Azure Disks for virtual machines

Azure Virtual Machines

1	Management	You have Azure Managed Disks that are completely managed by Azure.
2	Virtualized	Its like having physical disks but they are virtualized.
3	Highly available	Designed with 99.999% availability .
4	Support	Has support with features such as Availability Zones, Azure Backup etc.

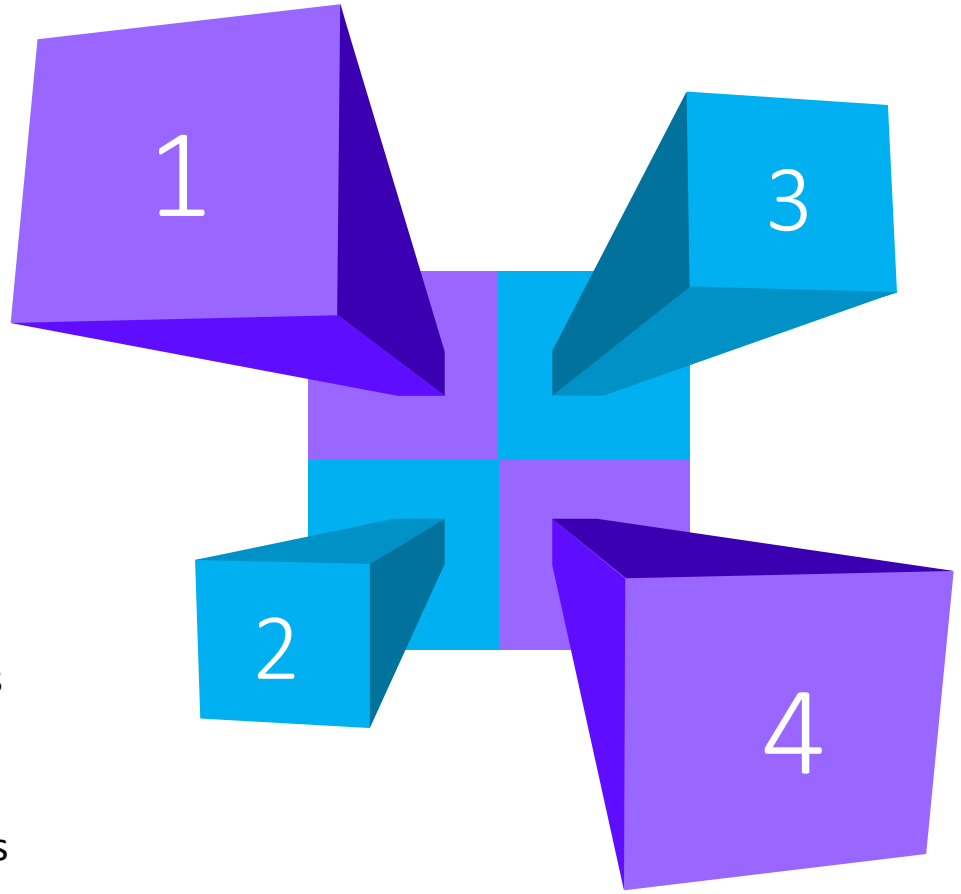
Disk Types

Standard HDD

This is ideal for backup environments and non-critical workloads.
Max disk size – 32,767 GiB
Max throughput – 500 MB/s
Max IOPS - 2000

Standard SSD

This is ideal for Web Servers and Dev/Test Environments.
Max disk size – 32,767 GiB
Max throughput – 750 MB/s
Max IOPS - 6000.



Premium SSD

This is ideal for Production environments.
Max disk size – 32,767 GiB
Max throughput – 950 MB/s
Max IOPS – 20,000.

Ultra Disk

This is ideal for IO intensive workloads – SQL , Oracle databases.
Max disk size – 32,767 GiB
Max throughput – 950 MB/s
Max IOPS – 20,000.

Un-managed disks

Un-managed vs Azure Managed Disks

There are many benefits to using Azure Managed Disks.

You get 99.999% availability. This is ensured by creating multiple replicas of the data.

Integrates well with the use of Availability Sets and Availability Zones.

With Un-managed disks , you only pay for how much you consume.

With Un-managed disks , you only pay for how much you consume.

Custom Script Extensions

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

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 in different data centers.

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 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.

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.

Network Watcher Service

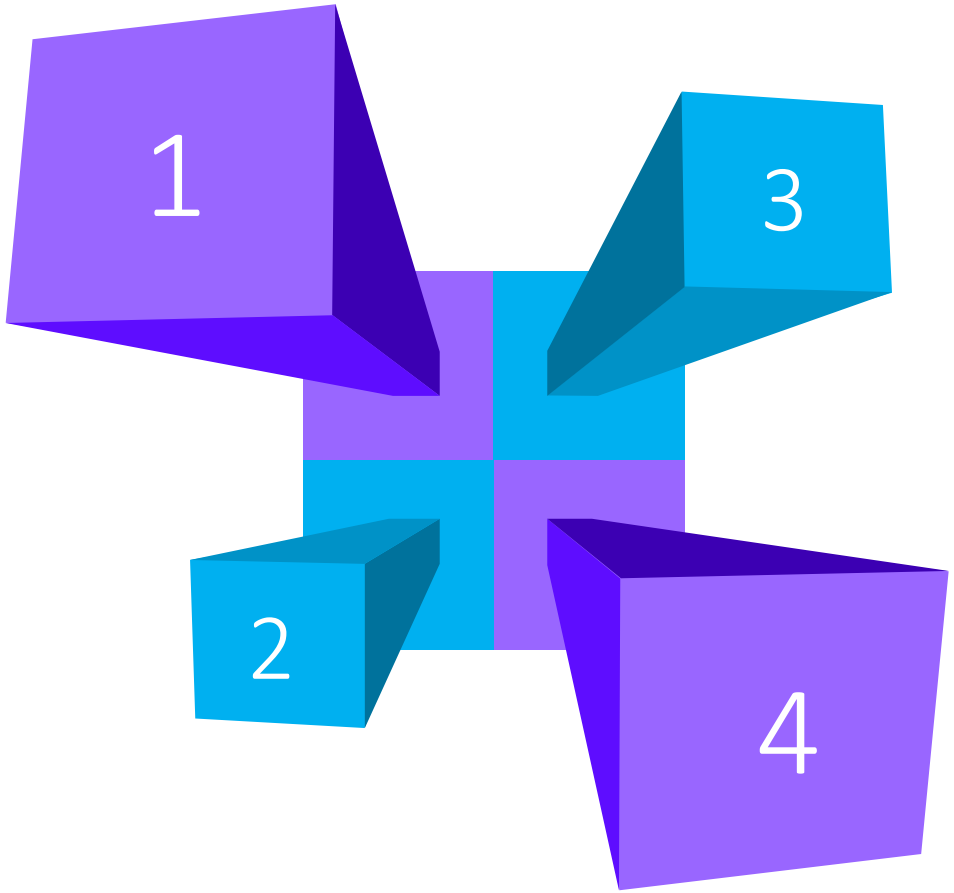
Network Watcher service

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

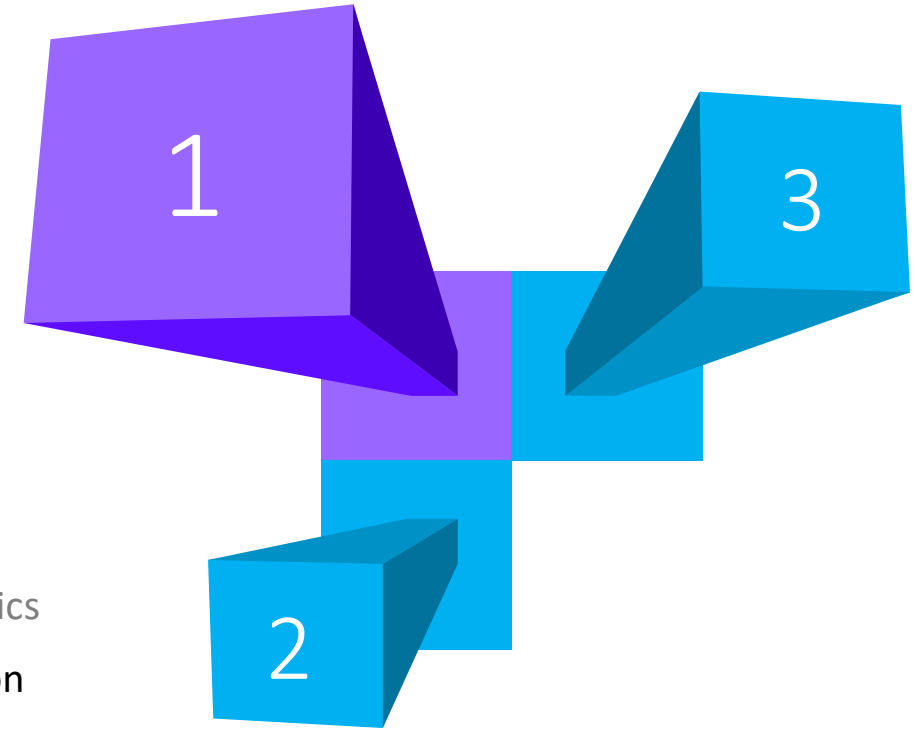
Check the connection from a virtual machine to a virtual machine, fully qualified domain name, URI or IPv4 address.

