

// Jivops

Tungsten Fabric

Guía completa — 20 lecciones

Fundamentos · Redes virtuales · Integración · Operación

Contenido

Módulo 1: Fundamentos y arquitectura

- Lección 01 — Qué es Tungsten Fabric
- Lección 02 — Arquitectura y componentes
- Lección 03 — El vRouter
- Lección 04 — Plano de control: XMPP y BGP
- Lección 05 — Encapsulación del overlay

Módulo 2: Redes virtuales y servicios

- Lección 06 — Redes virtuales y subredes
- Lección 07 — Políticas de red y grupos de seguridad
- Lección 08 — IP flotantes y NAT
- Lección 09 — Encadenamiento de servicios
- Lección 10 — Conectividad externa y SDN gateway

Módulo 3: Integración y rendimiento

- Lección 11 — Integración con OpenStack
- Lección 12 — Integración con Kubernetes
- Lección 13 — Despliegue
- Lección 14 — Multitenencia y RBAC
- Lección 15 — Rendimiento: DPDK y SmartNIC

Módulo 4: Operación

- Lección 16 — Analítica y observabilidad
- Lección 17 — Resolución de problemas
- Lección 18 — Alta disponibilidad y escalado
- Lección 19 — Copias de seguridad y actualización
- Lección 20 — Proyecto final: nube privada con Tungsten Fabric

Módulo 1: Fundamentos y arquitectura

Lección 01 — Qué es Tungsten Fabric

Una plataforma SDN de código abierto (antes OpenContrail, impulsada por la Linux Foundation) que crea redes virtuales superpuestas (overlay) sobre cualquier red física, con un controlador centralizado y un vRouter en cada host, integrándose con OpenStack, Kubernetes y otros orquestadores.

Es independiente de la red física, automatizable y permite aislar redes virtuales por inquilino.

Lección 02 — Arquitectura y componentes

Nodos de configuración (API y esquema), nodos de control (hablan XMPP con los agentes y BGP con otros controladores y routers), nodos de analítica (recogen eventos, métricas y flujos) y el vRouter con su agente en cada host de cómputo, además de bases de datos y colas de mensajes.

La configuración expone la API y guarda el modelo de red; el control distribuye rutas y políticas a los vRouters.

Lección 03 — El vRouter

Un módulo de reenvío (en el kernel, en DPDK o en una SmartNIC) que sustituye al switch virtual del host: encapsula y desencapsula el tráfico del overlay, aplica políticas y grupos de seguridad, y es programado por un agente que habla con el controlador.

Es distribuido: no hay un punto central que limite el tráfico este-oeste y escala con los hosts.

Lección 04 — Plano de control: XMPP y BGP

Cada agente se comunica con los nodos de control mediante XMPP para intercambiar rutas y políticas de los workloads; los controladores se hablan entre sí y con routers físicos mediante BGP, usando familias como EVPN y L3VPN.

Para intercambiar rutas con gateways y routers físicos, y así dar conectividad externa e interoperar.

Lección 05 — Encapsulación del overlay

MPLS sobre UDP (la habitual), MPLS sobre GRE y VXLAN, que envuelven los paquetes de las redes virtuales para transportarlos sobre la red física de capa 3 entre los vRouters, con identificadores que separan cada red virtual.

Evita depender de VLAN y STP físicos, escala mejor y aprovecha ECMP en la red subyacente.

Módulo 2: Redes virtuales y servicios

Lección 06 — Redes virtuales y subredes

Un dominio de comunicación lógico aislado, con una o varias subredes (IPAM), al que se conectan interfaces virtuales de VM o pods; por defecto solo se comunican las interfaces de la misma red, y hay que habilitar políticas para conectar redes distintas.

Da seguridad y segmentación: cada red solo se comunica si se permite expresamente.

Lección 07 — Políticas de red y grupos de seguridad

Con políticas de red entre redes virtuales (permiten tráfico entre redes con reglas de protocolo y puerto) y con grupos de seguridad aplicados a las interfaces, que filtran en el vRouter de forma distribuida y con estado.

Es distribuido y cerca del workload, sin cuello de botella ni desvío del tráfico.

Lección 08 — IP flotantes y NAT

Para dar acceso externo a una interfaz virtual asociándole una IP de una red externa (pool de IP flotantes) mediante NAT uno a uno, de modo que la carga es accesible desde fuera sin cambiar su IP interna.

Para publicar un servicio y darle acceso externo o desde internet sin cambiar su IP interna.

