Deploy and Manage Azure Compute services

Azure Virtual Machines

Custom Script Extensions

This tool can be used on Azure virtual machines to download and execute scripts.

This is ideal when you want to deploy any custom configuration of any software installation on a virtual machine.

The scripts can be located in an Azure storage account or even in GitHub.

A time duration of 90 minutes is allowed for the script to run. Any longer and the result will be a failed extension provision.

It’s ideal not to place reboots inside the script, because the extension will not continue after the reboot. Hence if you have other commands that need to run via the extension after the reboot , they won’t run.

Custom Script Extensions

If your script does need a reboot , then maybe you can look at other tools such as Desired State Configuration, Chef or Puppet.

The script will run only once.

The Custom Script Extension will run under the impersonation of the LocalSystem Account.

Proximity Placement groups

- Normally when you create multiple virtual machines or virtual machines that are part of a virtual machine scale set, these machines could be located on different physical servers.
- Sometimes an application/system that uses multiple virtual machines , want the virtual machines to be located closer together to get least latency when it comes to communication between the virtual machines.
- By placing the virtual machines as part of a proximity group, the virtual machines will be physically located close to each other.

Proximity Placement groups

- When using proximity placement groups, ensure the virtual machines have accelerated networking enabled. This also helps to improve network performance.

- When deploying VM’s from different families or SKU’s , try to deploy them as part of a single template. This will increase the probability of ensuring all VM’s are deployed successfully.

- A proximity placement group is assigned to a data center when the first resource (VM) is being deployed and released once the last resource is being deleted or stopped.

Azure Web App Logging

Azure Web App Logging

- You get a set of logging features that are available for the Azure Web App.
- The different types of logging that are available are
- **Application Logging** – This captures log messages that are generated by your application code.
- **Web server logging** – This records raw HTTP request data.

Azure Web App Logging

- **Detailed Error Messages** – This stores copies of the .htm error pages that would have been sent to the client browser.
- **Deployment logging** – These are logs when you publish content to an application.
- You can also stream logs in real time.

Azure Web App Backups

Azure Web App Backups

- The backup feature that is available with Azure Web App can be used to create backups of your web app.
- The backups are stored in an Azure storage account.
- Here the App configuration, the file content and the database connected to the application get backed up.
- To use the Backup and Restore feature, the App Service Plan needs to be in the Standard, Premium or Isolated tier.
- Backups of the app + database can be up to a maximum of 10 GB.

Configure and manage Virtual networking

Network Watcher Service

Network Watcher service

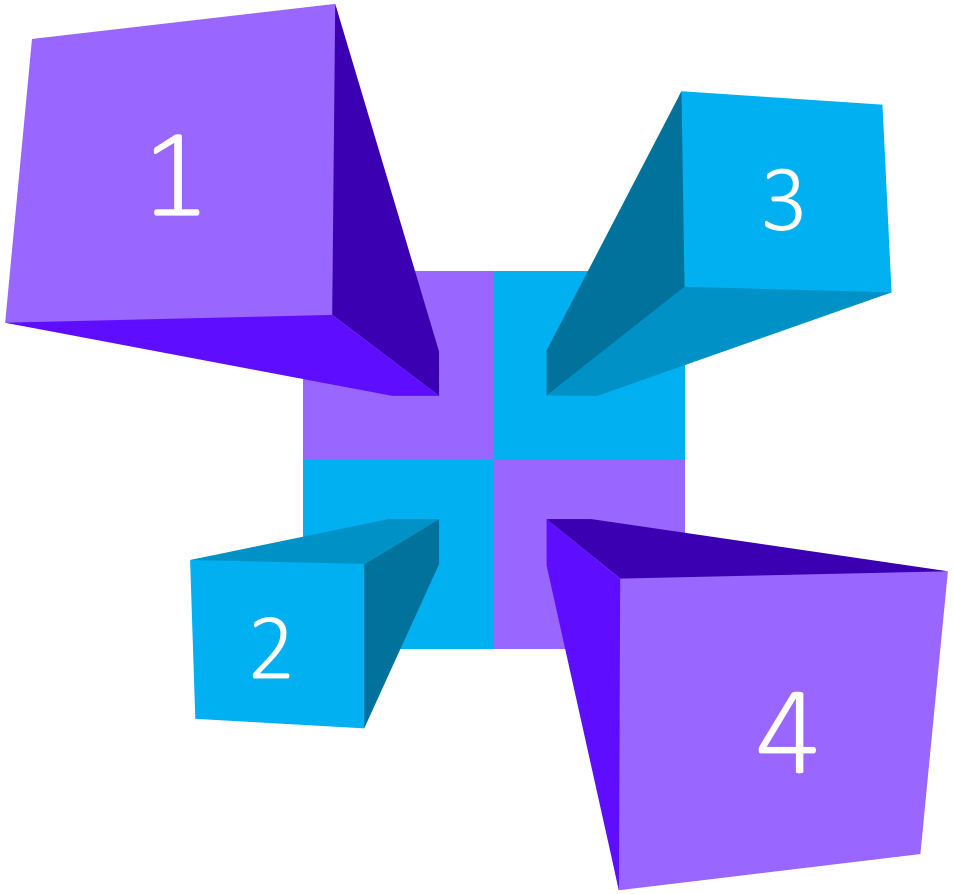
Network Watcher Service

Connection Monitor

Check the network connectivity between machines. These can be in Azure or on your on-premises environments.

Next hop

Here you can see the next route for a packet of data. This helps you understand whether the packet is being routed to the correct destination.



IP Flow Verify

This can be used to check if a packet is allowed or denied to or from a virtual machine. If a packet is being denied by a security group, you can see which rule is denying the packet.

