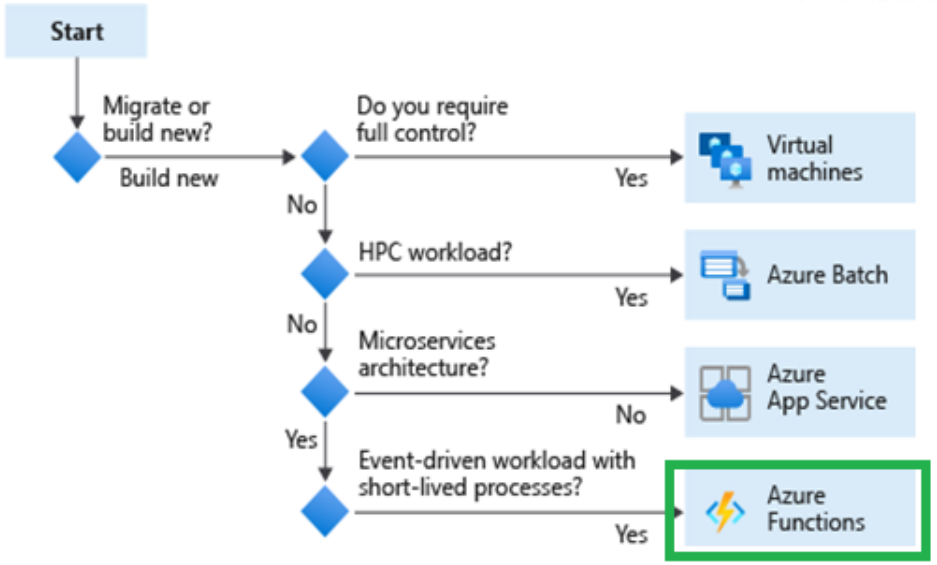


Design for Azure Functions

KodeKloud

When to use Azure Functions?

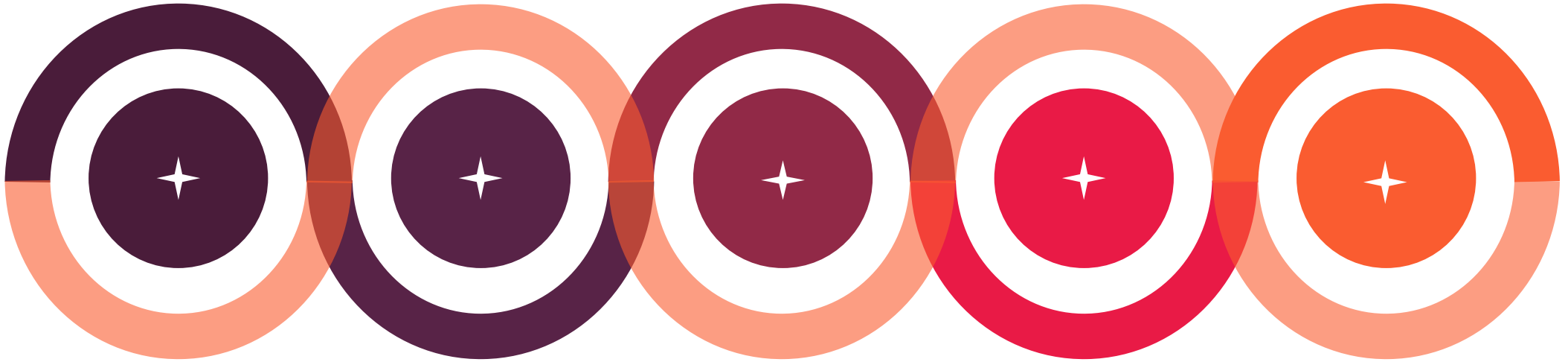
Review the flowchart and understand when should we use serverless functions



Write your application logic as code which can triggered as required.

Code reuse is promoted

Event-driven or can be triggered based on schedule



Supports microservices design

Scales easily based on consumption.
Also compatible with App Service Plans

Considerations

Keep these considerations in mind while you design a solution with ACI

Long running functions

Long running functions require more resources and it's not ideal in consumption model.

Durable functions

If you want to write stateful functions in Azure functions, we can use this extension

Performance

You can go with the Consumption plan, App Service Plan or a Premium plan

Scalability

Based on the billing model you select Azure will provide different scaling options.

Design defensive functions

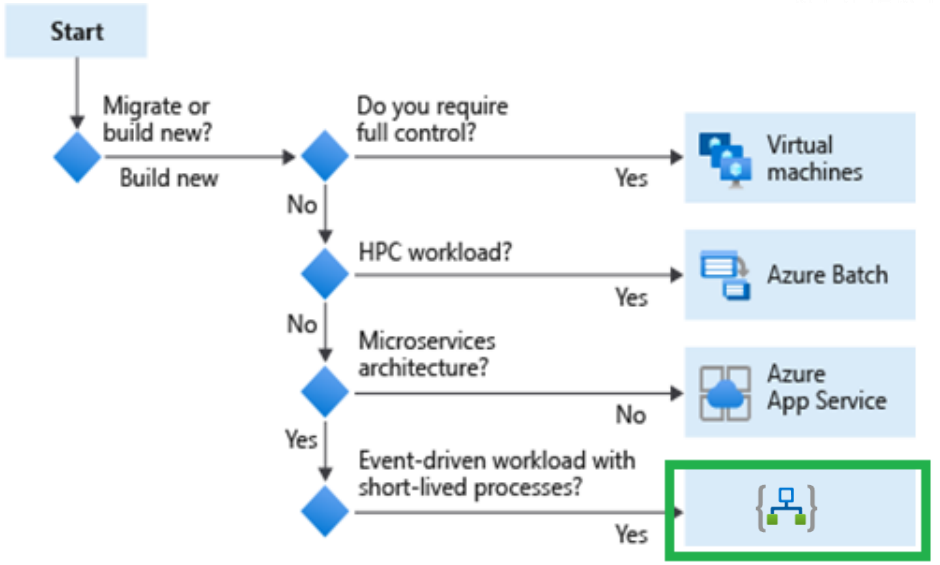
Implement exception handling in a way so that system will be able to continue from the previous failure point during next execution

Design for Azure Logic Apps

KodeKloud

When to use Azure Logic Apps?

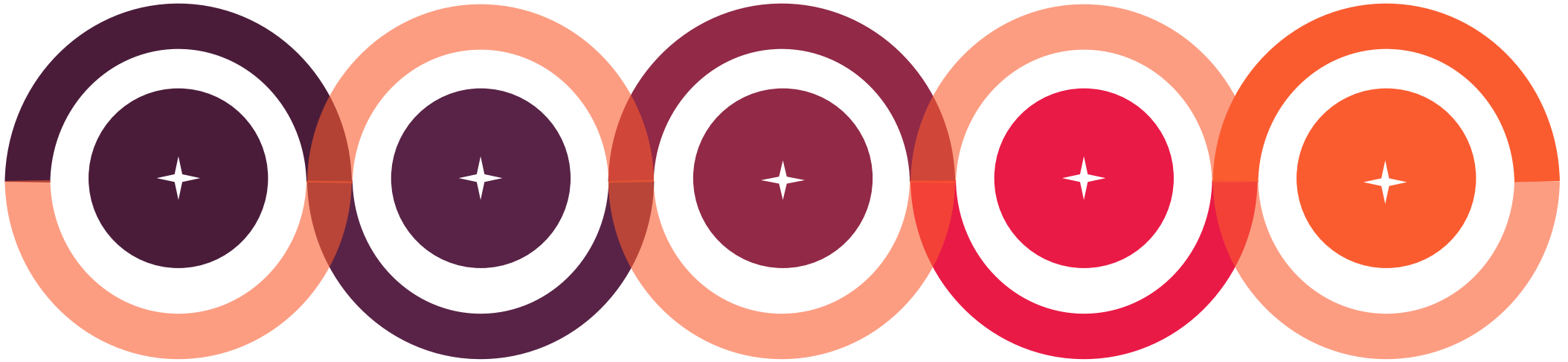
Review the flowchart and understand when should we use Logic Apps



Automatically forward emails in Office 365 to another user.

Whenever there is a tweet, analyze the sentiment and notify customer service

Set out of office emails automatically on weekend



Save all attachments in mail to OneDrive for Business

Post messages to Microsoft Teams channels

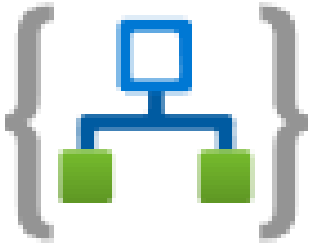
Comparison of Azure Functions and Azure Logic Apps

We have two approaches here, code first (Functions) and designer first (Logic Apps)

- Code first approach
- Develop functions by writing code
- Write code for any integrations that you want to do

VS

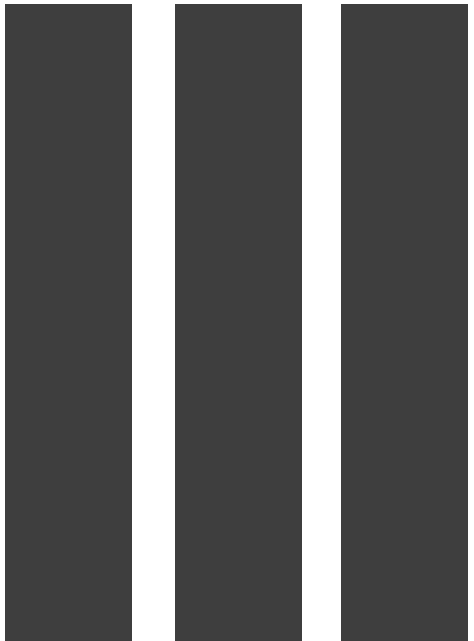
COMPARISON

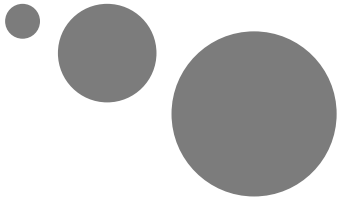


- Designer first approach
- Create workflows by designing using Azure Portal or config files
- Use built-in connectors or bring you own connectors to integrate with your services.

KodeKloud

Module 6: Design a nonrelational data storage solution





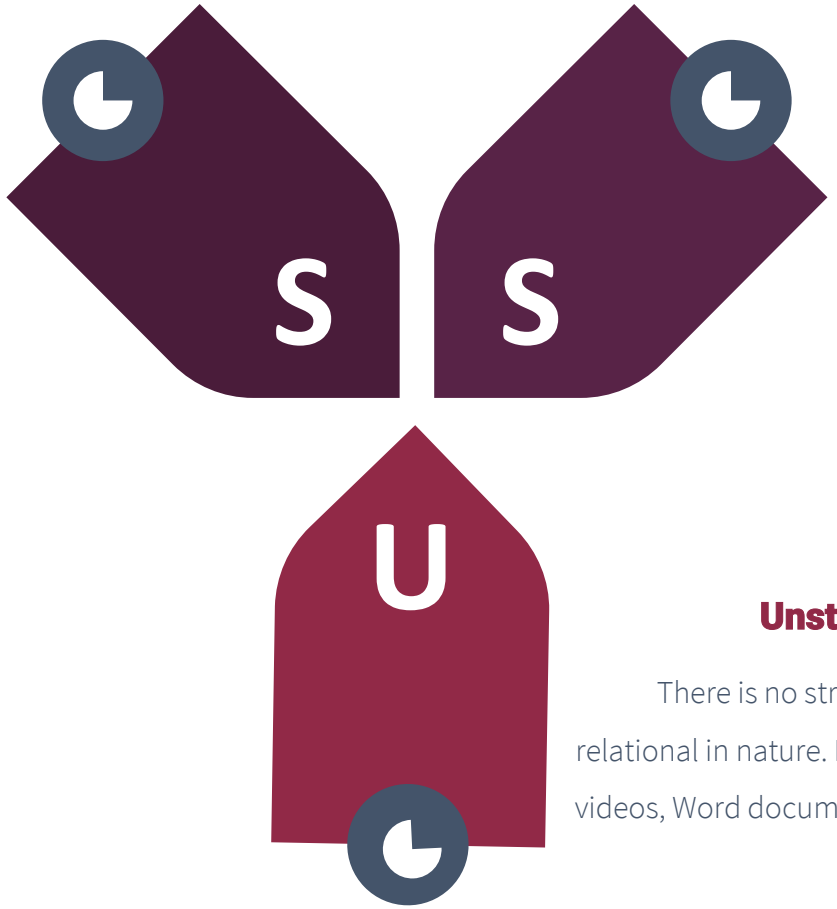
Design for data storage

Types of data

Determining the type of data will help you to choose the right data store

Structured data

Data stored will be in a database represented using rows and columns. This type of data includes relational data and has shared schema. Data in this format is used by applications like e-commerce websites for handling customer information and product catalog



Semi-structured data

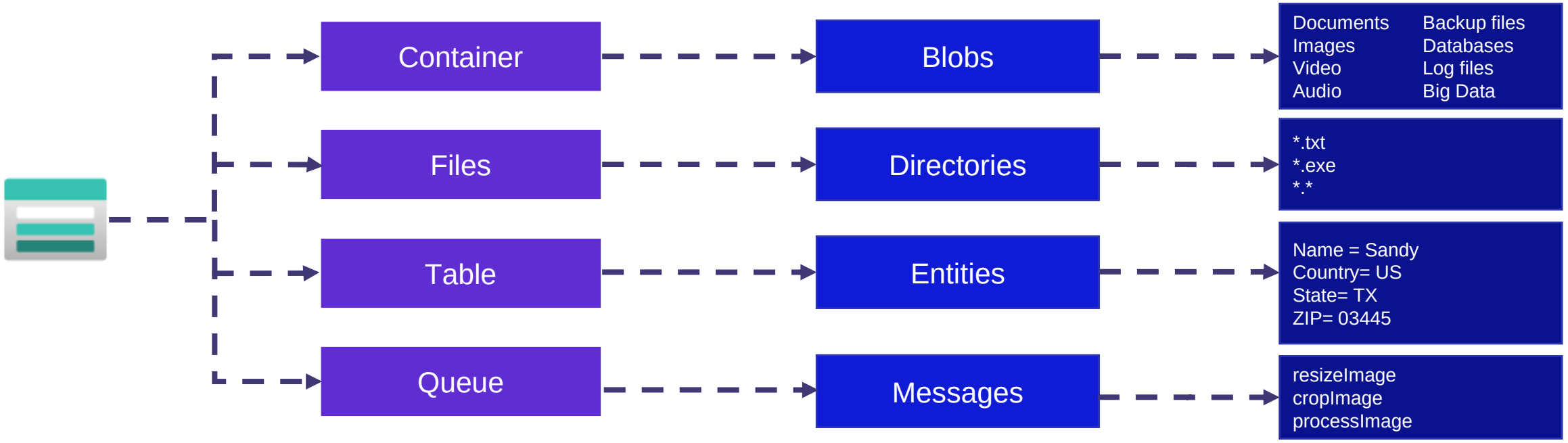
Data is structured; however, this is not in a relational format. With the help of embedded tags, the stored data is classified. JSON, XML, YAML are examples of semi-structured data

Unstructured data

There is no structure and is not relational in nature. Examples include videos, Word documents, , media files etc.

Storage services

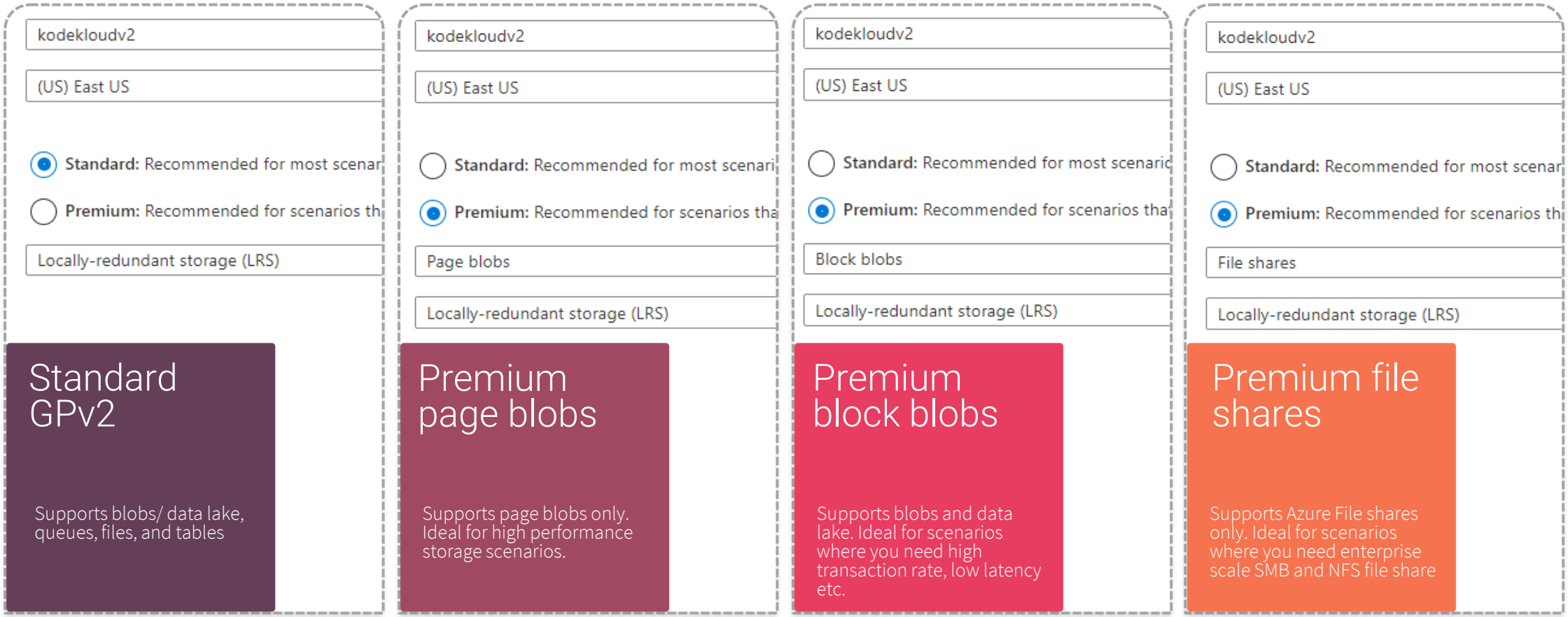
Storage services in available in Azure that you can choose based on the type of data you want to store



Design for Azure storage accounts

Choose the storage account type

Storage account type is determined based on the type of data you want to store and usage scenarios



KodeKloud

Plan for Azure Storage

Consider the following key points when you plan for Azure storage

Location

Check if the storage SKU is available in the region you selected. Also ensure that you have storage account deployed closer to your users to avoid latency

Replication

Plan your replication strategy based on the durability and SLA required by your application. Ensure that the replication is available in the selected region.

Compliance

Ensure that you meet the data residency and encryption requirements.

Management overhead

Creating and maintaining storage accounts require management overhead, plan accordingly.

Cost

Number of transactions, performance tier, replication, access tier are some of the factors affecting cost

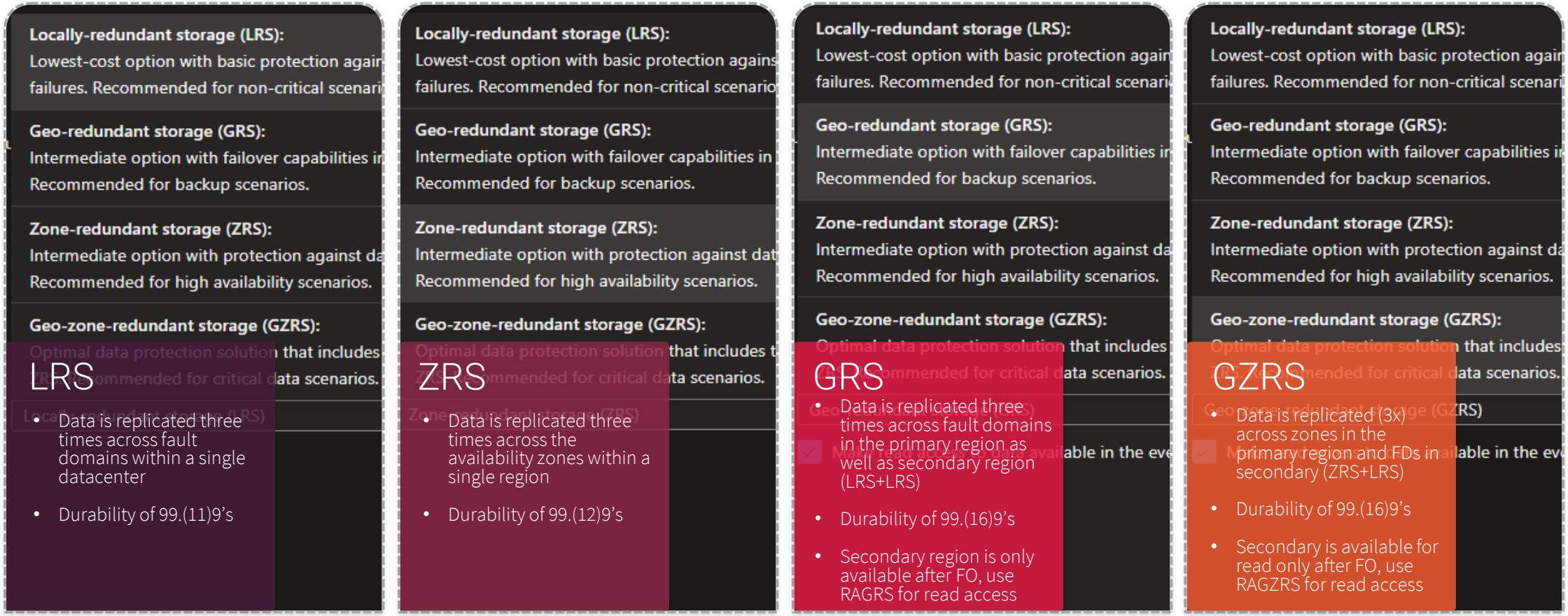
Security

Plan for security with the help of access management tools.

Design for data redundancy

Choose the storage replication

Replication strategy is selected based on SLA, durability and cost



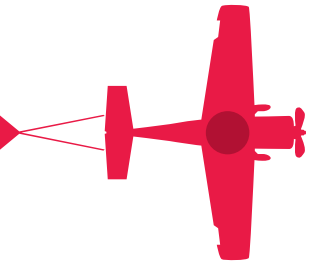
Design for Azure blob storage

Choose the storage access tier

Access tiers can be used to optimize the cost of the storage account based on how frequent the data is accessed

Access Tier	Data storage cost	Retrieval Cost	Storage Duration	Use cases
Premium	High	Lowest	N/A	• High IOPS and throughput
Standard Hot	Medium	Low	N/A	• Ideal for data that is frequently accessed • Data staged for processing
Standard Cool	Low	Medium	> 30 days	• Short-term backup • Older media infrequently viewed • Large data sets
Standard Archive	Lowest	High	> 180 days	• Long-term backup • Original (raw) data • Compliance or archival data

Use Lifecycle Management for blobs to automatically transition blobs from one tier to another based on last modified date. Eventually, we will be able to delete the blobs after 'n' number of days



Requirements for Azure blob immutable storage

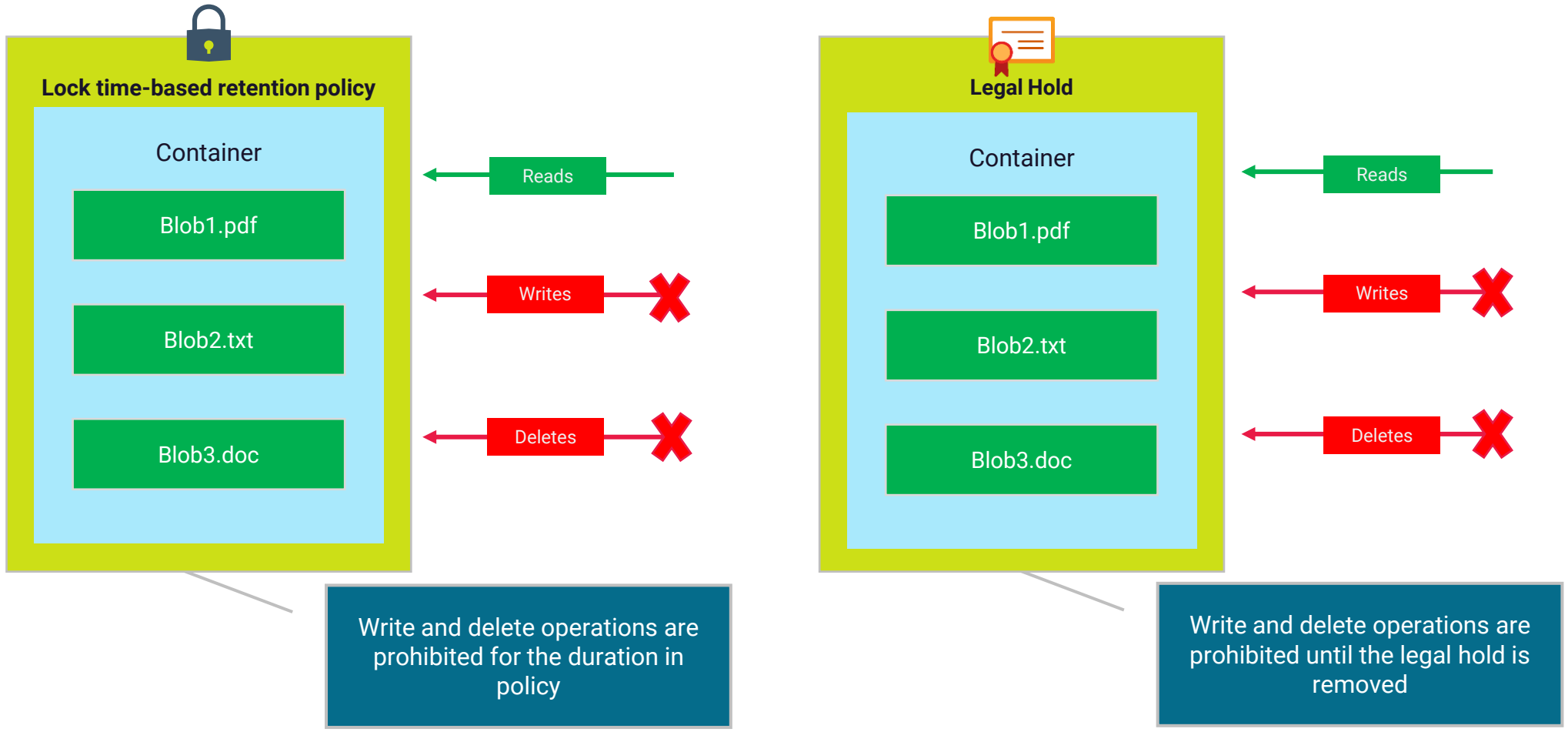
Store business critical data in Azure Blob storage in a WORM format (Write Once, Read Many)

Container level policies are applied and audit logs are available

All existing and new data is under the scope of policy

Requirements for Azure blob immutable storage

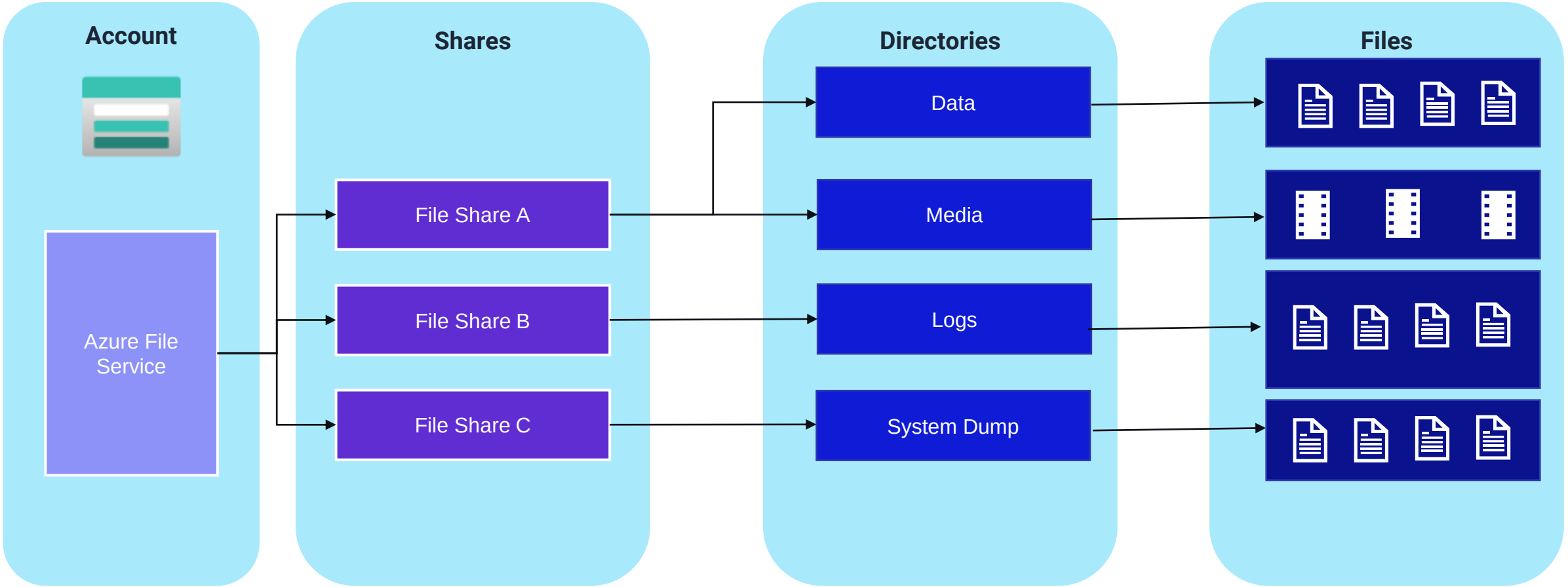
Store business critical data in Azure Blob storage in a WORM format (Write Once, Read Many)



Design for Azure Files

Azure Files

Create and mount enterprise grade file shares hosted in cloud



Accessing file shares

File shares can be accessed using the following methods:

- **Direct mounting**

  Using the SMB protocol, we can directly mount the file share to Windows, Linux and macOS computers. As this a cloud managed file share, there is no need to manage file servers or disks.

- **Azure File Sync**

  With Azure File Sync we can transform our on-premises Windows Servers into a cache of your Azure File Share. This will help you to centralize your file shares.

Performance levels

Performance levels are selected based on the performance you need and cost that you can afford

- **Standard**

  Uses HDD to store data and the latency will be double digit when calculated in milliseconds. Offers IOPS up to 10K and bandwidth of 300 MB/s. Cost will be low due to the lower performance metrics.

- **Premium**

  Uses SSD to store data and the latency will be single digit when calculated in milliseconds. Offers IOPS up to 100K and bandwidth of 5 GB/s. In terms of cost, Premium is an expensive choice and is currently available in ZRS only (selected regions)

Storage tiers

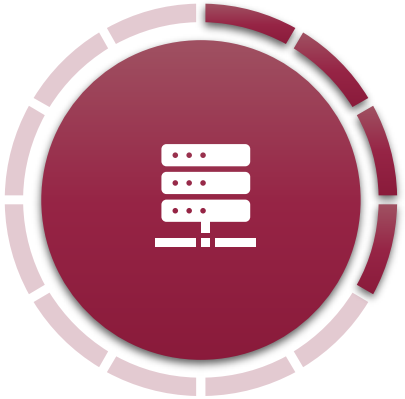
Use the access tier to determine the performance and to optimize the cost

Premium

SSD drives which provides low latency and high performance which is important for IO intensive workloads. Premium file shares can be mounted using the SMB and NFS protocols

Transaction optimized

Used in scenarios where workloads are transaction heavy and at the same time doesn't require the same level of latency offered by Premium file shares. This tier uses HDD to store data



Hot

General purpose file shares, ideal for small to medium file shares used by teams to share files. Hot tier used standard performance tier for storing data

Cool

Ideal for archival scenarios and is cost effective compared to Hot tier. Cold tier also uses standard performance tier.

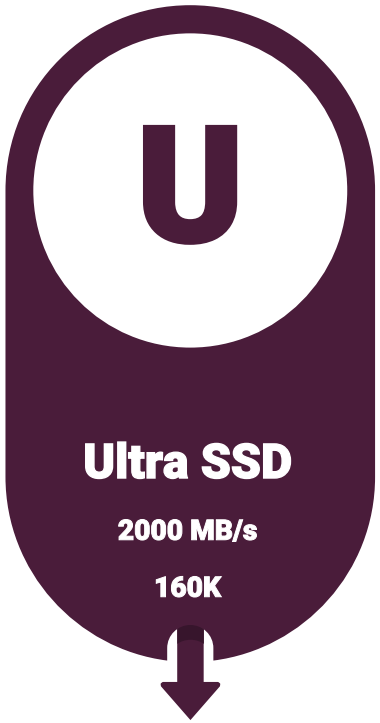
Comparing Blob Storage, Azure Files, and Azure NetApp files

Azure Blob Storage	Azure Files	Azure NetApp files
Ideal for large scale read-heavy sequential access workloads where data is ingested once and modified later. Lowest cost of ownership and zero to low maintenance	Highly available file share service which is best for random access workloads. NFS offers full POSIX FS support and can be used as persistent storage for containers in ACI and AKS.	Fully managed file share in the cloud powered by NetApp with advanced management abilities. Ideal for random access workloads which requires multiple protocol support and data protection features
NFS 3.0, REST API, ADLS GEN2	SMB, NFS 4.1 (No interoperability)	NFS 3.0, NFS 4.1, SMB
Up to 20K IOPS and up to 100 GB/s throughput	Up to 100K IOPS and up to 80 GB/s throughput	Up to 460K IOPS and up to 36 GB/s throughput

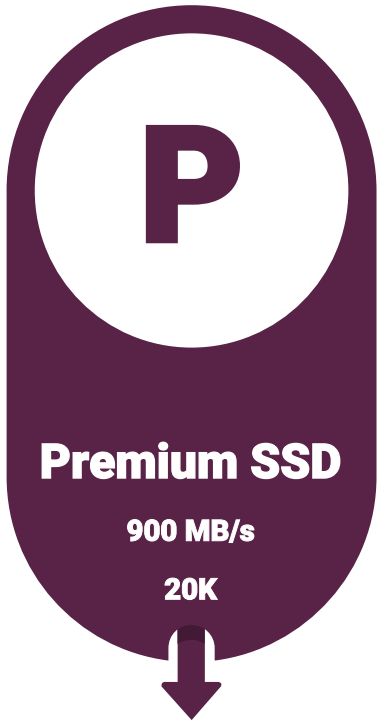
Design for Azure disks

Azure Disks types

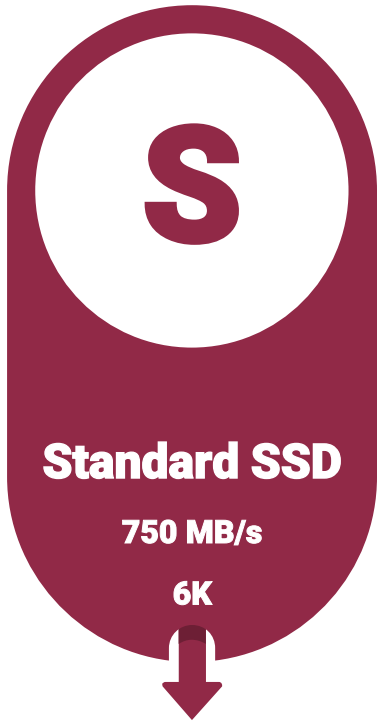
Select the type of disk based on the IOPS and throughput requirements



Ideal for heavy IO intensive workloads like SAP HANA, or transaction heavy databases like Oracle, SQL etc.



