Get the best out of Live Sessions

HOW?

Check your Internet Connection

Log in 10 mins before, and check your internet connection to avoid any network issues during the LIVE session.

Speak with the Instructor

By default, you will be on mute to avoid any background noise. However, if required you will be **unmuted by instructor**.

Clear Your Doubts

Feel free to clear your doubts. Use the "**Questions**" tab on your webinar tool to interact with the instructor at any point during the class.

Let us know if you liked our content

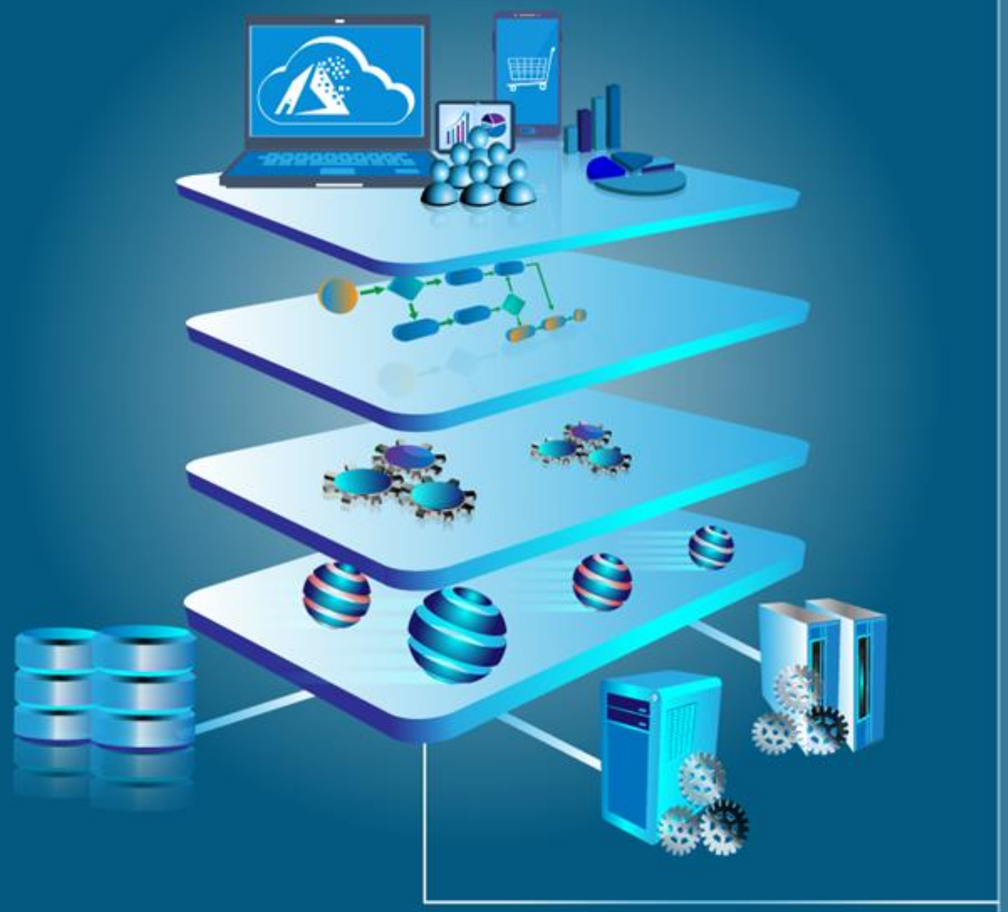
Please share feedback after each class. It will help us to enhance your learning experience.

edureka!

edureka!

Microsoft Certified Expert: Azure Solutions Architect (AZ-303) & (AZ-304)

COURSE OUTLINE



Module 11

Introduction to Microsoft Azure and Its Services

Azure Virtual Machines and Networking

Azure VMSS and Availability zones

Azure App Services and Its Features

Advanced Azure Hybrid Connectivity and Site Recovery

Azure Storage Solution and Design Patterns

Azure Kubernetes Service

Azure Active Directory and Role Based Access Control

Azure Messaging Service (Events, Hubs, Queue and Bus)

Azure Monitoring and Insights Service

Design Identity & Security & Design Storage

Design Azure Migration

Design Monitoring

Design Business Continuity

Module 11 – Design Identity & Security & Design Storage

edureka!

Topics

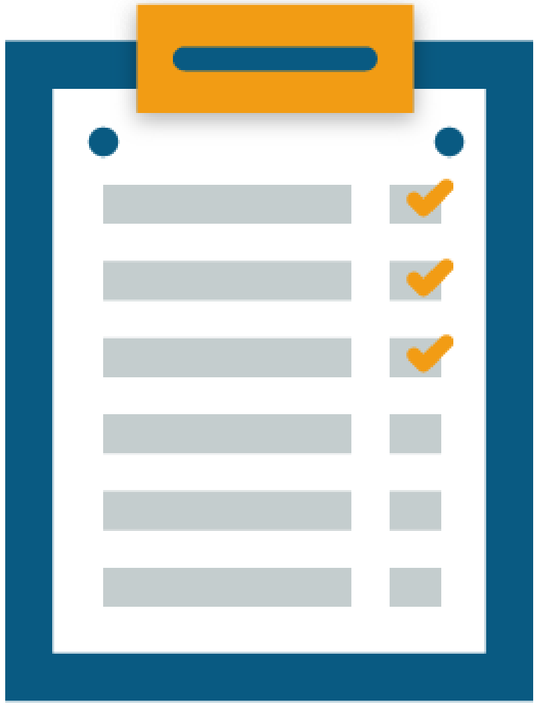
Following are the topics discussed in this module:

- Authorization and Authentication
- Authorization and Authentication Protocols
- Azure AD B2B B2C Security and Risk
- Management PIM Licensing & Compliance
- Understanding Azure Storage Setting Up Azure
- Storage Designing Storage Access Storage
- Demo: Using OAuth & OpenID
- Demo: Conditional Access Demo:
- Demo: Storage Account Creation and Shared Access Signatures

Objectives

After completing this module, you should be able to:

- Understand Azure Security & Storage from a design perspective
- Understand Authentication & Authorization Process
- Explore Security & Risk Management
- Design & Setup Cloud Security and Storage



edureka!

Design an Identity Solution

Managed Identities

Managed Identities aims at delegating complex identity management and User Authentication to a trusted third party so the organisation can focus on business logic and development

What would third party do:

- Manage identity management/authentication & assign tokens to authenticated user
- Based on tokens you can decide on granting/denying access and planning security

Key Terminologies

Claim-based architecture
It is a system design using an external party that manages identities and is also called a claim-based architecture.

Claim
It is an assertion that is made on an attribute of an entity. Any party is free to make assertions. But you should only trust claims from a trusted authority

Security token
A collection of claims is called as Security Token. It is digitally signed, encrypted to maintain its security.

Key Terminologies

Service Provider (SP) or Relying Party (RP)
A Service Provider (SP) is responsible for providing requested services. In context to claim-based architectures, an SP is also known as Relying Party, as it relies on a third-party to manage identities

Identity Provider
This body authenticates entities & issues security tokens to Dependent Parties. An Identity Provider offers numerous ways for an entity for authentication

Trust
Identity Provider and a Service Provider agree to common rules, and this is called as Trust. A Service Provider assumes a security token to be true since it is issued by a trusted party.

Authentication

The process where we identify what the given identity is what it claims to be is called as Authentication

- Microsoft Azure includes features, **like Azure Multi-Factor Authentication (Azure MFA)** and **Azure self-service password reset (SSPR)**, to help administrators protect their organizations and users with additional authentication methods

- Azure MFA and SSPR give admins control over configuration, policy, monitoring, and reporting using Azure portal to protect their organizations

- Additional verification may come in the form of authentication methods such as:

  - A code through email or message
  - A phone call
  - Password
  - Digital Certificate

edureka!

Authorization

edureka!

Understanding Authorization

1. Authorization occurs after your identity is successfully authenticated by the system, which therefore gives you full access to resources such as information, files, databases, funds, etc.

2. Authorization verifies your rights to grant you access to resources only after determining your ability to access the system and up to what extent

3. Authorization is the process to determine whether the authenticated user has access to the particular resources

4. A good example of this is, once verifying and confirming employee ID and passwords through authentication, the next step would be determining which employee has access to which floor and that is done through authorization

Protocols

edureka!

Protocols

Protocols are agreed processes, language or a framework that tell how to authenticate or authorise. In simple words how do we perform actions on behalf of a user

Types

OAuth 2.0

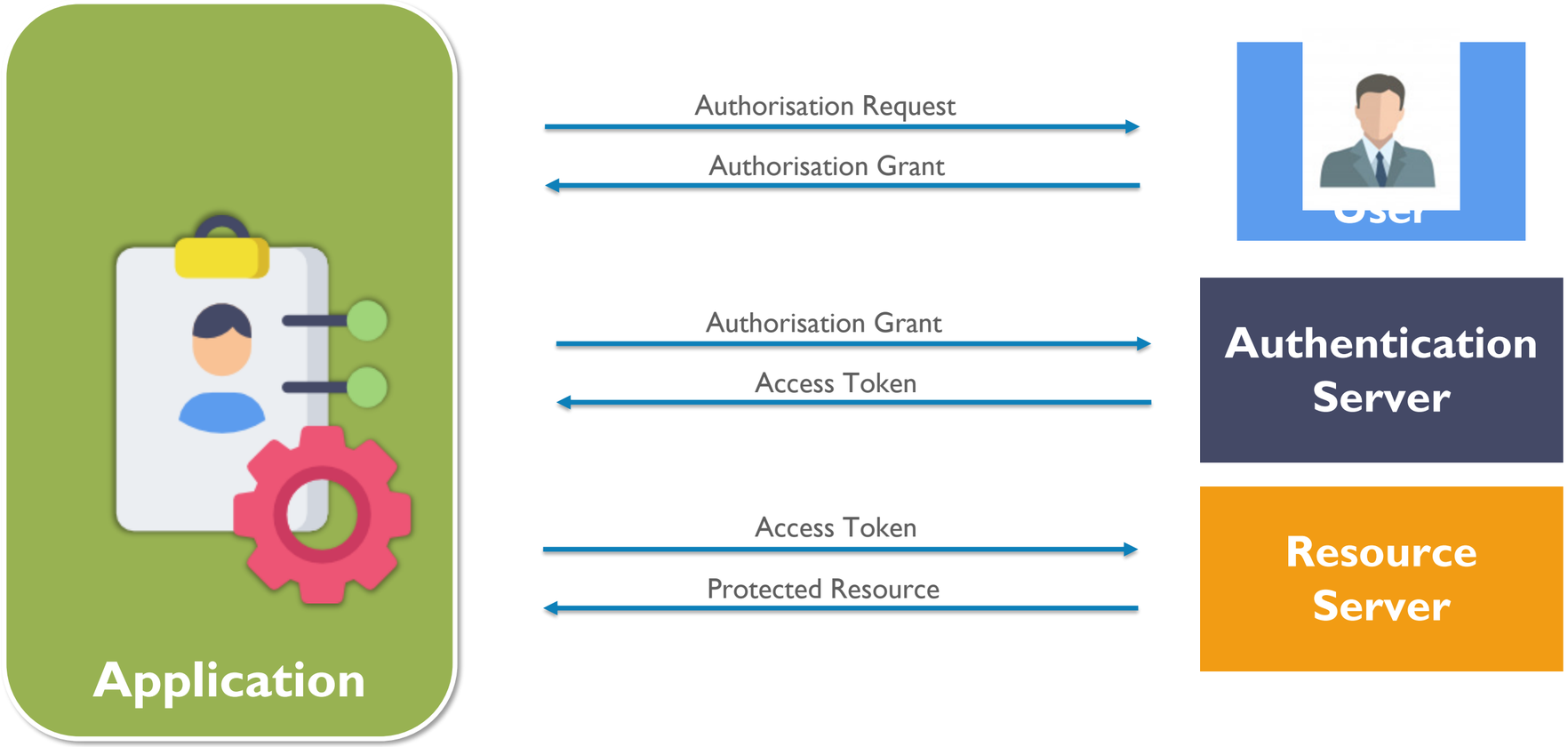
OpenID

SAML 2.0

WS-Fed

OAuth 2.0

OAuth 2.0 is a framework for authorization that lets applications, obtain limited access to user accounts through HTTP service for example Facebook, GitHub etc.



OAuth 2.0 Steps

01 Application will send authorization request to access service resources from the user. If the approved application will receive authorization Grant

02 Next, the Application will request for access token from the authorization server (API) by presenting its identity and the authorization grant received

03 If the authentication and the authorization grant is valid, the API issues an access token to the application. Now, Authorization is complete

04 The application will request the resource from the API & present the access token for authentication

05 With a valid token, the API serves the resource to the application

edureka!

OpenID

It is an authentication protocol built on OAuth 2.0 that is used to securely sign in a user to an application.

OpenID: Sign-In Flow Steps

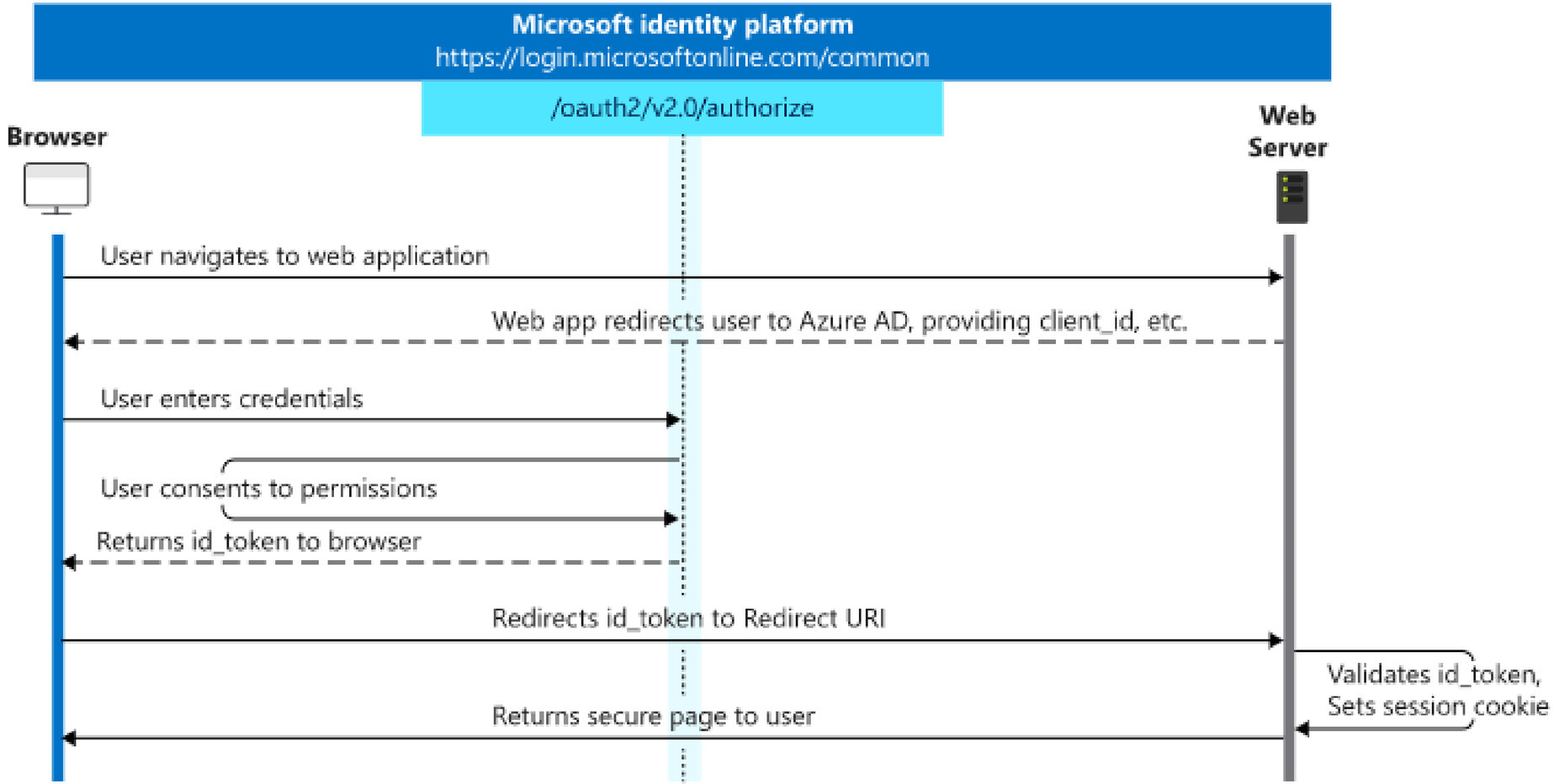


Image Source: https://bit.ly/3b1WZuo

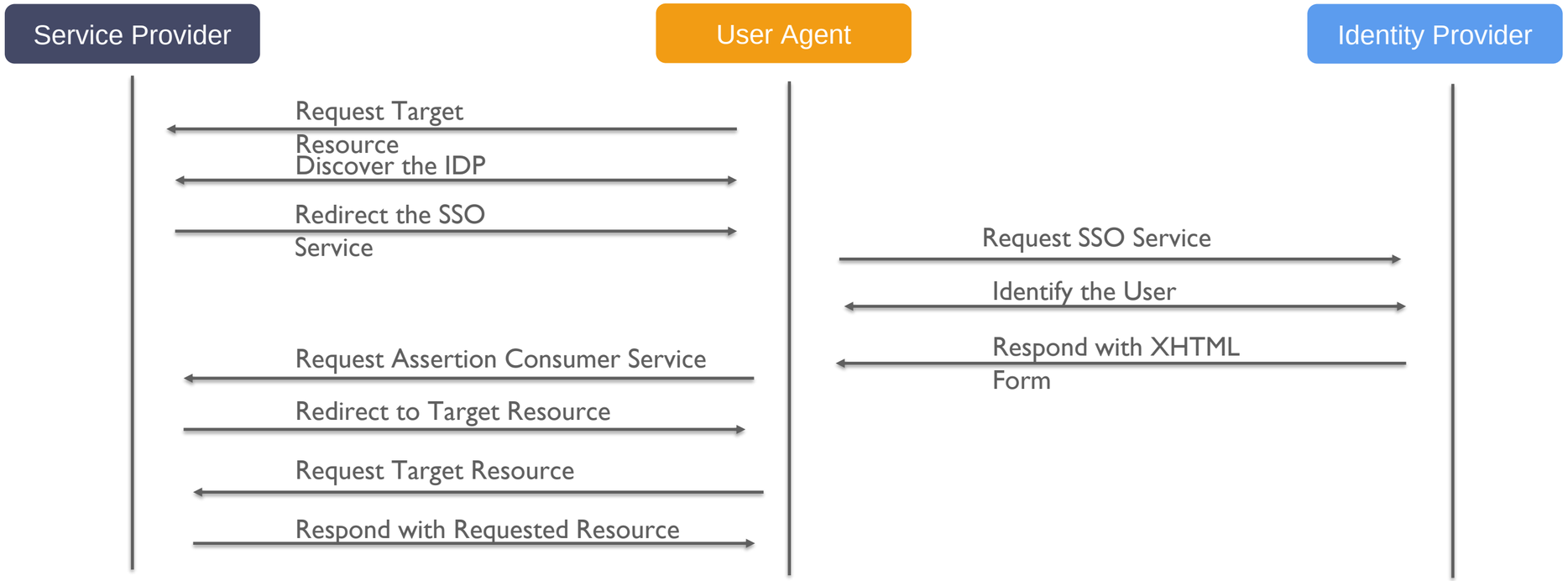
Demo: Using OAuth2.0 &OpenID

Note: Refer to Module-11 Demo-1 file on LMS for all the steps in detail

edureka!

SAML

SAML stands for Security Assertion Markup Language. It is an XML-based data format which is used for exchanging authentication and authorization data between parties(identity provider & service provider)



Steps involved in authentication process

WS-Fed

1. WS-Fed is part of the larger WS-Security framework and hence is an extension to the functionality of WS-Trust
2. Its Features can be used by SOAP apps and web services. It is a protocol used to negotiate the issuance of a token.
3. You can use this protocol for your apps such as Windows Identity Foundation-based app
4. It can be used for identity providers example AD Federation Services or Azure AppFabric Access Control Service

Azure AD B2C & B2B

edureka!

Azure AD B2C

Azure AD B2C is ***Azure Active Directory Business-to-Consumer***. It handles user account sign-up, sign-in, profile edit & password reset functionalities outside the applications which meet certain specific functionality

- With its own login portal management customized to a certain extent, it can change the look & feel as per customers needs
- It leverages identity stores outside your company & is also is an authentication service for applications that face public
- It readily integrates with other third-party identity providers like, Facebook, Google+, etc

edureka!

Features of Azure AD B2C

Easy Integration

- Avoids hassles of Integrating with social accounts such as Facebook or Google+
- Azure AD B2C, moves this work from developers, so they can concentrate on the core functionalities like development
- IT handles MFA and password SSR with basic configurations application.

