Over 35 Years Of Technology Training

Document Generated: 11/16/2024

Learning Style: Virtual Classroom

Provider: Cisco

Difficulty: Intermediate

Course Duration: 5 Days

Securing Cisco Digital Network Architecture (DNA) (DNASEC)

About this course:

Many challenges exist managing modern networks on a day to day basis. The problems are intensified when manual configuration changes using fragmented tool offerings result in non-centralized change and configuration management which

leads to various naming, configuration, backup and security compliance issues. Manual configuration changes when compared to automated, policy-based approaches are slow and error-prone. Break and fix, new network builds and change requests in dynamic environments where user requirements, devices and applications are evolving at ever increasing rates fueled in many cases by the big data of IoT. The networks of today face deployment, support and security challenges mitigated with modern tools such as Digital Network Architecture Centre (DNAC), Cisco Identity Services Engine (ISE) and Stealthwatch. In this course, you use these tools to build a centrally managed, authenticated, authorized, monitored and security-policy compliant solution.

Course Objective:

Upon completing this course, the learner will be able to deploy and setup a network built on DNA and SDA concepts and components and be prepared for daily operation tasks associated to such networks. The learner will meet these overall objectives:

- Know and understand Cisco’s DNA and SD-Access concepts, features, benefits, terminology and the way this approach innovates common administrative tasks on today’s networks.
- Differentiate and explain each of the building blocks of SD-Access Solution
- Be familiar with fabric and node types
- Deploy and configure Fabric Edge Nodes, Control Plane nodes and Border Nodes
- Configure LISP in Control Plane for SD-Access Solution
- Configure VXLAN in Data Plane for SD-Access Solution
- Configure TrustSec for segmentation and Policy Enforcement
- Understand the role of DNA Center as solution orchestrator and Intelligent GUI
- Deploy DNA Center and perform initial setup
- Use workflow approach in DNA Center and its 4 Steps: Design, Policy, Provision and Assurance
- Deploy ISE and integrate it with DNA Center and SD-Access Solution
- Deploy StealthWatch and Integrate it with DNA Center and SD-Access Solution
- Monitor and Troubleshoot SDA operation
- Know and understand the migration strategies from traditional networks to SD-Access Solution

Audience:

The primary audience for this course is as follows:

- Anyone interested in knowing about DNA and SD-Access
- Personnel involved in SD-Access Design and Implementation
- Network Operations team with SD-Access solution

Prerequisite:

The knowledge and skills that a learner must have before attending this course are as follows:

- Cisco CCNA or Equivalent Experience
- Basic Knowledge of Software Defined Networks
- Basic Knowledge of network security including AAA, Access Control and ISE
- Basic Knowledge and experience with Cisco IOS, IOS XE and CLI
- Basic Knowledge of virtualization, Hypervisors and Virtual Machines

Course Outline:

Module 1: Introduction to Cisco's Software Defined Access (SD-Access)

- DNA Introduction
- SD-Access Overview
- SD-Access Benefits
- SD-Access Key Concepts
- SD-Access Main Components
    - Campus Fabric
        - Wired
        - Wireless
    - Nodes
        - Edge
        - Border
        - Control Plane
- DNA Center (Controller)
- ISE (Policy)
- StealthWatch (Policy)
- NDP (Analytics and Assurance)

Module 2: SD-Access Campus Fabric

- The concept of Fabric
- Node types
    - Fabric Edge Nodes
    - Control Plane Nodes
    - Border Nodes
- LISP as protocol for Control Plane
- Configure LISP for Control Plane
- VXLAN as protocol for Data Plane
- Configure VXLAN for Data Plane
- Virtual Networks (VN)
- Fabric-enabled WLAN
    - Fabric Enabled WLC
    - Fabric Enabled AP's
- SDA-ready Cisco Catalyst LAN Switches
- Role of Cat9k in Cisco SD-Access solution and deployment models as border, control and edge nodes

Module 3: DNA Center and Workflow for SD-Access

- Introduction to DNA Center
- Workflow for SD-Access in DNA Center
    - Design Step overview
    - Policy Step overview
    - Provision Step overview
    - Assurance Step overview
- Integration with Cisco ISE for Policy Enforcement
- Integration with Cisco StealthWatch for Policy Enforcement
- Integration with Cisco NDP for Analytics and Assurance

Module 4: Deployment and initial setup for DNA Center

- Requirements
- Deployment Procedure
- Initial Setup
- GUI Navigation

Module 5: Deployment and initial setup for ISE and Integrate with DNA Center

- Introduction to Cisco ISE
- Requirements
- Cisco ISE Deployment Models
- Deployment Procedure
- Initial Setup
- GUI Navigation
- Integration with DNA Center

Module 6: Deploy Netflow Collector and StealthWatch Management Center (SMC)

- Introduction to Netflow and SMC
- Requirements
- Deployment Procedure
- Initial Setup
- GUI Navigation
- Integration with DNA Center / SD Access

Module 7: Implementing Policy Plane using Cisco TrustSec for Segmentation

- Cisco TrustSec phases
    - Classification
    - Propagation
    - Enforcement
- Configuring Classification
- Configuring SGT tag propagation
- Configure Enforcement
- Introducing Cisco TrustSec in ISE
- Cisco ISE as controller for Software-defined segmentation (groups and

policies)
    - Configuring ISE for Dynamic SGT assignment
    - Configuring ISE for Static SGT assignment
    - Configuring Policy Enforcement

Module 8: Cisco StealthWatch Management Console (SMC)

- Configuring Host Groups in the SMC
- Configuring Flexible NetFlow on Cisco Devices
- Verify Netflow Data Collection on SMC
- Configuring Cisco StealthWatch and ISE Integration

Module 9: DNA Center Workflow First Step - Design

- Creating Enterprise and Sites Hierarchy
- Configuring General Network Settings
- Loading maps into the GUI
- IP Address Management
- Software Image Management
- Network Device Profiles

Module 10: DNA Center Workflow Second Step - Policy

- 2-level Hierarchy
    - Macro Level: Virtual Network (VN)
    - Micro Level: Scalable Group (SG)
- Policy Types
    - Access Policy
    - Access Control Policy
    - Traffic Copy Policy
- Cross Domain Policies

Module 11: DNA Center Workflow Third Step - Provision

- Devices Onboarding
    - Discovering Devices
    - Assigning Devices to a site
    - Provisioning device with profiles
- Fabric Domains
    - Understanding Fabric Domains
    - Using Default LAN Fabric Domain
    - Creating Additional Fabric Domains
- Adding Nodes
    - Adding Fabric Edge Nodes
    - Adding Control Plane Nodes
    - Adding Border Nodes

Module 12: DNA Center Workflow Fourth Step – Assurance

- Introduction to Analytics

- NDP Fundamentals
- Overview of DNA Assurance
- Components of DNA Assurance
- DNA Center Assurance Dashboard

Module 13: Implementing WLAN in SD-Access Solution

- WLAN Integration Strategies in SD-Access Fabric
    - CUWN Wireless Over The Top (OTT)
    - SD-Access Wireless (Fabric enabled WLC and AP)
- SD-Access Wireless Architecture
    - Control Plane: LISP and WLC
    - Data Plane: VXLAN
    - Policy Plane and Segmentation: VN and SGT

Module 14: Implementing Campus Fabric External Connectivity for SD-Access

- Role of Border Nodes
- Types of Border Nodes
    - Border
    - Default Border
- Single Border vs. Multiple Border Designs
- Collocated Border and Control Plane Nodes
- Distributed (separated) Border and Control Plane Nodes
- Configuring Border Nodes

Module 15: SDA Migration Strategies

- Migrate to SD-Access using a quality-assured process, state-of-the-art tools and proven methodologies
- The need for additional planning
    - Typical considerations
    - Primary Approaches for migration
        - Building SD-Access network in parallel and then integrate
        - Do incremental migrations of access switches into an SD-Access fabric

Lab Outline

- Deploy and Setup DNA Center
- Deploy and Setup ISE
- Deploy and Setup StealthWatch
- Integrate ISE with DNA Center
- Integrate StealthWatch with SD-Access infrastructure
- Performing SD-Access Design Step in DNA Center
- Performing SD-Access Policy Step in DNA Center and ISE
- Performing SD-Access Provision Step in DNA Center
- Integrating WLAN services through SD-Wireless architecture
- Deploy and Setup Border Node

- Monitoring SDA Operations
- Troubleshooting SDA Operations

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges