

# Cisco SD Access Advanced

## Troubleshooting und Optimierungen

Das Software Defined Access von Cisco zeichnet sich durch eine gut strukturierte und deshalb leicht erlernbare Managementoberfläche aus, die durch den DNA Center Controller bereitgestellt wird. Weitgehend automatisiert können dadurch Features wie LISP und VXLAN auf der Netzinfrastruktur in Betrieb genommen werden. Auch die Implementierung der Security Policies und Scalable Groups ist mittels der Identity Services Engine (ISE) und dem DNA Center auf einfache Weise möglich. Geht es aber um Troubleshooting beim Betrieb der SD-Access-Lösung, so sind tiefergehende Kenntnisse der Zusammenhänge erforderlich. In diesem Kurs wird deshalb genauer auf das Locator/ID Separation Protocol (LISP) eingegangen, das die Control-Plane-Aufgaben in der SD Access Fabric übernimmt. Außerdem werden die Funktionen, die die ISE in der SD-Access-Lösung bereitstellt genauer betrachtet. Schwerpunkt ist es auch das Zusammenspiel der Komponenten detaillierter zu analysieren. Praktische Übungen am Testnetz mit Konfiguration und Troubleshooting ergänzen das erlernte Wissen.

### Kursinhalt

- Hochverfügbarkeit durch DNA Center Cluster
- Authentication und Authorization mit der ISE
- Logging und Monitoring auf der ISE
- Scalable Group Access
- Funktionale Komponenten von LISP
- LISP-Signalisierung
- Skalierbare VPNs mit LISP
- Host Mobility
- Troubleshooting von LISP
- LAN Automation
- Multi-Site Fabric Interconnect
- Fusion Router
- WLAN Integration
- Assurance

**E-Book** Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

### Zielgruppe

Der Kurs eignet sich für Administratoren und Operatoren, die eine SD-Access-Lösungen in ihren Cisco-Enterprise-Netzen betreiben oder implementieren möchten.

### Voraussetzungen

Die Teilnehmer müssen sattelfest im Umgang mit dem Cisco IOS-XE sein und über gute Routing-Kenntnisse verfügen. Grundkenntnisse zum DNA Center und der ISE sind ebenfalls erforderlich. Zur Vorbereitung eignet sich der Kurs Cisco DNA Center – SDN-basierte Netzwerkinfrastrukturen

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.de/go/SDAA](http://www.experteach.de/go/SDAA)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Stand 30.01.2025

Training		Preise zzgl. MwSt.	
<b>Termine in Deutschland</b>	<b>5 Tage</b>	<b>€ 3.395,-</b>	
<b>Online Training</b>	<b>5 Tage</b>	<b>€ 3.395,-</b>	
<b>Termin/Kursort</b>	<b>Kurssprache Deutsch </b>		
31.03.-04.04.25	03.11.-07.11.25		
31.03.-04.04.25	03.11.-07.11.25		



