CS 4037
Introduction to Cloud Computing
Lecture 29

Danyal Farhat

FAST School of Computing

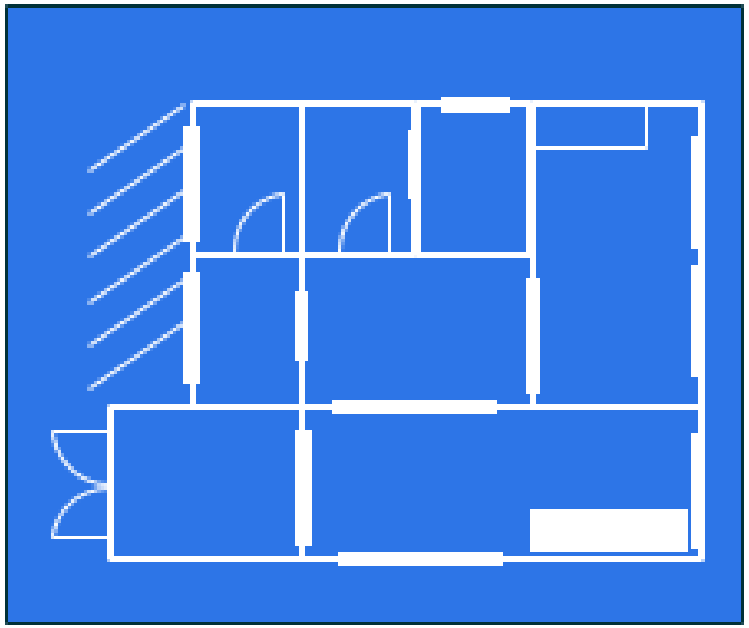
NUCES Lahore

AWS Cloud Architecture

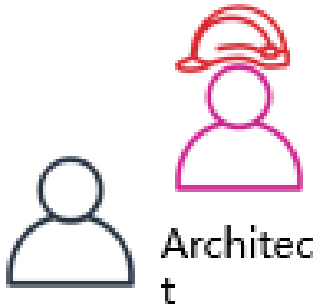
Lecture’s Agenda

- **AWS Well Architected Framework**
- AWS Trusted Advisor

Architecture: Designing and Building

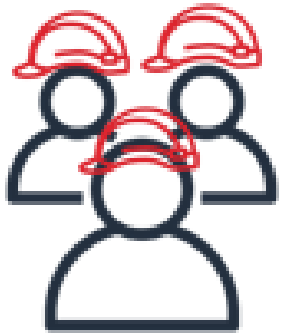


Structure design

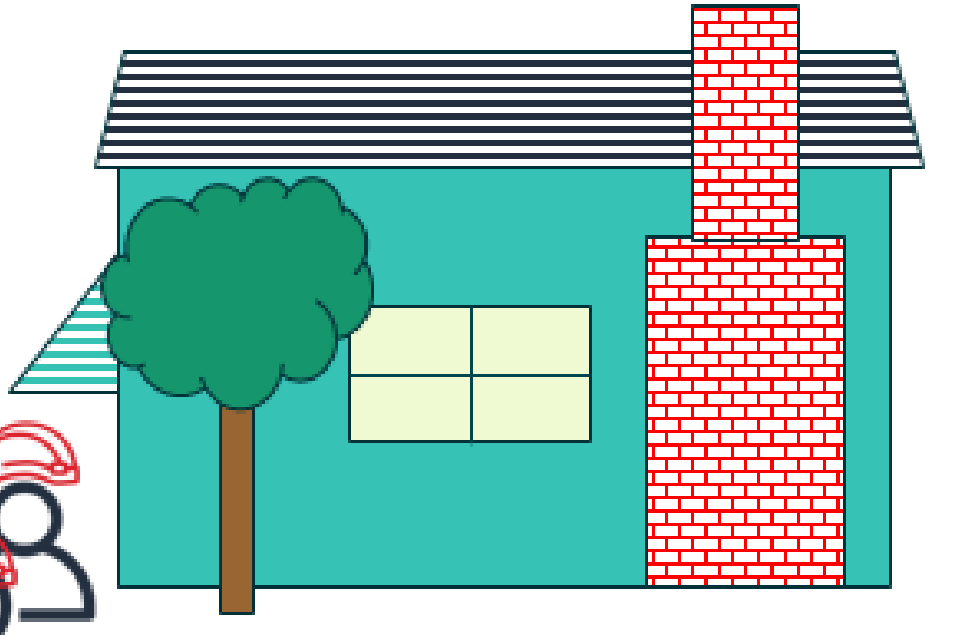


Customer
(Decision maker)

Architec
t



Building crew
(Delivery team)



Completed structure

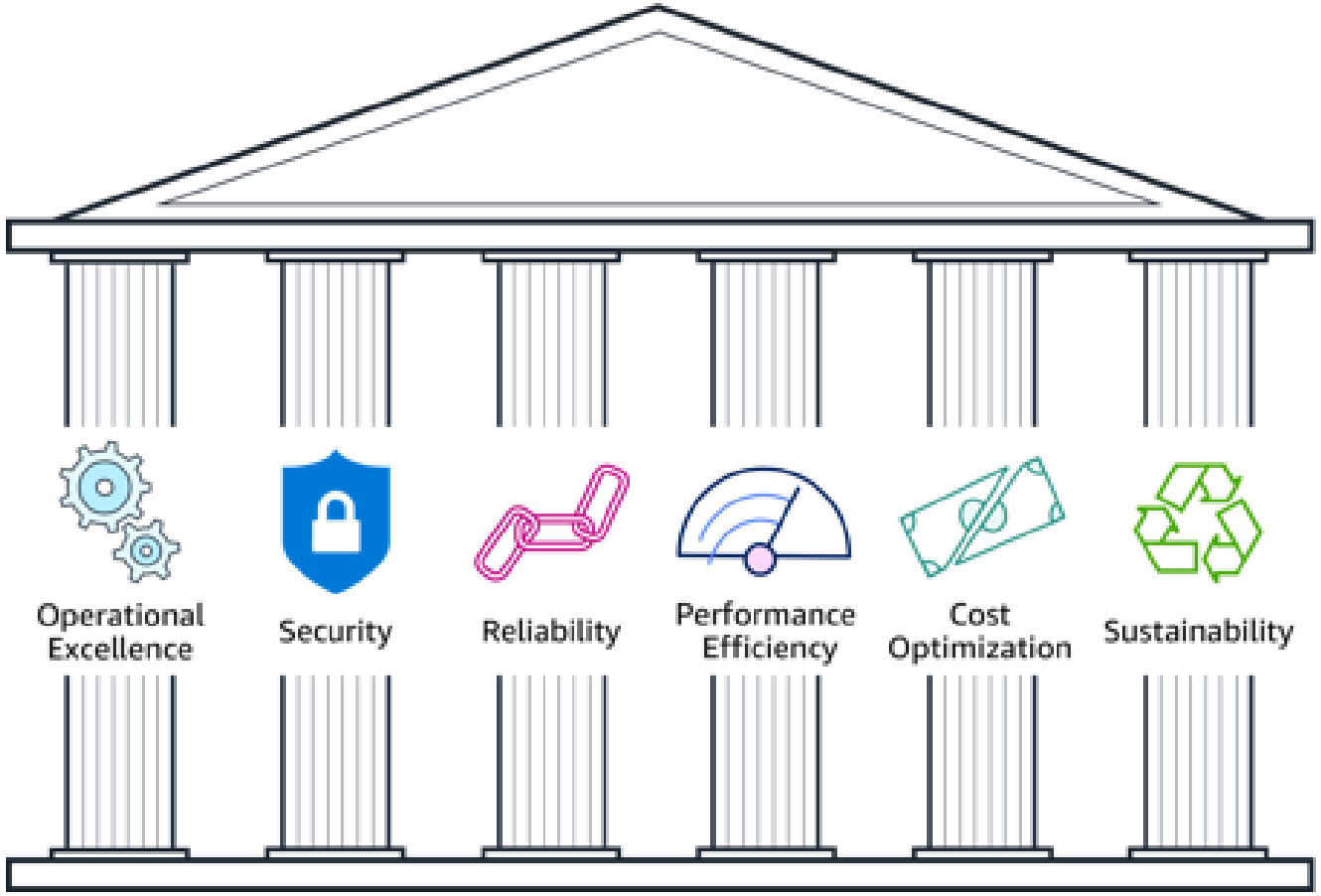
Architecture: Designing and Building (Cont.)

- **Art and science of designing and building large structures**
  - **Large systems require architects to manage their size and complexity**
- **Cloud architects:**
  - **Engage with decision makers to identify the business goal and the capabilities that need improvement**
  - **Ensure alignment between technology deliverables of a solution and the business goals**
  - **Work with delivery teams that are implementing the solution to ensure that the technology features are appropriate**
- **Having well-architected systems greatly increases the likelihood of business success**

What is the AWS Well-Architected Framework?