Performance sensitive workloads

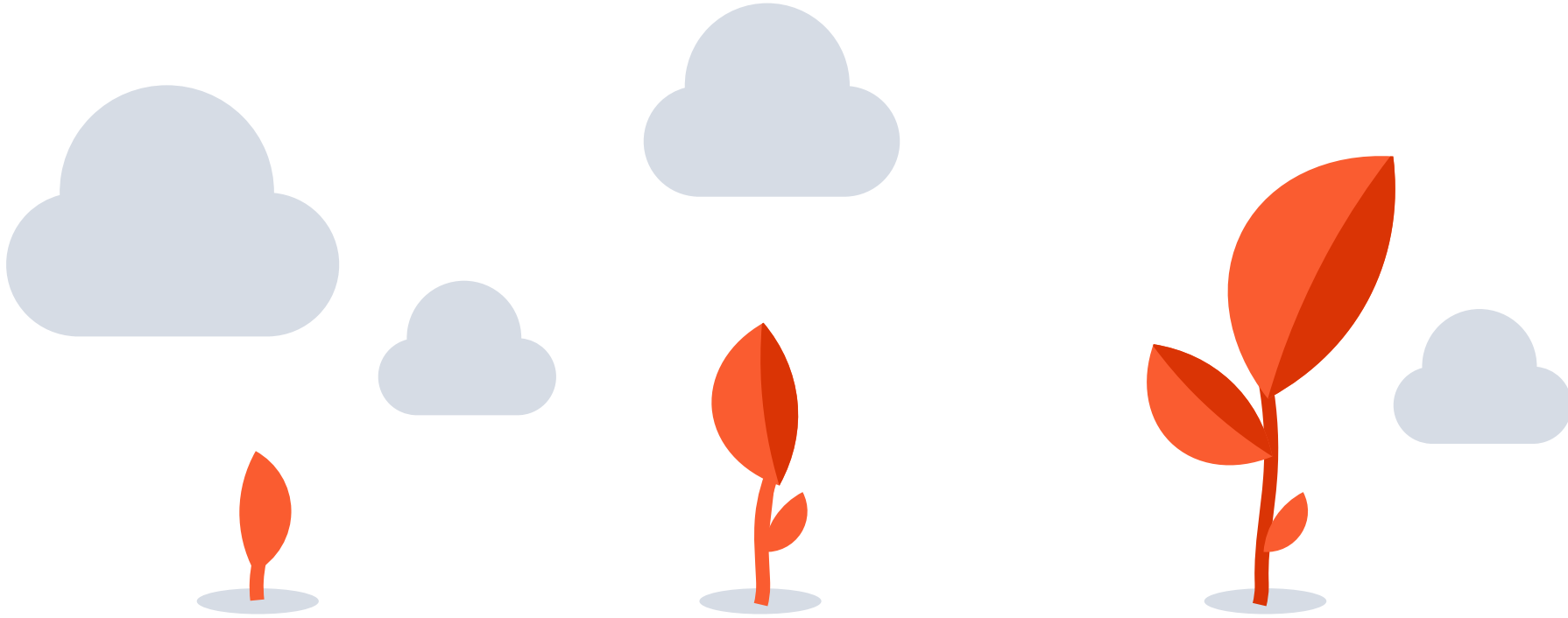


Webservers, medium transaction workloads

Backup, non-critical workloads, dev/test workloads

Enhance performance using disk caching

Optimize read and write operations to the VHDs using disk caching feature



None

Recommended to use with write-only and write-heavy disks

Read-only

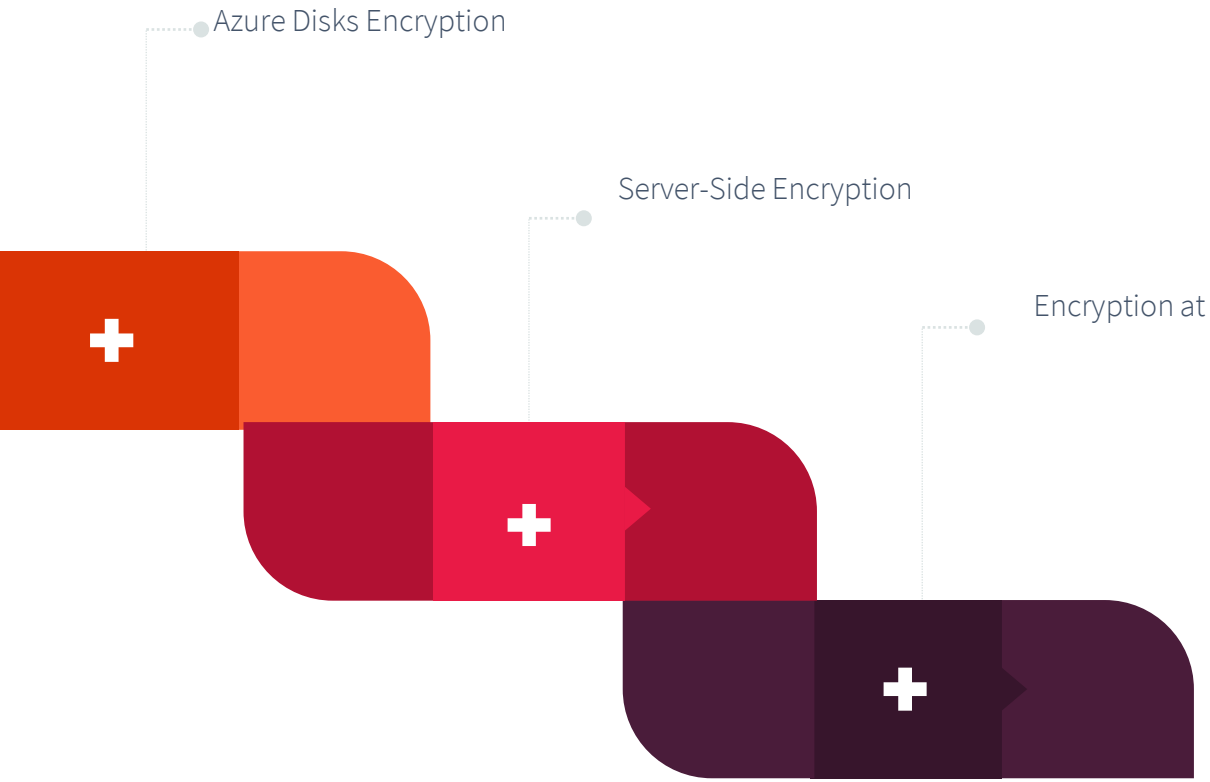
Low read latency and high read IOPS and throughput

Read-write

Ideal if your application requires to handle writing of cached data to persistent disks

Securing data disks

Azure offers multiple encryption strategies to encrypt the data stored in data disks



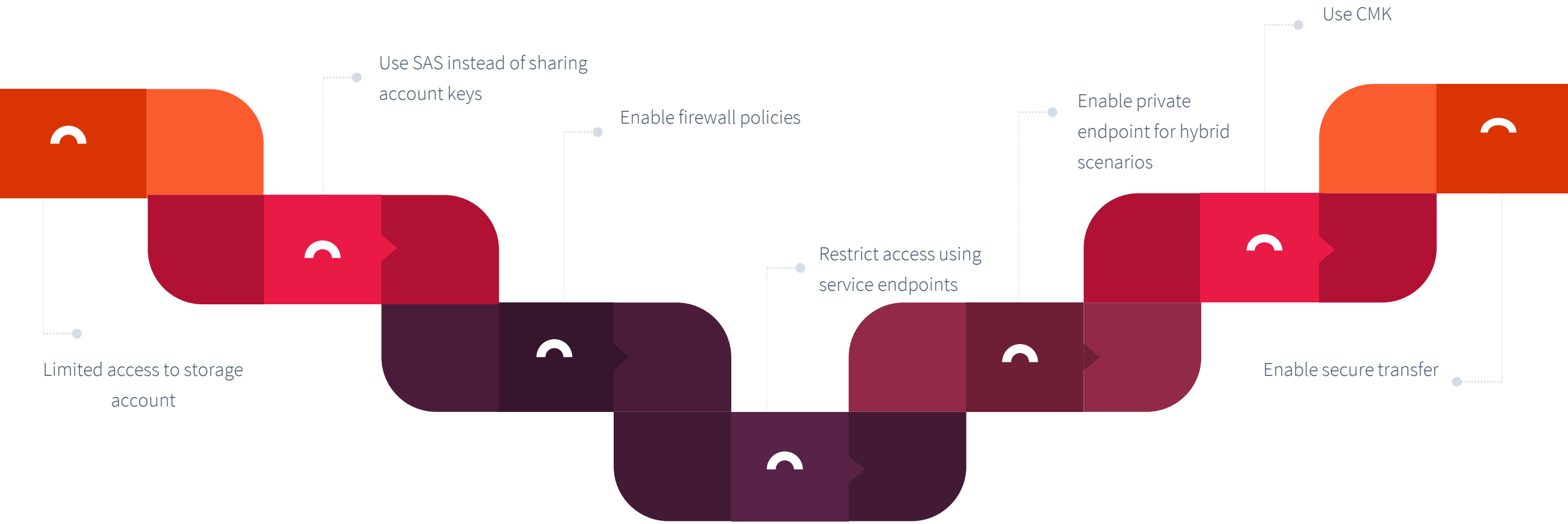
- With the help of ADE, we can encrypt the virtual machines virtual hard disk. For Windows encryption is done using BitLocker and for Linux dm-crypt is used.
- SSE ensures that all data is encrypted before it's written to the Azure Storage account. If someone tries to access these disks from the datacenter, they will not be able to read.
- Encryption at host ensures that the data stored on the VM host is encrypted at rest and flows as encrypted to the storage service

Design for storage security

KodeKloud

Storage Security – Best practices

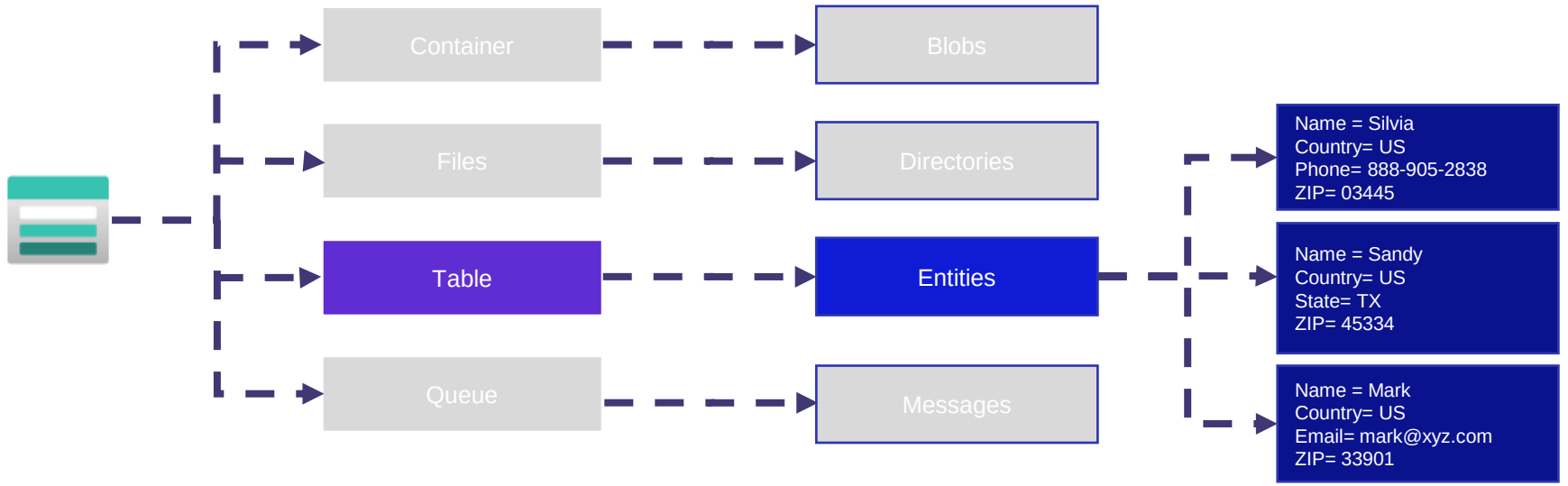
Follow these security best practices while designing storage accounts in Azure



Design for Cosmos DB and tables

Table Storage

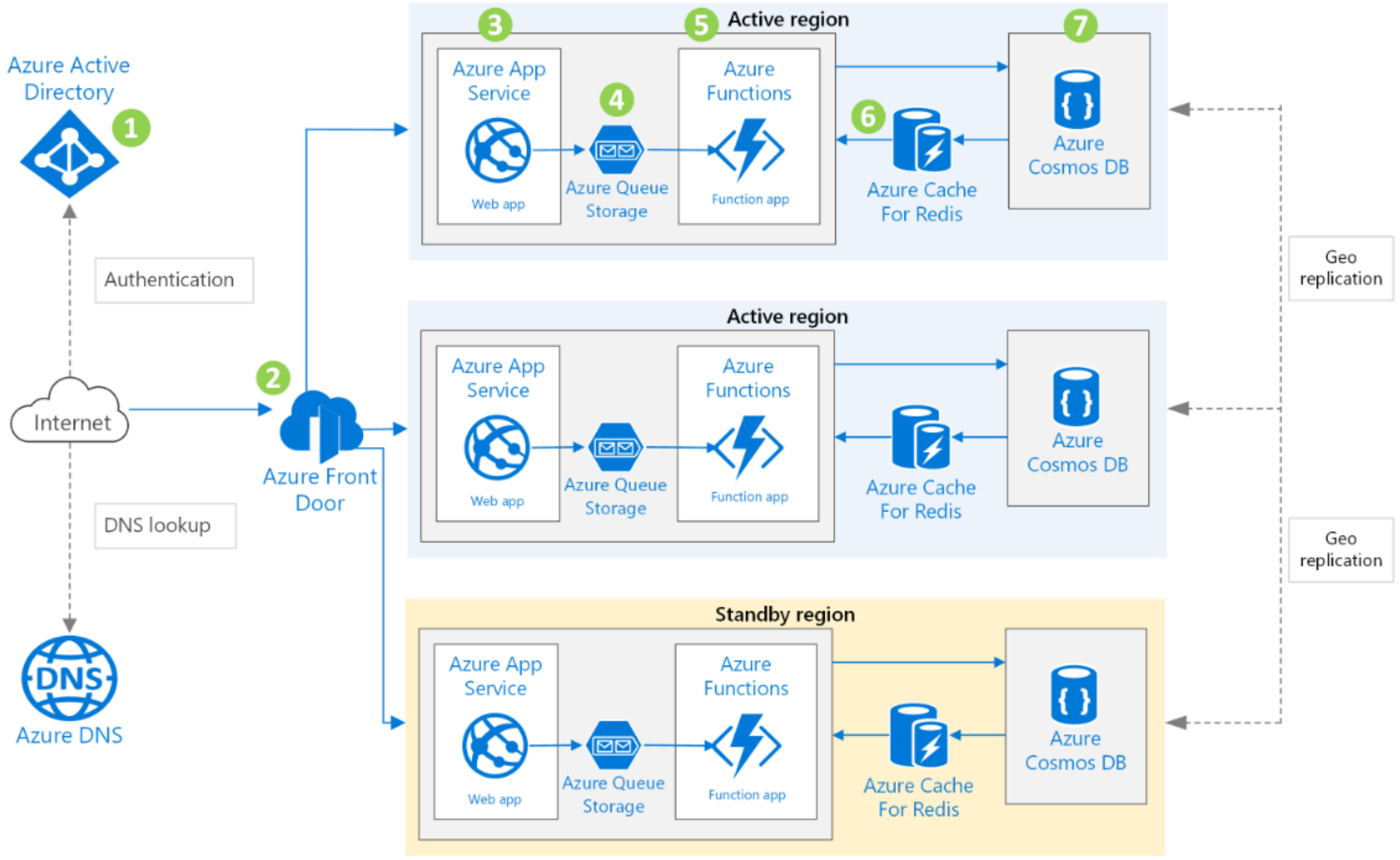
Table Storage stores NoSQL data in the cloud



- Storing large amounts of data which can be used web applications
- With the help of clustered index, you can query data easily
- Storing datasets that doesn't require complex joins, foreign keys or stored procedures
- Fast and cost effective

When to use Azure Cosmos DB?

A fully managed NoSQL datastore in the cloud which can fulfill any modern application data requirements



- Automatic and instant scalability
- Enterprise grade security and SLA of 99.999%
- Multi-region replication and failover.
- SDK and Open-source APIs available
- Fully platform managed solution, so there is no need for infrastructure management

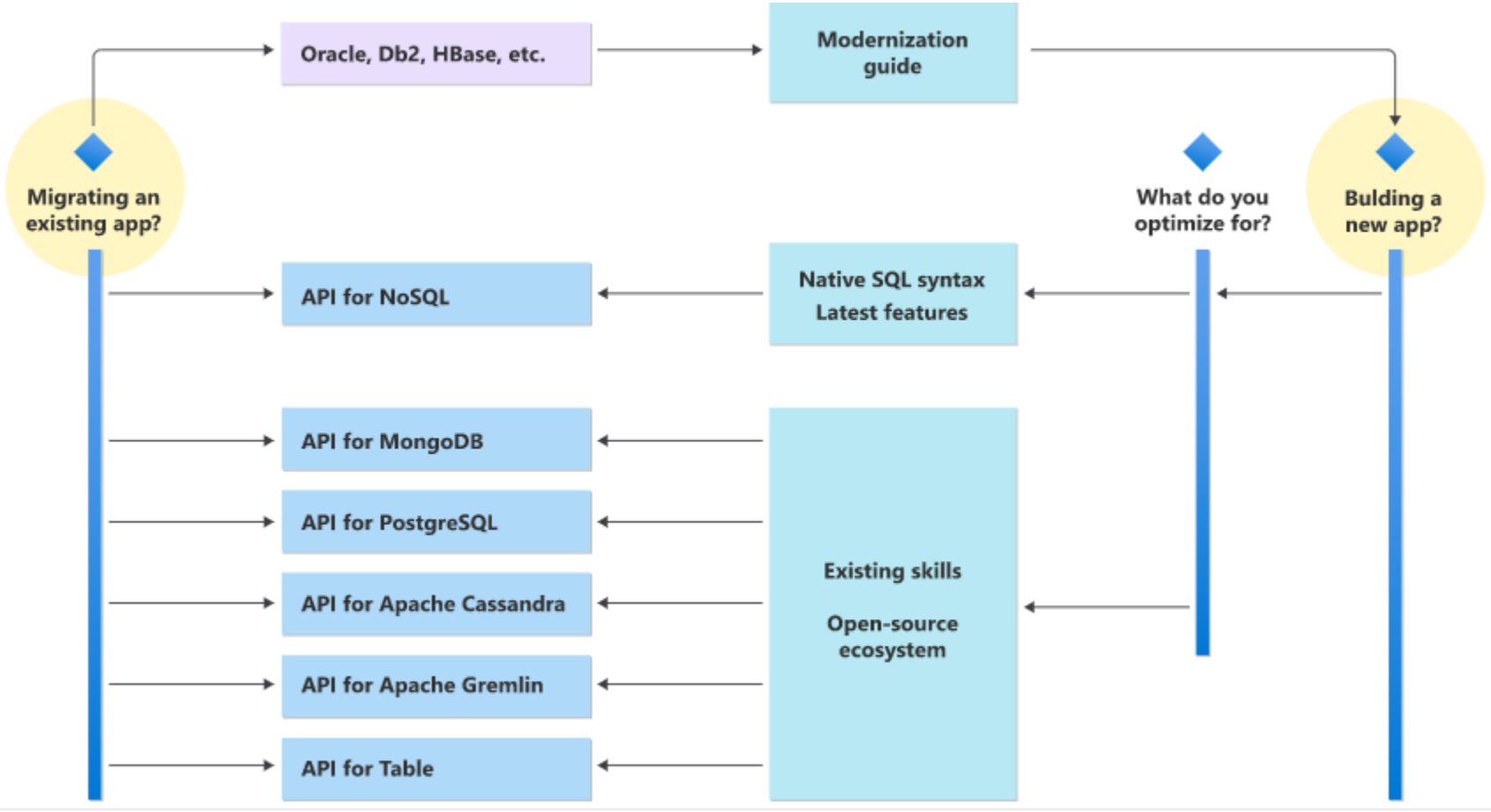
Benefits of moving to Cosmos DB

Migrating from Table Storage to Azure Cosmos DB offers following benefits

Benefit	Table Storage	Cosmos DB
Latency	Fast, but no upper bounds on latency	Offers single-digit millisecond latency
Throughput	Variable throughput	Dedicated throughput
Global distribution	Single region and can be expanded using GRS or GZRS	Turnkey global distribution from one region to 30+ regions
Indexing	Only primary index on PartitionKey and RowKey	Automatic and complete indexing for all properties
Query	Using index of PK and RK	Leverage automatic indexing for faster queries
Consistency	Strong within primary region	Five well defined consistency levels
Pricing	Consumption based	Consumption based and provisioned capacity model
SLAs	99.99% availability	99.99% (for single region accounts and all multi-region accounts with relaxed consistency) 99.999% read availability on all multi-region database accounts.

Choosing Cosmos DB API

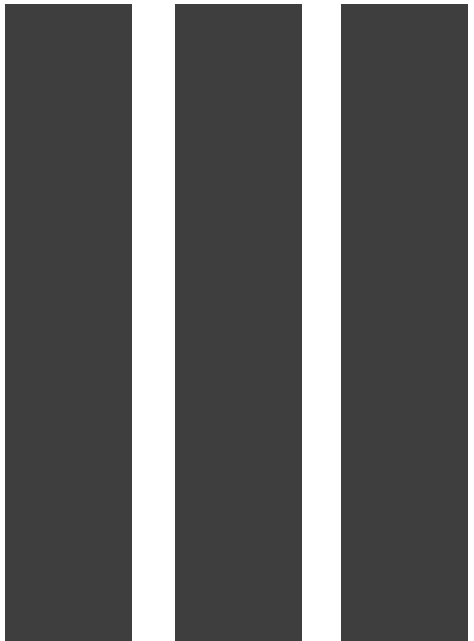
Cosmos DB offers six APIs : NoSQL, MongoDB, PostgreSQL, Apache Cassandra, Apache Gremlin, and Table API

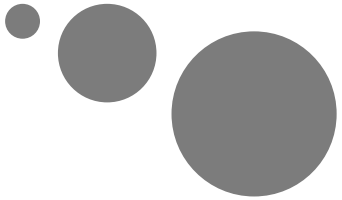


KodeKloud

KodeKloud

Module 7 : Design a relational data storage solution





Design for Azure SQL Database

KodeKloud

When to use Azure SQL Database

There are different Azure SQL offerings, choose the right one based on your requirement

SQL Virtual Machine

SQL VM

- IaaS implementation which offers access to the OS.
- SQL and OS version support.
- Automated manageability features

Managed Instances

Single instance

- Fully managed solution which runs the latest version of SQL.
- Native virtual network deployment

Instance pool

- Sharing of resources with multiple instances to optimize cost.
- Offers better performance management for multiple databases.
- Fully platform managed service.

Databases

Single database

- Offers provisioned compute and serverless
- Fully managed service
- Supports hyperscale storage up to 100 TB

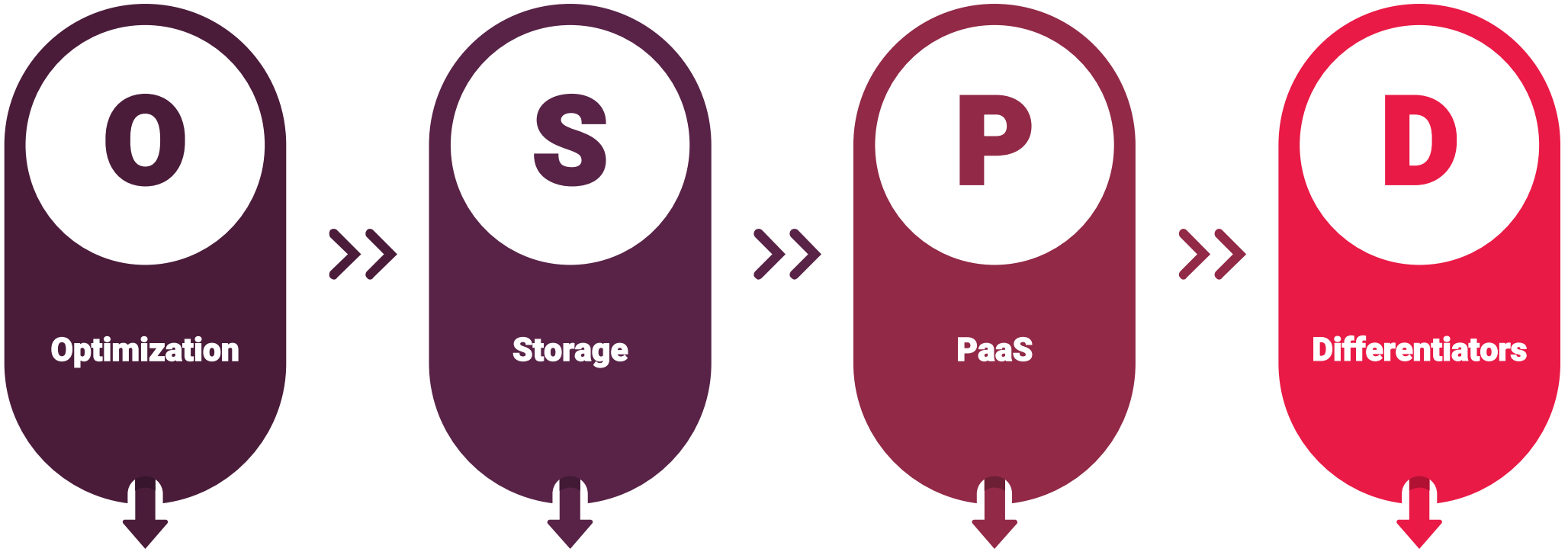
Elastic Pool

- Resource sharing between multiple SQL Databases to optimize cost.
- Offers better performance management for multiple databases.
- Fully platform managed service.

KodeKloud

Azure SQL Database

Highly scalable relational database PaaS solution



We can either deploy a single database or elastic pool where the resources will be shared by multiple databases

Offers Hyperscale storage up to 100 TB

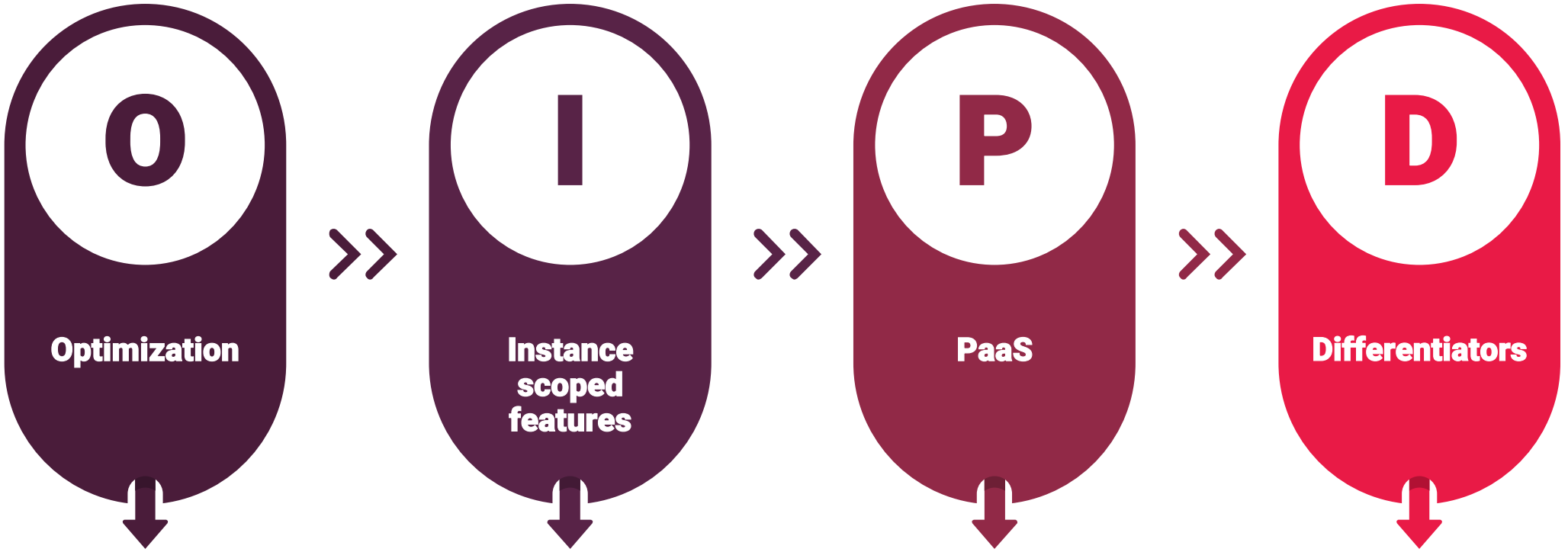
Fully managed PaaS solution and offers serverless compute as well.

- SLA of 99.995%
- RPO of 5 seconds and RTO of 30 seconds.
- 86% cheaper than AWS RDS

KodeKloud

Azure SQL Managed Instance

Ideal for customers who wants to lift-and-shift their database to Azure



We can either deploy a single database or instance pool where the resources will be shared by multiple databases

Supports instance-scoped features such as SQL server agent, Service Broker, CLR, Database Mail, Linked Servers, ML services

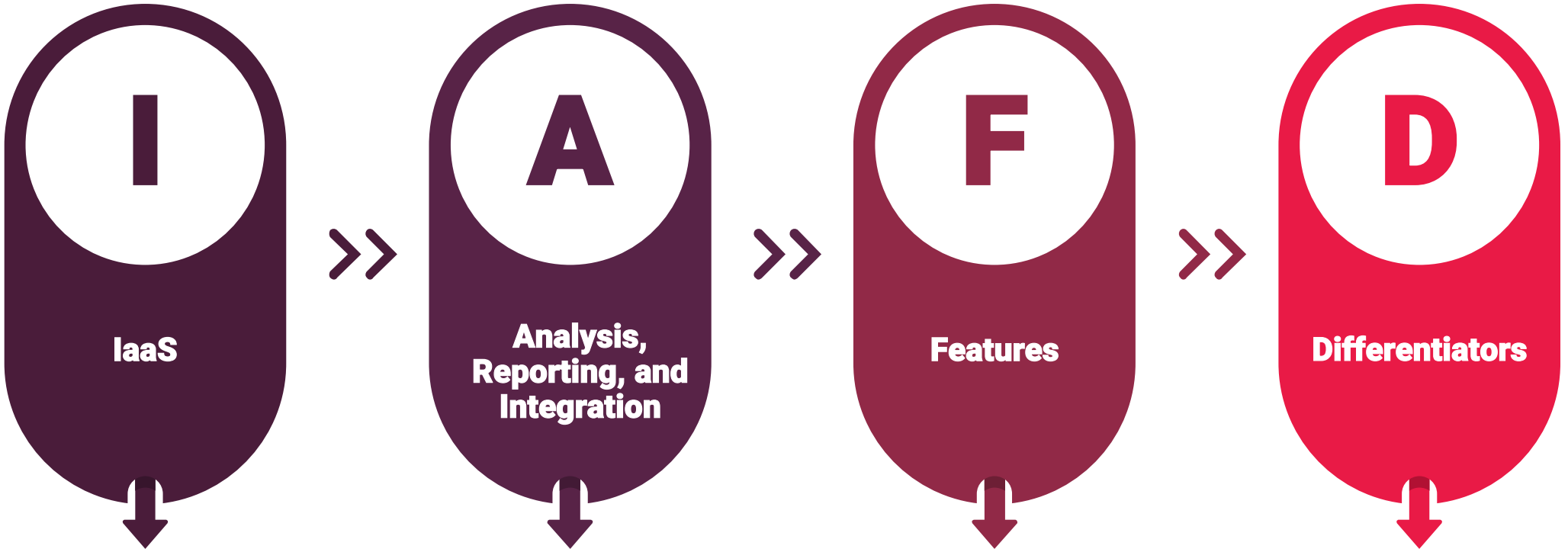
Best of SQL server with the benefits of fully platform managed service and native virtual network integration

- Near zero downtime migration
- Failover groups for BCDR.
- Integrate on-premises identities using Azure AD Connect

KodeKloud

Azure SQL Virtual Machine

Ideal for customers who wants to use SQL in the cloud with full control over the OS and SQL server



Being an IaaS implementation, SQL on VMs offers full control over the OS and SQL Server. Supports Linux, Windows, and SQL Containers

Supports SSAS, SSRS, and SSIS

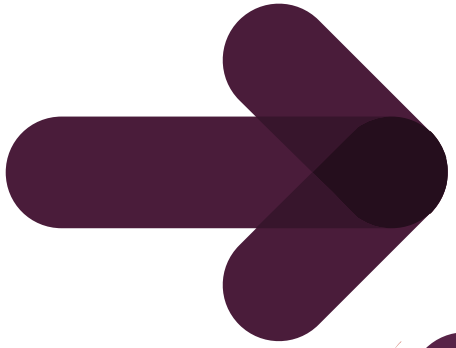
File stream, DTC, and simple recovery model

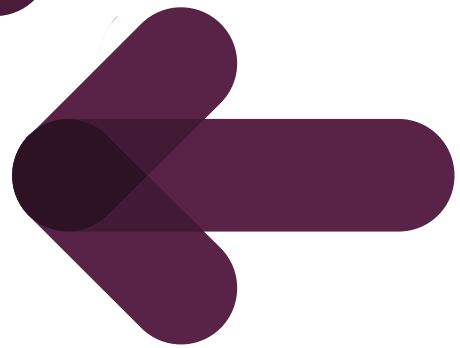
- Free extended support for SQL Server 2008/R2
- Automated backups and security patches
- PITR using Azure Backup
- Accelerated storage performance with Azure Blob Caching

Which one to choose?