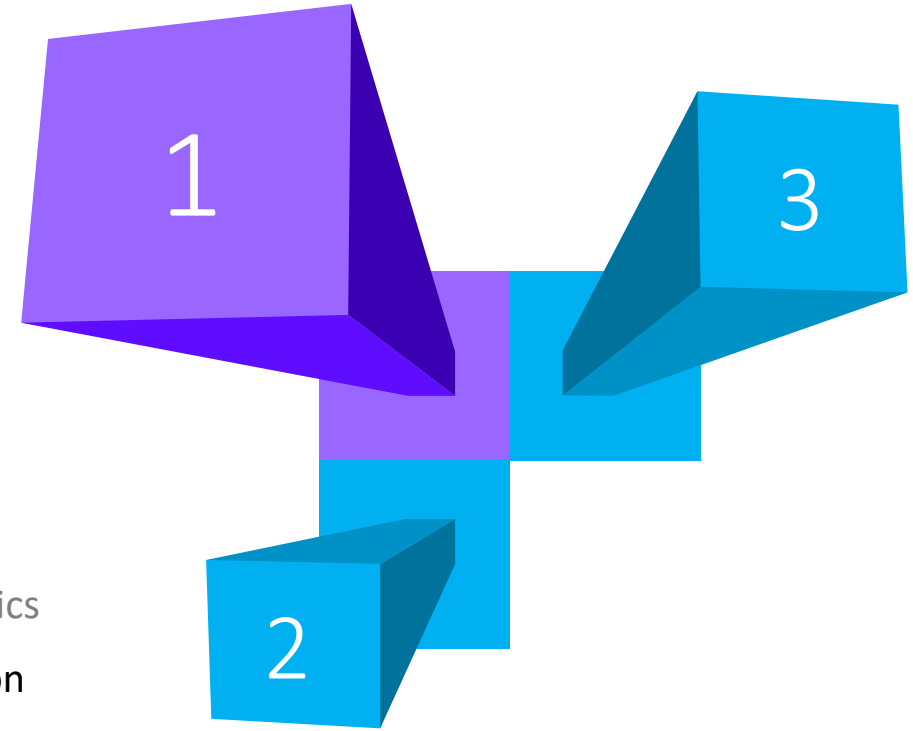
Connection troubleshoot

Check the connection from a virtual machine to a virtual machine, fully qualified domain name, URI or IPv4 address.

Network Watcher service

NSG Diagnostic

Provides detailed information that helps to understand and debug the security configuration of the network.



NSG Flow Logs

Helps to provide visibility into user and application activity in cloud networks.

Traffic Analytics

This helps to log information about the IP traffic that is flowing through an NSG.

Network Watcher Service

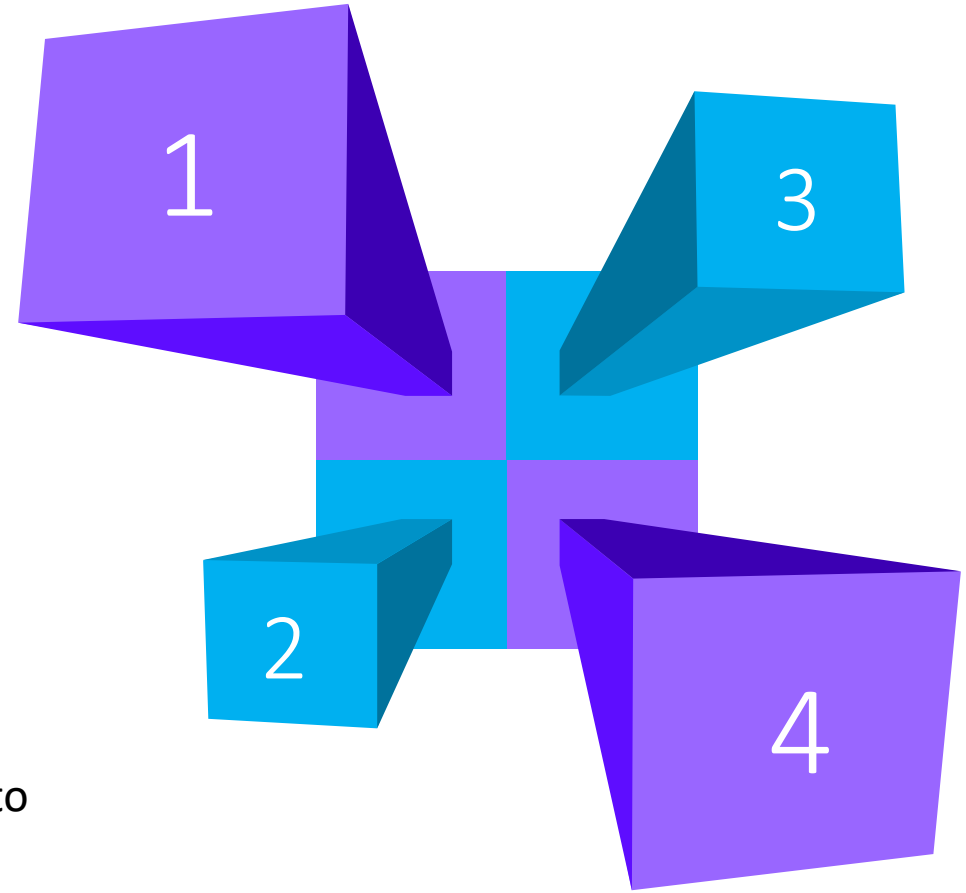
Summary

Virtual Network

Virtual Network

Isolated

This is an isolated network on Azure cloud.



Resources

You can then place resources such as Azure virtual machines within the virtual network.

Managed

Here you don’t need to deploy an infrastructure to have a network in place.

Internet

By default all resources in the virtual network can communicate outbound with the internet.

Summary

IP Addresses

- **Private IP addresses** – These allow communication between resources such as Azure virtual machines without the need of assigning Public IP addresses.
- **Public IP addresses** – These allow Internet resources to communicate inbound onto Azure resources such as Azure virtual machines.
- Public IP addresses - Static - The IP address is assigned the time the resource is created.
- Public IP addresses - Dynamic - The IP address is allocated when it is assigned to a resource. Also, the IP address is released when you stop or delete the resource.

Network Security Groups

- This is used to filter network traffic in an Azure virtual network.
- You define different rules as part of the Network Security Group. You have Inbound and Outbound rules.
- For each rule you mention the source and destination of traffic, the port and protocol.

Application Security Groups

- This is used when you want to apply network filtering rules for a group of machines.
- Instead of mentioning the IP address of the machine, you can make the machine part of an Application Security Group.
- And then you can mention the Application Security Group in the Network Security Group.

What is the Azure Load Balancer

- This service is used to distribute the incoming network traffic across a group of backend resources of servers
- You can define two types of load balancers – Public or Private Load Balancers
- You have 2 SKUs for the Load Balancer – Standard and Basic Load Balancer

