PGP in Cloud Computing

Azure Essentials

- **IaaS:** Set of machines or VMs hosted on the cloud with scalability
- **PaaS:** Managed Services where underlying hardware and VMs are managed by the cloud provider
    - Some PaaS are provided by Microsoft directly e.g. Azure Service Bus and Cosmos DB
- **SaaS:** Cloud hosted software working on a pay-as-you-go or subscription-based model
- Any Azure service being used on an account is called a **resource.**
- A **resource group** is a set of resources grouped together with the same lifecycle and access-control scope.
- **Subscriptions** will show you a list of Microsoft subscription on the email id linked to your Azure account
- **Monitor** and **Security Center** monitor your running resources and security risks respectively
- **Service Fabric Cluster** lets you run and monitor a cluster of machines to deploy your applications.
- **Marketplace** is a one-stop-shop for launching Azure services

Azure Virtual Machines

- The region and OS has to be specified when launching an Azure Virtual Machine
- Turning on Availability Zones can ensure resiliency in your application in case of a service outage, by switching to backup machines.
- Azure supports Bring Your Own License.
- Creating a virtual machine also creates the following components related to it in the same resource group
    - Disk
    - Network Interface
    - Public IP address
    - Network Security group
    - Storage account
    - Virtual network
- In the **Network Security Group,** inbound and outbound traffic rules can be set for the virtual machine.

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

Availability Sets in Azure

- An **Update Domain** and a **Fault Domain** is assigned to each VM in an Availability Zone
- Fault domains define the group of virtual machines that share a common power source and network switch
- Update domains are used for patching of the virtual machines. All virtual machines within an update domain will reboot together.
- By default Availability Sets have two Fault Domains, each sharing a common power source and network switch, and VMs are automatically separated across the Fault Domains.
- The number of Fault Domains in an Availability Set isn't exact, and the only guarantee that not all the VMs in the set will fail together.
- Availability Sets are assigned five Update Domains, and VMs are grouped into these Update Domains automatically.
- When a sixth VM is added to an Availability Set, it is assigned to the first Update Domain, and the seventh VM to the second Update Domain, etc. So the first and the sixth VMs added to an Availability Set could be rebooted at the same time in the instance of a planned maintenance event.
- Only one Update Domain is ever rebooted at a time, but the reboot order isn't necessarily sequential, so the fifth Update Domain could be rebooted before the first.
- **Horizontal Scaling** - The auto scale feature of Azure Monitor only scales horizontally, which is an increase ("out") or decrease ("in") of the number of VMs
- **Virtual Scaling** - Vertical scaling keeps the same number of VMs, but makes the more 'up") or less ("down") powerful. Power is measured in attributes such as memory, CPU speed, or disk space. Vertical scaling is dependent on the availability of larger hardware, which quickly hits an upper limit and can vary by region.
- Azure virtual machine scale sets let you create a set of identical load-balanced VMs which can be set to automatically scale up or scale down depending on requirements or a defined schedule.

Azure App Service Plan, Resource Groups.

- An **App Service Plan** is a set of compute resources that are required for an app to run.
- Multiple apps can be hosted on the same app service plan.
- An App Service Plan defines the following resource specifications
    - Region
    - Number of VM instances
    - Size of VM instances
    - Pricing tier
- A Service Plan is defined inside a Resource Group.

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

Azure Storage, Blob Storage

- Azure Storage offers the following options
  - **Blob Storage:** Massively scalable object store for data objects. It is suitable for
    - HTTP based file retrieval
    - Distributed file access
    - Media Streaming
    - Log and archival purposes
    - Data analysis
  - **File Storage:** File system storage for the cloud. This is ideal for
    - Replacing or supplementing on-premises storage
    - “Lift and Shift application”
    - Shared application settings
    - Development purposes
  - **Table Storage:** This is a NoSQL based storage system. It can be used for
    - Storage of high volume structured data
    - Storing datasets without complex joins and foreign keys
    - Querying data with clustered indices
    - Accessing data using the OData protocol and LINQ queries
  - **Storage Queue:** Messaging storage for reliable messaging. This is used for
    - Storing a list of asynchronous tasks
    - Passing messages from an Azure web role to a worker role
- The different storage options available are
  - **Standard** : Uses Magnetic drives and is best for bulk storage or infrequently accessed data
  - **Premium** : Uses Solid State drives and is best used for IO intensive applications, like databases, and Azure Virtual Machine drives.
- The following replication options are available
  - Locally Redundant Storage (LRS): The replicas are created in the same datacenter as the original
  - Geo-Redundant Storage(GRS): The replicas are created in a different geographical region
  - Read-Access Geo-Redundant Storage(RA-GRS): The replicas are created in a different geographical region, but with reduced performance and in read-only mode.
- The NuGet Package provides the APIs for the SDKs provided by Microsoft.

