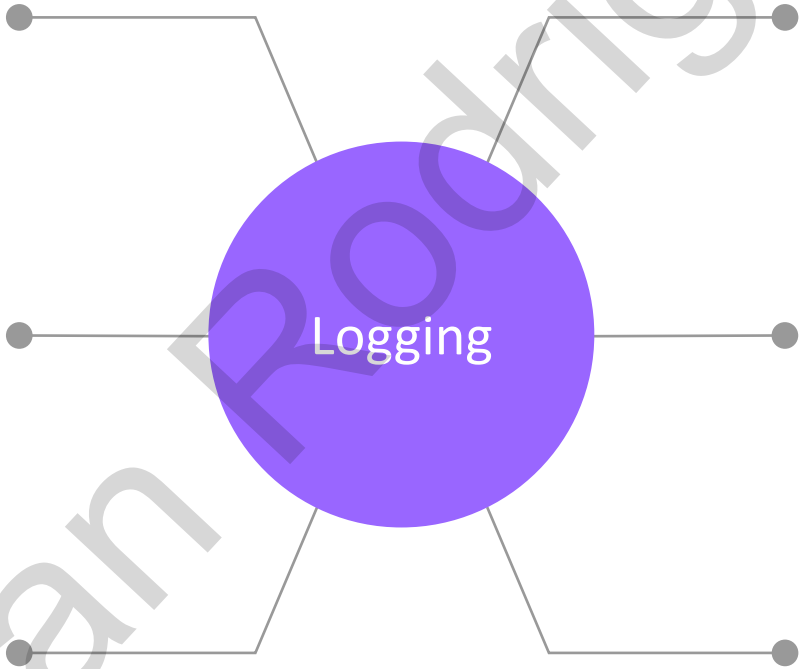
Design Monitoring

Logging

Azure Monitor Agent



Collection

Collects data from the guest operating system of Azure and send them onto Azure Monitor.

Other services

You can also send the data to other services like Microsoft Defender and Microsoft Sentinel.

Data ingestion

You can filter rules and create transformations on the data being ingested.

Multihoming

The Windows and Linux machines can send data to multiple Log Analytics workspaces at a time.

Single agent

Use a single agent to achieve all of this.

Security

There is enhanced security via the use of Azure AD and Managed Identity tokens.

Data Collection Rules

This defines the data collection process in Azure Monitor.

Here you can decide what data needs to be collected, how to transform the data and then send the data onto the destination.

The data collection rule will install the Azure Monitor agent on the machine.

Application *Insights*

Application Insights

Monitoring

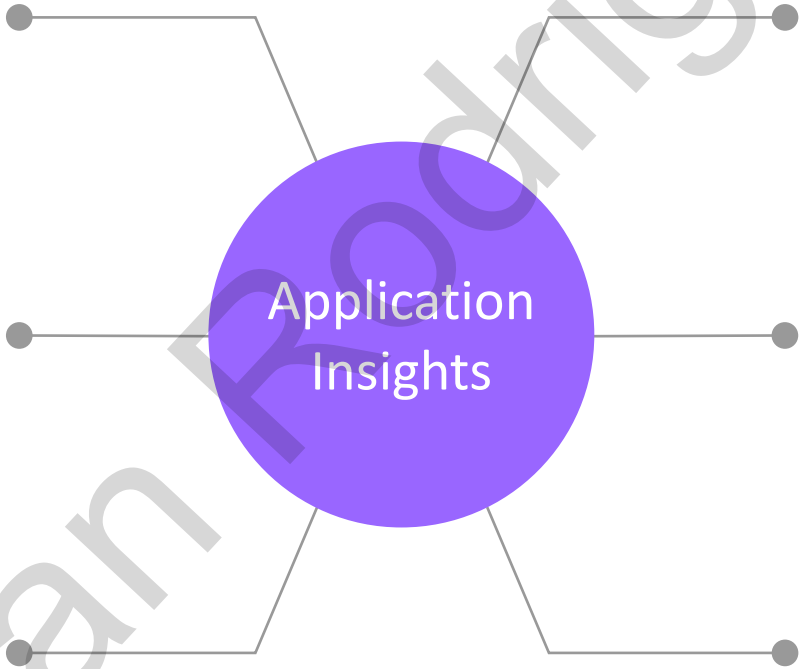
This provides the feature of application performance management and monitoring of live web applications.

Aspects

Here you can see aspects such as detecting performance issues or any other issues.

Support

There is support for .NET, Node.js, Java and Python.



Applications

This works for applications hosted in Azure, on-premises environments, or other cloud platforms.

