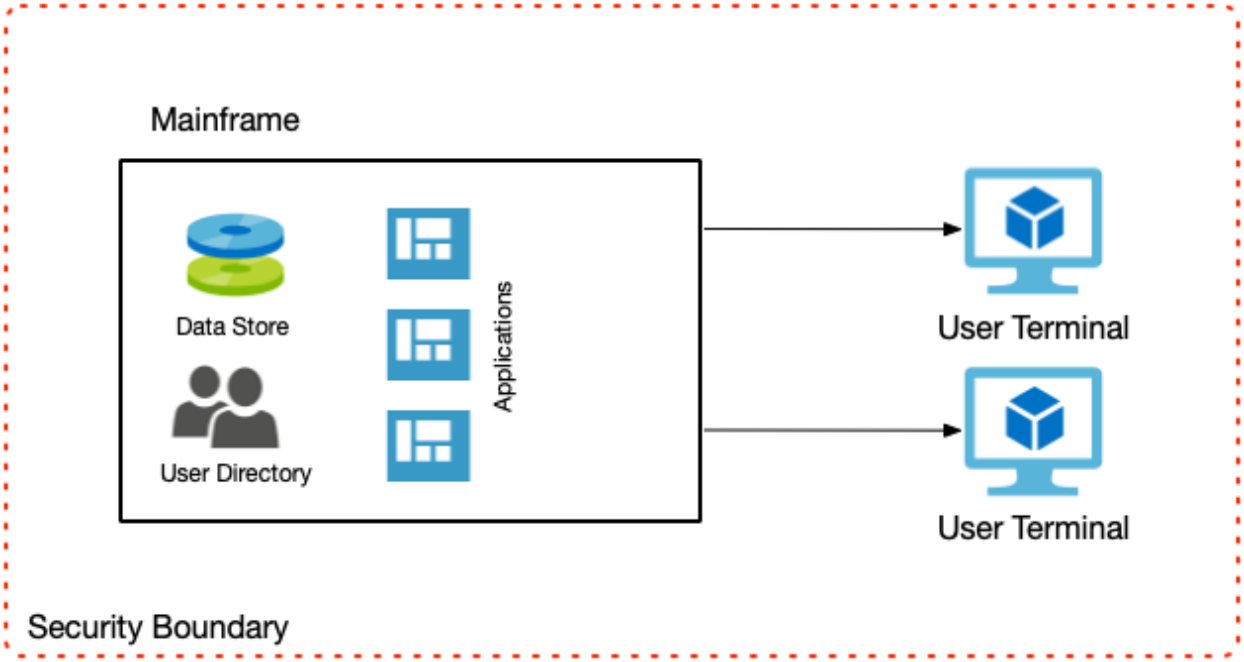
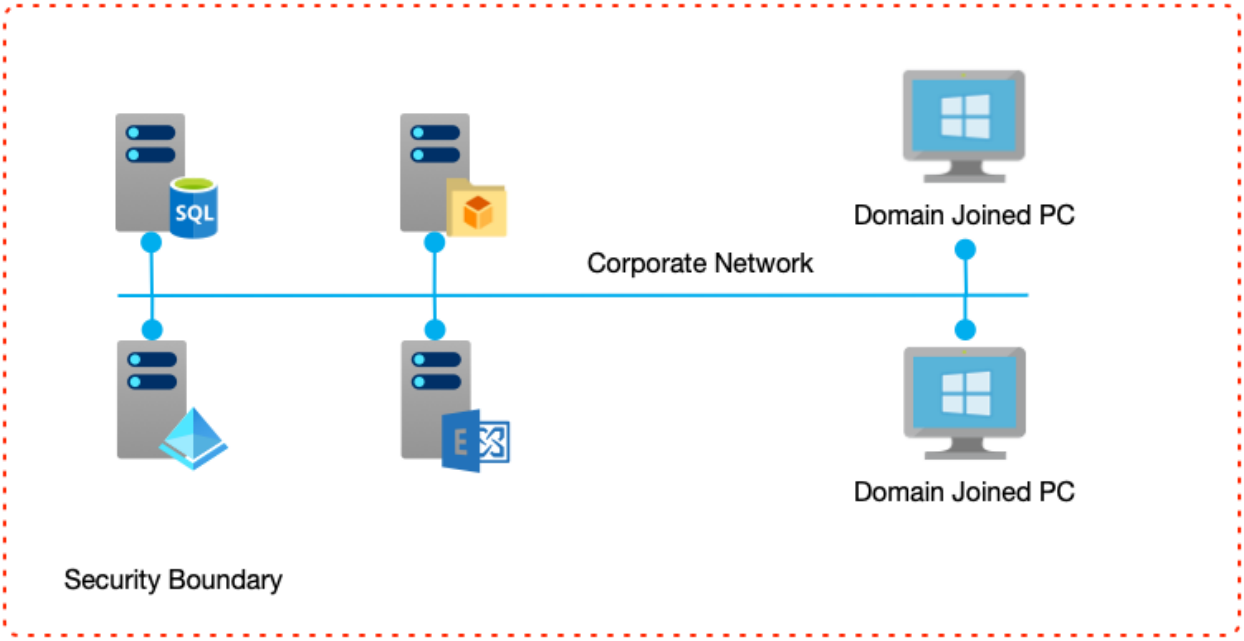
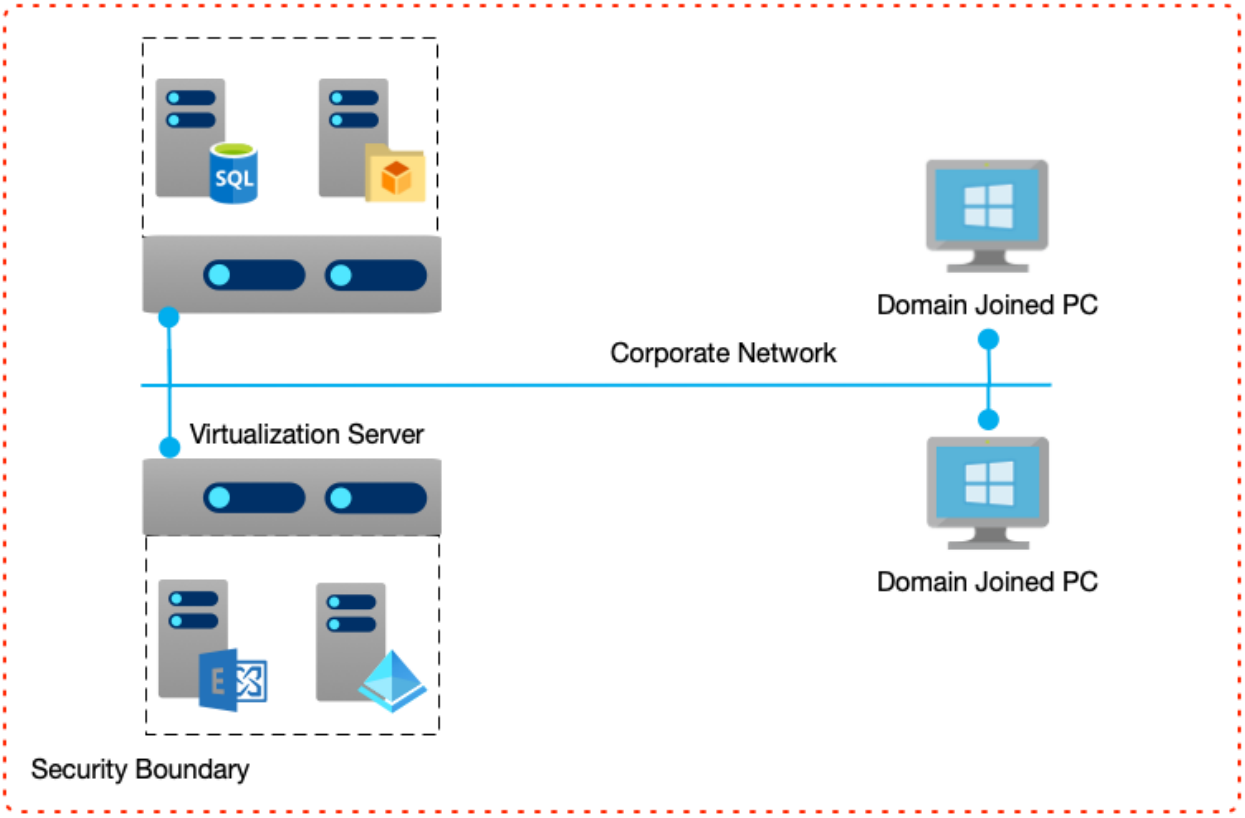
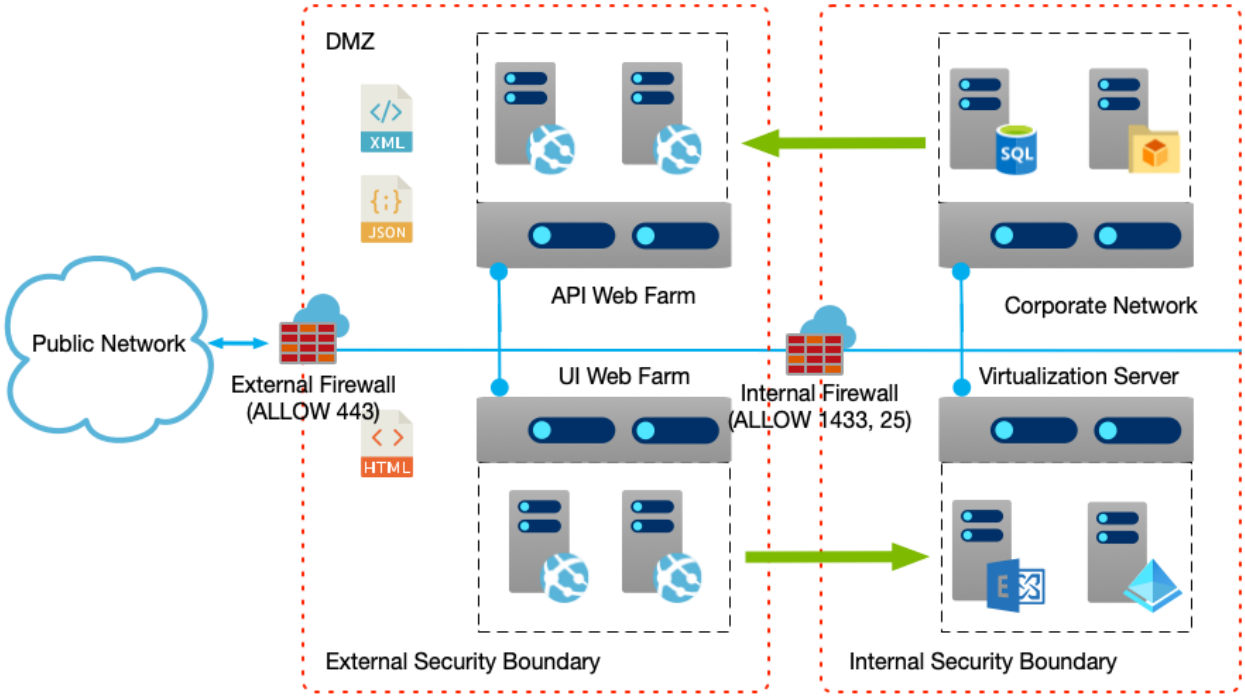
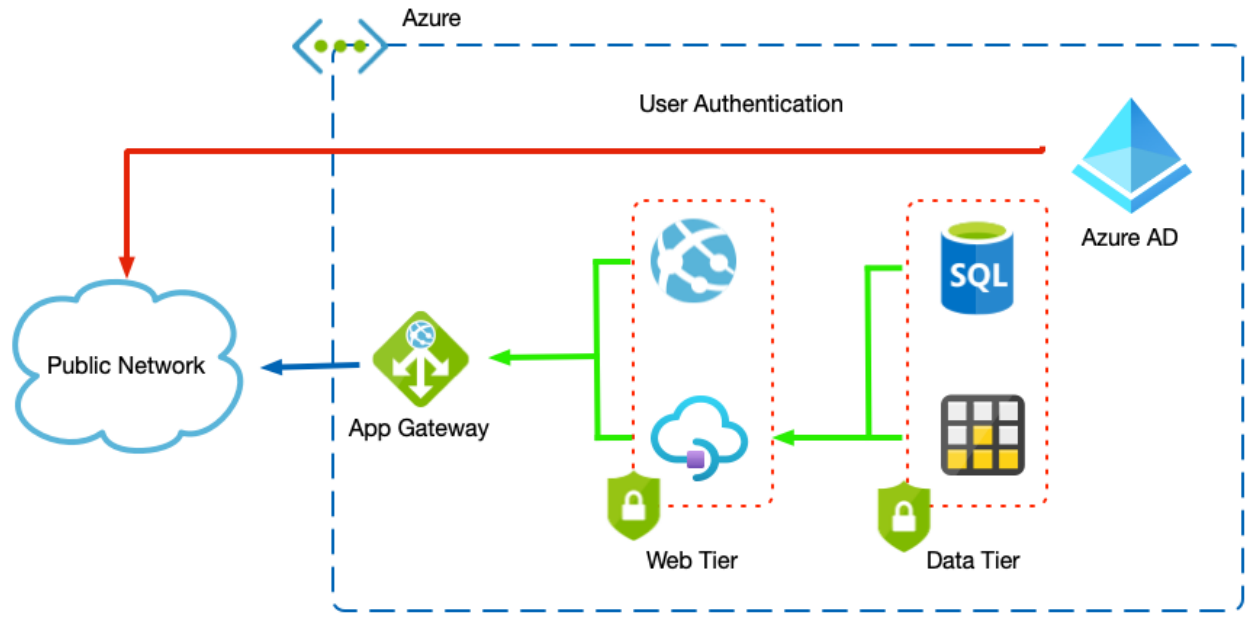
Chapter 1: Architecture for the Cloud

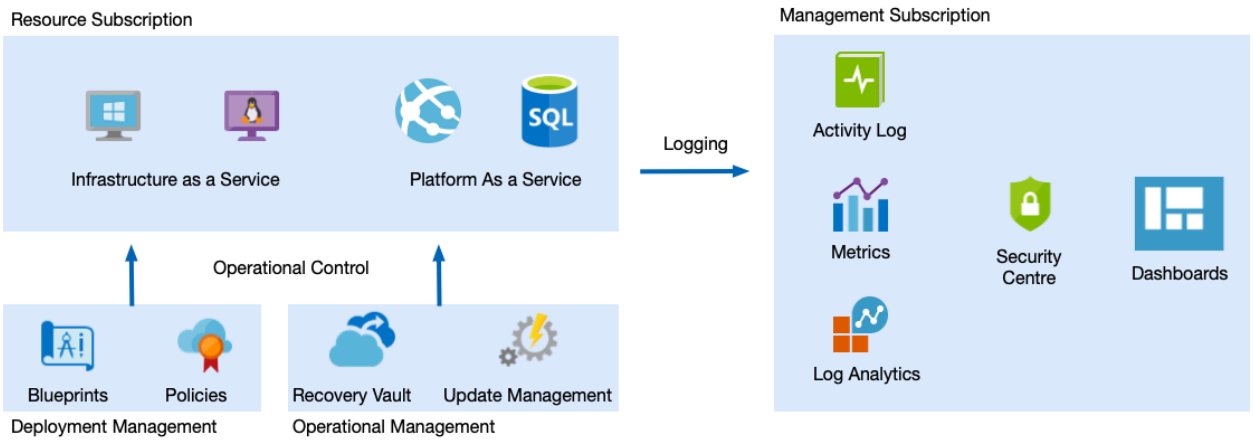


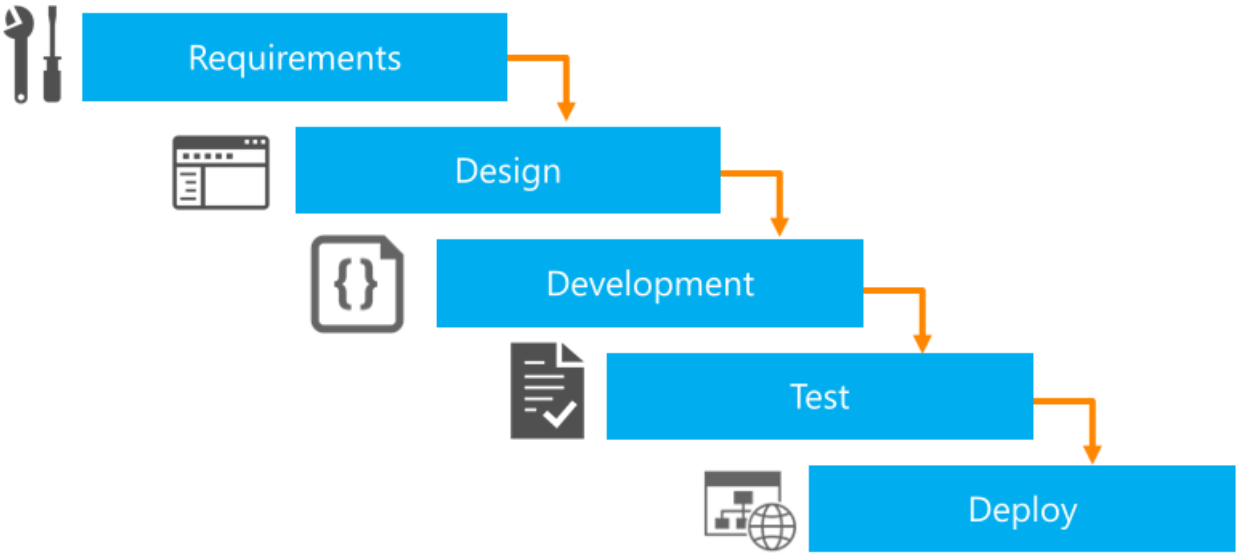


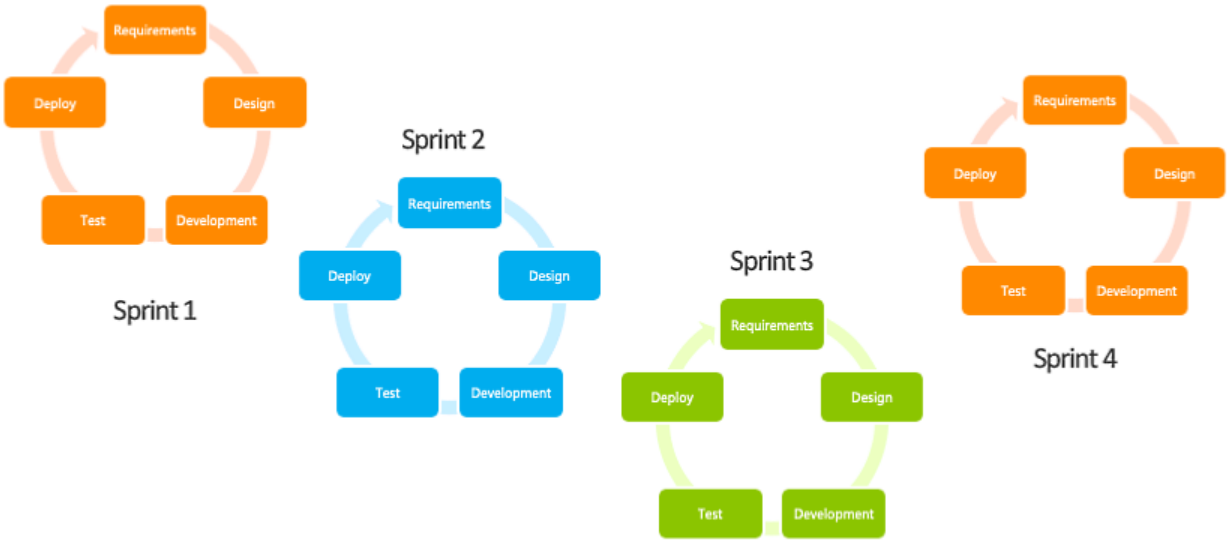

SQL
Domain Joined PC
Corporate Network
Virtualization Server
Domain Joined PC
Security Boundary


DMZ
XML
JSON
API Web Farm
SQL
Corporate Network
Public Network
External Firewall
(ALLOW 443)
UI Web Farm
Internal Firewall
(ALLOW 1433, 25)
Virtualization Server
HTML
External Security Boundary
Internal Security Boundary

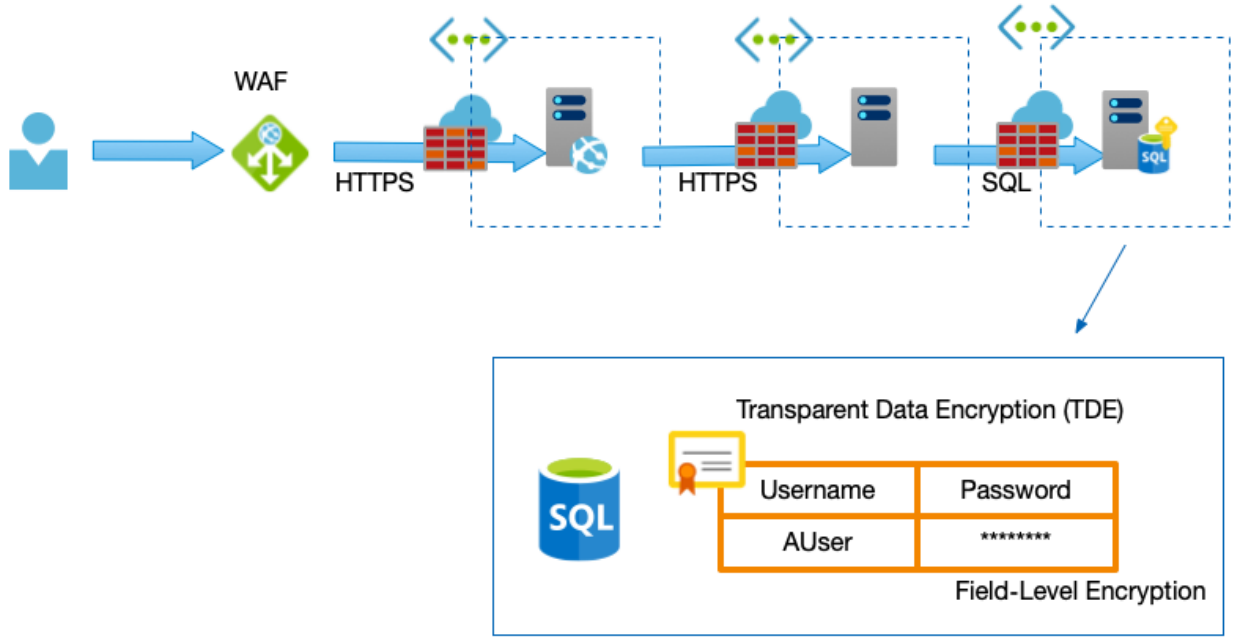

Azure
User Authentication
Azure AD
Public Network
App Gateway
SQL
Web Tier
Data Tier

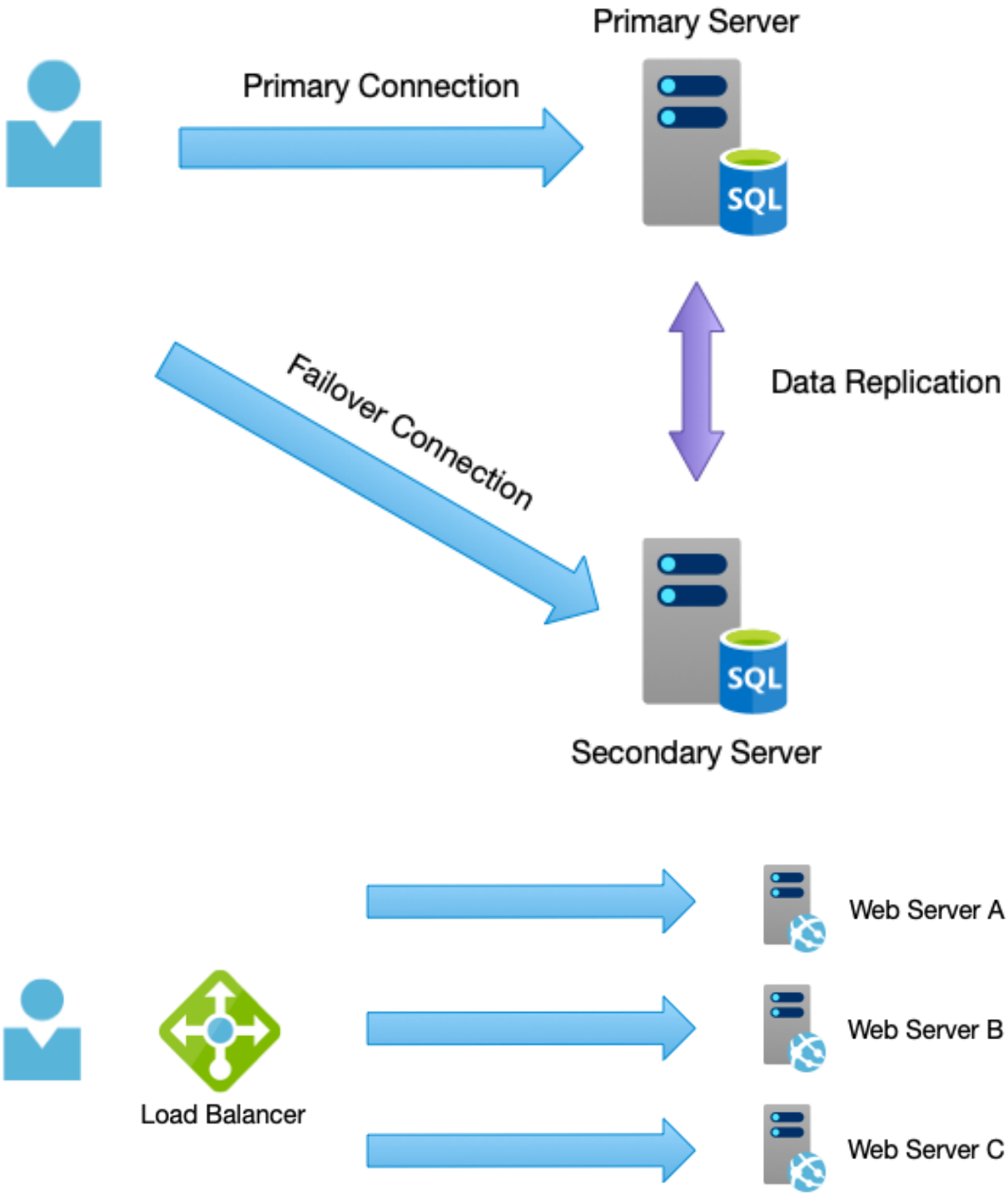

Resource Subscription
Infrastructure as a Service
Platform As a Service
SQL
Logging
Management Subscription
Activity Log
Metrics
Security Centre
Dashboards
Log Analytics
Operational Control
Blueprints
Policies
Deployment Management
Recovery Vault
Update Management
Operational Management

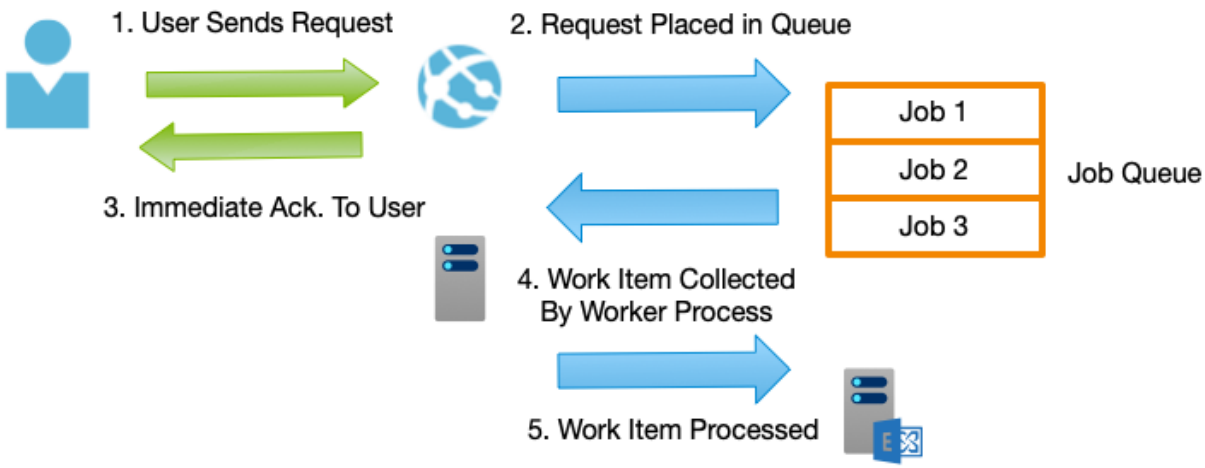

Requirements
Design
Development
Test
Deploy

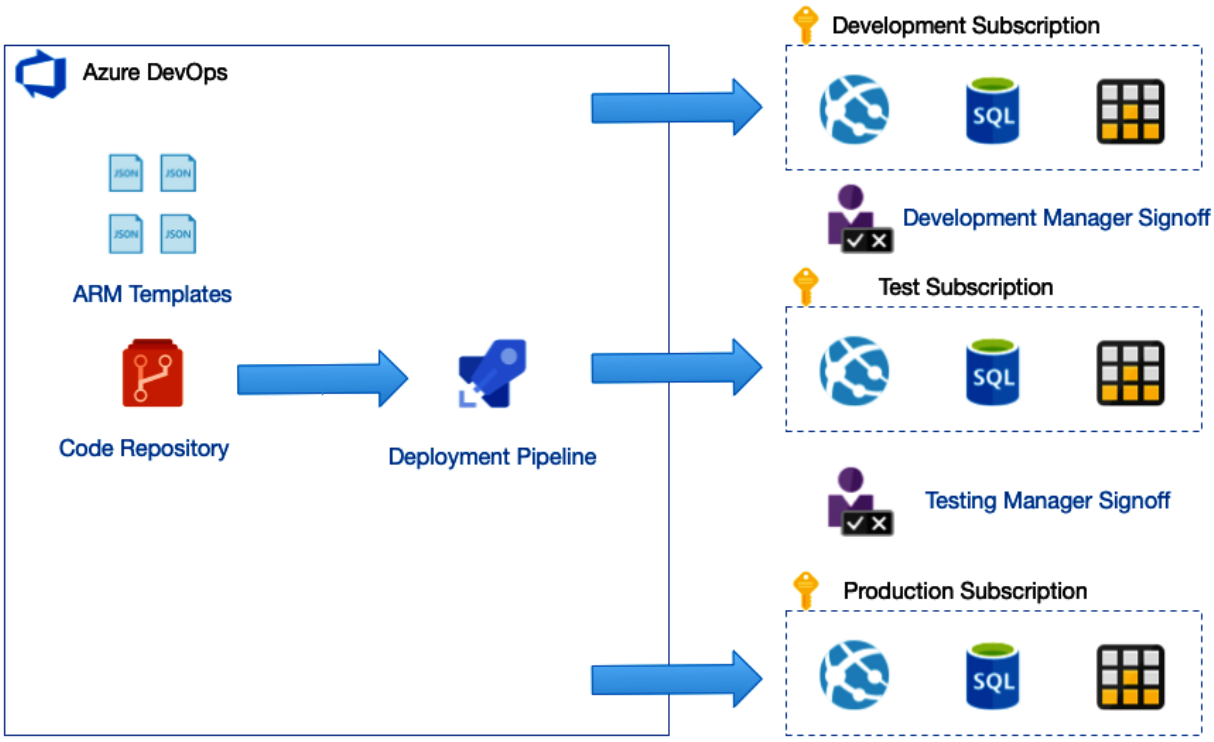

Requirements
Design
Development
Test
Deploy
Sprint 1
Sprint 2
Sprint 3
Sprint 4

Chapter 2: Principles of Modern Architecture



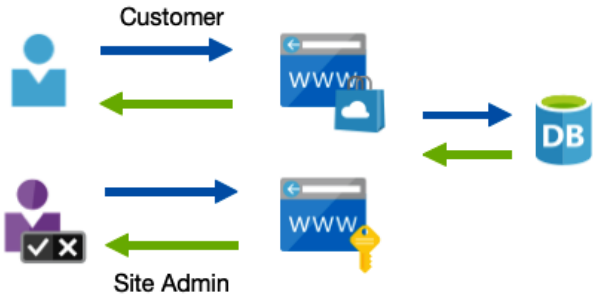

Primary Server
Primary Connection
SQL
Failover Connection
Data Replication
SQL
Secondary Server
Web Server A
Web Server B
Web Server C
Load Balancer


1. User Sends Request
2. Request Placed in Queue
Job 1
Job 2
Job 3
Job Queue
3. Immediate Ack. To User
4. Work Item Collected
By Worker Process
5. Work Item Processed

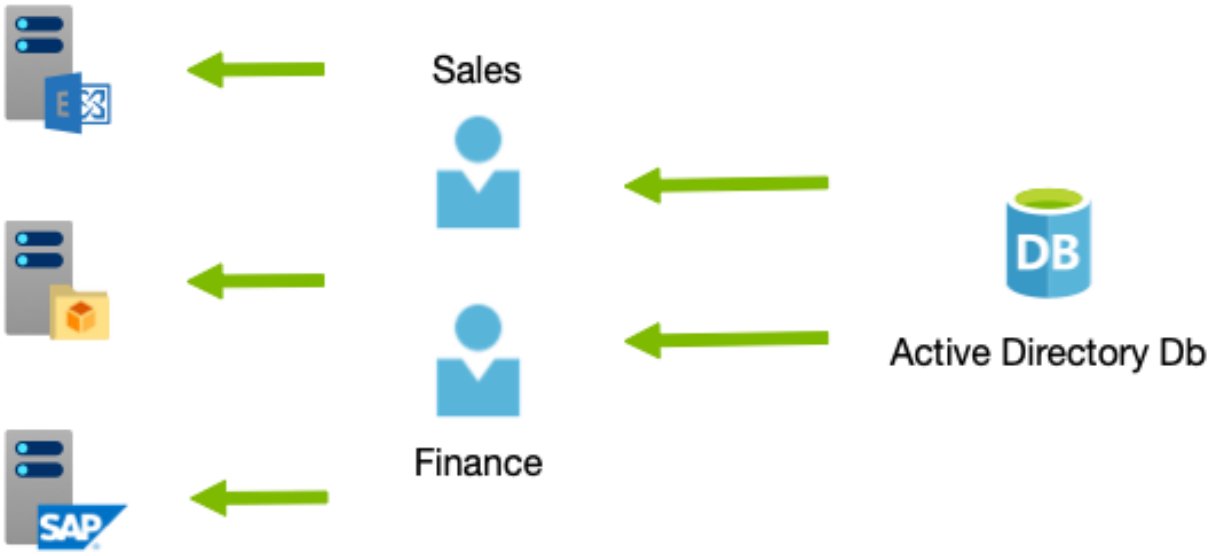

Development Subscription
Azure DevOps
SQL
Development Manager Signoff
ARM Templates
Test Subscription
SQL
Code Repository
Deployment Pipeline
Testing Manager Signoff
Production Subscription
SQL

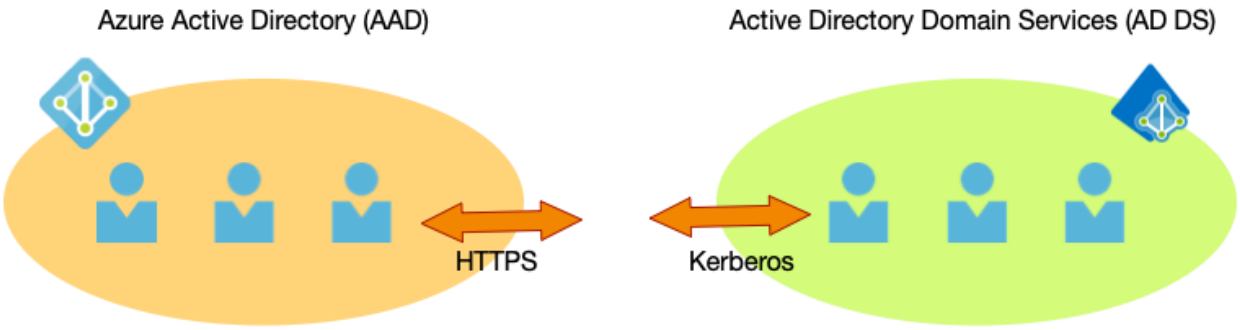
Chapter 3: Understanding User Authentication

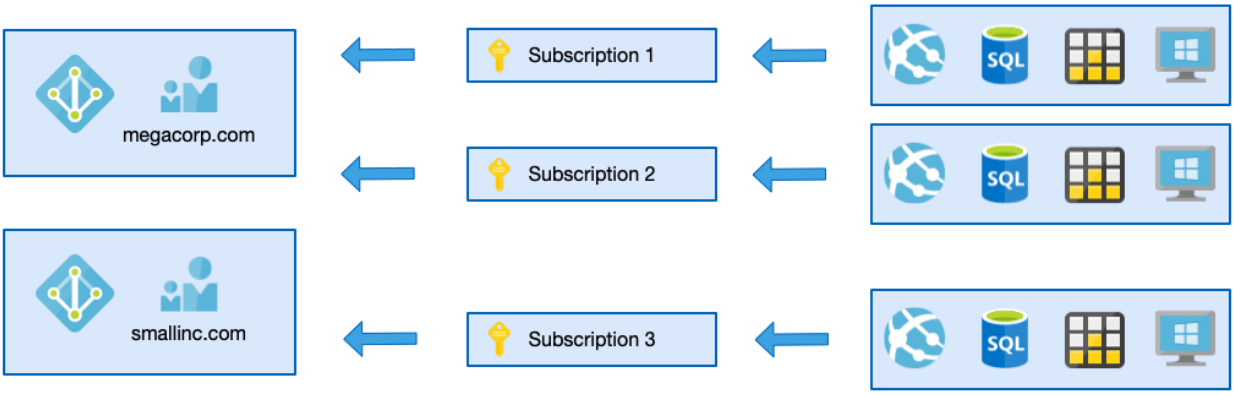
Username	Password
AUser	P@ssw0rd

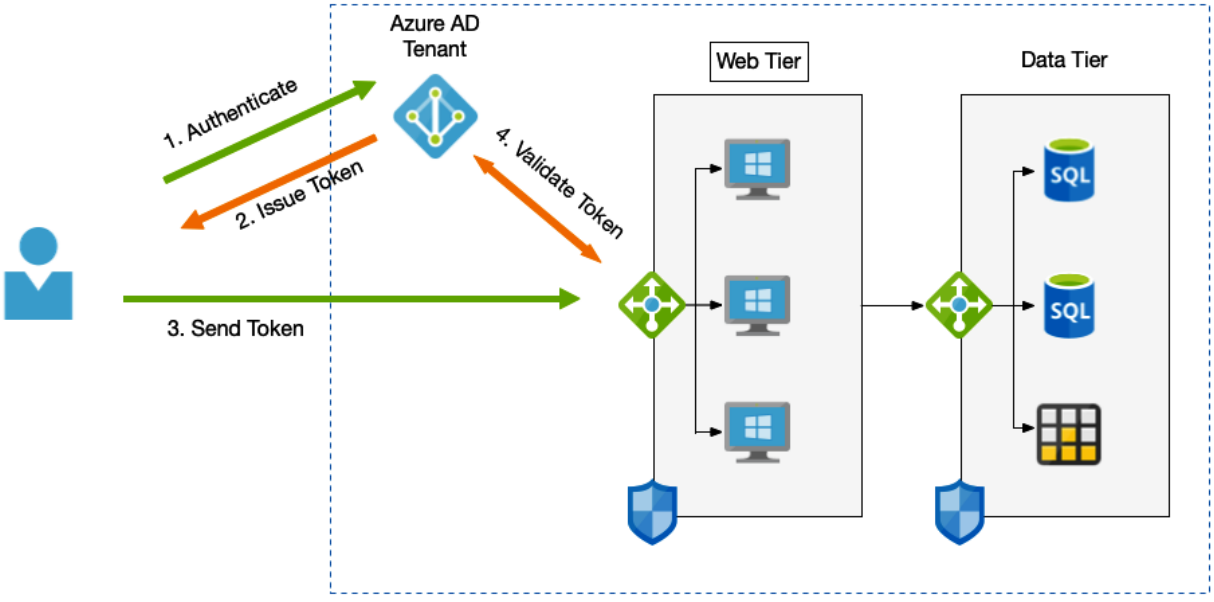


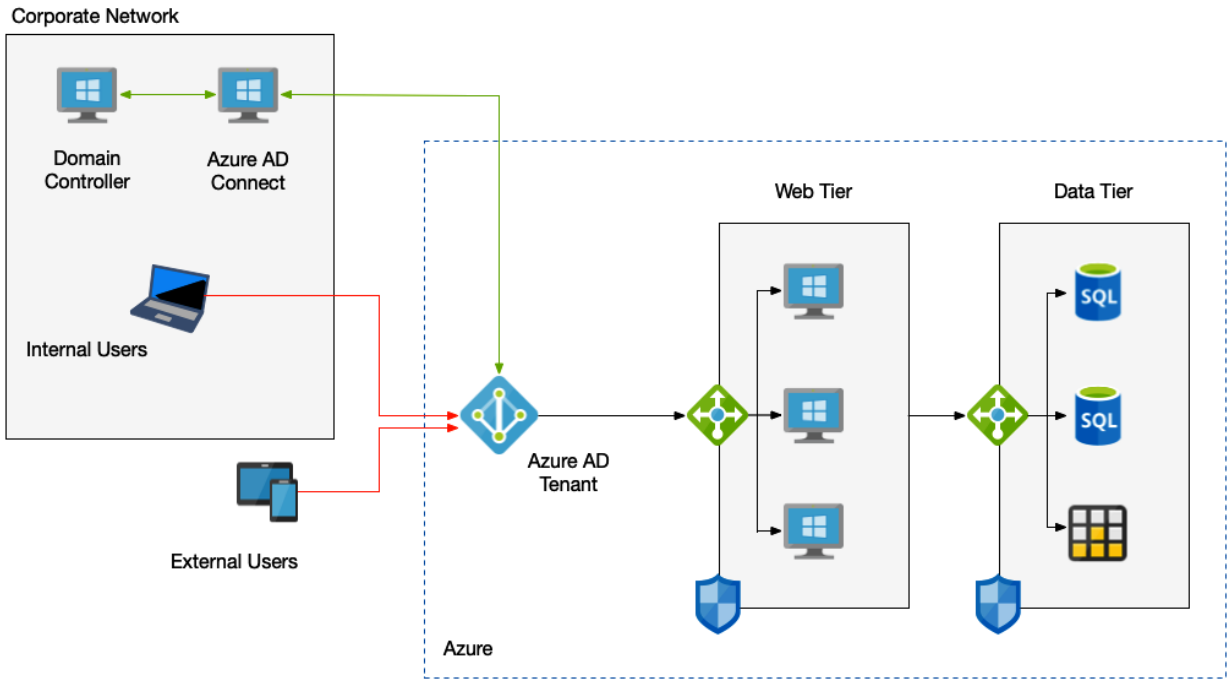
Username	Password	Role
AUser	P@ssw0rd	Customer
Admin	P@ssw0rd	Admin




Azure Active Directory (AAD)
Active Directory Domain Services (AD DS)
HTTPS
Kerberos


megacorp.com
smallinc.com
Subscription 1
Subscription 2
Subscription 3
SQL
SQL
SQL


Azure AD
Tenant
1. Authenticate
2. Issue Token
3. Send Token
4. Validate Token
Web Tier
Data Tier
SQL
SQL



PROVISION FROM ACTIVE DIRECTORY

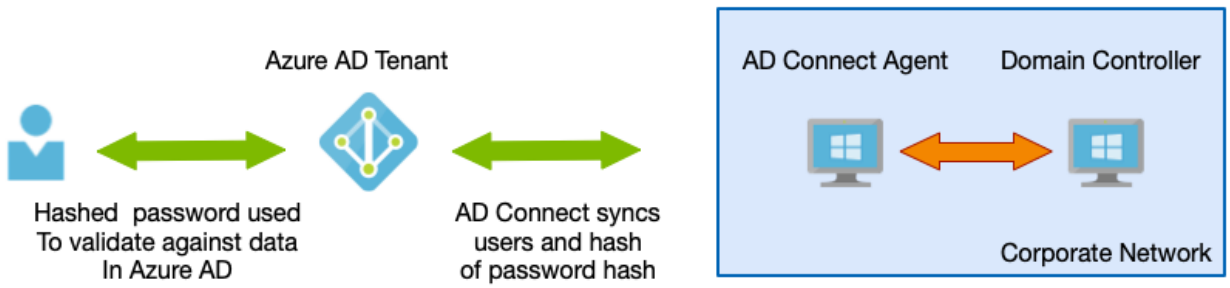
Azure AD Connect cloud provisioning

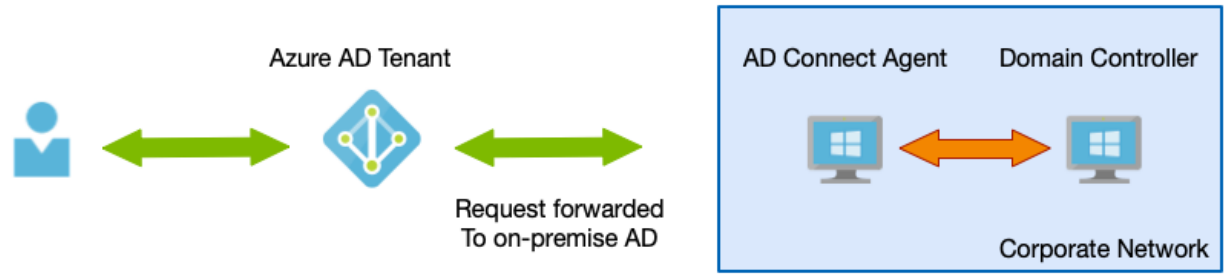
This feature allows you to manage provisioning from the cloud.