Lección 09 — Encadenamiento de servicios

Insertar funciones de red virtuales (firewalls, balanceadores, IDS) en el camino entre dos redes mediante una política con instancias de servicio, de modo que el tráfico pasa por la cadena de forma transparente.

Es flexible y automatizado: se cambia el camino sin tocar el cableado.

Lección 10 — Conectividad externa y SDN gateway

Mediante un SDN gateway (un router físico compatible, como un Juniper MX o un router software) que establece BGP con los controladores y traduce entre el overlay y las VRF o redes físicas, usando EVPN o L3VPN.

BGP, con familias como EVPN o L3VPN para intercambiar rutas.

Módulo 3: Integración y rendimiento

Lección 11 — Integración con OpenStack

Mediante un plugin de Neutron que traduce las peticiones de redes, subredes, puertos, grupos de seguridad y routers del cloud al modelo de Tungsten Fabric, y el vRouter sustituye a Open vSwitch en los hosts de Nova.

Es transparente: las herramientas y scripts de OpenStack siguen funcionando sin cambios.

Lección 12 — Integración con Kubernetes

Con un plugin CNI en cada nodo que conecta los pods al vRouter y un gestor que traduce objetos de Kubernetes (namespaces, servicios, network policies) en redes virtuales y políticas de Tungsten Fabric, con IP por pod y aislamiento.

Conectividad y políticas unificadas entre VM y pods, sin gateways intermedios.

Lección 13 — Despliegue

Con herramientas de automatización como el operador de Kubernetes, Helm o el deployer de Ansible, que instalan los nodos de configuración, control, analítica y los vRouters en contenedores, con definición de un archivo de instancias y parámetros.

La alta disponibilidad (por ejemplo tres nodos de control), la red subyacente y el dimensionamiento.

Lección 14 — Multitenencia y RBAC

Con proyectos (tenants) integrados con Keystone u otra identidad, que aíslan redes y políticas, con control de acceso basado en roles y cuotas, de modo que cada equipo gestiona solo sus recursos.

Da aislamiento y seguridad entre equipos, con responsabilidad y cuotas por proyecto.

Lección 15 — Rendimiento: DPDK y SmartNIC

Ejecutándolo en modo DPDK en espacio de usuario con núcleos dedicados y hugepages, o descargándolo en una SmartNIC, para aumentar el caudal de paquetes y reducir la latencia frente al vRouter en el kernel.

Núcleos de CPU dedicados y memoria hugepages.

Módulo 4: Operación

Lección 16 — Analítica y observabilidad

Recoge eventos, logs, estadísticas de interfaces y de flujos y el estado de los nodos mediante el protocolo Sandesh, los guarda en una base y los expone por API y por la interfaz web, además de poder integrarse con sistemas externos de métricas.

Para ver el tráfico real entre redes, diagnosticar problemas y detectar patrones o amenazas.

Lección 17 — Resolución de problemas

Que estén en la misma red virtual o con una política entre redes, los grupos de seguridad, que las interfaces estén activas en el vRouter y sus rutas aprendidas del controlador, que la sesión XMPP esté arriba y la conectividad de la red subyacente entre hosts.

La interfaz web, los comandos del vRouter (vif, rt, flow) y las páginas introspect de los servicios.

Lección 18 — Alta disponibilidad y escalado

Con varios nodos de configuración, control y analítica (normalmente tres) detrás de balanceadores, bases de datos y colas replicadas, sesiones XMPP del agente con dos controladores, y gateways redundantes; se escala añadiendo nodos.

Los agentes usan el otro controlador y el plano de datos sigue funcionando sin perder tráfico.

Lección 19 — Copias de seguridad y actualización

Haciendo copia de las bases de datos de configuración y de la definición de despliegue, probando la restauración, y actualizando por fases con un orden definido (nodos de control y configuración, luego vRouters) en una ventana, tras probar en un entorno previo.

Para reducir el riesgo y mantener el servicio, comprobando la compatibilidad y con posibilidad de volver atrás.

Lección 20 — Proyecto final: nube privada con Tungsten Fabric

Red subyacente leaf-spine de capa 3, tres nodos de configuración, control y analítica, vRouter en cada host (DPDK donde haga falta), proyectos con aislamiento y RBAC, políticas y grupos de seguridad, SDN gateway redundante con BGP, integración con Neutron y CNI, analítica, copias y actualizaciones por fases.

Crear el proyecto, las redes virtuales y subredes, las políticas y grupos de seguridad, y las IP flotantes si hace falta acceso externo.