FUNDAMENTALS

Friday, December 16, 2022 5:41 PM

Public availablity is the difference between the private and public cloud

Hybrid cloud: both public and private cloud
Multi cloud: multiple public cloud providers
Azure arc: Azure Arc is a set of technologies that helps manage your cloud environment. Azure Arc can help manage your cloud environment, whether it's a public cloud solely on Azure, a private cloud in your datacenter, a hybrid configuration, or even a multi-cloud environment running on multiple cloud providers at once.
Azure VMware Solution : What if you're already established with VMware in a private cloud environment but want to migrate to a public or hybrid cloud? Azure VMware Solution lets you run your VMware workloads in Azure with seamless integration and scalability.

CapEX: one time expense
Operational EX: spending over time(cloud computing)

Reliability is the thing to recover form failures and start to function as expectd

. In an IaaS model, the cloud provider is responsible for maintaining the hardware, network connectivity (to the internet), and physical securityYou're responsible for everything else: operating system installation, configuration, and maintenance; network configuration; database and storage configuration; and so on

Lift-and-shift migration: You're standing up cloud resources similar to your on-prem datacenter, and then simply moving the things running on-prem to running on the IaaS infrastructure.

In a PaaS environment, the cloud provider maintains the physical infrastructure, physical security, and connection to the internet. They also maintain the operating systems, middleware, development tools, and business intelligence services that make up a cloud solution.

With SaaS, you're essentially renting or using a fully developed application. (email,messaging)

Azure:

- To create and use azure services we need a azure subscription which is created when we create a azure account
- In each subscription we can create many resource groups as per out needs and inside the resource group resources are placed
- Most Azure regions are paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away.
- In addition to regular regions, Azure also has sovereign regions. Sovereign regions are instances of Azure that are isolated from the main instance of Azure. You may need to use a sovereign region for compliance or legal purposes.(eg:for government)
- It cant be nested like one inside another
- In Azure, subscriptions are a unit of management, billing, and scale. Similar to how resource groups are a way to logically organize resources, subscriptions allow you to logically organize your resource groups and facilitate billing.
- If used multiple subscriptions we can use a billing boundary for billing related and access control boundary thayt applies policies to the subscroiption level
- Organizing all the subcriptions or specific subscriptions into a groups is called management group in which e can apply govemance conditions(can be nested)

Important facts about management groups:

10,000 management groups can be supported in a single directory.
A management group tree can support up to six levels of depth. This limit doesn't include the root level or the subscription level.
Each management group and subscription can support only one parent.

VM's<-=> IAAS

Virtual machine scale sets let you create and manage a group of identical, load-balanced VMs.
Vm availablity sets: ensure that VMs stagger updates and have varied power and network connectivity, preventing you from losing all your VMs with a single network or power failure.

Availability sets do this by grouping VMs in two ways: update domain(update on set of vm's) and fault domain.(protect against a physical power or networking failure by having VMs in different fault domains)

Creating vms invloves specifying the image and resource groups in which it should be there and for installing anything we can use extensions feature to point to the .sh file snd give the command to execute
Eg: az vm extension set \
--resource-group learn-d17f5694-a8e1-4e2d-a884-a9018c69bd5b \
--vm-name my-vm \
--name customScript \
--publisher Microsoft.Azure.Extensions \
--version 2.1 \
--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \
--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

Another type of virtual machine is the Azure Virtual Desktop. Azure Virtual Desktop is a desktop and application virtualization service that runs on the cloud.

Azure Container Instances offer the fastest and simplest way to run a container in Azure; without having to manage any virtual machines or adopt any additional services. Azure Container Instances are a platform as a service (PaaS) offering.

Azure Functions runs your code when it's triggered and automatically deallocates resources when the function is finished. In this model, you're only charged for the CPU time used while your function runs.

Hosting options:
- VM's
- Containers
- Azure app service

App Service enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers automatic scaling and high availability. App Service supports Windows and Linux. It enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.

Azure App Service is a robust hosting option that you can use to host your apps in Azure. Azure App Service lets you focus on building and maintaining your app, and Azure focuses on keeping the environment up and running.

Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. It supports multiple languages, including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. It also supports both Windows and Linux environments.

Use the Mobile Apps feature of App Service to quickly build a back end for iOS and Android apps. With just a few actions in the Azure portal, you can:

Store mobile app data in a cloud-based SQL database.
Authenticate customers against common social providers, such as MSA, Google, Twitter, and Facebook.
Send push notifications.
Execute custom back-end logic in C# or Node.js.

Azure virtual networks,virtual subnets enable resources to communicate with each other

For name resolution, you can use the name resolution service that's built into Azure. You also can configure the virtual network to use either an internal or an external DNS server.

Virtual networks can connect not only VMs but other Azure resources, such as the App Service Environment for Power Apps, Azure Kubernetes Service, and Azure virtual machine scale sets.
Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

Point-to-site virtual private network connections are from a computer outside your organization back into your corporate network
Site-to-site virtual private networks link your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network.
Azure ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet.
Route tables can be used to route the packets as per our choice

Network security groups are Azure resources that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.

Network virtual appliances are specialized VMs that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.

You can link virtual networks together by using virtual **network peering.** Peering allows two virtual networks to connect directly to each other

Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.
In Route-based gateways, IPSec tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets.

By default, VPN gateways are deployed as two instances in an **active/standby configuration**, even if you only see one VPN gateway resource in Azure.

With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an **active/active configuration.**

Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections.
In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration. This configuration brings resiliency, scalability, and higher availability to virtual network gateways.

With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365. This allows you to connect offices, datacenters, or other facilities to the Microsoft cloud. Each location would have its own **ExpressRoute circuit.**

You could use **ExpressRoute Global Reach** to connect those two facilities, allowing them to communicate without transferring data over the public internet.

ExpressRoute supports four models that you can use to connect your on-premises network to the Microsoft cloud:

CloudExchange colocation
Point-to-point Ethernet connection
Any-to-any connection
Directly from ExpressRoute sites

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure

A storage account provides a unique namespace(unique name across azure) for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS

When you create your storage account, you'll start by picking the storage account type.below are redundancy options

- Locally redundant storage (LRS)(replicates 3 times in 1 datacenter) (low cost))
- Geo-redundant storage (GRS)(LRS in tow regions)
- Read-access geo-redundant storage (RA-GRS)
- Zone-redundant storage (ZRS)(replicates in three AZ's)
- Geo-zone-redundant storage (GZRS)(ZRS in primary region and LRS in secondary eegion(when failover this region is used))
- Read-access geo-zone-redundant storage (RA-GZRS)

Types:
- Standard general-purpose v2(blob,queue,table,azure file storages)
- Premium block blobs(blob storage)
- Premium file shares(azure files)
- Premium page blobs(page blobs)

Example for service endpoints for the storage service
Blob Storage https://<storage-account-name>.blob.core.windows.net (blob<=>dfs,file,queue,table

- Azure Blobs: A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2.
- Azure Files: Managed file shares for cloud or on-premises deployments.
- Azure Queues: A messaging store for reliable messaging between application components.
- Azure Disks: Block-level storage volumes for Azure VMs.