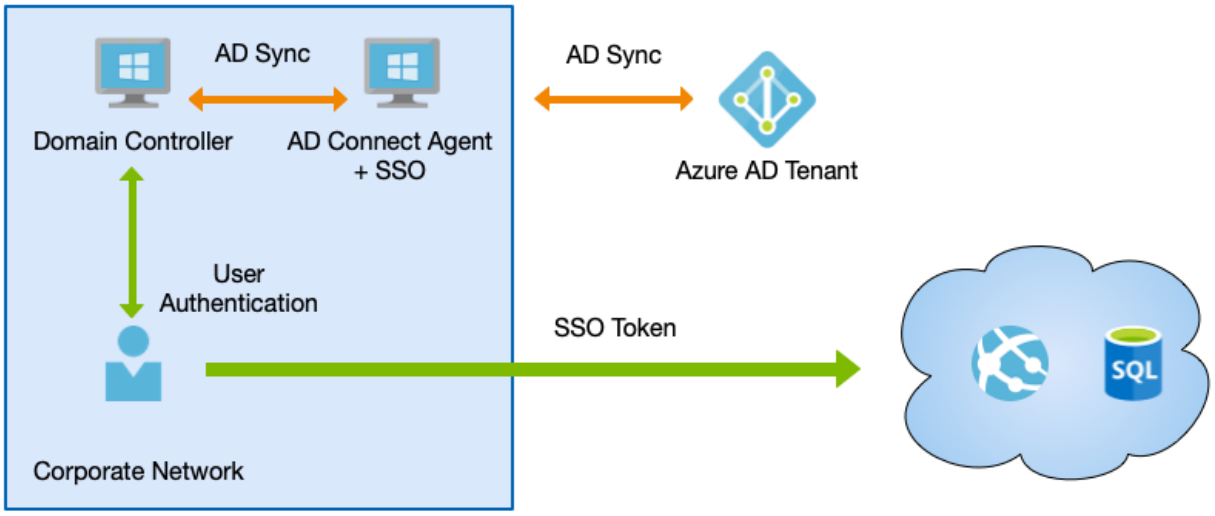
Manage provisioning (Preview)

Azure AD Connect sync

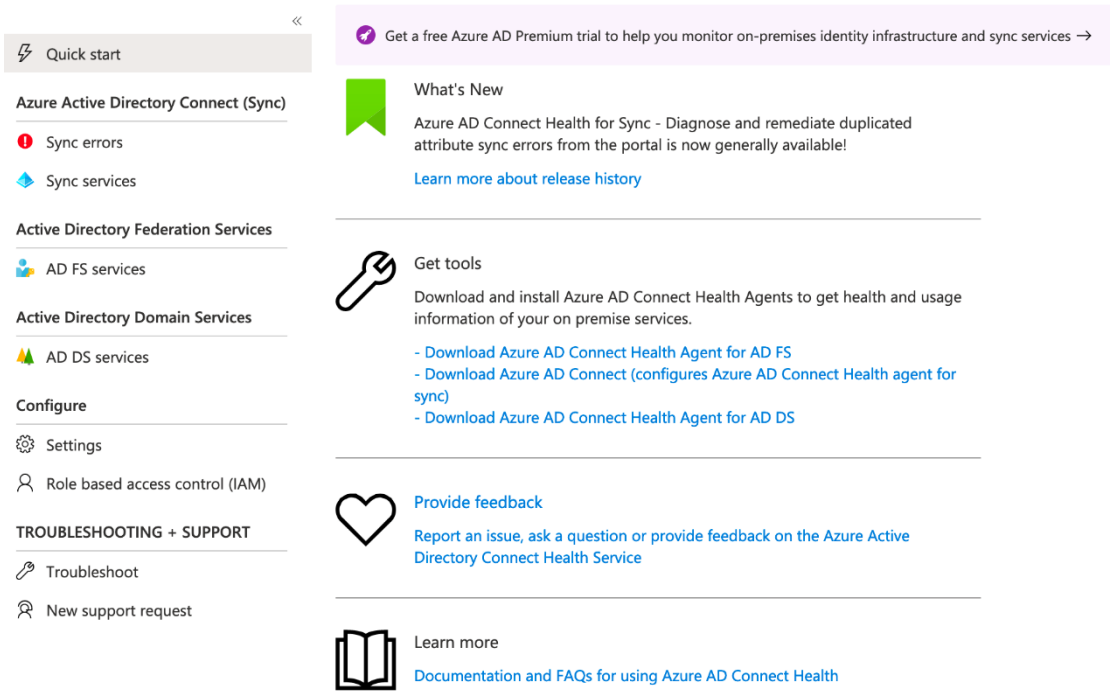
Not Installed	Download Azure AD Connect
Last Sync	Sync has never run
Password Hash Sync	Disabled

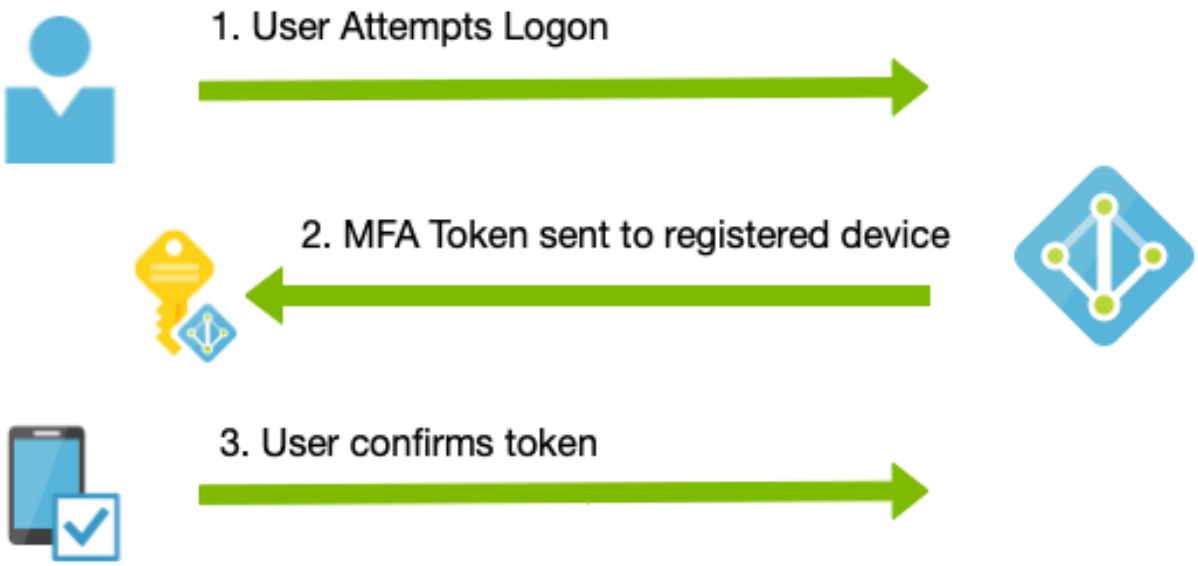

Azure AD Tenant
AD Connect Agent
Domain Controller
Hashed password used
To validate against data
In Azure AD
AD Connect syncs
users and hash
of password hash
Corporate Network

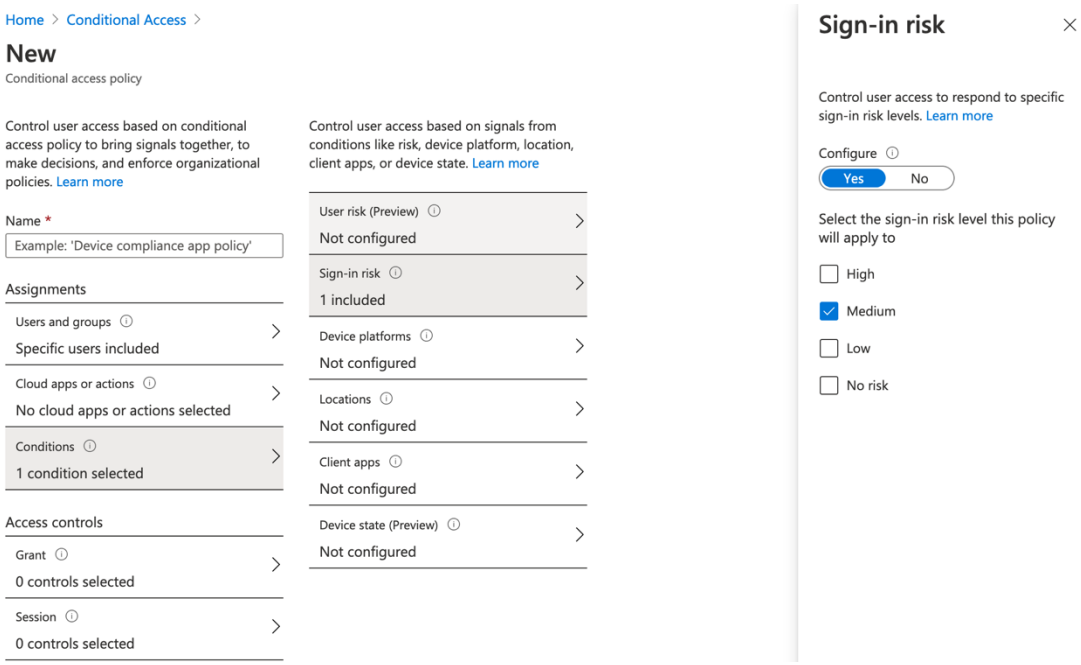

Azure AD Tenant
AD Connect Agent
Domain Controller
Request forwarded
To on-premise AD
Corporate Network


AD Sync
AD Sync
Domain Controller
AD Connect Agent
+ SSO
Azure AD Tenant
User
Authentication
SSO Token
SQL
Corporate Network

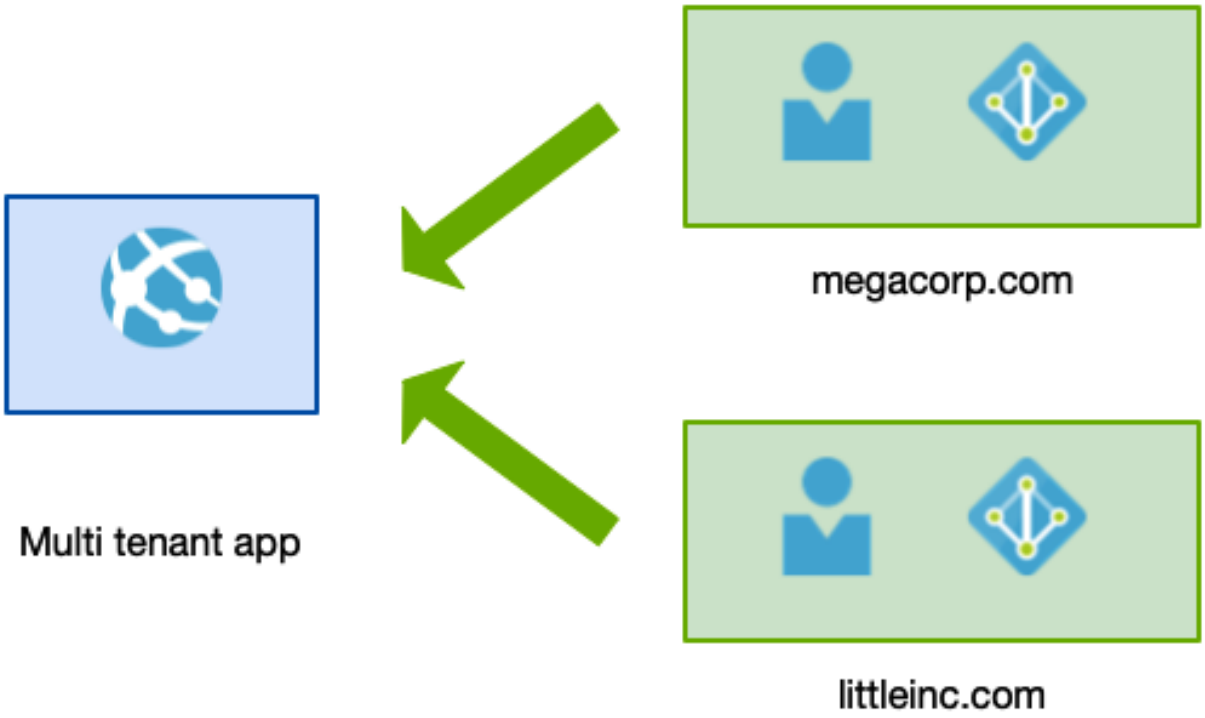
Azure Active Directory Connect Health | Quick start

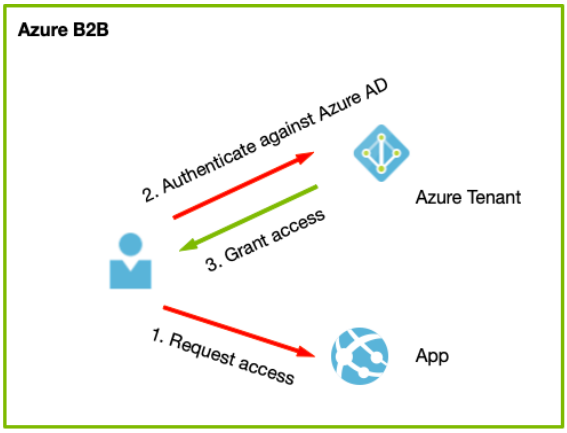


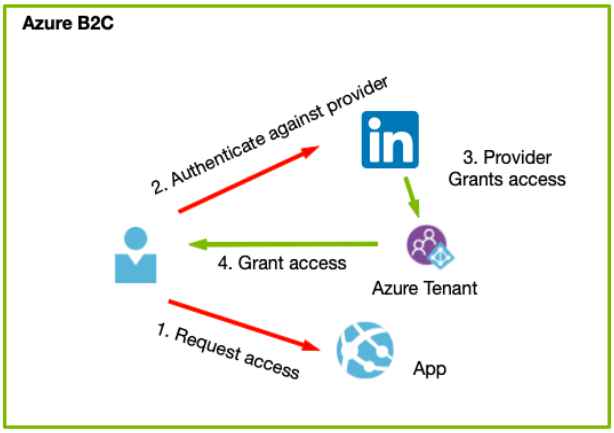



Home > Conditional Access >
New
Conditional access policy
Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
Example: 'Device compliance app policy'
Assignments
Users and groups
Specific users included
Cloud apps or actions
No cloud apps or actions selected
Conditions
1 condition selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more
User risk (Preview)
Not configured
Sign-in risk
1 included
Device platforms
Not configured
Locations
Not configured
Client apps
Not configured
Device state (Preview)
Not configured
Sign-in risk
Control user access to respond to specific sign-in risk levels. Learn more
Configure
Yes
No
Select the sign-in risk level this policy will apply to
High
Medium
Low
No risk

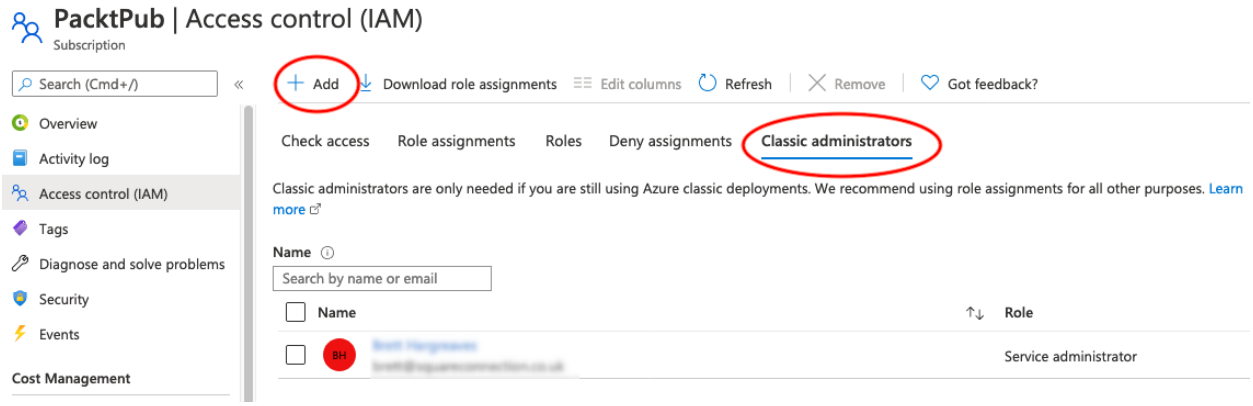
Single tenant app
megacorp.com

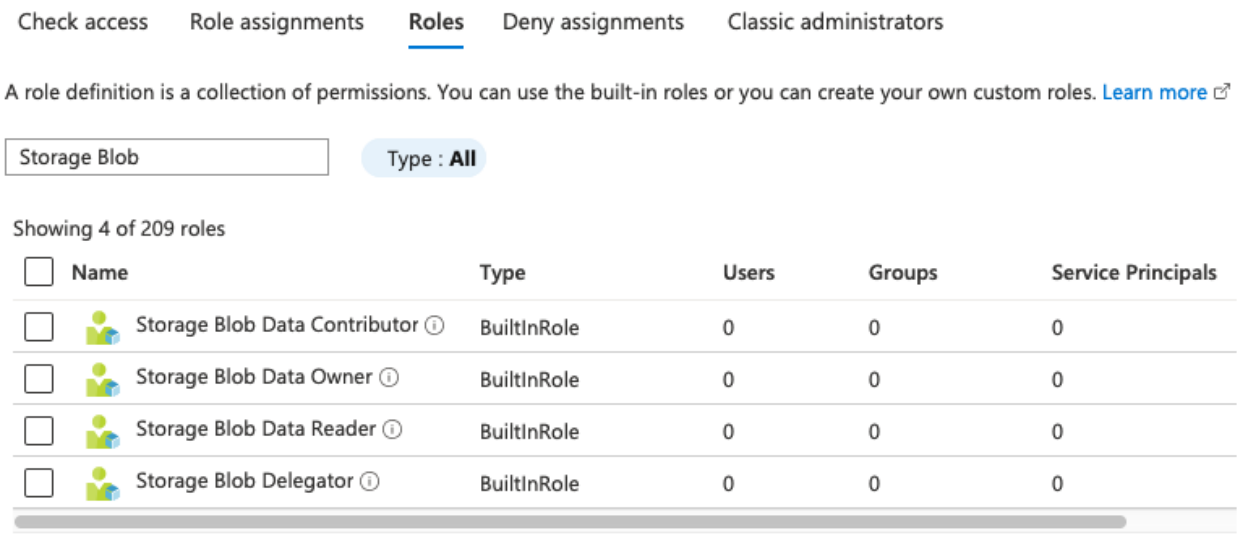

megacorp.com
Multi tenant app
littleinc.com

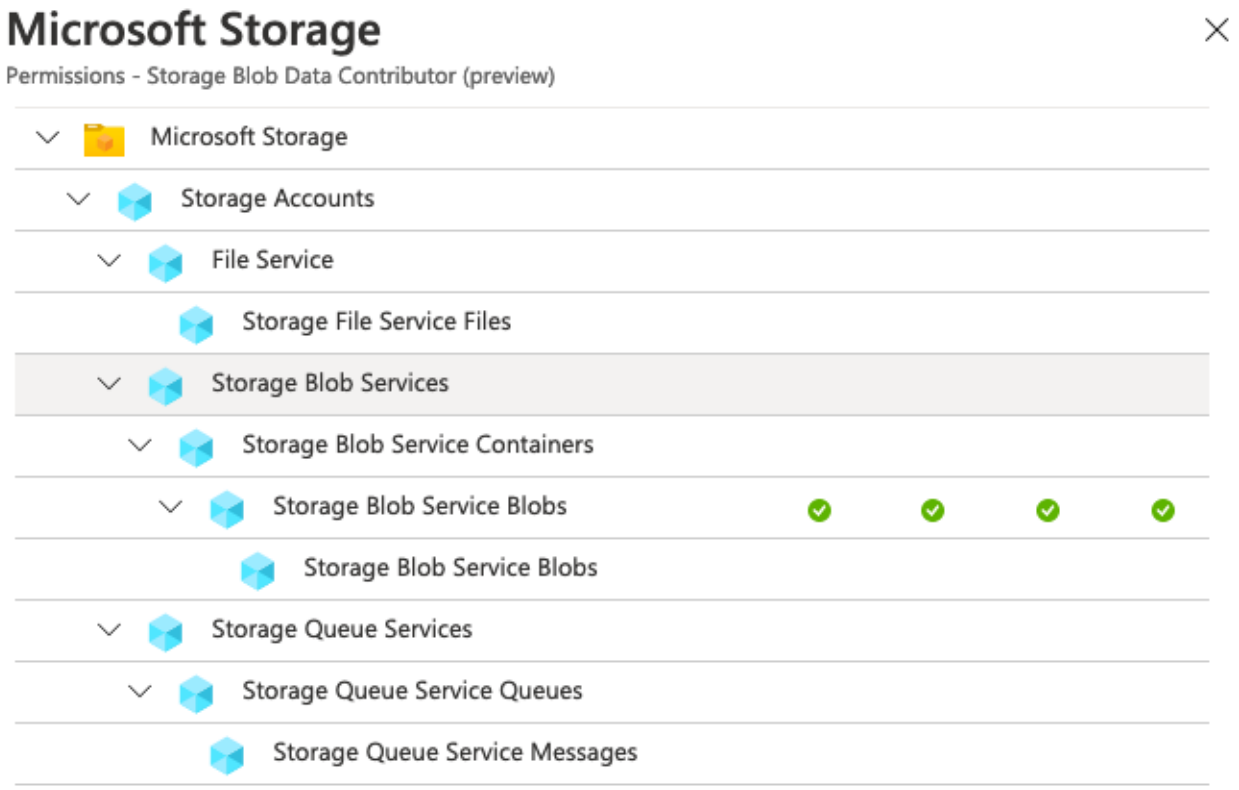

Azure B2B
2. Authenticate against Azure AD
Azure Tenant
3. Grant access
1. Request access
App

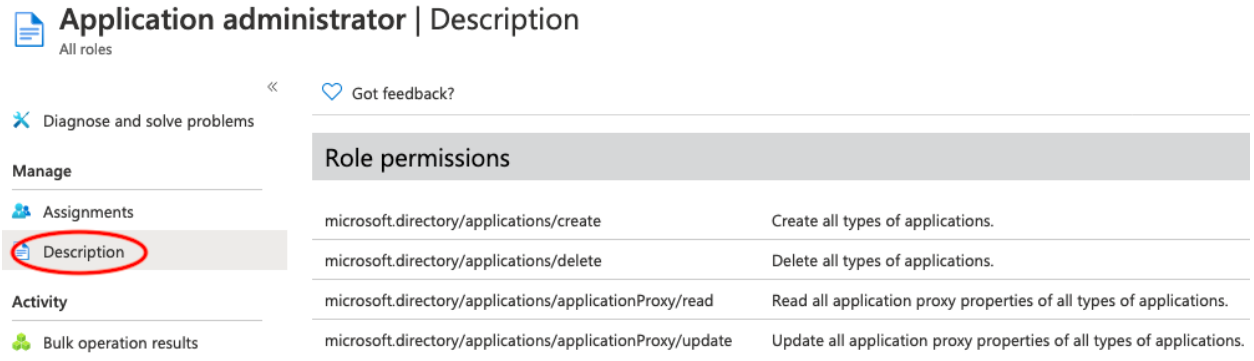

Azure B2C
2. Authenticate against provider
3. Provider
Grants access
4. Grant access
Azure Tenant
1. Request access
App

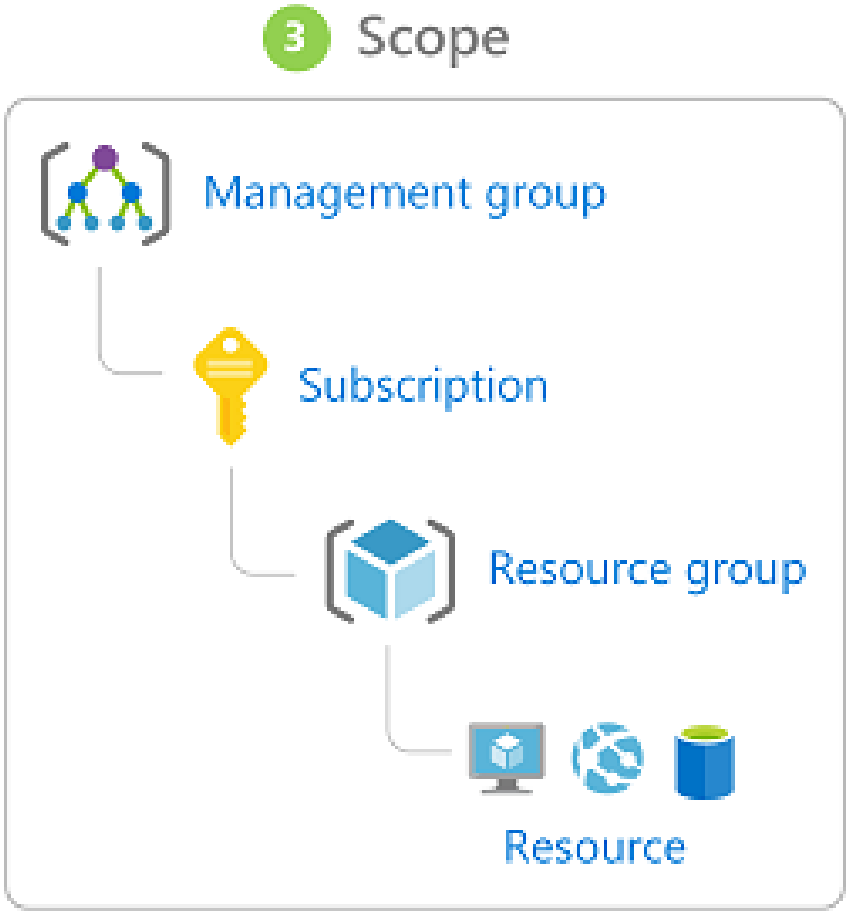
Chapter 4: Managing User Authorization

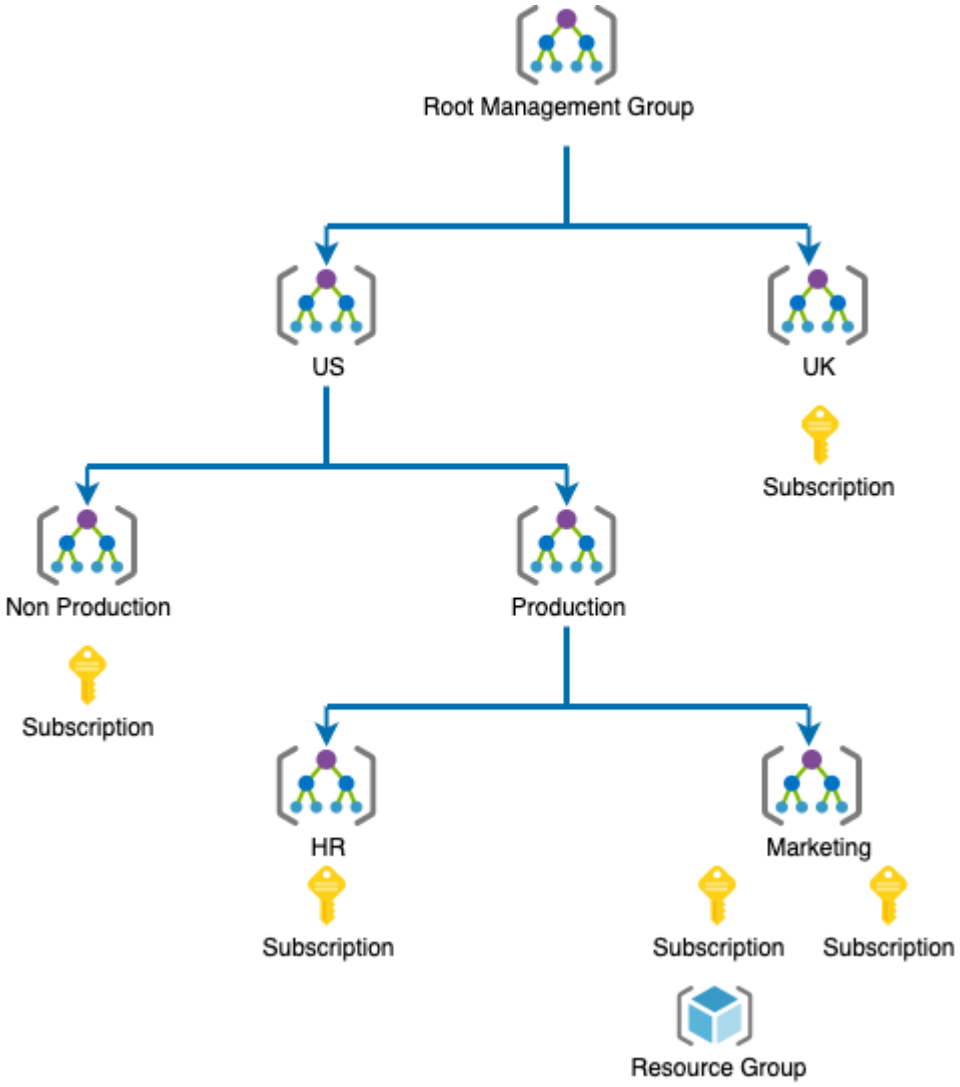


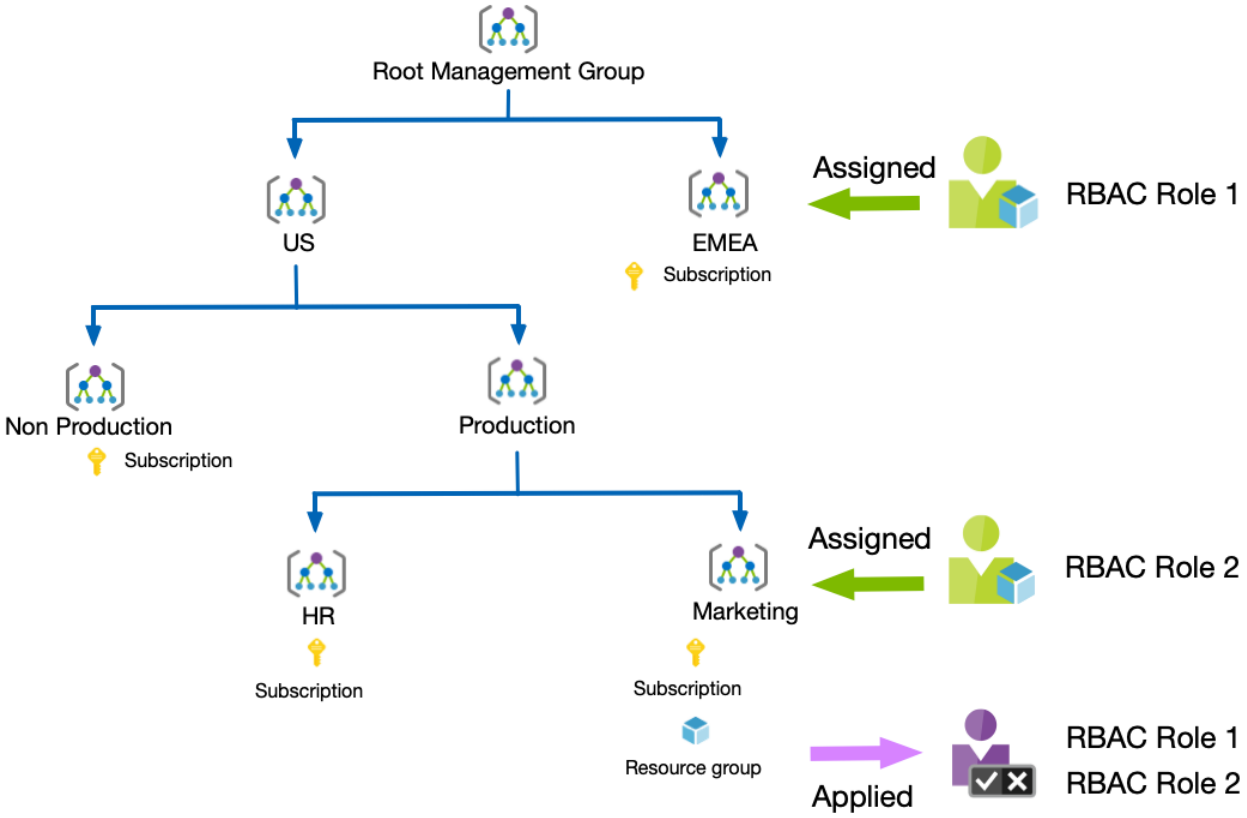


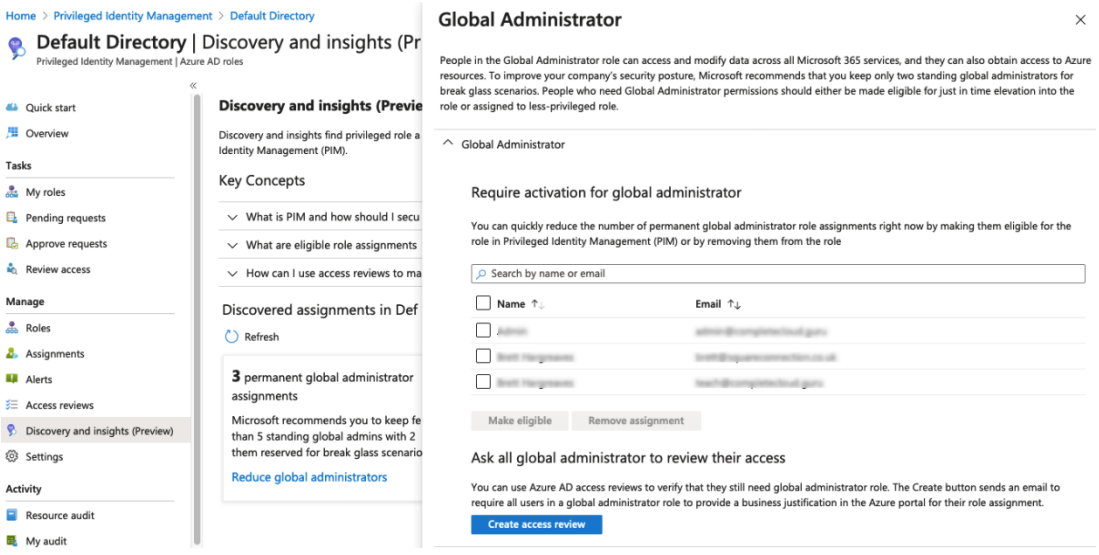

Microsoft Storage
Permissions - Storage Blob Data Contributor (preview)
Microsoft Storage
Storage Accounts
File Service
Storage File Service Files
Storage Blob Services
Storage Blob Service Containers
Storage Blob Service Blobs
Storage Blob Service Blobs
Storage Queue Services
Storage Queue Service Queues
Storage Queue Service Messages


Application administrator | Description
All roles
Diagnose and solve problems
Manage
Assignments
Description
Activity
Bulk operation results
Got feedback?
Role permissions
microsoft.directory/applications/create
Create all types of applications.
microsoft.directory/applications/delete
Delete all types of applications.
microsoft.directory/applications/applicationProxy/read
Read all application proxy properties of all types of applications.
microsoft.directory/applications/applicationProxy/update
Update all application proxy properties of all types of applications.


3
Scope
Management group
Subscription
Resource group
Resource


Root Management Group
US
UK
Subscription
Non Production
Production
Subscription
HR
Marketing
Subscription
Subscription
Subscription
Resource Group


Root Management Group
US
EMEA
Subscription
Assigned
RBAC Role 1
Non Production
Subscription
Production
HR
Subscription
Marketing
Subscription
Resource group
Assigned
RBAC Role 2
Applied
RBAC Role 1
RBAC Role 2


Home > Privileged Identity Management > Default Directory
Default Directory | Discovery and insights (Pr
Privileged Identity Management | Azure AD roles
Quick start
Overview
Tasks
My roles
Pending requests
Approve requests
Review access
Manage
Roles
Assignments
Alerts
Access reviews
Discovery and insights (Preview)
Settings
Activity
Resource audit
My audit
Discovery and insights (Previe
Discovery and insights find privileged role a
Identity Management (PIM).
Key Concepts
What is PIM and how should I secu
What are eligible role assignments
How can I use access reviews to ma
Discovered assignments in Def
Refresh
3 permanent global administrator assignments
Microsoft recommends you to keep fe
than 5 standing global admins with 2
them reserved for break glass scenario
Reduce global administrators
Global Administrator
People in the Global Administrator role can access and modify data across all Microsoft 365 services, and they can also obtain access to Azure resources. To improve your company's security posture, Microsoft recommends that you keep only two standing global administrators for break glass scenarios. People who need Global Administrator permissions should either be made eligible for just in time elevation into the role or assigned to less-privileged role.
Global Administrator
Require activation for global administrator
You can quickly reduce the number of permanent global administrator role assignments right now by making them eligible for the role in Privileged Identity Management (PIM) or by removing them from the role
Search by name or email
Name
Email
Make eligible
Remove assignment
Ask all global administrator to review their access
You can use Azure AD access reviews to verify that they still need global administrator role. The Create button sends an email to require all users in a global administrator role to provide a business justification in the Azure portal for their role assignment.
Create access review

Edit role setting - User Administrator

Privileged Identity Management | Azure AD roles

Activation | Assignment | Notification

Activation maximum duration (hours)

1

On activation, require

- (•) Azure MFA
- ( ) None

- [x] Require justification on activation
- [ ] Require ticket information on activation
- [x] Require approval to activate

Select approver(s)

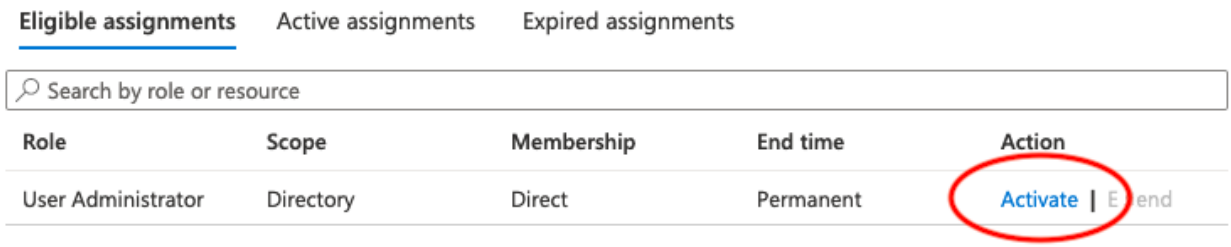
2 Member(s), 0 Group(s) selected

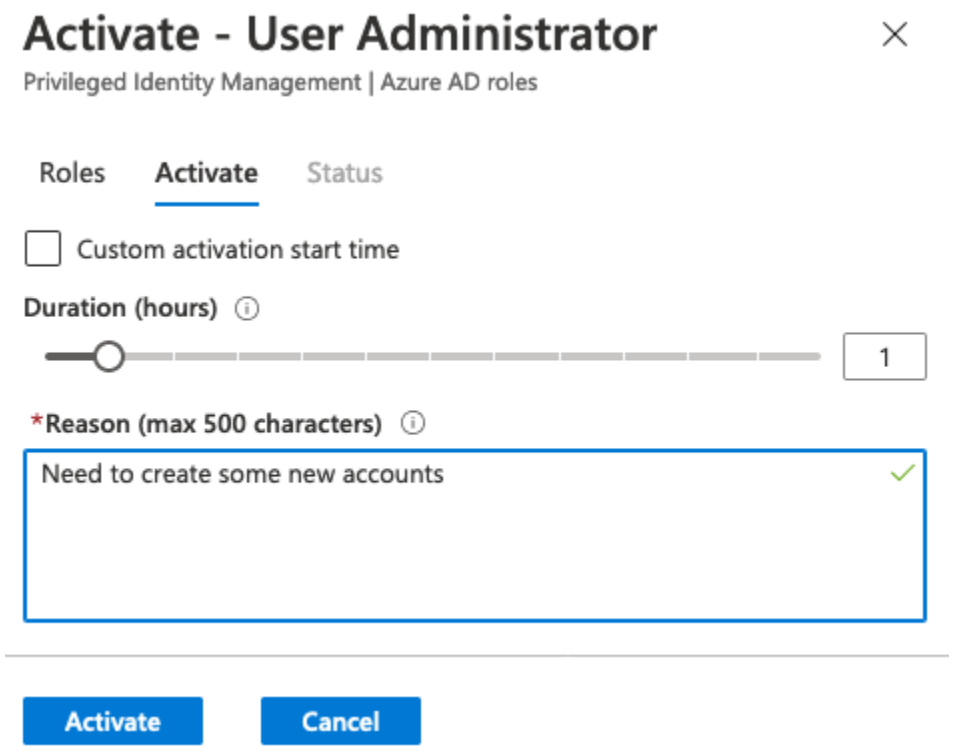
+ Add assignments | Settings | Refresh | Export

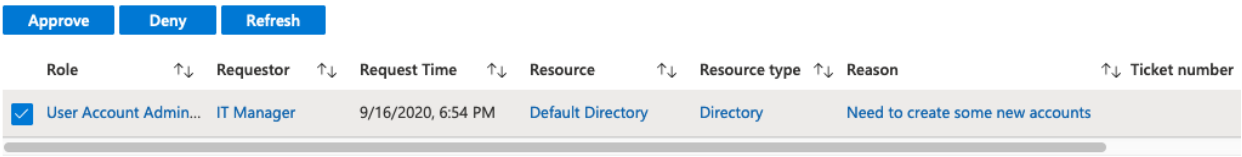
Eligible assignments | Active assignments | Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
User Administrator			
IT Manager	[redacted]	User	Directory


Eligible assignments
Active assignments
Expired assignments
Search by role or resource
Role
Scope
Membership
End time
Action
User Administrator
Directory
Direct
Permanent
Activate | End


Activate - User Administrator
Privileged Identity Management | Azure AD roles
Roles
Activate
Status
Custom activation start time
Duration (hours)
1
*Reason (max 500 characters)
Need to create some new accounts
Activate
Cancel


Approve
Deny
Refresh
Role
Requestor
Request Time
Resource
Resource type
Reason
Ticket number
User Account Admin...
IT Manager
9/16/2020, 6:54 PM
Default Directory
Directory
Need to create some new accounts

Default Directory

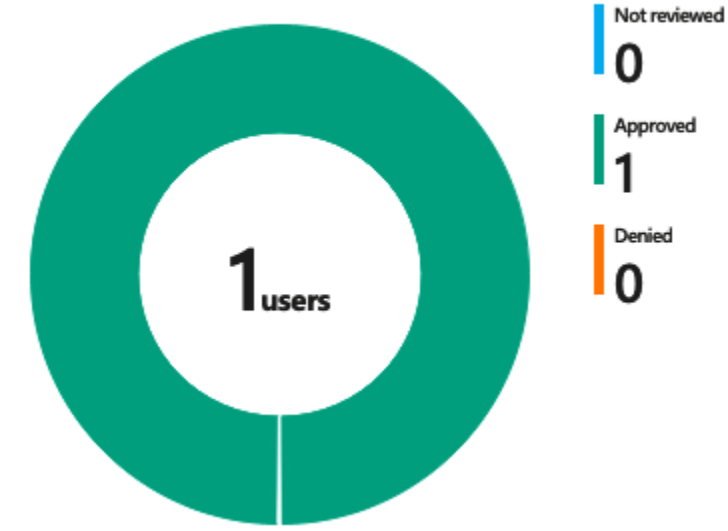
Please review access for users to the User Account Administrator role in the subscription

[redacted], your organisation requested that you approve or deny continued access for one or more users to the **User Account Administrator** role in the subscription. The review period will end on [redacted]

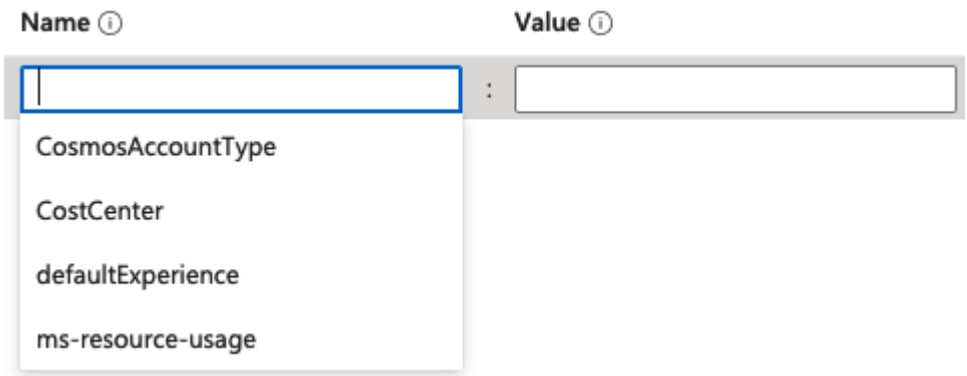
Azure Active Directory Privileged Identity Management enables organisations to regularly review the users in Azure roles to determine whether those users still need access.

Start review >

Progress



Chapter 5: Ensuring Platform Governance



Create a virtual machine

Basics Disks Networking Management Advanced **Tags** Review + create

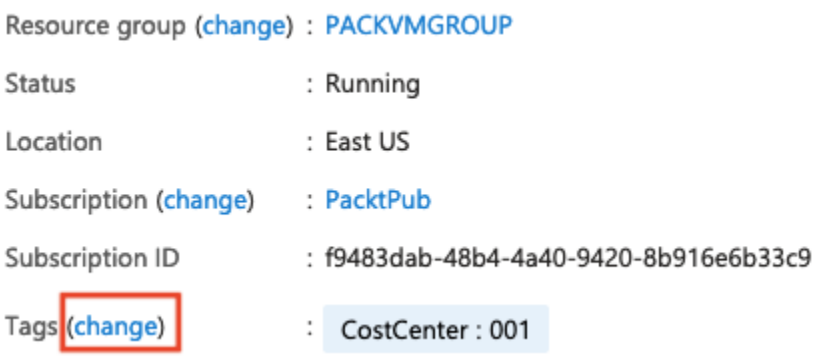
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

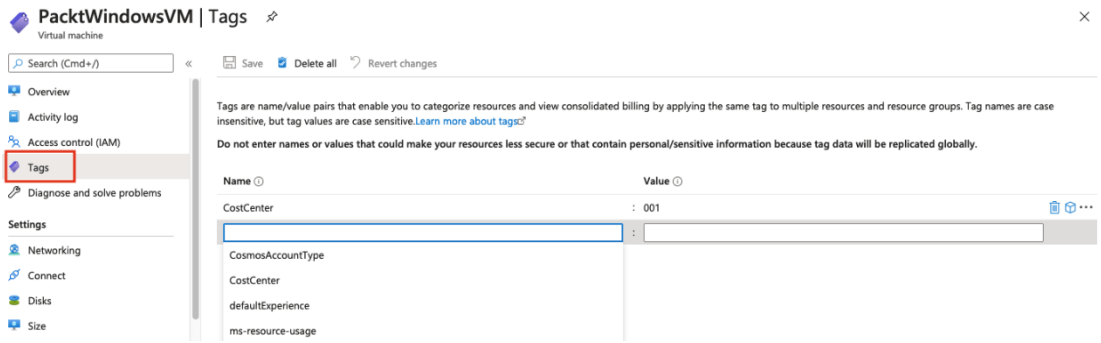
Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

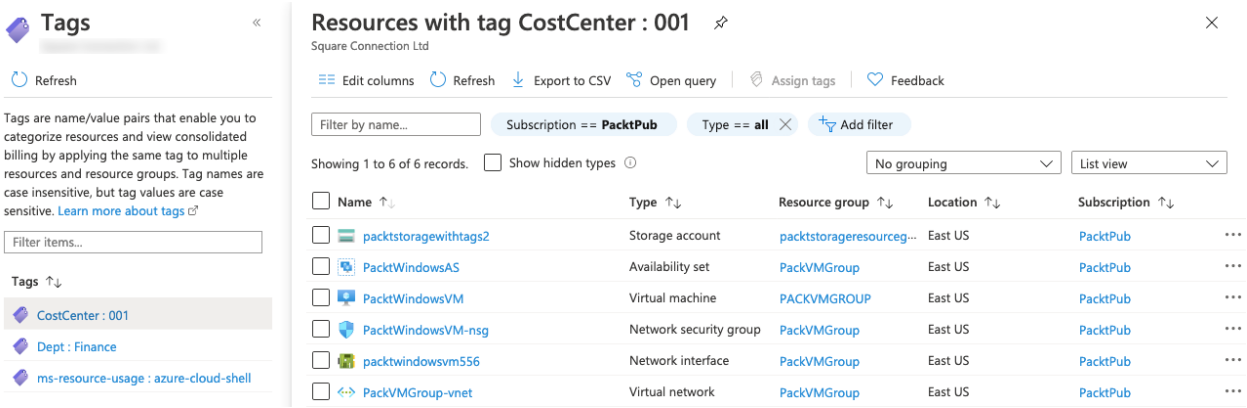
Name	Value	Resource
CostCenter	001	12 selected

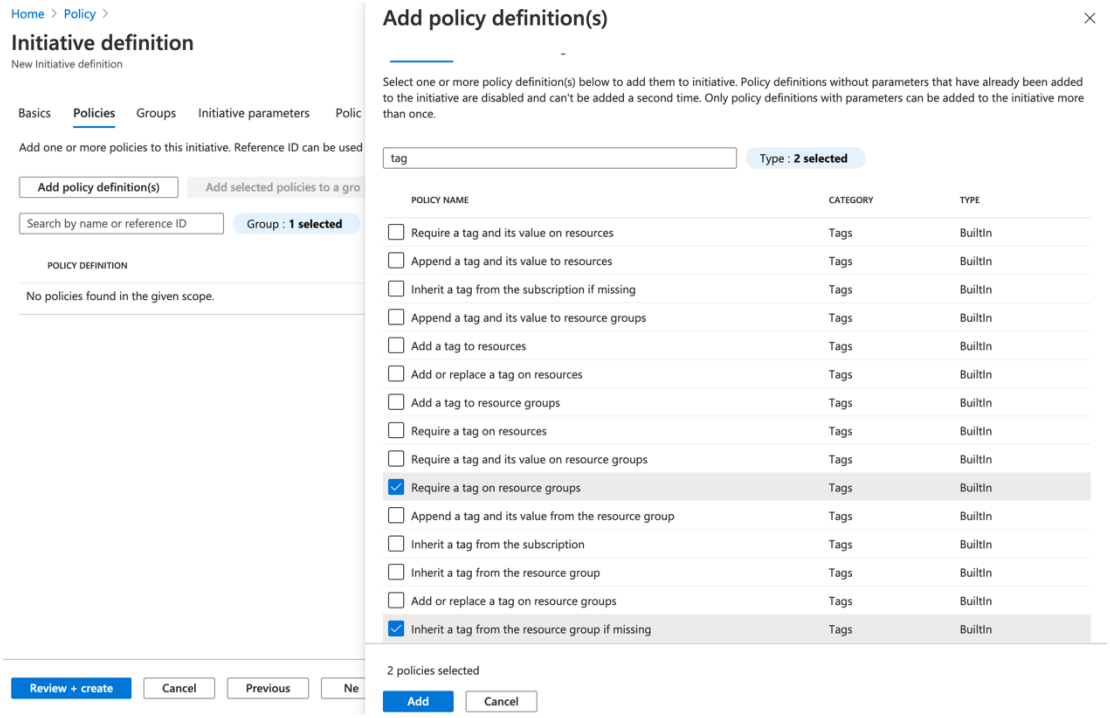
- Select all
- Auto-shutdown schedule
- Availability set
- Disk
- Network interface
- Network security group
- Public IP address
- Recovery Services vault
- SSH key
- Storage account
- Virtual machine
- Virtual machine extension
- Virtual network

Review + create < Previous Next : Review + create >


Resource group (change) : PACKVMGROUP
Status : Running
Location : East US
Subscription (change) : PacktPub
Subscription ID : f9483dab-48b4-4a40-9420-8b916e6b33c9
Tags (change) : CostCenter : 001


PacktWindowsVM | Tags
Virtual machine
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Save
Delete all
Revert changes
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case insensitive, but tag values are case sensitive.Learn more about tags
Do not enter names or values that could make your resources less secure or that contain personal/sensitive information because tag data will be replicated globally.
Name
Value
CostCenter : 001
CosmosAccountType
CostCenter
defaultExperience
ms-resource-usage


Tags
Refresh
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case insensitive, but tag values are case sensitive. Learn more about tags
Filter items...
Tags
CostCenter : 001
Dept : Finance
ms-resource-usage : azure-cloud-shell
Resources with tag CostCenter : 001
Square Connection Ltd
Edit columns
Refresh
Export to CSV
Open query
Assign tags
Feedback
Filter by name...
Subscription == PacktPub
Type == all
Add filter
Showing 1 to 6 of 6 records.
Show hidden types
No grouping
List view
Name
Type
Resource group
Location
Subscription
packtstoragewithtags2 Storage account packtstorageresourceg... East US PacktPub
PacktWindowsAS Availability set PackVMGroup East US PacktPub
PacktWindowsVM Virtual machine PACKVMGROUP East US PacktPub
PacktWindowsVM-nsg Network security group PackVMGroup East US PacktPub
packtwindowsvm556 Network interface PackVMGroup East US PacktPub
PackVMGroup-vnet Virtual network PackVMGroup East US PacktPub


Home > Policy >
Initiative definition
New Initiative definition
Basics
Policies
Groups
Initiative parameters
Polic
Add one or more policies to this initiative. Reference ID can be used
Add policy definition(s)
Add selected policies to a gro
Search by name or reference ID
Group : 1 selected
POLICY DEFINITION
No policies found in the given scope.
Review + create
Cancel
Previous
Ne
Add policy definition(s)
Select one or more policy definition(s) below to add them to initiative. Policy definitions without parameters that have already been added to the initiative are disabled and can't be added a second time. Only policy definitions with parameters can be added to the initiative more than once.
tag
Type : 2 selected
POLICY NAME
CATEGORY
TYPE
Require a tag and its value on resources
Tags
BuiltIn
Append a tag and its value to resources
Tags
BuiltIn
Inherit a tag from the subscription if missing
Tags
BuiltIn
Append a tag and its value to resource groups
Tags
BuiltIn
Add a tag to resources
Tags
BuiltIn
Add or replace a tag on resources
Tags
BuiltIn
Add a tag to resource groups
Tags
BuiltIn
Require a tag on resources
Tags
BuiltIn
Require a tag and its value on resource groups
Tags
BuiltIn
Require a tag on resource groups
Tags
BuiltIn
Append a tag and its value from the resource group
Tags
BuiltIn
Inherit a tag from the subscription
Tags
BuiltIn
Inherit a tag from the resource group
Tags
BuiltIn
Add or replace a tag on resource groups
Tags
BuiltIn
Inherit a tag from the resource group if missing
Tags
BuiltIn
2 policies selected
Add
Cancel

Details **Definition**

Duplicate this policy definition

```
{
  "properties": {
    "displayName": "Require a tag on resource groups",
    "policyType": "BuiltIn",
    "mode": "All",
    "description": "Enforces existence of a tag on resource groups.",
    "metadata": {
      "version": "1.0.0",
      "category": "Tags"
    },
    "parameters": {
      "tagName": {
        "type": "String",
        "metadata": {
          "displayName": "Tag Name",
          "description": "Name of the tag, such as 'environment'"
        }
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Resources/subscriptions/resourceGroups"
          },
          {
            "field": "[concat('tags[', parameters('tagName'), ']')]",
            "exists": "false"
          }
        ]
      },
      "then": {
        "effect": "deny"
      }
    }
  },
```

Initiative definition

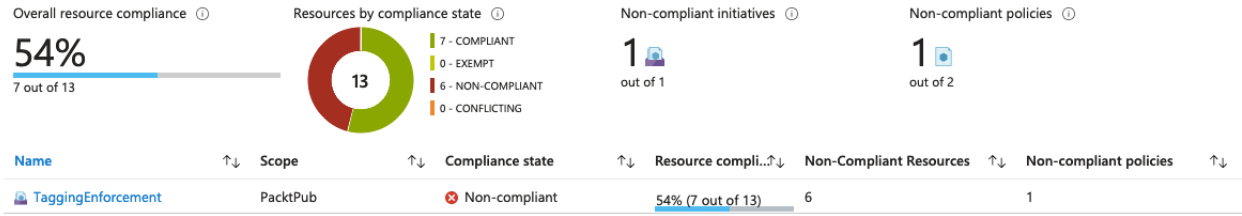
New Initiative definition

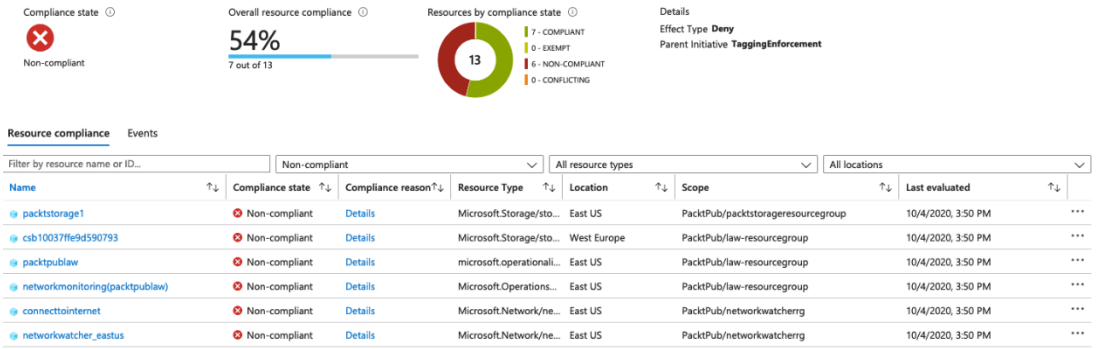
Basics Policies Groups Initiative parameters **Policy parameters** Review + create

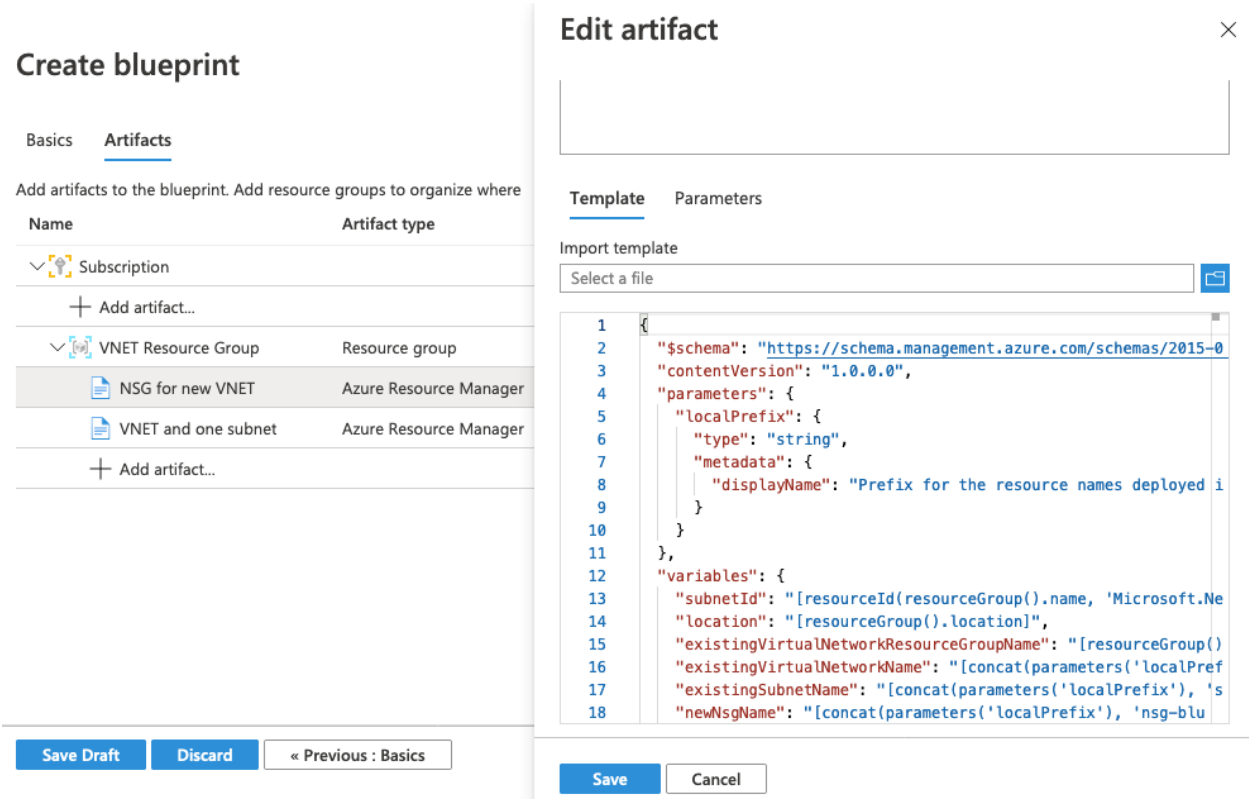
Policy parameters are inputs into individual policies.

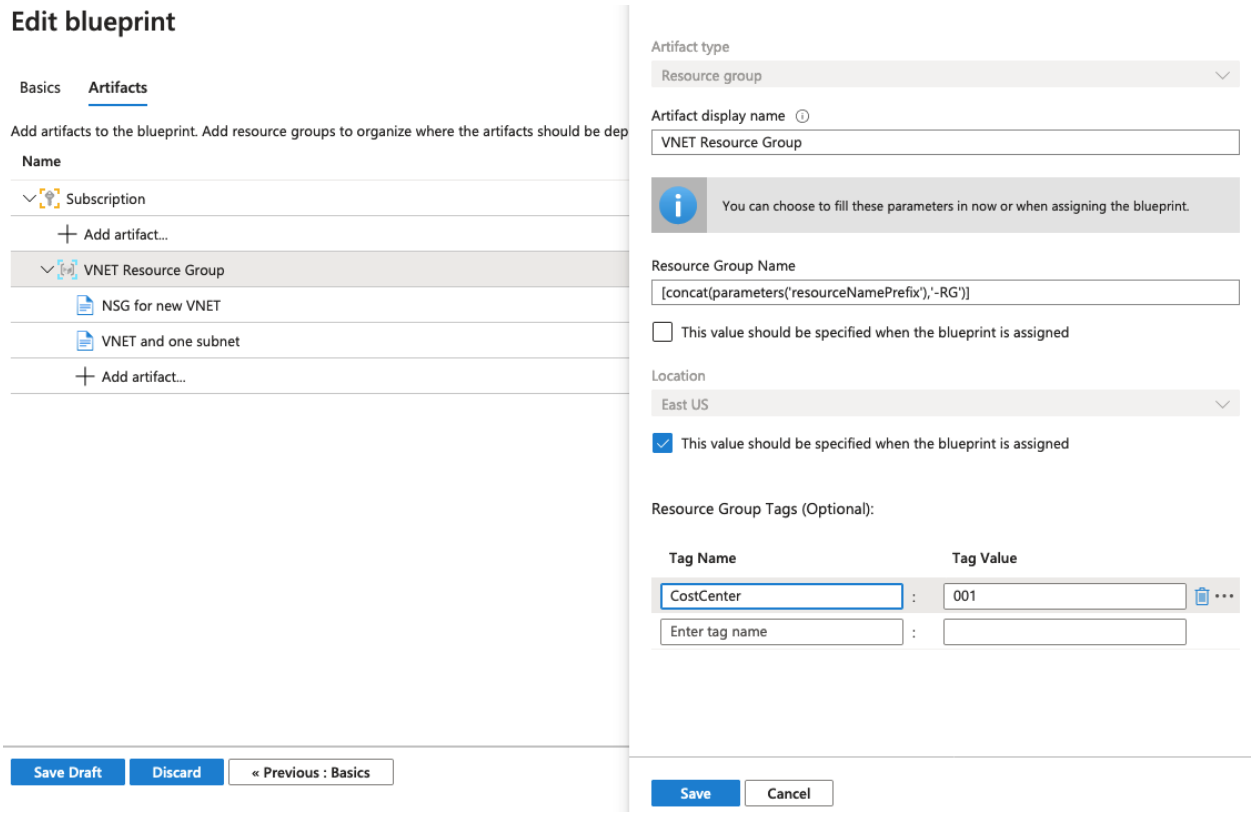
Search by reference ID or paramete...

REFERENCE ID	PARAMETER NAME	TYPE	VALUE TYPE	VALUE(S)
Require a tag on resource groups_1	Tag Name	String	Use Initiative Param...	TagName
Inherit a tag from the resource group i...	Tag Name	String	Use Initiative Param...	TagName


Overall resource compliance
54%
7 out of 13
Resources by compliance state
13
7 - COMPLIANT
0 - EXEMPT
6 - NON-COMPLIANT
0 - CONFLICTING
Non-compliant initiatives
1
out of 1
Non-compliant policies
1
out of 2
Name
Scope
Compliance state
Resource compli..
Non-Compliant Resources
Non-compliant policies
TaggingEnforcement
PacktPub
Non-compliant
54% (7 out of 13)
6
1


Compliance state
Non-compliant
Overall resource compliance
54%
7 out of 13
Resources by compliance state
13
7 - COMPLIANT
0 - EXEMPT
6 - NON-COMPLIANT
0 - CONFLICTING
Details
Effect Type Deny
Parent Initiative TaggingEnforcement
Resource compliance
Events
Filter by resource name or ID...
Non-compliant
All resource types
All locations
Name
Compliance state
Compliance reason
Resource Type
Location
Scope
Last evaluated
packtstorage1
csb10037ffe9d590793
packtpublaw
networkmonitoring(packtpublaw)
connecttointernet
networkwatcher_eastus
Non-compliant
Details
Microsoft.Storage/sto...
Microsoft.Operationali...
Microsoft.Operations...
Microsoft.Network/ne...
East US
West Europe
PacktPub/packtstorageresourcegroup
PacktPub/law-resourcegroup
PacktPub/networkwatcherrg
10/4/2020, 3:50 PM


Create blueprint
Basics
Artifacts
Add artifacts to the blueprint. Add resource groups to organize where
Name
Artifact type
Subscription
Add artifact...
VNET Resource Group
Resource group
NSG for new VNET
Azure Resource Manager
VNET and one subnet
Azure Resource Manager
Add artifact...
Save Draft
Discard
« Previous : Basics
Edit artifact
Template
Parameters
Import template
Select a file
{
"$schema": "https://schema.management.azure.com/schemas/2015-0
"contentVersion": "1.0.0.0",
"parameters": {
"localPrefix": {
"type": "string",
"metadata": {
"displayName": "Prefix for the resource names deployed i
}
}
},
"variables": {
"subnetId": "[resourceId(resourceGroup().name, 'Microsoft.Ne
"location": "[resourceGroup().location]",
"existingVirtualNetworkResourceGroupName": "[resourceGroup()
"existingVirtualNetworkName": "[concat(parameters('localPref
"existingSubnetName": "[concat(parameters('localPrefix'), 's
"newNsgName": "[concat(parameters('localPrefix'), 'nsg-blu
Save
Cancel


Edit blueprint
Basics
Artifacts
Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be dep
Name
Subscription
Add artifact...
VNET Resource Group
NSG for new VNET
VNET and one subnet
Add artifact...
Save Draft
Discard
« Previous : Basics
Artifact type
Resource group
Artifact display name
VNET Resource Group
You can choose to fill these parameters in now or when assigning the blueprint.
Resource Group Name
[concat(parameters('resourceNamePrefix'),'-RG')]
This value should be specified when the blueprint is assigned
Location
East US
This value should be specified when the blueprint is assigned
Resource Group Tags (Optional):
Tag Name
Tag Value
CostCenter
001
Enter tag name
Save
Cancel

Assign blueprint

Basics

Subscription(s) * ⓘ

PacktPub

Create new Learn more about creating subscriptions.

Assignment name * ⓘ

Assignment-CoreSystems

Location * ⓘ

East US

Blueprint definition version * ⓘ

1.0

Lock Assignment

Don't Lock | Do Not Delete | Read Only

The assignment is locked. Deployed resources can't be deleted - even by subscription owners. Not all resource types support locking. Due to caching, locks may take up to 30 minutes to become enforced.
Learn more

Assign | Cancel

Blueprint parameters

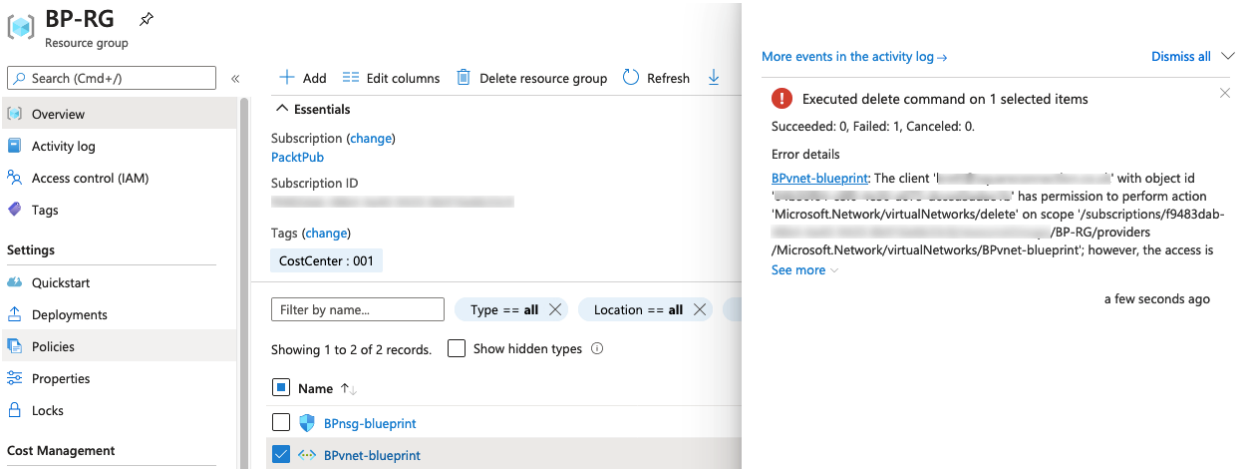
Resource name prefix * ⓘ

BP-

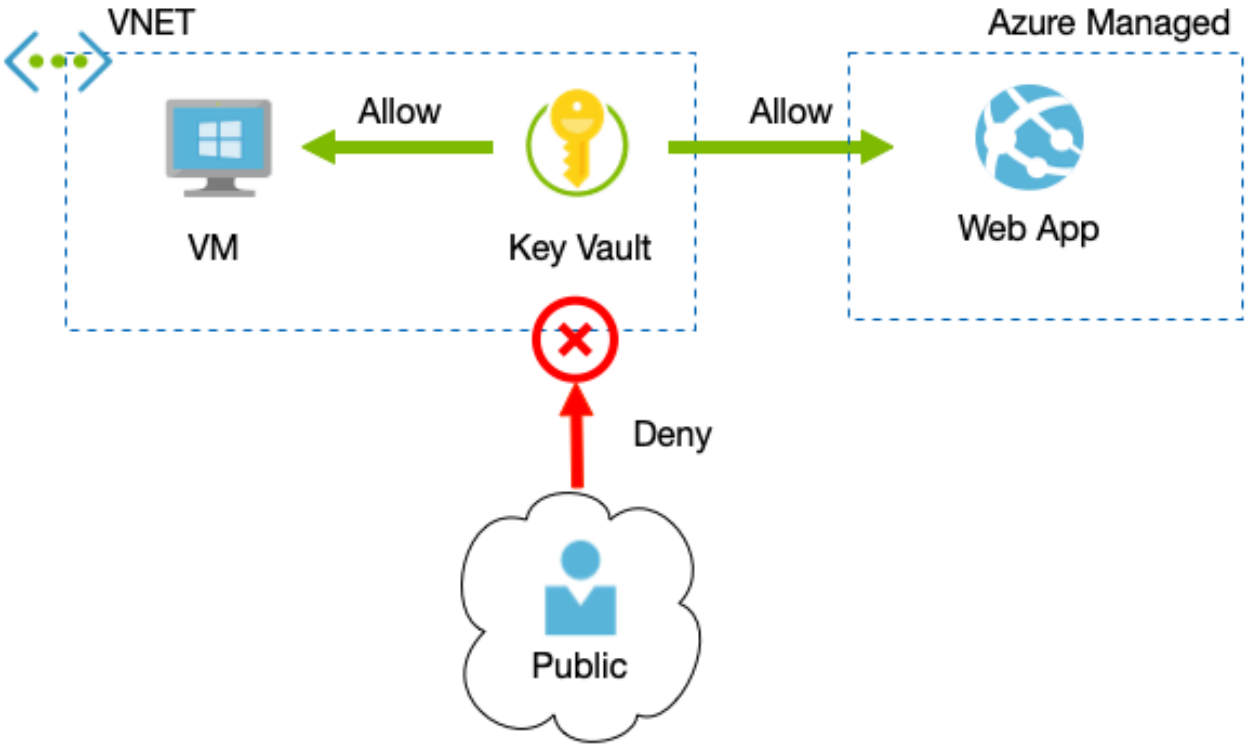
Artifact parameters

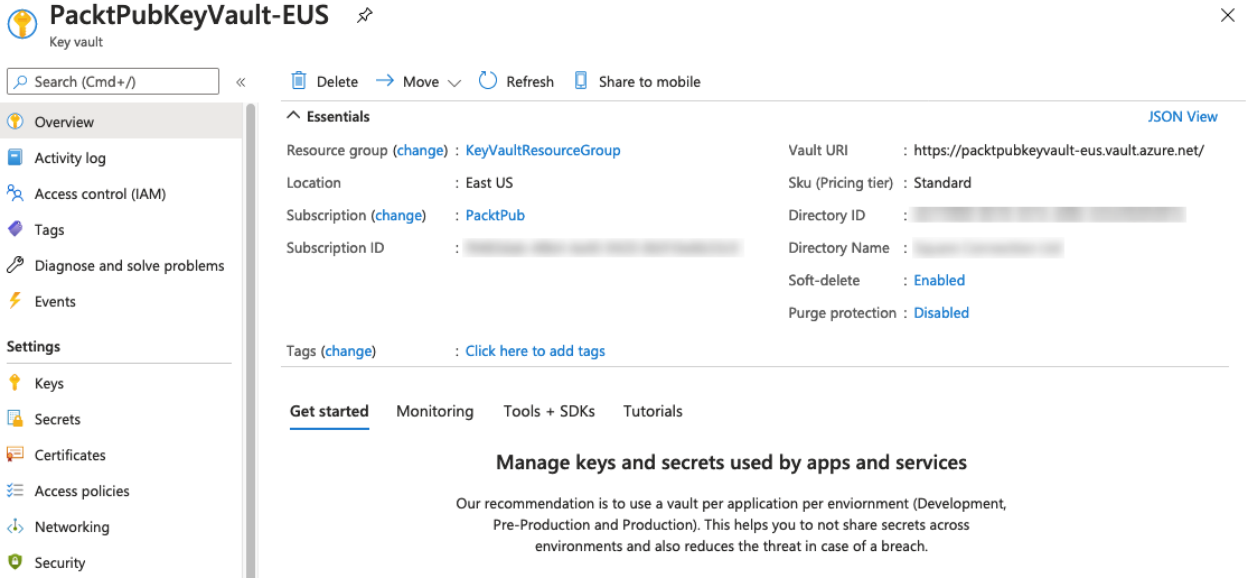
Artifact / Parameter	Parameter Value
Subscription	
VNET Resource Group	
Resource Group: Name	[concat(parameters('resourceNamePrefix'),'-RG')]
Resource Group: Location	East US
NSG for new VNET	
VNET and one subnet	
Addess space for vnet	10.0.0.0/16
Addess space for subnet	10.0.0.0/24

Assign Cancel



Chapter 6: Building Application Security





Properties

Created 10/14/2020, 11:09:16 AM

Updated 10/14/2020, 11:09:16 AM

Secret Identifier

https://packtpubkeyvault.vault.azure.net/secrets/SecureConnection ...

Settings

Set activation date?

Set expiration date?

Enabled? Yes No

Tags

0 tags

Secret

Content type (optional)

Hide Secret Value

Secret value

MyReallySecureConnectionString

SecureWebApp

Search (Cmd+/)

Overview

Quickstart

Integration assistant | Preview

Manage

Delete Endpoints Preview features

Essentials

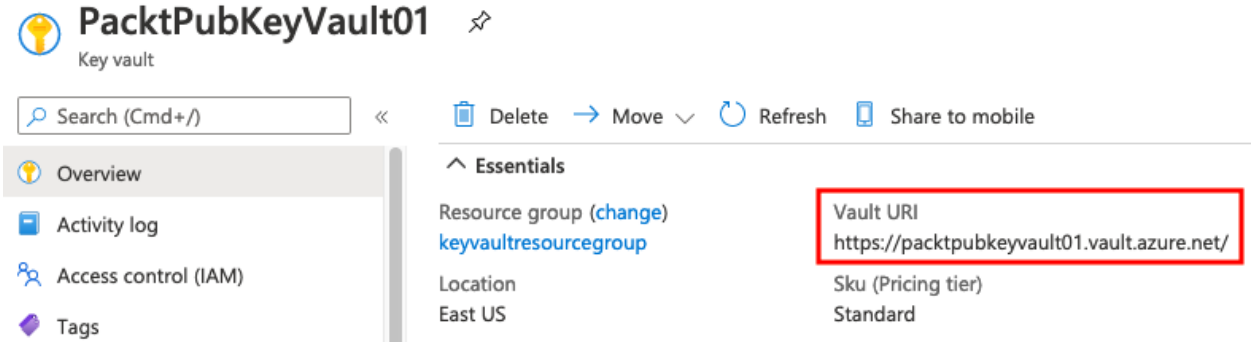
Display name	: SecureWebApp	Supported account types	: My organization only
Application (client) ID	: de167063-90a5-4bcd-88a7-3cd185c80901	Redirect URIs	: Add a Redirect URI
Directory (tenant) ID	: [redacted]	Application ID URI	: Add an Application ID URI
Object ID	: [redacted]	Managed application in l...	: SecureWebApp

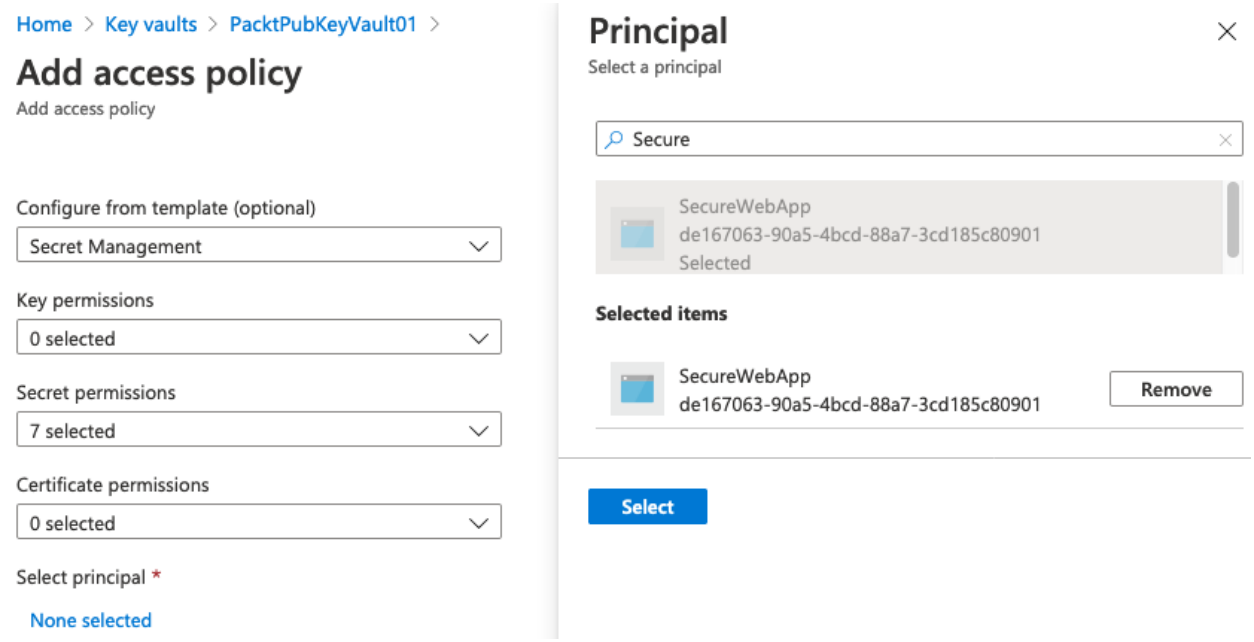
Client secrets

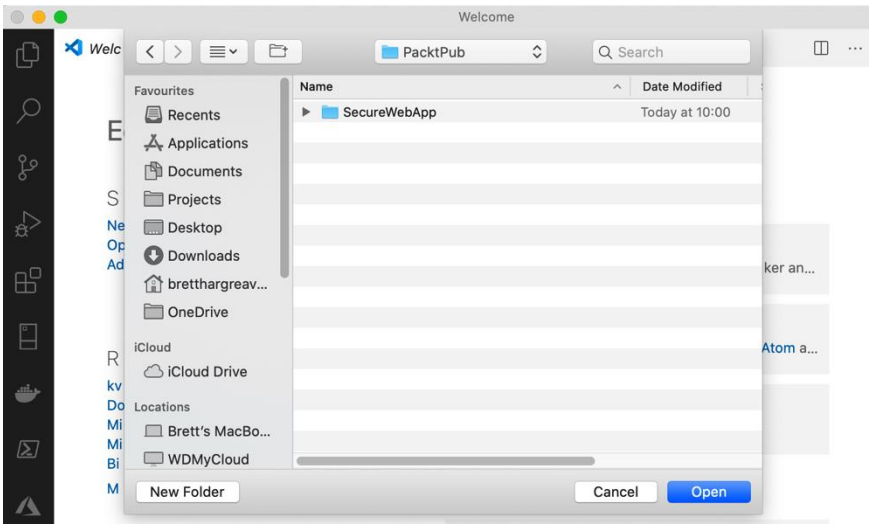
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

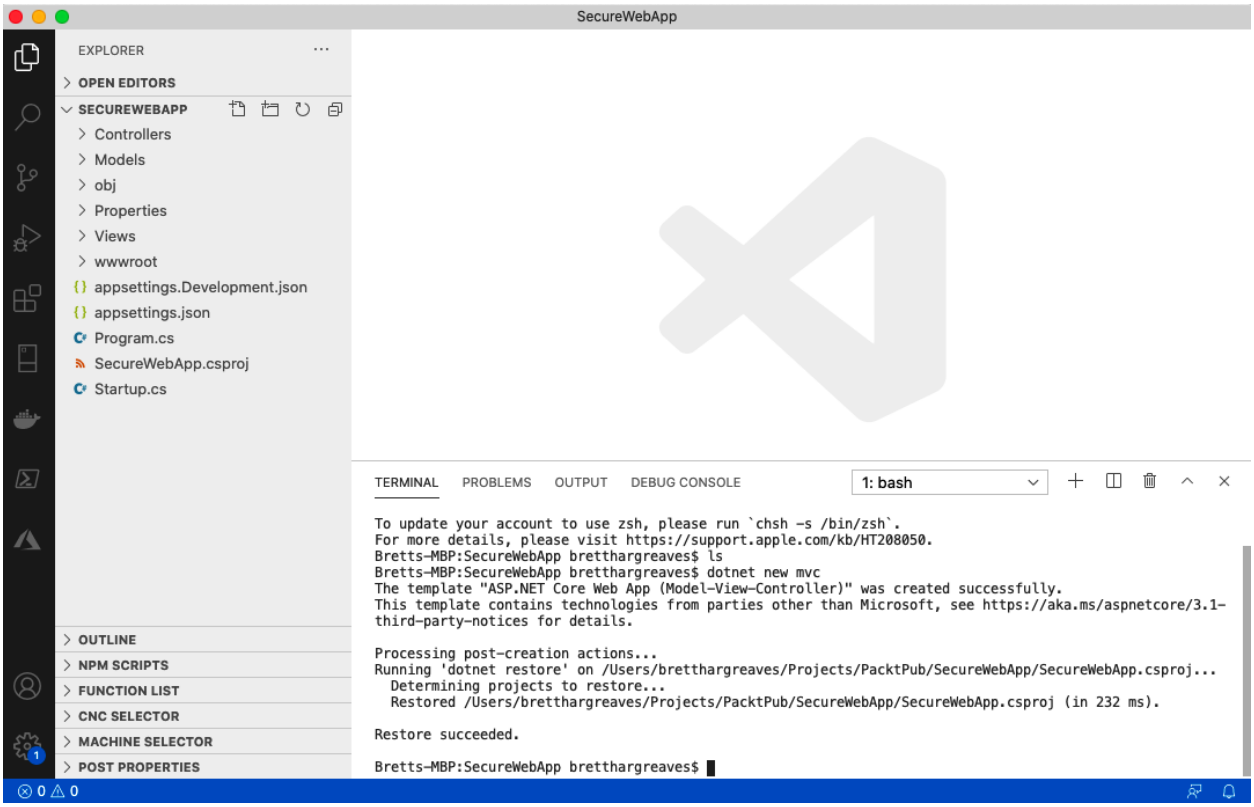
+ New client secret

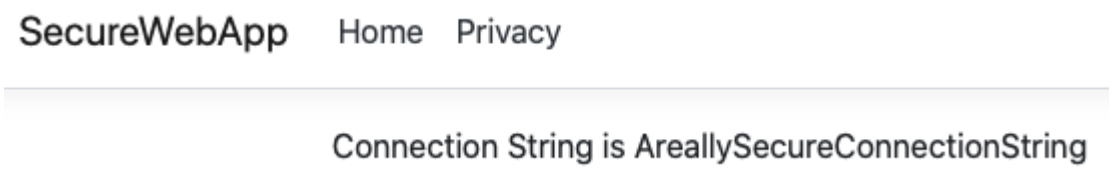
Description	Expires	Value
WebAppAccess	10/15/2021	u-94Gz_wOL_4nQa2Alz_K-Dui1u4416COt

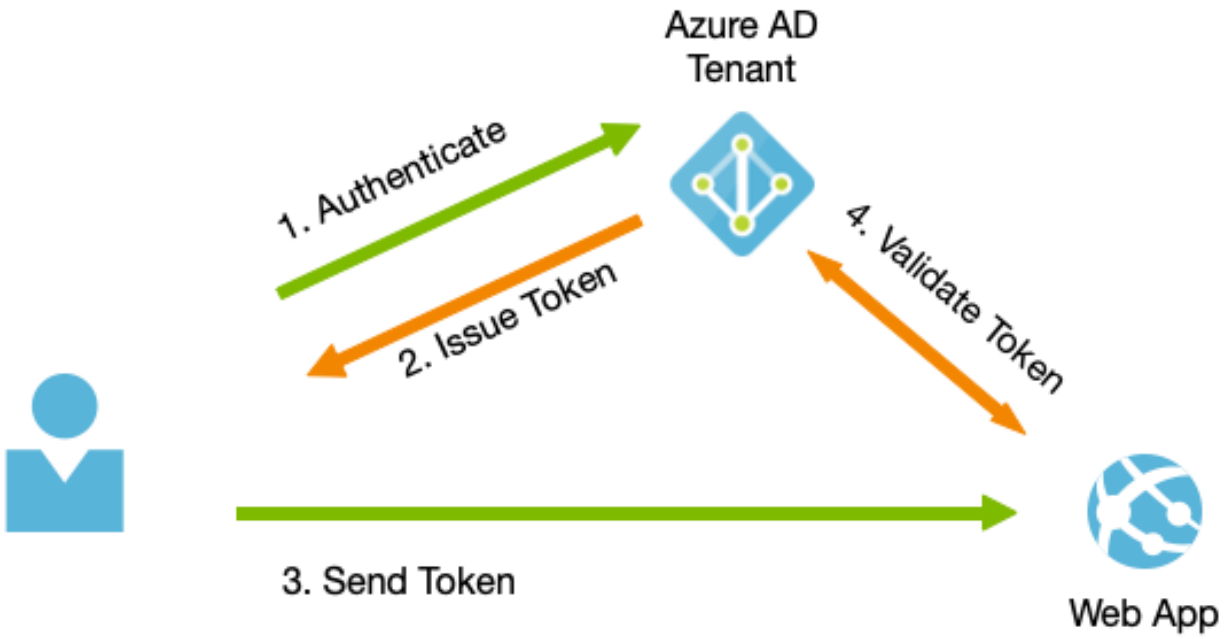


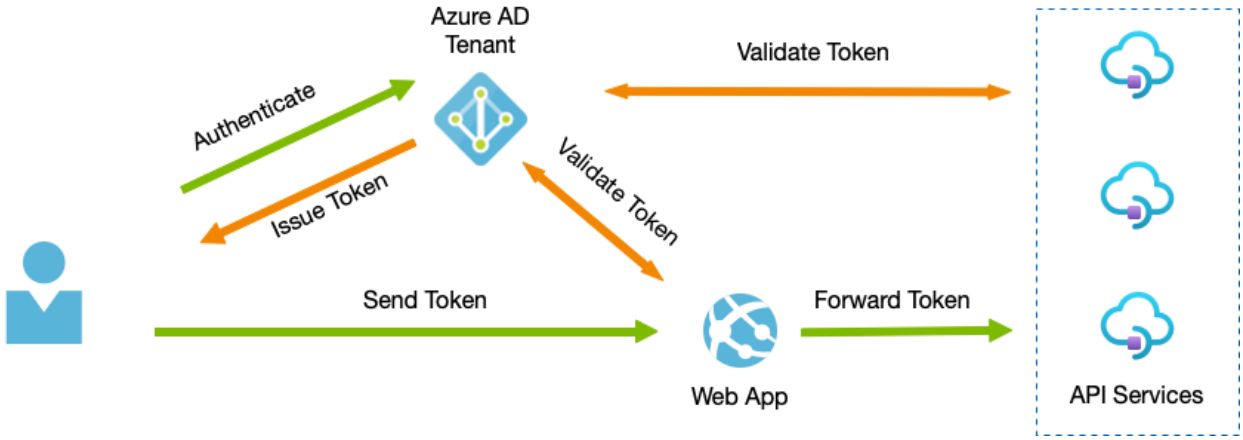


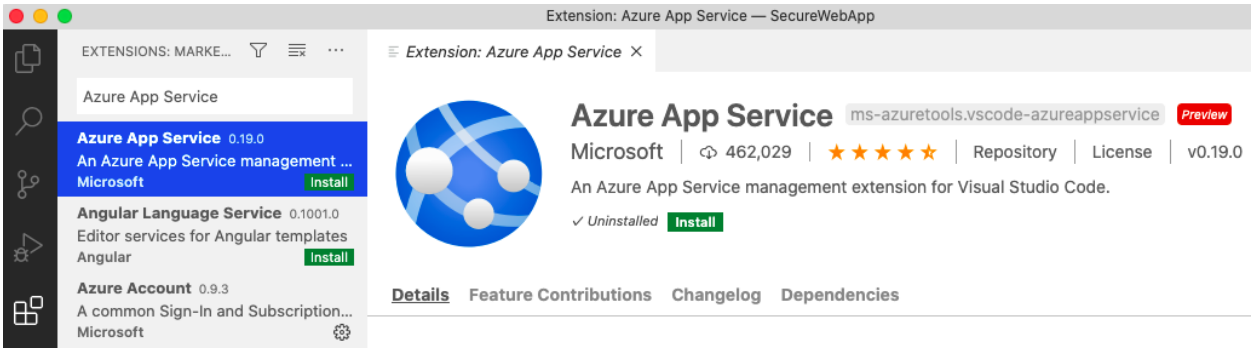

Welcome
PacktPub
Search
Favourites
Recents
Applications
Documents
Projects
Desktop
Downloads
bretthargreav...
OneDrive
iCloud
iCloud Drive
Locations
Brett's MacBo...
WDMyCloud
Name
Date Modified
SecureWebApp
Today at 10:00
New Folder
Cancel
Open

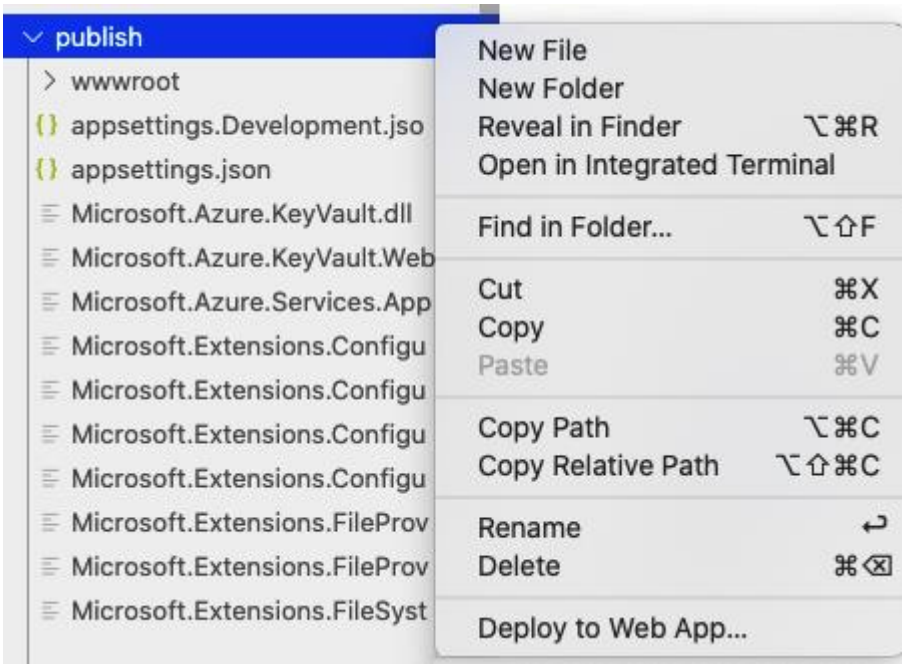

SecureWebApp
EXPLORER
OPEN EDITORS
SECUREWEBAPP
Controllers
Models
obj
Properties
Views
wwwroot
appsettings.Development.json
appsettings.json
Program.cs
SecureWebApp.csproj
Startup.cs
OUTLINE
NPM SCRIPTS
FUNCTION LIST
CNC SELECTOR
MACHINE SELECTOR
POST PROPERTIES
TERMINAL
PROBLEMS
OUTPUT
DEBUG CONSOLE
1: bash
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Bretts-MBP:SecureWebApp bretthargreaves$ ls
Bretts-MBP:SecureWebApp bretthargreaves$ dotnet new mvc
The template "ASP.NET Core Web App (Model-View-Controller)" was created successfully.
This template contains technologies from parties other than Microsoft, see https://aka.ms/aspnetcore/3.1-third-party-notices for details.
Processing post-creation actions...
Running 'dotnet restore' on /Users/bretthargreaves/Projects/PacktPub/SecureWebApp/SecureWebApp.csproj...
Determining projects to restore...
Restored /Users/bretthargreaves/Projects/PacktPub/SecureWebApp/SecureWebApp.csproj (in 232 ms).
Restore succeeded.
Bretts-MBP:SecureWebApp bretthargreaves$

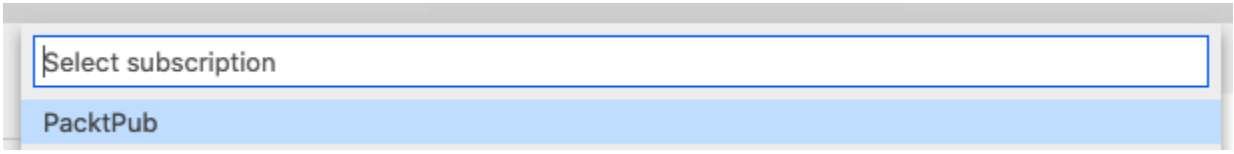

SecureWebApp
Home
Privacy
Connection String is AreallySecureConnectionString

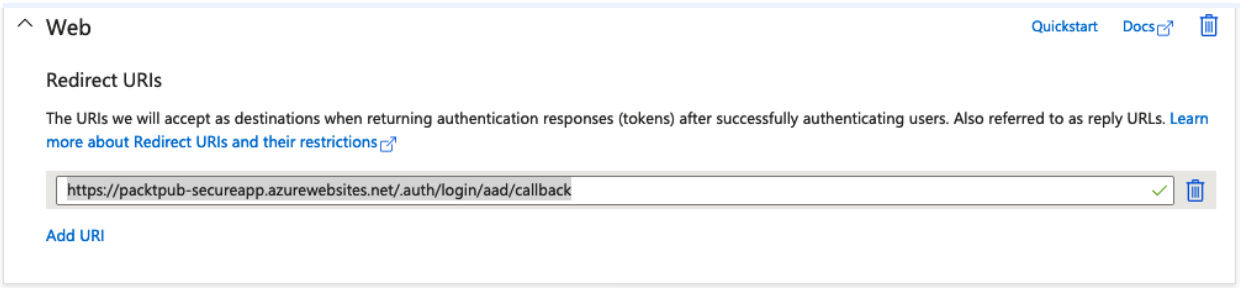

Azure AD
Tenant
1. Authenticate
2. Issue Token
4. Validate Token
3. Send Token
Web App


Azure AD
Tenant
Validate Token
Authenticate
Issue Token
Validate Token
Send Token
Forward Token
Web App
API Services


Extension: Azure App Service — SecureWebApp
EXTENSIONS: MARKE...
Extension: Azure App Service
Azure App Service
Azure App Service 0.19.0
An Azure App Service management ...
Microsoft
Install
Angular Language Service 0.1001.0
Editor services for Angular templates
Angular
Install
Azure Account 0.9.3
A common Sign-In and Subscription...
Microsoft
Azure App Service
ms-azuretools.vscode-azureappservice
Preview
Microsoft
462,029
Repository
License
v0.19.0
An Azure App Service management extension for Visual Studio Code.
✓ Uninstalled
Install
Details
Feature Contributions
Changelog
Dependencies







Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

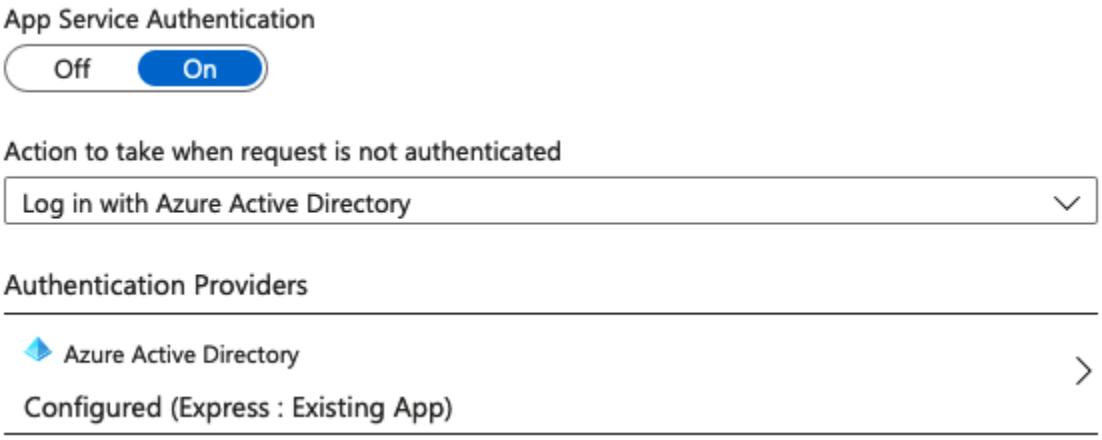
e.g. https://myapp.com/logout

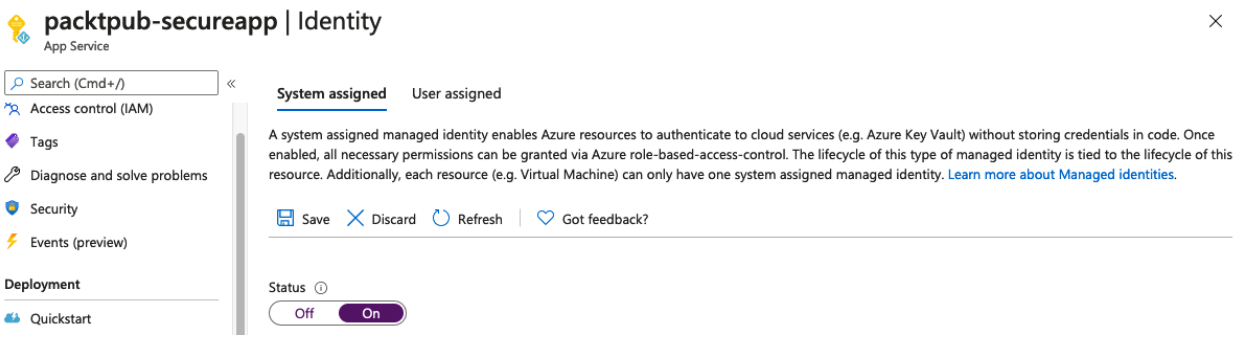
Implicit grant

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single-page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. Learn more about the implicit grant flow

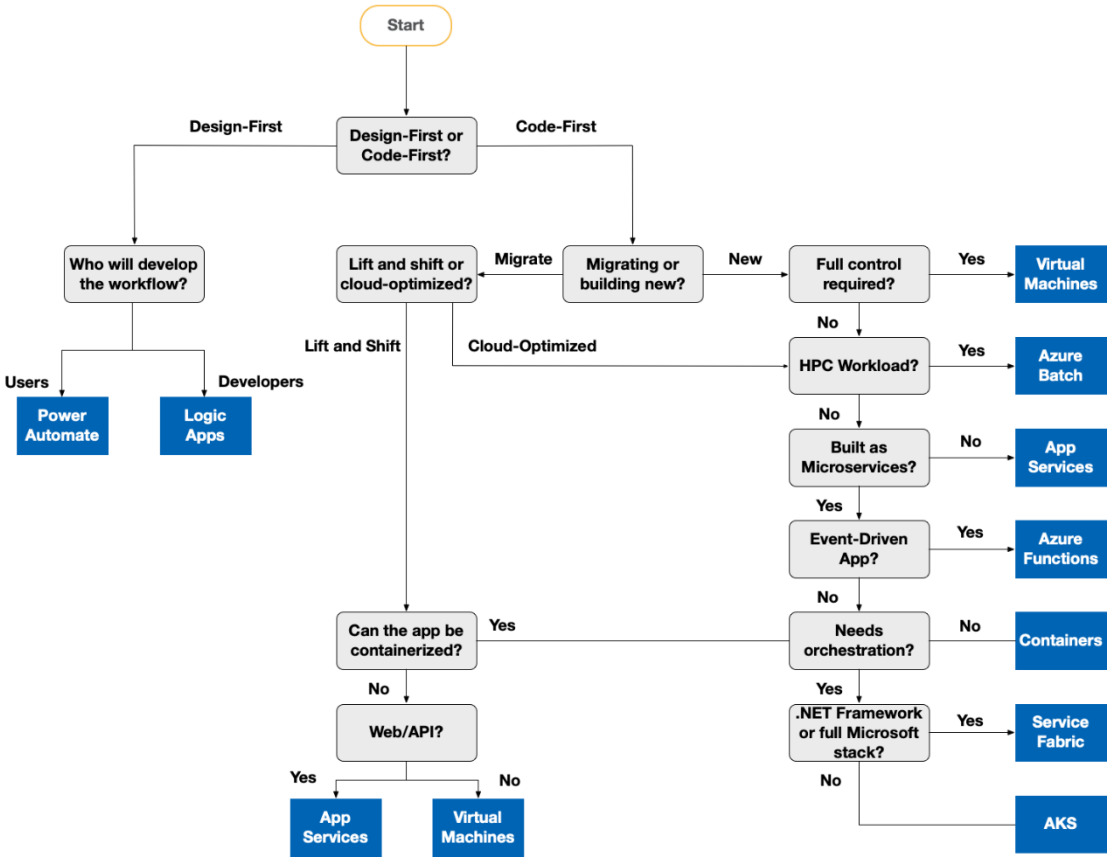
To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

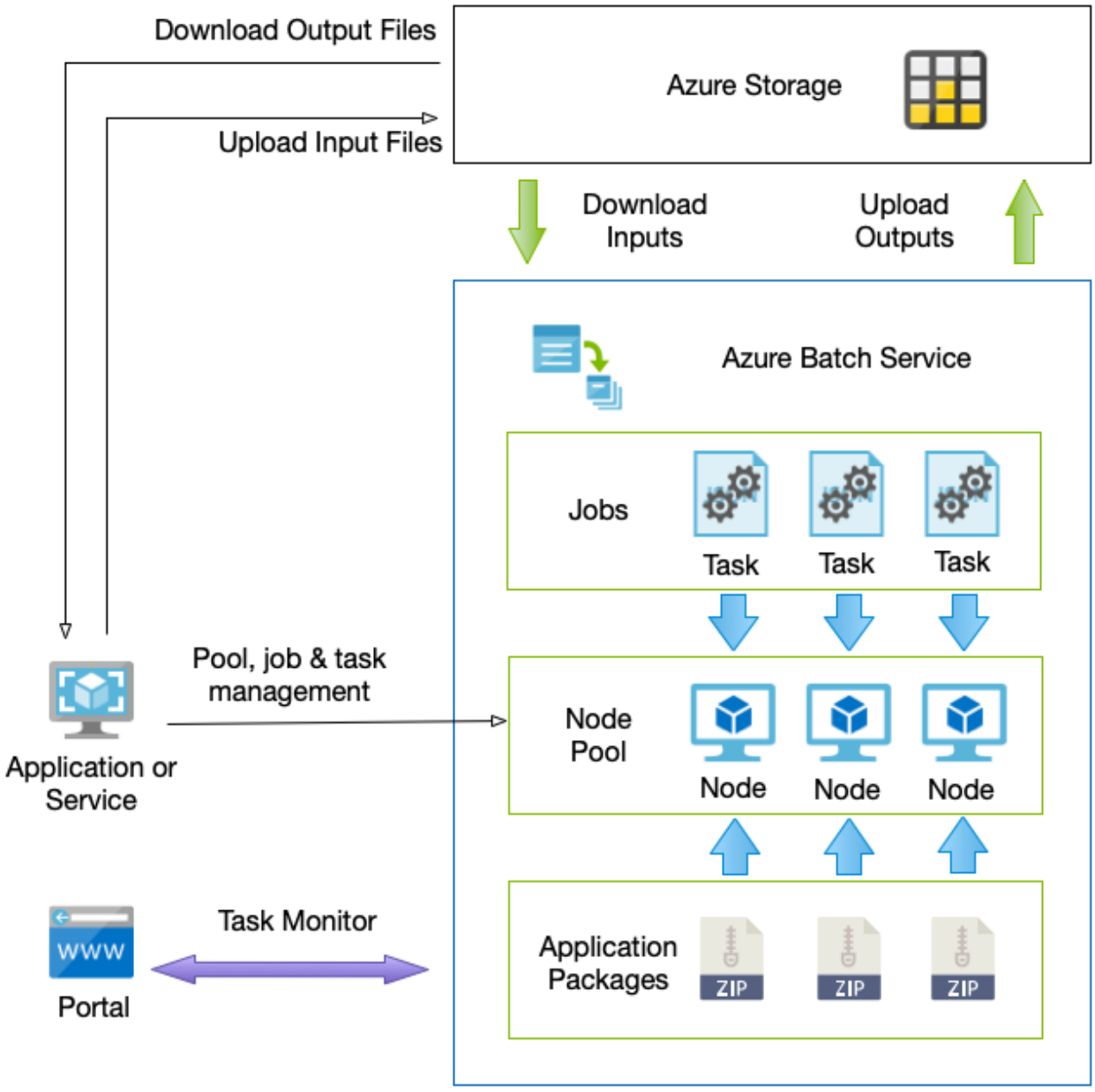
- [ ] Access tokens
- [x] ID tokens

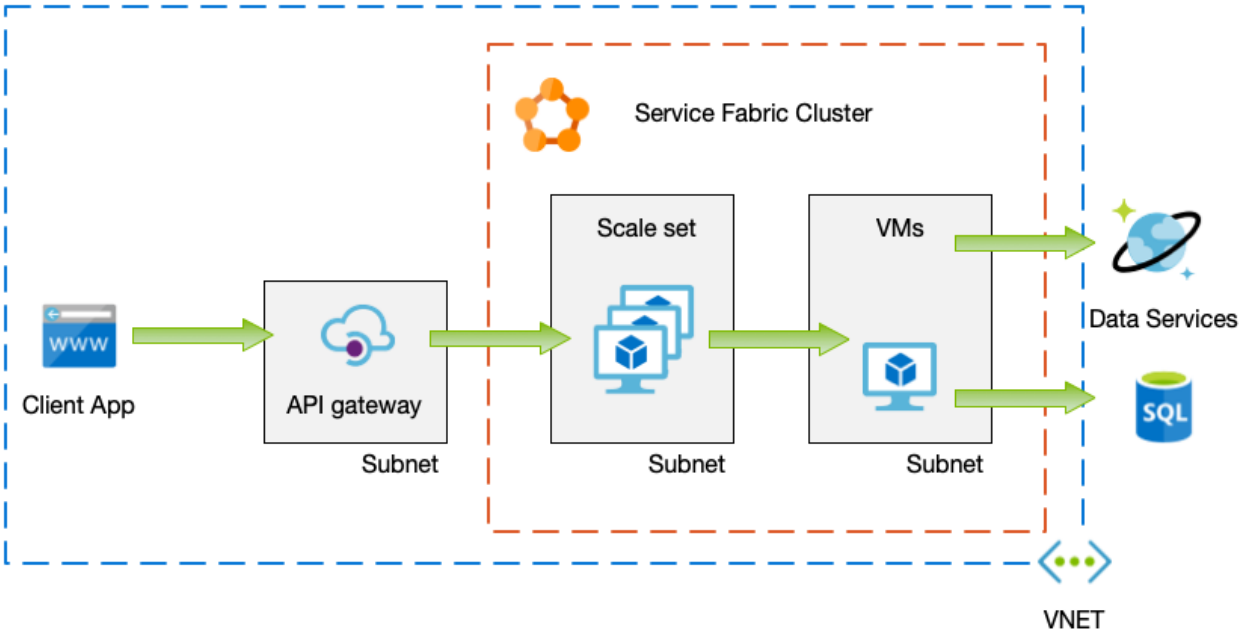

App Service Authentication
Off
On
Action to take when request is not authenticated
Log in with Azure Active Directory
Authentication Providers
Azure Active Directory
Configured (Express : Existing App)

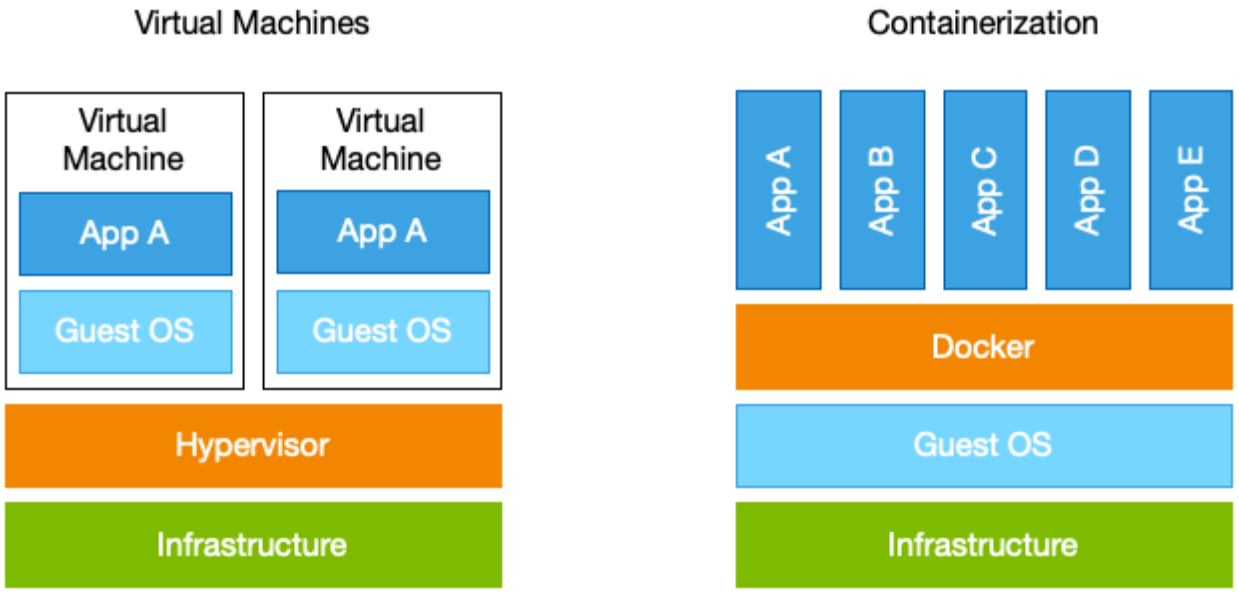

packtpub-secureapp | Identity
App Service
Search (Cmd+/)
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events (preview)
Deployment
Quickstart
System assigned
User assigned
A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned managed identity. Learn more about Managed identities.
Save
Discard
Refresh
Got feedback?
Status
Off
On

