

C S 54D: CLOUD INFRASTRUCTURE & SERVICES

Foothill College Course Outline of Record

Heading	Value
Effective Term:	Summer 2021
Units:	4.5
Hours:	4 lecture, 2 laboratory per week (72 total per quarter)
Advisory:	C S 50A.
Degree & Credit Status:	Degree-Applicable Credit Course
Foothill GE:	Non-GE
Transferable:	CSU
Grade Type:	Letter Grade (Request for Pass/No Pass)
Repeatability:	Not Repeatable

Student Learning Outcomes

- The student will be able to demonstrate knowledge of the requirement for self-service deployment model in a public cloud.
- The student will demonstrate knowledge of the architecture of a virtual data center.

Description

Presents the transition from a classic data center environment to a virtual data center. The student will understand Cloud virtualization at each layer—compute, storage, network, desktop, and application—along with business continuity in a virtual data center (VDC) environment. Explanation and discussion of Cloud computing basics, infrastructure components, service management activities, security concerns, and considerations for Cloud adoption.

Course Objectives

The student will be able to:

- Explain the phases of transition from classic data center to virtual data center and then to the Cloud
- Describe virtualization technology at compute, storage, network, desktop, and application layers of IT infrastructure
- Describe business continuity solutions in a VDC environment
- Explain the key characteristics, services, and deployment models of Cloud
- Describe the Cloud infrastructure components and service management processes
- Describe the Cloud security concerns and solutions
- List the key considerations for migration to the Cloud

Course Content

- Transitioning from a classic data center to a virtual data center and then to the Cloud
 - The business drivers, definition, essential characteristics, and phases of the journey to the Cloud
 - Business drivers
 - Globalization

- Aging data centers
- Application explosion
- Cost of ownership
- Acquisitions of the companies
- Cloud computing
 - The NIST definition
- Essential Cloud characteristics
 - On demand self-service
 - Broad network access
 - Resource pooling
 - Rapid elasticity
 - Measured service
- Building a Cloud infrastructure requires a phased approach
 - Understand the current infrastructure
 - Virtualize the current infrastructure
 - Allows resource pooling and rapid elasticity
 - Deploy service management tools to deliver the Cloud services
 - Automate service provisioning to enable on-demand self-service of computing resources over the network
 - Enable monitoring, control and optimization of resource usage
 - Facilitate measured services
 - Chargeback for resources used
 - Budgeting programs
 - Enable consumption based metering
- Virtualization technology at compute, storage, network, desktop, and application layers of IT infrastructure
 - Compute virtualization
 - Compute is the resource that runs applications with the help of underlying computing components
 - Storage virtualization
 - Storage is a resource that stores data persistently for subsequent use
 - Network virtualization
 - Network is a data path that facilitates communication between compute systems or between compute systems and storage
 - Desktop virtualization
 - Deployment of desktop infrastructure in a virtualized environment
 - Applications and DBMS in a virtualized environment
 - Basic characteristics
 - An application is a computer program that provides the logic for computing operations
 - Applications may use a DBMS, which uses operating system services, to perform store/retrieve operations on storage devices
 - DBMS provides a structured way to store data in logically organized tables that are interrelated. A DBMS optimizes the storage and retrieval of data
 - Business applications
 - Email
 - Enterprise resource planning (ERP)
 - Decision support systems
 - Data warehouse
 - Management applications
 - Resource management
 - Performance tuning
 - Data protection applications
 - Backup
 - Replication
 - Security applications
 - Authentication
 - Antivirus
 - Firewalls
- Business continuity

1. Processes and procedures for ensuring continued business operations in the presence of compute, storage, network, or application failure
 - a. Business continuity solutions address unavailability and degraded application performance
 - b. Business continuity is an integrated enterprise wide process and a set of activities to ensure "information availability"
 - c. Business continuity terminology
 - 1) Disaster recovery
 - 2) Hot site
 - 3) Cold site
 - 3) Cluster
 - 4) RPO and RTO
 - a) Recovery point objective (RPO) is the point in time to which systems and data must be recovered after an outage and the amount of data loss that a business can endure
 - b) Recovery time option (RTO) is the amount of time that can be tolerated within which applications must be recovered and operational after an outage, it is the amount of downtime a business can endure and still survive
 - d. Eliminating single points of failure
 - 1) Single point of failure refers to the failure of a single component, which can terminate the availability of the entire system or an IT service
 - 2) There are several single points of failure in a CDC:
 - a) The single HBA on the compute
 - b) The compute itself
 - c) The IP network
 - d) The Fibre Channel switch
 - e) The storage array ports
 - f) The storage array
 - e. Multipathing software
 - 1) Configuration of multiple paths increases the data availability through path failover
 - 2) Multiple paths to access data also improves I/O performance through load sharing and maximizes server, storage, and data path utilization
 - 3) Multipathing software also manages load balancing by distributing I/Os to all available, active paths
 - f. Backup and recovery
 - 1) Backup is a copy of the production data, created and retained for the sole purpose of recovering deleted or corrupted data
 - 2) Evaluating backup technologies, recovery, and retention requirements for data and applications is an essential step to ensure successful implementation of the backup and recovery solution
 - 3) Disaster recovery addresses the requirement to be able to restore all, or a large part, of an IT infrastructure in the event of a major disaster
 - g. Replication
 - 1) Replication is the process of creating an identical/exact copy of data
 - 2) The exact copy of data which is created is called a replica
 - 3) Replicas can be used to address a number of business continuity functions
 - a) Providing an alternate source for backup to alleviate the impact on production
 - b) Providing a source for fast recovery to facilitate faster RPO and RTO
 - c) Enabling decision support activities
 - D. Key characteristics, services, and deployment models of Cloud
 1. Essential characteristics of Cloud computing
 - a. Technological foundations
 - 1) Grid computing
 - 2) Utility computing
 - 3) Virtualization
 - 4) Service oriented architecture
 - b. Essential characteristics
 - c. Benefits of Cloud computing
 2. Cloud services
 - a. Infrastructure as a Service (IaaS)
 - 1) The base layer of the Cloud model
 - 2) The Cloud infrastructure such as servers, routers, storage, and other networking components are provided by the IaaS provider
 - 3) The consumer is able to deploy and run any software, which may include Operating Systems (OSs) and applications
 - 4) The consumer does not manage or control the underlying Cloud infrastructure, but has control over the OSs and deployed applications
 - 5) The consumer does not manage or control the underlying Cloud infrastructure
 - b. Platform as a Service (PaaS)
 - 1) The capability provided to the consumer to deploy consumer-created or acquired applications on the Cloud infrastructure
 - 2) An application development environments offered as a "service" by the Cloud provider
 - 3) The consumer uses these platforms to develop their applications
 - 4) They then deploy the applications on the infrastructure offered by the Cloud provider
 - c. Software as a Service (SaaS)
 - 1) The capability, provided to the consumer, to use the service provider's applications running on a Cloud infrastructure
 - 2) It is accessible from various client devices through a thin client interface such as a web browser
 3. Deployment models
 - a. Three deployment models: private, public, and hybrid
 - 1) Private Cloud - the Cloud infrastructure is operated solely for one organization and is not shared with other organizations
 - 2) Public Cloud - IT resources are made available to the general public or organizations and are owned by the Cloud service provider
 - 3) Hybrid Cloud - the organization consumes resources from both private and public Clouds, the ability to augment a private Cloud with the resources of a public Cloud can be utilized to maintain service levels in the face of rapid workload fluctuations
 - 4) Economics of Cloud computing
 - a) Infrastructure costs
 - b) Management costs
 - c) Power and energy costs
 4. Benefits and challenges of Cloud computing
 - a. The consumer perspective
 - 1) Safety and regulation
 - 2) Network latency
 - 3) Supportability
 - 4) Interoperability
 - b. The provider perspective
 - 1) Service cost
 - 2) Service warranty
 - 3) Huge variety of software to support
 - 4) No standard Cloud access standards
 - E. Describe the Cloud infrastructure components and service management processes
 1. Cloud infrastructure framework consists of the following components:
 - a. Physical infrastructure
 - 1) Physical servers
 - 2) Storage systems
 - 3) Physical network components
 - a) Physical adapters
 - b) Switches
 - c) Routers
 - 4) Physical servers are connected
 - a) To each other
 - b) To the storage systems

- c) To the clients via physical networks such as IP network, FC SAN, IP SAN, or FCoE network
- b. Virtual infrastructure
 - 1) Resource pools such as CPU pools, memory pools, network bandwidth pools, and storage pools
 - 2) Identity pools such as VLAN ID pools, VSAN ID pools, and MAC address pools
 - 3) Virtual IT resources consist of:
 - a) VMs, virtual volumes, and virtual networks
 - b) VM network components such as virtual switches and virtual NICs
 - c. Applications and platform software
 - 1) Applications and platform software layers include a suite of software such as:
 - a) Business applications
 - b) Operating systems
 - c) Database management systems
 - d) These softwares are required to build environments for running applications
 - 2) Migration tools
 - a) Enabling deployment of consumer's applications and platform software to Cloud
 - d. Cloud infrastructure management and service creation tools
 - 1) Management and service creation tools are responsible for managing physical and virtual infrastructures
 - 2) Tools to enable consumers to request for Cloud services
 - 3) Cloud infrastructure management and service creation tools automate consumer request processing and creation of Cloud services
 - F. Cloud security concerns and solutions
 - 1. Security concerns and counter measures in a VDC and Cloud environment
 - a. Basic security concepts
 - 1) CIA triad - a security framework for an information system has three primary goals
 - a) Confidentiality
 - b) Integrity
 - c) Availability of physical and logical resources
 - 2) AAA - the security framework an information system should provide
 - a) Authentication
 - b) Authorization
 - c) Auditing (assesses the effectiveness of security)
 - 3) Defense-in-Depth - a risk management strategy which provides multiple layers of defense against attacks
 - 4) Encryption - the conversion of data into a form that cannot be easily understood by unauthorized users
 - b. Security concerns and threats in a Cloud environment
 - 1) Multitenancy and "velocity-of-attack"
 - 2) Data privacy
 - 3) VM vulnerable
 - 4) VM theft
 - 5) Hyperjacking, a rootkit level vulnerability
 - 6) Data leakage
 - G. Migration to a Cloud infrastructure
 - 1. Migration considerations
 - a. Application suitability for the Cloud
 - b. Criteria for vendor selection
 - c. Service level agreements
 - d. Cloud-vendor lock-in
 - e. Cloud open standards
 - 2. Using a phased approach for migration
 - a. Assessment
 - b. Proof of concept
 - c. Migration

- d. Optimization

Lab Content

- A. Understanding RAID
 - 1. RAID 0
 - a. Create RAID 0 volume, identify properties
 - 2. RAID 1
 - a. Create RAID 1 volume, identify properties
 - 3. RAID 5
 - a. Create RAID 5 volume, identify properties
- B. Block-level and file-level storage
 - 1. Block-level storage with iSCSI
 - a. Create volume for iSCSI
 - b. Configure iSCSI target
 - c. Configure iSCSI initiator on client and mount
 - 2. File-level storage with NFS
 - a. Create a volume for NFS
 - b. Create a NFS share
 - c. Mount NFS share from client
- C. Backup and recovery concepts
 - 1. Setup and configure deduplication on NAS01
 - a. Setup dedup volume and NFS share
 - b. Copy the CentOS virtual machines from NAS01 to dedup
 - 2. Setup and configure replication of NAS01 to NAS02
 - a. Setup periodic snapshots
 - b. Setup SSH on both NAS systems
 - c. Setup a replication task
- D. Replication and deduplication
 - 1. Setup and configure deduplication on NAS01
 - a. Setup dedup volume and NFS share
 - b. Copy the CentOS virtual machines from NAS01 to dedup
 - 2. Setup and configure replication of NAS01 to NAS02
 - a. Setup periodic snapshots
 - b. Setup SSH on both NAS systems
 - c. Setup a replication task
- E. vSphere and vCenter
 - 1. Learning the ESXi hypervisor and virtual machines
 - a. Create a virtual machine
 - b. Adjusting virtual machine configurations
 - c. Monitor virtual machine performance
 - 2. Learning the vCenter environment
 - a. Identify datacenter, cluster, pool and vApp
- F. vSphere datastore implementation
 - 1. Storage vMotion
 - a. Configure ESXi for Storage vMotion
 - b. Storage DRS
 - c. Storage I/O control
- G. vSwitches: networking in the VDC
 - 1. vSwitch
 - a. vSwitch explained
 - b. Configure a vSwitch
 - 2. Distributed vSwitch
 - a. Configure a distributed vSwitch
- H. Benefits of vMotion and Storage vMotion
 - 1. vMotion
 - a. Migrate a virtual machine from ESXi01 to ESXi02
 - 2. Storage vMotion
 - a. Migrate a virtual machine from NAS01 to NAS02
- I. VMware HA and VMware FT
 - 1. VMware HA
 - a. Configure VMware HA

- b. Test VMware HA
- 2. VMware FT
 - a. Configure VMware FT
 - b. Test VMware FT

Special Facilities and/or Equipment

- A. Access to a network laboratory with current Cisco network equipment host computers required to support the class.
- B. Website or course management system with an assignment posting component (through which all lab assignments are to be submitted) and a forum component (where students can discuss course material and receive help from the instructor). This applies to all sections, including on-campus (i.e., face-to-face) offerings.
- C. When taught via Foothill Global Access on the Internet, the college will provide a fully functional and maintained course management system through which the instructor and students can interact.
- D. When taught via Foothill Global Access on the Internet, students must have currently existing email accounts and ongoing access to computers with internet capabilities.

Method(s) of Evaluation

- Tests and quizzes
- Written laboratory assignments
- Final examination

Method(s) of Instruction

- Lectures which include motivation for the architecture of the specific topics being discussed
- In-person or online labs (for all sections, including those meeting face-to-face/on-campus), consisting of:
 - 1. An assignment webpage located on a college-hosted course management system or other department-approved internet environment. Here, the students will review the specification of each assignment and submit their completed lab work
 - 2. A discussion webpage located on a college-hosted course management system or other department-approved internet environment. Here, students can request assistance from the instructor and interact publicly with other class members
- Detailed review of laboratory assignments which includes model solutions and specific comments on the student submissions
- In-person or online discussion which engages students and instructor in an ongoing dialog pertaining to all aspects of designing, implementing and analyzing programs
- When course is taught fully online:
 - 1. Instructor-authored lecture materials, handouts, syllabus, assignments, tests, and other relevant course material will be delivered through a college-hosted course management system or other department-approved internet environment
 - 2. Additional instructional guidelines for this course are listed in the attached addendum of CS department online practices

Representative Text(s) and Other Materials

- EMC Education Services. [Dell EMC Cloud Infrastructure and Services v3](#). 2019.

Types and/or Examples of Required Reading, Writing, and Outside of Class Assignments

- A. Reading
 - 1. Textbook assigned reading averaging 50 pages per week.
 - 2. Online resources as directed by instructor through links pertinent to networking.
 - 3. Library and reference material directed by instructor through course handouts.
- B. Writing
 - 1. Technical prose documentation that supports and describes the laboratory exercises that are submitted for a grade.

Discipline(s)

- Computer Science