NT-SDAOTS: Cisco Software-Defined Access (SDA): Use Case Implementation, Operations, & Troubleshooting

Course Code: NT-SDAOTS
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This 5-day deep dive training course explores the capabilities of the Cisco Software-Defined Access (SDA) solution. Students will learn how to implement SDA for different solution verticals. It also addresses the details of how to operate and troubleshoot the different capabilities of the underlying solution components.

SKILLS COVERED

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

- Articulate the value of Cisco SDA Use Cases including, for example: saving operational and management cost to maintain and support ever growing network infrastructure; central security policy to comply to regional or global regulatory requirements and enterprise security policy; deliver best-in-class services to end-users; leveraging networking insights and trends to optimize business process and workflows. Some real scenarios such as supporting multi-mode collaboration within shared workspaces in life sciences; accelerating the deployment of "pop-up" sites for emergency medical purposes; creating integrated building management solutions; zero-touch day 0 network turn-up of additional sites, rapid response to network threat and vulnerabilities, and similar.
- Describe the technical capabilities of Cisco DNA Center and how they are applied in SDA Use Cases. This includes the lifecycle stages of network device discovery, assigning network devices to sites, network design options, provisioning, software image management, building a fabric, segmentation design, assurance, application policy, etc.
- Set up an SDA environment, integrating Cisco Identity Services Engine (ISE) and other solution components as required.
- Apply troubleshooting methods, processes, tips to resolve implementation and maintenance issues of the following aspects of the technical solution:
- Device Onboarding, including device discovery, Plug-and-Play and LAN Automation
- Network design settings, including sites, AAA, SNMP, Syslog, IP address pools, image management, network profiles, and authentication templates
- Policies for access control, applications and virtual networks
- Provisioning, including template-based provisioning for day 0 and day N operations
- Network Segmentation, including the application of Cisco TrustSec security with Scalable Group Tags (SGTs) and Virtual Networks
- Assurance to monitor network, endpoint, and applications to ensure best user experience
- Integration of ServiceNow for an integrated IT service management lifecycle
- Integration of InfoBlox for integrated IPAM

WHO SHOULD ATTEND?

The primary audience for this course is as follows:

- IT management, to understand how to address key business requirements with greater efficiency and flexibility in network service delivery
- IT solution architects, to understand the role that SDA plays in enabling such efficiency and flexibility for network services in the context of IT solution delivery
- IT and network security architects, to understand how the integrated capabilities of the SDA solution are used to design and implement network segmentation-based security
- IT operations engineers, integrating network and application visibility and root cause analysis into integrated IT case handling workflows
- Networking Admin and Operations installing, integrating, configuring and operating Cisco DNA Center, Cisco Identity Services Engine (ISE), and other solution components, in the context of Cisco SDA based network services
- Networking Field Engineers using capabilities of Cisco Catalyst Center to deploy, monitor and maintain network infrastructure for SDA based network services

PREREQUISITES

The knowledge and skills that the learner should have before attending this course are as follows:

- Implementation of Enterprise LAN networks
- Basic understanding of Enterprise switching, and wireless connectivity
- Basic understanding of Enterprise routing connectivity
- Basic understanding of AAA (authentication, authorization, and accounting) process and workflow
- Programming knowledge such as Python, RestAPI is useful

MODULES

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

- Understanding Cisco Intent-Based Networking
- Understanding Cisco SDA Use Cases customer's benefits including business and technical outcomes and capabilities
- Cisco Catalyst Center (formerly DNAC) Introduction
- SD-Access Overview
- SD-Access Benefits
- SD-Access Key Concepts
- SD-Access Main Components
  - Fabric Control Plane Node
  - Fabric Border Node
  - Fabric Edge Node
  - Fabric Wireless LAN Controller and Fabric Enabled Access Points
- Cisco Catalyst Center Automation
- Cisco ISE (Policy)
- Cisco StealthWatch (Traffic Analysis)
- DNA Center Assurance

Module 2: Deployment and Initial setup for the Cisco DNA-Center

- Cisco Catalyst Center Appliances
- Cisco Catalyst Center Deployment Models
  - Single Node Deployment
  - Clustered Deployment
- Installation Procedure
- Initial Setup and Configuration
- GUI Navigation

Module 3: SDA - Design

- Network design options
- Sites
- Creating Enterprise and Sites Hierarchy
- Configuring General Network Settings
- Loading maps into the GUI
- IP Address Management
- Software Image Management
- Network Device Profiles
- AAA
- SNMP
- Syslog
- IP address pools
- Image management
- Creating Enterprise and Guest SSIDs
    - Creating the wireless RF Profile
    - Cresting the Guest Portal for the Guest SSIDs
- Network profiles
- Authentication templates

Module 4: SDA - Policy

- 2-level Hierarchy
    - Macro Level: Virtual Network (VN)
    - Micro Level: Scalable Group (SG)
- Policy
    - Policy in SD-Access
    - Access Policy: Authentication and Authorization
    - Access Control Policy
    - Application Policy
    - Extending Policy across domains
    - Preserving Group Metadata across Campus, WAN and DC
    - Enforcing policy in Firewall domains
    - Cross Domain Policies

Module 5: SDA - Provision

- Devices Onboarding
    - Lifecycle stages of network device discovery
    - Discovering Devices
    - Assigning Devices to a site
    - Provisioning device with profiles
    - Plug-and-Play
    - LAN Automation
- Templates
    - Templates for day 0
    - Templates for day N operations
- IP Transits
    - How to connect the Fabric Sites to the external network
    - Creating the IP Transit
    - Considerations for a SD-Access Border Node Design
    - BGP Hand-Off Between Border and Fusion
- Fabric Domains
    - Understanding Fabric Domains and Sites
    - Using Default LAN Fabric Domain
    - Creating Additional Fabric Domains and Sites
- Adding Nodes
    - Adding Fabric Edge Nodes
    - Adding Control Plane Nodes
    - Adding Border Nodes

Module 6: SDA - Assurance

- Overview of DNA Assurance
- Cisco Catalyst Center Assurance- Use Cases Examples
- Network Health & Device 360
- Client Health & Client 360
- Application Health & Application 360
- Cisco SD- Application Visibility Control (AVC) on Catalyst Center
- Proactive troubleshooting using Sensors

Module 7: Cisco SD-Access Distributed Campus Design

- Introduction to Cisco SD-Access Distributed Campus Design – The Advantage?
- Fabric Domain vs Fabric Site
- SD-Access Transits:
  - IP-Based Transit
  - Cisco SD-Access Transit
  - Cisco SD-WAN Transit
- Deploying the Cisco Distributed Campus with SD-Access Transit
  - Site considerations
  - Internet connectivity considerations
  - Segmentation considerations
  - Role of a Cisco Transit Control Plane
- Cisco SD-Access Fabric in a Box
  - The need for FiaB
  - Deploying the FiaB

Module 8: Cisco SD-Access Brownfield Migration

- Cisco SD-Access Migration Tools and Strategies
- Two Basic Approaches:
  - Parallel Deployment Approach
  - Incremental Deployment Approach
- Integration with existing Cisco ISE in the network – Things to watch out for!
- Choosing the correct Fusion Device
  - Existing Core as Fusion
  - Firewall as Fusion
- When do you need the SD-Access Layer-2 Border?
  - L2 Border – Understanding the requirement
  - Designing and Configuring the L2 Border
  - L2 Border – Not a permanent solution

Module 9: Cisco Catalyst Center Automation-Use Cases Examples

- DAY0: Onboarding new devices using Zero Touch Deployment
- DAY1: Configurations using Templates
- DAYN: Security Advisories based on Machine Reasoning Engine
- DAYN: Simplified Software Management based on Golden Images
- DAYN: Defective Device Replacement – RMA

Module 10: 3rd Party Integrations

- ServiceNow
  - Integration
  - Management
- InfoBlox IPAM
  - Integration
  - Management

Module 11: Specific Use Cases

- Use Case: STACK LAN Automation
- Use Case: Silent Hosts
- Use Case: Wake on LAN
- Use Case: The need for L2 flooding
- Use Case: Multicast in the SD-Access Fabric

Module 12: Cisco SD-Access Multi-Domain Integrations

- Cisco SD-Access to ACI Integrations
  - Phase-1: Policy Plane Integration
  - Phase-2: Data Plane Integration
- Cisco SD-Access to Cisco SD-WAN Integrations
  - What is possible today? SD-WAN Transit setup.
  - Phase-1: The one box solution
  - Phase-2: The two box solution

Module 13: Troubleshooting

- Fabric
- Layer 3 forwarding
- Layer 2 forwarding
- Multicast Forwarding
- Security in the Fabric
- Troubleshooting Multi-Site Deployments

Lab Outline

- Lab 1: SDA Fundamentals
- Lab 2: Using the Catalyst Center Discovery Tool
- Lab 3: Using the Catalyst Center Inventory Tool
- Lab 4: ISE and Catalyst Center Integration
- Lab 5: Using the Catalyst Center Design Application
- Lab 6: Using the Catalyst Center Policy Application
- Lab 7: Fabric Provisioning
- Lab 8: Wired and Wireless Host and Access Point Onboarding Configuration
- Lab 9: Configuring External Connectivity Using Fusion Router
- Lab 10: Configuring Cisco ISE Policies for User Onboarding
- Lab 11: Onboarding and Provisioning Access Points
- Lab 12: Fabric and Segmentation Verification
- Lab 13: Layer-2 Border Fundamentals
- Lab 14: Configuring a Layer-2 Border to Extend the Same IP Pool
- Lab 15: Transitioning the Traditional User to the SDA Anycast Gateway
- Lab 16: Testing IP Connectivity between SDA User and Traditional User
- Lab 17: Introduction to SDA Distributed Campus
- Lab 18: Configuring an SDA-Transit and the Transit Control Plane (TCP)
- Lab 19: Designing a Second Fabric Site
- Lab 20: Deploying a Second Fabric Site – Fabric in a Box
- Lab 21: Deploying a New Fabric Edge using LAN Automation
- Lab 22: Automate Network Devices Using Day-N Template
- Lab 23: Add as Edge Node to Fabric Site-2
- Lab 24: Host Onboarding at Fabric Site-2
- Lab 25: Connecting the two Fabric Sites Using the SDA-Transit
- Lab 26: Testing IP Connectivity and Micro-Segmentation between Fabric Site-1 and Fabric Site-2

END OF PAGE