Which SQL offering is right for you?

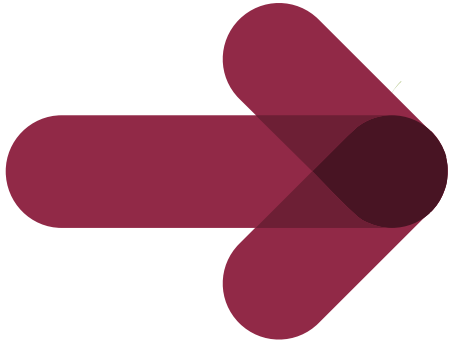
Need to migrate to database in cloud with full control to SQL server and OS





Need to use managed database for modern applications

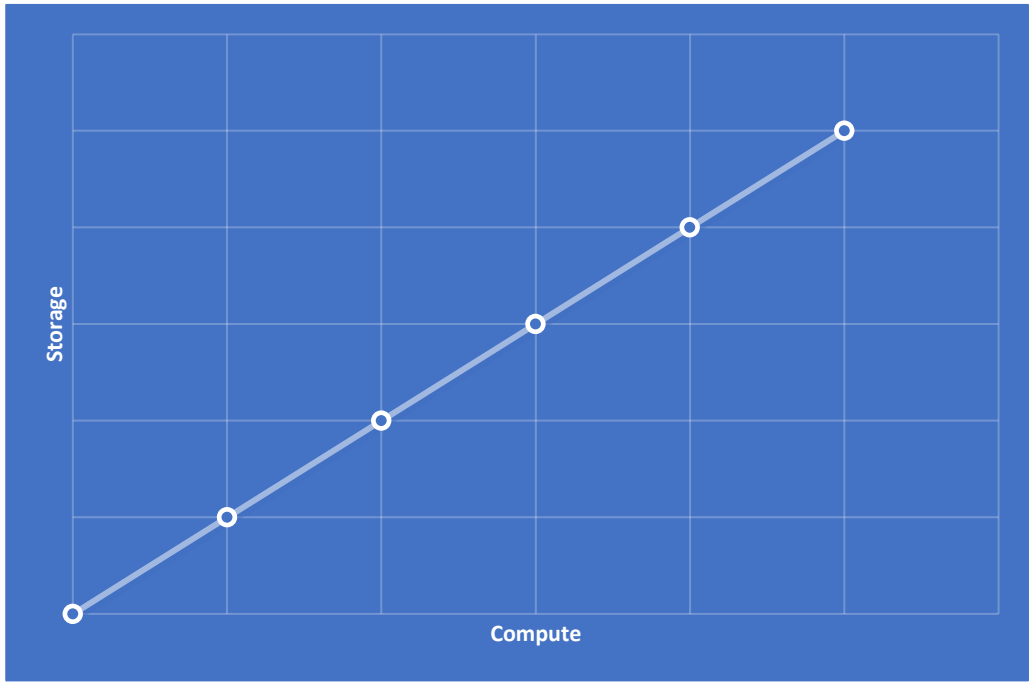
Need to lift-and-shift to cloud with access to instance-scoped features

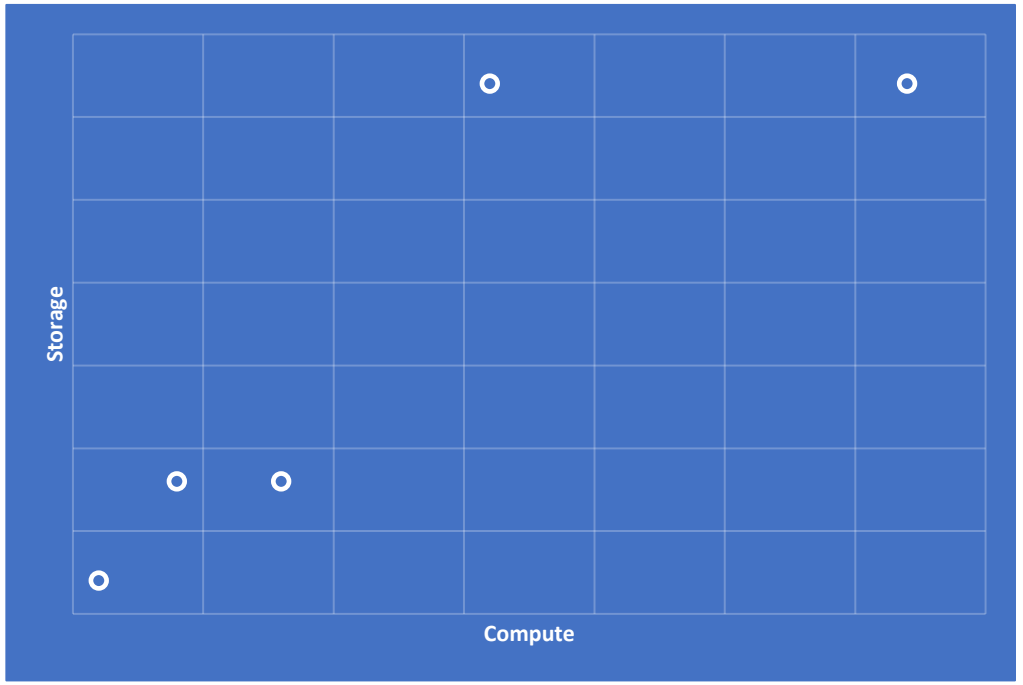


Design for database scalability

Azure SQL Database - Purchasing models

Understand the SQL Database purchasing models





DTU purchasing model

A combined unit for compute, storage and IO resources, you can scale to different DTU sizes based on your requirement

Tiers: Basic, Standard, Premium

vCore purchasing model

vCore model offers the flexibility to choose compute and storage resources independently based on your requirement.

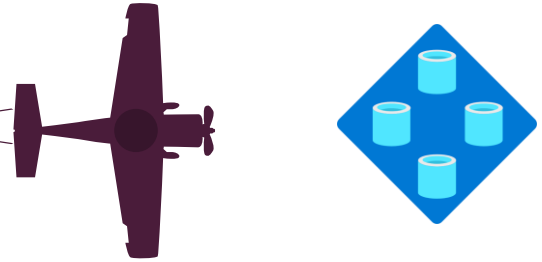
Tiers: General Purpose, Business Critical, Hyperscale

KodeKloud

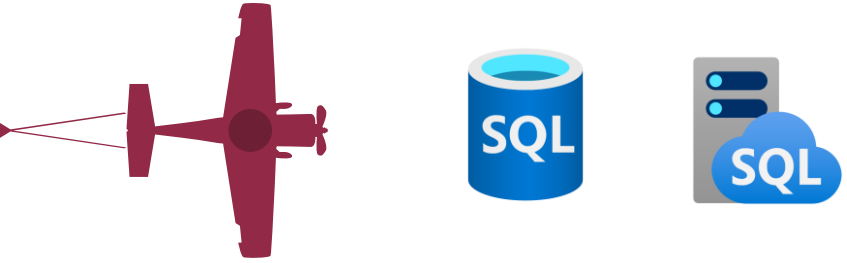
Scaling your databases

Based on the answers to the following scaling requirements, we can choose which database offering would be the right one

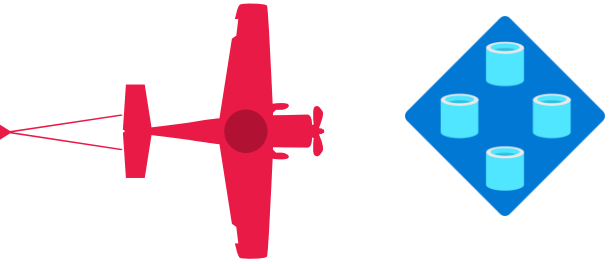
Do you want to manage multiple Azure SQL Databases that have varying and predictable resource requirements?



Do you need a single database to start developing your application and test the functionality?



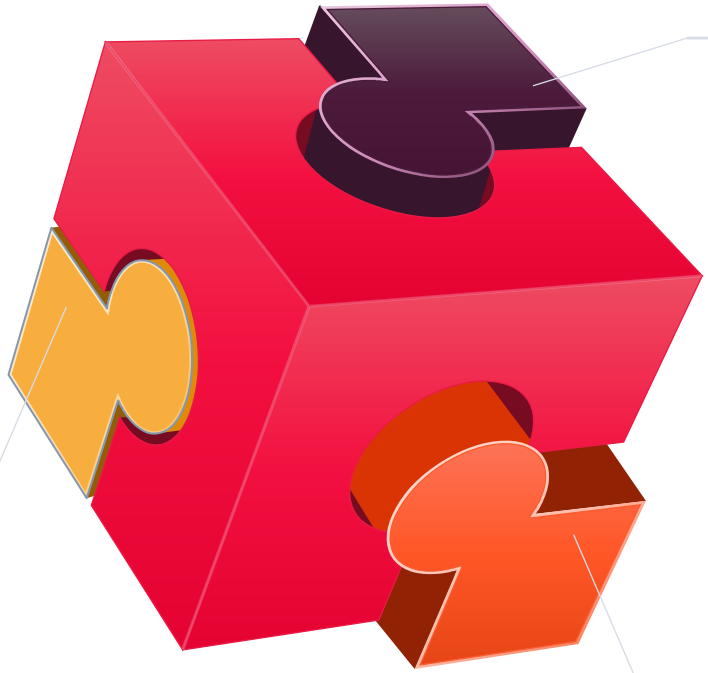
Do you want to optimize the cost of a group of databases so that the cost is limited to the approved budget without comprising the performance?



Design for database availability

High Availability in SQL Database

Learn the SQL HA models



Premium model
(DTU : Premium)
(vCore: Business Critical)

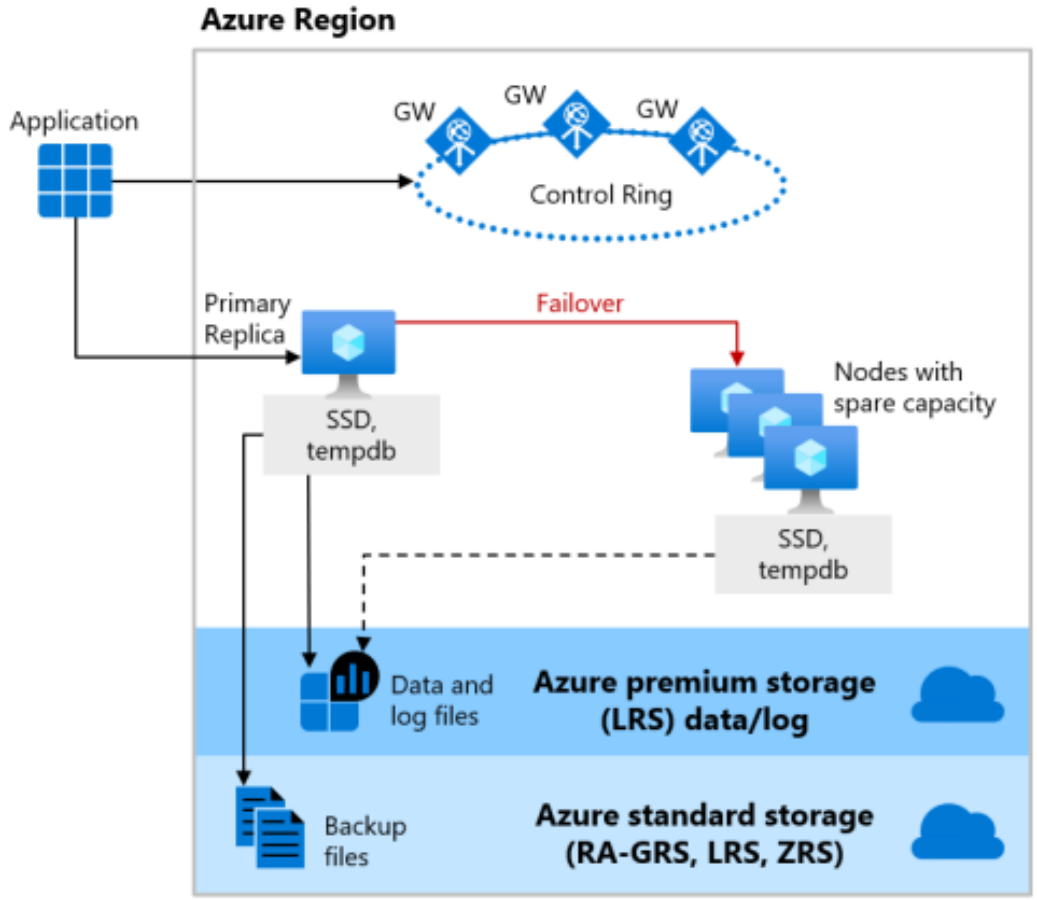
Standard model
(DTU : Basic, Standard)
(vCore: General Purpose)

Hyperscale model
(vCore: Hyperscale)

Standard Model – General Purpose / Standard / Basic

How Standard model helps with database availability for databases deployed in GP or Standard/Basic SKU.

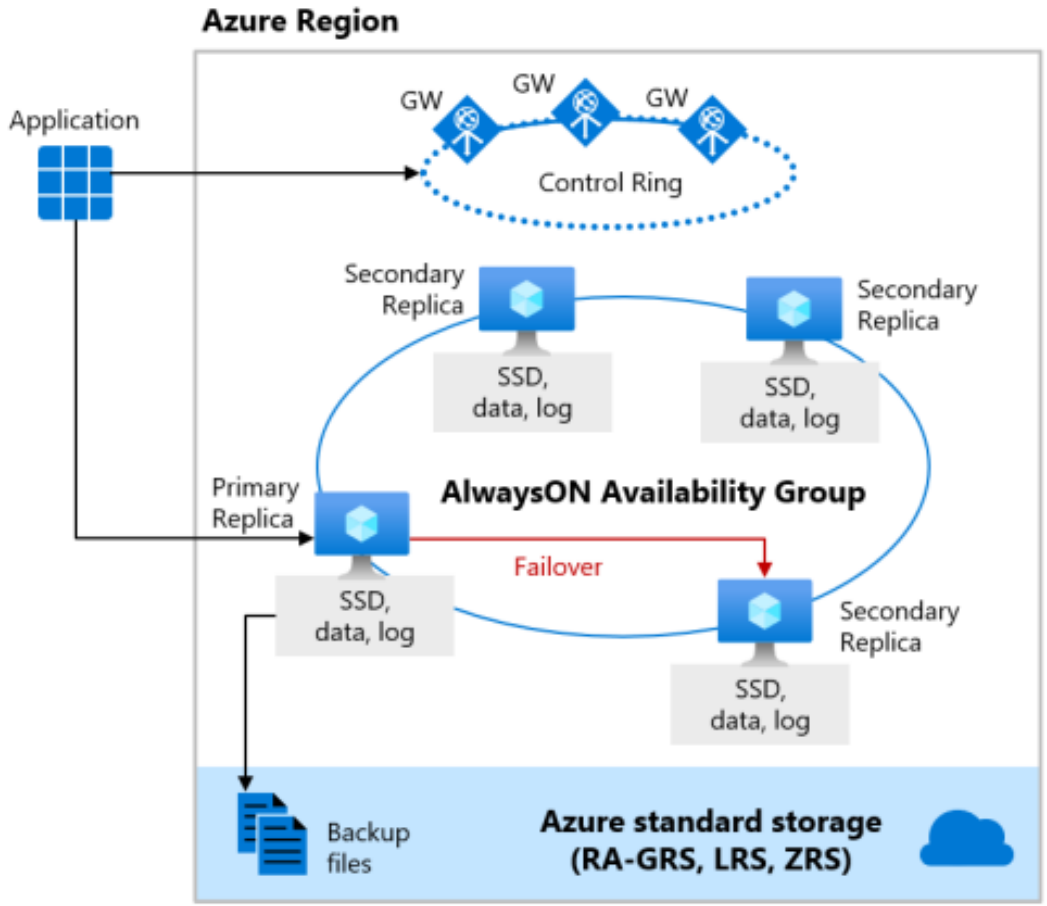
- Compute and storage layers are separated. Compute layer runs the SQL server executable and hosts tempdb and cached data. New instances are spun on the nodes with spare capacity.
- Storage layer stores the database files, and this uses Azure Storage. We can use the replication options available with Azure Storage. If something happens to the sqlserver.exe, storage will ensure that the files are available
- We can also implement backup, and this will be stored in Azure Storage



Premium Model – Business Critical / Premium

How Premium model helps with database availability for databases deployed in BC or Premium SKU.

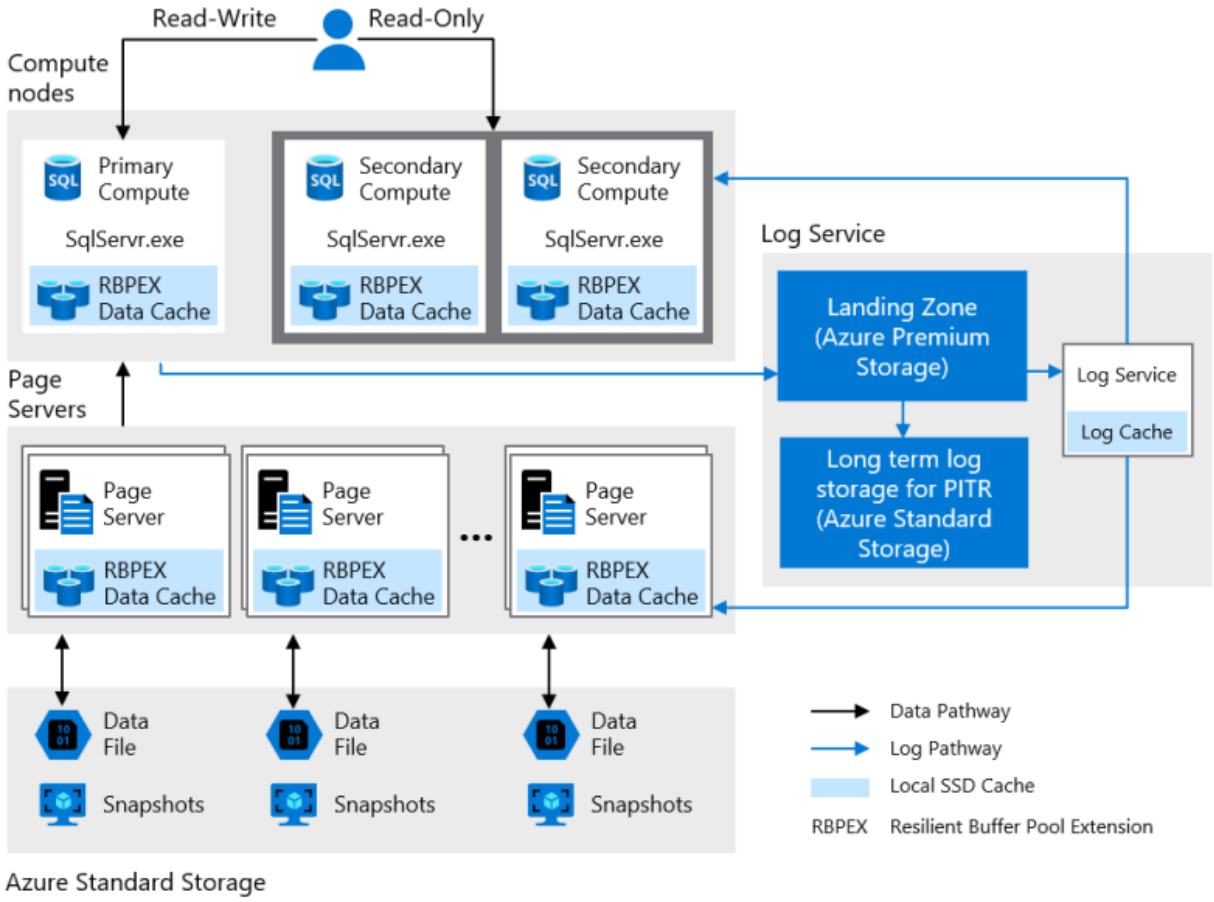
- Ideal for OLTP applications where you require high transaction rate and low IO latency
- The compute layer and storage layer is combined as a single node. All write operations will happen on the primary replica and Always ON Availability Group will ensure that the data is replicated to at least one secondary before it's committed.
- The data will be stored on the attached SSD of the compute, so the latency will be low.
- Backup of the database files will be stored in Azure Storage



Hyperscale Model – Hyperscale tier

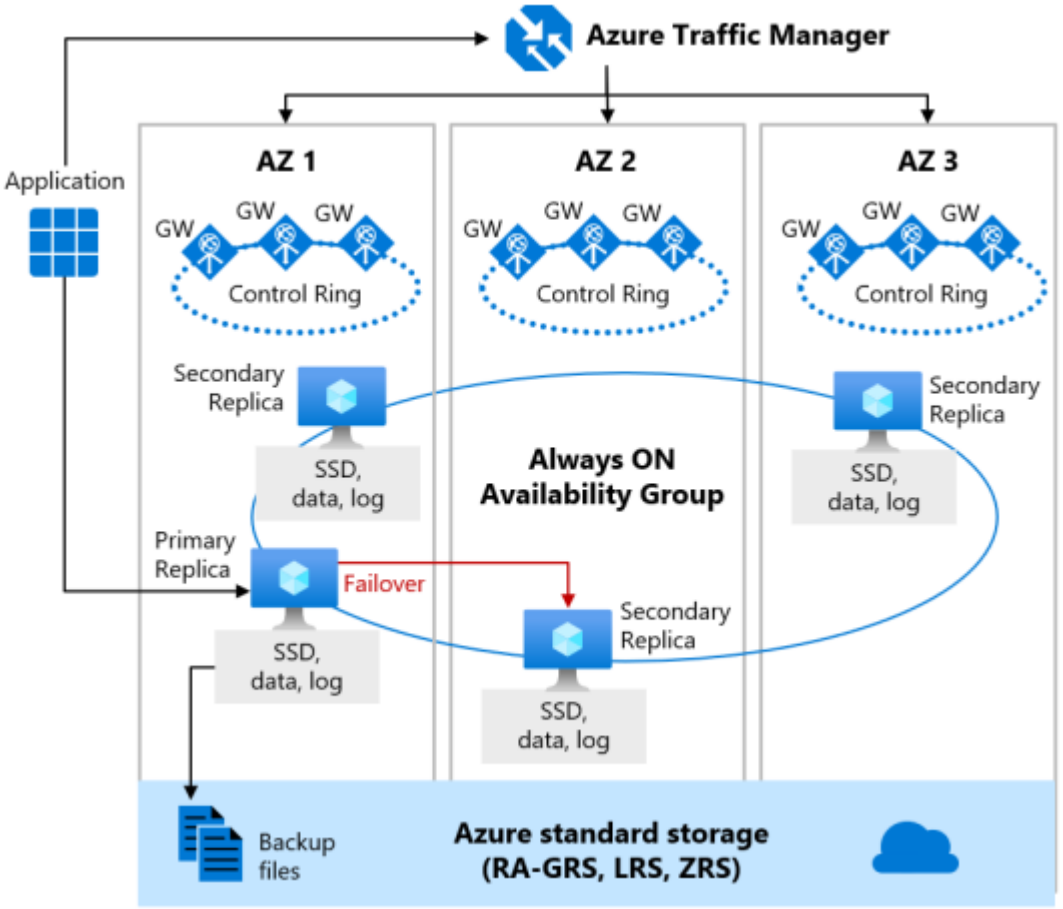
How Hyperscale model helps with database availability for databases deployed in Hyperscale tier

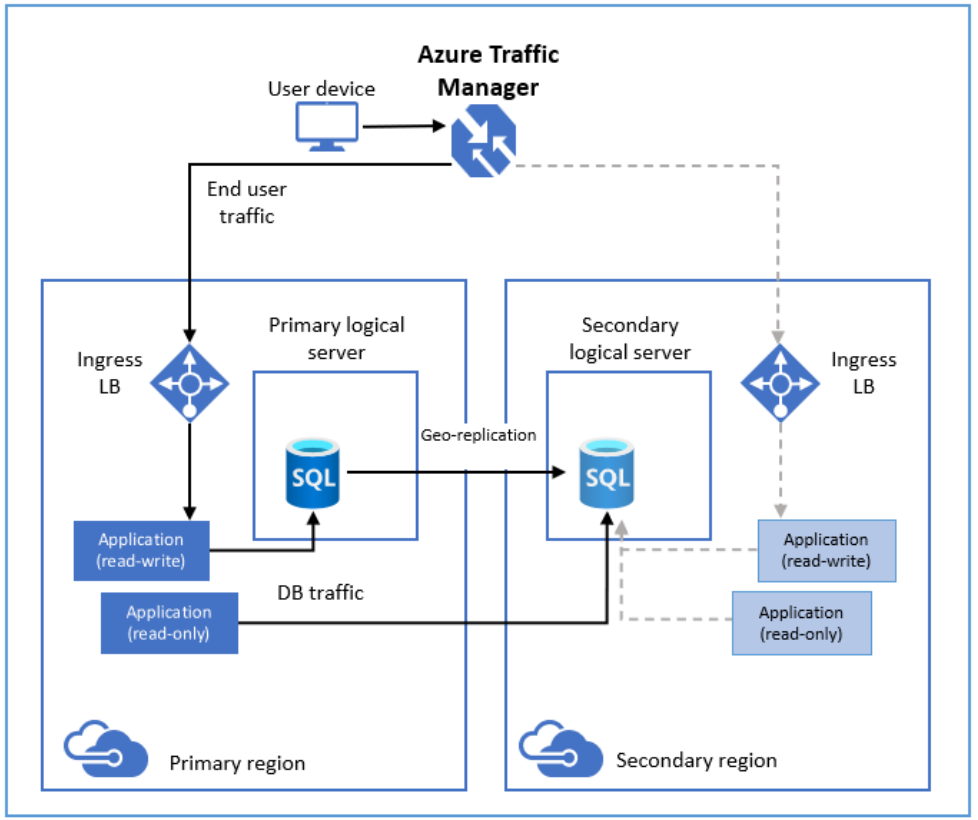
- A stateless compute layer where the sqlserver.exe process is running and contains the cache/transient data
- Stateless storage layer formed by a set of page servers. This layer acts as distributed storage engine for sqlserver.exe where the transient and cache data is stored.
- Stateful transaction log layer where the log service agent is running.
- Stateful storage layer will host all the database files which is updated by the page servers. If the compute node crashes, this layer will ensure that every bit of data is preserved.



Failover strategy

Learn how we can implement high availability within the same region or across regions

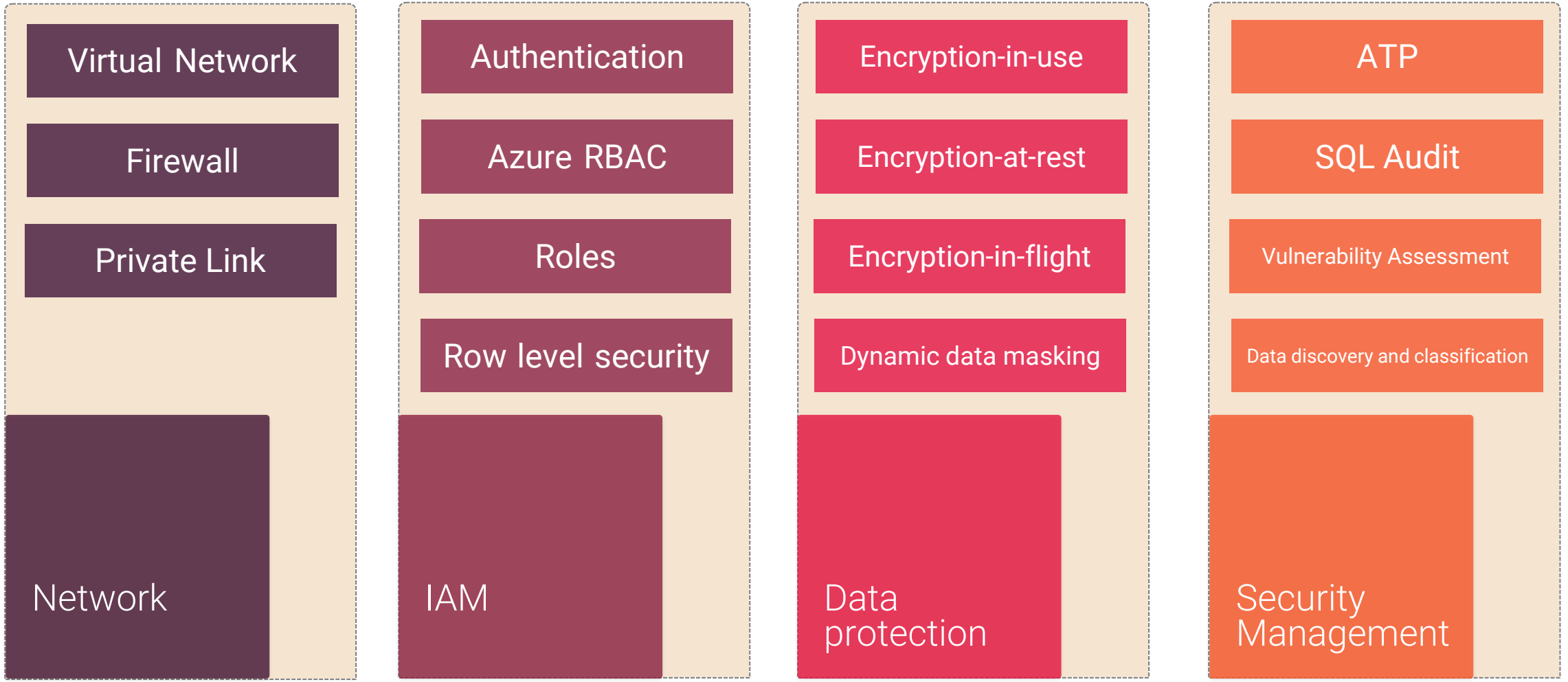




Design for data security

Data security strategy

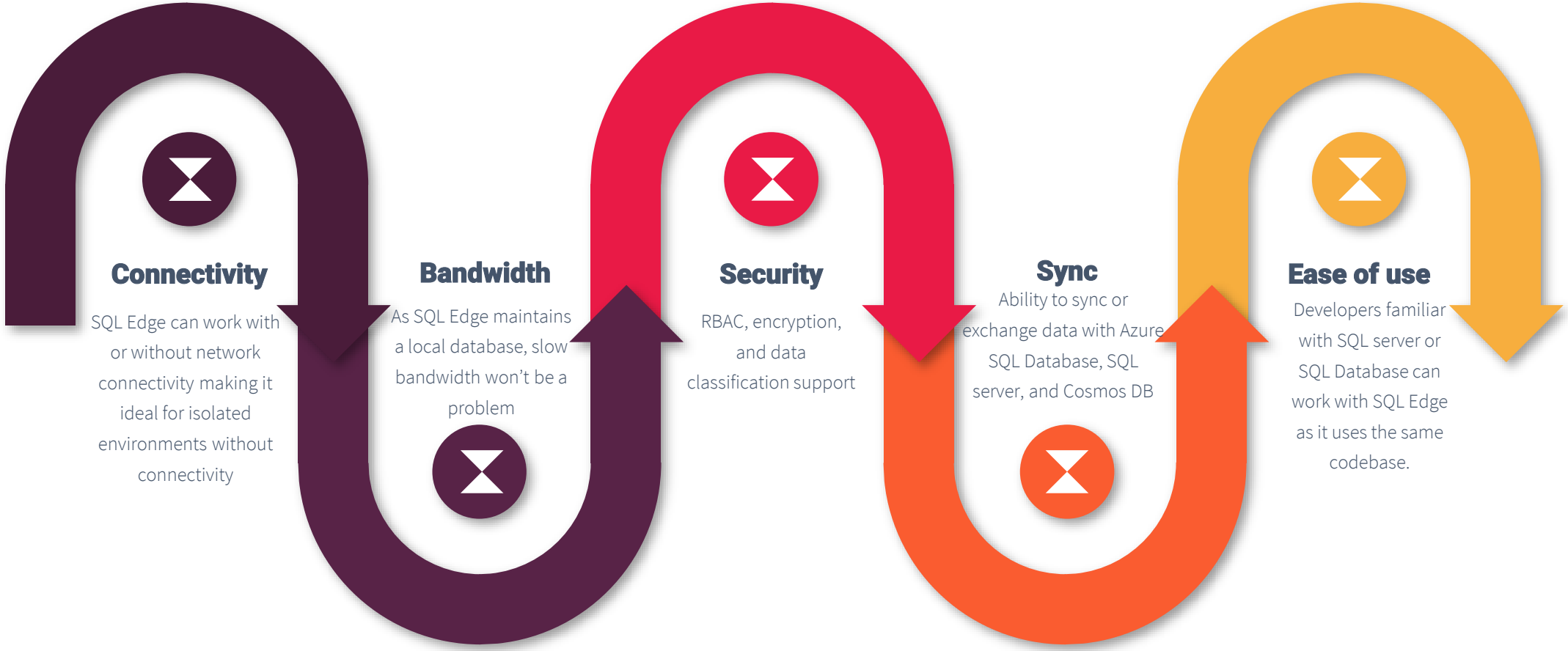
Using the following options, we can secure our database and the data stored in it.



