Professional Cloud Administrator Certification

Syllabus

Lead Authors: Dr Shiyghan Navti, Vladimir Baranek

PROFESSIONAL CLOUD ADMINISTRATOR

CLOUD CREDENTIAL COUNCIL

Table of Contents

What is the CCC Professional Cloud Administrator certification?

The CCC Professional Cloud Administrator certification provides network, systems and database administrators with insights to cloud administration to effectively manage cloud solutions. The interaction between a cloud environment and the existing network/administrative policies is one of the most challenging management issues to resolve. This certification guides administrators through the shift, covering all aspects of cloud administration.

The certification lays out the core components of the cloud administrator function and the necessary skills. Candidates will be able to apply the underpinning administration concepts in an enterprise cloud computing environment, while taking into account the impact of the shift of some aspects of a cloud administration role to external cloud providers.

The course also explores the broadening of cloud administration remit including IT environments that are elastic and involve self-service administration through third parties with varying degrees of access control. Overall, the certification establishes best practices in cloud administration.

PROFESSIONAL CLOUD ADMINISTRATOR

CLOUD CREDENTIAL COUNCIL

Who is this certification for?

- Network, Systems or Database Administrators
- IT Managers

Syllabus - Professional Cloud Administrator

Module 1. Cloud Resource Administration and Provisioning

1.1 Fundamentals of Cloud Administration
- Cloud Definition, Influences and Roles
- Cloud Computing Operational Characteristics
- Cloud Deployment Models
- Cloud Service Models

1.2 Cloud Workload Analysis and Capacity Planning
- Goals and Benefits of Workload Analysis
- Align Workload to Cloud Deployment Model
- Cloud Workload Patterns
- Risks and Challenges of Capacity Planning
- Workload Capacity Planning in the Cloud

1.3 Administering Cloud Technologies
- Remote Administration
- Network Administration
- Computing Hardware
- Network Hardware
- Storage Hardware

1.4 Cloud Resource Provisioning
- Provisioning Environments and Platform Services in Cloud
- Provisioning Control of Virtual Capacity
- Virtual Computing Resources Management and Issues
- Deployment Policies and Automation
- Storage and Compute Multi-Tenancy

1.5 Virtual Storage
- Management Control
- Provisioning Design
- Service Management

1.6 Cloud Marketplaces
- Marketplace Administration

Module 2. Scalable and Elastic Administration

2.1 Cloud Scalability Administration
- High-Availability Clustering
- Load Balancing
- Service Relocation
- Cloud Balancing
- Resource Reservation
- Storage Workload Management
- Direct IO Access

2.2 Cloud Elasticity Administration
- Workload Distribution
- Resource Pooling
- Dynamic Scalability
- Cloud Bursting
- Elastic Disk Provisioning
- Elastic Network Configuration
- Cross Storage Device Vertical Tiering
- Intra Storage Device Vertical Tiering

Module 3. Cloud Interoperability & Portability

3.1 The Need for Interoperability and Portability
- Interoperability and Portability Overview
- Common Motivations for Interoperability and Portability
- Portability and Interoperability Categories
- Data Portability
- Application Portability
- Platform Portability
- Application Interoperability
- Platform Interoperability
- Management Interoperability
- Publication Interoperability
- Interoperability and Portability Benefits
- Interoperability and Portability Risks and Challenges

3.2 Strategic Planning for Interoperability and Portability
- Cloud Deployment Models That Drive the Strategy
- Cloud Service Models That drive the Strategy
- Common Activities in Planning Interoperability and Portability in IaaS
- Common Activities in Planning Interoperability and Portability in PaaS
- Common Activities in Planning Interoperability and Portability in SaaS
- Solving the Security Problems

Module 4. Strategic Policy Design for Cloud Usage and Compliance

4.1 Policy Management and Control
- Audit and Compliance Overview and Objectives
- Identity Compliance and Audit Recommendations
- Audit Monitor
- Audit Management System

4.2 Service Level Management
- Overview and Objectives
- Monitors and Agents
- Reporting and Analysis
- Management System
- Service Performance Metrics

4.3 Metering and Billing Management
- Overview and Objectives
- Monitors and Agents
- Reporting and Analysis
- Cost Management System

4.4 Privacy and Data Management
- Overview and Objectives
- Licensing and Privacy
- Monitors and Agents
- Reporting and Analysis
- Management System

Module 5. Business Continuity Strategies and Disaster Recovery for Cloud

5.1 Business Continuity
- Guidelines
- Business Continuity Overview
- Business Continuity in Cloud
- Service Level Agreement Metrics
- Testing Programs