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

Table Storage

- Partition key: This uniquely identifies the partition where a particular record is stored
- Row key: This is the primary key for a stored record
- Partition key+Row key is used to uniquely identify an entity and is recommended to queries
- Querying an entity using other fields results in reduced performance, especially with increased number of partitions

Traffic Manager

- Services provided by Traffic manager
    - Handle service fail-overs
    - Direct traffic to endpoint with lowest latency
    - Direct traffic to alternative endpoints during maintainance or downtime
- Traffic manager supports non-Azure endpoints hosted on-premises or hybrid cloud scenarios.
- The following routing methods can be used
    - Priority: Can select a primary and secondary/backup endpoints
    - Weighted: Assign weights to endpoints, with a higher weight having a higher priority
    - Performance: Will automatically select closest endpoint with lowest latency
    - Geographic: Direct users to different endpoints based to location
    - Multivalue: To be used when only IPv4/v6 addresses can be used as endpoints
    - Subnet: A set of IP addresses can be mapped to a single endpoint in a many-to-one fashion

Networking

- **CIDR :** Used in virtual network configuration
    - Pattern : xxx.xxx.xxx.xxx/n
    - 172.168.0.1/34 results in range from 172.168.1.0 to 172.168.1.255
    - A **network security group** contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
- Attributes of a **network security group(NSG) rule** are as follows
    - Priority: Decides which rule will be checked first
    - Action: Allow/Deny
    - 5-tuple
        - Source IP
        - Source Port
        - Destination IP
        - Destination Port
        - Protocol

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

Storage Queue

- It is a service for storing messages that can be accessed using authenticated HTTP or HTTPS calls
- Contains the following components
    - **URL format**: Queues are addressable using the following URL format:
    - http://<storage account>.queue.core.windows.net/<queue>
    - **Storage Account**: All access to Azure Storage is done through a storage account.
    - **Queue**: A queue contains a set of messages. All messages must be in a queue. Note that the queue name must be all lowercase.
    - **Message**: A message, in any format, of up to 64 KB. The maximum time that a message can remain in the queue is 7 days.

Azure Redis Cache

- In-memory cached database for faster retrieval and other operations
- Supports geo-replication

Azure Cosmos DB

- Distributed NoSQL database
- Provides row-level authorization
- Natively built Spark for data analytics
- Supports open-source NoSQL APIs
- Suitable for applications with near real-time requirements

Azure SQL

- General purpose DBaaS(DataBase as a Service) based on the Microsoft SQL Server Engine

Azure API Management Gateway

- Publish APIs for external, internal and partner developers
- Provides statistics on developer engagement and other analytics required
- Uses API keys to track and authenticate API calls

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

- Support in-bound and out-bound processing

Identity Management in Azure

- **Azure Active Directory :** Multi-tenant , cloud based directory
- Can be implemented on-premises
- Uses OAuth 2.0 protocol

Azure Service Bus

- Enterprise Message Broker
- Provides asynchronous data and state transfer
- Supports point-to-point and pub-sub messaging

Azure Cognitive Services

- **LUIS (Language Understanding):** Natural Language Processor. Some use-cases are:
    - Social Media Feedback monitoring and response
    - Bot Servicing product queries and feedback
    - Speech enabledIntelligent desktop app for order tracking
- Bot service can be hosted inside an App Service plan
- Bot channel is a connection between a bot and communication apps. The communication app can be a direct client, Skype, a web service chat etc.