Network Watcher Service

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.

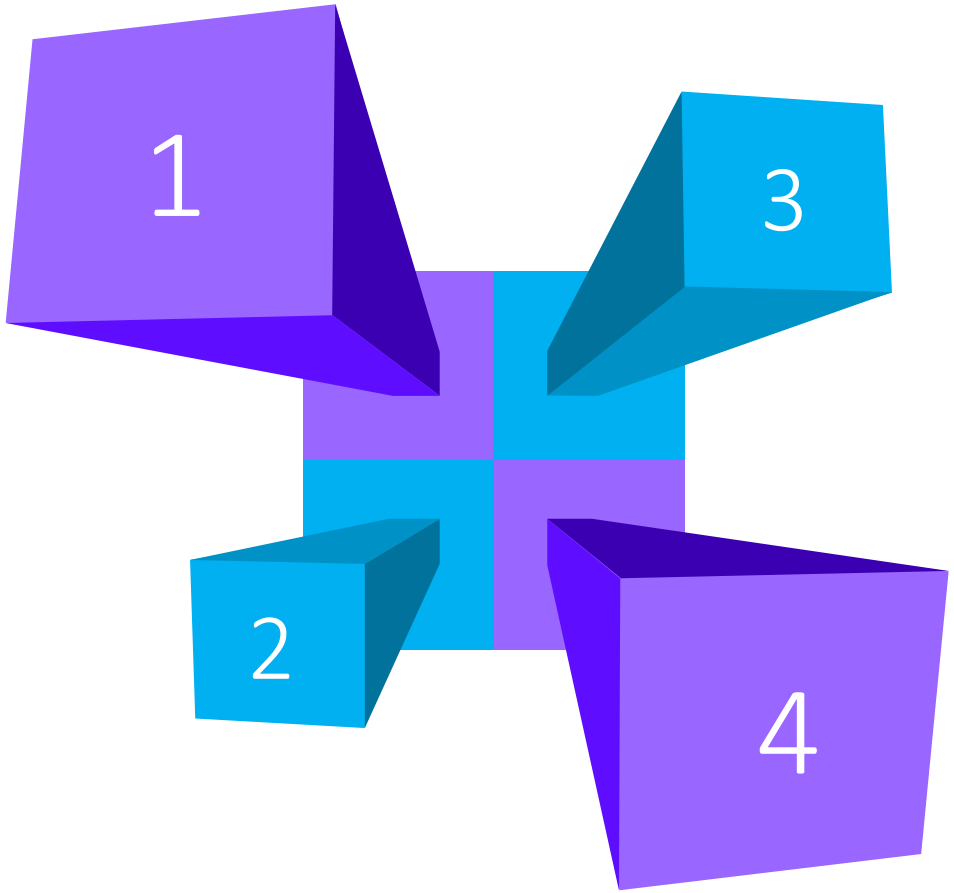
Network Watcher Service

Storage Account types

Storage Account types

Standard General Purpose V2

This is standard storage for blobs, file shares, queues and tables.



Premium Page blobs

This is supported for page blobs. This is when you want fast access to your blobs, high transaction rates.

Premium block blobs

This is supported for block and append blobs. This is when you want fast access to your blobs, high transaction rates.

Premium file shares

This is supported for file shares. This is when you want fast access to your files, high transaction rates.

Access tiers

Access tiers

Hot tier – This is used for storing data that is accessed or modified frequently. Here the storage costs are high but the access costs are less.

Cool tier – This is used for storing data that is infrequently accessed or modified. Here the data must be stored for at least 30 days. This tier has less storage costs but higher access costs that the Hot Access tier.

Archive tier – This is used for storing data that is rarely accessed. Here the data must be stored for at least 180 days. This tier has the least storage costs.

Access tiers

Archive tier – This tier can only be set at the object level.

In order to access an object which is in the Archive access tier you first need to rehydrate the object. The access tier of the object needs to be changed to either the Hot or the Cool Access tier first.

The process of rehydration could take several hours.

Access tiers

Support for Access tiers

General Purpose V2 storage accounts.

Data redundancy

Data Redundancy

Locally redundant storage – Here data gets copied synchronously three times within a single physical location in the primary region. This is the least expensive option but does not give you high availability or durability.

Zone- redundant storage – Here data gets copied synchronously across three Availability Zones in the primary region.

Data Redundancy

Geo-redundant storage – Here data gets copied synchronously three times within a single physical location in the primary region. Then data is copied synchronously to a single physical location in the secondary region. In the secondary location, data is copied synchronously three times using LRS.

