CLOUD DEPLOYMENT
Cloud Architecture
Interaction of Cloud Components
Interaction of Non-Cloud Deployment
Evaluation for Cloud Deployment
Automation and Orchestration

Configuration and Deployment: Cloud Architecture
Common Services & Common Deployment Models
Cloud Benefits
Resource pooling
On-Demand self-service
Elasticity
: to scale dynamically your resources in the cloud
as there is a demand or lack of demand for the
se
services, e
.g., AWS
(using autoscaling in order to scale up or down
resources dynamically based on demand
Measured services
Broad network access
CapEx
to
OpEx
:
in stead
of spending a lot of money upfront
on capital expenditure
s, we can spend nothing and still offer services
, e.g., free tier account with big cloud provider
s
. We start for free and as we add more resources
and we have more demand, we start paying
. Capital expenditures and traded for Operation expenditures
, and they can scale as our business scales
Service quality
New tech
: we can take advantage of new technology such as artificial intelligence (AI)
and machine learning
might be unavailable to us without
a
cloud
implementation.

Service Model (spending less money while offering services to clients
SaaS
(Software as a Service
)
: Gmail – many companies don’t have to have their own server for their corporate email
PaaS
(Platform as a Service):
allows us to have in the cloud virtual machines
spun up
(VMs)

; have the machines spun up
s
o our
software
developer
s can go in and develop software
. Today’s examples of software clients are
G
oogle,
android based phones,
ioS
apple device

IaaS
(Infrastructure as a Service): for outsourcing
-
-
Here the cloud provider
provides
the routers,
switches,
firewalls
.

XaaS
(Everything as a Service):
Everything on the service model can be offered as a service.

Deployment Model

Private
: you might have the equipment and the expertise
to do all in-house, and when you do it is called private. Advantage
, if you know what you are doing, is high security
because you own everything
that has to do with the cloud.

Public
: the exact opposite of private is public. An example is AWS
; we connect to AWS via the internet or private connection
and leverage their expertise to host the cloud resources for us
.

Hybrid
: today the most common approach is the hybrid
where some of our cloud
stuff
is
private,
and some is public
.

Community
: if a group of entities give their services to
one cloud
, e.g., US community cloud
being provided services by Microsoft, etc.

Others
: Single server, single cloud, multi-cloud

The Big 4 Public Clouds

Azure (gaining the fastest)
Google cloud platform
AWS (the biggest)
IBM cloud

Configuration and Deployment: Interaction of Cloud Components

Q: What do we do with a complex system like our IT infrastructure?
A: We modularize it and compartmentalize components of the complex infrastructure to make it more understandable, to ease our troubleshooting, to ease design.

Cloud Components (Components of Cloud Infrastructure)

Network components
Application components
Storage components
Compute components
Security components
Database components
: i
t may be separate or be included in application components;
might include AI
. But where do we put AI if it is big in our organization. It could
possible
be in three of the components.
Migration components
:
How do these components interact with one another?

Configuration and Deployment: Interaction of Non-Cloud Components

Network Resources:
Bandwidth
Authentication requests
Queries
Data transfer
Application related notification
s
Within multi-availability zones in a region (e.g., AWS has 3 zones in a region and provides high-speed connectivity between those availability zones in the region. If a resource in one zone wants to communicate with another resource in another zone, we do not have to worry about bandwidth. But when it comes to connecting into the public cloud for management, the bandwidth could be a concern. Do we have “plenty” for authentication requests, queries, application related notifications, API calls, and most importantly, is there sufficient data bandwidth for us to transfer the massive data.
The network resources that we are going to have to interact with cloud resources are going to need the appropriate bandwidth, which could be enormous.

Security Resources (located out of cloud implementation. They need to be utilized and altered in order to accommodate the cloud by making key configuration on the following so that we can seamlessly communicate in and out with a public cloud infrastructure (or private cloud located off premises) successfully**)**
Firewall
s
Proxies
Encryption
Antivirus

Compute Resources:
On-premise
inventory,
etc
APIs
(Application Program
ing
Interfaces)
Authentication
Storage
(not all of our
compute or storage
resources
will be in the cloud
most likely
.
So
for communication between the storage and the cloud, there must be sufficient bandwidth.

Other Resources
Monitoring
Logging
Compliance
Reporting
User interface (
U
I
)
: for those that will interact with our cloud
. May be they are on windows
workstation,
Linux boxes, Mac, iOS, Android
, and client systems
. We have to accommodate these when it comes to interacting with the cloud

Configuration and Deployment: Evaluation for Cloud Deployment
(Existing systems and applications)
Prepare for Deployment
Existing systems
Business goal
s
Fallback plan
Platforms
(
e.g.,
legacy systems)

Prepare for Deployment
Applications (do your applications need these)
Direct
Hardware (
HW
)
access

Hard coded IPs
Latency
File size
APIs
Cloud elements
Target objects

Configuration and Deployment: Automation and Orchestration
Automation and Orchestration tools are not only infrastructure that is already deployed in the cloud but are also used when it comes to initially deploying your cloud infrastructure.
Automation: typically performing one task or a couple of tasks in order to ease the workload on getting something done.
Orchestration: coordination of a whole bunch of tasks, or it is the automation combined, or multiple automations combined in a workflow. Or, is the organized controlled collection, and execution of many tasks in the cloud?

Configuration and Deployment: Preparing for Deployment
Things to gather as we prepare for deployment
Plans
(goals, business advantages
, stakeholders, who to communicate with,
risks, moving to the cloud)
Baselines
(gather performance baseline data
)
Structure
(resource grouping,
regions
of azure to use
,
networking components, band
width type
)
.
Target hosts
(most likely spinning up
VMs in
Microsoft
cloud
. How will the target hosts look like
?)
Command
s
(will help with deployment
;
there are
APIs that will allow us to script against
the various clouds
that we might be working with.
Tools
(e.g., cloud formation
tool in AWS
, migration tool in Azure
)

Configuration and Deployment: Execute a Deployment Plan

Steps to go through as we execute the plan

Change management

SOP

Workflow

Automat
e
and Orchestrat
e

Commands and Tools

Document

Configuration and Deployment: A Deployment Testing Plan

Types of Deployment

Production
: for clients

Development
: for software developers

Quality Assurance (
QA
)
or Testing

Cloud
:

Specialized Testing Techniques

Vulnerability

Penetration

Load

Shared Components (example of what to test)

Storage

Compute

Network

Connectivity

Sizing

Performance

High availability

Replication

Load balancing

Data integrity

Proper function

Automation/
O
rchestration

Configuration and Deployment: Analyzing Deployment Test Results

Test Results

Success Factors

Sizing

Performance

Availability
Connectivity
Data Integrity
Proper Functionality

We should do evaluate these after we obtain the test results
Document results
(we document all of the analysis done from listed items below)
Baseline
c
omparison
s
Service
Level
Agreement (SLA)
comparisons
Cloud Performance Fluctuation
Variables

Configuration and Deployment: Deploying a Virtual Network
Network Components
Subnets
(in addition to virtualization,
we
are shielded from configuration; this will be done by the provider)
NAT
Router
Switch
Port and Protocols

Configuration (we are shielded from configuration)
Address space required
(consider size for
future
growth)
Network segmentation/
microsegmentation
DMZ
:
we can do segmentation on DMZ
–
a kind of security device like a firewall
that
separate
or segment
the inside private stuff from the outside pri
vate stuff
. Since DMZ is an inside device, we can
park
it
to
be accessed by

the outside world
for resource outside world might need
but not prone to attack
V
(
X
)
LAN
: inherent limitation to the number of IDs it can have:
4,096
. V
(
X
)
LAN identifiers are used to
carry (customers') traffic
across the entire infrastructure
. So, VXLAN
is about is to increase the number of identifiers to 16
million
VPN –
(Intrusion Detection Systems)
IDS/
Intrusion Pr
even
tion Systems
(
IPS
)
SLA change management

Configuration and Deployment: Virtual Networking in Azure
Virtue Networking in Azure
Create
r
esource group
Create
virtual network
(can be used to host VMs
and other services that we are going to spin up
)
Create v
irtual machines
(example of a resource)
to be
sp
u
n up

Configuration and Deployment: CPU and Memory Sizing
Available vs proposed resources
CPU
RAM
CPU Technologies
Hyperthreading

(HT or HTT)
: allows multiple calculations to be run in parallel
.
VT-
x
(Virtual Technology Extension)
Overcommitment ratio
Memory Technologies
Bursting and ballooning
: memory is engaged in ballooning
. Repeated requests to the memory
without going through the normal steps they have to
go through in order to request resources
is termed bursting
.
Overcommitment ratio
Performance Considerations
Dedicated compute environment vs shared compute environment
Cost considerations
Effect to HA/DR
(High availability/Disaster re
c
overy
)
Energy saving

Configuration and Deployment: Storage Types
Storage types
NAS
(Network Attached Storage)
: using access protocol like SMB
DAS
(Direct Attached Storage)
: block storage
to access DAS
SAN
(Storage Area Network)
: using iSCSI, FC, FCOE
Object storage
Access protocols
Management differences

Configuration and Deployment: S3 in AWS
What is S3? Simple Storage Service
Buckets: storage device of unlimited sizes
Objects: stored in the bucket; 5 TB
Keys: object name is a key
AWS regions
Object URL
Security

Configuration and Deployment: Provisioning Storage

Configuration and Deployment: Protecting and Securing Storage

Protecting Storage

Protection Capabilities

High availability

Failover zone

Storage replication

Regional

Multiregional

Synchronous and asynchronous

Storage mirroring

Cloning

Redundancy level factor

Securing Storage

Security configurations for applicable platforms

ACL

s (Access control lists)

Obfuscation

:

protecting data in such a way that you can't make sense of it

Zoning

: hard and soft zoning

User

/host authentication and authorization

Configuration and Deployment: AWS S3 Versioning

Configuration and Deployment: Workload Migration Types

Workload migration is the movement of VMs on premises to a VMs on the cloud.

Workload can be referred to applications, VMs, containers (many VMs)

Migration types

P2V

(physical to virtual):

virtualizing physical server

and migrating it to

the cloud and operat

ing

it as a VM

. Must make the operating system and applications can run in the virtualized environment.

V2V

(virtual to virtual): this is when you are running a virtual machine

o

n premises and migrating it to

V instance

s

in the cloud.

V2P

(virtual to physical): very rare; could be because the virtualization did not work out

, or not getting the level of security needed

, and so want to dedicate a

hardware in the cloud for that purpose

to guarantee the level of desired security.

P2P
(physical to physical):
also,
rare; taking
physical server on premises to a hardware in the cloud
due to performance and or security metrics
Storage migration
s
Online vs offline migrations

Configuration and Deployment: Workload Migration Considerations
Source and destination format of the workload
Workload examples: database, analytical, transaction, batch
Virtualization format
(moving container? OVF
–
open virtualization format, an example of format
Application and data portability
(think of how portable
the application or data is
.
Network connections and data transfer methodologies
SOP for workload migration
Environmental constraints
Bandwidth
Working hour restrictions
Downtime impacts
Peak time frame
Legal restrictions
(
oversea migration)
Follow-the-sun constraint/time zones

Configuration and Deployment: Extend an Infrastructure
Identity management elements
Identification
Authentication
Authorization
Approval
Access policy
Federation
(no transmission of a password. An entity identifies you, then it sends to another entity that it is you
. A token is used.
)
Single
sign on
(SSO)
: password is transmitted her
e
.
You sign in
with a password
to one entity
/domain
, and to access the other entity a password from the first entity will be sent to the other.

For E-SSO, there is password
transmission
involved
(it is not entered by the individual
)
but the password is automatically
provided by software during the E-SSO approach.

Element considerations to deploy infrastructure services such as
DNS
DHCP
Certificate services
Local agents
Antivirus
Load balancer
Multifactor authentication
Firewall
IPS/IDS
(
IPS detects and protects against attacks; IDS detects attacks)

Security: Policies and Compliance
Complying with security policies of our organization
Complying with potential government regulations
Try to zero in on best practices

Security: Encryption and Tunneling
Encryption technologies
IPSec
(great security)
SSL/TLS
Other ciphers
Tunneling protocols
L2TP
(great security)
PPTP
GRE
(generic routing encapsulation)
: it does not offer security
; can be used in conjunction with security protocols
.
Key and certificate management
PKI
(public key infrastructure)
: useful in the area of identity and authentication.

Security: Securing the Infrastructure
Although there is shared responsibilities, but the following is a list of what we must still do for ourselves.
Appropriate configuration for the applicable platform as it applies to compute:
Disabling
unneeded ports
and services

Account management policies
Host-based/software firewalls
Antivirus/antimalware
software
Patching
Deactivating default accounts
Automation and orchestration processes as applicable (these can assist us in carrying out the above

Security: Using ACLs
(Access Control Lists)
:
An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object
.
Access control methods
Role-based administration
: based on roles user can do what they want to do
Mandatory access control
s
:
fine graining
what an entity can do
, not relying on any inheritance or relationship between objects.
Discretionary access controls
:
use a
group concept
and defines the groups then
put users in group, and
groups fine grains what users can do.
Non-discretionary access controls
: another term for mandatory access controls.
Multifactor authentication
Single sign on

Security: Security Groups Versus Network ACLs in AWS
Security Groups
Stateful
Apply to network interfaces
Allow only
Rules evaluated as a whole (most restrictive)
Can reference other security group
in the same VPC
Network ACL
Stateless
Apply to subnets
Allow and deny
Processed in order

Security: Secure a Cloud Service Model
Secure cloud model
Data classification
Concept
s

of segmentation and
microsegmentation
of resources
, storage,
etc
Network
Storage
Compute
Use encryption as defined
(for data in transit and at rest)
Use multifactor authentication as defined
Apply
defined audit/
compliance requirements

Security: Automation
Security Automation
Tools
APIs
(
Application Programming Interface
, which is a software intermediary that allows two applications to talk to each other.
)
Vendor application
CLI
Web GUI
Cloud portal
Techniques
Orchestration
Scripting
Custom programming

Maintenance: Applying Patches
Applying patches (a Patch is a modification to a program to improve its security, performance, or other feature. A patch is sometimes referred to as a bug fix since a reason for a patch is an imperfection that is discovered by its developers or users.)
Scope of cloud elements to be patched
Hypervisors
Virtual machines
Virtual appliances
Network
ing
components
Application
Storage components
Clusters

Maintenance: Applying Updates
Types of updates
Hotfix (does not cause disruption
,
a small update designed to fix a flaw and is often considered an emergency measure

)
Patch
Version update
Rollback
(this may be a back remedy for version update in case of any problem with update.
Activities to be performed by automation tools
Snapshot
Cloning
Patching
Restarting
Shut down
Maintenance mode
Enable/disable alerts

Maintenance: Backup and Restore
Backup types
Snapshot/redirect
-
on-write
Clone
Full
(classic)
Differential
(classic)
:
backs up everything since the last full backup
Incremental
(classic)
Change block/delta tracking

Maintenance: Disaster Recovery
(DR)
Methods
DR capabilities of cloud service providers
SLAs for DR
(
A Service Level Agreement (SLA) is a service-based commitment between Information Technology Services (the service provider) and the customer procuring the technology service. Each SLA
includes:
A description of the service. Service term and costs.
)
Corporate guidelines
Cloud service provider guidelines
Bandwidth or ISP
(
Internet service providers
)
limitations
Techniques
Site mirroring
Replication – file transfer
Archiving
: AWS uses Glacier for archiving
Third party sites
Recovery Time Objective (RTO) refers to how much time an interruption can last for any business function.

Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or “tolerance.”

Maintenance: Disaster Recovery in AWS
Availability zones (AZs) are isolated locations within data center regions from which public cloud services originate and operate.

Maintenance: Business Continuity
(or Business Continuity Plan – BCP)

Maintenance: Maintenance Automation
Maintenance automation tasks
Clearing and archiving logs
Compressing drives
Removing inactive accounts
Removing stale DNS entries
Removing orphan resources
Removing outdated rule
s
from firewall
Removing outdated rule
s
from
security
Resource reclamation
Maintain ACLs for the target object

Management: Forecasting Future Needs
Monitoring
Target object baselines
: monitoring to forecast for future we need to know the baseline, what’s normal
performance
Target object anomalies
: need
a
mechanism to
anomalies
Common alert methods/messag
ing
Alerting based on deviation from baseline
Even collection and event correlation

Management: Allocating Cloud Resources
Resources needed based on cloud deployment
Community
Hybrid
Private
Public
Allocate cloud resources
Support agreements

Configuration management tools
Resource balance techniques
Change management (advisory board,
approval process, document actions tak
en
– CMDB, spreadsheet
)
. CMDB is configuration management database.

Management: Planning Provisions/Deprovisions
Prov./Deprov.
Usage patterns
Cloud bursting (auto
-
scale technology)
Cloud provider migrations (migrating from one provider to another)
Extending cloud scope (
adding/extending our services maybe from
S
aaS to PaaS, for example
)
Application life cycle
Application deployment
Application upgrade
Application retirement
Application replacement
Application migration
Application feature use (increase/decrease)
Business need change
Mergers/acquisitions/divestitures
Cloud service requirement change
s
Impact of regulation and law changes

Management: Account Provisioning
Account life cycle
Account management policy
L
ockout
password complexity rules
Automation and orchestration activities
Use account reaction
Permission setting
s
Resource
access
User account removal
User account disablement

Management: Analyze Deployment Results
Procedure to confirm results
CPU usage
RAM usage
Storage utilization

Patch versions
Network utilization
Application version
Auditing
enable
Management tool compliance

Management: Applying Changes
Analyze performance trend
Refer to
baslines
Refer to SLAs (service level agreement)
Tuning of cloud target objects
Compute
Network
Storage
Service/application resources
Recommend changes to meet expected performance /capacity
Scale up/down (vertical)
Scale in/out (horizontal)
You've decided to provide a web application and scale it by using many small Linux instances. Adding four instances and load balancing between them over the last month is an example of which of the following? **Scale out**.

Management: Reporting Metrics
Chargeback/showback models
Reporting based on company policies
Reporting based on SLAs

Which of the following might govern how we need to report metrics for our cloud infrastructure? Based on corporate policy, based on SLAs

Troubleshooting: A Methodology
Identify the problem
Establish a theory of probable cause
Test the theory to determine the cause
Establish a plan of action to solve the problem
and identify potential effects
Implement the solution or escalate
as
necessary
Verify full system functionality
and, if applicable, implement preventive measures
Document finds, actions, and outcomes

Troubleshooting: Identify the Problem
Gather info
Duplicate problem, if possible
Question users
Identify symptoms
Determine if anything has changed

Approach multiple problems individually

Troubleshooting: Establish Theory of Probable Cause
Question the obvious
Consider multiple approaches
Remember the OSI
.
Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.
Layers
from top
:
Application, Presentation, Session, Transport, Network,
Datalink, Physical
.
Top-to-bottom approach
: for example, app to physical
Bottom-to-top approach
: for example, physical to app
Divide and conquer
:
We start at a layer
(e.g., network)
and
based on evidence we get
in problem identification
, we decide whether we
go up the stack or down the stack

Troubleshooting: Test the Theory
Once the theory is confirmed,
determine the next step to resolve the problem.
If the theory is not confirmed,
reestablish a new theory or escalate.

Troubleshooting: Establish a Plan of Action
Always consider corporate policies, procedures and impacts before implementing changes.
When developing your plan of action, it is most important to consider which of the following? Potential Effects

Troubleshooting: Solve, Verify, Document