Integration

It has Integration with the Visual Studio IDE.

Users

You can also see how users interact with your application.

Application Insights

How does it work

You can install a small instrumentation package (SDK) for your application. Or use the Application Insights agent.

You can instrument web applications, background components and JavaScript in web pages.

The telemetry data sent by Application Insights has very little impact on the performance of your application.

Microsoft Sentinel

Threat protection

What is Microsoft Sentinel

This is a cloud service that provides a solution for SEIM (Security Information Event Management) and SOAR (Security Orchestration Automated Response)

This provides a solution that helps in the following

Collection of data – Here you can collect data across all users, devices, applications and your infrastructure. The infrastructure could be located on-premise and on the cloud.

It helps to detect undetected threats.

What is Microsoft Sentinel

It helps to hunt for suspicious activities at scale.

It helps to respond to incident rapidly.

Once you start using Microsoft Sentinel, you can start collecting data using a variety of connectors.

You have connectors for a variety of Microsoft products and other third-party products as well.

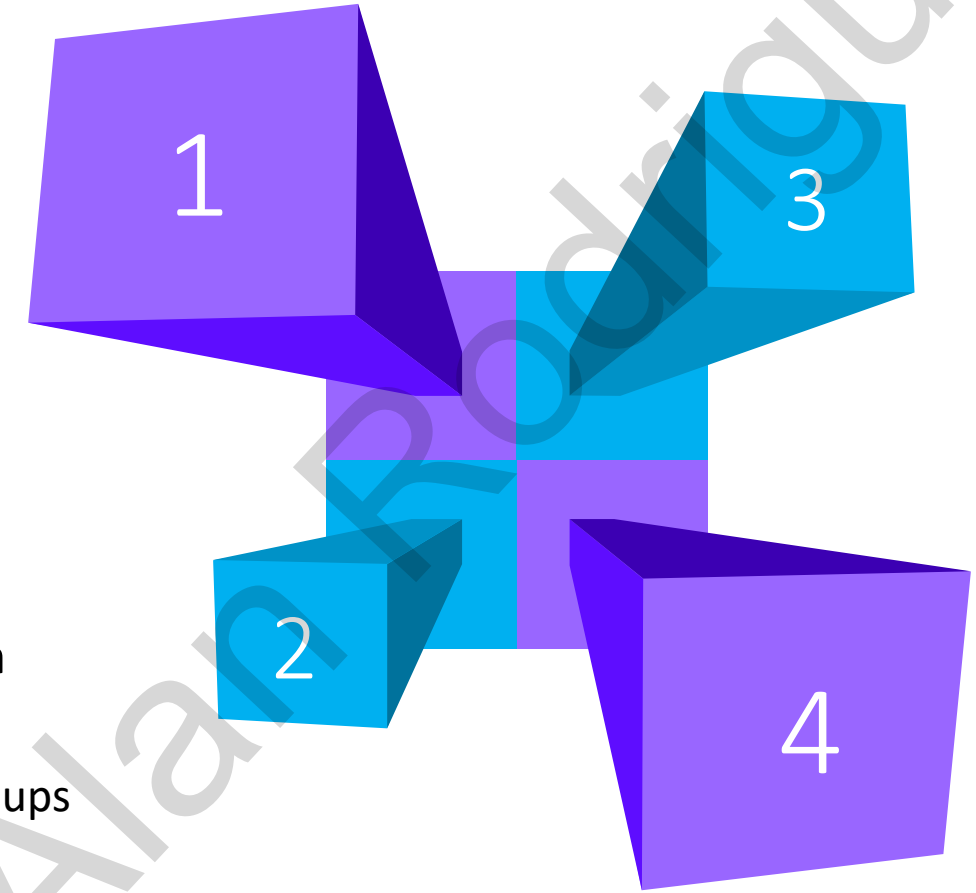
You can then use in-built workbooks to get more insights on the collected data.

Microsoft Sentinel

Microsoft Sentinel

Resource tags

Resource Tags



Basics

This is used to add metadata to your resources.

Costing

Tags can offer another way when it comes to filtering on costs.

Application

Tags can be applied to resources, resource groups and subscriptions.

Inheritance

If a tag is applied at a resource group level, it is not applied to the resources in the resource group.