5.2 Disaster Recovery
- Disaster Recovery Overview
- Administrator Recommendations
- Disaster Recovery in Cloud

- Disaster Recovery Fit for Purpose
- Workload Considerations
- Tools
- Testing Programs
- Failover
- Backup Sites
- Data Backup and Data Restoration
- Backup Implementation
- Benefit of Cloud Computing for Disaster Recovery
- Backup in the Cloud
- Hot Backup Site
- Warm Backup Site
- Cloud Backup Site
- Backup Plan
- Backup Automation
- Full System Backup and Differential Backup
- Incremental Backup
- Difference Between Backup Types
- Creating Backup
- Backup Storage

Module 6. Cloud Security Fundamentals

6.1 Fundamental Security Threats

- Basic Terms and Concepts
- Threat Agents
- Cloud Security Threats
- Security Threat Agents

6.2 Cloud Security Administration

- Security Concepts
- Cloud Security Risks
- Encryption and Digital Signatures
- Cryptography in Cloud Deployments
- Encryption in Cloud Databases
- Key Management
- Key Management Best Practices
- Identity and Access Management
- Identity, Entitlement, and Access Management Implementation
- Level of Trust with Identity and Attributes
- Policy Management
- Architecture for Interfacing to Access Policy Providers
- Trust Zones
- Infrastructure Hardening

- Intrusion Detection/Prevention
- Infrastructure Security

6.3 Security Standards
- Key IT Security Standards
- Web Security
- SOAP Web Services Security
- REST Web Services Security

Module 7. Federated Controls and Strategies for Multiple Cloud and Non-cloud Administration

7.1 Federated Identity Management
- Cloud Best Practices
- Authentication and Authorization
- Enterprise Application Recommendations
- Policy Decision Points
- Definitions
- Authorization Management Best Practices
- Access Management Best Practices

7.2 Systems Management
- Service Quality Metrics
- Usage Metrics
- Monitoring and Optimization

7.3 Service Level Management
- Cloud Deployment Model Considerations
- Cloud Service Model Considerations

7.4 Broker Platform
- Cloud Service Model Considerations
- Cloud Broker Metrics for Cloud
- Business Case Justification: Cloud Management Considerations
- Economic Model: Cloud Management Considerations
- Vendor Management: Cloud Management Considerations
- Cloud Service Brokerage Platform: Key Platform Highlights
- Cloud Broker Metrics for Cloud
- Cloud-Services Lifecycle Management
- Service Catalog Management
- Service User Provisioning
- Authentication, Authorization, and Access Control
- User and Service Administration
- Dashboards, Auditing, and Reporting
- Helpdesk Ticketing and Support

- Metering, Billing Settlement, and Chargeback

Module 8. Performance Measures, Monitoring and Optimization in Production

8.1 Lifecycle Management
- Cloud Lifecycle Management Needs
- Cloud Lifecycle Management Tooling Benefits
- Cloud Lifecycle Management Roles
- Automation in Cloud Computing
- Cloud Automated Processes Advantage

8.2 Management and Administration Policies
- Reducing Complexity of Cloud Delivery and Image Management
- Service Delivery Management
- Virtual Image Provisioning and Management
- Application Level and Platform Level Management
- Infrastructure Level Management
- Virtual Storage Management Challenges in Cloud Computing

8.3 Monitoring and Reporting
- Monitoring Definition and Objectives
- Monitoring Requirements for Cloud Deployments
- Monitoring Benefits in Cloud Computing
- Visualize Application Performance in Real Time
- Monitor Business Transaction Service Levels
- Monitor Cloud Infrastructure Health
- Isolate Latency and Bottlenecks
- Analyze Existing Application Dependencies
- Monitoring Alerts

8.4 Infrastructure Benchmarking
- Benchmarking Cloud Infrastructure Challenges
- Best Practices to Cloud Infrastructure Benchmarking: General Approach

8.5 Availability and Performance
- High Availability and Seamless Failover
- Definition, Scope, and Applicability of Quality of Service
- High Performance

8.6 Usage and Accounting
- Metering and Chargeback
- Managing Chargeback Metrics

PROFESSIONAL CLOUD ADMINISTRATOR

CLOUD CREDENTIAL COUNCIL

Exam Details

Professional Cloud Administrator Certification Exam	
Exam Type	Scenario Based, Complex Multiple Choice
No. of Questions	25
Duration	75 minutes
Additional Time Provisions	15 minutes additional time for candidates who speak English as a second language.
Prerequisite	There is no prerequisite for this course. It is recommended that participants have passed the CCC Cloud Technology Associate or hold the equivalent certification/experience.
Proctored	Yes (Live/Web)
Open Book	No
Pass Score	65%
Delivery	Online

Cloud Credential Council

The Cloud Credential Council (CCC) is an international member-based organization mandated to drive cloud readiness through effective competence development. The CCC has established critical cloud certifications for key IT roles in order to cultivate cloud-ready IT professionals. The certification scheme was developed after several years research investment in over 20 roles led by industry experts in conjunction with the leading technology vendors in the cloud computing arena.