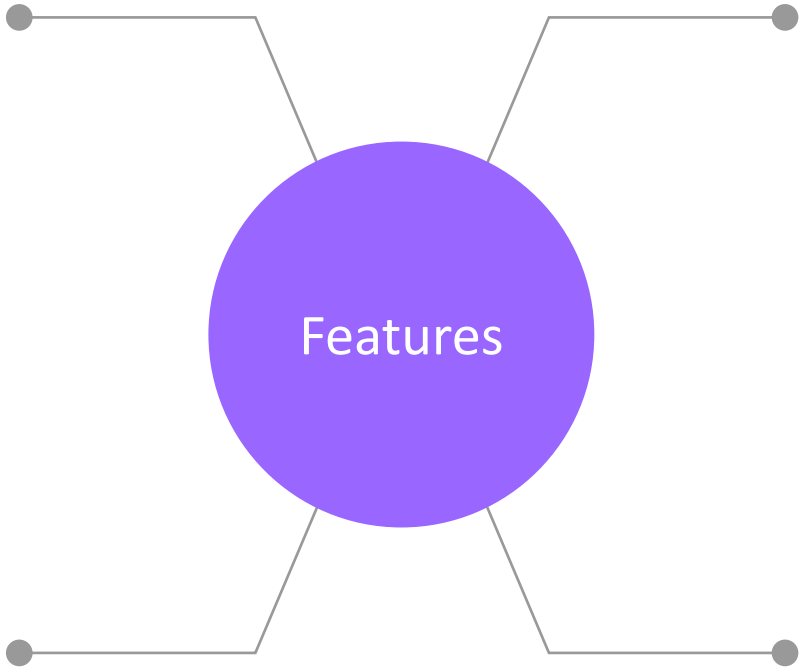
Basic Load Balancer

Pricing

You are not charged for the Load Balancer

SLA

There is no SLA



Backend machines

Here the machines need to be part of an availability set or scale set

Support for zones

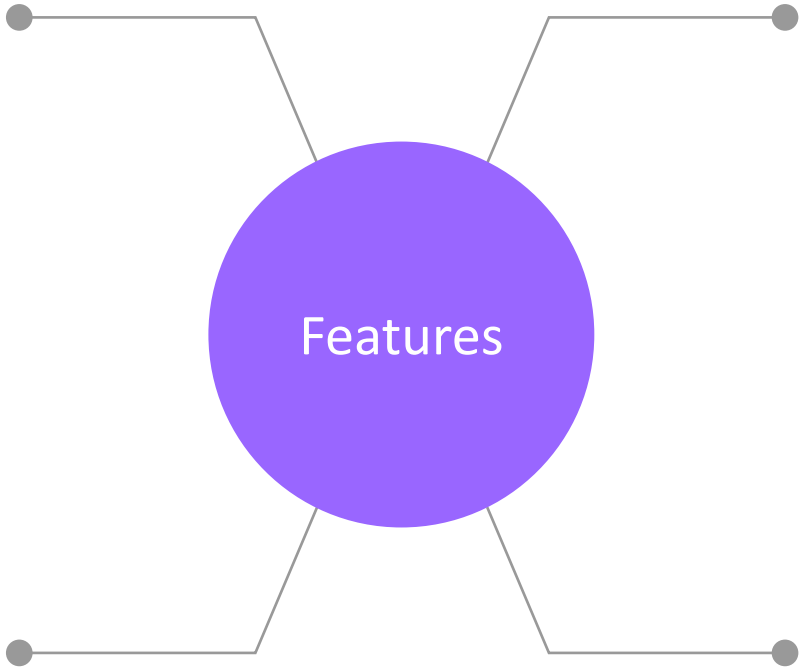
There is no support for availability zones

Summary

Standard Load Balancer

Pricing

There is a price per hour



SLA

There is an SLA of 99.99%

Backend machines

Here the machines need to be part of an availability set or scale set or they can be individual machines

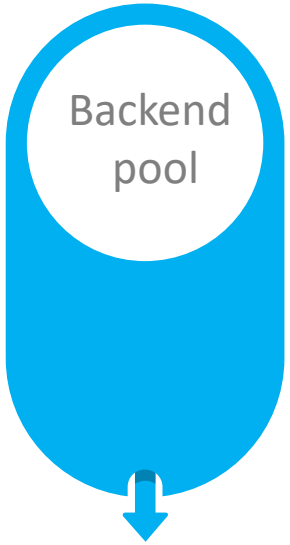
Support for zones

Here you get support for availability zones

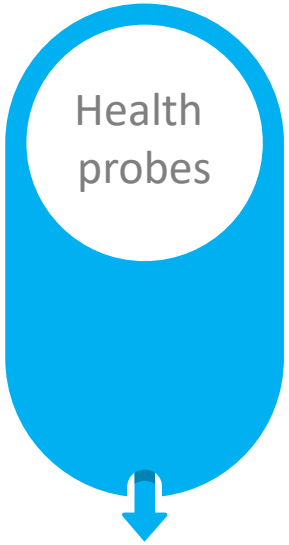
Summary

Components of a Load Balancer

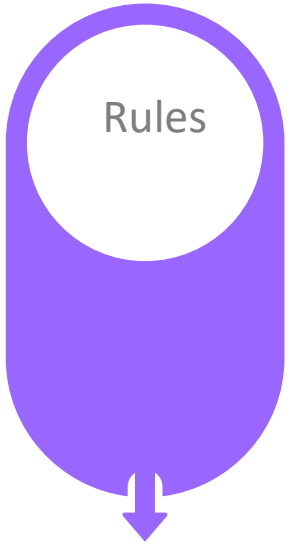
Here you define an IP address for the load balancer



This contains the backend virtual machines



This helps to check the status of the backend pool



The Load Balancing rules define how to distribute the incoming traffic

Summary

Azure Application Gateway

- This is a web traffic load balancer that works at layer 7 of the OSI model.
- Here the application gateway can make routing decisions based on the HTTP attributes.
- You also get other features such as Secure Sockets, Zone Redundancy etc.

Azure Virtual Network Peering

- This allows you to connect two or more Azure virtual networks.
- Here the traffic between the virtual machines in the virtual networks are routed via the Microsoft backbone infrastructure.
- Remember that you can just use one deployment of Azure Bastion in one network to RDP/SSH into machines in peered virtual networks.
- You can also peer virtual networks located in different Azure regions.

Azure VPN Gateway

- An Azure VPN gateway can be used to send encrypted traffic between an Azure virtual network and on-premises location over the Internet.
- **Point-to-Site VPN** – This let's you create a secure connection from the Azure virtual network to an individual client computer.
- **Site-to-Site VPN** – This provides connectivity between an on-premises network and an Azure virtual network.

Azure Bastion

- This service allows you to connect to a virtual machine by using the browser and the Azure portal.
- Here you can either RDP or SSH into your Azure virtual machines.
- This is a fully managed PaaS service. Here your machines don’t need to have a public IP address.