Design for SQL Edge

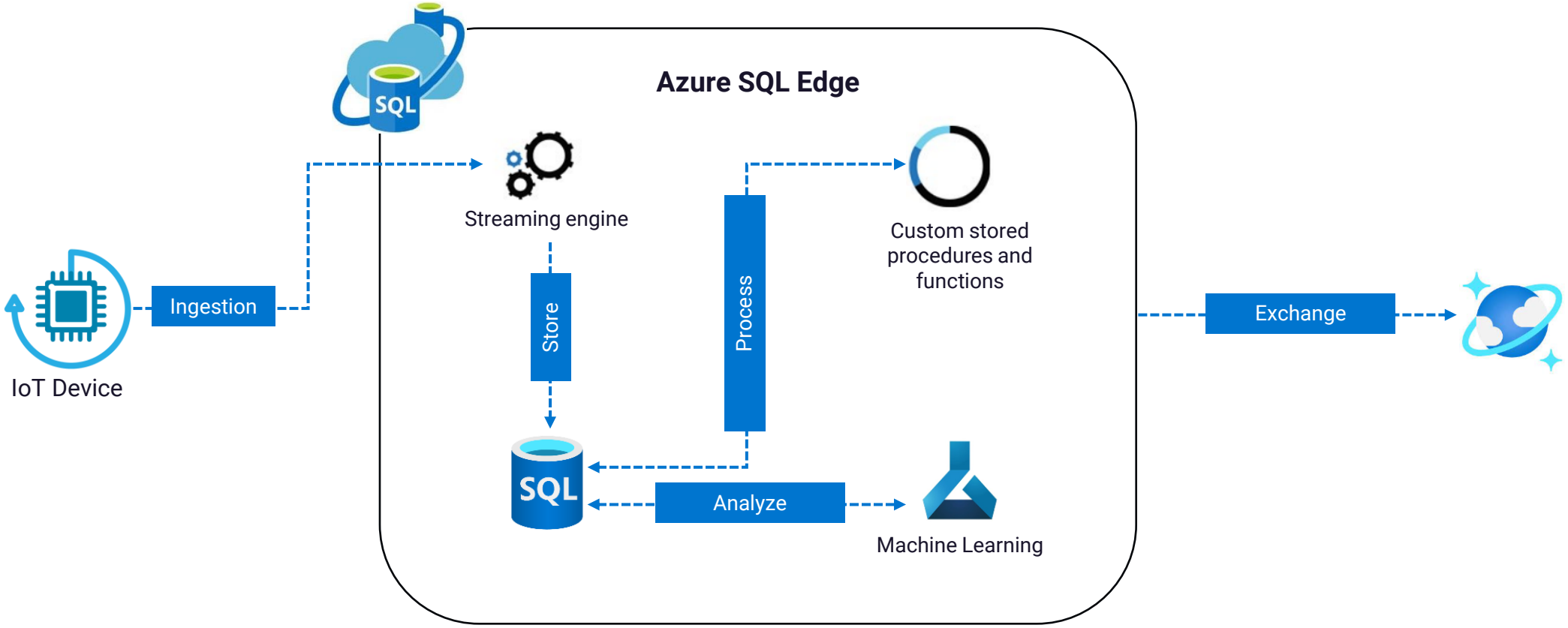
Design for SQL Edge

Relational database for IoT and IoT Edge deployments



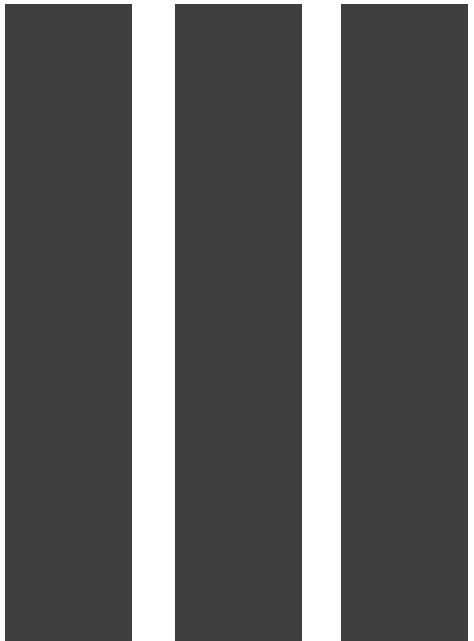
Design for SQL Edge

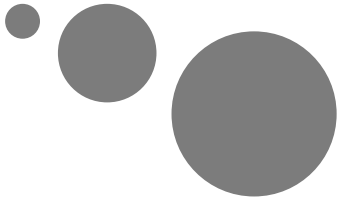
Relational database for IoT and IoT Edge deployments



KodeKloud

Module 8 : Design a data integration solution





Design for Azure Data Factory

Data driven workflows

Create and schedule data driven workflows using ADF for ingestion and transformation of data between different data sources

Ingestion

Connecting and collecting the data from data source is the first step in a data driven workflow. The collected data will be stored in a centralized location for further processing

Transform and enrich

With help of analytics solution such as Azure Databricks and Azure HDInsight, we will be transforming the data

CI/CD and publish

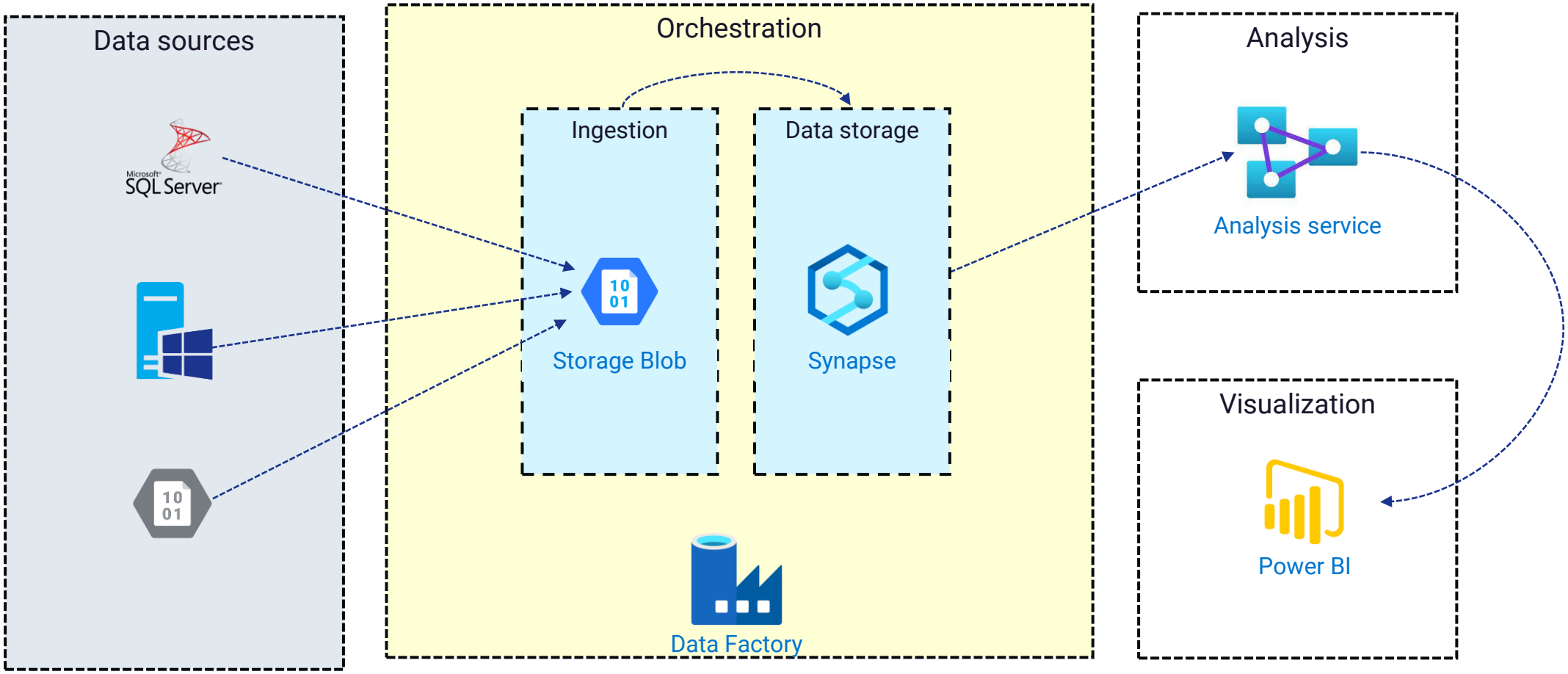
With the help of CI/CD integration we will be able to deliver the ETL process incrementally to GitHub or Azure DevOps before we publish to the analytics engine.

Monitor

Data pipelines can be monitored from Azure Portal to check if the activity was successful or not

Data driven workflows

Create and schedule data driven workflows using ADF for ingestion and transformation of data between different data sources



When to use ADF?

Following decision criteria is used to decide whether we need to use

Requirements

ADF can be used for Big Data and the Relation Data Warehousing using SSIS. Depending on the requirements, you need to configure pipelines to access Azure and non-Azure data sources

Development

Using the ADF authoring tool, you will be able to set up pipelines from the GUI. ADF offers low code/ no code process for working with data sources

Data sources

ADF offers 90+ connectors to ingest the data. You can ingest data from multiple data sources at the same time.

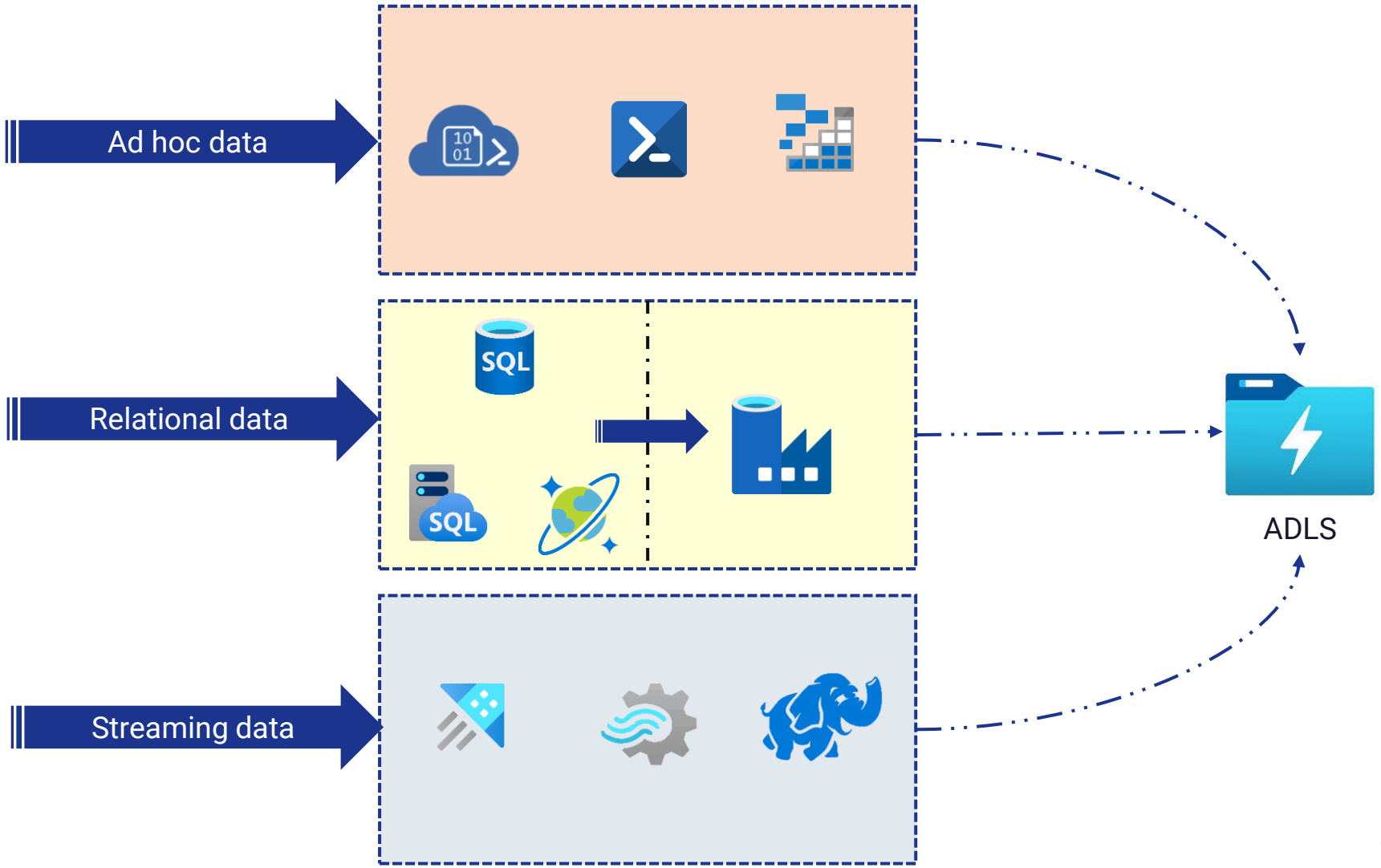
Provisioning

Offers dedicated and serverless provisioning. In serverless, based on the demand the system will scale without the need to deploy or manage compute servers.

Design for Azure Data Lake Storage

How ADLS works?

Comprehensive, scalable, and cost-effective storage for big data analytics



When to use ADLS?

Comprehensive, scalable, and cost-effective storage for big data analytics

01

Large amount of data

Data warehousing large amount of data. Due to scalability and reliability of ADLS, massive amounts of data is not a tedious task.

02

Manage multiple file types

In scenarios, where you need to manage multiple file types like JSON, CSV, XML etc. you can use ADLS. Azure will store the raw data which can be accessed used different tools such as Azure Data Explorer.

03

Real time streaming

If you have real-time data coming from Azure IoT Hub, Azure Event Hubs, or Azure Stream Analytics we can ingest it to ADLS.

Azure Blob Storage v/s ADLS

Understand the difference between Blob Storage and ADLS

VS

COMPARISON

- Ideal for storing unstructured data which non-text in nature like photos, videos etc
- Choose replication based on your need. Default selection will be GRS
- Flat namespaces
- Not compatible with Hadoop
- Granular access is not available

- Ideal for storing large volumes of text data
- Need to set up replication as it not offered by default
- Hierarchical namespace
- Hadoop data can be stored
- Granular access is available

Design for Azure Databricks

Azure Databricks

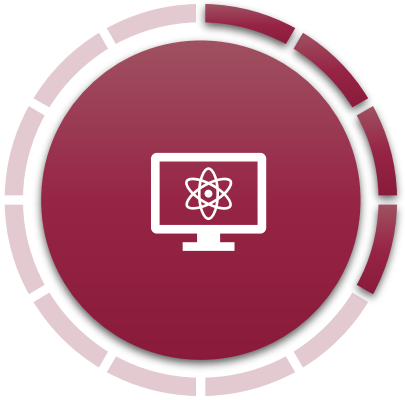
Fully managed, cloud based Big Data and Machine Learning platform

Databricks SQL

Analysts can run SQL queries against their data lake storage to analyze, visualize, and explore the data. The results can be portrayed in different ways and can be shared to dashboards for consumption

Databricks Data Science and Engineering

ML engineers, data engineers, and data scientists can use this platform for collaboration. The data ingested using ADF or any other service will be stored in ADLS. This stored data can be read using Databricks and create insights using Spark.



Databricks Machine Learning

End-to-end ML environment with the ability to perform experiment tracking, model training, feature development, and model serving.

How Azure Databricks works?

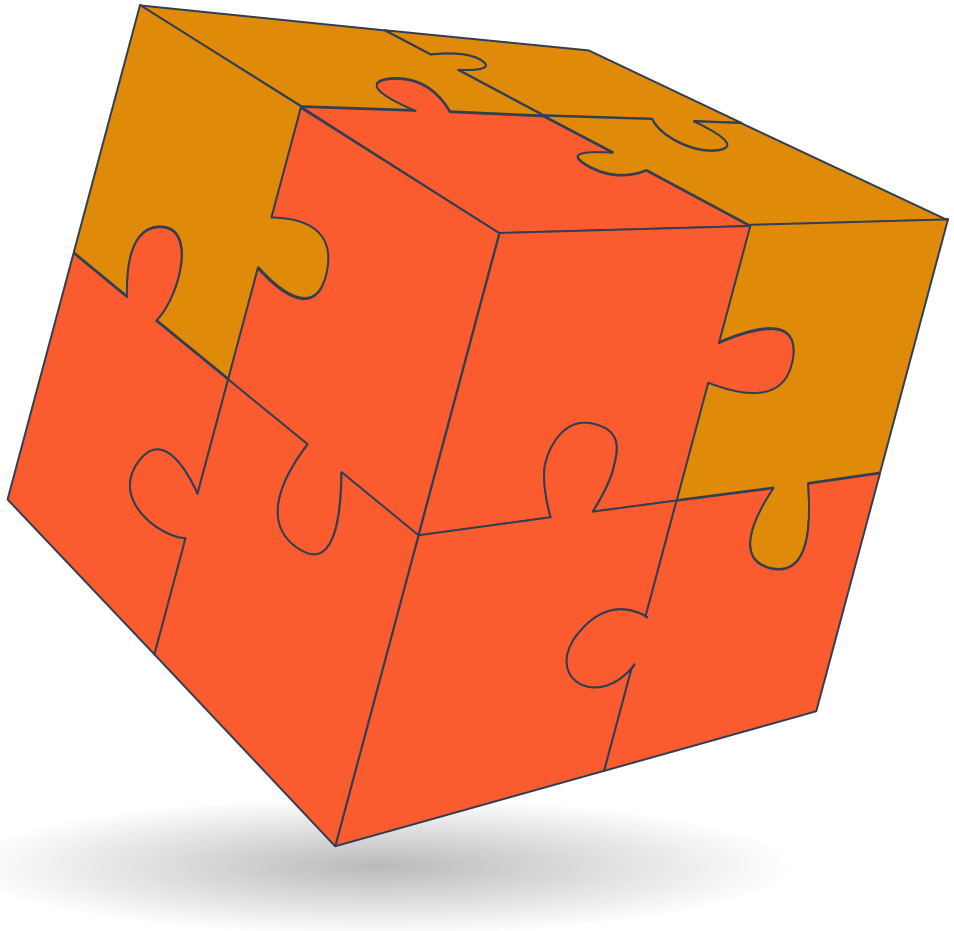
Azure Databricks has Control plane and Data plane

Control plane

Jobs, notebooks with query results, and cluster manager is hosted on the control plane of the Databricks. For managing the user sessions, the control plane has a web app, hive metastore, and access control lists. These components doesn't exist in your Azure subscription, and these are directly managed Databricks in collaboration with Microsoft.

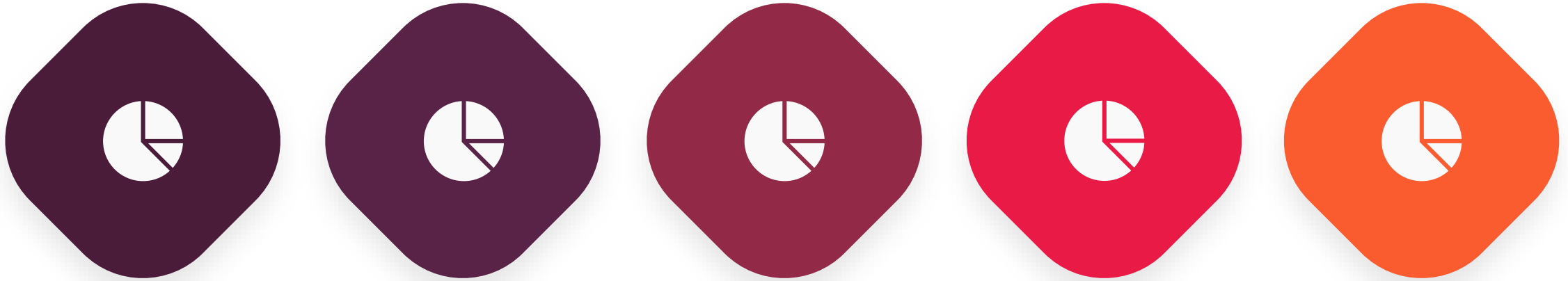
Data plane

The runtime clusters in the workspace are part of the data plane. All the data processing and storage exists within the subscription.



When to use Azure Databricks?

Learn the scenarios where you can use Azure Databricks



Data preparation

Preparation of unstructured data includes creation, cloning and convert them into jobs which can be further reviewed by data analysts and reviewers.

Develop insights

Common scenarios such as recommendation engines, churn analysis, and intrusion detection can be accomplished with the help of Databricks

Increase productivity

A common workspace can be created and that can be shared as a collaboration channel for data engineers, analysts, and scientists.

Big data

Multi-step data pipelines can be created with the help of data lake and engine. This will offer improved reliability and performance of your big data workloads.

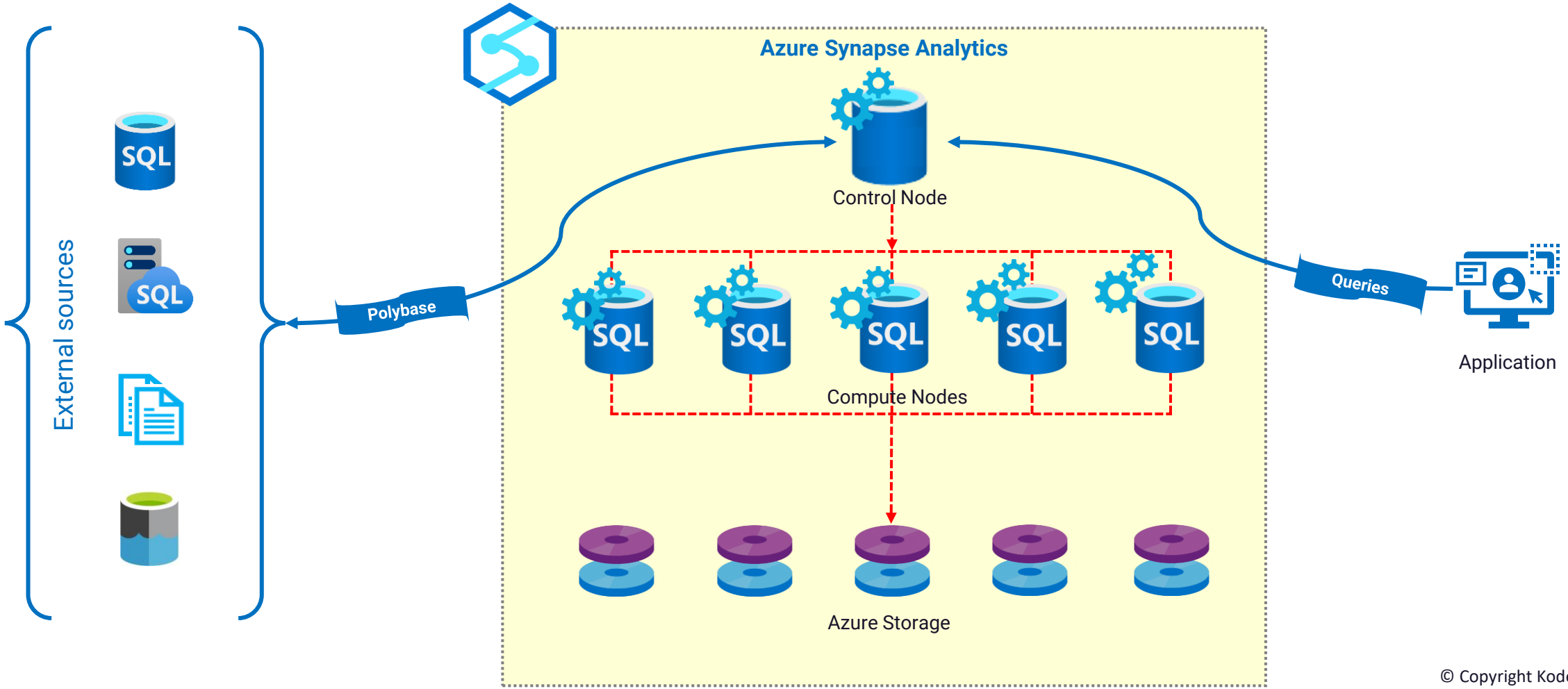
Machine Learning

With the help of Databricks Machine Learning environment, we can create end-to-end ML environment.

Design for Azure Synapse Analytics

Azure Synapse Analytics

Single service for data integration, enterprise data warehousing, big data analytics



Azure Synapse Analytics - Components

Synapse Analytics comprises of different components that can be used for various purposes

Synapse SQL Pool

Offers serverless and dedicated resources model to work with node-based architecture

Synapse Spark Pool

Clusters running the Apache Spark service. You can write your data processing logic in Python, Scala, SQL, and .NET.

Synapse Pipelines

By leveraging ADF, Synapse Pipelines offers cloud based ETL and data integration service by which you can create data driven workflows for data movement and transformation.

Synapse Link

Allows you to connect Synapse to Cosmos DB. Analytics can be developed on top of the data that is stored in Cosmos DB using Synapse.

Synapse Studio

Web based IDE that can be used to create Spark and SQL pools, create and run pipelines, and create connections to external data sources.

Azure Synapse Analytics – Types of analytics

Learn the types of analytics Synapse can perform on the data

Descriptive analytics
"What is happening?"

Descriptive analytics can be done with the help of dedicated SQL pools by creating persisted data warehouse.

Diagnostic analytics
"Why is it happening?"

With the hep of serverless SQL pools, we can explore the data stored in data lake interactively and perform this type of analytics.

Predictive analytics
"What is likely to happen?"

With the help of integrated Apache Spark engine and Azure Synapse Spark pools we can run predictive analytics with other services such as Azure ML services or Azure Databricks

Prescriptive analytics
"What needs to be done?"

This analytics is done using real time or near-real time ingestion of data and its analysis.

Compare ADF and Azure Synapse Analytics

Comparison between the working of ADF and Azure Synapse Analytics

Criteria	Azure Data Factory	Azure Synapse Analytics
Sharing of integration runtime	Runtime can be shared across multiple ADFs	Sharing of integration runtime is not allowed
Solution templates	Templates are available in the ADF template gallery	Templates are available in the Synapse Workspace Knowledge Center
Cross region data flows	Supported	Not supported
Sparks jobs for data flow monitoring	Not supported	Supported (Synapse Spark pools)

Compare Azure Databricks and Azure Synapse Analytics

Comparison between the working of Azure Databricks and Azure Synapse Analytics

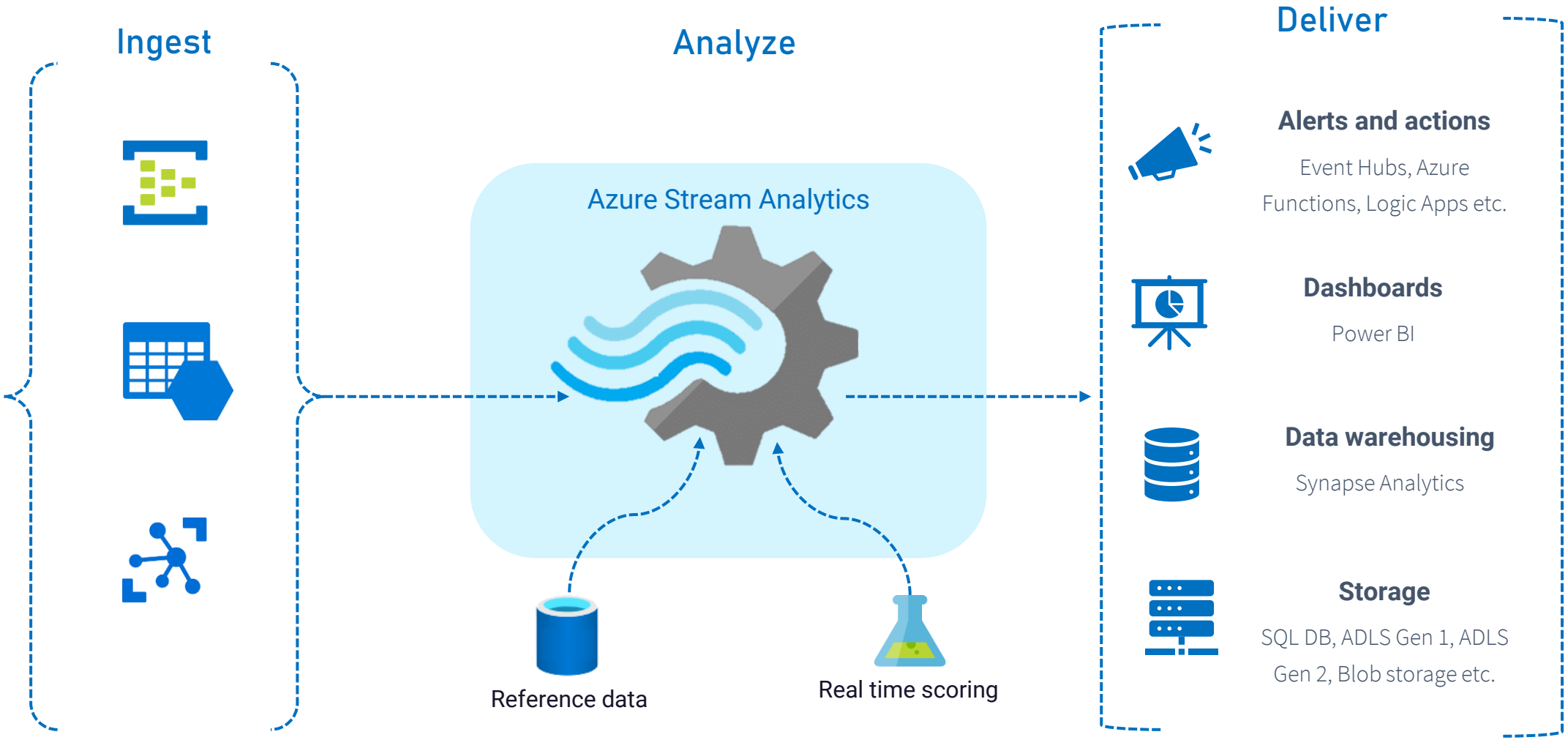
Capabilities	Azure Databricks	Azure Synapse Analytics
Machine Learning	• TensorFlow, PyTorch, and Keras is supported • GPU support	• Azure ML built-in support • Use SparkML, MLLib, and other OSS libraries to train models • GPU-accelerated pools
Feature Set	Optimized Apache Spark environment	• Distributed T-SQL system • Spark environment • Data Integration • Unified experience with Synapse Studio
Reporting	Azure Databricks connector for Power BI	Direct integration to Power BI using Synapse Studio

Design for Azure Stream Analytics

KodeKloud

Azure Stream Analytics

Fully managed service for delivering real-time analytics for data streams



Azure Stream Analytics - Benefits

Advantages of using Azure Stream Analytics

01

Fully Managed

As Stream Analytics is a fully platform managed solution, you don't have to worry about the hardware or underlying infrastructure.

02

Cheap

Resources scale up and down based on the business requirements and the scaling is measured in a unit called streaming units (SU). SU is billed in terms of the memory and CPU allocated for the service. There is no maintenance cost.

03

Deployment

Deploy Stream Analytics in cloud or on IoT Edge or Azure Stack. Cloud is better for large scale analytics while deploying to IoT Edge will be useful for low latency analysis.

04

Performance

Stream Analytics partitions the complex queries so that they can be processed parallelly in multiple nodes. Stream Analytics is capable of processing millions of events every second and results can be obtained quickly.

05

Security

All incoming is data is processed in memory and it won't be stored in the service. Incoming and outgoing traffic supports TLS 1.2. Built-in checkpoints are also encrypted.

When to use Azure Stream Analytics?

Some common use case scenarios where Azure Stream Analytics is used

01

IoT data stream

Real time IoT sensor data stream can be analyzed.

02

Clickstream

Based on web logs and click stream suggest new product to consumers based e-commerce analytics

03

Geospatial analytics

Collect real time stream from satellite images, mobile devices, and sensors to develop analytics on weather, application usage etc.

04

Remote monitoring

Gathering of data from industrial machinery and equipment to predict the maintenance of the equipment maximizing its life and eliminate production impact.