# Inhaltsverzeichnis

## Cisco SD Access Advanced – Troubleshooting und Optimierungen

<b>1</b>	<b>Hochverfügbarkeit für DNA Center</b>	<b>2.10</b>	SGT – Ein Einblick	<b>5.2.1</b>	Automation Boundary
<b>1.1</b>	Backup und Restore	<b>2.10.1</b>	Security Groups – Klassifizierung	<b>5.3</b>	Der LAN Automation Workflow
<b>1.1.1</b>	Voraussetzung für die Backup Server	<b>2.10.2</b>	Die Arbeitsweise von SGTs	<b>5.3.1</b>	Planen von LAN Automation
<b>1.1.2</b>	Die Konfiguration des DNAC Core System Backup Servers	<b>2.10.3</b>	SGTs – Die Übermittlung	<b>5.3.2</b>	Vorbereitung der Devices
<b>1.1.3</b>	Konfiguration des Assurance Data Backup Servers	<b>2.10.4</b>	SGT Exchange Protocol (SXP)	<b>5.3.3</b>	Die Design-Phase
<b>1.1.4</b>	Management der Backup-Daten	<b>2.10.5</b>	Zuweisung der SGTs	<b>5.4</b>	Provisioning beim LAN Automation
<b>1.2</b>	DNA Center Cluster	<b>2.11</b>	SGT-Konfiguration auf der ISE	<b>5.4.1</b>	LAN Automation Start
<b>1.2.1</b>	Voraussetzung für ein DNAC Cluster	<b>2.11.1</b>	Anlegen von Security Groups auf der ISE	<b>5.4.2</b>	LAN Automation Stop
<b>1.2.2</b>	Einrichten eines DNA Center Clusters	<b>2.11.2</b>	PACs einrichten	<b>5.5</b>	Zuweisen eines neuen Switches zum LAN Automation Stack
<b>2</b>	<b>Die Identity Services Engine (ISE)</b>	<b>2.12</b>	Zuweisung von SGTs	<b>5.5.1</b>	Zuweisen eines existierenden Switches zum LAN Automation Stack
<b>2.1</b>	Grundkonfiguration der ISE	<b>2.12.1</b>	Statisches Mapping der SGTs	<b>5.5.2</b>	Zuweisen von zusätzlichen Links zum LAN Automation Stack
<b>2.1.1</b>	Das ISE 2.x-Lizenzmodell (1/3)	<b>2.12.2</b>	SXP einrichten	<b>6</b>	<b>Migration hin zu SD Access</b>
<b>2.1.2</b>	Das ISE 3.x Lizenzmodell	<b>2.13</b>	Access Control mit SGTs	<b>6.1</b>	Migration hin zu SDA
<b>2.1.3</b>	Installation der ISE (1/3)	<b>2.13.1</b>	SGACLs auf der ISE	<b>6.2</b>	Segmentierung und Cross Domain Security
<b>2.1.4</b>	Maintenance	<b>2.13.2</b>	Die TrustSec Policy	<b>6.3</b>	Zuweisung der Fabric Roles
<b>2.2</b>	ISE – Basic Settings	<b>2.13.3</b>	SGACLs auf dem Switch	<b>6.4</b>	Routing auf dem Border Node
<b>2.2.1</b>	Deployments	<b>2.13.4</b>	SGTs zur Network Segmentation im SD-Access	<b>6.5</b>	Wireless Migration
<b>2.2.2</b>	Network Access Devices	<b>3</b>	<b>LISP im Detail</b>	<b>7</b>	<b>Fabric Interconnect</b>
<b>2.3</b>	Das ISE AAA-Konzept	<b>3.1</b>	Was ist LISP	<b>7.1</b>	Multi-Site Fabric Interconnect
<b>2.3.1</b>	Policy Sets	<b>3.1.1</b>	LISP-Übersicht	<b>7.1.1</b>	MPLS als IP Transit
<b>2.3.2</b>	Die Authentication Policy	<b>3.1.2</b>	Anwendungsfälle für LISP	<b>7.1.2</b>	Cisco SD Access Transit
<b>2.3.3</b>	User Stores	<b>3.2</b>	LISP Name Spaces	<b>7.1.3</b>	Konfiguration eines Transit
<b>2.3.4</b>	Interne User	<b>3.2.1</b>	Der Endpoint Identifier (EID)	<b>7.2</b>	Fusion Router im SD Access
<b>2.3.5</b>	Interne Endpoints	<b>3.2.2</b>	Der Routing Locator (RLOC)	<b>7.2.1</b>	Die Funktion des Fusion Routers
<b>2.3.6</b>	Externe Datenbanken	<b>3.3</b>	Funktionale Komponenten von LISP	<b>7.2.2</b>	Prinzip des Route Leakings
<b>2.3.7</b>	RADIUS Proxy-Konfiguration	<b>3.3.1</b>	Der Ingress Tunnel Router (ITR)	<b>7.2.3</b>	Konfiguration des Border Nodes
<b>2.3.8</b>	Identity Source Sequence	<b>3.3.2</b>	Der Egress Tunnel Router (ETR)	<b>7.2.4</b>	Konfiguration des Fusion Routers
<b>2.3.9</b>	Certificate Authentication Profiles	<b>3.3.3</b>	Der Map Server (MS)	<b>8</b>	<b>WLAN Integration</b>
<b>2.3.10</b>	Identity Stores in der Authentication Policy	<b>3.3.4</b>	Der Map Resolver (MR)	<b>8.1</b>	WLAN Integration
<b>2.3.11</b>	Authorization Policy	<b>3.4</b>	Die LISP-Signalisierung	<b>8.1.1</b>	SD Access Embedded Wireless
<b>2.3.12</b>	Authorization Condition	<b>3.4.1</b>	LISP Encapsulation	<b>8.2</b>	SD Access Wireless Design
<b>2.3.13</b>	Authorization Profiles	<b>3.4.2</b>	LISP Messages	<b>8.3</b>	Access Points verbinden sich mit der Fabric
<b>2.4</b>	Maschinen und User-Authentisierung	<b>3.4.3</b>	LISP-Prozeduren	<b>8.4</b>	Wireless Clients werden mit der Fabric verbunden
<b>2.4.1</b>	Chaining mit EAP-FASTv2	<b>3.5</b>	Skalierbare VPNs mit LISP	<b>8.5</b>	Mobility Events in der Fabric
<b>2.4.2</b>	Chaining Results	<b>3.5.1</b>	Instance ID	<b>8.6</b>	Wireless im SDA: Gastzugang
<b>2.5</b>	pxGrid	<b>3.5.2</b>	LISP Canonical Address Format	<b>9</b>	<b>Troubleshooting im SD Access</b>
<b>2.5.1</b>	pxGrid – Zentraler Informationsaustausch	<b>3.6</b>	LISP im IOS	<b>9.1</b>	Troubleshooting AAA Service
<b>2.5.2</b>	pxGrid aktivieren	<b>3.6.1</b>	Control Plane	<b>9.2</b>	Troubleshooting SGACLs
<b>2.5.3</b>	ISE als pxGrid Controller	<b>3.6.2</b>	Data Plane	<b>9.3</b>	Troubleshooting Host DHCP Onboarding
<b>2.5.4</b>	Operationen im Überblick	<b>3.6.3</b>	Konfiguration der LISP-Komponenten	<b>9.4</b>	Troubleshooting Host Registration
<b>2.6</b>	Radius Live Authentications	<b>4</b>	<b>Unicast und Multicast Forwarding</b>	<b>9.5</b>	Troubleshooting LISP Host Resolution
<b>2.6.1</b>	Details der Authentisierung (1/3)	<b>4.1</b>	SD Access im Überblick	<b>9.6</b>	Troubleshooting External Connectivity
<b>2.6.2</b>	Abgleich mit dem NAD	<b>4.1.1</b>	Das Referenzmodell	<b>9.7</b>	Troubleshooting Fusion Router Connectivity
<b>2.7</b>	Radius Reports	<b>4.1.2</b>	Netzwerktopologien für die Campus Fabric	<b>9.8</b>	Troubleshooting WLAN
<b>2.7.1</b>	Diagnostic Reports	<b>4.2</b>	Unicast Forwarding über die SDA-Fabric	<b>9.8.1</b>	Die Assurance App für WLAN Troubleshooting
<b>2.7.2</b>	Audit Reports	<b>4.2.1</b>	Unicast Forwarding innerhalb eines Subnetzes	<b>9.8.2</b>	CLI-Kommandos für das WLAN Troubleshooting
<b>2.8</b>	Troubleshooting – Authentisierung	<b>4.2.2</b>	Unicast Forwarding zwischen verschiedenen Subnetzen		
<b>2.8.1</b>	TCP Dumps	<b>4.3</b>	Multicast Forwarding über die SDA-Fabric		
<b>2.8.2</b>	Endpoint Debugs	<b>4.3.1</b>	PIM-ASM/SSM Control Plane Interaktion mit der Fabric		
<b>2.8.3</b>	Konfiguration der NADs	<b>4.3.2</b>	Head End Replication in der Multicast Data Plane der Fabric		
<b>2.8.4</b>	Optimierung des Loggings	<b>4.3.3</b>	Native Multicast Data Plane in der Fabric		
<b>2.8.5</b>	NAD – Log-Timer	<b>5</b>	<b>LAN Automation</b>		
<b>2.8.6</b>	Aggregation der Logs	<b>5.1</b>	LAN Automation im Überblick		
<b>2.8.7</b>	Collection Filter	<b>5.2</b>	Voraussetzungen für LAN Automation		
<b>2.8.8</b>	Log Targets				
<b>2.9</b>	Alarmer				

