Getting Started with Cisco Virtual Topology System

This chapter provides an overview of Cisco Virtual Topology System (VTS). It also provides a high level workflow of the tasks that you need to perform after you install Cisco VTS.

- Understanding Cisco VTS, page 1
- Cisco VTS Architecture Overview, page 2
- Cisco Virtual Topology Forwarder, page 3
- Virtual Topology System High Availability, page 3
- Logging in, page 4
- Initial Configuration Tasks, page 4
- Creating the VMware vSphere Distributed Switch (VDS), page 7

Understanding Cisco VTS

The Cisco Virtual Topology System (VTS) is a standards-based, open, overlay management and provisioning system for data center networks. It automates fabric provisioning for both physical and virtual workloads. Cisco VTS provides a network virtualization architecture and software-defined networking (SDN) framework that meets the requirements of multitenant data centers for cloud services. It automates overlay provisioning on network infrastructure and abstracts out the complexity involved in managing heterogeneous network environments.

Cisco VTS supports scalable deployment of multitenanted network services. It enables a policy-based approach for overlay provisioning.

Cisco VTS automates complex network overlay provisioning and management tasks through integration with cloud orchestration systems such as OpenStack and VMware vCenter. The solution can be managed from the embedded Cisco VTS GUI or entirely by a set of northbound Representational State Transfer (REST) APIs that can be consumed by orchestration and cloud management systems.

Cisco VTS supports:

- Fabric automation
• Programmability
• Open, scalable, standards based solution
• Cisco Nexus 5000, 7000, and 9000 Series Switches. For more information, see Supported Platforms in Cisco VTS 2.0 Installation Guide.
• Software forwarder (Virtual Topology Forwarder [VTF])

Cisco VTS Architecture Overview

Cisco VTS architecture has two main components: the Policy Plane and the Control Plane. These perform core functions such as SDN control, resource allocation, and core management function.

Figure 1: Cisco VTS Architecture

- **Policy Plane**: The policy plane enables Cisco VTS to implement a declarative policy model designed to capture user intent and render it into specific device-level constructs. The solution exposes a set of modular policy constructs that can be flexibly organized into user-defined services for use cases across service provider and cloud environments. These policy constructs are exposed through a set of REST APIs that can be consumed by orchestrators and applications to express user intent, or instantiated through the Cisco VTS GUI. Policy models are exposed as system policies or service policies.
System policies allow administrators to logically group devices into pods within or across data centers to define Admin Domains with common system parameters (for example, BGP-EVPN control plane with distributed Layer 2 and 3 gateways).

The inventory module maintains a database of the available physical entities (for example, data center interconnect [DCI] routers and top-of-rack leaf, spine, and border-leaf switches) and virtual entities (for example, VTFs) in the Virtual Topology System domain. The database also includes interconnections between these entities and details about all services instantiated within a Virtual Topology System domain.

The resource management module manages all available resource pools in the Virtual Topology System domain, including VLANs, VXLAN Network Identifiers (VNIs), IP addresses, and multicast groups.

• Control Plane: The control plane module serves as the SDN control subsystem that programs the various data planes including the VTFs residing on the x86 servers, hardware leafs, DCI gateways. The control plane hosts the Cisco IOS XRv Software instance that provides route peering capabilities between the DCI gateways or to a BGP route reflector. Cisco IOS XRv is the virtualized version of Cisco IOS XR Software. The control plane enables an MP-BGP EVPN-based control plane for VXLAN overlays originating from leafs or software VXLAN tunnel endpoints (VTEPs).

The device management module enables device configuration and management capabilities within Virtual Topology System, with multiprotocol support to support a multivendor environment.

Cisco Virtual Topology Forwarder

Cisco VTS can be deployed with a Virtual Topology Forwarder (VTF). VTF is a lightweight, multitenant software data plane designed for high performance packet processing on x86 servers. VTF uses Vector Packet Processing (VPP). VPP is a full-featured networking stack with a software forwarding engine. VTF leverages VPP technology and Intel Data Path Development Kit (DPDK) for high performance Layer 2 (L2), Layer 3 (L3), and VXLAN packet forwarding. VTF is multithreaded, and you can allocate additional CPU cores to scale its performance.

VTF allows Cisco VTS to terminate VXLAN tunnels on host servers by using the VTF as a Software VXLAN Tunnel Endpoint (VTEP). Cisco VTS also supports hybrid overlays by stitching together physical and virtual endpoints into a single VXLAN segment.