05

POS data

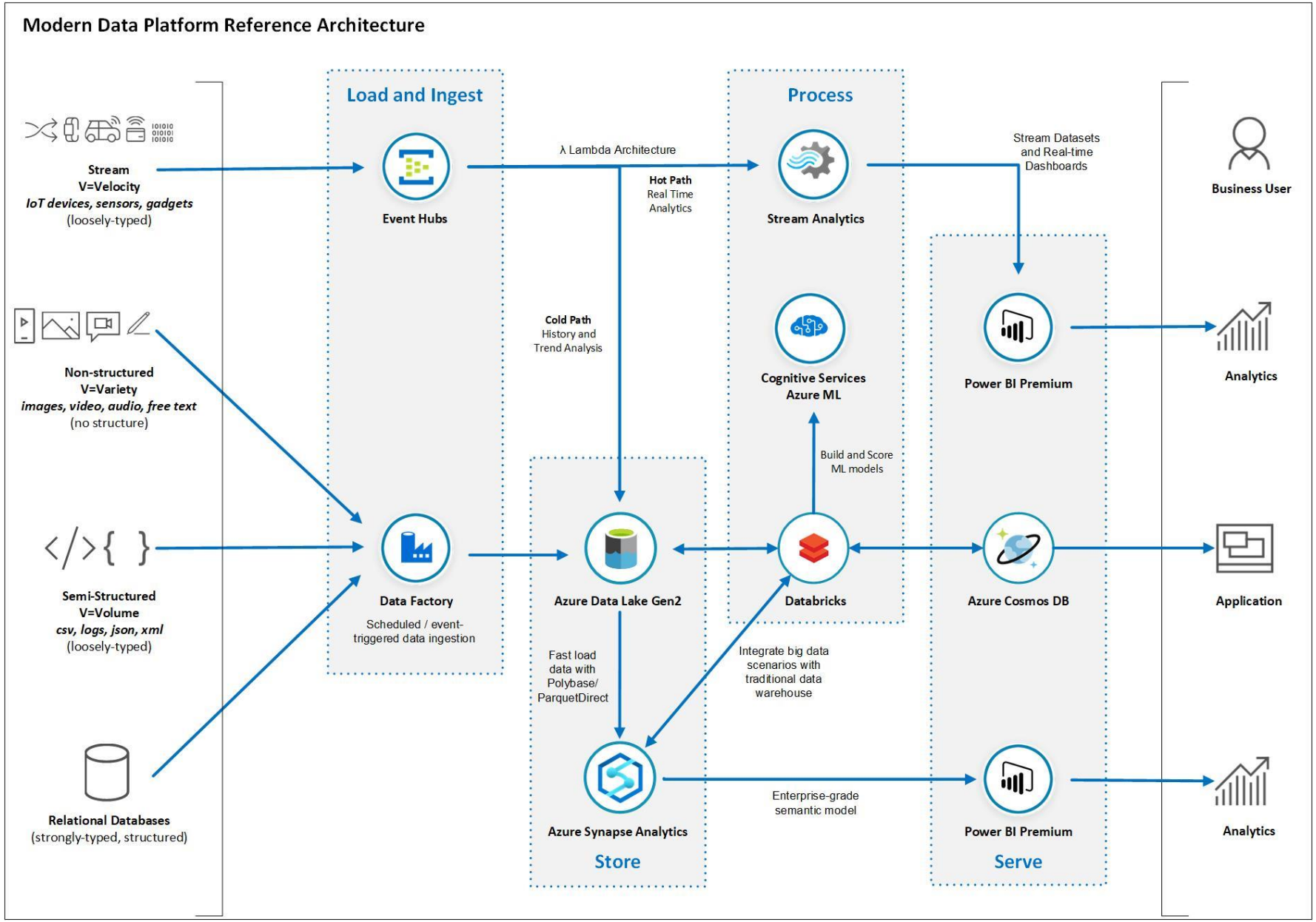
Data from POS machines can be analyzed to detect fraudulent credit card transactions based on location and value of the transaction.

Design for data flow strategy

When to use Hot/Warm/Cold data path

Choose the right data flow path based on the type of data and frequency of data ingestion

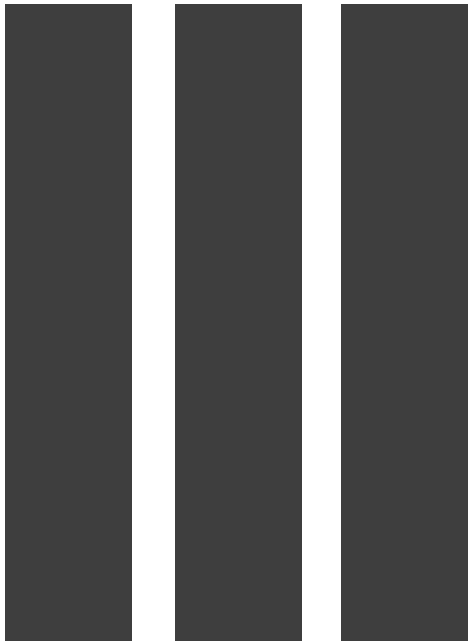
Path	Requirement
Hot data path	• When data requirements are known to change frequently • When processing or displaying data in real time
Warm data path	• When you need to store or display a recent subset of data • Used for data that is consumed for small analytical and batch processing
Cold data path	• When data is rarely used. The data might be stored for compliance or legal reasons • Used for data that is consumed for long term analytics and batch processing

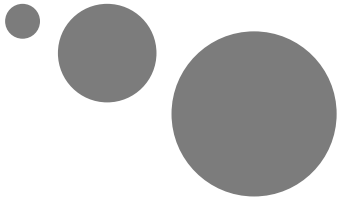


KodeKloud

KodeKloud

Module 9 : Design a migration solution



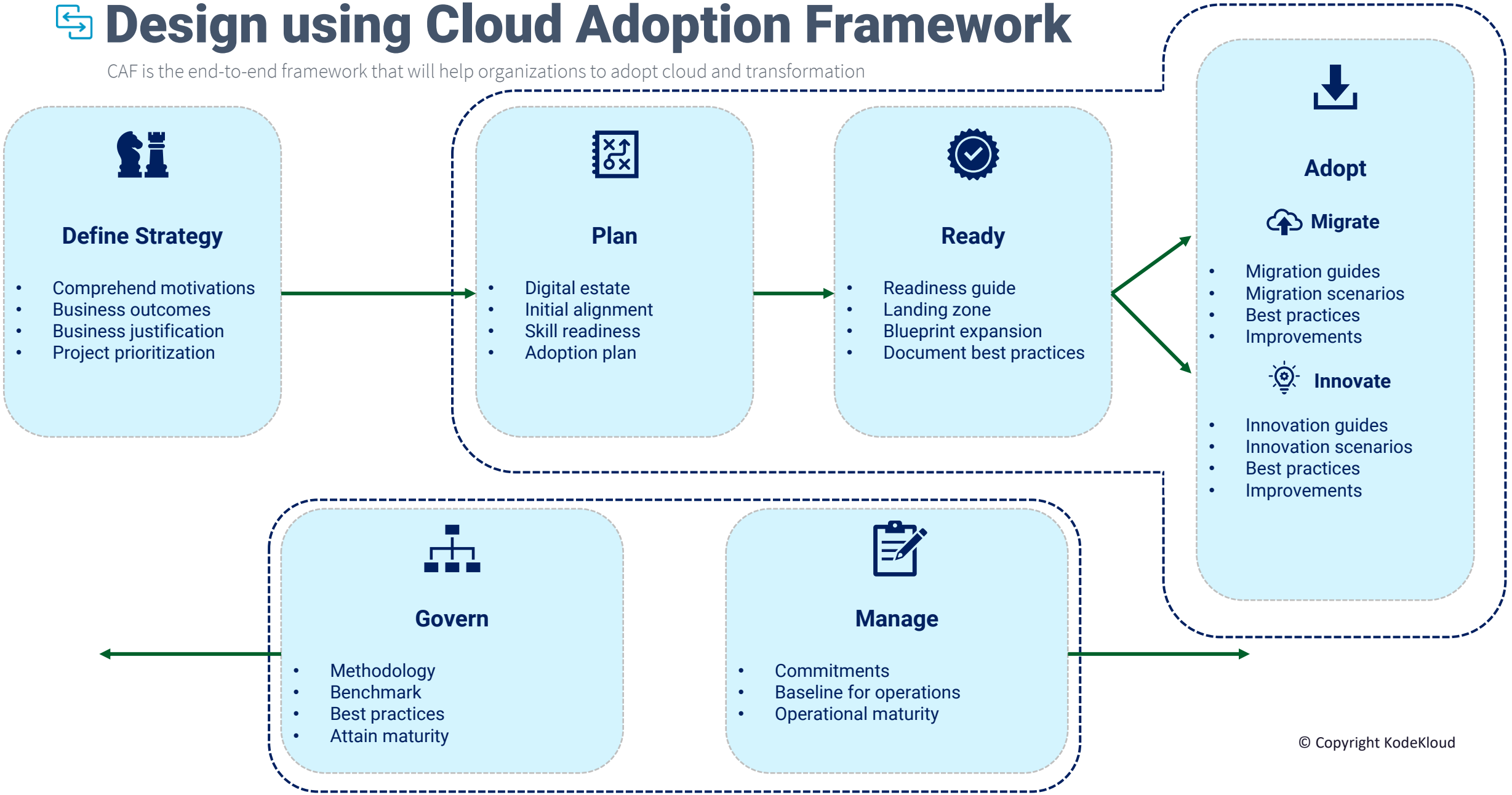


Design using Cloud Adoption Framework

KodeKloud

Design using Cloud Adoption Framework

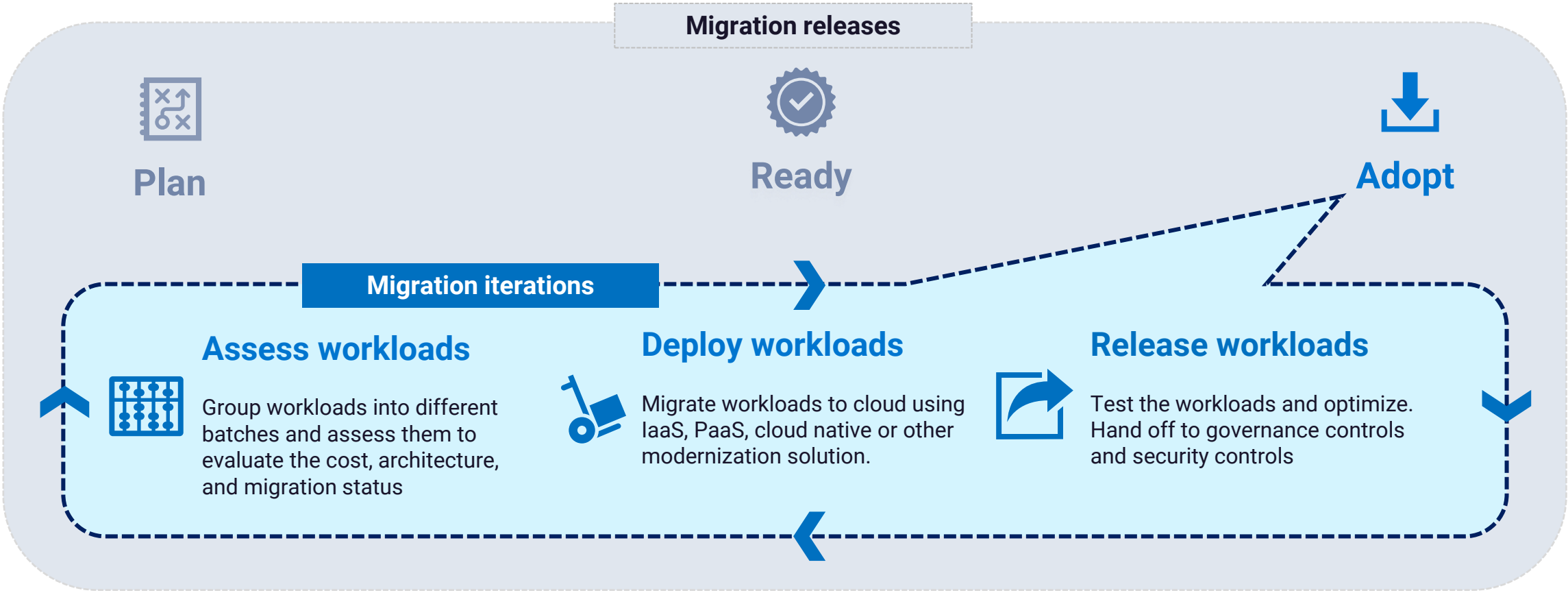
CAF is the end-to-end framework that will help organizations to adopt cloud and transformation



Azure Migration Framework

Azure Migration Framework

Includes the iterations for assessing, deploying, and releasing workloads to the cloud



Plan your migration strategy

Choose a strategy that matches your requirements and end goals

Rehost

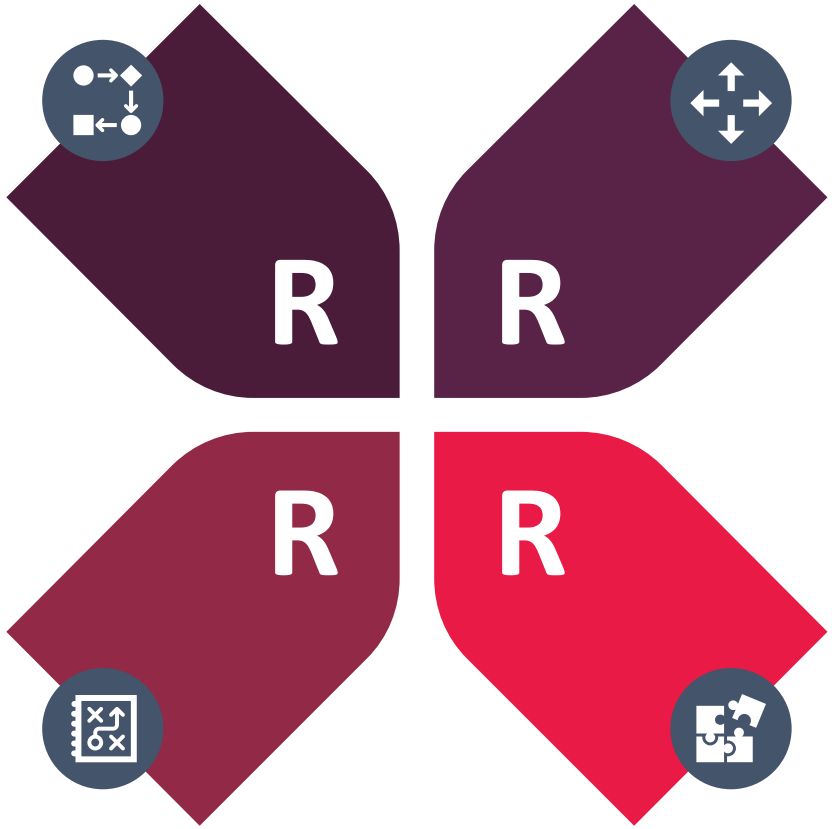
What?: Lift-and-shift process to move the workloads quickly without making any architectural/code changes

When?: When you want to move to cloud quickly without any change..

Rearchitect

What?: Rearchitecting an application to extend the app functionality and code to optimize the app architecture for cloud scalability.

When?: Ideal when your application needs many changes to work effectively with the cloud,



Refactor

What?: Repackaging the application to leverage PaaS and cloud-native options available in the cloud.

When?: If you would like to leverage the features of the cloud by minimum architectural changes

Rebuild

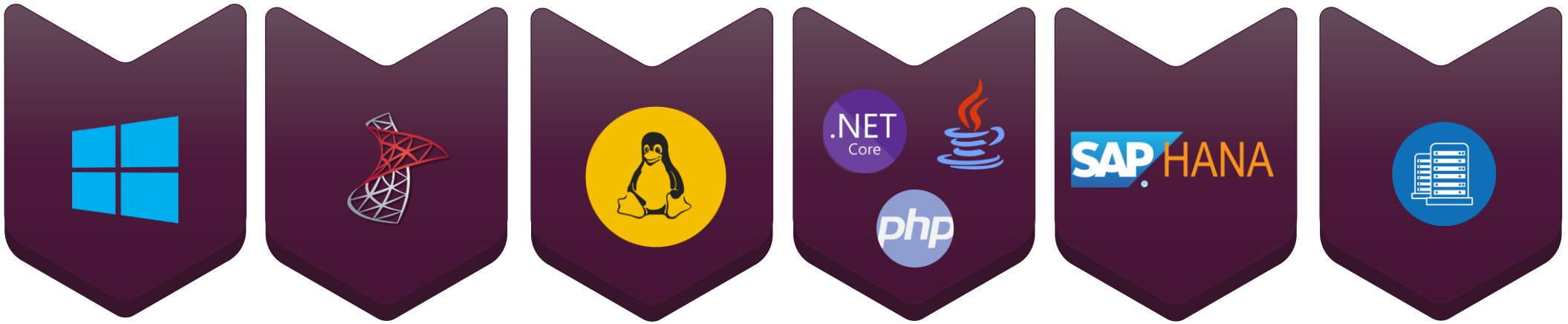
What?: Completely rebuilding the application to use the app in Azure.

When?: You have EOL apps and would like to rapidly develop and onboard to cloud.

Assessing workloads

Determine the workloads

Plan which type of workloads you want to migrate to Azure, prioritize mission critical workloads



Windows workloads

Windows servers from on-premises (databases not included)

SQL Server

Databases running on SQL server

Linux workloads

RedHat Linux, SUSE Linux, Ubuntu, Hadoop, and Linux containers

Applications

Internal and external applications (ASP.NET, .NET core, Java, PHP)

SAP HANA

ERP with a centralized database

Specialized workloads

HPC workloads

Assessment tools

Understand the type of assessment tool based on the type of workload you're migrating

Assess physical servers and virtual machines running in Hyper V and VMWare environments; preparing them for migrating to Azure

Assess on-premises Microsoft SQL Server database as preparation to migration to Azure SQL Database, Azure SQL MI, or SQL on VM.

Assess on-premises web applications and making them prepared for Azure migration

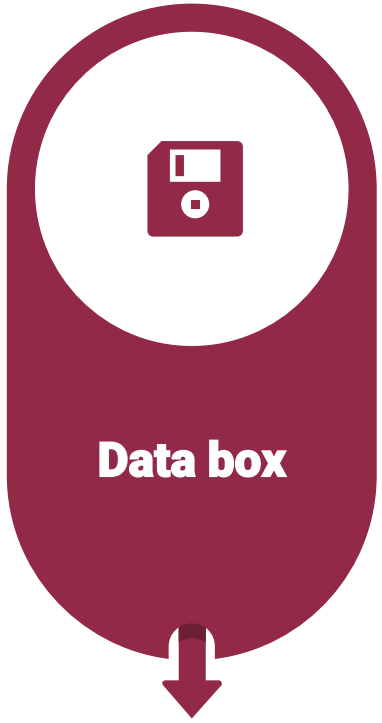
Migration tools

Migration tools

Migration tools are used after assessing the workloads to migrate the data to Azure

Migrate physical servers and virtual machines running in Hyper V and VMWare environments to Azure

Migrate on-premises Microsoft SQL Server database to Azure SQL Database, Azure SQL MI, or SQL on VM.



Migrate large amount of offline data to Azure Storage

Database migration

Database migration type

Online and offline migration of databases

- At the start of migration, the source server is required to be shutdown
- During migration, application will face downtime

Offline migration

- There won't be any downtime as there is no need to shutdown the server during online migration
- Continuous replication of data enabling cut over any time.

Online migration

Storage migration

Storage migration type

Online and offline migration of storage

- Windows Server Storage Migration Service
- Azure File Sync
- AzCopy
- Storage Explorer

Online migration

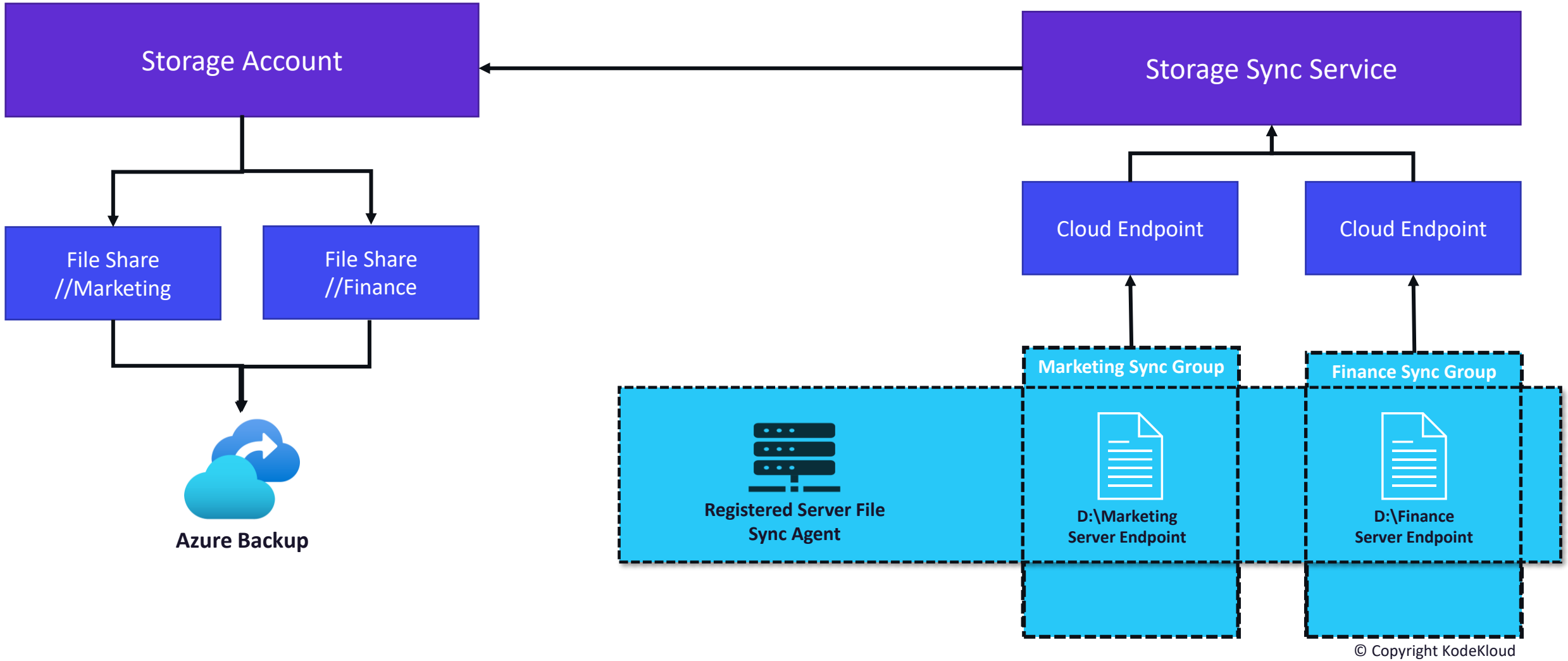
- Azure Import/Export
- Azure Data Box

Offline migration

KodeKloud

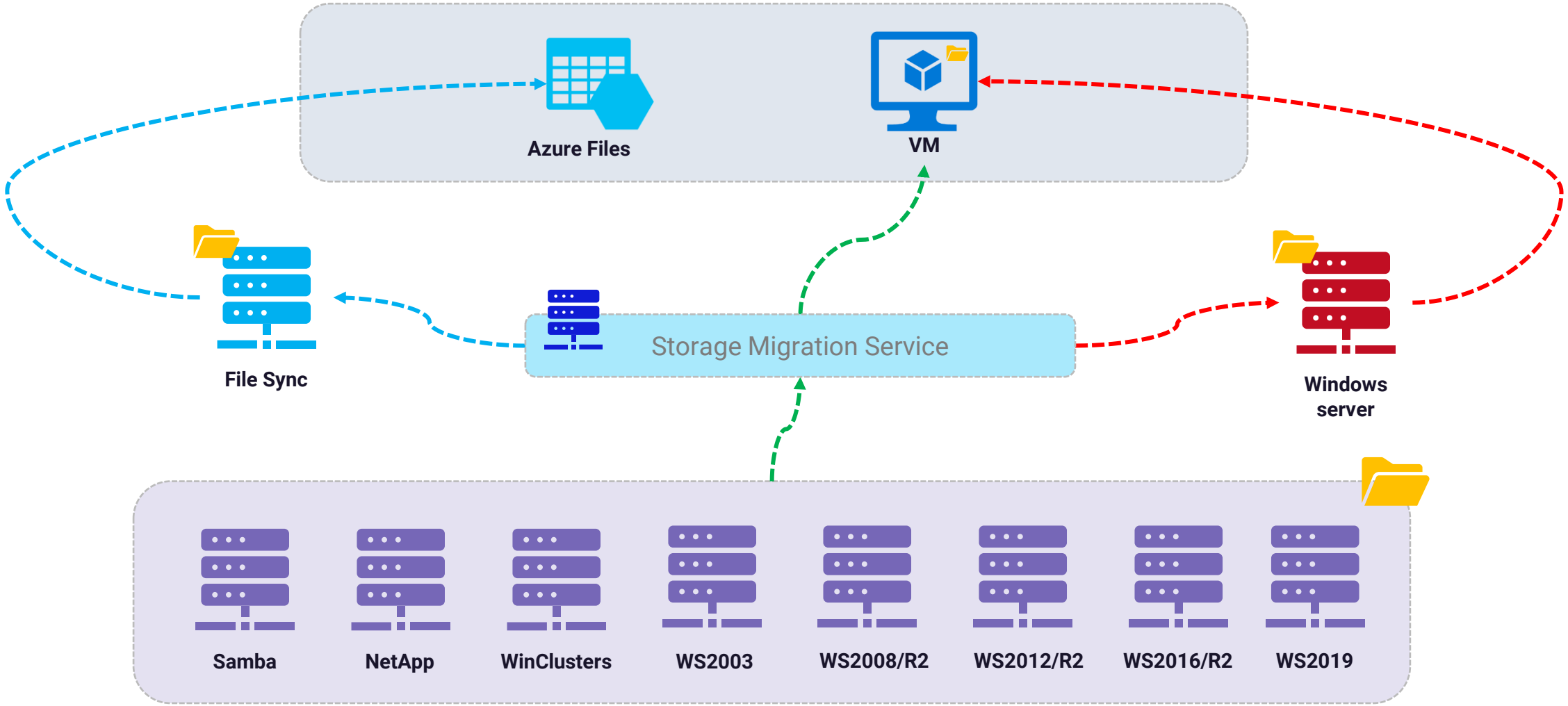
Azure File Sync

Migrate your data to a Windows server or to Azure



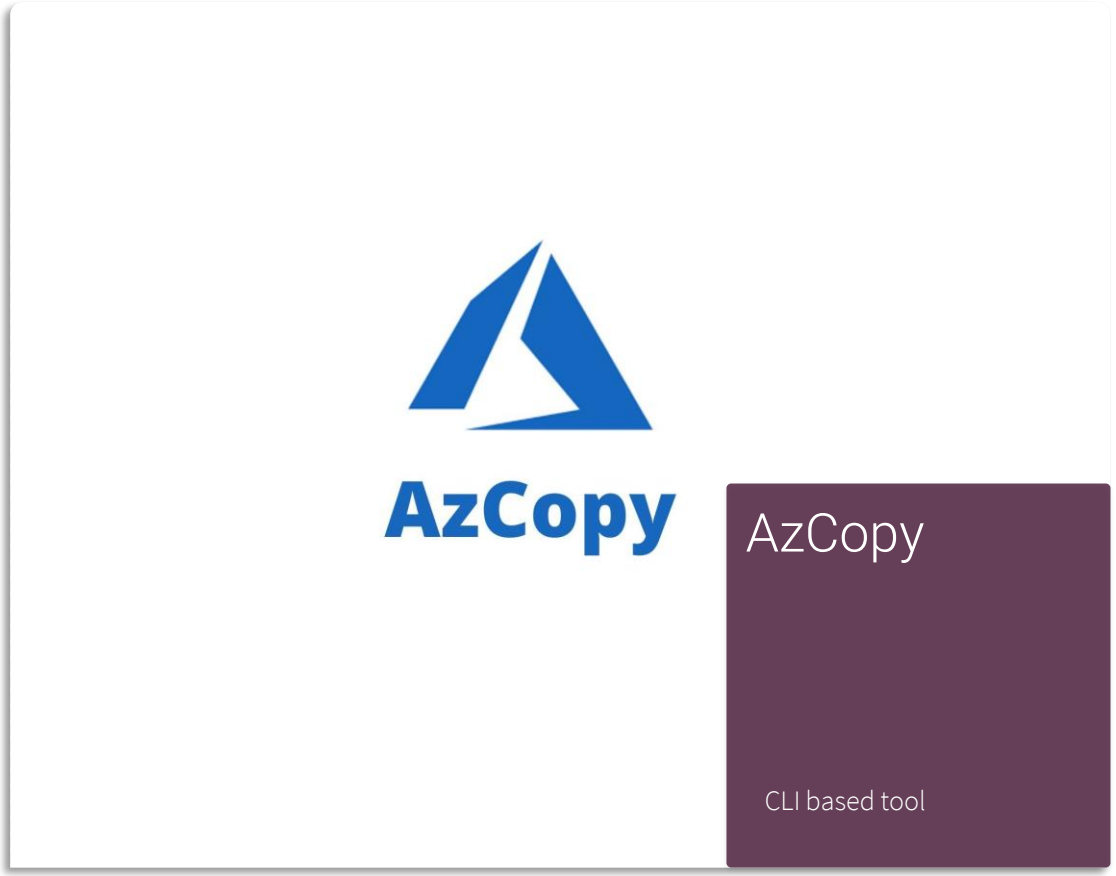
Windows Server Storage Migration Service

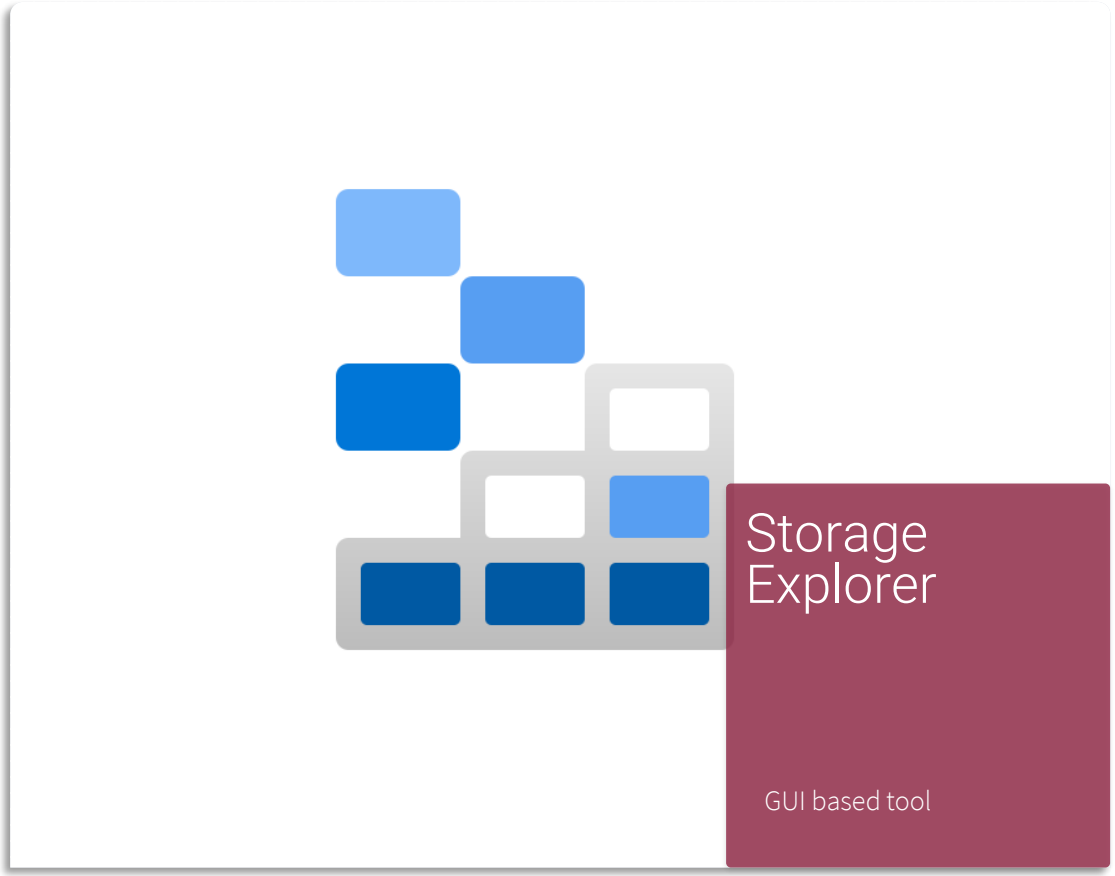
Migrate your data to a Windows server or to Azure



AzCopy and Storage Explorer

Use CLI based and GUI based tools to migrate your data

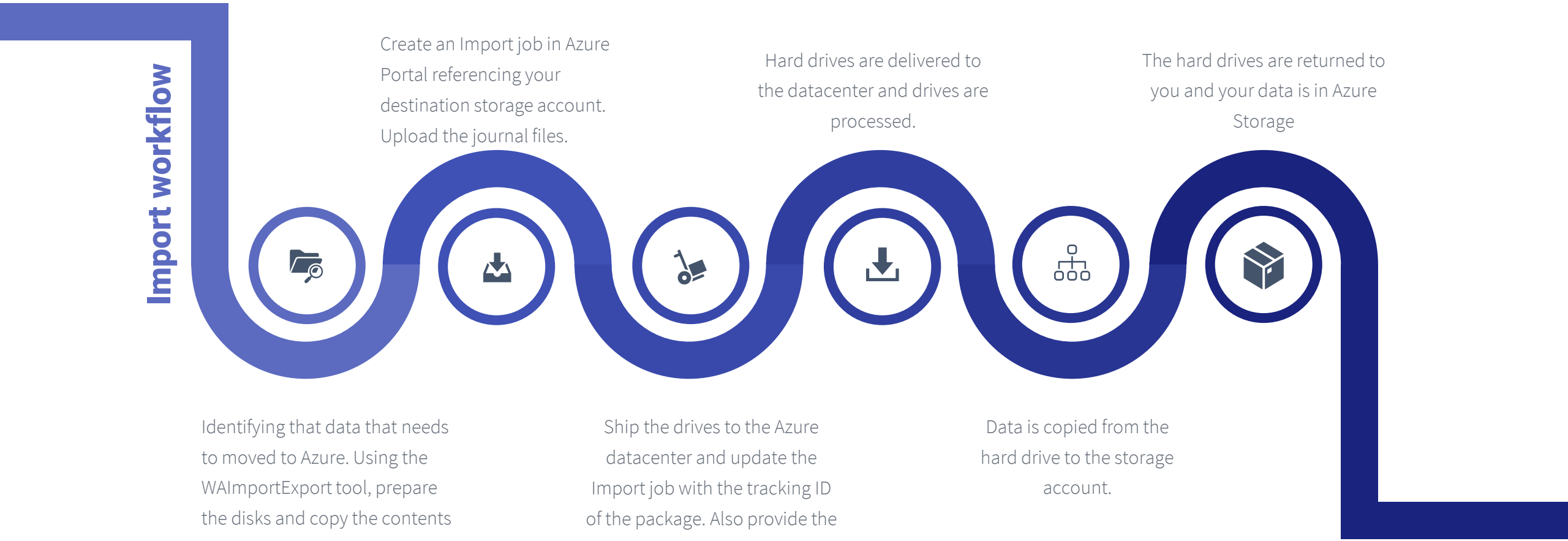




Import/Export Service

Using Import Service, you can import data from your on-premises environment to Azure

