Software Defined Access and ISE Integration for Policy Deployment and Enforcement (SDAISE)

Modality: Virtual Classroom

Duration: 3 Days

CLC: 34 Units

About this course:

SD-Access is Cisco’s Next Generation campus networking solution that simplifies management, automation, and improves security implications.

Who (People), what (Devices), when (Time) and where (Location) are questions we would like answered when working with users and devices! These questions are answered within a single pane of glass known as the Cisco Identity Services Engine (ISE). Once users and devices are identified we often segment these groups for management purposes. Cisco's Digital Networks Architecture Center (DNAC) is a means of configuring and maintaining that segmentation using software defined access. DNA Center is not limited to configuration changes. DNA Center also provides a policy-based approach to services that support the network such as NTP, DNS, DHCP. In this course, you integrate ISE and DNAC which gives you the ability to manage physical devices, logical segmentation, IP, transport rules as well as Authentication, Authorization and Accounting (AAA) of users and devices along with an overview and introduction to SD-Access and DNA Center.

Course Objective:

Upon completing this course, the learner will be able to meet these overall objectives:

- Explain the role that ISE plays as part of the solution
- Configure AAA services and TrustSec Policy in ISE
- Explain ISE Integration with DNA Center for Policy enforcement
- Know and understand Cisco’s 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
- Explain the concept of “Fabric” and the different node types that conform it (Fabric Edge Nodes, Control Plane Nodes, Border Nodes)
- Describe the role of LISP in Control Plane and VXLAN in Data Plane for SD-Access Solution
- Understand TrustSec concepts, deployment details and the way it is used as part of SD-Access Solution for segmentation and Policy Enforcement
- Understand the role of DNA Center as solution orchestrator and Intelligent GUI
- Be familiar with workflow approach in DNA Center - Design, Policy, Provision and Assurance

Audience:

The primary audience for this course is as follows:

- Anyone interested in knowing about 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 should have before attending this course are as follows:

- Knowledge level equivalent to Cisco CCNA Routing & Switching
- 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

Course Outline:

Module 1: Cisco ISE Integration for SD Access

- Introduction to Cisco ISE
- Using Cisco ISE as a Network Access Policy Engine
- Introducing Cisco ISE Deployment Models
- Introducing 802.1x and MAB Access: Wired and Wireless
- Introducing Identity Management
- Configuring Certificate Service
- Introducing Cisco ISE Policy
- Configuring Cisco ISE Policy Sets
- Introduction to Cisco TrustSec for segmentation
- The Concept of Security Group (SG) and Security Group Tag (SGT)
- Cisco TrustSec Phases
    - Classification
    - Propagation
    - Enforcement
- Methods for Classification
    - Static Classification
    - Dynamic Classification
- Methods for SGT tag propagation
    - Inline Tagging
    - SGT Exchange Protocol (SXP)

Module 2: Introduction to Cisco’s Software Defined Access (SD-Access)

- SD-Access Overview
- SD-Access Benefits
- SD-Access Key Concepts
- SD-Access Main Components
    - Campus Fabric
        - Wired
        - Wireless

    - Nodes
        - Edge
        - Border
        - Control Plane
    - DNA Controller (APIC-EM Controller)

    - Introducing Cisco ISE 2.x px
- 2-level Hierarchy
    - Macro Level: Virtual Network (VN)
    - Micro Level: Scalable Group (SG)

Module 3: DNA Center Workflow

- DNA Center Refresher
- Creating Enterprise and Sites Hierarchy
- Configuring General Network Settings
- Loading maps into the GUI
- IP Address Management
- Software Image Management
- Network Device Profiles
- Introduction to Analytics
- NDP Fundamentals
- Overview of DNA Assurance

Module 4: SD-Access Campus Fabric

- The concept of Fabric
- Node types (Breakdown)
- LISP as protocol for Control Plane
- VXLAN as protocol for Data Plane

Module 5: Campus Fabric External Connectivity for SD-Access

- Enterprise Sample Topology 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

Module 6: Implementing WLAN in SD-Access Solution

- WLAN Integration Strategies in SD-Access Fabric
    - Fabric CUWN
    - 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
- Sample Design for SD-Access Wireless

Lab Outline

- ISE basic setup and Navigating GUI
- Configuring TrustSec in ISE
- Connecting and getting familiar with DNA Center GUI
- Performing SD-Access Design Step in DNA Center
- Integrating ISE and DNA Center for Policy Deployment and Enforcement
- Performing SD-Access Policy Step in DNA Center and ISE
- Performing SD-Access Provision Step in DNA Center
- Performing SD-Access Assurance Step in DNA Center
- Integrating WLAN services through SD-Wireless architecture
- Integrate ISE with Active Directory
- Achieving External Connectivity to remote locations through Border Node