Azure Storage Accounts

Object replication

Object Replication

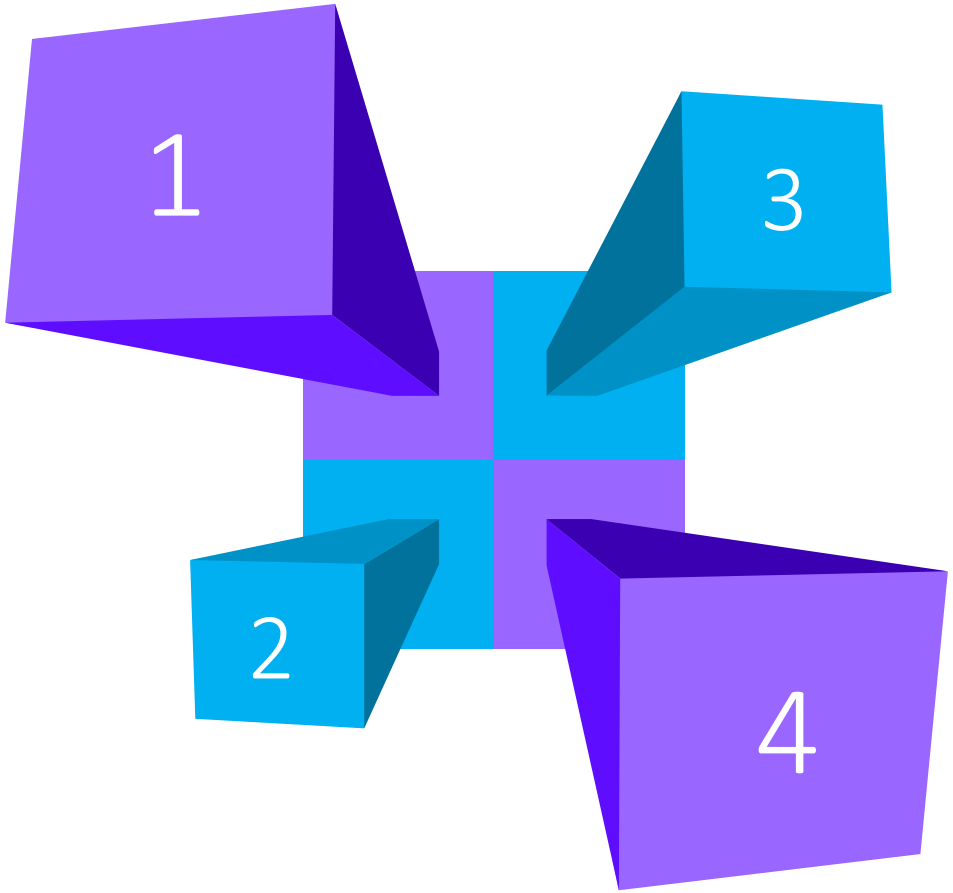
- This feature can be used to copy blobs between a source and destination storage account.
- You can create rules to specify which objects get replicated from the source to the destination.
- Storage Account support – General Purpose V2 and Premium Blob accounts.
- Blob versioning should be enabled on both the source and destination storage account.
- Change feed is enabled on the source storage account.

Copying data

Azure Import/Export Service

Copying Data

This is used for copying large amounts of data to Azure Blob storage and Azure Files.



Disk Drives

Here you make use of Disk Drives. You can use your own Disk drives or use the ones provided by Microsoft.

Transfer data

You can also transfer data from Azure Blob storage to your on-premises environment.

Jobs

You basically create a job via the Azure Portal. This will be used for transferring data to a storage account.

Azure Import/Export Service components

Import/Export Service

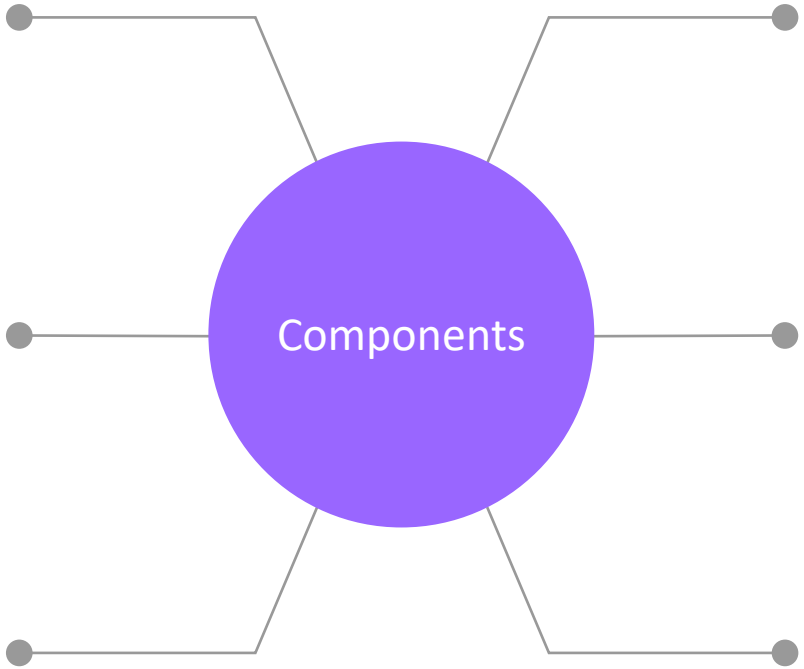
This is available in the Azure Portal. It helps to track the data import or export job.

WAImportExport tool

It prepare the disk drives that are required for import.

WAImportExport tool

It helps to copy the data onto the disk drive.



WAImportExport tool

It encrypts the data on the drive.

WAImportExport tool

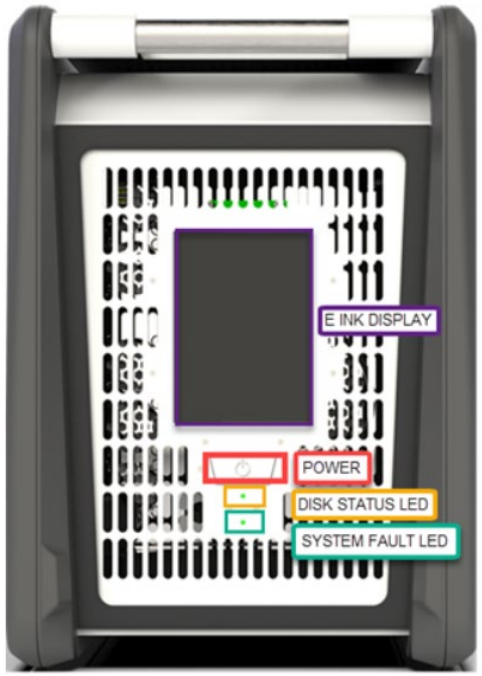
It generates the drive journal files that are used during the import creation.

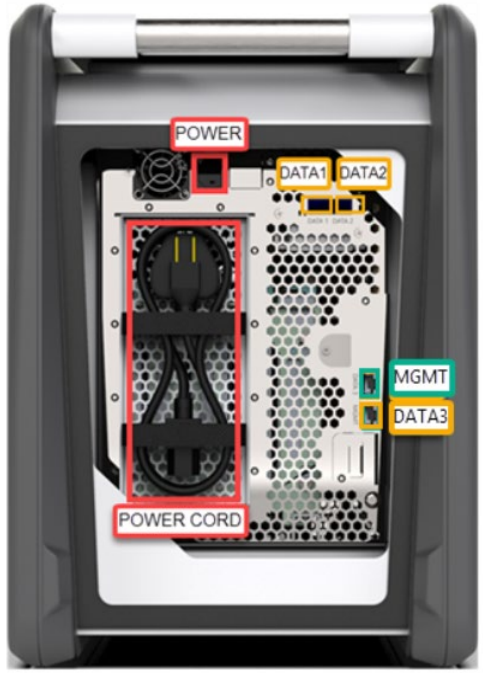
WAImportExport tool

It helps identify the number of drives needed for the export jobs.

Azure
Data Box

1. Data transfer — Helps to send terabytes of data in and out of Azure.
2. No Internet — You don’t need to use your Internet connection to transfer the data.
3. Scenario — Ideal when you want to transfer data sizes that are larger than 40 TB.
4. Device — You order the Data Box device via the Azure Portal.





Summary

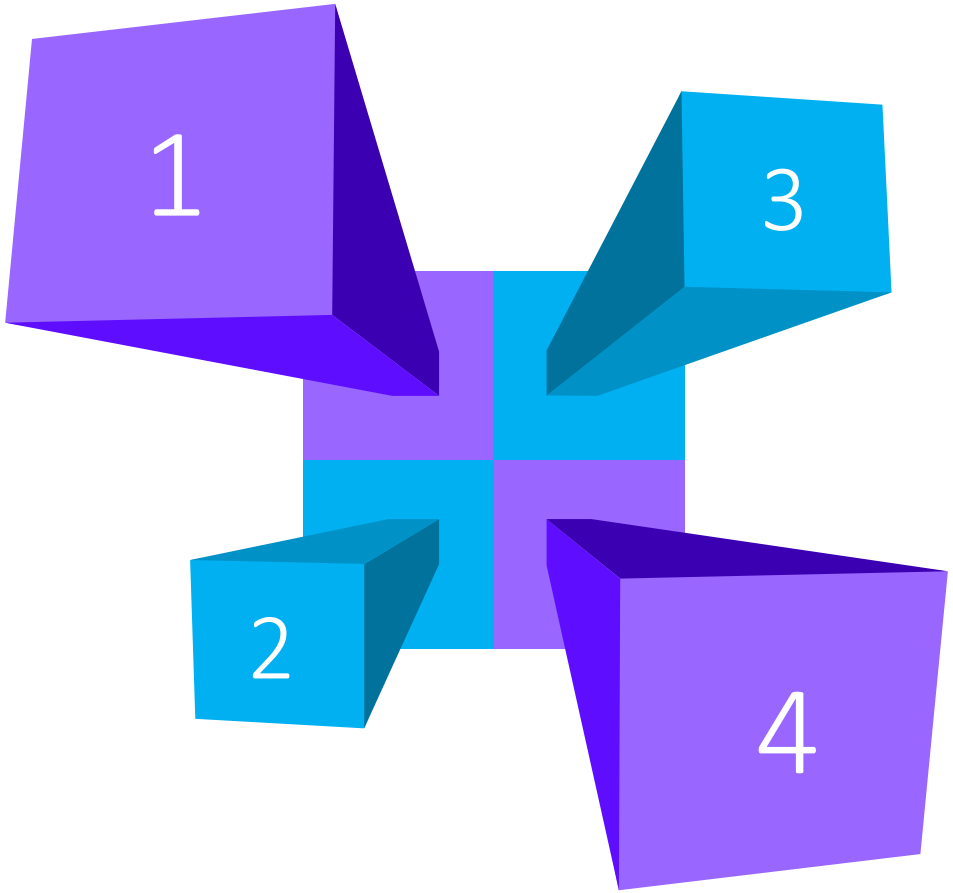
What are Azure storage accounts

- This service allows you to store objects on the cloud.
- Here you can make use of different services – Blob, Queue, File and Table.
- There are also different types of storage accounts.

Storage account types

Standard-general purpose v2

Gives you access to Blob, Queue, Table and File service



Premium file shares

This is a premium storage account for your file shares.

Premium block blobs

This is premium storage for your block blobs

Premium page blobs

This is premium storage for your page blobs.

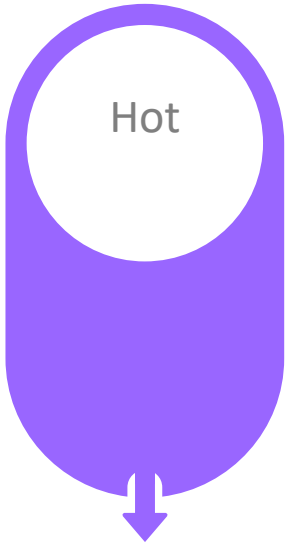
What is Blob storage

- This service is optimized for storing large amounts of unstructured data.
- Use case examples – storing images, videos, log files, documents.
- In the blob service, you will create a container. This is used to organize a set of blobs.
- Block blobs – This is used to store text and binary data.
- Page blobs – This is used to store virtual hard drive files that are used as disks for your Azure virtual machines.

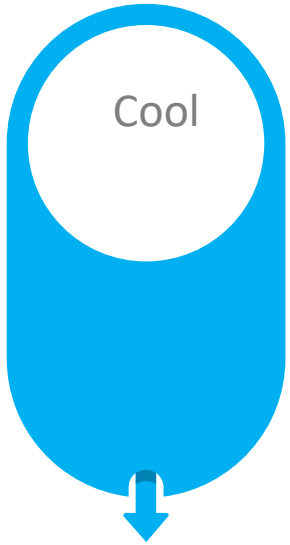
What is the File service

- This is used for hosting file shares on the cloud.
- This shares can be accessed via the SMB – Server Message Block protocol.
- You can mount the file shares from Windows, Linux and macOS clients.

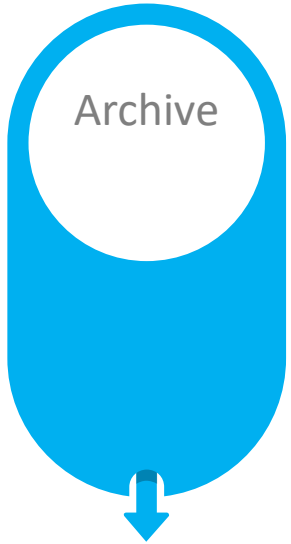
Access tiers



This is optimized for data that is accessed frequently.



This is optimized for data that is infrequently accessed and stored for at least 30 days.



This is optimized for storing data that is rarely accessed and stored for at least 180 days.

Access tiers

- The Archive access tier is good for long-term backups.
- You can set the access tier at the Storage account level to Hot or Cool.
- At the object level, you can also set the Archive access tier.

Data Redundancy

Locally redundant storage

Here data is copied synchronously three times within a single physical location in the primary region

Zone-redundant storage

Here data is copied synchronously across three Azure availability zones in the primary region

Geo-redundant storage

Here data is copied synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region

Geo-zone-redundant storage

Here data is copied synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the secondary region

Manage Azure identities and governance

Resource tags

Resource tags

This can be used to organize your resources.

Each tag consists of a name and a value pair.

For example, if you want to tag resources to a specific department, you can make use of resource tags.

Resource locks

Protecting resources

Resource locks

Locking resources can help ensure users don’t accidently delete or modify resources.

There are two types of locks

CanNotDelete - authorized users can still read and modify a resource, but they can't delete the resource..