Geo-Zone-redundant storage – Here data gets copied synchronously across three Availability Zones in the primary region. Then data is copied synchronously to a single physical location in the secondary region. In the secondary location, data is copied synchronously three times using LRS.

Data Redundancy

Read Access Geo-redundant storage or Read Access Geo-Zone-redundant storage – With the normal options data in the secondary region only becomes available if there is a failure in the primary region. This option can be utilized if you want data to be available in the secondary region as well for read-only purposes.

Change Replication

Replication Change

If you want to migrate the storage account from LRS to ZRS in the primary region, then you need to perform either a manual migration or a live migration.

For a manual migration, you basically create another storage account with the ZRS replication type. And then you copy the data from the source onto the destination.

You can also request Microsoft to perform a live migration. This ensures that you have no application downtime during the migration process. Here you can access the data as the migration is progressing.

Replication Change

To migrate from LRS to GZRS or RA-GZRS, first switch to GRS or RA-GRS and then request a live migration.

To migrate from GRS or RA-GRS to ZRS, first switch to LRS, then request a live migration.

Lifecycle management policies

Lifecycle Management

1. **Transition** — Here you can transition blobs from the cool to the hot access tier to save on storage costs.
2. **Blobs** — You can transition blobs, blob versions and blob snapshots.
3. **Deletion** — You can also define rules to delete blobs, blob versions and blob snapshots.
4. **Rules** — Rules can be applied at the storage account level or to a subset of blobs.

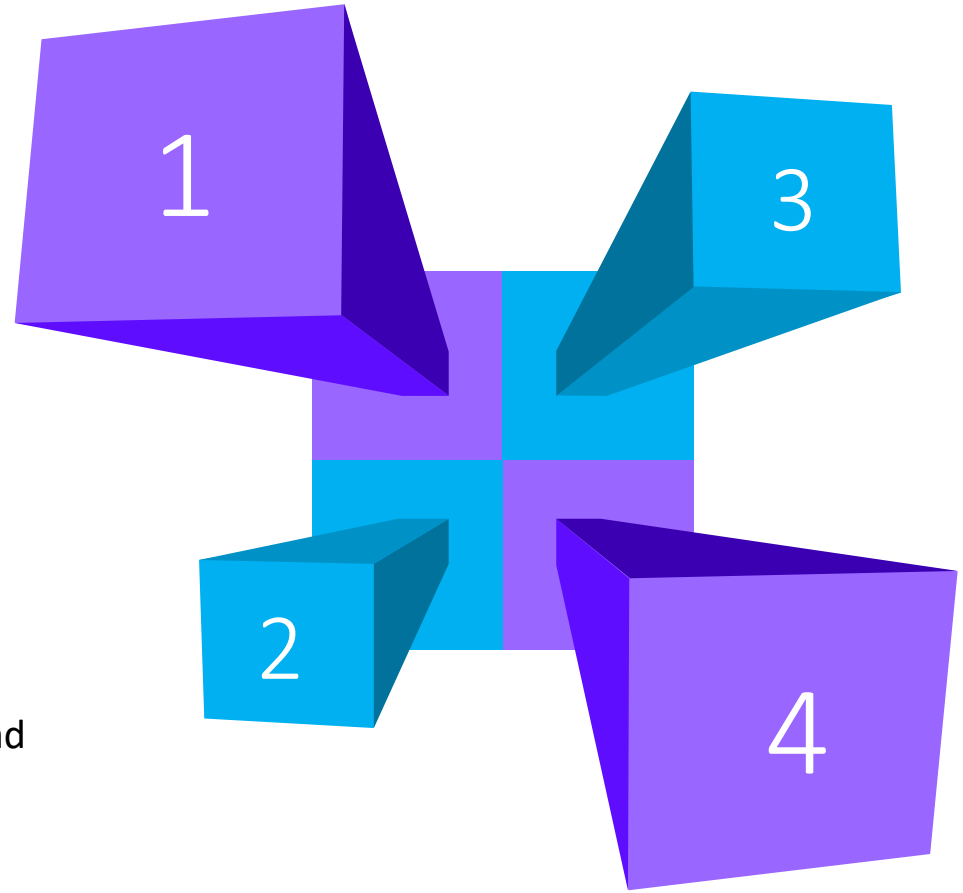
Lifecycle management

Rule filters

You can define filters for blobTypes – blockBlob, appendBlob.

Rule actions

You have actions such as tierToCool, tierToArchive and delete.



Support

Rules are supported for blob and append blobs in General-Purpose V2 accounts, Premium Block Blob and Blob Storage accounts.

Region

This feature is available in all regions.

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.

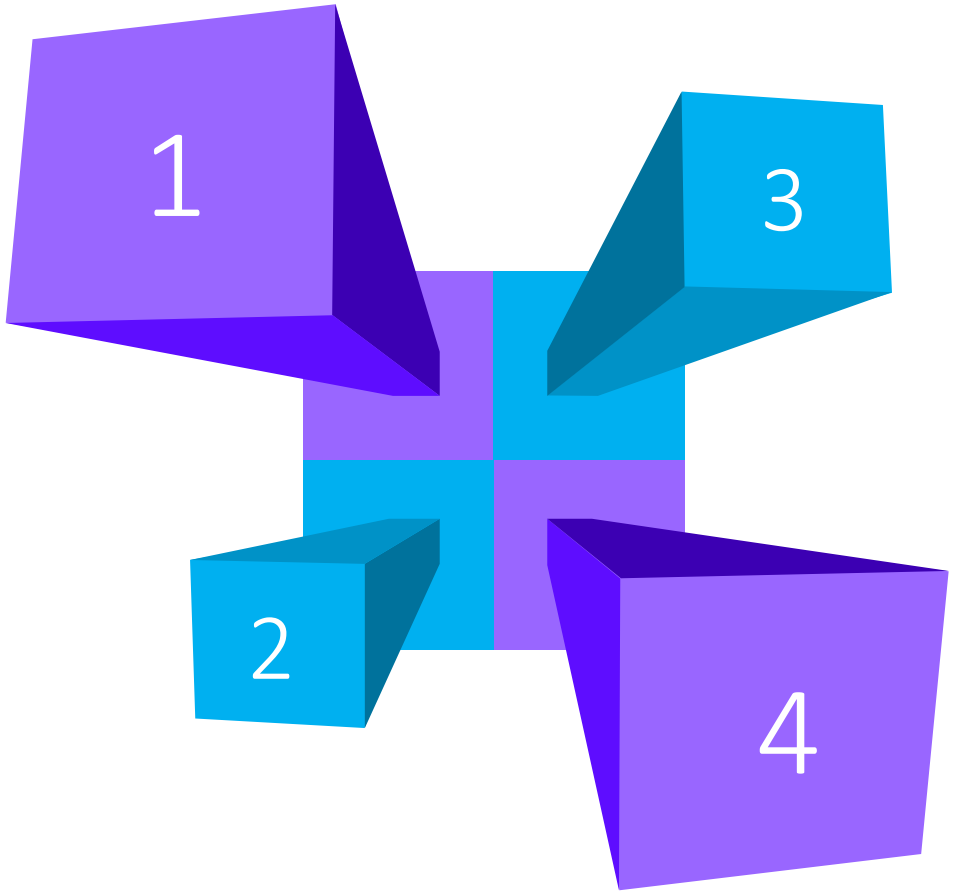
Change feed is enabled on the source storage account.

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

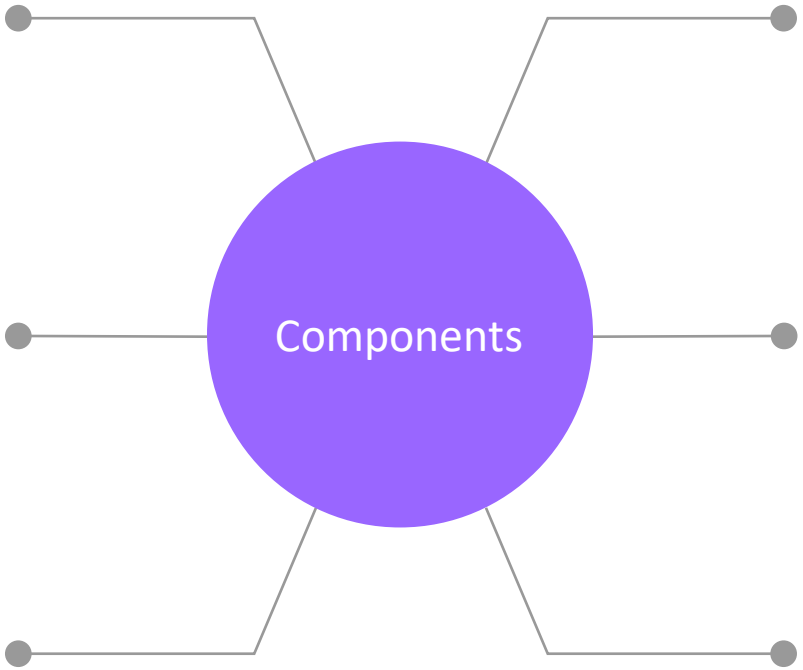
This is available in the Azure Portal. It helps to track the data import or export job.

