

Validated Solution Guide

Aruba Solution TME

May 28, 2025

Table of Contents

ESP Data Center Deploy Guide	5
Document Conventions	5
Data Center Introduction	6
Overview	6
EVPN-VXLAN Deployment Overview	7
Layer 2 Two-Tier Deployment Overview	7
Purpose of this Guide	7
Customer Use Cases	8
Fabric Composer EVPN-VXLAN Fabric	9
Initialize Fabric Components	10
Switch Installation	10
Physical Cabling	13
Out-of-Band Management	14
Switch Initialization	15
Download HPE Aruba Networking Fabric Composer	17
Install HPE Aruba Networking Fabric Composer	18
Download AMD Pensando Policy and Services Manager	29
Install AMD Pensando Policy and Services Manager	29
Configure the AMD PSM Cluster	31
EVPN-VXLAN Configuration	36
Physical Topology Overview	36
HPE Aruba Networking Fabric Composer Process	36
Plan the Deployment	37
HPE Aruba Networking Fabric Composer Prerequisites	41
Fabric Initialization	41
Host Port Configuration	20
Configure the Border Leaf	39
Configure Overlav Test Loophacks	90
Configure Overlay IP Multicast	210
VMWare vSphere Integration 2	223
Secure an Aruba EVPN Fabric 2	30
Overview 2	30
Configure PSM Integration with Aruba Fabric Composer 2	30
Configure Macro Firewall Policy	25
	.55
Verify Policy in PSM	.94
AFC Multifabric Configuration 2	88
Second Fabric Guidance	88
Configure Multifabric Underlay Connectivity	90
Configure Overlay Control Plane	04

Aruba Central Two-Tier Data Center	333
Overview	333
Planning the Deployment	334
Prepare Switches	337
Switch Installation	337
Physical Cabling	339
Management	340
Aruba Central Initial Configuration	342
	342
Configure Core Switch Group Settings	345
Configure Group VLANs	353
Clone Core Group for Access Switches	354
Assign Switches to a Group	355
Configure Switch Hostname	356
Configure Data Center Site	362
Verify Data Center Cabling	366
Two-Tier Core	372
Configure Core VSX ISL Interface	372
	375
	377
	270
	200
	380
Configure Core Switch MC-LAGS	381
Configure Routing Services	382
Two-Tier Multicast	387
Verify Operational State	388
Two-Tier Server Access	396
Configure Access VSX ISL Interface	396
Spanning Tree	399
Enter MultiEdit Configuration	400
Configure Access Switch VSX Pairs	401
Configure Access to Core MC-LAGs	402
Configure Access Switch to Host MC-LAGS	402
	404
Configure Physical Port Speeds	405
	403
	-00
Ansible Two-Tier Data Center	413
Overview	413
Ansible Project Prerequisites	413
Ansible Project Structure	414
Two-Tier Data Center Topology	414
Ansible Two-Tier Inventory	417
YAMI Inventory File	⊿ 17
Dianning Inventory File Values	122
	477

Inventory Variable Reference	424
Ansible Two-Tier Template	433
Overview	433
Template Syntax	433
Run the Two-Tier Playbook	437
Run the Two-Tier Playbook Aruba Validated Hardware and Software	437 438
Run the Two-Tier Playbook Aruba Validated Hardware and Software EVPN-VXLAN Fabric	437 438 438

ESP Data Center Deploy Guide

This guide provides IT professionals with prescriptive steps to deploy a Data Center network using the following products, as outlined in the Design document:

- Aruba Fabric Composer
- Aruba CX 10000 Series
- Aruba CX 8300 Series
- Aruba CX 8400 Series
- VMWare vSphere

Document Conventions

Bold text indicates a command, navigational path, or a user interface element.

Examples:

- the **show vsx status** command
- Go to Configurations > Routing > VRF

Italic text indicates important terminology or a value that appears in a field on the user interface.

Examples:

- A *VXLAN Tunnel Endpoint (VTEP)* function within leaf switches manages the origination and termination of point-to-point tunnels forming an overlay network.
- Name: DB_NET_PROD_DC1

Shaded blocks indicate variables for which you should substitute a value appropriate for your environment.

Example:

• BGP router id: 10.0.5.1

NOTE:

For the most up-to-date information on ESP Data Center solutions, please refer to the Validated Solution Guide Program

Data Center Introduction

The HPE Aruba Networking data center uses technology and tools to transform the data center into a modern, agile, services delivery platform. Organizations of any size, distributed or centralized, can benefit from streamlined perfomance and improved network cost-effectiveness using HPE Aruba Networking data center products.

Overview

The HPE Aruba Networking AOS-CX operating system simplifies overall operations and maintenance using a common switch operating system across the campus, branch, and data center. The system can be managed in the cloud or on-premises and supports a comprehensive application programming interface (API). AOS-CX employs robust artificial intelligence functions that continually analyze and realign network flow to ensure that the system operates seamlessly in accordance with network management best practice, without requiring manual IT staff intervention.

The use of converged Ethernet has changed the way hosts access storage within the modern data center. Dedicated storage area networks are no longer required. Lossless Ethernet and bandwidth management protocols ensure timely reads and writes using a traditional IP LAN. The combined cost savings and operational simplicity are driving a major conversion to converged Ethernet.

At the same time, network topologies have become virtualized. Although virtualization delivers the flexibility required to meet the changing data center requirements, it can present complexity and challenges with implementation and management. An HPE Aruba Networking data center addresses these challenges by automating installation and implementation of the Aruba AOS-CX operating system, with features such as automated device group configuration, Zero Touch Provisioning, scheduled configuration backups, dashboard-ready network performance metrics, and built-in alerts for critical network functions.

Before designing a new or transformed data center, it is important to consider the organization's current and projected strategy for hosting and accessing applications from the cloud. Determine the applications that will remain on-premises so you can establish a data center with ample throughput and storage to meet requirements.

The HPE Aruba Networking CX 93xx, 83xx, CX 84xx, and CX 10000 switching platforms provide a best-inclass suite of products featuring a variety of high-throughput port configurations, industry-leading operating system modularity, real-time analytics, and "always up" performance.

This guide explores deploying HPE Aruba Networking switches to create a modern EVPN-VXLAN solution and a traditional Layer 2 two-tier architecture.

EVPN-VXLAN Deployment Overview

An EVPN-VXLAN architecture accommodates growth and provides network flexibility using a Layer 3 spine-and-leaf underlay with a software-defined fabric overlay. Spine switches provide connectivity between leaves, while data center hosts are attached to leaf switches. The EVPN-VXLAN fabric overlay simultaneously supports Layer 3 segmentation and Layer 2 adjacency between hosts anywhere in the data center using standards-based protocols. Reachability information between hosts is shared using BGP's L2VPN-EVPN address family. VXLAN encapsulation is used to forward traffic between overlay hosts using the Layer 3 underlay as a transport service.

The HPE Aruba Networking EVPN-VXLAN architecture provides the following benefits:

- A fault tolerant design that accommodates hardware failures at multiple levels.
- Easy incremental east-west capacity expansion by adding switches at the spine layer.
- Programmatic Layer 2 VLAN reachability across the data center.
- Programmatic expansion of Layer 3 segments supporting data center multitenancy.
- Inline policy enforcement using the Aruba CX 10000 switch.
- Microsegmentation of attached hypervisor VMs and containers.
- Switch upgrades without a service outage.
- Orchestrated configuration, management, and operations using HPE Aruba Networking Fabric Composer.

Layer 2 Two-Tier Deployment Overview

A Layer 2 two-tier architecture supports a resilient, high capacity data center design without the need for specialized knowledge in overlay protocols. Multi-chassis link aggregations (MC-LAGs) provide multiple Layer 2 redundant data paths between a collapsed data center core and access switches, and between access switches and their attached data center hosts.

The HPE Aruba Networking Layer 2 two-tier architecture provides the following benefits:

- A fault tolerant design that can accommodate hardware failures at multiple levels.
- Layer 2 VLAN reachability across the data center.
- Inline policy enforcement using the Aruba CX 10000 switch.
- Microsegmentation of attached hypervisor VMs and containers.
- Switch upgrades without a service outage.
- Simplified configuration, management, and operations using Aruba Central cloud-based controls.

Purpose of this Guide

This guide describes HPE Aruba Networking data center implementation procedures, with reference for architectural options and associated hardware and software components. It delivers best-practice recommendations for the following deployment models:

- A next generation spine-and-leaf data center fabric using VXLAN and BGP EVPN to take advantage of the orchestration capabilities of **HPE Aruba Networking Fabric Composer**.
- A traditional Layer two-tier data center configured via HPE Aruba Networking Central.
- An Ansible automated configuration via AOS-CX API for a traditional Layer 2 two-tier data center.

Refer to volume one of this VSG for additional design guidance: HPE Aruba Networking Data Center Design

This guide assumes the reader has an equivalent knowledge of an Aruba Certified Switching Associate.

Audience

This guide is written for IT professionals who need to deploy an Aruba Data Center Network. These IT professionals serve in a variety of roles:

- Systems engineers who require a standard set of procedures to implement network solutions
- Project managers who create statements of work for Aruba implementations
- Aruba partners who sell technology or create implementation documentation.

Customer Use Cases

Data center networks change rapidly. The most pressing challenge is maintaining operational stability and visibility for users while moving or upgrading computing and storage resources. In addition, data center teams must continue to support the rapid pace of DevOps environments and meet growing requirements to connect directly and continue operations within the public cloud infrastructure.

Within a rapidly changing landscape, it is critical that network and system engineers responsible for meeting data requirements have efficient tools to streamline and automate complex infrastructure configurations.

Fabric Composer EVPN-VXLAN Fabric

HPE Aruba Networking Fabric Composer automates initial provisioning, ongoing configuration, and management of an EVPN-VXLAN data denter fabric. Fabric Composer's Guided Setup process configures baseline switch features, underlay addressing and routing, and overlay control and data plane components.

Fabric Composer integration with VMware vCenter provides visibility, policy automation, and vCenter configuration of DVS and PVLAN policy components.

Fabric Composer enables flexible management of AMD Pensando's Policy and Services Manager (PSM) firewall policy for the CX 10000 and access control lists available on all switch models. The API-based integration with PSM and AOS-CX switches allows Fabric Composer to provide a single pane of glass for all network-based policy management.

Fabric Composer provides a wizard-based microsegmentation policy builder. The end result of its PSM, switch, and vCenter policy component automation is a model that enables systems administrators to dynamically add a VM to network policy enforcement in their own independent workflows using VM tags.

Additionally, Fabric Composer provides ongoing visibility into fabric components. Alerts and troubleshooting tools allow quick identification and resolution to failures in the EVPN-VXLAN fabric.

Initialize Fabric Components

The first step for deploying a data center is the physical installation of the switches and computing hosts.

Switch Installation

Verify the airflow configuration for the products to be installed to ensure that they support the cooling design for the data center. If required, an optional air duct kit is available for Aruba data center top-of-rack (ToR) switches to redirect hot air away from servers inside the rack.

Before installing switches, download the Aruba Installation Guide for the specific models. Review the Installation Guide before installing and deploying the switches. Carefully review requirements for power, cooling, and mounting to ensure that the data center environment is outfitted adequately for safe, secure operations.

Step 1 Open a web browser, navigate to the HPE Networking Support Portal, and login with using appropriate credentials.

Step 2 On the landing page, click Software and Documents Search panel.



Step 3 On the **Software & Documents** page, select the following filters. - **File Type:** *Document* - **Product:** *Aruba Switches* - **File Category:** *Installation Guide*

HPE GreenLake	
HPE Networ	king Support Portal
< Home	
Software and D	ocuments
Q Search files	
FILTERS	Showing 168 Results
File Type	
Document (168)	File Type: 🗅 Document 🛛 😣 Product: Aruba Switch
Product 🗘	
Aruba Switches (168)	9300 Installation and Getting
Software Group	Aruba Switches v

File Category

Installation Guide (168)

Step 4 Download the Installation Guide version for the switch model to be installed.

Step 5 Complete the physical installation of switches in the racks.

NOTE:

Spine switches can be installed centrally, in middle-of-row or end-of-row locations depending on cabling requirements and space availability. The key consideration is cable distance and the types of media used between leaf and spine switches. Leaf switches should be installed top-of-rack (ToR) in high-density environments or middle-of-row in low-density environments.

Physical Cabling

Consistent port selection across racks and in the spine switches increases the ease of configuration management, monitoring, reporting, and troubleshooting tasks in the data center.

Breakout cables are numbered consistently with their split port designation on the switch.

Document all connections.

Ensure that distance limitations are observed for your preferred host connection media and between switches.

Top of Rack Cabling

The illustrations below show the port configuration on two types of 48-port ToR switches. Redundant ToR switch pairs must be the same model.

Ports on an Aruba CX 8325-48Y8C:



Figure 1: 8325 ToR switch

Ports on an Aruba CX 10000-48Y6C:





In a redundant ToR configuration, the first two uplink ports should be allocated to interconnect redundant peers (ports 49-50 on 8325-48Y8C and 10000-48Y6C switches), which provides physical link redundancy and sufficient bandwidth to accommodate a spine uplink failure on one of the switches.

Two links between redundant peers are sufficient for most deployments, unless the design may result in high traffic utilization of the inter-switch links under normal operating conditions, such as when many hosts in a rack are single-homed to only one of the redundant switches.

Additional uplink ports should be allocated to connect spine switches (ports 51-56 on an 8325-48Y8C and ports 51-54 on a 10000-48Y6C).

The highest numbered non-uplink port should be reserved as the VSX keepalive link between a ToR redundant pair.

NOTE:

VSX automation in HPE Aruba Networking Fabric Composer requires a dedicated physical port or a loopback address for the VSX keepalive interface. The recommended configuration is a dedicated port.

Determine a consistent number of leaf-to-spine links required on each ToR to achieve the desired oversubscription ratio. The number of spine switches is equal to the number of per ToR links required.

Follow a similar approach when using lower density ToR designs. Before deploying ToR configurations that require server connectivity at multiple speeds, review the switch guide to determine if adjacent ports are affected.

Configuration steps for changing port speeds are covered later in this guide. Refer to the Data Center Reference Architecture section for guidance on port speed groups on different hardware platforms.

Spine-to-Leaf Cabling

The illustration below shows the port configuration on an 8325 32-port spine switch.





In a dual ToR configuration, a spine switch must be connected to each switch in the redundant ToR pair in each rack. A 32-port spine switch supports up to 16 racks in this design. Use the same port number on each spine switch to connect to the same leaf switch to simplify switch management and documentation. For example, assign port 1 of each spine switch to connect to the same leaf switch.

Border Leaf Cabling

In a VXLAN spine-and-leaf design, a pair of leaf switches serves as the single entry and exit point to the data center. This is called the border leaf, but it does not require dedication to only border leaf functions. It may provide services leaf functions and, in some cases, provide connectivity to directly attached data center workloads. Cabling the border leaf can vary among deployments, depending on how the external network is connected and if services such as firewalls and load balancers are connected.

After all switches are physically installed with appropriate power and networking connections, continue to the next procedure.

Out-of-Band Management

The use of a dedicated management LAN for the data center is strongly recommended.

A dedicated management LAN on separate physical infrastructure ensures reliable connectivity to data center infrastructure for automation, orchestration, and traditional management access. The management LAN provides connectivity to HPE Aruba Networking Fabric Composer, Aruba NetEdit, and AMD Pensando Policy and Services Manager (PSM) applications. Ensure that the host infrastructure needed for those applications also can be connected to the management LAN or is reachable from the management LAN.

Deploy management LAN switches top-of-rack with switch and host management ports connected. Plan for an IP subnet with enough capacity to support all management addresses in the data center. DNS and NTP services for the fabric should be reachable from the out-of-band management network.

Configuration steps for the management LAN are not covered in this guide.

Switch Initialization

Go to the HPE Networking Support Portal and download the AOS-CX Fundamentals Guide for the version of the operating system you plan to run using the steps noted above for "Switch Installation."

NOTE:

Refer to the operating system release notes and consult with an HPE Aruba Networking SE or TAC team member for assistance with determining and selecting the version.

The "Initial Configuration" section of each Fundamentals Guide presents detailed instructions for connecting to the switch console port. After connecting to the console port, follow the steps below.

Step 1 Enable power to the switch by connecting power cables to the switch power supplies.

Step 2 Login with the username admin and an empty password.

Step 3 Enter a new password for the admin account.

NOTE:

The "Initial Configuration" section of the Fundamentals Guide provides detailed instructions for logging into the switch the first time.

Step 4 Confirm that all CX 10000 switches in the fabric are running an AOS-CX version compatible with the Fabric Composer and PSM versions of a deployment. Table 2 in the Fabric Composer's Pensando PSM & AOS-CX 10000 Software Selection Guidance document provides a matrix for compatibility. This guide uses the following versions of firmware and software:

- AOS-CX: 10.13.1050
- HPE Aruba Networking Fabric Composer: 7.0.5
- **PSM:** *1.80.1-T-6*

Step 5 Confirm that all other switches are running AOS-CX 10.10 long-term stability release or AOS-CX 10.13+ for compatibility with Fabric Composer 7.0.5 used in this guide.

Step 6 If the switch was previously configured, reset it to the factory default configuration. Fabric Composer requires a factory default configuration for orchestration during the fabric configuration process.

```
8325# erase all zeroize
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
Continue (y/n)? y
```

Step 7 Configure 6300M VSF stacks using the Aruba AOS-CX VSF Guide.

NOTE:

VSF stacks should be configured on 6300 switches before making any other configuration changes after zeroization.

Step 8 Configure switch hostnames.

hostname RSVDC-FB1-LF1-1

NOTE:

It is important to use a canonical naming scheme to easily identify the function of each switch. The hostname scheme above uses *<physical location>-<fabric identifier>-<role and unique VSX pair identifier>-<VSX pair member id>* to identify the correct fabric and role when using Fabric Composer. When using this scheme for switches that are not in a VSX pair, the number in the role field is sufficient for unique identification (i.e., RSVDC-FB1-SP1).

Step 9 Configure the Switch Management Interface. By default, the management interface uses DHCP for its configuration. DHCP reservations can be used to assign a consistent IP address, default gateway, and nameserver. Static IP configuration eliminates dependence on DHCP service availability.

```
interface mgmt
    no shutdown
    ip static 172.16.116.101/24
    default-gateway 172.16.116.1
    nameserver 172.16.1.98
```

NOTE:

Based on the existing IP address management process, determine a subnet to be used for the management LAN, where out-of-band (OOB) management ports on your switches are connected. Aruba Fabric Composer must be reachable from this network. The "Initial Configuration" section of the Fundamentals Guide provides detailed instructions for configuring the management interface.

Step 10 When spines use breakout cabling, configure split ports with the appropriate number of child interfaces and connection speeds, then confirm the operational port change.

```
interface 1/1/1-1/1/3
split 2 100g
```

RSVDC-FB1-SP1(config)# interface 1/1/1-1/1/3 RSVDC-FB1-SP1(config-if-<1/1/1-1/1/3>)# split 2 100g This command will disable the specified port, clear its configuration, and split it into multiple interfaces.

Continue (y/n)? y RSVDC-FB1-SP1(config-if-<1/1/1-1/1/3>)#

NOTE:

Typically, a spine uses a consistent split port strategy. An interface range is used to assign the same split configuration to multiple ports. The **confirm** parameter in the split configuration statement disables the operational warning. For example, **split 2 100g confirm**. Split interfaces also can be configured in HPE Aruba Networking Fabric Composer.

Download HPE Aruba Networking Fabric Composer

Step 1 Navigate to the HPE Networking Support Portal.

Step 2 Click the Software and Documents pane.

Step 3 In the File Type filter, select Software.

Step 4 In the Product filter, select "Aruba Fabric Composer", and click Apply.

Step 5 In the search results, select the appropriate OVA version and download it to your computer. This guide uses Fabric Composer 7.0.5.

Step 6 In the File Type filter, uncheck Software, then select Documents.

Step 7 Type release notes in the Search Files bar.

Step 8 Click on the HPE Aruba Networking Fabric Composer release notes for the version of software downloaded. The download link on the resulting page forwards the browser to Fabric Composer's online help, install guide, and compatibility matrix. Review the installation considerations in the **Install Guide** to ensure that adequate host resources are available.

NOTE:

HPE Aruba Networking Fabric Composer is provided in ISO format for installation using other hypervisors. High availability Fabric Composer clusters are only supported when using an ISO image.

Install HPE Aruba Networking Fabric Composer

Install Fabric Composer using the best process for your organization. The following process installs the Fabric Composer OVA using VMware vCenter.

Step 1 In the **Hosts and Clusters** tab, right click on the location to install Fabric Composer and select **Deploy OVF Template...** to launch the installation wizard.

vm	vSphe	ere Clien	ıt	Menu 🗸	Q
Ē.			<u> </u>	🗊 Sol	ution
~ 🗗 v⊂	enter.ora Roseville	inge-tme.	com	Summary	Мо
~[🗍 Solutir	Action	ns - Soluti	ons TME	
	🗍 rsv	🚹 Add	Hosts		
		🔁 New	Virtual I	Machine	
		🏷 New	Resourc	e Pool	
		🗊 Depl	oy OVF	Template	
	רא ר <u>ה</u> ר	🔠 New	vApp		

Step 2 On the **Select an OVF template** page, click **Local file**, choose the downloaded AFC OVA file, and click **NEXT**.



Step 3 On the **Select a name and folder** page, enter a virtual machine name, select a target folder for the installation, and click **NEXT**.

2 Select an OVF template	Select a name and folder		
3 Select a riane and rolder 3 Select a compute resource 4 Review details 5 Select storage	Virtual machine name:rsvdc-afc-01		
6 Ready to complete	Select a location for the virtual machine.		
	 vCenter.orange-tme.com Roseville Backend Clone and Template Machines Discovered virtual machine Home Lab Management Workstations Templates Test Clients Unit Under Test 		

Step 4 On the Select a compute resource page, select a cluster or cluster member and click NEXT.

2 Select a name and folder	Select a compute resource Select the destination compute resource for this operation
3 Select a compute resourc 4 Review details	V IR Roseville
5 Select storage	✓ 🗍 Solutions TME
6 Ready to complete	rsvbe-esx-1.orange-tme.com
	rsvbe-esx-2.orange-tme.com
	Compatibility
	✓ Compatibility checks succeeded.

Step 5 On the **Review details** page, read the information presented and click **NEXT**.

 Select an OVF template Select a name and folder Select a compute resource 	Review details Verify the templa	te details.
4 Review details 5 License agreements 6 Select storage	The OVF p risk. Review configuration	ackage contains advanced configuration options, which might pose a security v the advanced configuration options below. Click next to accept the advanced on options.
8 Customize template	Publisher	No certificate present
9 Ready to complete	Product	Aruba Fabric Composer
	Version	7.0.5-14110
	Vendor	Aruba, a Hewlett Packard Enterprise company
	Description	Aruba Fabric Composer Virtual Appliance. The Virtual Appliance consists of a single VM called Aruba Fabric Composer.
	Download size	941.0 MB
	Size on disk	2.2 GB (thin provisioned)
		100,0 GB (thick provisioned)
	Extra configuration	virtualhw.productcompatibility = hosted

Step 6 On the **License agreements** page, read the license agreement, select **I accept all license agreements**, and then click **NEXT**.

License agreements The end-user license agreement must be accepted.				
Read and accept the terms for the license agreement.				
exist. Modifications to the Agreement will be made only through a written amendment	*			
signed by both parties. If HPE doesn't exercise its rights under this Agreement, such delay				
is not a waiver of its rights.				
16. Australian Consumers. If you acquired the software as a consumer within the meaning				
of the 'Australian Consumer Law' under the				
Australian Competition and Consumer Act 2010 (Cth) then despite any other provision of				
this Agreement, the terms at this URL apply: http://www.hpe.com/software/SWLicensing.				
17. Russian Consumers. If you are based in the Russian Federation and the rights to use the				
software are provided to you under a				
separate license and/or sublicense agreement concluded between you and a duly				
authorized HPE partner, then this Agreement shall not be applicable.				
	•			
✓ Laccept all license agreements.				
CANCEL BACK NEX	кт			
	 Read and accept the terms for the license agreement. exist. Modifications to the Agreement will be made only through a written amendment signed by both parties. If HPE doesn't exercise its rights under this Agreement, such delay is not a waiver of its rights. 16. Australian Consumers. If you acquired the software as a consumer within the meaning of the 'Australian Consumer Law' under the Australian Competition and Consumer Act 2010 (Cth) then despite any other provision of this Agreement, the terms at this URL apply: http://www.hpe.com/software/SWLicensing. 17. Russian Consumers. If you are based in the Russian Federation and the rights to use the software are provided to you under a separate license and/or sublicense agreement concluded between you and a duly authorized HPE partner, then this Agreement shall not be applicable. I accept all license agreements. 			

Step 7 On the **Select storage** page, select the preferred provisioning method and storag volume, then click **NEXT**.

1 Select an OVF template	Select storage					
2 Select a name and folder	Select the storage for	the configuration and dis	sk files			
3 Select a compute resource						
4 Review details	Encrypt this virtual	machine (Requires Key I	Management Serve			
5 License agreements 6 Select storage	Select virtual disk form	at:	Thin Provision	· · · · · · · · · · · · · · · · · · ·	~	
7 Select networks	VM Storage Policy:		Da	atastore Defau	ilt	×
8 Customize template	Name	Capacity	Provisioned	Free	Туре	
9 Ready to complete	🗐 υυτ	10 TB	1.08 TB	9.41 TB	VMFS 6	
	4				,	
	< Compatibility				,	
	 Compatibility ✓ Compatibility che 	cks succeeded.			,	
	 Compatibility ✓ Compatibility che 	cks succeeded.			,	

Step 8 On the **Select networks** page, select a VM Network with connectivity to the data center out-ofband netowkr and click **NEXT**.

 1 Select an OVF template 2 Select a name and folder 	Select networks Select a destination network for each source network.					
3 Select a compute resource 4 Review details	Source Network	Ŧ	Destination Network			
5 License agreements	VM Network		BACKEND	~	4	
6 Select storage				1 iten	is	
8 Customize template 9 Ready to complete	IP Allocation Settings					
	IP allocation:	Sta	atic - Manual			
	IP protocol;	IP۱	/4			

Step 9 On the Customize template page, enter values for the following fields and click Next.

(A) Network - General settings - (1) Hostname: rsvdc-afc-01 - (2) Domain Name: example.local - (3) Primary NTP Server: 172.16.1.99 - (4) Secondary NTP Server: 172.16.1.98

(B) Network - Static IP settings - (1) IP Address: 172.16.1.50 - (2) Network Mask: 255.255.255.0 - (3) Default Gateway: 172.16.1.1 - (4) Primary Name Server: 172.16.1.99 - (5) Secondary Name Server: 172.16.1.98

(D) Linux Password - Password: <password> - Confirm Password: <password>

NOTE:

Check **Use DHCP** when dynamic addressing is preferred over static IP assignment.

4 Review details 5 License agreements 6 Select storage 7 Select networks 8 Customize template 9 Ready to complete	All properties have valid values (A) Network - General settings (1) Hostname (2) Domain Name	A settings (Short) host name to assign to this VM. For static IP addresses, this name must resolve to the IP address on your DNS server. rsvdc-afc-01
6 Select storage 7 Select networks 8 Customize template 9 Ready to complete	 (A) Network - General settings (1) Hostname (2) Domain Name 	4 settings (Short) host name to assign to this VM. For static IP addresses, this name must resolve to the IP address on your DNS server. rsvdc-afc-01
8 Customize template 9 Ready to complete	(1) Hostname (2) Domain Name	(Short) host name to assign to this VM. For static IP addresses, this name must resolve to the IP address on your DNS server. rsvdc-afc-01
	(2) Domain Name	
		Domain name to assign to this VM. For static IP addresses, this domain must resolve on your DNS server.
	(3) Primary NTP Server	Hostname or IP address of primary NTP server. Leave blank if not using or if NTP servers are provided by DHCP. 172.16.1.99
	(4) Secondary NTP Server	Hostname or IP address of secondary NTP server.
	 (B) Network - Static IP settings 	5 settings
	(1) IP Address	Static IP address to assign for this interface. (Note: For all IP address fields, specify as "0.0.0.0" to use DHCP) 172.16.1.50
	(2) Network Mask	Network mask for this interface. 255.255.255.0
	(3) Default Gateway	Default gateway for this interface.
	(4) Primary Name Server	Primary DNS name server IP address.
	(5) Secondary Name Server	Secondary DNS name server IP address. 172.16.1.98
	 (C) Network - DHCP settings 	1 settings
	Use DHCP	Check to use DHCP to obtain an IP address.
	 (D) Linux Password 	1 settings
	Linux admin Password	Set the Linux admin user account password.
		Password ······ ··· ··· ··· ··· ··· ··· ··· ··

Step 10 On the Ready to complete page, click FINISH.

1 Select an OVF template 2 Select a name and folder	Ready to complete Click Finish to start	creation.		
4 Review details				
5 License agreements	Provisioning type	Deploy from template		
6 Select storage	Name	rsvdc-afc-01		
7 Select networks 8 Customize template	Template name	ArubaFabricComposer-7.0.5-14110		
9 Ready to complete	Download size	941.0 MB		
	Size on disk	2.2 GB		
	Folder	Unit Under Test		
	Resource	Solutions TME		
	Storage mapping	1		
	All disks	Datastore: UUT; Format: Thin provision		
	Network mapping	1		
	VM Network	BACKEND		
	IP allocation settings			
	IP protocol	IPV4		
	IP allocation	Static - Manual		
	Properties	 Hostname = rsvdc-afc-01 Domain Name = example.local Primary NTP Server = 172.16.1.99 Secondary NTP Server = 172.16.1.98 P Address = 172.16.1.50 Network Mask = 255.255.255.0 Default Gateway = 172.16.1.1 Primary Name Server = 172.16.1.99 Secondary Name Server = 172.16.1.98 Use DHCP = False 		

Step 10 Open a web browser and connect to Fabric Composer at the previously configured IP address.

NOTE:

The software version is not displayed and login is not allowed while the system is initializing.

Step 12 On the **Fabric Composer** page, enter the following default credentials, and click **LOGIN**.

- Username: admin
- Password: aruba

Fabric Compo v7.0.5-14110	oser
admin	•••1
•••••	•••1
Remember Me	LOGIN
HPE	king

Step 13 Enter the current and new password and click APPLY.

A Change	e Password	? 🗙
Your password	must be changed to login.	
Current *		•••1
New *		
	Must be more than 1 character(s) long.	
Confirm *	••••••	•••]
	Must match the new password field	
	PASSWORD POLICY	
(* = Required)		CANCEL APPLY

Add HPE Aruba Networking Fabric Composer Licenses

Step 1 On the Maintenance menu, select Licenses.

C	rubo Fabric Composer	Dashboard	Configuration 👻	Maintenance Visualization
Panels	SWITCHES - ALL LOCAL FABRICS Switches in Fabrics 0	×		 Switches Audits Support Bundles Device Firmware Backups Switch Checkpoints Syslog
	FABRIC INVENTORY - ALL LOCAL FA	BRICS		High Availability
	0 MAC Attach	ments		Licenses

Step 2 On the ACTIONS menu in the Maintenance/Licenses pane, select ADD.

orubo Fabric Composer Das	nboard Configuration 🗸 Maintenance 🗸 V	Visualization 💙	Ø Where can I find? (
E: Switches	Maintenance / Licenses		
û Audits		ତେ⊽≮	
Support Bundles	Status	License K	4 Add
Device Firmware	Enter Regex for Status	Enter R	Delete
De Backups			

Step 3 On the License page, paste the JSON license string in the License field and click APPLY.

ଦ୍ଧୁ License	×
Enter a required I	icense string.
License *	k+EOfGzQ04c6EysRQ6TaGBTQhVJHyUk2AdBzNfY7rCMHp829A=\"},\"swsn\":\"A681E25F80A0F4F65B\"}"
	A JSON string.
([*] = Required)	CANCEL APPLY

Step 4 Review the installed license to verify that the **Start Date**, **End Date**, **Quantity**, and **Tier** values display as expected.

Status	1±	License Key	Product	1=	Start Date
Enter Regex for Status		Enter Regex for License Key	Enter Regex for Product		Enter R
VALID A7Y5YEHU34AJ		A7Y5YEHU34AJ	R7G99-DEMO		Fri Feb 1
					0600 (Ce

NOTE:

Fabric Composer manages two tiers of switches (Tier 3 and Tier 4). The datasheet for each switch model identifies the license tier required.

Install HPE Aruba Networking Fabric Composer for High Availability

Refer to the *HPE Aruba Networking Fabric Composer Installation Guide* available on the HPE Networking Support Portal. In the "Installing High Availability for HPE ANW Fabric Composer using ISO" section, review the installation requirements and ensure that adequate host resources are available. Follow the steps provided to deploy the HA cluster.

Download AMD Pensando Policy and Services Manager

When using the firewall capabilities of the CX 10000 switch in a data center, AMD Pensando Policy and Services Manager (PSM) VMs must be installed on a network that is accessible by Fabric Composer and switch management interfaces.

Step 1 Navigate to https://asp.arubanetworks.com/.

Step 2 On the menu at the top of the page, select Software & Documents.

Step 3 In the Search Files field at the top, type Pensando.

Step 4 In the search results, select the latest OVA version and download it to your computer.

Install AMD Pensando Policy and Services Manager

In the Aruba Support Portal search results, find the *Pensando Policy and Services Manager for Aruba CX 10000: User Guide*. Review the "PSM Installation" section and ensure that adequate host resources are available. PSM requires a minimum of three VM instances for a production deployment.

1 Select an OVF template 2 Select a name and folder	Select an OVF template Select an OVF template from remote URL or local file system					
3 Select a compute resource 4 Review details 5 Select storage 6 Ready to complete	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive. O URL http://remoteserver-address/filetodeploy.ovf .ova					
	Local file Browse psm.dss.1.54.5-T-2.ova					
	CANCEL BACK NE					

Step 1 Select the OVA file using the **Deploy OVF Template** workflow within vCenter and click **NEXT**.

Step 2 Choose the appropriate options in **Select a compute resource** and proceed through **Review details**.

Step 3 On the Configuration page, click the radio button for Production and click NEXT.

1 Select an OVF template 2 Select a name and folder	Configuration Select a deployment configuration	
4 Review details 5 Configuration	O Trials	Description IMPORTANT: This
6 Select storage 7 Select networks	O Scale	configuration is required for production
8 Customize template 9 Ready to complete		DSS or 100 DSCs This configuration requires the following: * 16 vCPU 64GB RAM * 250GB Storage
		3 Items

Step 4 Proceed with selecting the appropriate storage and network resources for the deployment.

Step 5 Complete the **Customize template** form using the example below.

 4 Review details 5 Configuration 6 Select storage 7 Select networks 8 Customize template 9 Ready to complete IP Address IP Address of eth0 (DHCP if left blank) 172.16.104.51 Netmask Remask of eth0 (DHCP if IP Address is left blank) 255.255.255.0 Gateway Gateway of eth0 (DHCP if IP Address is left blank) 172.16.104.1
 6 Select storage 7 Select networks 8 Customize template 9 Ready to complete IP Address IP Address of eth0 (DHCP if left blank) 172.16.104.51 Netmask Netmask of eth0 (DHCP if IP Address is left blank) 255.255.255.0 Gateway Gateway of eth0 (DHCP if IP Address is left blank) 172.16.104.1
 Y Select networks B Customize template 9 Ready to complete IP Address IP Address of eth0 (DHCP if left blank) 172.16.104.51 Netmask Netmask of eth0 (DHCP if IP Address is left blank) 255.255.255.0 Gateway Gateway of eth0 (DHCP if IP Address is left blank) 172.16.104.1
IP Address of eth0 (DHCP if left blank) 172.16.104.51 Netmask Netmask of eth0 (DHCP if IP Address is left blank) 255.255.255.0 Gateway of eth0 (DHCP if IP Address is left blank) 172.16.104.1
Netmask Netmask of eth0 (DHCP if IP Address is left blank) 255.255.255.0 Gateway Gateway of eth0 (DHCP if IP Address is left blank) 172.16.104.1
Gateway Gateway of eth0 (DHCP if IP Address is left blank) 172.16.104.1
DNS Server DNS server (Multiple servers need to be comma separate or DHCP if IP Address is left blank) 172.16.1.98
Domain Name Domain name, e.g. example.com example.local
v Password 1 settings
Console password (minimum 8 chacters with at least one upper case, one lower case, and oneConsole passwordnunber)Console password••••••••

Step 6 Complete the VM creation workflow.

Step 7 Create additional PSM VMs as needed.

NOTE:

Additional VMs can be created by importing the OVA again or by cloning the first VM as a template as described in the "Installing OVA on ESXi" section of the *Pensando Policy and Services Manager for Aruba CX 10000: User Guide.*

Configure the AMD PSM Cluster

Step 1 In vCenter, login to one of the Penando PSM VM consoles.

• Username: root

• Password: < Specified during VM creation process >

Step 2 At the VM console, bootstrap the PSM cluster with the bootstrap_PSM.py utility using the following command-line switch/value pairs followed by a space-delimited list of IP addresses for all cluster members.

- -enablerouting: < No value required >
- -distributed_services_switch: < No value required >
- -autoadmit: False
- -clustername: < User supplied cluster name >
- -domain: < Domain name >
- -ntpservers: < Comma-separated list of NTP servers >

```
bootstrap_PSM.py -enablerouting -distributed_services_switch -autoadmit False -
    clustername FB1_PSM -domain example.local -ntpservers 172.16.1.98,172.16.1.99
    172.16.104.51 172.16.104.52 172.16.104.53
```

NOTE:

The **-autoadmit** command line switch is set to *True* by default. This automatically enables any Distributed Services Switch to join PSM. When a strict admission policy to PSM is required, set this command line switch to *False*.

Step 3 When prompted, read and accept the End User License Agreement.

Step 4 Verify that the PSM cluster bootstrap completes successfully.

```
2023-02-16 23:30:55.815164: * PSM bootstrap completed successfully
2023-02-16 23:30:55.815989: * you may access PSM at https://172.16.104.51
2023-02-16 23:30:55.816779: * Note: For backup and disaster recovery, please fetch and store PSM sec
urity token using the "psmctl" command.
2023-02-16 23:30:55.818379: ** To generate and store PSM token which can be used to access all DSE's
-
2023-02-16 23:30:55.819859: ** /usr/pensando/bin/psmctl get node-token --psm-ip localhost --psm-port
443 --audience "*" --token-output ~/dse-tok
[root@psm-01 ~]#
```

Step 5 On the VM console, enter the following to generate a PSM security token.

```
/usr/pensando/bin/psmctl get node-token --psm-ip localhost --psm-port 443 --
audience "*" --token-output ~/dse-tok
```

NOTE:

The token can be used for disaster recovery and backup purposes. Store it with other sensitive network credentials.

Step 6 When prompted, enter the following default credentials:

- User name: admin
- Password: Pensando0\$

Step 7 Open a web browser and connect to PSM at one of the configured VM IP addresses.

Step 8 On the AMD Pensando login page, enter the following default credentials and click SIGN IN.

- Username: admin
- Password: Pensando0\$



Step 9 Go to **System > Cluster** and verify that each PSM VM is listed under **Nodes** in the **Cluster Detail** pane with the following values.

- Quorum: true
- Phase: Joined

AMDA Pensando I	ŧ	Search			• Q			E@) ()
➡ Dashboard তৄ System	^	Cluster	erview						
• 🛟 Cluster		Cluster Detail 🖍 Name: Firewall Log Search:	▲ FB1 Ena	I_PSM abled 🌂	Last Updated: 2023-02-16 23:44:34 GMT+00:00	CPU	7%	24h Avg Cluster	8%
Tenants		Healthy: Security Policy Rule So Creation time:	tru cale: Ma 202	e x 6K Rules 🔏 23-02-16 23:29:28 GMT+00:00	7 %	Memory Memory Usage	21%	24h Avg Cluster Usage	21% 24%
Monitoring Troubleshoot		Last Leader Transition Auto Admit DSSs: NTP Servers:	Time: 202 no 172	23-02-16 23:29:57 GMT+00:00 .16.1.98	CPU MEMORY STORAGE	Storage Storage Usage	4%	24h Avg Cluster Usage	4% 4%
L Orchestrator		Nodes: Name Qu	orum	Phase					~
		172.16.104.52 true 172.16.104.53 true 172.16.104.51 true	•	Joined Joined Joined					

Step 10 Go to **Admin > User Management**, mouse-over the **admin** user, and click the **Change password** icon.

AMDA Pensando 🖡 ∈	Search
- Dashboard	RBAC Management
ত্রু System 🗸 🗸	🚓 Manage User
🟥 Tenants 🛛 🗸	AdminRole (1)
🔿 Workload 🛛 🗸	admin L Admin User
😰 Monitoring 🗸 🗸	AdminRole admin@example.local Change password
🔾 Troubleshoot 🗸	
C Orchestrator ~	
🚓 Admin 🛛 🔨	
Preferences	
2 Auth Policy	
• 🚉 User Management	

Step 11 Enter the old and new passwords and click Save changes.

AMDA PENSANDO I 🖛		Search		
	Dashboard		RBAC Management	
្ន	System	~	🚢 Manage User	
ŵ	Tenants	~	AdminRole (1)	
Ō	Workload	~	admin D Admin User	
٢	Monitoring	~	AdminRole admin@example.local	Save changes
٩	Troubleshoot	~	Old Password:	•••••
G	Orchestrator	~	New Password:	•••••
.	Admin	^	Confirm New Password:	
\$	Preferences			
28	Auth Policy			
• **	User Management			
NOTE:				

Changing the password on one VM updates all cluster members.

EVPN-VXLAN Configuration

Configuring an HPE Aruba Networking data center fabric is best performed using the HPE Aruba Networking Fabric Composer guided setup process. Fabric Composer automates switch provisioning, underlay link and routing configuration, overlay configuration, and integration with VMware vCenter.

Physical Topology Overview

The diagram below illustrates the physical links and hardware that comprise the primary data center in this guide. Fabric Composer is used to configure a routed underlay and EVPN-VXLAN overlay for the topology.



HPE Aruba Networking Fabric Composer Process

Fabric Composer's Guided Setup automates configuration following these steps:

- Switch discovery: Discover and inventory data center switches in Fabric Composer.
- Fabric Composer fabric creation: Define the logical construct that identifies a fabric within Fabric Composer.
- Switch assignment: Assign roles to fabric switches.
- NTP and DNS configuration: Assign NTP and DNS servers to fabric switches.
- VSX configuration: Create VSX-redundant ToR leaf pairs.
- Leaf/Spine configuration: Assign IP addresses to leaf/spine links.
- **Underlay configuration:** Establish OSPF underlay to support the EVPN-VXLAN overlay data plane and control plane.
- **Overlay configuration:** Establish BGP peerings to enable the EVPN overlay control plane and VXLAN tunnel endpoints for overlay data plane.
- **EVPN configuration**: Establish Layer 2 EVPN mapping of VLANs to VXLAN Network Identifiers (VNIs).

When the Guided Setup is complete, additional configuration details for host onboarding, external fabric connectivity, testing, and multicast are required:

- Layer 3 services within overlays.
- Multi-chassis LACP LAG configuration for host connectivity.
- Routing between the data center and campus.
- Overlay loopbacks for testing reachability to directly connected hosts and resources both inside and external to the fabric.
- PIM-SM and IGMP to support overlay multicast services.

For additional details on the Guided Setup steps, refer to the "Guided Setup" section of the HPE Aruba Networking Fabric Composer User Guide.

Plan the Deployment

Before starting the guided setup, plan ahead and develop a naming convention and address scheme with values that can accommodate the current deployment size and leave room for growth. Using a consistent approach in the physical and logical configurations improves the management and troubleshooting characteristics of the fabric.

This section provides sample values and rationale. Adjust the values and formats as needed to accommodate the current and projected sizes of the fabric effectively.

Naming Conventions

Fabric Composer supports the execution of operations on a single switch or on a selected group of switches.

Establish a switch naming convention that indicates the switch type, role, and location to simplify identification and increase efficiency when operating production-scale fabrics. Configure switch names before importing them into Fabric Composer.

Example values used in this guide:

Switch Name	Fabric Role	Description
RSVDC-FB1-SP1	Spine	Fabric #1, Spine #1
RSVDC-FB1-LF1- 1	Leaf	Fabric #1, VSX Leaf Pair #1, Member #1

Switch Name	Fabric Role	Description
RSVDC-FB1-LF1- 2	Leaf	Fabric #1, VSX Leaf Pair #1, Member #2
RSVDC-FB1-LF3- SA1	Server Access (Sub Leaf)	Fabric #1, VSF Server Access Stack #1 attached to Leaf Pair #3

NOTE:

VSF stacks used in the server access role contain two or more switches. The stack operates as a single logical switch with a single control plane. It is not possible to differentiate between stack members using a unique hostname.

The Guided Setup prompts for a **Name Prefix** on some steps. Name prefixes are logical names used within Fabric Composer. Choose a descriptive name to make it easy to monitor, edit, and execute operations. The procedures below include examples of effective names that can be used.

Underlay Connectivity and Addressing

Point-to-point connections between spine-and-leaf switches are discovered and configured automatically for IP connectivity using /31 subnets within a single network range. Fabric Composer supports addressing up to 128 links inside a fabric using a /24 subnet mask. The maximum number of links on a fabric is determined by the aggregate port count of the spine switches.

Another network range is provided to create: * A/32 loopback address on each switch, used as the router ID for OSPF and BGP. * A/31 transit VLAN between ToR switch pairs to ensure data plane continuity in case of host link failure. * A/31 point-to-point interface between ToR switch pairs to transmit keep-alive messages for VSX peer loss detection.

Fabric Composer creates each of these subnet types automatically from a single network range provided during the VSX setup process. If VSX is not used, the network range is provided during the underlay configuration process.

Purpose	Description	Example
Leaf-Spine IP address block	An IPv4 address block used to create /31, point-to-point layer 3 links between leaf and spine switches.	10.255.0.0/23

Example values used in this guide are:

Purpose	Description	Example
Routed loopback, VSX transit VLAN, and VSX Keep-Alive Interface IP address block	An IPv4 address block used to allocate unique loopback addresses (/32) for each switch, for VSX keep-alive point-to-point connection (/31) and also used as a transit-routed VLAN between redundant ToRs (/31)	10.250.0.0/2

Overlay Connectivity and Addressing

The overlay network is created using VXLAN tunnels established between Virtual Tunnel Endpoints (VTEPs) within the leaf switches in the fabric. Loopback addresses assigned to establish route peerings are unique per switch and cannot be used as a VTEP IP when using VSX. A single logical VTEP per rack is defined by creating a dedicated /32 loopback interface common to both ToR peer switches. The interfaces are assigned automatically from a single subnet scope provided during the overlay guided setup.

Purpose	Description	Example
VTEP IP address block	An IPv4 address block used to allocate VXLAN tunnel endpoint (VTEP) loopback addresses (/32) for each ToR switch pair	10.250.2.0/24

A Virtual Network Identifier (VNI) is a numerical value that identifies network segments within the fabric's overlay topology. The VNI is carried in the VXLAN header to enable switches in the fabric to identify the overlay to which a frame belongs and apply the correct policy to it.

When configuring the overlay topology, a Layer 3 VNI represents the routed component of the overlay. Each Layer 3 VNI maps to a VRF. A Layer 2 VNI represents the bridged component of the overlay. Each Layer 2 VNI maps to a VLAN ID. Multiple Layer 2 VNIs can be associated to a single VRF.

Plan your VNI numbering scheme in advance to ensure that values do not overlap. Example values used in this guide are:

VNI Type	Description	Example
L2 VNI	VLAN ID + 10,000	VLAN100 == L2 VNI 10100, VLAN200 == L2VNI 10200
L3 VNI	Overlay # + 100,000	Overlay1 == L3 VNI 100001, Overlay2 == L3 VNI 100002

Internal BGP (iBGP) is used to share overlay reachability information between leaf switches. Layer 3 and Layer 2 information associated to a local switch's VNIs is advertised with its associated VTEP to other members of the fabric. Two of the spines operate as BGP route reflectors. All leaf switches are clients of the two route reflectors.

A unique IP loopback IP address is assigned to each overlay VRF for testing and troubleshooting.

Overlay VLAN switched virutal interface (SVI) and Active Gateway IP address assignments are not unique on leaf switches. A ping test to a directly attached host is not supported when the SVI/AG IP is the traffic source, because the ping response may be sent to the switch that did not originate the ping. Using a unique IP source from a loopback IP allows the attached switch to source a ping test to the host.

Additionally, the SVI/AG IP address for each VLAN is present on all leaf switches in a fabric. A unique loopback IP provides a source IP address for testing reachability within the fabric and to external hosts. It also provides a unique destination IP to test individual switch reachability within an overlay.

Plan an IP block per overlay VRF large enough that a unique IP address can be assigned to each leaf switch in the fabric. A single maskable block allows summarizing route advertisements to external networks.

Purpose	Description	Example
VRF 1 IP address block	An IPv4 address block used to assign loopback IPs for reachability testing in VRF 1	10.250.4.0/24
VRF 2 IP address block	An IPv4 address block used to assign loopback IPs for reachability testing in VRF 2	10.250.5.0/24

Each VSX pair requires an overlay transit VLAN to share routed reachability of the loopback IP addresses assigned from the IP block above. Assign a single maskable block of IP addresses for each overlay VRF, where /31 blocks can be assigned to the transit VLANs.

Purpose	Description	Example
VRF 1 IP address block	An IPv4 address block used to assign loopback IPs for reachability testing in VRF 1	10.255.4.0/24
VRF 2 IP address block	An IPv4 address block used to assign loopback IPs for reachability testing in VRF 2	10.255.5.0/24

MAC Address Best Practice

A Locally Administered Address (LAA) should be used when Fabric Composer requires entry of a MAC address for the switch virtual MAC, a VSX system-MAC, or an Active Gateway MAC for a distributed SVI. An LAA is a MAC in one of the four formats shown below:

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx-xx
```

The *x* positions can contain any valid hex value. For more details on the LAA format, see the IEEE tutorial guide.

An active gateway IP distributes the same gateway IP across all leaf switches in a fabric to support gateway redundancy and VM movement across racks. An active gateway MAC associates a virtual MAC address with an active gateway IP. Only a small number of unique virtual MAC assignments can be configured per switch. The same active gateway MAC address should be reused for each active gateway IP assignment.

HPE Aruba Networking Fabric Composer Prerequisites

The following items must be configured before building a Fabric Composer-based fabric.

- **Physically cable all switches in the topology.** VSX pairs, VSF stacks, and leaf-spine links must be connected fully to support Fabric Composer's automation.
- Configure VSF stacking for server access switches. When optional server access switches are
 present, VSF auto-stacking must be configured when the switches are at their default configuration. VSF configuration guidance is available in the HPE Networking Support Portal. Enable split
 detection after the stack is formed.
- Assign management interface IP addresses. A DHCP scope using MAC address reservations for each switch can be used in place of manual IP address assignment. When using DCHP, MAC address reservations ensure that each switch is assigned a consistent IP address.
- **Assign switch hostnames**. Assigning unique hostnames using a naming convention helps administrators identify a switch and its role quickly during setup and future troubleshooting.

Fabric Initialization

Configuring an HPE Aruba Networking data center fabric using a spine-and-leaf topology is best performed using the Fabric Composer guided setup process. To return to guided setup at any time, simply select it in the menu bar at the top right of the Fabric Composer user interface.



Discover Switches on the Network

The first procedure adds switches to the Fabric Composer device inventory. An orderly naming convention for switch host names should be implemented before continuing with this procedure in order to simplify switch selection in the following steps.



NETWOR	C DISTRIBUTED SERVICES				
Network Setup Perform the following steps to initialize and configure					
your system.	CHES * ver new Switches.				
Add a	IC * Fabric to the system.				
Selected Fab	Selected Fabric:				
Select a Fabric 👻					
Assig	IN SWITCH TO FABRIC * n Switch To Fabric				

Step 2 In the Discover Switches window, enter the following switch information and click APPLY.

- Switches: < OOBM IP addresses for fabric switches >
- admin Switch Password: < password created during switch initialization >
- admin Switch Password: < password created during switch initialization >
- Service Account Password: < new password for the afc_admin account >
- Confirm Service Account Password: < new password for the afc_admin account >

Discover Switche	S	×
Enter the details of the Switch	ies to be discovered.	
Switches *	172.16.116.101-172.16.116.109	
	An IPv4 address, Hostname and/or an IPv4 hyphenated range, not to exceed 256 switches, example: 198.162.3.4, hostname.example.com, 172.10.1.1-172.10.1.10	
Switch "admin" Account)
Password *	The switches admin account password for switch access. If the switches have no password, this password set on them. Any non empty string, example: thing.red.7	will be
Confirm Switch "admin"		•••]
Account Password *	Must match the Switch "admin" Account Password	
Service Account User *	afc_admin	
	A non-empty Switch service account used for REST access to the Switch(es) from AFC. Default is the 'afc_ switch account.	admin'
Service Account Password		••••]
*	A password to be used for the service account creation for switch access. Any non empty string, example: o 2	ar.top-
Confirm Service Account		••••]
Password *	Must match the Service Account Password	
(* = Required)	CANCEL	PLY

NOTE:

Switch IP addresses can be entered in a comma-separated list or in one or more ranges. If the IP addresses provided include devices not supported by Fabric Composer or switches with different credentials, a "Discovery Partially Successful" warning message appears after the import. This step creates a new afc_admin account on all the switches for API access from Fabric Composer.

Step 3 Review the list of imported switches in the **Maintenance > Switches** window and verify that the health status of each switch is **HEALTHY, BUT...** Hovering over the health status value of an individual switch provides additional details.

HPE Composer Dash	board Configuratic	on 🗸 Maintenance 🕯	 Visua 	lization 🗸 🔎 W	here can I fi	nd? (e.g.	
Switches	Maintenance / Sw	itches					
Ĵ Audits							~
Support Bundles		Health	μE	Status	1Ē.	🕑 Name	1£
👍 Device Firmware		Select Health	•	Select Status	*	Enter Regex for Name	
Backups		HEALTHY, BUT		Unassigned		RSVDC-FB1-SP2	
Dackups		HEALTHY, BUT		Unassigned		RSVDC-FB1-SP1	
Switch Checkpoints		HEALTHY, BUT		Unassigned		RSVDC-FB1-LF3-SA1	
Svelog		HEALTHY, BUT		Unassigned		RSVDC-FB1-LF3-2	
E Syslog		HEALTHY, BUT		Unassigned		RSVDC-FB1-LF3-1	
High Availability		HEALTHY, BUT		Unassigned		RSVDC-FB1-LF2-2	
(a) Licenses		HEALTHY, BUT		Unassigned		RSVDC-FB1-LF2-1	
		HEALTHY, BUT		Unassigned		RSVDC-FB1-LF1-2	
		HEALTHY, BUT		Unassigned		RSVDC-FB1-LF1-1	

Create a Fabric

A fabric container is created in Fabric Composer for collective configuration of a group of switches. The fabric name is internal to Fabric Composer operations and is not tied to configuration elements on a switch. Fabric Composer supports the configuration of spine and leaf, Layer 2 two-tier, and management networks. All topologies assign switches to a Fabric Composer internal fabric for configuration and management.

The fabric in this guide is used to implement a spine-and-leaf routed network with an EVPN-VXLAN overlay.

Step 1 On the Guided Setup menu, select FABRIC.

NET	WORK	DISTRIBUTED SERVICES				
Netw	Network Setup					
Perforn your sy	n the follov rstem.	ving steps to initialize and configure				
	SWITCHES Discover r	s new Switches.				
	FABRIC * Add a Fab	pric to the system.				
Selected Fabric:						
Sele	ct a Fabric					
	ASSIGN S Assign Sw	WITCH TO FABRIC * vitch To Fabric				

Step 2 Define a unique logical name, set the Type to Data, specify a time zone, and click APPLY.

IIII Fabric		? ×
Enter a required Fab	ric Name and an optional Description and Time Zone. A time zone will be applied to all switches in the fat	oric.
Name *	RSVDC-FB1	
	Any non empty string, example: fabric01	
Description	OWL Roseville data center fabric #1	
	Example: My New Fabric	
Type *	Data	× •
	Select Data for your network traffic, Management for out of band management traffic.	
Time Zone	America/Los_Angeles	× •
	Default Time Zone is UTC if none are selected	
Auto Save Interval	600	
	A value between 600 seconds (10 minutes) and 43200 seconds (12 hours) for the system to automatically copy the running config startup config for each switch in fabric. 0 disables Auto Save.	j to
(* = Required)	CANCEL	APPLY

Assign Switches to the Fabric

Switches must be added to a fabric before they can be configured. When adding a switch to a fabric, a role is declared. In the following steps, begin by adding spine switches. Leaf switches can then be added more easily as a group.

Step 1 On the **Guided Setup** menu, verify that the fabric created in the previous step appears under **Selected Fabric** and click **ASSIGN SWITCH TO FABRIC**.

NETWORK	DISTRIBUTED SERVICE	S
Network Set	up ving steps to initialize and o	configure
SWITCHES Discover r	s new Switches.	
Add a Fab	pric to the system.	
ASSIGN ST Assign Sw	WITCH TO FABRIC * itch To Fabric	× *
Configure	Switch NTP.	

Step 2 Assign switches to the fabric grouped by role. Assign the following values for spine switches, then click **ADD**.

- Fabric: RSVDC-FB1
- Switches: < All spine switches >
- Role: Spine
- Force LLDP Discovery: checked
- Initialize Ports: checked
- Exclude this switch from association to any Distributed Services Manager: unchecked

🗰 Assign S	witches To Fabric	;				×		
Fabric	RSVDC-FB1			× •				
Switches	× RSVDC-FB1-S	SP1 × RSVDC-FB1-SP2	adal auitakaa may ka aa		SELECT ALL			
Role *	Spine Select a role for the se	elected Switches.	iodei switches may be as:	signed to a management radiic.				
 Force LLDP I Initialize Ports Enable ports, rou Exclude this s CLEAR 	Discovery ting, and set default MTU value switch from association to	s. any Distributed Services Mar	ager					
Switch	Role	Force LLDP Discov	Initialize Ports	Exclude this switch				
(* = Required) Scro	* = Required) Scroll for more options CANCEL APPLY							
Checking I port config	nitialize Ports e juration is perfor	enables all switch p med in the previous	orts for use i Switch Initia	n LLDP neighbor c	liscovery. Spl to allow prope	it er		

port configuration is performed in the previous *Switch Initialization* procedure to allow proper port initialization by Fabric Composer. The MTU of the physical ports also is adjusted to 9198 in order to support jumbo frames that allow VXLAN encapsulation overhead. Checking **Force LLDP Discovery** prompts Fabric Composer to use LLDP neighbor information to discover link topology between spine-and-leaf switches and ToR VSX pairs dynamically.

Step 3 Repeat the steps above for VSF server access switch stacks. Verify that all server access switch stacks are listed with the **Sub Leaf** role selected and click **ADD**.

IIII Assign Swite	ches To Fabric					×	
Fabric	RSVDC-FB1						
Switches	× RSVDC-FB1-LF3-	SA1		× •	SELECT ALL		
	Select switches to assign	to the fabric. Only 6300 or 8300 m	odel switches may be ass	signed to a Management Fabric.			
Role *	Sub Leaf			× •			
	Select a role for the select	ted Switches.					
Force LLDP Discov	very						
 Initialize Ports Enable ports, routing, at Exclude this switch CLEAR 	nd set default MTU values.	y Distributed Services Man	ager				
Switch	Role	Force LLDP Discovery	Initialize Ports	Exclude this switch f			
RSVDC-FB1-SP1	Spine	Yes	Yes	No	団		
RSVDC-FB1-SP2	Spine	Yes	Yes	No	莭		
* = Required) Scroll for more options APPLY NOTE:							
This step is op Each VSF swit	tional. It is requ ch stack has a s	ired only when se ingle entry that re	rver access sv epresents all s	vitches are present switch members of	in the topology f the stack. This		

example implementation contains a single VSF stack.

Step 4 Repeat the previous step for border leaf switches with the **Border Leaf** role selected and click **ADD**.

HIII Assign Switch	nes To Fabric					×		
Fabric	RSVDC-FB1							
Switches	Switches X RSVDC-FB1-LF1-1 X RSVDC-FB1-LF1-2 X X SELECT ALL Select switches to assign to the fabric. Only 6300 or 8300 model switches may be assigned to a Management Fabric.							
Role *	Border Leaf Select a role for the selected	Switches.		× •				
 Initialize Ports Enable ports, routing, and Exclude this switch f CLEAR ADD Switch 	I set default MTU values. rom association to any E Role	Distributed Services Mana Force LLDP Discovery	ager Initialize Ports	Exclude this switch f				
RSVDC-FB1-SP1	Spine	Yes	Yes	No	Ū			
RSVDC-FB1-SP2	Spine	Yes	Yes	No	— 匝			
RSVDC-FB1-LF3-SA1	Sub Leaf	Yes	Yes	No	Ū			
(* = Required) Scroll for me	ore options			[CANCEL	.Y		

Step 5 Repeat the previous step for the remaining leaf switches with the **Leaf** role selected and click **ADD**.

abric	RSVDC-FB1				
witches	× RSVDC-FB1-LF × RSVDC-FB1-LF	72-1 × RSVDC-FB1-LF2-2	× RSVDC-FB1-LF3-1	× •	DESELECT
ole *	Select switches to assig	in to the fabric. Only 6300 or 8300 r	model switches may be as	signed to a Management Fabric.	
Force LLDP Disco	Select a role for the sel	ected Switches.			
 Force LLDP Disco Initialize Ports Enable ports, routing, Exclude this switc 	Select a role for the sel overy and set default MTU values th from association to a	ected Switches. any Distributed Services Ma	nager		
 Force LLDP Disco Initialize Ports Enable ports, routing, Exclude this switce CLEAR ADD Switch 	Select a role for the sel	ected Switches any Distributed Services Ma	inager Initialize Ports	Exclude this switch	
 Force LLDP Disco Initialize Ports Enable ports, routing, Exclude this switch CLEAR ADD Switch RSVDC-FB1-SP1 	Select a role for the sel overy and set default MTU values th from association to a Role Spine	ected Switches any Distributed Services Ma. Force LLDP Discov Yes	Inager Initialize Ports Yes	Exclude this switch	面

NOTE:

Leaf switches typically comprise the majority of switches in a fabric. Use **SELECT ALL** to catch all remaining leaf switches, when switch assignments containing smaller sets of switches are assigned first.

Step 6 Scroll through the list of switches to verify role assignments and ensure successful configuration of the fabric. After adding all switches to the fabric with the correct role, click **APPLY**.

IIII Assign Switc	hes To Fabric					×			
Fabric	RSVDC-FB1								
Switches	Select	Select 👻 SELECT ALL							
	Select switches to assign to	the fabric. Only 6300 or 8300	model switches may be assign	ed to a Management Fabric.					
Role	Select a Role			~					
	Select a role for the selected	l Switches.							
Force LLDP Discov	ery								
 Initialize Ports Enable ports, routing, and Exclude this switch 	nd set default MTU values. from association to any	Distributed Services Ma	nager						
CLEAR ADD			Initializa Danta	Euclude Altie cuilete		l			
Switch	Role	Force LLDP Discov	Initialize Ports	Exclude this switch		-			
RSVDC-FB1-SP1	Spine	Yes	Yes	No	Ĩ	а.			
RSVDC-FB1-SP2	Spine	Yes	Yes	No		ч.			
RSVDC-FB1-LF3-SA1	Sub Leaf	Yes	Yes	No	Ū				
RSVDC-FB1-LF1-1	Border Leaf	Yes	Yes	No					
(* RSVDC-FB1-LF1-2	Border Leaf	Yes	Yes	No	団				
RSVDC-FB1-LF2-1	Leaf	Yes	Yes	No					
RSVDC-FB1-LF2-2	Leaf	Yes	Yes	No	Ē				
RSVDC-FB1-LF3-1	Leaf	Yes	Yes	No	Ē				
RSVDC-FB1-LF3-2	Leaf	Yes	Yes	No					
= Required) Scroll for m	nore options				CANCEL	LY			

Step 7 Guided Setup displays the list of switches in the **Maintenance > Switches** window. Switch status should sync in a few seconds. Verify that all switches in the fabric are listed as **HEALTHY** in green.

Maintenance / Swi	itches			$\odot \otimes \mathbb{Y}$	C ACTIONS Y
	Health 1	Status 1	☑ Name	Fabric Ja	IPv4 Address
	Select Health 🔻	Select Status 💌	Enter Regex for Name	Enter Regex for Fabric	Enter Regex for IPv4 Add
	HEALTHY	Synced	RSVDC-FB1-SP2	RSVDC-FB1	172.16.116.102
	HEALTHY	Synced	RSVDC-FB1-SP1	RSVDC-FB1	172.16.116.101
	HEALTHY	Synced	RSVDC-FB1-LF3-SA1	RSVDC-FB1	172.16.116.109
	HEALTHY	Synced	RSVDC-FB1-LF3-2	RSVDC-FB1	172.16.116.108
	HEALTHY	Synced	RSVDC-FB1-LF3-1	RSVDC-FB1	172.16.116.107
	HEALTHY	Synced	RSVDC-FB1-LF2-2	RSVDC-FB1	172.16.116.106
	HEALTHY	Synced	RSVDC-FB1-LF2-1	RSVDC-FB1	172.16.116.105
	HEALTHY	Synced	RSVDC-FB1-LF1-2	RSVDC-FB1	172.16.116.104
	HEALTHY	Synced	RSVDC-FB1-LF1-1	RSVDC-FB1	172.16.116.103

Configure Switch Profile

The switch profile optimizes hardware resources for a switch's role in the network. Most switches are assigned a leaf role by default. The following procedure assigns the spine profile to the spine switches in the network.

NOTE:

When using IPsec or NAT on a CX10000 border leaf, the border leaf switches profile must be changed to **spine**. East-west policy enforcement for hosts attached to the border leaf is not supported after this change.

Step 1 On the Maintenance > Switches page, click a checkbox to select one of the spine switches.

Main	tenance / <mark>Sw</mark>	itches							
1 se	elected								S 🗸
		Health	μ£.	Status	1£	♂ Name	ĮΞ	Fabric	ĻΞ
		Select Health	~	Select Status	•	Enter Regex for Name		Enter Regex for Fabric	
		HEALTHY		Synced		RSVDC-FB1-SP2		RSVDC-FB1	
		HEALTHY		Synced		RSVDC-FB1-SP1		RSVDC-FB1	

Step 2 Click the ACTIONS menu on the right, and select Change Profile.

Maintenance / Swi	itches							
1 selected							0	
	Health	ĮΞ	Status	ΨĒ	♂ Name	Æ	F٤	Discover Switches
	Select Health	•	Select Status	•	Enter Regex for Name			Edit
	HEALTHY		Synced		RSVDC-FB1-SP2		R٤	Delete
	HEALTHY		Synced		RSVDC-FB1-SP1		R٤	Assign Switch To Fabric
	HEALTHY		Synced		RSVDC-FB1-LF3-SA1		R٤	Reboot
								Reconcile
	HEALTHY		Synced		RSVDC-FB1-LF3-2		R	Save Configuration
	HEALTHY		Synced		RSVDC-FB1-LF3-1		R	Stage Firmware
	HEALTHY		Synced		RSVDC-FB1-LF2-2		R	Update
	HEALTHY		Synced		RSVDC-FB1-LF2-1		R٤	DSM
	HEALTHY		Synced		RSVDC-FB1-LF1-2		R٤	Change Password
	HEALTHY		Synced		RSVDC-FB1-LF1-1		R٤	Change Profile
								< Statistics
								Clear Software State
								< Launch

Step 3 Select **Spine** in the **New Profile** field dropdown, check **Reboot switch after changing profile**, and click **Apply**.

😂 Change Pro	ofile RSVDC-FB1-SP1	×
Select a new Hardwa	re Profile for this switch. Profile changes do not take affect without a switch reboot.	
Profile	Leaf	
Configured Profile	Spine	
New Profile *	Spine	,
Description	MAC Addresses 32768, Unicast Routes(IPv4: 1269760, IPv6: 624640), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel: 31742)	
✓ Reboot switch af	ter changing profile.	
(* = Required)	CANCEL APPL	1
NOTE:		
When selectin cally from Le	ng Spine in the New Profile field, the Configured Profile value changes dynami af to Spine .	-

Step 4 Repeat the procedure for each spine switch.

Configure Infrastructure Split Ports

This process is necessary only when using links between fabric switches that require split port operation. The most common case is using a CX 9300 in the spine role to increase rack capacity of a fabric. In this sample deployment, CX 9300-32D spine ports are set to operate in 2 x 100 Gbps mode.



Step 1 On the Configuration menu, select Ports > Ports.



Configuration / Ports /	/ Ports			
Fabric	RSVDC-FB1	Switch × R	SVDC-FB1-SP1	SELECT ALL
		×R	SVDC-FB1-SP2	
				C ACTIONS ~
				$\odot \bigcirc \bigcirc$
H	ealth ↓≞	Reason J=	Switch J=	Port Ji
	Select Health 🔻	Enter Regex for Reason	Enter Regex for Switch	Enter Regex for Port
	HEALTHY	Invalid speed	RSVDC-FB1-SP1	1/1/1
	HEALTHY	Invalid speed	RSVDC-FB1-SP1	1/1/2
	HEALTHY	Invalid speed	RSVDC-FB1-SP1	1/1/3
	HEALTHY	No XCVR installed	RSVDC-FB1-SP1	1/1/4
	HEALTHY	No XCVR installed	RSVDC-FB1-SP1	1/1/5
	HEALTHY	No XCVR installed	RSVDC-FB1-SP1	1/1/6

NOTE:

Typing a value in the **Switch** field filters selectable switch names to those containing that value in their name. Following the naming convention in this guide, only the spine switches are displayed for selection by typing **sp** in the **Switch** field.

Step 3 Filter displayed ports by entering **Invalid** in the regex field below the **Reason** column heading and click the **Apply Table Filters** icon.

Configuration / Ports / Ports							
Fabric	RSVDC-FB1	- Switc	h × R	SVDC-FB1-SP1		SELECT ALL	
			× R	SVDC-FB1-SP2			
Ħ						C ACTIONS ~	
					i Unap	oplied table filters	
He	ealth J=	Reason	μ <u>ε</u>	Switch	μE	Port Apply table filters	
	Select Health	Invalid		Enter Regex for Switch		Enter Regex for Port	
	HEALTHY	Invalid speed		RSVDC-FB1-SP1		1/1/1	
	HEALTHY	Invalid speed		RSVDC-FB1-SP1		1/1/2	
	HEALTHY	Invalid speed		RSVDC-FB1-SP1		1/1/3	
	HEALTHY	No XCVR installed		RSVDC-FB1-SP1		1/1/4	
	HEALTHY	No XCVR installed		RSVDC-FB1-SP1		1/1/5	

NOTE:

Invalid speed is displayed in the **Reason** column when there is a mismatch between a physical port's configured operation and an attached Active Optical Cable's (AOC's) physical split configuration. No error message is displayed when using a standard 400 Gbps transceiver before defining split port operation.

Step 4 Click the box at the top of the selection column to select all the displayed ports on both spine switches that match the search criteria.

Configuration / Ports / Ports							
Fabric RSVDC-FB1	Swite	ch × RSVDC-FB1-SP1	SELECT ALL				
		× RSVDC-FB1-SP2					
6 selected 🔠 🖂			C ACTIONS ~				
			$\odot \bigcirc \bigcirc$				
Health	L≟ Reason	↓≟ Switch ↓≟	Port 📖				
Select Health	- Invalid	Enter Regex for Switch	Enter Regex for Port				
HEALTHY	Invalid speed	RSVDC-FB1-SP1	1/1/1				
HEALTHY	Invalid speed	RSVDC-FB1-SP1	1/1/2				
HEALTHY	Invalid speed	RSVDC-FB1-SP1	1/1/3				
HEALTHY	Invalid speed	RSVDC-FB1-SP2	1/1/1				
HEALTHY	Invalid speed	RSVDC-FB1-SP2	1/1/2				
HEALTHY	Invalid speed	RSVDC-FB1-SP2	1/1/3				

Step 5 On the ACTIONS menu, select QSFP Transform > Split > 2x 100.

Configuration	Configuration / Ports / Ports							
	Fabric	RSVDC-FB1		Switch	× RSVDC-FB1-SP1		SELE	CT ALL
					× RSVDC-FB1-SP2			
6 selected	▦							C ACTIONS ~
								Edit
	He	alth 📖	Reason		↓≞_ Switch	ĮΞ	Port	< Enable/Disable
E	-	Select Health 🔻	Invalid		Enter Regex f	or Switch	Enter Re	< VLANs
	2	HEALTHY	Invalid speed		2x100	< Split		< QSFP Transform
		HEALTHY	Invalid speed		2x10	Unsplit		< Persona
	2	HEALTHY	Invalid speed		2x200		1/1/3	
		HEALTHY	Invalid speed		2x25		1/1/1	
		HEALTHY	Invalid speed		4x100		1/1/2	
		HEALTHY	Invalid speed		4x10		1/1/3	
					4x25			

Step 6 When prompted to confirm the split operation, click OK.

Confirm Performing a Split/Unsplit Operation on a Port will remove the existing configuration. A reboot is required for the operation to take effect. Are you sure you want to continue? CANCEL OK NOTE:

NUTE:

The split ports are enabled by Fabric Composer for use in LLDP neighbor discovery, and the MTU of the split ports is adjusted to 9198 to support jumbo frames for VXLAN encapsulation. The **Confirm** prompt indicates that a reboot is required, but a reboot is not required to enable split ports.

Configure NTP for the Fabric

Modern networks require accurate, synchronized time. The NTP wizard is used to enter NTP server hosts and associate them with all fabric switches. The NTP servers must be reachable from the data center management LAN. The Fabric Composer CLI Command Processor shows the time synchronization status of each switch. At the completion of this procedure, the date and time are synchronized between the data center switches and the NTP servers.

Step 1 On the Guided Setup menu, select NTP CONFIGURATION.

NET	WORK	DISTRIBUTED SERVICES						
Network Setup								
your sys	Perform the following steps to initialize and configure your system.							
	SWITCHES Discover r	s new Switches.						
	FABRIC Add a Fabric to the system.							
Selecte	d Fabric:							
RSVE	C-FB1		$\times =$					
	ASSIGN S Assign Sw	WITCH TO FABRIC vitch To Fabric						
0	NTP CONF Configure	FIGURATION Switch NTP.						
	DNS CONI Configure	FIGURATION Switch DNS.						

Step 2 On the Name page, enter a Name and Description, then click NEXT.

NTP Confi	figuration	%				
Name	Entries Application	Summary				
Enter a required Na	ame and an optional Description.					
Name *	Name * RSVDC-FB1-NTP					
	Any non empty string, example ntp-fabric					
Description	NTP servers for RSVDC fabric 1					
	Example: NTP Configuration settings for NTP Config 1					
(* = Required)	CANCE	L BACK NEXT				

Step 3 On the **Entries** page, enter a valid hostname or IP address and optional NTP authentication information, then click **ADD**.

NTP Configu	uration						? ×
Name		Entries	6	Application	n	Summary	
Enter a required Serve	r(s) and an option	nal Mode, Key	ld, and Key Pas	sword. Select a Ke	y Type as require	d.	
Server *	Server * 10.2.120.98						
	Valid Hostname, IP	v4 or IPv6 Addres	s, example: hostnam	e.example.com, 198.16	2.3.4, 2001:db8:85a3	::1234	
Mode	Select						-
Prefer Enable NTP Auther	ntication						
Key ID	NTP Au	thentication No					
	Enter a num	ber between 1 and	d 65534, example: 30				
Key Password							
	Enter a valid	password betwee	en 8 and 80 character	s. Example: ntp-config.	10		
Кеу Туре	NTP Aut	hentication No	t Enabled				
Enable Trust							
CLEAR ADD	UPDATE						
Server	Mode	Prefer	Key ID	Кеу Туре	Trust Enabled	Key Passw	
			There is no da	ata to display			
(* = Required) Se	croll for more or	otions			СА	NCEL BACK	NEXT

Step 4 Repeat the step above for each NTP server in the environment.

Step 5 After all NTP servers have been added, click **NEXT**.

NTP Configurat	tion						? *
Name		Entries		Application	1	Summary	
Key ID	NTP Authentication Not Enabled Enter a number between 1 and 65534, example: 30						
Key Password Key Type	Enter a valid password between 8 and 80 characters. Example: ntp-config.10 NTP Authentication Not Enabled						
CLEAR ADD	UPDATE						
Server	Mode	Prefer	Key ID	Кеу Туре	Trust Enabled	Key Passwo	
		No			No	No	<u>ت</u>

Step 6 On the Application page, select the name of the fabric in the Fabric field and click NEXT.

NTP Conf	iguration	? ×
Name	Entries Application Summary	
Select a Fabric or S	witches for this configuration to be applied to. A fabric implies all switches contained in it	
Fabric	× RSVDC-FB1	× •
Switches	Not applicable when a Fabric is selected.	
(* = Required)	CANCEL BACK N	EXT

Step 7 On the **Summary** page, verify that the information is entered correctly and click **APPLY**.

					\checkmark
Name	9	Entries	Application		Summary
Name		RSVDC-FB1-NTP			
Description		NTP servers for RSVD	OC fabric 1		
Fabric		RSVDC-FB1			
Switches					
Server	Mode	Prefer	Key ID	Кеу Туре	Trust Enabled
10.2.120.98		No			No
10.2.120.99		No			No

Step 8 On the **Configuration > Network > NTP** page, click the radio button for the NTP config applied to an individual switch, click the **ACTIONS** menu on the right, and click **Delete**.

Configuration / Network / NTP								
		۲	○ 🔽 🏵 C ACTIONS ▾					
	☑ Name	Servers JE	Applies To Add					
	Enter Regex for Name	Enter Regex for Servers	Enter Re Edit					
۲	ntp_config_172.16.116.102	pool.ntp.org	RSVDC-FB Delete					
0	ntp_config_172.16.116.103	pool.ntp.org	RSVDC-FB1-LF1-1					
0	ntp_config_172.16.116.104	pool.ntp.org	RSVDC-FB1-LF1-2					
0	ntp_config_172.16.116.105	pool.ntp.org	RSVDC-FB1-LF2-1					
0	ntp_config_172.16.116.106	pool.ntp.org	RSVDC-FB1-LF2-2					
0	ntp_config_172.16.116.107	pool.ntp.org	RSVDC-FB1-LF3-1					
0	ntp_config_172.16.116.108	pool.ntp.org	RSVDC-FB1-LF3-2					
0	ntp_config_172.16.116.109	pool.ntp.org	RSVDC-FB1-LF3-SA1					
0	RSVDC-FB1-NTP	10.2.120.98	RSVDC-FB1					
		10.2.120.99						

NOTE:

Fabric Composer dynamically creates switch level objects that reconcile configuration performed by an administrator directly on the switch. A switch level configuration object has a higher precedence than Fabric Composer objects defined at the fabric level. At this time, the default NTP config is reconciled in a switch level configuration object. In this case, it is necessary to delete switch level NTP configuration objects to apply the fabric level config. If per-switch reconciled config is not present, omit steps 8, 9, and 10.

Step 9 In the Delete confirmation window, click OK.

i Delete	×
Are you sure you want to delete ntp_config_172.16.104.101? This will attempt to remove configuration from one or more switches.	
	CANCEL

Step 10 Repeat steps 8 and 9 to remove reconciled NTP configuration for all switches.

Step 11 In the menu bar at the top right of the Fabric Composer display, click the **CLI Commands** icon and select **Show Commands**.

<u>\$</u>	3 - 🔳	admin 🖌	? *		
>_ Show Command	ls DIST				
Configuration Ed	litor	DISTRIBUTED SERVICES			

Step 12 On the CLI Command Processor page, enter the following values, then click RUN.

- Fabrics: RSVDC-FB1
- **Commands:** show ntp status

>_ CLI Command Processor								
Select Fabrics or Switches	s, and select or add Saved Commar	ids that can be customized. Press Run for results.						
Fabrics	× RSVDC-FB1	× •						
Switches	Not applicable when a Fabric is	Not applicable when a Fabric is selected.						
Saved Commands	Select from Saved Commands of	r Add new commands.						
Commands	show ntp status							
	A comma separated list of commands to be	run.						
Download Options	Download Results Download J	SON Data						
Results	Switch : RSVDC-FB1-LF1-1 NTP Status Information	Command : show ntp status						
	NTP	: Enabled						
	NTP DHCP	: Enabled						
	NTP Authentication	: Disabled						
	NTP Server Connections	: Using the mgmt VRF						
	System time	: Wed Oct 11 09:35:59 PDT 2023						
	NTP uptime	: 22 minutes, 15 seconds						
	NTP Synchronization Infor	nation						
	NTP Server	: 10.2.120.99 at stratum 3						
	Poll interval	: 64 seconds						
	Time accuracy	: Within -0.063994 seconds						
	Reference time	: Wed Oct 11 2023 9:24:04.035 as per America/Los_Angeles						
	Switch : RSVDC-FB1-LF1-2	Command : show ntp status						
	NTP Status Information							
(* = Required)		CANCEL RUN						

:::info Multiple commands are supported in the **Commands** field in a comma-separated list. CLI commands can be saved for future reuse by clicking the **ADD** button. When typing a command in the **Saved Commands** field, preconfigured and saved commands appear in a list. Select a command in the list to add it to the **Commands** field.

:::

Step 13 Verify that the output for each switch displays an NTP server IP address with stratum level, poll interval, and time accuracy information.

NOTE:

NTP synchronization can take several minutes to complete. If a hostname was used instead of an IP address, complete the next step to configure DNS for the fabric before NTP verification.

Configure DNS for the Fabric

Use the DNS wizard to enter DNS host details and associate them with all fabric switches. The DNS servers must be reachable from the data center management LAN.

At the completion of this procedure, the data center switches can resolve DNS hostnames to IP addresses.

Step 1 On the Guided Setup menu, select DNS CONFIGURATION.

NETWORK	DISTRIBUTED SERVICES
Network S Perform the for your system.	Setup Ilowing steps to initialize and configure
Discov	HES ver new Switches.
FABRI Add a	C Fabric to the system.
Selected Fabr	ic:
RSVDC-FB1	× *
Assign	N SWITCH TO FABRIC Switch To Fabric
Config	ONFIGURATION ure Switch NTP.
ONS C Config	ONFIGURATION ure Switch DNS.
Config	ONFIGURATION ure VSX Switch Pairing.

Step 2 On the Name page, enter a Name and Description, then click NEXT.

DNS Config	uration			? ×
Name	Settings	Application	Summary	
Enter a required Nam	e and an optional Description.			
Name *	RSVDC-FB1-DNS Any non empty string, example: dns-fabric			
Description	DNS servers for RSVDC Fabric 1 Example: DNS Configuration settings for DNS Config 1			
(* = Required)			CANCEL BACK N	IEXT

Step 3 On the **Settings** page, enter the **Domain Name**. Enter a valid DNS server IP address in the **Name Servers** field. Press the TAB or ENTER key to complete the server entry.

DNS Configuration							
Name	Settings Application Summary						
Enter the required [Domain Name or Domain List, and any Name Servers.						
Domain Name *	example.local						
	Any valid Domain Name, example: mynet.com						
Domain List	Domain Name specified.						
	A valid list of Domains, example: mynet.com, mynet.org						
Name Servers *	10.2.120.98						
	Create option "10.2.120.98"						
(* = Required)	CANCEL BACK	IEXT					

Step 4 Create additional entries as needed. After all required DNS servers are entered, click NEXT.

DNS Cont	figuration	? ×					
	 ? 						
Name	Settings Application Summary						
Enter the required I	Jomain Name or Domain List, and any Name Servers.						
Domain Name *	example.local						
	Any valid Domain Name, example: mynet.com						
Domain List	Domain Name specified.						
	A valid list of Domains, example: mynet.com, mynet.org						
Name Servers *	× 10.2.120.98 × 10.2.120.99	• × •					
	A valid IPv4 or IPv6 address, example: 192.168.1.10, 2001:db8:85a3::1234. Maximum of 3 allowed.						
(* = Required)	CANCEL BACK	NEXT					

Step 5 On the Application page, select the name of the fabric in the Fabrics field and click NEXT.

DNS Configu	ıration			?
			?	
Name	Settings	Application	Summary	
Select the Fabric or Sw	itches in which to apply this configuration	on. A Fabric implies all Switches	contained within it.	
Fabrics	× RSVDC-FB1			× -
Switches	Not applicable when a Fabric is sele			
(* – Required)				NEXT
(= nequired)			BAOK	

Step 6 On the **Summary** page, verify that the information is entered correctly and click **APPLY**.

DNS Configuration					? 🗙
Name	Settings	Application		Summary	
Name	RSVDC-FB1-DNS				
Description	DNS servers for RSVI	DC Fabric 1			
Domain Name	example.local				
Domain List					
Name Servers	10.2.120.98				
	10.2.120.99				
Fabrics	RSVDC-FB1				
Switches					
				PACK	
			CANCEL	BACK	APPLY

Configure VSX on Leaf Switches

VSX enables a pair of ToR leaf switches to appear as a single logical switch to downstream hosts using multi-chassis link aggregation. VSX improves host availability in case of switch failure or maintenance downtime. Fabric Composer automatically identifies VSX switch pairs and configures them with the values supplied in the VSX wizard. Resource Pool wizards create IP and MAC address objects. The Fabric Composer CLI Command Processor verifies VSX operational status.

The diagram below highlights leaf and border leaf VSX pairs created in this procedure.



Step 1 On the Guided Setup menu, select VSX CONFIGURATION.

NET	WORK	DISTRIBUTED SERVICES	
Netw	ork Set	tup	
Perforn your sy	n the follov stem.	wing steps to initialize and co	nfigure
	SWITCHE Discover r	s new Switches.	
	FABRIC Add a Fat	oric to the system.	
Selecte	ed Fabric:		
RSVI	DC-FB1		$\times =$
	ASSIGN S Assign Sw	WITCH TO FABRIC vitch To Fabric	
()	NTP CONF Configure	FIGURATION Switch NTP.	
۲	DNS CON Configure	FIGURATION Switch DNS.	
R	VSX CONI Configure	FIGURATION VSX Switch Pairing.	
~	L3 LEAF-S Configure	SPINE CONFIGURATION L3 Leaf-Spine Connections.	

Step 2 On the Create Mode page, leave Automatically generate VSX Pairs selected and click NEXT.

ह्य VSX (RSVD	C-FB1)						? ×	
Create Mode	? Name	Inter-Switch Link Settings	Reep Alive Interfaces	Reep Alive Settings	Options	Summary		
Select an option to cre single VSX Pair. Automatically gene Ports used to interconn	Select an option to create the VSX Pair(s). Choose to automatically generate the VSX Pairs based on discovered connection data or manually configure a single VSX Pair. Automatically generate VSX Pairs Ports used to interconnect switches must be enabled and have LLDP enabled in order to discover VSX pairs. 							
 Manually configure 	a VSX Pair							
(* = Required)					CANCEL	BACK	IEXT	

Step 3 On the Name page, enter a Name Prefix and Description, then click NEXT.

ह्न VSX (RSVE	DC-FB1)						? ×
Create Mode	Name	Inter-Switch Link Settings	Keep Alive Interfaces	Reep Alive Settings	O ptions	Summary	
Enter a required Nam	e Prefix and an op	tional Description.					
Name Prefix *	RSVDC-FE	31-VSX					
	Any non empty s	string, example: MyVsxPair					
Description	VSX pair c	onfiguration for RSVDC	Fabric 1				
	Example: VSX F	Pair					
(* = Required)					CANCEL	BACK	IEXT

Step 4 On the Inter-Switch Link Settings page, leave the default values and click NEXT.

ह्य VSX (RSVDC	-FB1)						? ×
Create Mode	Name	Inter-Switch Link Settings	Reep Alive Interfaces	Reep Alive Settings	Options	? Summary	
Specify the required Hel Links.	lo and Peer Detec	t Intervals as well as th	e Hold Time and	Timeout. This will be appli	ed to the automatic	cally generated Inter	r-Switch
Hello Interval *	1						
	A number of second	is between 1 and 5, example	: 1				
Peer Detect Interval *	300						
	A number of second	ls between 60 and 600, exar	nple: 300				
Hold Time *	0						
	A number of second	is between 0 and 3, example	: 0				
Timeout *	20						
	A number of second	Is between 2 and 20, examp	le: 20				
(* = Required)					CANCEL	BACK	EXT

Step 5 On the **Keep Alive Interfaces** page, select *Point-to-Point* as the **Interface Mode**. Click **ADD** to launch the **Resource Pool** wizard.

民 VSX (RSVD	C-FB1)						⊘ 🗙
Create Mode	Name	Inter-Switch Link Settings	Reep Alive Interfaces	Reep Alive Settings	Options	Summary	
Specify the required Ke Switch members.	ep Alive Interface at	ttributes. This will be t	used to automatic	ally generate and associa	ate IP Interfaces of	the selected type to	the VSX
Interface Mode	Point-to-Point						× •
Select or add an IPv4 A to the generated IP Inte	ddress Resource Po rfaces.	ool or specify an IPv4	subnetwork. The	set of addresses will be u	utilized to automatic	cally assign IPv4 Ad	dresses
IPv4 Address Resource Pool	Select					▼	ADD
IPv4 Subnetwork Address	A valid IPv4 Subnet i	n CIDR format. Example: 1	92.168.1.0/24				
(* = Required)					CANCEL	BACK	EXT

NOTE:

The **Resource Pool** wizard is launched in this step to create an object representing the IPv4 address range used for underlay loopback interfaces on all switches, VSX keep-alive interfaces, and routed transit VLAN interfaces on VSX pairs. A resource pool is a reusable object that ensures consistency and reduces errors when adding switches to the fabric in the future.

Step 6 Resource Pool wizard: On the **Name** page, enter a **Name** and **Description** for the IPv4 address pool, then click **NEXT**.

🗊 Resource	Pool			×		
	Name	Settings	Summary			
Enter a required Name and an optional Description.						
Name *	RSVDC-FB1-LOOP-VSX-IP					
	Any unique non empty string, example: ResourcePool-1					
Description	Loopback, VSX keep-alive, and VSX routed transit VLAN interface IP pool					
	Example: ResourcePool-1 description					
([*] = Required)			CANCEL BACK N	IEXT		

Step 7 Resource Pool wizard: On the **Settings** page, enter an IPv4 address block in the **Resource Pool** field and click **NEXT**.

🗊 Resource Po	loc		×		
N	ame	Settings	Summary		
Select a required resou	urce type and a set/range of r	esources.			
Resource Type	IPv4				
Resource Pool *					
	A set and/or ranges of IPv4 Addresses up to 65535 addresses. Ranges may be defined as a hyphenated range or subnet using CIDR notation. Example: 192.168.1.100-192.168.1.200, 192.168.1.0.0/24. Cannot include multicast addresses.				
Resource Count	Resource Count 510				
(* = Required)			CANCEL BACK NEXT		
NOTE					
NOTE:					
This IPv4 address block is used to allocate IP addresses to loopback interfaces (/32) for all fabric					
switches, VSX keep-alive point-to-point interfaces (/31), and routed transit VLAN interfaces on					
entire fabric.					

Step 8 Resource Pool wizard: On the **Summary** page, verify the IP address pool information and click **APPLY**. The **Resource Pool** wizard closes and returns to the main **VSX Configuration** workflow.

🗊 Resource Po	ool			×
Na	ame	Settings	Summary	
Name	RSVDC-FB1-LOOP-V	/SX-IP		
Description	Loopback, VSX keep	-alive, and VSX routed transit VLAN inte	rface IP pool	
Resource Type	IPv4			
Resource Pool	10.250.0.0/23			
Resource Count	510			
			CANCEL BACK A	PPLY

Step 9 On the **Keep Alive Interfaces** page, verify that the new **IPv4 Address Resource Pool** is selected and click **NEXT**.

民 VSX (RSVD	C-FB1)						? ×
Create Mode	Name	Inter-Switch Link	Keep Alive	Reep Alive Settings	O ptions	Summary	
Specify the required Ke	Settings Interfaces Specify the required Keep Alive Interface attributes. This will be used to automatically generate and associate IP Interfaces of the selected type to the						
Interface Mode	Point-to-Po	int					× -
Select or add an IPv4 Address Resource Pool or specify an IPv4 subnetwork. The set of addresses will be utilized to automatically assign IPv4 Addresses to the generated IP Interfaces.							
IPv4 Address Resource Pool	RSVDC-FB1-LOOP-VSX-IP (10.250.0.0/23) × •				ADD		
IPv4 Subnetwork Address	A valid IPv4 Sub	onet in CIDR format. Example:	192.168.1.0/24. Can	not include multicast addresse:	з.		
(* = Required)					CANCEL	ВАСК	NEXT

Step 10 On the Keep Alive Settings page, leave the default values and click NEXT.
ह्य VSX (RSVE	DC-FB1)	⑦ ×
Create Mode	Name Inter-Switch Link Keep Alive Keep Alive Settings Options Summary	
Specify the required H	Hello and Dead Intervals as well as the UDP Port to be used for the Keep Alive Interfaces.	
Hello Interval *	1	
	A number of seconds between 1 and 5, example: 1	
Dead Interval *	3	
	A number of seconds between 2 and 20, example: 3	
UDP Port *	7678	
	A number between 1024 and 65535, example: 7678	
([*] = Required)	CANCEL BACK	NEXT

Step 11 On the **Options** page, enter the value *600* for the **Linkup Delay Timer** field. Click **ADD** to launch the **Resource Pool** wizard.

民 VSX (RSVDC	-FB1)						? ×
					?	?	
Create Mode	Name	Inter-Switch Link Settings	Keep Alive Interfaces	Keep Alive Settings	Options	Summary	
Set the required Linkup	Delay Timer, an	d System MAC Address.					
Linkup Delay Timer *	600						
	A number of sec	conds between 0 and 600, exam	ple: 180				
Set the System MAC Ad	dress Range. S	elect or add a MAC Addr	ess Resource Po	ol or specify a range.			
MAC Address	Select					~	ADD
Resource Pool							
MAC Address Range							
	A hyphen-separ	ated range of valid MAC Addres	ses, example: 02:00:0	00:00:01:00-02:00:00:00:01:FF			
Disable Split Recover	ery Mode						
					CANCEL	BACK	IEVT
(= Requirea)					CANCEL	BACK	IEAT
NOTE:							

It is recommended to set a 600-second **Linkup Delay Timer** value on CX 10000 switches using firewall policy to ensure that policy and state have synchronized before forwarding traffic attached on a multi-chassis LAG.

Step 12 Resource Pool wizard: On the **Name** page, enter a **Name** and **Description** for the system MAC address pool. Click **NEXT**.

🗊 Resource	e Pool		×
	Name	Settings	Summary
Enter a required N	ame and an optional Descrip	tion.	
Name *	RSVDC-FB1-VSX	MAC	
	Any unique non empty str	ng, example: ResourcePool-1	
Description	VSX system-MAC	address pool for RSVDC Fabric 1	
	Example: ResourcePool-1	description	
(* = Required)			CANCEL BACK NEXT

Step 13 Resource Pool wizard: On the **Settings** page, enter a MAC address range to be used for the VSX system MAC addresses, then click **NEXT**.

🗊 Resource F	Pool
	Name Settings Summary
Select a required res	source type and a set/range of resources.
Resource Type	MAC Address 🗸
Resource Pool *	02:00:00:10:00-02:00:00:10:FF
	A range of MAC Addresses up to 1000 addresses. Example: 00:00:00:00:00:00:00:00:00:00:00:00:00
Resource Count	256
(* = Required)	CANCEL BACK NEXT

Step 14 Resource Pool wizard: On the **Summary** page, verify the system MAC address pool information and click **APPLY**. The **Resource Pool** wizard closes and returns to the main **VSX Configuration** workflow.

🔋 Resource Pool		×
Name	Settings	Summary
Name	RSVDC-FB1-VSX-MAC	
Description	VSX system-MAC address pool for RSVDC Fabric 1	
Resource Type	MAC Address	
Resource Pool	02:00:00:00:10:00-02:00:00:00:10:FF	
Resource Count	256	
		CANCEL BACK APPLY

Step 15 On the **Options** page, verify that the new **MAC Address Resource Pool** is selected and click **NEXT**.

民 VSX (RSVD	C-FB1)						? ×
						?	
Create Mode	Name	Inter-Switch Link Settings	Keep Alive Interfaces	Keep Alive Settings	Options	Summary	
Set the required Linku	o Delay Timer, a	and System MAC Addre	SS.				
Linkup Delay Timer	600						
*	A number of see	conds between 0 and 600, ex	ample: 180				
Set the System MAC A	ddress Range.	Select or add a MAC A	ddress Resource	Pool or specify a range.			_
MAC Address Besource Pool	RSVDC-FE	31-VSX-MAC (02:00:00:0	00:10:00-02:00:0	0:00:10:FF)		× •	ADD
MAC Address Range	A humbon conce	rated range of valid MAC Add	access exemples 000	0.00.00.01.00.00.00.00.01.	FF		
Instable Split Recovery Mode							
(* = Required)					CANCEL	BACK	NEXT

Step 16 On the **Summary** page, verify the complete set of VSX settings and click **APPLY**.

民 VSX (RSVDC-FB1)		? ×
Create Mode Name	Inter-Switch Link Keep Alive Keep Alive Settings Options Summary	
Name Prefix	RSVDC-FB1-VSX	
Description	VSX pair configuration for RSVDC Fabric 1	
ISL Hello Interval	1	
ISL Peer Detect Interval	300	
ISL Hold Time	0	
ISL Timeout	20	
Keep Alive Interface Mode	Point-to-Point	
IPv4 Address Resource Pool	RSVDC-FB1-LOOP-VSX-IP (10.250.0.0/23)	
Keep Alive Hello Interval	1	
Keep Alive Dead Interval	3	
Keep Alive UDP Port	7678	
Linkup Delay Timer	600	
MAC Address Resource Pool	RSVDC-FB1-VSX-MAC (02:00:00:10:00-02:00:00:10:FF)	
Split Recovery Disabled	No	
	CANCEL BACK A	PPLY

Step 17 Guided Setup displays the list of VSX pairs in the **Configuration / Network / VSX** window. Review the information to verify that the VSX pairs created are consistent with physical cabling.

Configuration / Network / VSX			
	Fabric RSVDC-FB1		
Health 1	I Name ↓	Primary Switch	Primary Switch ISL LAG
Select Health	Enter Regex for Name	Enter Regex for Primary Switc	Enter Regex for Primary Switc
HEALTHY	RSVDC-FB1-VSX_RSVDC-FB1-	RSVDC-FB1-LF3-1	ISL-RSVDC-FB1-LF3-1
	LF3-2_RSVDC-FB1-LF3-1		
HEALTHY	RSVDC-FB1-VSX_RSVDC-FB1-	RSVDC-FB1-LF2-2	ISL-RSVDC-FB1-LF2-2
	LF2-1_RSVDC-FB1-LF2-2		
O HEALTHY	RSVDC-FB1-VSX_RSVDC-FB1-	RSVDC-FB1-LF1-2	ISL-RSVDC-FB1-LF1-2
	LF1-1_RSVDC-FB1-LF1-2		

NOTE:

VSX **Health** status in Fabric Composer can update slowly. Click the **Refresh** button in the upper right of the **Configuration / Network / VSX** window to refresh the switch status manually.

Step 18 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**

Show Commands DISTRIBUTED SERVICES	🕸 🔁 Y	ा ि ि admin ► ? ►	
DISTRIBUTED SERVICES	>_ Show Commands	DISTRIBUTED SERVICES	
	Configuration Editor		

Step 19 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < All leaf switches >
- **Commands:** *show vsx status*

>_ CLI Command	Processor	×
Select Fabrics or Switche	s, and select or add Saved Commands that can be customized. Press Run for results.	
Fabrics	Not applicable when a Switch is selected.	~
Switches	× RSVDC-FB1-LF1-1 × RSVDC-FB1-LF1-2 × RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-LF3-1 × RSVDC-FB1-LF3-2	× •
Saved Commands	Select from Saved Commands or Add new commands.	E
Commands	show vsx status	
	A comma separated list of commands to be run.	
Download Options	Download Results Download JSON Data	
Results	Switch : RSVDC-FB1-LF1-1 Command : show vsx status VSX Operational State 	
	ISL channel : In-Sync ISL mgmt channel : operational Config Sync Status : In-Sync NAE : peer_reachable HTTPS Server : peer_reachable	
	Attribute Local Peer	
	ISL link lag256 lag256 ISL version 2 2 System MAC 02:00:00:00:10:02 02:00:00:00:10:02 Platform 10000 10000 Software Version DL.10.13.1050 DL.10.13.1050 Device Role secondary primary	
	Switch : RSVDC-FB1-LF1-2 Command : show vsx status VSX Operational State 	
(* = Required)	CANCEL	RUN

Step 20 Verify that each switch has both **Local** and **Peer** information populated with the following values:

- ISL channel: In-Sync
- ISL mgmt channel: operational
- Config Sync Status: In-Sync
- **NAE:** *peer_reachable*

• HTTPS Server: peer_reachable

Configure Layer 3 Leaf-to-Spine Connections

Fabric Composer automatically identifies leaf-to-spine connections and configures them with the values supplied in the **Leaf-Spine** wizards. A resource pool is created to assign IP addresses to routed leaf and spine interfaces using /31 subnets. At the completion of this procedure, IP addresses are assigned to all interfaces required to support deployment of the OSPF fabric underlay.

Step 1 On the **Guided Setup** menu, select **L3 LEAF-SPINE CONFIGURATION** to start the **Leaf-Spine** workflow.



Step 2 On the **Create Mode** page, leave **Automatically generate Leaf-Spine Pairs** selected and click **NEXT**.

ĸ Leaf-Spine (RSVDC-FB1)		×
Create Mode	? Name	Settings	Summary
Select an option to create the L3 Leaf-Sp manually configure a single L3 Leaf-Spir	pine Pair(s). Choose to automa ne Pair.	tically generate the L3 Leaf-Spine Pa	irs based on discovered connection data or
Automatically generate L3 Leaf-Spin	e Pairs		
O Manually configure an L3 Leaf-Spine	Pair		
(* = Required)			CANCEL BACK NEXT

Step 3 On the Name page, enter a Name Prefix and Description, then click NEXT.

⊷ Leaf-Spine (RSVDC-FB1)		×
		?	?
Create Mod	de Name	Settings	Summary
Enter a required Name	Prefix and an optional Description.		
Name Prefix *	RSVDC-FB1-LF-SP		
	Any non empty string, example: MyLeafSpinePair		
Description	Routed point-to-point links between RSVE	DC Fabric 1 switches	
	Example: Leaf-Spine Pair		
(* = Required)			CANCEL BACK NEXT

Step 4 On the Settings page, click ADD to launch the Resource Pool wizard.

⊷a Leaf-Spine (R	SVDC-FB1)	×
Create Mode	Name Settings	Summary
Select or add an IPv4 Ad Addresses to the generat IPv4 Address	Idress Resource Pool or specify an IPv4 subnetwork. The set of addresses will be utilize ted IP Interfaces.	ed to automatically assign IPv4
Resource Pool IPv4 Subnetwork		
Address	A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24	
(* = Required)		CANCEL BACK NEXT

Step 5 Resource Pool wizard: On the **Name** page, enter a **Name** and **Description** for the IPv4 address pool, then click **NEXT**.

🕞 Resource	Pool		×
	Name	Settings	Summary
Enter a required Na	ame and an optional Description.		
Name *	RSVDC-FB1-P2P-IP		
	Any unique non empty string, example: R	esourcePool-1	
Description	Spine/leaf routed underlay link	address pool for RSVDC Fabric 1	
	Example: ResourcePool-1 description		
(* = Required)			CANCEL BACK NEXT

Step 6 Resource Pool wizard: On the **Settings** page, enter an IPv4 address block in the **Resource Pool** field and click **NEXT**.

Resource Po	loc		×
N	Jame	Settings	Summary
Select a required reso	urce type and a set/range of i	resources.	
Resource Type	IPv4		
Resource Pool *	10.255.0.0/23		
	A set and/or ranges of IPv4 Add 192.168.1.100-192.168.1.200, 1	iresses up to 65535 addresses. Ranges may be defined as 192.168.10.0/24. Cannot include multicast addresses.	s a hyphenated range or subnet using CIDR notation. Example:
Resource Count	510		
(* = Required)			CANCEL BACK NEXT
NOTE:			
Use a subnet	t distinct from oth	per subnets used in the over	day networks. The assigned sub-
net is used to	o configure routed	l ports between fabric switc	hes. Use a block large enough to
accommodat	e anticipated fabr	ic growth.	

Step 7 Resource Pool wizard: On the **Summary** page, verify the IP address pool information and click **APPLY**. The **Resource Pool** wizard closes and returns to the main **Leaf-Spine Configuration** workflow.

Resource Pool			×
Name	RSVDC-FB1-P2P-IP	Summary	
Description	Spine/leaf routed underlay link address pool for RSVDC Fabric 1		
Resource Type	IPv4		
Resource Pool	10.255.0.0/23		
Resource Count	510		
		CANCEL BACK AP	PLY

Step 8 On the **Settings** page, verify that the new **IPv4 Address Resource Pool** is selected and click **NEXT**.

⊷ ª Leaf-Spine (RSVDC-FB1)	×
Create Moo	de Name Settings Summary	
Select or add an IPv4 A Addresses to the gene	Address Resource Pool or specify an IPv4 subnetwork. The set of addresses will be utilized to automatically assign IPv prated IP Interfaces.	<i>v</i> 4
IPv4 Address Resource Pool	RSVDC-FB1-P2P-IP (10.255.0.0/23) × 🔻	ADD
IPv4 Subnetwork Address	A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24. Cannot include multicast addresses.	
(* = Required)	CANCEL BACK	NEXT

Step 9 On the **Summary** page, verify that the information is correct and click **APPLY**.

🛩 Leaf-Spine (RSVDC-FB1)				×
Create Mode	Name	Settings	Summary	
Name Prefix Description IPv4 Address Resource Pool	RSVDC-FB1-LF-SP Routed point-to-poi RSVDC-FB1-P2P-IF	int links between RSVDC Fabric 1 s 2 (10.255.0.0/23)	witches	
			CANCEL BACK A	PPLY

Step 10 Guided Setup displays the list of leaf-to-spine links in the **Configuration/Network/Leaf-Spine** window. Review the information to verify that the leaf-spine links created are consistent with physical cabling.

Configuration / Ne	twork / Leaf-Spine			Fa	abric	RSVDC-FB1		Ÿ
	ℤ Name	Æ	Spine Switch	Spine Interface	Sp	pine Status	1E	Leaf Switch
	Enter Regex for Name		Enter Regex for	Enter Regex for Spine Interface		Select Spine Status	~	Enter Regex for Leaf
0	RSVDC-FB1-LF-SP-RSVDC-FB1-SP1:1/1/1:1-RSVDC-FB1-LF1-1:1/1/53		RSVDC-FB1-SP1	Leaf Spine RPI on 1/1/1:1 - 10.255.0.2/31	Co	onnection Established		RSVDC-FB1-LF1-1
0	RSVDC-FB1-LF-SP-RSVDC-FB1-SP1:1/1/1:2-RSVDC-FB1-LF1-2:1/1/53		RSVDC-FB1-SP1	Leaf Spine RPI on 1/1/1:2 - 10.255.0.4/31	Co	onnection Established		RSVDC-FB1-LF1-2
0	RSVDC-FB1-LF-SP-RSVDC-FB1-SP1:1/1/2:1-RSVDC-FB1-LF2-1:1/1/53		RSVDC-FB1-SP1	Leaf Spine RPI on 1/1/2:1 - 10.255.0.6/31	Co	onnection Established		RSVDC-FB1-LF2-1
0	RSVDC-FB1-LF-SP-RSVDC-FB1-SP1:1/1/2:2-RSVDC-FB1-LF2-2:1/1/53		RSVDC-FB1-SP1	Leaf Spine RPI on 1/1/2:2 - 10.255.0.0/31	Co	onnection Established		RSVDC-FB1-LF2-2

Configure Server Access Switch Links

Fabric Composer refers to server access switches as subleaf switches. Compute and storage hosts are typically attached directly to leaf switches. Server access switches are primarily used to achieve two objectives: they provide a transition strategy to connect existing server infrastructure into an EVPN-VXLAN fabric, and they provide an economical strategy to support a large number of 1 Gbps connected hosts. Server access switches extend Layer 2 services from the leaf, but do not participate directly in underlay routing or overlay virtualization mechanisms.

The following procedure establishes an MC-LAG between a VSX leaf pair and a downstream VSF server access switch stack. The LAGs defined on both sets of switches are 802.1Q trunks that allow all VLANs.

The diagram below highlights the server access MC-LAG created in this procedure.



Step 1 On the Configuration > Network > Leaf-Spine page, click SUBLEAF-LEAF.

Configuration / Ne	etwork / Leaf-Spine				
	Fabric	RSVDC-FB1			
L3 LEAF-SPIN	L2 LEAF-SPINE SUBLEAF-LEAF				
				ତ \ \ \ \ \ \ \ \ \ C	ACTIONS V
	♂ Name	μE.	Spine Switch	Spine Interface	1E
	Enter Regex for Name		Enter Regex for Sp	Enter Regex for Spine In	terface
0	RSVDC-FB1-LF-SP-RSVDC-FB1-SP1:1/1/1:1-I	RSVDC-FB1-LF1-1:1/1/55	RSVDC-FB1-SP1	Leaf Spine RPI on 1/1/1:1 -	10.255.0.14/31
0	RSVDC-FB1-LF-SP-RSVDC-FB1-SP1:1/1/1:2-	RSVDC-FB1-LF1-2:1/1/55	RSVDC-FB1-SP1	Leaf Spine RPI on 1/1/1:2 -	10.255.0.16/31

Step 2 On the ACTIONS menu, select Add.

Configuration / Network / Leaf-Spine										
	Fabric	RSVDC-FB1								
L3 LEAF-SPINE L2 LEAF-SPINE	SUBLEAF-L	LEAF								
						\otimes	70	C	ACTIONS	•
Leaf Switch	J≞ Le	eaf Status	ĻĒ	Leaf LAG		1E	Lea	Add		
Enter Regex for Leaf S	witch	Enter Regex for L	eaf Status	Enter Rege	x for Leaf LAG		E	Edit		
								Delete	9	
								Delete	e All	

Step 3 When prompted to continue, click OK.

Discover SubLeaf-Leaf pairs		×
This will automatically discover and generate SubLeaf-Leaf switch pairs within the selected fabric.		
It is recommended to create subleaf VSX switch pairs before discovering SubLeaf-Leaf switch pairs.		
Would you like to continue?		
	CANCEL	ок

Step 4 Review the leaf and server access MC-LAG information. Verify that the values in the **Leaf LAG Status** and **SubLeaf LAG Status** columns are *up*.

Configuration / Ne	atwork / Leaf-Spine			Fabric BSVDC-FB1	~			
L3 LEAF-SPINE	E L2 LEAF-SPINE	SUBLEAF-LEAF						
							Þ	STO C ACTIONS -
	Leaf Switch	Leaf Status 1	Leaf LAG	Leaf LAG Status ↓	SubLeaf Switch	SubLeaf Status	SubLeaf LAG	SubLeaf LAG Status
	Enter Regex for Leaf §	Enter Regex f	Enter Regex for Leaf LAG	Enter Regex for	Enter Regex for SubLeaf Swite	Enter Regex for	Enter Regex for SubLeaf LAG	Enter Regex for SubLeaf LAG
0	RSVDC-FB1-LF3-1	up	subleaf_leaf_mlag_RSVDC-FB1-	up	RSVDC-FB1-LF3-SA1	up	subleaf_leaf_lag_RSVDC-FB1-	up
			LF3-2_1/1/13_RSVDC-FB1-LF3-				LF3-SA1_2/1/28_1/1/28	
			1_1/1/13					
0	RSVDC-FB1-LF3-2	up	subleaf_leaf_mlag_RSVDC-FB1-	up	RSVDC-FB1-LF3-SA1	up	subleaf_leaf_lag_RSVDC-FB1-	up
			LF3-2_1/1/13_RSVDC-FB1-LF3-				LF3-SA1_2/1/28_1/1/28	
			1_1/1/13					
NOT	'E:							
								<i>c</i> ,
The status field values may take a few minutes to populate and may require a screen refresh.								

Configure Underlay Network Routing

The HPE Aruba Networking data center spine-and-leaf design uses OSPF as the underlay routing protocol. The Fabric Composer **Underlay Configuration** wizard creates a transit VLAN between redundant ToRs to support routing adjacency, assigns IP addresses to loopback and transit VLAN interfaces, and creates underlay OSPF configuration. OSPF shares the loopback0 IP addresses for later use in establishing overlay routing. The Fabric Composer CLI Command Processor verifies OSPF adjacencies.

At the completion of this procedure, a functional underlay for the data center fabric is complete. The diagram below illustrates the assigned loopback IP addresses and the links where OSPF adjacencies are formed between leaf and spine switches.



Step 1 On the **Guided Setup** menu, select **UNDERLAYS** to start the **Underlay Configuration** work-flow.

NET	WORK	DISTRIBUTED SERVICES						
Netw Perform your sy	ork Set	up ving steps to initialize and configure						
	SWITCHES Discover r	SWITCHES Discover new Switches.						
	FABRIC Add a Fat	FABRIC Add a Fabric to the system.						
Selecte	d Fabric:							
RSVI	DC-FB1	× *						
	ASSIGN S Assign Sw	WITCH TO FABRIC itch To Fabric						
٩	NTP CONF Configure	Switch NTP.						
	DNS CONI Configure	FIGURATION Switch DNS.						
Ę	VSX CONF Configure	FIGURATION VSX Switch Pairing.						
P	L3 LEAF-S Configure	PINE CONFIGURATION L3 Leaf-Spine Connections.						
	L2 LEAF-S Configure	PINE CONFIGURATION L2 Leaf-Spine Connections.						
•	UNDERLA Configure	YS Underlays.						
9	OVERLAY Configure	<mark>s</mark> Overlays.						

Step 2 On the Name page, enter a Name and Description, then click NEXT.

🖌 Underlay	Configuration				? ×
Name	Underlay Type	Settings	(?) Max Metric	Summary	
Enter a required N	ame and an optional Description.				
Name *	RSVDC-FB1-UNDERLAY				
	Any non empty string, example: My Unde	rlay			
Description	OSPF underlay routing for RSV	/DC Fabric 1			
	Example: My Underlay Description				
(* = Required)			CA	NCEL BACK N	IEXT

Step 3 On the Underlay Type page, leave the default OSPF selection and click NEXT.

Underlay Co	nfiguration				⊘ 🗙
Name	Underlay Type	Settings	(?) Max Metric	Summary	
Select an Underlay typ	e. Only one of each Underlay config	juration type may be created.			
 OSPF eBGP 					
(* = Required)			C.	ANCEL BACK	NEXT

Step 4 On the **Settings** page, set the **Transit VLAN** to 3999. Leave other settings at their defaults and click **NEXT**.

Name Underlay Type Setting Nax Metric Summary Select or add an IPv4 Address Resource Pool or specify an IPv4 subnetwork. IPv4 Address Resource Pool Is ave empty to utilize Loopback addresses configured for VSX Imv Resource Pool Is ave empty to utilize Loopback addresses configured for VSX Imv Address Lasve empty to utilize Loopback addresses configured for VSX Imv Address Lasve empty to utilize Loopback addresses configured for VSX Address Auste IPv4 Subnet to CIOR format. Exempte: 192.108.1.024 Set the required Transt VLAN Helio and Dead Intervals, and Authentication Type. Tanst VLAN Imp Authentication Type Imv Authentication Type Imv Authentication Type None In ander Descent I and 6555, example: 10 Dead Interval Immediation Key Authentication Type None Authentication Type None Immediation Key Not Applicable Authentication Key Not Applicable Authentication Types<	Underlay Con	figuration (RSVDC-FB1)			(2) ×
Name Underlay Type Settings Max Metric Summary Select or add an IPv4 Address Resource Pool or specify an IPv4 subnetwork. IPv4 Address Leave empty to utilize Loopback addresses configured for VSX Impact Configured for VSX Impact Configured for VSX Resource Pool Impact Configured for VSX Impact Configured for VSX Impact Configured for VSX Address A valid IPv4 Subnetwork Leave empty to utilize Loopback addresses configured for VSX Impact Configured for VSX Address A valid IPv4 Subnetwork Leave empty to utilize Loopback addresses configured for VSX Impact Configured for VSX Address A valid IPv4 Subnetwork Leave empty to utilize Loopback addresses configured for VSX Impact Configured for VSX Address A valid IPv4 Subnetwork Leave empty to utilize Loopback addresses configured for VSX Impact Configured for VSX Address A valid IPv4 Subnetwork Leave empty to utilize Loopback addresses configured for VSX Address A valid IPv4 Subnetwork Impact Configured for VSX Address A valid IPv4 Subnetwork Impact Configured for VSX Authentication for of accords between 1 and 65535, example: 10 Impact Configured for VSX Authentication Key Not Applicable Impact Configured for VSX Authentication Key Not Applicable Impact Configured for VSX Authentication Key Not Applicable Impact Configured for VSX Authentication Rowarding Detection (BFD) Impact Configured for VSX Impact Configured Trapic <t< td=""><td></td><td></td><td></td><td>?</td><td>?</td><td></td></t<>				?	?	
Select or add an IPV4 Address Resource Pool IPv4 Address Resource Pool IPv4 Subnetwork Address Ausile IPv4 Subnet to Utilize Loopback addresses configured for VSX Address Ausile IPv4 Subnetwork Address Ausile IPv4 Subnetwork Address Ausile IPv4 Subnet to UBI format. Example: 102.183.1.024 Set the required Transit VLAN, Hello and Dead Intervals, and Authentication Type. Transit VLAN 3959 AVAN between 2 and 4094, example: 2. Helio Interval 0 Authentication Type Authentication Type None Authentication Key Not Applicable Authentication Key value. MDS Key ID Not Applicable Authentication Forwarding Detection (BFD) Enable Bidirectional Forwarding Detection (BFD) Enable SIMP Traps	Name	Underlay Type	Settings	Max Metric	Summary	
IPv4 Address Resource Pool IPv4 Subnetwork Address Address A valal IPv4 Subnetwork Address A valal IPv4 Subnet in CIDR format. Example: 192-186.1.024 Set the required Transit VLAN, Hello and Dead Intervals, and Authentication Type. Transit VLAN Transit VLAN 3999 A VLAN between 2 and 4094, example: 2. Hello Interval 10 A number of seconds between 1 and 6535, example: 10 Dead Interval Authentication Type None Authentication Type None Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable Authentication Ecowering Detection (BFD) I Enable Bidirectional Forwarding Detection (BFD) I Enable Reserve Interface I Enable SNMP Traps	Select or add an IPv4 Ad	dress Resource Pool or specify an IPv	/4 subnetwork.			
IPv4 Subnetwork Address Availd IPv4 Subnet in CIDR format. Example: 192:188.1.024 Set the required Transit VLAN, Helio and Dead Intervals, and Authentication Type. Transit VLAN* 3999 AVLAN between 2 and 4094, example: 2. Helio Interval* 10 Anumber of seconds between 1 and 65535, example: 10 Dead Interval* 40 Authentication Type None Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable Anumber of seconds Detection (BFD) © Enable Bidirectional Forwarding Detection (BFD) © Enable SNMP Traps	IPv4 Address Resource Pool	Leave empty to utilize Loopback	addresses configured for VS	X	Ţ AD	
Audiess Availat IPv4 Subret in CIDR format. Example: 192.188.1.024 Set the required Transit VLAN, Hello and Dead Intervals, and Authentication Type. Transit VLAN* 3999 A VLAN between 2 and 4094, example: 2. Hello Interval* 10 A number of seconds between 1 and 65535, example: 10 Dead Interval* 40 A number of seconds between 1 and 65535, example: 40 Authentication Type None Authentication Key Not Applicable Authentication Key value. Anumber of seconds between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Enable Bidirectional Forwarding Detection (BFD) Chable SNMP Traps Constit	IPv4 Subnetwork	Leave empty to utilize Loopback	addresses configured for VS>	<		
Set the required Transit VLAN, Hello and Dead Intervals, and Authentication Type. Transit VLAN* 3999 AVLAN between 2 and 4094, example: 2. Hello Interval* 10 A number of seconds between 1 and 65536, example: 10 Dead Interval* 40 Authentication Type None Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable A number of between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Enable Passive Interface Enable SNMP Traps	Address	A valid IPv4 Subnet in CIDR format. Example	e: 192.168.1.0/24			
Transit VLAN* 3999 A VLAN between 2 and 4094, example: 2. Hello Interval* 10 A number of seconds between 1 and 65535, example: 10 Dead Interval* 40 A number of seconds between 1 and 65535, example: 40 Authentication Type None Authentication Key Not Applicable Authentication Key value. Not Applicable A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) © Enable Passive Interface Enable SNMP Traps	Set the required Transit V	LAN, Hello and Dead Intervals, and A	uthentication Type.			11
A VLAN between 2 and 4094, example: 2. Hello Interval * 10 A number of seconds between 1 and 65535, example: 10 Dead Interval * 40 A number of seconds between 1 and 65535, example: 40 Authentication Type None Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) © Enable Passive Interface Enable SNMP Traps	Transit VLAN *	3999				
Hello Interval • 10 A number of seconds between 1 and 65535, example: 10 Dead Interval • 40 A number of seconds between 1 and 65535, example: 40 Authentication Type None Authentication Type None Authentication Key Not Applicable Authentication Key value. MD5 Key ID MD5 Key ID Not Applicable A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) • Enable Passive Interface • Enable SNMP Traps		A VLAN between 2 and 4094, example: 2.				
A number of seconds between 1 and 65535, example: 10 Dead Interval 40 A number of seconds between 1 and 65535, example: 40 Authentication Type None Authentication Type None Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable A number between 1 and 255, example 1 Image: Complete C	Hello Interval *	10				
Dead Interval* 40 A number of seconds between 1 and 65535, example: 40 Authentication Type None Authentication Key None Authentication Key Not Applicable Authentication Key value. Not Applicable MD5 Key ID Not Applicable Anumber between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Image: SNMP Traps		A number of seconds between 1 and 65535,	, example: 10			
A number of seconds between 1 and 65535, example: 40 Authentication Type Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Enable Passive Interface Enable SNMP Traps	Dead Interval *	40				
Authentication Type None X Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Image: Enable Passive Interface Enable SNMP Traps		A number of seconds between 1 and 65535,	, example: 40			
Authentication Key Not Applicable Authentication Key value. MD5 Key ID Not Applicable A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Image: Enable Passive Interface Enable SNMP Traps	Authentication Type	None			×	r
Authentication Key value. MD5 Key ID Not Applicable A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Enable Passive Interface Enable SNMP Traps	Authentication Key					
MD5 Key ID Not Applicable A number between 1 and 255, example 1 C Enable Bidirectional Forwarding Detection (BFD) C Enable Passive Interface Enable SNMP Traps		Authentication Key value.				
A number between 1 and 255, example 1 Enable Bidirectional Forwarding Detection (BFD) Enable Passive Interface Enable SNMP Traps	MD5 Key ID					
		A number between 1 and 255, example 1				
Enable Passive Interface Enable SNMP Traps CANCEL RACK NEXT	Enable Bidirectional I	Forwarding Detection (BFD)				
	Enable Passive Interf	ace				
	Enable SNMP Traps					
(= Hequired) Scroll for more options	(* = Required) Scr	oll for more options			CANCEL BACK NEXT	

NOTE:

Enter a VLAN ID that cannot be confused easily with other VLANs within the network.

Step 5 On the **Max Metric** page, enter the value *600* in the **On Startup** field. Leave other settings at their defaults and click **NEXT**.

Underlay Configure	ration				? ×
Name	Underlay Type	Settings	Max Metric	Summary	
Configure optional Router-LSA	s, On Startup Time, and Stub	Links			
✓ Advertise Router LSAs					
🗹 Include Stub Links					
On Startup	600				
	A number of seconds between 5 and	86400, example: 300			
(* = Required)			с	ANCEL BACK	NEXT

NOTE:

It is recommended to set a 600-second OSPF **On Startup** max metric value for CX 10000 switches using firewall policy in a VSX pair to ensure that policy and state have synchronized before fabric traffic is forwarded to the switch VTEP. The same value is applied to all switches in this sample fabric.

Step 6 On the **Summary** page, verify that the information is entered correctly and click **APPLY** to create the OSPF configuration.

