

Designing and Implementing Cloud Connectivity (ENCC) v1.0

Course Description

The Designing and Implementing Cloud Connectivity training helps you develop the skills required to design and implement enterprise cloud connectivity solutions. You will learn how to leverage both private and public internet-based connectivity to extend the enterprise network to cloud providers. You will explore the basic concepts surrounding public cloud infrastructure and how services like Software as a Service (SaaS) can be integrated. You will practice how to analyze and recommend connectivity models that provide the best quality of experience for users. You will learn to implement both Internet Protocol Security (IPsec) and Software-Defined Wide-Area Network (SD-WAN) cloud connectivity, as well as build overlay routing with Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). Finally, you will practice troubleshooting cloud connectivity issues relating to IPsec, SD-WAN, routing, application performance, and policy application.

This training prepares you for the 300-440 ENCC exam. If passed, you earn the Cisco Certified Specialist–Enterprise Cloud Connectivity certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Enterprise certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

How You'll Benefit

This training will help you:

- Develop the skills required to design and implement enterprise cloud connectivity solutions
- Learn how to apply the VPN and overlay networking technology, including Cisco Catalyst SD-WAN to extend the enterprise network to cloud providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) using both private connectivity services and public internet as an underlay
- Examine the solutions for optimizing access to SaaS cloud providers and the workflows for diagnosing and troubleshooting cloud connectivity issues
- Gain knowledge for protocols, solutions, and designs to acquire professional-level and expert-level enterprise roles
- Earn 40 CE credits toward recertification

Who Should Enroll

- Cloud Architects
- Cloud Administrators
- Cloud Engineers
- Cloud Network Engineers
- Cloud Automation Engineers
- Cloud Systems Engineers
- Security Analysts
- Cloud Security Managers
- Cloud Consultants
- Cloud Application Developers
- Systems Engineers
- Technical Solutions Architect

What to Expect in the Exam

300-440 ENCC: Designing and Implementing Cloud Connectivity is a 90-minute exam associated with the Cisco Certified Specialist–Enterprise Cloud Connectivity certification and satisfies the concentration exam requirement for the CCNP Enterprise certification.

The multiple-choice format tests your knowledge of designing and implementing cloud connectivity, including:

- Architecture models
- IPsec
- SD-WAN
- Operation
- Design

Course Objectives

- Describe the fundamental components and concepts of cloud computing, including deployment models, cloud services, and cloud providers, to provide learners with a comprehensive overview of the subject
- Describe the options available for establishing connectivity to public cloud services, including point-to-point IPsec VPN and various Cisco Catalyst SD-WAN Cloud OnRamp deployment options
- Explain the public cloud connectivity architecture similarities and differences between different cloud service providers and explore the available connectivity options to the public cloud from a Cisco Catalyst SD-WAN environment
- Describe private connectivity options to public cloud provider infrastructure
- Describe direct connections to different public cloud providers for private peering
- Describe connectivity solutions such as colocation, cloud exchange, and software-defined cloud interconnect providers for connecting to the public cloud infrastructure

- Describe the available options for connectivity to SaaS applications from a geographically distributed organization's premises
- Explain the emergence of DIA to optimize cloud application performance and user experience
- Describe the essential business and technical prerequisites for achieving high availability, resiliency, and scalability within an enterprise cloud connectivity network solution
- Describe AWS, Azure, and GCP native security
- Describe PCI DSS, FedRAMP, and HIPAA compliance requirements and their role in public cloud integration
- Implement underlay (internet-based) connectivity to connect to the public cloud
- Configure overlay tunnels over public transport to a cloud-native gateway in AWS, Azure, and GCP and to a cloud-hosted Cisco IOS XE router
- Deploy a cloud-hosted Cisco IOS XE-based router instance and customize the cloud networking setup
- Configure OSPF and BGP routing for typical enterprise network
- Explore Cisco Umbrella SIG
- Introduce Cisco vManage Policy Architecture and centralized data policies
- Explain AAR policy components and implementation
- Understand Microsoft 365 Traffic categories and service areas
- Describe the AppQoE feature
- Describe DRE deployment considerations
- Describe how to diagnose and troubleshoot common issues for connectivity to public cloud environments using internet-based connectivity
- Introduce the BGP routing protocol used for establishing connectivity between on-premises and public cloud devices over different connection options
- Discuss BGP peering and connectivity issues with Microsoft Azure and explore various troubleshooting and test tools and techniques
- Discuss some common configuration, networking, and routing issues encountered on customer edge devices when connecting to Microsoft Azure ExpressRoute

Course Prerequisites

The knowledge and skills you are expected to have before attending this training are:

- Basic understanding of enterprise routing
- Basic understanding of WAN networking
- Basic understanding of VPN technology
- Basic understanding of Cisco Catalyst SD-WAN
- Basic understanding of Public Cloud services

These skills can be found in the following Cisco Learning Offerings:

- Implementing and Administering Cisco Solutions 2.0
- Implementing and Operating Cisco Enterprise Network Core Technologies 1.3
- Cisco SD-WAN Fundamentals 2.0

- Implementing Cisco SD-WAN Security and Cloud Solutions 1.1

Course Outline

1. Public Cloud Fundamentals
2. Internet-Based Connectivity to Public Cloud
3. Private Connectivity to Public Cloud
4. SaaS Connectivity
5. Resilient and Scalable Public Cloud Connectivity
6. Cloud-Native Security Policies
7. Regulatory Compliance Requirements
8. Internet-Based Public Cloud Connectivity
9. Overlay Routing Deployment
10. Cisco SD-WAN Internet-Based Cloud Connectivity
11. Cisco SD-WAN Cloud Security
12. Cloud OnRamp for SaaS
13. Cisco SD-WAN Policies
14. Application Quality of Experience
15. Internet-Based Public Cloud Connectivity Diagnostics
16. Overlay Routing Diagnostics
17. Cisco SD-WAN Public Cloud Connectivity Diagnostics

Lab Outline

1. Initial Lab Network Exploration
2. Implement IPsec Connectivity to Public Cloud Gateways
3. Implement IPsec Connectivity to Cloud-Hosted Cisco IOS-XE Routers
4. Implement Overlay Routing
5. Deploy Cloud OnRamp for Multicloud
6. Deploy Umbrella Cloud Security
7. Implement Cloud OnRamp for SaaS
8. Troubleshoot Underlay Connectivity
9. Troubleshoot Overlay Routing
10. Diagnose Cloud OnRamp for Multicloud