VTF is deployed as a virtual machine to deliver a high-performance software data plane on a host server.

Virtual Topology System High Availability

The Virtual Topology System solution is designed to support redundancy, with two solution instances running on separate hosts in an active-standby configuration.

During initial setup, each instance is configured with both an underlay IP address and a virtual IP address. Virtual Router Redundancy Protocol (VRRP) is used between the instances to determine which instance is active.

The active-instance data is synchronized with the standby instance after each transaction to help ensure consistency of the control-plane information to accelerate failover after a failure. BGP peering is established from both Virtual Topology System instances for the distribution of tenant-specific routes. During the switchover, nonstop forwarding (NSF) and graceful restart help ensure that services are not disrupted.
See the *Configuring High Availability* section of the *Cisco VTS 2.0 Installation Guide* for the detailed procedure about setting up high availability.

## Logging in

To log in to the Cisco VTS GUI:

### Step 1
Open a supported browser, and enter the url of the server. For example: https://<IP Address>:8443/VTS. Cisco VTS supports Google Chrome and Mozilla Firefox browsers. Cisco VTS 2.0 has been tested on Google Chrome version 46.0.2490.71 and Mozilla Firefox version 41.0.2.

### Step 2
Enter the username and password, and click **Login**. The default username/password is admin/admin. The Cisco VTS homepage appears. You will be required to change the password for the admin account the first time you are logging in.

**Note**
- To change your password subsequently, click **Change Password** on the top right settings button.
- Enter **New Password** and **Confirm New Password** and then click **Change Password**.

## Initial Configuration Tasks

After bringing up the Virtual Topology Controller (VTC) Virtual Machine (VM), do the following:

**Note**
Before you perform the tasks below, ensure that installation is complete, day zero configuration on leafs is done, and all underlay configurations are working.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
<th>Navigation in VTS GUI / User Guide Section</th>
<th>Additional Notes</th>
</tr>
</thead>
</table>
| 1        | Create an Authorization Group | Inventory > Authorization Group  
For more information about creating authorization group, see Managing Users and Groups | This will have credentials for logging into your devices. You can create as many auth groups as necessary. |
<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
<th>Navigation in VTS GUI / User Guide Section</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Discover the Topology of all the leafs, spine, border-leafs, and DCI</td>
<td>Discovery &gt; Topology Discovery&lt;br&gt;For more information about adding devices and host information, see Performing Auto Discovery</td>
<td>VTFs and IOS XRv are not detected in topology discovery.</td>
</tr>
<tr>
<td>3</td>
<td>Import the devices after adding the auth group</td>
<td>Inventory &gt; Import Inventory&lt;br&gt;For more information about adding devices and host information, see Importing Inventory</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Add the Domain ID, DHCP Server IP, and Anycast Gateway MAC</td>
<td>Administration &gt; System Settings&lt;br&gt;For more information about adding devices and host information, see Administering Cisco VTS.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Perform IOS XRv and VTF Registration. <strong>Note</strong> This step is required only if you have a VTF-based deployment.</td>
<td>See the Installing the Virtual Topology Forwarder section in the Cisco VTS 2.0 Installation Guide.</td>
<td>IOS XRv takes a few minutes to boot. Register the VTF only after you see the VFG group on the GUI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To verify that the VFG group is created, go to Inventory &gt; Virtual Forwarding Groups.</td>
</tr>
<tr>
<td>6</td>
<td>Login into the IOS XRv and verify that the network-controller config is pushed. <strong>Note</strong> This step is required only if you have a VTF-based deployment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sequence</td>
<td>Task</td>
<td>Navigation in VTS GUI / User Guide Section</td>
<td>Additional Notes</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-------------------------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 7        | Update the BGP ASN information for the devices | Inventory > Network Inventory  
For more information, see Viewing Network Inventory. | |
|          | Create resource pools | • Resource Pools > Global VNI Pool  
• Resource Pools > Device Specific VLAN Pools  
• Resource Pools > Multicast IP Pool  
For more information about creating an admin domain, see Managing Resource Pools | |
| 8        | Create an Admin Domain | Admin Domains > Domains  
For more information about creating an admin domain, see Creating and Managing Admin Domains | Properties for the L2/L3 Gateway Group are as follows:  
• Control Protocol: BGP-EVPN  
• Replication Modes: Multicast and Ingress  
• Distribution Mode: Decentralized |
### Task Sequence