- **A guide for designing infrastructures that are:**
  - **Secure, High-performing, Resilient, and Efficient**
- **"A consistent approach to evaluating and implementing cloud architectures."**
- **"A way to provide best practices that were developed through lessons learned by reviewing customer architectures."**
- **Organized into six pillars**
  - **Each pillar includes its own set of design principles and best practices**

Pillars of the AWS Well-Architected Framework



Pillars Organization

Best practice area Identity and Access Management

Question text SEC 1: How do you manage credentials and authentication?

Question context Credential and authentication mechanisms include passwords, tokens, and keys that grant access directly or indirectly in your workload. Protect credentials with appropriate mechanisms to help reduce the risk of accidental or malicious use.

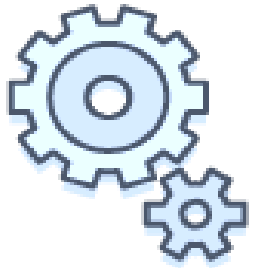
Best practices Best practices:

- Define requirements for identity and access management
- Secure AWS account root user
- Enforce use of multi-factor authentication
- Automate enforcement of access controls
- Integrate with centralized federation provider
- Enforce password requirements
- Rotate credentials regularly
- Audit credentials periodically

Operational Excellence Design Principles

- **Perform operations as code**
  - **With defined SOPs**
- **Make frequent, small, reversible changes**
- **Refine operations procedures frequently**
- **Anticipate failure**
- **Learn from all operational events and failures**

Operational Excellence pillar



Deliver business value

Operational Excellence Questions

Organization

- How do you determine what your priorities are?
- How do you structure your organization to support your business outcomes?
- How does your organizational culture support your business outcomes?

Prepare

- How do you design your workload so that you can understand its state?
- How do you reduce defects, ease remediation, and improve flow into production?
- How do you mitigate deployment risks?
- How do you know that you are ready to support a workload?

Operate

- How do you understand the health of your workload?
- How do you understand the health of your operations?
- How do you manage workload and operations events?

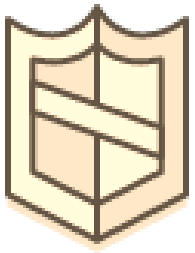
Evolve

- How do you evolve operations?

Security Design Principles

- Implement a strong identity foundation
  - IAM, AD Policies
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

Security pillar



Protect and monitor systems

Security Questions

Security

- How do you securely operate your workload?

Identity and Access Management

- How do you manage identities for people and machines?
- How do you manage permissions for people and machines?

Detection

- How do you detect and investigate security events?

Infrastructure Protection

- How do you protect your network resources?
- How do you protect your compute resources?

Data Protection

- How do you classify your data?
- How do you protect your data at rest?
- How do you protect your data in transit?

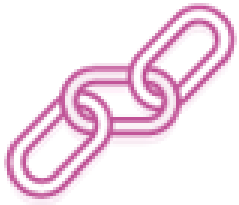
Incident Response

- How do you anticipate, respond to, and recover from incidents?

Reliability Design Principles

- **Automatically recover from failure**
- **Test recovery procedures**
- **Scale horizontally to increase aggregate workload availability**
  - **Using multiple small systems rather single large system**
- **Manage change in automation**

Reliability pillar



Recover from failure and mitigate disruption.

Reliability Questions

Foundations

- How do you manage service quotas and constraints?
- How do you plan your network topology?

Workload Architecture

- How do you design your workload service architecture?
- How do you design interactions in a distributed system to prevent failure?
- How do you design interactions in a distributed system to mitigate or withstand failures?

Change Management

- How do you monitor workload resources?
- How do you design your workload to adapt to changes in demand?
- How do you implement change?

Failure Management

- How do you back up data?
- How do you use fault isolation to protect your workload?
- How do you design your workload to withstand component failures?
- How do you test reliability?
- How do you plan for disaster recovery?

Performance Efficiency Design Principles

- **Democratize advanced technologies**
  - **Specialized depts. for ML, DBMS**
- **Use serverless architectures**
- **Consider mechanical sympathy**
  - **Use the technology approach that aligns best to what users are trying to achieve**
  - **Example: consider data access patterns when selecting approaches for databases or storage**

Performance Efficiency Questions

Selection

- How do you select the best performing architecture?
- How do you select your compute solution?
- How do you select your storage solution?
- How do you select your database solution?
- How do you configure your networking solution?

Review

- How do you evolve your workload to take advantage of new releases?

Monitoring

- How do you monitor your resources to ensure they are performing?

Tradeoffs

- How do you use tradeoffs to improve performance?