Import workflow

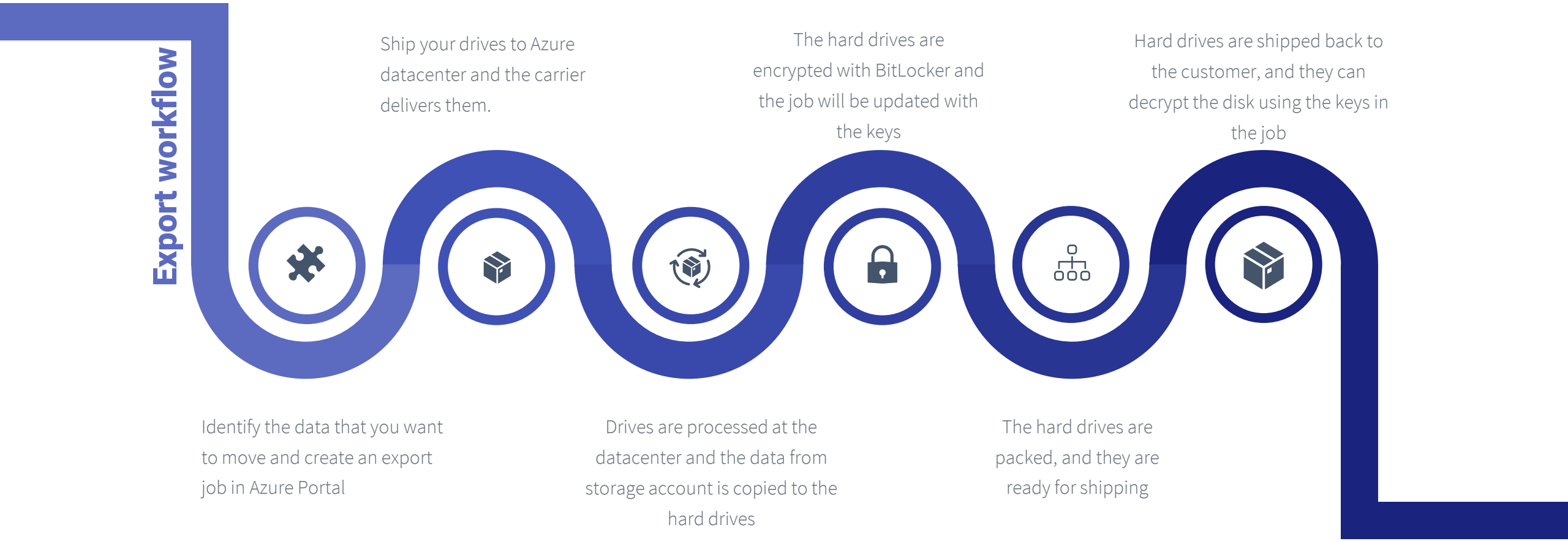


1. Identifying that data that needs to moved to Azure. Using the WAImportExport tool, prepare the disks and copy the contents to the disk. This will generate the journal files.
2. Create an Import job in Azure Portal referencing your destination storage account. Upload the journal files.
3. Ship the 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
4. Hard drives are delivered to the datacenter and drives are processed.
5. Data is copied from the hard drive to the storage account.
6. The hard drives are returned to you and your data is in Azure Storage

Import/Export Service

Using Export Service, you can import data from Azure and send it to your on-premises sites

Export workflow

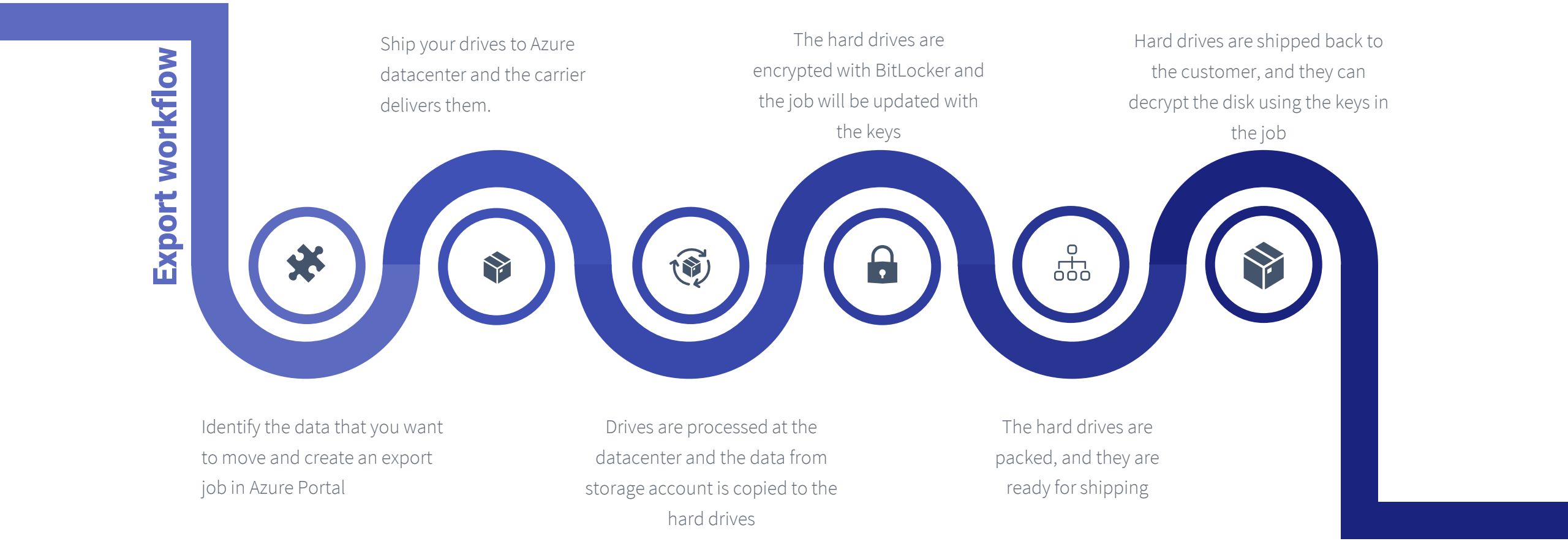


1. Identify the data that you want to move and create an export job in Azure Portal
2. Ship your drives to Azure datacenter and the carrier delivers them.
3. Drives are processed at the datacenter and the data from storage account is copied to the hard drives
4. The hard drives are encrypted with BitLocker and the job will be updated with the keys
5. The hard drives are packed, and they are ready for shipping
6. Hard drives are shipped back to the customer, and they can decrypt the disk using the keys in the job

Import/Export Service

Using Export Service, you can import data from Azure and send it to your on-premises sites

Export workflow



1. Identify the data that you want to move and create an export job in Azure Portal
2. Ship your drives to Azure datacenter and the carrier delivers them.
3. Drives are processed at the datacenter and the data from storage account is copied to the hard drives
4. The hard drives are encrypted with BitLocker and the job will be updated with the keys
5. The hard drives are packed, and they are ready for shipping
6. Hard drives are shipped back to the customer, and they can decrypt the disk using the keys in the job

Azure Data Box offerings

Reliable, quick, and inexpensive method to move large amount of data to Azure

Data box disk

- Amount of data that needs to be transferred is less than 40 TB (35 TB usable)
- Support for Azure Blob Storage
- USB SATA 2 and 3
- 128-bit encryption

Data box

- Device with 100 TB capacity that uses standard NAS protocols
- Rugged and hardened case
- Support for Azure Blob Storage
- AES 256-bit encryption

Data box heavy

- Rugged device that can help you transfer up to 1 PB of data
- AES 256-bit encryption

When to use Azure Data Box?

Ideal for scenarios where the network bandwidth is low and requires to transfer data more than 40 TB

Comparison of data migration solutions

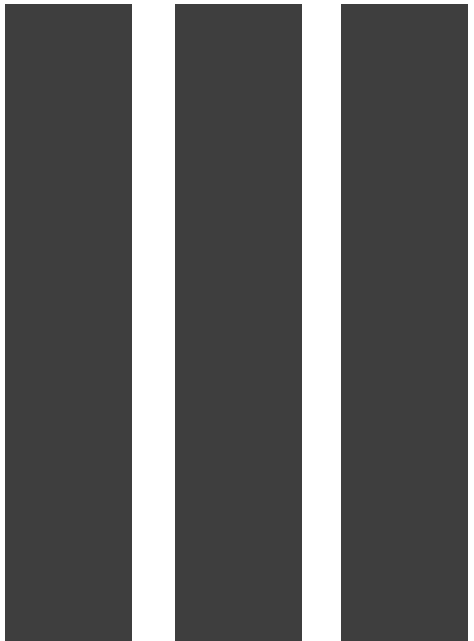
Selection of migration solution depends on the size of data and the network bandwidth

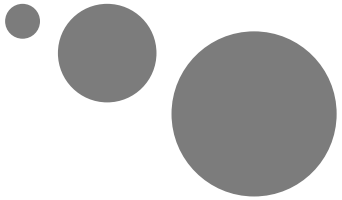
Dataset	Solution to use
Large dataset with low-bandwidth network or direct connectivity to on-premises storage is restricted by policies	Export: Azure Import/Export or Data Box Import: Data Box Disk or Data Box (in supported regions), Azure Import/Export
Large dataset with high-bandwidth network (1 Gbps to 100 Gbps)	AZCopy for online transfers; or to import data, Azure Data Factory, Azure Stack Edge, or Azure Data Box Gateway
Large dataset with moderate-bandwidth network (100 Mbps - 1 Gbps)	Azure Import/Export or Azure Data Box family where it is supported
Small dataset (few GBs to a few TBs) with low to moderate-bandwidth network: up to 1 Gbps	Azure Storage Explorer, Azure portal, AZCopy, Azure PowerShell or AZ CLI

KodeKloud

KodeKloud

Module 10 : Design a business continuity solution





Design for backup and recovery

Design for backup and recovery

Planning of backup and recovery starts with identifying the business requirements and onboarding the workloads

- **Workloads**
- **Usage patterns**
- **Availability metrics**
- **Recovery metrics**
- **Workload availability and SLA**

Design for Azure Backup

Design for Azure Backup

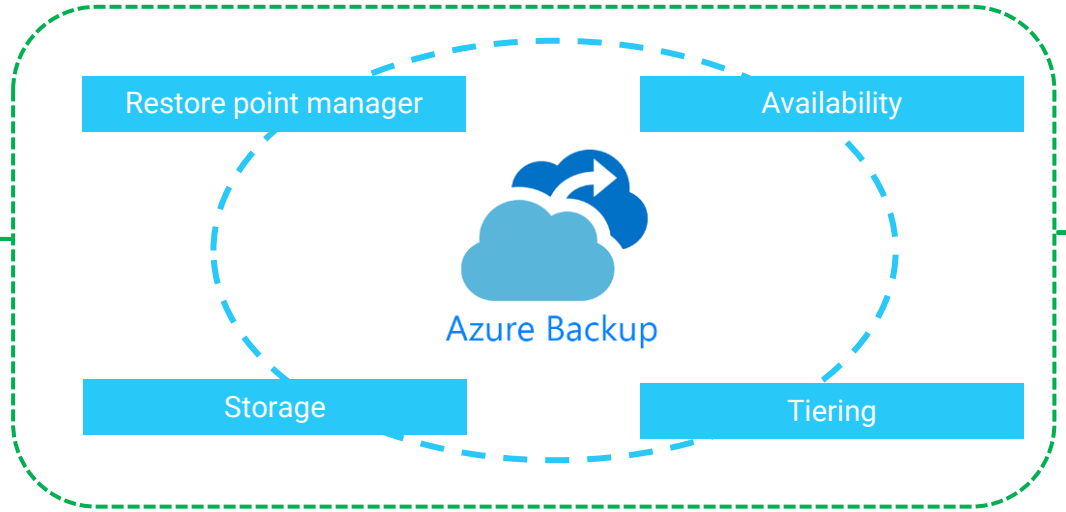
Azure Backup is a service which can be used to backup Azure and non-Azure workloads

Backup agents

- On-premises
- Non-Azure workloads

Built-in backup

- Azure VM
- Azure file share
- Microsoft SQL server in Azure VMs
- SAP HANA databases in Azure VMs



Backup vault

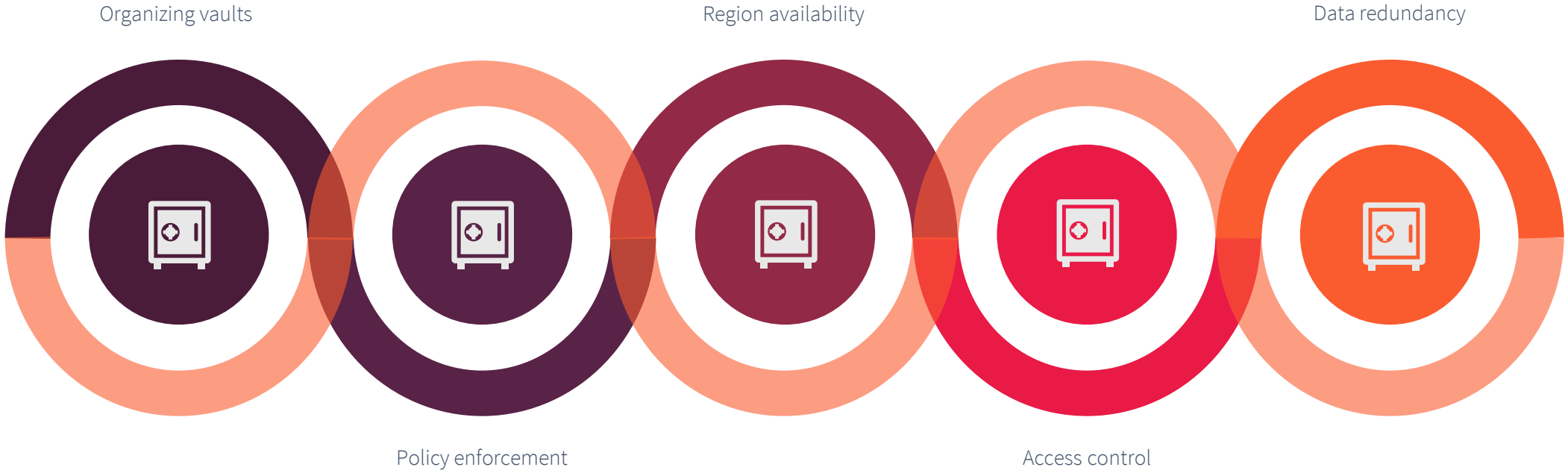
- Azure database for PostgreSQL servers
- Azure blobs
- Azure disks

Recovery services vault

- Azure VM
- SQL in Azure VM
- SAP HANA in Azure VM
- Azure Backup Server
- Azure Backup Agent
- DPM

Vault- Considerations

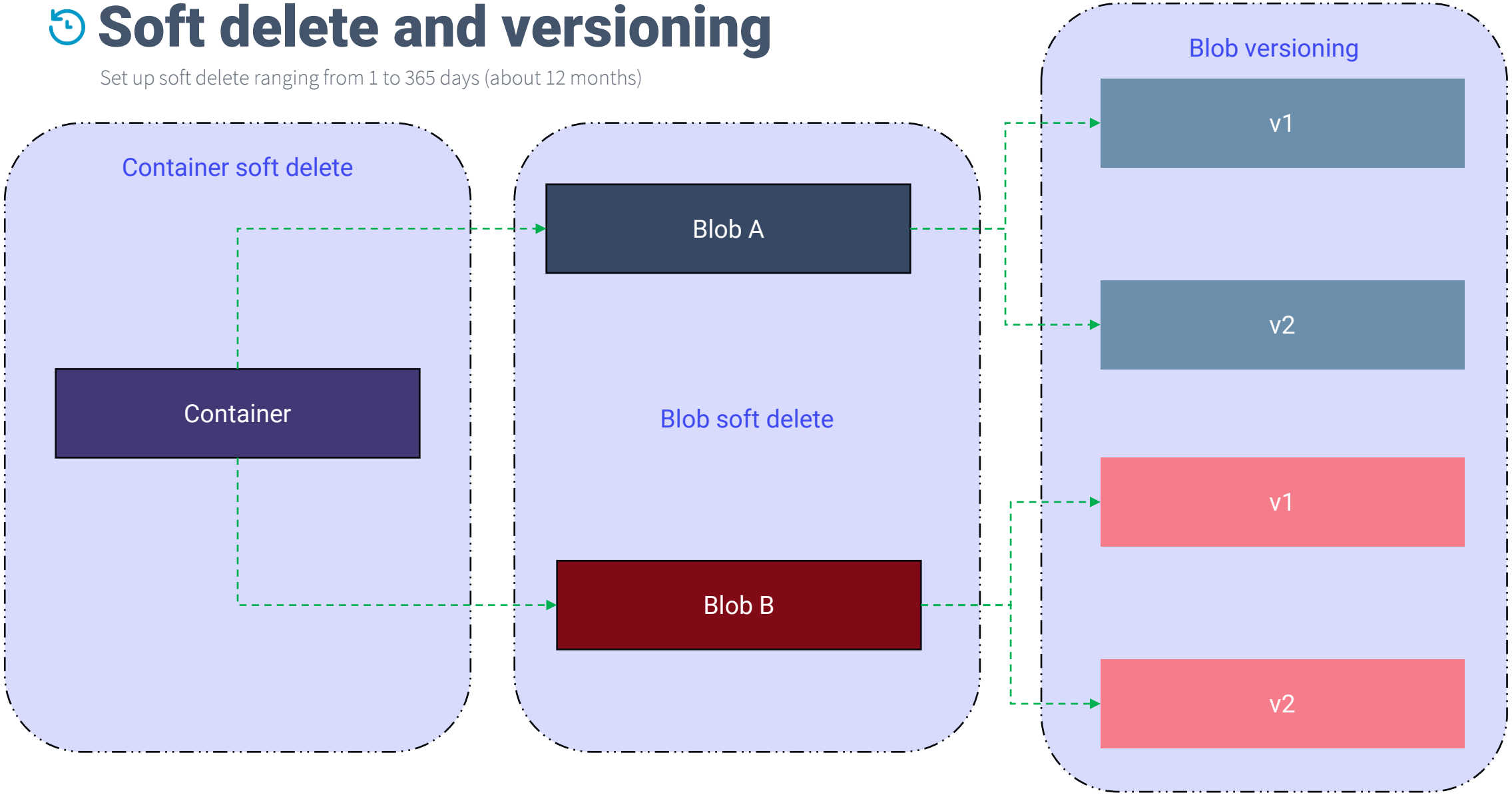
Keep the following considerations in mind while designing



Design for Azure blob backup and recovery

Soft delete and versioning

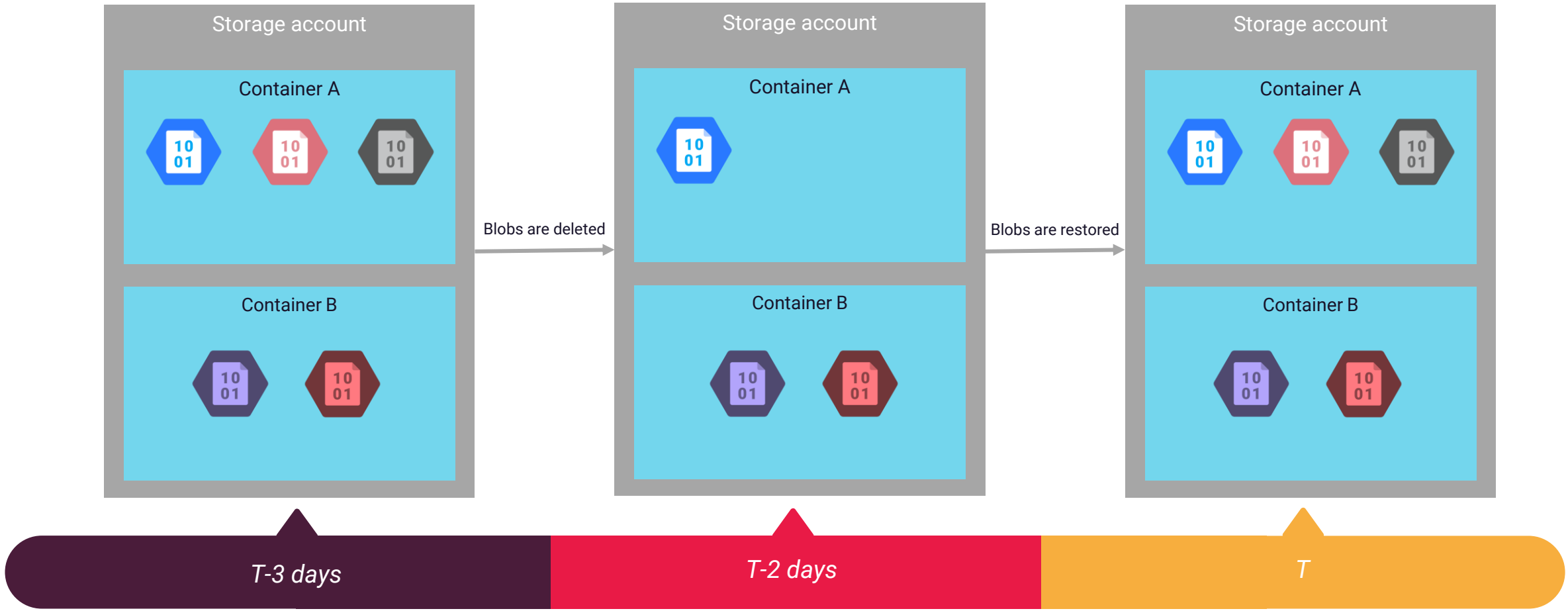
Set up soft delete ranging from 1 to 365 days (about 12 months)



KodeKloud

PITR for blobs

Protect your blobs from accidental deletion or corruption using point-in-time restore for blobs

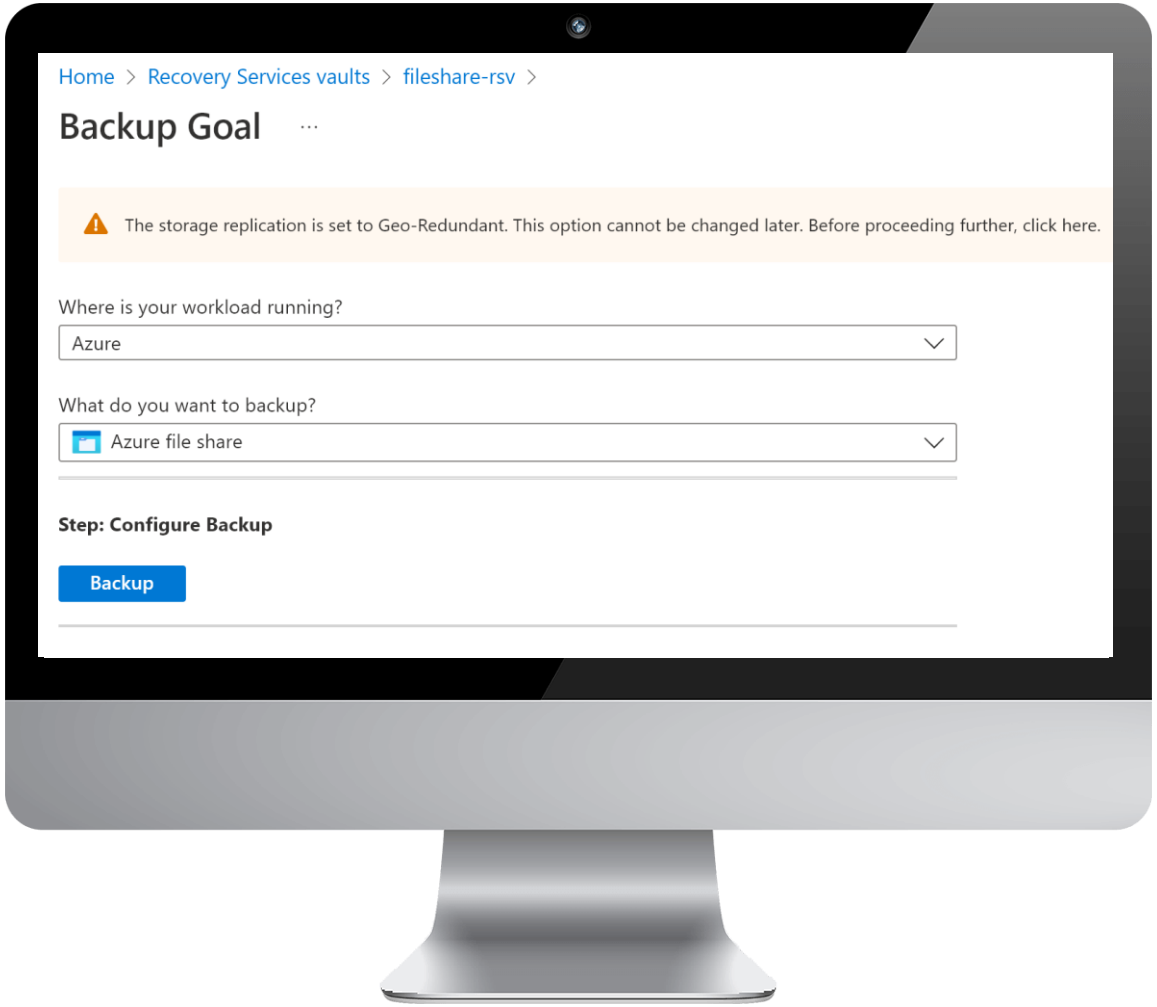


Design for Azure files backup and recovery

Azure files backup and recovery

With the help of share snapshots, we can take snapshot of our file shares and store in a recovery services vault

- Snapshots enables you to capture point-in-time state of your file share and this can be created using Azure Portal, Azure PowerShell, Azure CLI, REST and SDK
- Snapshot is taken at the root level of the file share comprising all files and folder in the share. In case of restore, we can go till individual file level
- All snapshots taken are incremental, only the changes between the snapshots will be stored in the snapshot
- After creation, snapshots can be read, copied or deleted, but not modified. Also, we cannot delete any file share that has snapshots associated to it.
- Snapshot creation process is manual; however, you can integrate with Backup policies to automate the snapshots.



Design for Azure VM backup and recovery

Azure VM backup and recovery

By onboarding the VM to recovery service vault and associating with a backup policy, we can take backup of Azure VMs

Snapshot tier: These are stored locally, and the retention is 5 days. Offers easier restore also known as Instant Restore

Vault tier: Snapshots taken locally are transferred to recovery service vault for retention and additional security

Backup schedule

Group VMs that needs to start backup together using backup policies. Consider scheduling backup during non-peak hours. For better distribution of traffic, consider multiple policies for different groups.

Retention policies

Set up both short-term and long-term backup and decide the retention period as per your business requirement. If you don't want to schedule backup, you can take backups on-demand

Revisit backup policies

As business requirements change, ensure that you revisit the backup policies and update them to align to the current business requirements

CRR

Cross Region Restore enables you to restore Azure VMs in the Azure paired region. You can enable in feature in the vault and use this for DR drills or when there is disaster in the primary region

Design for Azure SQL backup and recovery

KodeKloud

Azure SQL backup and recovery

Following backups will be taken by Azure for ensuring the consistency of backup

Every week

Full backup

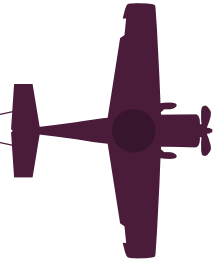
12 - 24 h

Differential backup

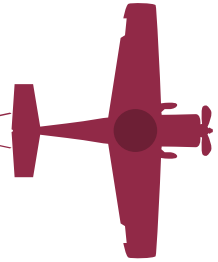
5 -10 m

Tx log backup

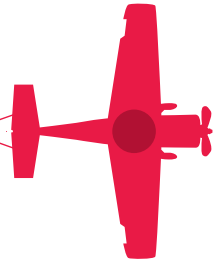
Full backup consists of everything in the database which include the data files and log files

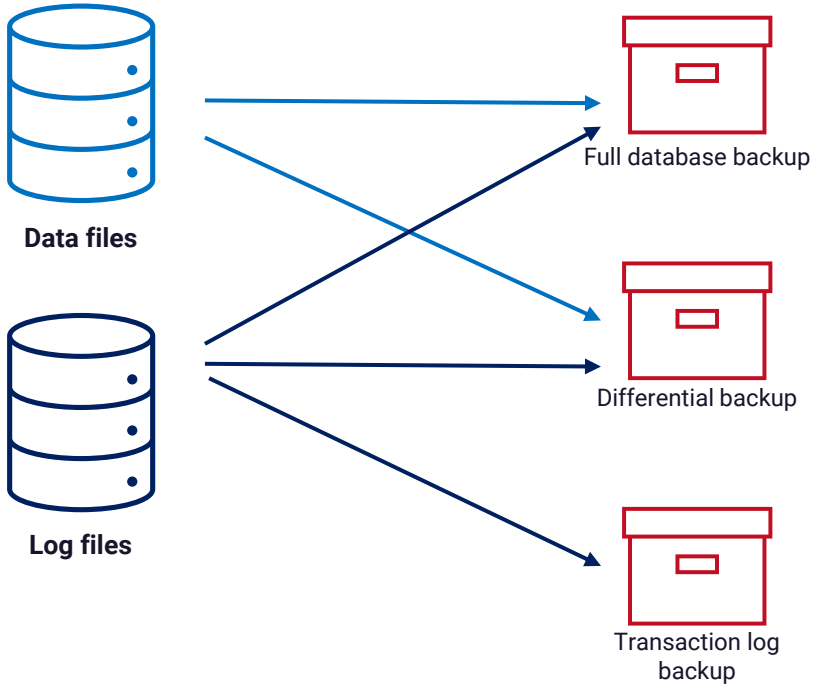


Any delta since the last full backup is backed up in differential backup



Transaction log files are backed up. This enables DB admins to fall back to previous transaction log backup if the transaction log fails





Azure SQL backup – Use cases

Following are some of the scenarios where you can rely on the SQL backup

01

Restore an existing DB to point-in-time in the past

Within the retention period, you can choose any point and restore your database. This process creates a new database on the same server with a different name to avoid overwriting the existing database. You can delete the database after restore is complete

02

Restore a deleted database to the time of deletion

We can restore the database to any point within the retention period or to the time of deletion. Restore process can be only done to the same server or managed instance from which the database was deleted.

03

Restore a database to another Azure region

If the primary region is not available, then you cannot access the database or the backups in the primary region. In this case, we can use the geo-restore option to create a new database on any existing server or managed instance in any Azure region.

04

Restore a database from a specific long-term backup

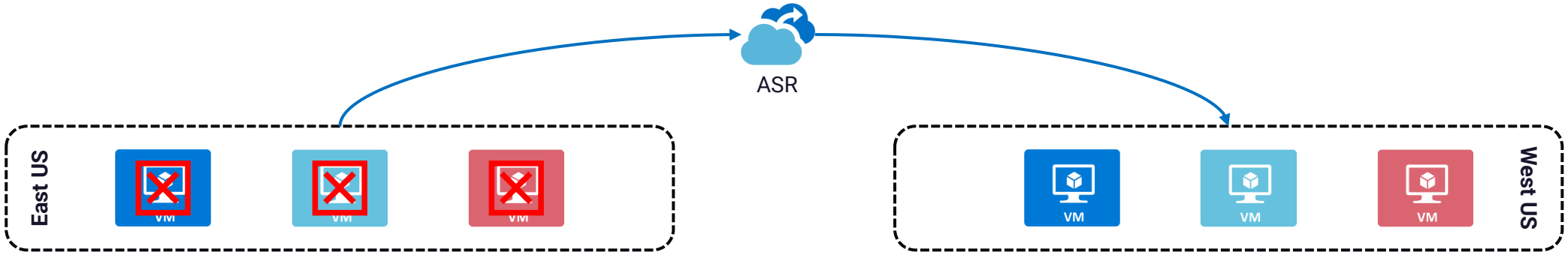
The retention period for automatic backup is 35 days, this adequate for most of the scenarios. However, if your organization requires to store the backup for a longer period, then you can opt for LTR backup up to 10 years. With LTR, you can restore to an older version of the database.

Design for Azure Site Recovery

KodeKloud

Azure Site Recovery

Disaster recovery for Azure, on-premises, and other cloud providers



01

BCDR

With ASR, we can replicate the infrastructure to a secondary site and failover if required. ASR also helps you to conduct DR drills

02

Migration

Though we have Azure Migrate, we can use ASR to replicate infrastructure from on-premises and cut over once the replication is done

03

Replication

Enables you to replicate your Azure VMs between regions.

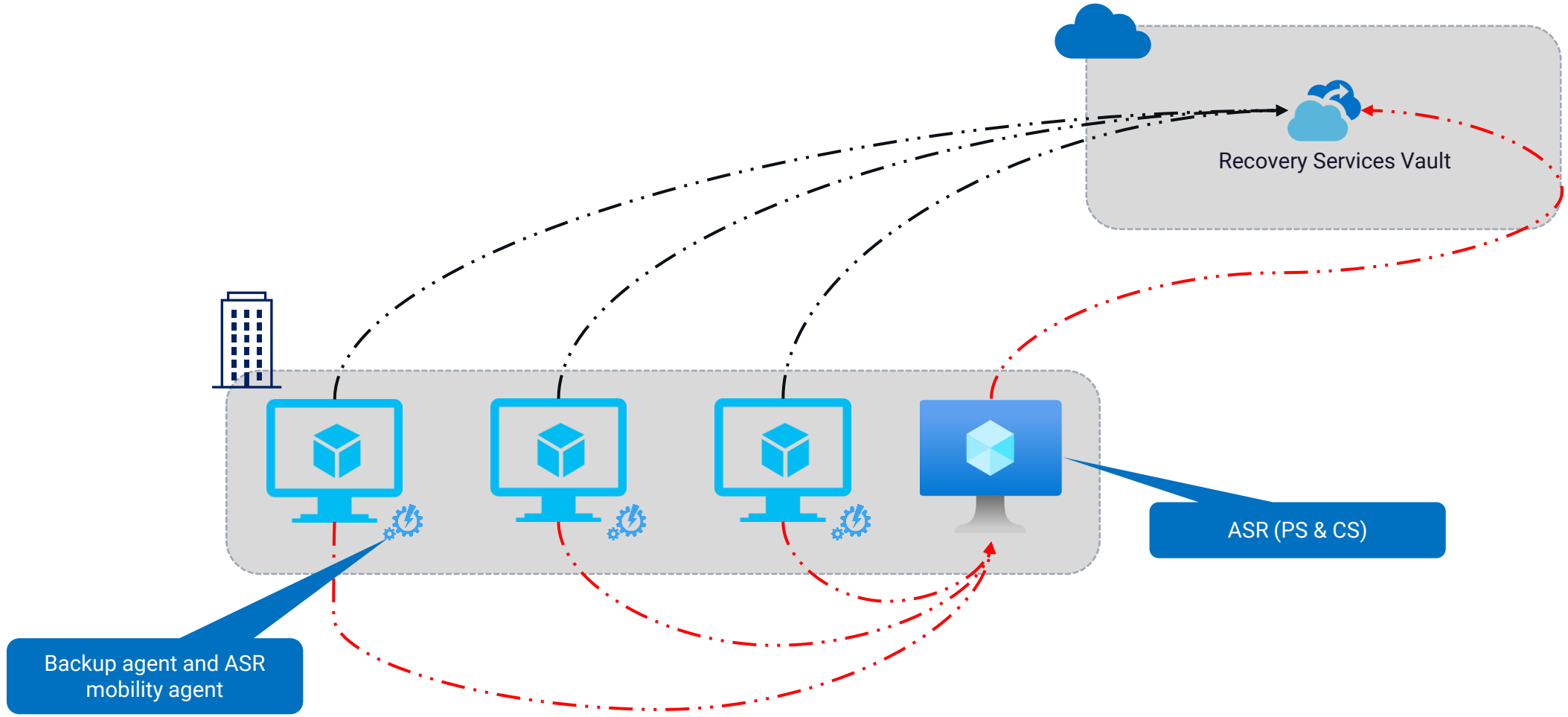
04

Retention

You can define the retention period of the replicated restore points

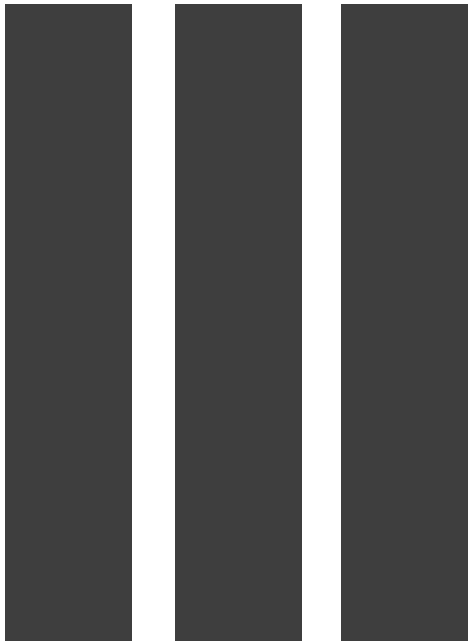
Combining ASR and Azure Backup

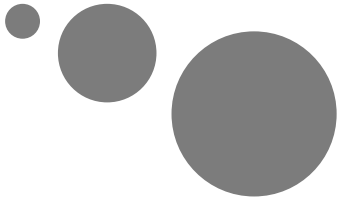
Ideal for scenarios where you need backup and disaster recovery



KodeKloud

Module 11 : Design an app architecture solution





Differentiate event and message

Differentiate message and event

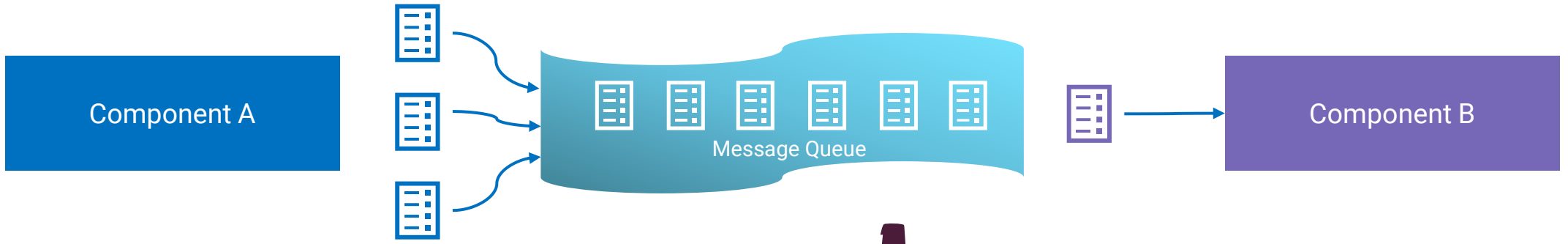
Understand difference between message and event

Type	Definition	When to use?
Message	Comprises of raw data, generated by one component and will be consumed by another component Message contains the data itself, not just the reference to the data	Ideally used where distributed applications requires a guarantee that the communication will be processed.
Event	Lightweight than messages and most often used for broadcast communications. Consists of a publisher (which sends the events)and a subscriber (which receive the events)	Mostly used for broadcasts and are often ephemeral. Ephemeral as in the communication might not be handled by any receiver if none is currently subscribing.

Design a messaging solution

Design for Azure Queue storage

With the help of Azure Queue storage, we can store large number of messages that needs to be processed asynchronously



Queues can be accessed with authenticated calls using HTTP or HTTPS

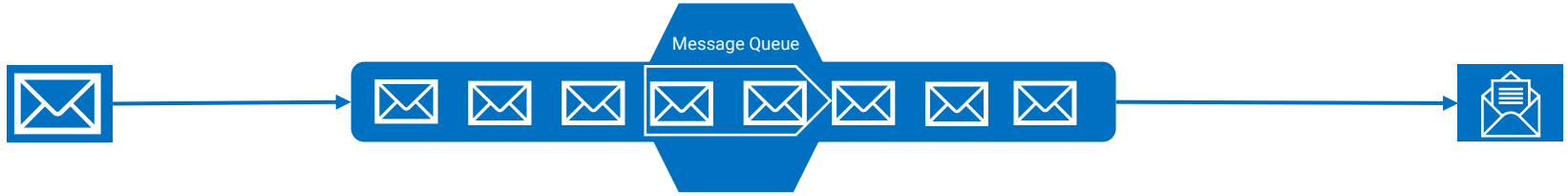
Size of messages can be up to 64 KB

A queue may contain millions of messages or up to the total capacity of the storage account

KodeKloud

Design for Service Bus

Learn Azure Service Bus Queues



Message broker system built on top of dedicated messaging infrastructure

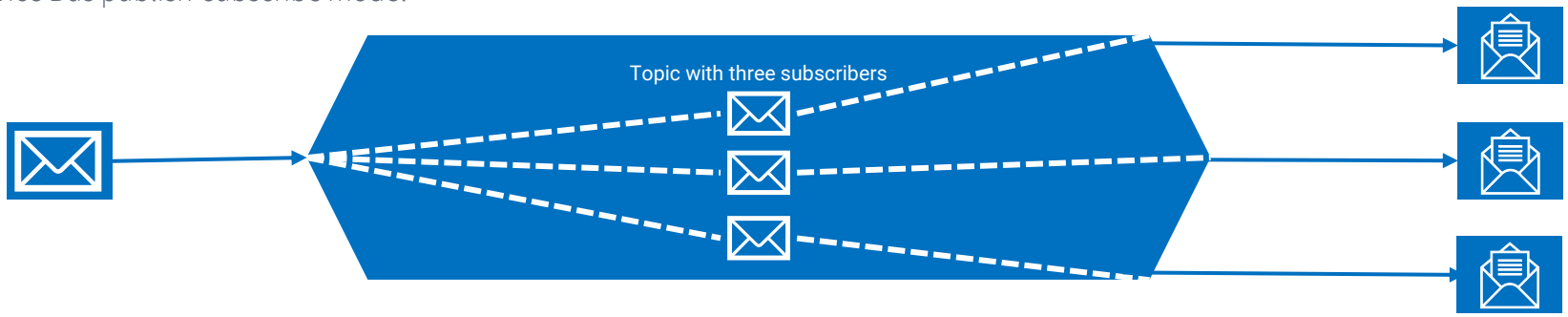
Like Azure Queues, Service Bus Queues offers delivery guarantee

Built for enterprise applications that requires a dedicated messaging broker

KodeKloud

Design for Service Bus

Learn Azure Service Bus publish-subscribe model



Message broker system like Service Queues but follows a publish subscribe model, means you can have multiple subscribers

Messages sent to a topic will be forwarded to all receivers that are subscribed to be topic

With multiple subscribers, you can have multiple actions triggered when a message comes

Comparison between the messaging services

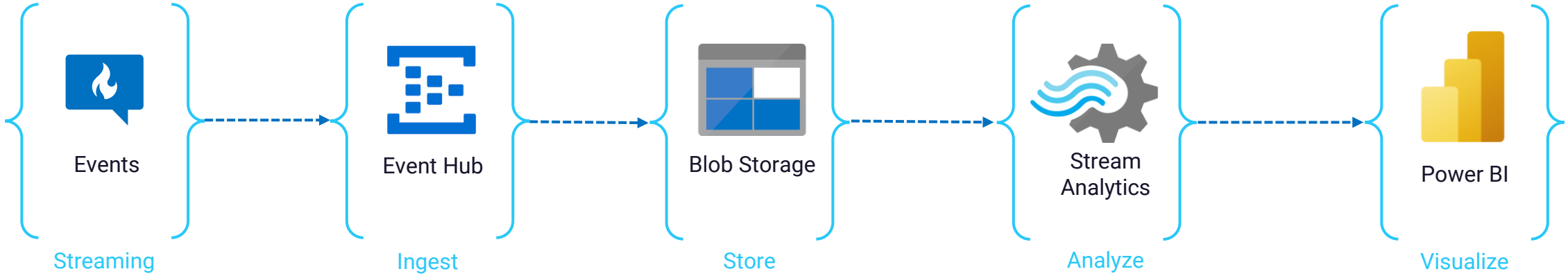
Comparison between Azure Queues, Azure Service Bus queues, and Azure Service Bus publish-subscribe topic

Solution	Use cases	SLA
Queue storage	• Simple queue to organize messages • Size exceeds 80 GB • Message tracking once the message is inside the queue	Storage tier dependent
Service bus queues	• FIFO guarantee • Peek-Lock receive mode • Receive and Delete receive mode • Operations can be grouped to transactions • Doesn’t require polling to receive messages. • Batches of messages can be published and consumed.	99.9%
Service bus topics	• Multiple receivers to handle each message • Multiple destinations for a single message	99.9%

Design an event solution

Design an Event Hub messaging solution

Fully platform managed ingestion service that supports real time data



Anomaly detection and live visualization in dashboards

Analytics pipelines like clickstreams, and transaction processing with real-time analysis

Event Hub - considerations

Following considerations should be considered if you are building a solution with Event Hub

01

Language and framework integration

Different languages can be used to send and receive events. Apache Storm can be also used to receive messages from Event Hubs.

02

Tier and throughput

Based on the number of processing units or throughput units purchased we can control the scaling of event hubs. Basic, Standard, Premium, and Dedicated tiers are being available.

03

Pull model

Event hub holds the message in it cache for consumers to read. With the pull model, Event Hub doesn't delete message after read, it will be kept for more consumers to consume.

04

Data failures

Event Hubs doesn't have any process to handle messages that aren't processed. When you design a solution using Event Hubs, ensure you account for this.

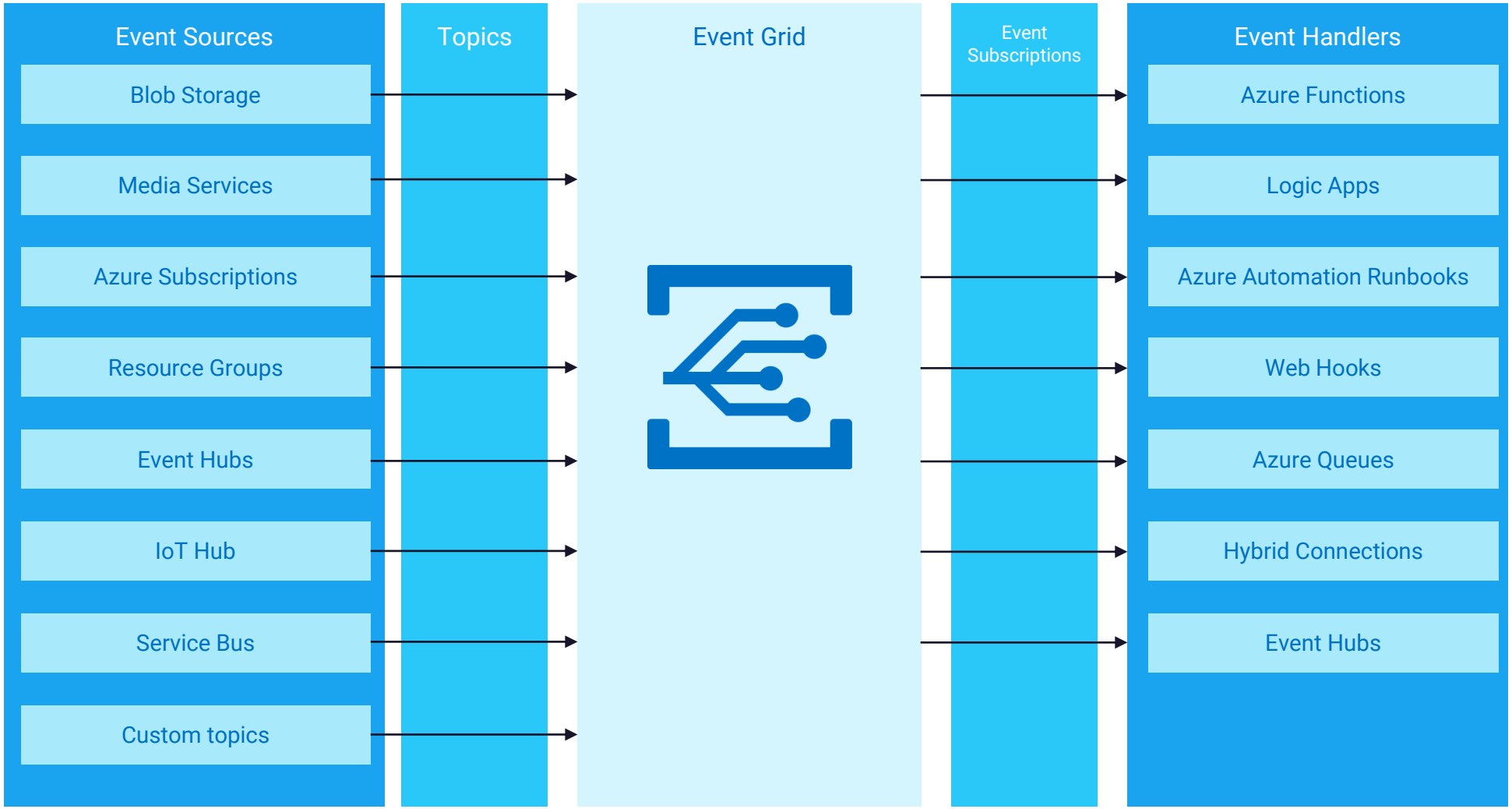
05

Data stream

Received events are added to the end of Event Hub's data stream. The order of the data stream is based on the time the events are received.

Design an event driven solution

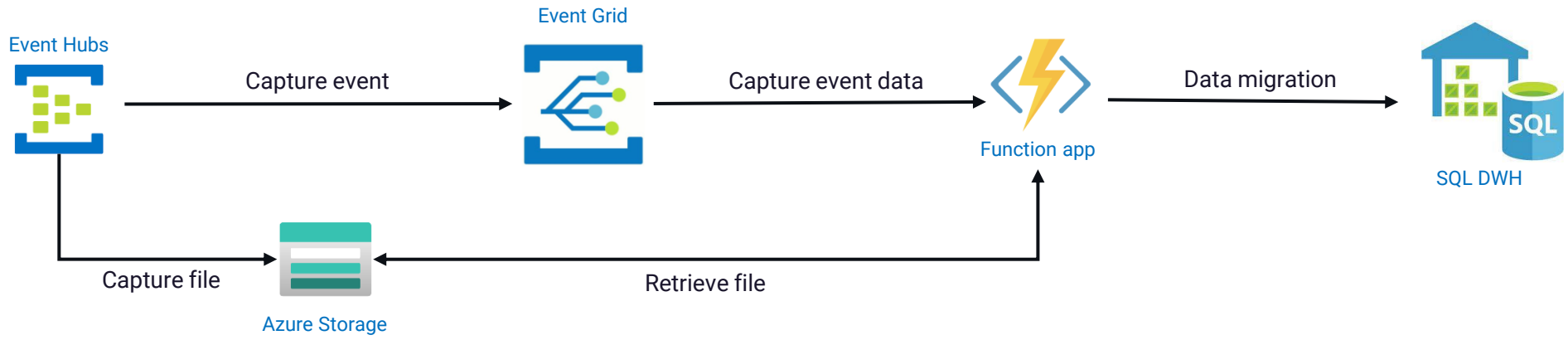
Implement an event driven solution using Azure's fully platform managed event routing service which is running on top of Azure Service Fabric



Comparison and combination of services

Let's review the messaging and event solutions and understand their applications

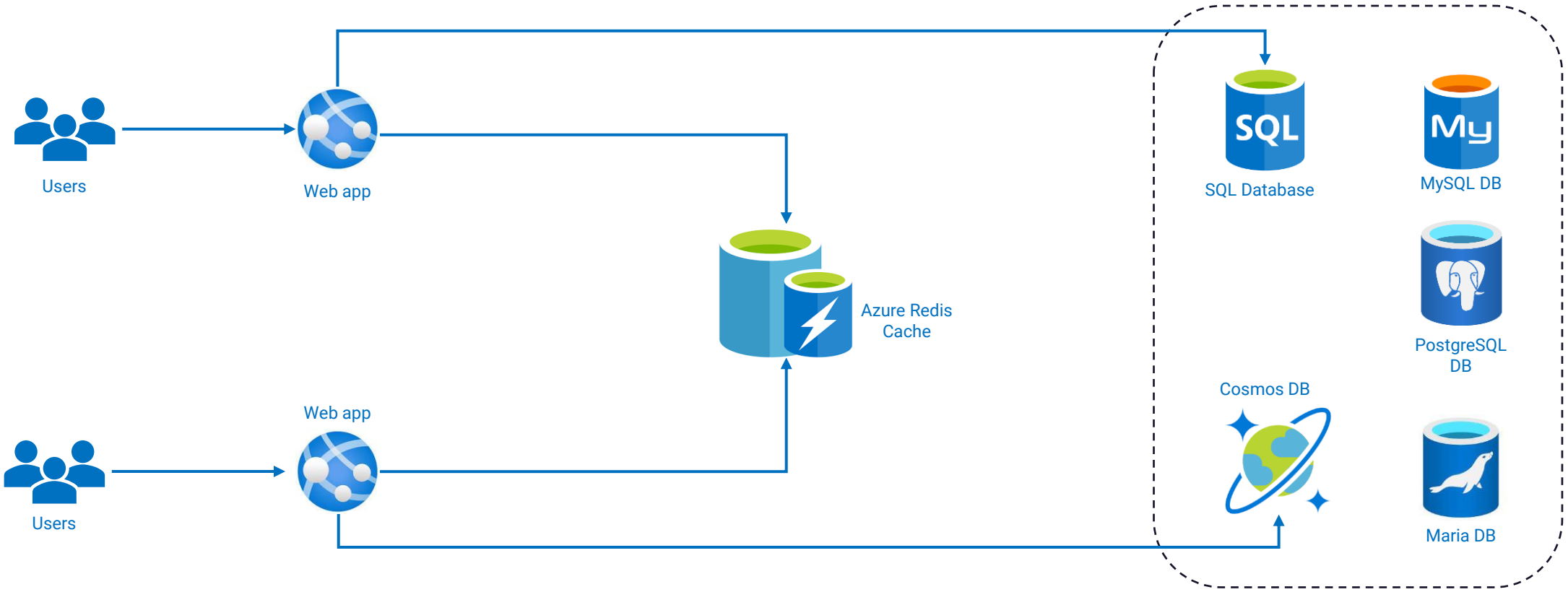
Service	Purpose	Type	When to use
Event Grid	Reactive programming	Event distribution (discrete)	React to status changes
Event Hubs	Big data pipeline	Event streaming (series)	Telemetry and distributed data streaming
Service Bus	High-value enterprise messaging	Message	Order processing and financial transactions



Design an application optimization solution

What is Azure Redis Cache?

Cache frequently accessed data for ease of access by applications



When to use Azure Redis Cache?

Cache frequently accessed data for ease of access by applications

01

Caching

It's not easy to load the entire database into a cache. With the cache-aside pattern, we can load cache data as required. When the data in the database is updated by the system, we can update the cache as well. Alternatively, we can set up TTL and trigger updates when TTL is expired.

02

Content Cache

Static content in webpages such as header, footers and banners can be cached to save the page load time. With the help of Redis Output Cache Provider we can cache static content in ASP.NET applications

03

Session persistence

Instead of increasing the size of cookie for session persistence, we can use the cookie as a key to query the database to retrieve the user information. With Azure Redis, we can easily retrieve the user information much faster than relational database.

04

Task queuing

With built-in distributed queue we can queue the long running operations to be processed in a sequence. This pattern is taken when the tasks take more time than expected.

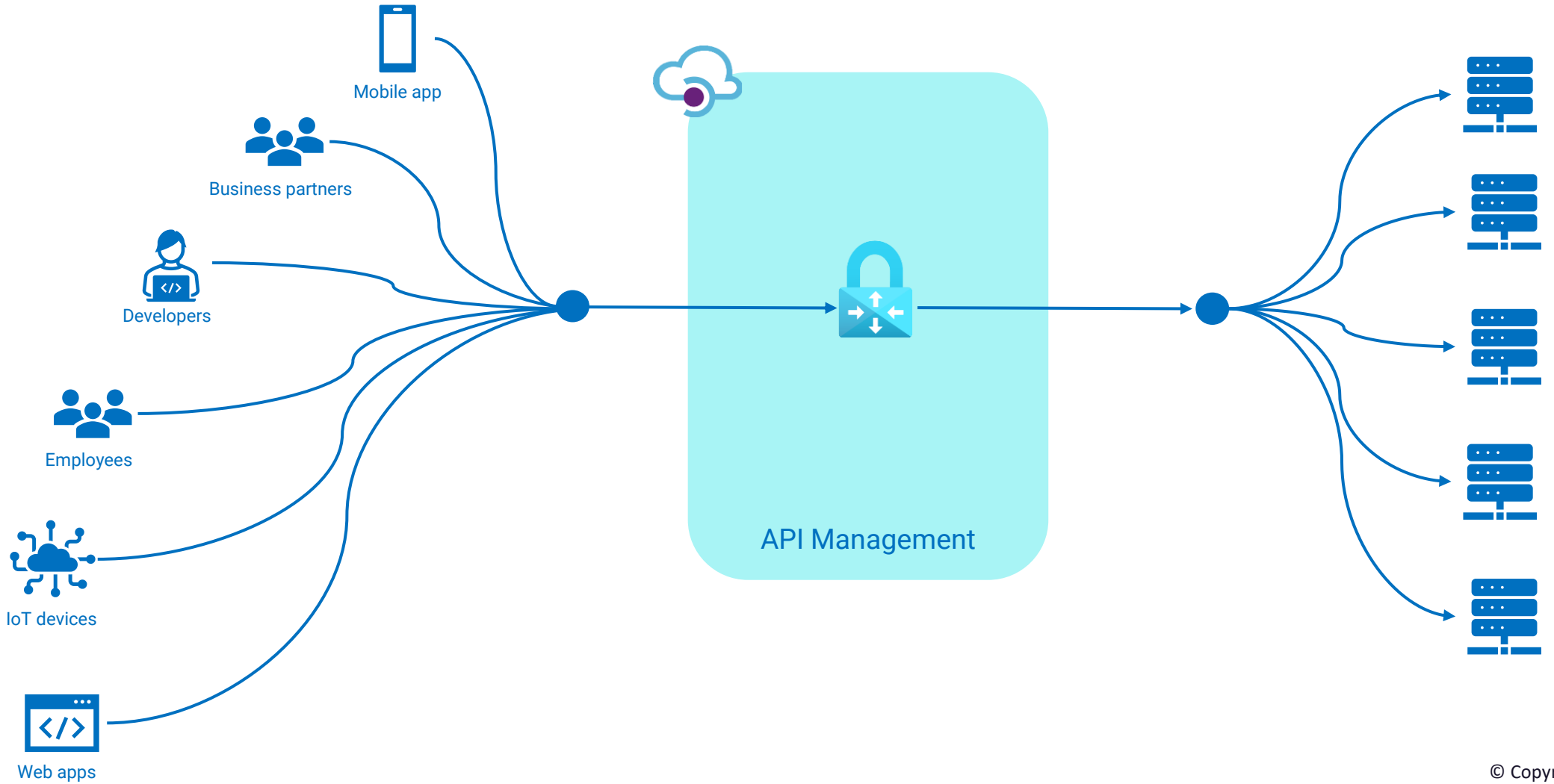
05

Distributed transactions

Some applications requires a series of operations to be executed as a single operation against the datastore. If one of these operations goes wrong, then we must roll back to the previous state. With Azure Redis Cache, we can execute a series of commands as a single operation.

What is Azure API Management?

Publish, manage, secure, maintain, and analyze all your APIs using a fully managed cloud service

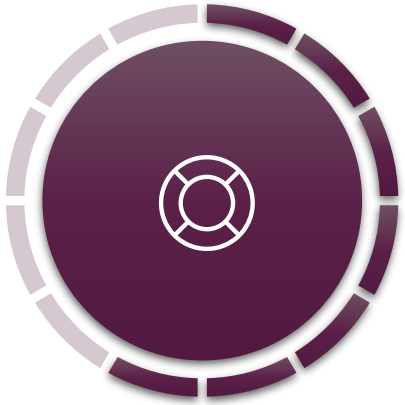


Should we use API Management?

API Management may not be the apt solution when you want to host a small, static, or simple API

Number of APIs

The more APIs you have in your environment, higher the need for a centralized solution for API control



Rate of change of APIs

The rate at which API revisions and versions released also influences the need for centralized API control

API Administration Load

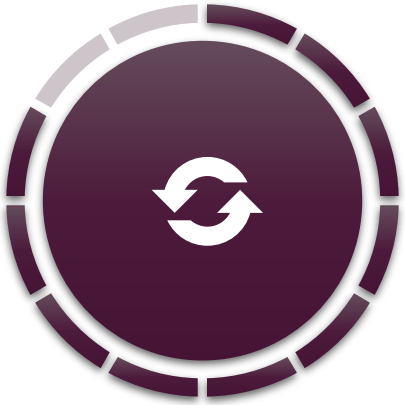
If you need to implement usage quota, rate limits, request transformations, policies, and validation then you need API management

Standardize APIs → Centralize APIs operations → Secure APIs

Design an application lifecycle

Infrastructure-as-Code

Provision your infrastructure in an automated fashion with the help of IaC tools.

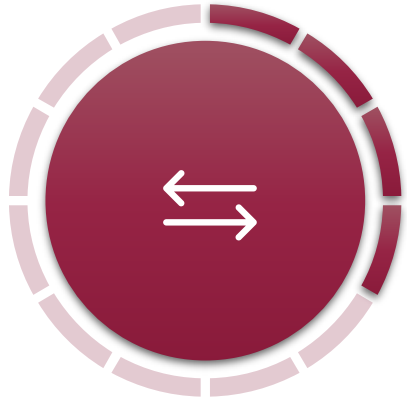


Repeatable results

You can deploy the same template repeatedly and get the same results

Testing and development

With the help of IaC, we can easily spin up test environments using templates

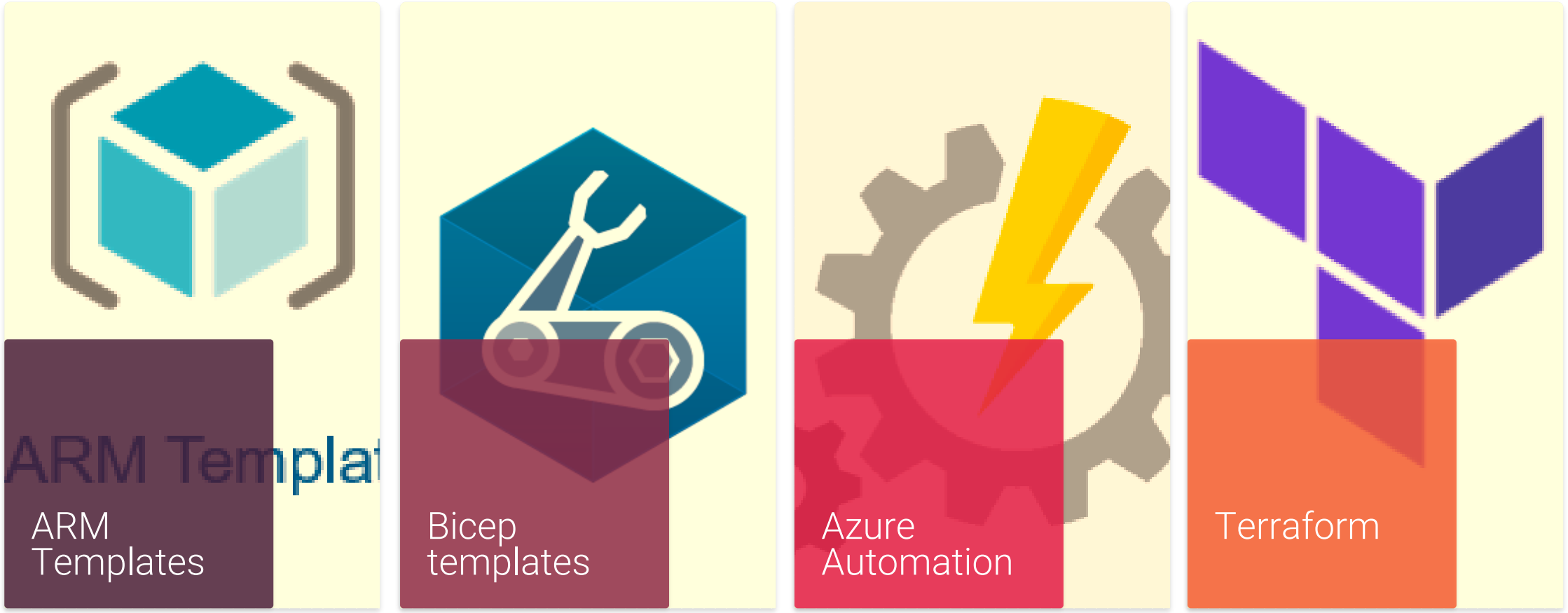


Avoids environmental drift

With the help of state management, we can ensure that there is no environmental drift

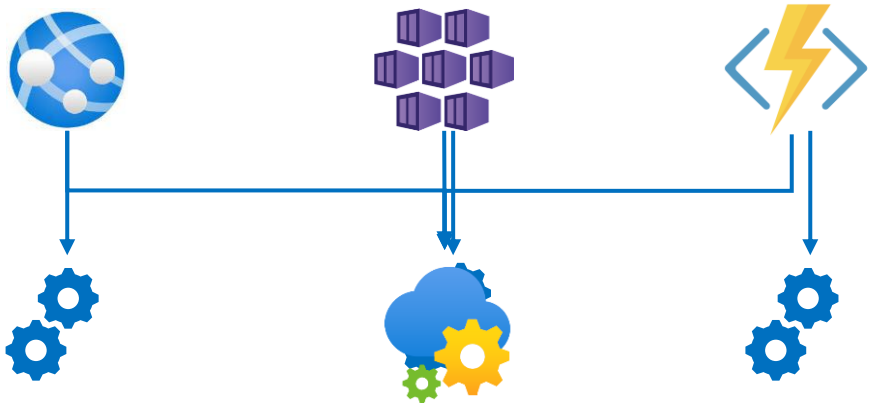
Infrastructure-as-Code

Provision your infrastructure in an automated fashion with the help of IaC tools.