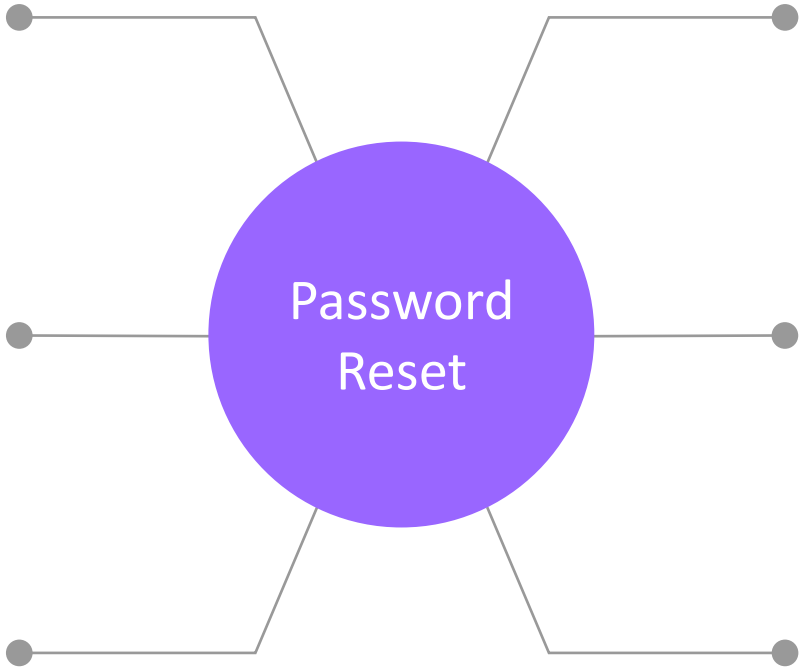
ReadOnly - authorized users can read a resource, but they can't delete or update the resource.

Self *Service Password Reset*

Self-Service
Password Reset

This feature helps users to reset their password without the need of contacting the IT help desk staff.

Password Reset



License

Password reset needs Azure AD Premium P1 or P2 licenses for users.

Password writeback

If there is a hybrid environment, the changed passwords can be written back to the on-premises Active Directory

Authentication Methods

You can define authentication methods to reset the password.

Number of methods

Define the number of authentication methods required to reset the password.

Number of days

Number of days before users need to reconfirm their authentication information.

Notification

Notify users when password is reset.

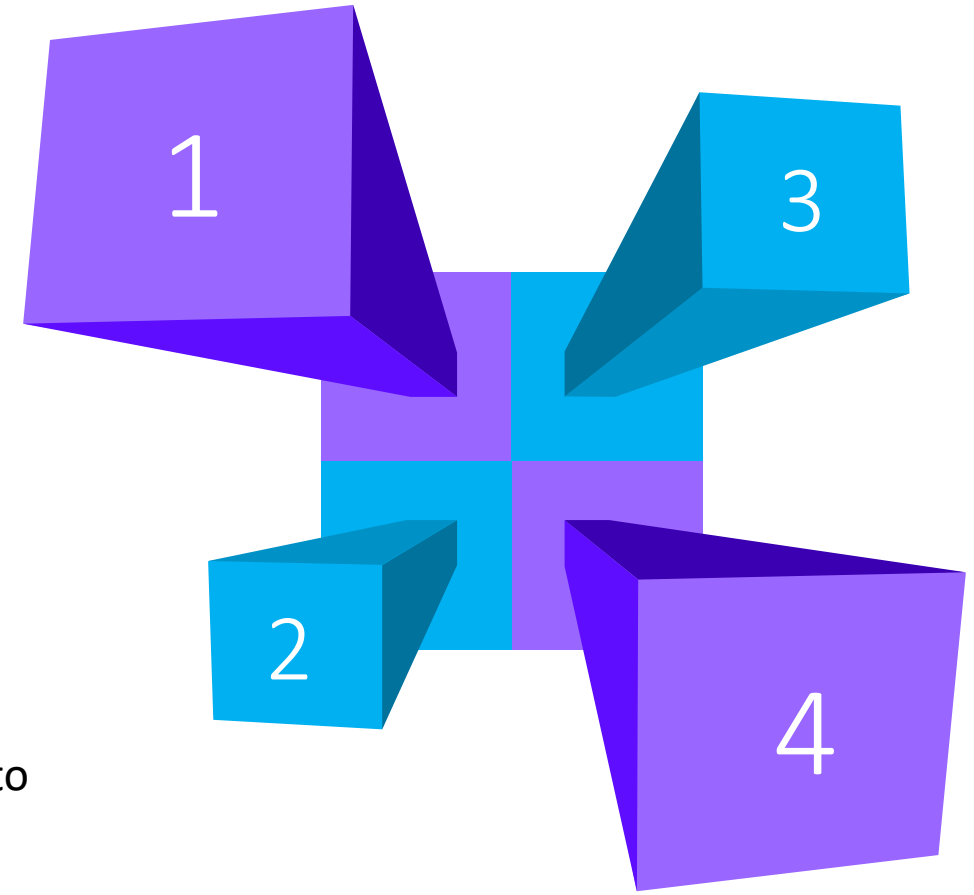
Summary

Azure Active Directory

Azure Active Directory

Identity

This is a cloud-based identity and access management service.



Azure and Microsoft 365

This identity provider works for both Azure and Microsoft 365.

Access

You can authenticate users and grant access to resources.

Security

You have different security features available.

Summary

Azure Active Directory Licensing

- **Azure Active Directory Free** – Here you get user and group management, basic reports.
- **Azure Active Directory Premium P1** – Dynamic groups, more hybrid capabilities.
- **Azure Active Directory Premium P2** – Azure AD Identity Protection, Privileged Identity Management.

Trust Relationship

- There is a trust relationship between an Azure Active Directory and an Azure subscription.
- Each subscription can only trust a single Azure AD directory.
- Multiple subscriptions can trust the same Azure AD directory.

Role-based access control

- You can give access to resources within your subscription with the use of Role-based access control.
- There are many in-built roles.
- You can create your own custom roles. When creating a custom role, you can clone an existing in-built role or even clone an existing custom role.
- You can assign roles at different levels. If you assign the role at a higher level , the role will apply to all of the child resources. For example, a resource group, it will apply to all resources within the resource group.

Azure AD Custom Domains

- You can map your own custom domain to an Azure Active Directory tenant.
- To implement this, you need to add a TXT record to your domain registrar.

Multi-Factor Authentication

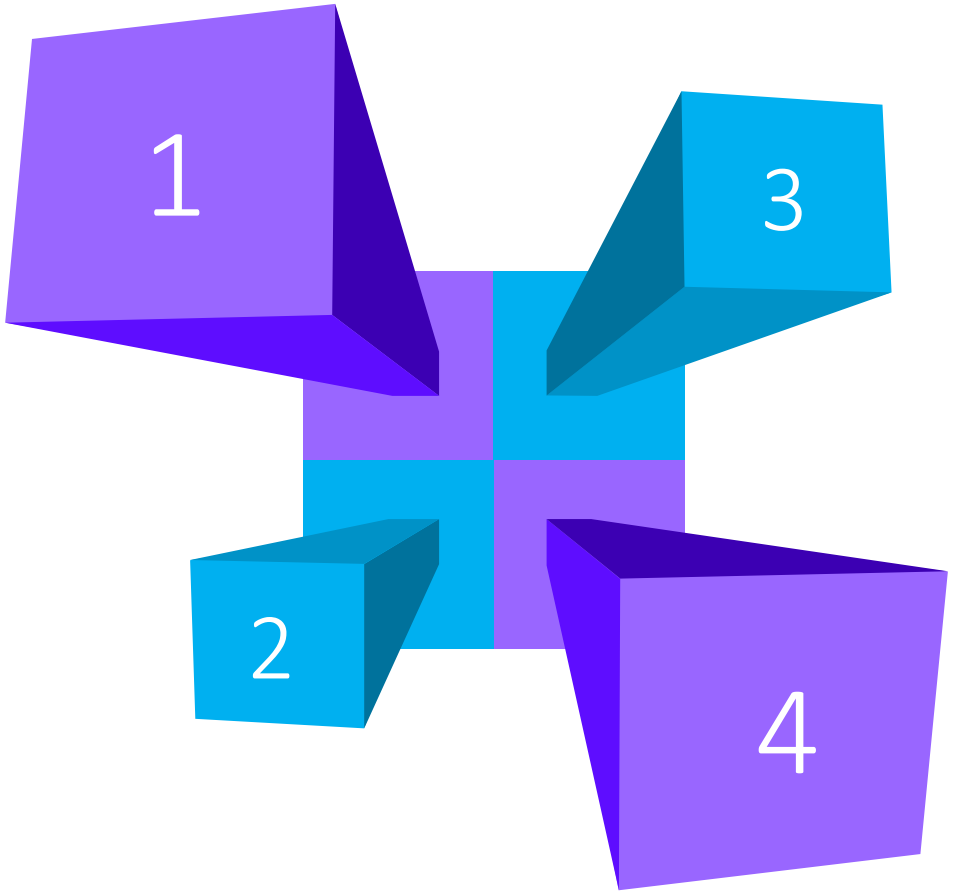
- The use of MFA - Multi-Factor Authentication to provide an extra layer of security when it comes to authentication.
- It’s a good practice to enable MFA for your privileged users.

Conditional *Acess*

Azure AD Conditional Access

Conditions

Here you can define conditions based on which you want to give access to users for a resource.



Access

Based on the condition you can decide whether the user should be allowed access , blocked access or they require the user of MFA.

Signals

You can make use of different signals for the conditions – User and their location, device they are logging from, the Application , real-time risk.

Enforced

These rules are enforced after the first-factor authentication is complete.

Summary

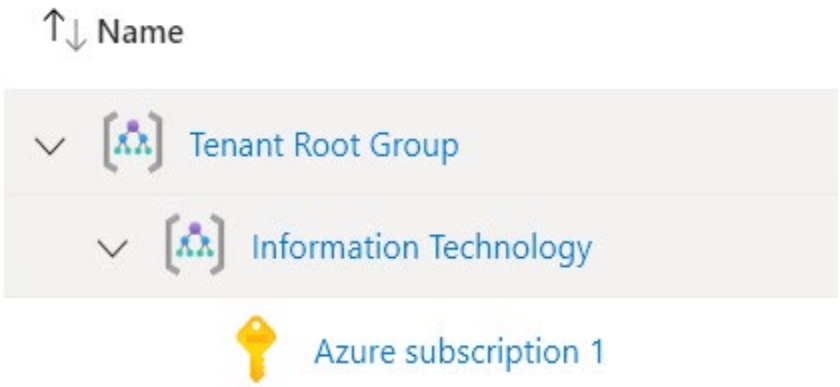
Administrative Units

- This is a resource in Azure Active Directory that can be used as a container for other Azure Active Directory resources.
- Here the administrative unit can only contain users, groups or devices.
- Here you can restrict permissions in a role to a portion of the defined organization.

Management Groups

Management Groups

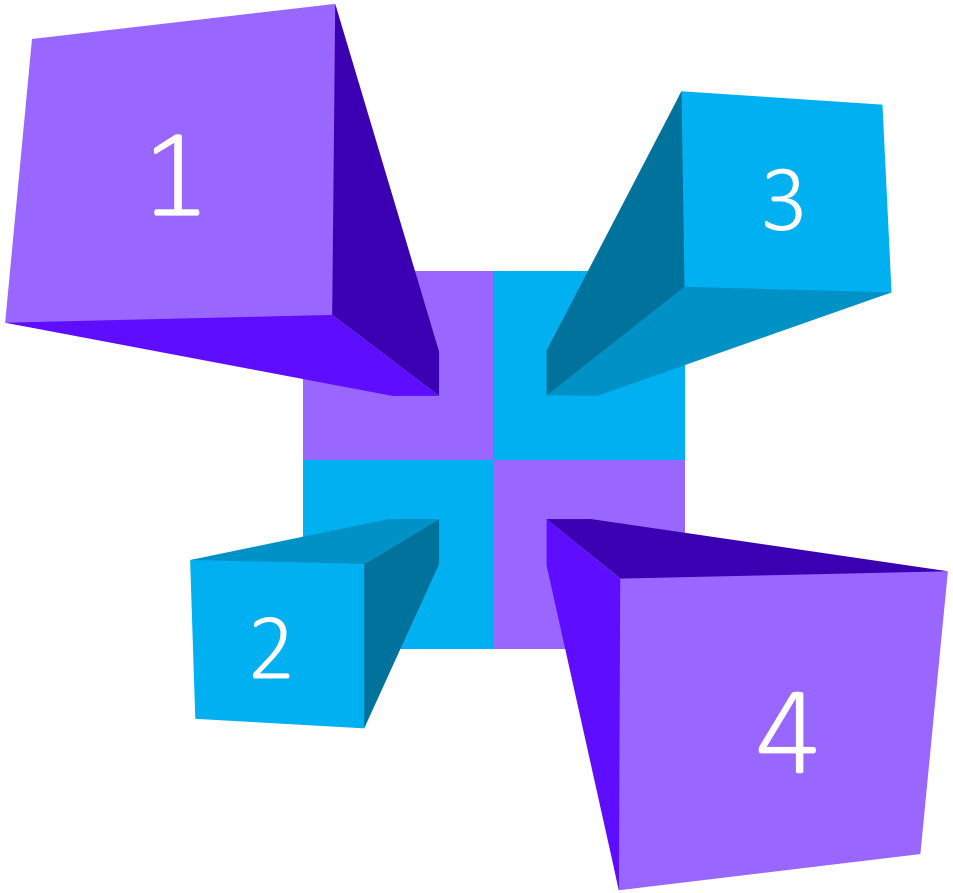
1. **Organization** — You can organize your subscriptions into management groups.
2. **Azure AD Tenant** — All subscriptions in the Management group must trust the same Azure AD tenant.
3. **Access permissions** — You can apply access permissions at the Management Group Level.
4. **Policy** — You can apply policies at the Management Group Level.