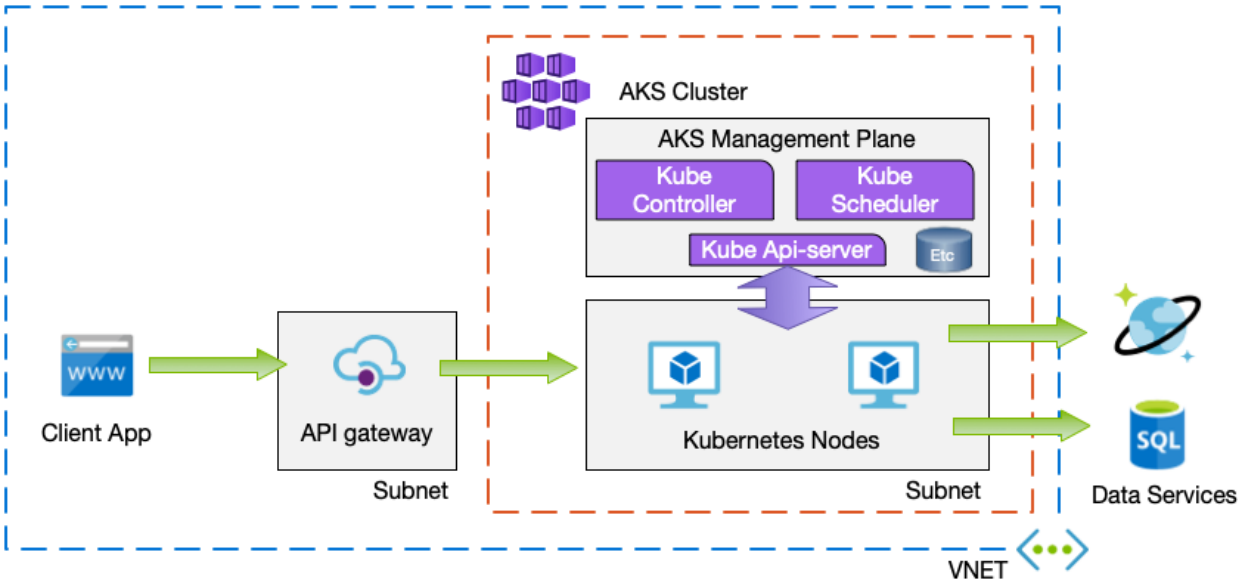
Chapter 7: Designing Compute Solutions

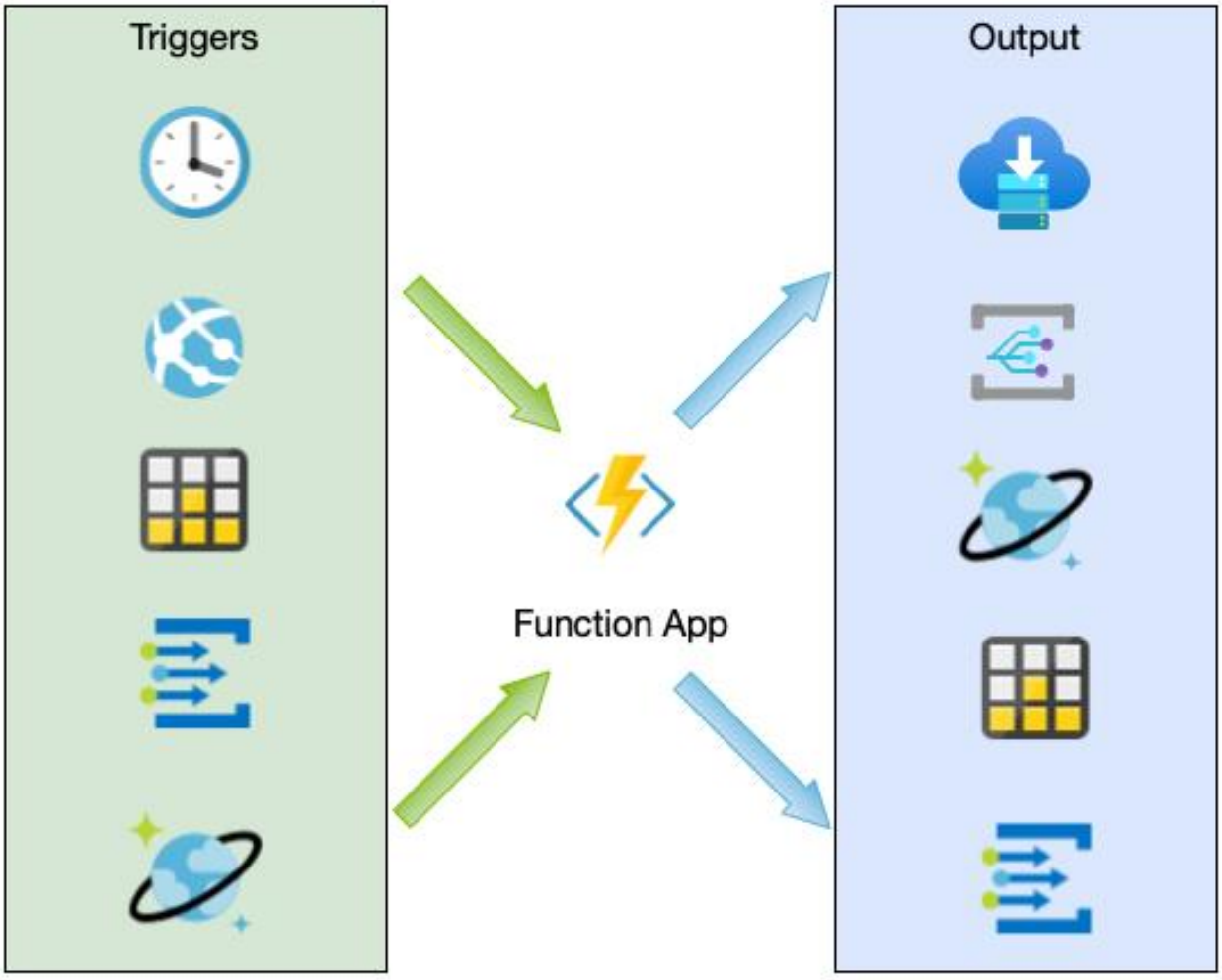


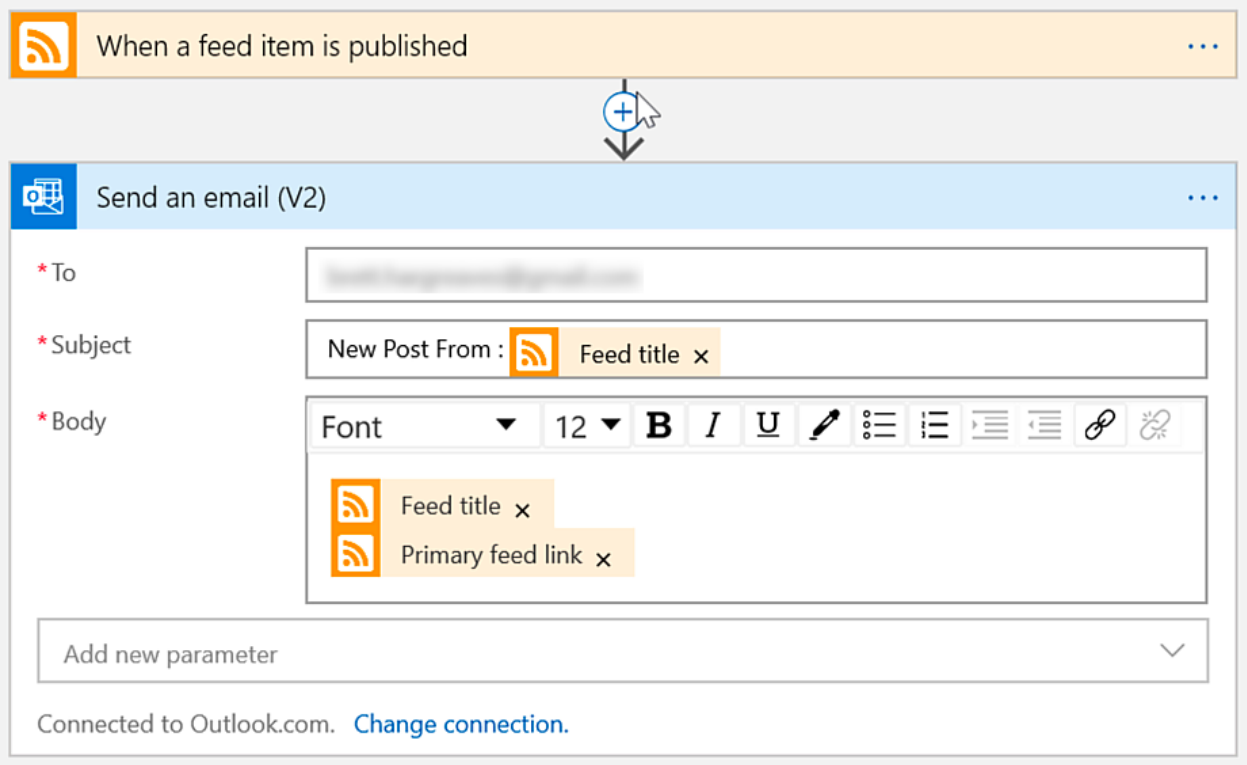

Download Output Files
Azure Storage
Upload Input Files
Download Inputs
Upload Outputs
Azure Batch Service
Jobs
Task
Task
Task
Pool, job & task management
Node Pool
Node
Node
Node
Application or Service
Application Packages
ZIP
ZIP
ZIP
Task Monitor
www
Portal

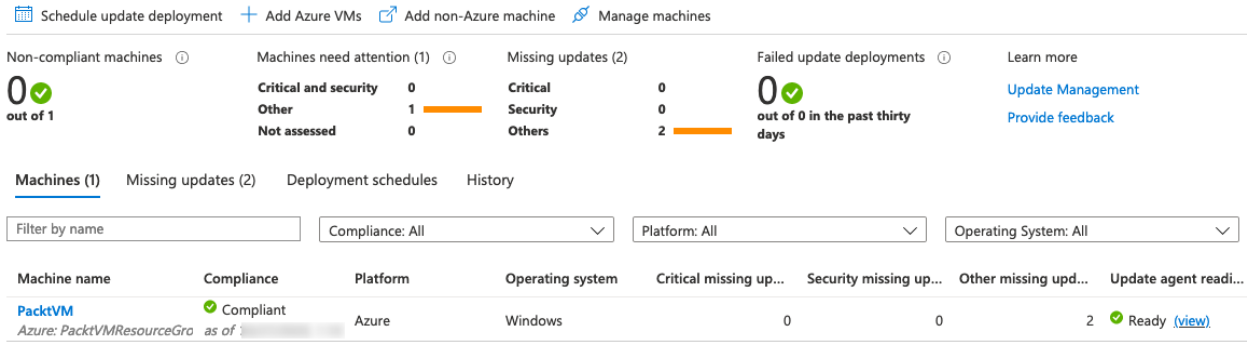

Service Fabric Cluster
Scale set
VMs
Client App
API gateway
Subnet
Subnet
Subnet
Data Services
SQL
VNET


Virtual Machines
Virtual Machine
App A
Guest OS
Virtual Machine
App A
Guest OS
Hypervisor
Infrastructure
Containerization
App A
App B
App C
App D
App E
Docker
Guest OS
Infrastructure


AKS Cluster
AKS Management Plane
Kube Controller
Kube Scheduler
Kube Api-server
Etc
Client App
API gateway
Subnet
Kubernetes Nodes
Subnet
Data Services
VNET


Triggers
Function App
Output


When a feed item is published
Send an email (V2)
*To
*Subject
New Post From :
Feed title
*Body
Font
12
Feed title
Primary feed link
Add new parameter
Connected to Outlook.com.
Change connection.


Schedule update deployment
Add Azure VMs
Add non-Azure machine
Manage machines
Non-compliant machines
0
out of 1
Machines need attention (1)
Critical and security 0
Other 1
Not assessed 0
Missing updates (2)
Critical 0
Security 0
Others 2
Failed update deployments
0
out of 0 in the past thirty days
Learn more
Update Management
Provide feedback
Machines (1)
Missing updates (2)
Deployment schedules
History
Filter by name
Compliance: All
Platform: All
Operating System: All
Machine name
Compliance
Platform
Operating system
Critical missing up...
Security missing up...
Other missing upd...
Update agent readi...
PacktVM
Azure: PacktVMResourceGro
Compliant
Azure
Windows
0
0
2
Ready (view)

Configuration (used when enabling new VMs)

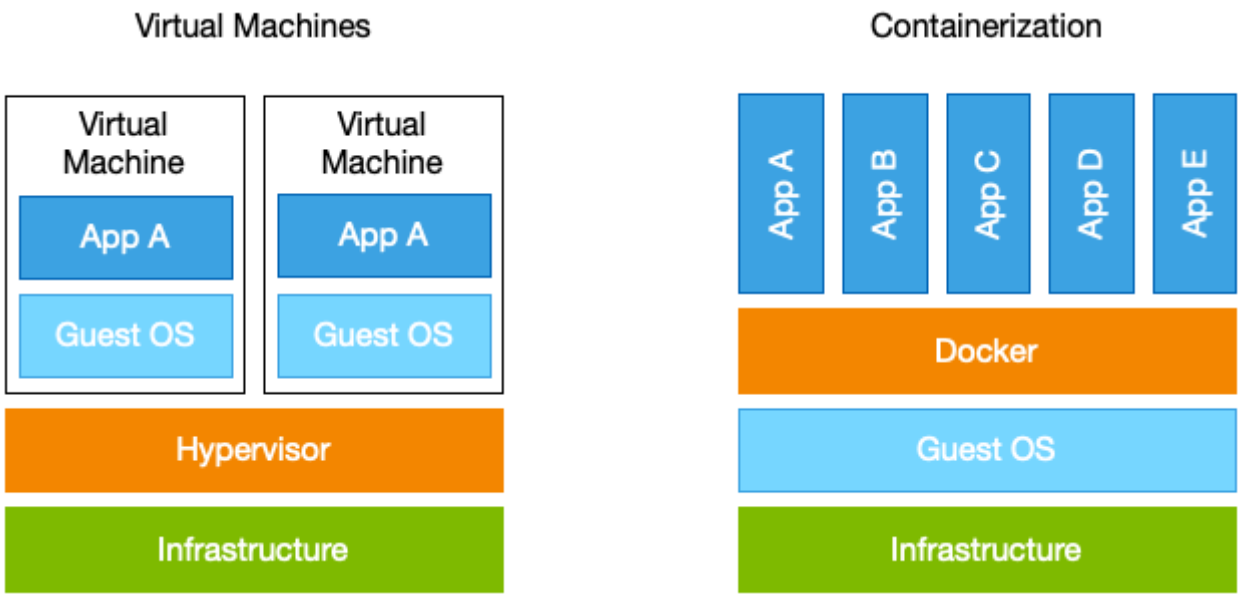
AUTO: Auto-configure Log Analytics workspace and Automation account based on VMs subscription and location

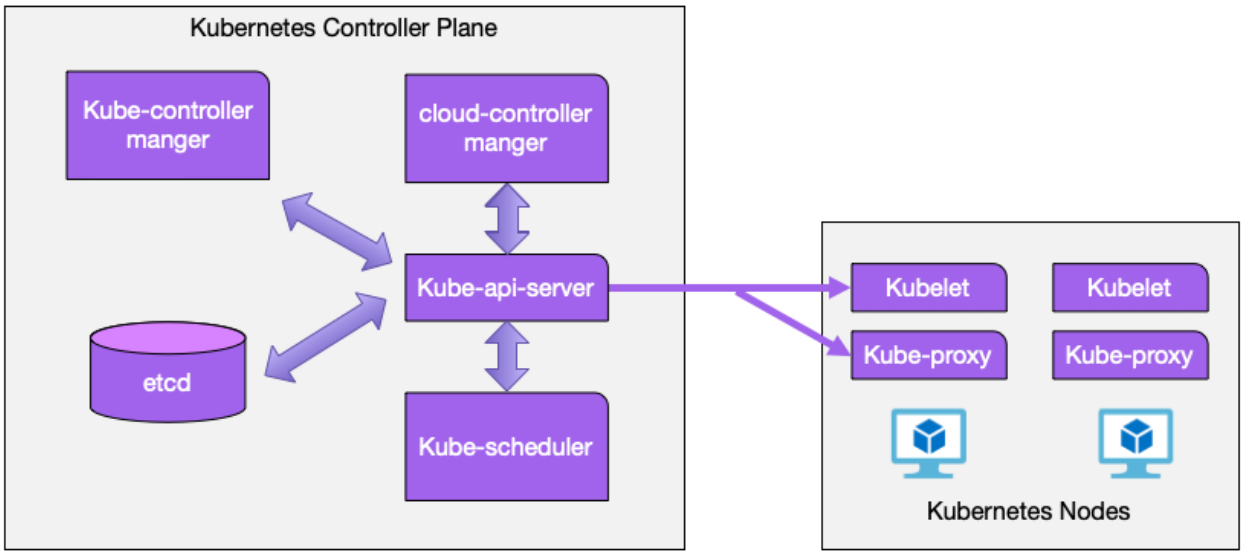
Log Analytics workspace: defaultworkspace-f9483dab-48b4-4a40-9420-8b916e6b33c9-eus
Automation account: Automate-f9483dab-48b4-4a40-9420-8b916e6b33c9-EUS

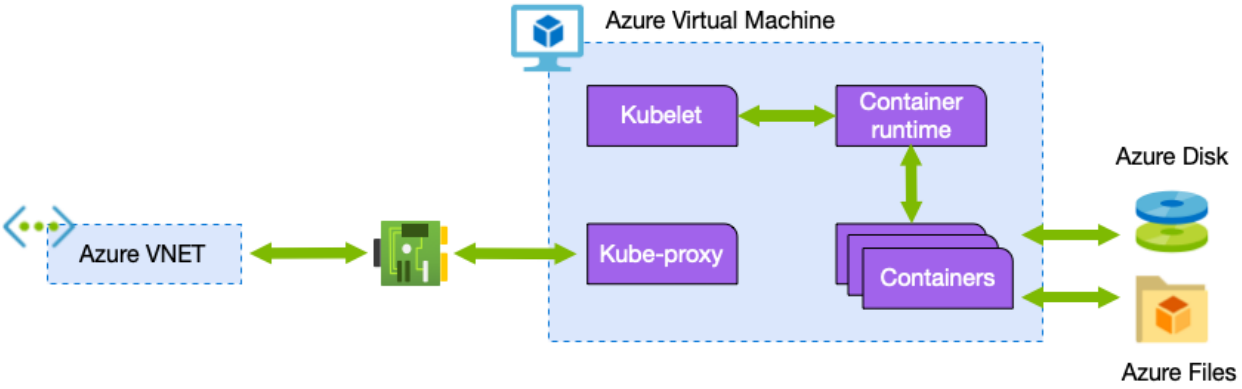
Summary

Ready to enable	Already enabled	Cannot enable
1	1	0

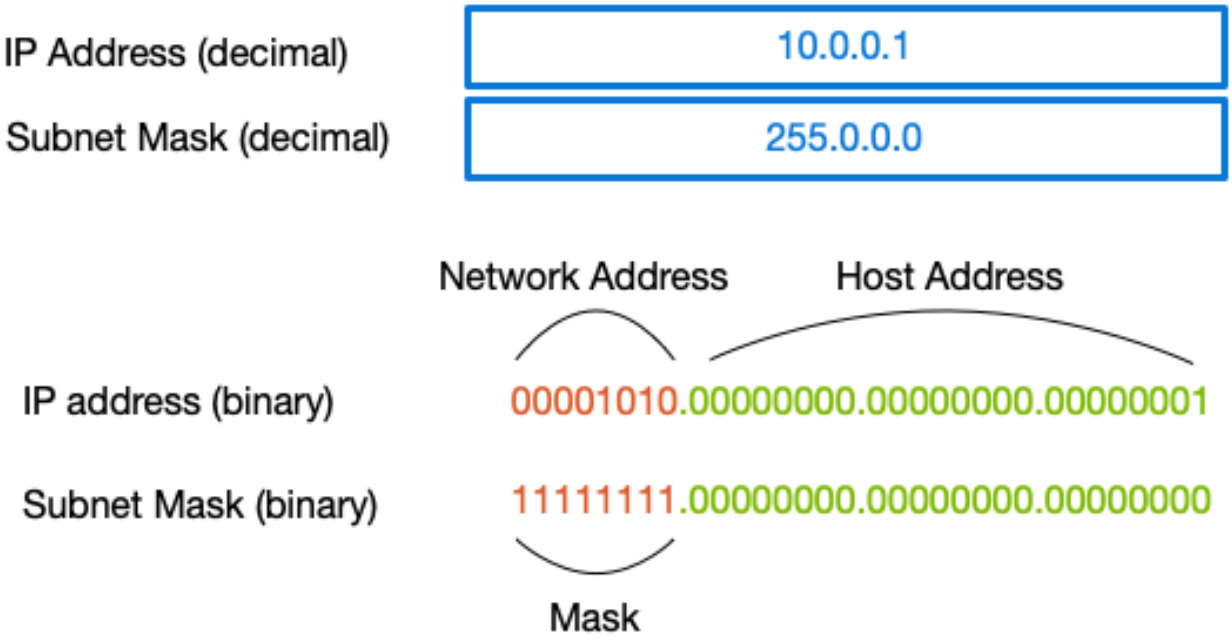
Name	Update Managem...	Details
packtvm	Already enabled	
packtvm2	Ready to enable	

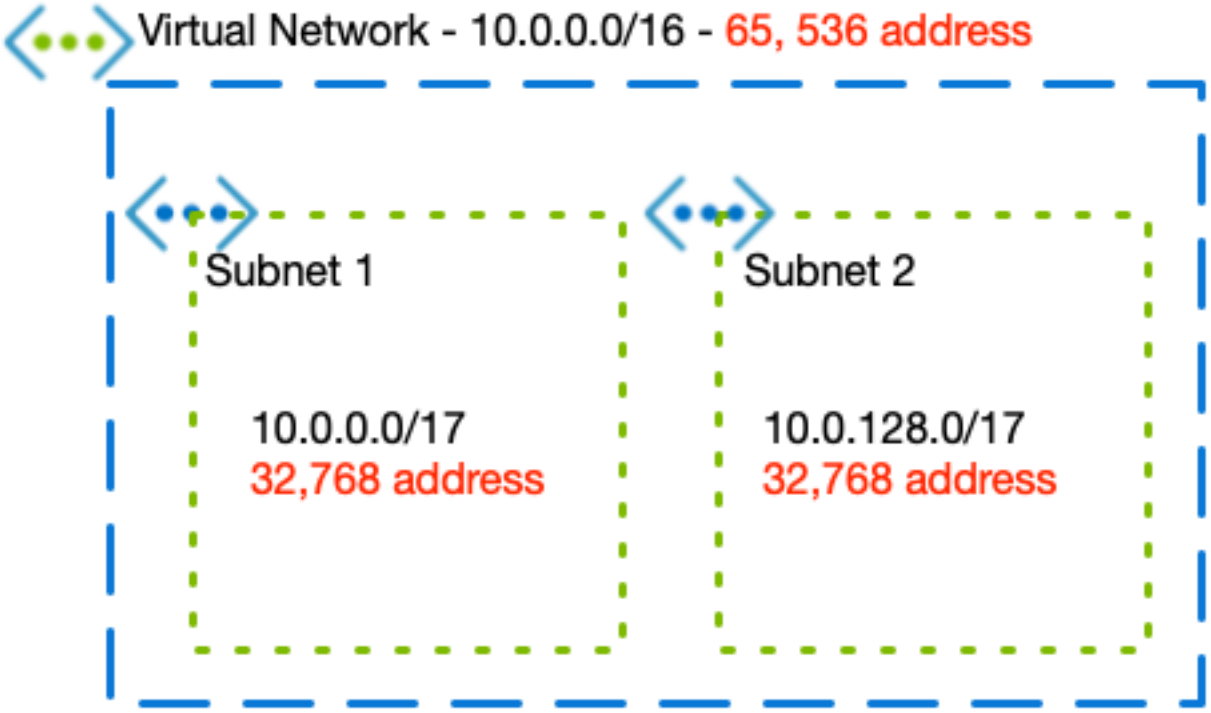


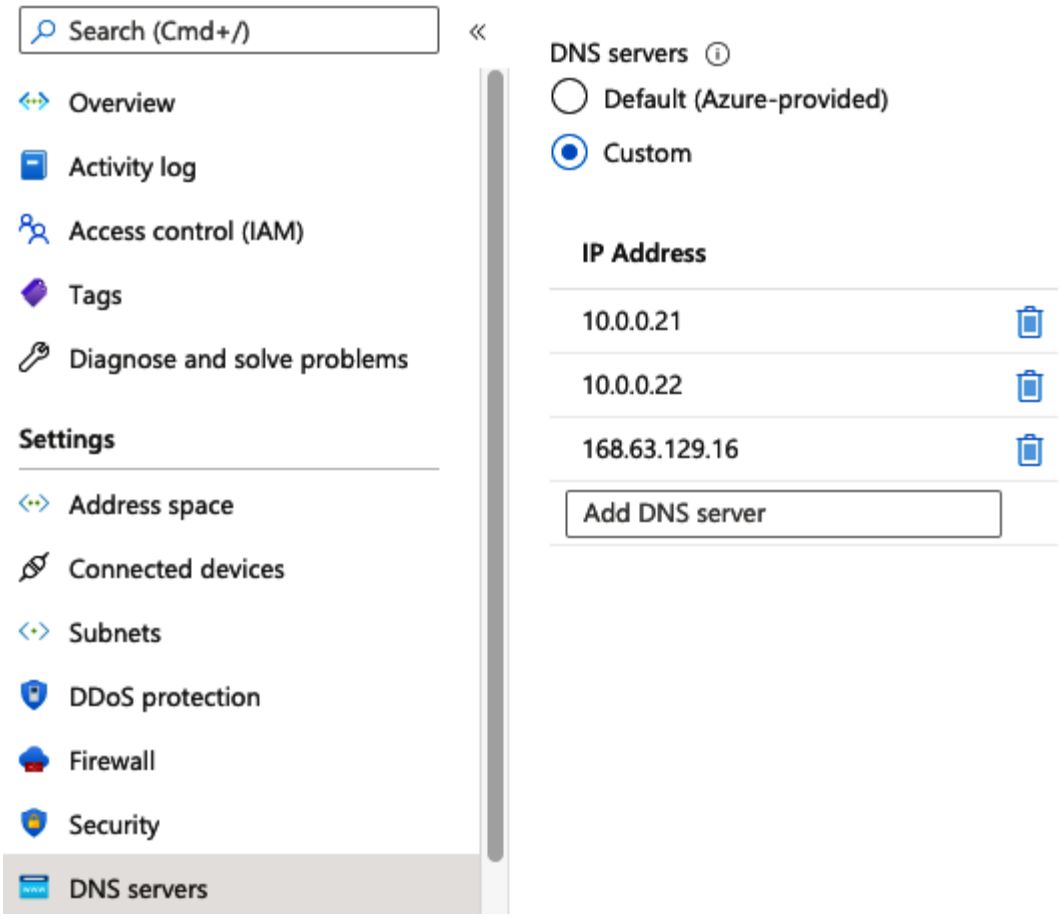

Kubernetes Controller Plane
Kube-controller manger
cloud-controller manger
Kube-api-server
etcd
Kube-scheduler
Kubelet
Kubelet
Kube-proxy
Kube-proxy
Kubernetes Nodes

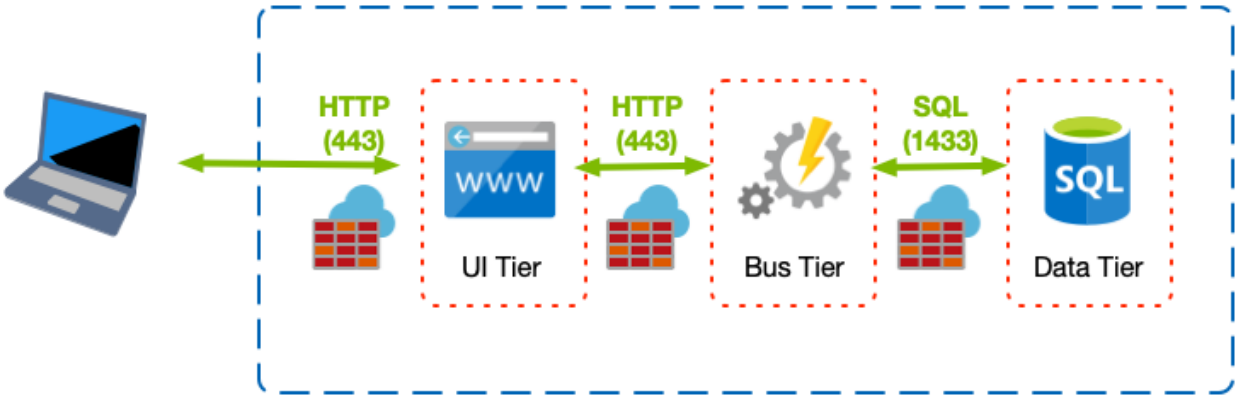

Azure Virtual Machine
Kubelet
Container runtime
Azure Disk
Azure VNET
Kube-proxy
Containers
Azure Files

Chapter 8: Network Connectivity and Security






Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
DNS servers
DNS servers
Default (Azure-provided)
Custom
IP Address
10.0.0.21
10.0.0.22
168.63.129.16
Add DNS server


HTTP
(443)
HTTP
(443)
SQL
(1433)
WWW
SQL
UI Tier
Bus Tier
Data Tier

Resource group (change) : PacktLBResourceGroup

Location : East US

Subscription (change) : PacktPub

Subscription ID : [redacted]

Tags (change) : Click here to add tags

Custom security rules : 2 inbound, 0 outbound

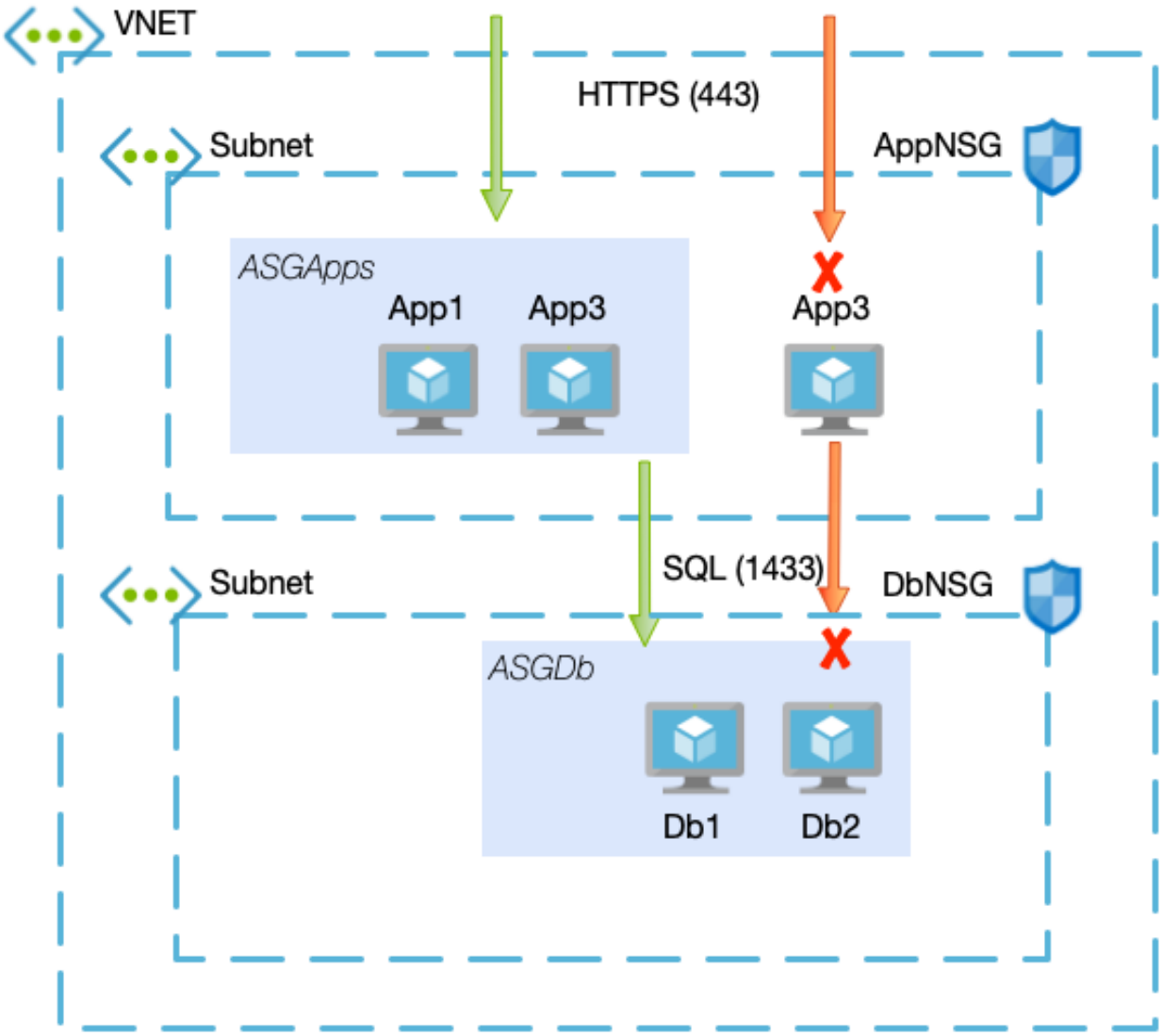
Associated with : 0 subnets, 1 network interfaces

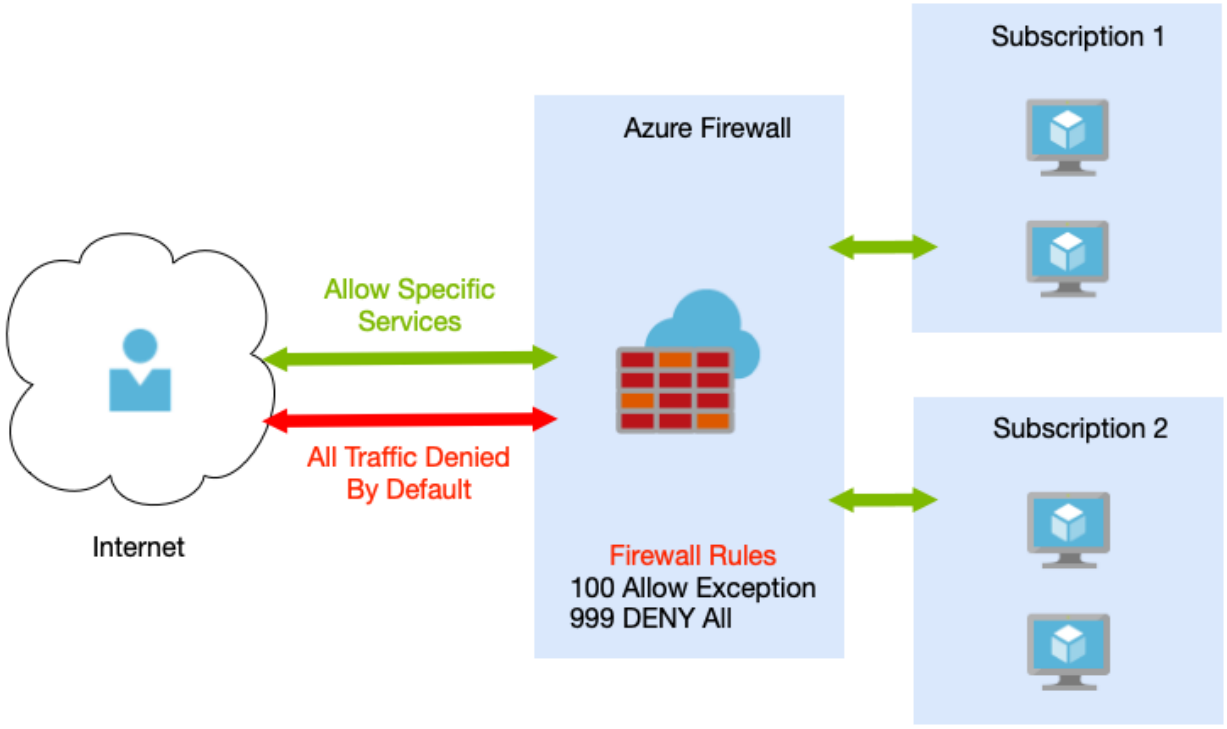
Inbound security rules

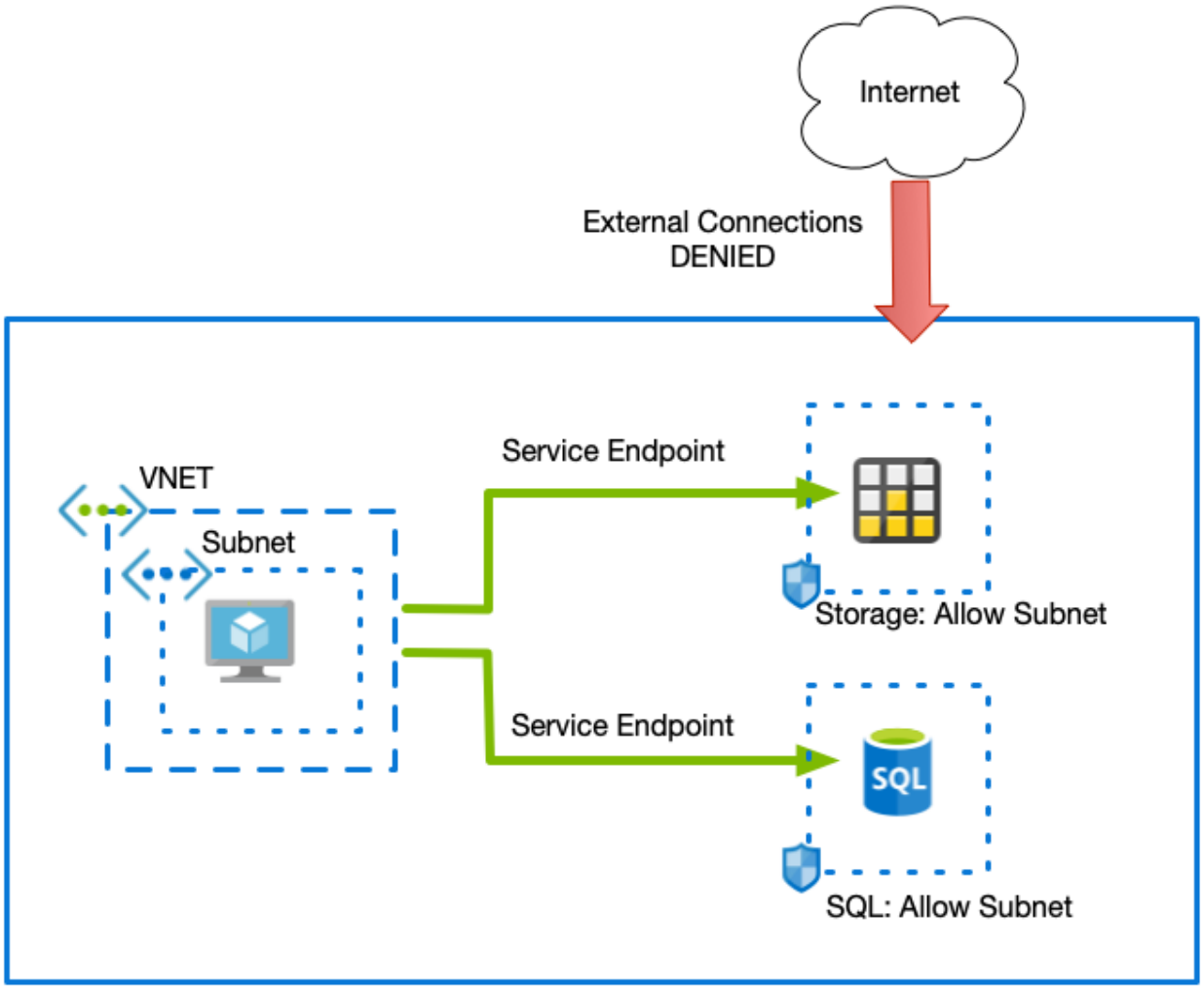
Priority	Name	Port	Protocol	Source	Destination	Action
300	⚠ RDP	3389	TCP	Any	Any	Allow •••
310	HTTP	80	TCP	Any	Any	Allow •••
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow •••
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow •••
65500	DenyAllInBound	Any	Any	Any	Any	Deny •••

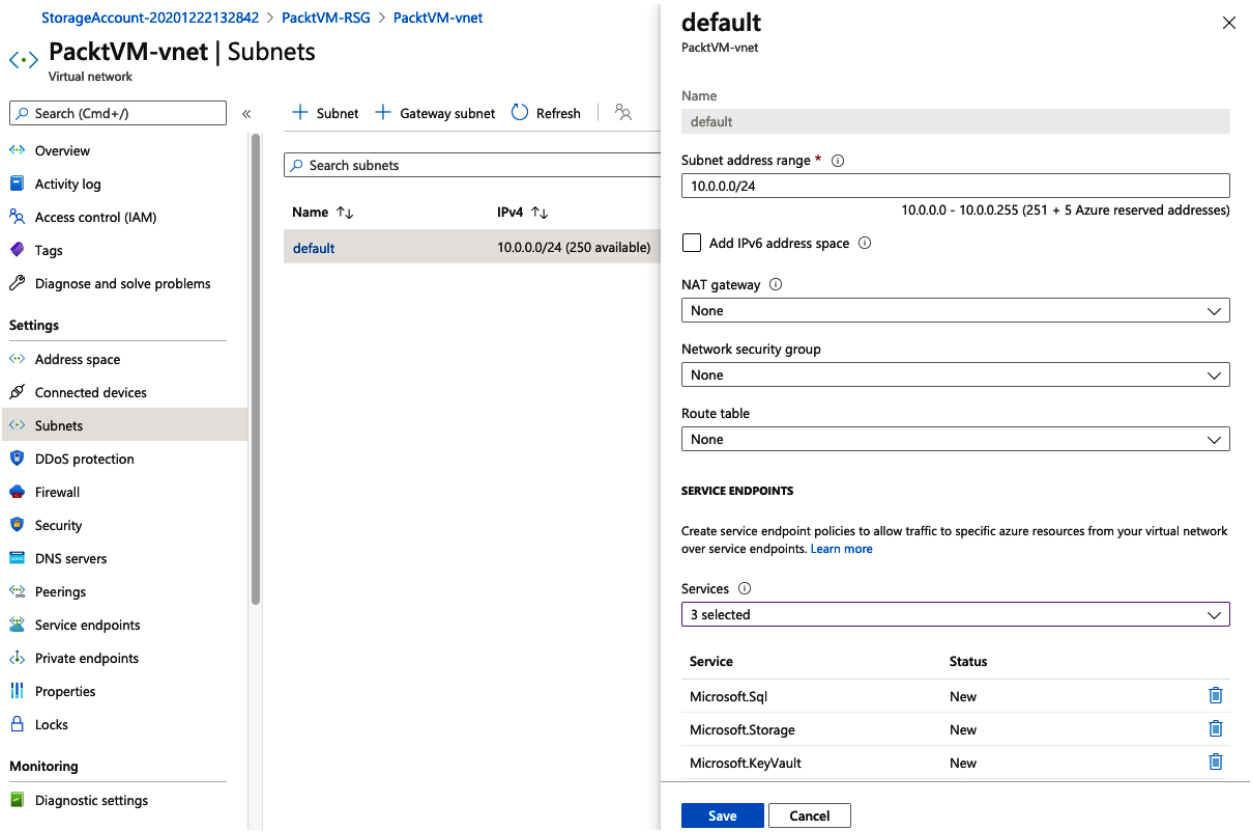
Outbound security rules

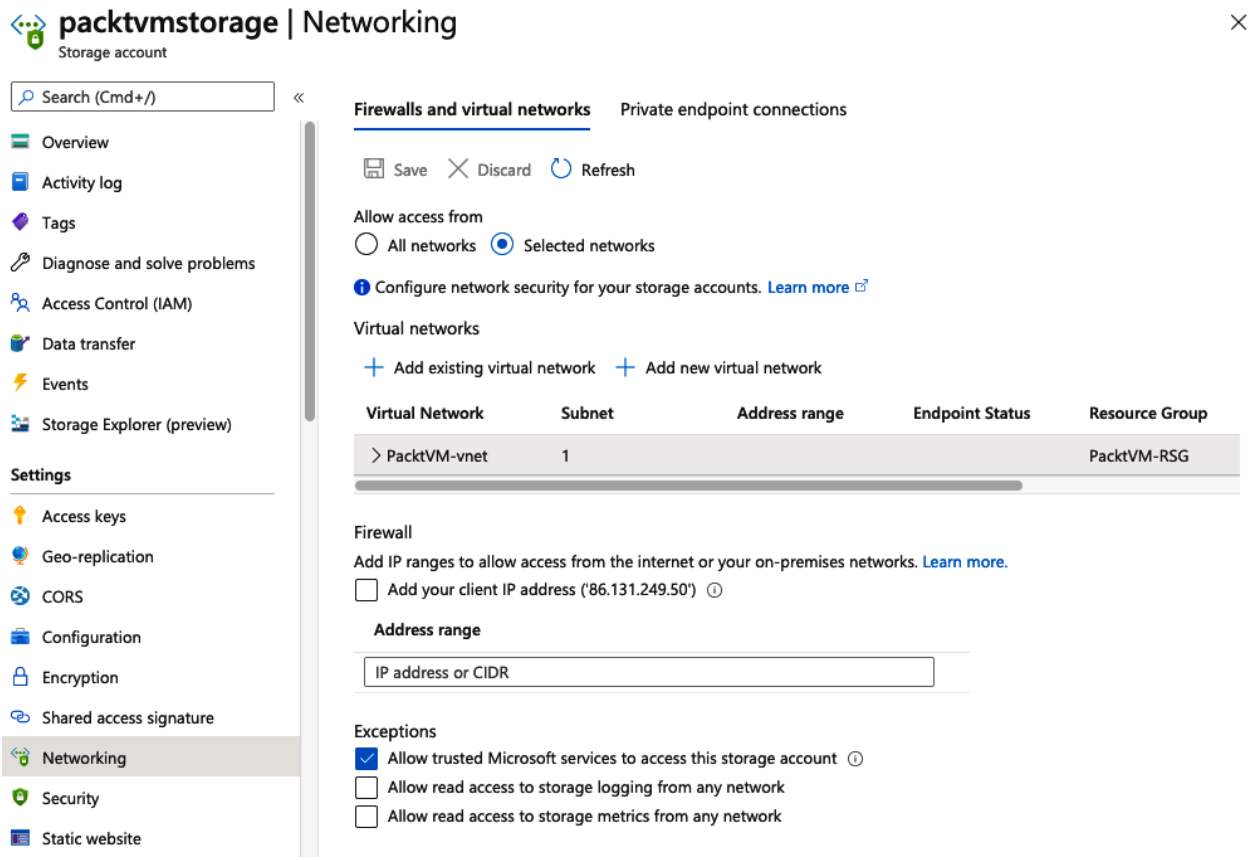
Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow •••
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow •••
65500	DenyAllOutBound	Any	Any	Any	Any	Deny •••

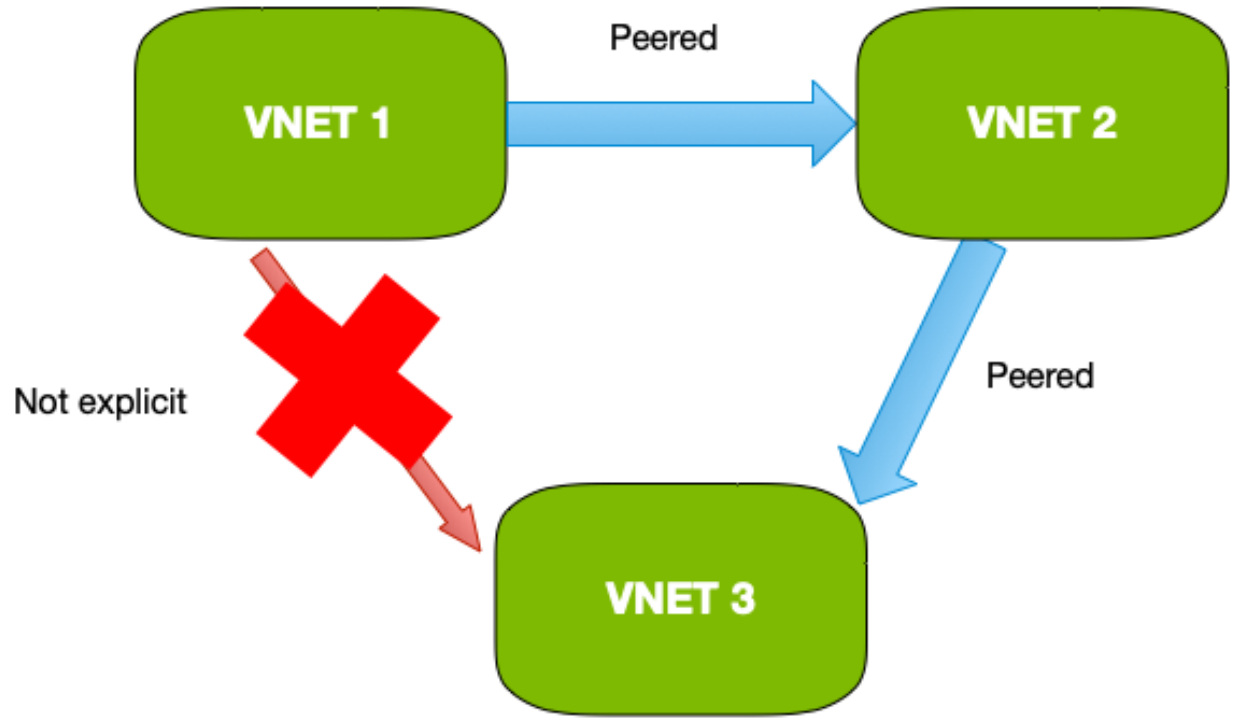

VNET
HTTPS (443)
Subnet
AppNSG
ASGApps
App1
App3
App3
SQL (1433)
Subnet
DbNSG
ASGDb
Db1
Db2

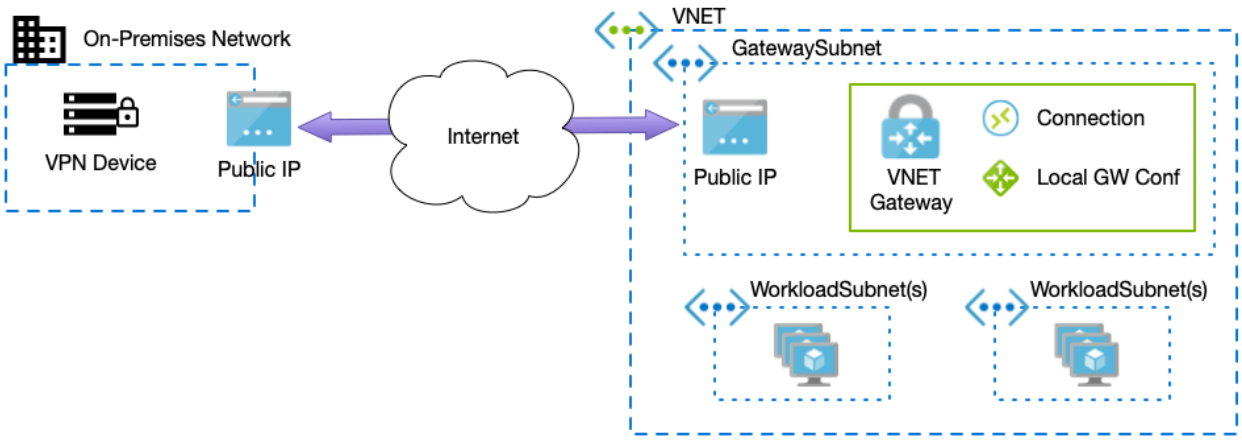

Subscription 1
Azure Firewall
Allow Specific
Services
All Traffic Denied
By Default
Internet
Firewall Rules
100 Allow Exception
999 DENY All
Subscription 2

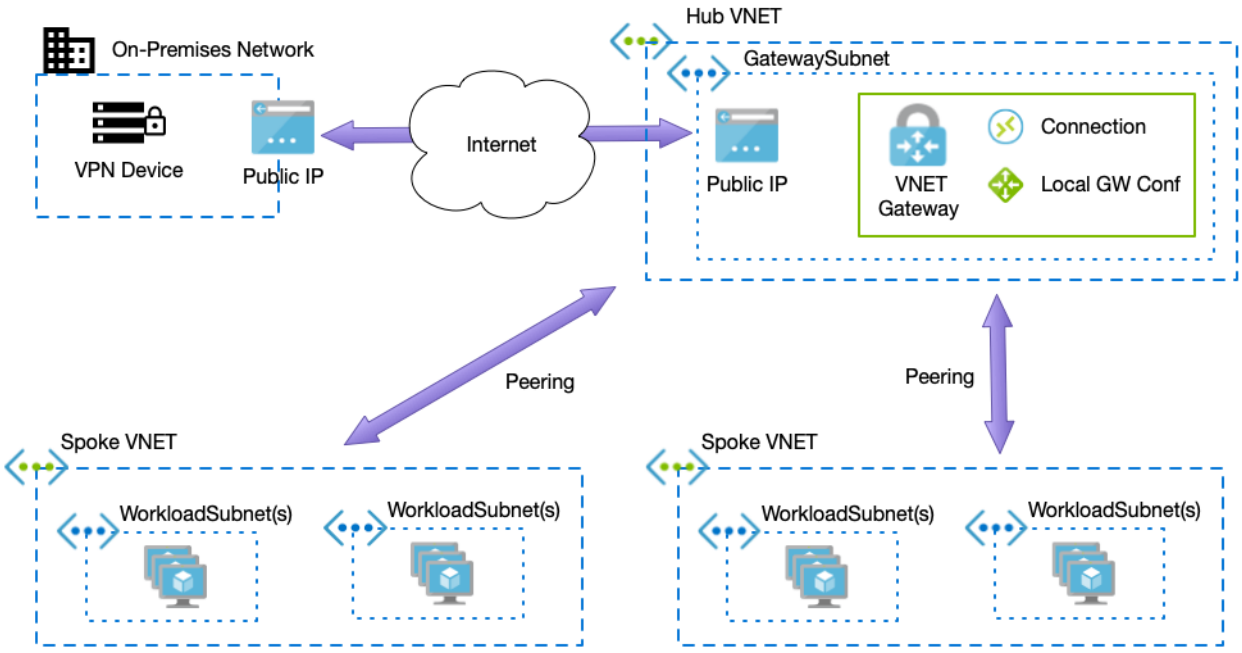

Internet
External Connections
DENIED
VNET
Subnet
Service Endpoint
Storage: Allow Subnet
Service Endpoint
SQL
SQL: Allow Subnet


StorageAccount-20201222132842 > PacktVM-RSG > PacktVM-vnet
PacktVM-vnet | Subnets
Virtual network
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
DNS servers
Peerings
Service endpoints
Private endpoints
Properties
Locks
Monitoring
Diagnostic settings
Subnet
Gateway subnet
Refresh
Search subnets
Name
IPv4
default
10.0.0.0/24 (250 available)
default
PacktVM-vnet
Name
default
Subnet address range *
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)
Add IPv6 address space
NAT gateway
None
Network security group
None
Route table
None
SERVICE ENDPOINTS
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more
Services
3 selected
Service
Status
Microsoft.Sql
New
Microsoft.Storage
New
Microsoft.KeyVault
New
Save
Cancel


packtvmstorage | Networking
Storage account
Search (Cmd+/)
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data transfer
Events
Storage Explorer (preview)
Settings
Access keys
Geo-replication
CORS
Configuration
Encryption
Shared access signature
Networking
Security
Static website
Firewalls and virtual networks
Private endpoint connections
Save
Discard
Refresh
Allow access from
All networks
Selected networks
Configure network security for your storage accounts. Learn more
Virtual networks
Add existing virtual network
Add new virtual network
Virtual Network
Subnet
Address range
Endpoint Status
Resource Group
PacktVM-vnet
1
PacktVM-RSG
Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.
Add your client IP address ('86.131.249.50')
Address range
IP address or CIDR
Exceptions
Allow trusted Microsoft services to access this storage account
Allow read access to storage logging from any network
Allow read access to storage metrics from any network