App Configuration

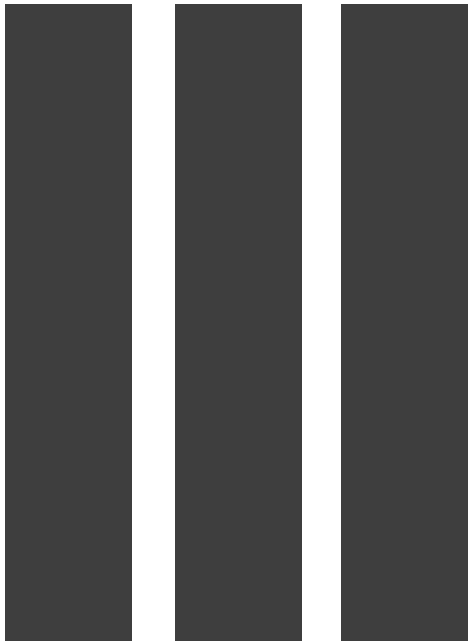
Fully managed service that can be used to centralize application settings and feature flags

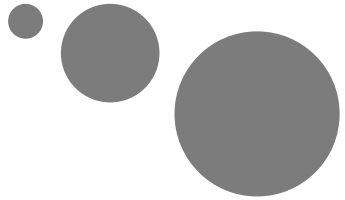


- Easy and flexible approach for key representations and mappings.
- Fully managed service which can be configured in minutes
- Labels can be used to tag configurations
- Point-in-time replay of settings and native integration will popular frameworks
- Compare two configurations and understand the changes
- Enhanced security with the help of managed identities

KodeKloud

Module 12 : Design a logging and monitoring solution

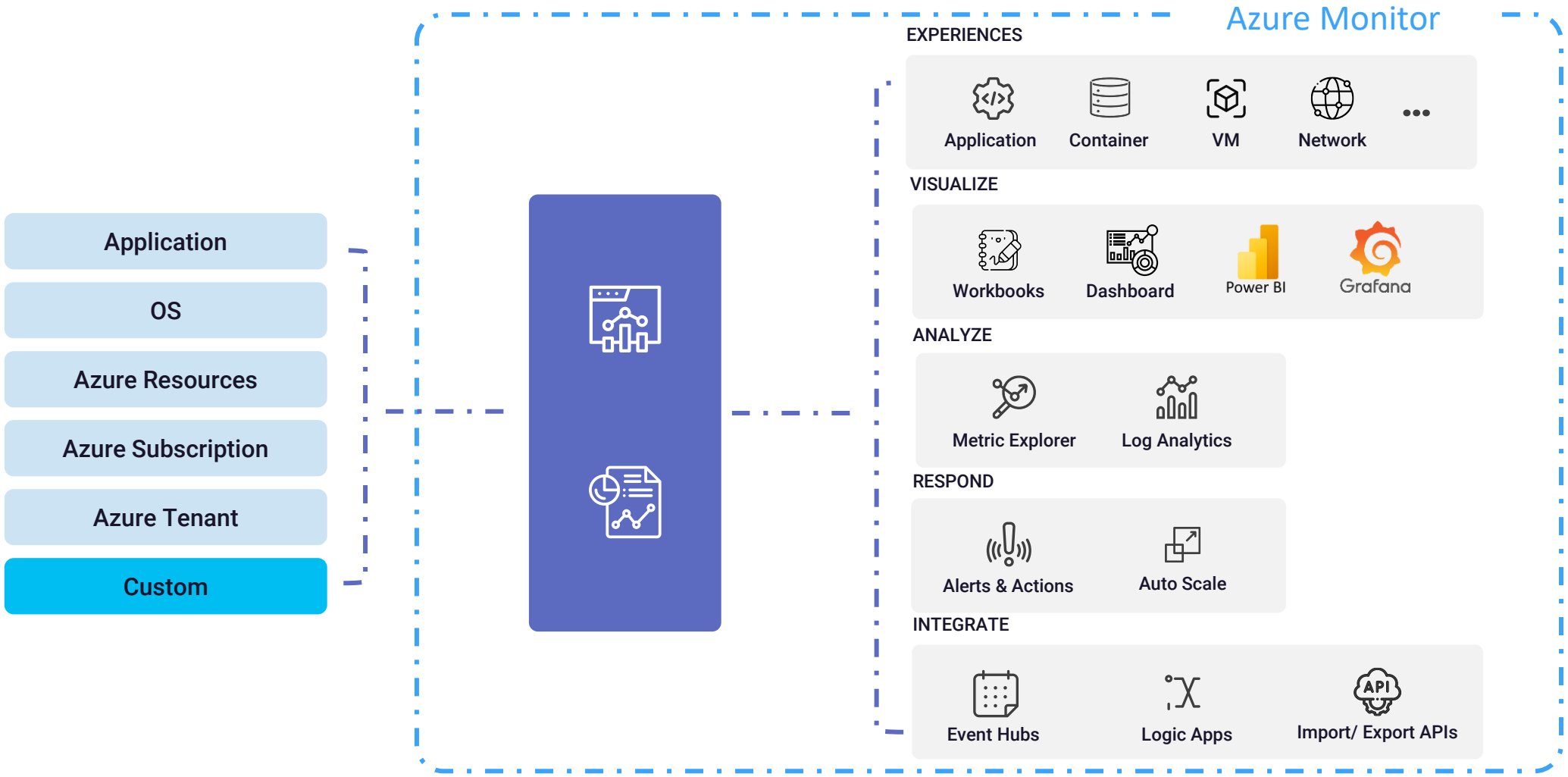




Design for Azure Monitor

Azure Monitor - Overview

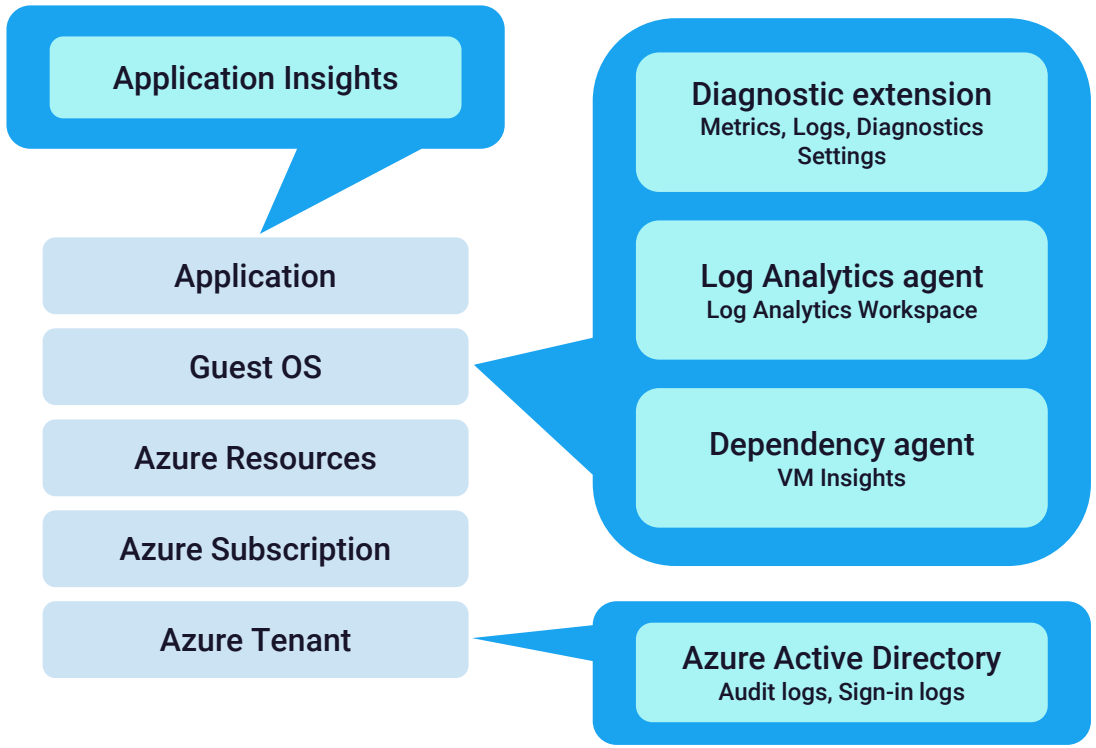
Centralized solution to manage monitoring for Azure and non-Azure solutions



Data sources

Identifying data sources for collection of logs and metrics

- Supports collection of data from different tiers starting from Application level (highest) all the way up to Azure platform level (lowest) .
- Collection of data from different tier varies – some uses agent while others are available out of the box.
- Collected data can be ingest to internal services such as Log Analytics, Azure Storage, Event Hub etc. or to external systems like Grafana, Splunk etc.
- Thumb rule is understanding the data you need and prioritizing them. Enabling all of them will be influence the billing. So, start prioritizing and collect only the data you need for monitoring.



Design for Log Analytics

What is Log Analytics?

Managed service which lets you collect and analyze data that is ingested from Azure Monitor

Data collection

Data generated from resources in cloud and on-premises can be collected to Azure Log Analytics workspace. Azure monitor stores the data in LAW

Querying and consolidation

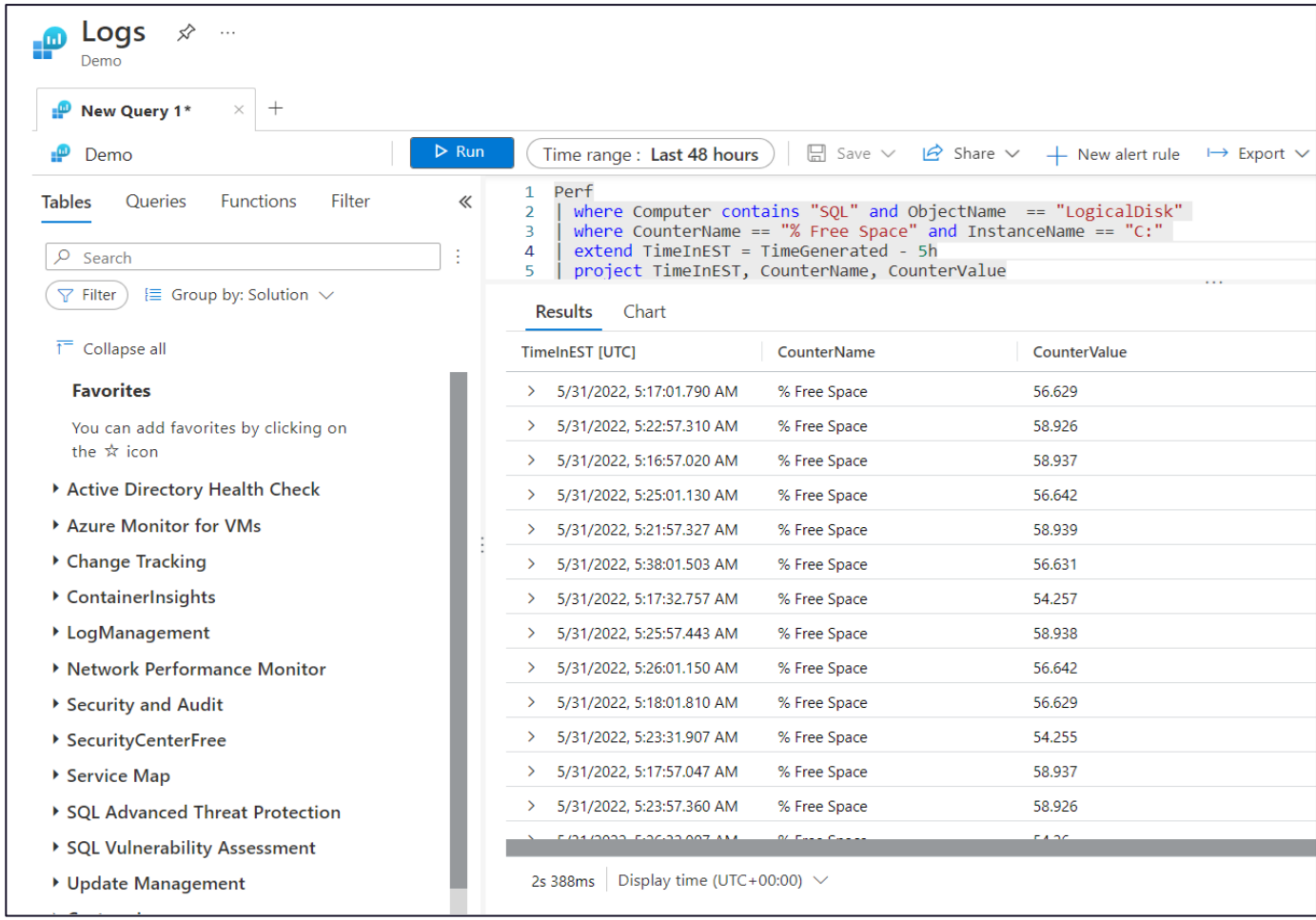
Use KQL to create rich reports and visualization. Data collected is organized into different tables which you can query

Data residency

Workspaces can be created in different regions to provide data residency.

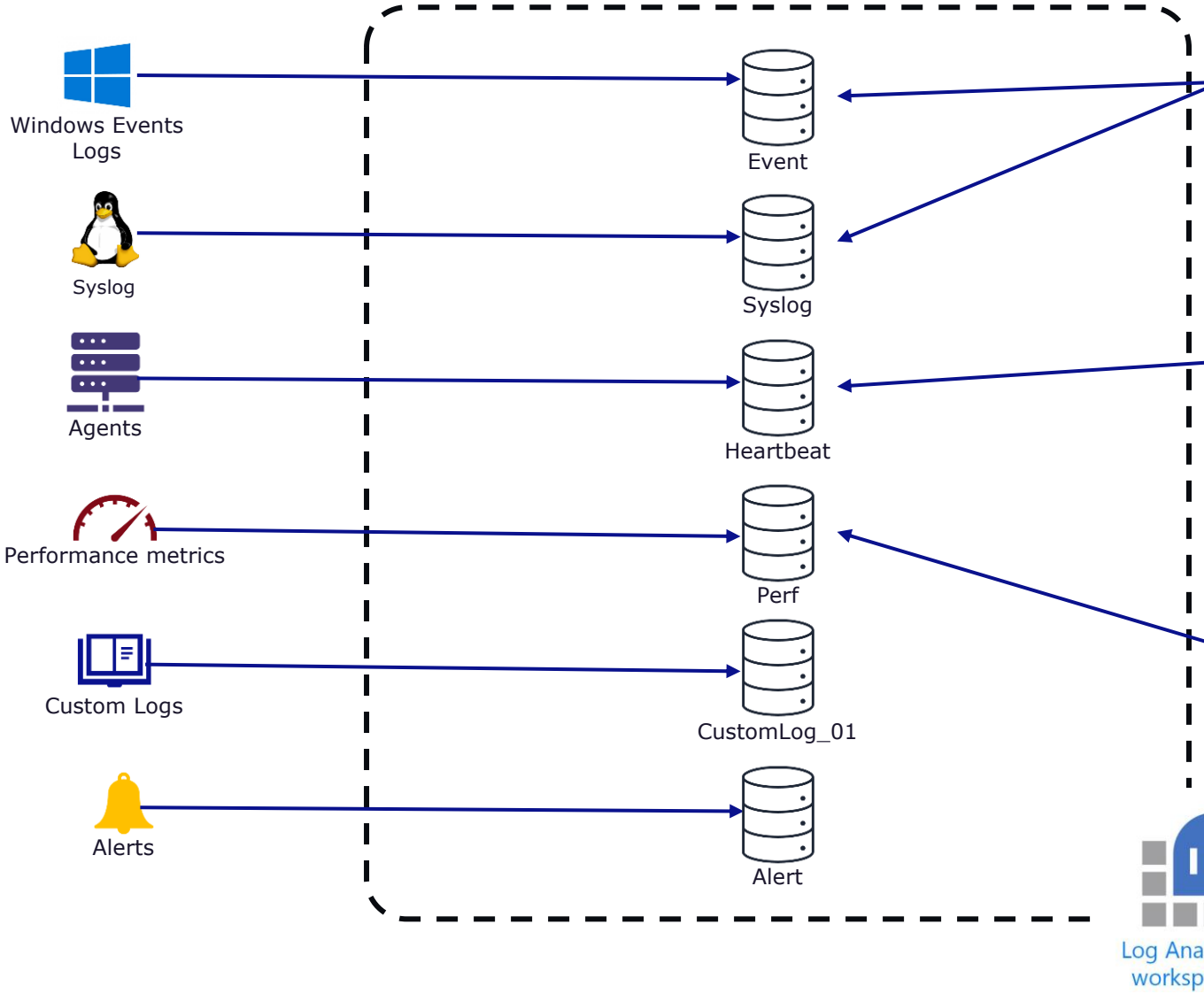
Design

When we design for Log Analytics, we need to decide pricing (Per GB or Capacity), data retention, data capping, and access rights



What is Log Analytics?

Managed service which lets you collect and analyze data that is ingested from Azure Monitor



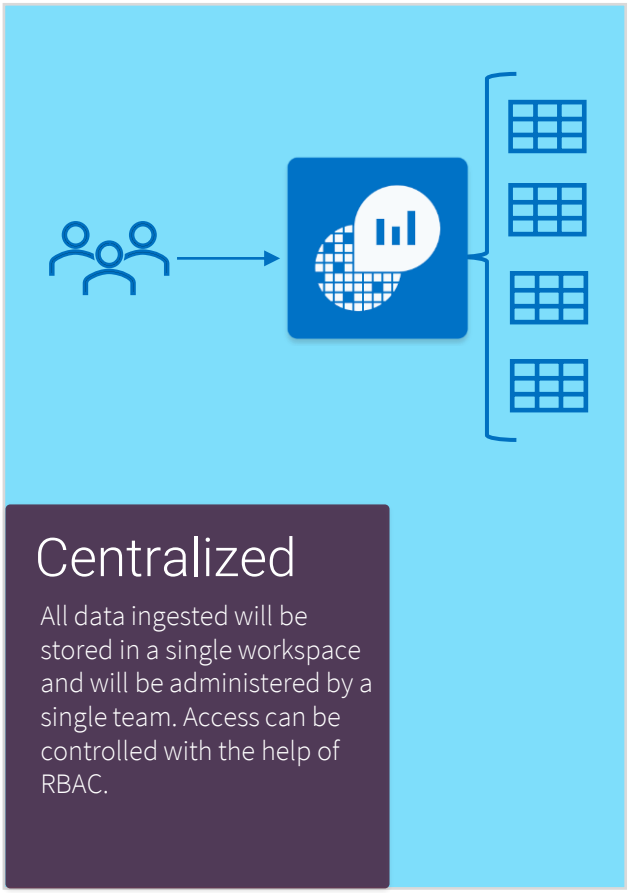

```
Syslog
| union Event
| where SeverityLevel == “Error”
```

```
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
```

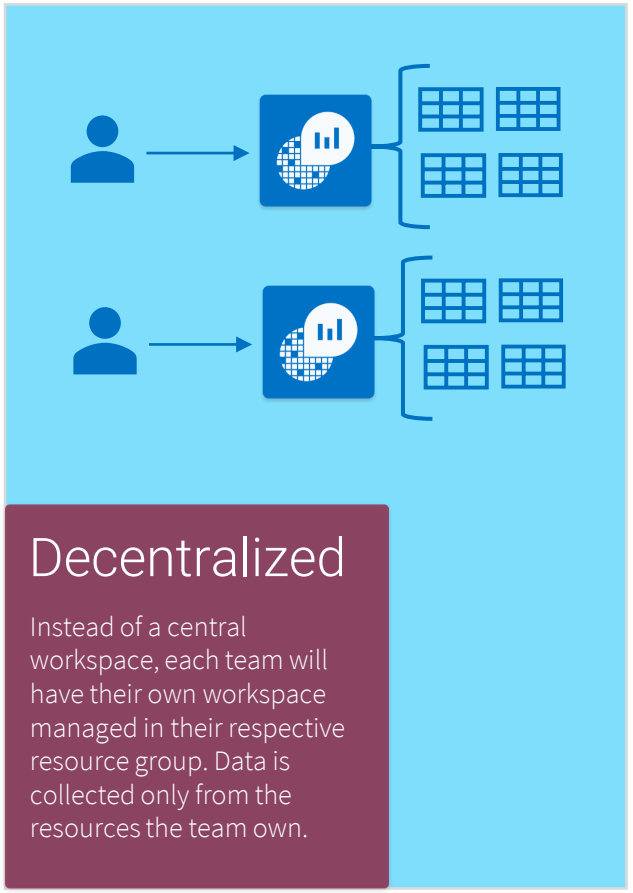
Design for workspace access control

Access can be managed as centralized, decentralized, and hybrid



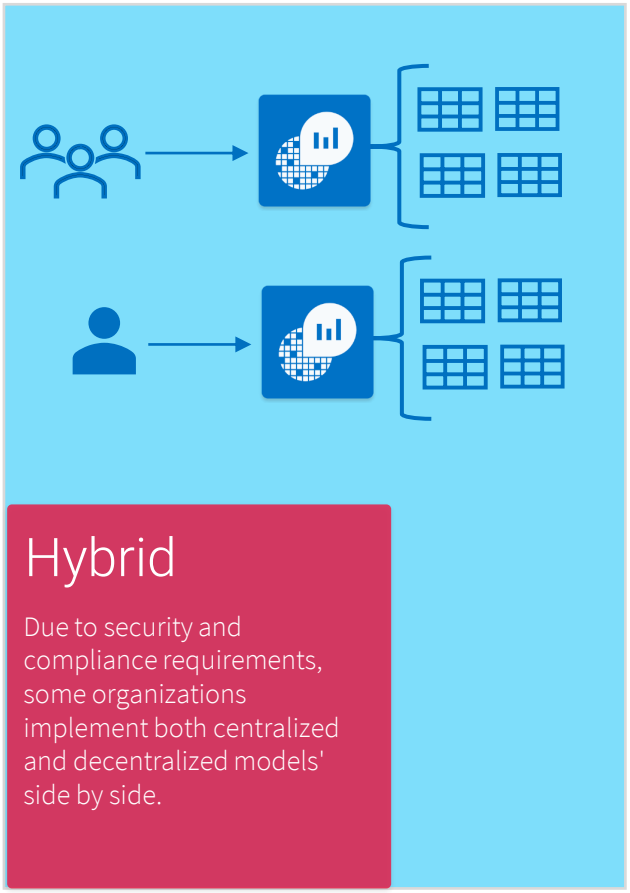
Centralized

All data ingested will be stored in a single workspace and will be administered by a single team. Access can be controlled with the help of RBAC.



Decentralized

Instead of a central workspace, each team will have their own workspace managed in their respective resource group. Data is collected only from the resources the team own.

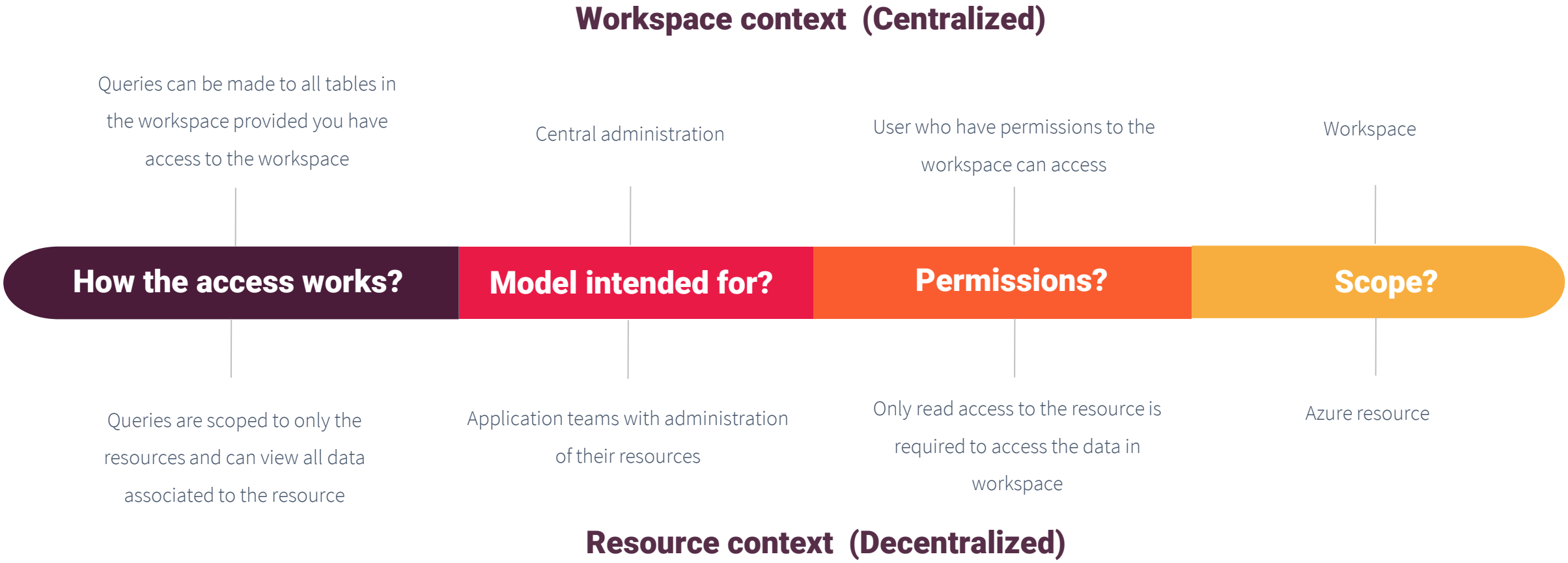


Hybrid

Due to security and compliance requirements, some organizations implement both centralized and decentralized models' side by side.

Design for workspace access control

Access can be managed as centralized, decentralized, and hybrid



Design for Azure workbooks and Insights

Design for Azure Workbooks

Design rich visuals by bringing in data from disparate sources to a single canvas for monitoring

Data visualization

Azure Workbooks helps you to design rich visual reports on a flexible canvas which can be shared across teams for monitoring

Multiple sources

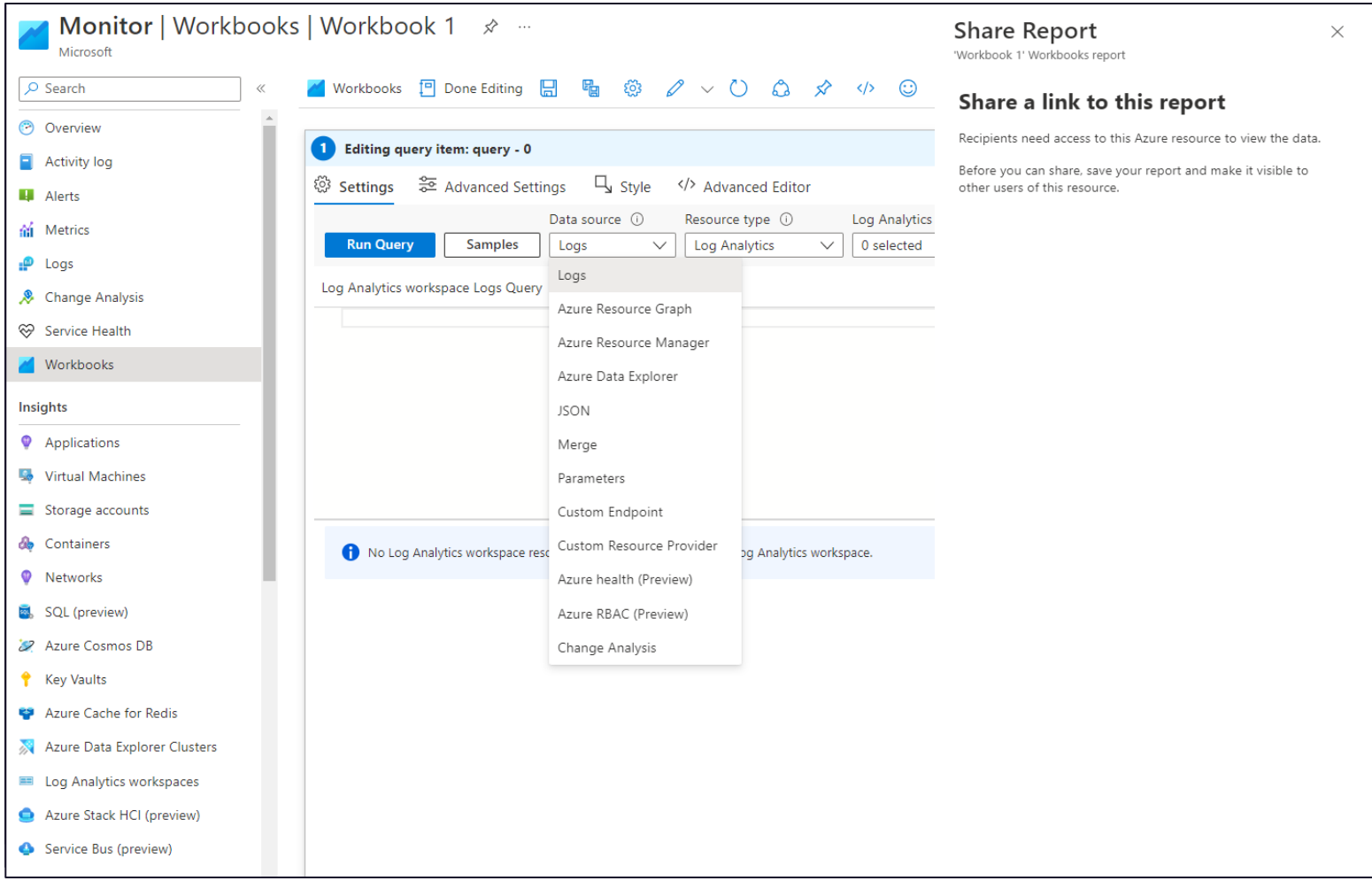
We can add text, parameters, links, tabs, query, metrics and further group the visuals

Metrics and queries

Metrics from resources can be easily added to the workbooks. When it comes to queries Workbooks supports Log Analytics queries, Azure Resource Graph, Azure Resource Manager, Data explorer etc.

Sharing

Workbooks can be deployed to resource groups can access can be provided to team members.



KodeKloud

Design for Azure Insights

Monitor your resources closely by collecting telemetry data

Application Insights

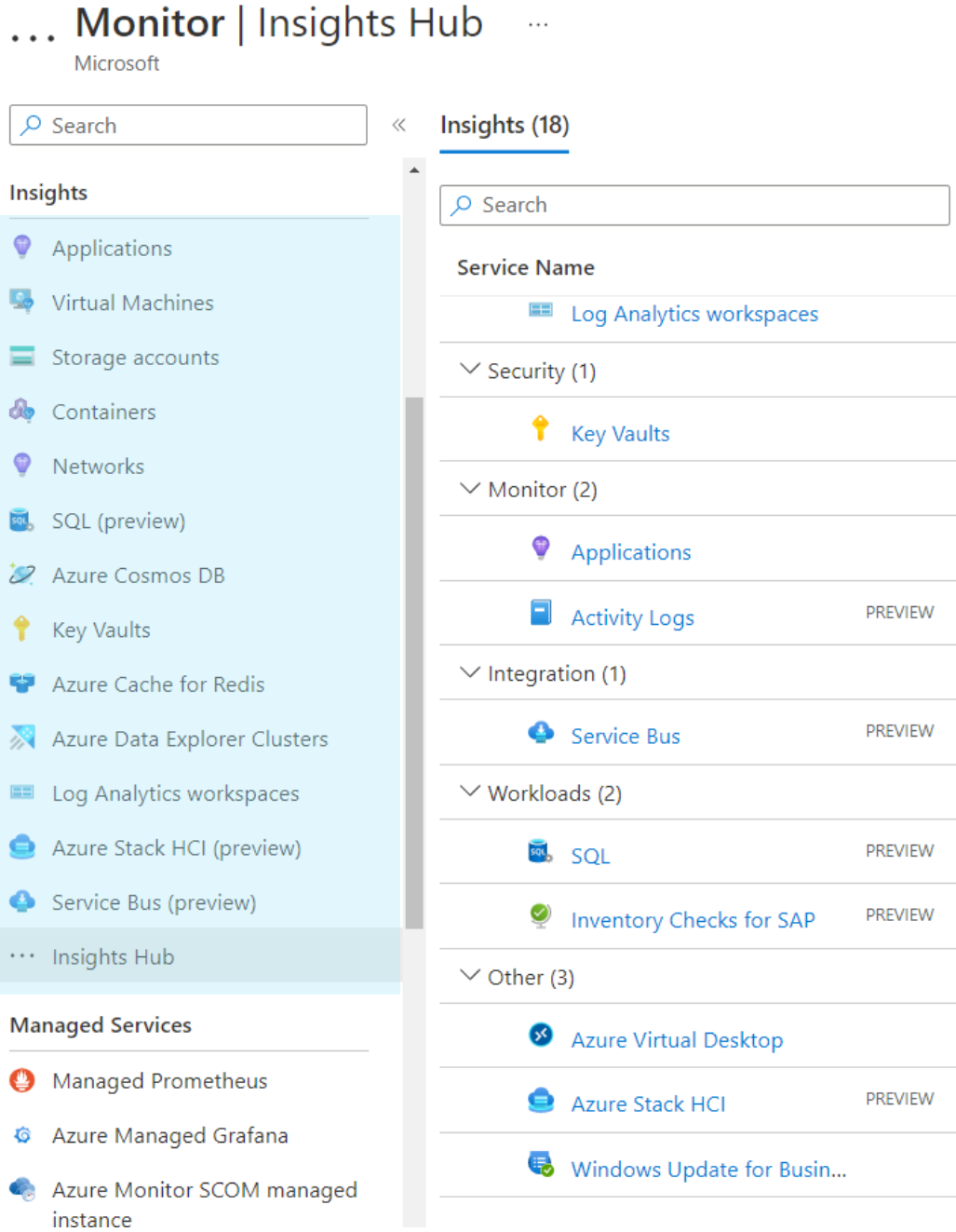
- Monitor and address issues that affect the performance and health of the application.
- Improve application development cycle using telemetry
- Evaluate user experience and user behavior using usage patterns

VM Insights

- Monitor heath and performance of VMs
- Compare performance of VMs from multiple environments under a single glass pane
- Get more insights into the processes, dependencies and network topology

Container Insights

- Monitor health and performance of Kubernetes workloads across multiple environments.
- Detailed insights into the memory and metrics of controllers, nodes, and pods.
- Collect and store container logs for analysis and troubleshooting



Design for Azure Data Explorer

Design for Azure Data Explorer

Managed, fast, and highly scalable data exploration service for analyzing log and telemetry data

Purpose

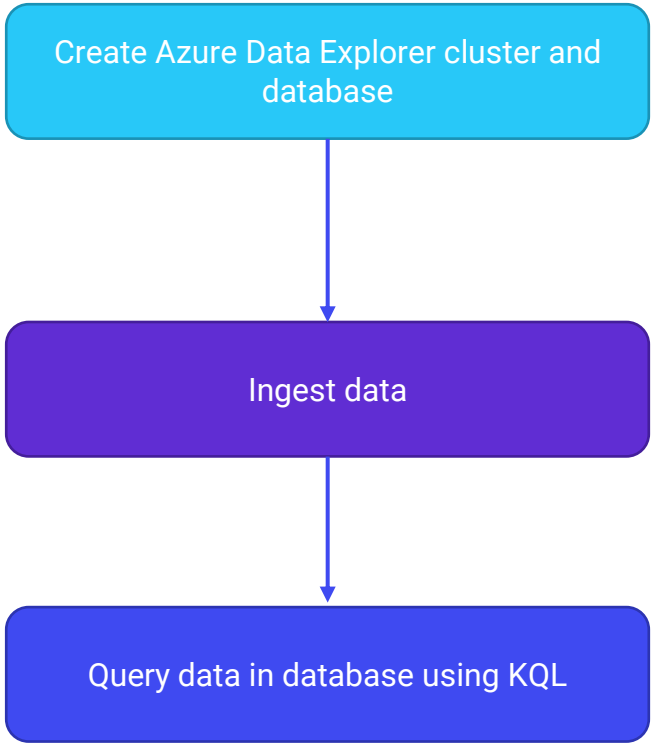
Data streams emitted by modern software can be collected, stored, and analyzed using Azure Data Explorer. This service is ideal for analyzing large volumes of data from various data sources such as websites, applications, IoT devices and more.

When should you use?

If you need to collect data from various sources for diagnostics, monitoring, reporting, analytics, or machine learning then you can use Azure Data Explorer.

Integrations

Azure Data Explorer can be further integrated with Azure Monitor and Sentinel. With this you can ingest security logs and other diagnostics logs to Azure Data Explorer and use that for analytics, ML or for building dashboards.



KodeKloud