Learning objectives

5 std. cloud computing characteristics:

On demand self-service

Broad network access

Resource pooling

Rapid elasticity

Measured service

Cloud deployment modes:

Public

Private

Hybrid

Community

Cloud service models:

IaaS

PaaS

SaaS

Core Azure items:

Data centers

Regions

Availability zones

Azure Arc – to manage on premises & multi-cloud environments

Cloud computing characteristics

Idea with cloud computing – have a metered self-provisioned way to access IT services over a network

5 main cloud computing characteristics

Resource pooling –

Cloud service provider (CSP) has equipment available for cloud tenants (us)

Some resources of a cloud are – compute, network, storage, etc.

Resource pooling means that all these resources **appear** to be infinite to the cloud tenant

Broad access –

We can use a wide array of devices to access a cloud service

Cloud service – Some kind of IT service available on cloud

Rapid Elasticity –

We as tenants have the ability to add or remove IT services running in the cloud.

This allows us to scale.

Eg:- Adding or removing storage as needed, Adding/Removing VMs, resizing VMs, autoscaling

On-demand self-service –

Cloud user can deploy & manage resources by themselves. The CSP technicians don’t have to get involved.

This provides us with control to provision & de-provision resources by ourselves.

Metered Usage –

Our usage of power-based resources, etc. are tracked & we pay for what we use.

Virtualization & Azure

Virtualization doesn’t mean that the environment is a cloud. But cloud means that virtualization is possible.

OS virtualization requires a hypervisor.

A hypervisor is a streamlined OS that’s designed to regulate access from multiple VMs to one set of underlying hardware.

Type 1 hypervisor

Type 2 hypervisor

Application virtualization / App streaming – Users have access to an app but it isn’t installed on the device they are using. It’s running in the cloud.

Application container – Logical boundary containing everything an app needs to run. It runs on a host that has an installed engine that can run containers. They are smaller than VMs & run faster.

Virtual Desktop Infrastructure (VDI) – Access a desktop OS which actually runs on the cloud.

SDN – Allows customers to configure their own cloud networks without connecting to an underlying network infrastructure device. It provides an abstraction layer that allows user to easily configure networks using CLI or GUIs instead of native language of routers & switches.

Type 1 hypervisor

Is an OS.

Runs directly on hardware. Therefore the name “Bare metal hypervisor”

Streamlined to support virtualization hosting.

Eg:- VMWare

Type 2 hypervisor

Runs as an app within OS.

Stability & performance of host OS affects VM guests.

Type 1 > Type 2 hypervisor

In Azure cloud we have an option of dedicated VM Hosting

A single cloud customer has access to a hypervisor running on a physical host in a data center. It will not run any other VMs of other customers on it.

This is more expensive than shared hosting of VMs.

We use it especially when there’s legal/regulatory compliance.

VM Sprawl – It’s quick & easy to provision VMs in cloud. However, it is also very easy to forget about VMs. VM Sprawl occurs when no: of VMs increase to the extent that admins can no longer control or manage them. This will lead to wasteful consumption of resources, increased costs, loss of performance & even server crash.

Cloud deployment models

Public clouds –

Available to anyone over the internet

Cloud provider owns the IT infrastructure

Adhere to strict data security & data center security standards

Providers probably will have data centers in multiple locations

CSP security accreditations are required so that users will use them.

Shared responsibility models – CSP responsible for hardware, Customer responsible for configuration, software install, updates, etc.

Data Sovereignty – laws of the location will apply to data

Larger target for malicious users

Cloud service offerings may vary between geographical regions.

Private cloud –

Infrastructure is owned & used by a single organization

They have full config control

Full responsibility for what happens

Metered usage can still be used in internal clouds

Also uses virtualization

Hybrid cloud –

Combination of private & public cloud

Owner has full configuration control (private)

Also uses virtualization

Confidential processes and data might have to remain under a single org. Due to company or country laws.

Community clouds –

Adheres to all cloud computing characteristics

It’s a specialized cloud with services tailored for specific needs/audience

Eg: Azure US Govt., Azure Germany

Azure Data Centers –

All azure cloud services are located here

Physical locations are not disclosed in the interest of security

There will be one or more within an availability zone (AZ)

Designed with redundancy in mind – power failure, network failure, etc.

There will be physical security at the location

IaaS –

Underlying infrastructure is provided

Data centers

Configured by IT sys admins

Network, Network security, Storage, Compute etc. are to be deployed by us.

Service-level agreement guarantees a certain amount of uptime.

CSP & tenant has shared responsibility

CSP – Hypervisor, network equipment, physical storage, provisioning

Tenant – VM deployment, management, VNETs, storage provisioning

Eg: - Storage accounts (can store BLOBS, shared folders, can be used to create message cubes), make VMs, make VNets, Azure Firewall – Lets us configure firewall for Azure env.

IaaS benefits

Less provisioning time than on-premises

Accessible from anywhere

Shared responsibility

Azure IaaS can be managed via

GUI management – Azure portal

Azure CLI

Azure PowerShell

Programmatic API calls

Templates

PaaS

Underlying infrastructure required to support IT services are provisioned by the CSP

It’s a managed service

Configuration of PaaS is done by cloud customers

Service Level Agreements are provided

CSP – Infrastructure, VM maintenance, software patching etc.

Tenant – Configuration of the solution, data

Eg: of PaaS – Azure Active Directory (Azure AD)

Network configs, servers are deployed & managed for us

No organizational units (OUs)

No group policy

(If you need OUs you can deploy AD in a VM so that you can have full AD control)

Azure SQL Database

No network config, servers to be managed

No DB software to be installed

We can directly use it.

However, if you want complete SQL database control, deploy them manually as IaaS

Azure Virtual Desktop (AVD)

No network config to deploy or manage

No client-based VM to deploy or manage

We can select a bundle – Hardware + software config

We can create customized bundles

Azure PaaS can be managed using:

GUI management (Azure Portal), Azure CLI, Azure PowerShell, Programmatic API calls

SaaS

End-user applications. You are paying for the use of the application

Limited config options

Isolated from other cloud tenants

Managed services

Software managed by CSP

SLAs provided

CSP – Infrastructure, software maintenance, patching of software, tenant isolation, provisioning user accounts & groups, multi-factor authentication, single sign-on, user permissions

Tenant – Application config, usage, data privacy

SaaS benefits

Accessible from anywhere using any platform

Normally no software deployment needed

Users are familiar with cloud-based applications, learning curve is small

Pay only for what you used

Most of the time, it’s accessible using a web browser

Eg: - Microsoft 365

On premises IT hardware responsibilities

Acquisition & shipping

Config

Ongoing management

Firmware updates

Decommissioning

On-premises IT software responsibilities

Acquisition, licensing

Configuration

Ongoing management, user provisioning

Software updates

Decommissioning

On-premises vs public cloud

CapEx (Capital Expenditure) is high for On-premises

OpEx (Operational Expenditure) depends on a lot of variables including time

Total cost of ownership could be less for public cloud providers

CSPs are economies of scale so they can provide their services for a relatively low rate

On-premises cloud might not work during natural/man-made disasters

Public clouds have resiliency due to IT system duplication & data duplication

Azure regions

We can specify azure region when deploying a resource

More than 60 worldwide

Service availability vary by region

Some configurations require resources to be in the same region. Eg: Key Vault & storage account using customer managed keys

Azure Availability Zones

Contained within an Azure region & each region has at least 1.

Each availability zones are linked using high-speed networks

Some services can be replicated across availability zones for resiliency

Azure Sovereign Regions

A type of community cloud tailored for a specific need or regulatory requirement

Isolated from standard public Azure cloud

Eg: Azure Govt. , Azure German cloud, Azure China cloud

Azure Arc

Allows ppl to manage IT resources across platforms, different clouds, data centers as if they were running in Azure. Therefore for all of them we can easily use Azure management tools.

Eg: An on-premises IT service, multi-cloud IT services etc. Edge IT services etc. can be managed via Azure Arc

Azure Arc allows for Unified Management

Azure Arc can be managed via

Azure portal

Azure CLI

Azure PowerShell – Object Oriented

Azure REST API

Azure Arc can be used to manage external services

E: Physical/Virtual machines like Windows, Linux,

Kubernetes

Microsoft SQL Server

In order for these to show up in Azure arc we need to enable the servers for azure arc.

To do this we have to install Azure Connected Machine agent on it.

The server is then assigned a resource id, becomes part of a resource group and is assigned a managed identity. Thus making it possible for us to manage it via Azure Arc

Server is treated as a std. Azure resource and can have tags applied to it, azure policy can be applied

Servers can be monitored using logging tools like Log Analytics workspace

Azure arc is used for

Centralized compliance

Centralized server config management