VNET 1
Peered
VNET 2
Not explicit
Peered
VNET 3


On-Premises Network
VPN Device
Public IP
Internet
VNET
GatewaySubnet
Public IP
VNET Gateway
Connection
Local GW Conf
WorkloadSubnet(s)
WorkloadSubnet(s)


On-Premises Network
VPN Device
Public IP
Internet
Hub VNET
GatewaySubnet
Public IP
VNET Gateway
Connection
Local GW Conf
Peering
Peering
Spoke VNET
WorkloadSubnet(s)
WorkloadSubnet(s)
Spoke VNET
WorkloadSubnet(s)
WorkloadSubnet(s)

Traffic to remote virtual network ⓘ

- (●) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- (●) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

Virtual network gateway ⓘ

- ( ) Use this virtual network's gateway
- (●) Use the remote virtual network's gateway
- ( ) None (default)

RouteInternetTxToFirewall

Save | Discard | Delete

Address prefix * ⓘ

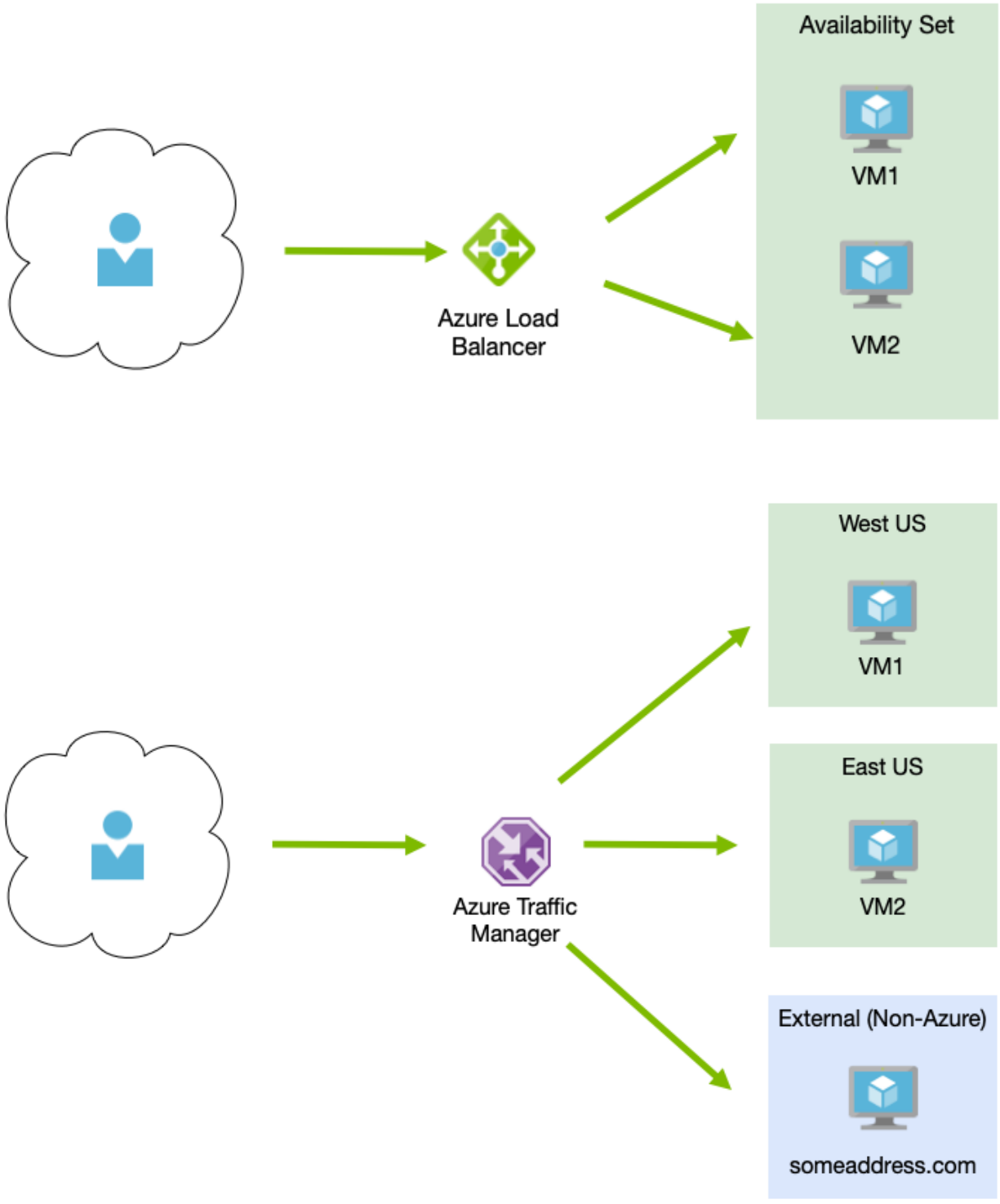
0.0.0.0/0

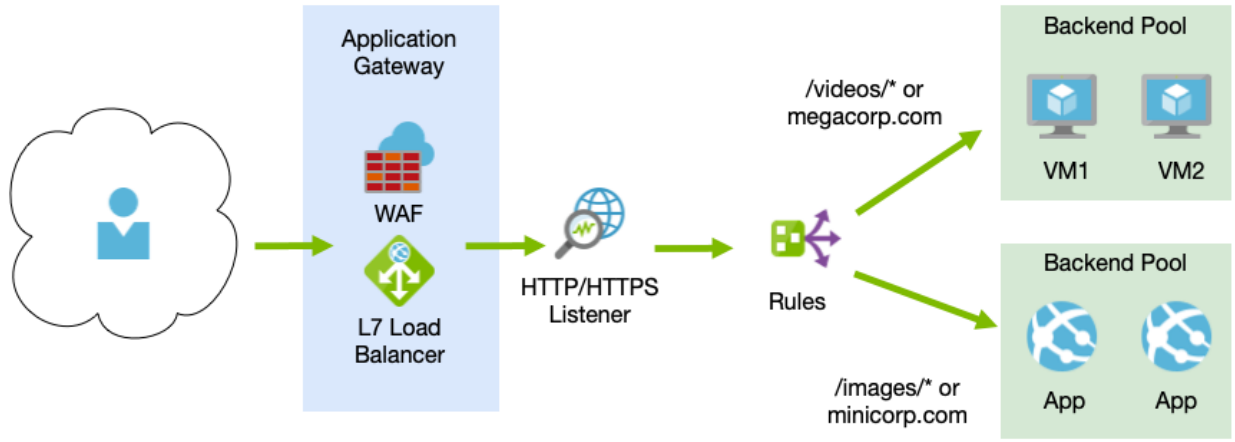
Next hop type ⓘ

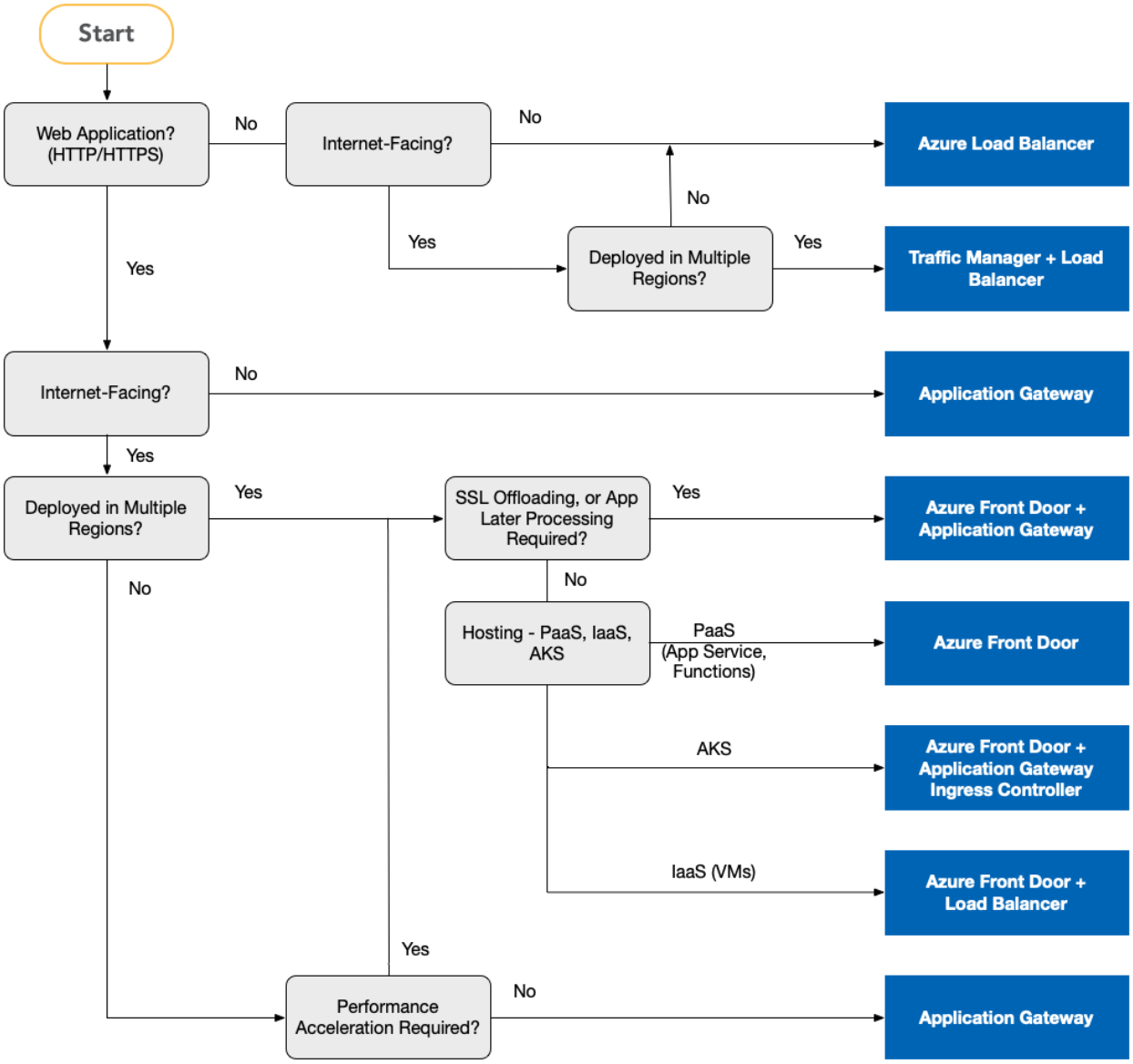
Virtual appliance

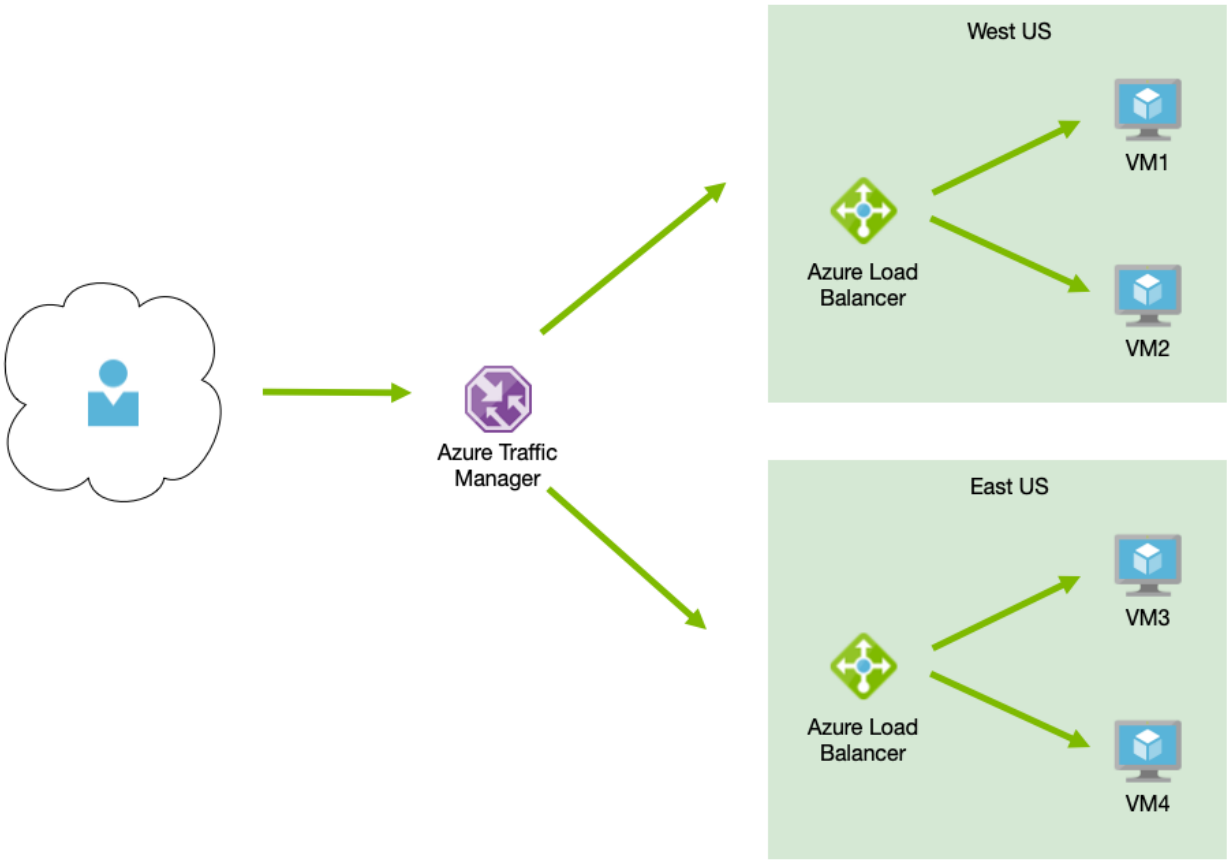
Next hop address * ⓘ

10.0.0.10

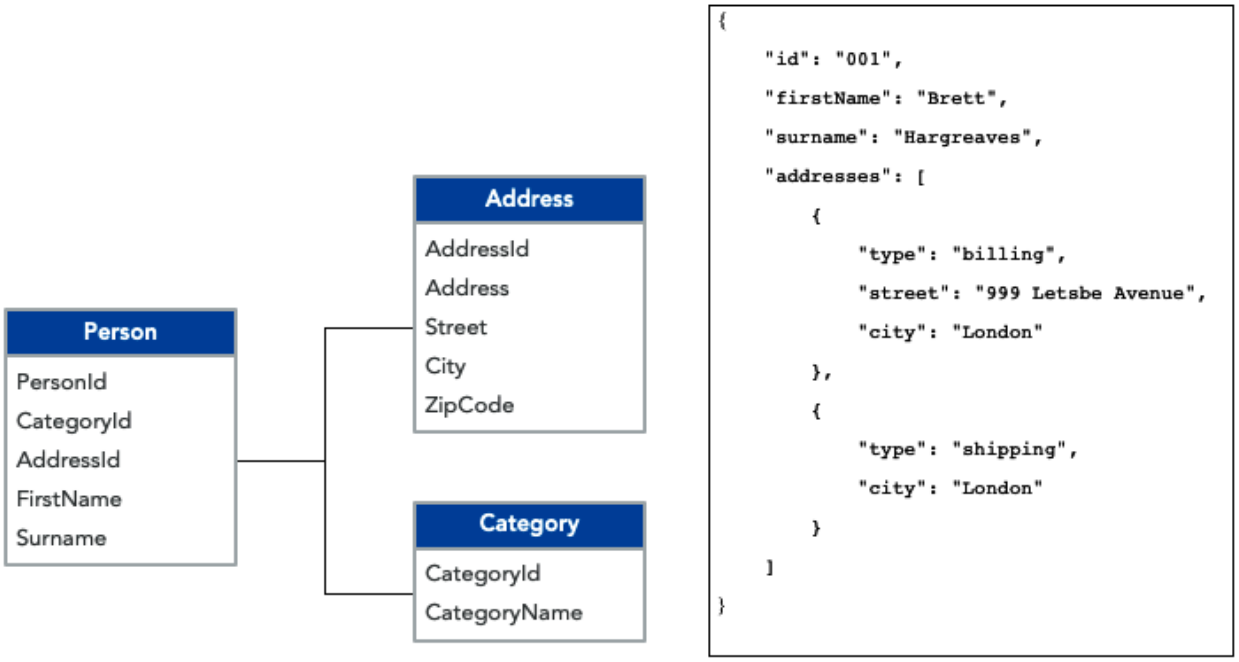

Availability Set
VM1
VM2
Azure Load Balancer
West US
VM1
East US
VM2
Azure Traffic Manager
External (Non-Azure)
someaddress.com


Application Gateway
WAF
L7 Load Balancer
HTTP/HTTPS Listener
Rules
/videos/* or megacorp.com
/images/* or minicorp.com
Backend Pool
VM1
VM2
Backend Pool
App
App


Start
Web Application? (HTTP/HTTPS)
No
Internet-Facing?
No
Azure Load Balancer
Yes
Yes
Deployed in Multiple Regions?
No
Yes
Traffic Manager + Load Balancer
Internet-Facing?
No
Application Gateway
Yes
Deployed in Multiple Regions?
Yes
SSL Offloading, or App Later Processing Required?
Yes
Azure Front Door + Application Gateway
No
Hosting - PaaS, IaaS, AKS
PaaS (App Service, Functions)
Azure Front Door
AKS
Azure Front Door + Application Gateway Ingress Controller
IaaS (VMs)
Azure Front Door + Load Balancer
Yes
Performance Acceleration Required?
No
Application Gateway

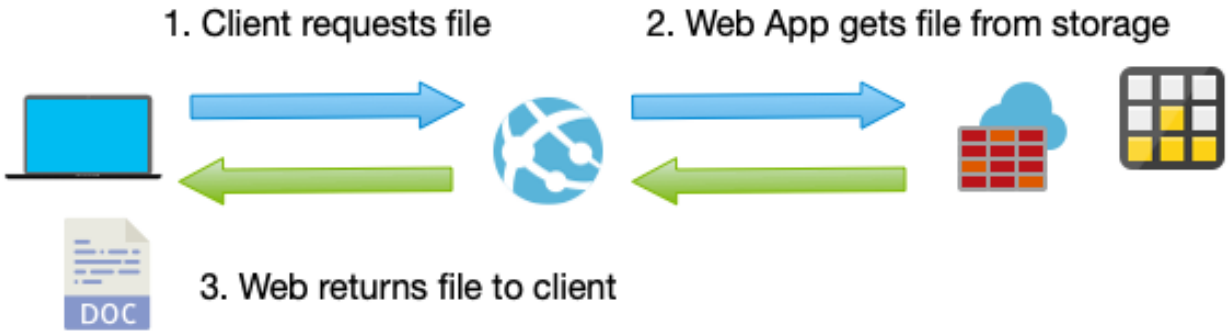

West US
VM1
Azure Load Balancer
VM2
Azure Traffic Manager
East US
VM3
Azure Load Balancer
VM4

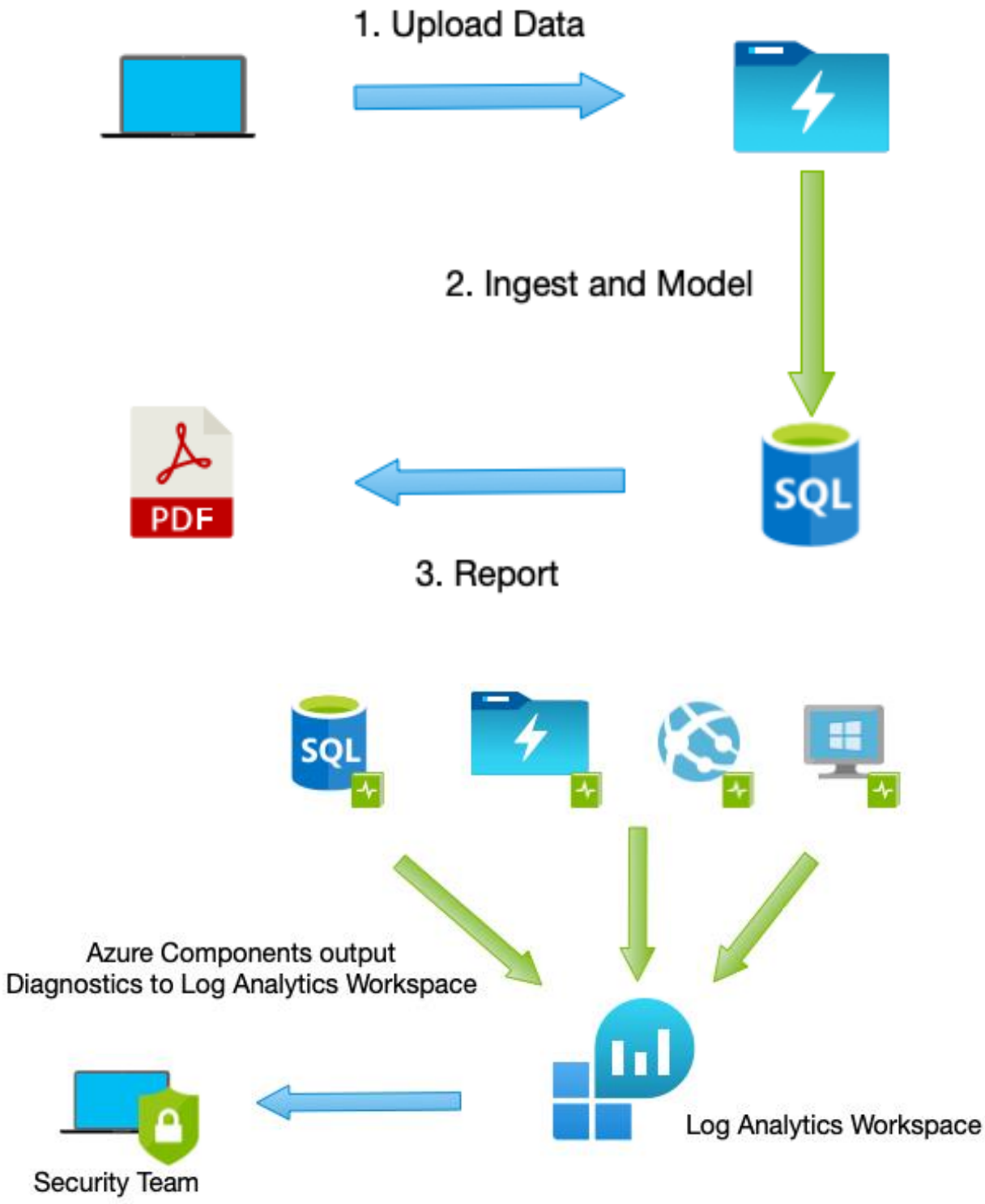
Chapter 9: Exploring Storage Solutions

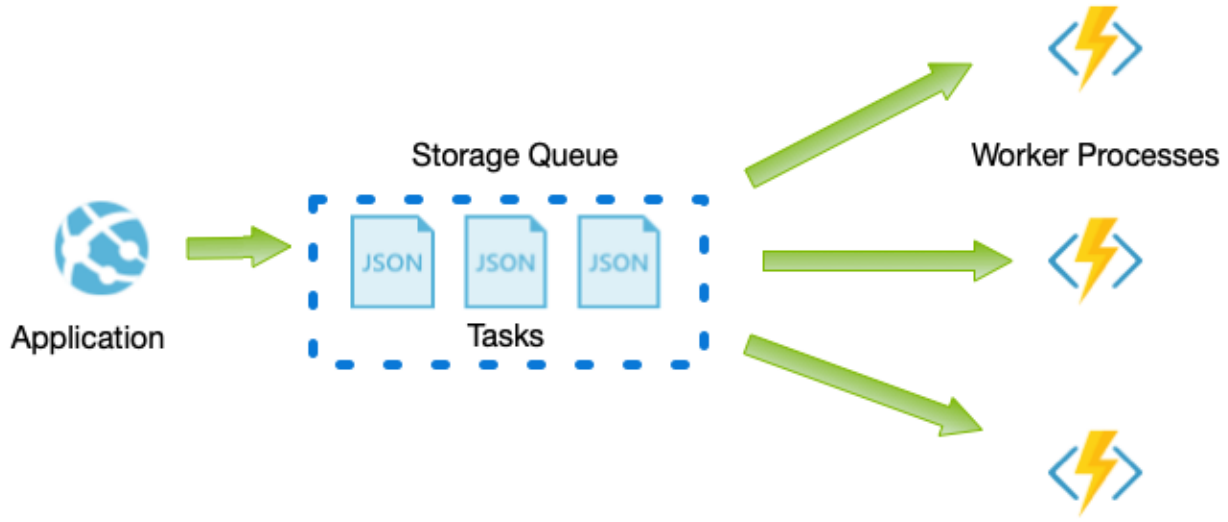


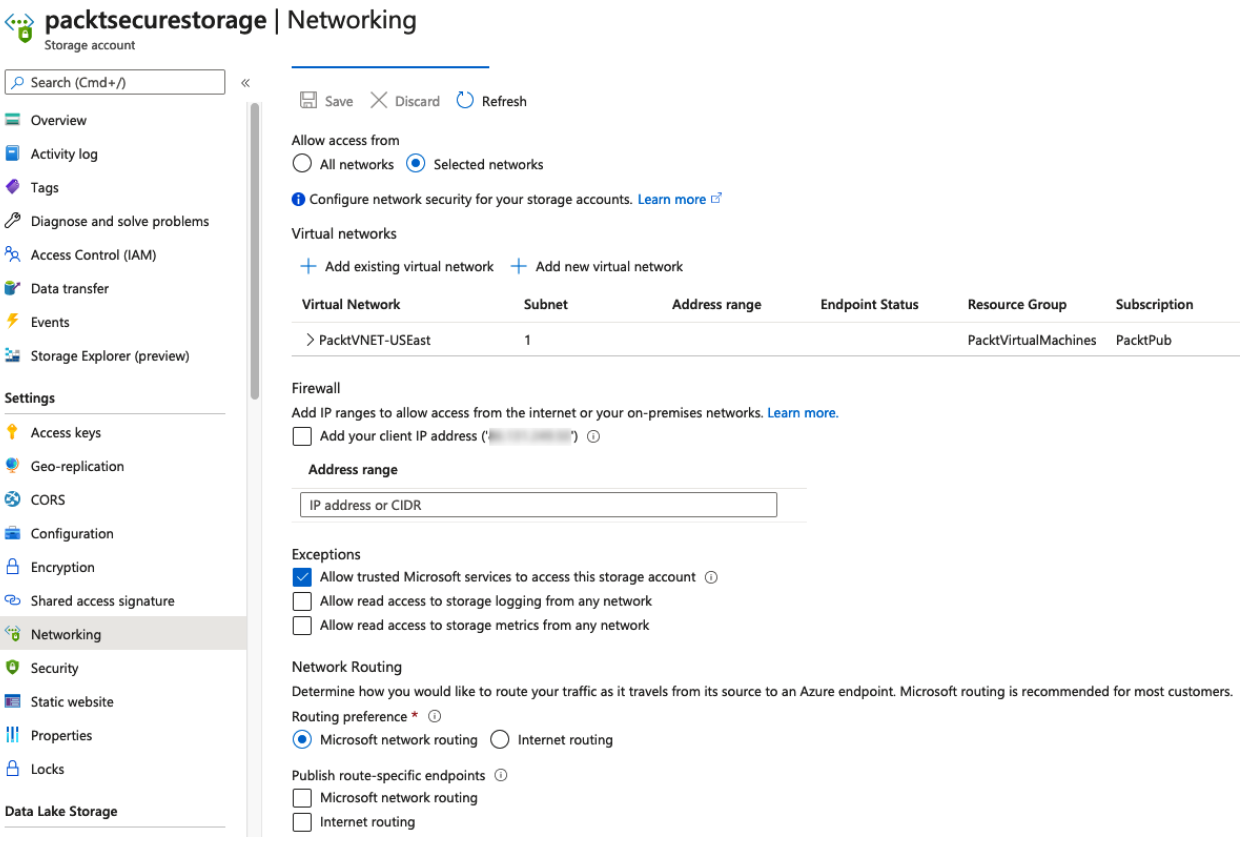
Structured Data

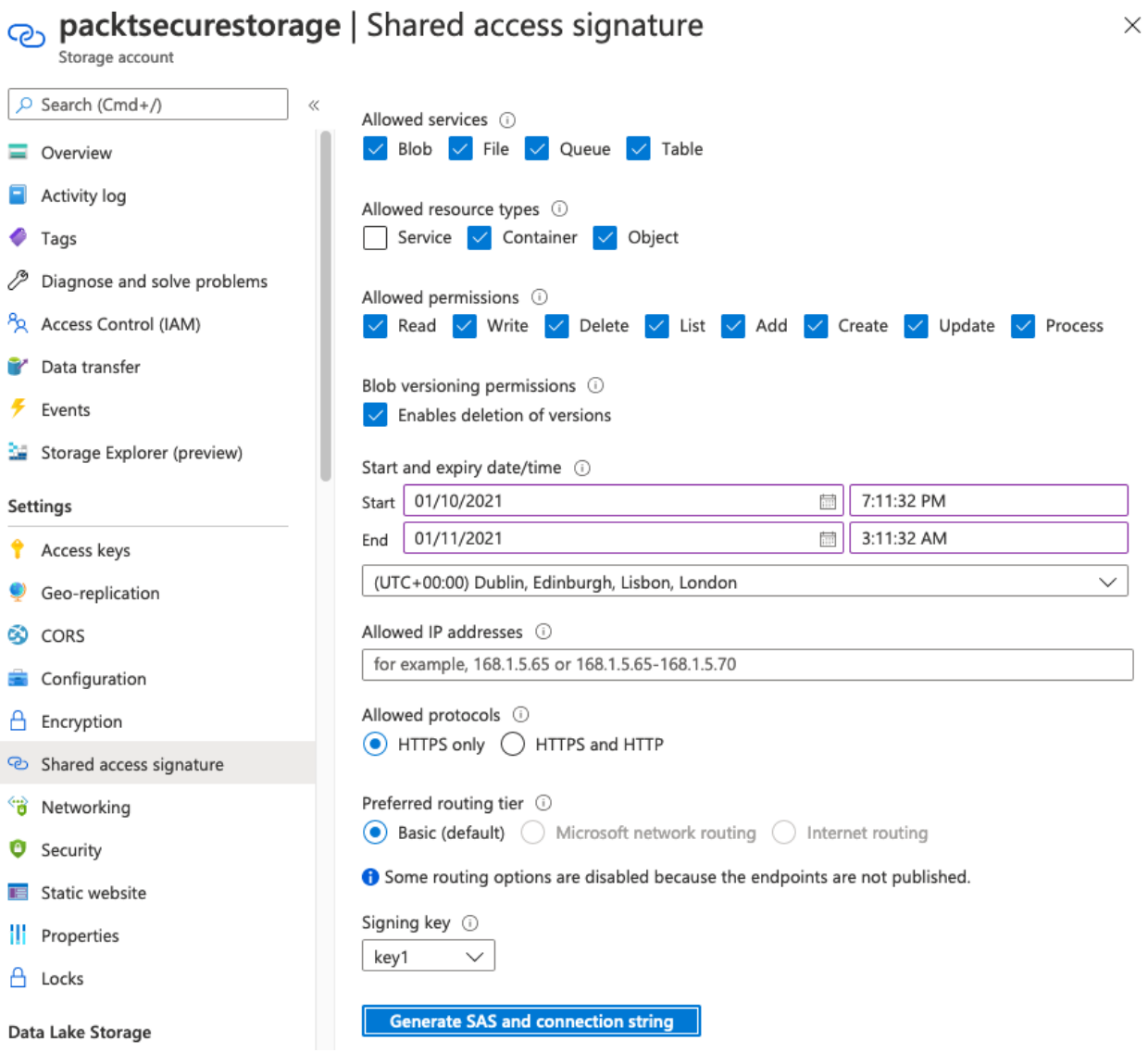
Semi-structured Data

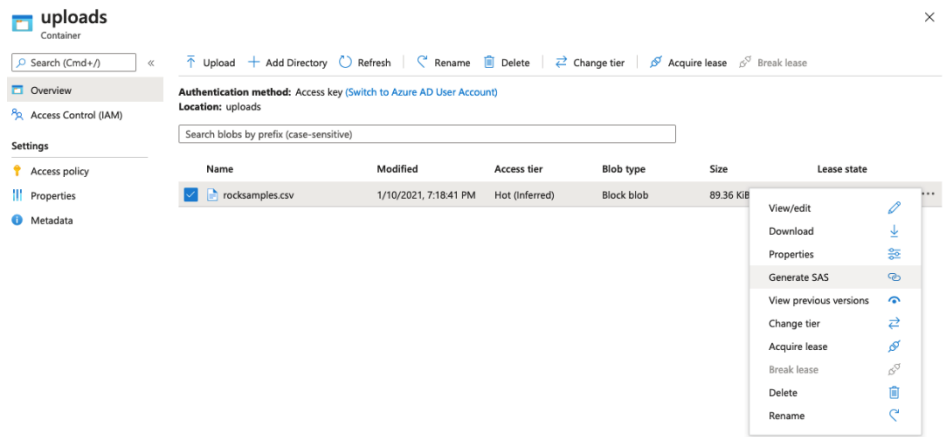


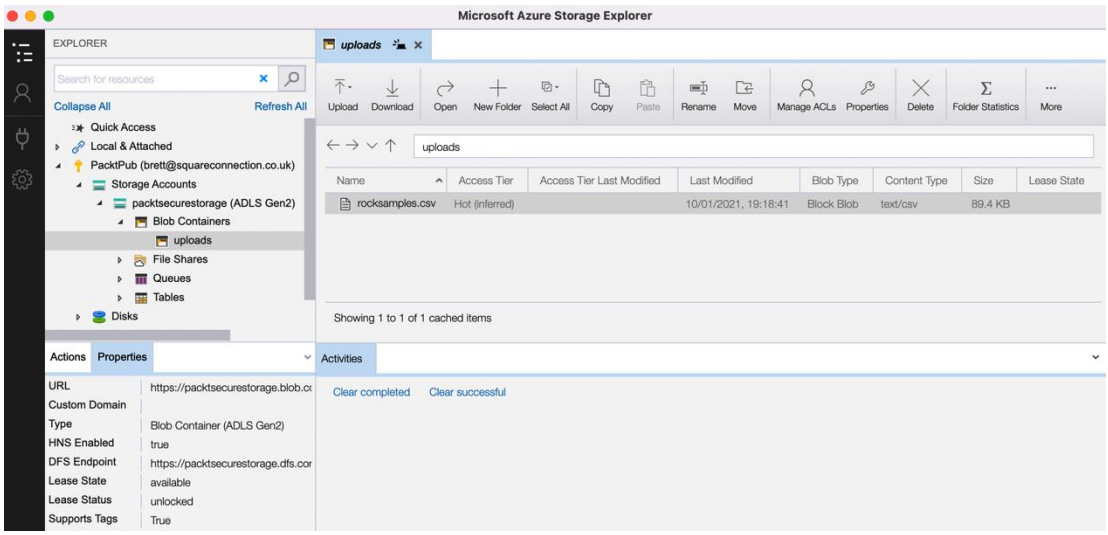

1. Upload Data
2. Ingest and Model
3. Report
PDF
SQL
SQL
Azure Components output
Diagnostics to Log Analytics Workspace
Log Analytics Workspace
Security Team


Storage Queue
Worker Processes
JSON
JSON
JSON
Application
Tasks

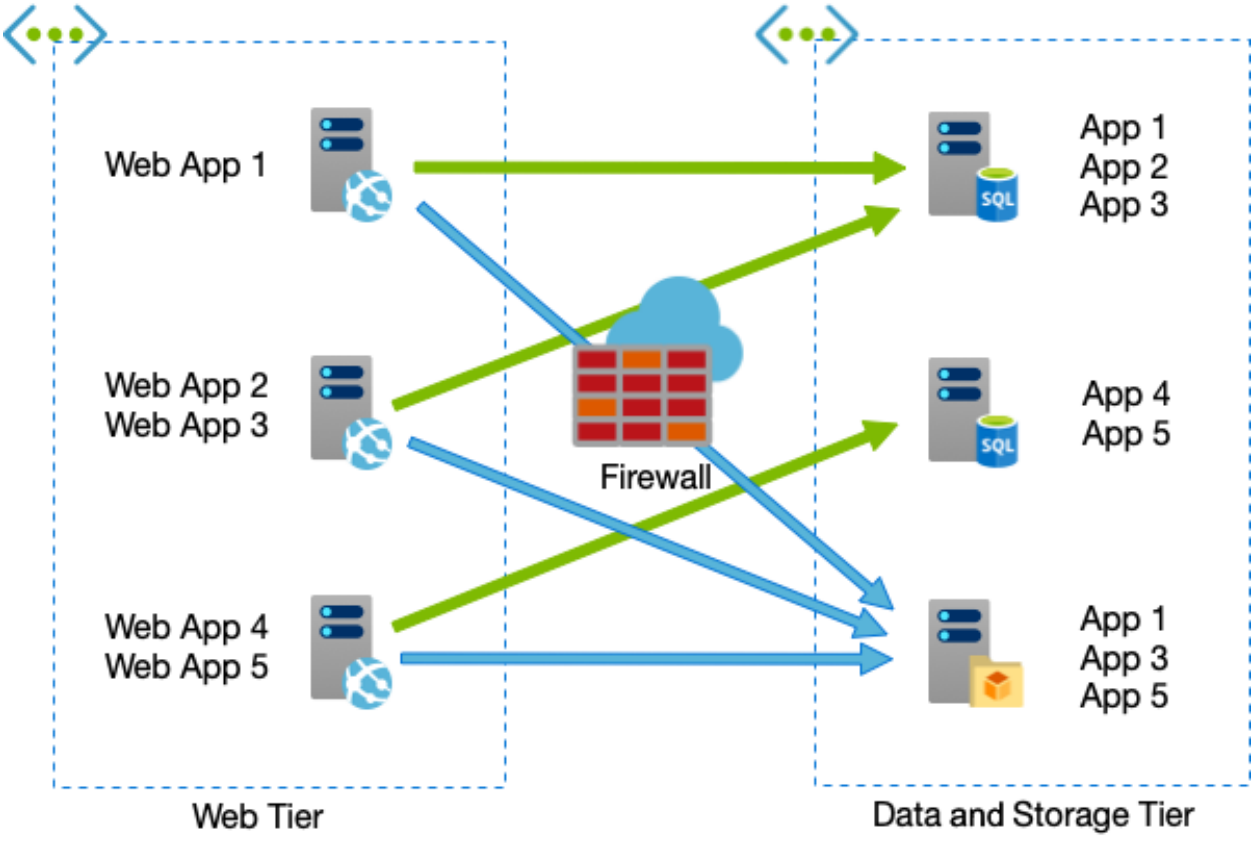

packtsecurestorage | Networking
Storage account
Search (Cmd+/)
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data transfer
Events
Storage Explorer (preview)
Settings
Access keys
Geo-replication
CORS
Configuration
Encryption
Shared access signature
Networking
Security
Static website
Properties
Locks
Data Lake Storage
Save
Discard
Refresh
Allow access from
All networks
Selected networks
Configure network security for your storage accounts. Learn more
Virtual networks
Add existing virtual network
Add new virtual network
Virtual Network
Subnet
Address range
Endpoint Status
Resource Group
Subscription
PacktVNET-USEast
1
PacktVirtualMachines
PacktPub
Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.
Add your client IP address
Address range
IP address or CIDR
Exceptions
Allow trusted Microsoft services to access this storage account
Allow read access to storage logging from any network
Allow read access to storage metrics from any network
Network Routing
Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.
Routing preference *
Microsoft network routing
Internet routing
Publish route-specific endpoints
Microsoft network routing
Internet routing


packtsecurestorage | Shared access signature
Storage account
Search (Cmd+/)
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data transfer
Events
Storage Explorer (preview)
Settings
Access keys
Geo-replication
CORS
Configuration
Encryption
Shared access signature
Networking
Security
Static website
Properties
Locks
Data Lake Storage
Allowed services
Blob File Queue Table
Allowed resource types
Service Container Object
Allowed permissions
Read Write Delete List Add Create Update Process
Blob versioning permissions
Enables deletion of versions
Start and expiry date/time
Start 01/10/2021 7:11:32 PM
End 01/11/2021 3:11:32 AM
(UTC+00:00) Dublin, Edinburgh, Lisbon, London
Allowed IP addresses
for example, 168.1.5.65 or 168.1.5.65-168.1.5.70
Allowed protocols
HTTPS only HTTPS and HTTP
Preferred routing tier
Basic (default) Microsoft network routing Internet routing
Some routing options are disabled because the endpoints are not published.
Signing key
key1
Generate SAS and connection string


uploads
Container
Search (Cmd+/)
Overview
Access Control (IAM)
Settings
Access policy
Properties
Metadata
Upload Add Directory Refresh Rename Delete Change tier Acquire lease Break lease
Authentication method: Access key (Switch to Azure AD User Account)
Location: uploads
Search blobs by prefix (case-sensitive)
Name Modified Access tier Blob type Size Lease state
rocksamples.csv 1/10/2021, 7:18:41 PM Hot (Inferred) Block blob 89.36 KiB
View/edit
Download
Properties
Generate SAS
View previous versions
Change tier
Acquire lease
Break lease
Delete
Rename


Microsoft Azure Storage Explorer
EXPLORER
Search for resources
Collapse All
Refresh All
Quick Access
Local & Attached
PacktPub (brett@squareconnection.co.uk)
Storage Accounts
packtsecurestorage (ADLS Gen2)
Blob Containers
uploads
File Shares
Queues
Tables
Disks
uploads
Upload
Download
Open
New Folder
Select All
Copy
Paste
Rename
Move
Manage ACLs
Properties
Delete
Folder Statistics
More
uploads
Name
Access Tier
Access Tier Last Modified
Last Modified
Blob Type
Content Type
Size
Lease State
rocksamples.csv
Hot (inferred)
10/01/2021, 19:18:41
Block Blob
text/csv
89.4 KB
Showing 1 to 1 of 1 cached items
Actions
Properties
URL
https://packtsecurestorage.blob.co
Custom Domain
Type
Blob Container (ADLS Gen2)
HNS Enabled
true
DFS Endpoint
https://packtsecurestorage.dfs.cor
Lease State
available
Lease Status
unlocked
Supports Tags
True
Activities
Clear completed
Clear successful

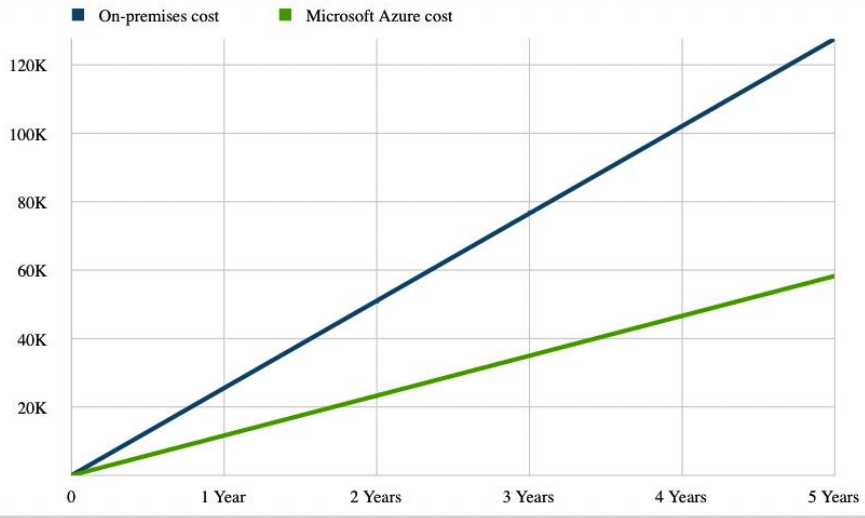
Chapter 10: Migrating Workloads to Azure



Over 5 year(s) with Microsoft Azure, your estimated cost savings could be as much as US$69,339

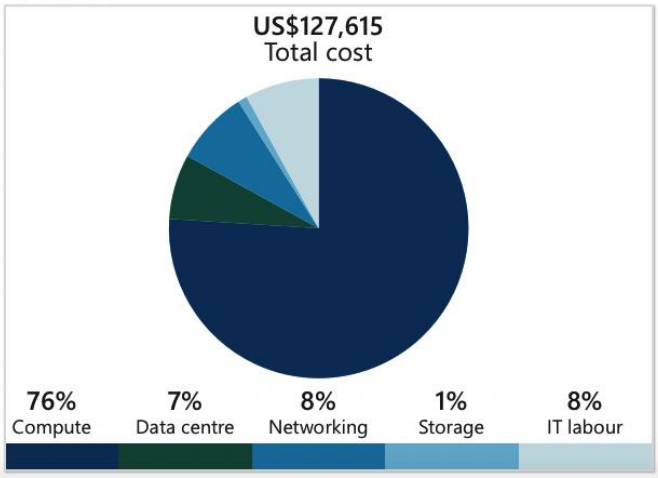
Total on-premises vs Azure cost over time

Savings from running workloads in Azure accrue over time. The following shows how those savings add up over years.



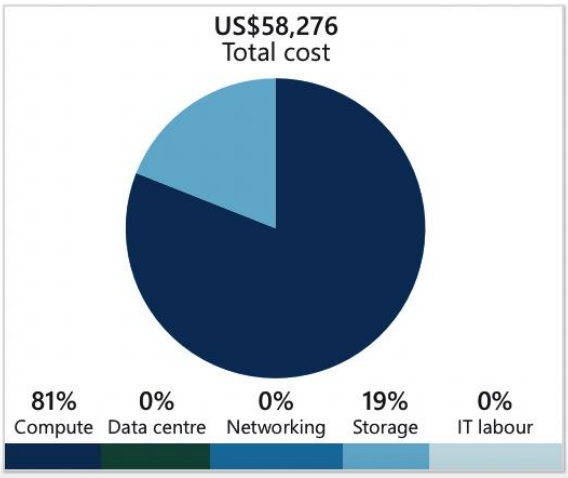
Total on-premises over 5 year(s)

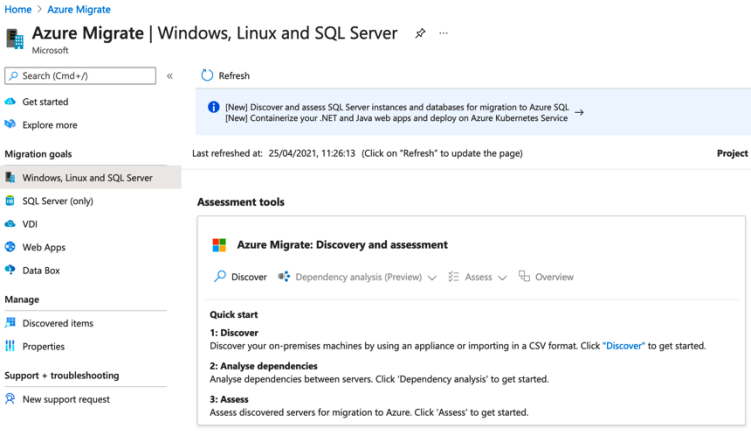
TCO of on-premises environments tends to be driven by compute and data centre costs.

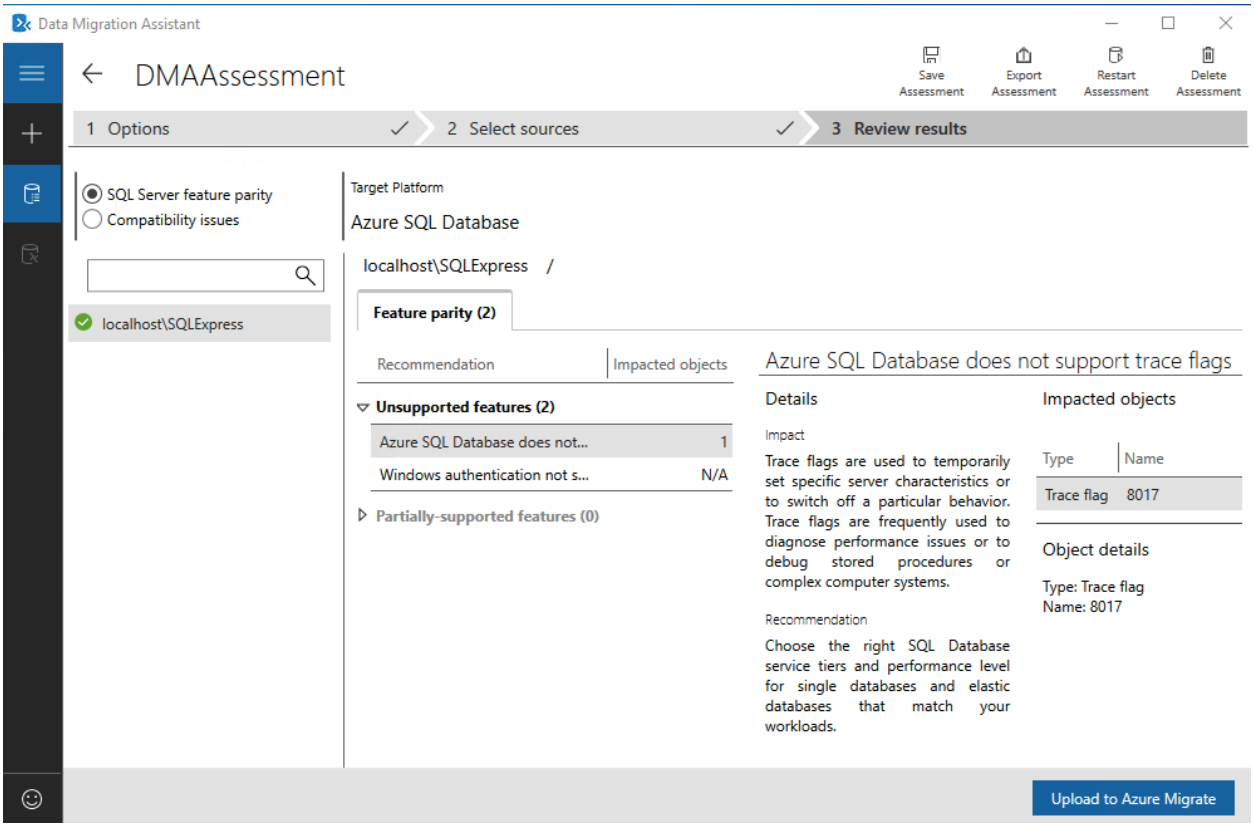


Total Azure cost over 5 year(s)

In Azure, certain cost categories decrease or go away completely.



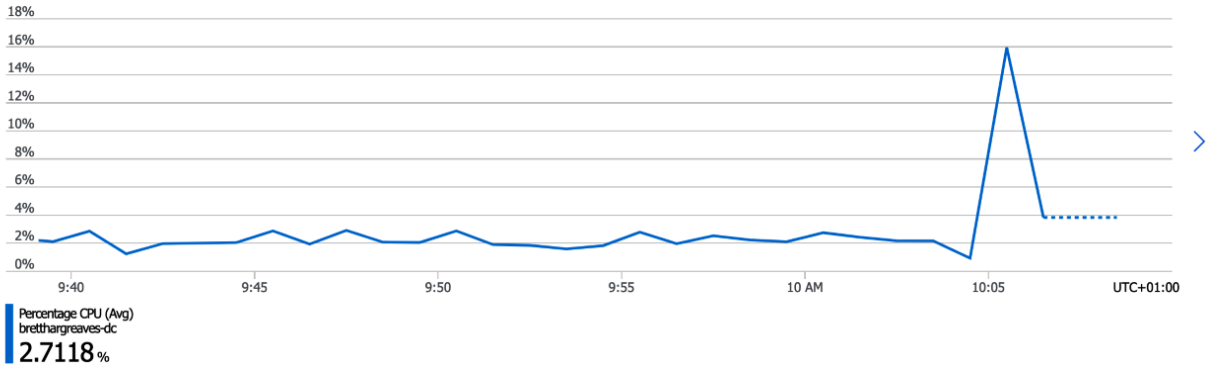

Home > Azure Migrate
Azure Migrate | Windows, Linux and SQL Server
Microsoft
Search (Cmd+/)
Refresh
Get started
Explore more
[New] Discover and assess SQL Server instances and databases for migration to Azure SQL
[New] Containerize your .NET and Java web apps and deploy on Azure Kubernetes Service
Migration goals
Last refreshed at: 25/04/2021, 11:26:13 (Click on "Refresh" to update the page)
Project
Windows, Linux and SQL Server
SQL Server (only)
VDI
Web Apps
Data Box
Assessment tools
Manage
Azure Migrate: Discovery and assessment
Discovered items
Properties
Discover
Dependency analysis (Preview)
Assess
Overview
Support + troubleshooting
Quick start
New support request
1: Discover
Discover your on-premises machines by using an appliance or importing in a CSV format. Click "Discover" to get started.
2: Analyse dependencies
Analyse dependencies between servers. Click 'Dependency analysis' to get started.
3: Assess
Assess discovered servers for migration to Azure. Click 'Assess' to get started.


Data Migration Assistant
DMAAssessment
Save Assessment
Export Assessment
Restart Assessment
Delete Assessment
1 Options
2 Select sources
3 Review results
SQL Server feature parity
Compatibility issues
Target Platform
Azure SQL Database
localhost\SQLExpress
localhost\SQLExpress /
Feature parity (2)
Recommendation
Impacted objects
Unsupported features (2)
Azure SQL Database does not...
1
Windows authentication not s...
N/A
Partially-supported features (0)
Azure SQL Database does not support trace flags
Details
Impact
Trace flags are used to temporarily set specific server characteristics or to switch off a particular behavior. Trace flags are frequently used to diagnose performance issues or to debug stored procedures or complex computer systems.
Recommendation
Choose the right SQL Database service tiers and performance level for single databases and elastic databases that match your workloads.
Impacted objects
Type
Name
Trace flag
8017
Object details
Type: Trace flag
Name: 8017
Upload to Azure Migrate

Avg Percentage CPU for bretthargreaves-dc

Add metric | Add filter | Apply splitting | Line chart | Drill into Logs | New alert rule | Pin to dashboard | ...

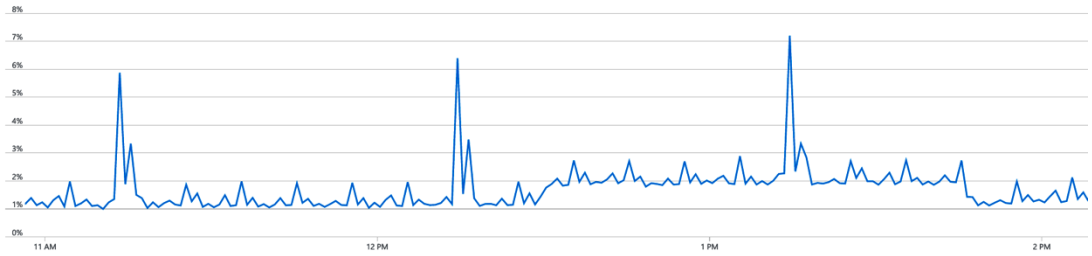
bretthargreaves-dc, **Percentage CPU**, Avg



Percentage CPU (Avg)
bretthargreaves-dc
2.7118 %

Host Metrics | Alerts

CPU percentage

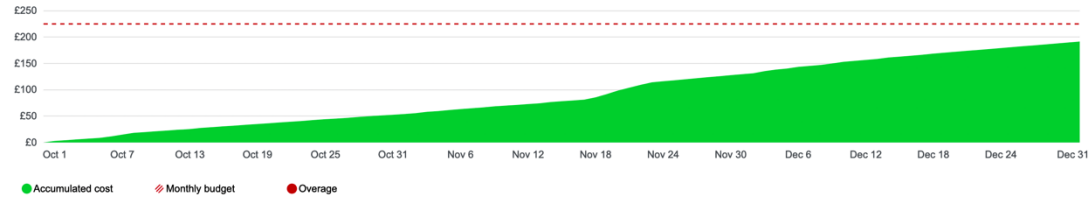


Percentage CPU (Avg)
bretthargreaves-dc
1.75 %

ACTUAL COST (GBP ONLY) | FORECAST UNAVAILABLE | BUDGET: MONTHLYBUDGET

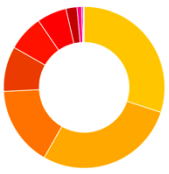
£191.46 | -- | £75 /mo

Group by: None | Granularity: Accumulated | Area



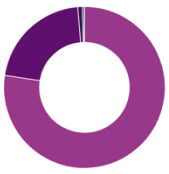
Accumulated cost | Monthly budget | Overage

Service name



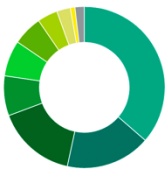
storage £57.44
virtual machines £54.13
backup £30.50
azure bastion £17.28
sql database £13.76
container registry

Location

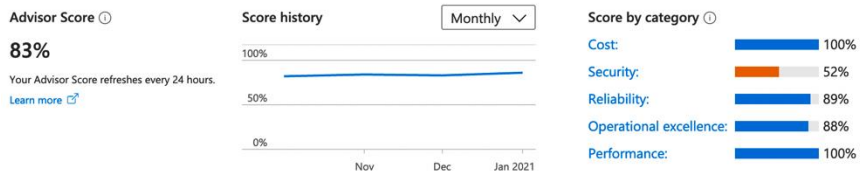


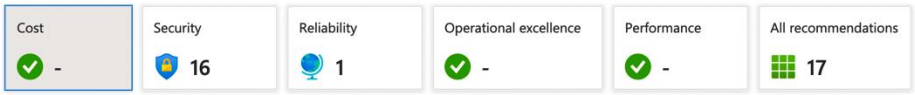
uk south £148.18
eu west £40.73
unknown £1.75
eu north £0.67
uk west £0.12
intercontinental

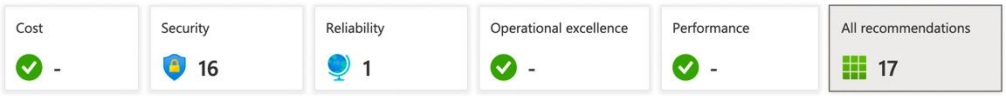
Resource group name



rsq-winvms £69.65
insight100 £32.59
rsq-backups £30.50
rsq-rdpfarm £15.25
rsq-sql £13.76
rsq-kubernetes

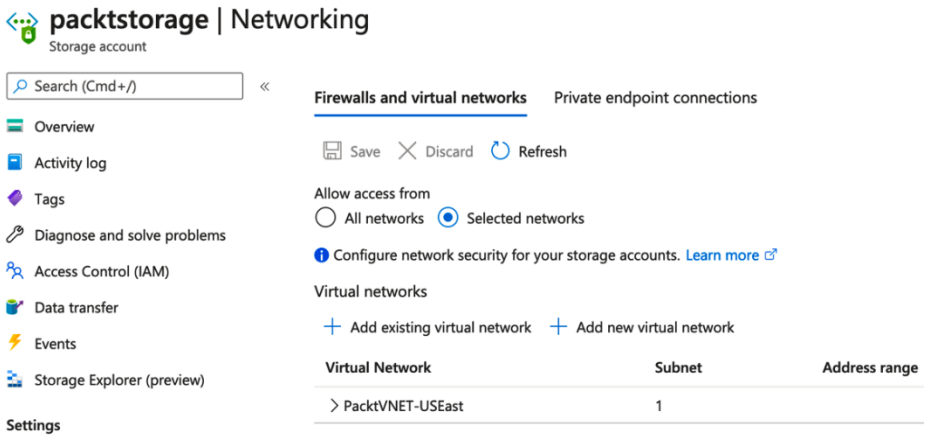


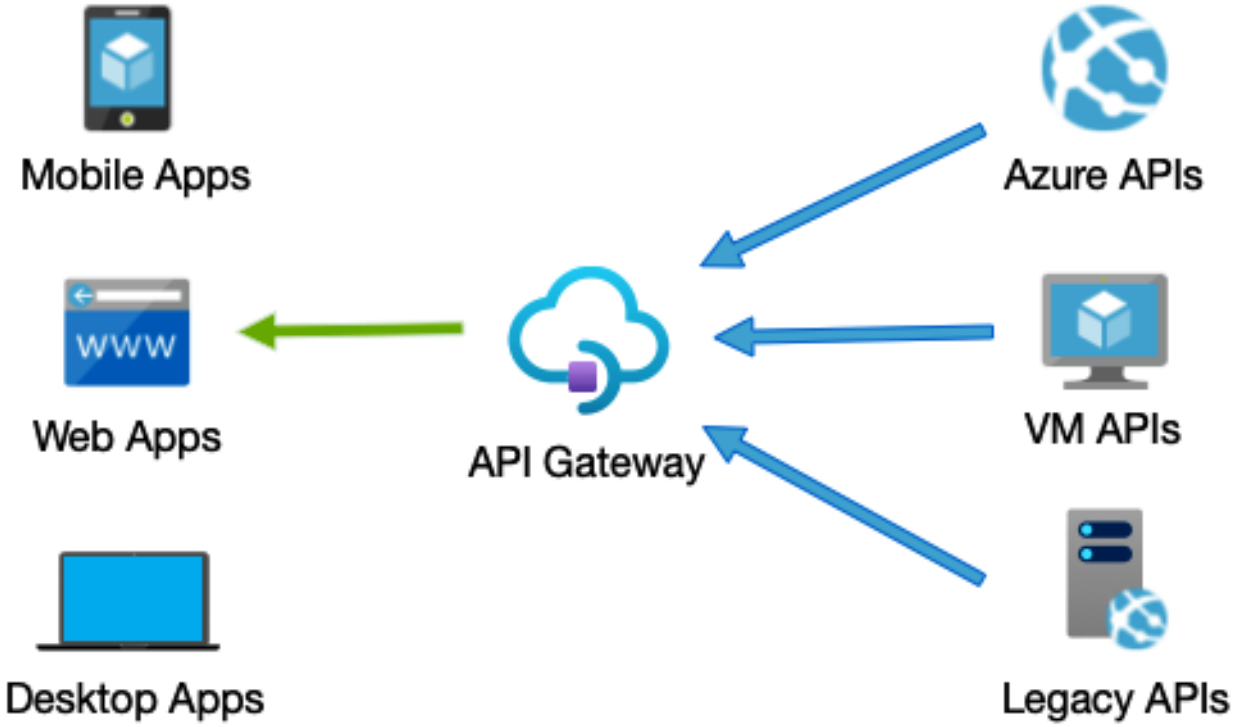


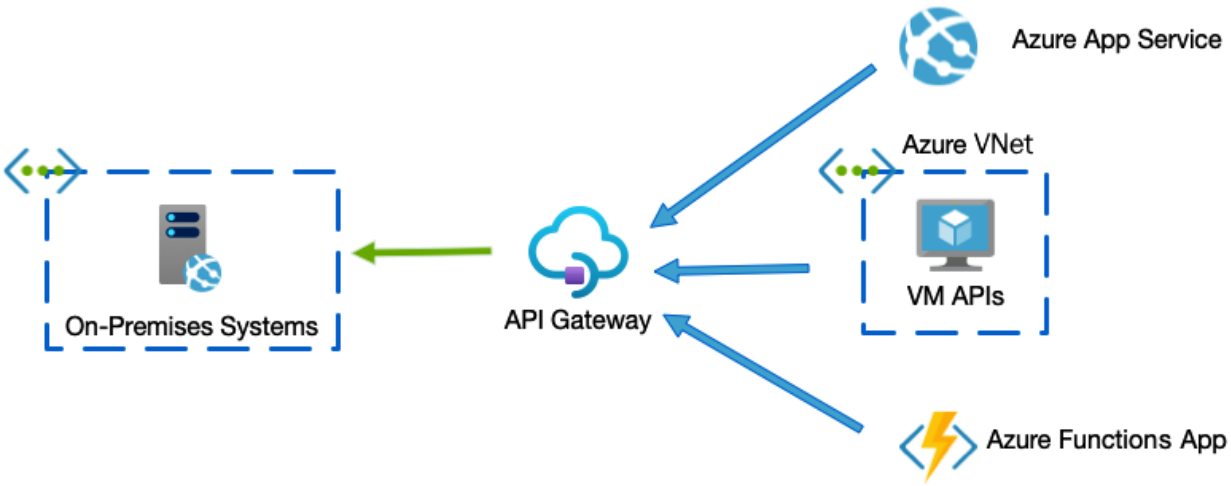


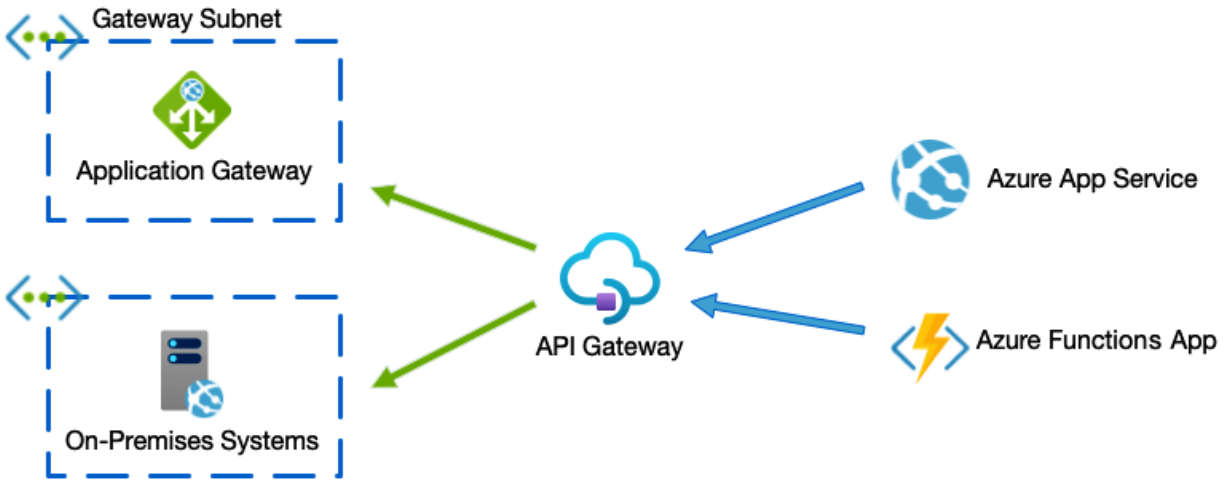
Description	Category	Potential benefits	Impacted resources
Enable virtual machine backup to protect your data from corruption and accidental deletion	Reliability	Improved data resilience and performance	1 Virtual machine
Log Analytics agent should be installed on your virtual machine	Security		1 Virtual machine
All network ports should be restricted on network security groups associated to your virtual machine	Security		2 Virtual machines
There should be more than one owner assigned to your subscription	Security		1 Subscription
Azure Defender for SQL servers on machines should be enabled	Security		1 Subscription
Azure Defender for Storage should be enabled	Security		1 Subscription

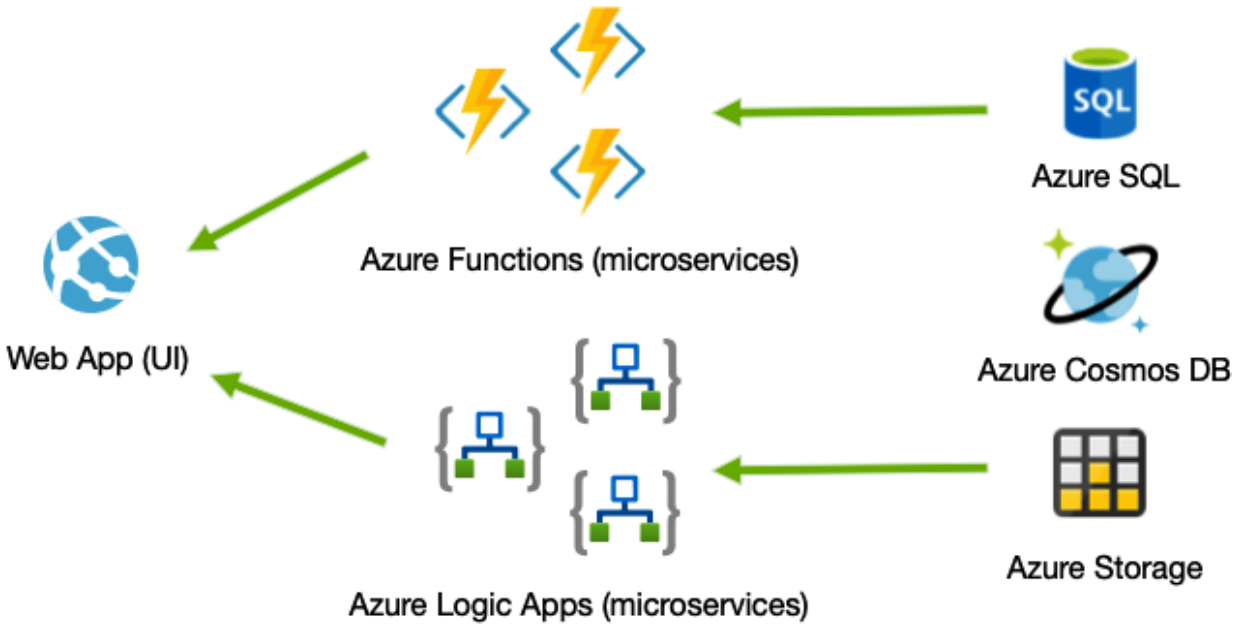
Chapter 11: Comparing Application Components

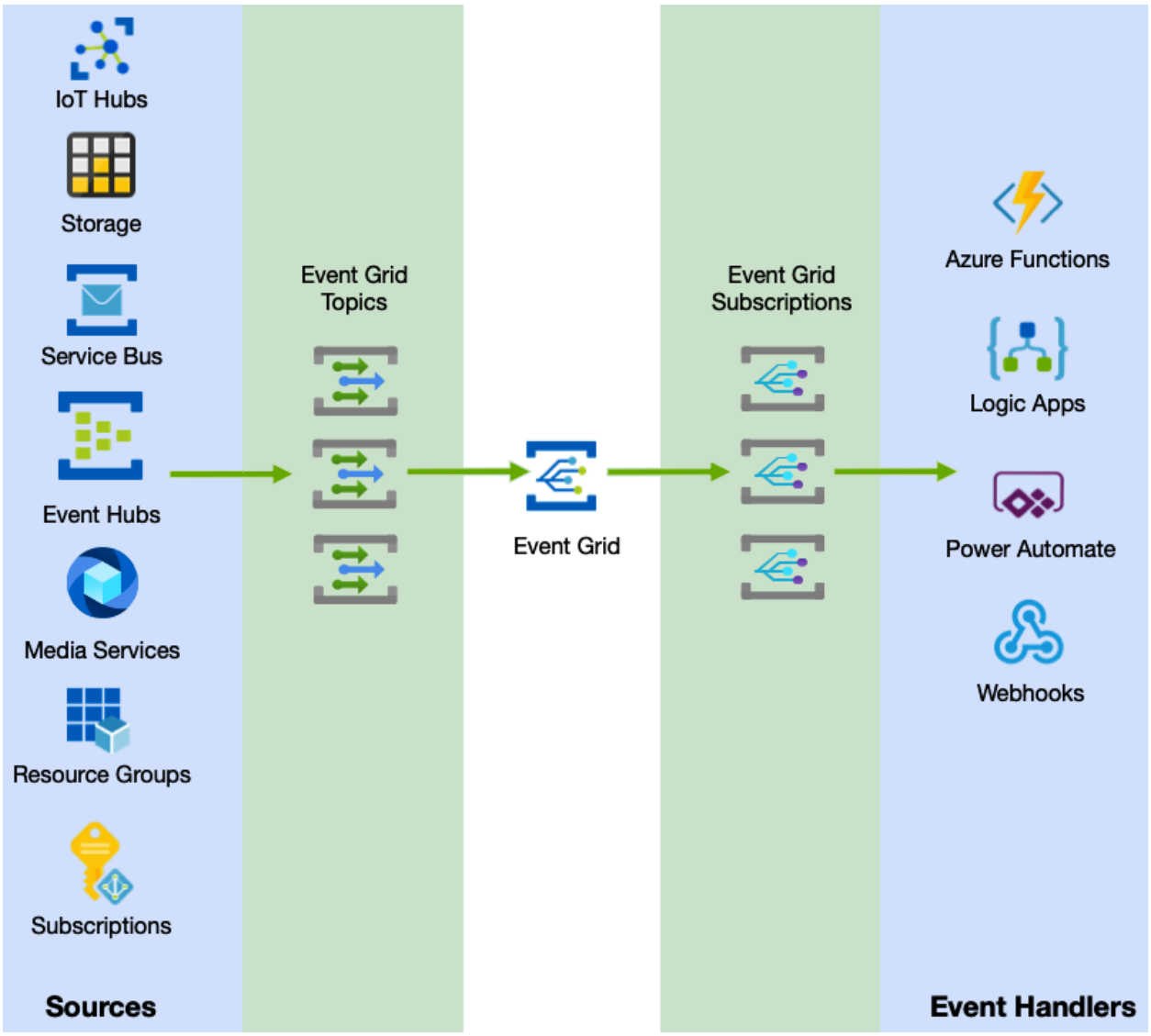





Azure App Service
Azure VNet
On-Premises Systems
API Gateway
VM APIs
Azure Functions App


Gateway Subnet
Application Gateway
Azure App Service
API Gateway
On-Premises Systems
Azure Functions App

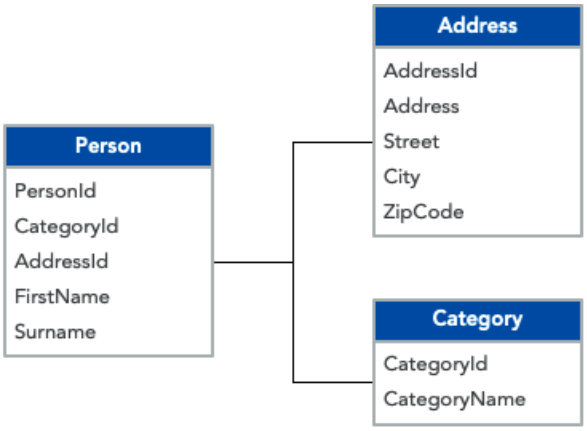

Azure SQL
Azure Functions (microservices)
Web App (UI)
Azure Cosmos DB
Azure Storage
Azure Logic Apps (microservices)


IoT Hubs
Storage
Service Bus
Event Hubs
Media Services
Resource Groups
Subscriptions
Sources
Event Grid Topics
Event Grid
Event Grid Subscriptions
Azure Functions
Logic Apps
Power Automate
Webhooks
Event Handlers

Sender
Consumer
Storage Queue

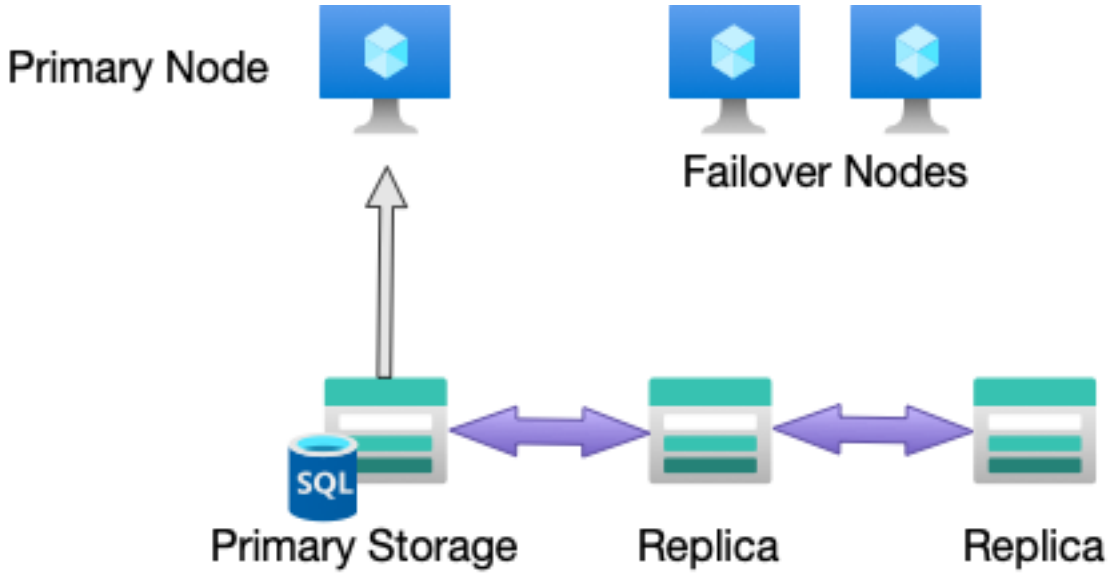
Order
Service Bus Topics
Subscription
(US Filter)
Subscription
(EU Filter)
US Ordering Function
EU Ordering Function

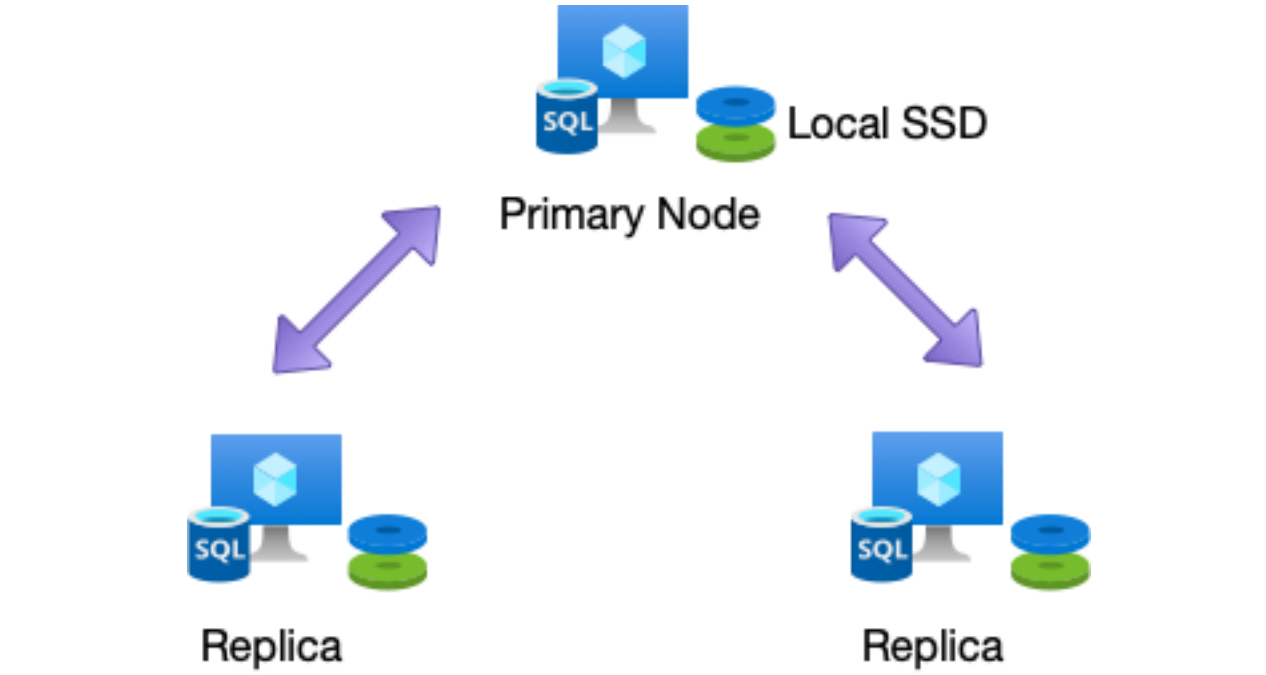
Chapter 12: Creating Scalable and Secure Databases

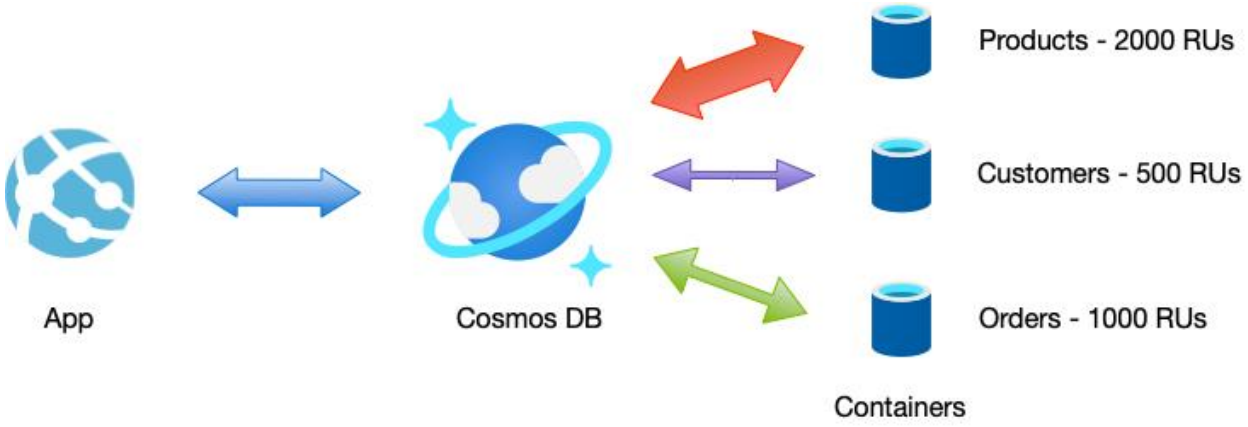


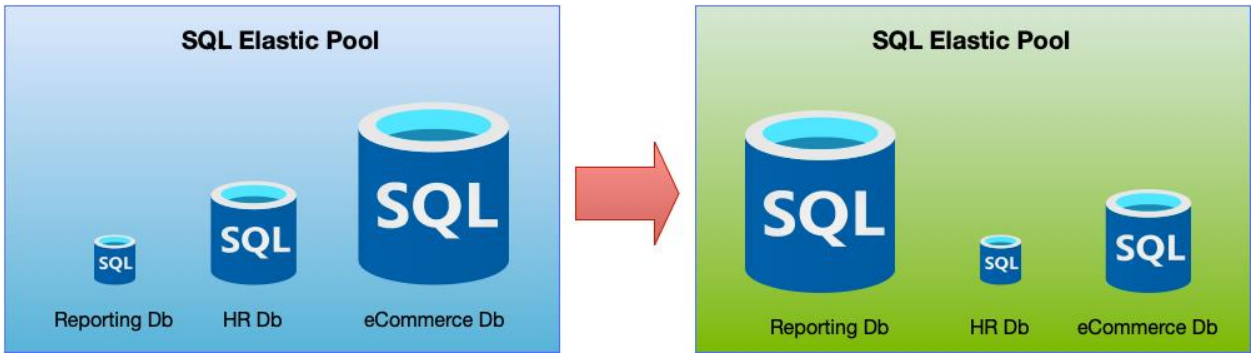
Example Combined Query

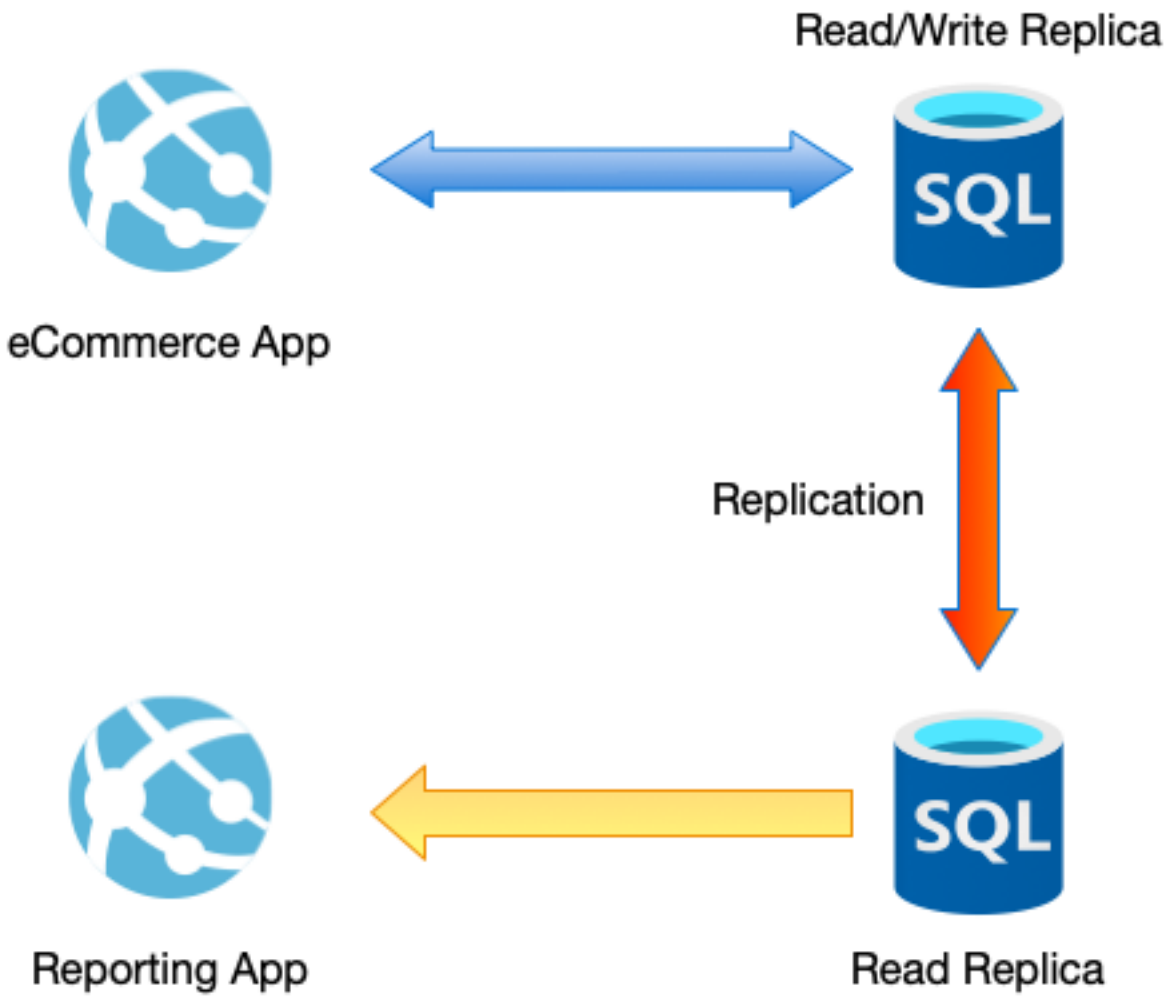
Person.PersonId	Person.FirstName	Person.Surname	Category.Name	Address.Street	Address.City
100	Brett	Hargreaves	Active	999 Letsbe Avenue	London

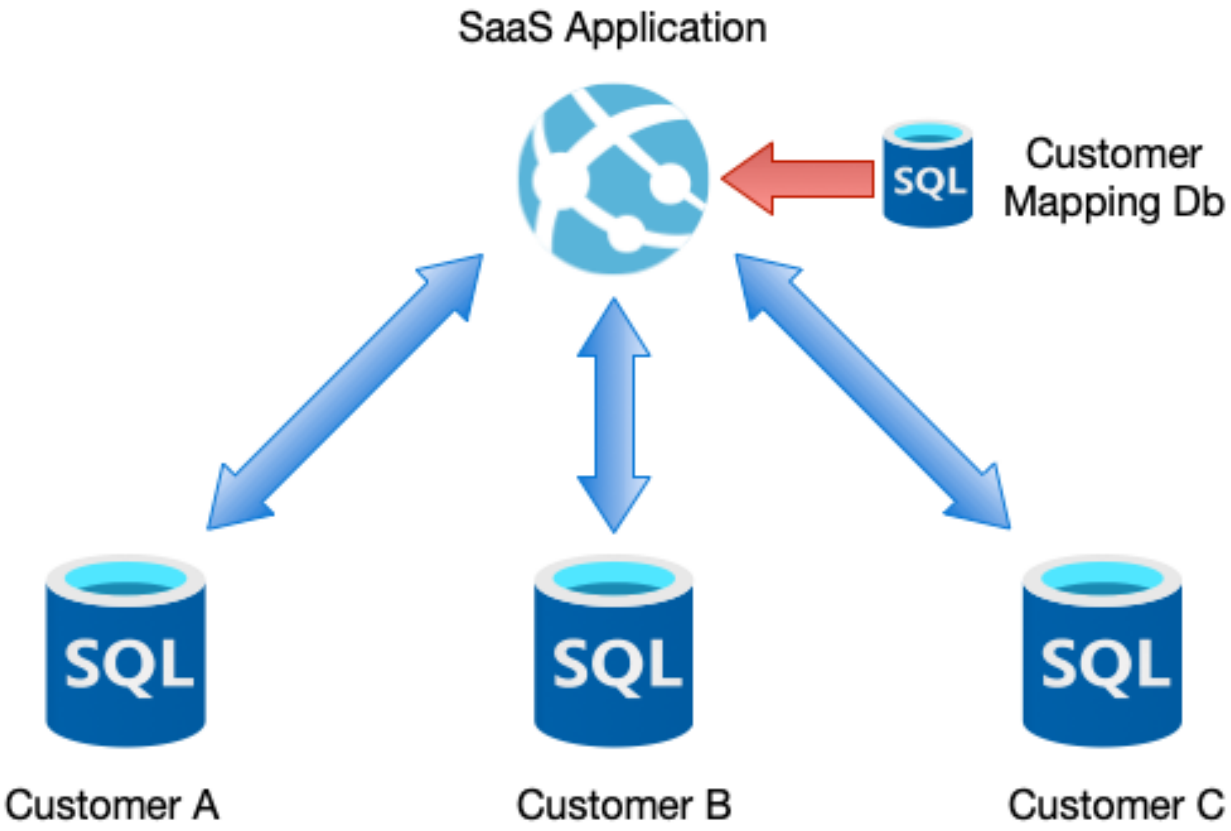


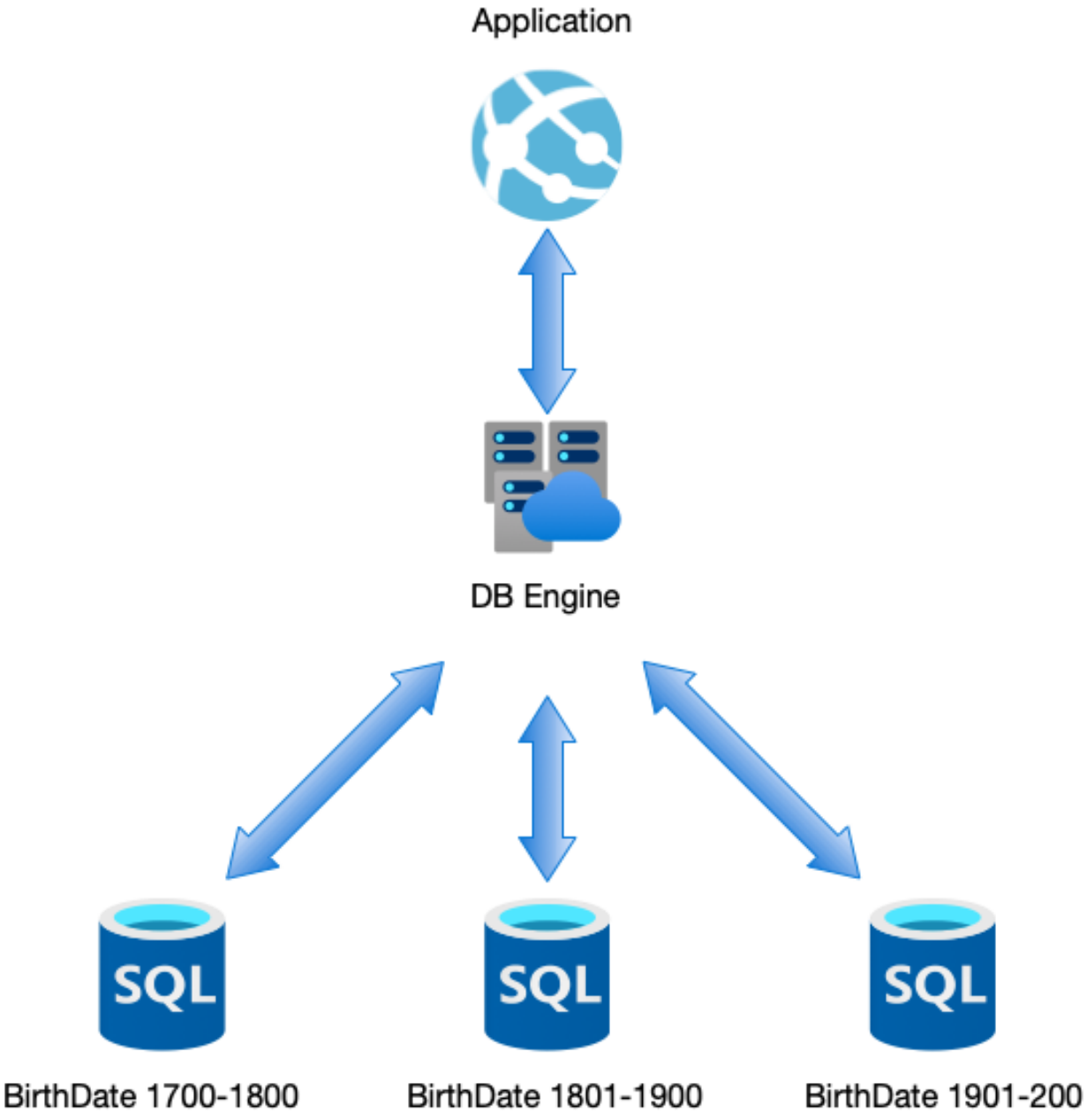

Local SSD
Primary Node
Replica
Replica

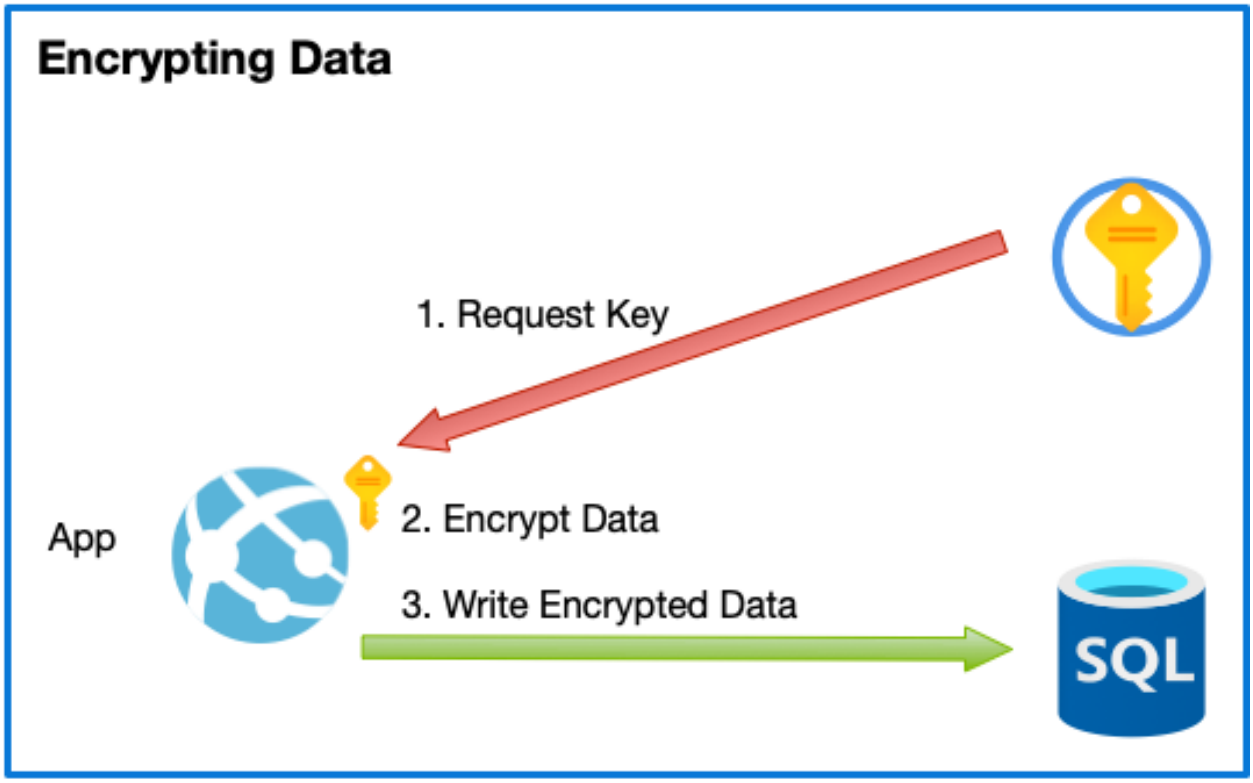

Products - 2000 RUs
Customers - 500 RUs
Orders - 1000 RUs
App
Cosmos DB
Containers

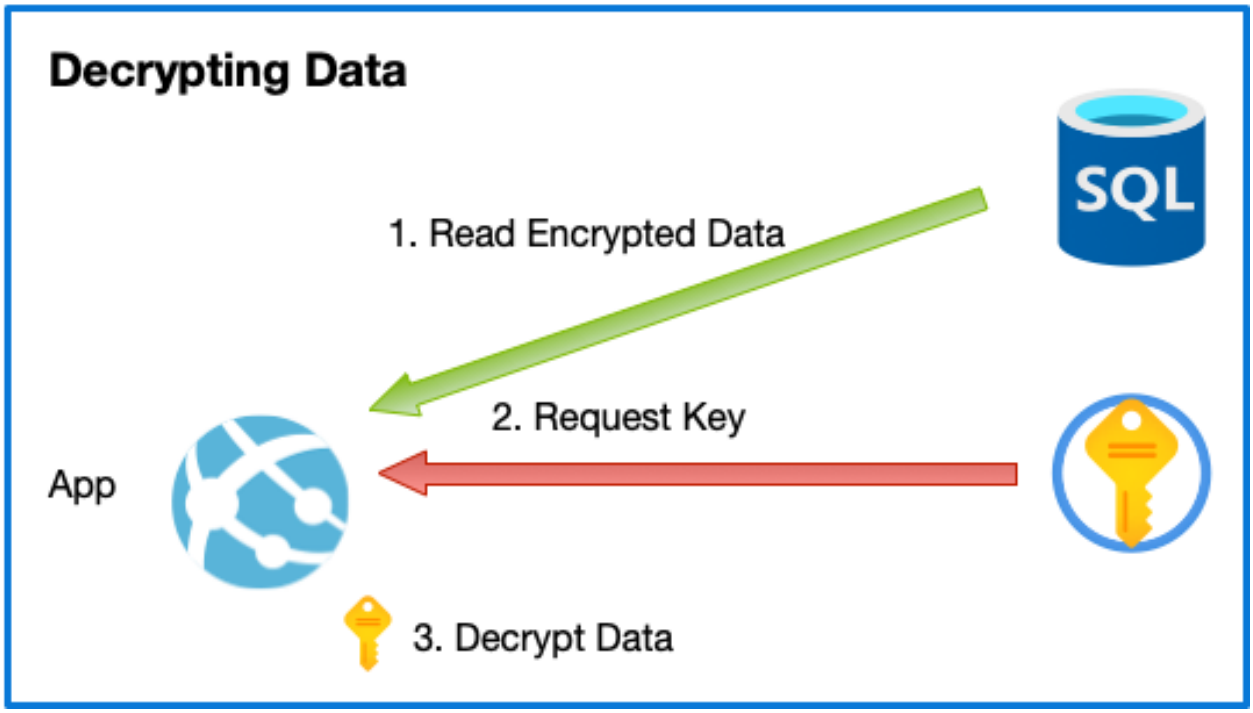

SQL Elastic Pool
Reporting Db
HR Db
eCommerce Db
SQL Elastic Pool
Reporting Db
HR Db
eCommerce Db


Read/Write Replica
SQL
eCommerce App
Replication
Reporting App
SQL
Read Replica


SaaS Application
SQL
Customer
Mapping Db
SQL
SQL
SQL
Customer A
Customer B
Customer C


Application
DB Engine
SQL
SQL
SQL
BirthDate 1700-1800
BirthDate 1801-1900
BirthDate 1901-200


Encrypting Data
1. Request Key
App
2. Encrypt Data
3. Write Encrypted Data
SQL


Decrypting Data
SQL
1. Read Encrypted Data
2. Request Key
App
3. Decrypt Data

Chapter 13: Options for Data Integration

Create storage account

Basics | Networking | Data protection | **Advanced** | Tags | Review + create

Security

Secure transfer required ⓘ — ○ Disabled ◉ Enabled

Allow shared key access ⓘ — ○ Disabled ◉ Enabled

Minimum TLS version ⓘ — Version 1.2

Infrastructure encryption ⓘ — ◉ Disabled ○ Enabled

ⓘ Sign up is currently required to enable infrastructure encryption on a per-subscription basis. Sign up for infrastructure encryption

Blob storage

Allow Blob public access ⓘ — ○ Disabled ◉ Enabled

Blob access tier (default) ⓘ — ○ Cool ◉ Hot

NFS v3 ⓘ — ◉ Disabled ○ Enabled

ⓘ Sign up is currently required to utilize the NFS v3 feature on a per-subscription basis. Sign up for NFS v3

Data Lake Storage Gen2

Hierarchical namespace ⓘ — ○ Disabled ◉ Enabled

Azure Files

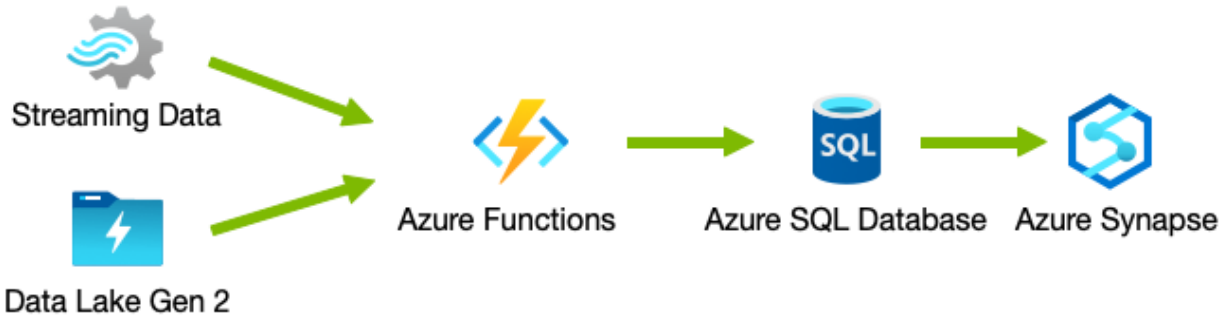
Large file shares ⓘ — ◉ Disabled ○ Enabled

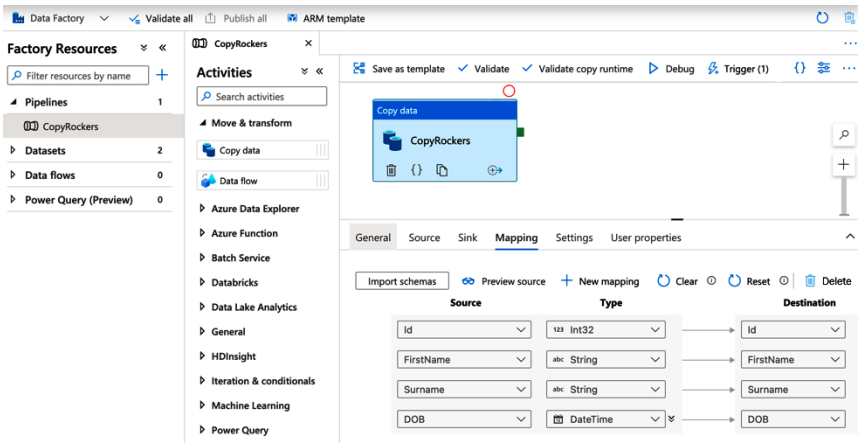
ⓘ The current combination of storage account kind, performance, replication and location does not support large file shares.

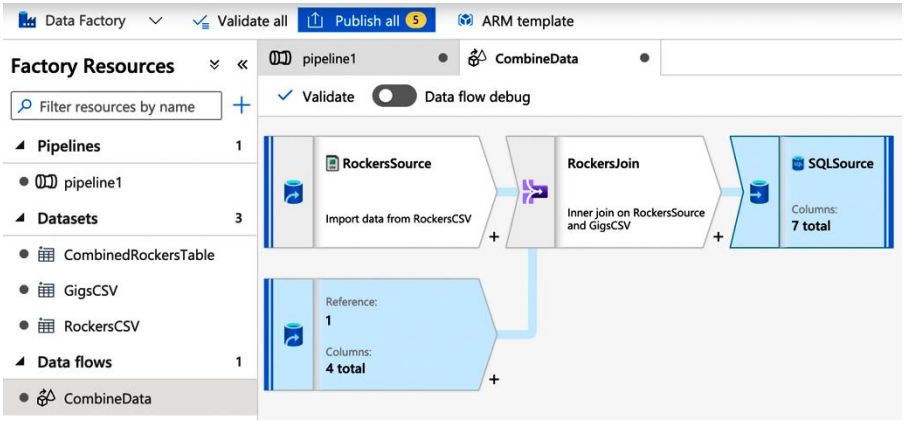
Tables and Queues

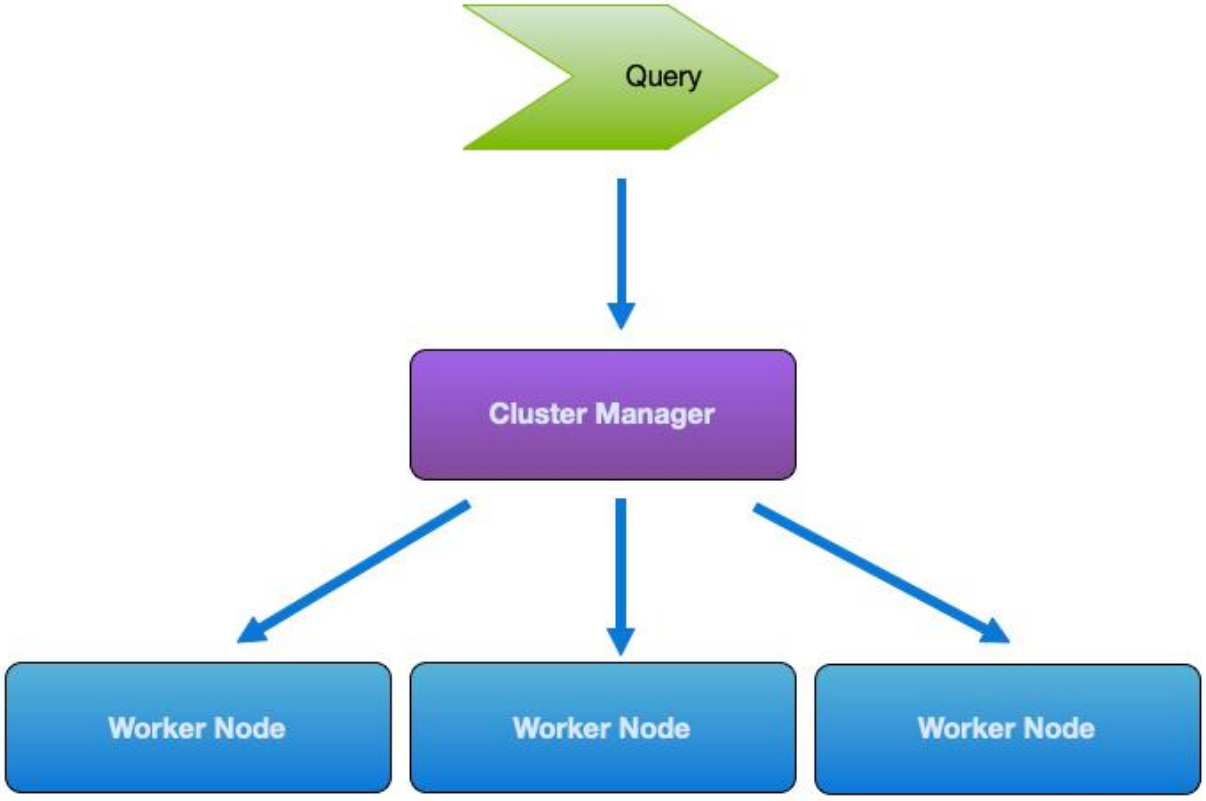
Customer-managed keys support ⓘ — ◉ Disabled ○ Enabled

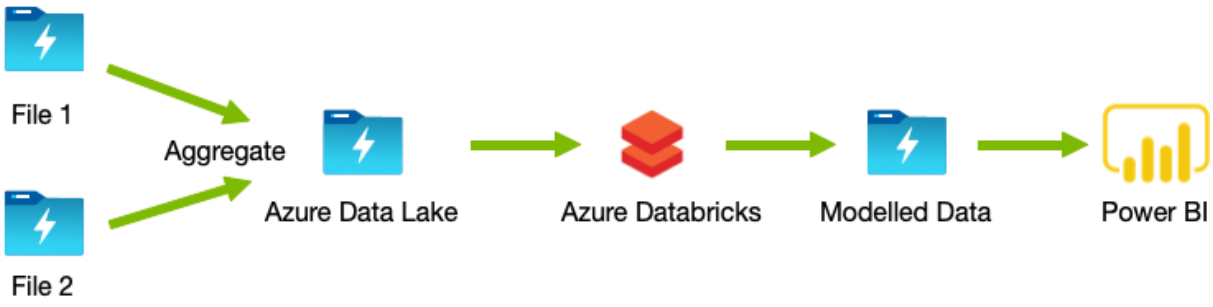
Review + create | < Previous | Next : Tags >

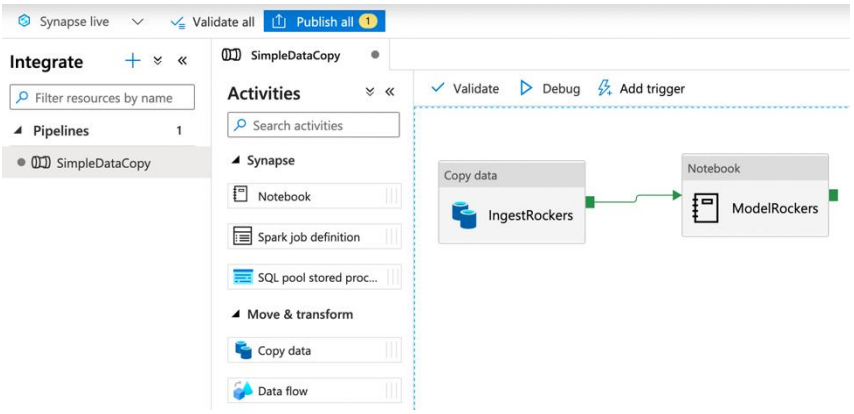

Streaming Data
Data Lake Gen 2
Azure Functions
SQL
Azure SQL Database
Azure Synapse

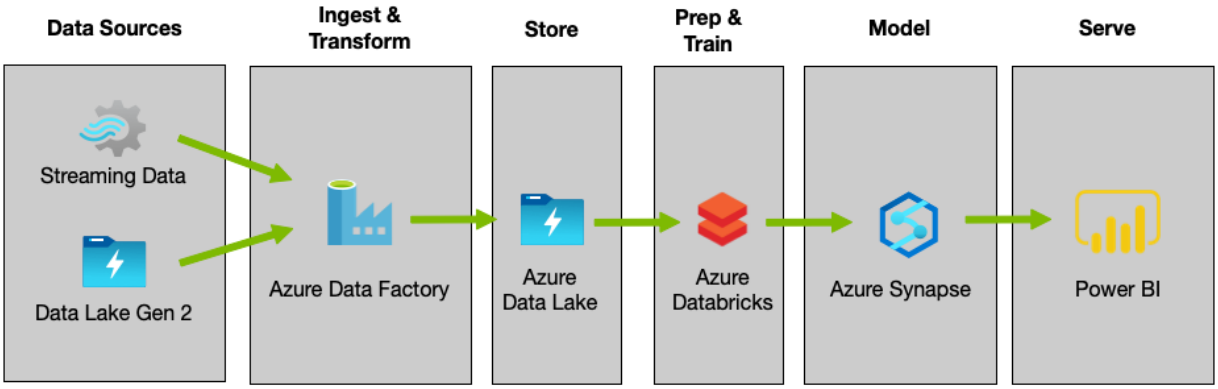

Data Factory
Validate all
Publish all
ARM template
Factory Resources
Filter resources by name
Pipelines 1
CopyRockers
Datasets 2
Data flows 0
Power Query (Preview) 0
CopyRockers
Activities
Search activities
Move & transform
Copy data
Data flow
Azure Data Explorer
Azure Function
Batch Service
Databricks
Data Lake Analytics
General
HDInsight
Iteration & conditionals
Machine Learning
Power Query
Save as template
Validate
Validate copy runtime
Debug
Trigger (1)
Copy data
CopyRockers
General
Source
Sink
Mapping
Settings
User properties
Import schemas
Preview source
New mapping
Clear
Reset
Delete
Source
Type
Destination
Id
Int32
FirstName
String
Surname
String
DOB
DateTime


Data Factory
Validate all
Publish all 5
ARM template
Factory Resources
Filter resources by name
Pipelines 1
pipeline1
Datasets 3
CombinedRockersTable
GigsCSV
RockersCSV
Data flows 1
CombineData
pipeline1
CombineData
Validate
Data flow debug
RockersSource
Import data from RockersCSV
RockersJoin
Inner join on RockersSource and GigsCSV
SQLSource
Columns:
7 total
Reference:
1
Columns:
4 total

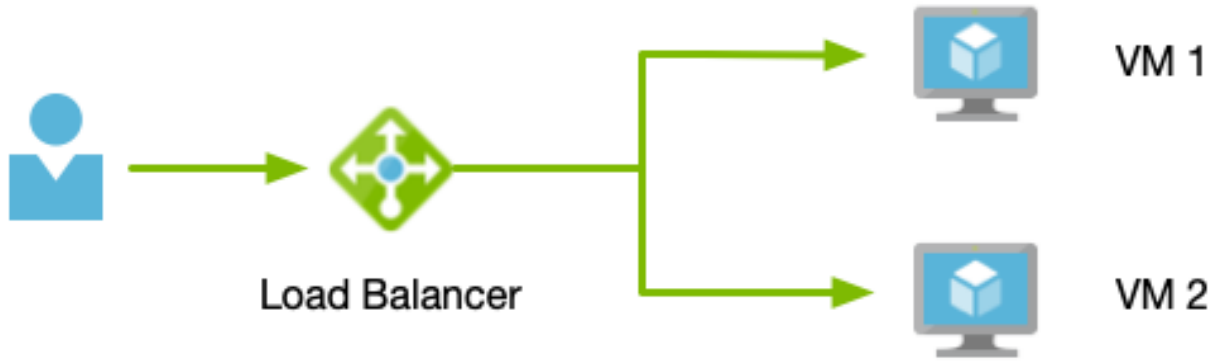

Query
Cluster Manager
Worker Node
Worker Node
Worker Node

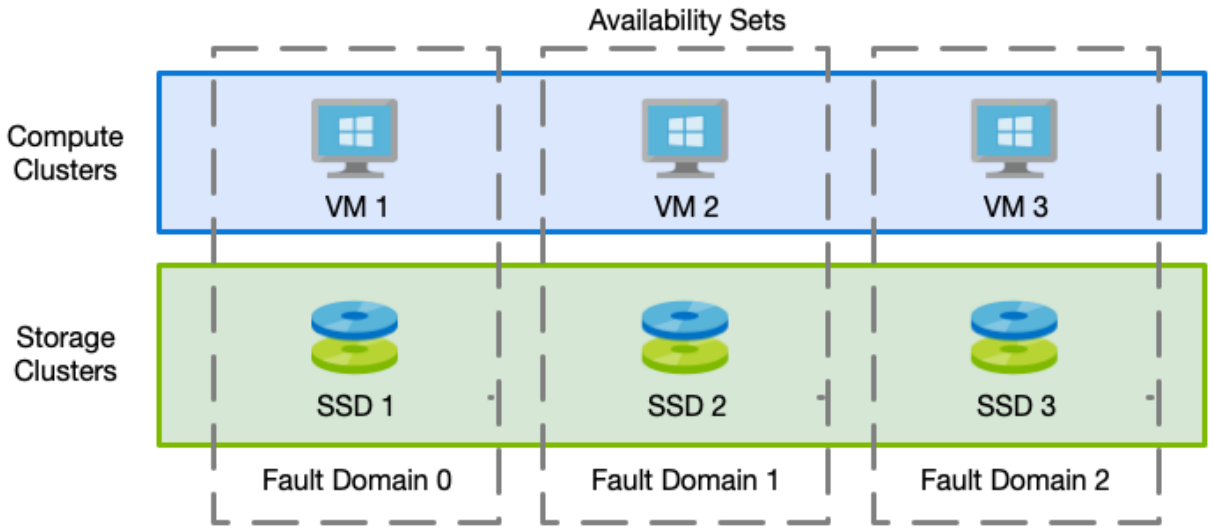

File 1
File 2
Aggregate
Azure Data Lake
Azure Databricks
Modelled Data
Power BI

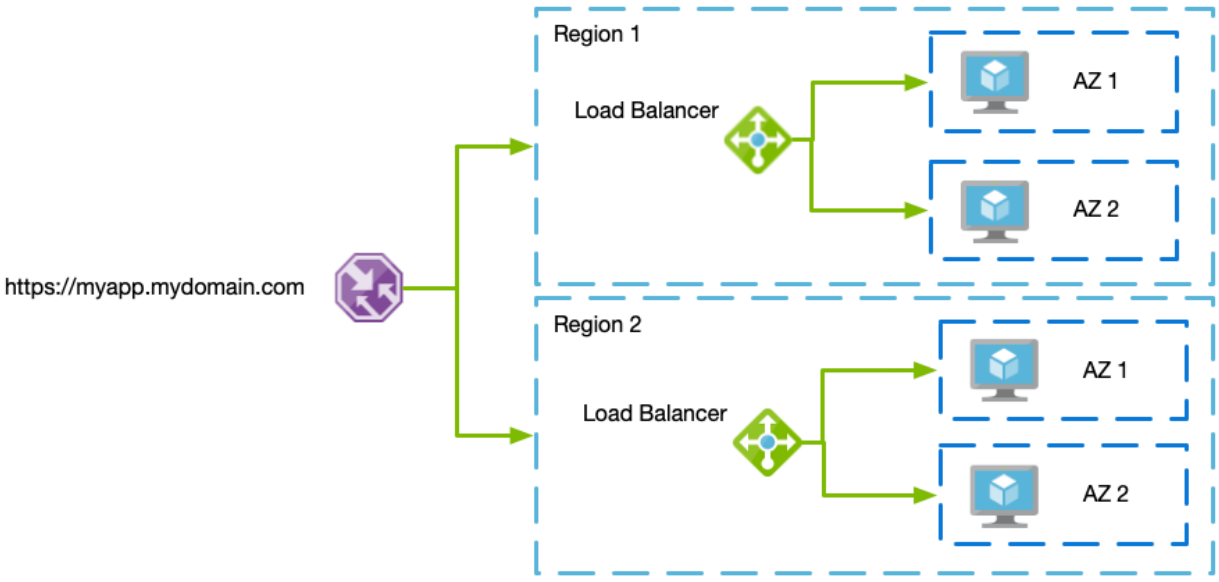

Synapse live
Validate all
Publish all 1
Integrate
Filter resources by name
Pipelines 1
SimpleDataCopy
SimpleDataCopy
Activities
Search activities
Synapse
Notebook
Spark job definition
SQL pool stored proc...
Move & transform
Copy data
Data flow
Validate
Debug
Add trigger
Copy data
IngestRockers
Notebook
ModelRockers

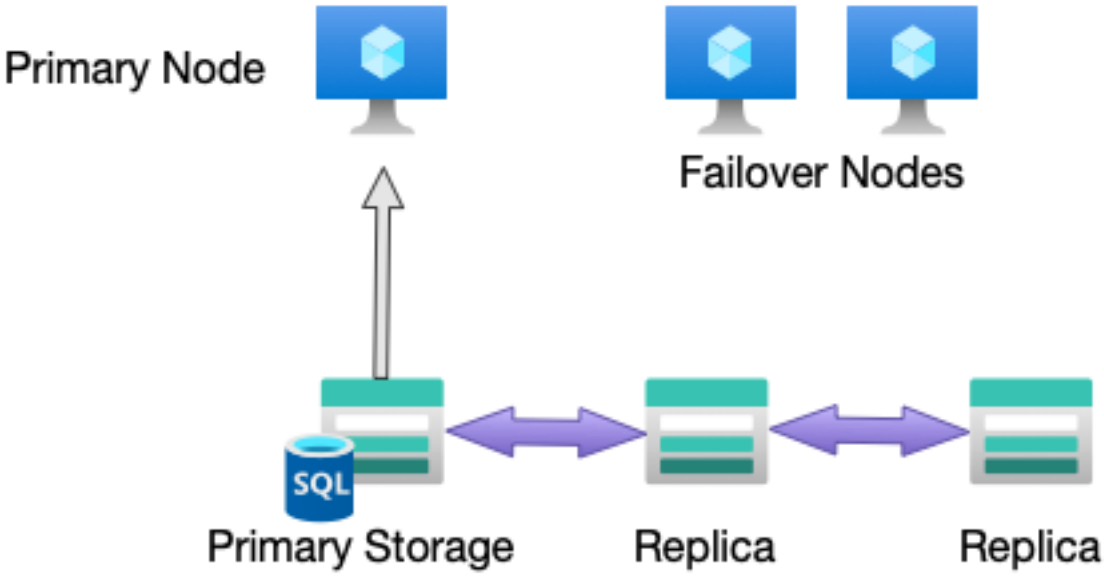

Data Sources
Ingest & Transform
Store
Prep & Train
Model
Serve
Streaming Data
Data Lake Gen 2
Azure Data Factory
Azure Data Lake
Azure Databricks
Azure Synapse
Power BI

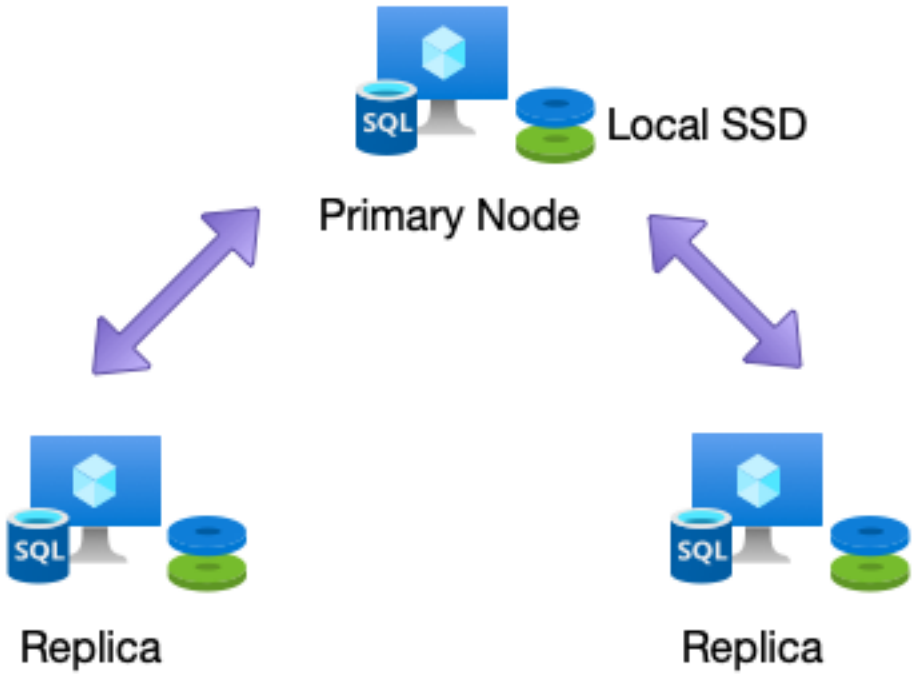
Chapter 14: High Availability and Redundancy Concepts






Region 1
Load Balancer
AZ 1
AZ 2
https://myapp.mydomain.com
Region 2
Load Balancer
AZ 1
AZ 2


Primary Node
Failover Nodes
SQL
Primary Storage
Replica
Replica



packtsqlfailover

packtsqlserver

Save | Discard | Add databases | Edit configuration | Remove databases | Failover | Forced Failover | Delete

Configuration details | Databases within group | Databases selected to be added (0) | Databases selected for removal (0)

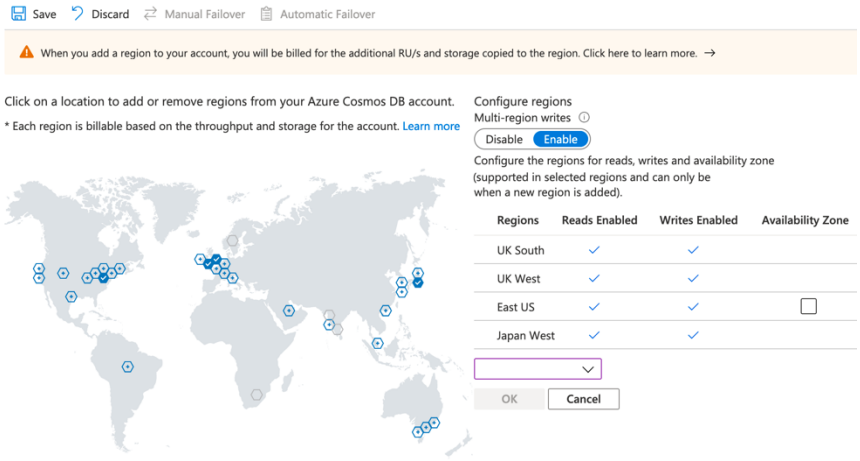
Server	Role	Read/Write failover policy
packtsqlserver (East US)	Primary	Automatic
packtsqlserver-westus (West US)	Secondary	

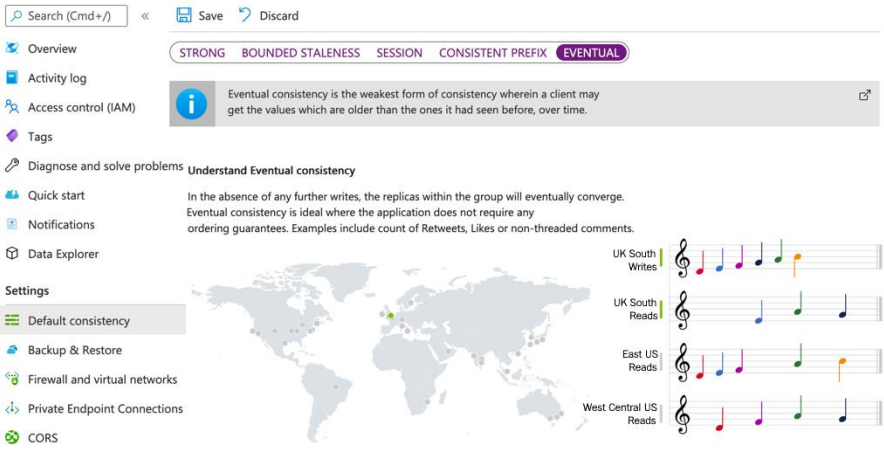
Read/write listener endpoint

packtsqlfailover.database.windows.net

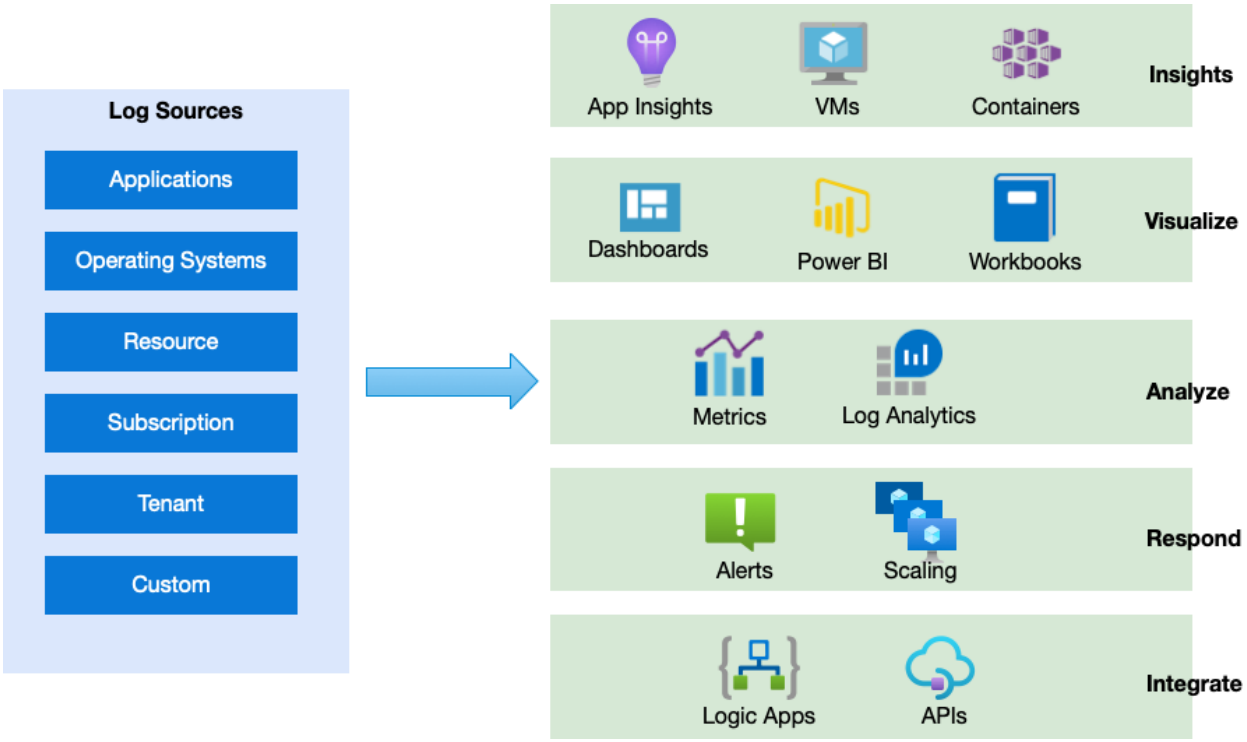
Read-only listener endpoint

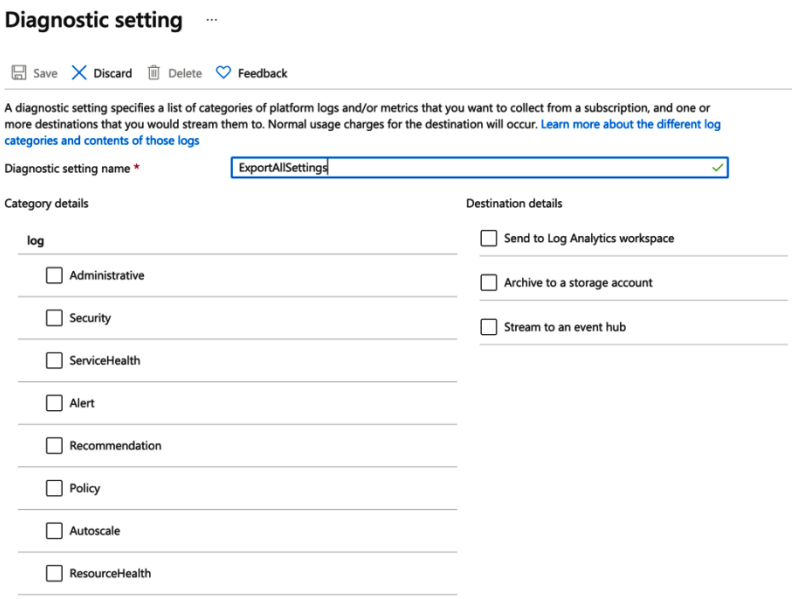
packtsqlfailover.secondary.database.windows.net


Save
Discard
Manual Failover
Automatic Failover
When you add a region to your account, you will be billed for the additional RU/s and storage copied to the region. Click here to learn more.
Click on a location to add or remove regions from your Azure Cosmos DB account.
* Each region is billable based on the throughput and storage for the account. Learn more
Configure regions
Multi-region writes
Disable
Enable
Configure the regions for reads, writes and availability zone (supported in selected regions and can only be when a new region is added).
Regions
Reads Enabled
Writes Enabled
Availability Zone
UK South
UK West
East US
Japan West
OK
Cancel


Search (Cmd+/)
Save
Discard
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Quick start
Notifications
Data Explorer
Settings
Default consistency
Backup & Restore
Firewall and virtual networks
Private Endpoint Connections
CORS
STRONG
BOUNDED STALENESS
SESSION
CONSISTENT PREFIX
EVENTUAL
Eventual consistency is the weakest form of consistency wherein a client may get the values which are older than the ones it had seen before, over time.
Understand Eventual consistency
In the absence of any further writes, the replicas within the group will eventually converge. Eventual consistency is ideal where the application does not require any ordering guarantees. Examples include count of Retweets, Likes or non-threaded comments.
UK South Writes
UK South Reads
East US Reads
West Central US Reads

Chapter 15: Designing for Logging and Monitoring





Diagnostic settings are used to configure streaming export of platform logs and metrics for a subscription to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

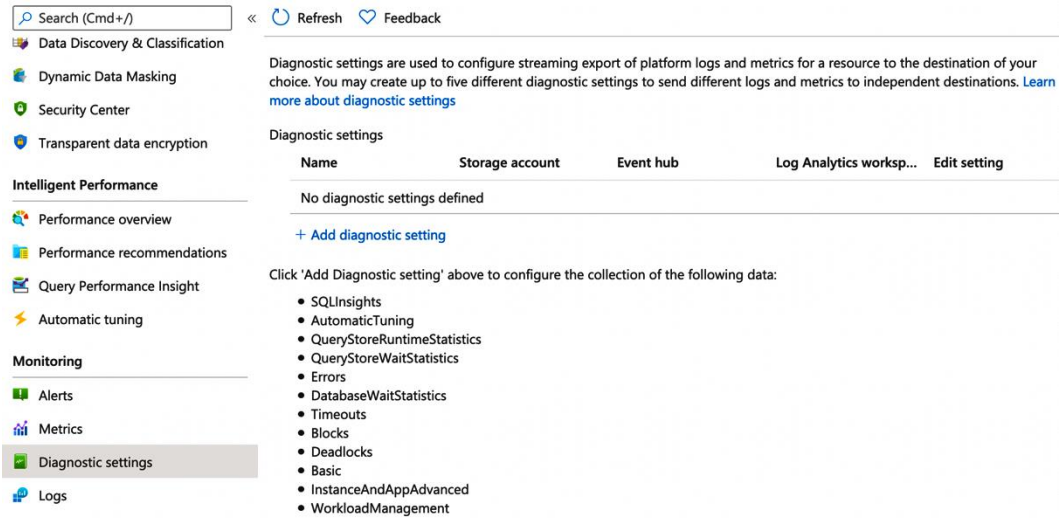
Diagnostic settings

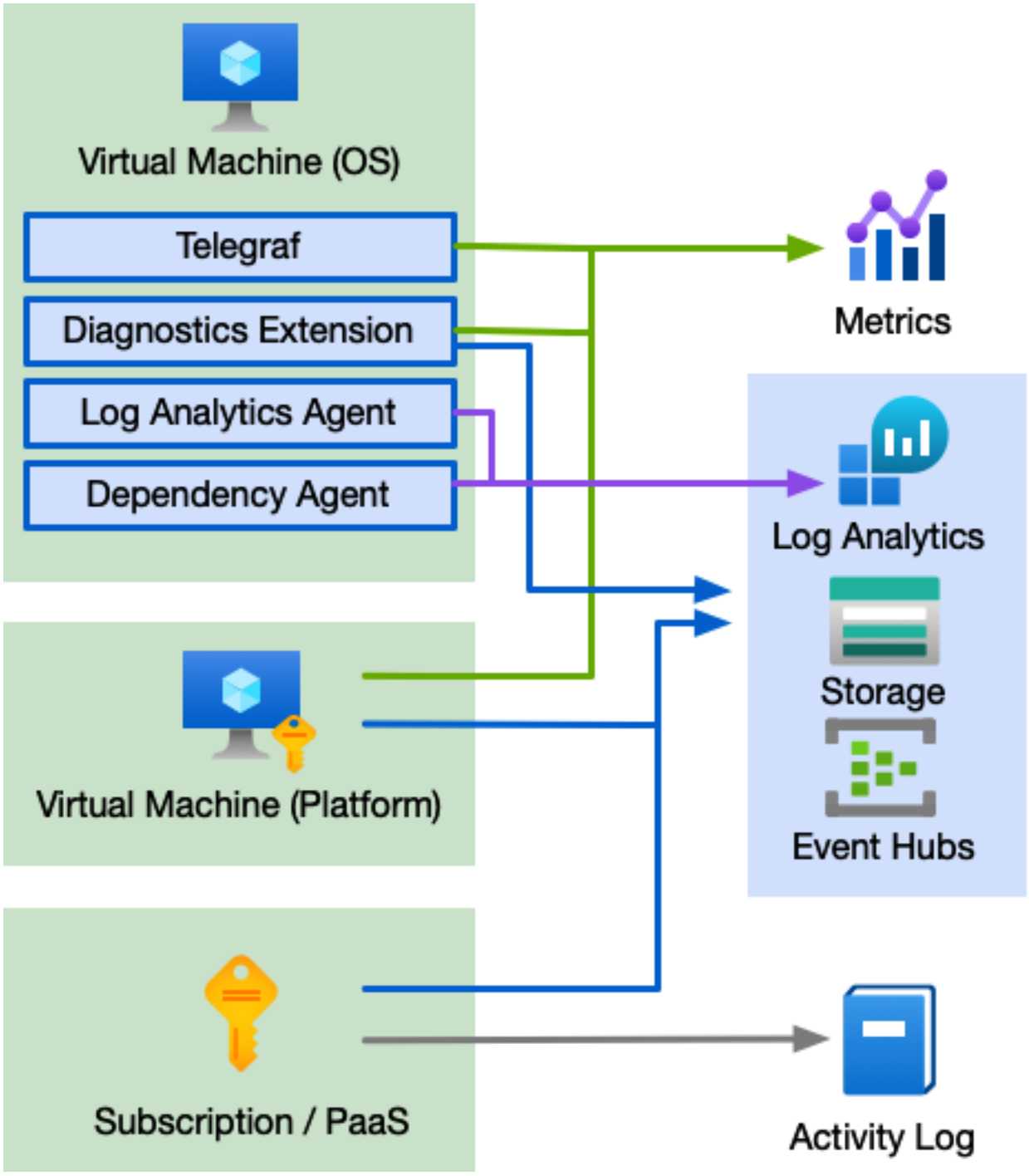
Name	Storage account	Event hub	Log Analytics workspace	Edit setting
MyApplicationsLogs	vmlogging	-	brett-app-specific-logs	Edit setting
SubscriptionActivityLogs	-	-	completecoder-siem	Edit setting

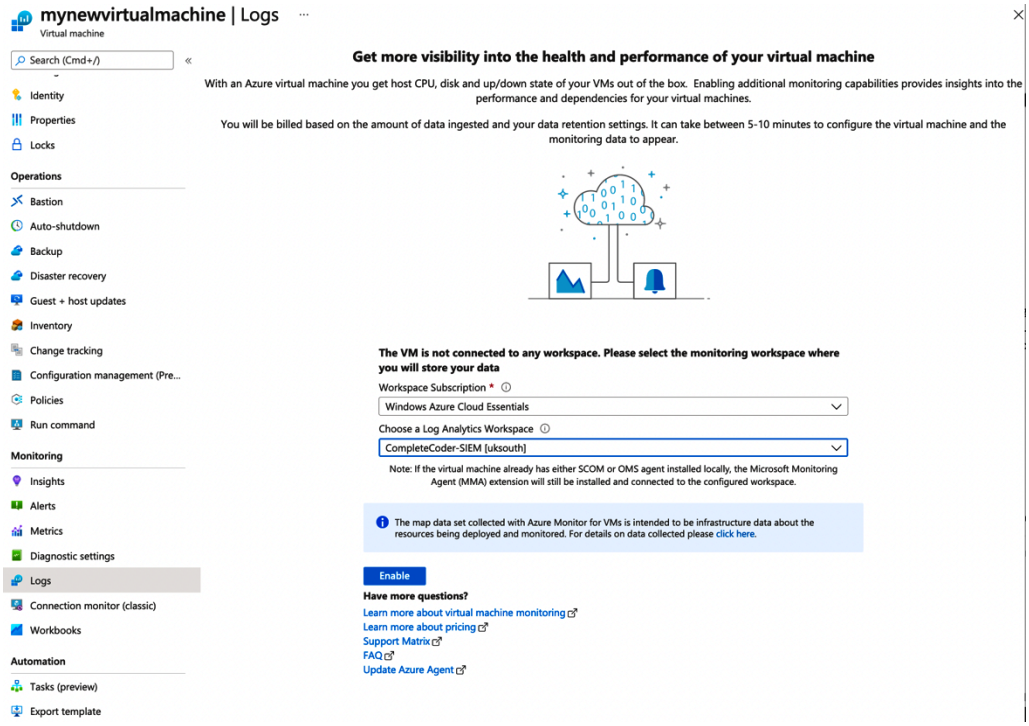
+ Add diagnostic setting

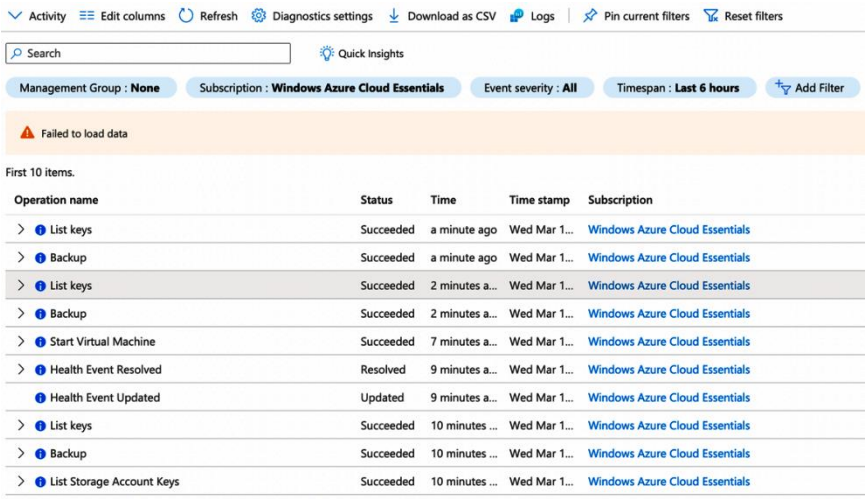
Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Administrative
- Security
- ServiceHealth
- Alert
- Recommendation
- Policy
- Autoscale
- ResourceHealth




Virtual Machine (OS)
Telegraf
Diagnostics Extension
Log Analytics Agent
Dependency Agent
Virtual Machine (Platform)
Subscription / PaaS
Metrics
Log Analytics
Storage
Event Hubs
Activity Log


mynewvirtualmachine | Logs
Virtual machine
Search (Cmd+/)
Identity
Properties
Locks
Operations
Bastion
Auto-shutdown
Backup
Disaster recovery
Guest + host updates
Inventory
Change tracking
Configuration management (Pre...
Policies
Run command
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Connection monitor (classic)
Workbooks
Automation
Tasks (preview)
Export template
Get more visibility into the health and performance of your virtual machine
With an Azure virtual machine you get host CPU, disk and up/down state of your VMs out of the box. Enabling additional monitoring capabilities provides insights into the performance and dependencies for your virtual machines.
You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to configure the virtual machine and the monitoring data to appear.
The VM is not connected to any workspace. Please select the monitoring workspace where you will store your data
Workspace Subscription *
Windows Azure Cloud Essentials
Choose a Log Analytics Workspace
CompleteCoder-SIEM [uksouth]
Note: If the virtual machine already has either SCOM or OMS agent installed locally, the Microsoft Monitoring Agent (MMA) extension will still be installed and connected to the configured workspace.
The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please click here.
Enable
Have more questions?
Learn more about virtual machine monitoring
Learn more about pricing
Support Matrix
FAQ
Update Azure Agent


Activity
Edit columns
Refresh
Diagnostics settings
Download as CSV
Logs
Pin current filters
Reset filters
Search
Quick Insights
Management Group : None
Subscription : Windows Azure Cloud Essentials
Event severity : All
Timespan : Last 6 hours
Add Filter
Failed to load data
First 10 items.
Operation name
Status
Time
Time stamp
Subscription
List keys Succeeded a minute ago Wed Mar 1... Windows Azure Cloud Essentials
Backup Succeeded a minute ago Wed Mar 1... Windows Azure Cloud Essentials
List keys Succeeded 2 minutes a... Wed Mar 1... Windows Azure Cloud Essentials
Backup Succeeded 2 minutes a... Wed Mar 1... Windows Azure Cloud Essentials
Start Virtual Machine Succeeded 7 minutes a... Wed Mar 1... Windows Azure Cloud Essentials
Health Event Resolved Resolved 9 minutes a... Wed Mar 1... Windows Azure Cloud Essentials
Health Event Updated Updated 9 minutes a... Wed Mar 1... Windows Azure Cloud Essentials
List keys Succeeded 10 minutes ... Wed Mar 1... Windows Azure Cloud Essentials
Backup Succeeded 10 minutes ... Wed Mar 1... Windows Azure Cloud Essentials
List Storage Account Keys Succeeded 10 minutes ... Wed Mar 1... Windows Azure Cloud Essentials

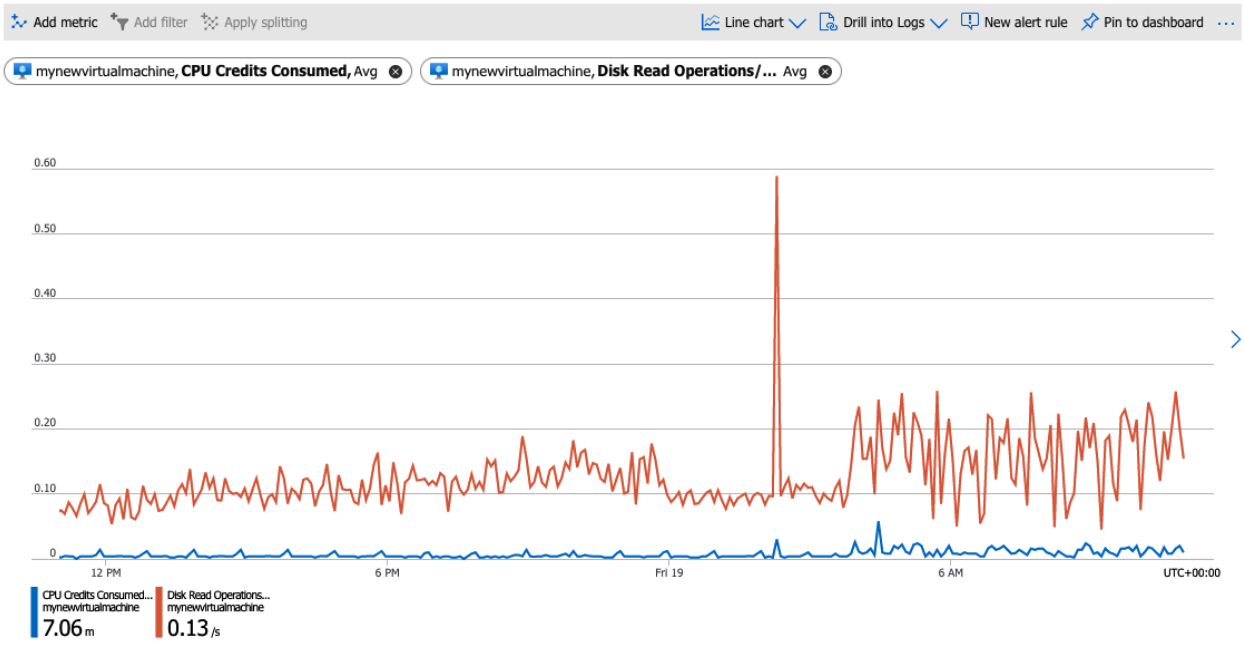
Create or Update Virtual Machine

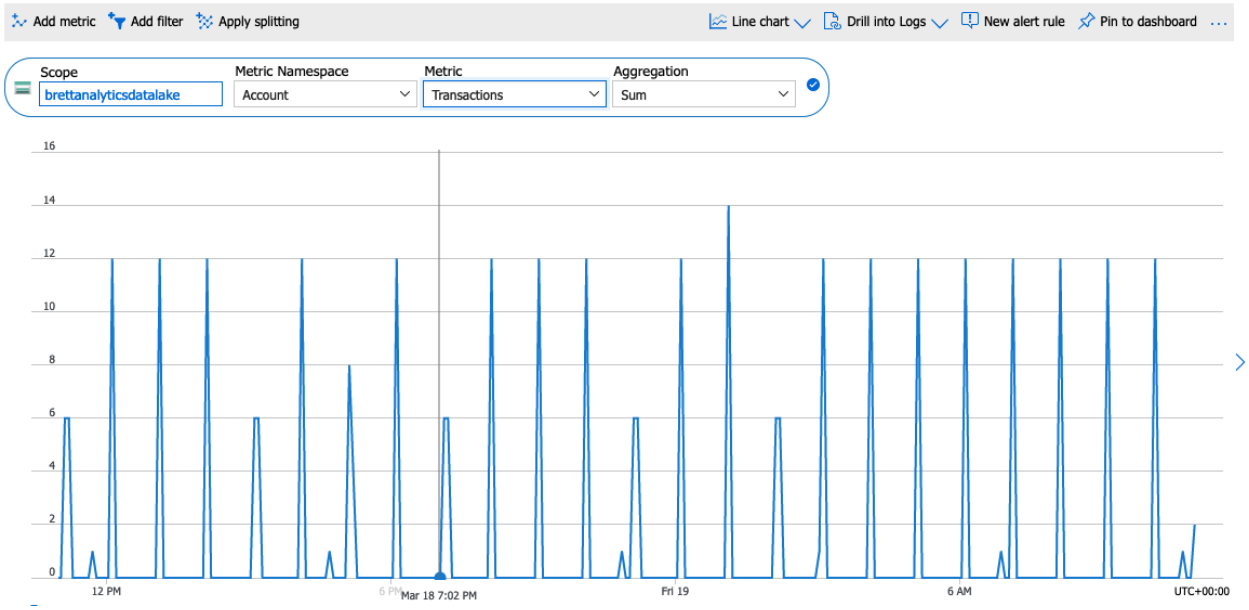
Wed Mar 17 2021 05:53:59 GMT+0000 (Greenwich Mean Time)

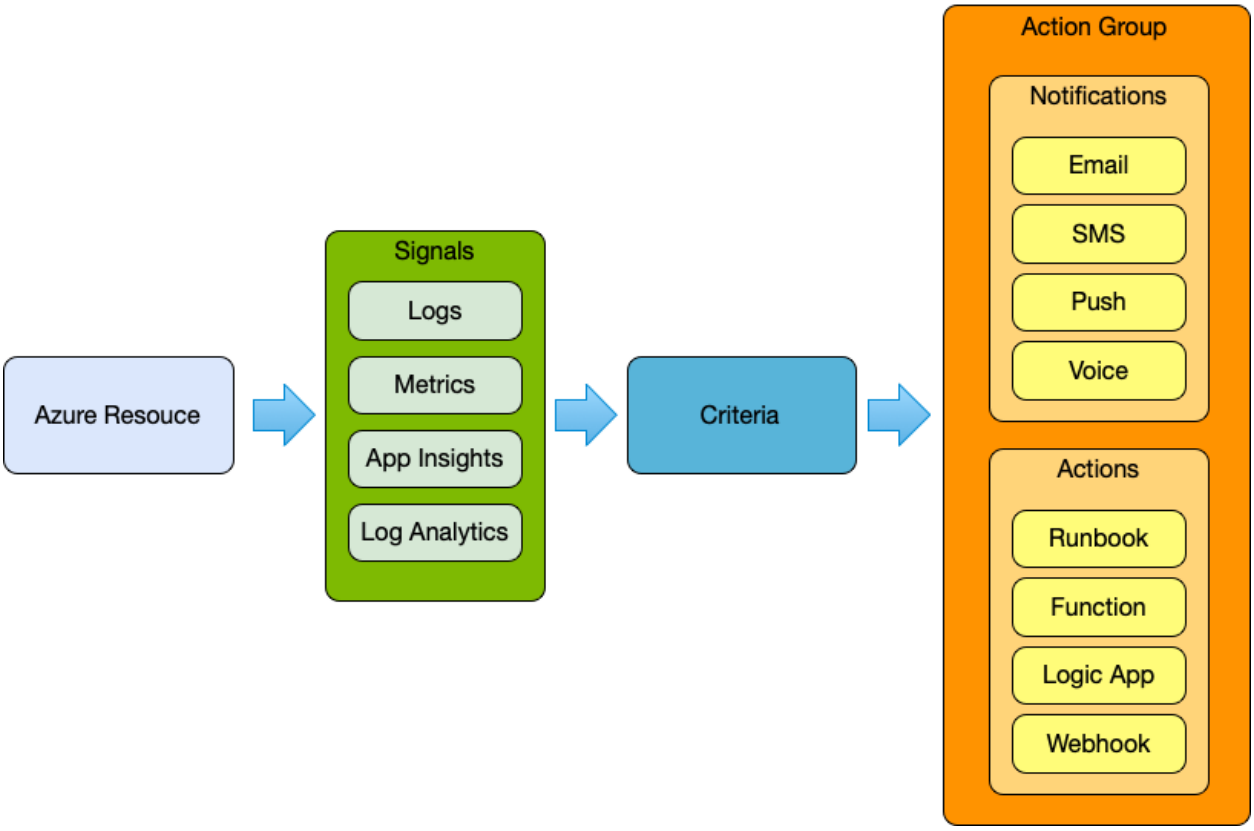
+ New alert rule

Summary | JSON | Change history (Preview)


```
{
    "authorization": {
        "action": "Microsoft.Compute/virtualMachines/write",
        "scope": "/subscriptions/[redacted]/resourceGroups/rsg-WinVMs/providers/Microsoft.Compute/virtualMachines/mynewvirtualmachine"
    },
    "caller": "[redacted]",
    "channels": "Operation",
```


Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Pin to dashboard
Scope
brettanalyticsdatalake
Metric Namespace
Account
Metric
Transactions
Aggregation
Sum
16
14
12
10
8
6
4
2
0
12 PM
Mar 18 7:02 PM
Fri 19
6 AM
UTC+00:00


Azure Resouce
Signals
Logs
Metrics
App Insights
Log Analytics
Criteria
Action Group
Notifications
Email
SMS
Push
Voice
Actions
Runbook
Function
Logic App
Webhook

Create alert rule

Rules management

Create an alert rule to identify and address issues when important conditions are found in your monitoring data. View tutorial + read more
When defining the alert rule, check that your inputs do not contain any sensitive content.

Scope

Select the target resource you wish to monitor.

Resource	Hierarchy
mynewvirtualmachine	Windows Azure Cloud Essentials > rsg-WinVMs

Edit resource

Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name
Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete Virtual Machine (Microsoft.Compute/virtualMachines)', Level='all', Status='all'

Add condition

You can define only one activity log signal per alert rule. To alert on more signals, create another alert rule.

Actions

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group. Learn more

Action group name	Contains actions
MyActionGroup	1 Email

Manage action groups

Alert rule details

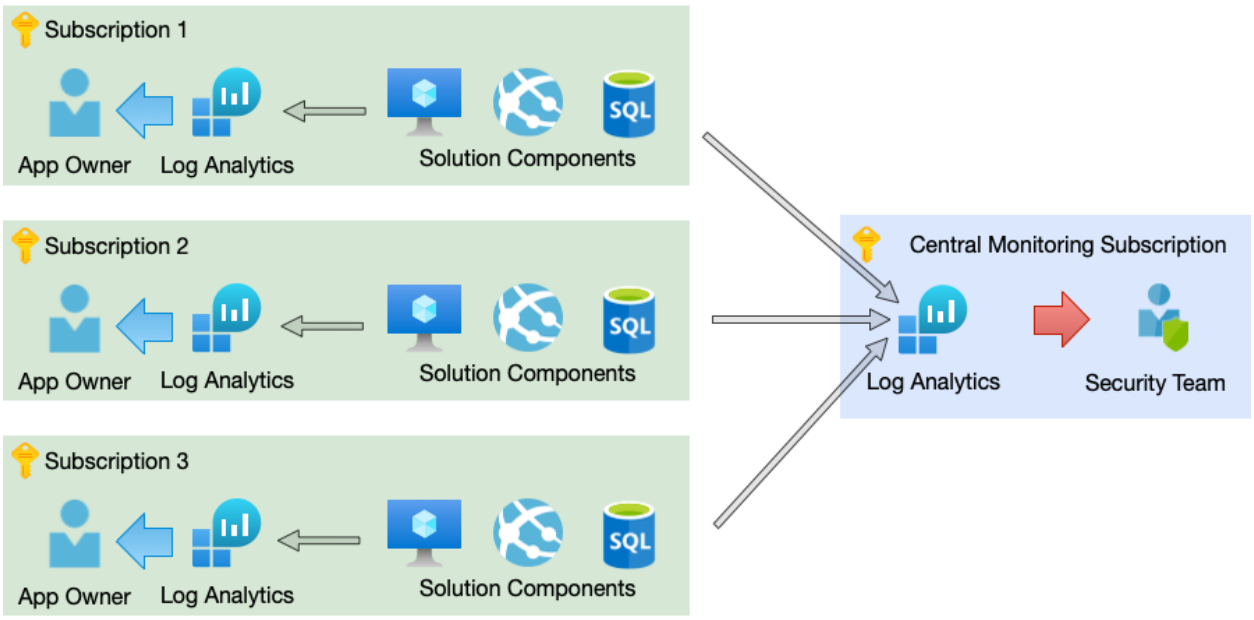
Provide details on your alert rule so that you can identify and manage it later.