Blob: Hot(frequent),cool(30 days acces),archive(180 days(high cost to acces data within 180 dyas))
Only the hot and cool access tiers can be set at the account level. The archive access tier isn't available at the account level.(biut can be set at the blob level)

Inside the storage account we will create a container for uploading blobs(similar to buckets)

Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud.
- Discovery and assessment
- Server migration
- Data migration assistant
- Databse migrayion service
- Web app migration assistant
- Azure data box(offline data(data device shipped))

AzCopy is a command-line utility that you can use to copy blobs or files to or from your storage account. With AzCopy, you can upload files, download files, copy files between storage accounts, and even synchronize files

Azure File Sync is a tool that lets you centralize your file shares in Azure Files and keep the flexibility, performance, and compatibility of a Windows file server.(SMB, NFS, and FTPS.)

Azure Active Directory (Azure AD) is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop. Azure AD can also help you maintain your on-premises Active Directory deployment.(authentication,singlesign on,app management,device management)

Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD.

Azure Active Directory Domain Services (Azure AD DS) is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication

When you create an Azure AD DS managed domain, you define a unique namespace. This namespace is the domain name. Two Windows Server domain controllers are then deployed into your selected Azure region. This deployment of DCs is known as a replica set.

An external identity is a person, device, service, etc. that is outside your organization. Azure AD External Identities refers to all the ways you can securely interact with users outside of your organization

Can implement conditional acces slike only through certain client managd devices we should sign in

Azure enables you to control access through Azure role-based access control (Azure RBAC).
Scopes include:

A management group (a collection of multiple subscriptions).
A single subscription.
A resource group.
A single resource.

Defender for Cloud is a monitoring tool for security posture management and threat protection
When necessary, Defender for Cloud can automatically deploy a Log Analytics agent to gather security-related data. or hybrid and multicloud environments, Microsoft Defender plans are extended to non Azure machines with the help of Azure Arc. Cloud security posture management (CSPM) features are extended to multicloud machines without the need for any agents.(detect across,azure paas srvices,data services,networks)

Defender for Cloud can also protect resources in other clouds (such as AWS and GCP).

For example, if you've connected an Amazon Web Services (AWS) account to an Azure subscription, you can enable any of these protections:

Defender for Cloud groups the recommendations into security controls and adds a secure score value to each control.

When Defender for Cloud detects a threat in any area of your environment, it generates a security alert.

Role-based access control, using an allow model, grants all of the permissions assigned in all of the assigned roles.

Azure marketplace gives us premade solutions mad by azure and partners

Pricing calculator we can approximately get the cost for our resource utilization but in **tco calculator** it compares the onprem and the azure cost when inoutted

Cost Management provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.

Cost analysis is a subset of Cost Management that provides a quick visual for your Azure costs

Cost alerts provide a single location to quickly check on all of the different alert types that may show up in the Cost Management service. The three types of alerts that may show up are:

Budget alerts
Credit alerts
Department spending quota alerts.
Resource tags are another way to organize resources

Azure Blueprints lets you standardize cloud subscription or environment deployments. Instead of having to configure features like Azure Policy for each new subscription, with Azure Blueprints you can define repeatable settings and policies that are applied as new subscriptions are created.

Each component in the blueprint definition is known as an **artifact.**

It is possible for artifacts to have no additional parameters (configurations). An example is the Deploy threat detection on SQL servers policy, which requires no additional configuration.

Azure Blueprints deploy a new environment based on all of the requirements, settings, and configurations of the associated artifacts. Artifacts can include things such as:

Role assignments
Policy assignments
Azure Resource Manager templates
Resource groups

Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. These policies enforce different rules across your resource configurations so that those configurations stay compliant with corporate standards.

Azure Policy enables you to define both individual policies and groups of related policies, known as initiatives. Azure Policy evaluates your resources and highlights resources that aren't compliant with the policies you've created. Azure Policy can also prevent noncompliant resources from being created.

In some cases, Azure Policy can automatically remediate noncompliant resources and configurations to ensure the integrity of the state of the resources. For example, if all resources in a certain resource group should be tagged with AppName tag and a value of "SpecialOrders," Azure Policy will automatically apply that tag if it is missing.

A resource lock prevents resources from being accidentally deleted or changed.

There are two types of resource locks, one that prevents users from deleting and one that prevents users from changing or deleting a resource.

The Microsoft Service Trust Portal is a portal that provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices.

In addition to be available via Azure Cloud Shell, you can install and configure Azure PowerShell on Windows, Linux, and Mac platforms.

In utilizing Azure Resource Manager (ARM), **Arc** lets you extend your Azure compliance and monitoring to your hybrid and multi-cloud configurations. Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

Currently, Azure Arc allows you to manage the following resource types hosted outside of Azure:

- Servers
- Kubernetes clusters
- Azure data services
- SQL Server
- Virtual machines (preview)

Azure Resource Manager (ARM) is the deployment and management service for Azure. It provides a management layer that enables you to create, update,

and delete resources in your Azure account. Anytime you do anything with your Azure resources, ARM is involved.

nfrastructure as code is a concept where you manage your infrastructure as lines of code. Leveraging Azure Cloud Shell, Azure PowerShell, or the Azure CLI are some examples of using code to deploy cloud infrastructure. **ARM template**s are another example of infrastructure as code at work.

Azure Advisor evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. Azure Advisor is designed to help you save time on cloud optimization. The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

The recommendations are available via the Azure portal and the API, and you can set up notifications to alert you to new recommendations.
The recommendations are divided into five categories:

- Reliability is used to ensure and improve the continuity of your business-critical applications.
- Security is used to detect threats and vulnerabilities that might lead to security breaches.
- Performance is used to improve the speed of your applications.
- Operational Excellence is used to help you achieve process and workflow efficiency, resource manageability, and deployment best practices.
- Cost is used to optimize and reduce your overall Azure spending.

Azure Service Health helps you keep track of Azure resource, both your specifically deployed resources and the overall status of Azure(azure status,service,health,resouce health)

Azure Monitor is a platform for collecting data on your resources, analyzing that data, visualizing the information, and even acting on the results. Azure Monitor can monitor Azure resources, your on-premises resources, and even multi-cloud resources like virtual machines hosted with a different cloud provider

Azure Log Analytics is the tool in the Azure portal where you'll write and run log queries on the data gathered by Azure Monitor. Azure Monitor Alerts are an automated way to stay informed when Azure Monitor detects a threshold being crossed. You set the alert conditions, the notification actions, and then Azure Monitor Alerts notifies when an alert is triggered.
Application Insights, an Azure Monitor feature, monitors your web applications. Application Insights is capable of monitoring applications that are running in Azure, on-premises, or in a different cloud environment.

There are two ways to configure Application Insights to help monitor your application. You can either install an SDK in your application, or you can use the Application Insights agent.

AZURE DATA FUNDAMENTALS

Saturday, December 17, 2022 10:36 AM

Structured: CSV/TABLE
Semi structured: JSON
Unstructured: DOCUMENTS,IMAGES,FILES

Blob(Binary large objects)

Optimized frile formats:
- Avro(row based format)
- ORC(optimized row columnar format)
- Parquet(columnar format)

No relational databases:
- Key value db
- Document db(JSON)
- Column family db(hbaseetc..)
- Graph db

Relational offerings:
- Azure SQL database(mysql,mariadb,postgresql)
- Azure sql managed instance(a hosted instance of SQL Server with administartivee responsibility for owner)
- Azure SQL VM

Non relational offerings:
- Azure cosmos db(nosql(JSONdocs,keyvalue,column families,graphs)
- Azure storage(blob,file share,tanles(keyvalue)

Azure data factory is an azure service that does the ETL

Azure synapse Analytics is a comprehensive data analytics solution(PIPELINES,SQL,APACHE SPARK,DATA EXPLORER)

Azure Databricks is an Azure-integrated version of the popular Databricks platform, which combines the Apache Spark data processing platform with SQL database semantics

Azure HDInsight is an Azure service that provides Azure-hosted clusters for popular Apache open-source big data processing technologies, including:(spark,hadoop,hbase,kafka)

Azure Stream Analytics is a real-time stream processing engine that captures a stream of data from an input, applies a query to extract and manipulate data from the input stream, and writes the results to an output for analysis or further processing.

Azure Data Explorer is a standalone service that offers the same high-performance querying of log and telemetry data as the Azure Synapse Data Explorer runtime in Azure Synapse Analytics.

Microsoft Purview provides a solution for enterprise-wide data governance and discoverability. You can use Microsoft Purview to create a map of your data and track data lineage across multiple data sources and systems, enabling you to find trustworthy data for analysis and reporting.

Power BI for business intelligence

Normalization:

- Separate each entity into its own table.
- Separate each discrete attribute into its own column.
- Uniquely identify each entity instance (row) using a primary key.
- Use foreign key columns to link related entities.

Dialects:

- T-SQL(transact sql) (sql server,azure sql services)
- pgSQL(postgres)
- PL/SQL(oracle

The index creates a tree-based structure that the database system's query optimizer can use to quickly find rows (index in book sorted lexicographically)

We can use elastic pool functionality in azure database service to provision same resources in a fleet

Cosmos DB:(serverless distributed db)

- IOT and telematics
- Retail and marketing
- Gaming
- Web and mobile app

We can query the data using sql
you can enable multi-region writes in the regions where you want users to work with the data.
DB:

- For Mongodb(mongo ql)
- For Postgressql(sql)
- For table(key value tables)(table api to query)
- For apache cassandra(sql)
- For apache gremlin(graph)(gremlin syntax query)

Azure blob storage:

- Has three different type of blob
    - Block blobs
      Max size of a block blob is 4.7 TB
    - Page blobs
      Organized as a collection of fixed size 512-byte pages(azure uses this for virtual disk storage for vms)
    - Append blobs
      Support append operations on blob
      The maximum size of an append blob is just over 195 GB

Azure Data Lake Store (Gen1) is a separate service for hierarchical data storage for analytical data lakes, often used by so-called big data analytical solutions that work with structured, semi-structured, and unstructured data stored in files. **Azure Data Lake Storage Gen2** is a newer version of this service that is integrated into Azure Storage; enabling you to take advantage of the scalability of blob storage and the cost-control of storage tiers, combined with the hierarchical file system capabilities and compatibility with major analytics systems of Azure Data Lake Store.

To create an Azure Data Lake Store Gen2 files system, you must enable the Hierarchical Namespace option of an Azure Storage account.
after upgrading a storage account to support a hierarchical namespace for blob storage, you can’t revert it to a flat namespace.

Azure File Storage supports up to 2000 concurrent connections per shared file.(ma size of one

file is 1 tb

Azure File Storage offers two performance tiers. The Standard tier uses hard disk-based hardware in a datacenter, and the Premium tier uses solid-state disks. The Premium tier offers greater throughput, but is charged at a higher rate.

Azure Files supports two common network file sharing protocols:

- *Server Message Block* (SMB) file sharing is commonly used across multiple operating systems (Windows, Linux, macOS).
- *Network File System* (NFS) shares are used by some Linux and macOS versions. To create an NFS share, you must use a premium tier storage account and create and configure a virtual network through which access to the share can be controlled.

Azure Table Storage is a NoSQL storage solution that makes use of tables containing key/value data items. Each item is represented by a row that contains columns for the data fields that need to be stored.
Azure Table Storage tables have no concept of foreign keys, relationships, stored procedures, views, or other objects you might find in a relational database.
When you search for data, you can include the partition key in the search criteria. This helps to narrow down the volume of data to be examined,
The key in an Azure Table Storage table comprises two elements; the partition key that identifies the partition containing the row, and a row key that is unique to each row in the same partition

SQL pools in Azure Synapse Analytics include PolyBase, which enables you to define external tables based on files in a datalake (and other sources) and query them using SQL

Azure Event Hubs: A data ingestion service that you can use to manage queues of event data, ensuring that each event is processed in order, exactly once.
Azure IoT Hub: A data ingestion service that is similar to Azure Event Hubs, but which is optimized for managing event data from Internet-of-things (IoT) devices.
Delta Lake is an open-source storage layer that adds support for transactional consistency, schema enforcement, and other common data warehousing features to data lake storage.

Azure Data Explorer is a great choice of technology when you need to:

Capture and analyze real-time or batch data that includes a time-series element; such as log telemetry or values emitted by Internet-of-things (IoT) devices.
Explore, filter, and aggregate data quickly by using the intuitive and powerful Kusto Query Language (KQL).

AZURE AI FUNDAMENTALS

Saturday, December 17, 2022 12:27 PM

If we want to deploy no code ml then
Automated machine learning & Azure Machine learning designer lets you to create and publish models

Supervised learning: Regression,classification
Unsupervised learning: clustering

We need to create a workspace resource in azure subscription to manage data ,stuffs related to machine learning workloads

Compute targets are cloud-based resources on which you can run model training and data exploration processes.

Compute resources that you czn create:

- Compute instances
- Compute clusters
- Inference Clusters
- Attached compute

To deploy your pipeline, you must first convert the training pipeline into a real-time inference pipeline. This process removes training components and adds web service inputs and outputs to handle requests.

The inference pipeline performs the same data transformations as the first pipeline for new data. Then it uses the trained model to infer, or predict, label values based on its features

Creating an image classification solution with Custom Vision consists of two main tasks. First you must use existing images to train the model, and then you must publish the model so that client applications can use it to generate predictions.

For each of these tasks, you need a resource in your Azure subscription. You can use the following types of resource:

Custom Vision: A dedicated resource for the custom vision service, which can be training, a prediction, or both resources.
Cognitive Services: A general cognitive services resource that includes Custom Vision along with many other cognitive services. You can use this type of resource for training, prediction, or both.

To use you model, client application developers need the following information:

- Project ID: The unique ID of the Custom Vision project you created to train the model.
- Model name: The name you assigned to the model during publishing.
- Prediction endpoint: The HTTP address of the endpoints for the *prediction* resource to which you published the model (*not* the training resource).
- Prediction key: The authentication key for the *prediction* resource to which you published the model (*not* the training resource).

Microsoft Azure provides multiple cognitive services that you can use to detect and analyze faces, including:

Computer Vision, which offers face detection and some basic face analysis, such as returning the bounding box coordinates around an image.
Video Indexer, which you can use to detect and identify faces in a video.
Face, which offers pre-built algorithms that can detect, recognize, and analyze faces.

To use Face, you must create one of the following types of resource in your Azure subscription:

- Face: Use this specific resource type if you don't intend to use any other cognitive services, or if you want to track utilization and costs for Face separately.
- Cognitive Services: A general cognitive services resource that includes Computer Vision along with many other cognitive services; such as Custom Vision, Form Recognizer, Language, and others. Use this resource type if you plan to use multiple cognitive services and want to simplify administration and development.

Whichever type of resource you choose to create, it will provide two pieces of information that you will need to use it:

- A key that is used to authenticate client applications.
- An endpoint that provides the HTTP address at which your resource can be accessed.

The Read API uses the latest recognition models and is optimized for images that have a significant amount of text or has considerable visual noise.

The Read API can handle scanned documents that have a lot of text
The results from the Read API are arranged into the following hierarchy:

- Pages - One for each page of text, including information about the page size and orientation.
- Lines - The lines of text on a page.
- Words - The words in a line of text, including the bounding box coordinates and text itself.

Azure's Form Recognizer service can solve for this issue by digitizing fields from forms using optical character recognition (OCR). Azure's OCR technologies extract the contents and structure from forms, such as key, value pairs (eg. Quantity: 3).Form Recognizer in Azure provides intelligent form processing capabilities that you can use to automate the processing of data in documents such as forms, invoices, and receipts

The Computer Vision service is a cognitive service in Microsoft Azure that provides pre-built computer vision capabilities. The service can analyze images, and return detailed information about an image and the objects it depicts.

The Language service is a part of the Azure Cognitive Services offerings that can perform advanced natural language processing over raw text.

To use the Language service in an application, you must provision an appropriate resource in your Azure subscription. You can choose to provision either of the following types of resource:

- A Language resource - choose this resource type if you only plan to use natural language processing services, or if you want to manage access and billing for the resource separately from other services.
- A Cognitive Services resource - choose this resource type if you plan to use the Language service in combination with other cognitive services, and you want to manage access and billing for these services together.

To enable this kind of interaction, the AI system must support two capabilities:

- Speech recognition - the ability to detect and interpret spoken input.
- Speech synthesis - the ability to generate spoken output.

The Speech-to-Text API
The Text-to-Speech API
To use the Speech service in an application, you must create an appropriate resource in your Azure subscription. You can choose to create either of the following types of resource:

A Speech resource - choose this resource type if you only plan to use the Speech service, or if you want to manage access and billing for the resource separately from other services.
A Cognitive Services resource - choose this resource type if you plan to use the Speech service in combination with other cognitive services, and you want to manage access and billing for these services together.

The Translator service, which supports text-to-text translation.
The Speech service, which enables speech-to-text and speech-to-speech translation.

Azure bot service for bot creation

An Azure Cognitive Search index can be thought of as a container of searchable documents. Conceptually you can think of an index as a table and each row in the table represents a document. Tables have columns, and the columns can be thought of as equivalent to the fields in a document. Columns have data types, just as the fields do on the documents.

Index schema

Azure Cognitive Search lets you create and load JSON documents into an index with two approaches:

Push method: JSON data is pushed into a search index via either the REST API or the .NET SDK. Pushing data has the most flexibility as it has no restrictions on the data source type, location, or frequency of execution.

Pull method: Search service indexers can pull data from popular Azure data sources, and if necessary, export that data into JSON if it isn't already in that format.

- Data Source: Persists connection information to source data, including credentials. A data source object is used exclusively with indexers.
- Index: Physical data structure used for full text search and other queries.
- Indexer: A configuration object specifying a data source, target index, an optional AI skillset, optional schedule, and optional configuration settings for error handling and base-64 encoding.
- Skillset: A complete set of instructions for manipulating, transforming, and shaping content, including analyzing and extracting information from image files. Except for very simple and limited structures, it includes a reference to a Cognitive Services resource that provides enrichment.
- Knowledge store: Stores output from an AI enrichment pipeline in tables and blobs in Azure Storage for independent analysis or downstream processing.

Azure Cognitive Search queries can be submitted as an HTTP or REST API request, with the response coming back as JSON. Queries can specify what fields are searched and returned, how search results are shaped, and how the results should be filtered or sorted.
coffee (-"busy" + "wifi")(eg query)

Security, Compliance, and Identity Fundamentals

Saturday, December 17, 2022 5:29 PM

Defense Depth:

Example layers of security might include:

- Physical security such as limiting access to a datacenter to only authorized personnel.
- Identity and access security controls, such as multifactor authentication or condition-based access, to control access to infrastructure and change control.
- Perimeter security of your corporate network includes distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- Network security, such as network segmentation and network access controls, to limit communication between resources.
- Compute layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- Application layer security to ensure applications are secure and free of security vulnerabilities.
- Data layer security including controls to manage access to business and customer data and encryption to protect data.

Confidentiality refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential, but then you also need to keep the encryption keys confidential. Confidentiality is the most visible part of security; we can clearly see need for sensitive data, keys, passwords, and other secrets to be kept confidential.

Integrity refers to keeping data or messages correct. When you send an email message, you want to be sure that the message received is the same as the message you sent. When you store data in a database, you want to be sure that the data you retrieve is the same as the data you stored. Encrypting data keeps it confidential, but you must then be able to decrypt it so that it's the same as before it was encrypted. Integrity is about having confidence that data hasn't been tampered with or altered.

Availability refers to making data available to those who need it, when they need it. It's important to the organization to keep customer data secure, but at the same time it must also be available to employees who deal with customers. While it might be more secure to store the data in an encrypted format, employees need access to decrypted data.

Zero Trust guiding principles

The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach.

- Verify explicitly. Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.
- Least privileged access. Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
- Assume breach. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

Six foundational pillars

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- Identities may be users, services, or devices. When an identity attempts to access a resource, it

must be verified with strong authentication, and follow least privilege access principles.
- Devices create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is an important aspect of security.
- Applications are the way that data is consumed. This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally. This pillar also includes managing permissions and access.
- Data should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.
- Infrastructure, whether on-premises or cloud based, represents a threat vector. To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies. This allows you to automatically block or flag risky behavior and take protective actions.
- Networks should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

Symmetric encryption uses the same key to encrypt and decrypt the data. Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but a single key can't be used to decrypt encrypted data. To decrypt, you need a paired key. **Asymmetric encryption** is used for things such accessing sites on the internet using the HTTPS protocol and electronic data signing solutions. Encryption may protect data at rest, or in transit.

Government agencies and industry groups have issued regulations to help protect and govern the use of data. From personal and financial information to data protection and privacy, organizations can be accountable for meeting dozens of regulations to be compliant. Listed below are some important concepts and terms that relate to data compliance.

Data residency - When it comes to compliance, data residency regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally. These regulations can differ significantly depending on jurisdiction.

Data sovereignty - Another important consideration is data sovereignty, the concept that data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed. This can add a layer of complexity when it comes to compliance because the same piece of data can be collected in one location, stored in another, and processed in still another; making it subject to laws from different countries/regions.

Data privacy - Providing notice and being transparent about the collection, processing, use, and sharing of personal data are fundamental principles of privacy laws and regulations. Personal data means any information relating to an identified or identifiable natural person. Privacy laws previously referenced "PII" or "personally identifiable information" but the laws have expanded the definition to any data that is directly linked or indirectly linkable back to a person. Organizations are subject to, and must operate consistent with, a multitude of laws, regulations, codes of conduct, industry-specific standards, and compliance standards governing data privacy.

In most cases, laws and regulations don't define or prescribe specific technologies that organizations

Identity is a concept that spans an entire environment, so organizations need to think about it broadly. There's a collection of processes, technologies, and policies for managing digital identities and controlling how they're used to access resources. These can be organized into four fundamental pillars that organizations should consider when creating an identity infrastructure.

Administration. Administration is about the creation and management/governance of identities for users, devices, and services. As an administrator, you manage how and under what circumstances the characteristics of identities can change (be created, updated, deleted).

Authentication. The authentication pillar tells the story of how much an IT system needs to know about an identity to have sufficient proof that they really are who they say they are. It involves the act of challenging a party for legitimate credentials.
Authorization. The authorization pillar is about processing the incoming identity data to determine the level of access an authenticated person or service has within the application or service that it wants to access.
Auditing. The auditing pillar is about tracking who does what, when, where, and how. Auditing includes having in-depth reporting, alerts, and governance of identities.

In the context of a computer network, a directory is a hierarchical structure that stores information about objects on the network. A directory service stores directory data and makes it available to network users, administrators, services, and applications.

Active Directory (AD) is a set of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks. The best-known service of this kind is Active Directory Domain Services (AD DS). It stores information about members of the domain, including devices and users, verifies their credentials, and defines their access rights. A server running AD DS is a domain controller (DC).

Microsoft Entra is a product family that encompasses all of Microsoft's identity and access capabilities, including Microsoft Azure Active Directory (Azure AD).

Azure AD => Devices,Public cloud Azure,Business partners,On prem Apps,On prem AD

- Used by it admins to control access to apps,resources
- To automate user provisioning between windows server ad,cloud apps
- Developers use ad for SSO to apps
- Subscribers to azure services,microsoft 365 etcc automatically have access to azure ad

Azure AD editions

Azure Active Directory Free. The free version allows you to administer users and create groups, synchronize with on-premises Active Directory, create basic reports, configure self-service password change for cloud users, and enable single sign-on across Azure, Microsoft 365, and many popular SaaS apps. The free edition is included with subscriptions to Office 365, Azure, Dynamics 365, Intune, and Power Platform.

Office 365 Apps. The Office 365 Apps edition allows you to do everything included in the free version, plus self-service password reset for cloud users, and device write-back, which offers two-way synchronization between on-premises directories and Azure AD. The Office 365 Apps edition of Azure Active Directory is included in subscriptions to Office 365 E1, E3, E5, F1, and F3.

Azure Active Directory Premium P1. The Premium P1 edition includes all the features in the free and Office 365 apps editions. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.

Azure Active Directory Premium P2. P2 offers all the Premium P1 features, and Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data. P2 also gives you Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources, and to provide just-in-time access when needed.

Azure AD manages different types of identities: users, service principals(like service accounts), managed

identities(managed service principal), and devices.
A device is a piece of hardware, such as mobile devices, laptops, servers, or printers. A device identity gives administrators information they can use when making access or configuration decisions. Device identities can be set up in different ways in Azure AD.

Azure AD registered devices. The goal of Azure AD registered devices is to provide users with support for bring your own device (BYOD) or mobile device scenarios. In these scenarios, a user can access your organization's resources using a personal device. Azure AD registered devices register to Azure AD without requiring an organizational account to sign in to the device. Supported operating systems for Azure AD registered devices include Windows 10 and above, iOS, Android, and macOS.
Azure AD joined. An Azure AD joined device is a device joined to Azure AD through an organizational account, which is then used to sign in to the device. Azure AD joined devices are generally owned by the organization. Supported operating systems for Azure AD joined devices include Windows 10 or greater (except Home edition) and Windows Server 2019 Virtual Machines running in Azure.
Hybrid Azure AD joined devices. Organizations with existing on-premises Active Directory implementations can benefit from the functionality provided by Azure AD by implementing hybrid Azure AD joined devices. These devices are joined to your on-premises Active Directory and Azure AD requiring organizational account to sign in to the device

Azure AD External Identities is a feature of Premium P1 and P2 Azure AD editions,

Azure AD Connect is an on-premises Microsoft application that's designed to meet and accomplish your hybrid identity goals. Azure AD password hash synchronization is the simplest way to enable authentication for on-premises directory objects in Azure AD Azure AD pass-through authentication allows users to sign in to both on-premises and cloud-based applications using the same passwords, like password hash synch. A key difference, however, is when users sign in using Azure AD, pass-through authentication validates users' passwords directly against your on-premises Active Directory
Federation is recommended as an authentication for organizations that have advanced features not currently supported in Azure AD, including sign-on using smart cards or certificates, sign-on using on-premises multi-factor authentication (MFA) server, and sign-on using a third party authentication solution.

Azure ad supports 2 veritfication SMS-based,VOICE CALL
OATH (Open Authentication) is an open standard that specifies how time-based, one-time password (TOTP) codes are generated. (software oath tokens,oath totp hardware tokens)

Passwordless authentication:
- Windows hello
- **Fast Identity online** sign in to their resources using an external security key or a platform key built into a device,

These FIDO2 security keys are typically USB devices, but could also be Bluetooth or Near Field Communication (NFC) based devices, which are used for short-range wireless data transfer.
- Microsoft authenticator

Password Protection is a feature of Azure AD that reduces the risk of users setting weak passwords. Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block other weak terms that are specific to your organization.

Conditional Access is a feature of Azure AD that provides an extra layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Azure AD. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate decisions for authorizing access to resources (apps and data).

Signals for conditional access:
- User or group membership
- Named location information

- Device
- App
- Real time sign in detection
- Cloud app or actions
- User risk

Access controls for conditional access:
- Block access
- Grant access
- Require one or more conditions like MFA,app policy etcc.
- Session based control

Role based access control:
- Built in roles:
    - Global administrator
    - User administrator
    - Billing administrator
- Custom roles
  Custom roles require an Azure AD Premium P1 or P2 license.
- Service specific roles are there

Azure AD RBAC - Azure AD roles control access to Azure AD resources such as users, groups, and applications.
Azure RBAC - Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management.

Azure AD Privileged Identity Management (PIM) provides extra controls tailored to securing access rights. PIM helps you minimize the number of people who have access to resources across Azure AD, Azure, and other Microsoft online services. PIM provides a comprehensive set of governance controls to help secure your company's resources. PIM is a feature of Azure AD Premium P2.

Entitlement management is an identity governance feature that enables organizations to manage the identity and access lifecycle at scale. Entitlement management automates access request workflows, access assignments, reviews, and expiration.

Entitlement management includes the following capabilities to address these challenges:

Delegate the creation of access packages to non-administrators. These access packages contain resources that users can request. The delegated access package managers then define policies that include rules such as which users can request access, who must approve their access, and when access expires.
Managing external users. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.
Entitlement management, a feature of Azure AD Premium P2, uses access packages to manage access to resources.
Access reviews are a feature of Azure AD Premium P2.

Identity Protection categorizes risk into three tiers: low, medium, and high. It can also calculate the sign-in risk, and user identity risk.
A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. Sign-in risk can be calculated in real-time or calculated offline using Microsoft's internal and external threat intelligence sources. Listed below are some of the sign-in risks that Identity Protection in Azure AD is able to identify:

- Anonymous IP address. This risk detection type indicates a sign-in from an anonymous IP address;

for example, a Tor browser or anonymized VPNs.
- Atypical travel. This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior.
- Malware linked IP address. This risk detection type indicates sign-ins from IP addresses infected with malware that is known to actively communicate with a bot server.
- Unfamiliar sign-in properties. This risk detection type considers past sign-in history to look for anomalous sign-ins. The system stores information about previous locations used by a user, and considers these "familiar" locations. The risk detection is triggered when the sign-in occurs from a location that's not already in the list of familiar locations.
- Password spray. This risk detection is triggered when a password spray attack has been performed.
- Azure AD threat intelligence. This risk detection type indicates sign-in activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

The three most frequent types of DDoS attack are:

Volumetric attacks: These are volume-based attacks that flood the network with seemingly legitimate traffic, overwhelming the available bandwidth. Legitimate traffic can't get through. These types of attacks are measured in bits per second.
Protocol attacks: Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols. These types of attacks are typically measured in packets per second.
Resource (application) layer attacks: These attacks target web application packets, to disrupt the transmission of data between hosts.

The Azure DDoS Protection service is designed to help protect your applications and servers by analyzing network traffic and discarding anything that looks like a DDoS attack.

Azure DDoS Protection comes in three tiers:
- Default DDoS infrastructure protection (previously referred to as Basic): The default DDoS infrastructure protection service is automatically enabled for every property in Azure, at no extra cost, as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft’s online services use. Azure’s global network is used to distribute and mitigate attack traffic across regions.
- DDoS Network Protection: The DDoS Network Protection service (available as a SKU), combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks. It's automatically tuned to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it requires no application or resource changes. DDoS Network Protection has several advantages over the default infrastructure-level DDoS protection, including logging, alerting, and telemetry. See DDoS Protection overview for more details.
- DDoS IP Protection (Preview): DDoS IP Protection is a pay-per-protected IP model. DDoS IP Protection contains the same core engineering features as DDoS Network Protection, but will differ in the following value-added services: DDoS rapid response support, cost protection, and discounts on WAF.

Key features of Azure Firewall

Azure Firewall comes with many features, including but not limited to:
- Built-in high availability and availability zones: High availability is built in so there's nothing to

configure. Also, Azure Firewall can be configured to span multiple availability zones for increased availability.

- Network and application level filtering: Use IP address, port, and protocol to support fully qualified domain name filtering for outbound HTTP(s) traffic and network filtering controls.
- Outbound SNAT and inbound DNAT to communicate with internet resources: Translate the private IP address of network resources to an Azure public IP address (source network address translation or SNAT) to identify and allow traffic originating from the virtual network to internet destinations. Similarly, inbound internet traffic to the firewall public IP address is translated (Destination Network Address Translation or DNAT) and filtered to the private IP addresses of resources on the virtual network.
- Multiple public IP addresses: These addresses can be associated with Azure Firewall.
- Threat intelligence: Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains.
- Integration with Azure Monitor: Integrated with Azure Monitor to enable collecting, analyzing, and acting on telemetry from Azure Firewall logs.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. A centralized WAF helps make security management simpler, improves the response time to a security threat, and allows patching a known vulnerability in one place, instead of securing each individual web application. A WAF also gives application administrators better assurance of protection against threats and intrusions.

Azure virtual network allows to segment the networks

Network security groups (NSGs) let you filter network traffic to and from Azure resources in an Azure virtual network; for example, a virtual machine.

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. Azure Bastion provides secure and seamless RDP and SSH connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS).

Just-in-time (JIT) access allows lock down of the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

When you enable just-in-time VM access, you can select the ports on the VM to which inbound traffic will be blocked.
JIT requires Microsoft Defender for servers to be enabled on the subscription.

Microsoft Azure provides many different ways to secure your data, each depending on the service or usage required.

Azure Storage Service Encryption helps to protect data at rest by automatically encrypting before persisting it to Azure-managed disks, Azure Blob Storage, Azure Files, or Azure Queue Storage, and decrypts the data before retrieval.
Azure Disk Encryption helps you encrypt Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and data disks.
Transparent data encryption (TDE) helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

Azure Key Vault is a centralized cloud service for storing your application secrets. Key Vault helps you

control your applications' secrets by keeping them in a single, central location and by providing secure access, permissions control, and access logging capabilities. It's useful for different kinds of scenarios:

Secrets management. You can use Key Vault to store securely and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.
Key management. You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
Certificate management. Key Vault lets you provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates for Azure, and internally connected, resources more easily.
Store secrets backed by hardware security modules (HSMs). The secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Cloud security posture management (CSPM) is a relatively new class of tools designed to improve your cloud security management. It assesses your systems and automatically alerts security staff in your IT department when a vulnerability is found. CSPM uses tools and services in your cloud environment to monitor and prioritize security enhancements and features.

CSPM uses a combination of tools and services:

Zero Trust-based access control: Considers the active threat level during access control decisions.
Real-time risk scoring: To provide visibility into top risks.
Threat and vulnerability management (TVM): Establishes a holistic view of the organization's attack surface and risk and integrates it into operations and engineering decision-making.
Discover risks: To understand the data exposure of enterprise intellectual property, on sanctioned and unsanctioned cloud services.
Technical policy: Apply guardrails to audit and enforce the organization's standards and policies to technical systems.
Threat modeling systems and architectures: Used alongside other specific applications.

Microsoft Defender for Cloud is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms.

Microsoft Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

Continuously assess - Know your security posture, identify and track vulnerabilities.
Secure - Harden all connected resources and services.
Defend - Detect and resolve threats to resources, workloads, and services.
The second pillar of cloud security is cloud workload protection. Through cloud workload protection capabilities, Microsoft Defender for Cloud is able to detect and resolve threats to resources, workloads, and services.

Microsoft Defender for Cloud is offered in two modes:

- Microsoft Defender for Cloud (Free) - Microsoft Defender for Cloud is enabled for free on all your Azure subscriptions. Using this free mode provides the secure score and its related features: security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.
- Microsoft Defender for Cloud with enhanced security features - Enabling enhanced security extends the capabilities of the free mode to workloads running in Azure, hybrid, and other cloud platforms, providing unified security management and threat protection across your workloads. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of resources in your subscriptions and provide enhanced security features for your workloads.

Defender plans

Microsoft Defender for Cloud includes a range of advanced intelligent protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. The Microsoft Defender for Cloud plans you can select from are:

- Microsoft Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.
- Microsoft Defender for App Service identifies attacks targeting applications running over App Service.
- Microsoft Defender for Storage detects potentially harmful activity on your Azure Storage accounts.
- Microsoft Defender for SQL secures your databases and their data wherever they're located.
- Microsoft Defender for Kubernetes provides cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.
- Microsoft Defender for container registries protects all the Azure Resource Manager based registries in your subscription.
- Microsoft Defender for Key Vault is advanced threat protection for Azure Key Vault.
- Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization.
- Microsoft Defender for DNS provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.
- Microsoft Defender for open-source relational protections brings threat protections for open-source relational databases.

Microsoft has found that using security benchmarks can help organizations quickly secure their cloud deployments and reduce risk to their organization.

The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multicloud environment.
Some of the key pieces of information in MCSB V1 are:

ID - Each line item in the MCSB has an identifier that maps to a specific recommendation.
Control domain - A control is a high-level description of a feature or activity that needs to be addressed and isn't specific to a technology or implementation. MCSB control domains include network security, data protection, identity management, privileged access, incident response, endpoint security to name just a few.
Mapping to industry frameworks - The recommendations included in the MCSB map to existing industry frameworks, such as the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standards (PCI DSS) frameworks. This makes security and compliance easier for customer applications running on Azure services.
Recommendation - For each control domain area there can be many distinct recommendations. Each recommendation captures specific functionality associated with the control domain area and is itself a control. For example, the "Network Security" control domain in MCSB v1 has 10 distinct recommendations identified as NS-1 through NS-10. Each of these recommendations describes a specific control under network security. The recommendation identified as NS-1 is to establish network segmentation boundaries.
Security principle - Each recommendation lists a "Security Principle" that explains the "what" for the control at the technology-agnostic level. For the recommendation to establish network segmentation boundaries, one of the points included in the security principle is that any workload that could incur higher risk for the organization should be

in isolated virtual networks.
Azure Guidance - Azure Guidance is focused on the "how", elaborating on the relevant technical features and ways to implement the controls in Azure. Continuing with the example of NS-1, the Azure guidance includes information regarding creating a virtual network (VNet), using network security groups (NSG), and using an application security group (ASG).
AWS Guidance - The AWS guidance is focused on the "how" specific to AWS, explaining the AWS technical features and implementation basics.

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.

A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.

Microsoft Sentinel is a scalable, cloud-native SIEM/SOAR solution that delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.

After you connect data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks. You'll see a canvas for data analysis and the creation of rich visual reports within the Azure portal.

Incidents are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve
You can use Microsoft Sentinel(incidents,workbooks,hunting,threat intelligence) to automate some of your security operations and make your security operations center (SOC) more productive. Use Microsoft Sentinel's powerful hunting search-and-query tools, based on the MITRE framework (a global database of adversary tactics and techniques), to proactively hunt for security threats across your organization’s data sources, before an alert is triggeredMicrosoft Sentinel supports Jupyter notebooks. Jupyter Notebook is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations, and narrative text. Y

Capacity Reservations and Pay-As-You-Go.

Capacity Reservations: With Capacity Reservations, you're billed a fixed fee based on the selected tier, enabling a predictable total cost for Microsoft Sentinel.
Pay-As-You-Go: With Pay-As-You-Go pricing, you're billed per gigabyte (GB) for the volume of data ingested for analysis in Microsoft Sentinel and stored in the Azure Monitor Log Analytics workspace.

With the integrated Microsoft 365 Defender solution, security professionals can stitch together the threat signals that each of these products receive and determine the full scope and impact of the threat; how it entered the environment, what it's affected, and how it's currently impacting the organization.(in apps,endpoints,identities,data,secure score,reports)

Microsoft Defender for Office 365 Plan 1

This plan offers configuration, protection, and detection tools for your Office 365 suite:

- Safe Attachments: Checks email attachments for malicious content.
- Safe Links: Links are scanned for each click. A safe link remains accessible, but malicious links are blocked.
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams: Protects your organization when users collaborate and share files by identifying and blocking malicious files in team sites and document libraries.
- Anti-phishing protection: Detects attempts to impersonate your users and internal or custom domains.
- Real-time detections: A real-time report that allows you to identify and analyze recent threats.

Microsoft Defender for Office 365 Plan 2

This plan includes all the core features of Plan 1, and provides automation, investigation, remediation, and simulation tools to help protect your Office 365 suite:

- Threat Trackers: Provide the latest intelligence on prevailing cybersecurity issues, and allow an organization to take countermeasures before there's an actual threat.
- Threat Explorer: A real-time report that allows you to identify and analyze recent threats.
- Automated investigation and response (AIR): Includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually. A security playbook can start an automated investigation, provide detailed results, and recommend actions that the security team can approve or reject.
- Attack Simulator: Allows you to run realistic attack scenarios in your organization to identify vulnerabilities. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.
- Proactively hunt for threats with advanced hunting in Microsoft 365 Defender: Advanced hunting is a query-based threat hunting tool that lets you explore up to 30 days of raw data. You can proactively inspect events in your network to locate threat indicators and entities.
- Investigate alerts and incidents in Microsoft 365 Defender: Microsoft Defender for Office 365 P2 customers have access to Microsoft 365 Defender integration to efficiently detect, review, and respond to incidents and alerts.

Microsoft Defender for Office 365 availability

Microsoft Defender for Office 365 is included in certain subscriptions, such as Microsoft 365 E5, Office 365 E5, Office 365 A5, and Microsoft 365 Business Premium.
If your subscription doesn’t include Defender for Office 365, you can purchase it as an add-on.
Use Microsoft 365 Defender for Office 365 to protect your organization's collaboration tools and messages.

The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

The Service Trust Portal (STP) is Microsoft's public site for publishing audit reports and other compliance-related information associated with Microsoft’s cloud services. S

Microsoft Priva helps you meet these challenges so you can achieve your privacy goals. Priva's capabilities are available through two solutions: Priva Privacy Risk Management, which provides visibility into your organization's data and policy templates for reducing risks; and Priva Subject Rights Requests, which provides automation and workflow tools for fulfilling data requests.

The Microsoft Purview compliance portal brings together all of the tools and data that are needed to help understand and manage an organization's compliance needs.

The compliance portal is available to customers with a Microsoft 365 SKU with one of the following roles:

Global administrator
Compliance administrator
Compliance data administrator

Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps admins to manage an organization's compliance requirements with greater ease and convenience. Compliance Manager can help organizations throughout their compliance journey, from taking inventory of data protection risks, to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Compliance score measures progress in completing recommended improvement actions within controls. The score can help an organization to understand its current compliance posture. It also helps organizations to prioritize actions based on their potential to reduce risk.

Microsoft Purview provides three ways of identifying items so that they can be classified:

manually by users
automated pattern recognition, like sensitive information types
machine learning

Sensitivity labels, available as part of information protection in the Microsoft Purview compliance portal, enable the labeling and protection of content, without affecting productivity and collaboration

After sensitivity labels are created, they need to be published to make them available to people and services in the organization. Sensitivity labels are published to users or groups through label policies. Sensitivity labels will then appear in Office apps for those users and groups.

Microsoft Purview Data Loss Prevention (DLP) is a way to protect sensitive information and prevent its inadvertent disclosure. With DLP policies, admins can:

Identify, monitor, and automatically protect sensitive information across Microsoft 365, including:
OneDrive for Business
SharePoint Online
Microsoft Teams
Exchange Online
Help users learn how compliance works without interrupting their workflow. For example, if a user tries to share a document containing sensitive information, a DLP policy can send them an email notification and show them a policy tip.
View DLP reports showing content that matches the organization's DLP policies. To assess how the organization is following a DLP policy, admins can see how many matches each policy has over time.
DLP policies protect content through the enforcement of rules that consist of:

Conditions that the content must match before the rule is enforced.
Actions that the admin wants the rule to take automatically when content that matches the conditions has been found.
Locations where the policy will be applied, such as Exchange, SharePoint, OneDrive, and more.

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices

Endpoint DLP enables admins to audit and manage activities that users complete on sensitive content. Listed below are a few examples:

Creating an item
Renaming an item
Copying items to removable media
Copying items to network shares
Printing documents
Accessing items using unallowed apps and browsers

Retention labels and policies help organizations to manage and govern information by ensuring content is kept only for a required time, and then permanently deleted. Applying retention labels and assigning retention policies helps organizations:

Comply proactively with industry regulations and internal policies that require content to be kept for a minimum time.
Reduce risk when there's litigation or a security breach by permanently deleting old content that the organization is no longer required to keep.
Ensure users work only with content that's current and relevant to them. When content has retention settings assigned to it, that content remains in its original location. People can continue to work with their documents or mail as if nothing's changed. But if they edit or delete content that's included in the retention policy, a copy of the content is automatically kept in a secure location. The secure locations and the content are not visible to most people. In most cases, people don't even need to know that their content is subject to retention settings.

Microsoft Purview Records Management helps an organization look after their legal obligations. It also helps to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be kept, no longer of value, or no longer required for business purposes. Microsoft Purview Records Management includes many features, including:

Labeling content as a record.
Establishing retention and deletion policies within the record label.
Triggering event-based retention.
Reviewing and validating disposition.
Proof of records deletion.
Exporting information about disposed items.

Microsoft Purview Insider Risk Management is a solution that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Insider risk management is available in the Microsoft Purview compliance portal.

Microsoft Purview Information Barriers is supported in Microsoft Teams, SharePoint Online, and OneDrive for Business.

Information barriers are policies that admins can configure to prevent individuals or groups from communicating with each other.

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic

information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft Purview to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use eDiscovery cases to identify, hold, and export content found in mailboxes and sites.

Microsoft Purview provides three eDiscovery solutions: Content search, eDiscovery (Standard), and eDiscovery (Premium).

- Content Search. Use the Content search tool to search for content across Microsoft 365 data sources and then export the search results to a local computer.
- eDiscovery (Standard). The eDiscovery (Standard) solution builds on the basic search and export functionality of Content search by enabling you to create eDiscovery cases and assign eDiscovery managers to specific cases. The eDiscovery (Standard) solution also lets you associate searches and exports with a case and lets you place an eDiscovery hold on content locations relevant to the case.
- eDiscovery (Premium). The eDiscovery (Premium) solution builds on the existing capabilities in eDiscovery (Standard). In addition, eDiscovery (Premium) provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations. It lets legal teams manage custodians, people that you've identified as people of interest in the case, and the workflow to communicate with custodians. It allows you to collect and copy data into review sets, where you can filter, search, and tag content so you can identify and focus on content that's most relevant. The eDiscovery (Premium) solution provides analytics and machine learning-based predictive coding models to further narrow the scope of your investigation to the most relevant content.

Aduti standard and audit premium for auditing

Azure policy,azure blueprints

AZ-500

Sunday, December 18, 2022 6:11 PM

Azure AD is a HTTP/HTTPS based identity solution so it can be queried using rest api through http,https

I does not use kerberos authentication it uses SAML,WS-federation,OpenID connect(authentication),Oauth(authorization)

There are no organizational units or group policy objects and it is a flat structure AD

Whereas ACTIVE DIRECTORY DOMAIN SERVICES uses LDAP for querying, use kerberos,have organizational units, group policy objects

Azure active directory domain services provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos / NTLM authentication that is fully compatible with Windows Server Active Directory.

LDAP write support is available for objects created in the Azure AD DS managed domain, but not resources synchronized from Azure AD

Users:

- Cloud identities(Created using azure AD)
- Directory-synchronized identities(AD CONNECT)
- Guest users

AD GROUPS:

- Security groups
    - For providing access to resources
        - Assigned(add speicific users(usual one))
        - Dynamic user(dynamic membership rules for add or remove if rule requirements are met)
        - Dynamic device(dynamic groups rules to automaticallly add or remove devices)
- Microsoft 365 groups
    - Provides access for shared mailbox,calendar,files,sharepoint etcc..
        - Assigned(add speicific users(usual one))
        - Dynamic user(dynamic membership rules for add or remove if rule requirements are met)

An administrative unit is an Azure AD resource that can be a container for other Azure AD resources. An administrative unit can contain only users and groups. Administrative units restrict permissions in a role to any portion of your organization that you define.

To use administrative units, you need an Azure Active Directory Premium license for each administrative unit admin, and Azure Active Directory Free licenses for administrative unit members.

Passwordless authentication methods:

- Windows hello
- FIDO2 security keys
- Authenticator
- FIDO2 smatcards
- Temporary access pass

Azure AD Connect will integrate your on-premises directories with Azure Active Directory. This allows you to provide a common identity for your users for Microsoft 365, Azure, and SaaS

applications integrated with Azure AD.

Azure Active Directory (Azure AD) Connect Health provides robust monitoring of your on-premises identity infrastructure

Password hash synchronization (PHS) is a feature used to synchronize user passwords from an on-premises Active Directory instance to a cloud-based Azure AD instance

Azure AD Pass-through Authentication (PTA) is an alternative to Azure AD Password Hash Synchronization, and provides the same benefit of cloud authentication to organizations. PTA allows users to sign in to both on-premises and cloud-based applications using the same user account and passwords. When users sign-in using Azure AD, Pass-through authentication validates the users' passwords directly against an organization's on-premise Active Directory.

Use federation Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization.

Password writeback is a feature enabled with Azure AD Connect that allows password changes in the cloud to be written back to an existing on-premises directory in real time.

Identity Protection:
Policies:

- MFA registration policy
- User risk remediation policy
- Sign in risk remediation policy

To prevent repeated MFA attempts as part of an attack, the account lockout settings let you specify how many failed attempts to allow before the account becomes locked out for a period of time. Configure the fraud alert feature so that your users can report fraudulent attempts to access their resources.

User's states can be Enabled, Enforced, or Disabled.

Trusted IPs is a feature to allow federated users or IP address ranges to bypass two-step authentication.

Conditional access comes with six conditions: user/group, cloud application, device state, location (IP range), client application, and sign-in risk.

Azure AD Privileged Identity Management (PIM) allows you to manage, control, and monitor access to the most important resources in your organization. You can give just-in-time access and just-enough-access to users to allow them to do their tasks.

Microsoft Identity Manager or MIM helps organizations manage the users, credentials, policies, and access within their organizations and hybrid environments. With MIM, organizations can simplify identity lifecycle management with automated workflows, business rules, and easy integration with heterogenous platforms across the datacenter.

Priveledged identity management can do just in time , time bound,approval based mfa based etc..

Azure Resource Manager is the deployment and management service for Azure. It provides a consistent management layer that allows you to create, update, and delete resources in your Azure subscription. You can use its access control, auditing, and tagging features to help secure and organize your resources after deployment.

Azure provides four levels of scope: management groups, subscriptions, resource groups, and

resources

Network Virtual Appliances
You can deploy an NVA to a perimeter network in many architectures. In the previous diagram, the NVA helps provide a secure network boundary by checking all inbound and outbound network traffic and then passing only the traffic that meets the network security rules

Application security groups
ASGs enable you to configure network security as a natural extension of an application's structure. You then can group VMs and define network security policies based on those groups.

You also can reuse your security policy at scale without manual maintenance of explicit IP addresses. T

A virtual network service endpoint provides the identity of your virtual network to the Azure service. Once service endpoints are enabled in your virtual network, you can secure Azure service resources to your virtual network by adding a virtual network rule to the resources.

Azure Private Link works on an approval call flow model wherein the Private Link service consumer can request a connection to the service provider for consuming the service. The service provider can then decide whether to allow the consumer to connect or not. Azure Private Link enables the service providers to manage the private endpoint connection on their resources
Approved
Reject
Remove

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on the source IP address and port to a destination IP address and port.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

Azure Front Door enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reaches a global audience with Azure. Azure Front Door grants the ability to define, manage, and monitor the global routing for web traffic by optimizing for best performance and instant global failover for high availability.

ExpressRoute is a direct, private connection from your WAN (not over the public Internet) to Microsoft Services, including Azure. Site-to-Site VPN traffic travels encrypted over the public Internet. Being able to configure Site-to-Site VPN and ExpressRoute connections for the same virtual network has several advantages.

Privileged Access Workstations (PAWs) provide a dedicated system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides very strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket.

Azure Update Management is a service included as part of your Azure subscription. With Update Management, you can assess your update status across your environment and manage your

Windows Server and Linux server updates from a single location—for both your on-premises and Azure environments.

Azure Disk Encryption for Windows VMs helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the BitLocker (DM-CRYPT FOR LINUX) feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.