AWS Well-Architected Framework & Architecting for the Cloud

Agenda

01 Traditional Vs. Cloud Computing Environments

02 General Design Principles

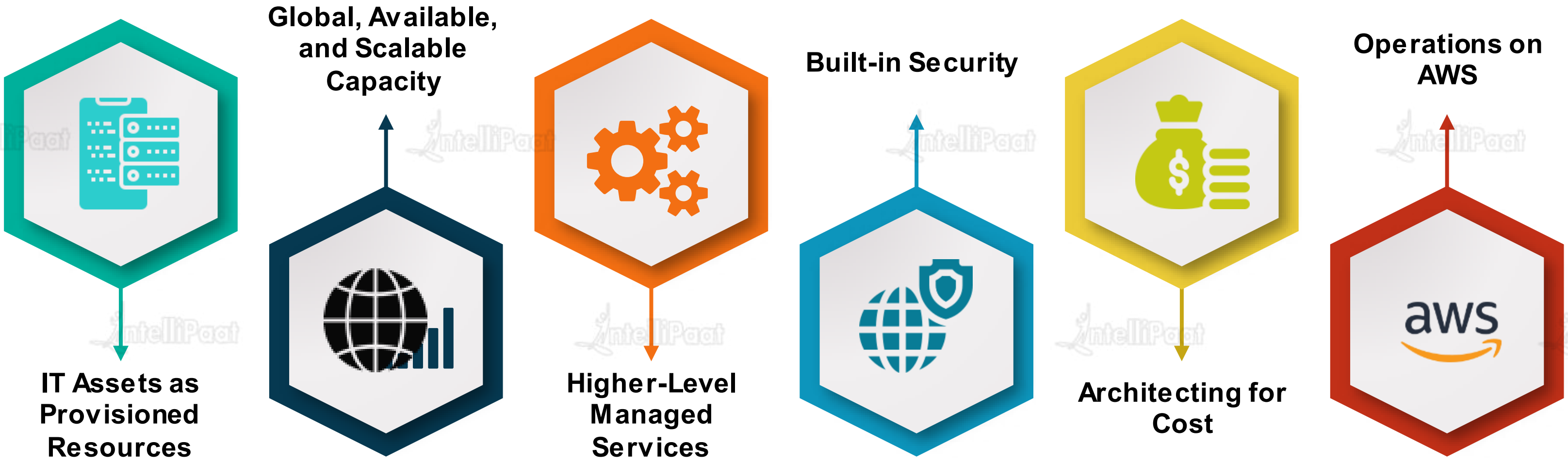
04 Five Pillars of a Well Architected Framework

05 Best Practice Areas & Key AWS Services

Traditional Vs. Cloud Computing Environments

Difference Between Traditional & Cloud

Whether you are re-architecting the applications that currently run in your on-premise environment to run on AWS, or migrating directly to AWS, or designing cloud-native applications, you must consider the differences between traditional environments and cloud computing environments.



Traditional Vs. Cloud Computing

IT Assets as Provisioned Resources

Global, Available, and Scalable Capacity

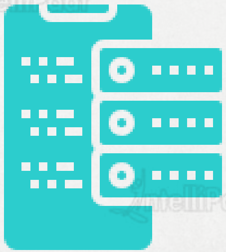
Higher-Level Managed Services

Built-in Security

Architecting for Cost

Operations on AWS

In a traditional computing environment, you provision capacity based on an estimate of a theoretical maximum peak. With cloud computing, you can access as much or as little capacity as you need and dynamically scale to meet actual demand, while only paying for what you use.



Traditional Vs. Cloud Computing

- IT Assets as Provisioned Resources
- **Global, Available, and Scalable Capacity**
- Higher-Level Managed Services
- Built-in Security
- Architecting for Cost
- Operations on AWS

Using the global infrastructure of AWS, you can deploy your application to the AWS Region that best meets your requirements. For global applications, you can reduce latency to end users around the world by using the Amazon CloudFront content delivery network (CDN)

Traditional Vs. Cloud Computing

IT Assets as Provisioned Resources

Global, Available, and Scalable Capacity

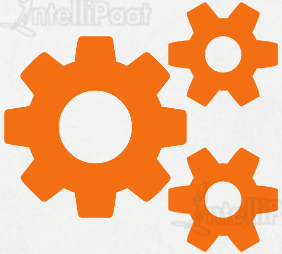
Higher-Level Managed Services

Built-in Security

Architecting for Cost

Operations on AWS

Apart from the compute resources of Amazon Elastic Compute Cloud (Amazon EC2), you also have access to a broad set of storage, database, analytics, application, and deployment services. These services are instantly made available within a few clicks.