Pricing

- It is cost-effective due to reasonable pricing when compared to other providers or for developing your own identity management framework
- With the first 50,000 authentications and users being free

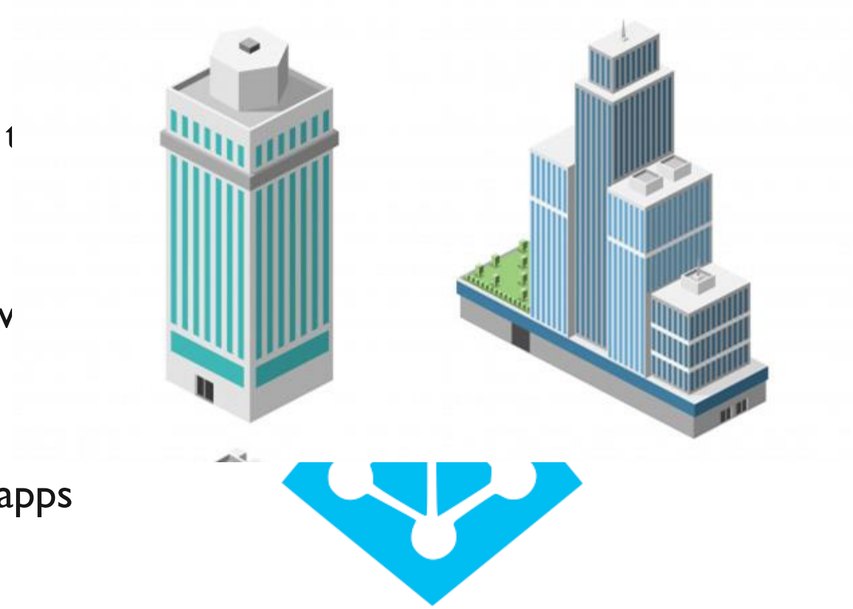
Security

- The authentication system provided is very secure as it protects user identity and credentials.
- It provides identity as a service for apps as it supports two industry standard protocols: OpenID Connect and OAuth 2.0.

Azure AD B2B

Azure Active Directory business-to-business (B2B) collaboration is nothing but a feature within External Identities which lets you invite guest users to collaborate with your organization

- It lets securely share your company's applications & services with guest users from any other organization, at the same time allowing to maintain control over your own corporate data
- You can work safely & securely with external parties, be it large or small, even if t don't have Azure AD or an IT department.
- In the above case, a simple invite & redemption process lets partners use their ov credentials to access your company's resources.
- Developers use Azure AD B2B APIs for customizing invitation process or write apps like SS sign-up portals



PIM: Privileged Identity Management

edureka!

PIM: Privileged Identity Management

It is a service in Azure AD which lets you manage, control, and monitor access to important resources. These resources can be Azure AD, Azure, and other Microsoft Online Services.

- Organizations these days want to minimize access to key resources to prevent malicious activities. But is impossible to restrict access to certain resources for all users, this is where privileged Identity comes into picture

- Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about

PIM: Key Features

- **Just-in-time** privileged access to resources
- **Time-bound** access to resources with start and end dates
- Request **approval** to activate privileged roles
- Enforce **MFA** to activate any role
- Use **justification** to understand why users activate
- **Notifications** on privileged roles being activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit

PIM: Privileges

Administrator Permissions

- Approve Specific Roles
- Specify User & Group Request Approval
- View request & Approval History

Approver Permissions

- View Pending Approvals
- Approve Reject role elevations
- Justify Approval & Rejections

Role User Permissions

- Request activation of role needing approval
- View Request Status
- Complete AD tasks on Approval

Security & Risk Management

- Attackers these days have got more tricks up their sleeves given the increasing computing power at their disposal to attack.
- Hence System administrators are expected to apply smart strategies to shorten to prevent these malicious attackers from gaining ground
- As an Azure Architect, you should be able to consider the following pointers
- There are two main concepts to understand when working with role-based access co
  - Identify, Access & Mitigate risks
  - Learn and practice when to use different protection strategy methods
  - Use Advanced threat Detection methods
  - Design an endpoint protection strategy

Azure Security Center

Azure Security Center is a unified view of security across all the workloads, irrespective of those being on Azure Cloud Platform or On-Premises

With the vast experience that Microsoft as whole possesses, Azure Security Center ensures automatic detection and fixing of vulnerabilities before those get exploited by attackers

On activation, Azure Security Center automatically discovers, onboards, and monitors your resources

It ensures constant evaluation against numerous built-in security assessments 7 notifies you for prompt action

It can be accessed directly from Azure management portal. Security Center portal, gives you a wholistic view over your compute, storage and networking

Operation Management Suite Security

Microsoft Management Suite (OMS) is a hosted IT management solution which manages both, Azure cloud resources and the ones on-premises

It is group of services, that includes Log Analytics, Automation, Backup & Site Recovery. With specific configuration combinations of these that can be packed into Management Solution it is tailored for specific workloads

Insights & Analytics

Monitor and troubleshoot, both, application and infrastructure issues with Log Analytics

Automation & Control

Increase Control using Automation & Configuration Management

Security & Compliance

Secure and Audit your Data Center with complete visibility and advanced Threat Detection

Production & Recovery

Use Cloud Backup & Disaster Recovery

Manage Security Risks

With Hybrid Work Environments, where human intervention is a must, our application & data is at a lot risk enabling lot more opportunities for attackers to exploit loopholes. Microsoft Azure comes with Services that help secure these infrastructures

Azure AD Identity Protection

Advanced Threat Protection

What is Azure Active Directory Identity Protection?

Azure AD Identity Protection is a feature of the **Azure AD Premium P2 edition** that enables you to:

1. Detect potential vulnerabilities affecting your organization's identities
2. Configure conditional access policies to automatically respond to suspicious actions related to your organization's identities
3. Investigate suspicious incidents and take appropriate action to resolve them

edureka!

Identity Protection Capabilities

Detecting Vulnerabilities And Risky Accounts

- Providing custom recommendations to improve overall security posture by highlighting vulnerabilities
- Calculating sign-in risk levels
- Calculating user risk levels

Investigating Risk Events

- Sending notifications for risk events
- Investigating risk events using relevant information
- Providing basic workflows to track investigations
- Providing easy password reset actions

Risk Based Conditional Access Policies

- Policy to mitigate risky sign-ins by blocking them
- Policy to block or secure risky user accounts
- Policy to require users to register for multi-factor authentication

Identity Protection Roles

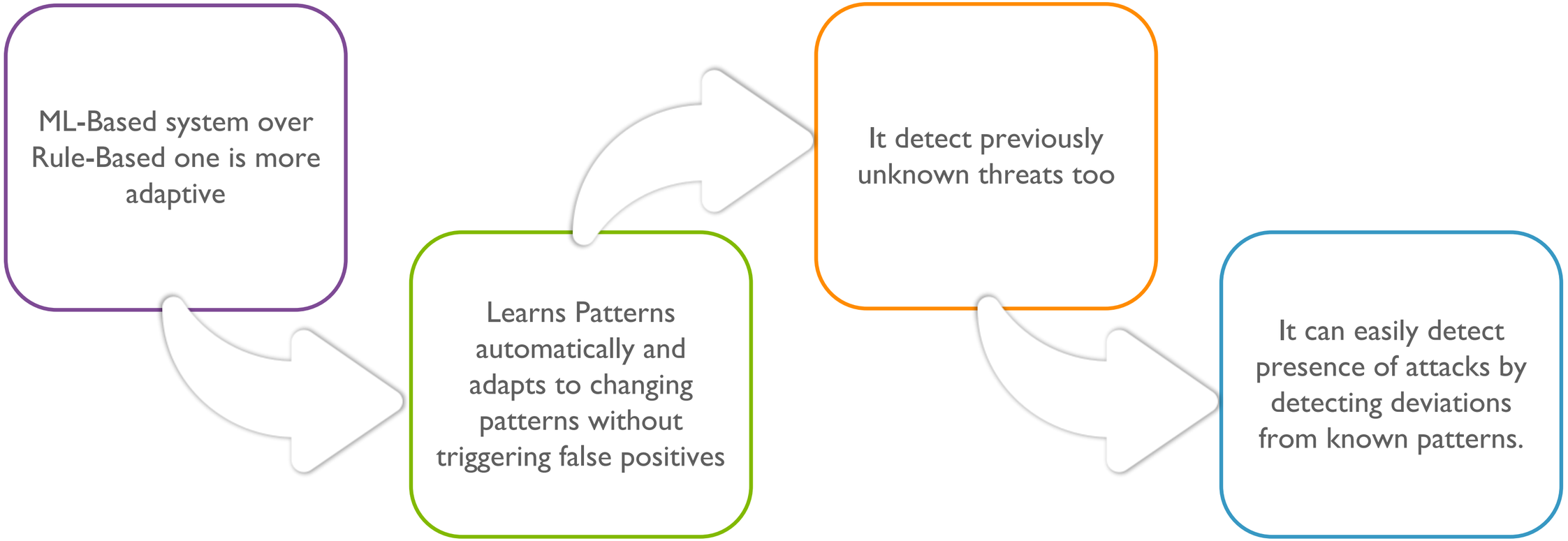
Azure AD Identity Protection supports 3 directory

roles:

Role	Can do	Cannot do
Global administrator	Complete access to Identity Protection and Onboard Identity Protection	Can do everything
Security administrator	Complete access to Identity Protection	Onboard Identity Protection, reset passwords for a user
Security reader	Read-only access to Identity Protection	Onboard Identity Protection, remediate users, configure policies, reset passwords

Advanced Threat Protection

Azure Threat Protection (ATP) uses ML to detect security breaches. It analyzes huge amounts of data & automatically learns working patterns from the data. It can also compare these patterns with existing attack patterns to identify potential attacks.



Azure Policy Compliance

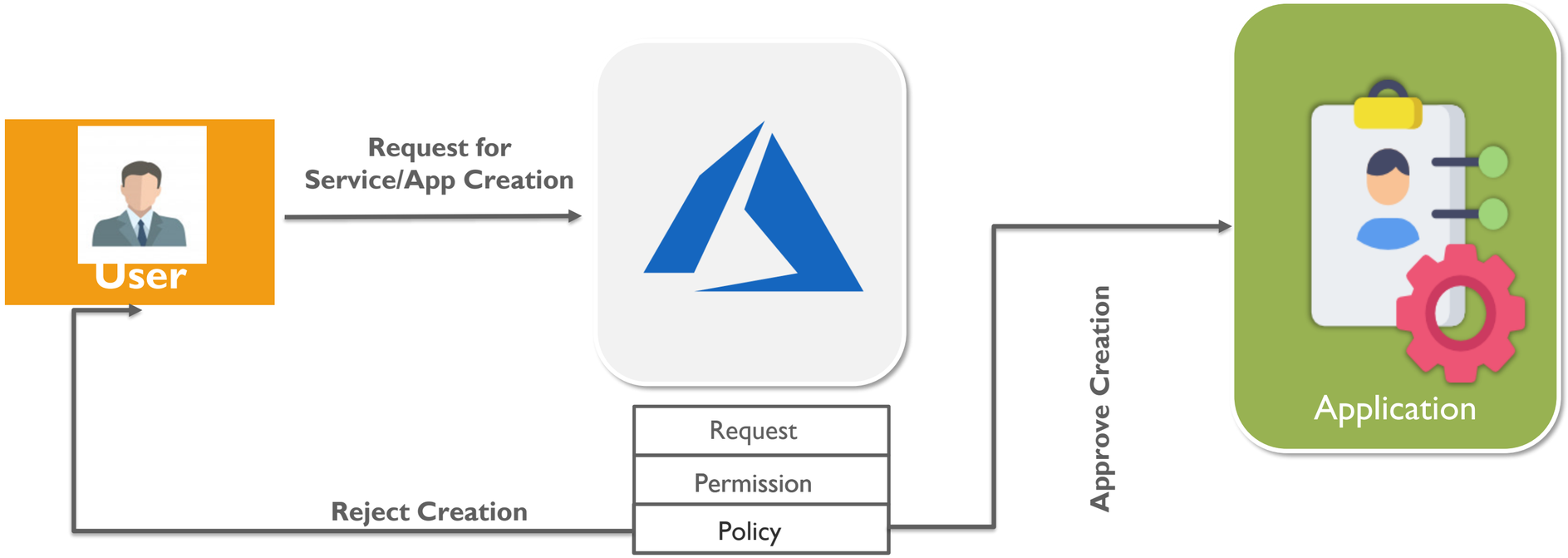
Azure Policy enforces organizational standards to assess compliance at-scale. It uses compliance dashboard, to provide an aggregated view that evaluates an overall state of the environment. It lets you drill down to the per-resource, per-policy granularity

- It provides bulk and automatic Remediation for existing and new resources respectively
- All Data and Objects that fall under Azure Policy are encrypted
- Here are some uses:
  - -Governance for resource consistency
  - -Security
  - -Management
  - -Cost
  - -Regulatory Compliance

When Should You Evaluate A Resource?

- Each time you create, update, or delete a resource which is in a scope with a policy assignment
- Whenever a policy or initiative gets assigned to a scope
- Whenever you update a policy or initiative that is assigned to a scope
- At the time of standard compliance evaluation cycle

Scenario: Azure Policy



Policy is a set of rules that decides a particular action(For ex: User may pass location parameter and policy may decide if to approve creation of service or app)

Microsoft Azure Storage

edureka!

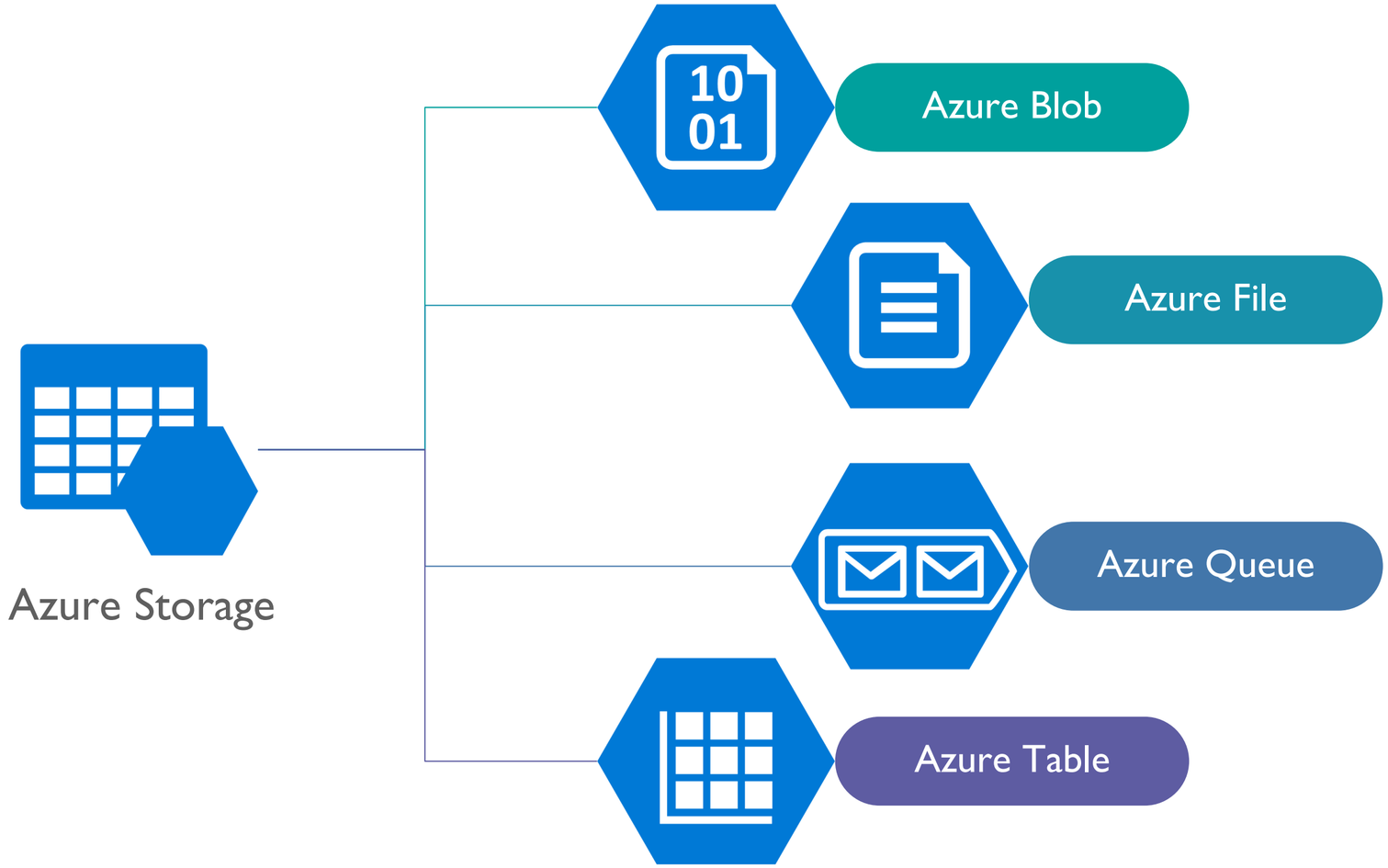
Microsoft Azure Storage – Features

- Cloud storage
- Modern data storage scenarios
- High availability
- Secure and redundant
- Reliable and scalable storage
- Accessible from anywhere
- Managed storage

Understanding Microsoft Azure Storage

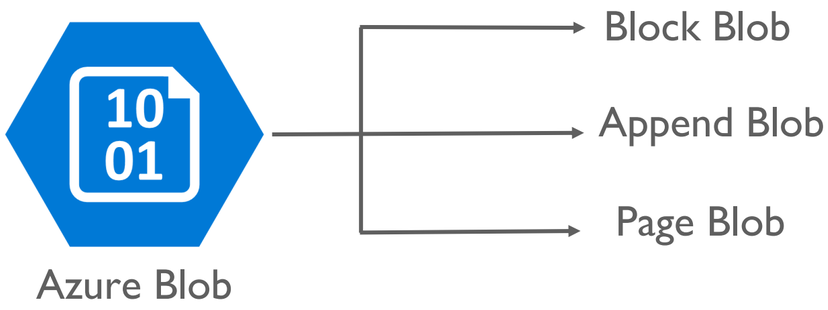
edureka!

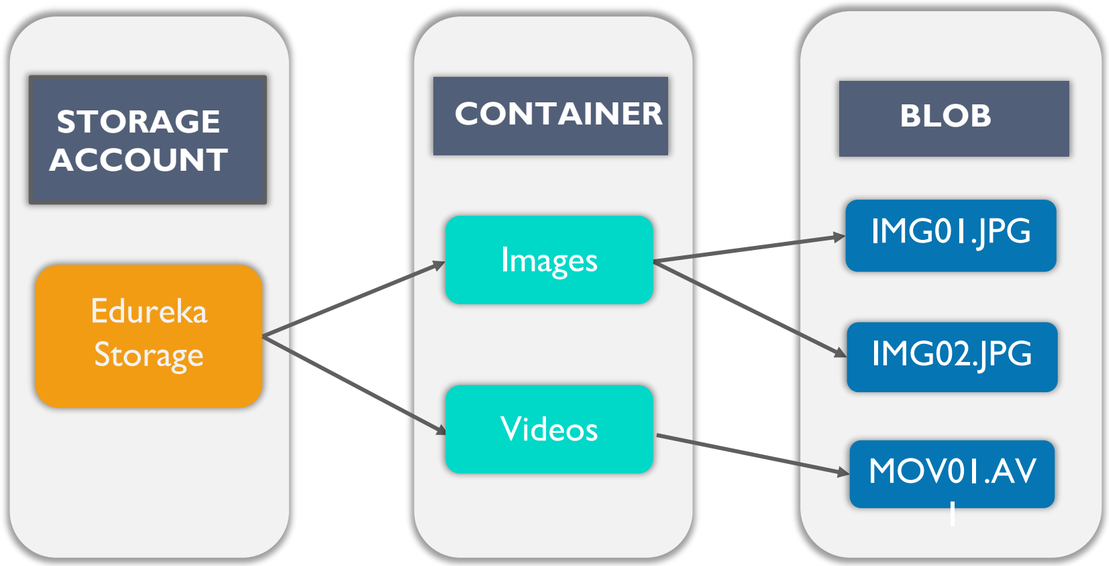
Microsoft Azure Storage Services



Azure Blob

- **Object** storage
- **REST** based object storage
- Ideal to store and stream media
- Secure storage
- Multiple types of Blob storage are available, such as:





Azure Blob Service Components

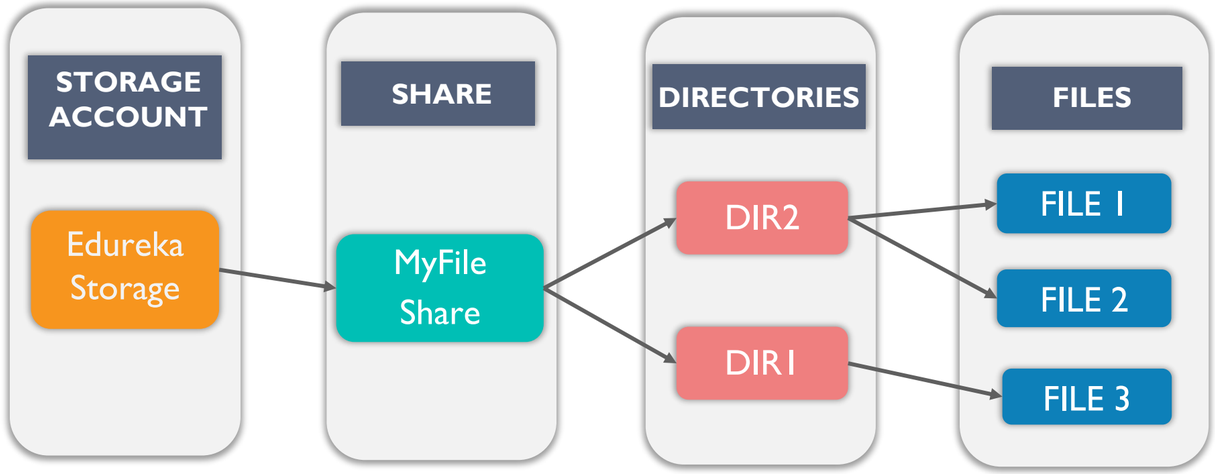
When to Use Azure Blob?

When your application

edureka!

Azure File

- **Fully managed** way to share information between application and users
- It access storage account using **SMB**(Server Message Block) and **REST** from anywhere
- SMB 3.0 and HTTPS is used
- You can mount your Azure file share on **any platform** (Windows, Linux or Mac)
- You can create and manage Azure File Share by using
  - PowerShell cmdlets
  - Azure CLI
  - Azure Portal and Azure Storage Explorer

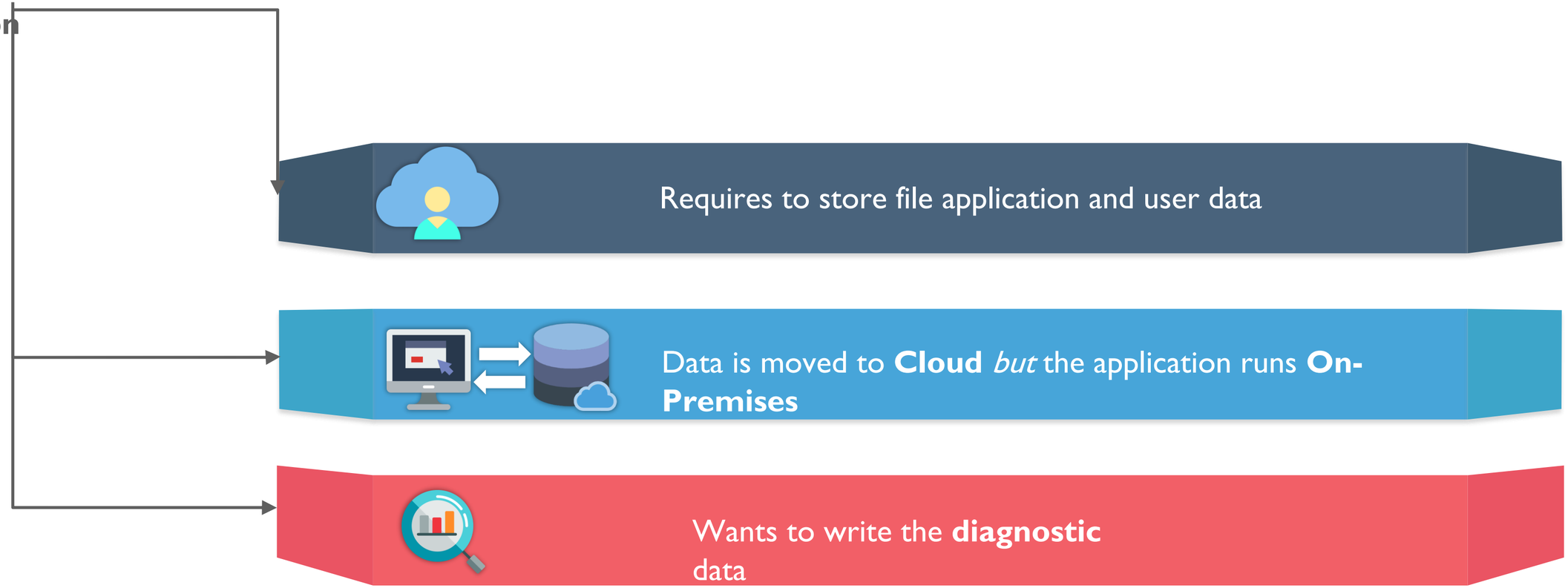


Azure File Service Components

edureka!

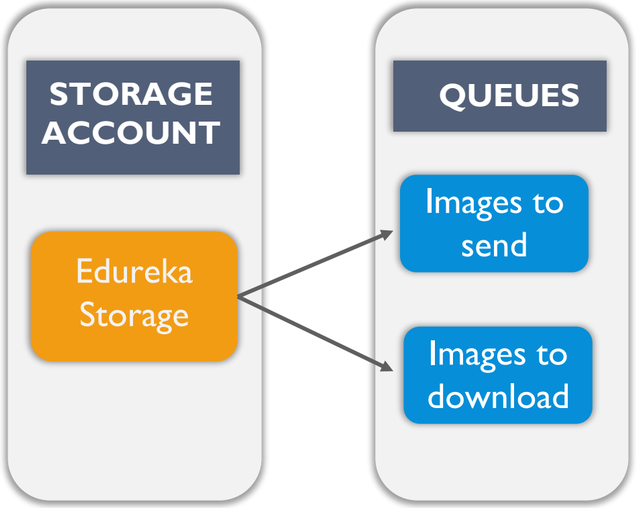
When to Use Azure File?

When your application



Azure Queues

- Stores large number of messages
- Maximum size of a Single Queue is 64KB
- A Queue can contain millions of messages
- Asynchronous messaging



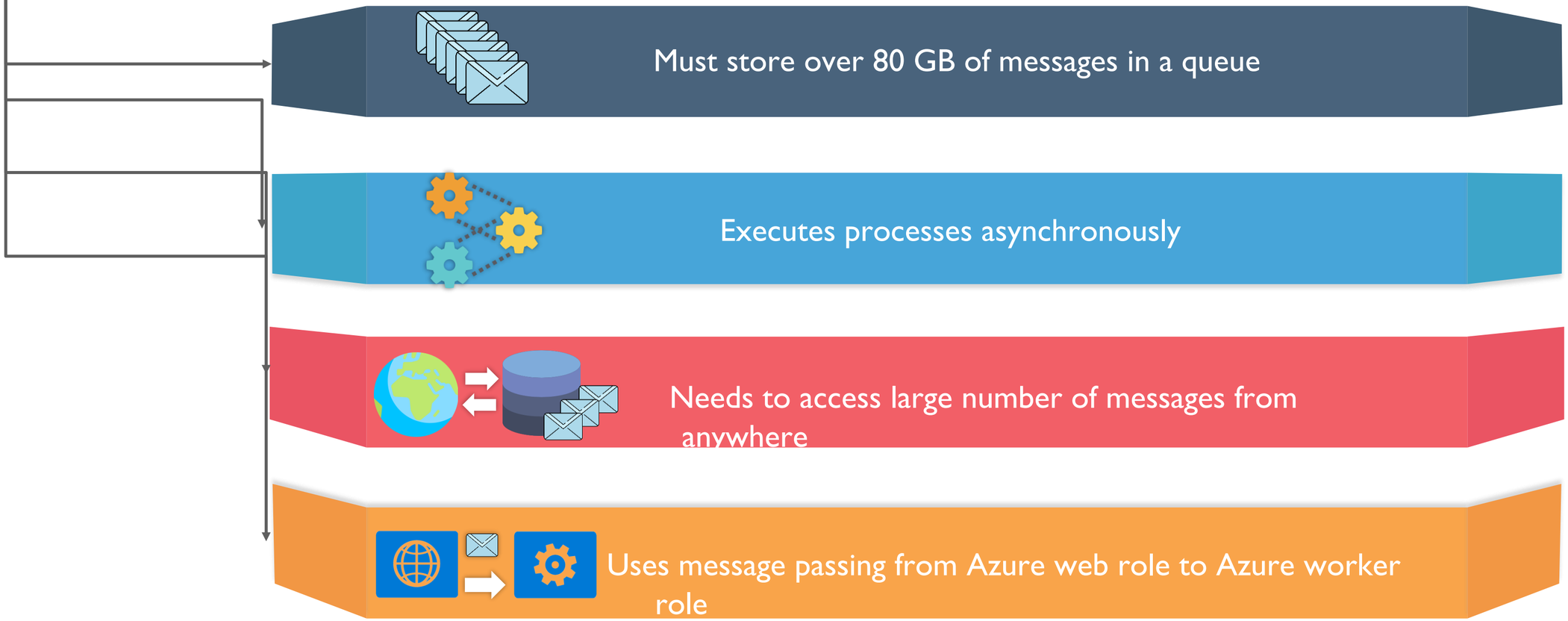
Azure Queue Service Components

The URL format of Queue is : http://<StorageAccountName>.windows.net/<QueueName>

edureka!

When to Use Azure Queue?

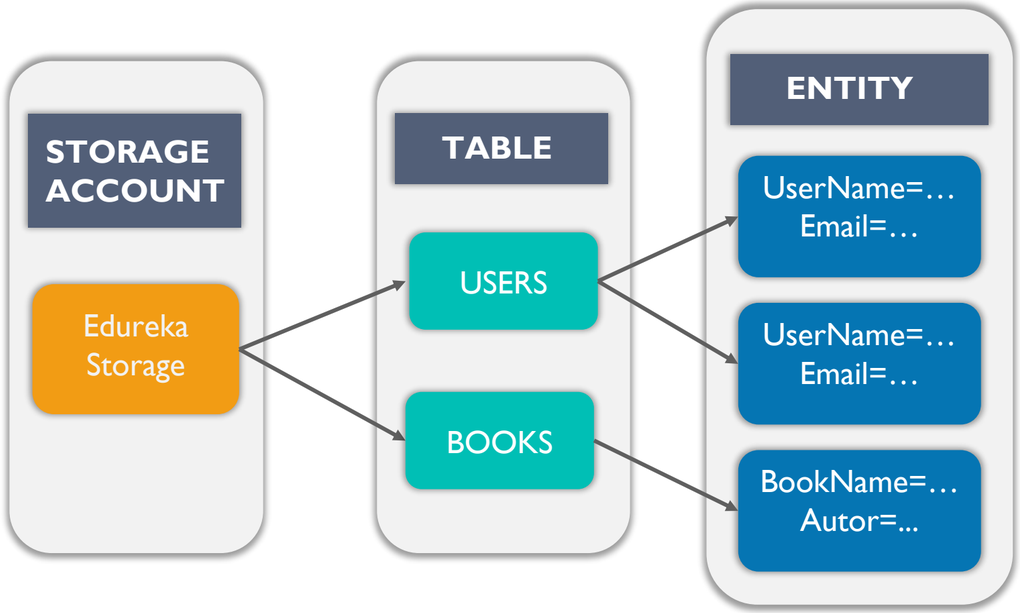
When your application



edureka!