Serverless Computing

- Abstraction of servers, infrastructure and operating systems
- Driven by the reaction to triggers and events happening in the cloud environment
- **Azure Functions :** Perform tasks based on a trigger from an Azure service, an HTTP request or a predefined timer or schedule.
- **Durable Functions :**
    - Extension of Azure Functions
    - Define stateful functions in a serverless environment
    - Uses an orchestrator function
    - Progress is checkpointed when the function is idle.
    - Some application patterns that can be used with Durable Functions are :
        - Chaining
        - Fan-out/fan-in
        - Async HTTP APIs
        - Monitoring

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

- Human Interaction

Azure Logic Apps

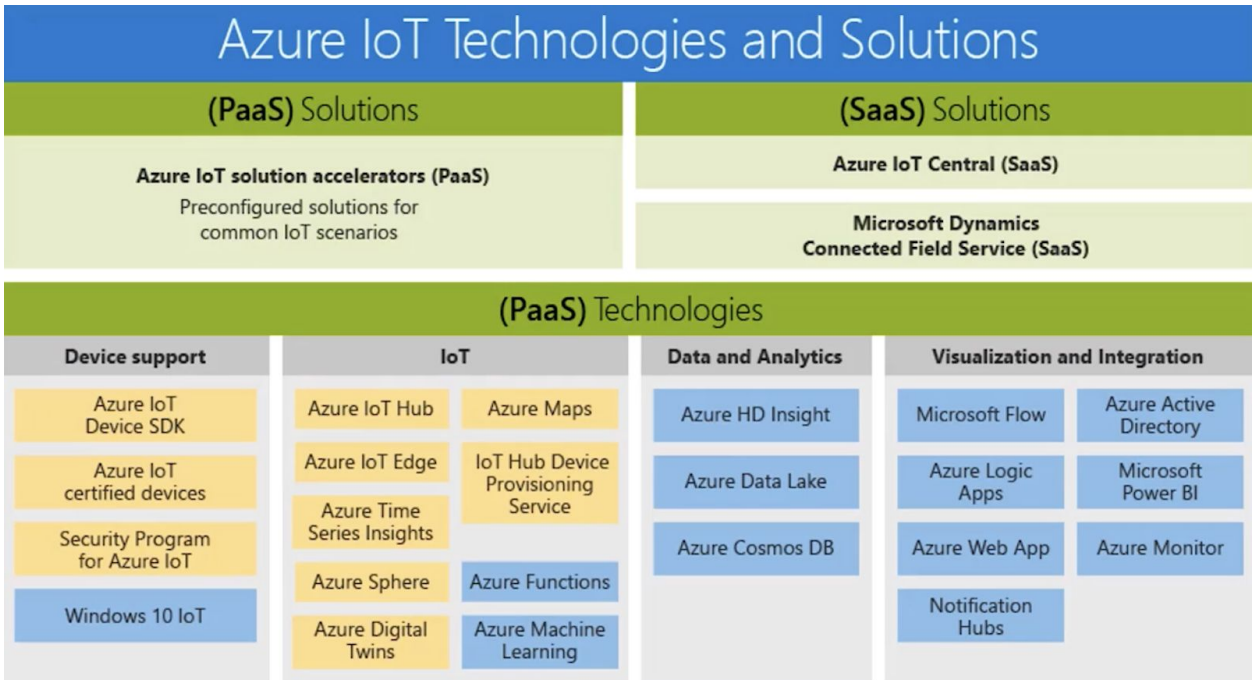
- Automate tasks and business processes
- Example use-cases:
  - Process and route orders across on-premises and cloud systems
  - Send email notifications with Office 365 when events happen in various systems, apps and services
  - Move uploaded files from an SFTP or FTP server to Azure storage
  - Monitor social media for a specific sentiment

Azure IoT

- **Internet of Things :** The network of physical objects that contain embedded technology to communicate and interact with their internal states or external environment
- This includes health equipment,environmental sensors,smart appliances etc.

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing



Azure Event Hub

- Big Data Streaming and Event Ingestion
- Possible Use-cases
    - Anomaly Detection
    - Application Logging
    - Analytics pipelines
    - Live dashboarding
    - Archiving Data
    - Transaction Processing
    - User telemetry processing
    - Device Telemetry Streaming
- Connects data source to listeners
- Reading the data stream is done using **Checkpointing** where a pointer is placed on the stream and is shifted as the data is read. The location of the pointer is written into storage in case of a transient failure
- Data is placed into the stream in partitions. Load balancing is performed automatically across partitions

Azure IoT Hub

- Central message hub for bi-directional communication between IoT applications and their corresponding devices

