

HPE Digital Learner Cloud Computing Fundamentals Content Pack

HPE Content Pack number	CP022
Content Pack length	20 Hours
Content Pack category	Category 2
Learn more	View now

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

This self-paced eLearning Content Pack provides baseline cloud fundamentals training as part of a strategy to enhance IT capabilities across the enterprise. There are many cloud technologies, solutions, platforms and tools available. As part of an enterprise training strategy, it is imperative that the IT organization is properly trained with baseline cloud fundamentals prior to choosing specific cloud solutions. Our cloud fundamentals training provides a foundational baseline for all levels within the typical IT organization, covering cloud concepts, operational models, technologies and platforms, while also adhering to cloud training standards from Comp TIA. This training is recommended for all roles across a typical IT organization prior to moving down the path of planning and deploying specific private and/or public cloud technologies and/or platforms.

Audience

- IT professionals including managers, engineers and technical staff evaluating or implementing cloud applications and services

Content Pack objectives

This Content Pack provides the information necessary to help prepare a typical IT organization for transition to a hybrid cloud operational model.

This training series concentrates on cloud fundamentals, introducing basic cloud concepts, technologies, operating models, tools and platforms.

This training includes a cloud overview and also covers the more detailed areas of virtualization, cloud data centers, data storage, management of cloud infrastructures and

applications, migration to cloud, identity, access, privacy, and security. This series also includes specific Comp TIA courses for planning cloud deployments, networking, compute and storage resources, governance and compliance, disaster recovery, performance management and troubleshooting. This training enables students from multiple IT and technology backgrounds to establish a cloud training baseline, setting the stage for higher level training as required by the enterprise as it moves deliberately toward specific private and/or public cloud platforms and technologies. This training should be considered as part of any enterprise's baseline cloud training plans to ensure talent enablement across the new digital enterprise.

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Detailed Content Pack outline

Cloud Computing Fundamentals: Overview

Cloud computing is massively growing in importance in the IT sector as more and more companies are eschewing traditional IT and moving applications and business processes to the cloud. This course provides IT professionals with a working definition of cloud computing, explores the technological precursors of today's cloud, and covers current technologies that the cloud is dependent on. It also covers the benefits and drawbacks of cloud computing for the IT department and the business as a whole. It then explores in more detail the different types of services that have become available in the cloud with examples of key pioneers in those areas.

- Describe the development of computing from mainframes to the cloud
- List the key technologies that enable cloud computing
- Define cloud computing according to relevant standards
- Define the core attributes of a cloud computing service
- List the three main cloud service models
- Recognize STaaS, CaaS, BPaaS and other cloud service models
- Evaluate security issues in cloud services against traditional IT
- Evaluate cloud services in a number of areas, including levels of control and interoperability
- Describe the function of service level agreements in cloud services
- Describe use cases for the cloud from the perspective of users and different types of business
- Describe compliance and regulatory issues as they pertain to the cloud
- Describe the barriers to cloud adoption and changing attitudes to cloud
- Describe how cloud services can be stacked to form complete solutions
- Describe the Infrastructure as a Service or IaaS cloud service model
- Describe the Platform as a Service or PaaS cloud service model
- Describe the Software as a Service or SaaS cloud service model
- Describe the cost of cloud computing compared to traditional IT in terms of capital expense (CAPEX) and operational expense (OPEX)
- Describe the four main cloud deployment models
- Describe costing considerations for different cloud deployment models
- Assess an application's suitability to move to the cloud
- Determine the suitability for given IT services to be moved to the cloud

Cloud Computing Fundamentals: Virtualization and Data Centers

While the cloud is not necessarily dependent on virtualization, it is widely accepted that it will be used by any competitive cloud. Infrastructural and network connectivity considerations of the modern data center are greatly influenced by the requirements of the cloud. Data center infrastructure and components must be designed to address security, scalability, disaster recovery and redundant high speed connectivity needed to provide a successful cloud service. This course takes a closer look at the main enabling technologies including data centers and virtualization.

- Describe the key terms associated with virtualization
- Describe the processes and components of hardware virtualization
- Describe Type I and Type II virtualization hypervisors
- Describe virtual desktop infrastructure and application virtualization as components of desktop virtualization
- Describe network functions virtualization
- Describe storage types and storage virtualization technologies
- Describe how virtualization enables key characteristics of cloud computing
- Describe Microsoft Hyper-V®, VMware vSphere®, and Citrix XenServer®
- Describe Oracle and IBM server virtualization products
- Describe the components of a modern data center
- Describe the functions provided by a modern data center
- Describe how data centers relate to and enable cloud computing
- Describe the business trends in cloud computing
- Describe the technical trends in cloud computing
- Describe how cloud data centers are designed to support applications
- Describe the functional components of a cloud data center including storage, networking, computing, management and services
- Describe the functions of the cloud data center and how they utilize virtualization technologies

Cloud Computing Fundamentals: Storing and Managing Cloud Data

Cloud storage is of key interest to many consumers since it has a number of advantages over traditional data storage. Cloud-stored data is available from any location that has internet access. However, depending on the type of business and data, some organizations need to carefully evaluate if and what types of regulations and compliance standards may apply. This course provides a closer look at enterprise resources in the cloud and the use of cloud storage services. It describes the importance of classifying your type of data, what type of security regulations or restrictions apply, and whether a cloud provider's offering aligns with those requirements. This course also takes a closer look at the protocols, standards and mobile client access involved in accessing cloud resources. It explores the meaning of open source software and its role in provisioning and accessing cloud resources.

- Describe the Storage as a Service (STaaS) model as it relates to cloud computing
- List the advantages of the Storage as a Service model
- List the risks associated with the Storage as a Service model
- List the main providers of Storage as a Service and describe their offering
- Describe the Cloud Security Alliance cloud governance domains as they pertain to data stored on cloud services
- Describe cloud storage governance issues
- Describe privacy concerns for personally identifiable information stored on public cloud services
- Describe the function of data classification in cloud storage governance
- Describe data security considerations in cloud storage systems
- Describe emerging standards for cloud computing
- List the groups working on cloud computing standards
- List the common cloud security protocols
- Describe the Cloud Standards Customer Council recommendations for cloud security
- List the common protocols and standards in use for cloud computing
- List the common cloud application programming interfaces
- List the web standards relevant to cloud computing
- Describe open source and how it pertains to the cloud
- Describe open source cloud software for n-tier applications
- Describe OpenStack open source cloud software
- Describe the characteristics of mobile devices connecting to cloud services
- Describe the best practices for working with cloud storage in terms of governance and standards for a given scenario

Cloud Computing Fundamentals: Migrating to the Cloud

Migrating services to the public cloud has a number of unique challenges. This course explores the steps you should take to determine if your infrastructure has components that are suitable for a cloud solution. It discusses the Service Oriented Architecture (SOA) and grid computing, and highlights characteristics that make these infrastructures suitable or unsuitable for extension to the cloud. The course also explores the recommended steps to analyze your current infrastructure to inventory data, services and processes used, and to identify problem areas that may be addressed through a cloud solution. Upon completion of your analysis, it is time to determine cloud service candidates, match cloud services, and look at examples of how to leverage different services to your problem areas. Finally, you will learn about the use of private clouds as an alternative to public clouds.

- Describe Service Oriented Architecture (SOA)
- List the benefits of Service Oriented Architecture compared to traditional IT solutions
- Describe the link between Service Oriented Architecture and cloud computing
- Describe common application architectures and how they relate to Service Oriented Architecture and the cloud
- Contrast grid computing and cloud computing
- Plan deployment of services to the cloud
- Describe the function of a service directory in deploying cloud services
- Describe the process of migrating IT services and business processes to the cloud
- Contrast loosely and tightly coupled processes when considering a cloud migration
- Describe the technical factors affecting a migration to the cloud
- Describe the business factors affecting a migration to the cloud
- Assess cloud platforms for migration to the cloud
- Describe potential privacy, regulatory and security issues with public clouds
- Describe strategies to mitigate potential privacy, regulatory and security issues with public clouds
- Describe how private and hybrid clouds can mitigate potential privacy, regulatory and security issues with public clouds
- Assess a service for migration to public or private clouds and determine which cloud type to select

Cloud Computing Fundamentals: Identity, Presence, and Privacy

As we move toward more applications being delivered via the cloud and businesses using a cloud computing model, we also need to consider the implications for managing identity. This course ensures you are familiar with identity and access management (IAM) and the common industry protocols used to extend identity to the cloud. This course covers the concept of federation between different cryptographic services providers (CSPs) and businesses, the need for proper identity and access control management, and the use of a cloud Identity as a Service (IDaaS) offering. The course also discusses the importance of presence and privacy factors when conducting business in the cloud and how it is crucial to understand the CSP's responsibility to not only provide security but also a proper level of privacy.

- Describe the basic concepts of identity and access management
- List reasons for using identity federation
- Describe the operational areas of identity and access management
- Describe how cloud service providers can provide identity and access management
- Describe the concepts associated with identity federation
- Describe the considerations for implementing identity federation in cloud services
- Describe the standards for identity federation
- Describe access control systems with single sign-on
- List the benefits and risks of single sign-on
- Describe the Identity as a Service authentication infrastructure
- Describe the challenges in implementing Identity as a Service
- Describe methods for integrating Identity as a Service with other service models
- List the pros and cons of the Identity as a Service provider
- Describe presence information and how it is used in cloud systems
- Describe the components of a presence system
- Describe the processes and tools associated with a presence system
- Describe the security considerations for presence systems
- Describe the privacy concerns for cloud systems
- Describe privacy policies and how they are implemented in cloud systems
- Describe the data life cycle in the context of cloud computing
- Describe the data security challenges in cloud computing
- Map the cloud security measures to the data life cycle stage to which they apply
- Describe the methods of controlling access to data stored on the cloud

Cloud Computing Fundamentals: Cloud Security

IT security is a concern for most modern organizations; moving to the cloud heightens those concerns for most. The security implications are potentially magnified by large amounts of data existing outside the immediate control of the organization. Although some of the fears with regard to security in the cloud are exaggerated, there are specific areas to be aware of and cautious about. This course explores some of the key risk areas when it comes to security and cloud computing. It also introduces control assessment frameworks and models that can be used in assessing risk in going to the cloud and evaluating the cloud provider's security offering. It goes on to outline basic guidelines that you should follow to ensure an adequate level of security in an SaaS environment, including key areas of the IT infrastructure and issues relating to data transfer and storage.

- Describe the objectives of information security and how they relate to the cloud
- Describe the challenges associated with cloud security
- Describe the three models for public cloud security responsibilities
- Describe relevant ISO standards for information security
- Describe the Security as a Service model
- Describe the security risk areas for cloud computing
- Describe how to assess security offerings for cloud services
- Describe the challenges associated with security in a Software as a Service (SaaS) offering
- Describe the best practices for securing a Software as a Service offering
- Describe secure software development practices
- Describe the Jericho Forum Cloud Cube Model for defining cloud characteristics
- Describe the considerations for infrastructure security in cloud computing
- Describe the host-level security considerations in cloud computing
- Describe considerations for security virtualization hosts in a cloud environment
- Describe application level security in cloud computing
- Describe the measures to secure data at rest and data in transit
- Describe how to perform risk assessment in a cloud environment
- Describe the service-level agreements for cloud security
- Describe the measures to secure data and connection in a cloud environment

CompTIA Cloud+ CV0-002: Planning Cloud Deployments

To start deploying to the cloud, you must know what you are deploying and what you are deploying to. In this course, you will learn about analyzing and executing the requirements for a successful test cloud deployment.

- Specify cloud benefits, components and service models
- Compare cloud deployment models and select the best model for a particular deployment
- Identify how the change management process integrates with a cloud deployment plan
- Select the correct environmental considerations for a particular test cloud deployment
- Choose the best testing techniques for acquiring desired information from a test cloud deployment
- Validate a test cloud deployment's success or failure in meeting the organization's business needs
- Perform a deployment of a cloud service

CompTIA Cloud+ CV0-002: Planning Cloud Networking

Cloud resources must be able to connect to each other and to any on-premises locations using networking technologies. In this course, you will examine the configuration and troubleshooting of those networks.

- Specify the network components that are used in a cloud deployment
- Recognize the relationship between various deployment models and their networking scheme
- Choose the correct ports to enable relative to the services used in the cloud
- Configure internal cloud network settings to meet business needs
- Distinguish between the various network configurations used to connect to the cloud
- Describe how to correctly segment cloud networks and integrate them with on-premise networks
- Perform the tasks necessary to connect technology services with a cloud deployment
- Differentiate between common cloud networking issues and their causes
- Select the appropriate network tool for troubleshooting a network problem
- Use cloud networking troubleshooting tools

CompTIA Cloud+ CV0-002: Planning Cloud Compute Resources

Cloud elasticity is largely based on the ability to assign and revoke memory and CPU resources. In this course, you will explore memory and CPU configuration options that administrators must define to manage cloud technologies.

- Differentiate between different cloud memory management technologies
- Configure memory for cloud resources
- Identify different cloud CPU management technologies
- Configure CPU settings for cloud resources
- Specify the different costs associated with the choices made when allocating CPU and memory in the cloud

CompTIA Cloud+ CV0-002: Planning Cloud Storage Resources

Cloud-managed IT generally always involves storing data in the cloud. In this course, you will explore storage options that administrators must define to manage cloud technologies.

- Identify the qualities that distinguish different types of cloud storage
- Identify cloud storage protocols and describe cloud storage tiers
- Select appropriate storage efficiency technologies
- Differentiate between object provisioning options in cloud storage
- Create cloud stored data
- Specify storage redundancy technologies
- Perform steps to ensure cloud data high availability
- Apply storage security mechanisms
- Configure cloud storage security
- Choose and configure the correct cloud storage technology in a given scenario

CompTIA Cloud+ CV0-002: Planning Cloud Migrations and Extensions

One of the biggest challenges with moving to the cloud is just that - the migration of resources from on-premise solutions to cloud solutions. In this course, you will explore migration tools and integration of on-premise and cloud environments.

- Recognize considerations when performing a migration to a cloud environment including choosing a provider and preparing to migrate workloads to the cloud
- Specify the constraints on the process of migrating to a cloud environment
- Compare the different types of migrations possible relative to the cloud
- Enumerate the benefits of a hybrid cloud environment
- Recall the management of elements and protocols needed to secure a hybrid cloud environment including authorization and Federation
- Identify the services needed to successfully connect an on-premise and cloud environment

CompTIA Cloud+ CV0-002: Security Configurations and Compliance Controls

The most prevalent concern with cloud computing is the question of security. In this course, you will explore the technologies used to secure cloud resources.

- Recognize the qualities of a well-defined cloud security policy
- Specify how to secure a cloud infrastructure using certificate-based technologies
- Compare different tunneling protocols that can be used to securely connect to a cloud environment
- Identify the different techniques used to reduce the vulnerabilities of the resources in a cloud environment
- Describe the different security issues that are dependent upon the cloud service and deployment models
- Choose the appropriate authentication technology to identify users connecting to the cloud
- Compare different access control options available to cloud administrators
- Choose the correct level of access to use to secure cloud resources
- Configure authorization of cloud resources
- Identify the correct processing techniques to ensure the safety of cloud user accounts
- Configure account settings in a cloud environment for best security

CompTIA Cloud+ CV0-002: Security Technologies and Automation Techniques

Security is an absolutely critical part of cloud deployments. Security must be configured correctly or it will prevent valid users from accessing resources. In this course, you will explore the technologies used to secure and troubleshoot cloud deployments

- Specify the correct level of cloud security based upon data classification
- Use segmentation to correctly encapsulate areas of a cloud network into safe zones
- Define the data and network cloud components that need encryption to meet safety standards
- Choose the cloud auditing standards that meet the compliance level of an organization
- Recognize the situations where multifactor authentication is required
- Enable cloud security services that protect cloud resources
- Use appropriate tools to handle different cloud security situations
- Describe the scope of impact that security services will have on the behavior of the cloud resources
- Troubleshoot authentication issues
- Troubleshoot certificate-related issues
- Troubleshoot issues related to users, roles and ACLs
- Troubleshoot vulnerabilities in cloud security configuration

CompTIA Cloud+ CV0-002: System Patching and Maintenance

A good maintenance plan is an important part of protecting the resources you keep in the cloud from security and performance issues. In this course, you will explore the technologies used to patch and maintain cloud resources.

- Identify the cloud resources that need to be routinely checked for updates
- Choose between different patching methodologies
- Enable cloud update management
- Differentiate between different types of cloud updates
- Automate cloud patching processes
- List the various cloud resource related tasks that need routine automation
- Compare the benefits of maintenance tasks with the cost to the cloud systems
- Apply a PowerShell DSC configuration to a Microsoft Azure® virtual machine

CompTIA Cloud+ CV0-002: Disaster Recovery

Disasters are going to happen and administrators must use tools to survive even the worst case scenarios. In this course, you will explore the technologies used to back up cloud data and other disaster recovery technologies.

- Identify the different types of cloud backup
- Choose between different options for cloud backup targets
- Recognize the interaction between backup and other cloud operations
- Execute a point-in-time restore for an Azure SQL database
- Rate the capabilities of a service provider to provide disaster recovery
- Choose between different techniques for ensuring a recovery site is available
- Recall the components of a business continuity plan
- Configure Azure SQL database geo-replication

CompTIA Cloud+ CV0-002: Performance Management

In order to gauge success in a cloud deployment, administrators must be able to accurately monitor their environment. In this course, you will explore methods and processes used to monitor and manage cloud environments.

- Recognize the need for monitoring and the scope of monitoring tasks
- Monitor cloud resources using common tools
- Adjust cloud virtual machine sizing to accommodate a given workload
- Configure an Azure scale set
- Use PowerShell DSC to ensure cloud virtual machines adhere to required configurations
- Adjust the amount of cloud vCPUs that can be allocated
- Correlate Azure SQL Database metrics with the Azure SQL Database SLA

CompTIA Cloud+ CVO-002: Troubleshooting Deployments

In a perfect world, everything would be deployed correctly and without issues. In our world, we need to troubleshoot everything. In this course, you will explore troubleshooting cloud resources.

- List the troubleshooting methodology steps in order
- Identify common issues in cloud resources that need troubleshooting

Learn more at

www.hpe.com/ww/digitallearner

www.hpe.com/ww/digitallearner-contentpack

Follow us:



© Copyright 2019 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community. Pivotal and Cloud Foundry are trademarks and/or registered trademarks of Pivotal Software, Inc. in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

CP022 A.00, February 2019

