Contact:
Info@silverlake.sg
+65 - 65882456

Software Defined Access & ISE Integration for Policy Deployment & Enforcement v1.0

Course#:SDAISE
Duration:3 Days
Price:0.00

Course Description

Software-Defined Access (SD-Access) is the industrys first intent-based networking solution for the Enterprise built on the principles of Ciscos Digital Network Architecture (DNA). SD-Access provides automated end-to-end segmentation to separate user, device and application traffic without redesigning the network.

There are many challengesto manage enterprise networks including manual configuration and fragmented tool offerings. Manual operations are slow and error-prone and these issues are exacerbated by constantly changing environments with more users, devices and applications. With the growth of users and different devices types accessing the network, it is has become more complex to configure user credentials and maintain a consistent policy across the network.

Without a consistent access policy, it is difficult to maintain separate policies between wired and wireless or to locate users and troubleshoot issues as users move around the network. The bottom line is that networks today do not addresscurrent network needs. TheSDAISEcourse addresses these issues.

Objectives

Upon completion of 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 Ciscos SD-Access concepts, features, benefits, terminology and the way this approach innovates common administrative tasks on todays 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

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

Prerequisites

It is recommended that students have the following knowledge and skills prior to attending this course:

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

Content

Virtual Classroom Live 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 Ciscos 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

Virtual Classroom Live Labs

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