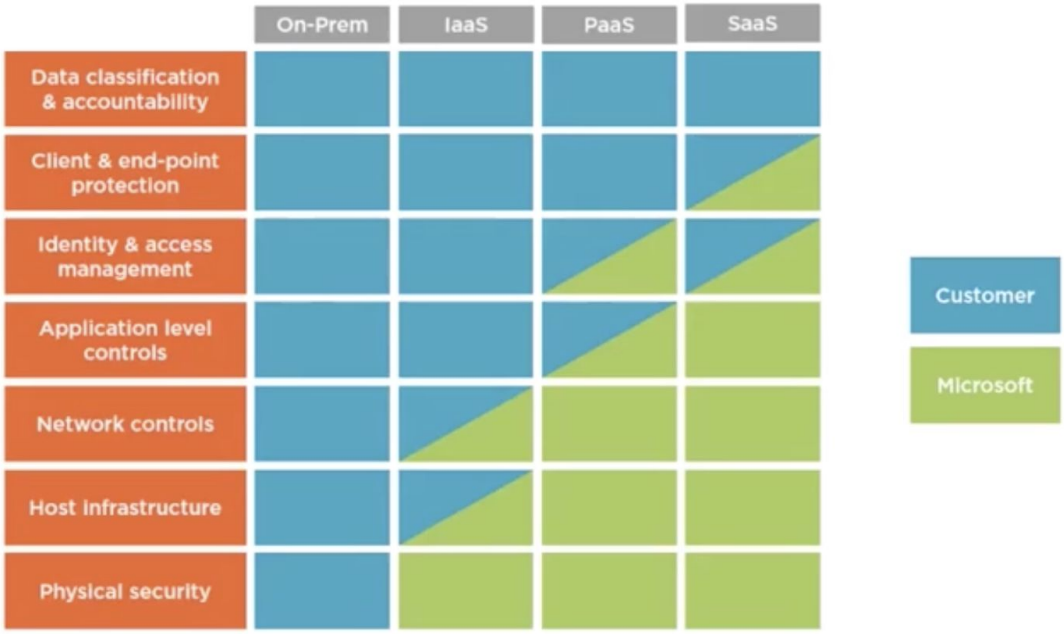
Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

- **Protocol Gateway** bridges the traffic using AMQP 1.0 protocol.
- Protocol gateway can be deployed using Azure Service Fabric,Azure Cloud Services worker roles or Windows Virtual Machines, or can be deployed on-premises.

Azure Security Center

- Works on shared responsibility model



- Features:
  - Policy and Compliance
  - Advance Deference
  - Threat protection
  - Automation

Azure Application Insights

- Collects telemetry from on-premises and cloud environments
- **Application Insights:** Application Performance Management platform for web developers
  - Monitor health of application
  - Continuous export of data
  - Push data into another application

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

- Generate alerts

Azure Log Analytics

- Construct queries to search the generated log data
- Create customized dashboard to visualize constructed queries
-

Azure Key Vault

- Stores keys in HSMs (Hardware key Modules)
- Provision,manage and deploy public and private SSL/TLS certificates
- Create and control encryption keys

Azure Service Fabric

- Distributed Systems platform that makes it easy to package, deploy and manage scalable microservices and containers
- Microservices are run on a high-density shared pool of machines called a cluster
- Services provided are
  - Lifecycle management
  - Always On availability
  - Orchestration
  - Programming models
  - Health and monitoring
  - Dev and Ops tooling
  - Autoscaling
- **Stateless microservices** (such as protocol gateways and web proxies) do not maintain a mutable state outside a request and its response from the service. Azure Cloud Services worker roles are an example of a stateless service.
- **Stateful microservices** (such as user accounts, databases, devices, shopping carts, and queues) maintain a mutable, authoritative state beyond the request and its response.

Azure Data Factory

- **Azure Data Factory :** Managed Cloud Service used for for complex ELT (Extract-Load-Transform) operations and create data-driven workflows
- Create and Schedule Data-driven workflows
- Process and Transform the data using compute services like Azure HDInsight, Hadoop, Spark etc.

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

PGP in Cloud Computing

Azure SQL Data Warehouse

- Cloud based Enterprise Data Warehouse(EDW)
- Data is imported using PolyBase T-SQL queries
- Massively Parallel Processing (MPP) is used to run complex queries

Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited