

// Jivops

Cisco ACI

Guía completa — 20 lecciones

Fundamentos · Modelo de política · Servicios y multisitio · Operación

Contenido

Módulo 1: Fundamentos y arquitectura

- Lección 01 — Qué es Cisco ACI
- Lección 02 — Arquitectura spine-leaf
- Lección 03 — El clúster APIC
- Lección 04 — Descubrimiento y puesta en marcha de la fabric
- Lección 05 — Protocolos y encapsulación de la fabric

Módulo 2: Modelo de política

- Lección 06 — Tenants, VRF y bridge domains
- Lección 07 — EPG y contratos
- Lección 08 — Perfiles de aplicación
- Lección 09 — Políticas de acceso
- Lección 10 — Conexión externa con L3Out

Módulo 3: Servicios e integración

- Lección 11 — Service graph y PBR
- Lección 12 — Integración con virtualización: VMM
- Lección 13 — Multi-Pod
- Lección 14 — Multi-Site
- Lección 15 — Microsegmentación

Módulo 4: Operación y seguridad

- Lección 16 — Automatización: API REST, Ansible y Terraform
- Lección 17 — Monitorización y resolución de problemas
- Lección 18 — Actualizaciones y copias de configuración
- Lección 19 — Seguridad de gestión y RBAC
- Lección 20 — Proyecto final: fabric ACI para un centro de datos

Módulo 1: Fundamentos y arquitectura

Lección 01 — Qué es Cisco ACI

Una solución de red definida por software para centros de datos: una fabric de switches Nexus gestionada de forma centralizada por un clúster de controladores APIC, donde se define la conectividad mediante políticas de aplicación (modelo declarativo) en lugar de configurar cada switch.

La gestión es centralizada y automatizable, con configuración coherente y menos errores que switch a switch.

Lección 02 — Arquitectura spine-leaf

Una arquitectura spine-leaf: cada leaf se conecta a todos los spine, los servidores y los dispositivos se conectan a los leaf, los spine solo interconectan leafs, y todos los caminos tienen el mismo número de saltos, con ECMP para repartir tráfico.

Latencia predecible y escalado añadiendo leafs o spines, con caminos equivalentes (ECMP).

Lección 03 — El clúster APIC

Es el punto de gestión y política: se despliegan normalmente tres o más controladores con base de datos distribuida; almacena la política y la distribuye a los switches, pero no está en el plano de datos, así que la fabric sigue reenviando tráfico si los APIC caen.

La fabric sigue reenviando, pero no se pueden hacer cambios de política ni ver estado hasta recuperarlo.

Lección 04 — Descubrimiento y puesta en marcha de la fabric

Se inicializa el primer APIC con los parámetros de la fabric (nombre, rango de TEP, VLAN de infraestructura), este descubre un leaf, que descubre los spines y el resto de nodos; los switches se registran y se les asigna ID de nodo, tras lo cual se unen los demás APIC.

Es rápido y con menos errores, ya que no se configura cada switch a mano.

Lección 05 — Protocolos y encapsulación de la fabric

IS-IS como protocolo de enrutamiento de la red subyacente (underlay), VXLAN como encapsulación, COOP para el registro de endpoints en los spines y MP-BGP con EVPN para distribuir rutas externas en el overlay.

Escala a muchos más segmentos y permite extender la capa 2 sobre una red de capa 3.

Módulo 2: Modelo de política

Lección 06 — Tenants, VRF y bridge domains

El tenant es un contenedor administrativo que aísla políticas y recursos; el VRF es un espacio de enrutamiento de capa 3 aislado; y el bridge domain define el dominio de difusión de capa 2 y asocia subredes con puerta de enlace.

Para aislar políticas y recursos entre clientes, equipos o entornos.

Lección 07 — EPG y contratos

Los endpoints se agrupan en EPG (grupos de endpoints) y la comunicación entre EPG distintos está denegada por defecto hasta que un EPG proveedor y otro consumidor se asocian mediante un contrato con asuntos y filtros que permiten los puertos y protocolos.

Es más seguro: todo está denegado por defecto y solo se permite lo necesario, con segmentación clara.

Lección 08 — Perfiles de aplicación

Un contenedor lógico dentro de un tenant que agrupa los EPG y contratos de una aplicación, reflejando su estructura (web, aplicación, base de datos) en la política de red en lugar de VLAN o subredes sueltas.

En el centrado en red se mapea una VLAN a un EPG (útil en migraciones); el centrado en aplicación segmenta por función de aplicación.

Lección 09 — Políticas de acceso

Mediante políticas de acceso: un perfil de interfaz y de switch seleccionan los puertos, un grupo de políticas de interfaz define su configuración, un AAEP lo enlaza a un dominio, y un conjunto de VLAN asociado a ese dominio permite usar esas VLAN en los EPG.

El EPG no podrá usar esa VLAN en el puerto y no habrá conectividad.

Lección 10 — Conexión externa con L3Out

Con un L3Out, que usa un protocolo de enrutamiento (OSPF, BGP, EIGRP o rutas estáticas) con routers externos mediante border leafs, y EPG externos (external EPG) con contratos que controlan el tráfico hacia y desde fuera.

Los EPG externos con sus subredes y los contratos que controlan el tráfico, además de las interfaces.

Módulo 3: Servicios e integración

Lección 11 — Service graph y PBR

Para insertar dispositivos de servicio como firewalls o balanceadores en el camino entre EPG mediante un contrato, de forma automatizada; con policy-based redirect (PBR) el tráfico se redirige al servicio sin depender del diseño de capa 3 o capa 2 entre los EPG.

Se inserta el firewall o balanceador de forma automatizada, sin rediseñar la topología.

Lección 12 — Integración con virtualización: VMM

Una integración del APIC con vCenter, Hyper-V, OpenStack o Kubernetes: el APIC crea grupos de puertos o redes en el hipervisor para cada EPG y aprende la ubicación de las VM, de modo que la política sigue a las cargas cuando se mueven.

La política sigue a la VM (por ejemplo con vMotion) sin reconfigurar la red.

Lección 13 — Multi-Pod

Una sola fabric ACI repartida en varios pods (por ejemplo salas o edificios cercanos) interconectados por una red entre pods (IPN) que usa OSPF, multicast y retransmisión DHCP, gestionados por un único clúster APIC.

Cuando los pods están cerca, con baja latencia y se acepta un único clúster APIC y dominio administrativo.

Lección 14 — Multi-Site

Una interconexión de varias fabrics ACI independientes, cada una con su clúster APIC, gestionadas con una herramienta de orquestación central (Nexus Dashboard Orchestrator) que define políticas y esquemas coherentes entre sitios, con dominios de fallo separados.

Un fallo en un sitio no afecta a los demás, mejorando la resiliencia y la recuperación ante desastres.

Lección 15 — Microsegmentación

Agrupar endpoints en EPG de microsegmentación (uSeg) según atributos como nombre de VM, sistema operativo, IP o MAC, en lugar de por puerto o VLAN, para aplicar políticas más finas dentro de la misma red.

Para aplicar políticas finas y limitar el movimiento lateral de amenazas dentro de la misma red.

Módulo 4: Operación y seguridad

Lección 16 — Automatización: API REST, Ansible y Terraform

Con la API REST del APIC (JSON o XML) sobre el modelo de objetos, con módulos de Ansible, el proveedor de Terraform y SDKs como cobra o la herramienta Postman, de modo que tenants, EPG y contratos se definen como código.

Es versionable y repetible, con revisión de cambios y entornos idénticos.

Lección 17 — Monitorización y resolución de problemas

Con los fallos (faults) y eventos del APIC, el health score de objetos y nodos, las estadísticas, los contadores atómicos, la herramienta de traza de endpoints, el visor de objetos (Visore) y comandos en los switches para comprobar la política y los contratos aplicados.

Que estén en EPG con un contrato adecuado, que la VLAN, el AAEP y el dominio estén bien y que el endpoint se haya aprendido.

Lección 18 — Actualizaciones y copias de configuración

Con grupos de actualización de firmware gestionados desde el APIC: se sube la imagen, se actualiza primero el clúster APIC y después los switches por grupos (por ejemplo, un grupo de spines y otro de leafs) en ventanas, tras hacer una instantánea de configuración.

Para mantener redundancia sin interrumpir el servicio y reducir el riesgo.

Lección 19 — Seguridad de gestión y RBAC

Con control de acceso basado en roles (RBAC), dominios de seguridad que limitan qué tenants ve cada usuario, autenticación externa (LDAP, RADIUS, TACACS+ o SAML) y registro de cambios en las auditorías.

Centraliza altas y bajas con el directorio corporativo y mejora la auditoría.

Lección 20 — Proyecto final: fabric ACI para un centro de datos

Spine-leaf con pares de leafs y varios spines, clúster de tres APIC, tenants por entorno con VRF y bridge domains, EPG por aplicación con contratos de mínimo acceso, políticas de acceso con vPC, L3Out redundante en border leafs, integración VMM, servicios mediante service graph, automatización por API y monitorización.

Crear tenant o application profile, EPG y bridge domain, definir los contratos y las políticas de acceso necesarias y probar la conectividad.