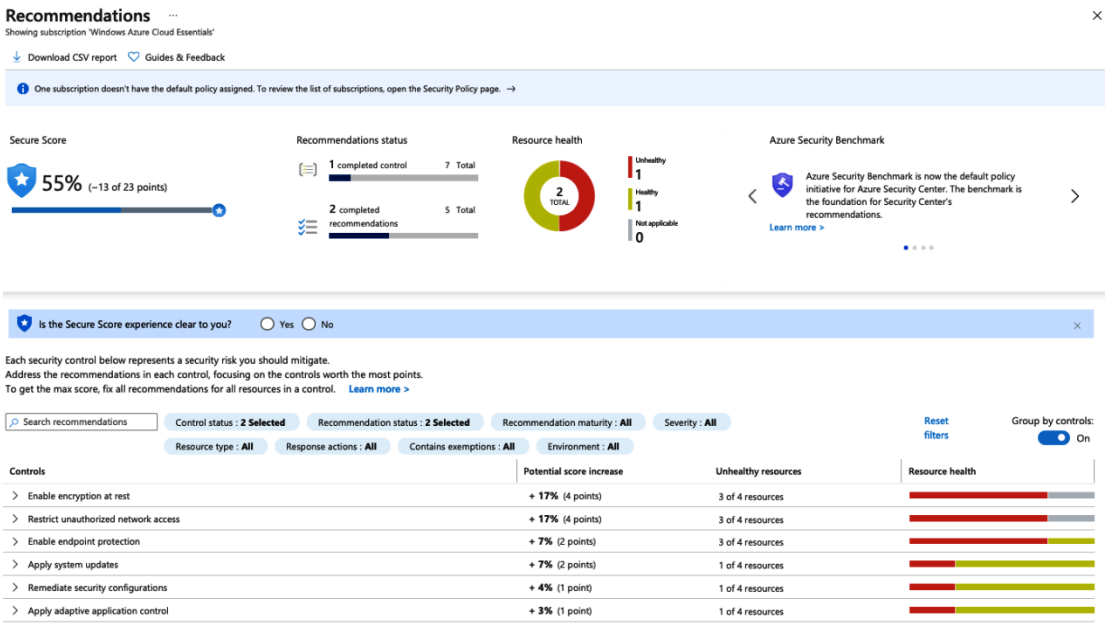
Alert rule name * : Specify the alert rule name

Description: Specify the alert rule description

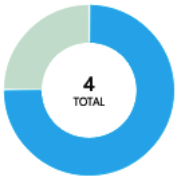
Save alert rule to resource group * : rsg-WinVMs

Enable alert rule upon creation


Subscription 1
App Owner
Log Analytics
Solution Components
Subscription 2
App Owner
Log Analytics
Solution Components
Subscription 3
App Owner
Log Analytics
Solution Components
Central Monitoring Subscription
Log Analytics
Security Team


Recommendations
Showing subscription 'Windows Azure Cloud Essentials'
Download CSV report
Guides & Feedback
One subscription doesn't have the default policy assigned. To review the list of subscriptions, open the Security Policy page.
Secure Score
55% (~13 of 23 points)
Recommendations status
1 completed control
7 Total
2 completed recommendations
5 Total
Resource health
2 TOTAL
Unhealthy 1
Healthy 1
Not applicable 0
Azure Security Benchmark
Azure Security Benchmark is now the default policy initiative for Azure Security Center. The benchmark is the foundation for Security Center's recommendations.
Learn more >
Is the Secure Score experience clear to you?
Yes
No
Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control.
Learn more >
Search recommendations
Control status : 2 Selected
Recommendation status : 2 Selected
Recommendation maturity : All
Severity : All
Resource type : All
Response actions : All
Contains exemptions : All
Environment : All
Reset filters
Group by controls: On
Controls
Potential score increase
Unhealthy resources
Resource health
Enable encryption at rest
+ 17% (4 points)
3 of 4 resources
Restrict unauthorized network access
+ 17% (4 points)
3 of 4 resources
Enable endpoint protection
+ 7% (2 points)
3 of 4 resources
Apply system updates
+ 7% (2 points)
1 of 4 resources
Remediate security configurations
+ 4% (1 point)
1 of 4 resources
Apply adaptive application control
+ 3% (1 point)
1 of 4 resources

Azure Defender coverage



1/1 Servers — Upgrade

1/1 Resource Manager subscriptions — Upgrade

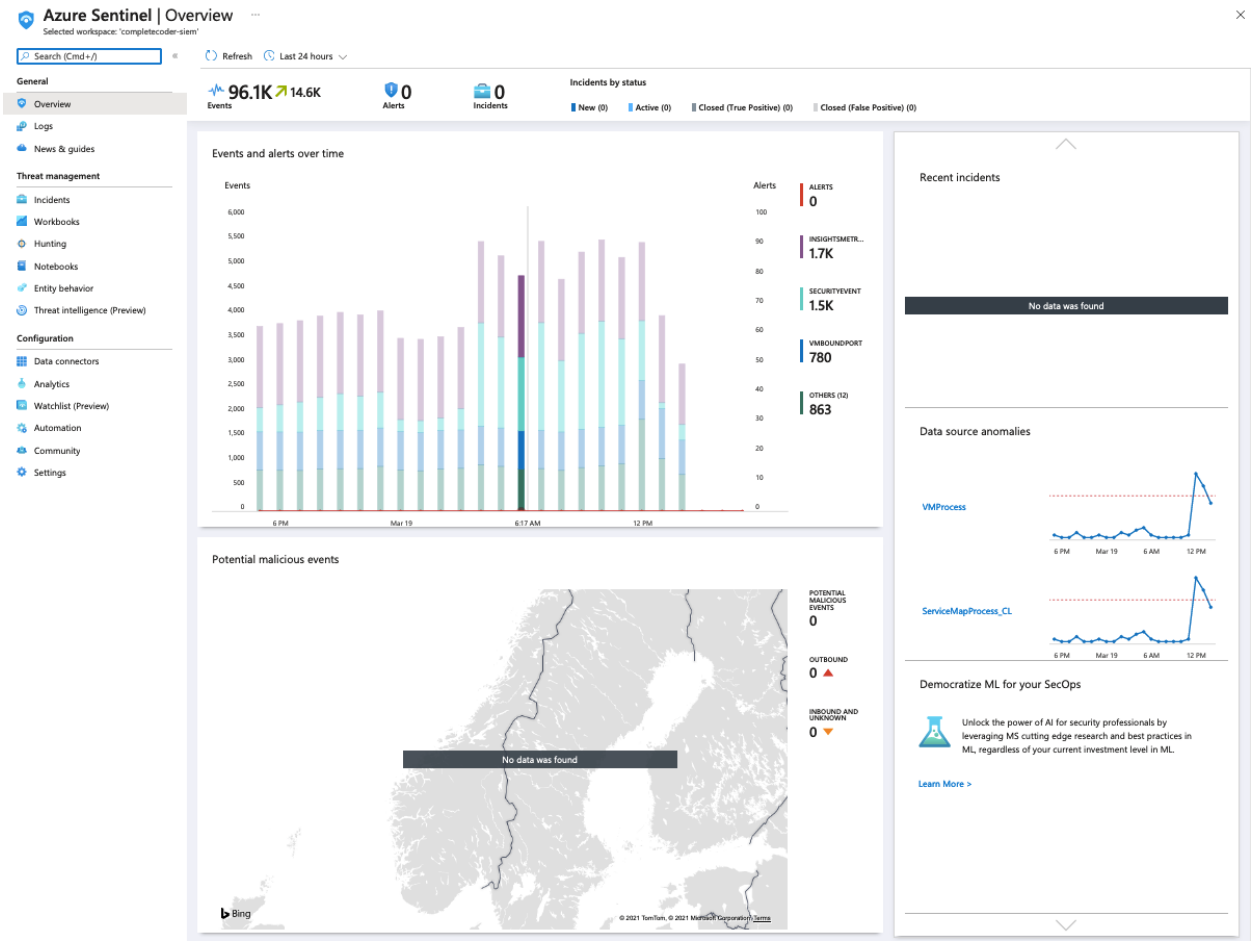
1/1 DNS subscriptions — Upgrade

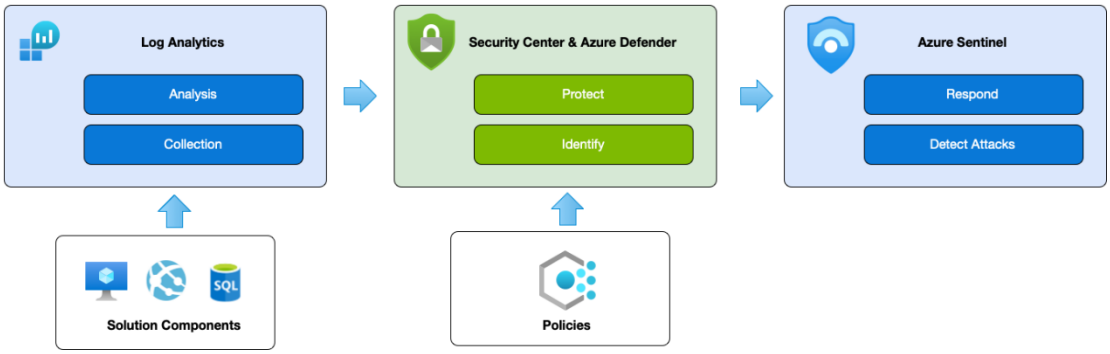
- Fully covered (75%)
- Agent not installed (25%) Install
- Not covered (0%)

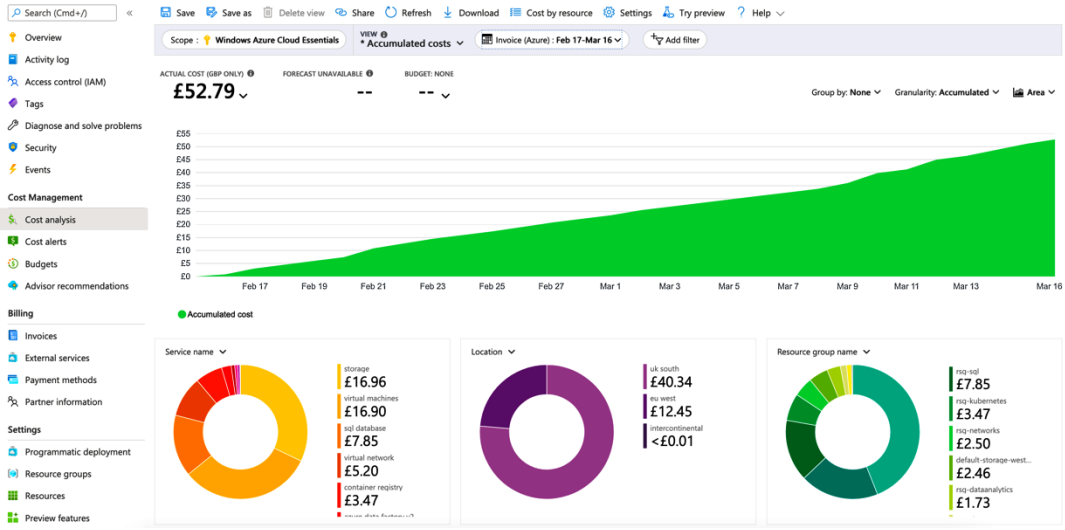
Advanced protection

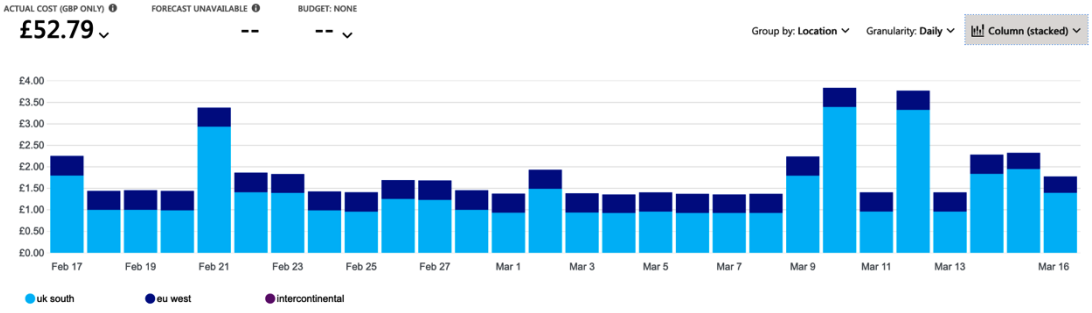
VM vulnerability assessment **1** Unprotected	Just-in-time VM access **None** Unprotected	Adaptive application control **None** Unprotected	Container image scanning **None** Unprotected	Adaptive network hardening **None** Unprotected
SQL vulnerability assessment **None** Unprotected	File integrity monitoring	Network map	IoT security	

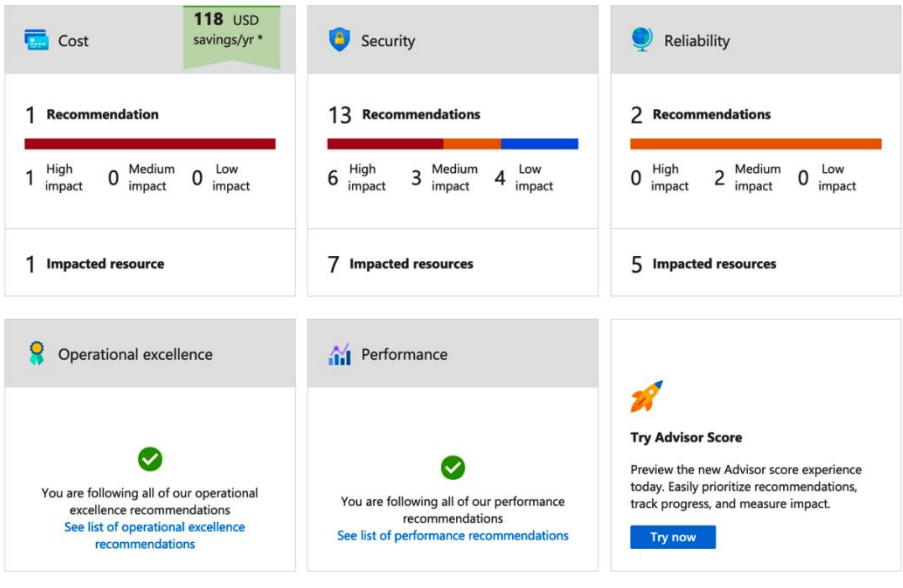
SEVERITY ↑↓	NAME ↑↓	RULE TYPE ↑↓	DATA SOURCES	TACTICS	CREATE RULE
High	Modified domain federation trust settings	Scheduled	Azure Active Directory	Credential Access	Create rule
High	First access credential added to Application or Service Principal where ...	Scheduled	Azure Active Directory	Credential Access	Create rule
High	Suspicious application consent similar to O365 Attack Toolkit	Scheduled	Azure Active Directory		Create rule
High	IN USE Known IRIDIUM IP	Scheduled	Office 365 +7	Command and Control	Create rule
High	Known Barium IP	Scheduled	Office 365 +8	Command and Control	Create rule
Medium	Brute force attack against Azure Portal	Scheduled	Azure Active Directory	Credential Access	Create rule
Medium	MFA disabled for a user	Scheduled	Azure Active Directory +1	Credential Access	Create rule


Azure Sentinel | Overview
Selected workspace: 'completecoder-siem'
Search (Cmd+/)
Refresh
Last 24 hours
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence (Preview)
Configuration
Data connectors
Analytics
Watchlist (Preview)
Automation
Community
Settings
96.1K 14.6K
Events
0
Alerts
0
Incidents
Incidents by status
New (0)
Active (0)
Closed (True Positive) (0)
Closed (False Positive) (0)
Events and alerts over time
Events
Alerts
ALERTS
0
INSIGHTSMETR...
1.7K
SECURITYEVENT
1.5K
VMBOUNDPORT
780
OTHERS (12)
863
Recent incidents
No data was found
Data source anomalies
VMProcess
ServiceMapProcess_CL
Democratize ML for your SecOps
Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.
Learn More >
Potential malicious events
No data was found
POTENTIAL MALICIOUS EVENTS
0
OUTBOUND
0
INBOUND AND UNKNOWN
0
Bing


Log Analytics
Analysis
Collection
Security Center & Azure Defender
Protect
Identify
Azure Sentinel
Respond
Detect Attacks
Solution Components
Policies


Search (Cmd+/)
Save
Save as
Delete view
Share
Refresh
Download
Cost by resource
Settings
Try preview
Help
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events
Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations
Billing
Invoices
External services
Payment methods
Partner information
Settings
Programmatic deployment
Resource groups
Resources
Preview features
Scope : Windows Azure Cloud Essentials
VIEW * Accumulated costs
Invoice (Azure) : Feb 17-Mar 16
Add filter
ACTUAL COST (GBP ONLY)
£52.79
FORECAST UNAVAILABLE
--
BUDGET: NONE
--
Group by: None
Granularity: Accumulated
Area
£55
£50
£45
£40
£35
£30
£25
£20
£15
£10
£5
£0
Feb 17
Feb 19
Feb 21
Feb 23
Feb 25
Feb 27
Mar 1
Mar 3
Mar 5
Mar 7
Mar 9
Mar 11
Mar 13
Mar 16
Accumulated cost
Service name
storage
£16.96
virtual machines
£16.90
sql database
£7.85
virtual network
£5.20
container registry
£3.47
Location
uk south
£40.34
eu west
£12.45
intercontinental
<£0.01
Resource group name
rsq-sql
£7.85
rsq-kubernetes
£3.47
rsq-networks
£2.50
default-storage-west...
£2.46
rsq-dataanalytics
£1.73


ACTUAL COST (GBP ONLY)
£52.79
FORECAST UNAVAILABLE
--
BUDGET: NONE
--
Group by: Location
Granularity: Daily
Column (stacked)
£4.00
£3.50
£3.00
£2.50
£2.00
£1.50
£1.00
£0.50
£0.00
Feb 17
Feb 19
Feb 21
Feb 23
Feb 25
Feb 27
Mar 1
Mar 3
Mar 5
Mar 7
Mar 9
Mar 11
Mar 13
Mar 16
uk south
eu west
intercontinental


Cost
118 USD savings/yr *
1 Recommendation
1 High impact
0 Medium impact
0 Low impact
1 Impacted resource
Security
13 Recommendations
6 High impact
3 Medium impact
4 Low impact
7 Impacted resources
Reliability
2 Recommendations
0 High impact
2 Medium impact
0 Low impact
5 Impacted resources
Operational excellence
You are following all of our operational excellence recommendations
See list of operational excellence recommendations
Performance
You are following all of our performance recommendations
See list of performance recommendations
Try Advisor Score
Preview the new Advisor score experience today. Easily prioritize recommendations, track progress, and measure impact.
Try now

Total recommendations
1

Recommendations by impact

1 High impact | 0 Medium impact | 0 Low impact

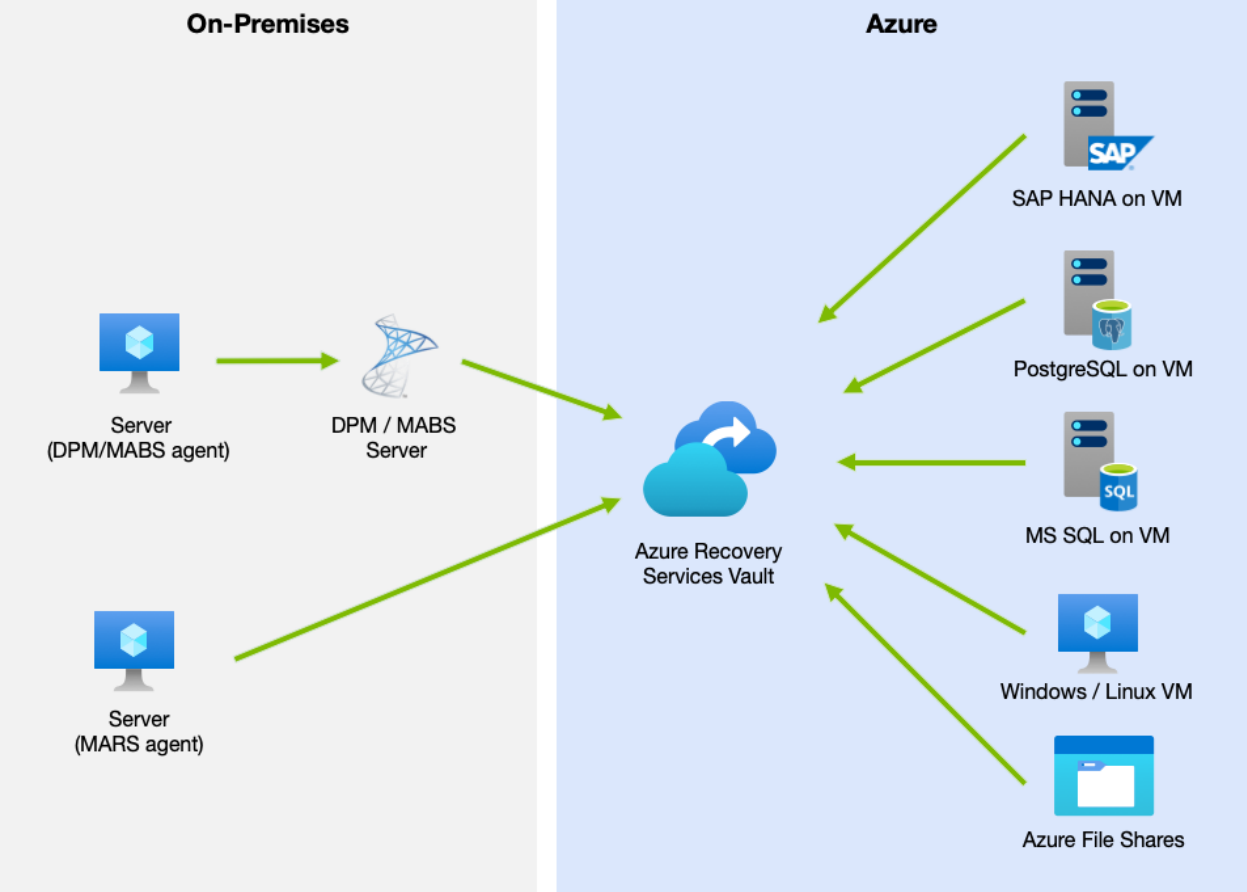
Impacted resources
1

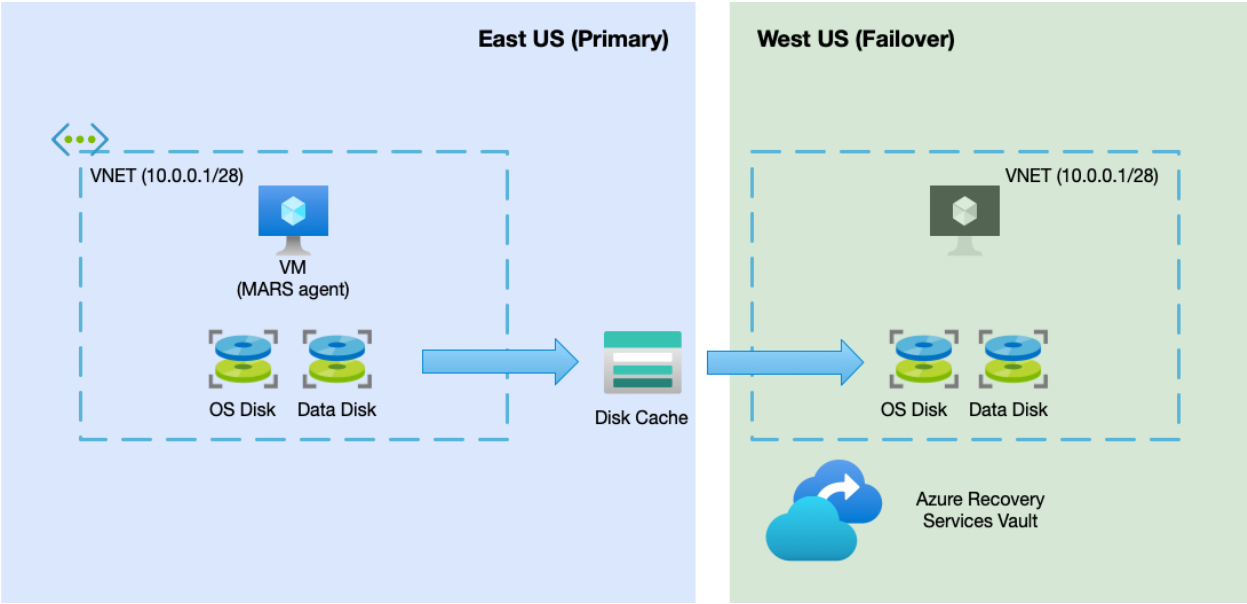
Potential yearly savings
118 USD

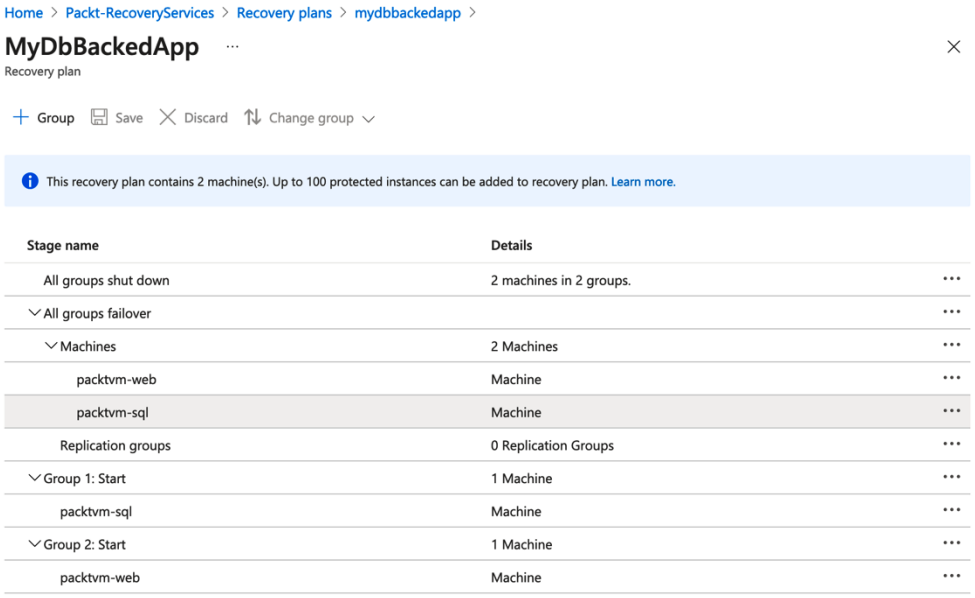
For more cost management and optimization capabilities, visit Azure Cost Management

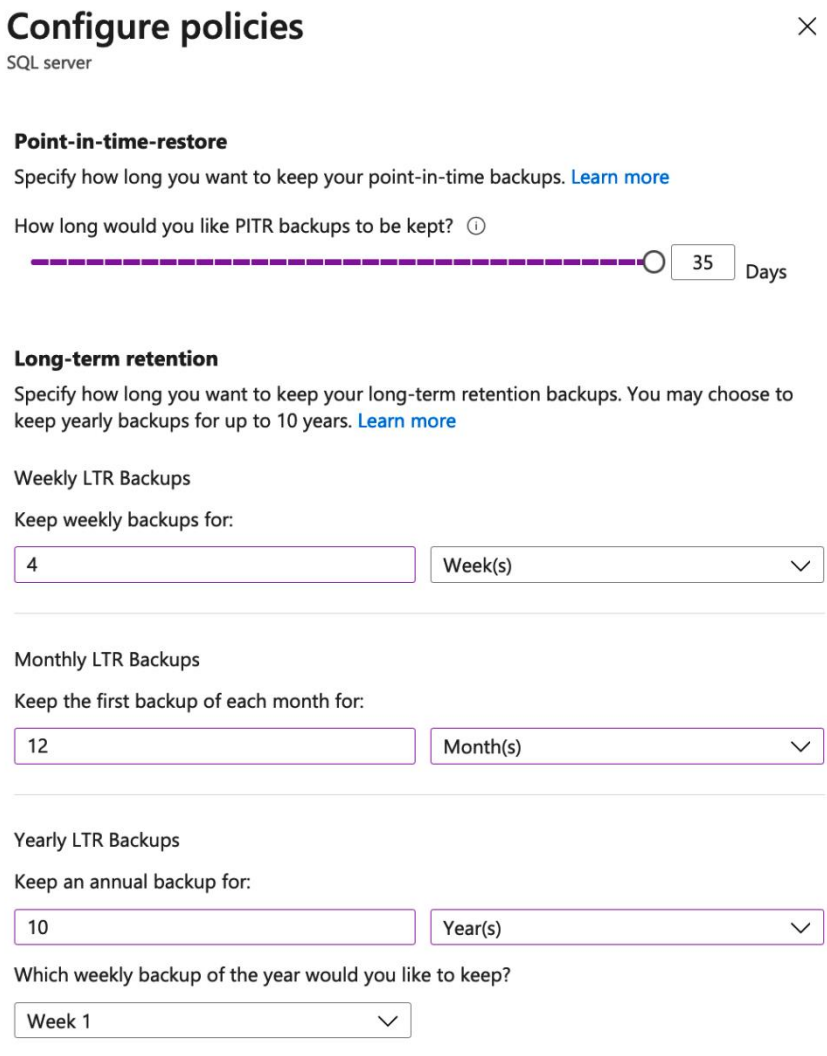
Impact	Description	Potential yearly savings	Impacted resources	Last updated
High	Buy virtual machine reserved instances to save money over pay-as-you-go costs	118.23 USD	1 Virtual machine	21/3/2021, 08:03

Chapter 16: Developing Business Continuity






Home > Packt-RecoveryServices > Recovery plans > mydbbackedapp >
MyDbBackedApp
Recovery plan
Group
Save
Discard
Change group
This recovery plan contains 2 machine(s). Up to 100 protected instances can be added to recovery plan. Learn more.
Stage name
Details
All groups shut down
2 machines in 2 groups.
All groups failover
Machines
2 Machines
packtvm-web
Machine
packtvm-sql
Machine
Replication groups
0 Replication Groups
Group 1: Start
1 Machine
packtvm-sql
Machine
Group 2: Start
1 Machine
packtvm-web
Machine


Configure policies
SQL server
Point-in-time-restore
Specify how long you want to keep your point-in-time backups. Learn more
How long would you like PITR backups to be kept?
35
Days
Long-term retention
Specify how long you want to keep your long-term retention backups. You may choose to keep yearly backups for up to 10 years. Learn more
Weekly LTR Backups
Keep weekly backups for:
4
Week(s)
Monthly LTR Backups
Keep the first backup of each month for:
12
Month(s)
Yearly LTR Backups
Keep an annual backup for:
10
Year(s)
Which weekly backup of the year would you like to keep?
Week 1

Backup Interval

How often would you like your backups to be performed?

240 Minute(s)

60-1440

Backup Retention

How long would you like your backups to be saved?

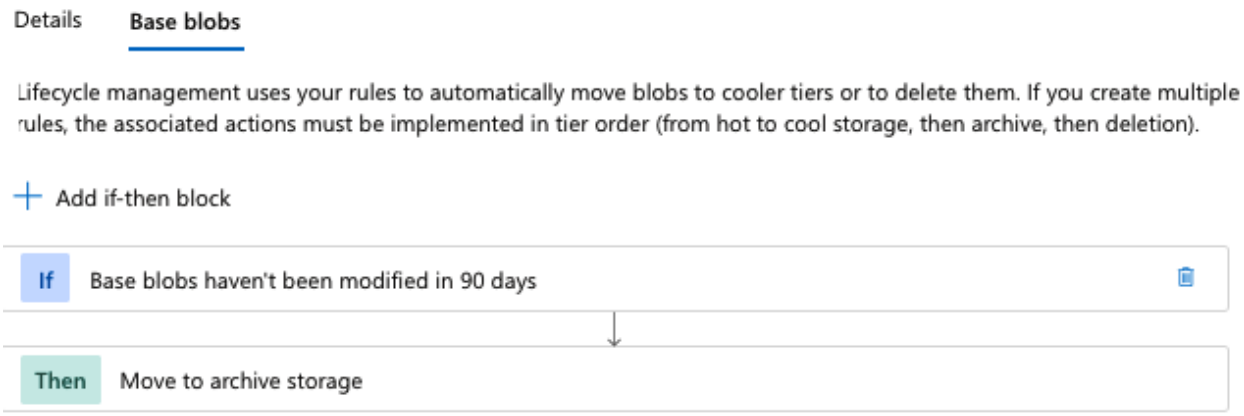
8 Hours(s)

8-720

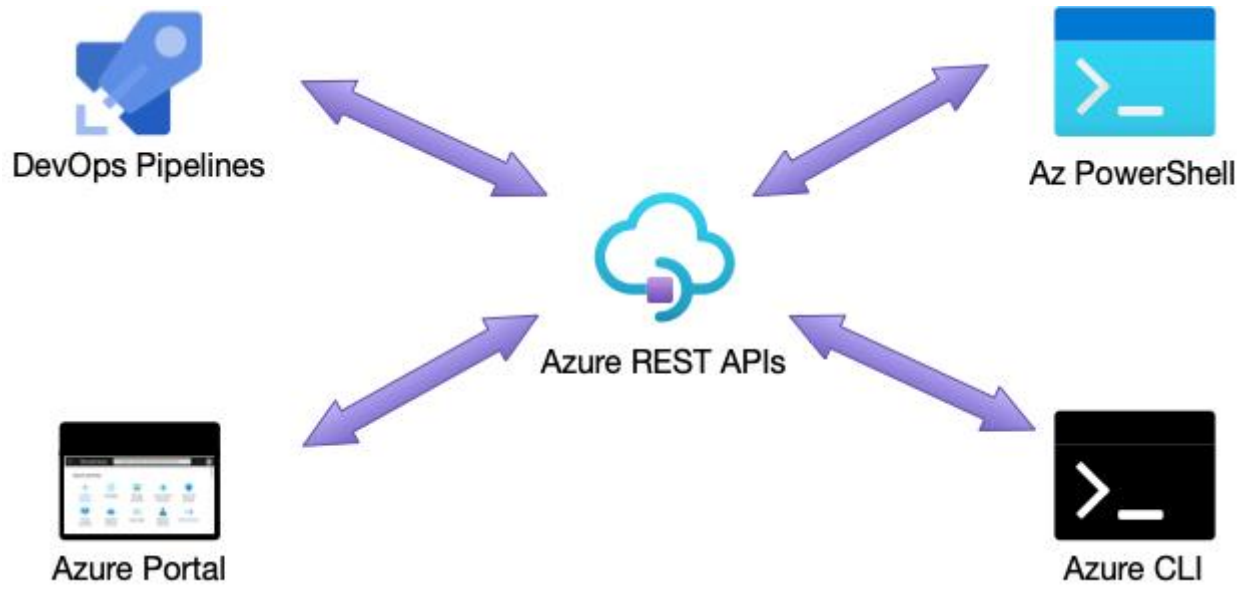
Copies of data retained 2

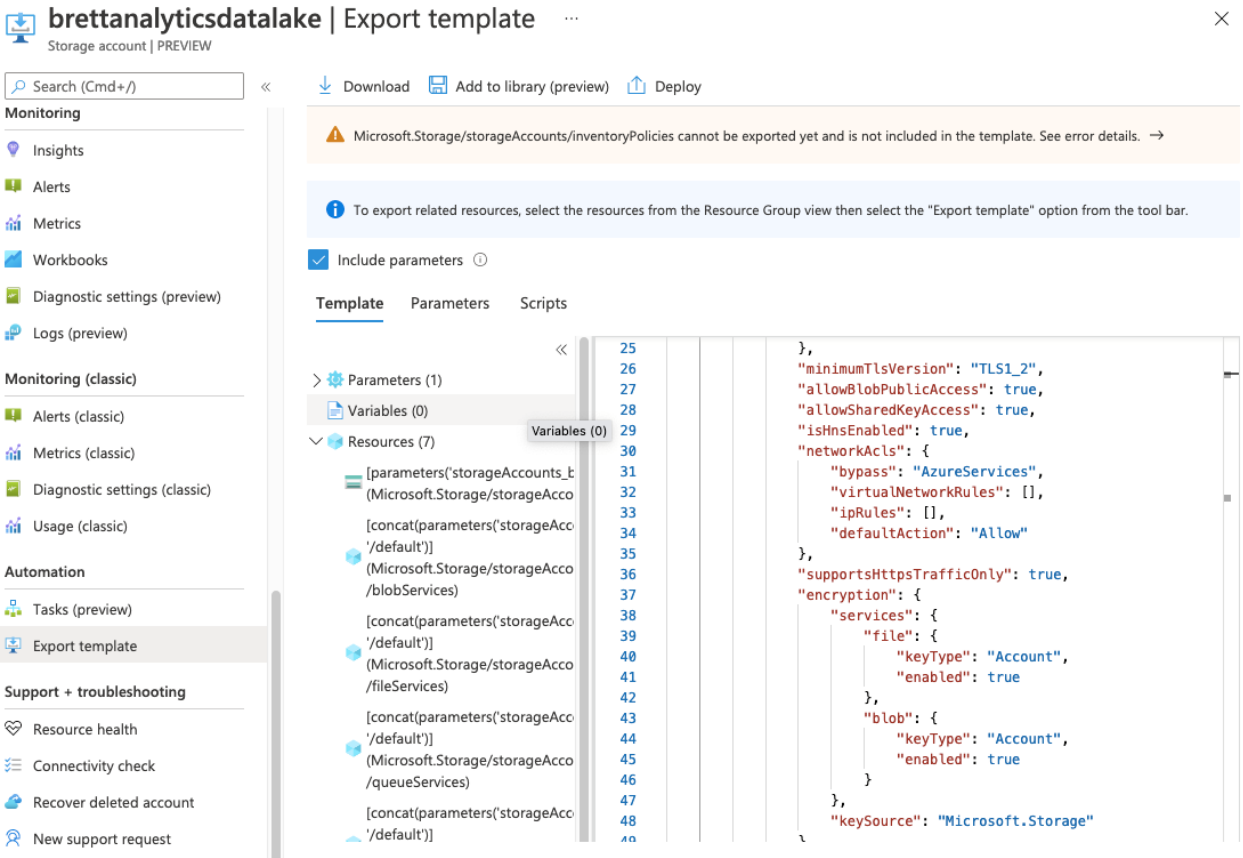
Backup storage redundancy *

- (•) Geo-redundant backup storage
- ( ) Zone-redundant backup storage
- ( ) Locally-redundant backup storage



Chapter 17: Scripted Deployments and DevOps Automation





Custom deployment

Deploy from a custom template

TEMPLATE

3 resources

Edit template | Edit paramet... | Learn more

BASICS

Subscription * PacktPub

Resource group * (New) Packt-Storage-RSG

Create new

Location * (Europe) UK South

SETTINGS

Storage Accounts_name * MyNewStorageAccount

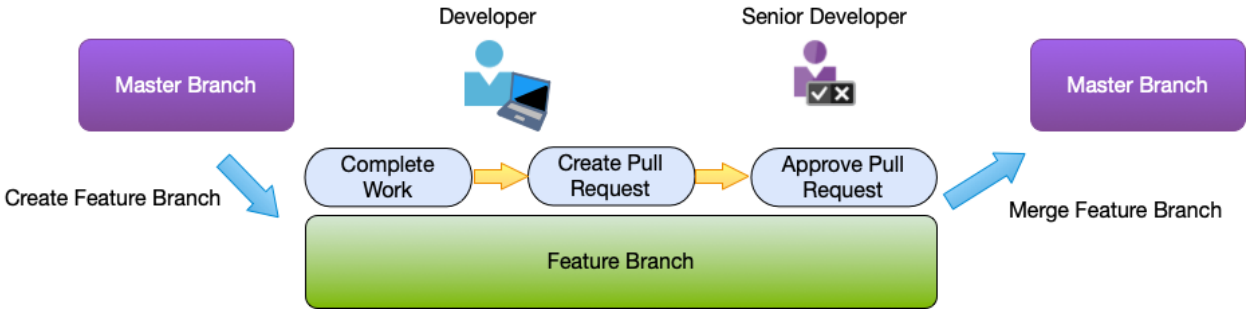
TERMS AND CONDITIONS

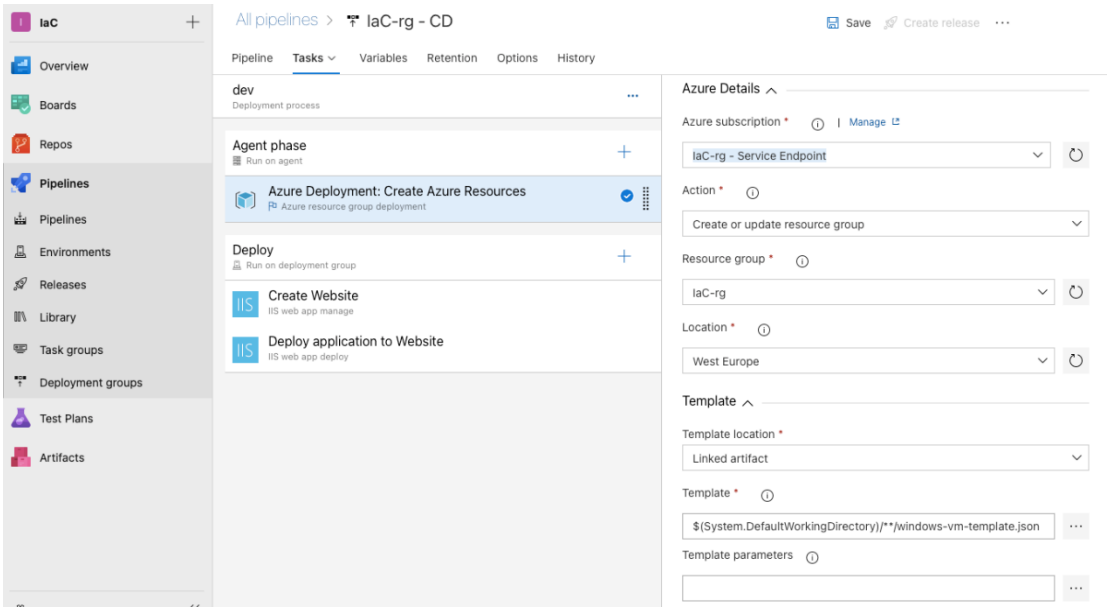
Azure Marketplace Terms | Azure Marketplace

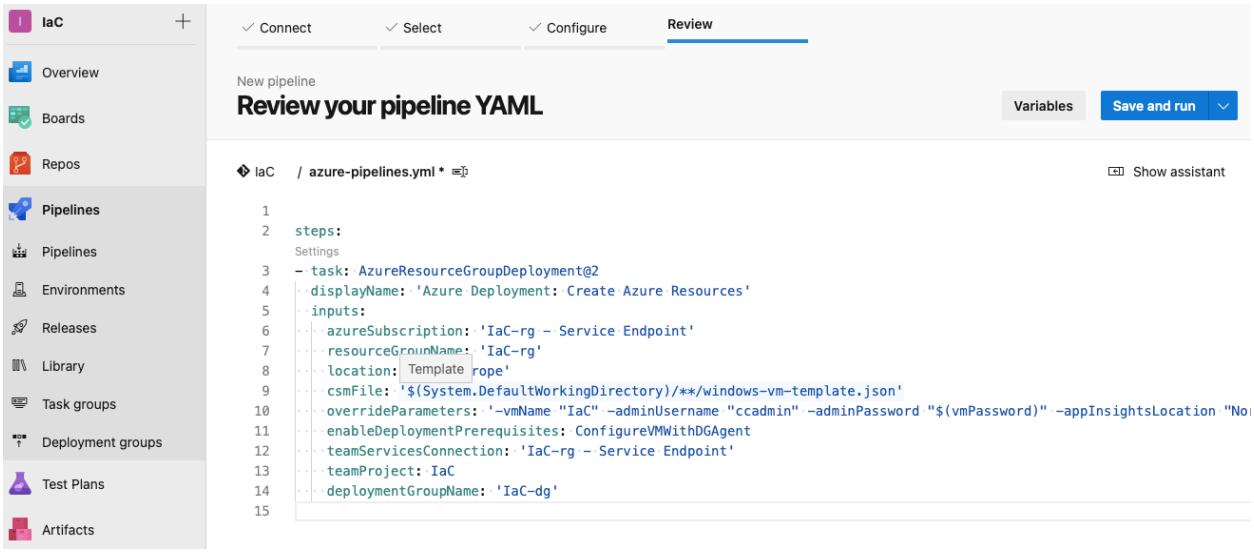
By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such

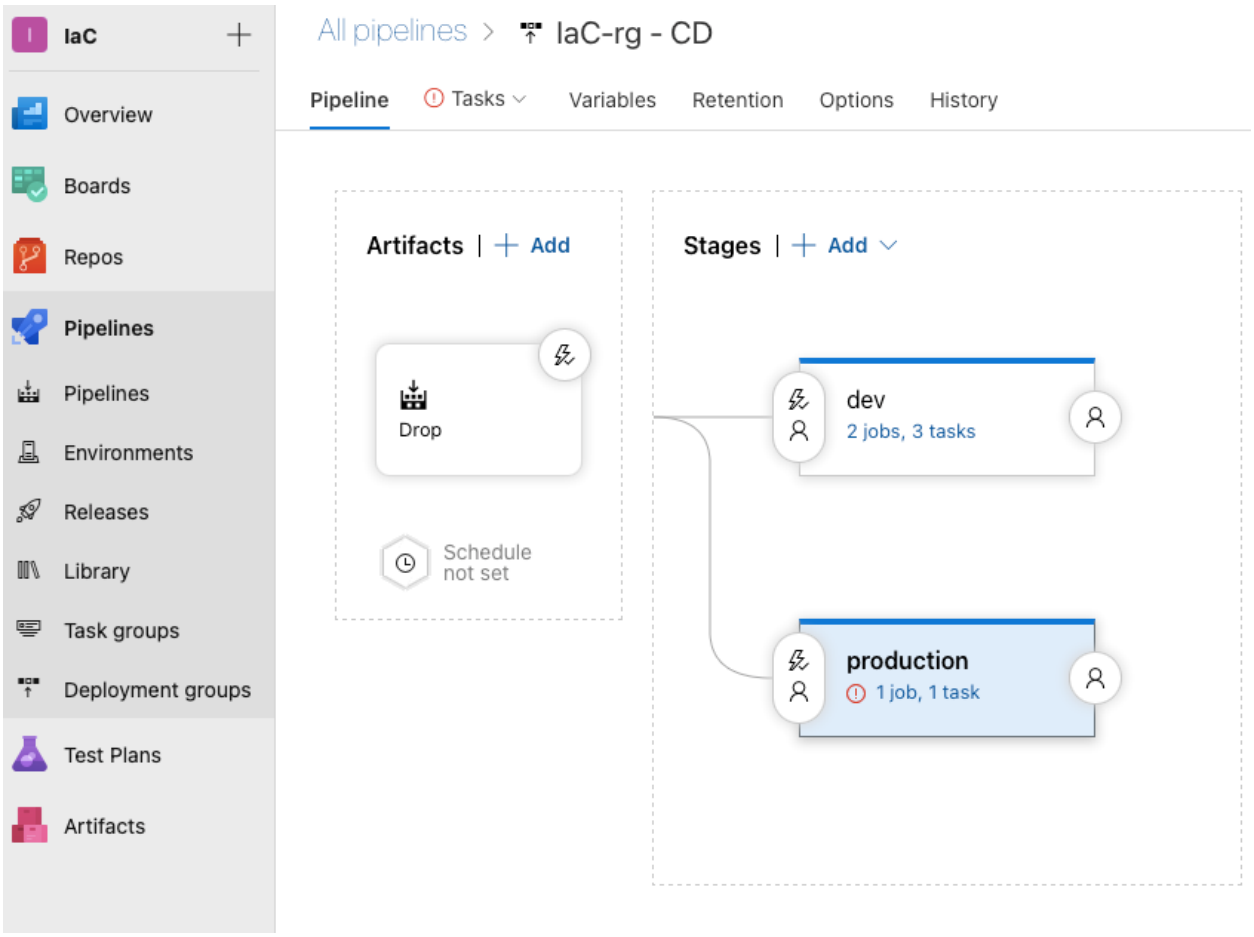
☑ I agree to the terms and conditions stated above

Purchase

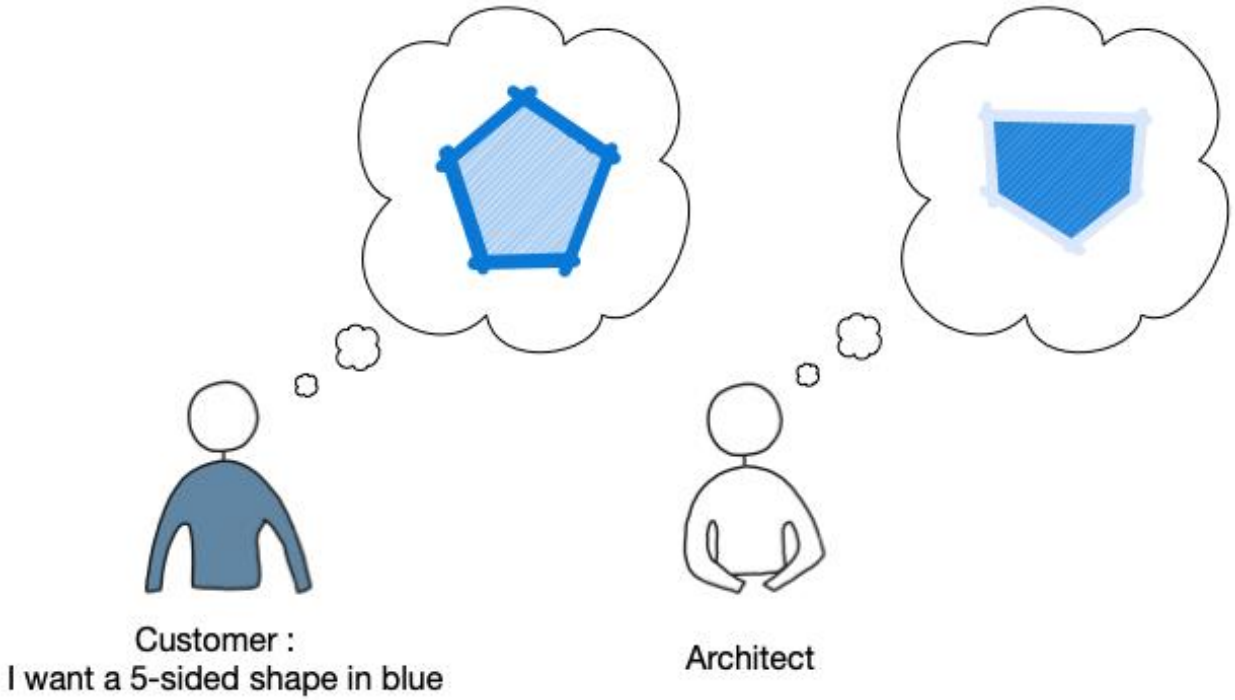
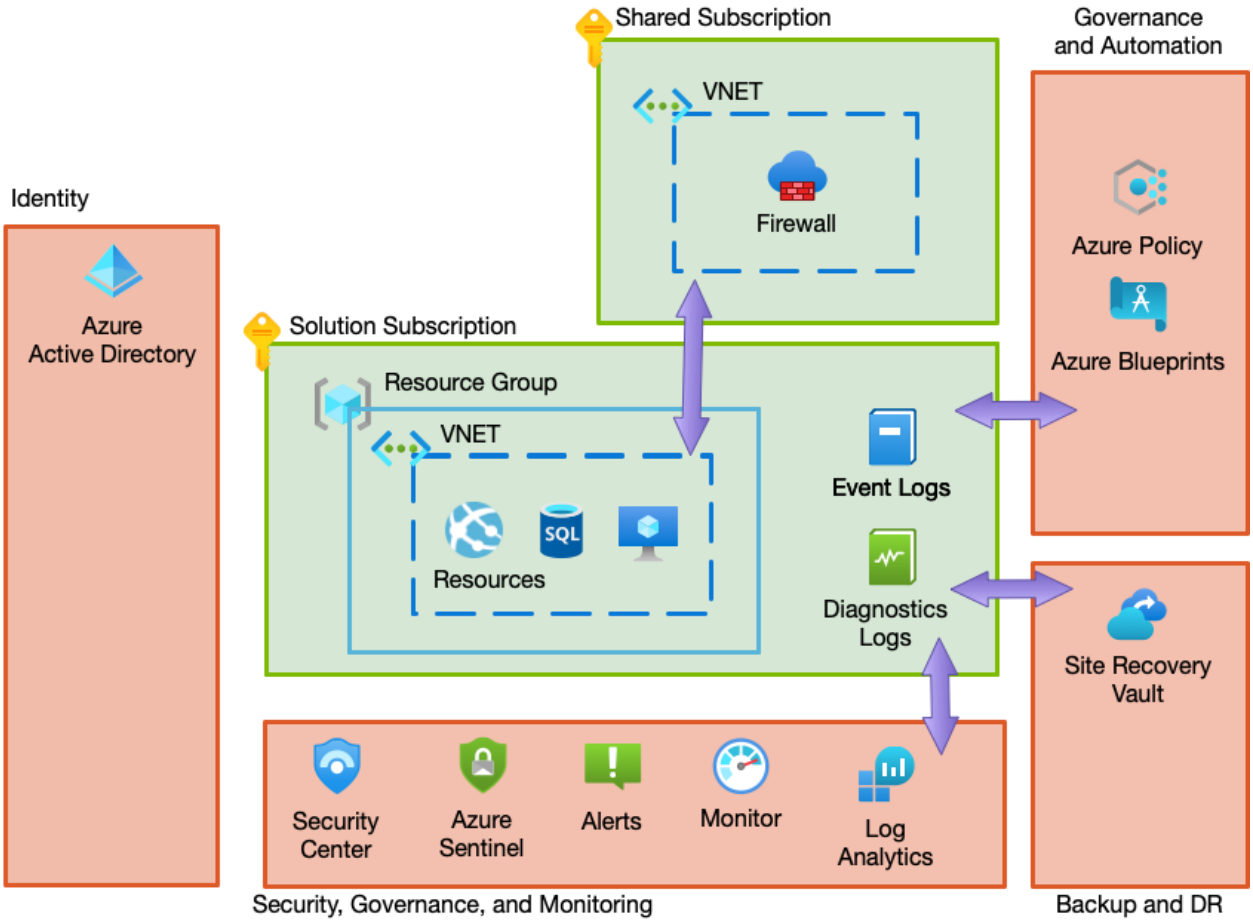



IaC
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Artifacts
All pipelines > IaC-rg - CD
Save
Create release
Pipeline
Tasks
Variables
Retention
Options
History
dev
Deployment process
Agent phase
Run on agent
Azure Deployment: Create Azure Resources
Azure resource group deployment
Deploy
Run on deployment group
Create Website
IIS web app manage
Deploy application to Website
IIS web app deploy
Azure Details
Azure subscription *
Manage
IaC-rg - Service Endpoint
Action *
Create or update resource group
Resource group *
IaC-rg
Location *
West Europe
Template
Template location *
Linked artifact
Template *
$(System.DefaultWorkingDirectory)/**/windows-vm-template.json
Template parameters


IaC
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Artifacts
Connect
Select
Configure
Review
New pipeline
Review your pipeline YAML
Variables
Save and run
IaC / azure-pipelines.yml *
Show assistant
steps:
Settings
- task: AzureResourceGroupDeployment@2
displayName: 'Azure Deployment: Create Azure Resources'
inputs:
azureSubscription: 'IaC-rg - Service Endpoint'
resourceGroupName: 'IaC-rg'
location: rope'
Template
csmFile: '$(System.DefaultWorkingDirectory)/**/windows-vm-template.json'
overrideParameters: '-vmName "IaC" -adminUsername "ccadmin" -adminPassword "$(vmPassword)" -appInsightsLocation "No
enableDeploymentPrerequisites: ConfigureVMWithDGAgent
teamServicesConnection: 'IaC-rg - Service Endpoint'
teamProject: IaC
deploymentGroupName: 'IaC-dg'


IaC
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Releases
Library
Task groups
Deployment groups
Test Plans
Artifacts
All pipelines
IaC-rg - CD
Pipeline
Tasks
Variables
Retention
Options
History
Artifacts | Add
Drop
Schedule not set
Stages | Add
dev
2 jobs, 3 tasks
production
1 job, 1 task

Chapter 18: Engaging with Real-World Customers



Chapter 19: Enterprise Design Considerations