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
<th>Navigation in VTS GUI / User Guide Section</th>
<th>Additional Notes</th>
</tr>
</thead>
</table>
| 9        | Add the devices to the Gateway Group | Admin Domains > Domains  
For more information about creating an admin domain, see Creating and Managing Admin Domains | See the Supported Platforms section in the Cisco VTS 2.0 Installation Guide for details about devices support for different roles. |
| 10       | Add the ToR and IOS XRv to the L2 and L3 Gateway Group | Admin Domains > Domains  
For more information about creating an admin domain, see Creating and Managing Admin Domains | |
| 11       | Save the Admin Domain you created | Admin Domains > Domains  
For more information about creating an admin domain, see Creating and Managing Admin Domains | |

---

**Creating the VMware vSphere Distributed Switch (VDS)**

For every ToR in the inventory, you must create a VDS. All the hosts that are attached to the ToR should be attached to the VDS.

**For Non-VPC Specific Configuration**

If you are not using VPC on the leaves:

- Create one VDS switch per leaf (at least 2).
• Attach the hosts' data interface to the VDS uplinks.

Step 1: Login to the web client, and browse to Networking.
Step 2: Select Create Distributed Switch.
Step 3: Enter the name of the VDS, preferably same as that of the ToR to which this distributed switch will connect to.
Step 4: Choose the data center where this VDS will be created. Click Next.
Step 5: Select Distributed switch 5.5.0.
Step 6: Choose number of uplink port to be used for this VDS. Click Next.
   The Ready to complete screen appears with the settings.
Step 7: Review the details, and click Finish.
   New VDS will be created and will be available in VDS inventory of vCenter.
   Now, you need to add the hosts which are connected to the ToRs for which the VDS has been created. All hosts connected to the ToR should be added.
Step 8: Select the VDS created in previous step, and select the Hosts tab.
   There will be no host in this tab as you have just created the VDS.
Step 9: Select the VDS created in previous step, and select the Hosts tab.
Step 10: Click the Actions drop-down, then select Add and Manage Hosts.
   The Add and Manage Hosts window appears.
Step 11: Select the Add Host radio button.
Step 12: Click + to add hosts. A popup window appears with a list of hosts.
Step 13: Select the hosts which are connected to the VDS ToR. Click OK.
   This will add selected hosts. The newly added hosts are listed in the Select hosts window.
Step 14: Click Next.
   The Select network adapter tasks window appears.
Step 15: Unselect Manage VMkernel adaptors, and click Next.
   The Manage physical network adapter window appears. This page allows you to add uplink for the selected host.
Step 16: Select the port, and click Assign uplink.
   You may have more than one uplink if two ports of the host are connected to the ToR.
Step 17: Select all up link ports, click Next, and then click Finish.

For VPC Specific Configuration

If you are using VPC on the leaves:

Step 1: Create one VDS switch per VPC pair.
Step 2: Enable enhanced LACP.
1. In the vSphere Web Client, navigate to the Distributed Switch.
2. In Features, click Enhance next to Link Aggregation Control Protocol.
3. In the Validate prerequisites page, click Next.
4. Click Finish.

**Step 3**

Create a Link Aggregation Group for each VDS.

1. Click the Networking view.
2. Expand Datacenter.
3. Select the Distributed Switch.
4. Click the Manage tab and click Settings.
5. In the LACP section, click the + symbol to create a new LAG.
6. Give the new LAG a name.
7. Select the number of ports desired. Later you will connect a physical network adapter to each port.
8. Choose the LACP mode you want to use from the dropdown list. Choose Active or Passive.
10. Click OK.
11. Reassign network adapters from the available uplink adapters to the new LAG.
   
   - Move the new link aggregation group to Standby state for the distributed portgroups where you want to use LACP.
   - Use the add and manage hosts wizard in template mode to migrate physical uplinks to the LAG on multiple hosts simultaneously: Reassign uplinks on template host, then apply configuration to the desired hosts.
   - Set the LAG to the active state for the desired portgroups by moving it to the active class, then moving individual unassociated uplinks to the unused class (leaving the standby class empty).

**Step 4**

You may remove the default port group that gets created as it will not be used.