Traditional Vs. Cloud Computing

IT Assets as Provisioned Resources

Global, Available, and Scalable Capacity

Higher-Level Managed Services

Built-in Security

Architecting for Cost

Operations on AWS

Cloud provides governance capabilities that enable continuous monitoring of configuration changes to your IT resources. Security at AWS is the highest priority, which means that you benefit from data centers and network architecture that are built to meet the requirements of the most security sensitive organizations.

Traditional Vs. Cloud Computing

- IT Assets as Provisioned Resources
- Global, Available, and Scalable Capacity
- Higher-Level Managed Services
- Built-in Security
- **Architecting for Cost**
- Operations on AWS

Traditional cost management of on-premise solutions is not typically tightly coupled to the provision of services. When you provision a cloud computing environment, optimizing for cost is a fundamental design tenant for architects. AWS provides fine-grained billing, which enables you to track the costs associated with all aspects of your solutions

Traditional Vs. Cloud Computing

- IT Assets as Provisioned Resources
- Global, Available, and Scalable Capacity
- Higher-Level Managed Services
- Built-in Security
- Architecting for Cost
- **Operations on AWS**

AWS provides tooling, processes, and best practices to support the transition of operational practices to maximize the benefits that can be leveraged from cloud computing.

General Design Principles

General Design Principles

01 Scalability

02 Automation

03 Services, Not Servers

04 Loose Coupling

05 Database & Data Volumes

06 Cost Optimization

07 Caching

08 Security

General Design Principles

01 Scalability

02 Automation

03 Services, Not Servers

04 Loose Coupling

Applications that are expected to grow over time need to be built on top of a scalable architecture. Such an architecture supports growth in users, traffic, or data size with no drop-in performance.

General Design Principles

01 **Scalability**

02 **Automation**

03 **Services, Not Servers**

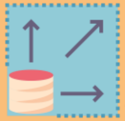
04 **Loose Coupling**

Traditional IT infrastructure requires you to manually react to a variety of events. With cloud computing environment, there is an opportunity for automation such as server less management and Deployment, Auto scaling and more.

General Design Principles

01

Scalability



02

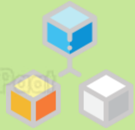
Automation

03

Services, Not Servers

04

Loose Coupling



With traditional IT infrastructure, organizations have to build and operate all the IT components on their own. While, with Cloud Computing, most of these required components are offered as services accessed via the internet.

General Design Principles

01 Scalability

02 Automation

03 Services, Not Servers

04 Loose Coupling

Cloud computing encourages multi architecture systems for applications which let's organizations design and keep the application complexity in check by creating smaller, loosely coupled components. It also reduces the interdepencies.

General Design Principles

05 **Database & Data Volumes**

06 **Cost Optimization**

07 **Caching**

08 **Security**

Cloud computing provides various managed database engines offering enterprise performance at open source cost. Data lake architecture is another plus point with cloud, which organizations can use to store massive amounts of data in a central location so that it's readily available to be categorized, processed, analyzed, and consumed by diverse groups within the organization.

General Design Principles

05

Database &
Data Volumes

06

Cost
Optimization

07

Caching

08

Security

Cloud reduces capital expenses and drive savings as a result. AWS even provides various ways for organization to track and identify the cost saving opportunities.

General Design Principles

05 Database & Data Volumes

06 Cost Optimization

07 Caching

08 Security

Cloud environment offers caching services to store any previously calculated data for future use. This helps in improving application performance.

General Design Principles

05

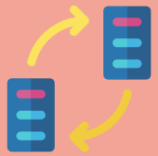
Database & Data Volumes

06

Cost Optimization

07

Caching



08

Security

Most of the security methods and tools available for traditional IT infrastructure can also be used in the cloud. AWS also offers it's own various security solutions for applications on AWS. It also let's you formalize the design of security controls.

The Five Pillars of A Well Architected Framework

Five Pillars of a Well Architected Framework

Incorporating the five pillars into the architecture, helps produce stable and efficient systems that will deliver on your expectations and requirements.

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization

Operational Excellence

How do we build the foundation of Operational Excellence pillar in our framework?

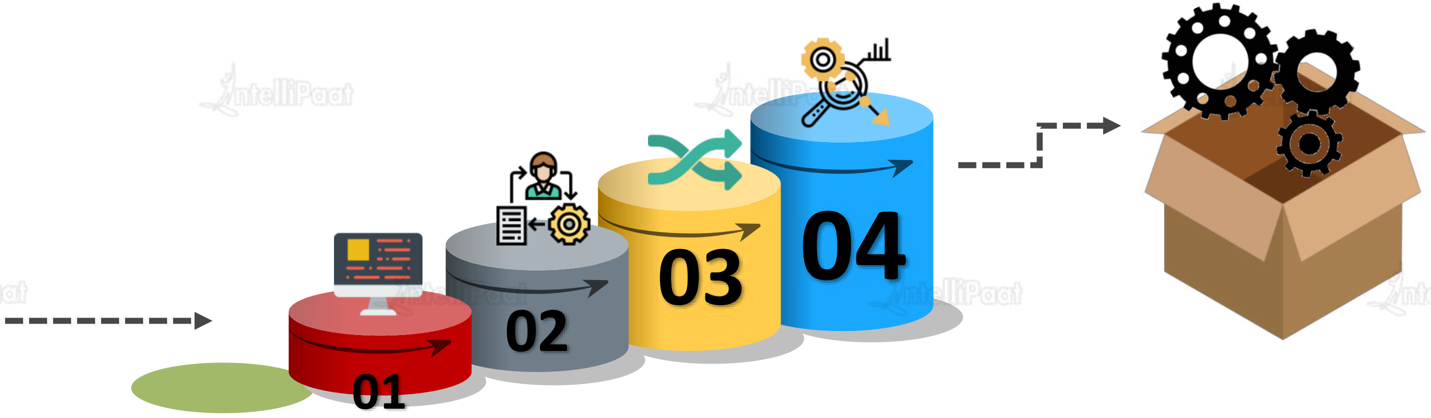
Operational Excellence pillar refers to the ability to run and monitor systems, and to gain insight into the system's operations in order to deliver business value.

Operational Excellence

Design Principles

Make frequent, small, reversible changes

Design workloads to allow components to be updated regularly to increase the flow of beneficial changes into your workload. Make changes in small increments that can be reversed if they fail.



Operational Excellence

Best Practice Areas & key AWS Services

Prepare

01

Create mechanisms to validate that workloads, or changes, are ready to be moved into production and supported by operations. Operational readiness is validated through checklists to ensure a workload meets defined standards.

Key AWS Service: AWS Config

Operate

02

Define expected outcomes, determine how success will be measured, and identify the workload and operations metrics that will be used in those calculations to determine if operations are successful.

Key AWS Service: Amazon CloudWatch

Evolve

03

Dedicate work cycles to making continuous incremental improvements. Regularly evaluate and prioritize opportunities for improvement.

Key AWS Service: Amazon Elasticsearch Services

Security

02

How do we build the foundation of Security pillar in our framework?

The security Pillar refers to the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

Security

Design Principles

Protect data in transit and at rest

Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.

Security

Best Practice Areas & key AWS Services

Identity and Access Management

01

Ensuring that only authorized and authenticated users are able to access your resources, and only in a manner that you intend could protect your data and applications from various security threats.

Key AWS Service: AWS IAM

Detective Controls

02

You can use detective controls to identify a potential security threat or incident. You can also use internal auditing, to ensure that practices meet policies and requirements and that you have set the correct automated alerting notifications based on defined conditions.

Key AWS Service: AWS CloudTrail

Infrastructure Protection

03

Infrastructure protection encompasses control methodologies, such as defense in depth in levels of your framework.

Key AWS Service: Amazon Virtual Private Cloud, Amazon CloudFront

Security

Best Practice Areas & key AWS Services

Data Protection

04

Implement data classification, that provides a way to categorize organizational data based on levels of sensitivity. Implement encryption which protects data by making it unintelligible to unauthorized access.

Key AWS Service:
ELB, Amazon EBS, Amazon S3, Amazon RDS, and AWS KMS

Incident Response

05

Even with extremely mature preventive measures and detective controls, your organization should still put processes in place to respond to security incidents and mitigate the potential impact of security incidents.

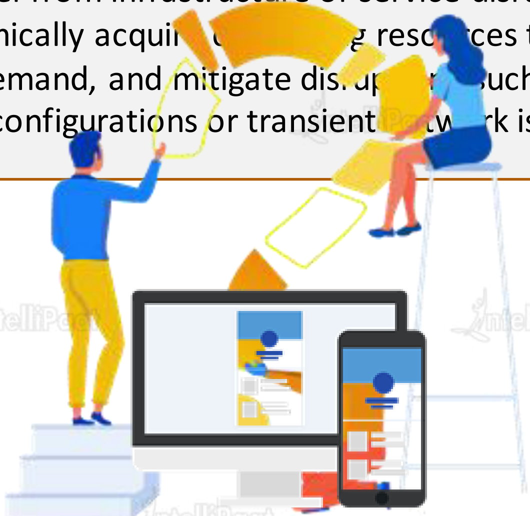
Key AWS Service: AWS CloudFormation

Reliability

03

How do we build the foundation of Reliability pillar in our framework?

Reliability pillar represents the ability of a system to recover from infrastructure or service disruptions, dynamically acquiring computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.



Reliability

Design Principles

Test recovery procedures
Automatically recover from failure
Scale horizontally to increase aggregate system availability
Stop guessing capacity

A common cause of failure in on-premises systems is resource saturation, when the demands placed on a system exceed the capacity of that system

Reliability

Best Practice Areas & key AWS Services

Foundations

01

Before architecting any system, foundational requirements that influence reliability should be in place. For example, you must have sufficient network bandwidth to your data center.

Key AWS Service: AWS IAM

Change Management

02

Being aware of how change affects a system allows you to plan proactively, and monitoring allows you to quickly identify trends that could lead to capacity issues or SLA breaches.

Key AWS Service: AWS CloudTrail

Failure Management

03

In any system of reasonable complexity it is expected that failures will occur. It is generally of interest to know how to become aware of these failures, respond to them, and prevent them from happening again.

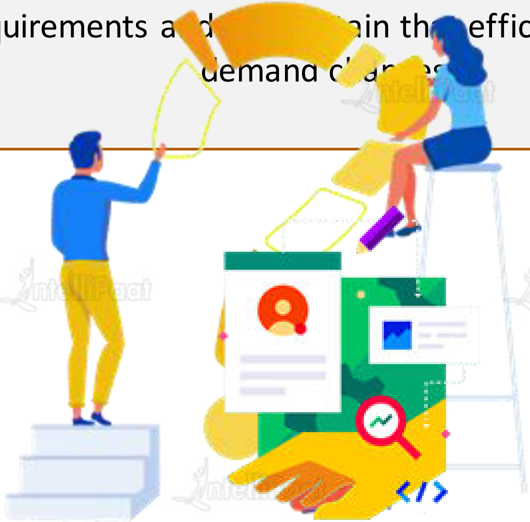
Key AWS Service: AWS CloudFormation

Performance Efficiency

04

How do we build the foundation of Performance Efficiency pillar in our framework?

Performance efficiency pillar represents the ability to use computing resources efficiently to meet system requirements and maintain the efficiency as the demand changes

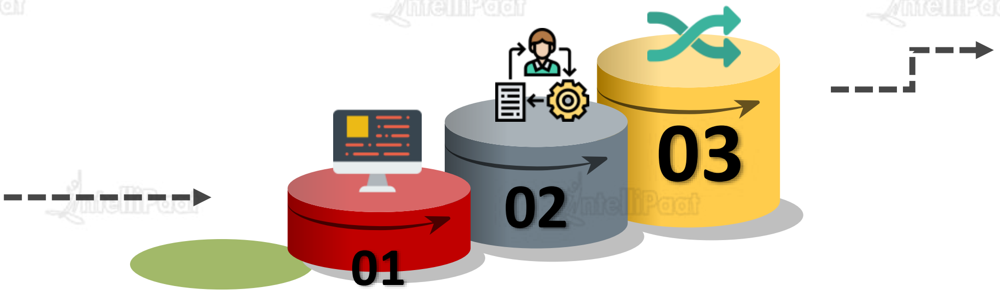


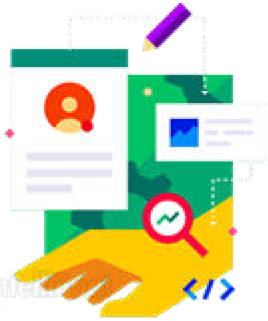
Performance Efficiency

Design Principles

Use serverless architectures
Democratize advanced technologies
Go global in minutes

Serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. This not only removes the operational burden of managing these servers, but also can lower transactional costs.