Root Management Group

Root Group

There is a top-level management group called “Root” management group.



Elevation

The Azure AD Global administrator needs to elevate themselves to the User Access Administrator role for this root group.

Tenant Root Group

The name assigned to the root group is the Tenant Root Group.

Policies and Access Permissions

You can assign permissions and role assignments at this level.

Summary

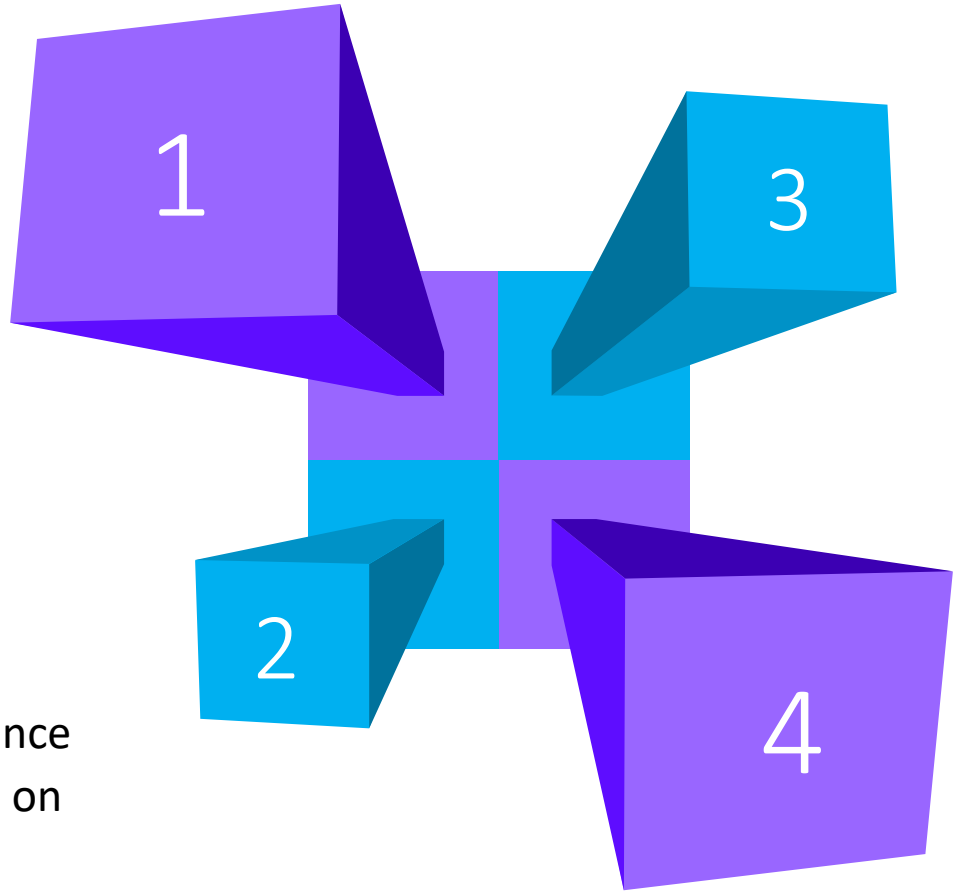
Monitor and backup Azure resources

Azure VM Insights

Azure VM Insights

Monitor

This helps to monitor the performance and health of virtual machines.



Support

Works for Azure virtual machines, Virtual Machine Scale sets, On-premises virtual machines.

Identify Issues

You can identify performance and network issues based on the data collected.

Data

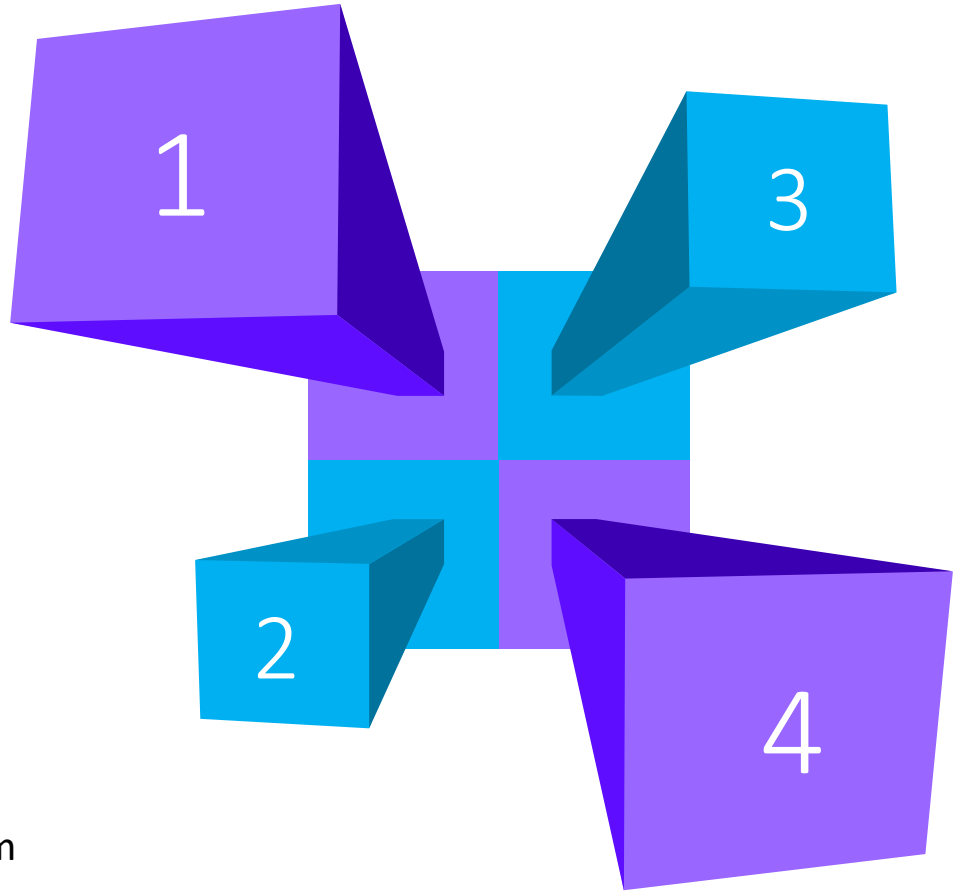
Here the data collected is stored in Azure Monitor logs.

Azure Recovery Services Agent

Microsoft Azure Recovery Services agent

Selective backups

Here you can perform selective backups of files and folders.



Machines

This can be done on your Azure virtual machines or your on-premises machines.

Backup

Windows Files and Folders.
Protect an entire Windows volume.
Protect the Windows system state.

Agent

Here you download and install the Recovery service agent.

MARS agent