Azure Tables

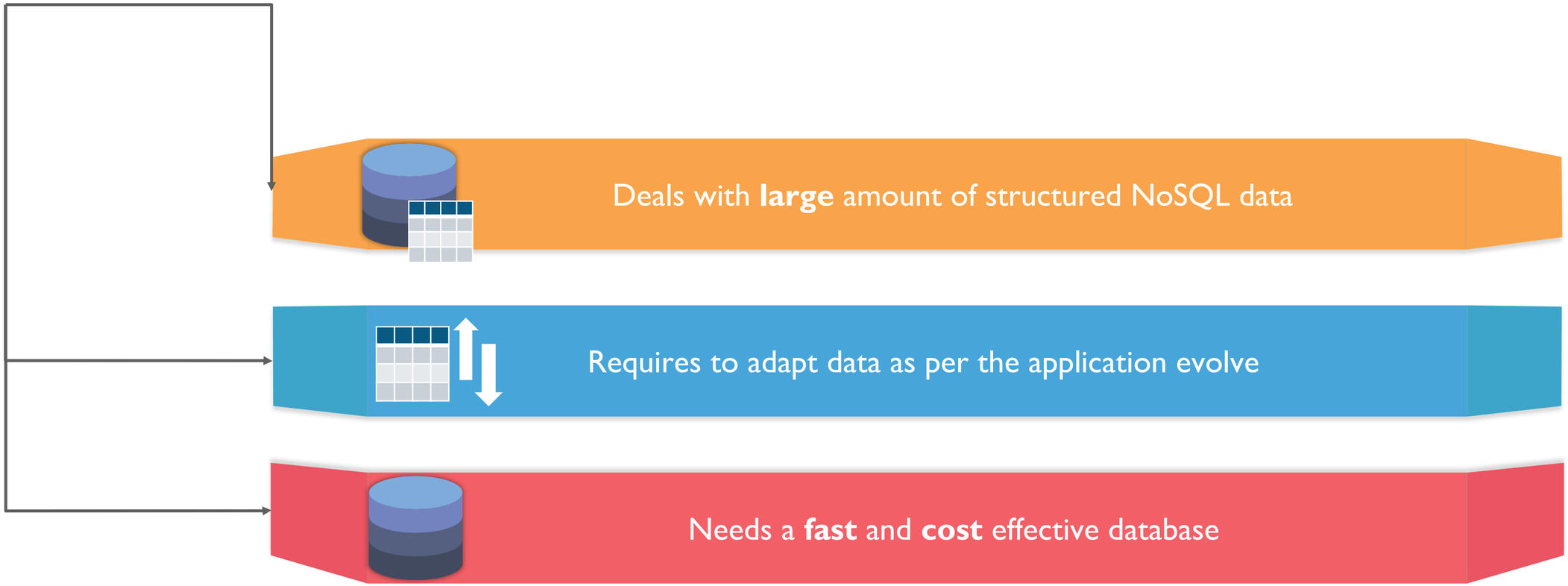
- **Structured** NoSQL data
- Schema less design
- A storage account can have **any number of tables** and the tables can have **any number of entities**, up to the capacity limit of the respective storage account
- **Lower** in cost than traditional SQL
- Transaction calls are from inside and outside of Azure cloud



Azure Table Service Components

When to Use Azure Table?

When your application

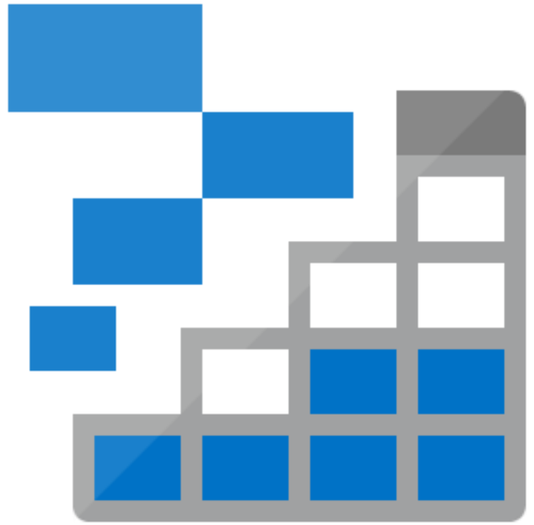


Azure Storage Explorer

Microsoft Azure Storage Explorer is an application that lets you easily connect & work with Azure Storage data on operating systems like Windows, macOS, and Linux.

With Azure Storage Explorer you can easily:

- Access Azure storage account through any device
- Connect to your subscription
- Manipulate your tables, blobs, queues, and files
- Connect & Manipulate Azure Cosmos DB Storage & Azure Data Lake Storage



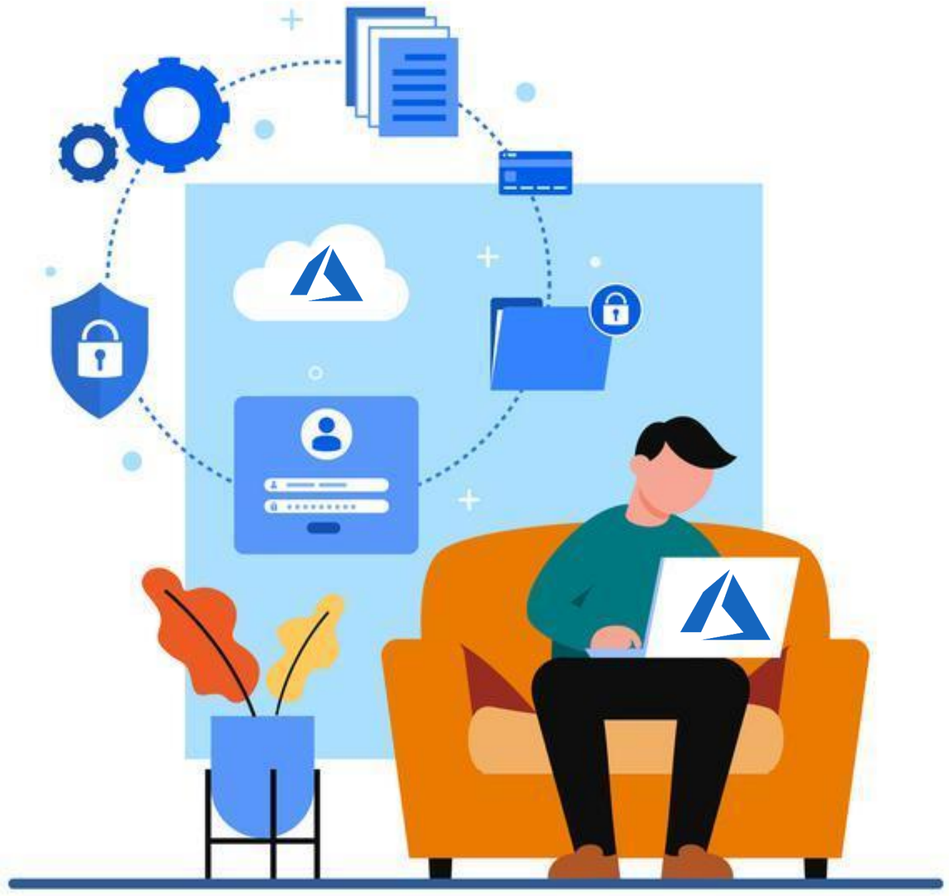
Azure Storage Security

edureka!

Azure Storage Security Features

Azure Cloud Storage Provides various High-Level Security benefits for your data like:

- Data Protection at rest
- Data Protection in transit
- Support for browser cross-domain access
- Control who gets to access your data (RBAC)
- Audit your storage access



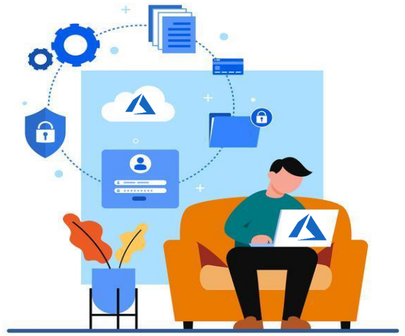
edureka!

Data Protection at Rest

Data written to Azure Storage gets automatically encrypted & also decrypted while reading. It Storage Service Encryption (SSE) with a 256-bit Advanced Encryption Standard (AES) cipher, and is FIPS 140-2 compliant for this process

In case of VM, Azure lets you encrypt virtual hard with Azure Disk Encryption. For Windows images Azure uses BitLocker whereas it uses dm-crypt for Linux

Azure Key Vault helps control and manage the disk-encryption keys and secrets by storing keys automatically. Hence even if people get access to the VHD image and download it, they can't access the data on the VHD

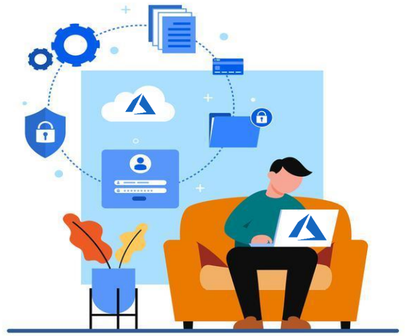


Data Protection in Transit

You can keep your data secure in transit by enabling *transport-level security* between Azure you. It is one uses *HTTPS* to secure communication over the public internet

you can enforce the use of HTTPS by requiring secure transfer for the storage account, when you call the REST APIs to access objects in storage accounts,

Once secure transfer is enabled, connections that use HTTP will be refused. This will also enforce secure transfer over SMB by requiring SMB 3.0 for all file share mounts.

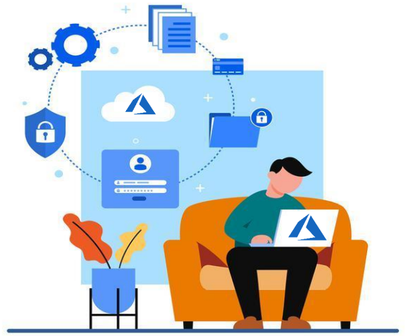


Data Protection in Transit

You can keep your data secure in transit by enabling *transport-level security* between Azure you. It is one uses *HTTPS* to secure communication over the public internet

you can enforce the use of HTTPS by requiring secure transfer for the storage account, when you call the REST APIs to access objects in storage accounts,

Once secure transfer is enabled, connections that use HTTP will be refused. This will also enforce secure transfer over SMB by requiring SMB 3.0 for all file share mounts.

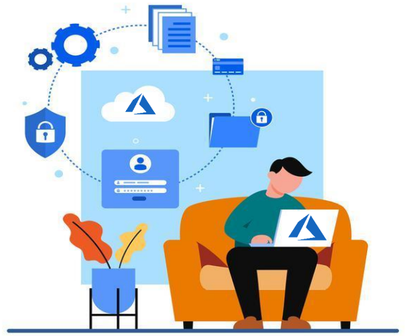


Support For Browser Cross Domain Access

Azure supports cross-domain access with cross-origin resource sharing (CORS). It uses HTTP headers so that a web application at one domain can access resources from a server which is at a different domain.

With CORS, web apps ensure that loading of only authorized content from sources that are authorized

CORS is an optional flag tht you can enable on Storage accounts. The flag adds the appropriate headers when you use HTTP GET requests so you can retrieve resources in a Storage account.

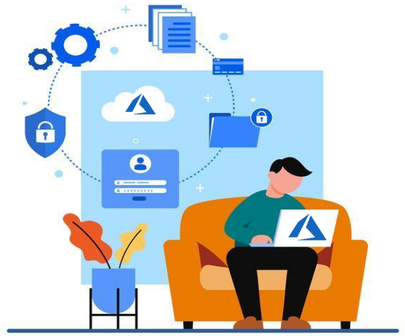


Audit Your Storage Access

If you wish to audit your Azure Storage access you can use the built-in Storage Analytics service

It logs every operation in real time, & you can search the Storage Analytics logs for specific requests

Filter based on the authentication mechanism, the success of the operation, or the resource that was accessed.



Demo: Conditional Access

Note: Refer to Module-11 Demo-2 file on LMS for all the steps in detail

edureka!

Azure Storage Keys

Shared keys in Azure Storage accounts are called *storage account keys*. Azure creates two of these keys (primary and secondary) for each storage account that is created. The keys can access anything in the account

With such powerful keys one should know when to regenerate them:

- Periodic regeneration of keys security reasons
- If there is unauthorized access to the key that was hard-coded or saved in a configuration file, then regenerate the key.
- If your team is using a Storage Explorer application that keeps the storage account key, and one of the team members leaves, regenerate the key

Shared Access Security (SAS)

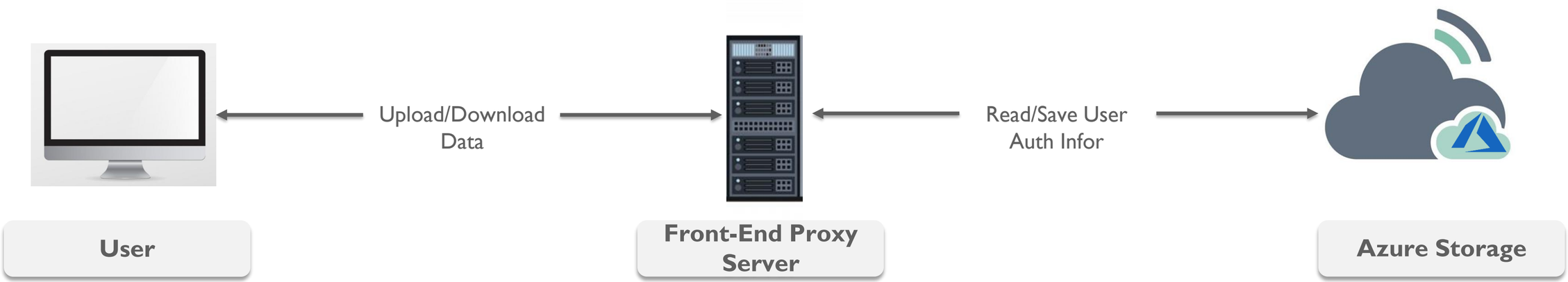
A SAS stands for Shared Access Signature. It is a string that contains a security token that can be attached to a URI. We use a SAS to delegate access to storage objects and specify constraints, such as the permissions and the time range of access.

- Sharing Storage Keys is not safe; hence it is advisable that third party sources are not given access to these Keys. This is where we use SAS
- **Example**: Giving a customer a SAS token, for uploading pictures to a file system or giving a web app permission to read pictures.
- In both situations you allow only the access that the application needs to do the task.
- There are two types of SAS

Service-Level SAS

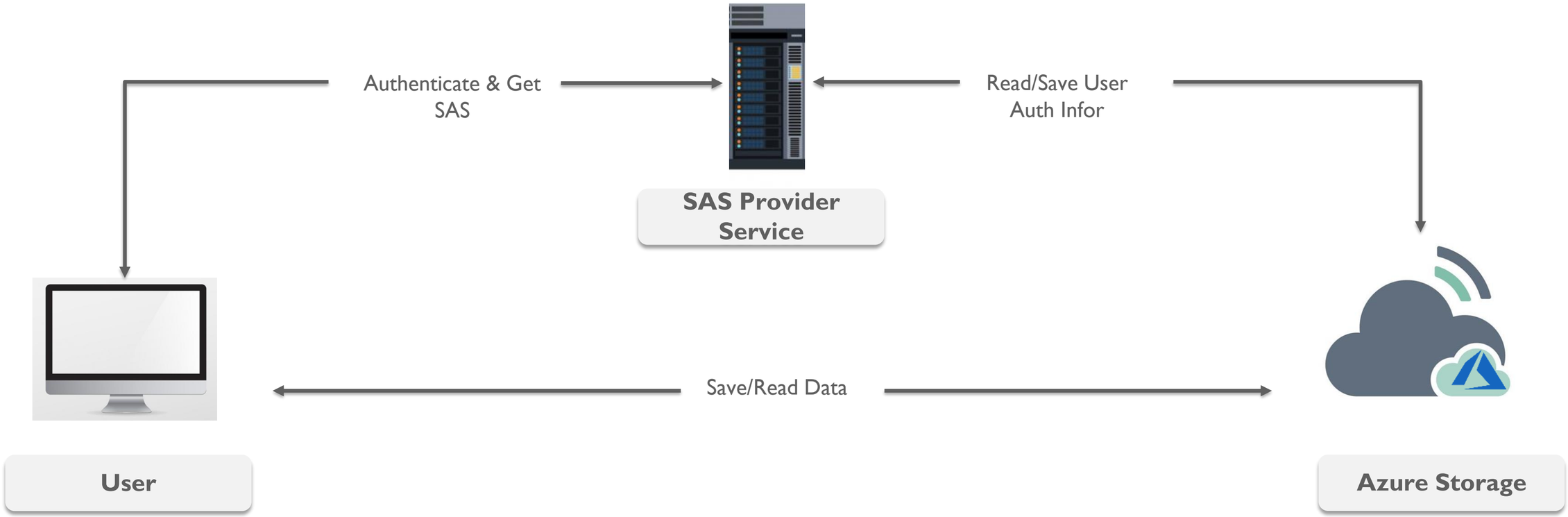
Application Level SAS

Shared Access Security (SAS): Scenario



If a client uploads data through Front-end Proxy Server the client will have business validation advantage while authenticating. These infrastructures however, suffer with scaling and cost issues when you are required to deal with high volume data

Shared Access Security (SAS): Scenario



With a lightweight service you can authenticate the client, as needed. Next, it will generate a SAS. On receiving SAS, the client can access storage account resources directly. The SAS here, defines the client's permissions & access interval. It reduces the need to route all data through the front-end proxy services.

Azure Data Box

As a Cloud Architect you will face situations where you are expected to design solutions to move huge amounts of data between cloud and on-premise

Time for Data movement over the network

Pipe size of Network

Questions faced by an Architect

Technology Used

Data size and rate of change

Azure Data Box is the solution

edureka!

Azure Data Box

With Azure Data Box, you can send terabytes of data in & out of Azure cloud quickly, inexpensively, and in reliable way

This secure data transfer is accelerated by shipping you a proprietary Data Box storage device

It has a maximum usable storage capacity of 80 TB which gets transported to datacenter with a carrier. It has a rugged casing to protect data in transit

You can order the Data Box device using Azure portal to import/export data from Azure. On receiving the device, you can set it up with the local web UI

Azure Data Box Types

Data Box

This rugged device has a 100-TB capacity & uses standard NAS protocols & also common copy tools. It has AES 256-bit encryption features for safer transit.

Data Box Disk

It is an 8-TB SSD with a USB/SATA interface & it comes with 128-bit encryption. Customize it to your needs - it comes in packs of up to five for a total of 40 TB.

Data Box Heavy

This ruggedized, self-contained device is the heaviest one and is designed to lift 1 PB of data to the cloud.

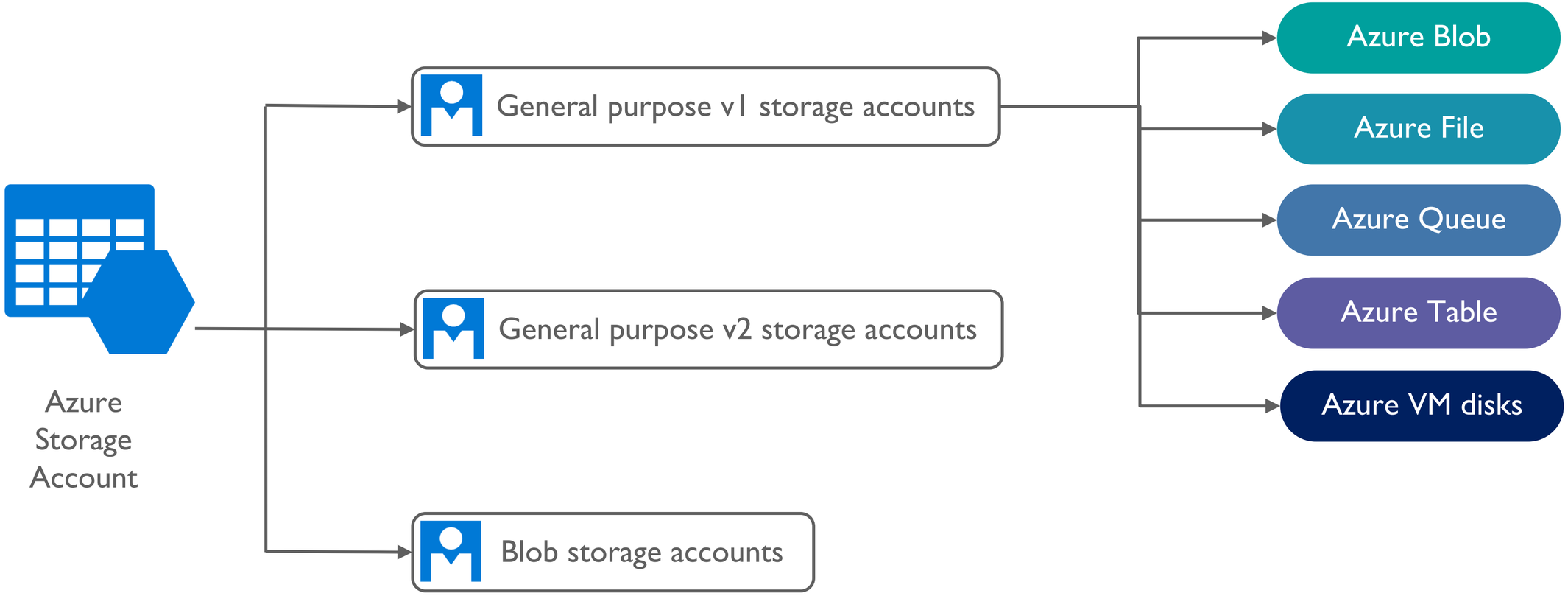
Data Box Gateway

Data Box Gateway transfers data to and from Azure—however it is a virtual appliance

Microsoft Azure Storage Account

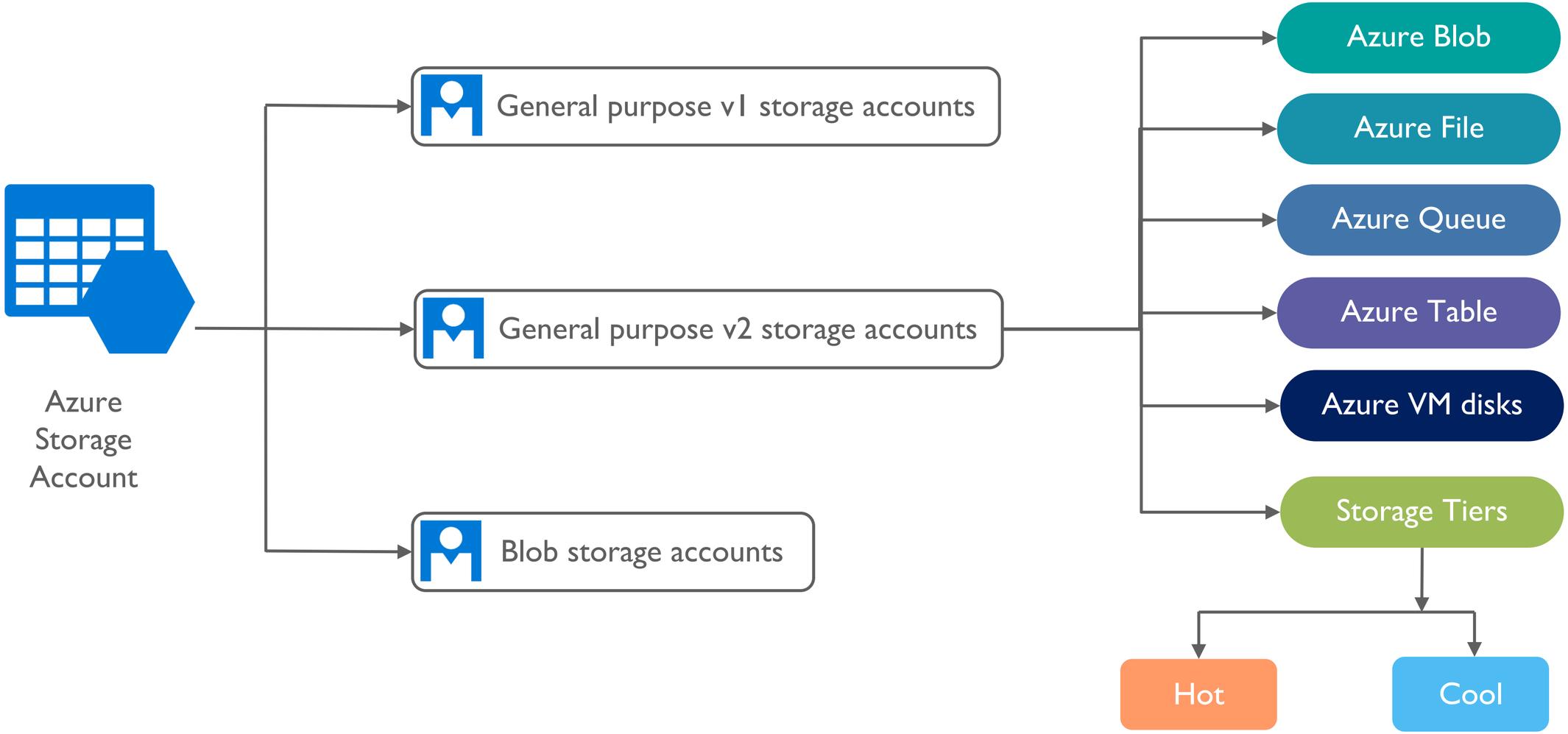
edureka!

Azure Storage Account

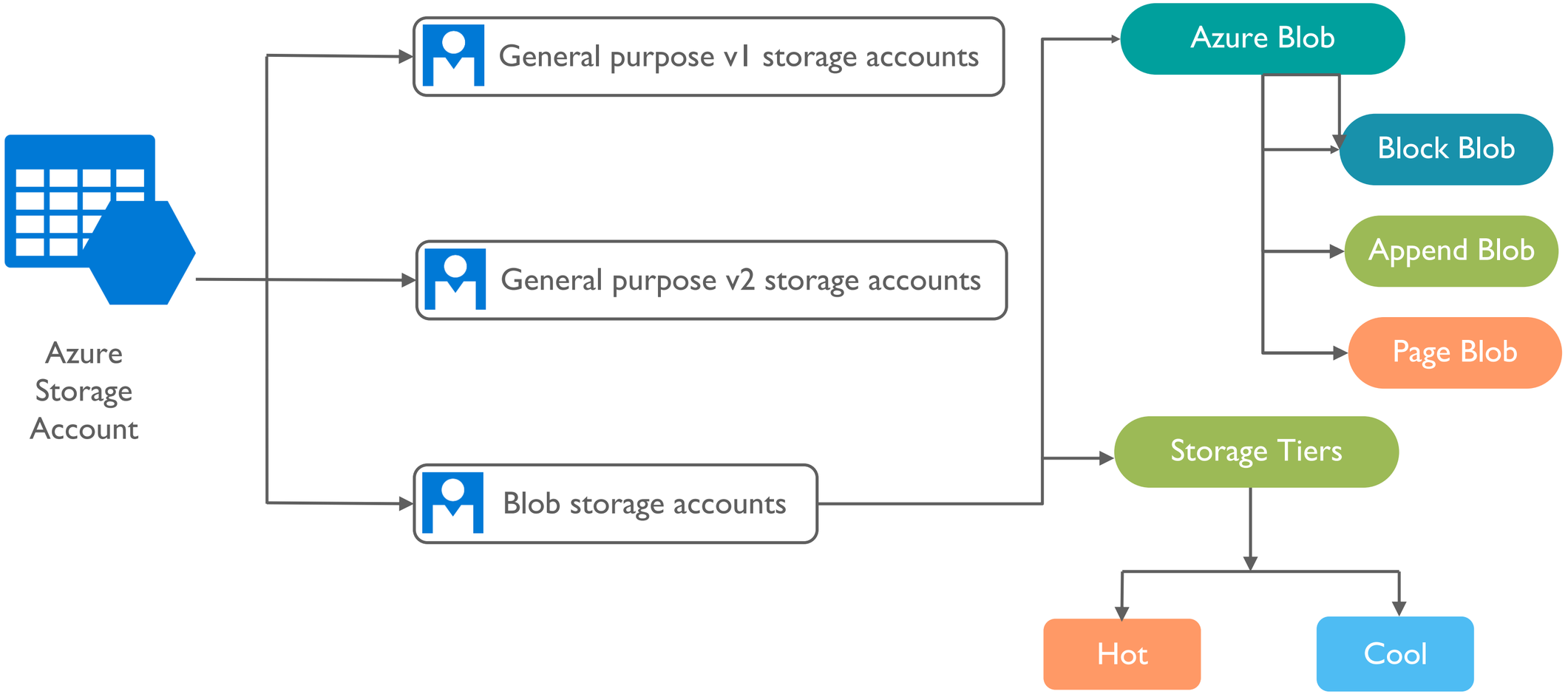


General purpose v1 and v2 storage accounts provide storage performance tiers: premium and standard, where the premium is only available for Azure VM disks

Azure Storage Account (Cont.)



Azure Storage Account (Cont.)



Demo: Create Azure Storage Account & SAS Token

Note: Refer to Module-11 Demo-3 file on LMS for all the steps in detail

edureka!

Summary

Design an Identity Solution

Managed Identities

Managed Identities aims at delegating complex identity management and User Authentication to a trusted third party so the organisation can focus on business logic and development

What would third party do:

- Manage identity management/authentication & assign tokens to authenticated user
- Manage identity management/authentication & assign tokens to authenticated user
- Based on tokens you can decide on granting/denying access and planning security

edureka!

Protocols

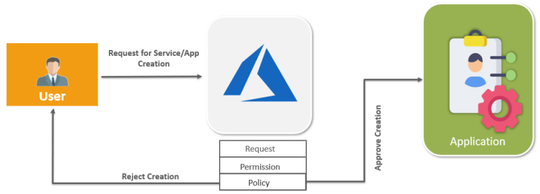
Protocols are agreed processes, language or a framework that tell how to authenticate or authorise. In simple words how do we perform actions on behalf of a user

Types

- OAuth 2.0
- OpenID
- SAML 2.0
- WS-Fed

edureka!

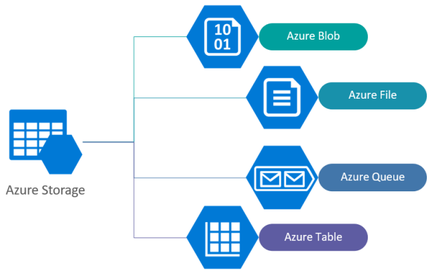
Scenario: Azure Policy



Policy is a set of rules that decides a particular action(For ex: User may pass location parameter and policy may decide if to approve creation of service or app)

edureka!

Microsoft Azure Storage Services



edureka!

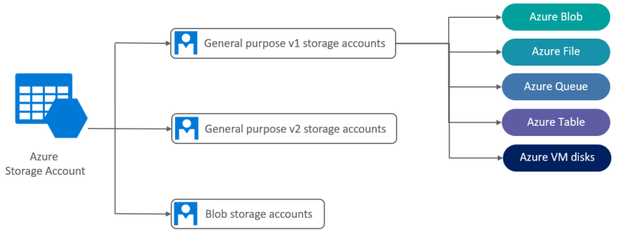
Azure Storage Security Features

Azure Cloud Storage Provides various High-Level Security benefits for your data like:

- Data Protection at rest
- Data Protection in transit
- Support for browser cross-domain access
- Control who gets to access your data (RBAC)
- Audit your storage access

edureka!

Azure Storage Account



General purpose v1 and v2 storage accounts provide storage performance tiers: premium and standard, where the premium is only available for Azure VM disks

edureka!

edureka!

edureka!

edureka!

Thank You

For more information please visit our website
www.edureka.co