Performance Efficiency

Best Practice Areas & key AWS Services

Selection

01

The optimal solution for a particular system will vary based on the kind of workload you have, often with multiple approaches combined. Well-architected systems use multiple solutions and enable different features to improve performance.

Key AWS Service: Services in compute, storage and more

Review

02

When architecting solutions, there is a finite set of options that you can choose from. However, over time new technologies and approaches become available that could improve the performance of your architecture.

The AWS Blog and the What's New section on the AWS website

Monitoring

03

After you have implemented your architecture you will need to monitor its performance so that you can remediate any issues before your customers are aware. Monitoring metrics should be used to raise alarms when thresholds are breached.

Key AWS Service: Amazon CloudWatch

Cost Optimization

How do we build the foundation of Cost Optimization pillar in our framework?

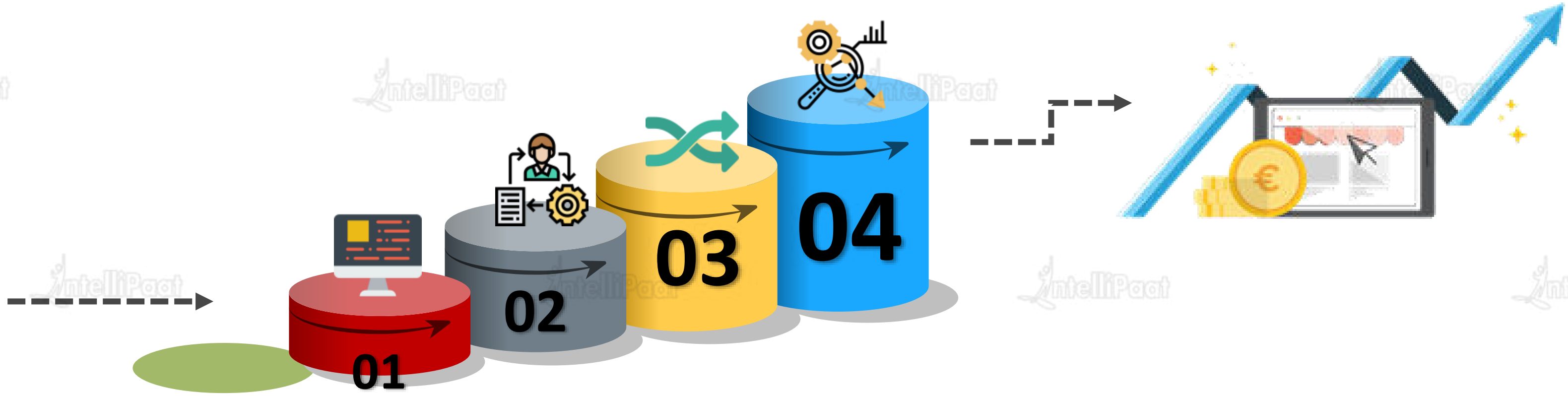
Cost optimization pillar refers to the ability to run systems to deliver business value at the lowest price

Cost Optimization

Design Principles

Adopt a consumption model
Measure overall efficiency
Stop spending money on data center operations
Analyze and attribute expenditure

The cloud makes it easier to accurately identify the usage and cost of systems, which then allows transparent attribution of IT costs to individual workload owners



Cost Optimization

Best Practice Areas & key AWS Services

Expenditure Awareness

01

The capability to attribute resource costs to the individual organization or product owners drives efficient usage behavior and helps reduce waste

Key AWS Service: AWS Cost Explorer

Cost-Effective Resources

02

Using the appropriate instances and resources for your workload is key to cost savings. A well-architected workload uses the most cost-effective resources, which can have a significant and positive economic impact.

AWS Key Services: AWS Direct Connect, Amazon CloudFront, Amazon RDS and more

Matching supply and demand

03

Optimally matching supply to demand delivers the lowest cost for a workload, but there also needs to be sufficient extra supply to allow for provisioning time and individual resource failures

Key AWS Service: AWS Auto Scaling

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

support@intellipaat.com

24/7 Chat with Our Course Advisor