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

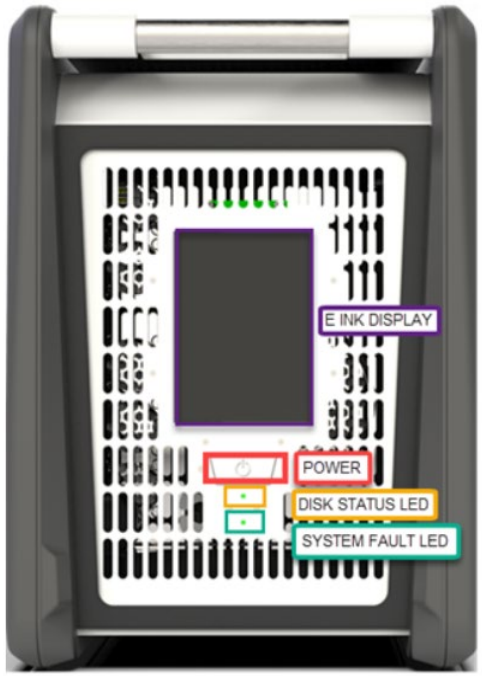
It generates the drive journal files that are used during the import creation.

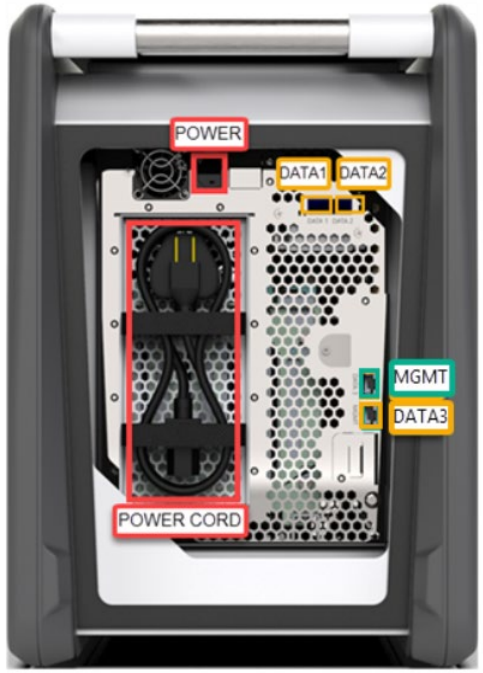
WAImportExport tool

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.





Different storage accounts

Premium Block Blob Storage

Resource group (move)	: app-grp	Performance	: Premium
Location	: East US	Replication	: Locally-redundant storage (LRS)
Subscription (move)	: Azure subscription 1	Account kind	: BlockBlobStorage
Subscription ID	: 6912d7a0-bc28-459a-9407-33bbba641c07	Provisioning state	: Succeeded
Disk state	: Available	Created	: 12/17/2021, 6:36:32 PM

Tags (edit) :

Storage accounts

Premium File Shares

Essentials

Resource group (move)	: app-grp	Performance	: Premium
Location	: East US	Replication	: Locally-redundant storage (LRS)
Subscription (move)	: Azure subscription 1	Account kind	: FileStorage
Subscription ID	: 6912d7a0-bc28-459a-9407-33bbba641c07	Provisioning state	: Succeeded
Disk state	: Available	Created	: 12/17/2021, 6:44:30 PM

General Purpose V1 Storage

Resource group (move)	: app-grp	Performance	: Standard
Location	: North Europe	Replication	: Locally-redundant storage (LRS)
Subscription (move)	: Azure subscription 1	Account kind (change)	: Storage (general purpose v1)
Subscription ID	: 6912d7a0-bc28-459a-9407-33bbba641c07	Provisioning state	: Succeeded
Disk state	: Available	Created	: 12/17/2021, 7:09:01 PM

Storage accounts

Zone Redundant data storage

1. General-purpose v2
2. Premium block blobs
3. Premium file shares

Zone Redundant data storage

1	Can we set the access tier at an object level for General Purpose v1 storage accounts	No
2	Can we set the access tier at an object level for Premium block blobs	No
3	Can we set the access tier at an object level for Premium file shares	No

Resource tags

Resource tags

This can be used to organize your resources.

Each tag consists of a name and a value pair.

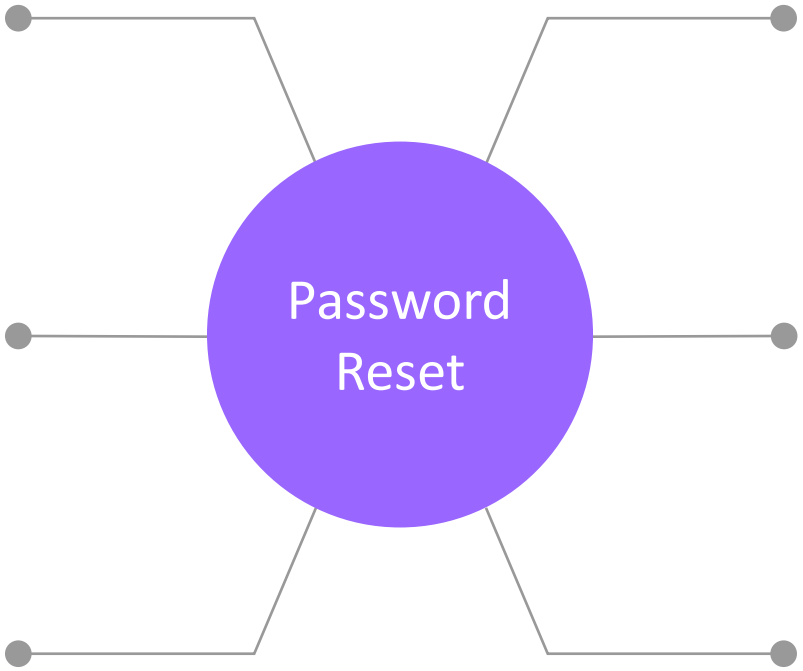
For example, if you want to tag resources to a specific department, you can make use of resource tags.

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

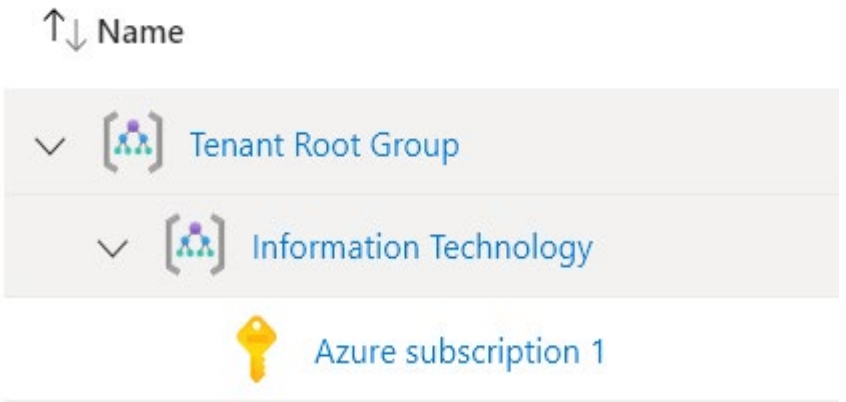
Notify users when password is reset.

Management Groups

Management

Groups

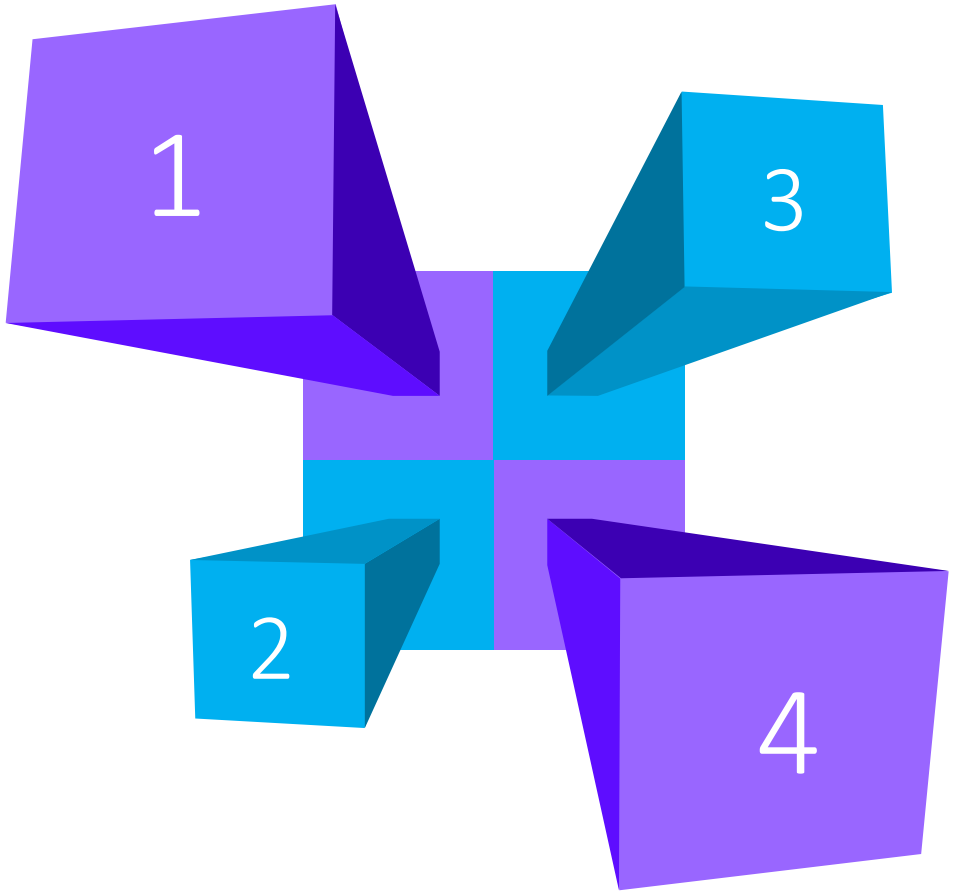
1. Organization — You can organize your subscriptions into management groups.
2. Azure AD Tenant — All subscriptions in the Management group must trust the same Azure AD tenant.
3. Access permissions — You can apply access permissions at the Management Group Level.
4. Policy — You can apply policies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

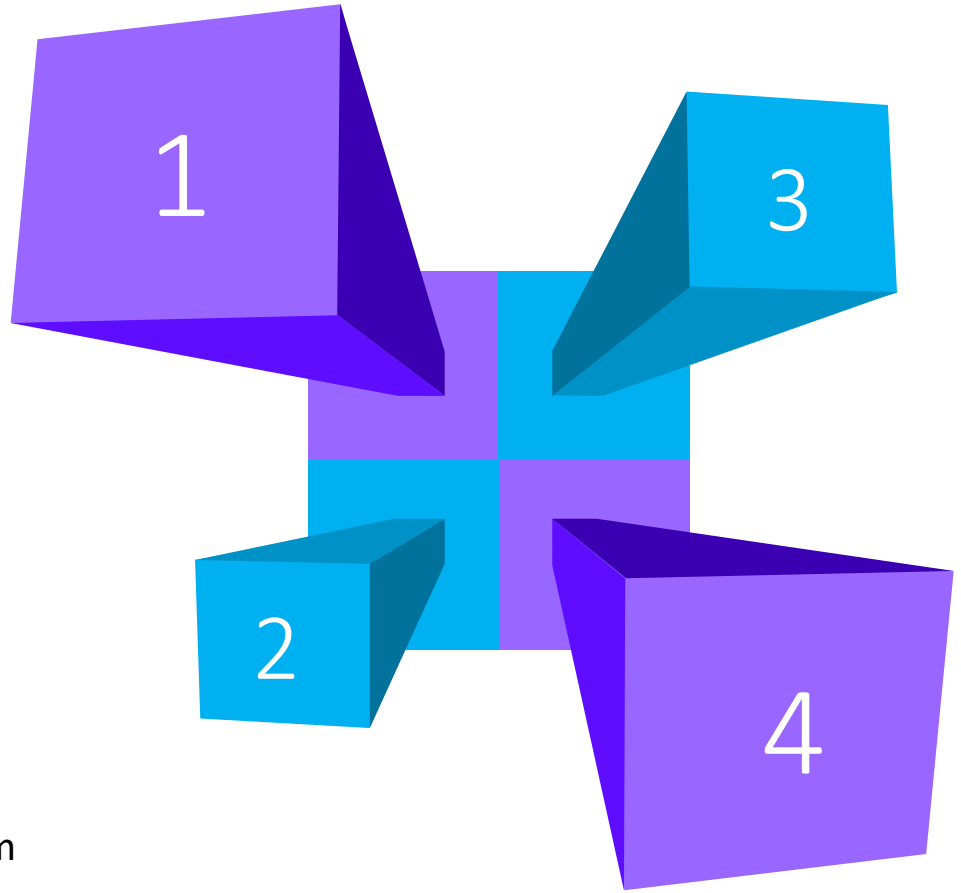
You can assign permissions and role assignments at this level.

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

Azure Backup reports

Azure

Backup reports

1. **Insights** — You can get insights on aspects such as the number of backups taken and storage consumed.
2. **Support** — Supported for Azure VMs, SAP HANA in Azure VMs.
3. **Data** — The backup reports data is sent to a Log Analytics workspace.
4. **Multiple items** — Reports can be viewed of multiple backup items, vaults, regions as long as the data is being sent to the same Log Analytics workspace.

Application Insights

Application Monitoring

What is Application Insights

Application Performance Management service for web developers.

You can use this tool to monitor your applications.

It can help developers detect anomalies in the application.

It can help diagnose issues.

It can also help understand how users use your application.

It also helps you improve performance and usability of your application.

What gets monitored

Request rates, the response times and failure rates – This is done at the page level.

Exception recorded by your application.

Page views and their load performance as reported from the user's browser.

User and session counts.

Performance counters of the underlying Windows or Linux Machines.

Diagnostic trace logs from your application.