Design Identity and Security

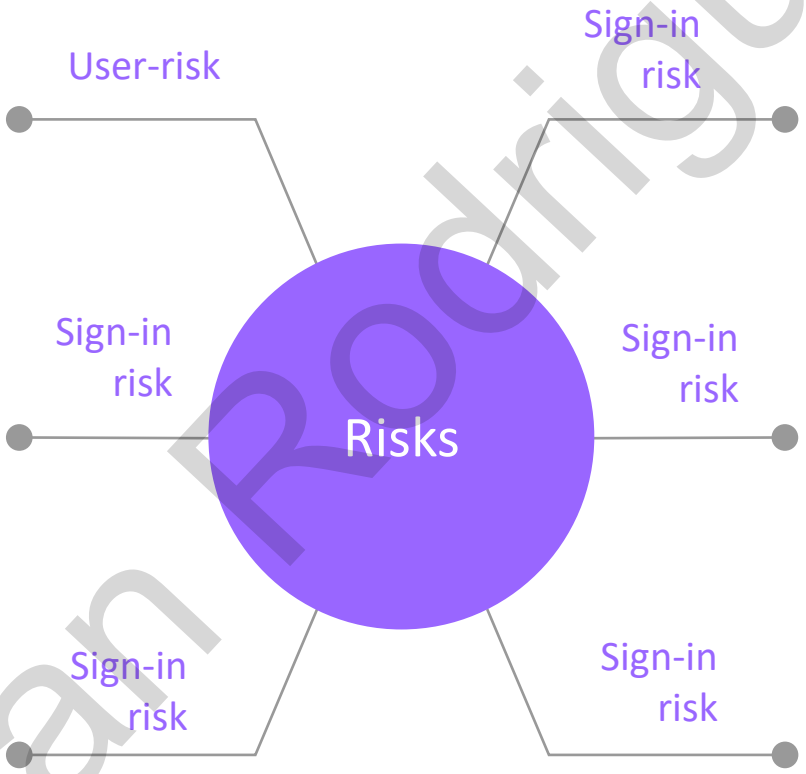
Identity Protection

Identity Protection

Has the ability to automatically detect and remediate identity-based risks

Uses its own threat intelligence to understand identity-based risks

The different risks



Leaked credentials

This detects if the users' credentials have been leaked

Anonymous IP Address

Anonymous IP address – The user is not signing in from a typical IP address

Atypical travel

Here sign-ins are happening from different geographic locations

Malware

Here the user's device could be infected with a malware

Password spray

Someone is trying out different passwords

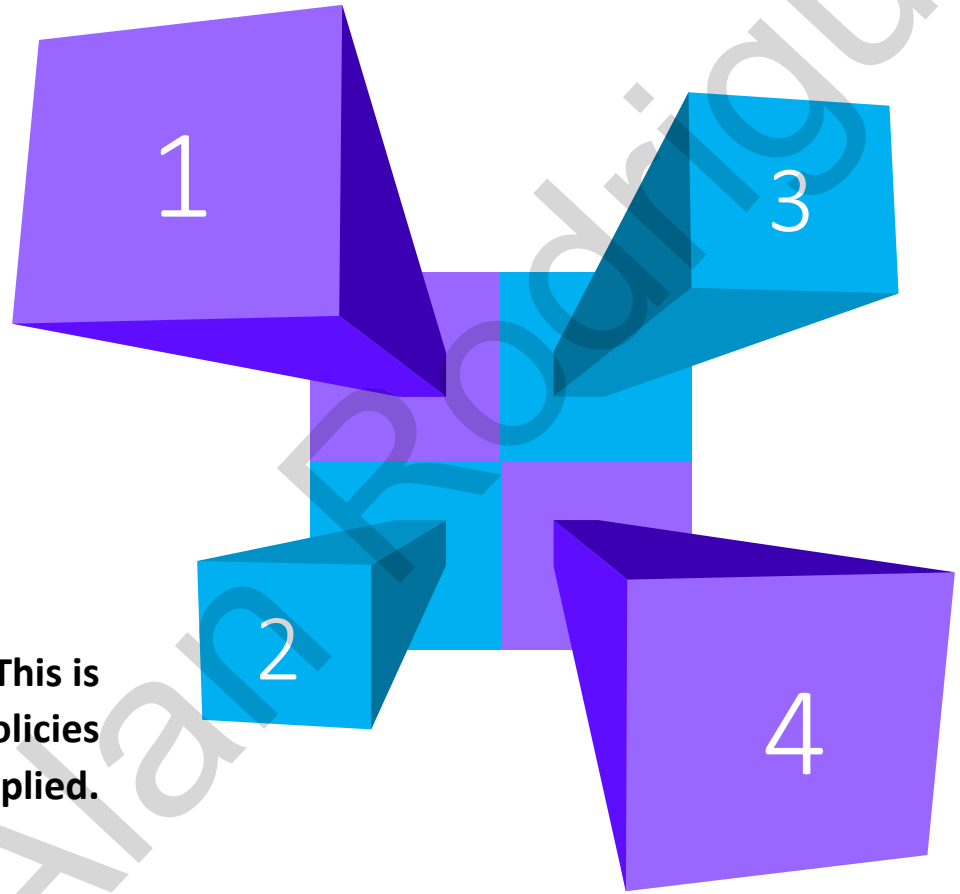
Unfamiliar sign-in properties

Not the typical behavior the user sign ins

Azure Blueprints

Azure Blueprints

Role assignments – If you need specific roles to be assigned.



Resource groups – If you need certain resource groups to be in place.

Policy assignments – This is if you need specific policies to be applied.

Azure Resource Manager templates – If there are resources that need to be deployed.

Azure Blueprints - Stages

Definition – Here you define the Blueprint itself. The Blueprint needs to be saved to either a management group or a subscription.

When you save the Blueprint to a management group, the Blueprint can be assigned to any subscription which is part of the management group.

To save the Blueprint definition, you need to have Contributor access to either the management group or the subscription.

Azure Blueprints - Stages

Publishing – Once the Blueprint is defined, you can publish it. Here you can assign a version number for the Blueprint.

Assignment – Here the Blueprint is then assigned to a subscription.

You can protect resources deployed via the Blueprint resource locks.

Here even if there is a user with the Owner role, still the user will not be able to remove the lock.

You can only remove the lock by unassigning the blueprint.

Design Data Storage

SQL Server on Azure

Microsoft SQL Server on Azure - IaaS

You can use the Infrastructure as a service facility wherein you deploy Microsoft SQL Server on an Azure Virtual machine.

This will give you complete administrative access over the virtual machine.

Here you can also use the pay-as-you-go model when using SQL server on an Azure virtual machine.

This provides an easy option for migrating your on-premise SQL Server workloads.

Here you can install the version of SQL Server that you require.

And then migrate the data onto the instance on the Azure virtual machine.

Microsoft SQL Server on Azure - PaaS

Then you have the Platform as a service wherein you can use the Azure SQL database service.

Here the underlying compute infrastructure is managed by Azure.

Here you also get an SLA of 99.995%.

With Azure SQL database server, you can choose from a variety of pricing tiers.

Here you can also make use of features such as Automated backup, Automated tuning, simplified patching etc.

Azure SQL Managed Instance

Azure SQL Managed Instance – This is an ideal option also for migrating existing SQL Server workloads onto Azure.

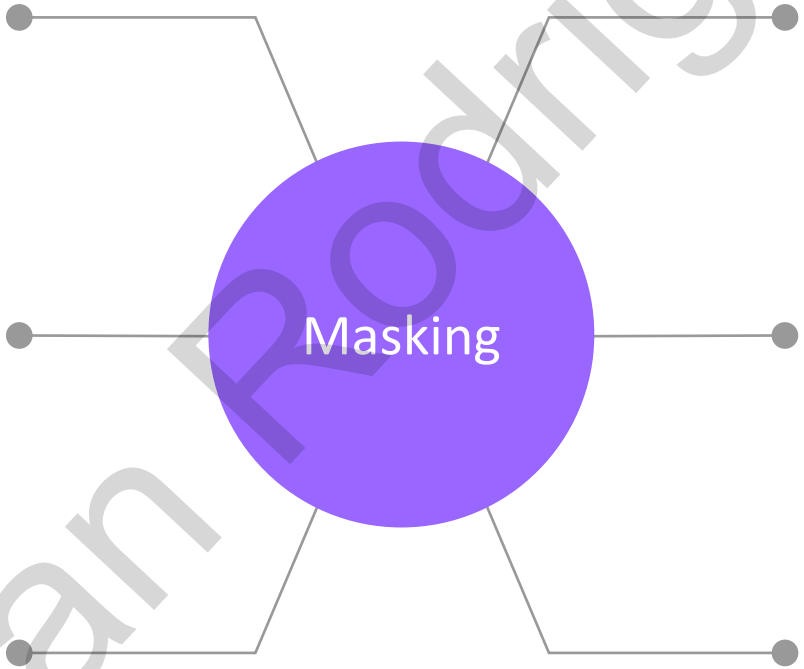
SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine.

You can also get native Virtual Network Integration.

You can also use the Hybrid benefits to use your own licenses to save on costs.

Dynamic Data Masking

Dynamic Data Masking



Exposure

Here you can limit the exposure of data.

Rule

You can create rules to mask the data.

Credit Card masking rule

This is used to mask the column that contain credit card details. Here only the last four digits of the field are exposed.

Email

Here first letter of the email address is exposed. And the domain name of the email address is replaced with XXX.com.

Custom text

Here you decide which characters to expose for a field.

Random number

Here you can generate a random number for the field.

Always Encrypted

Always Encrypted feature

The Always Encrypted Feature can be used to encrypt data at rest and in motion.

You can encrypt multiple columns located in different tables.

You can encrypt multiple columns located in the same table.

You can just encrypt one specific column.

Always Encrypted feature

You have 2 types of encryption

Deterministic encryption – Here the same encrypted value is generated for any given plain text value. This is less secure. But it allows for point lookups , equality joins, grouping and indexing on encrypted columns.

Randomized encryption – This is the most secure encryption method. But it prevents the searching, grouping , indexing and joining on encrypted columns.

Always Encrypted feature

We can enable the Always Encrypted feature using SQL Server Management Studio.

There are 2 keys that get created when the Always Encrypted feature is enabled for a database.

Column master key – This is an encryption key that needs to be stored in an external data store. Here you can store the key in a Windows certificate store or in the Azure key vault service.

Column Encryption key – This is generated from the column master key and is used to encrypt the actual column.

The user who is implementing the Always Encrypted feature needs to have the following permissions for keys – *create, get, list, sign, verify, wrapKey, unwrapKey*

Mapping Data Flows

Mapping Data Flows

This feature helps to visualize the data transformations in Azure Data Factory.

You can write the required transformation logic without actually writing any code.

The data flows run on Apache Spark clusters. Azure Data Factory will manage the transformations in the data flow.

Mapping Data Flows

Debug Mode – You can actually see the results of the data flow while designing the flow.

In the debug mode session, the data flow will run interactively on the Spark cluster.

In the debug mode, you will be charged on an hourly basis for the active cluster.

Design Business Continuity

Blob data protection

Azure Blob data protection

Blob soft delete – This helps to protect the individual blob from accidental deletes.

Here the deleted data is kept in the system for a defined duration of time.

You can then restore a deleted object.

You can specify a retention period between 1 and 365 days.

You also have the soft delete for containers to protect the entire container from accidental deletion.

Azure Blob data protection

Versioning – This can be used to maintain the previous version of a blob.

When a blob is modified a new version ID is created for the blob.

Blob snapsthots – This is a read-only version of a blob taken at a particular point in time.

Design Infrastructure

Design Infrastructure

Migrating solutions – Start a base wherein you start deciding on the compute infrastructure.

We already covered a lot when it comes to compute infrastructure.

Initially review Azure VM's vs Azure Web Apps and then look at the Azure Batch Service.

Then we will look at Container-based services – Azure Container Instances, Container Registry, Azure Kubernetes.

Azure File Sync when it comes to bringing files in Azure File shares closer to your on-premises users.

Design Infrastructure

Networking perspective – Review on Virtual Network Peering, VPN connectivity, VirtualWAN.

Internal Azure Load Balancer for SQL Server hosted on Azure VM's.

Review on the Azure Application Gateway.

Look at other routing tools – Azure Traffic Manager and Azure Front Door.

Design Infrastructure

Development Services – Review on Azure Event Hubs.

Look at Azure Functions, Azure Service Bus, Azure Logic Apps, Azure Event Grid.

Implementation scenarios – Azure Service Bus, Azure Functions, Azure CosmosDB.

See how to make use of Azure API Management Instance.

Design Infrastructure

Azure DevOps services – Continuous Integration and Continuous Deployment.

Azure Boards – Epics, Stories and Tasks.

Azure Repos – Git-based repositories.

Azure Pipelines – Build and Release pipelines.

How to integrate ARM templates in pipelines

Design Infrastructure

Migration Patterns – How to migrate applications.

Data transfer options.

Database Migration Service.

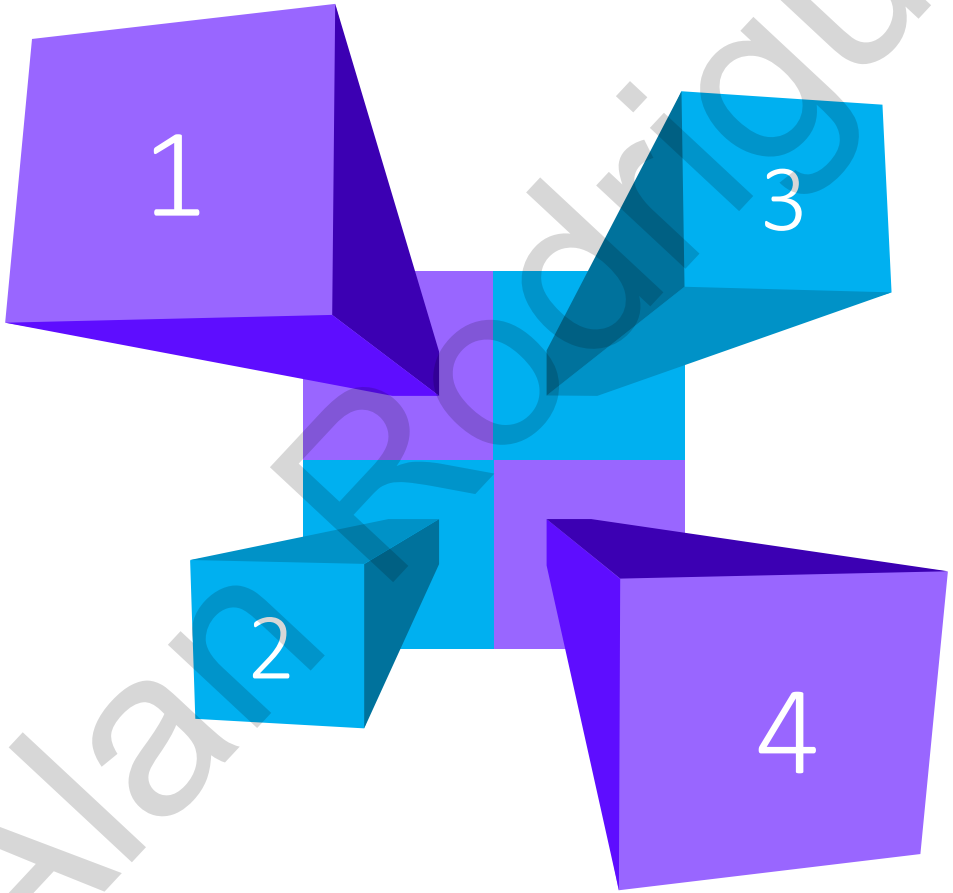
Exploring the Azure Migrate tool.

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.

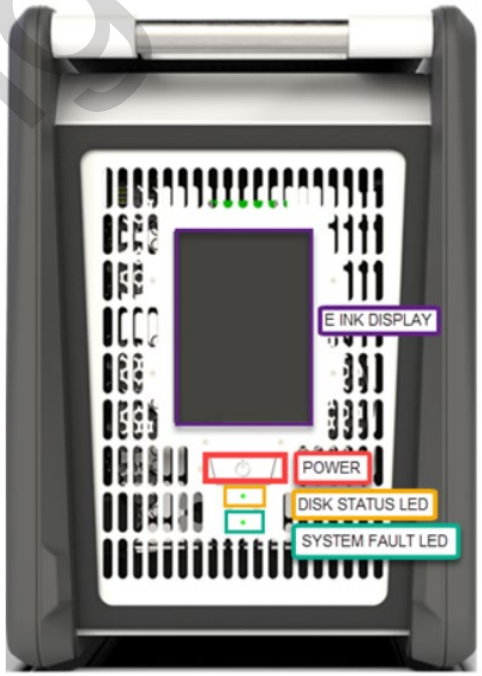
Jobs

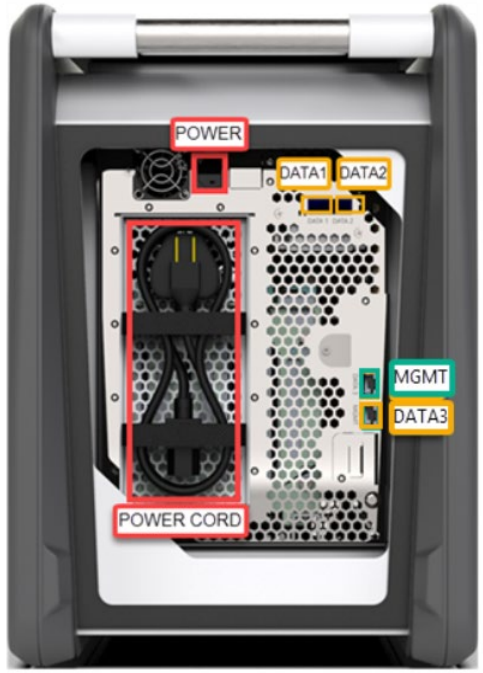
You basically create a job via the Azure Portal. This will be used for transferring data to a storage account.

