Miami Dade College

Course Description

CTS2375C | Cloud Infrastructure and Services | 4.00 credits

This course helps students develop technical expertise in Cloud computing and prepares them for Cloud computing industry certification. Students will learn the essentials of Cloud computing, business security and compliance considerations, migrating to the Cloud, architecting a Cloud server, and how to troubleshoot Cloud services. Prerequisite: CTS1145, Corequisite: CTS2960

Course Competencies:

Competency 1: The student will demonstrate an understanding of the business essentials required to implement and support a cloud network by:

1. Explaining the value and benefits of Cloud computing.
2. Discussing the security capabilities, controls, and assurances in place to maintain security and data protection.
3. Identifying the financial impact of Cloud computing on an organization's procurement cycle, cost management, and contracts.
4. Discussing best practices for the successful
5. implementation and operation of an IT environment with Cloud components.

Competency 2: The student will demonstrate an understanding of the technical essentials of the Cloud computing platform by:

1. Describing a Virtual Private Cloud (VPC).
2. Navigating Cloud management consoles and portals.
3. Identifying Cloud security measures.
4. Describing Cloud storage options.
5. Identifying the various Cloud services and networking options.
6. Describing Cloud database options. Launching an application using Cloud database services.
7. Identifying deployment and management options.

Competency 3: The student will demonstrate how to plan and design Cloud platform architecture by:

1. Identifying Cloud architecture considerations, including:
   a. designing and monitoring Cloud services
   b. best practices in designing and incorporating Cloud services.
   c. developing Client Specifications
   d. architectural trade-off decisions, integrating existing development environments, and building scalable architecture and elasticity and scalability
2. Making decisions based on recommended architectural principles and best practices, including:
   a. designing storage subsystems
   b. leveraging global infrastructure
   c. choosing data storage
   d. designing web-scale media hosting
   e. orchestrating batch processing
   f. reviewing large-scale design patterns
   g. designing for cost planning for distributed environments.
   h. designing event-driven scalable, highly available, and fault-tolerant servers.
3. Incorporating security best practices into cloud design.
4. Creating a cloud migration roadmap and plan, including extending on-premises into the cloud.

5. Creating business continuity and disaster recovery plans.

Competency 4: The student will demonstrate how to implement and deploy a Cloud computing platform by:

1. Identifying the appropriate techniques and methods to code and implement a Cloud solution.
2. Operating and extending service management in the private Cloud.
3. Configuring compliance in the private and public Cloud. Launching instances in a variety of geographical regions.
4. Selecting the appropriate Cloud computing service based on data, compute, database, or security requirements.
5. Identifying appropriate use of the Cloud computing architectural best practices.
6. Estimating Cloud platform costs and identifying cost control mechanisms.
7. Troubleshooting and monitoring performance.

Competency 5: The student will demonstrate an understanding of cybersecurity procedures for optimum Cloud deployment and maintenance by:

1. Discussing Cloud security best practices.
2. Applying Cloud security architecture services, including:
    a. shared responsibility for Cloud computing platform compliance
    b. security attributes and services
    c. virtual Private Cloud CIA and AAA models, ingress vs. egress filtering, and which services and features fit. Developing a threat model.
3. Creating a data flow diagram for risk management to include use cases and abuse/negative use cases.
4. Incorporating everyday conventional security products (Firewall, IDS: HIDS/NIDS, SIEM, and VPN).
5. Mitigating Distributed Denial-of-Service (DDoS) attacks encryption solutions.
6. Implementing complex access controls (e.g., building sophisticated security groups, ACLs, etc.).

Competency 6: The student will demonstrate an understanding of disaster recovery techniques by:

1. Discussing disaster recovery issues and considerations.
2. Identifying how to apply Cloud platform disaster recovery (DR) architectures (e.g., pilot light, hot standby, etc.).
3. Designing a disaster recovery plan.
4. Differentiating between “pilot light” and “hot standby” environments.
5. Describing how to apply the specific elements of the Cloud platform to a disaster recovery architecture.
6. Testing recovered data.

Learning Outcomes:

1. Information Literacy
2. Numbers / Data
3. Communication
4. Computer / Technology Usage
5. Critical Thinking