Cost Optimization Design Principles

- **Adopt a consumption model**
- **Analyze and attribute expenditure**
- **Implement Cloud Financial Management**
- **Stop spending money on undifferentiated heavy lifting**

Cost Optimization pillar

Eliminate unneeded expense.

Cost Optimization Questions

Practice Cloud Financial Management

- How do you implement cloud financial management?

Expenditure and Usage Awareness

- How do you govern usage?
- How do you monitor usage and cost?
- How do you decommission resources?

Cost-Effective Resources

- How do you evaluate cost when you select services?
- How do you meet cost targets when you select resource type, size, and number?
- How do you use pricing models to reduce cost?
- How do you plan for data transfer changes?

Manage Demand and Supply Resources

- How do you manage demand and supply resources?
- Optimize over time
- How do you evaluate new services?

Lecture’s Agenda

- AWS Well Architected Framework
- **AWS Trusted Advisor**

AWS Trusted Advisor

- **"Online tool that provides real-time guidance to customers to provision resources following AWS best practices."**
- **"Looks at customer's entire AWS environment and gives real-time recommendations in five categories."**

Interpret AWS Trusted Advisor Recommendations

Recommendation # 1 - MFA on Root Account:

- **Description:** Checks the root account and warns if multi-factor authentication (MFA) is not enabled. For increased security, we recommend that user protect the account by using MFA, which requires a user to enter a unique authentication code from their MFA hardware or virtual device when interacting with the AWS console and associated websites.
- **Alert Criteria:** MFA is not enabled on the root account.
- **Recommended Action:** Log in to the root account and activate an MFA device.

Interpret AWS Trusted Advisor Recommendations

Recommendation # 2 - IAM Password Policy:

- **Description:** Checks the password policy for account and warns when a password policy is not enabled, or if password content requirements have not been enabled. Password content requirements increase the overall security of AWS environment by enforcing the creation of strong user passwords. When user create or change a password policy, the change is enforced immediately for new users but does not require existing users to change their passwords.
- **Alert Criteria:** A password policy is enabled, but at least one content requirement is not enabled.
- **Recommended Action:** If some content requirements are not enabled, consider enabling them. If no password policy is enabled, create and configure one. See Setting an Account Password Policy for IAM Users.

Interpret AWS Trusted Advisor Recommendations

Recommendation # 3 - Security Groups – Unrestricted Access:

- **Description:** Checks security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).
- **Alert Criteria:** A security group rule has a source IP address with a /0 suffix for ports other than 25, 80, or 443.)
- **Recommended Action:** Restrict access to only those IP addresses that require it. To restrict access to a specific IP address, set the suffix to /32 (for example, 192.0.2.10/32). Be sure to delete overly permissive rules after creating rules that are more restrictive.

Interpret AWS Trusted Advisor Recommendations

Recommendation # 4 - Amazon EBS Snapshots:

- **Description:** Checks the age of the snapshots for Amazon EBS volumes (available or in-use). Even though Amazon EBS volumes are replicated, failures can occur. Snapshots are persisted to Amazon S3 for durable storage and point-in-time recovery.
- **Alert Criteria:**
  - Yellow: The most recent volume snapshot is between 7 and 30 days old.
  - Red: The most recent volume snapshot is more than 30 days old.
  - Red: The volume does not have a snapshot
- **Recommended Action:** Create weekly or monthly snapshots of the volumes.

Interpret AWS Trusted Advisor Recommendations

Recommendation # 5 - Amazon S3 Bucket Logging:

- **Description:** **Checks the logging configuration of Amazon S3 buckets. When server access logging is enabled, detailed access logs are delivered hourly to a bucket that user choose. An access log record contains details about each request, such as the request type, the resources specified in the request, and the time and date the request was processed. By default, bucket logging is not enabled; customer should enable logging if user wants to perform security audits or learn more about users and usage patterns.**
- **Alert Criteria:**
  - **Yellow: The bucket does not have server access logging enabled.**
  - **Yellow: The target bucket permissions do not include the owner account. Trusted Advisor cannot check it.**
- **Recommended Action: Enable bucket logging for most buckets.**
  - **If the target bucket permissions do not include the owner account and you want Trusted Advisor to check the logging status, add the owner account as a grantee.**

Additional Resources

- **AWS Well-Architected Website**
  - **https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc**
- **AWS Well-Architected Labs**
  - **https://wellarchitectedlabs.com/**
- **AWS Trusted Advisor Best Practice Checks**
  - **https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor-check-reference.html**

Questions?