Azure

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.





Network Watcher Service

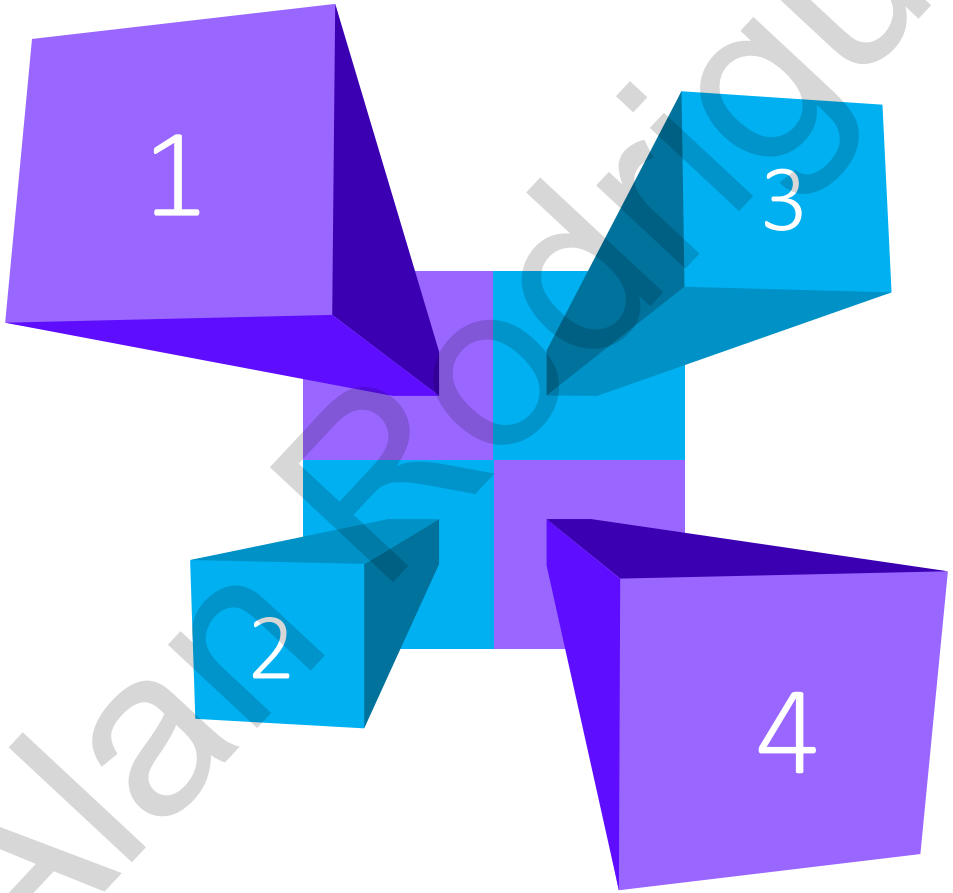
Network Watcher service

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.

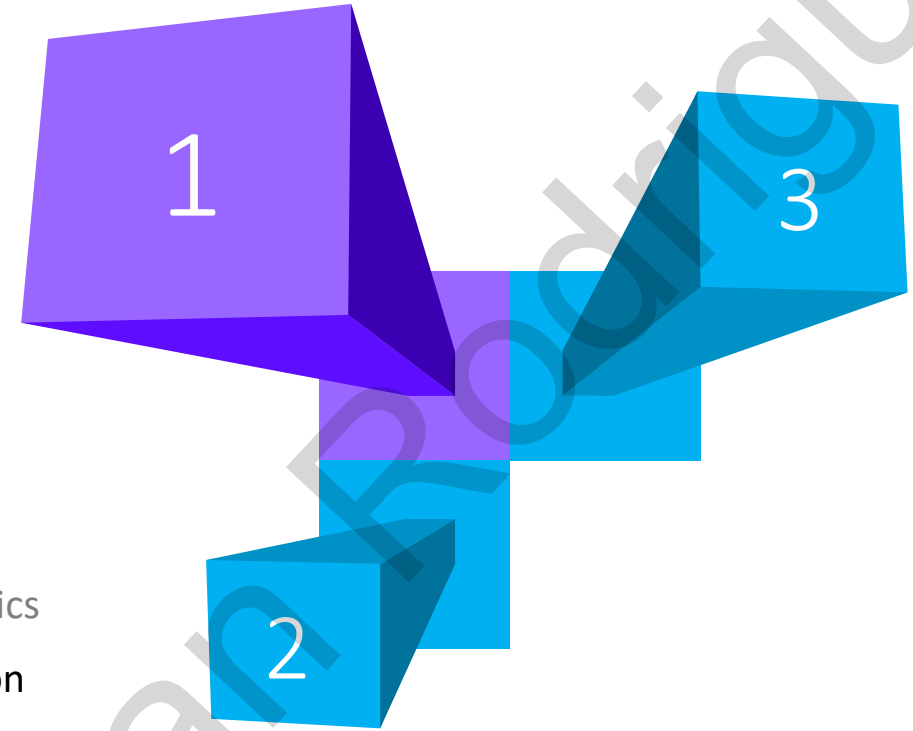
Connection troubleshoot

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.

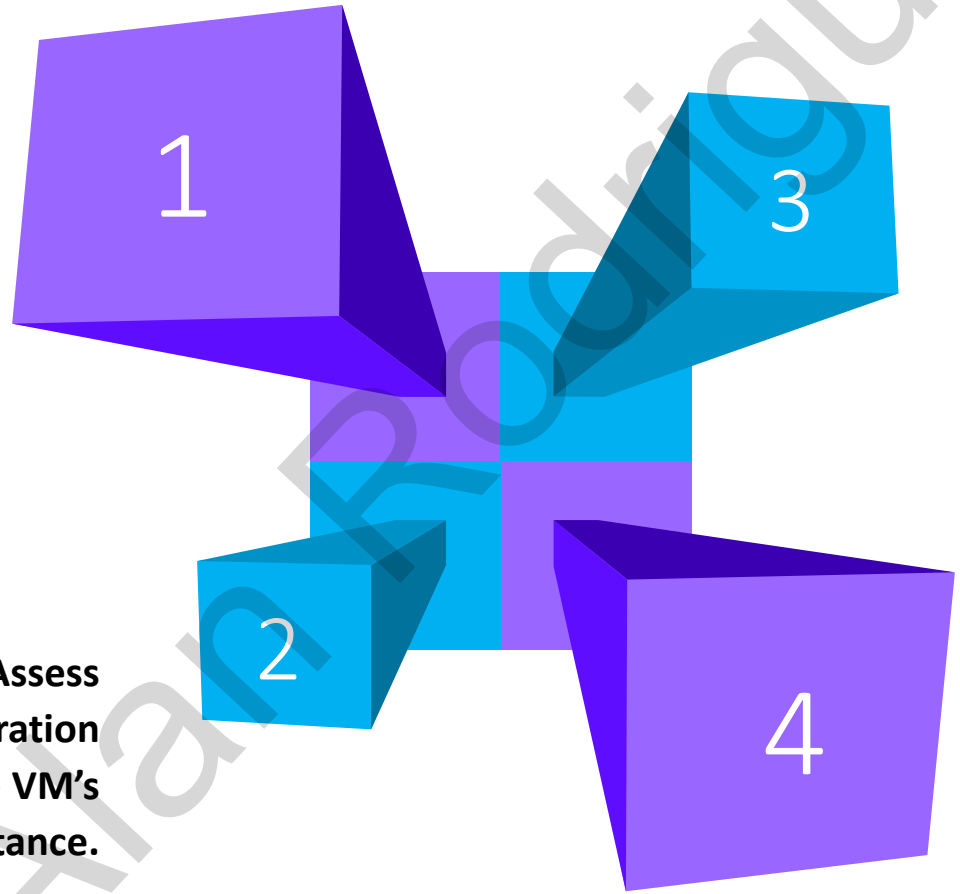
Azure Migrate

Azure Migrate

- You can use this tool to assess and migrate assets such as Servers, databases and web applications.
- You can also assess the on-premises virtual desktop infrastructure and migrate it to Azure Virtual Desktop.
- You have tools such as Azure Migrate: Discovery and assessment, Data Migration assistant, Azure Database Migration service, Web app migration assistant.

Azure Migrate tools

Azure Migrate: Discovery and assessment – On-premises servers running Hyper-V and VMware.



Azure Database Migration Service – Migrate on-premises databases to Azure VM's with SQL, Azure SQL database, Managed Instances.

Data Migration Assistant – Assess SQL Server databases for migration to Azure SQL database, Azure VM's and SQL Managed Instance.

Web app migration assistance – Assess and migrate web apps to Azure.

Azure Migrate

Azure Migrate

Azure Migrate: Discovery and assessment tool

- You can assess whether you're on-premises servers, SQL servers and web applications are ready to be migrated to Azure.
- You can also get an estimation when it comes to the size of the Azure VMs and the Azure SQL databases required to host your workloads.