

## NCTA CERTIFIED CLOUD ARCHITECT (NCA-110)

### Who Should Attend

This course is designed for System Administrators who wish to plan, design, and implement cloud services for their organizations. This includes the ability to understand cloud solution features, capabilities, and components offered by cloud providers at a deep level so as to design cloud and hybrid solutions for application deployment and infrastructure scenarios. Cloud architects must also evaluate and plan for the appropriate compute, network, database and security components to build a solution that meets the needs of their organization. In addition, they must secure, monitor, and optimize those solutions.

### Course Objectives

Upon successful completion of this course, students will be able to:

- Prepare for and pass the Certified Cloud Architect exam (NCA-110).
- Prepare the organization for cloud migration.
- Present solutions for organizational approval.
- Determine organizational requirements.
- Evaluate cloud service features and components.
- Select AWS infrastructure components.
- Select Rackspace cloud features and components.
- Select Microsoft Azure features and components.
- Determine licensing and SLA requirements.
- Evaluate SLAs.
- Evaluate cloud service scaling options.
- Manage, compute, memory and storage resources.
- Manage network connections.
- Implement cloud service continuity and disaster recovery plans.
- Secure data in the cloud.
- Provide secure access to cloud services.
- Present your cloud migration plan.

### Course Outline

#### DOMAIN 1 – CLOUD IMPLEMENTATION PREPARATION

##### 1.1 Prepare the Organization for Cloud Migration

- Cloud Risks

- Organizational Goals vs. Cloud Strategy
- Vendor Considerations
- Legacy IT Issues
- Integration Challenges
- Organizational Culture
- Communication
- Migration Failures
- Cloud Teams
  - Roles and Responsibilities
  - Executed Sponsorship
- Documentation
  - Migration Goals/Benefits
  - Project Structure
  - KPI's
  - Business Reports
    - Financial
    - CRUSH

## 1.2 Present Solutions for Organizational Approval

- Present/Pitch to Organization
- TCO
  - Acquisition
  - O&M
  - Training
- ROI
- Case Studies
- Calls to Action

## **DOMAIN 2 – ORGANIZATIONAL REQUIREMENTS AND CLOUD SERVICE OPTIONS**

### 2.1 Determine Your Organizational Requirements

- Operating System Requirements
  - OS Cost Considerations
  - Patching Considerations
  - Maintenance and Support
  - Features and Capabilities
- Application Requirements

- APIs
- Legacy Application Considerations
- Data Migration Considerations
- Middleware
- Access and Performance Expectations
- Database Requirements
  - SQL Databases
    - Oracle MySQL
    - Oracle Database
    - Microsoft SQL Server
    - PostgreSQL
  - NoSQL Databases
    - Column Store
    - Document Database
    - Key-Value Store
    - Graph Databases

## 2.2 Evaluate Cloud Service Features and Components

- Facilities
  - Data Centers
    - Uptime Institute Tiers (I-IV)
    - Modular Data Centers
    - Power, Ping, and Pipe
    - Telecommunications
    - Electrical Redundancy
    - Geographic Location
- Cloud Compute Components
  - Blade vs. Rack-Mounted Servers
  - CPUs
    - Brand/Types
    - Cores
    - Frequency
  - Memory
  - Storage
  - Network Access
    - NICs
    - Converged Networking
    - Layers
    - Protocols and Ports
- Cloud Storage and Delivery Components
  - Disk Types

- SATA
- SCSI/SAS
- SSDs
- IOPS
- SANs/Block Storage
- NAS
- HTTP/Object Storage
- Virtualization Software
  - Host Servers
  - VMs
  - Container-Based vs. Hypervisor-Based Virtualization
  - Image Libraries and Templates
- Cloud Management Platform Components
  - Portals and Management APIs
  - Workflow Management
  - Identity Management
  - CDNs

## DOMAIN 3 – FEATURES AND COMPONENT SELECTION

### 3.1 Select AWS Infrastructure Components

- Global Data Center Infrastructure
  - Regions
  - Available Zones
- AWS Management and Administration
  - Command Line Interface
  - Web Console
  - AWS API
  - AWS SDK
    - Android
    - iOS
    - Browser
    - Java
    - .NET
    - Python
  - AWS Building Blocks
- AWS Compute Components
  - Amazon EC2
    - Load Balancing
  - Amazon VPC
    - Public/Private Subnets

- VPN
- Purchase Options
  - On-Demand
  - Reserved
  - Spot
  - Dedicated Hosts
- AWS Networking Components
  - Elastic Load Balancing
  - Amazon WorkSpaces
  - Amazon Route 53
  - AWS Direct Connect
- AWS Storage and Content Delivery Components
  - Amazon S3
    - Amazon S3 Standard
    - Amazon Glacier
  - Amazon EBS
    - Disk Types
  - AWS Import/Export Services
    - AWS Import/Export Snowball
    - AWS Import/Export Disk
    - AWS SDK for Java
  - Amazon CloudFront
- AWS Management and Monitoring
  - Amazon SWF
  - Amazon CloudWatch
  - Amazon EMR
  - Amazon Kinesis
  - Amazon Data Pipeline
  - Third-Party Solutions
    - BI Tools
    - Hunk
    - HParser
    - MapR for Hadoop
- AWS PaaS Features
  - AWS Elastic Beanstalk
  - Amazon SNS
  - Amazon SQS
  - Amazon SES
  - Amazon CloudSearch
- AWS Database Services
  - Amazon RDS
  - Amazon SimpleDB

- Amazon DynamoDB
- Amazon Redshift
- Amazon ElastiCache

### 3.2 Select Rackspace Cloud Features and Components

- Rackspace Cloud Compute and Network Components
  - Rackspace Cloud Networks
  - Rackspace Cloud Servers
  - Service Levels
    - Managed Infrastructure
    - Managed Operations
  - Rackspace Cloud Load Balancers
  - Rackspace Cloud DNS
    - The Cloud Control Panel and API
  - Rackspace OnMetal
  - Rackspace Auto Scale
  - RackConnect
  - Cloud Orchestration
- Rackspace Cloud Database Services
  - Rackspace SQL Databases
    - Rackspace MySQL
    - Percona Server
    - MariaDB
  - Rackspace NoSQL Databases
    - ObjectRocket for MongoDB
    - ObjectRocket for Redis
    - ObjectRocket for Elasticsearch
    - Cassandra
  - Cloud Big Data
  - Cloud Queue
- Rackspace Cloud Storage Components
  - Rackspace Cloud Block Storage
  - Cloud Files
  - Cloud Backup
  - Rackspace Cloud CDN
- Rackspace Service Monitoring
  - Rackspace Cloud Monitoring
    - Zone Checks
  - Rackspace Monitoring Agent
    - Load Average
    - Filesystem
    - Memory
    - CPU
    - Network
  - Alarms and Notifications

- Rackspace Third-Party Solutions
  - Airbrake
  - Alert Logic

### 3.3 Select Microsoft Azure Features and Components

- Azure Compute and Network Components
  - Azure VMs
    - Linux
    - Windows
  - Azure Cloud Services
  - Azure App Service
    - The Mobile Apps Feature
    - The Web Apps Feature
    - ExpressRoute
    - Azure Virtual Networks (VNETs)
    - Azure Traffic Manager
- Azure Database Services
  - Azure SQL Database
    - Single Database Model
    - Elastic Database Model
  - Azure NoSQL Database
    - DocumentDB
    - Table Storage
    - Redis Cache
    - HBase
  - Stretch Database
- Azure Storage Services
  - Azure Storage
    - Blob Storage
    - File Storage
    - Table Storage
    - Queue Storage
    - Premium Storage
  - Hot vs. Cool Storage
  - Replication Options
    - LRS
    - GRS
    - RA-GRS
  - Azure Site Recovery
- Azure App Services
  - Azure Media Services
  - Azure Service Bus
    - Queues
    - Topics
    - Relays
    - Event Hubs

- Azure Notification Hubs
- Azure Scheduler
- BizTalk Services
- Azure Active Directory
- Azure Monitoring Services
  - Azure Cloud Service Monitoring
  - Azure Diagnostics
    - VM
    - Cloud Service
  - Diagnostics Connection String
  - Azure Third-Party Solutions
    - Stackify
    - Cloudmonix
    - New Relic
    - Datadog

## DOMAIN 4 – CLOUD SERVICE LICENSING

### 4.1 Determining Your Organization’s Cloud Service Licensing Requirements

- Licensing Agreement Types
  - Enterprise License Agreements
  - Blanket License Agreements
  - End User License Agreements
  - Per Module (Component) Licensing
  - Service Provider License Agreements

### 4.2 Evaluate SLAs

- SLA Considerations
  - DLM
    - Contracts
    - Financial Records
    - Compliance (HIPAA, SOX, ect.)
  - High Availability
  - Backup and Disaster Recovery
  - Data Protection
    - PCI DSS
    - Security in Transit
    - Security at Rest
  - Intellectual Property and Copyright
- SLA Types



- Standard
- Premium
- Negotiated

## DOMAIN 5 – CLOUD SCALABILITY

### 5.1 Evaluate Cloud Service Scaling Options

- Scale Up vs. Scale Out
- Peak vs. Average Use
- Logical vs. Physical Upgrades
- Scaling Considerations
  - Load Balancing
  - Bolt-On Solutions
  - Testing
  - Policy-Based Scaling

### 5.2 Manage, Compute, Memory, and Storage Resources

- Compute Management
  - CPU Usage
    - Processing Power
- CPU-Bound Applications
- Concurrent Processing
- CPU Scalability
  - Vertical Growth
  - Horizontal Growth
- Memory Management
  - Transaction Processing
  - Memory-Bound Applications
  - Memory and Performance
  - Caching
  - Memory Scaling
- Storage Management
  - Disk and Spindles
  - Read/Write Characteristics
  - Storage-Related Application Performance Issues

### 5.3 Manage Network Components

- Network Performance Issues
  - Bandwidth (Volume)
  - Flow Rate vs. Storage Volume
  - Public and Private Networks

- LAN/WAN Considerations

## DOMAIN 6 – CLOUD SERVICE CONTINUITY, SECURITY, AND RECOVERY

### 6.1 Implement Cloud Service Continuity and Disaster Recovery Plans

- DLM Phases
  - Capture/Collection/Creation
  - Preservation
  - Integration
  - Analysis
  - Archiving
  - Purging
- Information Lifecycle Management
- Profile-Based Data Retention Policies
- Data Backup Options
  - Onsite
  - Offsite
  - Archive
  - Vault
- Data Replication
- High Availability
- System Snapshots
- Cloning
- Business Continuity
  - IT vs. Other Resources (People, Non-IT Facilities)
  - Chain of Command
    - Escalation Paths
  - IT Process Automation
  - Remote Network Connectivity
  - Failover and Testing
- Disaster Recovery
  - DRP
    - DRP Testing
  - BIAs
  - RTO
  - RPO
  - Geographical Separated Datacenters

### 6.2 Secure Data in the Cloud

- Encryption

- Encryption Strength
  - Cypher/Key
- Encryption Types
  - DH
  - RSA
  - DSA
- Encryption Methods
  - Symmetric
  - Asymmetric
- Key Pairs
- In-Transit Data Security
  - Secure Connections
    - IPsec VPN
    - TLS
  - File Level Encryption
- At-Rest Data Security
  - Disk Level Encryption
  - VM Encryption
  - Database Encryption
  - Application Encryption
  - Data Portability
  - At-Rest File Level Encryption

### 6.3 Provide Secure Access to Cloud Services

- Perimeter Security
  - Firewalls
  - DDoS Detection and Mitigation
  - Tracking
  - Vulnerability Scanning
- User Authentication
  - Authentication Requirements
  - Multifactor Authentication
    - Knowledge
    - Possession
    - Inherence
  - SSO
    - Social Login
  - AWS Identity and Access Management
- Security Incidents
  - FedRAMP
  - Security Threats
    - Unauthorized Access to Data

- Interruption of Services
- Access Interruption
- Hardware Damage
- Unauthorized Facility Access
- Attack Types
  - Physical Security
  - Network-Based
  - Software-Based
  - Web App-Based
  - Social Engineering
- Incident Response
  - Escalation/Notification
  - Documentation
  - Forensic Investigation
  - Chain of Custody
  - Correlated Event Management Portals