CompTIA Cloud+ (CV0-004) Exam Prep

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: October 7, 2024 - December 6, 2024

Duration: 9 weeks

Instructional Hours: 40 contact hours

Prerequisites: CompTIA Security+ or Network+ certification, or 5 years IT Experience including 2-3 years networking or sys admin experience recommended

Learning Setting: Hybrid Asynchronous Online / Instructor-led Zoom sessions (weekly)

Target Audience: IT practitioners (with 5+ years experience).

Level of instruction: Undergraduate

Course Instructors:

Instructor	Email Address
Dr. Guillermo Francia, III	gfranciaiii@uwf.edu
Mr. Amador Avila, Jr.	aavila@uwf.edu

Course Description

The CompTIA Cloud+ certification is mainly targeted to those candidates who want to build their career in Infrastructure domain. The CompTIA Cloud+ exam verifies that the candidate possesses the fundamental knowledge and proven skills required to:

- Understand cloud architecture and design concepts.
- Implement and maintain a secure cloud environment.
- Successfully provision and configure cloud resources.
- Demonstrate the ability to manage operations throughout the cloud environment life cycle using observability, scaling, and automation.

- Understand fundamental DevOps concepts related to deployment and integration.
- Troubleshoot common issues related to cloud management.

NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181 rev 1, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

Cybersecurity Competencies and Work Roles:

Competencies

- Cloud Security
- Access Control

Work Roles

- Technical Support (IO-WRL-007)
- Network Operations (IO-WRL-004)
- Systems Administrator (OG-WRL-013)

Learning Outcomes mapped to the NICE Cybersecurity Workforce Framework Knowledge, Skills and Abilities (KSAs):

Knowledge of computer networking concepts and protocols, and network security methodologies.

Upon completion of the course, students will be able to:

- T0418: Install, update, and troubleshoot systems/servers
- K0004: Knowledge of cybersecurity and privacy principles.
- T0494: Administer accounts, network rights, and access to systems and equipment.
- K0005: Knowledge of cyber threats and vulnerabilities.
- K0011: Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
- K0029: Knowledge of organization & Local and Wide Area Network connections.
- K0038: Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0088: Knowledge of systems administration concepts.
- K0100: Knowledge of the enterprise information technology (IT) architecture.
- K0104: Knowledge of Virtual Private Network (VPN) security.
- K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).

- K0160: Knowledge of the common attack vectors on the network layer.
- K0167: Knowledge of system administration, network, and operating system hardening techniques.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0242: Knowledge of organizational security policies.
- K0287: Knowledge of an organization & information classification program and procedures for information compromise.
- K0292: Knowledge of the operations and processes for incident, problem, and event management.
- K0294: Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.
- K0317: Knowledge of procedures used for documenting and querying reported incidents, problems, and events.
- S0040: Skill in implementing, maintaining, and improving established network security practices.
- S0076: Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
- S0077: Skill in securing network communications.
- S0079: Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
- S0084: Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
- T0494: Administer accounts, network rights, and access to systems and equipment.

GRADING

The course is designed as examination preparation. Students should complete all assignments and take time to review any incorrect answers. Non-credit course students shall receive a grade of either complete or incomplete at the conclusion of the course. Participants must earn a total of 70% or higher on graded assessments to earn a course completion grade.

Students must register to take the certification exam during the first 10 days of the course and report their exam date(s) to their instructor. Students shall take the certification exam(s) within one week of course end date to receive a course completion certificate and digital badge. Each student will receive a voucher to take the exam and students who do not pass on the first attempt will be provided with additional resources and a second voucher.

Grading Scheme:

Assignment	Percentage of Grade
Exam Registration	15%

• Register for the CompTIA Cloud+ (CV0-004) Exam • Submit Exam Date(s) to the instructor • Due no later than the 6th business day of the course.	
CompTIA Certification Exam • Sit for CompTIA Cloud+ (CV0-004) Exam • Submit Candidate Score Reports from the exam to the instructor. • Due no later than five business days after the course ends	10%
Assignment Completion • Labs • PBQs • Practice Questions	40%
Proficiency	20%
Final CompTIA Practice Assessment	15%
Total	100%

Technical Skills Covered

Domain	Percentage
1.0 Cloud Architecture	23%
2.0 Deployment	19%
3.0 Operations	17%
4.0 Security	19%
5.0 Dev Ops Fundamentals	10%
6.0 Troubleshooting	12%
Total	100%

Course Outline

Weekly Schedule:

Week 1 and 2: Cloud Architecture
Weeks 3: Deployment
Week 4: Operations
Week 5: Security
Week 6: Security (cont)

Weeks 7: Dev Ops Fundamentals
Week 8: Troubleshooting
Week 9: Review and Certification Prep

Course Modules

Modules and Lessons
Module 1: Cloud Architecture and Design Topics: ▪ Deployment Models ▪ Service Models ▪ Advanced Cloud Services ▪ Standard Templates ▪ Licensing ▪ Performance Capacity Planning ▪ Regions and Zones ▪ Scalability ▪ Requirement Analysis ▪ Environments ▪ Testing Techniques
Module 2: Deployment Topics: ▪ Subscription Services ▪ Provisioning Resources ▪ Application ▪ Containers ▪ Auto-scaling ▪ Types ▪ Tiers ▪ Protocols ▪ Storage Systems ▪ Hyperconverged ▪ Software-defined Storage ▪ Virtual Private Networks ▪ Virtual Routing ▪ Network Appliances ▪ Virtualization ▪ Storage Migrations Database Migrations
Module 3: Operations Topics:

- Subscription Services
- Provisioning Resources
- Application
- Containers
- Auto-scaling
- Types
- Tiers
- Protocols
- Storage Systems
- Hyperconverged
- Software-defined Storage
- Virtual Private Networks
- Virtual Routing
- Network Appliances
- Virtualization
- Storage Migrations

Database Migrations

Module 4: Security

Topics:

- Identification and Authorization
- Directory Services
- Federation
- Certificate Management
- Public Key Infrastructure
- Key Management
- Network Segmentation
- Protocols
- Network Services
- Log and Event Monitoring
- Network Flows
- Hardening and Configuration
- Policies
- Host-based IDS/Host-based IPS
- Builds
- Encryption
- Access Control
- Records Management
- Vulnerability Management
- Security Patches
- Incident Response

Module 5: Dev Ops Fundamentals

Topics:

- Logging

- Monitoring
- Life-cycle Management
- Change Management
- Asset Management
- Patching
- Upgrades
- Dashboard and Reporting
- Compute
- Storage
- Network
- Placement
- Device Drivers and Firmware
- Infrastructure as Code
- Version Control
- Secure Scripting
- Backup and Restoration

Module 6: Troubleshooting

Topics:

- Problem Identification, Analysis and Documentation
- Security Analysis: Authentication, Authorization, Keys and Certificates, Policies
- Connectivity Issues
- Performance Degradation
- Configurations
- Insufficient Capacity
- Licensing Issues
- Vendor-related Issues
- Network Configuration Issues
- Resource Utilization