 Underlay Configurat 	ion			0
Name	Underlay Type	Settings	Max Metric	Summary
Name		RSVDC-FB1-UNDERLA	λY	
Description		OSPF underlay routing	for RSVDC Fabric 1	
Underlay Type		OSPF		
Transit VLAN		3999		
IPv4 Subnetwork Address				
Hello Interval		10		
Dead Interval		40		
Authentication Type		None		
BFD Enabled		No		
Passive Interface Enabled		Yes		
SNMP Traps Enabled		No		
Router LSA Enabled		Yes		
Include Stub Links Enabled		Yes		
On Startup		600		
			C	ANCEL BACK APPLY

Step 7 In the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

Step 8 On the CLI Command Processor page, enter the following values, then click RUN.

• Fabrics: RSVDC-FB1

• Commands: show ip ospf neighbors

>_ CLI Command	Processor						×
Select Fabrics or Switches,	and select or add Sa	ved Command	ds that can be c	ustomized. Press Run for results			
Fabrics	× RSVDC-FB1						× •
Switches	Not applicable wh						~
Saved Commands	Select from Savec	Commands c	or Add new com	mands.		▼ ADD	REMOVE
Commands	show ip ospf neig	nbors					
	A comma separated list of	of commands to b	e run.				
Download Options	Download Results	Download J	SON Data				
Results	Switch : RSVDO VRF : default	-FB1-LF1-1	Command : s	show ip ospf neighbors Process : 1			
	Total Number of	• Neighbors	: 3				
	Neighbor ID	Priority	State	Nbr Address	Interface		
	10.250.0.9	n/a	FULL	10.255.0.2	1/1/53		
	10.250.0.10	n/a	FULL	10.255.0.12	1/1/54		
	10.250.0.13	n/a	FULL	10.250.0.19	vlan3999		
	Switch : RSVDO VRF : default	-FB1-LF1-2	Command : s	show ip ospf neighbors Process : 1			
	Total Number of	• Neighbors	: 3				
(* = Required)							CANCEL RUN

Step 9 Verify that each spine switch shows an OSPF neighbor adjacency in the "FULL" state for all leaf switches. Verify that all leaf VSX pairs show an OSPF neighbor adjacency in the "FULL" state between themselves over the routed transit VLAN in addition to an adjacency in the "FULL" state with each spine.

Configure Overlay Network Routing

The HPE Aruba Networking data center uses iBGP as the control plane for the fabric overlay within a single fabric. BGP provides a mechanism to build VXLAN tunnels dynamically and share host reachability across the fabric using the L2VPN EVPN address family. VTEP interfaces are the VXLAN encapsulation and decapsulation points for traffic entering and exiting the overlay. VSX leaf pairs share the same anycast VTEP IP address.

Use the Fabric Composer **Overlay Configuration** wizard to implement iBGP peerings using a private ASN and to establish VXLAN VTEPs. VTEP IP addresses are assigned as a switch loopback using a resource pool. iBGP neighbor relationships are verified using the Fabric Composer CLI Command Processor.

The diagram below illustrates the iBGP L2VPN EVPN address family peerings established using loopback interfaces between leaf switches and the two spines operating as iBGP route reflectors.



Step 1 From the **Guided Setup** menu, select **OVERLAYS** to start the **Overlay Configuration** work-flow.

NET	DISTRIBUTED SERVICES					
Netw Perform your sy	ork Set	up ving steps to initialize and co	nfigure			
	SWITCHES Discover r	s new Switches.				
	FABRIC Add a Fab	pric to the system.				
Selecte	ed Fabric:					
RSVI	DC-FB1		\times $-$			
	ASSIGN S Assign Sw	WITCH TO FABRIC vitch To Fabric				
•	NTP CONF Configure	Switch NTP.				
	DNS CONI Configure	FIGURATION Switch DNS.				
Ę	VSX CONF Configure	FIGURATION VSX Switch Pairing.				
	L3 LEAF-S Configure	SPINE CONFIGURATION L3 Leaf-Spine Connections.				
	L2 LEAF-S Configure	PINE CONFIGURATION L2 Leaf-Spine Connections.				
6	UNDERLA Configure	YS Underlays.				
9	OVERLAY Configure	<mark>s</mark> Overlays.				
9	EVPN CON Configure	FIGURATION EVPN Instances.				

Step 2 On the Name page, enter a Name and Description, then click NEXT.

G Overlay Co	onfiguration (RSVDC	-FB1)				? ×
	?	?	?	?	?	
Name	Overlay Type	iBGP Settings	IPv4 Network Address	Settings	Summary	
Enter a required Na	me and an optional Descriptio	n.				
Name *	RSVDC-FB1-OVERL	AY				
	Any non empty string, examp	ole: My Overlay				
Description	Routing/VTEP overla	v components for RS	VDC Fabric 1			
	Example: My Underlay Desc	ription				
(* = Required)				CANC	EL BACK	NEXT

Step 3 On the Overlay Type page, leave iBGP selected and click NEXT.

Gerlay Con	nfiguration (RSVDC-	FB1)			(? ×
Name	Overlay Type	iBGP Settings	Pv4 Network Address	Settings	Summary	
Select an Overlay type	e. Only one Overlay configur	ation may be created				
iBGP						
⊖ eBGP						
([*] = Required)				CANCEL	BACK	

Step 4 On the iBGP Settings page, enter the following settings, then click **NEXT**.

- Spine-Leaf ASN: 65001
- Route Reflector Servers: < Select two spine switches >

- Leaf Group Name: RSVDC-FB1-LF
- Spine Group Name: RSVDC-FB1-RR

Generation Overlay Con	figuration (RSVDC-FB1)	? ×
Name	Overlay Type iBGP Settings IPv4 Network Address Settings Summary	
Set the required Spine-	-Leaf ASN and optional iBGP fields.	
Spine-Leaf ASN *	65001	
	ASPLAIN notation between 1 and 4294967295 or ASDOT notation between 1 and 65535.65535, examples: 4294967295 and 65535.1	
Route Reflector	× RSVDC-FB1-SP1 × RSVDC-FB1-SP2	×·
Servers *	Select Spine switches.	
Leaf Group Name	RSVDC-FB1-LF	
	A string value for the BGP Peer Group name on Spine, example: 'leaf'. A default value will be set if empty.	
Spine Group Name	RSVDC-FB1-RR	
	A string value for the BGP Peer Group name on Leaf, example 'spine-RR'. A default value will be set if empty.	
([*] = Required)	CANCEL BACK N	ЕХТ
NOTE:		
Use a 2-byte / 4-byte ASN is	ASN in the private range of 64512-65534 for an easy-to-read switch configuration supported.	on. A

Step 5 On the IPv4 Network Address page, click ADD to launch the Resource Pool wizard.

Overlay Co	nfiguration (RSVDC-	·FB1)				? ×
Name	Overlay Type	iBGP Settings	Pv4 Network Address	Settings	Summary	
Set the required Loop	back IPv4 Network Address	i chi contrago		2		
IPv4 Address Resource Pool	Select				~	ADD
IPv4 Subnetwork Address	A valid IPv4 Subnet in CIDR f	ormat. Example: 192.168.	1.0/24. Cannot include multicast addres	SSES.		
(* = Required)				CANCEL	BACK	NEXT

Step 6 Resource Pool wizard: On the Name page, enter a Name and Description, then click NEXT.

🗊 Resource	Pool	0 ×
	Name Settings	Summary
Enter a required Na	me and an optional Description.	
Name *	RSVDC-FB1-VTEP-IP	
	Any unique non empty string, example: ResourcePool-1	
Description	VTEP IP address pool for RSVDC Fabric 1	
	Example: ResourcePool-1 description	
(* = Required)		CANCEL BACK NEXT

Step 7 Resource Pool wizard: On the **Settings** page, enter an IPv4 address block in the **Resource Type** field and click **NEXT**.

🗊 Resource Po	lool		@ ×
	Jame	Settings	Summary
Select a required resou	urce type and a set/range of re	sources.	,
Resource Type	IPv4		
Resource Pool *	10.250.2.0/24		
Resource Count	A set and/or ranges of IPv4 Addr 192.168.1.100-192.168.1.200, 15 254	esses up to 65535 addresses. Ranges may be defined as 22.168.10.0/24. Cannot include multicast addresses.	a hyphenated range or subnet using CIDR notation. Example:
([*] = Required)			CANCEL BACK NEXT
NOTE:			
This IPv4 adc VTEPs. Each	Iress block is used t member of a VSX le	to configure loopback addre eaf pair uses the same IP loo	esses on all leaf switches for VXLAN pback address.

Step 8 Resource Pool wizard: On the **Summary** page, verify the VTEP IP address pool information and click **APPLY**. The **Resource Pool** wizard closes and returns to the main **Overlay Configuration** workflow.

Resource Pool		? ×
Name	Settings	Summary
Name	RSVDC-FB1-VTEP-IP	
Description	VTEP IP address pool for RSVDC Fabric 1	
Resource Type	IPv4	
Resource Pool	10.250.2.0/24	
Resource Count	254	
		CANCEL BACK APPLY
		CANCEL BACK APPLY

Step 9 On the **IPv4 Network Address** page, verify that the new **IPv4 Address Resource Pool** is selected and click **NEXT**.

Overlay Co	nfiguration (RSVDC	-FB1)				? ×
Name	Overlay Type	iBGP Settings	IPv4 Network Address	Settings	Summary	
Set the required Loop	back IPv4 Network Address	5				
IPv4 Address Resource Pool	RSVDC-FB1-VTEP-IF	9 (10.250.2.0/24)			× -	ADD
IPv4 Subnetwork Address	A valid IPv4 Subnet in CIDR	format. Example: 192.168	.1.0/24. Cannot include multicast addr	esses.		
(* = Required)				CANC	EL BACK	NEXT

Step 10 On the Overlay Configuration Settings page, leave the default values and click NEXT.

Gerlay Con	figuration (RSVDC-	-FB1)				? ×
					?	
Name	Overlay Type	iBGP Settings	IPv4 Network Address	Settings	Summary	
Set the required Keep	Alive and Hold Down timers	S.				
Keep Alive Timer *	60					
	A number of seconds betwee	n 0 and 65535, example: 6	60			
Hold Down Timer *	180					••••]
	A number of seconds betwee	n 0 and 65535, example: 1	80			
Authentication						
Password						
(* = Required)				CANC	EL BACK	NEXT

Step 11 On the Summary page, verify that the iBGP information is correct, then click APPLY.

Overlay Configuration (RSVDC-FB1)					
Name Overlay Type	iBGP Settings IPv4 Network Address Settings Summa	ry			
Name	RSVDC-FB1-OVERLAY				
Description	Routing/VTEP overlay components for RSVDC Fabric 1				
Spine-Leaf ASN	65001				
Route Reflector Servers	RSVDC-FB1-SP1, RSVDC-FB1-SP2				
Leaf Group Name	RSVDC-FB1-LF				
Spine Group Name	RSVDC-FB1-RR				
IPv4 Address Resource Pool	RSVDC-FB1-VTEP-IP (10.250.2.0/24)				
Keep Alive Timer	60				
Hold Down Timer	180				
	CANCEL BACK	APPLY			

Step 12 In the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

Step 13 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select both route reflector spine switches >
- **Commands:** show bgp l2vpn evpn summary

>_ CLI Command	Processor							×
Select Fabrics or Switche	s, and select or add Saved Co	mmands that can be o	customized. Pres	s Run for re	sults.			
Fabrics	Not applicable when a Sw							~
Switches	× RSVDC-FB1-SP1 × R	× RSVDC-FB1-SP1 × RSVDC-FB1-SP2						
Saved Commands	Select from Saved Comm	Select from Saved Commands or Add new commands.						EMOVE
Commands	show bgp l2vpn evpn sun	show bgp I2vpn evpn summary						
	A comma separated list of comman	nds to be run.						
Download Options	Download Results Down	load JSON Data						
Results	Switch : RSVDC-FB1-SP1 Command : show bgp l2vpn evpn summary Codes: * Dynamic Neighbor VRF : default BGP Summary							
	Local AS	: 65001	BGP Router	Identif	ier : 10.	250.0.9		
	Peers	: 6	Log Neighb	or Change	es : Yes			
	Cfg. Hold Time Confederation Id	: 180 : 0	Cfg. Keep	Alive	: 60			
	Neighbor AdminStatus		Remote-A	S MsgRcvo	d MsgSent	Up/Down Time	e State	
	10.250.0.6		65001	6	6	00h:03m:19s	Established	Up
	10.250.0.7		65001	6	6	00h:03m:19s	Established	Up
	10.250.0.8		65001	6	6	00h:03m:19s	Established	Up
	10.250.0.11		65001	6	6	00h:03m:19s	Established	Up
	10.250.0.12		65001	6	6	00n:03m:205	Established	Up
	Switch : RSVDC-FB1- Codes: * Dynamic Nei VRF : default	SP2 Command : sho ghbor	ow bgp l2vpn	evpn sumr	nary			Cp.
(* = Required)							CANCEL	RUN

Step 14 Verify that both route reflectors show an L2VPN EVPN neighbor relationship in the "Established" state for all leaf switches.

Configure Overlay VRFs

An EVPN-VXLAN data center uses overlay VRFs to provide the Layer 3 virtualization and macro segmentation required for flexible and secure data centers. VRFs are distributed across all leaf switches. A VRF instance on one switch is associated to the same VRF on other leaf switches using a common L3 VNI and EVPN route-target, binding them together into one logical routing domain. VRFs are commonly used to segment networks by tenants and business intent. Use the **Virtual Routing & Forwarding** workflow to create overlay network VRFs and associate a VRF with an L3 VNI and EVPN route-target. The VNI and route target for each set of overlay VRFs must be unique to preserve traffic separation.

This guide uses a production VRF and development VRF as an example of route table isolation. TCP/IP hosts in one VRF are expected to be isolated from hosts in the other VRF. The diagram below illustrates the logical VRF overlay across all leaf switches.



NOTE:

The diagram above depicts the border leaf switches at the same horizontal level as all other leaf switches. This placement of the border leaf pair is a cosmetic preference for easier depiction of virtualization across leaf switches. The deployed topology is consistent with previous diagrams, but without the pictorial emphasis of the special role of the border leaf handling data center north/south traffic.Hosts attached to server access switches can be connected to subnets in either VRF by VLAN extension from the leaf switch, but the server access switches do not contain their own VRF definition.

Step 1 On the left menu, select **VRF**. If **VRF** does not appear in the left pane, select **Configuration > Routing > VRF** from the top menu.

orubo Fabric Compos	er Dashboar	d Configuration	✓ Ma	intenance	
🛞 VRF	si	Includes IP Interfaces, IP Static Routes, Underlays,			
🖧 BGP		and overlay		Fabric	

Step 2 On the ACTIONS menu on the right, select Add.

Configur	ation / Ro	outing / VRF						
			Fabric	DC1_Fabric				
							¥	C ACTIONS V
		Name	μE	Туре	ĻĒ	Switches	μE	Add
		Enter Name		Select Type	•	Enter Switches		Edit
	0	default	·	Default				Delete
	0	mgmt		Management				Reapply VRF



🛞 Virtual Rout	ing & Forwarding				? 🗙
Name	Cope	Routing	Route Targets	Summary	
Enter a required Name	e and an optional Description.				
Name *	PROD-DC-VRF				
	Any non empty string without spaces be	tween 1 and 92 characters, examp	le: VRF1.		
Description	Production VRF in data cente	roverlay			
	Example: New Virtual Routing and Forw	arding			
(* = Required)			CAI	NCEL BACK	NEXT

Step 4 On the **Scope** page, uncheck **Apply the VRF to the entire Fabric and all Switches contained within it**. Select the VSX leaf pairs in the **Switches** field, then click **NEXT**.

Ø Virtual Routing	& Forwarding (RSVD)	C-FB1)		(?) ×
Name	Scope	Routing	Route Targets	Summary
Set the scope of the VRF.	The VRF may be applied to all L	eaf and Border Leaf Switches	within the Fabric or to a specifi	c set of Switches.
Apply the VRF to the F	abric and all Leaf and Border Le	eaf Switches within it.		
Switches	X RSVDC-FB1-VSX_RSVDC-FB X RSVDC-FB1-VSX_RSVDC-FB V Device EB4 Vev Device EB	1-LF1-1_RSVDC-FB1-LF1-2 1-LF2-1_RSVDC-FB1-LF2-2		X T
([*] = Required)			CANC	EL BACK NEXT
NOTE:				
When a large n switches, then o not participate be configured c	number of leaf switc deselect spine and se in overlay virtualizat on them.	hes is present, clie erver access switch tion and do not pos	ck the SELECT ALL es. Spine and server ssess VTEPs, so over	button to select all access switches do lay VRFs should not

Step 5 On the **Routing** page, enter the following values to create a Layer 3 VNI and BGP route distinguisher * L3 VNI: 100001 * **Route Distinguisher**: *loopback1:1*

🛞 Virtual Routi	ng & Forwarding (RSV	DC-FB1)			Ø ×
		\bigtriangledown	(?)	?
Name	Scope	Routing	Route	Targets	Summary
Set the optional L3 VN	I and Route Distinguisher. L3 VN	Il is not applicable to Sub Le	eaf switches.		
L3 VNI	100001				
	A number between 1 and 16777214,	example 1			
Route Distinguisher	loopback1		× -	:	1
	Select Loopback value or enter a vali	d ASN, example: 65000.			A number between 0 and 65535,
					example 0
([*] = Required)					CANCEL BACK NEXT
NOTE:					
Refer to the "C)verlay Connectivity a	nd Addressing" se	ction abo	ve for a	a VNI numbering reference.

The Layer 3 VNI associates routes in an EVPN-VXLAN overlay with a VRF. The integer value in the **Route Distinguisher** should correlate to the VNI value without the addition of its 100,000 prefix for easier troubleshooting. The integer must be unique for each VRF.

Step 6 On the **Virtual Routing & Forwarding Route Targets** page, assign the following settings to add an EVPN route-target to the VRF, then click **ADD**.

- Route Target Mode: Both
- Route Target Ext-Community: 65001:100001
- Address Family: EVPN

Ø Virtual Routing	& Forwardin	g			? ×
Name	Sco	ppe Routing	Route Targets	Summary	
Enter the optional Route Ta	arget Mode and E	xt-Community. Enter both or none of	the fields.		
Route Target Mode	Both				× •
Route Target Ext- Community	65001:100001 A valid Autonomous S	ystem Number, example: 65001:101			
Address Family	EVPN				× -
CLEAR ADD	UPDATE				
Route Target Moo	de	Route Target Ext-Community	Address Family		
		There is no data	to display		
(* = Required)			с	ANCEL BACK NEX	Т
NOTE:					

Setting **Route Target Mode** to *Both* exports local switch VRF routes to BGP with the **Route Target Ext-Community** value assigned as the route target and imports BGP routes into the local VRF route table advertised by other switches with the same value.For **Route Target Ext-Community**, enter the private autonomous system number used in the "Configure Overlay Network Routing" procedure and the L3 VNI, separated by a colon. The L3 VNI is used in the BGP route target for logical consistency with the VXLAN L3 VNI. The complete route target value uniquely identifies a set of VRFs.

Step 7 Verify that the Route Targets information is correct and click NEXT.

Ø Virtual Routing) & Forwardin	g					? 🗙
Name	Sco	pe Rou	Juting F	Route Targets		? Summary	
Enter the optional Route T	arget Mode and E	t-Community. Enter both or	none of the fields.				
Route Target Mode	Select						~
Route Target Ext- Community Address Family	A valid Autonomous Sy Select	stem Number, example: 65001:101					•
Route Target Mo	de	Route Target Ext-Community	y Address Fami	ily			
Both		65001:100001	EVPN		$\uparrow \downarrow$		
(* = Required)				с	ANCEL	BACK	NEXT

Step 8 On the **Summary** page, verify that the complete set of VRF information is correct and click **APPLY**.

S Virtual Routing &	Forwarding (RSVD	C-FB1)			(3) >
Name	Scope	Routing	Route	Targets	Summary	
Name	PROD-DC-VR	F				
Description	Production VF	IF in data center overlay				
Switches	RSVDC-FB1-\	SX_RSVDC-FB1-LF1-1_R	SVDC-FB1-LF1-2			
	RSVDC-FB1-V	/SX_RSVDC-FB1-LF2-1_R	SVDC-FB1-LF2-2			
	RSVDC-FB1-V	/SX_RSVDC-FB1-LF3-2_R	SVDC-FB1-LF3-1			
Route Distinguisher	loopback1:1					
L3 VNI	100001					
Route Target Mode	Route	e Target Ext-Community		Address Famil	ly	
Both	6500	1:100001		EVPN		
				CAN	CEL BACK APPLY	

Step 9 Repeat this procedure for each additional overlay VRF.

Virtual Routing & I	Forwarding (RSVD	C-FB1)			0 >
Name	Scope	Routing	Route	Targets	Summary
Name	DEV-DC-VRF				
Description	Development	VRF in the data center ove	rlay		
Switches	RSVDC-FB1-V	SX_RSVDC-FB1-LF1-1_R	SVDC-FB1-LF1-2		
	RSVDC-FB1-V	SX_RSVDC-FB1-LF2-1_R	SVDC-FB1-LF2-2		
	RSVDC-FB1-V	SX_RSVDC-FB1-LF3-2_R	SVDC-FB1-LF3-1		
Route Distinguisher	loopback1:2				
L3 VNI	100002				
Route Target Mode	Route	a Target Ext-Community		Address Family	
Both	6500	1:100002		EVPN	
				CANC	EL BACK APPLY

Configure Overlay VLANs and SVIs

One or more VLANs within each VRF provide host connectivity. VLAN SVIs provide IP addressing within the fabric. The Fabric Composer **IP Interface** workflow creates consistent VLANs across all leaf switches within an overlay VRF. The workflow assigns an SVI IP address, a virtual gateway address, and a locally administered virtual MAC address to the VLAN interface on each leaf switch. Aruba Active Gateway permits the SVI IP and virtual gateway to be used on VSX leaf pairs.

The creation of VLANs and SVIs in this step is prerequisite to binding the VLANs across racks in logically contiguous Layer 2 domains in the next procedure. At the end of this procedure, each VLAN's broadcast domain is scoped to each VSX pair.

CX 10000 switches positioned in a border leaf role support east-west policy for attached hosts, when the switches are assigned a **leaf** switch profile. When IPsec or NAT features are enabled, the CX 10000 border leaf must be configured with a **spine** switch profile. After assigning the CX 10000 a **spine** switch profile, east-west policy enforcement is no longer supported, and directly attaching hosts to the border leaf is not recommended. This limitation does not apply to other switch models in the border leaf role. In this guide, CX 10000 switches positioned at the border leaf are not configured with host VLANs to support enabling IPsec in a separate procedure.

The diagram below illustrates the creation of VLANs on ToR VSX leaf pairs, except the CX 10000 border leaf.



Step 1 Confirm that the view is set to **Configuration/Routing/VRF**, then click the ••• symbol next to **PROD-DC-VRF** and select **IP Interfaces**.

Configura	ation / Ro	outing / VRF				
			Fabri	ic RSVDC-FB1		
					۲	
		Name	μE τ	jype ↓	Switches	L3 VNI
		Enter Name	••••	Select Type 👻	Enter Switches	Enter Regex for L3 VNI
	\bigcirc	default	C	Default		
	\bigcirc	DEV-DC-VRF	L	Jser	RSVDC-FB1-VSX_RSVDC-FB1-	100002
					LF1-1_RSVDC-FB1-LF1-2,	
					RSVDC-FB1-VSX_RSVDC-FB1-	
					LF2-1_RSVDC-FB1-LF2-2,	
					RSVDC-FB1-VSX_RSVDC-FB1-	
					LF3-2_RSVDC-FB1-LF3-1	
	0	mgmt	Ν	<i>M</i> anagement		
	\bigcirc	PROD-DC-VRF	L	Jser	RSVDC-FB1-VSX_RSVDC-FB1-	100001
IP Int	terfaces				LF1-1_RSVDC-FB1-LF1-2,	
ID St	tatic Rou	itos			RSVDC-FB1-VSX_RSVDC-FB1-	
		100			LF2-1_RSVDC-FB1-LF2-2,	
Netw	vorks				RSVDC-FB1-VSX_RSVDC-FB1-	
ARP	Tables				LF3-2_RSVDC-FB1-LF3-1	
IP Ro	oute Tab	les				
Swite	ches					

NOTE:

The ••• symbol is a shortcut to most options in the **ACTIONS** menu. This shortcut method is available in many Fabric Composer contexts. The IP Interfaces context also can be viewed by clicking the **PROD-DC-VRF** radio button and selecting **IP Interfaces** on the **ACTIONS** menu.

Step 2 On the **Configuration/Routing/VRF/PROD-DC-VRF** page, select the right **ACTIONS** menu below **IP INTERFACES** and click **Add**.

Configuration / Bouting / VBE / PBO	D-DC-VRF					
configuration, notating, vitre, rite	Fabric	RSVDC	-FB1			
					ତ ♥ ♥ ♥ ♥	ACTIONS ¥
Name JE	Туре	1E	Switches	JE.	L3 VNI	Route Target Ext
Enter Name	Select Type	-	Enter Switches		Enter Regex for L3 VNI	Enter Regex fo
PROD-DC-VRF	User		RSVDC-FB1-VSX_RSVD0	C-FB1-	100001	65001:100001
			LF1-1_RSVDC-FB1-LF1-;	2,		
			RSVDC-FB1-VSX_RSVD0	C-FB1-		
			LF2-1_RSVDC-FB1-LF2-2	2,		
			RSVDC-FB1-VSX_RSVD0	C-FB1-		
			LF3-2_RSVDC-FB1-LF3-	1		
IP INTERFACES IP STATIO	C ROUTES NETWO	RKS	ARP TABLES IP RO	OUTE TABL	ES SWITCHES	
					$\odot \odot \bigcirc \bigcirc$	ACTIONS ¥
Туре	↓≟ Enabled	1E	Switch	lΞ	VLAN Add	1
Select Type	▼ Select Ena	💌	Enter Switch		Enter Regex for VLAN. Edi	t i
] [[Del	ete

Step 3 On the IP Interfaces page, assign the following values, then click NEXT.

- Type: SV/
- VLAN: 101
- Switches: < Select all leaf switches, except CX 10000 border leaf>
- IPv4 Subnetwork Address: 10.5.101.0/24
- Switch Addresses: 10.5.101.1
- Active Gateway IP Address: 10.5.101.1
- Active Gateway MAC Address: 02:00:0A:05:00:01
| IP Interface | |) × |
|---------------------------------|--|-----|
| Interfa | ce Type Name Summary | |
| Select the IP Interface | Type and set the appropriate attributes.
ace | |
| Туре | SVI × • | - |
| VLAN * | 101
A VLAN between 1 and 4094, example: 1. | |
| Switches * | × RSVDC-FB1-VSX_RSVDC-FB1-LF2-1_RSVDC-FB1-LF2-2 × ▼ × RSVDC-FB1-VSX_RSVDC-FB1-LF3-2_RSVDC-FB1-LF3-1 × ▼ | |
| IPv4 Subnetwork
Address * | 10.5.101.0/24
A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24 | |
| IPv4 Addresses * | 10.5.101.1 | |
| | Enter a range of IPv4 Addresses to be assigned to the selected switches, example: 192.168.1.100-192.168.1.200. The range must include at least 4 addresses or match the Active Gateway IP Address. | |
| Active Gateway IP
Address * | 10.5.101.1 | |
| | A valid IPv4 Address, example: 192.168.1.10. Both Active Gateway values must be defined if using Active Gateway. | |
| Active Gateway
MAC Address * | 02:00:0A:05:00:01 A valid MAC Address, example: 00:00:00:00:00:01. Cannot include multicast or broadcast addresses Both Active Gateway values must be defined if | _ |
| Enable VSX Shutdo | using Active Gateway.
wn on Split | |
| Enable VSX Active I | Forwarding | |
| Enable Local Proxy | ARP | |
| (* = Required) So | croll for more options CANCEL BACK NEXT | |

The **SELECT ALL** button selects all switches assigned to the VRF where the SVI interface will be created. The range provided for **IPv4 Addresses** and the **Active Gateway IP Address** must be from the same network range as the **IPv4 Subnetwork Address**. The **IPv4 Addresses** field value is used to assign an IP address to each SVI interface. AOS-CX 10.09 and above supports assigning the same IP address as both the SVI interface and the active gateway. This maximizes the number of IPs available to assign to attached network hosts.

The Active Gateway IP address is not supported as a source IP address when using the ping command. When assigning the same IP address to both the Active Gateway and VLAN SVI, the ping command must specify a unique source interface or IP address, such as a loopback assigned to the same VRF, to verify reachability.For example:# *ping* 10.5.101.11 vrf PROD-DC-VRF source loopback11



🕑 IP Interfa	e ⑦ ×
- II	erface Type Name Summary
Enter an optional I	ame and Description.
Name	WEB-V101-PROD-DC
	A string, up to 42 characters. example: lpInterface1
Description	Production web app SVI/VLAN 101 in DC overlay
	Example: My New IP Interface
(* = Required)	CANCEL BACK NEXT
NOTE:	
Including I ment oper	ne associated VLAN ID and overlay VRF in the Name can be helpful during manage- itions.

Step 5 On the Summary page, verify that the information is entered correctly and click APPLY.

IP Interface	() ×
Interface Type	Name Summary
Name	WEB-V101-PROD-DC
Description	Production web app SVI/VLAN 101 in DC overlay
Туре	SVI
Enabled	Yes
VLAN	101
Switches	RSVDC-FB1-VSX_RSVDC-FB1-LF2-1_RSVDC-FB1-LF2-2, RSVDC-FB1-VSX_RSVDC-FB1-LF3-2_RSVDC-FB1- LF3-1
Active Gateway IP Address	10.5.101.1
Active Gateway MAC Address	02:00:0A:05:00:01
IPv4 Addresses	10.5.101.1
VSX Shutdown on Split	No
VSX Active Forwarding	No
Local Proxy ARP Enabled	No
	CANCEL BACK APPLY

Step 6 Repeat the procedure to create an additional overlay subnet in the production VRF using the following values:

Name	Description	TypeVLANSwitches	IPv4 Sub- network Address	IPv4 Address	Active Gateway IP Address	Active Gateway MAC Address
DB- V102- PROD- DC	Production database SVI/VLAN 102 DC overlay	SVI 102 < All non-border leaf switches >	10.5.102.0/	10.5.102	10.5.102.1	02:00:0A:05

Step 7 Repeat the procedure to create additional overlay subnets in the development VRF using the following values:

Name	Description	TypeVLANSwitches	IPv4 Sub- network Address	IPv4 Addres	Active Gateway IP s &d dress	Active Gateway MAC Address
WEB- V201- DEV- DC	Development web app SVI/VLAN 201 in DC overlay	SVI 201 < All non-border leaf switches >	10.6.201.0/	10.6.2(10.6.201.1	02:00:0A:06:00
DB- V202- DEV- DC	Development database SVI/VLAN 202 in DC overlay	SVI 202 < All non-border leaf switches >	10.6.202.0/2	2140.6.20	210.6.202.1	02:00:0A:06:00

Host connectivity can be extended to border leaf switches, when not using IPsec or NAT services on CX 10000 switches in the border leaf role.

Configure EVPN Instances

An EVPN instance joins each previously created VLAN across leaf switches into a combined broadcast domain. This procedure defines two key attributes to logically bind each VLAN across the leaf switches. A VNI is assigned to each VLAN. MP-BGP associates host MACs to VNI values in its EVPN host advertisements to support VXLAN tunneling. An auto-assigned route target per VLAN also is defined. The VLAN route-target associates a MAC address with the appropriate VLAN at remote switches for the purpose of building bridge table MAC reachability. Route targets are included in MP-BGP EVPN host advertisements.

The Fabric Composer EVPN wizard maps VLAN IDs to L2 VNI values. A prefix value is provided for automatic generation of route targets. The EVPN wizard also creates an EVPN instance to associate route targets with VLANs. When using iBGP for the overlay control plane protocol, route targets can be assigned automatically. A resource pool is used to assign the EVPN system MAC addresses.

At the completion of this procedure, distributed L2 connectivity across leaf switches in the fabric is established, with the exception of the border leaf. Aruba active gateway permits the same IP address to be used on all leaf switches in the fabric for a VLAN. Overlay reachability between the border leaf and other leaf switches is routed. The diagram below illustrates the the logical binding of VLANs across leaf racks into logically contiguous broadcast domains.



Step 1 On the Guided Setup menu, select EVPN CONFIGURATION to start the EVPN workflow.

NET	DISTRIBUTED SERVICES					
Netw	Network Setup					
your sy	rstern.	ing steps to initialize and co	Ingule			
	SWITCHES Discover n	ew Switches.				
	FABRIC Add a Fab	ric to the system.				
Selecte	ed Fabric:					
RSV	DC-FB1		$\times =$			
	ASSIGN SV Assign Sw	WITCH TO FABRIC itch To Fabric				
()	NTP CONF Configure	GURATION Switch NTP.				
۲	DNS CONF Configure	Switch DNS.				
Ę	VSX CONF Configure	IGURATION VSX Switch Pairing.				
1	L3 LEAF-S Configure	PINE CONFIGURATION L3 Leaf-Spine Connections.				
	L2 LEAF-S Configure	PINE CONFIGURATION L2 Leaf-Spine Connections.				
6	UNDERLAY Configure	YS Underlays.				
Đ	OVERLAYS Configure	s Overlays.				
	EVPN CON Configure	IFIGURATION EVPN Instances.				

Step 2 On the Introduction page, review the guidance and click NEXT.

몇 EVPN(RSVD	C-FB1)				() ×
Introduction	Switches	? Name	(?) VNI Mapping	Settings	Summary
This configuration will be The EVPN EVIs will not b	e used to generate mult be active until after an U	iple EVPN instances, Inderlay and Overlay	one for each VLAN includ has been configured on tl	led in the VNI Mapping he default VRF.	step.
(* - Poquirod)				CANCEL	BACK NEXT
NOTE:					
The prerequisi	tes noted above	e were comple	eted in previous s	teps.	

Step 3 On the **Switches** page, uncheck **Create EVPN instances across the entire Fabric and all Switches contained within it**, select all leaf switches except the border leaf, and click **NEXT**.

몇 EVPN (RSVD	C-FB1)				⑦ ×
	Switches	(?) Name		Settings	Summary
Create EVPN instances	across the entire Fabric	or select specific Sw	vitches.		
Create EVPN instanc	es across the entire Fab	pric and all Leaf and I	Border Leaf Switches con	tained within it.	
Switches *	× RSVDC-FB1-VSX_F	ISVDC-FB1-LF2-1_RSV	DC-FB1-LF2-2 DC-FB1-LF3-1	×	SELECT ALL
(* = Required)				CANCEL	BACK

Step 4 On the Name page, enter a Name Prefix and Description, then click NEXT.

몇 EVPN (RS	VDC-FB1)					? ×
			?	?	?	
Introduction	Switches	Name	VNI Mapping	Settings	Summary	
Enter a required Nar	me Prefix and an optional D	escription.				
Name Prefix *	DC-FB1-EVPN					
	Any non empty string, exam	ple: Evpn-mapping				
Description	VLAN to L2 VNI map	oping for the DC over	lay			
	Example: Evpn-mapping De	scription				
([*] = Required)				CANCE	BACK	NEXT

Step 5 On the VNI Mapping page, enter one or more VLANs and a Base L2VNI, then click NEXT.

몇 EVPN(RS)	/DC-FB1)				? ×
				?	?
Introduction	Switches	Name	VNI Mapping	Settings	Summary
Specify required VL/	Ns and Base L2VNI for ge	enerating the VLAN-to	o-VNI mappings.		
VLANs *	101-102,201-202				
	A number, set, or range of	VLANs between 2 and 409	94, example: 5, 10-45, 102.		
Base L2VNI *	10000				
	A number between 0 and 1	6777214, example 0. Com	puted VLAN + VNI cannot exceed	d 16777214.	
([*] = Required)				CANCEL	BACK NEXT
NOTE:					
The Base L2 VLAN autom	VNI value is adde atically.	d to each VLAI	N ID to generate a	unique L2 VNI	associated to each

Step 6 On the Settings page, click ADD to launch the Resource Pool wizard.

몇 EVPN (RSVDC-FB1)		? ×
Introduction Swit	ches Name VNI Mapping Settings Summary	
Set the Virtual MAC Address Rang	e. Select or add a MAC Address Resource Pool or specify a range.	
MAC Address Resource Pool *	Select	ADD
MAC Address Range *		
	A hyphen-separated range of valid MAC Addresses, example: 02:00:00:00:02:00-02:00:00:00:02:FF. Cannot include multicas	t addresses.
Set the required Route Target Type	and associated values. The Route Target Type determines the format of the route targets generated.	
Route Target Type *	Select	-
	'AUTO' is recommended only when an iBGP Overlay is configured.	
(* = Required)	CANCEL BACK	IEXT

Step 7 Resource Pool wizard: On the Name page, enter a Name and Description, then click NEXT.

🔋 Resource	Pool ×
_	Name Settings Summary
Enter a required N	ame and an optional Description.
Name *	EVPN-FB1-SYSTEM-MAC
	Any unique non empty string, example: ResourcePool-1
Description	EVPN system MAC address pool for the Fabric 1 DC overlay
	Example: ResourcePool-1 description
([*] = Required)	CANCEL BACK NEXT

Step 8 Resource Pool wizard: On the **Settings** page, enter a MAC address range for System MAC Addresses in the **Resource Pool** field and click **NEXT**.

📑 Resource	Pool
 N	ame Settings Summary
Select a required res	source type and a set/range of resources.
Resource Type	MAC Address
Resource Pool *	02:00:01:00:00-02:00:01:00:00:FF A range of MAC Addresses up to 1000 addresses. Example: 00:00:00:00:00:00:00:00:00:00:00:FF, 02:00:00:00:00:00:00:00:00:FF.
Resource Count	Cannot include multicast addresses. 256
([*] = Required)	CANCEL BACK NEXT

Step 9 Resource Pool wizard: On the **Summary** page, verify that the System MAC information is correct and click **APPLY**. The **Resource Pool** wizard closes and returns to the main **EVPN Configuration** workflow.

📮 Resource Pool		×
Name	Settings Summary	
Name Description Resource Type Resource Pool Resource Count	EVPN-FB1-SYSTEM-MAC EVPN system MAC address pool for the Fabric 1 DC overlay MAC Address 02:00:01:00:00-02:00:01:00:00:FF 256	
	CANCEL BACK APPLY	

Step 10 On the **Settings** page, verify that the **MAC Address Resource Pool** just created is selected, set the **Route Target Type** to *AUTO*, and click **NEXT**.

몇 EVPN (RSVDC	-FB1)					? ×
					?	
Introduction	Switches	Name	VNI Mapping	Settings	Summary	
Set the Virtual MAC Addres	s Range. Select or a	dd a MAC Address F	Resource Pool or specify	a range.		
MAC Address Resource Pc	ol * EVPN-F	B1-SYSTEM-MAC (02	2:00:01:00:00:00-02:00:0	1:00:00:FF)	× •	ADD
MAC Address Range						
0	A hyphen-se	parated range of valid MA	C Addresses, example: 02:00:0	00:00:02:00-02:00:00:00:02:F	F. Cannot include multica	st addresses.
Set the required Route Targ	et Type and associa	ted values. The Route	e Target Type determines	s the format of the route	targets generated.	
Route Target Type *	AUTO					× •
	'AUTO' is re	commended only when an	iBGP Overlay is configured.			
(* = Required)				CANCEL	ВАСК	NEXT
(= rioquiou)						
NOTE:						
EVPN route targe	ts can be set	automatically	by switches on	lv when using a	n iBGP overla	IV.



Step 11 On the **Summary** page, verify that the information is correct and click **APPLY**.

Step 12 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

Step 13 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select all non-border leaf switches >
- **Commands:** show interface vxlan vtep

>_ CLI Command Processor									×			
Select Fabrics or Switches, and select or add	Saved Commands that can be customized. Press Run for result	s.							1			
Fabrics												
Switches	× RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-	« RSVDC/FB1-LF2-1 × RSVDC/FB1-LF2-2 × RSVDC/FB1-LF3-1 × RSVDC/FB1-LF3-2										
Saved Commands	Select from Saved Commands or Add new commands.				v	ADD	REMO	VE				
Commands	show interface vxlan vtep											
	A comma separated list of commands to be run.											
Download Options	Download Results Download JSON Data											
Results	Switch : RSVDC-FB1-LF2-1 Command : show inter	face vxlan vtep Destination	Origin	Status	VNI	Routing	VLAN	VRF				
	10.250.2.1	10.250.2.0	evpn	operational	10101	disabled	101					
	10.250.2.1	10.250.2.0	evpn	operational	10102	dicabled	201					
	10.250.2.1	10.250.2.0	evon	operational	10201	disabled	201					
	10.250.2.1	10.250.2.0	evon	operational	100001	enabled		PROD-DC-VRF				
	10.250.2.1	10.250.2.0	evpn	operational	100002	enabled		DEV-DC-VRF				
	Switch · RSVDC-FR1-LF2-2 Command · show inter	face vylan vten										
	Source	Destination	Origin	Status	VNI	Routing	VLAN	VRF				
	10.250.2.1	10.250.2.0	evpn	operational	10101	disabled	101					
	10.250.2.1	10.250.2.0	evpn	operational	10102	disabled	102					
	10.250.2.1	10.250.2.0	evpn	operational	10201	disabled	201					
	10.250.2.1	10.250.2.0	evpn	operational	10202	disabled	202					
	10.250.2.1	10.250.2.0	evpn	operational	100001	enabled		PROD-DC-VRF				
	10.230.2.1	10.230.210	evpn	operacionac	100002	enableu		DEV-DC-VRF				
(* = Required)								CANCEL	4			

Step 14 Verify that the output for each switch displays a remote VTEP to each non-border leaf switch pair for each VLAN.

The Guided Setup is now complete.

Host Port Configuration

Use this section to configure the Port Groups and LACP Host LAG ports.

Configure Port Groups

The SFP28 ports on the Aruba 10000-48Y6C switches (R8P13A and R8P14A) are organized into 12 groups of four ports each. The SFP28 default port speed is 25 Gb/s and must be set manually to 10 Gb/s, if required. Port groups can be configured on CX 8325, 8360, 10000, and 9300S series switches.

For additional details, find the *Installation and Getting Started Guide* for a specific switch model on the Aruba Support Portal. Go to the section: **Installing the switch > Install transceivers > Interface-Group operation**.

The following procedure configures a set of ports for 10 Gbps operation.

Step 1 On the Configuration menu, select Ports > Ports.

HPE aruba Fabric Composer	Dashboard (Configuration 👻 Mainter	nance 🗸 Visualization 🖌 🔎 w
🛞 VRF	Cart	Ports >	Ports
A DOD	Cont	Routing >	EEE Link Aggregation Groups
G BGP		System >	CAN Groups
💢 OSPF	E'	Retwork >	문 PVLANs
🖽 EVPN	_	Administration >	C ^a Transceivers
		Integrations >	
EVPN VXLAN Multi-Fabric		🎉 Policy 🔹 🔪	↓≟ Switch Name



Configuration /	/ Ports /	Ports						
Fabric	RSVD	C-FB1		Switch × RSVDC	-FB1-	LF2-1	SEL	ECT ALL
				× RSVDC	-FB1-	LF2-2		
_	▦						С	ACTIONS 🗸
								$\odot \bigcirc \bigcirc$
	He	alth	Æ	Reason	1£	Switch	ĻΞ	Port
		Select Health	•	Enter Regex for Reason		Enter Regex for Switch		Enter Regex 1
		HEALTHY		Group speed mismatch		RSVDC-FB1-LF2-1		1/1/1
		HEALTHY		Group speed mismatch		RSVDC-FB1-LF2-1		1/1/2
		HEALTHY		No XCVR installed		RSVDC-FB1-LF2-1		1/1/3

Step 3 Enter mismatch in the Reason column's regex field and click the Apply table filters icon.

Configuration	n / Po	rts / Ports						
Fabric	RS	VDC-FB1		Switch	× RSVDC-FB	-LF2-1		SELECT ALL
					× RSVDC-FB	-LF2-2		
	Ⅲ							C ACTIONS -
						i	Inapplied table	filters 👰 🛇 🍸 🥸
		Health	lΞ	Reason	Ţ	Switch		Apply table filters
		Select Health	•	mismatch		Enter R	egex for Switch	Enter Rege
		HEALTHY		Group speed mis	smatch	RSVDC-FI	B1-LF2-1	1/1/1
C		HEALTHY		Group speed mis	smatch	RSVDC-FI	B1-LF2-1	1/1/2
		HEALTHY		No XCVR installe	d	RSVDC-FI	B1-LF2-1	1/1/3

This step is optional. Cabling must be complete before this step so the switch can generate a speed mismatch status used for filtering.

Step 4 Select an individual port in the port-group to be changed. On the right **ACTIONS** menu, select **Edit**.

Configuration /	/ Por	ts / Ports				
Fabric	RS	SVDC-FB1	SELECT ALL			
				× RSVDC-FB1	-LF2-2	
1 selected	▦					C ACTIONS ~
						Edit
		Health	μ <u>ε</u>	Reason JE	Switch	< Enable/Disable
		Select Health	•	mismatch	Enter Regex for Switch	< VLANs
		HEALTHY		Group speed mismatch	RSVDC-FB1-LF2-1	QSFP Transform
		HEALTHY		Group speed mismatch	RSVDC-FB1-LF2-1	< Persona
		HEALTHY		Group speed mismatch	RSVDC-FB1-LF2-1	1/1/11
		HEALTHY		Group speed mismatch	RSVDC-FB1-LF2-1	1/1/12
		HEALTHY		Group speed mismatch	RSVDC-FB1-LF2-2	1/1/1
		HEALTHY		Group speed mismatch	RSVDC-FB1-LF2-2	1/1/2

:::info The **Edit** option on the **ACTIONS** menu is available only when a single switch port is selected.

:::

Step 5 On the **Ports** page, select the **Speed** tab. Select the appropriate value in the **Speed** dropdown, then click **APPLY**.

Ports RSVD	C-FB1-LF2-1: 1/1/	/1		? ×
SETTINGS	SPEED	VLANS	⊘ NAME	SUMMARY
Set the line speed of the	port.			
Speed 1	0Gbps			× •
Port	ts 1/1/1-1/1/4 will be affected by	any Speed changes.		
(* = Required)			c	ANCEL APPLY

Observe the full list of ports affected by the speed change. Ensure that this is the correct speed setting for all listed ports.

Step 6 Repeat the procedure for additional leaf switch ports requiring speed changes. Be sure to make changes to corresponding ports on VSX-paired switches supporting MC-LAGs.

NOTE:

The displayed port list of mismatched transceiver speeds is updated dynamically. It may be necessary to toggle the select all/deselect all checkbox in the upper left column to deselect the previously selected port after the update hides it from view.

Multiple LACP MC-LAG Configuration

LACP link aggregation groups provide fault tolerance and efficient bandwidth utilization to physical hosts in the data center. The **Link Aggregation Group** wizard configures multi-chassis LAGs and LACP on fabric switches. Use the Fabric Composer **CLI Command Processor** to verify LAG interface state for LAG connected hosts.

Multiple MC-LAG creation can be applied to one or more switches using the Fabric Composer wizard. It enables quick setup of MC-LAGs across all leaf switches, when leaf switch models and cabling are consistent across the fabric. For example, a single pass of the Link Aggregation Groups wizard can configure all host leaf ports for MC-LAG given the following conditions:

- All leaf switches contain the same number of host facing ports.
- No more than one port per switch requires assignment to an individual MC-LAG.
- VLANs assigned to all MC-LAGs are consistent.

Configuration also is required on the connected hosts. Configuration varies by server platforms and operating systems and is not presented in this guide. Refer to the appropriate technical documentation for attached devices and operating systems.

Step 1 On the **Configuration** menu, select **Ports > Link Aggregation Groups**.

HPE aruba Fabric Composer	Dashboard	Configuration 🛩 Mainter	nance - Visualization - 🔎 w
Ports	Conf	Ports >	Ports
		🐼 Routing >	Link Aggregation Groups
EINK Aggregation Groups		☐ System >	្រុំ VLAN Groups
C VLAN Groups		品 Network >	문 급 PVLANs
PVLANs PV		Administration >	C ^a Transceivers
		🗂 Integrations 🔉	
🖕 Transceivers		🍰 Policy 🔹 🔉	
		00	<u>↓≟</u> Reason

Step 2 On the right ACTIONS menu, select Add.

Config	guration / Po	rts / Link Aggregation Groups								
				Fabric	RS	VDC-FB1				
									$\bigcirc \bigcirc \bigtriangledown $	C ACTIONS V
		♂ Name	1E	Туре	1£	LAG Number	Switch	1E	Ports	Add
		Enter Regex for Name		Select Type	•	Enter Regex	Enter Regex for Switch		Enter Regex for Ports	Edit
>		ISL-RSVDC-FB1-LF1-1		Inter-Switch Link		256	RSVDC-FB1-LF1-1		1/1/49-1/1/50	Delete
>		ISL-RSVDC-FB1-LF1-2		Inter-Switch Link		256	RSVDC-FB1-LF1-2		1/1/49-1/1/50	VLANs
>		ISL-RSVDC-FB1-LF2-1		Inter-Switch Link		256	RSVDC-FB1-LF2-1		1/1/49-1/1/50	all

Step 3 On the **Create Mode** page, select **Create multiple MLAGs for selected VSX Pairs** and click **NEXT**.

🚥 Link Aggrega	tion Group (RSVDC	C-FB1)			0	×
	?	?	?	?	?	
Create Mode	Settings	Ports	LACP Settings	VLANs	Summary	
Select an option to crea	te the LAG(s). Choose to cr	eate multiple MLAGs o	r to configure a single LAG.			
 Create a single LAG 	/MLAG.					
Create multiple MLA	Gs for selected VSX Pairs.					
(* = Required)				CANC	EL BACK NEXT	

Step 4 On the Settings page, enter a Name Prefix, LAG Number Base, then click NEXT.

🚥 Link Aggrega	tion Group (RSVDC	C-FB1)				(? ×
Create Mode	Settings	Ports	LACP Settings	VLANs	Summary	
Enter a required Name F	Prefix and optional LAG Nur	mber Base.				
Name Prefix *	ESX					
	Any non empty string, exampl	e: LAG-1				
LAG Number Base *	11					
	A number between 1 and 256,	, example 1				
(* = Required)				CANC	EL BACK	NEXT
NOTE						
NOTE:						
If individual h	iostname assigni	ments are req	uired per MC-LAG	in place of a n	nore general p	orefix-
based naming	g convention, cho	oose Create a	single LAG/MLAG	in the previou	us step to prov	/ide a
unique a nam	ne per LAG.LAG in	ndex values a	re numbered seq	uentially begin	nning with the	LAG
Number Base	e. The wizard will	not complete	e it a LAG value is a	lready in use o	n any switch t	arget.
The server ac	cess/subleaf MC-	LAG configure	ed from the RSVD	C-FB1-LF3-1 an	d RSVDC-FB1-	LF3-2
VSX pair to th	e downstream R	SVDC-FB1-LF3	3-SA1 switch uses	LAG index 1 or	n all three swit	tches.
LAG Number	Base 11 is chose	n to avoid a co	onflict with the ex	isting LAG.		

Step 5 On the **Ports** page, select one or more VSX-pairs of switches in the **VSX Pairs** field, enter the ports that are physically cabled for MC-LAG operation in **Ports**, then click **VALIDATE**.

🚥 Link Aggregation	on Group (RSVD	C-FB1)				? ×
Create Mode	Settings	Ports	(?) LACP Settings	(?) VLANS	Summary	
Select VSX Pairs and defir	ne a range of Ports to be	e included in the LAGs.	0		,	
VSX Pairs	× RSVDC-FB1-VSX_F	SVDC-FB1-LF2-1_RSVDC-F	FB1-LF2-2 × RSVDC-FB1-V	/SX_RSVDC-FB1-LF3-2_R	SVDC-FB1-LF3-1	• × •
Ports *	1/1/1					
	A number, set, or range of P	orts, example: 1/1/4-1/1/25, 1/1	/27, 1/1/31:1.			
	VALIDATE					
(* = Required)				CAN	CEL BACK	NEXT

Step 6 If Fabric Composer can validate that MC-LAG port configuration is consistent with LLDP neighbor data, a success message is presented.

✓ Success ESX is a valid configuration. ×	
NOTE:	
Validation of hypervisor host connections requires previous assignment of physical h to LACP LAGs. Validation is intended to verify that the requested configuration is co with cabling to attached hosts. It is not required to continue the process of MC-LAG or attached hosts are not configured or present. Fabric Composer configures an MC-LAG u 1/1/1on RSVDC-FB1-LF2-1 and RSVDC-FB1-LF2-2 switches, and a second MC-LAG using on RSVDC-FB1-LF3-1 and RSVDC-FB1-LF3-2 switches, when using the values above. S multiple ports will create additional MC-LAGs with corresponding port numbers beto VSX switch pairs.	ost ports onsistent eation, if sing port port 1/1/1 pecifying ween the

Step 7 On the Ports page, click NEXT.

Step 8 On the **LACP Settings** page, check **Enable LACP Fallback**, leave other LACP settings at their default values, and click **NEXT**.

🚥 Link Aggrega	tion Group (RSVDC	-FB1)				? ×		
Create Mode	Settings	Ports	LACP Settings	(?) VLANs	Summary			
Enable or disable LACP Fallback and configure LACP settings.								
LACP Mode	Active					× •		
LACP Interval	Slow					× •		
Priority	1							
	A number between 1 and 6553	5, example 1						
(* = Required)				CANC	ELBACK	NEXT		

Step 9 On the **VLANs** page, modify the untagged **Native VLAN** number if necessary, enter the tagged VLAN IDs in the **VLANs** field, then click **NEXT**.

🚥 Link Aggre	gation Group (RS	SVDC-FB1)				? ×
					?	
Create Mode	Settings	Ports	LACP Settings	VLANs	Summary	
Assign Native VLAN,	VLANs, VLAN Groups,	and PVLAN Port	Type to the LAG.			
Native VLAN	1					
	A VLAN between 1 and 409	4 or an empty value,	example: 1.			
	Tagged Native VLA	N				
	Can only be set when the	ere is a Native VLAN	at least one VLAN or VLAN	Group assigned.		
VLANs	101-102,201-202					
	'All' for all VLANs or a numb	per, set, or range of V	/LANs between 1 and 4094, e	example: 5, 10-45, 102.		
VLAN Group	Select					-
PVLAN Port Type	There are no PVLAN	ls configured on	the selected switch(es			
(* = Required)				CANCEL	BACK	IEXT

Step 10 On the **Summary** page, confirm that the information is entered correctly and click **APPLY** to create the LAGs.

Link Aggregatio	n Group (RSVDC-	-FB1)				? ×
Create Mode	Settings	Ports	LACP Settings	VLANs	Summary	
Name Prefix	ESX					
LAG Number Base	11					
VSX Pairs	RSVDC-FB1-VSX_RSV	DC-FB1-LF2-1_RSVD	C-FB1-LF2-2, RSVDC-FB1-V	SX_RSVDC-FB1-LF3-2	_RSVDC-FB1-LF3-1	
Ports	1/1/1					
Native VLAN	1					
VLANs	101-102,201-202					
VLAN Groups						
Enable LACP Fallback	No					
LACP Mode	Active					
LACP Interval	Slow					
Priority	1					
				CANC	EL BACK AP	PLY

Step 11 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

Step 12 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select all switches with newly configured LAGs >
- **Commands:** show lacp interfaces

>_ CLI Command	Processo	or									×
Select Fabrics or Switches	s, and select	or add Saved C	ommanc	ls that c	an be custo	omized. Press Run for res	ults.				
Fabrics	Not applic			lected.							~
Switches	× RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-LF3-1 × RSVDC-FB1-LF3-2							-			
Saved Commands	Select from	Select from Saved Commands or Add new commands.							E		
Commands	show lacp	show lacp interfaces									
	A comma sepai	rated list of comman	ds to be ru	in.							
Download Options	Download R	esults Downl	oad JSC	N Data							
Results	Switch :	RSVDC-FB1-L	.F2-1 C	ommand	: show	lacp interfaces					
	State abbreviations :A - ActiveP - PassiveF - Aggregable I - IndividualS - Short-timeout L - Long-timeout N - InSync0 - OutofSyncC - CollectingD - DistributingX - State m/c expiredE - Default neighbor state										
	Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State		
	 1/1/1	 lag11(mc)	1001	1	ALFNCD	02:00:00:00:10:01	65534	11	up		
	1/1/49	lag256	50	1	ALFNCD	ec:50:aa:a4:f0:c1	65534	256	up		
	1/1/50	lag256	51	1	ALFNCD	ec:50:aa:a4:f0:c1	65534	256	up		
	Partner d	etails of al	l inte	rfaces	:						
	Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key			
	1/1/1	lag11(mc)	1	255	PLFNCD	b4:7a:f1:7b:ab:66	1	15			
	1/1/49	lag256	50	1	ALFNCD	ec:50:aa:a4:40:77	65534	256			
	1/1/50	lag256	51	1	ALFNCD	ec:50:aa:a4:40:77	65534	256			
(* = Required)									C/	ANCEL	RUN

Step 13 When a host is connected to the LAG, verify that each port assigned to one of the host LAGs created in this procedure has a **State** of "ALFNCD" for its local interfaces and "PLFNCD" for its partner interfaces. The **Forwarding State** should be "Up" for local interfaces.

NOTE:

A combination of VSX peer LAG interfaces and VSX multi-chassis LAG interfaces to hosts may be included in the command output. As shown above, the multi-chassis interfaces are denoted with **(mc)** after the LAG name. The **Actor** is the switch where the command was run. The **Partner** is the host at the other end of the LAG. The **State** column shows the expected values for a switch set to **Active** LACP mode and a host set to **Passive** LACP mode with a healthy LAG running.

Single LACP MC-LAG Configuration

Individual LAGs are assigned for the following conditions:

- A unique LAG name is required in Fabric Composer.
- Assigned VLANs are unique to the LAG.
- More than one port per switch are assigned to an MC-LAG to increase capacity.

Step 1 On the **Configuration** menu, select **Ports > Link Aggregation Groups**.



Step 2 On the right ACTIONS menu, select Add.

Configu	Configuration / Ports / Link Aggregation Groups							
		Fabric	RSVDC-FB1					
						$\odot \odot \bigcirc \bigcirc$	С астю	NS 🗸
		I ⊘ Name L	Туре	ļΞ	LAG Number	Switch	Add	
		Enter Regex for Name	Select Type	•	Enter Regex	Enter Regex for	Edit	
>		ESX_RSVDC-FB1-LF2-	Provisioned		11	RSVDC-FB1-LF2-1	Delete	
		1_1/1/1_RSVDC-FB1-LF2-2_1/1/1				RSVDC-FB1-LF2-2	VLANs	
>		ESX_RSVDC-FB1-LF3-	Provisioned		11	RSVDC-FB1-LF3-2		1/1/1
		1_1/1/1_RSVDC-FB1-LF3-2_1/1/1				RSVDC-FB1-LF3-1		1/1/1

Step 3 On the Create Mode page, leave Create a single LAG/MLAG selected and click NEXT.

🚥 Link Agg	regation Group (RS	VDC-FB1)			? X
Create Mode	s Settings	Ports	? LACP Settings	(?) VLANs	Summary
Select an option t	o create the LAG(s). Choos	e to create multiple ML	_AGs or to configure a sin	igle LAG.	
Create a sing	le LAG/MLAG.				
 Create multip 	le MLAGs for selected VSX	Pairs.			
([*] = Required)				CANCEL	BACK

Step 4 On the Settings page, enter a Name, Description, and LAG Number. Click NEXT.

EIII Link Aggregation Group (RSVDC-FB1)							
Create Mode	Settings	Ports	C LACP Settings	? VLANs	Summary		
Enter a required Na	me and optional Descr	iption and LAG Nu	umber.				
Name *	ESXi-41-Rack4						
	Any non empty string, ex	ample: LAG-1					
Description	MC-LAG for ESXi	host 41					
	Example: Link Aggregation	on Group 1					
LAG Number	100						
	A number between 1 and	1 256, example 1					
Inter-Switch Lin	k						
(* = Required)				CANCEL	BACK	EXT	
NOTE:							
Consider using a Name that identifies the host and where it is connected.							

Step 5 On the **Ports** page, select a VSX-pair or a VSF stack of switches from the **LAG Switch Member** dropdown.

Link Aggregation Group (RSVD	C-FB1)	() ×
Create Mode Settings	Image: Constraint of the section o	Summary
Select ports to add to the LAG. Up to 2 switches r remove all associated LAG port members on the	ay be selected with up to 16 ports per switch. Re witch from the LAG.	moving a switch will also
EAG Switch Mem	er Select a Switch 1_RSVDC-FB1-LF2-2 RSVDC-FB1-VSX_RSVDC-FB1-LF3- 2_RSVDC-FB1-LF3-1	
Health J= Select Health	Sw RSVDC-FB1-LF3-SA1 Sw RSVDC-FB1-SP1 RSVDC-FB1-SP2 RSVDC-FB1-SP2	x for Port

Step 6 Click the Switch View mode icon to identify ports more easily.



Step 7 Click the port icons to add them as members of the link aggregation group and click NEXT.

🚥 Link Aggre	egation Group (F	RSVDC-FB1)			() ×
Create Mode	Settings	Ports	? LACP Settings	? VLANs	Summary
2 selected 🛛 🖽	LAG Switcl	h Member RSVE	DC-FB1-LF3-SA1	× •	
► Enabled	⊙ Selected ⊗ Not / Disabled No 1	Available LI	NK AGGREGATION GRO	DUP 🗘 UPLIN	K ink Up ● Link Down
✓ RSVDC-FB1-LF 1 3 5 5 ⊘	3-SA1 7 ● 9 ● 11 ●	13 • 15 • 17 •	19 • 21 • 23 • 2	5 • 27 • ×	
$\begin{array}{cccc} 2 & 4 & 6 \\ 1 & 3 & 5 \\ \hline \hline \hline \hline \hline \hline \hline \hline \hline 2 & 4 & 6 \\ \hline \hline$	8 10 12 7 9 11 8 10 12	14 16 18 18 13 15 17 17 16 18 16 18 16 18 18 16 18 18 18 18 18 18 18 18 18 18 18 18 18	20 22 24 2 19 21 23 2 20 22 24 2 23 2 20 22 24 24 2	6 28 0 5 27 0 ⊗ 6 28 0	
(* = Required)				CANCEL	BACK

A checkmark appears on the newly selected ports. The diamond icon appears on ports not currently available for a new LAG group assignment. Select ports on both VSX switches or multiple VSF switches to create a functional multi-chassis LAG.

Step 8 On the LACP Settings page, leave the settings at their defaults, and click NEXT.

••• Li	nk Aggre	egation G	roup (RS\	/DC-FB	1)					(?) ×
Crea Enable o	ate Mode	Setting ACP Fallback	gs for an MLAG	Ports and select	LACP Se	ttings	VLANs VLANs ure LACP settings.		Summary	
	Switch	LE LE	Ports	Æ	LACP Mode	ĻĒ	LACP Interval	↓ <u>≞</u>	Priority	1 <u>=</u>
	RSVDC-FE	31-LF3-SA1	1/1/1, 2/1/1		Active		Slow		1	
LACP M	ode	Active								
LACP In	terval	Slow								
Priority		1								
		A number be	tween 1 and 655	35, example 1						
(* = F	Required)						CANCEL		BACK	NEXT

Enable LACP Fallback is auto-selected for VSX pairs. LACP fallback is not a valid option on VSF stacks. CX switches default to "Active" mode to ensure that LACP can be established regardless of the LACP configuration of the host platform. Using the default settings is recommended. Click the box next to one or both switch names to modify default values.

Step 9 On the **VLANs** page, modify the untagged **Native VLAN** number if necessary, enter tagged VLAN IDs in the **VLANs** field, then click **NEXT**.

E Link Aggree	gation Group (RSVDC-FB1)	(?) ×
)
Create Mode	Settings Ports LACP Settings VLANs Summ	ary
Assign Native VLAN,	, VLANs, VLAN Groups, and PVLAN Port Type to the LAG.	
Native VLAN	1	
	A VLAN between 1 and 4094 or an empty value, example: 1.	
	Tagged Native VLAN	
	Can only be set when there is a Native VLAN at least one VLAN or VLAN Group assigned.	
VLANs	101-102,201-202	
	'All' for all VLANs or a number, set, or range of VLANs between 1 and 4094, example: 5, 10-45, 102.	
VLAN Group	Select	-
PVLAN Port Type	There are no PVLANs configured on the selected switch(es).	
(* = Required)	CANCEL BACK	NEXT

Step 10 On the **Summary** page, confirm that the information is entered correctly and click **APPLY** to create the LAGs.

Link Aggreg	atio	on Group (R	SVDC	-FB1)					?
Create Mode		Settings	Po	rts	LACP Setting	s VLANs		Summary	
Name				ESXi-41-	Rack4				
Description				MC-LAG	for ESXi host	41			
LAG Number				100					
Туре				Provision	ed				
Native VLAN				1					
VLANs				101-102,	201-202				
VLAN Groups									
PVLAN Port Type									
Switch	Æ	Ports	↓ <u>≞</u>	LACP Mode	ĻΞ	LACP Interval	↓ <u></u>	Priority	↓ <u>≞</u>
RSVDC-FB1-LF3-SA1		1/1/1, 2/1/1		Active		Slow		1	
						CANCE	:L	BACK	PPLY

Step 11 Repeat the procedure for each individual LAG connection in the fabric.

Step 12 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

Step 13 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select the switch LAG configured for the new LAG >
- **Commands:** show lacp interfaces

>_ CLI Command	Processo	or									5	
Select Fabrics or Switches	s, and select o	or add Saved C	ommand	s that ca	n be custo	mized. Press Run for resu	ults.					
Fabrics	Not applicable when a Switch is selected.											
Switches	× RSVDC	× RSVDC-FB1-LF3-SA1 × *										
Saved Commands	Select from	m Saved Comm	ands or /	Add new	command	S.			~	ADD R	EMOVE	
Commands	show lacp	interfaces										
	A comma sepa	rated list of comma	inds to be ru	ın.								
Download Options	Download F	Results Down	nload JSC	ON Data								
Results	Switch : State abb A - Activ S - Short	RSVDC-FB1- previations (e P :-timeout L	LF3–SA1 : – Passi – Long–	. Comma .ve .timeou	F – Ag	w lacp interfaces gregable I – Indiv Sync 0 – Outof:	idual Svnc					
	C – Colle	ecting D	- Distr	ibutir	ig	Sync o oucon.	byne					
	X – State	e m/c expire	d		E – De	fault neighbor sta	te					
	Actor det	ails of all	interf	aces:								
	Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State			
	1/1/28	lag1	29	1	ALFNCD	a8:52:d4:d3:ee:c0	65534	1	up			
	2/1/28	lag1	93	1	ALFNCD	a8:52:d4:d3:ee:c0	65534	1	up			
	1/1/1	lag100	2	1	ALFNCD	a8:52:d4:d3:ee:c0	65534	100	up			
	2/1/1	Lag100	66	1	ALFNCD	a8:52:04:03:ee:c0	65534	100	up			
	Partner o	letails of a	ll inte	erfaces	:							
	Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key				
	1/1/28	lag1	1013	1	ALFNCD	02:00:00:00:10:00	65534	1				
	2/1/28	lag1	13	1	ALFNCD	02:00:00:00:10:00	65534	1				
	1/1/1	lag100	1	255	PLFNCD	50:7c:6f:68:ba:f6	1	9				
	2/1/1	lag100	2	255	PLFNCD	50:7c:6f:68:ba:f6	1	9				
(* = Required)										CANCEL	RUN	

Step 14 When a host is connected to the LAG, verify the port status for each member of the LAG. On a VSX pair, the local interface **State** should be **ALFNCD** and the partner interface should be **PLFNCD**. Verify that all interfaces in a LAG defined on a VSF stack have a **Sate** of **ALFNCD**, when connected to a host. The **Forwarding State** should be "Up" for local interfaces.

NOTE:

When assigning VLANs to a LAG on a server access (sub-leaf) switch, Fabric Composer automatically creates VLAN configuration for VLANs not present on the switch.

Configure the Border Leaf

The border leaf is the ToR switch pair that connects the data center fabric to other networks such as a campus, WAN, or DMZ.

When connecting overlay networks to external networks, segmentation is preserved by establishing a distinct Layer 3 connection for each data center overlay VRF. A firewall often is used between the fabric hosts and an external network for policy enforcement, but this is not a requirement. A firewall also can be configured to permit traffic between VRFs based on policy. When connecting multiple overlay VRFs that require preserving route table separation upstream, the firewall must support VRFs or device virtualization.

The following diagram illustrates the topology and BGP peerings for connecting the production overlay VRF to an active/passive pair of upstream firewalls.



Figure 4: Border Leaf Topology Production VRF

An MC-LAG is used between the border leaf switch pair and each upstream firewall. This strategy provides network path redundancy to each firewall. When using an active/passive firewall, traffic is forwarded only to the active upstream firewall. Detailed firewall configuration is outside the scope of this document.

Each MC-LAG between the border leaf switches and the firewalls is an 802.1Q trunk, where one VLAN per VRF is tagged on the LAG. Tagging the same VLANs on both LAGs supports the active/passive operation of the firewall. Using VLAN tags when only one overlay VRF is present supports adding overlay VRFs in the future without additional cabling or changing port roles from access to trunk.

MP-BGP EVPN advertisements share host routes inside the data center (/32 IPv4 and /128 IPv6). EVPN host routes are commonly filtered to connections outside the data center. In the following example, only network prefixes containing overlay hosts are shared, which can be redistributed connected routes or learned within the fabric from type-5 EVPN route advertisements.

In this sample implementation, each overlay VRF on the border leaf switches learns a default route and a campus summary route from the firewalls. The border leaf shares learned external routes with other leaf switches by advertising a type-5 EVPN route.

The following diagram illustrates additional elements required when adding external connectivity to the development overlay VRF. The same set of physical links between the border leaf and the firewalls is used to connect both production and development overlay VRFs. A development VRF VLAN is tagged on the previously configured MC-LAG trunks between the border leaf switches and the firewalls to support an additional set of BGP peerings with the firewall.



Figure 5: Border Leaf Topology Multiple VRFs

NOTE:

When using an Aruba CX 10000 in the border leaf role, physical ports connecting to external networks must be configured with *persona access*.

Configure External Routing VLAN SVIs

In the configuration steps below, the VLAN SVIs are created to use in eBGP peerings between border leaf switches and the upstream active/passive firewall pair.

Step 1 On the Configuration menu, select Routing > VRF.

HPE orubo Fabric Composer	Dashboard	Configuration Mainte	nance 🗸 Visualization 🖌 🔎 W	here
Ports	Conf	Ports >		
		Routing >	🛞 VRF	
Link Aggregation Groups		System >	🖧 BGP	
VLAN Groups		民 Network >	SPF	
PVI ANS		Administration >	EVPN	15
		Integrations >	EVPN VXLAN Multi-Fabric	+=
Transceivers		Relicy >	Route Policy	•
			4	d

Step 2 On the **Configuration > Routing > VRF** page, click the ••• symbol left of **PROD-DC-VRF** and select **IP Interfaces**.

Configura	ation / Rc	outing / VRF					
			Fabric	RSVDC-FB1			
							ACTIONS 🗸
		Name	1E	Туре	ĻΈ	Switches J=	L3 VNI
		Enter Name	••••]	Select Type	•	Enter Switches	Enter Regex
	\bigcirc	default		Default			
	\bigcirc	DEV-DC-VRF		User		RSVDC-FB1-VSX_RSVDC-FB1-	100002
						LF1-1_RSVDC-FB1-LF1-2,	
						RSVDC-FB1-VSX_RSVDC-FB1-	
						LF2-1_RSVDC-FB1-LF2-2,	
						RSVDC-FB1-VSX_RSVDC-FB1-	
						LF3-2_RSVDC-FB1-LF3-1	
	\bigcirc	mgmt		Management			
	\bigcirc	PROD-DC-VRF		User		RSVDC-FB1-VSX_RSVDC-FB1-	100001
IP Ir	nterfaces					LF1-1_RSVDC-FB1-LF1-2,	
	nonacco					RSVDC-FB1-VSX_RSVDC-FB1-	
IP S	static Rou	tes				LF2-1_RSVDC-FB1-LF2-2,	
Netw	works					RSVDC-FB1-VSX_RSVDC-FB1-	
ARF	P Tables					LF3-2_RSVDC-FB1-LF3-1	
IPR	loute Teb	65					
	ioute lab	100					
Swit	tches						

Step 3 On the right **ACTIONS** menu of the **IP Interfaces** tab, select **Add** to launch the **IP Interfaces** wizard.

Configuration / Routing / VRF / PRC	D-DC-VRF				
	Fabric	RSVDC-FB1			
				ତ ସ 🖗 C	ACTIONS 🗸
Name JE	Type 1	Switches	L3 VNI 📋 F	Route Target Ext-Community	Route Target N
Enter Name	Select Type 🔻	Enter Switches	Enter Regex	Enter Regex for Route Target	Select Route
PROD-DC-VRF	User	RSVDC-FB1-VSX_RSVDC-FB1-	100001 6	5001:100001	Both
		LF1-1_RSVDC-FB1-LF1-2,			
		RSVDC-FB1-VSX_RSVDC-FB1-			
		LF2-1_RSVDC-FB1-LF2-2,			
		RSVDC-FB1-VSX_RSVDC-FB1-			
		LF3-2_RSVDC-FB1-LF3-1			
IP INTERFACES IP STATIO	C ROUTES NETWORKS	ARP TABLES IP ROUTE TABL	LES SWITCHES		
				$\odot \bigcirc \bigcirc$	ACTIONS 🗸
Туре	Enabled	Switch 1	VLAN	J≟ Port/LA Add	
Select Type		Enter Switch	Enter Regex for VI	LAN Ente Edit	
O SVI	Yes	RSVDC-FB1-LF2-1	102	Delete	Ð
O SVI	Yes	RSVDC-FB1-LF2-2	102		

Step 4 On the IP Interfaces page, enter the following values and click NEXT.

- Type: SV/
- VLAN: 2021
- Switches: < Select the border leaf VSX pair object >
- IPv4 Subnetwork Address: 10.255.2.0/29
- IPv4 Addresses: 10.255.2.1-10.255.2.2
- Active Gateway IP Address: < blank >
- Active Gateway MAC Address: < blank >
- Enable VSX Shutdown on Split: < unchecked >
- Enable VSX Active Forwarding: < unchecked >
- Enable Local Proxy ARP: < unchecked >

P IP Interface	() ()
Interf	Acce Type Name Summary
Select the IP Interface Select the IP Interface	Type and set the appropriate attributes. face
Туре	SVI × -
VLAN *	2021
Switches *	A VLAN between 1 and 4094, example: 1. × RSVDC-FB1-VSX_RSVDC-FB1-LF1-1_RSVDC-FB1-LF1-2 × ▼ SELECT ALL
IPv4 Subnetwork Address *	10.255.2.0/29 A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24
IPv4 Addresses *	10.255.2.1-10.255.2.2 Enter a range of IPv4 Addresses to be assigned to the selected switches, example: 192.168.1.100-192.168.1.200. The range must include at least 2 addresses or match the Active Gateway IP Address.
Active Gateway IP Address	A valid IPv4 Address, example: 192.168.1.10. Both Active Gateway values must be defined if using Active Gateway.
Active Gateway MAC Address	A valid MAC Address, example: 00:00:00:00:00:00:00:01. Cannot include multicast or broadcast addresses Both Active Gateway values must be defined if using Active Gateway.
Enable VSX Shutdo	own on Split
Enable VSX Active Not applicable if an Activ	Forwarding re Gateway is specified. ICMP Redirect should be disabled in Switch settings if this is enabled.
Enable Local Proxy	/ ARP
(* = Required) S	croll for more options CANCEL BACK NEXT

Step 5 On the Name page, enter a Name and Description, then click NEXT.
IP Interface	9	() ×
Int	Verface Type Name	Summary
Enter an optional Na	me and Description.	
Name	PROD-DC-BORDER-LF to FW	
	A string, up to 42 characters. example: lpinterface1	
Description	Border leaf PROD-DC-VRF uplink to external FW cluster	
	Example: My New IP Interface	
(* = Required)		CANCEL BACK NEXT

Step 6 On the Summary page, review the interface settings and click APPLY.

P IP Interface			?
Interface Type	Name	Summary	
Name	PROD-DC-BORDER-LF to FW		
Description	Border leaf PROD-DC-VRF uplink to external FW c	luster	
Туре	SVI		
Enabled	Yes		
VLAN	2021		
Switches	RSVDC-FB1-VSX_RSVDC-FB1-LF1-1_RSVDC-FB1	-LF1-2	
IPv4 Addresses	10.255.2.1-10.255.2.2		
VSX Shutdown on Split	No		
VSX Active Forwarding	No		
Local Proxy ARP Enabled	No		
		BACK	

Step 7 Repeat this procedure to create an additional VLAN and SVI interface for DEV-DC-VRF. In step 2, select **DEV-DC-VRF**, then create an SVI with the following values:

Name	Description	TypeVLANSwitches	IPv4 Sub- network Address	IPv4 Addresses
DEV-DC- BORDER-LF to FW	Border leaf DEV-DC-VRF uplink to external FW cluster	SVI 202 < Border leaf VSX pair object >	10.255.2.8/2	10.255.2.9- 10.255.2.10

Create Border Leaf to Firewall MC-LAGs

A VSX-based MC-LAG is created to each individual firewall in the active/passive cluster from the border leaf switches.

HPE aruba Fabric Composer	Dashboard	Configuration 🗸 Mainter	nance - Visualization - 🔎 V
⊛ VRF	Conf	Ports	Ports
🖧 BGP		Routing >	Link Aggregation Groups
🖾 OSPF		民 Network >	이 PVLANS
I EVPN	Na	Administration >	C ^a Transceivers
EVPN VXLAN Multi-Fabric	E	Integrations > % Policy >	Select Type 💌
	PR_	and	User RS

Step 1 On the **Configuration** menu, select **Ports > Link Aggregation Groups**.

Step 2 On the right ACTIONS menu, select Add.

Config	guration / Po	rts / Link Aggregation Groups								
				Fabric	RSV	DC-FB1				
									$\mathbb{D} \otimes \mathbb{V}$	C ACTIONS V
		♂ Name	Ξŧ	Туре	ļΞ	LAG Number	Switch	1E	Ports 4	Add
		Enter Regex for Name		Select Type	~	Enter Regex	Enter Regex for Switch		Enter Regex for Por	Edit
>		ESX_RSVDC-FB1-LF2-		Provisioned		11	RSVDC-FB1-LF2-1		1/1/1	Delete
		1_1/1/1_RSVDC-FB1-LF2-2_1/1	/1				RSVDC-FB1-LF2-2		1/1/1	VLANs
>		ESX_RSVDC-FB1-LF3-		Provisioned		11	RSVDC-FB1-LF3-2		1/1/1	1, 101-102, 201-202
		1_1/1/1_RSVDC-FB1-LF3-2_1/1	/1				RSVDC-FB1-LF3-1		1/1/1	

Step 3 On the Create Mode page, leave Create a single LAG/MLAG selected and click NEXT.

🚥 Link Aggreg	gation Group					? ×
	?	?	?	?	?	
Create Mode	Settings	Ports	LACP Settings	VLANs	Summary	
Select an option to cr	eate the LAG(s). Ch	loose to create mu	ultiple MLAGs or to con	figure a single LAG.		
Create a single LA	AG/MLAG.					
○ Create multiple M	LAGs for selected \	/SX Pairs.				
(* = Required)				CANCEL	BACK	ЕХТ

Step 4 On the Settings page, enter the following values and click NEXT.

- Name: RSVDC-BL to EXT-FW1
- **Description:** MC-LAG from border leaf switches to FW1 in firewall cluster
- LAG Number: 251

🚥 Link Aggre	egation Group				(3) ×
Create Mode	Settings	? Ports	? LACP Settings	? VLANs	Summary	
Enter a required Na	me and optional Desc	ription and LAG I	Number.			
Name *	RSVDC-BL to EX	T-FW1 kample: LAG-1				
Description	MC-LAG from bot	rder leaf switches	to FW1 in firewall clus	ster		
LAG Number	251					
☐ Inter-Switch Linł	A number between 1 and	d 256, example 1				
(* = Required)				CANCEL	BACK	

Step 5 On the Ports page, select the border leaf VSX object from the LAG Switch Member dropdown.

🚥 Link Aggro	egation Group (RSVD	C-FB1)		? ×
Create Mode Select ports to add remove all associat	Settings Por to the LAG. Up to 2 switches m ted LAG port members on the s	ts LACP Settings VI	ANs er switch. F	Summary Removing a switch will also
⊞	LAG Switch Member	Select a Switch RSVDC-FB1-VSX_RSVDC-FB1-LF1 1_RSVDC-FB1-LF1-2	-	
	Health ↓= Select Health ▼	RSVDC-FB1-VSX_RSVDC-FB1-LF2 1_RSVDC-FB1-LF2-2 RSVDC-FB1-VSX_RSVDC-FB1-LF3 2_RSVDC-FB1-LF3-1 RSVDC-FB1-LF3-SA1	2-	€ S

Step 6 Click the **Switch View** mode icon to identify ports more easily. Click the port icons connected to the first firewall to add them as members of the link aggregation group and click **NEXT**.

Link Aggregation Group (RSVDC-FB1)) ×
Create Mode Settings Ports LACP Settings VLANs Summary	
Select ports to add to the LAG. Up to 2 switches may be selected with up to 16 ports per switch. Removing a switch will also remove all associated LAG port members on the switch from the LAG.	C
LAG Switch Member RSVDC-FB1-VSX_RSVDC × 2 selected Ⅲ ☑	
Selected Trailable LINK AGGREGATION GROUP	
■ Enabled ■ Disabled ■ No Transceiver ■ Filtered ■ Port has a health issue ●/● Link Up ● Link Down	
✓ RSVDC-FB1-LF1-1 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37	
(* = Required) Scroll for more options CANCEL BACK NEXT	
NOTE:	

A checkmark appears on the newly selected ports. The diamond icon appears on ports that are not currently available for a new LAG group assignment.

Step 7 On the LACP Settings page, leave all settings at their defaults and click NEXT.

∎ Li	nk Aggre	gation G	aroup (R	SVDC-F	B1)					?
)	(?)		\bigcirc	
Crea	ate Mode	Settin	gs	Ports	LACP Set	ttings	VLANs		Summary	
Enable	or disable LA	CP Fallbac	k for an ML	AG and sele	ect a Switch entry	/ to cor	nfigure LACP sett	ings.		
🖌 Enal	ble LACP Fa	llback	I						1	
	Switch	1E	Ports	ĻΞ	LACP Mode	ĻΞ	LACP Interval	ĻΞ	Priority	ĻΞ
	RSVDC-FB	1-LF1-1	1/1/11		Active		Slow		1	
	RSVDC-FB	1-LF1-2	1/1/11		Active		Slow		1	
ACP M	lode	Active								
ACP In	iterval	Slow								
riority		1								
		A number be	etween 1 and 6	5535, example	1					
	Required)						CANCEL		BACK	NEXT

Step 8 On the **VLANs** page, enter the VLAN ID for each VRF previously created to connect to external networks in the **VLANs** field, and click **NEXT**.

🚥 Link Aggr	egation Group (RSVDC-FB1)	? ×
Create Mode	Settings Ports LACP Settings VLANs Summa	ary
Assign Native VLA MLAG.	N, VLANs, VLAN Groups, and PVLAN Port Type to the LAG. At least one VLAN must be config	gured for an
Native VLAN	1 A VLAN between 1 and 4094 or an empty value, example: 1. Tagged Native VLAN Can only be set when there is a Native VLAN at least one VLAN or VLAN Group assigned.	
VLANs	2021-2022 'All' for all VLANs or a number, set, or range of VLANs between 1 and 4094, example: 5, 10-45, 102.	
VLAN Group	Select	▼
PVLAN Port Type	There are no PVLANs configured on the selected switch(es).	
(* = Required)	CANCEL BACK	NEXT

Step 9 On the **Summary** page, review the link aggregation settings and click **APPLY**.

Link Aggre	gati	on Grou	ıp (RS	VD	C-FB1)						? ×
Create Mode		Settings		Poi	rts L	ACP Setting	gs	VLANs		Summa	iry
Name			RSVDC	C-BL t	o EXT-FW1						
Description			MC-LA	G fro	m border leaf	switches to	FW1 ir	firewall clus	ter		
LAG Number			251								
Туре			Provisio	oned							
Native VLAN			1								
VLANs			2021-2	022							
VLAN Groups											
PVLAN Port Type											
Enable LACP Fallb	ack		Yes								
Switch	1E	Ports		ļΞ	LACP Mode	ΨĒ	LACP	Interval	ΨĒ	Priority	ΨĒ
RSVDC-FB1-LF1-1		1/1/11			Active		Slow			1	
RSVDC-FB1-LF1-2		1/1/11			Active		Slow			1	
								CANCEL		ВАСК	APPLY

Step 10 Repeat the procedure to create an additional MC-LAG on ports connecting the VSX border leaf switch pair to the second firewall using the following settings:

		LAG			
Name	Description	Numbe	er Ports	LACP Settings	VLANs
RSVDC-BL	MC-LAG from border leaf switches	252	12 (on each	< Leave all	2021-
to	to FW2 in firewall cluster		switch	defaults >	2022
EXT-FW2			member)		

Configure Host Filter Prefix List

Host routes and point-to-point link prefixes should not be advertised to external networks. The following procedure creates a prefix list used in route policy to filter /31 and /32 IPv4 prefix advertisements.

Step 1 On the Configuration menu, select Routing > Route Policy.

HPE or Ubo Fabric Composer	Dashboard Configuration 🛩 Main	tenance 🗸 Visualization 🖌 🔎 Whe
Ports	Conf	
Link Aggregation Groups	System >	€ VRF BGP
🔁 VLAN Groups	Retwork >	OSPF
문권 PVLANs	Administration >	EVPN
	Integrations >	EVPN VXLAN Multi-Fabric
cª Transceivers	> Policy >	Route Policy

Step 2 Click the PREFIX LISTS tab. On the right ACTIONS menu, select Add.

onfiguration / Rou	iting / Route Policy							
ROUTE MAPS	COMMUNITY LISTS	PREF	IX LISTS	AS PATH	LISTS			
							070	C ACTIONS -
	Name	1E	Address Far	nily 📖	Origin	1£	Switches	Add
	Enter Regex for Name		Select Add	ire 🔻	Select Origin	-	Enter I	Edit
					There is no data to disp	lay		Delete
								Clone
								Merge
								Unmerge
								Entries

Step 3 On the Settings page, enter a Name and Description, then click NEXT.

Prefix List	×
Settings	Scope Entries Summary
Enter a required Nam	ne and an optional Description.
Name *	PL-HOST-P2P
	Any non-empty string without spaces and without " or ?, example: PrefixList1
Description	Match /31 and /32 routes
	Any non-empty string up to 80 characters long, example: My Prefix List
(* = Required)	CANCEL BACK NEXT
NOTE:	
The Name valu	ue defines the name of the prefix list in Fabric Composer and on the switch.

Step 4 On the Scope page, select the two border leaf switches in the Switches field, then click NEXT.

Prefix List	0	×
Sottings		
Select optional Fabrics Switches.	s or Switches to apply this configuration. A Fabric implies all Switches contained within it, excluding Sub Leaf	
Fabrics	Select	r
Switches	× RSVDC-FB1-LF1-1 (RSVDC-FB1) × RSVDC-FB1-LF1-2 (RSVDC-FB1)	r
(* = Required)	CANCEL BACK NEXT	

Step 5 On the Entries page, enter the following non-default values and click Add

- Action: Permit
- Prefix: 0.0.0.0/0
- **GE:** 31

Prefix List						>
				\checkmark	?	
Settings		Scope	E	Entries	Summary	
Enter a required Seque	nce, Action, and P	refix Address an	d an optional des	scription, GE, a	and LE.	1
Sequence *	10					
Ą	number between 1 and	d 4294967295, exam	ple 1. The Sequence	must be unique.		
Description						
L A	ny non-empty string up	to 80 characters lon	g, example: My Prefix	x List		
Action *	Permit					-
Prefix *	0.0.0/0					
	Any" or a valid IPv4 Sul	onet in CIDR format.	Example: 192.168.1.	0/24. Prefix Length	n must be less than or equal to G	E.
GE	31					Ī
Ą	number between 0 and	d 32, example: 0. GE	must be greater thar	n or equal to the Pr	efix Length and less than or equ	al to LE.
LE						
L A	number between 0 and	d 32, example: 0. LE	must be greater than	or equal to GE.		
CLEAR ADD	UPDATE					
Sequence	Description	Action	Prefix	GE	LE	
		There	is no data to displa	ay		
(* = Required) Sc	croll for more opti	ons			CANCEL BACK	NEXT

Step 6 Click NEXT.

🖪 Pre	efix List						:	×
				($\overline{\mathcal{A}}$?)	
	Settings		Scope	En	tries	Summa	ary	
AGUON		JEIEUL					•	
Prefix *								
	"Ai	ny" or a valid IPv4 Subr	net in CIDR format. Ex	ample: 192.168.1.0/2	24. Prefix Length mus	t be less than or equa	to GE.	
GE								
GE								
	A r	umber between 0 and	32, example: 0. GE m	ust be greater than o	r equal to the Prefix L	ength and less than o.	r equal to LE.	
LE								
	Ar	umber between 0 and	32 example: 0 I E m	ust be greater than o	regual to GE			
CLEA	R ADD	UPDATE						
	Sequence	Description	Action	Prefix	GE	LE		
	10		Permit	0.0.0.0/0	31		位	
(* = Re	equired) Scr	oll for more optio	ns		с	ANCEL	CK NEXT	

Step 7 On the **Summary** page, review the prefix list settings and click **APPLY**.

Prefix List					
Settings		Scope	Entries	S	Summary
Name		PL-HOST-P2P			
Description		Match /31 and /32	2 routes		
Fabrics					
Switches		RSVDC-FB1-LF1-	1		
		RSVDC-FB1-LF1-	2		
Sequence	Description	Action	Prefix	GE	LE
10	1	Permit	0.0.0/0	31	/
				CANCEL	BACK APPLY

Configure Campus AS Path List

An internal BGP peering is established between the border leaf pair to create a routed backup path to the upstream firewall. IP prefixes learned in the fabric should not be advertised in the overlay BGP peering between the border leaf pair to avoid a routing loop. The following procedure creates an AS path list that matches only prefix advertisements sourced from the upstream firewall and campus routers.

Step 1	Click the	AS PATH LIS	TS tab. On	the right A	CTIONS menu	select Add
Step i	Click the		J (ab. 011	une ngnu n		, sciect nuu .

Configuration / Routing / Route Policy					
ROUTE MAPS COMMUNITY LISTS	PREFIX LISTS	AS PATH LISTS			
				ତ ⊗ Ţ €	C ACTIONS V
Name	J <u>≞</u> Sv	vitches	ĻΞ	Fabrics	Add
Enter Regex for Name		Enter Regex for Switches		Enter Regex f	Edit
	The	re is no data to display			Delete
					Clone
					Merge
					Unmerge
					Entries

Step 2 On the Name page, enter a Name and Description, then click NEXT.

편 AS Path L	ist		×
Settings	s Scope	Entries	Summary
Enter a required Na	me and an optional Description.		
Name *	ALLOWED-EXT-AS		
	Any non-empty string without spaces and without " or	r ?, example: AsPathList1	
Description	External ASNs allowed to advertise into	DC overlay	
	Any non-empty string up to 80 characters long, exam	ple: My AS Path List	
([*] = Required)		CANC	EL BACK NEXT

Step 3 On the Scope page, select the two border leaf switches in the Switches field, then click NEXT.

🗗 AS Path Lis	t ×
	 ?
Settings Select optional Fabric Switches	Scope Entries Summary s or Switches to apply this configuration. A Fabric implies all Switches contained within it, excluding Sub Leaf
Fabrics	Select 👻
Switches	× RSVDC-FB1-LF1-1 (RSVDC-FB1) × RSVDC-FB1-LF1-2 (RSVDC-FB1)
(* = Required)	CANCEL BACK NEXT

Step 4 On the **Entries** page, enter the following values and click **ADD**.

- Sequence: 10
- **Description**: permit campus originated advertisements
- Action: Permit
- Regex: ^65501 65000\$

					?
Settings	Scope		Entries	Summary	
Add one or more entrie	es with a required Sequence,	Action, and Regex a	nd an optional descripti	ion.	
Sequence *	10				
1	A number between 1 and 429496729	95, example 1. The Seque	nce must be unique.		
Description	permit campus originated a	dvertisements			
	Any non-empty string up to 80 chara	cters long, example: My A	S Path List		
Action *	Permit				•
Regex *	^65501 65000\$				
	A regular expression to match the BC	GP AS Paths, example: _6	5001\$		
CLEAR ADD	UPDATE				
Sequence	Description	Action	Regex		
	1	There is no data to di	splay	1	
(* = Required) S	croll for more options		CA	NCEL BACK	NEXT
NOTE:					

The **Regex** field value matches BGP advertisements originated by the campus AS (65000) that are received by the RSVDC fabric border leaf via the firewall AS (65501). Routes advertised by the campus that are received from other external AS numbers are not accepted.

Step 5 On the Entries page, enter the following values and click ADD.

- Sequence: 20
- Description: permit firewall originated advertisements
- Action: Permit
- **Regex**: ^65501\$

🖪 AS Path Li	ist			×			
Settings	Scope	Entri	es	Summary			
Enter a required Sec	, quence, Action, and Regex and ar	n optional description.					
Sequence *	20						
	A number between 1 and 4294967295,	example 1. The Sequence must	be unique.				
Description	permit firewall originated adve	ertisements					
	Any non-empty string up to 80 characte	rs long, example: My AS Path Li	st				
Action *	Permit			~			
Regex *	^65501\$						
	A regular expression to match the BGP	AS Paths, example: _65001\$					
CLEAR AD	UPDATE						
Sequence	Description	Action	Regex				
10	permit campus	Permit	^65501 65000\$	₫			
	originated						
([*] = Required)	(* = Required) Scroll for more options CANCEL BACK NEXT						
NOTE:							

The **Regex** field value matches BGP advertisements originated by the firewall AS. In this example topology, the default route is originated by the firewall.

Step 6 Click NEXT.

				?	
Settings	Scope		Entries	Summary	
nter a required Sequen	ce, Action, and Regex and a	n optional descriptio	on.		
equence *	30				
A number between 1 and 4294967295, example 1. The Sequence must be unique.					
Description					
Any	y non-empty string up to 80 characte	ers long, example: My AS	Path List		
Action * Select					
legex *					
Ar	egular expression to match the BGP	PAS Paths, example: _65	001\$		
CLEAR ADD	UPDATE				
Sequence	Description	Action	Regex		
10	permit campus	Permit	^65501 65000\$	団	
	originated				
	advertisements				
20	permit firewall	Permit	^65501\$	団	
	advertisements				

Step 7 On the **Summary** page, verify the AS path list settings and click **APPLY**.

Settings	Scope	Entries	Summary
Name	ALLOWED-EXT-AS		
Description	External ASNs allowed to advertise	se into DC overlay	
Fabrics			
Switches	RSVDC-FB1-LF1-1		
	RSVDC-FB1-LF1-2		
Sequence	Description	Action	Regex
10	permit campus originated	Permit	^65501 65000\$
	advertisements		
20	permit firewall originated	Permit	^65501\$
	advertisements		

Configure Firewall Route Map

The following procedure creates a route map that will be applied outbound to external BGP peers. The route map policy filters host and point-to-point prefixes using the previously created host filter prefix list.

Step 1 On the **Configuration > Routing > Route Policy** page, click the **ROUTE MAPS** tab. On the right **ACTIONS** menu, select **Add**.

Configuration / Rou	ting / Route Policy							
ROUTE MAPS	COMMUNITY LISTS	PRE	FIX LISTS	AS PATH LIST	ΓS			
							C	ACTIONS 🗸
	Name	ΤE	Switches		μĒ	Fabrics	Add	
	Enter Regex for Name		Enter Reg	ex for Switches		Enter	Edit	
		The	re is no data to	o display			Delet	e
							Clone	Э
							Merg	e
							Unm	erge
							Entrie	es

🕸 Route Ma	р	×
Name	Scope Entries Summary	
Enter a required Na	ame and an optional Description.	
Name *	RM-EXT-OUT	
	Any non-empty string without spaces and without " or ?, example: RouteMap1	
Description	Route map to filter outbound prefixes to external network BGP peers	
	Any non-empty string up to 80 characters long, example: My Route Map	
(* = Required)	CANCEL BACK NEX	кт

Step 2 On the Name page, enter a Name and Description, then click NEXT.

Step 3 On the Scope page, select the two border leaf switches in the Switches field, then click NEXT.

🛿 Route Map		×
Name	Scone Entries Summary	
Select optional Fabrics Switches.	s or Switches to apply this configuration. A Fabric implies all Switches contained within it, excluding Sub	Leaf
Fabrics	Select	-
Switches	× RSVDC-FB1-LF1-1 (RSVDC-FB1) × RSVDC-FB1-LF1-2 (RSVDC-FB1)	× -
(* = Required)	CANCEL BACK NEXT	г

Step 4 On the **Entries** page, click the right **ACTIONS** menu and select **Add** to launch the **Route Map Entries** wizard.

19 Route Map				×
Name	Scope	Entries		Summary
Configure optional entries. Entries w	Il be added when the Rou	te Map configuratio	n is applied.	
			$\bigcirc \bigcirc$	ACTIONS Y
Sequence L	Action 1	Route Map 1	Match IPv4 Prefix	Add
Enter Regex	Enter Regex for Act	Enter Regex	Enter Regex for Ma	Remove a
(* = Required) Scroll for more	options		CANCEL	BACK NEXT

Step 5 Route Map Entries wizard: On the **Settings** page, enter the following non-default values and click **NEXT**.

- Description: filter host and P2P prefixes
- Action: Deny

🕸 Route Ma	p Entries ×
	??
Setting	Match Attributes Set Attributes Summary
Configure a require	a Sequence and Action and optional Description and Houte Map Continue.
Sequence *	10
	A number between 1 and 4294967295, example 1. The Sequence must be unique.
Description	filter host and P2P prefixes
	Any non-empty string up to 80 characters long, example: My Route Map
Action *	Deny 🗸 🗸
Route Map	
Continue	A number between 2 and 4294967295, example 2. Boute Map Continue must be greater than the Sequence
(* = Required)	CANCEL BACK NEXT

Step 6 Route Map Entries wizard: On the **Match Attributes** page, enter the following values and click **NEXT**.

- Attributes: Match IPv4 Prefix List
- Match IPv4 Prefix List: PL-HOST-P2P

🕸 Route Map	Entries			×
Settings	Match Attributes	Set Attributes	Summary	
Configure optional Ma	atch values for this entry.			
Attributes	× Match IPv4 Prefix List			× -
	Select which match attributes to configure for this entry.			
Match IPv4 Prefix List	PL-HOST-P2P		~	ADD
(* = Required)			CANCEL BACK	NEXT

Step 7 Route Map Entries wizard: On the Set Attributes page, click NEXT.

😰 Rout	e Map Entries	5			×
	Settings	Match Attributes	Set Attributes	Summary	
Configure of	ptional Set values f	or this entry.			
Attributes	Select				-
	Select wh	ich set attributes to configure for this entr	у.		
(* = Requ	uired)			CANCEL BACK	NEXT

Step 8 Route Map Entries wizard: On the **Summary** page, review the route map entry settings and click **APPLY**.

SettingsNatch AttributesSet AttributesSummarySequence10Descriptionfilter host and P2P prefixesActionDenyMote Map ContinueMatch IPv4 Prefix ListPL-HOSTP2P	Route Map Entries					×
SettingsMatch AttributesSet AttributesSummarySequence10Descriptionfilter host and P2P prefixesActionDenyRoute Map ContinueMatch IPv4 Prefix ListPL-HOST-P2P						
Sequence10Descriptionfilter host and P2P prefixesActionDenyRoute Map ContinueMatch IPv4 Prefix ListPL-HOST-P2P	Settings	Match Attributes	Set Attributes		Summary	
Descriptionfilter host and P2P prefixesActionDenyRoute Map ContinueMatch IPv4 Prefix ListPL-HOST-P2P	Sequence		10			
ActionDenyRoute Map ContinuePL-HOST-P2P	Description		filter host and P2P prefixes			
Route Map Continue Match IPv4 Prefix List PL-HOST-P2P	Action		Deny			
Match IPv4 Prefix List PL-HOST-P2P	Route Map Continue					
	Match IPv4 Prefix List		PL-HOST-P2P			
CANCEL BACK APPLY				CANCEL	ВАСК	APPLY

Step 9 Create a second route map sequence. On the **Entries** page, click the right **ACTIONS** menu, and select **Add**.

🛿 Route Ma	ар				3
		Scape			(?) Summary
Configure optiona	al entries. Entries will	be added when the Rou	te Map configuration	n is applied.	
					7 🥸 ACTIONS 🗸
	Sequence	Action 1	Route Map 1	Match IPv4 Prefix	Add
	Enter Regex	Enter Regex for Act	Enter Regex	Enter Regex for Ma	Remove
٢	10	Deny		PL-HOST-P2P	
(* = Required)	Scroll for more	options		CANCEL	BACK

Step 10 Route Map Entries wizard: On the **Settings** page, set the **Action** field to *Permit* and click **NEXT**.

🕸 Route Ma	o Entries	×
Sattinge	Match Attributes Set Attributes Surgmany	
Configure a required	d Sequence and Action and optional Description and Route Map Continue.	
Sequence *	20	
	A number between 1 and 4294967295, example 1. The Sequence must be unique.	
Description		
	Any non-empty string up to 80 characters long, example: My Route Map	
Action *	Permit	-
Route Map		
Continue	A number between 2 and 4294967295, example 2. Route Map Continue must be greater than the Sequence.	
(* = Required)	CANCEL BACK NEX	хт

Step 11 Route Map Entries wizard: On the Match Attributes page, click NEXT.

🛿 Ro	oute Map Ent	ries			×
	Settings	Match Attributes	? Set Attributes	? Summary	
Configur	e optional Match v	alues for this entry.			
Attribute	s Se	elect			-
	Selec	ct which match attributes to configure for thi	s entry.		
(* = R	equired)			CANCEL BACK	NEXT

Step 12 Route Map Entries wizard: On the Set Attributes page, click NEXT.

🛿 Route	e Map Entries	3			×
			Sat Attributes		
Configure op	otional Set values fo	or this entry.	Set Attributes	Summary	
Attributes	Select				•
	Select whi	ch set attributes to configure for this entr	ry.		
(* = Requi	ired)		C	CANCEL BACK NE	хт

Step 13 Route Map Entries wizard: On the **Summary** page, review the route map entry settings and click **APPLY**.

Route Map Entrie	S			×
Settings	Match Attributes	Set Attributes	Summary	
Sequence			20	
Description Action			Permit	
Route Map Continue				
			CANCEL BACK APP	PLY

Step 14 On the Entries page, click NEXT.

🛿 Route M	ар				? ×
Add one or more	entries. Entries will	Scope	Entrie Map configuration	s S	Summary
					ACTIONS Y
	Sequence	Action	Route Map 1	Match IPv4 Prefix 1	Match Community 1
0	10	Deny		PL-HOST-P2P	
0	20	Permit			
(1 - 2 of 2 total)	25 🗸				1
(* = Required)				CANCEL	BACK

19 Route Map	×
Name	RM-EXT-OUT
Description	Route map to filter outbound prefixes to external network BGP peers
Fabrics	
Switches	RSVDC-FB1-LF1-1
	RSVDC-FB1-LF1-2
	CANCEL BACK APPLY

Step 15 On the Summary page, review the route map settings and click APPLY.

Configure Internal Border Leaf Route Map

The following procedure creates a route map that is applied to the BGP peering between the border leaf switches. The route map permits advertising only prefixes originated by the campus AS number or the upstream firewall AS number.

Step 1 On the right ACTIONS menu of the ROUTE MAPS tab, select Add.

Step 2 On the Name page, enter a Name and Description, then click NEXT.

🛯 Route Ma	ар	×
	· · · · · · · · · · · · · · · · · · ·	
Name	e Scope Entries Summary	
Enter a required N	Name and an optional Description.	
Name *	RM-PERMIT-CAMPUS	
	Any non-empty string without spaces and without " or ?, example: RouteMap1	
Description	Permit prefixes originated by campus and upstream firewall ASNs	
	Any non-empty string up to 80 characters long, example: My Route Map	
(* = Required)	CANCEL BACK NE	EXT

Step 3 On the Scope page, select the two border leaf switches in the Switches field, then click NEXT.

🕸 Route Map		×
Name	Scope Entries Summary	
Select optional Fabric Switches.	cs or Switches to apply this configuration. A Fabric implies all Switches contained within it, excluding Sub	Leaf
Fabrics	Select	-
Switches	× RSVDC-FB1-LF1-1 (RSVDC-FB1) × RSVDC-FB1-LF1-2 (RSVDC-FB1)	. –
(* = Required)	CANCEL BACK NEXT	

Step 4 On the **Entries** page, click the right **ACTIONS** menu, and select **Add** to launch the **Route Map Entries** wizard.

19 Route Map				×
Name	Scope	Entries		Summary
Configure optional entries. Entries will	be added when the Rout	e Map configuration	n is applied.	
			\odot	ACTIONS Y
Sequence	Action 1	Route Map 1	Match IPv4 Prefix	Add
Enter Regex	Enter Regex for Act	Enter Regex	Enter Regex for N	Remove
(* = Required) Scroll for more	options		CANCEL	BACK NEXT

Step 5 Route Map Entries wizard: On the **Settings** page, enter the following non-default values and click **NEXT**.

- **Description:** allow campus and firewall ASNs
- Action: Permit

🕸 Route Ma	p Entries	×
	? ? ?	
Settings Configure a require	Match Attributes Set Attributes Summary	
Sequence *	10	
	A number between 1 and 4294967295, example 1. The Sequence must be unique.	
Description	allow campus and firewall ASNs	
	Any non-empty string up to 80 characters long, example: My Route Map	
Action *	Permit	•
Route Map		
Continue	A number between 2 and 4294967295, example 2. Route Map Continue must be greater than the Sequence.	
(* = Required)	CANCEL BACK NEXT	

Step 6 Route Map Entries wizard: On the **Match Attributes** page, enter the following values and click **NEXT**.

- Attributes: Match AS Path List
- Match IPv4 Prefix List: ALLOWED-EXT-AS

🛿 Route Map) Entries			×
Settings	Match Attributes	Set Attributes	Summary	
Configure optional N	latch values for this entry.			
Attributes	× Match AS Path List Select which match attributes to configure for this entry.			× •
Match AS Path List	ALLOWED-EXT-AS		•	ADD
(* = Required)		[CANCEL BACK	NEXT

Step 7 Route Map Entries wizard: On the **Set Attributes** page, click **NEXT**.

Step 8 Route Map Entries wizard: On the **Summary** page, review the route map entry settings and click **APPLY**.

Route Map Entries					×
Settings	Match Attributes	Set Attributes		Summary	
Sequence	10				
Description	allow carr	npus and firewall ASNs			
Action	Permit				
Route Map Continue					
Match AS Path List	ALLOWEI	D-EXT-AS			
				DACK	
			CANCEL	BACK	APPLY

Step 9 Create a second route map sequence. On the **Entries** page, click the right **ACTIONS** menu, and select **Add**.

🕸 Route Map				×
Name Configure optional entries. Entri	Scope	Entries	n is applied.	Summary
				ACTIONS V
Sequence Enter Rege	Lie Action Lie Enter Regex for Act	Route Map 1	Match IPv4 Prefix Enter Regex for N	Add · · Remove /
O 10	Permit			
(* = Required) Scroll for I	nore options		CANCEL	BACK NEXT

Step 10 Route Map Entries wizard: On the **Settings** page, set the **Action** field to **Deny** and click **NEXT**.

🕸 Route Map	> Entries ×
Settings	Match Attributes Set Attributes Summary
Configure a required	d Sequence and Action and optional Description and Route Map Continue.
Sequence *	20
	A number between 1 and 4294967295, example 1. The Sequence must be unique.
Description	
	Any non-empty string up to 80 characters long, example: My Route Map
Action *	Deny
Route Map	
Continue	A number between 2 and 4294967295, example 2. Route Map Continue must be greater than the Sequence.
(* = Required)	CANCEL BACK NEXT

Step 11 Route Map Entries wizard: On the Match Attributes page, click NEXT.

Step 12 Route Map Entries wizard: On the Set Attributes page, click NEXT.

Step 13 Route Map Entries wizard: On the **Summary** page, review the route map entry settings and click **APPLY**.

Route Map Entries	S			×
Settings	Match Attributes	Set Attributes	Summary	
Sequence			20	
Description				
Action			Deny	
Route Map Continue				
			CANCEL BACK APP	LY
		L		

Step 14 On the Entries page, click NEXT.

				(?
Nam	ne	Scope	Entries	Sum	nmary
onfigure option	al entries. Entries wil	II be added when the Rout	e Map configuration	n is applied.	
				$\bigcirc \bigcirc \blacksquare \blacksquare$	🔆 ACTIONS 🗸
	Sequence	Action 1=	Route Map ↓	Match IPv4 Prefix 1	Match Community
	Enter Regex	Enter Regex for Act	Enter Regex	Enter Regex for Ma	Enter Regex for N
0	10	Permit			
\bigcirc	20	Deny			

Step 15 On the **Summary** page, review the route map settings and click **APPLY**.
1 Route Map	×
Name	Scope Entries Summary
Name	RM-PERMIT-CAMPUS
Description	Permit prefixes originated by campus and upstream firewall ASNs
Fabrics	
Switches	RSVDC-FB1-LF1-1
	RSVDC-FB1-LF1-2
	CANCEL BACK APPLY

Configure Border Leaf BGP Peerings

The following procedure configures the eBGP peerings between the border leaf switches and the upstream firewalls with a route map applied to filter host routes and point-to-point link prefixes. A single BGP peering is defined to the upstream firewalls, which is established only with the active firewall in the active/passive pair.

Step 1 On the left navigation menu, click **BGP**. Click the **PROD-DC-VRF** radio button. On the right **ACTIONS** menu, select **Edit**.

Configura	ation / Ro	outing / BGP			
		Fabric	RSVDC-FB1		
					C ACTIONS -
		VRF Name	ĮΞ	Switches	Edit
		Enter VRF Name		Enter Switches	Switches
	0	default		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2, RSVDC-FB1	Neighbors Summary
				LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-LF3-1, RSVE	
				FB1-LF3-2, RSVDC-FB1-SP1, RSVDC-FB1-SP2	
	\bigcirc	DEV-DC-VRF			No
	۲	PROD-DC-VRF			No

Step 2 On the **Settings** page, check **Enable BGP on PROD-DC-VRF**, check **Redistribute Loopback**, and click **APPLY**.

🖒 BGP Global	Configuration PROD-DC-VRF		?	×			
		SUMMARY					
Set the required Keep	Alive and Hold Down Timers and Maximum Paths.						
Enable BGP on PF	ROD-DC-VRF			L			
Default Keep Alive	60						
Timer *	A number of seconds between 1 and 65535, example: 65535. Keep Alive must be less than Hold Down. Setting both timers to 0 will reset to defaults.						
Default Hold Down	180						
Timer *	A number of seconds between 3 and 65535, example: 65535. Keep Alive must be less than Hold Down. Setting both timers to 0 will reset to defaults.						
Maximum Paths *	8						
	A number between 1 and 8, example: 8			1			
	✓ Redistribute Connected Routes			L			
	Redistribute OSPF						
	Redistribute Static Routes						
	✓ Redistribute Loopback						
	✓ ECMP Best Path						
	✓ Fast External Fallover						
	🗋 Trap Enable						
	Log Neighbor Changes						
	Deterministic Multi Exit Discriminator						
	Always Compare Multi Exit Discriminator						
(* = Required)	croll for more options	CANCEL	PPLY				
NOTE							
NOTE:							
The loopbac	interfaces that are redistributed ar	e created in the Assign Unique Overlay	Loop	-			

backs procedure later in this guide.

Step 3 On the **Configuration > Routing > BGP** page, click the ••• symbol left of **PROD-DC-VRF** and select **Switches**.

Configur	ation / R	outing / BGP			
		Fabri	c RSVDC-FB1		
					🖓 🥸 C actions 🗸
		VRF Name	lΞ	Switches	↓≟ I Enabled ↓≟
		Enter VRF Name		Enter Switches	Select Ena 🔻
	\bigcirc	default		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2, RSVDC-FB	31- Yes
				LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-LF3-1, RSV	VDC-
				FB1-LF3-2, RSVDC-FB1-SP1, RSVDC-FB1-SP2	
	\bigcirc	DEV-DC-VRF			No
	\bigcirc	PROD-DC-VRF		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2, RSVDC-FB	31- Yes
Suri	tohoo			LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-LF3-1, RSV	VDC-
Swi	liches			FB1-LF3-2	
Nei	ghbors S	ummary			

Configura	ation / Ro	uting / BGP / PROD-DC-VRF				
		Fa	abric RSVE	DC-FB1		
VRF Na	ame		1E	Switches		↓≟ I Enabled ↓≟
Enter	VRF Nam	e		Enter Switches		Select Ena 🔻
PROD-E	DC-VRF			RSVDC-FB1-LF1-1, RS	VDC-FB1-LF1-2, RSVDC-FB1-LF2-	1, Yes
				RSVDC-FB1-LF2-2, RS	VDC-FB1-LF3-1, RSVDC-FB1-LF3-	2
SWIT	TCHES	NEIGHBORS SUMMARY				
SWIT	TCHES	NEIGHBORS SUMMARY	↓≟ Enablec	1	ASN (ASPLAIN)	O ♥ ↔ ACTIONS ♥
SWIT	TCHES	NEIGHBORS SUMMARY	LE Enabled	i Enabled 👻	ASN (ASPLAIN) Enter Regex for ASN (ASP	O Image: Second state with the seco
SWIT	TCHES	NEIGHBORS SUMMARY	Jà Enablec Select Yes	t t Enabled 👻	ASN (ASPLAIN) Enter Regex for ASN (ASPL 65001	O Image: Constraint of the second
SWIT	ICHES	NEIGHBORS SUMMARY Name Enter Name RSVDC-FB1-LF1-1 -FB1-LF1-2	Lia Enablec Select Yes Yes	t Enabled 👻	ASN (ASPLAIN) Enter Regex for ASN (ASP) 65001 65001	ACTIONS V La Router ID LAI Enter Regex for Router 10.250.0.11 10.250.0.13
SWIT	rches	NEIGHBORS SUMMARY Name Enter Name RSVDC-FB1-LF1-1 -FB1-LF1-2 -FB1-LF2-1	Lia Enablec Select Yes Yes Yes	t Enabled 👻	ASN (ASPLAIN) Enter Regex for ASN (ASPL 65001 65001 65001	O Image: Construct of the second secon
SWIT	rches O ighbors	NEIGHBORS SUMMARY Name Enter Name RSVDC-FB1-LF1-1 -FB1-LF1-2 -FB1-LF2-1 RSVDC-FB1-LF2-2	LE Enableo Select Yes Yes Yes Yes	t Enabled 👻	ASN (ASPLAIN) Enter Regex for ASN (ASPL 65001 65001 65001 65001 65001	O Image: Constraint of the second seco
SWIT	rches o ighbors o	NEIGHBORS SUMMARY	Jà Enablec Select Yes Yes Yes Yes Yes	i Enabled 👻	ASN (ASPLAIN) Enter Regex for ASN (ASPL 65001 65001 65001 65001 65001 65001 65001	Image: Non-Section Section Sec

Step 4 On the SWITCHES tab, click • • • next to RSVDC-FB1-LF1-1 and select Neighbors.

Step 5 On the right ACTIONS menu of the NEIGHBORS tab, select Add.

Configuration / Routi	ing / BGP / PRC	DD-DC-VRF / RSVDC-	-B1-LF1-1					
		Fab	oric RSVDC	-FB1				
						۲	o ∖ o c	ACTIONS 🗸
Name	1E	Enabled	ĮΞ	ASN (ASPLAIN)	μ <u>ε</u>	Router ID	1E	Networks
Enter Name		Select Enabled	•	Enter Regex for	ASN (ASPLAI	Enter Regex fo	r Router ID	Enter Regex for
RSVDC-FB1-LF1-1		Yes		65001		10.250.0.11		
NEIGHBORS							• • •	ACTIONS 🗸
	🖉 Name	LE C	Description	μ <u>ε</u>	Туре	UE.	Neighbo Ac	ld
	Enter Name		Enter Descri	ption	Select Type	. •	Enter Ec	lit
						Th	nere is no da De	nete

Step 6 On the Settings page, enter the following non-default values and click NEXT.

- Neighbor AS Number: 65501
- IP Address: 10.255.2.3
- IPv4 Route Map In: RM-PERMIT-CAMPUS
- IPv4 Route Map Out: RM-EXT-OUT
- Enable Bidirectional Forwarding Detection (BFD) Fall Over: < checked >

Se	ttings Name Summary	
Specify BGP Neighbo	or settings.	
leighbor AS	05504	
Number *		
	ASPLAIN notation between 1 and 4294967295 or ASDOT notation between 1 and 65535.65535, examples: 4294967295 and 65535.	I
P Address *	10.255.2.3	
	A valid IPv4 or IPv6 Address, example: 192.168.1.10 or 2001:db8:85a3::1234.	
Authentication		
Password	Authorition Paceward up to 29 abarostera lang	
	Authentication Fassword up to 52 characters long.	
Jpdate Source		
Address	Any valid IPv4 Address, example: 192.168.1.10. The packets Source IP Address, this can be entered manually or the Loopback Address	ess can be
	uuuu	
Keep Alive Timer *	60	
	Number of seconds between 1 and 65535. A value of 0 will use the default Keep Alive Timer value.	
Hold Down Timer *	180	
	Number of seconds between 3 and 65535. A value of 0 will use the default Hold Down Timer value	
BGP Multi-hop		
	Number of hops, between 0 and 255, to an eBGP peer. A value of 0 indicates not in use.	
Weight	0	
	A number between 0 and 65535. example: 0	
Allow AS in Path	0	
	Number of occurrences of AS number, between 0 and 10, if allow routes with own AS present in the AS-Path. No value or 0 indicates	not in use.
Address Families *	× IPv4	× -
EVPN Route Map	Select 💌	ADD
n		
EVPN Route Map	Select 👻	ADD
Dut		
Du4 Douto Mon In		100
Pv4 Route Map In	RM-PERMIT-CAMPUS X *	ADD
Pv4 Route Map	RM-EXT-OUT × -	ADD
Dut		
EVPN Send Community	Select	
,		
Pv4 Send	Select	~
Community		
	Accept Incoming Soft Reconfiguration	
	Default Route Originate	
	Enable Admin State	
	Enable Fall Over	
	Remove Private AS	
	Enable Bidirectional Forwarding Detection (BFD) Fall Over	

BGP Switc	h Neighbor Configuration	? X
Settin Optional External BC	ngs Name Summary GP Neighbor Name and Description.	
Name	PROD-DC-VRF LF1-1 to FW	
Description	BGP peering from LF1-1 PROD VRF to FW cluster	
(* = Required)	CANCEL BACK	NEXT

Step 7 On the Name page, enter a Name and Description, then click NEXT.

Step 8 On the **Summary** page, review the BGP neighbor settings and click **APPLY**.

BGP Switch Neighbor Configuration		? ×
Settings	Name Summary	
Name	PROD-DC-VRF LF1-1 to FW	
Description	BGP peering from LF1-1 PROD VRF to FW cluster	_
Neighbor AS Number	65501	_
IP Address	10.255.2.3	_
Update Source Address		_
Keep Alive Timer	60	_
Hold Down Timer	180	_
eBGP Multi-hop		_
Weight	0	_
Allow AS in Path	0	_
Address Families	IPv4	_
IPv4 Route Map In	RM-PERMIT-CAMPUS	_
IPv4 Route Map Out	RM-EXT-OUT	_
IPv4 Send Community		_
Accept Incoming Soft Reconfiguration	No	_
Default Route Originate	No	_
Enable Admin State	Yes	_
Enable Fall Over	No	_
Remove Private AS	No	_
BFD Fall Over	Yes	_
Route Reflector Client	No	
	CANCEL BACK A	PPLY

Step 9 Repeat steps 5 to 8 to add an iBGP peering between the border leaf switches in the production VRF with the following non-default settings:

Name	Description	Neighbor ASN	IP Addresses	IPv4 Route Map Out
PROD-DC-VRF LF1-1 to LF1-2	PROD VRF peering between border leaf switches	65001	10.255.2.1	RM-PERMIT- CAMPUS

Step 10 In the top left current context path, click PROD-DC-VRF.

	Fabric	RSVDC-	-FB1			
				$\odot \ \bigcirc \ \bigtriangledown $	С	ACTIONS ¥
Name 📙	Enabled	ψ <u>ε</u>	ASN (ASPLAIN)	Router ID	11	Networks
Enter Name	Select Enabled	-	Enter Regex for ASN (ASPLAI	Enter Regex for Router ID		Enter Regex for
RSVDC-FB1-LF1-1	Yes		65001	10.250.0.11		

Step 12 On the SWITCHES tab, click • • • next to RSVDC-FB1-LF1-2 and select Neighbors.

Configura									
	ation / Rou	uting / BGP / PROD-DC-V	RF						
			Fabric	RSVDC	C-FB1				
								\circ Y	ACTIONS V
VRF Na	me			IΕ	Switches			Ļ	Enabled
Enter	VRF Nam	e			Enter Switches				Select Ena 🔻
PROD-D	C-VRF				RSVDC-FB1-LF1-1,	, RSVDC	C-FB1-LF1-2, RSVDC-FB1-L	.F2-1,	Yes
					RSVDC-FB1-LF2-2,	, RSVDC	C-FB1-LF3-1, RSVDC-FB1-L	F3-2	
SWIT	CHES	NEIGHBORS SUMMA	RY						
								$\bigcirc \bigcirc$	ACTIONS 🗸
		Nama	12						
		Name	1E E	Enabled		1E	ASN (ASPLAIN)	ĻΞ	Router ID
		Enter Name		Enabled Select E	Enabled	↓ <u>1</u>	ASN (ASPLAIN)	J≟ SPLAI	Router ID Enter Regex for Router I
	0	Enter Name RSVDC-FB1-LF1-1		Enabled Select E Yes	nabled	↓ <u>1</u>	ASN (ASPLAIN) Enter Regex for ASN (A 65001	↓ <u>E</u> SPLAI	Router ID Enter Regex for Router I 10.250.0.11
•••	0	RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2	, , , , , , , , , , , , , , , , , , ,	Enabled Select E Yes Yes	Enabled	↓ <u>1</u>	ASN (ASPLAIN) Enter Regex for ASN (A 65001 65001	JE SPLAI	Router ID Enter Regex for Router I 10.250.0.11 10.250.0.13
•••• ••••		RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2 -FB1-LF2-1		Enabled Select E Yes Yes Yes	Enabled	↓ <u>1</u>	ASN (ASPLAIN) Enter Regex for ASN (A 65001 65001 65001	J <u>E</u> SPLAI	Router ID Enter Regex for Router I 10.250.0.11 10.250.0.13 10.250.0.7
Nei) O Ighbors	RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2 -FB1-LF2-1 -FB1-LF2-2		Enabled Select E Yes Yes Yes Yes	Enabled	↓ <u>1</u> ▼	ASN (ASPLAIN) Enter Regex for ASN (A 65001 65001 65001 65001	J <u>E</u> SPLAI	Router ID Enter Regex for Router I 10.250.0.11 10.250.0.13 10.250.0.7 10.250.0.12
···· Nei	O O Ighbors	RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2 -FB1-LF2-1 -FB1-LF2-2 RSVDC-FB1-LF3-1		Enabled Select E Yes Yes Yes Yes Yes	Enabled	↓ <u>1</u> ▼	ASN (ASPLAIN) Enter Regex for ASN (A 65001 65001 65001 65001 65001	J <u>E</u> SPLAI	Router ID Enter Regex for Router I 10.250.0.11 10.250.0.13 10.250.0.7 10.250.0.12 10.250.0.8

Step 13 Repeat steps 6 to 9 to create additional BGP peerings on RSVDC-FB1-LF1-2 with the following settings:

Name	Description	Neighbo ASN	r IP Addresse	IPv4 Route sMap In	IPv4 Route Map Out	BFD
PROD-DC- VRF LF1-2 to FW	BGP peering from LF1-2 PROD VRF to FW cluster	65501	10.255.2.	RM- PERMIT- CAMPUS	RM-EXT- OUT	< checked >
PROD-DC- VRF LF1-2 to LF1-1	PROD VRF peering between border leaf switches	65001	10.255.2.	2	RM- PERMIT- CAMPUS	< unchecked >

Step 13 Repeat this procedure for each overlay VRF network that requires external connectivity. Reachability between overlay VRFs is governed by policy at the upstream firewall. Strict overlay route table separation can be maintained by connecting to discrete VRFs or virtual firewall contexts on the upstream firewall.

		Noighbo	rID	IPv4 Pouto	IPv4 Pouto	
Name	Description	ASN	Addresse	esMap In	Map Out	BFD
DEV-DC-VRF LF1-1 to FW	BGP peering from LF1-1 DEV VRF to FW cluster	65501	10.255.2.	RM- PERMIT- CAMPUS	RM-EXT- OUT	< checked >
DEV-DC-VRF LF1-1 to LF1-2	DEV VRF peering between border leaf switches	65001	10.255.2.	9	RM- PERMIT- CAMPUS	<unchecked< td=""></unchecked<>
DEV-DC-VRF LF1-2 to FW	BGP peering from LF1-2 DEV VRF to FW cluster	65501	10.255.2.	RM- PERMIT- CAMPUS	RM-EXT- OUT	< checked >
DEV-DC-VRF LF1-2 to LF1-1	DEV VRF peering between border leaf switches	65001	10.255.2.	10	RM- PERMIT- CAMPUS	< unchecked >

Verify Border Leaf Routing

Step 1 In the top-left current context path, click **BGP**.

Configuration / Routing / <u>BGP</u> / PRC	D-DC-VRF / RSVDC-	FB1-LF1-2					
	Fabric	RSVDC-FB1					
						🔆 С астіс	ons 🗸
Name 🗦	Enabled	ĮΞ	ASN (ASPLAIN)	1 <u>E</u>	Router ID	ĮΞ	Networks
Enter Name	Select Enabled	-	Enter Regex for	ASN (ASPLAI	Enter Regex for	Router ID	Enter F
RSVDC-FB1-LF1-2	Yes		65001		10.250.0.13		
NEIGHBORS							
					\bigcirc	🖓 💮 АСТІС	ons 🗸
I Name	15	Description	Ļ	Туре	1 <u>=</u>	Neighbor AS Nu	Imber
Enter Name		Enter Descrip	otion	Select Type		Enter Regex f	for Neighbo
> O PROD-DC-VRF	LF1-2 to FW	BGP peering fro	om LF1-2 PROD	External		65501	
		VRF to FW clust	ter				

NOTE:

To display information and the current state of an individual BGP peering, click the expansion icon (>) at the beginning of the row for each BGP peer definition. After a BGP peering is defined, the Fabric Composer web page may require a refresh to display the expansion icon.

Step 2 Click ••• next to PROD-DC-VRF and select Neighbors Summary.

Configur	ration / R	outing / BGP				
		Fal	bric RSVDC-FB1			
					© \ \ \ @	C ACTIONS -
		VRF Name	15	Switches	μ <u>ε</u>	
		Enter VRF Name		Enter Switches		Select Ena 🔻
	\bigcirc	default		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2,	RSVDC-FB1-	Yes
				LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-	LF3-1, RSVDC-	
				FB1-LF3-2, RSVDC-FB1-SP1, RSVDC-F	B1-SP2	
	\bigcirc	DEV-DC-VRF				No
	\bigcirc	PROD-DC-VRF		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2,	RSVDC-FB1-	Yes
Qui	tabaa			LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-	LF3-1, RSVDC-	
SWI	liches			FB1-LF3-2		
Nei	ghbors S	ummary				

Step 3 In the **NEIGHBORS SUMMARY** window, verify that each peering displays **Established** in the **State** column.

Configuration / Routing / BGP / PROD-DC-VRF							
Fabric	RSVE	DC-FB1					
					\triangleright	⊘ 🛛 🕆 C	ACTIONS 🗸
VRF Name	45	Switches				ji Z	Enabled
Enter VRF Name		Enter Swite	ches			s	elect Ena 🔻
PROD-DC-VRF		RSVDC-FB1-	LF1-1, RSVDC-FB1-I	LF1-2, RSVDC-FB1-LF	2-1, RSVDC-FB1-	-LF2-2, Ye	3
		RSVDC-FB1-	LF3-1, RSVDC-FB1-I	LF3-2			
SWITCHES NEIGHBORS SUMMARY							• •
Switch	ψ	Local AS	Router ID	Address Family 1	Neighbor	Remote AS	State 1
Enter Regex for Switch Enter Name		Enter R	Enter Regex	Select A 🔻	Enter Re	Enter Reg	Enter Regex
RSVDC-FB1-LF1-1 PROD-DC-VRF LF1-1 to FW			10.250.0.11	IPv4 Unicast	10.255.2.3	65501	Established
RSVDC-FB1-LF1-1 PROD-DC-VRF LF1-1 to LF1-2			10.250.0.11	IPv4 Unicast	10.255.2.1	65001	Established
RSVDC-FB1-LF1-2 PROD-DC-VRF LF1-2 to FW			10.250.0.13	IPv4 Unicast	10.255.2.3	65501	Established
RSVDC-FB1-LF1-2 PROD-DC-VRF LF1-2 to LF1-1			10.250.0.13	IPv4 Unicast	10.255.2.2	65001	Established

Step 4 Repeat steps 1 to 3 for each overlay VRF.

Step 5 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

Step 6 On the CLI Command Processor page, enter the following values, then click RUN.

• Switches: < Select all leaf switches >

• **Commands:** show ip route bgp vrf PROD-DC-VRF

>_ CLI Command Pro	cessor							×
Select Fabrics or Switches, and	select or add Saved Con	nmands that can be customized. Pres	s Run for results.					
Fabrics	Not applicable whe	n a Switch is selected.						~
Switches	× RSVDC-FB1-LF1	-1 × RSVDC-FB1-LF1-2 × RSVDC	-FB1-LF2-1 × RSVDC-F	B1-LF2-2 × F	RSVDC-FB1-LF3-1 × F	RSVDC-FB1-LF3-	2	• × •
Saved Commands	Select from Saved	Commands or Add new commands.				-	ADD	REMOVE
Commands	show ip route bgp	vrf PROD-DC-VRF						
	A comma separated list of	commands to be run.						
Download Options	Download Results	Download JSON Data						
Results	Switch : RSVDC-	-FB1-LF1-1 Command : show ip	o route bgp vrf PROD	-DC-VRF				
	Displaying ipv4 Origin Codes: C R Type Codes: E Iv	routes selected for forward – connected, S – static, L – RIP, B – BGP, O – OSPF, D – External BGP, I – Interna A – OSPF internal area, E1 –	ling - local) - DHCP &l BGP, V - VPN, EV - OSPF external type	- EVPN				
	E: VRF: PROD-DC-VR	2 – OSPF external type 2 F						
	Prefix	Nexthop	1	nterface	VRF(egress)	Origin∕ Type	Distance/ Metric	Age
	0.0.0.0/0 10.0.0.0/12	10.255.2.3 10.255.2.3	\	lan2021 lan2021	-	B/E B/E	[20/0] [20/0]	00h:33m:14s 00h:33m:14s
(* = Required)								CANCEL

Step 7 Verify that there is a default route and campus summary route learned on all leaf switches in the production VRF. The border leaf switch routes use the upstream firewall IP as a next hop. The remaining leaf switches use a next hop of the border leaf Anycast VTEP, learned via BGP EVPN type-5 advertisements.

NOTE:

The prefixes advertised into an overlay fabric vary based on the environment. A default route is often the only learned prefix required. The campus summary route is used in the Validation Solution Guide's multifabric configuration.

Step 8 Repeat steps 6 to 7 for each overlay VRF.

Configure Overlay Test Loopbacks

A unique loopback IP per switch in each overlay VRF is required to verify connectivity to directly attached hosts and reachability through the overlay.

Sourcing a ping from a switch to one of its directly attached hosts is a common method to verify reachability at the point of attachment. When a VSX leaf pair provides redundant links to attached hosts, the return data path from the host may not be the same link as the originating traffic. By default, a switch will use the SVI interface IP for the VLAN connecting the downstream host. The same VLAN SVI IP address is configured on both VSX member switches to conserve IP address space. If the response to a ping originated by one member of the VSX pair is received by the other member, the response will be dropped, because the switch receiving the response has no state for the ping conversation.

Sourcing a ping from a unique IP address that is present only on one of the VSX switch pair members resolves the issue, when combined with a static route to share reachability of the unique IP between the VSX pair members. On any leaf switch, one loopback IP address in a VRF can be used to test reachability to all locally attached hosts in all subnets associated locally with that VRF. If a response is received by the non-originating member of the VSX pair, the destination IP address is not local to the VSX member, so the route table is consulted and the static route is used to forward the ping response to the originating member of the pair. A unique IP loopback per VRF per switch is required for full testing capability.

A similar problem exists when sourcing a ping from a switch to verify overlay reachability. Up to this point, the only IP interfaces configured in the overlay are VLAN SVIs. For each VLAN, the same SVI IP address is assigned to all leaf switches. Sourcing a ping with a VLAN SVI to an IP host connected to another leaf in the fabric will result in the ping response being dropped at the remote host's point of attachment, which also owns the destination IP address in the ping response. In the case where a ping response can be received by the originating VTEP, it is not guaranteed that the response will be received by the originating switch. A VSX pair of switches represent a single logical VTEP. If the response to a ping originated by one member of the VSX pair is received by the other member, the response will be dropped for the same reason noted above.

Sourcing a ping from an IP address that is unique to an individual switch resolves the reachability problem in the overlay as well.

The following procedure configures a transit VLAN in each overlay VRF between leaf switch VSX pairs, unique loopback on each switch in both the PROD and DEV VRFs, and a static route using the transit VLAN for loopback reachability between the pair. The loopback address can be used to test overlay reachability to directly attached hosts and remote IP destinations.

The following procedure configures the required elements for one VSX leaf pair.

Configure Overlay Transit VLAN

Each redundant pair of ToR switches requires a transit VLAN in the overlay VRF to enable routed reachability to its VSX partner's IP loopback address in the same VRF.

HPE aruba Fabric Composer	Dashboard Configuration 🗸 Main	tenance Visualization V Whe
🙊 VRF	Ports >	
A PCD	Conf 😯 Routing >	🛞 VRF
6 BUF	System >	🖧 BGP
🖾 OSPF	品 Network >	🔀 OSPF
EVPN	VR Administration >	
EVPN VXLAN Multi-Fabric	B Policy >	Route Policy
10 Route Policy	PR	

Step 1 On the Configuration menu, select Routing > VRF.

Configura	ation / Ro	outing / VRF					
			Fabric	RSVDC-FB1			
							ACTIONS V
		Name	1E	Туре	1E	Switches	L3 VNI
		Enter Name	••••]	Select Type	•	Enter Switches	Enter Regex
	\bigcirc	default		Default			
	0	DEV-DC-VRF		User		RSVDC-FB1-VSX_RSVDC-FB1- LF1-1_RSVDC-FB1-LF1-2, RSVDC-FB1-VSX_RSVDC-FB1- LF2-1_RSVDC-FB1-LF2-2, RSVDC-FB1-VSX_RSVDC-FB1- LF3-2_RSVDC-FB1-LF3-1	100002
	\bigcirc	mgmt		Management			
IP In IP Si Netv	Onterfaces tatic Rou vorks 7 Tables	PROD-DC-VRF		User		RSVDC-FB1-VSX_RSVDC-FB1- LF1-1_RSVDC-FB1-LF1-2, RSVDC-FB1-VSX_RSVDC-FB1- LF2-1_RSVDC-FB1-LF2-2, RSVDC-FB1-VSX_RSVDC-FB1- LF3-2_RSVDC-FB1-LF3-1	100001
IP R	oute Tab	les					

Step 2 Click ••• next to PROD-DC-VRF and select IP Interfaces.

Step 3 On the right ACTIONS menu, select Add.

Configuration / Pou	iting / VRE / PPC						
Configuration / Not		Fabric	RSVDC-FB1				
					(C ACTIONS V
Name	ξĘ	Туре	ĮΞ	Switches	μĒ	L3 VNI	Route Target Ext-C
Enter Name		Select Type	•	Enter Switches		Enter Rege	Enter Regex for F
PROD-DC-VRF		User		RSVDC-FB1-VSX_RSVDC-F	B1-	100001	65001:100001
				LF1-1_RSVDC-FB1-LF1-2,			
				RSVDC-FB1-VSX_RSVDC-F	B1-		
				LF2-1_RSVDC-FB1-LF2-2,			
				RSVDC-FB1-VSX_RSVDC-F	B1-		
				LF3-2_RSVDC-FB1-LF3-1			
IP INTERFACE	S IP STATIO	C ROUTES	IETWORKS	ARP TABLES IP ROU	ITE TABL	ES SWITC	CHES
						$\bigcirc \bigcirc $	ACTIONS ¥
	Туре	↓ <u>⊨</u> Enabl	ed 📖	Switch	Ļ	VLAN	Add
	Select Type	- Sele	ect Ena 🔻	Enter Switch		Enter Re	Edit
0	SVI	Yes		RSVDC-FB1-LF2-1		102	Delete
0	SVI	Yes		RSVDC-FB1-LF2-2		102	

Step 4 On the Interface Type page, assign the following non-default values and click NEXT.

- VLAN: 3001
- Switches: < Select a VSX leaf switch pair >
- IPv4 Subnetwork Address: < Assign a /31 block of addresses >
- IPv4 Address: < Assign the range of 2 IP address that comprise the /31 subnet >

IP Interfac	e	?
Interfa	Image: Name Image: Summary	
Select the IP Interfa	ce Type and set the appropriate attributes.	
Enable this IP Int	rerface	
Туре	SVI ×	•
VLAN *	3001	
	A VLAN between 1 and 4094, example: 1.	
Switches *	× RSVDC-FB1-VSX_RSVDC-FB1-LF1-1_RSVDC-FB1-LF1-2 × • SELECT	
IPv4 Subnetwork	10.255.4.0/31	
Address	A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24	
IPv4 Addresses *	10.255.4.0-10.255.4.1	
	Enter a range of IPv4 Addresses to be assigned to the selected switches, example: 192.168.1.100-192.168.1.200. The range mu include at least 2 addresses or match the Active Gateway IP Address.	st
Active Gateway		
Active Gateway (* = Required)	Scroll for more options CANCEL BACK NEX	T

Step 5 On the Name page, assign a Name and Description, then click NEXT.

IP Interfa	ace	(?) ×
Inte	vrface Type Name Summary	
Enter an optional	Name and Description.	
Name	LF1-PROD-Transit-VLAN	
	A string, up to 42 characters. example: lpInterface1	
Description	Overlay transit VLAN for PROD VRF on LF1 VSX pair	
	Example: My New IP Interface	
([*] = Required)	CANCEL BACK N	EXT

Step 6 On the **Summary** page, review the transit VLAN settings and click **APPLY**.

IP Interface			?
Interface Type	Name	Summary	
Name	LF1-PROD-Transit-VLAN		
Description	Overlay transit VLAN for PROD VRF or	n LF1 VSX pair	
Туре	SVI		
Enabled	Yes		
VLAN	3001		
Switches	RSVDC-FB1-VSX_RSVDC-FB1-LF1-1_	RSVDC-FB1-LF1-2	
IPv4 Addresses	10.255.4.0-10.255.4.1		
VSX Shutdown on Split	No		
VSX Active Forwarding	No		
Local Proxy ARP Enabled	No		
		CANCEL BACK	

Assign Unique Overlay Loopbacks

Step 1 On the right ACTIONS menu of the Configuration > Routing > VRF > PROD-DC-VRF page, select Add.

Configuration / Routing / VRF / PR	OD-DC-VRF				
	Fabric RS	VDC-FB1			
					J ACTIONS V
Name 📘	Туре	μ <u>ε</u>	Switches	L3 VNI	Route Target Ext-C
Enter Name	Select Type	-	Enter Switches	Enter Regex	Enter Regex for F
PROD-DC-VRF	User		RSVDC-FB1-VSX_RSVDC-FB1-	100001	65001:100001
			LF1-1_RSVDC-FB1-LF1-2,		
			RSVDC-FB1-VSX_RSVDC-FB1-		
			LF2-1_RSVDC-FB1-LF2-2,		
			RSVDC-FB1-VSX_RSVDC-FB1-		
			LF3-2_RSVDC-FB1-LF3-1		
IP INTERFACES IP STAT	TIC ROUTES NETV	VORKS	ARP TABLES IP ROUTE TA	BLES SWITCH	ES
					ACTIONS 🗸
Туре	LE Enabled	Ļ	Switch	LE VLAN	Add
Select Type	🔻 Select E	na 🔻	Enter Switch	Enter Re	Edit
O svi	Yes		RSVDC-FB1-LF2-1	102	Delete
O svi	Yes		RSVDC-FB1-LF2-2	102	

Step 2 On the **Interface Type** page, enter the following non-default values:

- Type: Loopback
- Loopback Name: < An unused loopback interface value >
- Switch: < Select an individual switch in the VSX pair where a transit VLAN was created >

IP Interface)	? ×
Interface Typ	pe IPv4 Addresses Name Summary	
Select the IP Interface	e Type and set the appropriate attributes.	
Enable this IP Inte	rface	
Туре	Loopback	× -
EVPN VTEP Loop!	oack Interface	
Loopback Name	loopback11	
	Name for Loopback interface. Must be in the format of "loopback#" where the numeric value must be between 0-255.	
Switch *	RSVDC-FB1-LF1-1	× •
(* = Required)	Scroll for more options CANCEL BACK	NEXT

Step 3 On the IPv4 Addresses page, enter a /32 host address and click NEXT.

IP Interface	9			? ×
Interface Ty	De IPv4 Addresses	? Name	Summary	
Enter a required Prin	nary Network Address.			
Primary IPv4	10.250.4.1/32			••••]
Network Address *	IPv4 Network address in CIDR format. Example: 192	2.168.1.10/32		
(* = Required)			CANCEL BACK	NEXT

Step 4 On the Name page, enter a Name and Description, then click NEXT.

IP Interfa	се	? ×
Interface	Type IPv4 Addresses Name Summary	
Enter an optional I	Name and Description.	
Name	LF1-1 PROD LOOPBACK	
	A unique name up to 42 characters. example: lpInterface1	
Description	Unique overlay loopback IP address in the PROD VRF for LF1-1	
	Example: My New IP Interface	
(* = Required)	CANCEL BACK	NEXT

Step 5 On the Summary page, review the loopback interface settings and click APPLY

P Interface				? ×
		Name		
		Name	Summary	
Name	LF1-1 PROD LOG	DPBACK		
	Unique overlay lo	opback IP address in the F	PROD VRF for LF1-1	
Туре	Loopback			
	Yes			
EVPN VIEP Loopback Interface	No			
	loopback11			
Switch	RSVDC-FB1-LF1	-1		
Primary IPv4 Network Address	10.250.4.1/32			
		Г	CANCEL BACK AP	PLY
		L		

Step 6 Repeat steps 1 to 5 to assign a loopback interface to the VSX partner switch with the following non-default values:

					Primary IPv4
			Loopback		Network
Name	Description	Туре	Name	Switch	Address
LF1-2	Unique overlay loopback IP	Loopb	Loopback	RSVDC-	10.250.4.0/32
PROD	address in the PROD VRF for LF1-2			FB1-LF1-	
LOOPBACK				2	

Configure Static Route for VSX Routed Loopback Reachability

Step 1 On the **Configuration > Routing > VRF > PROD-DC-VRF** page, click **IP STATIC ROUTES**. On the right **ACTIONS** menu, select **Add**.

Configuration / Rout	ing / VRF / PRO	D-DC-VRF					
		Fabric	RSVDC-FB1				
					0		C ACTIONS V
Name	4E	Туре	1ª	Switches	ĻÈ	L3 VNI	Route Target Ext-C
Enter Name		Select Type	~	Enter Switches		Enter Rege	x Enter Regex for
PROD-DC-VRF		User		RSVDC-FB1-VSX_RSV	DC-FB1-	100001	65001:100001
				LF1-1_RSVDC-FB1-LF	1-2,		
				RSVDC-FB1-VSX_RSV	DC-FB1-		
				LF2-1_RSVDC-FB1-LF	2-2,		
				RSVDC-FB1-VSX_RSV	DC-FB1-		
				LF3-2_RSVDC-FB1-LF	3-1		
IP INTERFACES	IP STATIC	ROUTES	NETWORKS	ARP TABLES IP	ROUTE TAB	LES SWIT	CHES
	Name	Į	Destination	Prefix 1	Next Hop Ad	dress	Add
	Enter Name		Enter Reg	gex for Destination P	Enter Reg	jex for Next Hc	Edit
					*	There is no d	Delete
							Delete All

Step 2 On the **Route** page, enter the following values and click **NEXT**.

- Destination Prefix: < Host IP prefix of VSX peer's overlay loopback interface >
- Next Hop Address: < IP address of VSX peer's transit VLAN interface >
- Switch: < Individual VSX member target for static route >

🛛 IP Static F	loute	? ×
R	Name Summary	
Enter a required De	stination Prefix, Next Hop Address, Switch(es), an optional Distance and Tag	
Destination Prefix	10.250.4.0/32	
*	A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24	
Next Hop Address *	10.255.4.0	•••
	Any valid IPv4 Address, example: 192.168.1.10	
Distance	A number between 1 and 255 example 1	
Tog		
lay	A number between 1 and 4294967295, example 1	
Switch *	× RSVDC-FB1-LF1-1	× -
(* = Required)	CANCEL BACK	NEXT

Step 3 On the Name page, enter a Name and Description, then click NEXT.

IP Static	Route	? ×
F	Route Name Summary	
Enter a required N	ame and an optional Description.	
Name *	to-LF1-2-PROD-loopback	
	Any non empty string, example: lpStaticRoute1	
Description	Static route to L1-2 PROD VRF loopback IP	
	Example: My New IP Static Route	
(* = Required)	CANCEL BACK	NEXT

Step 4 On the Summary page, review the static route settings and click APPLY.

P IP Static Route		() ×
Route	Name	Summary
Name	to-LF1-2-PROD-loopback	
Description	Static route to L1-2 PROD VRF loopback IP	
Destination	10.250.4.0/32	
Next Hop Address	10.255.4.0	
Distance		
Тад		
Switches	RSVDC-FB1-LF1-1	
		CANCEL BACK APPLY

Step 5 Repeat steps 1 to 4 to create a static route to the VSX peer's loopback interface using the following non-default values:

		Next Hop	
Name	Description	Destination Address	Switches
to-LF1-1-PROD- loopback	Static route to L1-1 PROD VRF loopback IP	10.250.4.1/3 10.255.4.1	RSVDC-FB1- LF1-2

Repeat the **Configure Overlay Test Loopbacks** procedure for each VRF in the overlay on each VSX leaf pair in the network. For standalone leaf switches, perform only the **Assign Loopbacks to Individual Switches** steps in this section for each VRF in the overlay.

Configure Loopback Summary Route

A summary static route for the collective set of loopback interfaces is configured on the border leaf to advertise loopback reachability to external networks. This static route points to null. A summary route is created for each VRF in the overlay.

Step 1 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Configuration Editor**.

 🕸 🎦 V	:=	Radmin 🖌	? *
>_ Show Commands			
Configuration Editor			
	1		

Step 2 On the Configuration Editor page, select the two border leaf switches in the Switch field.

Configuratio	on / System / C	Configuration Editor				
Fabric	RSVDC-FB1		Switch	× RSVDC-FB1-LF1-1 × RSVDC-FB1-LF1-2	× •	SELECT ALL
RSVDC-	FB1-LF1-1	RSVDC-FB1-LF1-2				

Step 3 Enter the summary static route configuration for the loopback addresses in the same section where the previously created static routes appear on both switch tabs, and click **VALIDATE ALL**.

ip	route	10.250.4.0/24	nullroute	vrf	PROD-DC-VRF
ip	route	10.250.5.0/24	nullroute	vrf	DEV-DC-VRF

onfiguration / System / Configuration Editor			
Fabric RSVDC-FB1	Switch × RSVDC-FB1-LF	F1-1 SELECT A	ALL
	× RSVDC-FB1-LF	.F1-2	
RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-	-2		
SX			
system-mac 02:00:00:00:10:02			
inter-switch-link lag 256			
role secondary			
keepalive peer 10.250.0.5 sou	rce 10.250.0.4		
linkup-delay-timer 600			
vsx—sync vsx—global			
p route 10.250.5.0/32 10.255.5.0	vrf DEV-DC-VRF		
p route 10.250.4.0/32 10.255.4.0	VTT PROD-DC-VRF		
p route 10.250.4.0/24 nullroute	VFT PROD-DC-VRF		
p dos domain-name example local	vrt momt		•
p dns server-address 10.2.120.98	vrf mamt		
p dns server-address 10.2.120.99	vrf mamt		
•	5		
		NEXT ERI	ROR
Create a Checkpoint before Apply		VALIDATE ALL APPLY	ALL

Success Successfully validated configuration

NOTE:

Fabric Composer 7.0.X and previous versions require creating static null routes using Fabric Composer's **Configuration Editor** or the switch CLI.

If the configuration is valid, a **Success** message is presented.

Step 4 Click APPLY ALL.

NOTE:

Create Checkpoint before Apply is selected by default. Fabric Composer creates a checkpoint on the switch to restore the switch configuration back to its state prior to the change.

If the checkpoint was successfully created, the **Success** message indicates the time of its creation.



Redistribute Static Routes on the Border Leaf

The loopback summary route created in the previous procedure is redistributed into BGP for advertisement to campus. Redistribution is applied to each VRF.

Step 1 On the Configuration menu, select Routing > VRF.

HPE Crubo Fabric Composer	Dashboard Configuration - Maintenance - Visualization - 🖓 Wh
Fabrics & Switches	Ports >
	Routing > 🛞 VRF
AFC Remote Sites	System > 🔥 BGP
Configuration Editor	R Network > ◎ OSPF
R Monitor Agents	R Administration > 😰 EVPN
L0	! 🗗 Integrations > 😰 EVPN VXLAN Multi-Fabric
Diagram SmartNICs	!Ve Se Policy > D Route Policy
System Settings	hostname RSVDC-FB1-LF1-1 user admin group administrators password ciphertext

Step 2 On the **Configuration > Routing > BGP** page, right-click • • • next to **PROD-DC-VRF** and select **Switches**.

Configu	ration / Ro	outing / BGP			
		Fabric	RSVDC-FB1		
					C ACTIONS V
		VRF Name	1E	Switches	Enabled ↓
		Enter VRF Name		Enter Switches	Select Ena 💌
	\bigcirc	default		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2, RSVDC-FB1-	Yes
				LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-LF3-1, RSVDC	-
				FB1-LF3-2, RSVDC-FB1-SP1, RSVDC-FB1-SP2	
	\bigcirc	DEV-DC-VRF		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2, RSVDC-FB1-	Yes
				LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-LF3-1, RSVDC	-
				FB1-LF3-2	
	\bigcirc	PROD-DC-VRF		RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-2, RSVDC-FB1-	Yes
0	itabaa			LF2-1, RSVDC-FB1-LF2-2, RSVDC-FB1-LF3-1, RSVDC	-
5w	liches			FB1-LF3-2	
Nei	ighbors S	ummary			

Step 3 Click the radio button for the **RSVDC-FB1-LF1-1** border leaf switch. On the right **ACTIONS** menu, select **Edit**.

	ation / Ro	uting / BGP / PROD-DC-VRI	F										
			Fabric	RSVD	C-FB1								
								(70	C A	CTIONS	~
VRF Na	me			1E	Switches					1E	🕑 Enabl	ed	臣
Enter	VRF Nam	ne			Enter Switches						Select	Ena	•
PROD-D	C-VRF				RSVDC-FB1-LF1-1,	RSVDO	C-FB1-LF1-2	2, RSVDC-F	31-LF2-1,		Yes		
					RSVDC-FB1-LF2-2,	RSVDO	C-FB1-LF3-	I, RSVDC-F	31-LF3-2				
										∇	A 454	CTIONS	~
		Name	1E I	Enabled		1£	ASN (ASF	PLAIN)			A 🕀	CTIONS	•
		Name Enter Name	<u>1</u>	Enabled Select	Enabled	↓:: ↓ ▼	ASN (ASF	PLAIN) egex for AS	N (ASPLA		Add Edit	CTIONS	~
	۲	Name Enter Name RSVDC-FB1-LF1-1		Enabled Select Yes	Enabled	↓ <u>1</u>	ASN (ASF Enter R 65001	PLAIN) egex for AS	N (ASPLA		Add Edit Delete	CTIONS	•
••••	•	Name Enter Name RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2		Enabled Select Yes Yes	Enabled	↓ ↓ ▼	ASN (ASF Enter R 65001	PLAIN) egex for AS	N (ASPLA		Add Add Edit Delete	OTIONS	~
····		Name Enter Name RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2 RSVDC-FB1-LF2-1		Enabled Select Yes Yes Yes	Enabled		ASN (ASF Enter R 65001 65001	PLAIN) egex for AS	N (ASPLA		Add Edit Delete Neighbu	OTIONS	~
····	 • •	Name Enter Name RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2 RSVDC-FB1-LF2-1 RSVDC-FB1-LF2-2		Enabled Select Yes Yes Yes Yes	Enabled	→ <u>1</u>	ASN (ASF Enter R 65001 65001 65001	PLAIN) egex for AS	N (ASPLA		Add Edit Delete	Ors 2	•
····		Name Enter Name RSVDC-FB1-LF1-1 RSVDC-FB1-LF1-2 RSVDC-FB1-LF2-1 RSVDC-FB1-LF2-2 RSVDC-FB1-LF3-1		Enabled Select Yes Yes Yes Yes Yes	Enabled	↓ <u>1</u>	ASN (ASF Enter R 65001 65001 65001 65001 65001	PLAIN) egex for AS	N (ASPLA		Image: Constraint of the second sec	ors 2	•

Step 4 Click the **REDISTRIBUTE ROUTES** tab, click the **Redistribute Static Routes** option, and click **APPLY**.

BGP Switch Configu	uration RSVDC-FB1-LF	1-1	@ ×
SETTINGS		⊘ NETWORKS	SUMMARY
Configure optional Redistributed	Route Maps and optional OSPF Proc	ess - Route Map Pairs.	
Redistribute Connected Route	28		
Redistribute Connected	Select		- ADD
Route Map			
Redistribute Static Routes			
Redistribute Static Route Map	Select		- ADD
Redistribute Loopback			
Redistribute Local Route Map	Select		▼ ADD
Redistribute OSPF			
Redistribute OSPF Route Map	Select		- ADD
Route Map	Select		- ADD
(* = Required) Scroll for m	ore options		CANCEL APPLY

If the BGP configuration is updated, a **Success** message is presented.



Step 5 Repeat steps 3 to 4 for the second border leaf to redistribute the static route on the second border leaf.

Step 6 Click **BGP** in the path at the top of the main configuration window and repeat steps 2 to 5 for each overlay VRF.



Verify Overlay Test Loopback

On each leaf switch, ping a directly connected host in the overlay using the loopback interface in the host's VRF as a ping source to verify the overlay test loopback is working.

ping 10.5.101.121 vrf PROD-DC-VRF source loopback11

RSVDC-FB1-LF2-1# ping 10.5.101.121 vrf PROD-DC-VRF source loopback11 PING 10.5.101.121 (10.5.101.121) from 10.250.4.3 : 100(128) bytes of data. 108 bytes from 10.5.101.121: icmp_seq=1 ttl=63 time=0.497 ms 108 bytes from 10.5.101.121: icmp_seq=2 ttl=63 time=0.450 ms 108 bytes from 10.5.101.121: icmp_seq=3 ttl=63 time=0.434 ms 108 bytes from 10.5.101.121: icmp_seq=4 ttl=63 time=0.406 ms 108 bytes from 10.5.101.121: icmp_seq=5 ttl=63 time=0.456 ms --- 10.5.101.121 ping statistics ---5 packets transmitted, 5 received, 0% packet loss, time 4115ms rtt min/avg/max/mdev = 0.406/0.448/0.497/0.029 ms RSVDC-FB1-LF2-1#

Configure Overlay IP Multicast

Protocol Independent Multicast–Sparse Mode (PIM-SM) is configured to build multicast route state between VTEPs within the data center and to external networks. PIM-SM is required for both sources and listeners in the data center. Internet Group Management Protocol (IGMP) manages known multicast listener state on data center leaf switches. IGMP snooping is configured to optimize Layer 2 forwarding of multicast traffic to only ports with interested listeners on leaf and server access switches.

In this guide, the PIM-SM rendezvous point (RP) is located outside the data center fabric in the campus network. The RP is learned with PIM-SM's Bootstrap Router (BSR) mechanism.

Configuration of multicast can be done at the command line of the switch or using Fabric Composer's **Configuration Editor**. Enter the configuration in code blocks in the procedures below to enable multicast in the EVPN-VXLAN overlay. The code blocks may include existing configuration to set context and existing descriptions to assist the reader.

Configure Overlay PIM Multicast

The configuration examples in each step should be applied to all leaf switches, except where noted that configuration is only applied to border leaf switches.

Step 1 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Configuration Editor**.

<u>*</u>	× ۔ ا	i ≡	A ^{admin} ×	? ~
>_ Show Comma	ands			
E Configuration	Editor			
)		

Step 2 In the **Switch** field, select the border leaf and all other leaf switches.

Configuration / System	/ Configuration Editor				
Fabric F	RSVDC-FB1	Switch	× RSVDC-FB1-LF1-1 × RSVDC-FB1-LF1-2 × PSVDC-FB1-LF1-2	× •	SELECT ALL
RSVDC-FB1-LF1-1	RSVDC-FB1-LF1-2	RSVDC-FB1-LF2-1	RSVDC-FB1-LF2-2	RSVDC-FB1-LF3-1	RSVDC-FB1-LF3-2
! !Version Aruba0S- !export-password: hostname RSVDC-FB user admin group AQBapeIqjq8+U9ADi XRvdT2aYANRe60UqL user afc_admin gr AQBapaW0wY1GRLmvJ BZr5aIKtiGjjAYnW7 clock timezone am bfd no ip icmp redire profile leaf	CX DL.10.13.1050 default 1-LF1-1 administrators passw .qC6Fm327NesimJe5KBRd .h3NEU6MIborgltAAH1zw roup administrators p VdcrjS0me4DGUVjIn7+ '2HVV720sXdTLD5741kDa erica/los_angeles ect	vord ciphertext DimnupyHc4EHYgAAAP/ vFoy1jSZm43Tq0f5fd1 Dassword ciphertex1 (0Io1MkyEI2uYgAAABp acnTJ/GPpmh3lHMD9jH	Aq∕gYOU4T53G3BVl7qt tjzwxI50lirAH10lfbl t oXhi8yxVW13XNw9Dx14 n0XS1nmKUsp2s+YrAoI	NqyZryv7s8qSdkewVI DW0 4ln4QX2Pm2Gqy0M+S! D9l	bVsQwVTvMvxCtPpP25ar 5z4wg2v+ANuX1k8FsLn6
	aint bafara Annly			VALIDAT	E ALL APPLY ALL
🔽 Стеане а спескр	отт регоге Арріу				

NOTE:

The spine switches do not contain multicast configuration for the overlay. Layer 2 server access switches are configured in a separate procedure in this guide. If there are few spine and server access switches, click **SELECT ALL** to select all switches in the fabric and deselect spine and server access switches.

Step 3 Enable PIM routing in each overlay VRF.

```
router pim vrf PROD-DC-VRF
enable
register-source loopback11
router pim vrf DEV-DC-VRF
enable
register-source loopback12
```

Configuration / Syste	m / Configuration Editor				
Fabric	RSVDC-FB1	✓ Switch	 × RSVDC-FB1-LF1-1 × RSVDC-FB1-LF1-2 × PSVDC-FB1-LF1-2 	× •	SELECT ALL
RSVDC-FB1-LF1	-1 RSVDC-FB1-LF1-2	RSVDC-FB1-LF2-1	RSVDC-FB1-LF2-2	RSVDC-FB1-LF3-1	RSVDC-FB1-LF3-2
nei nei red red exit-ad ! router pim vrf enable register-so router pim vrf enable register-so https-server vr	ghbor 10.255.2.3 route ghbor 10.255.2.3 activ istribute connected istribute local loopba istribute static dress-family PROD-DC-VRF urce loopback11 DEV-DC-VRF urce loopback12 f mgmt	e-map RM-EXT-OUT ou vate ack	t		
VALIDATE	APPLY				NEXT ERROR
✓ Create a Checl	kpoint before Apply			VALIDAT	E ALL APPLY ALL

NOTE:

In the configuration above, the **register-source** command instructs PIM to send register messages to the RP using the unique overlay loopback IP configured in the previous **Assign Unique Overlay Loopbacks** procedure. This is required to send register-stop messages originated by the RP to reach the individual leaf switch originating PIM register messages.When entering configuration in Fabric Composer's **Configuration Editor**, new configuration must be entered below any references to other configuration elements. In this example, VRF names and loopback interfaces are referenced in the PIM router configuration, which requires placing the new PIM router config after those elements are defined in the existing configuration.

Step 4 Enable PIM for each unique overlay loopback interface by adding **ip pim-sparse enable** in each configuration stanza. Do not modify existing configuration.

```
interface loopback 11
    ip pim-sparse enable
interface loopback 12
    ip pim-sparse enable
```

Configuration / Syste	em / Configuration Editor				
Fabric	RSVDC-FB1	Swit	ch × RSVDC-FB1-LF1-1		SELECT ALL
			× RSVDC-FB1-LF1-2		
RSVDC-FB1-LF1	-1 RSVDC-FB1-LF1-2	RSVDC-FB1-LF2-1	RSVDC-FB1-LF2-2	RSVDC-FB1-LF3-1	RSVDC-FB1-LF3-2
ip address	10.250.0.11/32				
interface loopb	ack 1				
description	BGP VXLAN overlay				
ip address	10.250.2.2/32				
description	ack II Unique overlav looph:	ock TD address i	the PPOD VPE for	L F1_1	
vrf attach	PROD-DC-VRF	ick if address i			
ip address	10.250.4.1/32				
ip pim-spar	se enable				
interface loopb	ack 12				•
description	Unique overlay loopba	ack IP address i	n the PROD DEV for I	LF1-1	
vrf attach	DEV-DC-VRF				
ip address	10.250.5.1/32				
ip pim-spar	se enable				
VALIDATE	APPLY				NEXT ERROR
✓ Create a Chec	kpoint before Apply			VALIDAT	TE ALL APPLY ALL

Step 5 Enable PIM on overlay VLAN SVIs. This includes adding PIM to all data center host VLANs and overlay transit VLANs. On the border leaf, this includes campus routed interfaces.

On the border leaf, add the following configuration lines:

```
interface vlan2021
   description Border leaf PROD-DC-VRF uplink to external FW cluster
   ip pim-sparse enable
   ip pim-sparse vsx-virtual-neighbor
interface vlan2022
   description Border leaf DEV-DC-VRF uplink to external FW cluster
   ip pim-sparse enable
   ip pim-sparse vsx-virtual-neighbor
interface vlan3001
   description Overlay transit VLAN for PROD VRF
    ip pim-sparse enable
   ip pim-sparse vsx-virtual-neighbor
interface vlan3002
   description Overlay transit VLAN for DEV VRF
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
```

On all other leaf switches, add the following configuration lines:

interface vlan101
description Production web app SVI/VLAN 101 in DC overlay
ip pim-sparse enable
ip pim-sparse vsx-virtual-neighbor
interface vlan102
description Production database SVI/VLAN 102 DC overlay
ip pim-sparse enable
ip pim-sparse vsx-virtual-neighbor
interface vlan201
description Development web app SVI/VLAN 201 in DC overlay
ip pim-sparse enable
ip pim-sparse vsx-virtual-neighbor
interface vianzoz
description Development database SVI/VLAN 202 in DC overlay
ip pim-sparse enable
interface vlan2001
description Overlay transit VIAN for PROD VRE
in nim-sparse enable
ip pim-sparse vsx-virtual-neighbor
interface vlan3002
description Overlay transit VIAN for DEV VRE
ip pim-sparse enable
ip pim-sparse vsx-virtual-neiahbor

Configuration / System / C	Configuration Editor				
Fabric	RSVDC-FB1	Switch	× RSVDC-FB1-LF1-	1	SELECT ALL
			× RSVDC-FB1-LF1-	2	
		L		4	
RSVDC-FB1-LF1-1	RSVDC-FB1-LF1-2 RS	SVDC-FB1-LF2-1 RS	SVDC-FB1-LF2-2	RSVDC-FB1-LF3-1	RSVDC-FB1-LF3-2
interface <u>vlan</u> 2021	L				
description Bor	der leaf PROD-DC-VRF	uplink to external	FW cluster		
vrf attach PROD)-DC-VRF				
ip mtu 9198					
vsx active-forw	varding				
ip address 10.2	255.2.2/29				
ip pim-sparse e	enable				
1p p1m-sparse v	/sx-virtual-neighbor				
description Bor	: dor loof DEV_DC_VPE u	nlink to external	EW cluster		
vrf attach DEV		ptink to externat	rw cluster		
in mtu 9198	-DC-VIA				
in address 10.7	255.2.10/29				
ip pim-sparse e	enable				
ip pim-sparse v	/sx-virtual-neighbor				
interface vlan 3001					
description Ove	arlay transit VLAN for	DDAD VDE op LE1 V	CY nair		
VALIDATE	PLY				NEXT ERROR
✓ Create a Checkpoin	it before Apply			VA	LIDATE ALL APPLY ALL

NOTE:

The border leaf switches in our example are dedicated to the border leaf function and do not include overlay host VLANs. When overlay VLANs are present on border leaf switches, configure PIM on those VLAN interfaces.

Step 6 Click VALIDATE ALL.

Step 7 Click APPLY ALL.

Verify Overlay PIM

Step 1 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

<u>*</u>	<u>>-</u> ~	:=	admin ∽	? *
>_ Show Comr	>_ Show Commands			
E Configuratio]			

Step 2 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select all leaf switches >
- **Commands:** show ip pim neighbor brief all-vrfs

elect Fabrics or Switches, a	ind select or add Saved C	ommands that can be	customized. Press Run fo	r results.					
abrics									
witches	× RSVDC-FE	31-LF1-1 × RSVDC-F	B1-LF1-2 × RSVDC-FB1-	F2-1 × RSVDC-FB1-LF2-2 ×	RSVDC-FB1-LF3-1	RSVDC-FB1-LF3-2		 × -	
aved Commands	Select from 5	Select from Saved Commands or Add new commands.							
ommands	show ip pim	show ip pim neichbor brief all-wrfs							
	A comma separate	ed list of commands to be ri	Jn.						
ownload Options	Download Res	ults Download JSC	DN Data						
	Switch - P	CVDC_EP1_LE1_1_1	ommand , chou in ni	m poighbor brief all um	f.c.				
Results	SWITCH : P	Switch : RSVDC-FB1-LF1-1 Command : show ip pim neighbor brief all-vrfs							
		VRF	: DEV-DC-VRF	Total n	umber of neighbor	s : 5			
	Interface	Neighbor (IPV4)	Uptime (HH:MM:SS)	Expires (HH:MM:SS)	DR Priority	Hold Time (HH:MM:SS)	Secondary Address (IPV4)		
	vni100002	10.250.2.0	00:00:18	00:03:13	1	00:03:30			
	vni100002 vlan2022	10.250.2.1 10.255.2.9	00:00:18 00:00:59	00:03:13 00:01:17	1 33749514	00:03:30 00:01:45	Nil		
	vlan2022	10.255.2.11	00:00:31	00:01:17	1	00:01:45	Nil		
	vlan3002	10.255.5.0	00:00:58	00:01:17	33749514	00:01:45	Nil		
		VRF : PROD-DC-VRF Total number of neighbors : 5							
		VRF : PROD-DC-VRF		00:03:25	00+03+25 1 00+03+30				
	vni100001	10.250.2.1	00:00:08	00:03:22	1	00:03:30			
	vlan2021	10.255.2.1	00:01:01	00:01:45	33749514	00:01:45	Nil		
	vlan2021	10.255.2.3	00:00:30	00:01:19	1	00:01:45	Nil		
	vlan3001	10.255.4.0	00:01:01	00:01:44	33749514	00:01:45	Nil		

Step 3 Review the output to verify that the following PIM neighbor adjacencies are established:

- Each VRF logical L3 VNI interface has a PIM neighbor relationship with each other VTEP in the EVPN-VXLAN fabric.
- Each VRF overlay transit VLAN has a PIM neighbor adjacency.
- Each host facing VLAN has a PIM neighbor adjacency on all VSX redundant leaf switches.
- Two PIM adjacencies are formed on the border leaf VLAN that supports external routed connectivity. One adjacency is with the peer VSX switch and the second is with the external firewall.

NOTE:

Overlay PIM adjacencies formed between logical L3 VNI interfaces take longer to establish than PIM adjacencies between switches. It may take a minute for the logical adjacencies to form. The RP in the fabric is learned from PIM BSR messages received by the border leaf switches from the external network.

Step 4 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select all leaf switches >
- **Commands:** show ip pim rp-set all-vrfs

>_ CLI Command Pr	ocessor								×
Select Fabrics or Switches, and select or add Saved Commands that can be customized. Press Run for results.									
Fabrics	Not applicable when a Switch is selected.								
Switches	× RSVDC-FB1-LF1-1 × RSVDC-FB1-LF1-2 × RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-LF3-1 × RSVDC-FB1-LF3-2 ×								
Saved Commands	Select from Saved Commands or Add new commands.								
Commands	show ip pim rp-set all-vrfs								
	A comma separated list of	commands to be run.							
Download Options	Download Results Download JSON Data								
Results	Switch : RSVDC-	-FB1-LF1-1 Command	: show ip pim rp	-set all-vr	fs				
	VRF: DEV-DC-VRF								
	Status and Count Group Address	ters – PIM Learned Group Mask	RP-Set Informati RP Address	on Hold Time	Expire Time	Priority			
	224.0.0.0	240.0.0.0	10.0.0.100	150	114	192			
	VRF: PROD-DC-VRF								
	Status and Counters - PIM Learned RP-Set Information Group Address Group Mask RP Address Hold Time Expire Time Priority								
	224.0.0.0	240.0.0.0	10.0.0.100	 150	 114	 192			
	Switch : RSVDC-FB1-LF1-2 Command : show ip pim rp-set all-vrfs VRF: DEV-DC-VRF								
	Status and Counters – PIM Learned RP-Set Information Group Address Group Mask RP Address Hold Time Expire Time Priority								
	224.0.0.0	240.0.0.0	10.0.0.100	150	114	192			
(* = Required)							CANCEL	RUN	4
Step 5 Review the output to verify that the campus RP is learned in all overlay VRFs on all leaf switches.

Redistribute Local SVI into EVPN

Redistribute local SVI interfaces into EVPN instances on leaf switches to distribute system-MAC values. This ensures proper distribution of IGMP querier information throughout the fabric.

Step 1 On the Configuration menu, select Routing > EVPN.



Step 2 On the right ACTIONS menu, select Settings.

Configuration / R	outing / EVPN			
	Fabr	ic RSVDC-FB1		
EVPN EV	PN MULTI SITE			
			\triangleright \bigcirc	C ACTIONS V
	I Name ↓ 1/2	Switch Name	E VLAN IE	Add
	Enter Name	Enter Switch Name	Enter Regex for VLAN	Edit
	DC-FB1-EVPN-RSVDC-FB1-LF2-1-101	RSVDC-FB1-LF2-1	101	Delete
	DC-FB1-EVPN-RSVDC-FB1-LF2-2-101	RSVDC-FB1-LF2-2	101	VLAN
	DC-FB1-EVPN-RSVDC-FB1-LF3-1-101	RSVDC-FB1-LF3-1	101	Import Route Targets
	DC-FB1-EVPN-RSVDC-FB1-LF3-2-101	RSVDC-FB1-LF3-2	101	Export Route Targets
	DC-FB1-EVPN-RSVDC-FB1-LF2-1-102	RSVDC-FB1-LF2-1	102	Redistribute Host Route
	DC-FB1-EVPN-RSVDC-FB1-LF2-2-102	RSVDC-FB1-LF2-2	102	Settings
	DC-FB1-EVPN-RSVDC-FB1-LF3-1-102	RSVDC-FB1-LF3-1	102	Reapply EVPN
	DC-FB1-EVPN-RSVDC-FB1-LF3-2-102	RSVDC-FB1-LF3-2	102	10102

Step 3 On the EVPN Settings Page, assign the following values and click APPLY.

- Enable ARP Suppression: < checked >
- Redistribute Local MAC Address: < unchecked >
- Redistribute Local SVI: < checked >
- Apply the EVPN Settings across the entire Fabric and all Switches contained within it: <
 unchecked >
- Switches: < Select leaf switches containing EVPN mapped overlay VLANs >

😦 EVPN Sett	ings ×
The ARP Suppressio	n, Local MAC, and Local SVI will be applied to all of the selected switches. pression I MAC Address
Redistribute Loca Apply the EVPN S Switches *	I SVI Settings across the entire Fabric and all Switches contained within it. X RSVDC-FB1-VSX_RSVDC-FB1-LF2-1_RSVDC-FB1-LF2-2 X RSVDC-FB1-VSX_RSVDC-FB1-LF3-2_RSVDC-FB1-LF3-1 X T
VXLAN Tunnel Bridging Mode	Select The VXLAN Tunnel Bridging Mode will be applied to the Border Leader Switches under the Fabric or to all selected Switches.
(* = Required)	CANCEL
NOTE:	
ARP suppres ARP Suppres overwritten u	sion was enabled when originally creating the EVPN instance. Checking Enable ssion when changing EVPN settings is required, because existing settings will be using the values specified on the EVPN Settings page after clicking APPLY . When

enable system-MAC propagation.

Configure Overlay IGMP and IGMP Snooping

IGMP is configured on all leaf switches, and IGMP snooping is configured on both leaf switches and server access switches.

routed multicast is not performed in the overlay, select Redistribute Local MAC Address to

Step 1 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Configuration Editor**.

🖄 🎦 🗸	₽	Aadmin 🖌	? *
>_ Show Commands			
🔒 Configuration Editor			

Step 2 In the **Switch** field, select all other leaf switches with data center overlay VLANs and server access switches

Configurat	tion / System / C	Configuration Editor				
Fabric	RSVDC-FB1		Switch	 × RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-LF2-1 	× •	SELECT ALL
RSVDC	-FB1-LF2-1	RSVDC-FB1-LF2-2	RSVDC-FB1-L	F3-1 RSVDC-FB1	-LF3-2 RSVDC-	FB1-LF3-SA1
<pre>! !Versior !export- hostname user adm AQBapCYF /ndYLzx3 user afd AQBapTEF Pf0l+4Er clock t: bfd profile vrf DEV- rd 1 rout vrf PROD rd 1 rout vrf PROD vrf QCreat VALID</pre>	n Aruba0S-CX -password: d e RSVDC-FB1- min group ad RgjEFVKYXXkz 3i9a1cRDpYxd c_admin grou Rot5rje3DXp5 npi+UodfMuGw imezone amer leaf -DC-VRF 10.250.2.1:3 te-target ex te-target im D-DC-VRF 10.250.2.1:2 te-target ex te-target im	DL.10.13.1050 efault LF2-1 ministrators pass NEffqoCkxjeLzmVTl daxUrjzKZPtpaFiyh p administrators CzMr3akCjkt4V5UGW v1cFQooxEukzogMTC ica/los_angeles port 65001:100002 port 65001:100001 port 65001:100001	word cipherte kUSmqA6c0q1CY 4DRGaCMU3toTi password ciph NLA34lZvd6rAY 2yQAlGacZJoEx evpn evpn evpn	ext /gAAAJtr4pogR6sAq fpDuXnDNYq0vfHjm nertext /gAAAAtiFw5Z4ngQh caTEGJwe8dvjPfxrV	y/+cwnsft7FlvNu 17Ty1MbGH08laCA wz7h0V0dPKMFx5c nESCh0cR6eKKrZK	yaeAl9ZqLSj59j1 vjeTNXp87 k9v2aDDnZcoC/GZ mfzD6NzRS NEXT ERROR
NOTE	•					

The border leaf switches in our example are dedicated to the border leaf function and do not include overlay host VLANs. Configure IGMP on border leaf switches, when overlay host VLANs are present.

Step 3 Enable IGMP on all overlay VLAN interfaces on each leaf switch.

interface vlan 101 ip igmp enable interface vlan 102 ip igmp enable interface vlan 201 ip igmp enable interface vlan 202 ip igmp enable

Configuration / System / Configuration Editor	
Fabric RSVDC-FB1 Switch Switch	SELECT ALL
x BSVDC-EB1-I E2-2	× •
RSVDC-FB1-LF2-1 RSVDC-FB1-LF2-2 RSVDC-FB1-LF3-1 RSVDC-FB1-LF3-2	RSVDC-FB1-LF3-SA1
interface vlan 101	
description Production web app SVI/VLAN 101 in DC overlay	
vrf attach PROD-DC-VRF	
ip mtu 9198	
ip address 10.5.101.1/24	
active-gateway ip mac 02:00:0a:05:00:01	
active-gateway ip 10.5.101.1	
ip igmp enable	
ip pim-sparse enable	
ip pim-sparse vsx-virtual-neighbor	
interface vlan 102	
description Production database SVI/VLAN 102 DC overlay	
vrf attach PROD-DC-VRF	
ip mtu 9198	
1p address 10.5.102.1/24	
active-gateway ip mac 02:00:03:05:00:01	
in igmn onable	
ip nim_sparse enable	
in nim-sparse vsx-virtual-neighbor	
VALIDATE APPLY	NEXTERROR
VALID/	ATE ALL APPLY ALL

Step 4 Enable IGMP snooping on all overlay VLANs for both leaf switches and server access switches.

Configuration / Syster	m / Configuration Editor			
Fabric RSVDC-F	-B1	Switch × RSV × RSV	DC-FB1-LF2-1	
RSVDC-FB1-LF2-	1 RSVDC-FB1-LF2-2	RSVDC-FB1-LF3-1	RSVDC-FB1-LF3-2	RSVDC-FB1-LF3-SA1
ssh server vrf m vlan 1 vlan 101 description ip igmp snoo vlan 102 description ip igmp snoo vlan 201 description ip igmp snoo vlan 202 description ip igmp snoo vlan 3001 description vlan 3002 description vlan 3999 virtual-mac 02:0	AFC-created VLAN oping enable AFC-created VLAN oping enable AFC-created VLAN oping enable AFC-created VLAN oping enable AFC-created VLAN AFC-created VLAN AFC-created VLAN			
VALIDATE	APPLY			NEXT ERROR
✓ Create a Check	point before Apply		VALIE	DATE ALL APPLY ALL

Step 5 Click VALIDATE ALL.

Step 6 Click APPLY ALL.

Verify Overlay IGMP and IGMP Snooping

On all leaf and server access switches, start a multicast listener for a multicast group with an active source, then use the follow procedure to verify IGMP and IGMP snooping optimizations.

Step 1 On the menu bar at the top right of the Fabric Composer window, click the **CLI Commands** icon and select **Show Commands**.

🕸 🎦 🗸	:=	Sadmin 🖌	? ~
>_ Show Commands			
E Configuration Editor			

Step 2 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select all leaf switches with overlay VLANs >
- **Commands:** show ip igmp groups all-vrfs

>_ CLI Comman	d Processor ×							
Select Fabrics or Switches, and select or add Saved Commands that can be customized. Press Run for results.								
Fabrics	Not applicable when a Switch is selected.							
Switches	× RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-LF3-1 × RSVDC-FB1-LF3-2							
Saved Commands	Select from Saved Commands or Add new commands.							
Commands	show ip igmp groups all-vrfs							
	A comma separated list of commands to be run.							
Download Options	Download Results Download JSON Data							
Results	Switch : RSVDC-FB1-LF2-1 Command : show ip igmp groups all-vrfs							
	IGMP group information for group 239.1.1.1							
	Interface Name : vlan201 VRF Name : DEV-DC-VRF							
	Group Address : 239.1.1.1 Last Reporter : 10.6.201.121							
	V1 V2 Sources Vers Mode Uptime Expires Timer Timer Forwarded Blocked							
	3 EXC 0m 53s 3m 27s							
	IGMP group information for group 239.1.1.1							
	Interface Name : vlan202 VRF Name : DEV-DC-VRF							
	Group Address : 239.1.1.1 Last Reporter : 10.6.202.121							
	V1 V2 Sources Vers Mode Uptime Expires Timer Timer Forwarded Blocked							
	3 EXC 0m 30s 3m 50s							
(* = Required)	CANCEL							

Step 3 Verify that the multicast group is learned on each switch on the VLAN corresponding with the attached listening hosts.

Step 4 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select all leaf switches with overlay VLANs and server access switches >
- **Commands:** show ip igmp snooping groups

>_ CLI Command	rocessor ×
Select Fabrics or Switches,	and select or add Saved Commands that can be customized. Press Run for results.
Fabrics	Not applicable when a Switch is selected.
Switches	× RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-LF3-1 × RSVDC-FB1-LF3-2 × RSVDC-FB1-LF3-SA1 ×
Saved Commands	Select from Saved Commands or Add new commands.
Commands	show ip igmp snooping groups
	comma separated list of commands to be run.
Download Options	Download Results Download JSON Data
Results	witch : RSVDC-FB1-LF2-1 Command : show ip igmp snooping groups
	[GMP Group Address Information
	/LAN ID Group Address Expires UpTime Last Reporter Type
	L01 239.1.1.1 3m 51s 5m 10s 10.5.101.121 Filter
	102 239.1.1.1 3m 9s 4m 34s 10.5.102.121 Filter
	201 239.1.1.1 3m 13s 4m 13s 10.6.201.121 Filter
	202 239.1.1.1 3m 18s 3m 50s 10.6.202.121 Filter
	Switch : RSVDC-FB1-LF2-2 Command : show ip igmp snooping groups
	IGMP Group Address Information
	/LAN ID Group Address Expires UpTime Last Reporter Type
	l01 239.1.1.1 3m 50s 5m 10s 10.5.101.121 Filter
	102 239.1.1.1 3m 9s 4m 34s 10.5.102.121 Filter
	201 239.1.1.1 3m 13s 4m 12s 10.6.201.121 Filter
	202 239.1.1.1 3m 17s 3m 51s 10.6.202.121 Filter
(* = Required)	CANCEL RUN

Step 5 Verify that that IGMP snooping has state for all VLANs with a listener.

VMWare vSphere Integration

VMware vSphere integration enables VMware host and virtual machine visualization within Fabric Composer. This procedure also enables automated switch port provisioning of VLANs based on how the vSwitch and VMs are setup.

Step 1 On the Configuration menu, select Integrations > VMware vSphere.

HPE aruba retworking Fa	bric Composer	Dashboard	Config	uration 🗸	Maintena	ance 🗸	Visualization 🗸	
🔗 Settings 🗸			•	Ports	>			
				Routing	>			
SWITCHES - ALL L	OCAL FABRICS	© X	₽	System	>			
Owit	9		昂	Network	>			
	•		٥°	Administrati	on >			
			Ē	Integrations	>		Aruba NetEdit	
	9		*	Policy	>		HPE iLO Amplifier	r
		L			_		HPE SimpliVity	
FABRIC INVENTOR	Y - ALL LOCAL FABRI	CS			_	×	Nutanix Prism	
90	MAC Attachmer	nts	0	CDP No	eighbor	2	Pensando PSM	
61	LLDP Neighbors	S	450	Ports	0	NSX	VMware NSX-T	
13	LAGs					- 🗗	VMware vSphere	
						۵	VMware SDDC	
							_	

Step 2 On the right ACTIONS menu, click Add to start the VMware vSphere wizard.

Configuration / Integrations / VMware vSphere				
			\triangleright	
Status 1	Host 🗦	Username	Enabled 1	Add
Select Status 👻	Enter Regex for Host	Enter Regex for Usernam	Select Ena 🔻	Edit
		There is no data to display		Delete
				Refresh vSphere Integration

Step 3 On the **Host** page, assign the following settings:

- Name: Example-vSphere1
- **Description:** Example vSphere Integration
- Host: rsvdc-vcenter.example.local
- Username: administrator@example.local
- Password: < password >
- Validate SSL/TLS certificates for Aruba Fabric Composer: unchecked
- Enable this configuration: checkmark

🚱 VMware vSp	phere	(?) ×
Host	Aruba Fabric vSphere Summary	
Configure an integratic	on between Aruba Fabric Composer and VMware vSphere	
Name *	Example-vSphere1	
	Any non empty string, example: integration 1	
Description	Example vSphere Integration	
	Example: My new Integration.	
Host *	rsvdc-vcenter.example.local	••••
	A valid Hostname at least two characters long or IPv4 Address, example: hostname.example.com, 198.162.5.4	
Username *	administrator@example.local	•••1
	Any non empty string, example: administrator@vspnere.local	
Password *	Any non-empty string, example: tan boot-13	••••
	 Validate SSL/TLS server certificate when communicating with this system (self-signed and private CA-signed server certificates not supported) Enable this configuration 	
([*] = Required)	CANCEL BACK N	EXT
NOTE:		

Host is the resolvable hostname or IP address of the vCenter server. **Username** is the name of an administrator account on the vCenter server. **Password** is the password for the administrator account on the vCenter server.

Step 4 Click **VALIDATE** to verify that the provided credentials are correct. A green success message appears at the bottom right. Click **NEXT**.



Automated PVLAN provisioning for ESX hosts direction connected to the fabric and enter a VLAN range. Check **Automated Endpoint Group Provisioning**, then click **NEXT**.

- If the hosts are directly connected from the NIC to the switch, select **Automated VLAN provi**sioning for ESX hosts directly connected to the fabric.
- If host infrastructure is HPE Synergy or another chassis with an integrated switch solution, select **Automated VLAN provisioning for ESX hosts connected through intermediate switches**.

Host	Aruba Fabric vSphere Summary
nfigure how Aruba Fabric Co	mposer interacts with VMware vSphere.
Enable automatic VLAN provisionin	ig on Aruba switch ports based on changes that occur in VMware virtual networking.
Automated VLAN pro	ovisioning for ESX hosts directly connected to the fabric.
VLAN Range	1-4094
	Enter the VLAN range Aruba Fabric Composer is allowed to modify on Aruba switches as part of an integration. An empty VLAN Range will prevent Aruba Fabric Composer from modifying VLANs. A number, set, or range of VLANs between 1 and 4094, example: 5, 10-45, 102.
Automated VLAN pro directly connected to	ovisioning for ESX hosts connected through intermediate switches. Requires Automatic VLAN Provisioning for ESX hosts of the fabric to be enabled.
Intermediate VLAN	1-4094
Range	Enter the VLAN range Aruba Fabric Composer is allowed to modify on Aruba switches as part of an integration. An empty VLAN Range will prevent Aruba Fabric Composer from modifying VLANs. A number, set, or range of VLANs between 1 and 4094, example: 5, 10-45, 102.
 Automated PVLAN p connected to the fab 	rovisioning for ESX hosts directly connected to the fabric. Requires Automatic VLAN Provisioning for ESX hosts directly ric to be enabled.
PVLAN Range	1-4094
PVLAN Range	1-4094 Enter the PVLAN range Aruba Fabric Composer is allowed to modify as part of an integration. An empty PVLAN Range will prevent Aruba Fabric Composer from modifying PVLANs. A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102.
PVLAN Range	1-4094 Enter the PVLAN range Aruba Fabric Composer is allowed to modify as part of an integration. An empty PVLAN Range will prevent Aruba Fabric Composer from modifying PVLANs. A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102. up Provisioning
PVLAN Range Automated Endpoint Gro Automatically create Endpoint (1-4094 Enter the PVLAN range Aruba Fabric Composer is allowed to modify as part of an integration. An empty PVLAN Range will prevent Aruba Fabric Composer from modifying PVLANs. A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102. up Provisioning Groups based on VM tags.
PVLAN Range Automated Endpoint Gro Automatically create Endpoint (* = Required)	1-4094 Enter the PVLAN range Aruba Fabric Composer is allowed to modify as part of an integration. An empty PVLAN Range will prevent Aruba Fabric Composer from modifying PVLANS. A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102. pup Provisioning Groups based on VM tags. CANCEL BACK
PVLAN Range Automated Endpoint Gro Automatically create Endpoint (* = Required)	1-4094 Enter the PVLAN range Aruba Fabric Composer is allowed to modify as part of an integration. An empty PVLAN Range will prevent Aruba Fabric Composer from modifying PVLANs. A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102. pup Provisioning Groups based on VM tags. CANCEL BACK

uisite for microsegmentation automations built into Fabric Composer. **Automated Endpoint Group Provisioning** enables assigning VMs dynamically to firewall policy using VM tags. The IP addresses used in the policy are modified dynamically in the future, if a VM IP changes or the VMs associated with the tag change. For additional details on all options, refer to the *HP Aruba Networking Fabric Composer User Guide*.

Step 6 On the vSphere page, click the checkbox for Discovery protocols and click NEXT.

VMware vSphere			0
			?
Host	Aruba Fabric	vSphere	Summary
Enable discovery settings for this VMv	vare vSphere configuration.		
Z Discovery protocols	, ,		
Required to enable host visualizations. This	selection automatically enables CDP for Stand	lard vSwitch, and LLDP for Distributed vSw	vitch in vSphere.
(* = Required)			CANCEL BACK NEXT
If Discovery protocols	is not enabled, the VM	ware integration can	not display virtual switches
correctly		0	
correctly.			

Step 7 On the **Summary** page, confirm that the information is entered correctly and click **APPLY**.

VMware vSphere			() ×
Host	Aruba Fabric	vSphere	Summary
Host		rsvdc-vcenter.exa	mple.local
Username		administrator@exa	ample.local
Password		******	
Enabled		Yes	
Verify SSL		No	
Name		Example-vSphere	1
Description		Example vSphere	Integration
Auto Discovery		Yes	
Automated VLAN Provisioning		Yes	
VLAN Range		1-4094	
Automated Intermediate VLAN Provis	sioning	No	
Intermediate VLAN Range		1-4094	
Automated PVLAN Provisioning		Yes	
PVLAN Range		1-4094	
Automated Endpoint Group Provisior	ning	Yes	
			CANCEL BACK APPLY

Step 8 Go to Visualization > Hosts.

HOSTS VMS								
1 selected								
	Name	lΞ	Network Interfaces		vSwitches	ĻΞ		
	Enter Regex for Name		Enter Regex for Network Interfaces		Enter Regex for vSwitches			
	esxi-12.example.local		vmnic0		RSVDC-DS			
			vmnic2		vSwitch0			
			vmnic4					
	vmnic1							
			vmnic3					
	esxi-13.example.local		vmnic0		RSVDC-DS			
			vmnic1		vSwitch0			
			vmnic2					
			vmnic4					
			vmnic3					
	esxi-14.example.local		vmnic0		RSVDC-DS			
			vmnic1		vSwitch0			
			vmnic2					
(1 - 3 of 3 total)	25 🗸							

Step 9 Select the checkbox next to the Name of an ESXi VM host to add it to the visualization window.

HOSTS VI	IS						
2 selected						(70
	Name	48	Network Interfaces	vSwitches	IL.	IP Addresses	E
	Enter Regex for Name		Enter Regex for Network Interfaces	Enter Regex for vSwitches		Enter Regex for IP Addresses	
	esxi-05.example.local		vmnic0	DSwitch-DC1			
			vmnic1	vSwitch0			- 1
			vmnic2				- 1
			vmnic3				- 1
			vmnic4				- 1
			vmnic5				- 1
	esxi-06.example.local		vmnic0	DSwitch-DC1			
			vmnic1	vSwitch0			
			vmnic2				
			vmnic3				
			vmnic4				
(1 - 3 of 3 total)	25 🗸						1

Step 10 Verify the connectivity displayed from the hypervisor layer to the leaf switches.



Secure an Aruba EVPN Fabric

AFC orchestrated security policy is applied to east-west traffic using CX 10000 switches and AMD Pensando's Policy and Services Manager in this example fabric. ACL policy also can be applied to east-west and north-south traffic.

Overview

This chapter describes enforcing policy in the Aruba ESP data center network using the Aruba CX 10000 switch platform's stateful firewall. Policy is implemented using the AMD Pensando Policy and Services Manager (PSM) orchestrated by Aruba Fabric Composer (AFC). Stateful firewall policy filters traffic between VLANs, between hosts in the same VLAN, and between VM guests assigned to the same hypervisor (microsegmentation).

The Aruba CX 10000 series switch is a data-center-class Distributed Services Switch (DSS). It includes hardware dedicated to performing stateful firewall functions on data center host traffic. Configuring and managing these capabilities require deployment of PSM. AFC is recommended to manage PSM. Refer to the Aruba ESP Data Center Design VSG and the *Pensando Policy and Services Manager for Aruba CX 10000: User Guide* for additional details.

NOTE:

Aruba CX 10000 switches running AOS-CX 10.13 and above require a feature pack license to enable firewall features. Information on the installation and purchase of feature packs can be found in the Feature Pack Ordering Guide and Deployment Guide.

Configure PSM Integration with Aruba Fabric Composer

Use this procedure to associate a PSM cluster with a fabric in AFC to enable centralized management of firewall policy.

Step 1 On the menu bar at the top right of the AFC user interface, select **Guided Setup**.



Step 2 At the top of the **Guided Setup** window, click the **Distributed Services** tab, then click **PEN-SANDO PSM**.

NETWORK DISTRIBUTED SERVICES							
Distributed Services Setup							
Perform the following steps to initialize and configure distributed services.							
O PENSANDO PSM * Configure the Distributed Services Manager							
CONFIGURE VRFS Configure VRFs to sync with PSM							
Selected VRF:							
RSVDC-FB1/default × -							
CONFIGURE NETWORKS Configure Networks for Selected VRF							
Configure Policies.							
CONFIGURE MICROSEGMENTATION Configure Microsegmentations.							
* = Required • = Completed • = Incomplete							
CLOSE							

Step 3 On the **Host** page, enter the following values and click **VALIDATE**.

- Name: RSVDC-FB1-PSM
- **Description:** *PSM cluster for RSVDC fabric 1*
- Host: 172.16.104.51
- Username: admin
- Password: < Password for the PSM admin user >

Pensando	PSM ⑦	K
	Host Settings Summary	
Configure an integra	tion between Aruba Fabric Composer and Pensando PSM	
Name *	RSVDC-FB1-PSM	
	Any non empty string, example: integration 1	
Description	PSM cluster for RSVDC fabric 1	
	Example: My new Integration.	
Host *	172.16.104.51	
	A valid Hostname at least two characters long or IPv4 Address, example: hostname.example.com, 198.162.5.4	
Username *	admin	
	Any non empty string, example: IntegrationUser	
Password *		
	Any non empty string, example: tan.boot-13	
	 Validate SSL/TLS server certificate when communicating with this system (self-signed and private CA-signed server certificates not supported) 	
	Z Enable this configuration	
	VALIDATE	
(* = Required)	CANCEL BACK NEXT	
NOTE:		
The Host fiel	ld requires only a single DNS name or IP address of one PSM VM. The IP addresses	

of the remaining cluster members are discovered automatically.

Step 4 After the validation success message appears, click NEXT.



Step 5 On the **Settings** page, select the fabric. Leave other settings at their default and click **NEXT**.

Pensando PSM		? ×
Hos All Distributed Services ope support Distributed Services	t Settings Summary rations associated with the specified Fabric will be applied to this PSM instance. Do not specify a Fabric if this PSM instance s Switches.	does not
Fabric	RSVDC-FB1	× •
 Enable auto decommissi Enable auto VLAN place VMware vCenters which PSI 	oning for switches deleted from the system ment on all switches when creating a Network V will monitor. <i>PSM Experimental</i>	
VMware vCenters	Select 👻	ADD
(* = Required)	CANCEL BACK	NEXT

Step 6 On the Summary page, verify that the PSM cluster settings are correct and click APPLY.

Pensando PSM		@ ×
Host	Settings	Summary
Host	172.16.104.51	
Username	admin	
Fabric	RSVDC-FB1	
VMware vCenters		
Password	****	
Enabled	Yes	
Name	RSVDC-FB1-PSM	
Description	PSM cluster for RSVDC fabric 1	
Auto Decommission	No	
Auto VLAN Placement	Yes	
		CANCEL BACK APPLY



Aruba CX 10000 switches that are members of the same fabric make a join request to the PSM cluster at the completion of this step. AFC instructs PSM to admit CX 10000 switches, when auto-admission to the PSM cluster has been set to false.



Step 7 On the AFC top right menu bar, click the CLI Commands icon.

Step 8 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: < Select Aruba CX 10000 fabric leaf switches >
- Commands: show psm

>_ CLI Command	d Processor		×
Select Fabrics or Switche	es, and select or add Saved Commands that can be customized. Press Run for results.		
Fabrics	Not applicable when a Switch is selected.		
Switches	× RSVDC-FB1-LF2-1 × RSVDC-FB1-LF2-2 × RSVDC-FB1-LF3-1	× •	
Saved Commands	Select from Saved Commands or Add new commands.	REMOVE	
Commands	show psm		
	A comma separated list of commands to be run.		Ŀ
Download Options	Download Results Download JSON Data		L
Results	Switch : RSVDC-FB1-LF2-1 Command : show psm		L
	Policy and Services Manager Information		
	Operational Status : admitted Host Addresses : 172.16.104.51, 172.16.104.52, 172.16.104.53 VRF : mgmt PSM Identifier : 172.16.104.105 Operational Addresses : 172.16.104.51, 172.16.104.52, 172.16.104.53		
	Switch : RSVDC-FB1-LF2-2 Command : show psm		
	Policy and Services Manager Information		
(* = Required)	CANCEL	RU	N

Step 9 Verify that each CX 10000 has the following values in the command output.

• **Operational Status:** admitted

- Host Addresses: < IP address list of PSM cluster members >
- VRF: mgmt
- Operational Addresses: < IP address list of PSM cluster members >

Configure Macro Firewall Policy

A firewall policy is a collection of rules applied to a PSM *Network* object or *Virtual Routing and Forwarding* (*VRF*) objects. When PSM policy is applied to a DSS switch, a *Network* object corresponds to a VLAN on the switch, and a *VRF* object corresponds to a VRF on the switch.

A policy contains a set of rules that specify the traffic allowed or denied between endpoint groups. Each rule contains service qualifiers or applications (sets of service qualifiers) that identify traffic type by port number. An implicit "deny all" rule is applied at the end of every policy.

The following firewall policy example restricts traffic allowed to the database server VLAN. It is applied to a PSM *Network*. For information on choosing between applying a policy to a *Network* or a *VRF*, refer to the Network Design section of the Data Center Design VSG.

The primary purpose of the sample policy is to protect database servers. At the completion of this process, web application servers are allowed to send MSSQL, ICMP, and traceroute traffic to the database servers. Other traffic is denied.

The process defines the following: - PSM *Network* objects to inform CX 10000 switches which VLANs to redirect to the firewall engine - Endpoint group objects to specify IP ranges applied to firewall rules - Firewall rules to specify allowed or denied traffic - Firewall policy that stitches the above components together

The web servers are distributed across both CX 10000 switches and non-DSS switch models in this example. The database servers are connected only to a CX 10000 leaf pairs.

Configure PSM Networks

In this procedure, PSM *Network* objects are created to specify which VLANs redirect traffic for firewall policy enforcement. Creating a PSM *Network* in AFC will not create a VLAN on the switch. A corresponding VLAN and SVI must be defined, if they do not already exist. For complete configuration steps for prerequisite VRFs, VLANs, and SVIs, refer to Deploying the Fabric earlier in this guide.

Step 1 On the **Distributed Services** tab of **Guided Setup**, choose **RSVDC-FB1/PROD-DC-VRF** in the **Selected VRF** dropdown. Click **CONFIGURE NETWORKS**.



Step 2 To add a PSM *Network* for the web server VLAN, click the right **ACTIONS** menu and select **Add** to start the **Network** workflow.

onfiguration / Rou	iting / VRF / PRC	D-DC-VRF							
			Fabric	RSVDC-FB					
							۲) 🛇 🏹 🕸 📿 🛛 AC	tions 🗸
Name	15	Туре	IE.	Switches	μ <u>μ</u>	L3 VNI	1 <u>1</u>	Route Target Ext-Comm	unity 🞼
Enter Name		Select Type	~	Enter Switch	es	Enter F	Regex for L3 VNI	Enter Regex for Route	Target
PROD-DC-VRF		User		RSVDC-FB1-LI	F1-1,RSVDC-FB1-	100001		65001:100001	
LF1-2,RSVDC-FB1-LF2-				FB1-LF2-1,RSVDC-					
				FB1-LF2-2,RSV	/DC-FB1-LF3-				
				1,RSVDC-FB1-	LF3-2				
IP INTERFACES	S IP STATIC	ROUTES NETW	ORKS	ARP TABLES	IP ROUTE TA	BLES			
									tions 🗸
	Name			4E	Health	1£	VLAN	Add	
	Enter Mama				Select Health	-	Enter Regex for VLAN	L. Edit	
	Enter Name.				ooloot noulin				

Step 3 On the Name page, enter a Name and Description, then click NEXT.

昂 Network			×
		?	?
	Name	Settings	Summary
Enter a required Na	me and an optional Description	วท.	
Name *	DB-PROD-NET		
	Any non-empty string, exam	ple: Network-1	
Description	Production database	server network in the RSVDC overlay	
	Example: Network-1 Descrip	tion	
([*] = Required)			CANCEL BACK NEXT

Step 4 On the **Settings** page, enter the database server VLAN ID in the **VLAN** field to associate it with the *Network* object, then click **NEXT**.

昂 Network				×
			?	
Nan	ne	Settings	Summary	
Set the required VLAN.				
VLAN *	102			
	A VLAN between 1 and 4094, example: 1.			
(* = Required)			CANCEL BACK NEXT	

Step 5 On the **Summary** page, verify that the information is correct and click **APPLY**.

			×
	Name	Settings	Summary
Name Description VLAN	DB-PROD-NET Production datab 102	ase server network in the RSVDC overlay	
			CANCEL BACK APPLY

Step 6 Repeat the procedure to define a Network object for every VLAN in PROD-DC-VRF.

CAUTION:

Communication failures may result between two hosts in different VLANs, if a *Network* object is not associated to both VLANs. It is best practice to define a *Network* for every VLAN in a VRF.

Review Dynamic Endpoint Groups

Endpoint group objects represent source and destination IP addresses referenced in firewall rules. Dynamic endpoint groups are autopopulated based on the assignment of vSphere tags to VMs identified through AFC's vCenter integration.

All VMs assigned the same tag are autopopulated as a member of the dynamic group. When member IP addresses change or tag assignments are changed in vCenter, dynamic group objects are updated automatically.

Step 1 On the Configuration menu, select Policy > Endpoint Groups.



Step 2 Verify that the VMs assigned tags in vSphere are populated in the dynamic endpoint groups.

Configuration / F	Policy / Endpoint Groups		
	I ⊘ Name ↓≟	Rules	j≞_
	Enter Regex for Name	Enter R	▼ Enter Regex for IPv4 Address
	rsvdc-vcenter.example.local_prod:app1_db	Layer 3	10.5.102.60
			10.5.102.70
	rsvdc-vcenter.example.local_prod:app1_webui	Layer 3	10.5.101.50
			10.5.101.51
			10.5.101.61
			10.5.101.62
			10.5.101.70

NOTE:

If no dynamic endpoint groups are present, verify that **Automated Endpoint Group Provisioning** is enabled in **Configuration > Integration > VMware vSphere**. Verify that VMs in vSphere have been assigned tags and are currently running. Refer to the Deploying the Fabric section for more information on integration.

Configure Static Endpoint Groups

Additional endpoint groups are created to represent IP addresses not automatically populated in a dynamic group.

Step 1 To create an endpoint group for the network services subnet, in the **Configuration > Policy > Endpoint Groups** context, click the right **ACTIONS** menu and select **Add**.

Configuration / Po	olicy / Endpoint Groups		
	♂ Name	Rules 1= Type	J≟
	Enter Regex for Name	Enter R Select Type	✓ Ente Edit
	rsvdc-vcenter.example.local_prod:app1_db	Layer 3	10.5.10 Delete
			10.5.102.70

Step 2 On the Name page, enter a Name and Description, then click NEXT.

n Endpoint Gr	quo			×
Name	(?) Type	Endpoints	Summary	
Enter a required Name	and an optional Description.			
Name *	Network-Services-EG			
	Any non-empty string, example: EndpointGroup-1.			
Description	Supporting network services hosts (DNS, N	ITP, etc.)		
	Example: EndpointGroup-1 Description.			
(* = Required)			CANCEL BACK NEXT	r

Step 3 On the Type page, leave Type set to the default Layer 3 value and click NEXT.

n Endpoint Grou	p				×
Name	Ту	pe	Endpoints	Summary	
Select the required Type.					
Туре	Layer 3				× •
(* = Required)				CANCEL BACK	NEXT

Step 4 On the **Endpoints** page, click the **Manual Endpoint entry** radio button, enter the web server subnet value in the **IPv4 Network Address** field, and click **ADD**.

🖷 Endpoint Group			×
Name	Type	Endpoints	Summary
Add one or more IPv4 Addres	ss endpoints.		
○ VM/VNIC/VMKernel Endp	oint		
Criteria	VM Name		
VM Name	Select		
VNIC	Select		▼ SELECT ALL
Manual Endpoint entry			
IPv4 Network	10.2.120.0/24		
CLEAR ADD	A range of IPv4 Addresses defined as a hyphenated	I range or subnet using CIDR notation. Ex.	amples: 192.168.1.100-192.168.1.200, 192.168.10.0/24
	There is	no data to display	
(* = Required)			CANCEL BACK NEXT

A single endpoint group can be a collection of IP ranges and individual addresses. Static endpoint groups can be made using AFC's vSphere integration. When making static assignments in the Endpoint Group wizard based on a VM Name or VM Tag, the IP addresses added to the endpoint group are established at the time of the endpoint group's creation. Future changes to VM IP addresses or tag assignments are not updated automatically in the address object. Use dynamic endpoint groups to automatically update VM IP assignments.

Step 5 Verify that the subnet was added to the list at the bottom of the Endpoint Group window and click **NEXT**.

n Endpoint Group		×
Name Add one or more IPv4 Addr	ess endpoints.	oints Summary
O VM/VNIC/VMKernel End	lpoint	
Criteria	VM Name	
VM Name		
VNIC	Select	▼ SELECT ALL
Manual Endpoint entry		
IPv4 Network Address	A range of IPv4 Addresses defined as a hyphenated range or subnet using	CIDR notation. Examples: 192.168.1.100-192.168.1.200, 192.168.10.0/24
CLEAR ADD		
IPv4 Network Address	VM/VNIC/VMKernel	
10.2.120.0/24		団
(* = Required)		CANCEL BACK NEXT

Step 6 On the **Summary** page, verify that all information is correct and click **APPLY**.

🕞 Endpoint Group			>
Name	Туре	Endpoints	Summary
Name	Network-Services-EG		
Description	Supporting network services hosts (DN	IS, NTP, etc.)	
Туре	Layer 3		
Endpoints			
IPv4 Network Address		VM/VNIC/VMKernel	
10.2.120.0/24			
			CANCEL BACK APPLY

Step 7 Repeat the procedure to create additional endpoint groups to be used in firewall rules using the following values:

Name	Description	Туре	Address
PROD-DC-VRF- Summary-EG	Summary IP prefix for PROD-DC-VRF in the DC overlay	Layer 3	10.5.0.0/16

Name	Description	Туре	Address
Campus-Admins-EG	Campus IP subnet used by application administrators	Layer 3	10.254.1.0/24
All-Hosts-EG	All hosts endpoint group	Layer 3	0.0.0.0/0

Configure Firewall Rules

In the following procedure, firewall rules are created to define the inbound traffic allowed to the backend database server VLAN.

In addition to allowing communication from frontend web servers, rules that enable network service functions and troubleshooting protocols are defined. This is required because any traffic not explicitly allowed in firewall policy is blocked by an implicit deny rule.

It is important to consider the policy direction, when defining rules. In this example, an ingress policy is used to filter both DSS and non-DSS sourced traffic to the database servers. Policy direction and design vary based on requirements and administrator preferences.

An individual rule identifies source and destination endpoint groups, a service qualifier or application to specify the traffic type, and an action of "allow" or "deny". A rule does not allow or deny traffic until it is added to a policy.

Step 1 In the AFC left navigation pane, click Rules.

or	TUDO Fabric Composer Das
Ē	Policy Groups
	Policies
Ē.	Rules
匾	Endpoint Groups
	Applications
\$11 1	Service Qualifiers
+	Microsegmentation
盘	Firewall Log
Å	Firewall Profiles
Û	PSM Alerts

Step 2 To create a rule that allows web servers to reach database servers using the MSSQL protocol, click the right **ACTIONS** menu and select **Add**.

Configuration / Pol	licy / Rules						
						$\odot \odot \heartsuit$	
	♂ Name	1E	Policies	1E	Type ↓ <u>⊥</u>	Source Endpoint Gro… ↓	Add
	Enter Regex for Name		Enter Regex for Policies		Select Ty▼	Enter Regex for Source I	Edit
							Delete

Step 3 On the Name page, enter a Name and Description, then click NEXT.

🗊 Rule	×
Name	Settings Image: Constraint Groups Image: Constraint Groups Image: Constraint Groups Image: Constraint Groups Settings Endpoint Groups Applications and Service Qualifiers Summary
Enter a required Nam	e and an optional Description.
Name *	Allow-PROD-WEB-to-DB-MSSQL
	Any non-empty string, example: Rule-1
Description	Allow MSSQL traffic from prod web ui servers to backend DB servers
	Example: Rule-1 Description
(* = Required)	CANCEL BACK NEXT
NOTE:	
A helpful rul	e naming convention is to include the action of allow or deny, endpoint group, and

service in the rule name. This simplifies policy construction later.

Step 4 On the Settings page, leave the Type and Action fields at their default values and click NEXT.

🗐, Rule				×
Name	Settings	Endpoint Groups	Applications and Service Qualifiers	Summary
Select the required Type a	and Action.			
Туре	Layer 3			× •
Action	Allow			× •
([*] = Required)			CANC	EL BACK NEXT

Step 5 On the **Endpoint Groups** page, select the endpoint groups dynamically created using VM tags as follows, then click **NEXT**.

- **Source Endpoint Groups:** *rsvdc-vcenter.example.local_prod:app1_webui*
- **Destination Endpoint Groups:** *rsvdc-vcenter.example.local_prod:app1_db*

🗐, Rule		×
Name	Settings Endpoint Groups Applications and Service Summary Qualifiers	
Select or add one or more Source Endpoint Groups. No specified En	and Destination Endpoint Groups. Endpoint Group IPv4 Addresses may be added directly to the Source and Destination dpoint Groups implies any IP Addresses.	n
Source Endpoint Groups	× rsvdc-vcenter.example.local_prod:app1_webui	DD
	A range of IPv4 Addresses defined as a hyphenated range or subnet using CIDR notation. Examples: 192.168.1.100- 192.168.1.200, 192.168.10.0/24	
Destination Endpoint Groups	× rsvdc-vcenter.example.local_prod:app1_db × -	NDD
	A range of IPv4 Addresses defined as a hyphenated range or subnet using CIDR notation. Examples: 192.168.1.100- 192.168.1.200, 192.168.10.0/24	
(* = Required)	CANCEL BACK NEXT	
NOTE:		
AFC automatically up groups when a VM a	pdates IP addresses in a firewall rule that uses dynamically created endpoin Idministrator changes IP assignments or VM tags in vCenter.	nt

Step 6 On the **Applications and Service Qualifiers** page, begin typing the predefined *mssql_server* name in the **Service Qualifier** field, click **mssql_server** when it appears in the list, then click **NEXT**.

🗐, Rule	*		×
		?	
Name	Settings Endpoint Groups Applications and Service Qualifiers	Summary	
Select or add either App	ications or Service Qualifiers.		
Applications	Select		ADD
Service Qualifiers	× mssql_server	× •	ADD
(* = Required)	CANCEL	ВАСК	NEXT

Step 7 On the Summary page, verify that all information is correct and click APPLY.

🗐, Rule				×
Name	Settings	Endpoint Groups	Applications and Service Qualifiers	Summary
Name	Allow-PR	OD-WEB-to-DB-MSSQL		
Description	Allow MS	SQL traffic from prod web u	servers to backend DB servers	
Туре	Layer 3			
Action	Allow			
Source Endpoint Groups	rsvdc-vc	enter.example.local_prod:ap	p1_webui	
Destination Endpoint Groups	rsvdc-vc	enter.example.local_prod:ap	p1_db	
Service Qualifiers	mssql_se	erver		
			CANC	EL BACK APPLY

Step 8 Repeat the procedure to create rules with the following values for use in the the database server *Network* ingress policy.

Name	Description	Type Actio	rEndpoint Groups	Applications and Service Qualifiers
Allow-All- ICMP	Allow ICMP from all hosts to all hosts	Laye Allov 3	Source : All-Hosts-EG Destination : All-Hosts-EG	Service Qualifiers: icmp
Allow-All- UDP- Traceroute	Allow UDP-based traceroute from all hosts to all hosts	LayerAllov 3	v Source : All-Hosts-EG Destination : All-Hosts-EG	Service Qualifiers: traceroute
Allow- Admins-to- PROD-DC- VRF	Allow campus admin net hosts to production VRF in DC overlay	Laye Allov 3	Source: Campus-Admins- EG Destination : PROD-DC-VRF-Summary- EG	Service Qualifiers: all

NOTE:

Reduce the total number of rules created by defining rules that can be applied to more than one policy. A new rule can be cloned from an existing rule by selecting **ACTIONS > Clone**, when minor modifications are required for similar rules.

Configure Ingress Policy

When using an EVPN-VXLAN overlay, a PSM ingress policy filters all traffic arriving from other switches inside the fabric (DSS or non-DSS). This includes both Layer 2 and Layer 3 VXLAN forwarded traffic, and traffic originating from outside the data center fabric. An ingress policy also applies to routed traffic between hosts attached to the same CX 10000 switch, when using AOS-CX 10.10.1000 or later.

By default, an ingress policy does not apply to traffic between hosts in the same subnet attached to the same CX 10000 switch. This type of policy application can be achieved when using a PVLAN-based microsegmentation strategy, as described in ESXi VM Microsegmentation. Egress policy also can be applied to filter traffic between hosts attached to the same CX 10000 that are in the same VLAN and subnet, as long as the traffic traverses the switch.

The diagram below illustrates the components that protect the database servers from non-MSSQL traffic sourced by web servers:



Figure 6: Ingress Policy Diagram

In the following procedure, the previously created rules are assigned to a policy to filter traffic destined for the database server VLAN.

Step 1 In Configuration / Policy / Policies, click the right ACTIONS menu and select Add.

Configuration / Po	licy / Policies						07	🔆 C ACTIONS 🗸
	☑ Name	1E	Policy Groups	Health	1E	Туре	1£	E Add
	Enter Regex for Name		Enter Regex for Policy Groups	Select Health	~	Select Type	~	Edit
					There	is no data to display		Delete

Step 2 On the Name page, enter a Name and Description, then click NEXT.

Policy				×
Name	Settings	Rules	Enforcers	Summary
Enter a required Nam	ne and an optional Description.			
Name *	To-PROD-DB-Servers			
	Any non-empty string without spaces, e	example: Policy-1		
Description	Firewall policy applied to traff	ic destined to prod app1 D	B server VLAN hosts	
	Example: Policy-1 Description			
(* = Required)			CAN	CEL BACK NEXT

Step 3 On the **Settings** page, leave the default value of *Distributed Firewall* for **Type** selected and click **NEXT**.

Policy					×
Name	Settings	Rules	Enforcers	Summary	
Select a required type. Th	e Policy type will determine the a	pplicable Rules and Enforce	ers.		
Туре	Distributed Firewall			>	× -
(* = Required)			с	ANCEL BACK NEXT	

Step 4 On the Policy Rules page, click the right ACTIONS menu and select Add > Existing.

iet one or more Rules on the Policy. Rules may be enabled/disabled and reordered for this Policy. Image: Sequence inter Regex for Sequence Enabled inter Regex for Name in	Set one or more Rules on the Policy. Rules may be enabled/disabled and reordered for this Policy.	Policy	Settings	Rules	Enfo	Prcers	Summary
Sequence Enabled Name New < Add Enter Regex for Sequence Select En Enter Regex for Name Existing Remove	Sequence Enabled Name New < Add Enter Regex for Sequence Select En Enter Regex for Name Existing Move	et one or more F	Rules on the Policy. Rules may be e	nabled/disabled and reo	rdered for this Policy.		
Enter Regex for Sequence Select En Enter Regex for Name Remove	Enter Regex for Sequence Select En Enter Regex for Name Remove					ightarrow	
Move	Move		Sequence	Enabled	Name	New	ACTIONS ✓
			Sequence Enter Regex for Sequence	Enabled Select En 👻	Name Enter Regex for Nam	New Existing	ACTIONS ✓ <add Remove</add

Step 5 In the **Select Rules** window, click the checkboxes for rules allowing traffic destined to the database servers in the following order, then click **APPLY**.

- Allow-PROD-WEB-to-DB-MSSQL
- Allow-Admins-to-PROD-DC-VRF
- Allow-All-ICMP
- Allow-All-UDP-Traceroute

	Name	1E	Shared	Æ	Source Endpoint Groups	Source Endpoint G… ↓	Destination Endpoint Gr J
~	Enter Regex for Name		Select Shared	•	Enter Regex for Source I	Enter Regex for Sol	Enter Regex for Destinat
√	Allow-Admins-to-PROD-DC-	VRF	No		Campus-Admins-EG	10.254.1.0/24	PROD-DC-VRF-Summary-E
~	Allow-All-ICMP		No		All-Hosts-EG	0.0.0/0	All-Hosts-EG
~	Allow-All-UDP-Traceroute		No		All-Hosts-EG	0.0.0/0	All-Hosts-EG
- 4 of 4	4 total) 25 🗸				vcenter.example.local_prod: app1_webui	10.5.101.51 10.5.101.61 10.5.101.62 10.5.101.70	vcenter.example.local_prod app1_db
equirec	i)						CANCEL APP

exception is traffic originated in the database server VLAN where the source and destination are attached to the same CX 10000 switch.

Step 6 Verify that the rule set is in the desired order and click NEXT.

Policy										
	Nan	ne		Settings	Rules	Enforcers	Summary			
Set one or more Rules on the Policy. Rules may be enabled/disabled and reordered for this Policy.										
		Sequence	Enabled	Name	Source Endpoint Groups	Source Endpoint Group IPv4	Destination Endpoint Groups			
		Enter F	S 🔻	Enter Regex for Name	Enter Regex for Source I	Enter Regex for Source En	Enter Regex for Destinat			
\uparrow \downarrow		1		Allow-PROD-WEB-to-DB-MSSQL	rsvdc-	10.5.101.50	rsvdc-			
					vcenter.example.local_prod:	10.5.101.51	vcenter.example.local_prod:			
					app1_webui	10.5.101.61	app1_db			
						10.5.101.62				
						10.5.101.70				
$\uparrow \downarrow$		2		Allow-Admins-to-PROD-DC-VRF	Campus-Admins-EG	10.254.1.0/24	PROD-DC-VRF-Summary-EG			
$\land \downarrow$		3		Allow-All-ICMP	All-Hosts-EG	0.0.0/0	All-Hosts-EG			
$\uparrow \downarrow$		4	~	Allow-All-UDP-Traceroute	All-Hosts-EG	0.0.0/0	All-Hosts-EG			
(1 - 4 of 4	total)	25 🗸					1			
(* = Rec	quired)	Scroll for	more optior	15		CANC	EL BACK NEXT			

Step 7 On the **Enforcers** page, select the following values. Click the **ADD** button near the bottom left of the window (below the dropdowns).

- Fabric: RSVDC-FB1
- Direction: Ingress
- VRF: PROD-DC-VRF
- Networks: DB-NET-PROD VLAN: 102

Policy				×		
Name	Settings Rules	Enforcers	Summary			
Specify direction and	VRFs or individual networks within a VRF on which to apply the Policy.					
Fabric	RSVDC-FB1		× •			
Direction	Ingress					
VRF	PROD-DC-VRF		× •			
Networks	× DB-NET-PROD - VLAN: 102		× •	ADD		
CLEAR AD						
Enforcer	Direction					
	There is no data to display					
(* = Required)		CA	NCEL BACK	NEXT		
Policy						×
----------------------------	-------------------------------	------------------------------------	-------	------------	----------	------
				\bigcirc	?	
Name	Settings	Rules	Enfor	rcers	Summary	
Specify direction and VRFs	or individual networks within	n a VRF on which to apply the Poli	су.			
Fabric	Select				-	
Direction	Select				-	
VRF						
Networks						ADD
CLEAR ADD						
Enforcer		Direction				
undefined - DB-PROD-NET	- VLAN: 102	Ingress				
(* = Required)				CAN	CEL BACK	NEXT

Step 8 Verify that the enforcer information was added correctly and click NEXT.

Step 9 On the Summary page, verify that the information is correct and click APPLY.

Policy				×
Name	Settings	Rules	Enforcers	Summary
Name	To-PROD-DB-Servers			
Description	Firewall policy applied to traffic de	stined to prod app1 DB server VI	_AN hosts	
Туре	Distributed Firewall			
Enforcers				
Enforcer		Direction		
undefined - DB-PF	ROD-NET - VLAN: 102	Ingress		
				CANCEL BACK APPLY

The frontend web application server to backend database server policy configuration is now complete.

VM Microsegmentation

Microsegmentation enables the application of firewall policy between VM guests on the same hypervisor.

A PVLAN-based configuration forces all traffic from microsegmented VMs to the upstream CX 10000 switch for firewall policy inspection. Without the PVLAN setup, a hypervisor forwards traffic directly between hosts in the same VLAN. Egress and ingress policy can be applied.

The following diagram illustrates the networking components used to support a microsegmentation policy:



Figure 7: Microsegmentation Policy Diagram

In this procedure, egress firewall policy is applied between two VMs on the same ESXi host. Egress policy brings all traffic initiated by hosts in the VLAN into scope for policy rule creation.

AFC is used to create a virtual distributed switch (vDS) and microsegmentation PVLAN in vSphere. A corresponding PVLAN structure is created on CX 10000 switches attached to the ESXi host. An SVI is created with proxy ARP on the primary PVLAN to allow proxied communication between VMs placed in an isolated PVLAN, and a firewall policy is applied to the primary PVLAN *Network* to specify allowed traffic between hosts in the isolated PVLAN. In this example implementation, the microsegmentation is created across multiple CX 10000 switches.

The AFC microsegmentation workflow uses a series of wizards to complete microsegmentation set-up in a single fluid process. In addition to creating some of the vCenter configuration, the following related config components can be modified within the same workflow:

- PSM Network definition for the primary PVLAN
- VLAN SVI for the primary PVLAN
- CX 10000 MC-LAG configuration
- Policy endpoint groups
- Policy applications and service qualifiers
- Policy rules
- Firewall policy
- vCenter vDS and virtual port groups
- vCenter LAG/LACP configuration
- Assignment of distributed port groups to vCenter VMs

Configure Policy Applications

Applications in AFC provide an administrator the flexibility to bundle multiple service qualifiers together into a set of protocols. The definition can represent a broad set of requirements for an application or logically group any collective set of protocols together for firewall or ACL policy purposes.

The following procedure defines an application that represents a set of network services that must be reachable from the microsegmented data center hosts.

Step 1 In the AFC left navigation pane, click **Applications**.

aruba Fabric Composer	Dasl
Policy Groups	
Policies	
F. Rules	
Fe Endpoint Groups	
Applications	
Service Qualifiers	
Hicrosegmentation	
🚔 Firewall Log	
Firewall Profiles	
PSM Alerts	

Step 2 Click the right ACTIONS menu and select Add.

Configuration / Policy / Applications							
		⊘ Name	Rules	11	Service	Add	
		Enter Regex for Name	Enter Regex for Rules		Enter R	Edit	
		AH	'		proto: ah,	Delete	
		ALL_ICMP			icmp		
		ALL_TCP			all_tcp		

Step 3 On the Name page, enter a Name and Description, then click NEXT.

H Applica	ation			×
	Name	Service Qualifiers	ALG Settings	Summary
Enter a require	d Name and an optio	nal Description.		
Name *	Base-N	et-Services		
	Any non-em	oty string, example: Application-1		
Description	Support	ing network services for DC hosts		
	Example: Ap	plication-1 Description		
(* = Require	ed)			CANCEL BACK NEXT

Step 4 On the **Service Qualifiers** page, begin to enter the name of a service qualifier. A list of matching qualifiers is displayed. Press TAB or ENTER when a selection is highlighted to autocomplete the entry, or click the qualifier name in the list. Continue selecting service qualifiers until the following selections appear in the **Qualifiers** field, then click **NEXT**.

- syslog
- dns
- ntp
- radius_auth_udp
- radius_acct_udp
- Idaps

器 Application			×
Name	Service Qualifiers	ALG Settings	Summary
Select Service Qualifer(s)	to be applied to this Application		
Qualifiers	× syslog × dns × ntp × radius_auth_udp	× radius_acct_udp × Idaps	ADD
(* = Required)			CANCEL BACK NEXT

NOTE:

If a predefined service qualifier does not exist for the desired protocol and port combination, click **ADD** to create a new service qualifier.

Step 5 On the ALG Settings page, leave Type set to the default value of None and click NEXT.

H Application				×
	\bigcirc		?	
Name Set an optional Applicat	Service Qualifiers	ALG Settings	Summary	
Туре	None			× •
([*] = Required)			CANCEL BACK	NEXT

Step 6 On the **Summary** page, verify that all information is correct and click **APPLY**.

器 Application				×
Name	Service Qualifiers	ALG Settings	Summary	
Name	Base-Net-Services			
Description	Supporting network services for I	DC hosts		
Qualifiers	dns			
	ldaps			
	ntp			
	radius_acct_udp			
	radius_auth_udp			
	syslog			
			CANCEL BACK APPLY	

Configure Microsegmentation Rules

Using the procedure in the Configure Firewall Rules section, create the firewall rules below. The AFC Microsegmentation wizard supports rule creation as a part of its workflow. Predefining rules simplifies the microsegmentation process.

Name	Description	Type ActiorEndpoint Groups	Applications and Service Qualifiers
Allow-	Allow DC hosts to reach	Laye Allov Source : PROD-DC-VRF-	Applications:
Base-Net-	supporting network	3 Summary-EG Destination :	Base-Net-
Services	services	Network-Services-EG	Services

Name	Description	Type Actio	orEndpoint Groups	Applications and Service Qualifiers
Allow- MSEG1- HTTPS	Allow HTTPS between MSEG1 hosts	LayerAllov 3	v Source : rsvdc- vcenter.example.local_rsvdc: rsvdc- vcenter.example.local_rsvdc:	Service n QuglDisstination : https mseg1
Allow- MSEG1- SSH	Allow SSH/SCP between MSEG1 hosts	Laye Allov 3	Source : rsvdc- vcenter.example.local_rsvdc: rsvdc- vcenter.example.local_rsvdc:	Service Qualifiers: ssh :

NOTE:

Rules between microsegmented endpoints can be granular to an individual level. In the Allow-MSEG1 examples above, the same rule is applied to allow communication between the collective set of VMs assigned to the microsegmentation. It is best practice to apply policy to sets of hosts when possible to minimize the number of rules. In this example implementation, dynamic endpoint groups are used in microsegmentation firewall rules.

ESXi Microsegmentation Using AFC

Microsegmentation uses PSM firewall policy to filter traffic between VMs installed on the same hypervisor, when attached to a CX 10000 switch.

The AFC **Create Microsegmentation** workflow automates microsegmentation in a vSphere environment.

The workflow below can be used for a new ESXi host deployment or on an existing host. The ESXi host must have at least one available VNIC that is not currently assigned to a virtual switch. Only unassigned VNICs are displayed and available in the wizard. If unused VNICs are not available on the target ESXi host, microsegmentation can be created by running appropriate AFC wizards individually after configuring PVLANs in vCenter.

Step 1 On the **DISTRIBUTED SERVICES** tab of **Guided Setup**. Select **RSVDC-FB1/PROD-DC-VRF** in the **Selected VRF** field and click **CONFIGURE MICROSEGMENTATION**.



Step 2 On the Settings page, enter the following values to select an ESXi host, then click ADD.

- Name: MSEG1
- Host Addresses: < ESXi host target for microsegmentation >
- NICs: vmnic3 vmnic4

日 Distributed	Virtual Switch					×	
	?	?	?	?	?	?	
Settings	PVLAN	Fabric	LAGs	VRF	Policy	Summary	
Enter a required nam	ne and add one or mo	ore required Hosts a	nd NICs.		k		
Name *	MSEG1						
	Any non empty strin	g, example: DVS-1					
Host *	esxi-06.examp	ole.local				× -	
NICs *	× vmnic4 ×	vmnic5			× -	SELECT ALL	
CLEAR ADD							
Host		NICs					
	There is no data to display						
(* = Required)					CANCEL	BACK NEXT	

Step 3 Repeat the step above to assign additional ESXi hosts to the microsegmentation instance. All assigned ESXi hosts must be attached to a CX 10000 switch.

Step 4 Verify that all ESXi hosts were added to the list at the bottom of the dialogue box and click **NEXT**.

Ep. Distributed Virtual Switch								
Settings	? PVLAN	? Fabric	? LAGs	(?) VRF	Policy	Summary		
Enter a required name ar	Enter a required name and add one or more required Hosts and NICs.							
Name *	MSEG1							
	Any non empty string, exam	ole: DVS-1						
Host *	Select					-		
NICs *	Select				•	SELECT ALL		
CLEAR ADD								
Host		NICs						
esxi-06.example.local	ocal vmnic4,vmnic5 🛅					<u>ت</u>		
esxi-07.example.local	esxi-07.example.local vmnic3,vmnic4							
(* = Required) CANCEL BACK NEXT								

Step 5 On the **PVLAN** page, enter the following values. Next to **Isolated VLAN VNICs**, click **SELECT VNICS**.

- Portgroup Name Prefix: DPG
- Primary VLAN: 50
- Isolated VLAN: 51

☐ Distributed V	irtual Switch					×		
		?	?	?	?	?		
Settings	PVLAN	Fabric	LAGs	VRF	Policy	Summary		
Configure an optional P	ortgroup Name Pref	ix, Primary VLAN, ar	nd Isolated VLAN, an	d select up to 500 op	tional VNICs to be m	noved into the Portgroup.		
Portgroup Name	DPG							
Prefix	Any non empty string	, example: Portgroup-1						
Primary VLAN	50							
	A VLAN between 2 and 4094, example: 2.							
Primary VLAN VNICs	SELECT VNIC	S						
Isolated VLAN	51							
	A VLAN between 2 and 4094, example: 2.							
Isolated VLAN VNICs	SELECT VNIC	s						
([*] = Required)					CANCEL	BACK		

Step 6 Check the VM virtual network adapters to be assigned to the PVLAN distributed port group, then click **APPLY**.

耳 Select V	NICs			×
Select up to 500	VNICs.			⊙ ⊘ 🛛 🕸
	Name 1	IP Addresses	MAC Addresses	Virtual machine
	Enter Regex for Name	Enter Regex for IP Addresses.	Enter Regex for MAC Address	Enter Regex for Virtual n
	Network adapter 1	10.1.101.71	00:50:56:9e:48:ae	prod_web-10.1.101.71
	Network adapter 1	10.1.101.72	00:50:56:9e:a7:75	prod_web-10.1.101.72
	Network adapter 1	10.5.50.61	00:50:56:9e:27:11	mseg1-10.5.50.61
	Network adapter 1	10.5.50.62	00:50:56:9e:d8:23	mseg1-10.5.50.62
	Network adapter 1	10.5.50.71	00:50:56:9e:d2:b3	mseg1-10.5.50.71
	Network adapter 1	10.5.50.72	00:50:56:9e:a9:29	mseg1-10.5.50.72
	Network adapter 1	10.5.101.60	00:50:56:9e:38:f1	prod_web-10.5.101.60
	Network adapter 1	10.5.101.61	00:50:56:9e:bd:c4	prod_web-10.5.101.61
	Network adapter 1	10.5.101.62	00:50:56:9e:dc:a4	prod_web-10.5.101.62
	Network adapter 1	10.5.101.70	00:50:56:9f:a5:7b	prod_web-10.5.101.70
	Network adapter 1	10.5.102.60	00:50:56:9e:92:cd	prod_db-10.5.102.60
	· · · · · · · ·			
(1 - 18 of 18 total)	25 🗸			1
(* = Required)				CANCEL APPLY

NOTE:

Each column supports filtering and sorting to manage the displayed VNICs in large VM deployments.

Step 7 Verify that the number of Isolated VLAN NICs is correct, then click NEXT.

E3. Distributed Virtual Switch									
Settings	PVLAN	? Fabric	(?) LAGs	VRF	Policy	Summary			
Configure an optional Po	Configure an optional Portgroup Name Prefix, Primary VLAN, and Isolated VLAN, and select up to 500 optional VNICs to be moved into the Portgroup.								
Portgroup Name	DPG								
FIEIX	Any non empty string, example: Portgroup-1								
Primary VLAN 50									
	A VLAN between 2 and 4094, example: 2.								
Primary VLAN VNICs	SELECT VNIC	s							
Isolated VI AN	F1								
	51 A VLAN between 2 and 4094, example: 2.								
Isolated VLAN VNICs	SELECT VNIC	S 4 selected							
([*] = Required)					CANCEL	BACK			

Step 8 On the Fabric page, select the data center fabric and click NEXT.

E Distributed Virtual Switch							
Settings	PVLAN	Fabric	? LAGs	(?) VRF	Policy	Summary	
Select a Fabric. LAG	and VRF configura	ations will be applied	to the selected Fab	ric.			
Fabric	RSVDC-FB1					× •	
(* = Required)					CANCEL	BACK	EXT

Step 9 On the LAGs page, enter the following VM values. Next to Switch LAG, click ADD.

- vSphere LAG Name: MSEG1
- Host: < ESXi host >
- Host NICs: < VM NICs connected to switch MC-LAG >

耳. Distributed V	irtual Switch						×		
				?	?	?			
Settings	PVLAN	Fabric	LAGs	VRF	Policy	Sumn	nary		
Configure optional LAG	is/MLAGs on the vS	phere Distributed Switch	and Aruba Sw	itch Ports.					
vSphere LAG Name	a Name MSEG1								
	Any non empty string up to 12 characters long, example: VSphereLag								
Host	esxi-06.examp	ole.local				× •			
	Select a Host to cor	figure the LAG.							
Host NICs	× vmnic4: RSV	/DC-FB1-LF2-1 - 1/1/2 ×	vmnic5: RSVD0	C-FB1-LF2-2 - 1/1/2	l	× 🔻 Des	SELECT ALL		
	Select NIC Ports to	be configured on the LAG.							
Switch LAG	Select					- ADI			
CLEAR ADD									
Host	Ν	ICs	LA	AG					
(* = Required) Sc	roll for more optio	ns			CA	NCEL BACK	K NEXT		

Step 10 LAG wizard: On the **Settings** page, enter a **Name**, **Description**, and **LAG Number**. Click **NEXT**.

E Link Aggregation Group MSEG1-lag-esxi-06.example.local									
Settings	Ports LACP Settings VLANs Summary								
Enter a required Name	e and optional Description and LAG Number.								
Name *	MSEG1-ESXI-06								
	Any non empty string, example: LAG-1								
Description	MC-LAG for example microsegmentation of ESXI-06								
	Example: Link Aggregation Group 1								
LAG Number	11								
	A number between 1 and 256, example 1								
Inter-Switch Link	Inter-Switch Link								
(* = Required)	CANCEL BACK	NEXT							

Step 11 LAG wizard: On the **Ports** page, select the switch corresponding to the ESXi host, verify that ports are preselected correctly, and click **NEXT**.

Link Aggregation Group mseg1-lag-esxi-06.example.local								
Settings	Ports	CO LACP Settings	(?) VLANS	Summary				
Select ports to add to the L LAG.	AG. Up to 2 switches may be selected with up to 16	ports per switch. Removing a	switch will also remove all associated	LAG port members on the switch from the				
	LAG Switch Mem	ber × RSVDC-FB1-VSX_RSVI	DC-FB1-LF2-2_RSVDC-FB1-LF2-1 (RSVDC	C-FB1-LF2-1 / RSVDC-FB1-LF2-2)				
₩ ⊠ ~	🔗 Selected 🗞 Not Availa							
	Enabled Disabled No Transce	viver Filtered Port ha	us a health issue ●/● Link Up ● Lin	nk Down				
 ✓ RSVDC-FB1-LF2-1 1 3 5 5 7 6 2 3 5 7 6 	9 11 13 15 17 19 21 23	25 • 27 • 29 • 31 • 33	● 35 ● 37 ● 39 ● 41 ● 43 ● 45	• 47 ● 49 ● 51 ● ◆				
 2 ▲ 4 ▲ 6 ▲ 8 ▲ ✓ RSVDC-FB1-LF2-2 		26 • 28 • 30 • 32 • 34	● 36 ● 38 ● 40 ● 42 ● 44 ● 4e	♦ 48 50 52				
1 3 5 7 ⊗	9 11 13 15 17 19 21 23 10 12 14 15 18 20 22 24	25 • 27 • 29 • 31 • 33 26 • 28 • 30 • 32 • 34	35 37 39 41 43 45 36 38 40 42 44 46	47 49 51				
(* = Required) Scroll	for more options			CANCEL BACK NEXT				

Step 12 LAG wizard: On the LACP Settings page, leave settings at their defaults and click NEXT.

Em Link Aggregation Group mseg1-lag-esxi-06.example.local									? ×	
	Settings		Ports	L	ACP Settings		? VLANs		Summary	
Enable Z Ena	or disable LACP I able LACP Fallbac	Fallback for k	an MLAG anc	select a Switc	h entry to configu	re LACP se	ettings.			
	Switch	ĮΞ	Ports	↓ <u>≞</u>	LACP Mode	ΨĒ	LACP Interval	Ļ	Priority	μ <u>ε</u>
	RSVDC-FB1-LF2	2-1	1/1/2		Active		Slow		1	
	RSVDC-FB1-LF	2-2	1/1/2		Active		Slow		1	
LACP N	lode	Active								
LACP Ir	nterval	Slow								
Priority		1								
		A number bet	ween 1 and 6553	5, example 1						
(* = F	Required)						[CANCEL	ВАСК	NEXT

Step 13 LAG wizard: On the **VLANs** page, enter both primary and isolated VLAN IDs in the **VLANs** field, then click **NEXT**.

Link Aggregation Group mseg1-lag-esxi-06.example.local								
				?				
Settings	Ports	LACP Settings	VLANs	Summary				
Assign Native VLAN, \	/LANs, VLAN Groups, and PVLA	N Port Type to the LAG. At least	one VLAN must be configu	ured for an MLAG.				
Native VLAN	1							
	A VLAN between 0 and 4094, examp	ole: 1. Empty or 0 disables the Native VL	AN.					
VLANS	50-51							
	'All' for all VLANs or a number, set, o	r range of VLANs between 1 and 4094,	example: 5, 10-45, 102.					
VLAN Group	Select				-			
PVLAN Port Type	There are no PVLANs confi	gured on the selected switch(es						
(* = Required)			C/	NNCEL BACK N	ЕХТ			

Step 14 LAG wizard: On the **Summary** page, verify that all information is correct and click **APPLY**. The wizard closes and returns to the main **Distributed Virtual Switch** workflow.

E Link Aggregati	Em Link Aggregation Group MSEG1-lag-esxi-06.example.local								? ×
Settings		Ports		LACP Settings	6	VLANs		Summary	
Name	Jame MSEG1-ESXI-06								
Description	Description MC-LAG for example microsegmentation of ESXI-06								
LAG Number			11						
Туре			Provisioned						
Native VLAN			1						
VLANs			50-51						
VLAN Groups									
PVLAN Port Type									
Enable LACP Fallback			Yes						
Switch	1E	Ports	μE	LACP Mode	J≞	LACP Interval	μE	Priority	μE
RSVDC-FB1-LF2-1		1/1/2		Active		Slow		1	
RSVDC-FB1-LF2-2		1/1/2		Active		Slow		1	
							CANCEL	ВАСК	APPLY

Step 15 On the **LAGs** page, in the lower left, click **ADD**.

☐ Distributed '	타 Distributed Virtual Switch									
			?	?	?					
Settings Configure optional LA	Configure optional LAGs/MLAGs on the vSphere Distributed Switch and Aruba Switch Ports.									
Host	esxi-06.example.local									
	Select a Host to configure the LAG.									
Host NICs	× vmnic4: RSVDC-FB1-LF2-1	- 1/1/2 × vmnic5: RSVDC	-FB1-LF2-2 - 1/1/2	× -	DESELECT					
	Select NIC Ports to be configured on	the LAG.			ALL					
Switch LAG	MSEG1-ESXi6			× •	ADD					
CLEAR ADD										
Host	NICs	LAG								
	1	There is no data to c	lisplay	1						
(* = Required)				CANCEL	BACK NEXT					

Step 16 Repeat steps 9–15 to create additional MC-LAGs for each VM included in the microsegmentation, then click **NEXT**.

다. Distributed Virtual Switch ×										
Settings	PVLAN	Fabric	LAGs	VRF	Policy	Summary				
Configure optional LAC	Configure optional LAGs/MLAGs on the vSphere Distributed Switch and Aruba Switch Ports.									
Host	Select 👻									
	Select a Host to configure the LAG.									
Host NICs	Select 👻 SELECT ALL									
	Oalaat NIIO Davta ta ba	and an the LAC								
CLEAR ADD						I				
Host	NICs		LAG							
esxi-06.example.local	vmnic	4	MSEC	G1-ESXI-06		団				
	vmnic	5								
esxi-07.example.local	vmnic	3	MSEC	G1-ESXI-07		Ш				
	vmnic	4								
(* = Required) S	croll for more option	S			CANCEL	BACK				

Step 17 On the **VRF** page, select the VRF, then click **ADD** on the **Network** field to launch the **Network** wizard.

타 Distributed Vir	tual Switch						×
					?	?	
Settings	PVLAN	Fabric	LAGs	VRF	Policy	Summary	
Select or add an optional	VRF, Network, and SV	I to be associated	with the DVS and F	Portgroup.			
VRF	PROD-DC-VRF					× •	ADD
Network	Select					-	ADD
SVI							ADD
Disable ICMP Redirec	t on all switches within	the selected Fab	ric.				
(* = Required)					CANCEL	BACK	NEXT

Step 18 Network wizard: On the Name page, enter a Name and Description, then click NEXT.

昂 Network			×
	\bigcirc	?	?
Enter a required N	Name ame and an optional Description	Settings	Summary
Name *	MSEG1-PROD-NET		
	Any non-empty string, exampl	e: Network-1	
Description	PSM Network object f	or MSEG1 VLAN	
	Example: Network-1 Description	on	
(* = Required)			CANCEL BACK NEXT

Step 19 Network wizard: On the **Settings** page, review the auto-selected primary PVLAN value and click **NEXT**.

昂 Network			×
Na	ne	Settings	Summary
Set the required VLAN.			
VLAN *	50 A VLAN between 1 and 4094, example: 1.		
(* = Required)			CANCEL BACK NEXT
NOTE:			
When creating	a PSM Network within th	he microsegmentation wo	orkflow, the VLAN is automati-

cally set to the primary PVLAN ID. This value cannot be modified. If a different VLAN ID is present, click **CANCEL** to exit the **Network** wizard, and click **BACK** to the **PVLANs** page for review.

Step 20 Network wizard: On the **Summary** page, verify that the settings are correct and click **APPLY**. The wizard closes and returns to the main **Distributed Virtual Switch** workflow.

恳 Network		×
Name	Settings	Summary
Name	MSEG 1-PROD-NET	
Description	PSM Network object for MSEG1 VLAN	
VLAN	50	
		CANCEL BACK APPLY

Step 21 Verify that the new PSM *Network* is populated in the **Network Field**, then click **ADD** on the **SVI** field to launch the **IP Interface** wizard.

Distributed Vir	tual Switch			×
Settings	PVLAN Fabric LAGs VRF	Policy	? Summary	
Select or add an optional	VRF, Network, and SVI to be associated with the DVS and Portgroup.			
VRF	PROD-DC-VRF		× •	ADD
Network	MSEG1-PROD-NET (50)		× •	ADD
SVI	Select			ADD
Disable ICMP Redirec	on all switches within the selected Fabric.			
(* = Required)		CANCEL	BACK	NEXT

Step 22 IP Interface wizard: On the **Interface Type** page, review the auto-populated values for **Type**, **VLAN**, and **Enable Local Proxy ARP** fields. Enter the following values, then click **NEXT**.

- Switches: < CX 10000 switches attached to the ESXi microsegmentation >
- IPv4 Subnetwork Address: 10.5.50.0/24
- IPv4 Addresses: 10.5.50.1
- Active Gateway IP Address: 10.5.50.1
- Active Gateway IP MAC Address: 02:00:0A:05:00:01

IP Interface		? ×
Interfa	ce Type Name Summary	
Select the IP Interface Ty	ype and set the appropriate attributes.	
Enable this IP Interfa	ce	
Туре	SVI	~
VLAN *	50	
	A VLAN between 1 and 4094, example: 1.	
Switches *	× RSVDC-FB1-LF2-2 × RSVDC-FB1-LF2-1 × RSVDC-FB1-LF3-1 × RSVDC-FB1-LF3-2 × SELECT ALL	1
IPv4 Subnetwork	10.5.50.0/24	
Address	A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24	
IPv4 Addresses *	10.5.50.1	
	Enter a range of IPv4 Addresses to be assigned to the selected switches, example: 192.168.1.100-192.168.1.200. The range must include at least 4 address or match the Active Gateway IP Address.	ses
Active Gateway IP	10.5.50.1	
Address *	A valid IPv4 Address, example: 192.168.1.10. Both Active Gateway values must be defined if using Active Gateway.	
Active Gateway MAC	02:00:0A:05:00:01	
Address *	A valid MAC Address, example: 00:00:00:00:00:00:01. Cannot include multicast or broadcast addresses Both Active Gateway values must be defined if using A Gateway.	Active
Enable VSX Shutdow	n on Split	
Enable Local Proxy A	NRP	
(* = Required) Scr	roll for more options CANCEL BACK NEX	ст
NOTE:		
Enable Local	Proxy ARP is checked by the wizard and cannot be modified. Proxy ARP is requi	red

to enable communication between VMs assigned to the same isolated PVLAN.

Step 23 IP Interface wizard: On the Name page, enter a Name and Description, then click NEXT.

IP Interface	ce	Ø ×			
In	terface Type Name	Summary			
Enter an optional N	lame and Description.				
Name	MSEG1-V50-PROD-DC				
	A string, up to 42 characters. example: IpInterface1				
Description	Example microsegmentation SVI				
	Example: My New IP Interface				
(* = Required)		CANCEL BACK NEXT			

Step 24 IP Interface wizard: On the **Summary** page, verify that all information is correct, then click **APPLY**. The wizard closes and returns to the main **Distributed Virtual Switch** workflow.

Interface Type	Name	Summary
Name	MSEG1-V50-PROD-DC	
Description	Example microsegmentation SVI	
Гуре	SVI	
Enabled	Yes	
/LAN	50	
Switches	RSVDC-FB1-LF2-1, RSVDC-FB1-LF2-2, RSVDC-F	B1-LF3-1, RSVDC-FB1-LF3-2
Active Gateway IP Address	10.5.50.1	
Active Gateway MAC Address	02:00:0A:05:00:01	
Pv4 Addresses	10.5.50.1	
/SX Shutdown on Split	No	
Local Proxy ARP Enabled	Yes	
		CANCEL BACK APPL

Step 25 Verify that the new SVI was populated in the SVI field and click NEXT to proceed.

타. Distributed Vir	tual Switch					×
Settings	PVLAN Fabric	LAGs	VRF	Policy	Summary	
Select or add an optional	VRF, Network, and SVI to be a	ssociated with the DVS an	d Portgroup.			
VRF	PROD-DC-VRF				× -	ADD
Network	MSEG1-PROD-NET (50)				× •	ADD
SVI	MSEG1-V50-PROD-DC - 10.5.5	0.1/24 (50)				ADD
Disable ICMP Redirect	on all switches within the sele	cted Fabric.				
(* = Required)				CANCEL	ВАСК	NEXT

Step 26 On the **Policy** page, click **ADD** in the **Policies** field to start the **Policy** wizard.

臣 Distributed	Virtual Switch						×
Settings	PVLAN	Fabric	LAGs	VRF	Policy	Summary	
Configure an optiona	I Policy if a Network	is selected.					
Policies	Select						ADD
(* = Required)					CANCEL	BACK	NEXT

Step 27 Policy wizard: On the Name page, enter a Name and Description, then click NEXT.

Policy					×
Name	Settings	Rules	Enforcers	? Summary	
Enter a required Nam	e and an optional Description.				
Name *	From-MSEG1				
	Any non-empty string without spaces, e	xample: Policy-1			
Description	Egress PSM policy for MSEG	1 microsegmented hosts			
	Example: Policy-1 Description				
(* = Required)			C/	ANCEL BACK NEX	т

Step 28 Policy wizard: On the **Settings** page, verify that the prepopulated **Type** field value is set to *Distributed Firewall* and click **NEXT**.

Policy					×
	\bigcirc	?	?	?	
Name Select a required type. Th	Settings	Rules applicable Rules and Enfor	Enforcers	Summary	
Туре	Distributed Firewall				
([*] = Required)			CAN	ICEL BACK N	EXT

Step 29 Policy wizard: Click ACTIONS, then select Add > Existing.

Policy	Settings	Rules	(?	Summary
t one or more R	ules on the Policy. Rules may be e	enabled/disabled and reo	rdered for this Pol	icy.	Caninary
) 🚫 🌄 🗱 ACTIONS 🗸
	Sequence	Enabled	Name Enter Regex (New Existing	ACTIONS ~

Step 30 Policy wizard. In the **Select Rules** window, select the checkbox for existing rules in the following order, and click **APPLY**.

- Allow-MSEG1-HTTPS
- Allow-MSEG1-SSH
- Allow-Base-Net-Services
- Allow-All-ICMP
- Allow-All-UDP-Traceroute

🛐 Se	elect Rules				\$
Select or 5 selecte	ne or more Rules to add to the Polic	:y.			
-	Name	Shared ↓ <u>⊥</u> S ▼	Source Endpoint Groups	Source Endpoint G 1	Destination Endpoint Gr 1
	Allow-Admins-to-PROD-DC-VRF	No	Campus-Admins-EG	10.254.1.0/24	PROD-DC-VRF-Summary-EG
	Allow-All-ICMP	No	All-Hosts-EG	0.0.0/0	All-Hosts-EG
~	Allow-All-UDP-Traceroute	No	All-Hosts-EG	0.0.0/0	All-Hosts-EG
	Allow-Base-Net-Services	No	PROD-DC-VRF-Summary-EG	10.5.0.0/16	Network-Services-EG
	Allow-MSEG1-HTTPS	No	rsvdc- vcenter.example.local_rsvdc: mseg1	10.5.50.61 10.5.50.62 10.5.50.71 10.5.50.72	rsvdc- vcenter.example.local_rsvdc: mseg1
	Allow-MSEG1-SSH	No	rsvdc- vcenter.example.local_rsvdc: mseg1	10.5.50.61 10.5.50.62 10.5.50.71 10.5.50.72	rsvdc- vcenter.example.local_rsvdc: mseg1
= Require	ld)				CANCEL APPLY

Step 31 Policy wizard: Verify the rule order matches requirements, then click NEXT.

		Name		Setting	gs Rules	Enforcers	Summary
Set one or more Rules on the Policy. Rules may be enabled/disabled and reordered for this Policy.							
			Sequence	Enabled	Name	Source Endpoint Groups	Source Endpoint Group IPv4
			Enter F	S ▼	Enter Regex for Name	Enter Regex for Source I	Enter Regex for Source En
	\downarrow		1		Allow-MSEG1-HTTPS	rsvdc-	10.5.50.61
						vcenter.example.local_rsvdc:	10.5.50.62
						mseg1	10.5.50.71
							10.5.50.72
¢	\downarrow		2		Allow-MSEG1-SSH	rsvdc- vcenter.example.local_rsvdc: mseg1	10.5.50.61 10.5.50.62 10.5.50.71 10.5.50.72
¢	\downarrow		3		Allow-Base-Net-Services	PROD-DC-VRF-Summary-EG	10.5.0.0/16
\uparrow	\downarrow		4		Allow-All-ICMP	All-Hosts-EG	0.0.0.0/0
↑	\downarrow		5		Allow-All-UDP-Traceroute	All-Hosts-EG	0.0.0/0
1 -	5 of 5	i total)	25 🗸				1

Step 32 Policy wizard: On the **Enforcers** page, verify the pre-populated egress enforcer is listed, then click **NEXT**.

Policy							×
						?	
Name	Settings	Ru	les	Enforce	rs	Summary	
Specify direction and	VRFs or individual netwo	rks within a VRF on wl	hich to apply t	he Policy.			
Fabric	Select					~	
Direction	Select					~	
VRF	Select						
Networks	Select						ADD
CLEAR ADD							
Enforcer		Direction					
undefined - MSEG1-P	ROD-NET - VLAN: 50	Egress				茴	
(* = Required)					CANCEL	BACK	NEXT
NOTE:							
Policy directionall hosts are a	on and design val ttached to CX 10 gress policy is p	ry based on red 000 switches, referred, the p	quiremen egress po re-popula	ts and adm blicy is reco	ninistrator p mmended enforcer c	preferences to filter eas	. When st-west

clicking the **trash can** icon.

Step 33 Policy wizard: On the **Summary** page, verify that all information is correct, then click **APPLY**. The **Policy** wizard closes, returning to the main **Distributed Virtual Switch** workflow.

Policy				:		
Name	Settings	Rules	Enforcers	Summary		
Name	From-MSEG1	i taloo		cannary		
Description Egress policy for MSEG1 microsegmented hosts						
Туре	Distributed Firewall					
Enforcers						
Enforcer		Direction				
undefined - MSEG1-PR	OD-NET - VLAN: 50	Egress				
			CAN	ICEL BACK APPLY		

Step 34 On the **Policy** page, verify that the newly created policy is populated in the **Policies** field, then click **NEXT**.

E. Distributed	Virtual Switch	I				×
Settings		Fabric	VBF	Policy	Summary	
Configure an optiona	I Policy if a Network	is selected.		,		
Policies	× From-MSEC	G1			× •	ADD
(* = Required)				CANCEL	BACK	EXT

Step 35 On the **Summary** page, verify that all information is correct, then click **APPLY**.

E Distributed Virtual Sv	vitch			×
Settings PVLAN	Fabric LAG	s VRF	Policy	Summary
Name Portgroup Name Prefix Primary VLAN Primary VLAN VNICs Isolated VLAN Isolated VLAN VNICs LAGs VRF	MSEG1 DPG 50 51 Network adapter 1,Network ada MSEG1-ESXI-06,MSEG1-ESXI-00 PROD-DC-VRF MSEG1-V50-PROD-DC	pter 1,Network adapter 1,Ne 7	twork adapter 1	
Policies	No From-MSEG1			
Host		NICs		
esxi-06.example.local		vmnic4,vmnic5		
esxi-07.example.local		vmnic3,vmnic4		
			CANCEL	BACK APPLY

At the completion of this step, AFC creates the PVLAN and LAG/LACP configuration on all included ESXi hosts and the MC-LAGs on uplink ToR switches.

Add the Primary PVLAN to the EVPN

The primary PVLAN is added to the EVPN config to advertise reachability of the microsegmented hosts in the fabric. A microsegmentation can exist in a single rack or multiple racks in the fabric.

Step 1 On the Configuration menu, select Routing > EVPN.

a	Tubo Fabric Composer	Dashboard	I Config	uration 🐱	Maintena	ance 🗸	Visualization 🐱	Я v	/here can
Ŀ Ê E	Policy Groups			Ports	>				
		Co	nf 📀	Routing	>	-	VRF		
	Policies		모	System	>	٩	BGP		
Ē,	Rules		昂	Network	>	\sim	OSPF		
L.	Endpoint Groups		¢°	Administratio	on >	÷	EVPN		osts
' म			Ē	Integrations	>	Ŧ	EVPN VXLAN Multi-F	abric	al
	Applications		38	Policy	>		esxi-07.ex	ample.lo	cal
41 1 - 1 1 - 1	Service Qualifiers					1		,	

Step 2 To modify the EVPN configuration, click the right ACTIONS menu and select Add.

Configuration ,	/ Routing / EVPN				
		Fabric RSVDC-FB1			
EVPN	EVPN MULTI SITE				
				$\bigcirc \bigcirc$	C ACTIONS V
	I Name ↓≟	Switch Name	VLAN JE	L2VNI	Add
	Enter Name	Enter Switch Name	Enter Regex for VLAN	Enter Re	Edit
	DC-EVPN-RSVDC-FB1-LF1-1-101	RSVDC-FB1-LF1-1	101	10101	Delete
	DC-EVPN-RSVDC-FB1-LF1-2-101	RSVDC-FB1-LF1-2	101	10101	VLAN
	DC-EVPN-RSVDC-FB1-LF2-1-101	RSVDC-FB1-LF2-1	101	10101	Import Route Targets
	DC-EVPN-RSVDC-FB1-LF2-2-101	RSVDC-FB1-LF2-2	101	10101	Export Route Targets
	DC-EVPN-RSVDC-FB1-LF3-1-101	RSVDC-FB1-LF3-1	101	10101	Redistribute Host Route
	DC-EVPN-RSVDC-FB1-LF3-2-101	RSVDC-FB1-LF3-2	101	10101	Settings
	DC-EVPN-RSVDC-FB1-LF1-1-102	RSVDC-FB1-LF1-1	102	10102	Reapply EVPN
	DC-EVPN-RSVDC-FB1-LF1-2-102	RSVDC-FB1-LF1-2	102	10102	auto

Step 3 On the Introduction page, read the configuration note and click NEXT.

몇 EVPN(RSVD	C-FB1)					? ×
Introduction	Switches	R Name	(?) VNI Mapping	Settings	Summary	
This configuration will be The EVPN EVIs will not b	used to generate multi e active until after an Ur	ole EVPN instances, or nderlay and Overlay ha	ne for each VLAN included as been configured on the	d in the VNI Mapping s e default VRF.	tep.	
(* = Required)				CANCE	BACK	NEXT

Step 4 On the **Switches** page, unselect the **Create EVPN instance across the entire Fabric and all Switches contained within it** checkbox. Specify all DSS switches connected to the PVLAN microsegmentation, then click **NEXT**.

몇 EVPN(RSVDC	C-FB1)				⑦ ×
Introduction	Switches	? Name	(?) VNI Mapping	Settings	Summary
Create EVPN instances a	across the entire Fabric	or select specific Swi	tches.		
Create EVPN instance	es across the entire Fab	oric and all Leaf and E	Border Leaf Switches conta	ained within it.	
Switches *	× RSVDC-FB1-VSX_F × RSVDC-FB1-VSX_F	RSVDC-FB1-LF2-2_RSVI	DC-FB1-LF2-1 (RSVDC-FB1-I DC-FB1-LF3-1 (RSVDC-FB1-I	LF2-1 / RSVDC-FB1-LF2-2	2) SELECT ALL
(* = Required)				CANCE	BACK NEXT

Step 5 On the **Name** page, enter the **Name Prefix** previously used to create an EVPN map and click **NEXT**.

몋 EVPN(RS\	/DC-FB1)					? ×
Introduction	Switches ne Prefix and an optional D	Name escription.	(?) VNI Mapping	Settings	Summary	
Name Prefix * Description	DC-EVPN Any non empty string, exam Example: Evpn-mapping De	iple: Evpn-mapping escription				
([*] = Required)				CANCE	BACK	NEXT
NOTE:						
It is best prac	ctice to use the sa	ıme prefix valı	ue for all EVPN co	onfiguration wi	thin a single f	fabric.

Step 6 On the **VNI Mapping** page, the previously used value for **Base L2VNI** is autopopulated. Enter the microsegmentation primary PVLAN in the **VLANs** field, then click **NEXT**.

EVPN(RSVDC-FB1)								
Introduction	Switches	Name	VNI Mapping	Settings	Summary			
VLANs *	50 A number, set, or range of VI	LANs between 2 and 4094	4, example: 5, 10-45, 102.					
Base L2VNI *	10000 A number between 0 and 16	777214, example 0. Comj	puted VLAN + VNI cannot exceed	16777214.				
(* = Required)				CANCE	L BACK NEXT			

Step 7 On the **Settings** page, the previously used MAC resource pool is autopopulated in the **MAC Address Resource Pool** field. Specify *AUTO* as the **Route Target Type** and click **NEXT**.

몇 EVPN(RSVDC-FB1)				? ×
Introduction	Switches Name	VNI Mapping	Settings	Summary	
Set the Virtual MAC Address Rar	ge. Select or add a MAC Address I	Resource Pool or specify a range.			
MAC Address Resource Pool *	EVPN-FB1-SYSTEM-MAG	C (02:00:01:00:00:03-02:00:01:00:0	00:ff)	× •	ADD
MAC Address Range					
	A hyphen-separated range of vali	d MAC Addresses, example: 02:00:00:00:00	2:00-02:00:00:00:02:FF. Cannot i	include multicast addresses.	
Set the required Route Target Typ	be and associated values. The Rout	e Target Type determines the form	at of the route targets gen	erated.	
Route Target Type *	AUTO				× •
	'AUTO' is recommended only who	en an iBGP Overlay is configured.			
(* = Required)			CANG	CEL BACK NE	кт

Step 8 On the **Summary** page, verify that all values are correct and click **APPLY**.

₽ EVPN(RSVDC-FB1)					? ×
Introduction	Switches	Name	VNI Mapping	Settings	Summary	
Switches	RSVDC-FB1- RSVDC-FB1-	/SX_RSVDC-FB1-LF2 /SX_RSVDC-FB1-LF3	-2_RSVDC-FB1-LF2-1 (RSVI -1_RSVDC-FB1-LF3-2 (RSVI	DC-FB1-LF2-1 / RSVDC- DC-FB1-LF3-1 / RSVDC-	FB1-LF2-2) FB1-LF3-2)	
Name Prefix	DC-EVPN					
Description						
VLANs	50					
Base L2VNI	10000					
Route Target Type	AUTO					
MAC Address Resource Pool	EVPN-FB1-SY	STEM-MAC (02:00:0	1:00:00:03-02:00:01:00:00:ff))		
				CANC	EL BACK A	PPLY

Externally Advertise Microsegmented Networks

During the AFC EVPN-VXLAN creation, BGP was enabled for the PROD-DC VRF. AFC configures redistribution of connected interfaces for all leaf switches where the VRF is configured, when BGP is enabled. This configuration installs the primary PVLAN SVI prefix into BGP, which facilities the advertisement of the primary PVLAN network to campus and other fabrics without the need for additional steps.

Verify Policy in PSM

AFC policy is pushed to AMD Pensando's PSM, which installs the policy on CX 10000 DPUs.

Verify Networks

Step 1 On PSM, expand Tenants in the left pane and click Networks.



Step 2 Verify that the PSM Networks displayed have the correct ingress and egress policies applied.

Netw	orks									ADD NETWO	RK
🔆 Networks Overview											
	Network	s (3)					10 Columns 🗸	\$	Search	Aa Ab R* Q	× ®,
	Name	VRF	VLAN	Ingress Policy	Egress Policy	Maximun CPS	Maximum Sessions	Labels	Propagation Status	Modification Time	\checkmark
	MSEG1-PROD	PROD-DC	50		From-MSEG1	Inherited	Inherited from VRF		Propagation Complet	2023-10-29 01:24:39	GMT
	DB-PROD-NE	PROD-DC	102	To-PROD-DB-Servers		Inherited	Inherited from VRF		Propagation Complet	2023-10-28 22:02:20	GMT
	WEB-PROD-N	PROD-DC	101			Inherited	Inherited from VRF		Propagation Complet	2023-10-28 22:02:19	GMT
N	DTE:										

Each defined *Network* should display "Propagation Complete" in the **Propagation Status** column, indicating that all CX 10000 switches have installed the displayed policy.

Step 3 To view a complete list of policies, on the left navigation menu, click **Security Policies**.



Step 4 Review the list of policies. To view the rules included in a policy, click a policy name.

Secu	irity Policies							Table View 🥆	ADD SECURITY POLICY
G Security Policies									
Ħ	Security Policies	(2)					9 Columns	s 🗸 🏟 Search	Aa Ab R* Q 🗸 🗞
	Policy Name	Policy/Rule Entries Consumed per DSS	Associated Networks (Ingress Policy)	Associated Networks (Egress Policy)	Associated VRFs (Ingress Policy)	Associated VRFs (Egress Policy)	Propagatic Status	Creation Time	Modification Time ψ
	To-PROD-DB-Servers	View Details	DB-PROD-NET				Propag	2023-03-07 17:43:33 GMT+00:00	2023-03-08 00:23:47 GMT+00:00
	From-MSEG1	View Details		MSEG1-PROD-NET			Propag	2023-03-08 00:09:10 GMT+00:00	2023-03-08 00:23:47 GMT+00:00

Step 5 To view the full text of a rule in the displayed rule set, mouse-over a rule in the list.

Security Policies > To-PROD-DB-Servers				CLONE POLICY	COMPARE CLONED POLICY				
🕞 Security Policy									
Security Policy Details					^				
Policy Name: To-PROD-DB-Servers 🌶									
Tenant: default Attach-tenant: true Creade on: 202 - 30-30 07.14.33.3 GMT-00.00 Last Modified: 202 - 30-30 00.23.47 GMT-00.00 Ingress Policy for VRFs: Egress Policy for Metworks: Egress Policy for Metworks: Ingress Policy for VRFs: Propagation: Egress Policy for Networks: Propagation: Propagation: Egress Policy for Networks: Policy/Hule Enrine: Steveets Egress Policy for Networks:									
		± + ∎ ××							
E Policy Rules (4) Search: Rule Name Source IP/Workload Group	Destination IP/Workload Gro	oup <protocol>/<port> App × V Action</port></protocol>	$\times \vee$		10 Columns 🗸				
□ ∨ Number Rule Name Sources	Destinations Action	Protocol Port Applications	Description	Status Tot	al Connection Hits				
To PROD DB Servers. Allow PROD WEB to IPs: 10.5.101.50, 10.5.101.60, 1 -DB MSSQL 0.5.101.70	IPs: 10.5.102.60, 10.5.102.70, 1 Permit 0.5.102.71	tcp/1433, tcp/22	Allow MSSQL traffic from prod web fronte nd to backend DB servers	Enabled RS ¹ RS ¹ RS ¹ RS ¹	VDC-FB1-LF2-2 DSM 1/1: 1 VDC-FB1-LF2-2 DSM 1/2: 0 VDC-FB1-LF2-1 DSM 1/1: 1 VDC-FB1-LF2-1 DSM 1/1: 0 VDC-FB1-LF2-1 DSM 1/2: 0				
E C 2 To-PROD-DB-ServersAllow-Admins-to-PRO IPs: 10.254.1.0/24	IPs: 10.5.0.0/16 Permit	any	Allow campus admin net hosts to production	c Enabled					
To-PROD-DB-ServersAllow-All-ICMP IPs: 0.0.0.0/0	IPs: 0.0.0.0/0 Permit	icmp	Allow ICMP from all hosts to all hosts	Enabled RS ¹	VDC-FB1-LF2-2 DSM 1/1: 2 RSVDC-FB				
To-PROD-DB-ServersAllow-All-UDP-Tracerc IPs: 0.0.0.0/0	IPs: 0.0.0.0/0 Permit	udp/33434-33535	Allow UDP-based traceroute from all hosts	Enabled					

AFC Multifabric Configuration

Combining multiple EVPN fabrics into a single overlay allows sharing Layer 2 and Layer 3 reachability between data center pods at the same site as well as more distant data center locations.

Developing an effective multifabric strategy supports growth, location diversity, and disaster recovery. Aruba Fabric Composer (AFC) can simplify the configuration process and automate building a multifabric EVPN-VXLAN overlay.

Multiple data center fabrics and locations can be combined into a single overlay topology. This guide focuses on the common usage of combining two data center locations.

Additional considerations are required when adding three or more fabrics or when multiple fabrics are present at a single site which co-exist with fabrics at remote locations. Details on supporting these configurations can be found in the *AOS-CX EVPN VXLAN Guide* in the Aruba Support Portal.

The primary data center fabric in this guide is named RSVDC-FB1, which was previously created. The new fabric established in a colocation facility is named RSVCO-FB2.

Second Fabric Guidance

Use the process outlined in the AFC EVPN-VXLAN Configuration guide to create a second fabric. The same AFC instance can be used to build the new fabric, if IP connectivity can be established between AFC and the new fabric location with a latency of 50 ms or less. A second AFC instance can be deployed and linked to the first instance, if latency exceeds this value.

The diagram below illustrates the physical topology of the second fabric used in this guide. The new fabric is located at a colocation facility and identified as RSVCO-FB2.


The RSVCO-FB2 fabric uses unique IP numbering for loopbacks and VTEPs. The following IP ranges are used to build the second fabric.

Purpose	Description	Example
Leaf-Spine IP address block	An IPv4 address block used to create /31, point-to-point layer 3 links between leaf and spine switches.	10.255.4.0/
Routed loopback and VSX transit VLAN IP address block	An IPv4 address block used to allocate unique loopback addresses (/32) for each switch and transit-routed VLAN between redundant ToRs (/31)	10.250.3.0/
VTEP loopback IP address block	An IPv4 address block used to assign VTEP loopback addresses (/32) on VSX redundant ToRs	10.250.4.0/

The following network elements are logically contiguous between fabrics.

Network Element	Description
PROD-DC-VRF	A virtual routing and forwarding table defined for the data center production network.
VLAN 101	Production web server VLAN and SVI.
VLAN 102	Production database server VLAN and SVI.

VXLAN Data Plane Configuration

The PROD-DC-VRF is Layer 3, extended across the RSVDC and RSVCO data center fabrics. VLANs 101 and 102 are Layer 2, extended between the fabrics. To allow a contiguous overlay for network segments extended between fabrics, VXLAN VNI values in each data center must agree. The same L3 VXLAN VNI value for PROD-DC-VRF must be defined in both fabrics.

To assign the same L2 VXLAN VNIs to both fabrics, assign the same **Base L2VNI** value in the **EVPN CONFIGURATION** wizard.

Underlay WAN IP

Border leaf switches typically establish underlay route peerings between fabrics, but other switch members of a fabric can perform this function.

IP addresses must be assigned to WAN interfaces in both fabrics. When Layer 2 WAN services or dark fiber are used, IP addresses are assigned for peering directly between switches at each site. The following IP addresses are reserved for underlay interfaces connecting to the sample Layer2 metro Ethernet circuit: 10.255.6.0/29. When using Layer 3 WAN services, IP addresses are assigned to allow direct peering with the service provider.

Configure Multifabric Underlay Connectivity

A multifabric underlay serves the same purpose as the underlay within a single fabric. It shares IP loopbacks to enable MP-BGP EVPN peerings and VTEP reachability.

WAN Underlay Connectivity

Several methods can be used to establish connectivity between fabrics at different sites. Dark fiber and most metro Ethernet services support jumbo frame capabilities. Fragmentation of VXLAN encapsulated traffic is not supported. The WAN path between fabrics must accommodate an increase of 50 bytes in MTU over the encapsulated traffic. A WAN path MTU of 1600 is recommended.

This guide uses a Layer 2 metro Ethernet service with multi-port customer premise equipment (CPE). The border leaf switches for each fabric use a single physical connection to the CPE at their respective locations.

The diagram below illustrates the sample connectivity between data center locations. RSVDC Fabric 1 is the fabric created in the AFC EVPN-VXLAN Configuration guide. RSVCO Fabric 2 is the second fabric located in the colocation facility.



Improved WAN resiliency can be realized by using multiple CPE devices at each location, by provisioning a second metro Ethernet circuit, or by using multiple dark fiber links.

Assign WAN IP Addresses

A single IP subnet is used over the Layer 2 metro Ethernet service. IP addresses are assigned to physical switch interfaces. Routed interfaces are used to avoid Layer 2 loops.

Step 1 Select **Configuration > Routing > VRF** on the top menu.

C	rubo Fabric Composer	Dashboard	Configuratio	on 🗙 Ma	aintena	nce 🗸	Visualization	∽ 𝒫 wr
Pa	SWITCHES - ALL LOCAL FABRICS	×	Por	ts	>			
nels	Switches in Fabrics		🐼 Rou	ıting	>	÷	VRF	
			🖵 Sys	tem	>	٩	BGP	
			昂 Net	work	>	\sim	OSPF	
			🗳 Adn	ninistration	>	臣	EVPN	
	14		🗂 Inte	grations	>	₽	EVPN VXLAN N	lulti-Fabric
			😽 Poli	су	>	09	Route Policy	



Configuration / Routing / VRF		
Fabric	RSVDC-FB1	× 🔻
Name	↓≞ Туре	J≞ Switches J≞
Enter Name	Select Type	▼ Enter Switches
••• O default	Default	
C-VRF	User	RSVDC-FB1-LF1-1,RSVDC-FB1-
		LF1-2,RSVDC-FB1-LF2-1,RSVDC-
IP Static Routes		FB1-LF2-2,RSVDC-FB1-LF3-
Networks		1,RSVDC-FB1-LF3-2
Underlays	Management	
Overlays	User	RSVDC-FB1-LF1-1,RSVDC-FB1-
evenays		LF1-2,RSVDC-FB1-LF2-1,RSVDC-
ARP Tables		FB1-LF2-2,RSVDC-FB1-LF3-
IP Route Tables		1,RSVDC-FB1-LF3-2

Step 3 On the lower ACTIONS menu of the IP INTERFACES tab, select Add.

onfiguration / Rou	uting / VRF / defa	ult						
		Fabric	RSVDC-FI	31				
						$\bigcirc \bigcirc \bigtriangledown$	🕀 C АСТІ	ons 🗸
Name	1E.	Туре	Ļ	Switches	ĮΞ	L3 VNI	μ <u>ε</u>	Route Ta
Enter Name		Select Type	•	Enter Switches		Enter Regex for	L3 VNI	Enter F
default		Default						
IP INTERFACE	ES IP STATIO	C ROUTES NI	ETWORKS	UNDERLAYS	OVERLAYS	ARP TABLES	IP ROUTE TA	BLES
						\bigcirc		ons 🗸
	Туре	Enable	d ↓	Switch	ļ	VLAN	Add	
	Select Type	- Selec	t Ena 🔻	Enter Switch		Enter Regex	_{fo} Edit	
0	RPI	Yes		RSVDC-FB1-SP1			Delete	

Step 4 On the **Interface Type** page, assign the following values:

- Type: RPI
- Switch: RSVDC-FB1-LF1-1
- Port/LAG: 1/1/13

IP Interface		0	×
Interface Type	IPv4 Addresses Name	Summary	
Select the IP Interface Type	and set the appropriate attributes.		
Enable this IP Interface			
Туре	RPI	× •	~
Switch *	RSVDC-FB1-LF1-1	×	~
Port/LAG *	1/1/13	×	
	Select a Port or LAG. MLAGs or LAGs in use or with a non-default VLAN are excluded.		
([*] = Required)		CANCEL BACK NEXT	

Step 5 On the **IPv4 Addresses** page, enter the WAN IP address for the **Primary IPv4 Network Address**. Click **NEXT**.

IP Interface	0	×
Interface Typ	e IPv4 Addresses Name Summary	
Enter a Primary Network Primary IPv4 Network Address *	Include	
Secondary IPv4 Network Address	IPv4 Network address in CIDR format. Example: 192.168.1.10/24	
Secondary IPv4 Network	Address	
	There is no data to display	
(* = Required)	CANCEL BACK NEXT	

Step 6 On the Name page, enter a Name and Description, then click NEXT.

IP Interfac	e	0 ×
Interfac	e Type IPv4 Addresses Name	Summary
Enter an optional Na	ame and Description.	
Name	RSVDC LF1-1 WAN	
	A string, up to 42 characters. example: lpInterface1	
Description	WAN IP address for multifabric on RSVDC-LF1-1	
	Example: My New IP Interface	
(* = Required)		CANCEL BACK NEXT

Step 7 On the **Summary** page, verify the interface settings and click **APPLY**.

P Interface			C) ×
Interface Type	IPv4 Addresses	Name	Summary	
Name	RSVDC LF1-1	WAN		
Description	WAN IP addre	ss for multifabric on RSVDC-LF1	-1	
Туре	RPI			
Enabled	Yes			
Switch	RSVDC-FB1-L	F1-1		
Port/LAG	1/1/13			
Primary IPv4 Network Address	10.255.6.1/29			
			CANCEL BACK APPLY	

Step 8 Repeat the procedure to assign IP addresses to the physical WAN interface of each border leaf.

Switch	Туре	Port/LA	Primary IPv4 GNetwork Address	Name	Description
RSVDC- LF1-2 WAN	RPI	1/1/13	10.255.6.2/29	RSVDC LF1-2 WAN	WAN IP address for multifabric on RSVDC-LF1-2
RSVCO- LF1-1 WAN	RPI	1/1/13	10.255.6.3/29	RSVCO LF1-1 WAN	WAN IP address for multifabric on RSVCO-LF1-1
RSVCO- LF1-2 WAN	RPI	1/1/13	10.255.6.4/29	RSVCO LF1-2 WAN	WAN IP address for multifabric on RSVCO-LF1-2

NOTE:

Click **VRF** in the current **Configuration / Routing / VRF / default** display in the upper left or in the left navigation pane to return to the **VRF** window. Select **RSVCO-FB2** in the **Fabric** menu to assign IP addresses in the second fabric.

Configure Underlay Routing

External BGP (eBGP) using the IPv4 address-family is used to share IP loopback and VTEP reachability. The diagram below illustrates the eBGP IPv4 sessions established to share loopback and VTEP reachability information.



Step 1 Select Configuration > Routing > BGP on the top menu.

C	rubo Fabric Composer	Dashboard	Configu	ration 🐱	Mainten	iance 🗸	Visualization \checkmark	р wh
Pa	SWITCHES - ALL LOCAL FABRICS	×		Ports	>		BIAA	
nels	Switches in Fabrics		\odot	Routing	>	÷2	VRF	
	14		₽	System	>	٩	BGP	
			昂	Network	>	\square	OSPF	1
			¢°	Administrat	ion >	믛	EVPN	
	14		Ē	Integrations	; >	₽	EVPN VXLAN Mul	lti-Fabric
			æ	Policy	>	۵9	Route Policy	



Configuration / Routing / BGP				
	F	abric RSVDC-FB1 × 🔻		
		()	\odot	🖓 🏟 C ACTIONS 🗸
VRF Na	me 🗜	Switches	μĒ	Enabled
Enter	VRF Name	Enter Switches		Select Enabled 👻
••• O default				Yes
.DC	-VRF	RSVDC-FB1-LF1-1,RSVDC-FB1-LF1-2,RSVDC-FB1-LF2-1,RSVDC-FB1-	LF2-	Yes
		2,RSVDC-FB1-LF3-1,RSVDC-FB1-LF3-2		
D-D	C-VRF	RSVDC-FB1-LF1-1,RSVDC-FB1-LF1-2,RSVDC-FB1-LF2-1,RSVDC-FB1-	LF2-	Yes
		2,RSVDC-FB1-LF3-1,RSVDC-FB1-LF3-2		

Step 3 Click the ••• symbol next to RSVDC-FB1-LF1-1 and select Neighbors.

Configuration / Routing / BGP / default		
Fabric	RSVDC-FB1	
VRF Name		L는 Enabled L는
Enter VRF Name Enter Switch	nes	Select Enabled 🔻
default		Yes
SWITCHES NEIGHBORS SUMMA	RY	
Name	JE Enabled	ן≟ ASN (ASPLAIN) ↓≟
Enter Name	Select Enabled	▼ Enter Regex for ASN (ASPLAI
··· O RSVDC-FB1-LF1-1	Yes	65001
-FB1-LF1-2	Yes	65001
-FB1-LF2-1	Yes	65001
O RSVDC-FB1-LF2-2	Yes	65001

Step 4 On the lower ACTIONS menu, select Add.

Configuration / Rou	ting / BGP / default /	RSVDC-FB1-L	F1-1			
	Fabr	ric RSVDC-F	B1			
				۲	\odot	C ACTIONS ~
Name	JE Ena	abled	ĮΞ	ASN (ASPLAIN)		Router ID
Enter Name	S	elect Enabled	~	Enter Regex for	or ASN (ASPLAI	Enter Regex for
RSVDC-FB1-LF1-1	Yes	3		65001		10.250.0.11
NEIGHBORS						🔅 actions 🗸
	🕑 Name	1E	Description	Ļ	Туре	Add
	Enter Name		Enter Descrip	otion	Select	Edit
> 0	Loopback peering to	RSVDC-FB1-			Internal	Delete
	SP1					
> O	Loopback peering to	RSVDC-FB1-			Internal	
	SP2					

Step 5 On the Settings page, enter the following non-default values and click NEXT.

• Neighbor AS Number: 65002

- IP Address: 10.255.6.3
- Enable Bidirectional Forwarding Detection (BFD) Fall Over: < checked >

BGP Switch	n Neighbor Configuration	? ×
Se	ttings Name Summary	
Specify BGP Neighbo	or settings.	
Neighbor AS	65002	
Number *	ASPLAIN notation between 1 and 4294967295 or ASDOT notation between 1 and 65535.65535, examples: 4294967295 and 65535.1	
Local AS Number		
	ASPI Ally notation between 1 and 4204087205 or ASPOT notation between 1 and 85535 85525 examples: 4204087205 and 85535 1	-1
		_
IP Address *	10.255.6.3	
	A valid IPv4 or IPv6 Address, example: 192.168.1.10 or 2001:db8:85a3::1234.	
Authentication		U
Password	Authentication Password up to 32 characters long.	
		-T.
Address		_1
	Any valid IPv4 Address, example: 192.168.1.10. The packets Source IP Address, this can be entered manually or the Loopback Address can b used	e
Koop Alivo Timor *		-L
Keep Alive Timer	60	-1
	Number of seconds between 1 and 65535. A value of 0 will use the default Keep Alive Timer value.	_1
Hold Down Timer *	180	
	Number of seconds between 3 and 65535. A value of 0 will use the default Hold Down Timer value.	
eBGP Multi-hop		
	Number of hops, between 0 and 255, to an eBGP peer. A value of 0 indicates not in use.	
Weight	0	
	A number between 0 and 65535, example: 0	
Allow AS in Path	0	
	L. Number of occurrences of AS number, between 0 and 10, if allow routes with own AS present in the AS-Path. No value or 0 indicates not in use	э.
Address Families *	× IPv4 ×	_ I
Route Map In	Select 👻 🗛	D
Route Map Out	Select	D
Boute Map In IP	Select	
noute map in in		
Route Map Out IP	Select 💌 🗛	D
Send Community	Select	-
IF		
Send Community	Select	-
EVPN		_
	Accept Incoming Soft Reconfiguration	
	Default Route Originate	
	Z Enable Admin State	
	Enable Fall Over	
	Remove Private AS	
	Lnable Bidirectional Forwarding Detection (BFD) Fall Over	
(* = Required)	Scroll for more options CANCEL BACK NEX	α

C BGP Switch	Neighbor Configuration	? X
Optional External BGP	Ings Name Summary	
Name	RSVDC-LF1-1 to RSVCO-LF1-1	
Description	Underlay BGP between RSVDC-LF1-1 and RSVCO-LF1-1	
(* = Required)	CANCEL BACK	NEXT

Step 6 On the Name page, enter a Name and Description, then click NEXT.

Step 7 On the **Summary** page, verify the BGP settings and click **APPLY**.

BGP Switch Neighbor Configur	ation		?
Settings	Name	Summary	
Name	RSVDC-LF1-1 to RSVCO-LF1	-1	
Description	Underlay BGP between RSVI	DC-LF1-1 and RSVCO-LF1-1	
Neighbor AS Number	65002		
Local AS Number			
IP Address	10.255.6.3		
Update Source Address			
Keep Alive Timer	60		
Hold Down Timer	180		
eBGP Multi-hop			
Weight	0		
Allow AS in Path	0		
Address Families	IPv4		
Accept Incoming Soft Reconfiguration	No		
Default Route Originate	No		
Enable Admin State	Yes		
Enable Fall Over	No		
Remove Private AS	No		
BFD Fall Over	Yes		
Route Reflector Client	No		
		CANCEL BACK	

Step 8 Repeat the procedure to configure underlay eBGP peerings on the remaining border leaf switches in the RSVDC-FB1 fabric.

		Neighbor	IP
Name	Description	ASN	Addresses
RSVDC-LF1-1 to RSVCO-LF1-2	Underlay BGP between RSVDC-LF1-1 and RSVCO-LF1-2	65002	10.255.6.4
RSVDC-LF1-2 to RSVCO-LF1-1	Underlay BGP between RSVDC-LF1-2 and RSVCO-LF1-1	65002	10.255.6.3
RSVDC-LF1-2 to RSVCO-LF1-2	Underlay BGP between RSVDC-LF1-2 and RSVCO-LF1-2	65002	10.255.6.4

Step 9 Repeat the procedure to configure underlay eBGP peerings on the border leaf switches in the RSVCO-FB2 fabric. In step 2, Select **RSVCO-FB2** in the **Fabric** menu to configure BGP peerings in the second fabric.

Name	Description	Neighbor ASN	IP Addresses
RSVCO-LF1-1 to RSVDC-LF1-1	Underlay BGP between RSVCO-LF1-1 and RSVDC-LF1-1	65001	10.255.6.1
RSVCO-LF1-1 to RSVDC-LF1-2	Underlay BGP between RSVCO-LF1-1 and RSVDC-LF1-2	65001	10.255.6.2
RSVCO-LF1-2 to RSVDC-LF1-1	Underlay BGP between RSVCO-LF1-2 and RSVDC-LF1-1	65001	10.255.6.1
RSVCO-LF1-2 to RSVDC-LF1-2	Underlay BGP between RSVCO-LF1-2 and RSVDC-LF1-2	65001	10.255.6.2

Step 10 Click BGP in the left navigation pane and select RSVDC-FB1 for the Fabric field.

Orubo Fabric Composer Das	hboard Configurati	on 🗸 Maintenance 🖌 Visualization	• Ø Where can I find? (e
🛞 VRF	Configuration / R	outing / BGP	
ඪ BGP		Fabric	RSVDC-FB1 × 🔻
🔯 OSPF			
EVPN		VRF Name	Switches
EVPN VXLAN Multi-Fabric		Enter VRF Name	Enter Switches
	0	default	
Route Policy	0	DEV-DC-VRF	RSVDC-FB1-LF1-1,RSVDC-FB1-LF1-2,RSVDC-F
			LF2-2,RSVDC-FB1-LF3-1,RSVDC-FB1-LF3-2
	0	PROD-DC-VRF	RSVDC-FB1-LF1-1,RSVDC-FB1-LF1-2,RSVDC-F
			LF2-2,RSVDC-FB1-LF3-1,RSVDC-FB1-LF3-2

Step 11 Click the ••• symbol next to default and select Neighbors Summary.

Configuration / Ro	outing / BGP			
		Fabric	RSVDC-FB1 × 👻	
			$\odot \odot \heartsuit$	C ACTIONS V
	VRF Name	1E	Switches 1	Enabled 1
	Enter VRF Name		Enter Switches	Select Ena 🔻
0	default			Yes
Switches	'RF		RSVDC-FB1-LF1-1,RSVDC-FB1-LF1-2,RSVDC-FB1-LF2-1,RSVDC-FB1-	No
			LF2-2,RSVDC-FB1-LF3-1,RSVDC-FB1-LF3-2	
Neighbors Si	ummary -VRF		RSVDC-FB1-LF1-1,RSVDC-FB1-LF1-2,RSVDC-FB1-LF2-1,RSVDC-FB1-	Yes
			LF2-2,RSVDC-FB1-LF3-1,RSVDC-FB1-LF3-2	

Step 12 In the **Address Family** column filter, select **IPv4 Unicast**. Click the **Apply table filters** (arrow) icon.

Configuration / Routing / BGP / de	fault				
	Fa	bric RSVDC-FB1			
VRF Name	Switches			ĮΞ	Enabled 1
Enter VRF Name	Enter Switche	S			Select Enabled 🔻
default					Yes
SWITCHES NEIGHBORS	SUMMARY				
				i Unapplie	ed table filters
Switch	↓ <u>≞</u> Nam	ne 🎼	Local AS	Router ID	🛓 🖌 Apply table filters 🗄
Enter Regex for Switch	n Er	nter Name	Enter Reç	Enter Rege	× IPv4 Unicast × -
RSVDC-FB1-LF1-1	Loop	pback peering to RSVDC-FB1-SP1		10.250.0.11	L2VPN EVPN
RSVDC-FB1-LF1-1	Loop	pback peering to RSVDC-FB1-SP2		10.250.0.11	L2VPN EVPN

Step 13 Verify that each BGP session displays Established in the State column.

Configuration / Routing / BGP / default							
	Fabric	RSVDC-FB1					
						$\mathbf{O} \otimes \mathbf{A} \otimes \mathbf{A}$	C ACTIONS ~
VRF Name	Switches				JE.	Enabled	1E.
Enter VRF Name	Enter Switches					Select Enabled	~
default						Yes	
SWITCHES NEIGHBORS SUMMAR	Ŷ						$\odot \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
Switch 📖	Name	Local AS	Router ID	Address Family	Neighbor	Remote AS	E State
Enter Regex for Switch	Enter Name	Enter Reç	Enter Rege	× IPv4 Unicast × ▼	Enter F	Regex Enter Rege:	Enter Regex
RSVDC-FB1-LF1-1	RSVDC-LF1-1 to RSVCO-LF1-1		10.250.0.11	IPv4 Unicast	10.255.6.	3 65002	Established
RSVDC-FB1-LF1-1	RSVDC-LF1-1 to RSVCO-LF1-2		10.250.0.11	IPv4 Unicast	10.255.6.	4 65002	Established
RSVDC-FB1-LF1-2	RSVDC-LF1-2 to RSVCO-LF1-1		10.250.0.7	IPv4 Unicast	10.255.6.	3 65002	Established
RSVDC-FB1-LF1-2	RSVDC-LF1-2 to RSVCO-LF1-2		10.250.0.7	IPv4 Unicast	10.255.6.	4 65002	Established

Configure Overlay Control Plane

The overlay control plane uses MP-BGP EVPN advertisements to share host MAC and IP reachability across both fabrics. The diagram below illustrates the eBGP EVPN sessions established to share overlay reachability information.



Each site contains one border leader VTEP. Border leader VTEP switches establish eBGP EVPN addressfamily peerings with border leaders in other sites. A full mesh of peerings is established between sites.

When more than one fabric is present in a single site, the border leader VTEP switches also establish eBGP EVPN address-family peerings with border leaf switches of each fabric in the same site.

NOTE:

The border leader is a control plane role that optimizes the number of eBGP sessions required to share EVPN reachability information between sites, when any individual site contains multiple fabrics. The multifabric VXLAN data plane still establishes a full mesh of VXLAN tunnels between between border leaf VTEPs.

Multifabric VXLAN Tunnel Requirements

Overlay host traffic within a fabric only requires encapsulation in a single VXLAN tunnel, because a full mesh of tunnels is established between VTEPs. In a multifabric environment, a full mesh of tunnels between all leaf switches is not present. Traffic between fabrics is enabled using a VXLAN tunnel between the border leaf switches of each fabric. In this model, overlay host traffic between fabrics may traverse multiple VXLAN tunnels: VXLAN tunnels internal to a fabric and the inter-fabric VXLAN tunnel.

Join Fabric Overlay Control Planes Together

The AFC **EVPN VXLAN Multi-Fabric** wizard configures eBGP EVPN peerings between the border leader switches of each fabric. Supporting prefix lists, route maps, OSPF redistributions, and BGP redistributions also are configured. VXLAN forwarding between iBGP and eBGP learned VXLAN tunnels is also enabled. These peerings share overlay host and prefix reachability between fabrics and are established between border leader loopback addresses.

AFC adds configuration to share the complete set of VTEP IPs in both fabrics to assist with troubleshooting.

Crubo Fabric Composer	Dashboard Configuration Maintenance Visualization
🛞 VRF	Configuration / Routing / EVPN VXLAN Multi-Fabric
🖧 BGP	Fabric RSVDC-FB1 × -
🖾 OSPF	
EVPN	Image: Second
	Enter Regex for Name Enter Regex for Border Leader Enter Regex for L3 Connect
19 Route Policy	There is no data to display
NOTE:	
If the left pane no	longer displays routing options, select Configuration > Routing > EVPN

Step 1 On the left navigation pane, click EVPN VXLAN Multi-Fabric.

Step 2 Verify that RSVDC-FB1 is selected in the Fabric menu. On the ACTIONS menu, select Add.

VXLAN Multi-Fabric on the top menu.

Orubo Fabric Composer Dash	board Configuration Maintenance	Visualiz 🗸	ation ${\cal O}$ Where can I find	*	<u>ب</u>	E Radmin	n ?
⊗ VRF	Configuration / Routing / EVPN VXLAN	Multi-Fabric					
🖧 BGP		Fabric	RSVDC-FB1 ×	-			
🔯 OSPF					$\bigcirc \bigcirc \bigtriangledown$	¢C ∧	CTIONS 🗸
EVPN	i ∕ Name	1E	Border Leader	JE.	Add		
😰 EVPN VXLAN Multi-Fabric	Enter Regex for Name		Enter Regex for Border Leader There is no data to display		Edit Delete		
19 Route Policy					Reapply E\	(PN VXLAN M	Iulti-Fabric



€ EVPN VX	(LAN Multi-Fabric		×
Name	Settings	Remote Fabrics	Summary
Enter a required N	lame and an optional Description.		
Name *	OWL-DC-MFAB Any non empty string, example EVPN VXL	AN Multi-Fabric-01	
Description	Data center multifabric for OWL Example: EVPN VXLAN Multi-Fabric Descr	ription	
(* = Required)		C	ANCEL BACK NEXT

Step 4 On the **Settings** page, select the border leader VSX pair in the **Border Leader** field, verify that both border leader switches are listed in the **L3 Connect** field, and click **NEXT**.

€ EVPN VXL	AN Multi-Fabric	×
Name	Settings Remote Fabrics Summary	
Select a required Bo	rder Leader and optional L3 Connect Switches and BGP Authentication Password.	
Border Leader *	RSVDC-FB1-VSX_RSVDC-FB1-LF1-2_RSVDC-FB1-LF1-1 (RSVDC-FB1-LF1-1 / RSVDC-FB1-L × 💌	
L3 Connect	× RSVDC-FB1-LF1-1 × RSVDC-FB1-LF1-2 × ▼ SELECT ALL	
	Switches to be used for inter-fabric L3 Underlay connectivity.	
BGP Auth]
Password	Any non empty string, example: pass1231%	
(* = Required)	CANCEL BACK NEXT	

Step 5 On the **Remote Fabrics** page, select **Local AFC** in the **AFC Site** field and **RSVCO-FB2** in the **Fabric** field. Verify that the auto-populated values for **AS Number**, **Remote Border Leader Address**, and **Secondary Remote Border Leader Address** are correct. Click **Add**.

😰 EVPN VXI	AN Multi-F	abric				;		
				\bigcirc	?			
Name		Settings	R	emote Fabrics	Summary			
Add optional Remot Border Leader Addr	e Fabrics. Sele ess. At least or	ct a Border Leader to le Remote Fabric mus	populate the ASN t be configured.	and addresses or m	anually define an ASN and	d Remote		
AFC Site	Local AFC					× •		
Fabric	RSVCO-FE	32				× •		
Border Leader	RSVCO-FE	32-VSX_RSVCO-FB2-	LF1-2_RSVCO-FB	2-LF1-1 (RSVCO-FB2	2-LF1-1 / RSVCO-FB2	× •		
AS Number *	65002 ASPLAIN notat	ion between 1 and 429496	7295 or ASDOT notatic	n between 1 and 65535.6	5535, examples: 4294967295 an	d 65535.1		
Remote Border	10.250.3.	7						
Leader Address *	Any valid IPv4	Any valid IPv4 Address, example: 192.168.1.10						
Secondary	10.250.3.	5						
Remote Border Leader Address	Any valid IPv4	Address, example: 192.168	.1.10					
CLEAR AD	D							
AFC Site	Fabric	Border Leader	AS Number	Remote Borde	Secondary Re			
		Tr	nere is no data to di	splay	· · · · · · · · · · · · · · · · · · ·			
(* = Required)	Scroll for more	e options			CANCEL BACK	NEXT		

NOTE:

More than one fabric can be added on this page. Fabrics managed by remote AFC instances can be selected when the remote AFC instance is configured as an AFC Site on the local AFC application.

Step 6 Click NEXT.

					0	
Name		Settings	F	Remote Fabrics	Summar	v
dd optional Remot Border Leader Addi	e Fabrics. Selec ess. At least one	t a Border Leader to Remote Fabric mus	populate the ASI st be configured.	N and addresses or m	anually define an ASN	and Remote
AFC Site	Select AFC	Site				•
Fabric	Select Fabr					
Border Leader	Select Bord	der Leader				
AS Number *						
	ASPLAIN notation	on between 1 and 429496	7295 or ASDOT notat	ion between 1 and 65535.6	5535, examples: 42949672	95 and 65535.1
Remote Border Leader Address *	Any valid IPv4 A	ddress, example: 192.168	3.1.10			
Secondary Remote Border						
_eader Address	Any Valid IPV4 A	adress, example: 192.168	3.1.10			
CLEAR	D					
AFC Site	Fabric	Border Leader	AS Number	Remote Borde	Secondary Re	
	RSVCO-FB2	RSVCO-FB2-	65002	10.250.3.7	10.250.3.5	
		VSX_RSVCO-				
		FB2-LF1-				
		2_RSVCO-FB2-				
		2_RSVCO-FB2- LF1-1 (RSVCO-				
		2_RSVCO-FB2- LF1-1 (RSVCO- FB2-LF1-1 /				

Step 7 On the **Summary** page, verify the multifabric BGP settings and click **APPLY**.

Name		Settings	Remote Fabrics	Sum	mary
Name	OWL-DC-MFAB				
Description	Data center multifa	bric for OWL corp			
Border Leader	RSVDC-FB1-VSX_F	RSVDC-FB1-LF1-2_RSV	DC-FB1-LF1-1 (RSVD0	C-FB1-LF1-1 / RSVDC	-FB1-LF1-2)
L3 Connect	RSVDC-FB1-LF1-1,	RSVDC-FB1-LF1-2			
AFC Site	Fabric	Border Leader	AS Number	Remote Border L	Secondary Rem
	RSVCO-FB2	RSVCO-FB2-	65002	10.250.3.7	10.250.3.5
		VSX_RSVCO-FB2-			
		LF1-2_RSVCO-			
		FB2-LF1-1			
		(RSVCO-FB2-LF1-			
		1 / RSVCO-FB2-			
		LF1-2)			

Step 8 Repeat the procedure to configure eBGP EVPN peerings in the second fabric. At step 2, select **RSVCO-FB2** on the **Fabric** menu.

Step 9 In the menu bar at the top right of the AFC display, click the **CLI Commands** icon and select **Show Commands**.

🚊 🎦 🗸	🗉 음 ^{admin} * ? *
>_ Show Commands	
E Configuration Editor	DISTRIBUTED SERVICES
	1

Step 10 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: RSVDC-FB1-LF1-1, RSVDC-FB1-LF1-1, RSVCO-FB2-LF1-1, RSVCO-FB2-LF1-2
- **Commands:** show bgp l2vpn evpn summary

>_ CLI Command	Processor							×
Select Fabrics or Switches,	and select or add Saved Co	mmands that can be	customized. Press I	lun for resu	llts.			
Fabrics	Not applicable when a Sw							~
Switches	× RSVDC-FB1-LF1-1 ×	RSVDC-FB1-LF1-2 ×	RSVCO-FB2-LF1-1	× RSVCO	-FB2-LF1-2			
Saved Commands	Select from Saved Comma	ands or Add new com	nmands.			~	ADD RE	MOVE
Commands	show bgp I2vpn evpn sum	mary						
	A comma separated list of comman	ds to be run.						
Download Options	Download Results Downl	oad JSON Data						
Results	Switch : RSVDC-FB1-L Codes: * Dynamic Neig VRF : default BGP Summary	.F1-1 Command : hbor	show bgp l2vpn	evpn sum	mary			
	Local AS	: 65001	BGP Router I	dentifie	r : 10.2	250.0.11		
	Peers	: 4	Log Neighbor	Changes	: Yes			
	Confederation Id	: 180	стд. кеер ат	ive	: 00			
	Neighbor AdminStatus		Remote-AS	MsgRcvd∣	MsgSent	Up/Down Time	State	
	10.250.0.9		65001	6892	2769	23h:37m:15s	Established	Up
	10.250.0.13		65001	6877	2781	23h:37m:15s	Established	Up
	10.250.3.5		65002	17	33	00h:01m:16s	Established	Up
	10.250.3.7		65002	18	34	00h:01m:16s	Established	Up
	Switch : RSVDC-FB1-L Codes: * Dynamic Neig VRF : default	.F1-2 Command : hbor	show bgp l2vpn	evpn sum	mary			
(* = Required)							CANCEL	RUN

Step 11 Verify that the output for each switch displays the newly configured peers with an *Established* state.

The eBGP EVPN route peerings establish the control plane mechanism to share overlay reachability between fabrics. Additional steps are necessary to install IP prefixes and MAC addresses between fabrics.

Extend Layer 3 Reachability Across Fabrics

When using EVPN, MP-BGP EVPN route-type 5 advertisements share IP prefix reachability for a VRF. Route targets included in these advertisements control how Layer 3 IP addresses are installed in IP forwarding tables. Route targets defined during the creation of each fabric are typically used only to share information locally. New VRF route-targets are defined to share IP reachability between fabrics.

Step 1 On the left navigation pane, click VRF.

αr∪bo Fabric Composer Dash	board Co	nfigurati	on 👻 Maintenance 👻	Visualiza	ation 🗸	Ø Where can I	find? (e.g	<u>*</u>
⊛ VRF	Configur	ation / R	outing / VRF					
🖒 BGP					Fabric	RSVDC-FB1	×	•
🕅 OSPF								
EVPN			Name	ΨĒ	Туре	Ļ	Switches	Ļ
EVPN VXLAN Multi-Fabric			Enter Name		Select	Туре 🔻	Enter Switches	
		\circ	default		Default			
Route Policy		\bigcirc	DEV-DC-VRF		User		RSVDC-FB1-LF1-1,F	RSVDC-FB1-
							LF1-2,RSVDC-FB1-L	F2-1,RSVDC-
							FB1-LF2-2,RSVDC-F	B1-LF3-
							1,RSVDC-FB1-LF3-2	2
		\circ	mgmt		Manager	nent		
		\bigcirc	PROD-DC-VRF		User		RSVDC-FB1-LF1-1,F	RSVDC-FB1-
							LF1-2,RSVDC-FB1-L	F2-1,RSVDC-
							FB1-LF2-2,RSVDC-F	B1-LF3-
							1,RSVDC-FB1-LF3-2	2
NOTE:								

If the left pane no longer displays routing options, select **Configuration > Routing > VRF** on the top menu.

Step 2 Select **RSVDC-FB1** in the **Fabric** field. Click the radio button next to **PROD-DC-VRF**. On the **ACTIONS** menu, select **Edit**.

Configur	ration / Ro	outing / VRF				
			Fabric RSVDC-FB1	× -		
					$\bigcirc \bigcirc \bigtriangledown $	C ACTIONS Y
		Name 🖡	Туре ↓≞	Switches	L3 VNI	Add
		Enter Name	Select Type 🔻	Enter Switches	Enter Regex for L	Edit
	0	default	Default			Delete
	\bigcirc	DEV-DC-VRF	User	RSVDC-FB1-LF1-1,RSVDC-FB1-	100002	Reapply VRF
				LF1-2,RSVDC-FB1-LF2-1,RSVDC-		IP Interfaces
				FB1-LF2-2,RSVDC-FB1-LF3-		IP Static Routes
				1,RSVDC-FB1-LF3-2		Networks
	\bigcirc	mgmt	Management			ARP Tables
	۲	PROD-DC-VRF	User	RSVDC-FB1-LF1-1,RSVDC-FB1-	100001	IP Route Tables
				LF1-2,RSVDC-FB1-LF2-1,RSVDC-		
				FB1-LF2-2,RSVDC-FB1-LF3-		
				1,RSVDC-FB1-LF3-2		

Step 3 Click the the **ROUTE TARGETS** page heading. On the page, enter the values below and click **ADD**.

- Route Target Mode: Both
- Route Target Ext-Community: 1:100001
- Address Family: EVPN

B VIRTUAL ROUTING &	Forwarding (RSVL	ЈС-ГВТ) РКОД-ДС	-VRF	() ()
✓ NAME	SCOPE	ROUTING	NOUTE TARGETS	SUMMARY
Enter the optional Route Targ	get Mode and Ext-Communi	ty. Enter both or none of the fi	elds.	
Route Target Mode	oth			× *
Route Target Ext-	: 100001 Iid Autonomous System Number, e	example: 65001:101 or 10.10.10.1:10	1	
Address Family	VPN			× •
CLEAR ADD	JPDATE			
Route Target Mode	Route Targe	t Ext-Community Addres	s Family	
Both	65001:1000	01 EVPN	\uparrow	↓ Ш
(* = Required)				CANCEL
NOTE:				
It is best practice	to use a route tar	rget between fabrio	s that is distinct fro	om the route target

Step 4 Click Apply.

→ NAME	\bigcirc	SCOPE	ROUTING	ROUTE TARGET	rs	SUMMARY	
Enter the optional Rout	e Target Mode and	Ext-Community. Enter	both or none of the field	S.			
Route Target Mode	Select						-
Route Target Ext- Community	A valid Autonomous S	ystem Number, example: 6	5001:101 or 10.10.10.1:101				
Address Family	Select						•
CLEAR ADD	UPDATE						
Route Target	Mode	Route Target Ext-Con	nmunity Address F	amily			
Both		65001:100001	EVPN		$\uparrow \downarrow$	₫	
Both		1:100001	EVPN		$\uparrow \downarrow$		
(* = Required)						CANCEL	Y

Step 5 Repeat the procedure to assign the new route target to the RSVCO-FB2 PROD-DC VRF. Select **RSVCO-FB2** in the **Fabric** field to begin.

Enable External Layer 3 Multifabric Advertisements

The AFC default configuration applies a route map that permits only local fabric prefixes to be shared across fabrics. The AFC created route map named *to-border-leaders* must be modified, if IP prefixes learned in the overlay from outside the fabric must be shared.

In this sample deployment, a campus summary prefix learned in PROD-DC-VRF of the RSVDC-FB1 fabric is shared with PROD-DC-VRF in the RSVCO-FB2 fabric. The default route learned in the same VRF also is shared as a backup default route if Internet connectivity in the colocation facility fails.

A new route map is created for the RSVDC-FB1 border leaders and applied to its eBGP EVPN peerings to allow advertising of routes learned from outside the fabric.

Create Route Map

A new route map is created to allow local fabric reachability and enable advertising of campus-learned IP prefixes from the RSVDC-FB1 border leaders to the RSVCO-FB2 fabric. The route map **ALLOWED-EXT-AS** defined in the initial EVPN-VXLAN configuration is re-used in this procedure.

Step 1 Click the ROUTE MAPS tab. On the ACTIONS menu, select Add.

Configuration / Routing / Route Policy								
ROUTE MAPS	MAPS COMMUNITY LISTS PREFIX LISTS AS PATH LISTS							
						ତେ⊽⊄	C ACTIONS V	
		Name	1E	Switches	1£	Fabrics	Add	
		Enter Regex for Name		Enter Regex for Switches		Enter Regex for F	Edit	
		BGP-OSPF		RSVDC-FB1-LF1-1			Delete	
				RSVDC-FB1-LF1-2			Clone	
				RSVCO-FB2-LF1-1			Merge	
				RSVCO-FB2-LF1-2			Unmerge	
		connected-ospf				RSVDC-FB1	Entries	
						RSVCO-FB2		

Step 2 On the Name page, enter a Name and Description, then click NEXT.

🛿 Route Ma)		×		
) (?)	?	?		
Nam	Scope	Entries	Summary		
Enter a required Na	me and an optional Description.				
Name *	RSVDC-to-borders				
	Any non-empty string without spaces and without " or ?, example: RouteMap1				
Description	RSVDC border leader route map to othe	r fabric border leaders			
	Any non-empty string up to 80 characters long, exam	ple: My Route Map			
(* = Required)			CANCEL BACK NEXT		

Step 3 On the **Scope** page, select the RSVDC-FB1 border leaders in the **Switches** field and click **NEXT**.

🕸 Route Map		×
Name Select optional Fabrics c	r Switches to apply this configuration. A Fabric implies all Switches contained within it, excluding Sub Leaf Swit	iches.
Fabrics	Select	▼
Switches	× RSVDC-FB1-LF1-1 (RSVDC-FB1) × RSVDC-FB1-LF1-2 (RSVDC-FB1)	• × •
(* = Required)	CANCEL BACK	NEXT

Step 4 On the ACTIONS menu, select Add.

🕼 Route Ma	ıp					×
Nan Configure optional	entries. Entries will	Scope	e Map configuratio	Entries n is applied.	Summary	
						•
	Sequence LE	Action J= Enter Regex for Act	Route Map Ji	Match IPv4 Prefix 1	Match Con Add Enter Re Remove	K
(* = Required)	Scroll for more	options		[CANCEL BACK N	EXT

Step 5 On the Settings page, enter the following values and click NEXT

- Sequence: 10
- **Description**: permit local overlay advertisements
- Action: Permit

ß Route Map I	Entries	×
	? ? ?	
Settings	Match Attributes Set Attributes Summary	
Configure a required S	Sequence and Action and optional Description and Route Map Continue.	
Sequence *	10	
	A number between 1 and 4294967295, example 1. The Sequence must be unique.	
Description	permit local overlay advertisements	
	Any non-empty string up to 80 characters long, example: My Route Map	
Action *	Permit	-
Route Map Continue		
	A number between 2 and 4294967295, example 2. Route Map Continue must be greater than the Sequence.	
(* = Required)	CANCEL BACK N	IEXT

Step 6 On the Match Attributes page, enter the following values and click NEXT.

- Attributes: Match AS Path List
- Match AS Path List: local-fabric

😰 Route Map E	intries			×
Settings	Match Attributes	Set Attributes	Summary	
Configure optional Mate	ch values for this entry.			
Attributes	× Match AS Path List			× •
	Select which match attributes to configure for this entry.			
Match AS Path List	local-fabric		▼	ADD
(* = Required)			CANCEL BACK	NEXT

Step 7 On the Set Attributes page, click NEXT.

🕼 Route Map E	ntries		×
			?
Settings	Match Attributes	Set Attributes	Summary
Configure optional Set v	alues for this entry.		
Attributes	Select		~
	Select which set attributes to configure for this entry.		
(* = Required)			CANCEL BACK NEXT

Step 8 On the **Summary** page, verify the multifabric BGP settings and click **APPLY**.

Route Map Entries			×
Settings	Match Attributes	Set Attributes	Summary
Sequence	10		
Description	permit local ove	rlay advertisements	
Action	Permit		
Route Map Continue			
Match AS Path List	local-fabric		
			CANCEL BACK APPLY

Step 9 Repeat steps 11 to 15 to add a second route map entry with the values below.

- Sequence: 20
- Description: permit campus/firewall prefixes
- Action: Permit
- Attributes: Match AS Path List

• Match AS Path List: ALLOWED-EXT-AS

Route Map Entries			×
Settings	Match Attributes	Set Attributes	Summary
Sequence	20		
Description	permit car	mpus/firewall prefixes	
Action	Permit		
Route Map Continue			
Match AS Path List	ALLOWED	D-EXT-AS	
			CANCEL BACK APPLY

Step 10 Click NEXT.

					0	
Nam	ne	Scope		Entries	Summary	
figure optional	entries. Entries will	l be added when the Rout	e Map configuration	n is applied.		
						TIONS 🗸
	Sequence	Action 1	Route Map ↓	Match IPv4 Prefix 1	Match Community 1	Match Ext-
	Enter Regex	Enter Regex for Act	Enter Regex	Enter Regex for Ma	Enter Regex for Ma	Enter Re
0	10	Permit				
\bigcirc	20	Permit				

Step 11 On the **Summary** page, verify the route map settings and click **APPLY**.

🕸 Route Map				×
			\bigcirc	
Name	Scope	Entries	Summary	
Name	RSVDC-to-borders			
Description	RSVDC border leader route map to oth	er fabric border leaders		
Fabrics				
Switches	RSVDC-FB1-LF1-1			
	RSVDC-FB1-LF1-2			
				-
			CANCEL BACK APPLY	

Apply Route Map to EVPN Peering

Step 1 On the menu bar at the top right of the AFC display, click the **CLI Commands** icon and select **Show Commands**.

	<u>\$</u>	Þ *	I=	A ^{admin} ~	? *
	>_ Show Comm	ands			
	🔒 Configuration	Editor			
_					



Configuration	/ System / Configuration Editor							
Fabric	RSVDC-FB1	× •	Switch	× RSVDC-FB1-LF1-1	× •	SELECT ALL		
RSVDC-FB	11-LF1-1 RSVDC-FB1-LF1-2							
! !Version ArubaOS-CX GL.10.12.1010 !export-password: default hostname RSVDC-FB1-LF1-1 user admin group administrators password ciphertext								

Step 3 In the switch configuration window, scroll to the **address-family l2vpn evpn** stanza in the BGP configuration section. Set the **border-leaders** peer group's outbound route map to **RSVDC-to-borders**.

Configuration	/ System / Configuration Editor		_				
Fabric	RSVDC-FB1	× •	Switch	× RSVDC-FB1-LF1-1		SELECT ALL	
			_	× RSVDC-FB1-LF1-2			
RSVDC-FE	1-LF1-1 RSVDC-FB1-LF1-2						
ne	1gnbor 10.255.6.3 activate						
ne	ighbor 10.255.6.4 activate						
re	distribute connected						
re	distribute local loopback						
re	distribute ospf 1 route-map	0SPF-	-BGP				
exit-a	ddress-family						
addres	s-family <u>l2vpn</u> evpn						
ne	ighbor RSVDC-FB1-RR next-ho	p-self	F				
ne	ighbor RSVDC-FB1-RR send-co	mmuni	ty both				
ne	ighbor border-leaders route	-map F	RSVDC-to	-borders out			
ne	ighbor border-leaders send-	commur	nity bot	h			
ne ne	ighbor 10.250.0.9 activate						
ne	ighbor 10.250.0.13 activate						
ne	ighbor 10.250.3.5 activate						
ne evit e	Ignbor 10.250.3.7 activate						•
exit-a	duress-railitty						
							-
VALIDATE	APPLY					NEXT ERROR	
🔽 Create a	Checkpoint before Apply				VALIDATE ALL		

Step 4 Click the **RSVDC-FB1-LF1-2** tab. Set the **border-leaders** peer group's outbound route map to **RSVDC-to-borders**. Click **VALIDATE ALL**.

Configuration	/ System / Configuration Editor								
Fabric	RSVDC-FB1	× •	Switch	× RSV × RSV	/DC-FB1-LF1-1 /DC-FB1-LF1-2		×·	SELECT ALL	
RSVDC-FB	1-LF1-1 RSVDC-FB1-LF1-2								
ne ne re re exit-a addres ne ne ne ne ne ne ne ne ne ne	ighbor 10.255.6.3 activate ighbor 10.255.6.4 activate distribute connected distribute local loopback distribute ospf 1 route-map ddress-family s-family l2vpn evpn ighbor RSVDC-FB1-RR next-ho ighbor RSVDC-FB1-RR send-co ighbor border-leaders route ighbor border-leaders send- ighbor 10.250.0.9 activate ighbor 10.250.3.5 activate ighbor 10.250.3.7 activate ddress-family	OSPF- p-self mmunit -map R: commun	BGP y both SVDC-to ity bot	-borden h	's out				•
VALIDATE	APPLY							NEXT ERROR	
Create a	Checkpoint before Apply					VA	LIDATE AL	L APPLY ALL	

Step 5 A success message verifies the configuration is valid. Click APPLY ALL.

\checkmark Success Successfully validated configuration changes. \times	
NOTE:	
If configuration errors are present on a switch, a red error is the configuration errors are highlighted in red. Correct the er again. It is possible an incomplete spanning-tree configur in the AFC guided setup process. If spanning-tree config- parameter and no other spanning-tree configuration preser	con appears on the switch tab and rrors and validate the configuration ration was unintentionally created name is in the config with no name nt, it is safe to delete the line.

Step 6 Success messages verify a configuration checkpoint was created and the configuration changes were applied.



Step 7 On the RSVDC-FB1-LF1-1 switch CLI, clear the EVPN BGP sessions to the second fabric to apply the new route map policy.

clear bgp 10.250.3.5 clear bgp 10.250.7

RSVDC-FB1-LF1-1# show b Codes: * Dynamic Neighb VRF : default BGP Summary	gp l2vpn evpn s or	ummary					
Local AS Peers Cfg. Hold Time Confederation Id	: 65001 : 4 : 180 : 0	BGP Router Id Log Neighbor Cfg. Keep Ali	entifier Changes ve	: 10.2 : Yes : 60	50.0.11		
Neighbor 10.250.0.9 10.250.0.13 10.250.3.5 10.250.3.7		Remote-AS M 65001 65001 65002 65002	lsgRc∨d M 14663 14684 543 541	sgSent 6782 6792 876 873	Up/Down Time 01d:19h:09m 01d:19h:09m 03h:44m:35s 03h:44m:33s	State Established Established Established Established	AdminStatus Up Up Up Up
RSVDC-FB1-LF1-1# clear RSVDC-FB1-LF1-1# clear RSVDC-FB1-LF1-1#	bgp 10.250.3.5 bgp 10.250.3.7						

Step 8 Repeat step 7 on the RSVDC-FB1-LF1-2 switch.

Step 9 On the menu bar at the top right of the AFC display, click the **CLI Commands** icon and select **Show Commands**.



Step 10 On the CLI Command Processor page, enter the following values, then click RUN.

- Switches: RSVCO-FB2-LF1-1, RSVCO-FB2-LF1-1, RSVCO-FB2-LF2, RSVCO-FB2-LF3
- **Commands:** show ip route vrf PROD-DC-VRF
| >_ CLI Command Processor X | | | | | | | |
|------------------------------------|---|---|--------------------|-------------|-----------------|---------------------|---------------------|
| Select Fabrics or Switches, and se | lect or add Saved Comma | unds that can be customized. Press Run for results. | | | | | |
| Fabrics | | | | | | | v. |
| Switches | × RSVCO-FB2-LF1-1 | × RSVCO-FB2-LF1-2 × RSVCO-FB2-LF2 × RSVCO- | B2-LF3 | | | | ■ × • |
| Saved Commands | Select from Saved Con | Select from Saved Commands or Add new commands. | | | | | |
| Commands | show ip route vrf PRO | D-DC-VRF | | | | | |
| | A comma separated list of com | mands to be run. | | | | | |
| Download Options | Download Results Do | wnload JSON Data | | | | | |
| Results | Switch : RSVCO-FB | 2-LF1-1 Command : show ip route vrf PROD- | DC-VRF | | | | |
| | Displaying ipv4 ro | utes selected for forwarding | | | | | |
| | Origin Codes: C - H
R - H
Type Codes: E - H
IA -
E2 - | Origin Codes: C - connected, S - static, L - local
R - RIP, B - BGP, 0 - OSPF
Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
IA - OSPF internal area, E1 - OSPF external type 1
E2 - OSPF external type 2 | | | | | |
| | VRF: PROD-DC-VRF | | | | | | |
| | Prefix | Nexthop | Interface | VRF(egress) | Origin∕
⊤ype | Distance/
Metric | Age |
| | 0.0.0.0/0 | 10.255.5.3 | vlan2021 | _ | B/E | [20/0] | 03h:20m:39s |
| | 10.0.0/12 | 10.250.2.1 | - | - | B/EV | [200/0] | 03h:13m:03s |
| | 10.5.50.0/24 | 10.250.2.1 | - | - | B/EV | [200/0] | 00h:19m:20s |
| | 10.5.50.1/32 | 10.250.2.1 | - | - | B/EV | [200/0] | 00h:07m:10s |
| | 10.5.50.61/32 | 10.250.2.1 | - | - | B/EV | [200/0] | 00h:07m:35s |
| | 10.5.50.71/32 | 10.250.2.1 | - | - | B/EV | [200/0] | 00h:07m:35s |
| | 10.5.50.72/32 | 10.250.2.1 | - | - | B/EV | [200/0] | 00h:07m:35s |
| | 10.5.101.0/24
10.5.101.1/32 | - | vlan101
vlan101 | - | C
L | [0/0]
[0/0] | - |
| (* = Required) | | | | | | [| CANCEL RUN |

Step 11 Verify that each leaf switch in the RSVCO fabric learns the 10.0.0.0/12 campus summary route and the 10.5.50.0/24 prefixes that are present only on CX 10000 switches in the RSVDC-FB1 fabric.

Extend Layer 2 Reachability Across Fabrics

When using EVPN, host reachability advertisements include a route-target to inform remote VTEPs of the VLAN associated with the host MAC address advertisement. VLAN route-targets can be generated automatically within a fabric using an iBGP EVPN peering. The eBGP EVPN peering between fabrics requires an explicitly defined route target for each VLAN. This additional route target controls when MAC advertisements shared between fabrics are installed in local MAC address tables.

Step 1 On the Configuration menu, select Routing > EVPN, then click the EVPN MULTI SITE tab.

orubo Fabric Composer	Dashboard (Configuration 🖌 Mainte	nance - Visualization - 🔎 When
Fabrics & Switches	0	Ports >	
🖄 AEC Domoto Siton	Conf	Routing >	🛞 VRF
AFC Remote Sites	_	System >	🖧 BGP
Configuration Editor		界 Network >	SPF OSPF
🛃 Monitor Agents	R	Administration >	EVPN
		Integrations >	EVPN VXLAN Multi-Fabric
SmartNICs		🔆 Policy کې	Route Policy
🔗 System Settings	!		
NOTE:			
If the left pane no longer dis	olays routing o	options, select Confi	guration > Routing > EVPN on

Step 2 With RSVDC-FB1 selected in the Fabric menu, click the ACTIONS menu and select Add.

Configuration	n / Routing / EVPN				
		Fabric	RSVDC-FB1	× -	
EVPN	EVPN MULTI SITE				
	Fabrics	μ <u>ε</u>	Stretched VLANs	Route Target Types	Add
	Enter Regex for I	Fabrics	Enter Regex for Stretched VL/	Select Route Target	Edit
			There is no data to dis	play	Delete
					Delete All Reapply EVPN Multi Sites

Step 3 On the Fabrics page, select both fabrics and click NEXT.

the top menu.

몇 EVPN Mult	i Site(RSVDC-FB1)			×
Fabrics	(?) VLANs	Route Targets	Summary	
Select one or more F	abrics. The configuration will be app	lied to all selected Fabrics.		
Fabrics *	× RSVDC-FB1 × RSVCO-FB2			
(* = Required)			CANCEL BACK	NEXT

Step 4 On the **VLANs** page, enter the VLAN IDs that share Layer 2 reachability information across both fabrics.

몇 EVPN Mult	ti Site(RSVDC-FB1))		×
Fabrics	VLAN	s Ro	? ute Targets	Summary
Enter a required Stre	etched VLAN range.			
Stretched VLANs *	101-102 A number, set, or range of VLAN	ls between 2 and 4094, examp	ble: 5, 10-45, 102.	
([*] = Required)			CANCEL	BACK NEXT

Step 5 On the **Route Targets** page, enter the following values and click **ADD**.

- Route Target Type: NN:VNI
- Administrative Number: 1

몇 EVPN Mul	로VPN Multi Site(RSVDC-FB1) ×					
Fabrics		/LANs	Route Targets		Summary	
Add required Route	Targets.					
Route Target Type *	NN:VNI					× •
Administrative Number *	A number between 1 and	4294967295, example 1				
Route Target Type		Administrative Number				
		There is no data	to display			
(* = Required)				CANCEL	BACK	NEXT

Step 6 Click NEXT.

宴 EVPN Mult	ti Site(RSVDC-F	-B1)		×
Fabrics		VLANS	Route Targets	Summary
Add required Route	Targets.			
Route Target Type *	Select			~
Administrative Number *	A number between 1 and	4294967295, example 1		
Route Target Type		Administrative Number		
NN:VNI		1		
(* = Required)				CANCEL BACK NEXT

Step 7 On the **Summary** page, verify the route target settings and click **APPLY**.

EVPN Multi Site(F	{SVDC-FB1)		
Fabrics	VLANs	Route Targets	Summary
Fabrics	RSV	CO-FB2,RSVDC-FB1	
Stretched VLANs	101-	102	
Route Target Type		Administrative Number	
NN:VNI		1	
		CAN	ICEL BACK APPLY

If the fabrics are managed by different AFC instances, the **EVPN** wizard must be run for each instance.

Step 8 On the menu bar at the top right of the AFC display, click the **CLI Commands** icon and select **Show Commands**.

	🖄 🎦 Y	🗉 🖁 🖓 admin 👻 ? 👻		
>_	Show Commands			
6	Configuration Editor	DISTRIBUTED SERVICES		
		1		

Step 9 On the CLI Command Processor page, enter the following values, then click RUN.

- Fabrics: RSVDC-FB1, RSVCO-FB2
- **Commands:** show mac-address-table

>_ CLI Command	Processor				×	
Select Fabrics or Switches,	and select or add Saved (Commands	that can be customize	d. Press Run for results.	1	
Fabrics	× RSVDC-FB1 × RSV	× RSVDC-FB1 × RSVCO-FB2				
Switches	Not applicable when a F	Not applicable when a Fabric is selected.				
Saved Commands	Select from Saved Comr	mands or A	dd new commands.	- ADD	REMOVE	
Commands	show mac-address-table	e				
	A comma separated list of comm	ands to be rur	L.			
Download Options	Download Results Dow	nload JSO	N Data			
Results	Switch : RSVCO-FB2 MAC age-time Number of MAC addres	-LF1-1 Cc : 30 sses : 24	ommand : show mac- 00 seconds	-address-table		
	MAC Address	VLAN	Туре	Port		
	00:50:56:9f:a5:7b	101	evpn	vxlan1(10.250.2.2)		
	00:50:56:9e:de:f9	101	evpn	vxlan1(10.250.2.2)		
	00:50:56:9e:dc:a4	101	evpn	vxlan1(10.250.2.2)		
	00:50:56:9e:bd:c4	101	evpn	vxlan1(10.250.2.2)		
	00:50:56:9e:a7:75	101	evpn	vxlan1(10.250.2.2)		
	00:50:56:9e:a3:95	101	evpn	vxlan1(10.250.2.2)		
	00:0c:29:ac:e3:bb	101	dynamic	lag2		
	00:0c:29:28:cb:7c	101	dynamic	lag1		
	b8:d4:e7:d5:29:00	101	dynamic	lag256		
	00:0c:29:03:10:ea	101	evpn	vxlan1(10.250.4.1)		
	00:50:56:9e:38:f1	101	evpn	vxlan1(10.250.2.2)		
	00:50:56:9e:48:ae	101	evpn	vxlan1(10.250.2.2)		
	00:50:56:9f:bc:c8	102	evpn	vxlan1(10.250.2.2)		
	00:50:56:9f:68:70	102	evpn	vxlan1(10.250.2.2)		
	00:0c:29:fc:d2:4b	102	dynamic	lag1		
	00:0c:29:31:86:f6	102	dynamic	lag2		
	b8:d4:e7:d5:29:00	102	dynamic	lag256		
	00:0c:29:28:c8:5b	102	evpn	vxlan1(10.250.4.1)		
	00:50:56:9e:92:cd	102	evpn	vxlan1(10.250.2.2)		
	b8:d4:e7:d5:29:00 4a:5e:d2:6c:ce:46	2021 2021	dynamic dynamic	lag256 lag251		
(* = Required)				CAN	CEL RUN	
NOTE						

VXLAN-learned MAC address entries include the VTEP IP in parentheses in the **Port** column.

Step 10 Verify that each switch in both fabrics learns MAC addresses from the other fabric (the MAC address entires are displayed with a VTEP IP of the border leader in the other fabric).

At the completion of this procedure, a multifabric EVPN is established between the RSVDC-FB1 and RSVCO-FB2 fabrics.

Aruba Central Two-Tier Data Center

The Aruba ESP Two-Tier Data Center can be configured using Aruba Central or Aruba Fabric Composer (AFC). The Two-Tier architecture uses Layer 2 multi-chassis links between a VSX pair of core switches and a set of server access switches. The following deployment example uses Aruba Central, enabling a single management platform for both campus and data center networks that provides advanced troubleshooting features and performance feedback.

Overview

The Aruba CX switching portfolio includes a range of products for data center core and access layers. Aruba Central documentation contains a list of supported AOS-CX switches.

Aruba ESP Two-Tier data centers meet the requirements for small- and medium-size data centers. It provides network resiliency by using multi-chassis link aggregations (MC-LAGs) at both switch tiers.

Two-Tier Data Center Topology

The diagram below summarizes the physical topology configured in this deployment guide and the relationship between components.



Validated Solution Guide

Two-Tier Core Layer

The core layer provides redundant Layer 2 connectivity to downstream access switches. A VSX pair of core switches is configured with an MC-LAG to each downstream rack. All links from the core layer to the access layer for a single rack are members of the same MC-LAG, whether the rack is populated with a single switch or with a VSX-pair of access switches. MC-LAG provides network resiliency and load-balancing. It also mitigates the need for loop avoidance mechanisms between the core and access layer switches.

Layer 3 services for the data center are provided by the core layer. VLAN switched virtual interfaces (SVIs) are defined on core switches that route packets between data center subnets and provide redundant IP gateways to data center hosts. The core layer also provides redundant IP connectivity to upstream external networks. Typically, firewalls are placed between a data center and external networks for policy enforcement. The redundancy models between the data center core and external networks can vary, depending on device feature sets and organizational requirements. In this guide, a traditional active/passive redundant pair of firewalls is connected to the core switch pair using MC-LAGs.

Two-Tier Access Layer

The access layer provides Layer 2 connectivity to downstream data center hosts.

When a single access switch is at the top-of-rack (ToR) position, the access layer connects to the core layer using a standard LAG. A single ToR switch can provide physical link redundancy using a standard LAG, but host connectivity is lost when performing firmware upgrades or when the ToR switch fails.

When using a VSX pair of ToR switches, the access layer provides physical switch redundancy to directly attached hosts. This model supports uninterrupted host connectivity, even when one of the ToR switches fails or a firmware upgrade is performed. Each access layer switch also is connected to each core switch. All core links across redundant access switches are members of the same MC-LAG for redundancy and loop avoidance.

Planning the Deployment

This section provides sample values and rationale for naming and numbering schemes. Adjust values and formats as needed to accommodate specific requirements. Using a consistent approach in the physical and logical configurations improves the management and troubleshooting characteristics of a network.

Naming Conventions

Establish a switch naming convention that indicates the switch type, role, and location to simplify identification and increase operating efficiency.

Example values used in this guide:

Switch Name	Role	Description
RSVDC-CORE1-1	Core	Roseville Data Center Core Switch, VSX Pair Member 1 (primary)
RSVDC-CORE1-2	Core	Roseville Data Center Core Switch, VSX Pair Member 2 (secondary)
RSVDC- ACCESS1-1	Access	Top-of-Rack Access Switch in Rack 1, VSX Pair Member #1 (primary)
RSVDC- ACCESS1-2	Access	Top-of-Rack Access Switch in Rack #1, VSX Pair Member 2 (secondary)

Aruba Central Groups

Aruba Central organizes devices in groups with common configuration elements. Two functional roles in the two-tier data center architecture share configuration elements: the data center core and access layers. An Aruba Central group should be created for each layer.

Example Aruba Central groups used in this guide are:

- DC-RSVCORE
- DC-RSVACESS

Aruba Central Sites

In addition to group membership, a device can be associated with a site that represents a physical location. Sites can be used to aggregate visibility, statistics, and troubleshooting tools across switches that are members of different groups.

In this guide, all data center switches are assigned to a site named **RSVDC**.

IP Address Planning

Plan a consistent IP numbering scheme with values that can accommodate the current deployment size and leave room for growth. Define a range that can represent loopback addresses, IP addresses used in support protocols, and a range for data center hosts. It is beneficial to assign data center host subnets from a larger range of maskable IP addresses that summarizes all host subnets in the data center.

Example IP address ranges used in this guide:

Subnet	Functional Description
10.255.12.0/24	Routed interface IP addresses

Subnet	Functional Description
10.250.12.0/24	Loopback IP addresses
10.12.0.0/16	Summary range of all data center host subnets
10.12.101.0/24	Example of a specific data center host subnet

MAC Address Planning

A Locally Administered Address (LAA) should be used when defining virtual MAC addresses for VSX and active gateway functions. This is required when configuring an Active Gateway for an SVI on a VSX pair and when configuring the system MAC address of VSX. An LAA is a MAC in one of the four formats shown below:

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

The *x* positions can contain any valid hex value. It is helpful to create a hexadecimal representation of the associated IP address or VLAN ID using the hex positions. For more details on the LAA format, see the IEEE tutorial guide.

In this guide, VSX system MAC addresses are set to 02:00:00:10:xx, where xx is replaced with the rack number of the VSX pair and the core switches use a value of 00.

Active Gateway MAC address are set to 02:00:xx:xx:xx, where the last four octets are assigned a hexadecimal representation of the Active Gateway IP address. For example, the IP address 10.1.101.1 results in a MAC address of 02:00:0a:01:65:01. This simple method ensures MAC address uniqueness associated with Active Gateway IP addresses for troubleshooting purposes.

Prepare Switches

After initial unboxing and inventory, the next step in deploying a data center network requires physical installation of network switches.

Switch Installation

Verify the airflow configuration for the products to be installed to ensure that they support the cooling design for the data center. If required, an optional air duct kit is available for Aruba data center top-of-rack (ToR) switches to redirect hot air away from servers inside the rack.

Before installing switches, download the Aruba Installation Guide for the specific models. Review the Installation Guide before installing and deploying the switches. Carefully review requirements for power, cooling, and mounting to ensure that the data center environment is outfitted adequately for safe, secure operation.

Step 1 Open a web browser and navigate to the Aruba Support Portal at https://asp.arubanetworks.com/.

Step 2 On the Support Portal page, select the Software & Documents tab.

a Hewlett Packard Enterprise company	<mark>Support</mark> Portal	
ASP v4.5 Rel Aruba Support Por	eased tal v4.5 includes User management en	hancements. Please review the Feature Pr e
Get started now and I	og in or register for a HPE Passport acc	count. You can also email us for help or fee
Create and mar	ment	Notifications

Step 3 On the Software & Documents tab, select Switches.

Service Management	Software & Documents	Notifications
Search for product docume	ntation, software updates, a	and release notes for your Aruba products
Hobility Controllers	(AOS)	⊖ Central
🕑 Switches		O NetInsight
⊖ ClearPass Policy Mar	nager (CPPM)	⊖ Virtual Intranet Access (VIA)
🔿 AirWave		Analytics and Location Engine (ALE)
Access Points		HPE DataCenter Switches
🕑 SD-WAN		HPE FlexNetwork Switches
ClearPass Device Ins	ight (CPDI)	\varTheta HPE Intelligent Management Center (IMC)

Step 4 Select the filter options on the left.

- File Type: Document
- Product: Aruba Switches

FILTERS
File Type
<mark> 🕒</mark> Document (2161)
Product ✓ Aruba Switches (2161)

• File Category: Installation Guide

File Category
✓ Installation Guide (157)
Release Type
Standard (157)

Step 5 Download the Installation Guide version for the switch model to be installed.

Step 6 Complete the physical installation of switches in the racks.

NOTE:

Core switches should be installed in a central location that meets cable distance requirements for the media used between core and access switches. Access switches should be installed at top-of-rack in high-density environments or middle-of-row in low-density environments.

Physical Cabling

Consistent port selection for core and access switches increases the ease of configuration management, monitoring, reporting, and troubleshooting tasks in the data center.

Document all connections.

Ensure that distance limitations are observed for the chosen host connection media and between switches.

Refer to the "Data Center Design" section for guidance on cabling design options for the installation.

Top of Rack Cabling

In a redundant ToR configuration, the first two uplink ports should be allocated to interconnect redundant peers (ports 49-50 on 8325-48Y8C and 10000-48Y6C switches), which provides physical link redundancy and sufficient bandwidth to accommodate a core uplink failure on one of the switches.

Two links between redundant peers are sufficient for most deployments unless the data center host implementation may result in high-traffic use of the inter-switch links under normal operating conditions, such as when many hosts in a rack are single-homed to only one of the redundant switches, or when the VM guest redundancy model uses only a single link to transmit traffic.

The heartbeat between a ToR redundant pair should be configured to use the out-of-band management port. Alternatively, the highest numbered non-uplink port can be used as a heartbeat link.

Before deploying ToR configurations that require server connectivity at multiple speeds, review the switch guide to determine if adjacent ports are affected by changing port speeds.

Core-to-Access Cabling

The illustration below shows the physical port configuration on an 8325 32-port core switch.



Figure 8: Spine switch

The core switches in a two-tier data center operate as a redundant VSX pair. The last two ports in a 1U core switch should be allocated to the inter-switch link (ISL) between them (ports 31-32 on an 8325-32C). When using a chassis-based switch model, the inter-switch links should use the last port on two different line cards to add line card diversity, enabling the ISL to continue to function in case of a single line card failure.

Connections from the core to access switches should begin with port 1. In a dual ToR configuration, each core switch must be connected to each ToR redundant switch. A 32-port core switch supports up to 14 racks in this design, after considering the inter-switch and external connectivity links. Use the same port number on each core switch to connect to the same access switch to simplify switch management and documentation. For example, assign port 1 of each core switch to connect to the same access switch.

Management

Out-of-Band Management

For an Aruba ESP data center, using a dedicated management LAN is strongly recommended. A dedicated management LAN on separate physical infrastructure ensures reliable connectivity to data center infrastructure for automation, orchestration, and management access. CX data center switches should be connected to the management network using their physical out-of-band (OOB) management port.

Deploy management LAN switches at the top-of-rack position. Plan for an IP subnet with enough capacity to support all switch and host OOB management ports in the data center. DNS and NTP services for the data center should be reachable from the out-of-band management network. The management LAN also must allow outbound connectivity to the Aruba Central cloud management platform.

Configuration steps for the management LAN are not covered in this guide.

DHCP

A new switch must receive an IP address, DNS server address, and a default gateway via DHCP in order to enable successful Zero Touch Provisioning.

In a data center, it is recommended to reserve an IP address for each switch on a DHCP server. This ensures a predictable IP address for local management connections, such as SSH, while also enabling the switch to contact Aruba Central on boot.

When switches are unpacked and prepared for bench configuration or rack mounting, access the orange luggage tag on the switch and record the base MAC address. The MAC address of the management interface is the base MAC + 1. For example, A0:A0:01:00:00 becomes A0:A0:01:00:00:01. Use this management MAC address to create a DHCP reservation.

Static Addressing

Static IP and gateway address assignments can be used when Zero Touch Provisioning is not required. A DNS server also must be assigned to enable reachability to Aruba Central.

Central On-Premise

When organizational policy requires on-premise management of data center infrastructure, Aruba Central On-Premise (CoP) enables customers to run the Aruba Central management platform on local infrastructure. CoP supports CX 8xxx and 6400 series switches.

This guide does not cover the installation or use of CoP. Refer to the *Aruba Central On-Premises Supported Devices Reference Guide, Aruba Central (on-premises) User Guide, and Aruba Central (on-premises) Release Notes* in the Aruba Support Portal for additional information.

Aruba Central Initial Configuration

This guide demonstrates initial configuration of Aruba Central UI *groups* and *sites* and the assignment of switches to both configurations.

Switches with a common set of configuration elements should be assigned to the same Central UI group. In a Two-Tier data center, one group is defined for core switches and a second group for access switches.

Configuration common to both groups is defined once for the core group, then cloned to create the access group.

Features configured at the group level include:

- the hostname,
- admin account password,
- Network Time Protocol (NTP) servers,
- Domain Name System (DNS) servers,
- VLANs,
- Spanning-Tree,
- Terminal Access Controller Access Control System (TACACS) servers,
- Authentication, Authorization, and Accounting (AAA) servers.

Best practice is to use as few groups as necessary to provide logical organization for the network and consistent configuration among devices. Configuration is not shared among groups.

Switches in the same physical location can be assigned to the same Central Site to aggregate statistics, reporting, and troubleshooting tools.

Create Core Switch Group

Step 1 Open HPE GreenLake in a web browser and login with administrator credentials.

Step 2 Locate the account associated with the data center switches and click Go to Account.

Step 3 Click Launch in the Aruba Central tile.

Step 4 On the left Aruba Central navigation menu, click Global.

HPE GreenLake				
aruba Central		Q Search or		
Customer: Orange TME	~	<u> </u>		
🛱 Global	Network Health	WAN Health		

Step 5 On the dropdown, click the **Groups** column title.

HPE GreenLake		
aruba Cent	ral	
Customer: Orange TME		گ
 		Network Structure
요 Global		
Y Filter lists		
ដ្ឋGroups ®		∎Sites
BR-BHAM-01 BR-IACITY01 BR-IACITY02 BR-SAC01 BR-SJC01		3HAM-01 3R-SAC01 DC-RSV DSM-DC-01 ESP-MB01

Step 6 At the upper right corner of the **Groups** table, click the **+** (plus sign).

HPE GreenLake							1	88
orubo Central			Q Search or ask Aruba		Q	¢	?	ሐ
Customer: Orange TME		ដំ	•					
🛱 Global ଁ	Netwo	ork Structure	Platform Integration					
Applications	←	Groups Combine de	(33) vices with common configuration into	o a single group to apply the same configuration		Q	+	
Security		→ Group Nam	ie					
	>	All connected	d devices (107)					
8 Network Services	>	Unprovisione	ed devices (4)					
— Analyze	>	default (9) ★						
🗘 Alerts & Events	>	BR-BHAM-01 ((2)					

Step 7 In the **Add Group** wizard, enter a UI group name for the data center core switches in the **Name** field, click the **Switches** checkbox, then click **Next**.

Add Group			
Name DC-RSVCORE			
Group will contain:			
Access points			
Gateways			
Switches			
Configure using templates	i -		
Enable this option to use scr configuration pages.	ipts/templates	s instead of device	
		Cancel	Next

Step 8 Click the AOS-CX only radio button, then click Add.

← Add Group	
Type of switches used in this group:	
● AOS-CX only ○ AOS-S only ○ Both AOS-CX and AOS-S	
Monitoring only for AOS-CX	
Make these the preferred group settings	

Configure Core Switch Group Settings

Device configuration can be performed at the UI group level or at an individual device level. In this section, the core switch group is defined with initial configuration settings. Configuration defined at the group level is applied to all member switches, but exceptions can be made at the individual device level.

The access group is cloned from the core group, inheriting all group level settings at the time of cloning. In this initial configuration of the core switch group, only values shared with the access group are defined.

Step 1 On the left navigation menu, click Global.

HPE GreenLake				
aruba Central		Q Search or		
Customer: Orange TME	<u>~</u>	<u> </u>		
🛱 Global	Network Health	WAN Health		

Step 2 In the Groups column, click the data center core switch group name.

HPE GreenLake	
aruba Central	
Customer: Orange TME	
硷 Global	\bigcirc
요 Global	
∀dc-	
ជGroups	
DC-RSVCORE	
DC-RSVCORE	
NOTE	

After clicking the group name, text can be entered immediately in the **Filter lists** field. Enter a portion of the switch group name in the **Filter lists** field to display items containing the string. The filter applies simultaneously to the groups, sites, and labels columns.

Step 3 On the left navigation menu, click Devices.

HPE GreenLake				
	aruba Central			
Cu	stomer: Orange TME			
ä	DC-RSVCORE	\bigcirc		
— Ma	anage			
88	Overview			
0	Devices			
Ĺ	Clients			
0	Guests			

Step 4 At the upper right of the Switches pane, click Config.

HPE GreenLake		00
aruba Central	Q Search or ask Aruba	۹ 🧔 🥠
Customer: Orange TME	Switches	li. ∷≣ 🔯 Summary List Config
ជ dc-rsvcore	MultiEdit •	
— Manage ————	Access to AOS-CX search and custom configuration (editor & express configuration).	Configuration Status

Step 5 In the **Set Device Password** window, enter the switch **Administrator password** value, then click **SAVE**.

SET DEVICE PASSWORD
Please specify an administrator password for devices in this group. Further configuration of the group will be prohibited until a password is set.
Administrator password
•••••
CANCEL SAVE

Step 6 In the System tile, click Properties.

HPE GreenLake	
orubo Central	Q Search or a
Customer: Orange TME	
다 DC-RSVCORE 이	MultiEdit
— Manage ————	Access to AOS-CX search and custom configuration (
B Overview	System
Devices	Properties Contact, location, time zone and VRF
🗖 Clients	HTTP Proxy
🙁 Guests	HTTP proxy server integration
Applications	SNMP SNMPv2 communities, SNMPv3 users and trap destinations

Step 7 In the **Edit Properties** window, assign the following values, then click **SAVE**. - **Contact**: *netadmin@orangetme.local* - **Location**: *DC01*, *Roseville*, *CA* - **Timezone**: *Los Angeles* (*UTC*-8:00) - **VRF**: *Management* - **DNS servers**: 10.2.120.98, 10.2.120.99 - **NTP servers**: 10.2.120.98, 10.2.120.99

Contact	VRF	Administrator username
netadinin@orangetine.iocai	VRF	admin
Location		Administrator password
DC01, Roseville, CA	DNS servers 10.2.120.98	
Timezone	10.2.120.99	
	T	
	NTP servers 10.2.120.98	
	10 2 120 99	
	+	

NOTE:

Set the VRF to the network where DNS and NTP will be reachable. When using a dedicated out-of-band management network connected to the mgmt interface, the *Management* value should be selected for **VRF**.Enter a complete IP address for DNS and NTP servers to make the + (plus sign) appear for entering additional servers.

Step 8 In the Security tile, select Authentication Servers.

HPE GreenLake		
aruba Central	Q Searc	h or ask Aruba
Customer: Orange TME		
ជ dc-rsvcore 이	MultiEdit	
— Manage —	Access to AOS-CX search and custom configuration (edit	or & express configuration).
🗄 Overview	System	Interfaces
Devices	Properties Contact, location, time zone and VRF	Ports & Link Aggregations Specific ports, LAGs and VLAN assignments
🗖 Clients	HTTP Proxy	
🙁 Guests	HTTP proxy server integration	Security
Applications	SNMP SNMPv2 communities, SNMPv3 users and trap destinations	Authentication Servers RADIUS & TACACS
Security	Logging	Authentication 802.1X and MAC authentication
- Analyze	Administrator	Access Control
Alerts & Events	Local device administration	Access policies and rules
🔀 Audit Trail	Source Interface	Dynamic Segmentation User-based tunneling
🖏 Tools	Stacking	Client Roles Client roles and local attributes
🛍 Reports	Switch stacks and chassis	

Step 9 Mouse-over the TACACS row. At the far right of the TACACS row, click the edit icon (pencil).

HPE GreenLake			
Central		Q Search or ask Art	ıba
Customer: Orange TME			
ជ dc-rsvcore	MultiEdit		
— Manage ———	Access to AOS-CX search and	custom configuration (editor & express	configuration).
🗄 Overview	← Server Groups	5 (3)	
Devices	Name	Servers	
	Cloud Auth	0	
	RADIUS	0	
🙁 Guests	TACACS	0	1
Applications			Edit
Security			

Step 10 At the top right corner of the **TACACS Servers** table, click the **+** (plus sign).

HPE GreenLake						00	}
aruba Central		Search or ask Aruba		۹	¢	0	ሕ
Customer: Orange TME				il.	i =	6) 6 m
DC-RSVCORE	Switches			Summary	List	Com	'b
— Manage ————	Access to AOS-C	search and custom configuration (editor & express configuration).		Conf	igurati	on Stat	tus
B Overview	🗲 ТАСА	CS Servers			ŀ	+ 😳)
Devices	FQDN or IP a	ddress	VRF		Add TAC	ACS Server	
□ Clients							
😩 Guests							
Applications		No data to display					
Security							

Step 11 Assign the following settings on the **Add TACACS** page, then click **Apply**. - **FQDN or IP address:** *10.2.120.94*

- Authentication Port: 49 (default)
- VRF: Management
- Shared secret: < shared secret >
- Timeout (secs): 5 (default)

FQDN or IP address 10.2.120.94	Shared secret
Authentication Port	Timeout (secs)
49	5
VRF	
Management V	

Step 12 Assign additional servers by clicking the + (plus sign) at the top right corner of the **TACACS Servers** table.

Step 13 After all servers are added, click SAVE.

HPE GreenLake				88
orubo Central	Q Search or ask Aruba		Q	¢ 🛛 🖁
Customer: Orange TME			II. Summary	∷⊒ 👸 List Config
ជ dc-rsvcore 이				
- Manage	Multiedit Access to AOS-CX search and custom configuration (editor & express configuration).		Cont	figuration Status
🗄 Overview	TACACS Servers (2)			+ 💬
Devices	FQDN or IP address	VRF		
G. Climte	10.2.120.94	Management		
	10.2.120.95	Management		
🖧 Guests				
Applications				
Security				
— Analyze ———				
🗘 Alerts & Events				
🗷 Audit Trail				
🖏 Tools	O Changes will be deployed on all	X switches in the group CA	NCEL	SAVE

Step 14 At the top left of the **Server Groups** table, click ← (left arrow).

HPE GreenLake				
orubo Central				
Customer: Orange TME				
ជ DC-RSVCORE	MultiEdit			
— Manage ————	- Manage Access to AOS-CX search and custom configu			
🗄 Overview	← Server Groups (3)			
Devices	Name			
	Cloud Auth			
	RADIUS			
🙁 Guests	TACACS			

12

Configure Group VLANs

Define the data center host VLANs shared by both core and access switches. Additional VLANs required only at the core level are defined in subsequent steps.

Step 1 In the Bridging tile, click VLANs.

HPE GreenLake				8
aruba Central	Q Search c	or ask Aruba	ې فې	ሐ
Customer: Orange TME	switches		II. ∷⊟ Summary List Con	<mark>}}</mark> nfig
다 DC-RSVCORE 이	MultiEdit			
— Manage —	Access to AOS-CX search and custom configuration (editor & express configuration).	Configuration Sta	atus
🗄 Overview	System	Interfaces	Bridging	
Devices	Properties Contact, location, time zone and VRF	Ports & Link Aggregations Specific ports, LAGs and VLAN assignments	VLANS Virtual subnet management	
🗔 Clients	HTTP Proxy	Socurity	Loop Prevention	
a Guests	SNMP	Authentication Servers	Loop protection and spanning tree	
Applications	SNMPv2 communities, SNMPv3 users and trap destinations	RADIUS & TACACS		

Step 2 At the top right of the VLANs table, click the + (plus sign).

HPE GreenLake					88		
Central		Q Search or ask Aruba			Q	? ب	ን ሕ
Customer: Orange TME	=				II. Summary	:≡ List	ැ ලි Config
ជ dc-rsvcore	Switches						
— Manage ————	Access to AOS-CX search a	Access to AOS-CX search and custom configuration (editor & express configuration).					
B Overview	$\leftarrow v_{LANs} (1) \qquad \qquad$						
Devices	ID	Name	Description	Admin Up	Voice		
Lī Clients	1	DEFAULT_VLAN_1		Enabled	Disabled		

Step 3 On the Add VLAN page, enter the following field values, then click ADD.

- ID: 101
- Name: PROD-WEB
- Description: < no value >
- Admin Up: < checked >
- Voice: < unchecked >

ID			
101			
Name			
PROD-WEB			
Description			
🗸 Admin Up			
Voice			
_			
Changes will be deployed	ad on all CV switches in the		

Step 4 Repeat this process to create additional data center host VLANs.

- **ID:** 102
- Name: PROD-DB
- Description: < no value >
- Admin Up: < checked >
- Voice: < unchecked >

Clone Core Group for Access Switches

Aruba Central supports cloning group settings to a new UI group. Follow the steps below to create an access switch group that contains the same initial settings configured for the core switch group.

Step 1 On the left navigation menu, click **DC-RSVCORE**.

Step 2 On the dropdown, click the Groups column heading.

Step 3 Enter search text in the Group Name column to filter displayed groups.

Step 4 Move the cursor to the right of the name, and click the **Clone Group** icon.

Step 5 On the **Clone Group** page, enter a name for the data center access switch group in the **Name** field, and click **Clone**.

Step 6 Verify that the new access switch group is populated in the list of groups.

Orubo Central		Q Search or ask Aruba		۾ 🤨 🕏
Customer: Orange TME				II. III 🚳
I DC-RSVCORE	MultiEdit Access to AOS-CX search a	nd custom configuration (editor & expre	ss configuration).	Configuration Stat
Overview	← VLANs (3)			0
Devices	ID	Name	Description	Admin Up
E Cliente	1	DEFAULT_VLAN_1		Enabled
	101	PROD-WEB		Enabled
Cuests	102	PROD-DB		Enabled
Applications				
Security				
Analyze	▶			
Alerts & Events				

Assign Switches to a Group

Use this procedure to assign switches to groups and synchronize initial configuration.

Step 1 Expand the **Unprovisioned devices** group by clicking > (greater than) next to its name.

NOTE: Only switches that were not previously configured in Central appear in the **Unprovisioned devices** group. If switches were removed from a different Central group for use in the data center, they appear in the **default** group.Switches new to Central must be identified by the unique serial number or MAC address.

Step 2 Click both core switches.

Step 3 In the lower right corner of the **Unprovisioned devices** group table, click the **Move** button.

Step 4 On the **Move Devices** page, select the appropriate destination group for the selected switches and click **Move**.

Step 5 Expand the list of switches for the destination group to verify that the switches moved.

NOTE:

The search filter in the top right corner of the Groups window can filter content to display devices matching the search criteria and the groups that contain those devices. The search criteria can match text in the **Name**, **Type**, **Serial Number**, and **MAC address** fields.Displayed group names also can be filtered by clicking the **Group Name** column heading and entering match criteria.

Step 6 Repeat this procedure to assign access switches to the access switch group.

HPE GreenLake				00 00
Orubo Central		Q Search o	or ask Aruba	۹ ¢ © ۸
Customer: Orange TME	۴			
🕸 Global 💦	Network Structure	Platform integration		
Security	← Groups Combine of	(35) devices with common configura	ition into a single group to apply the same configuration	Q +
% Network Services	√ Group Na All connect	me ed devices (109)		
Analyze	> Unprovision	ned devices (6)		
Alerts & Events	> default (9)	k .		
🛛 Audit Trail	> BR-BHAM-0	1 (2)		
Addit ITali	> BR-IACITY01	(4)		
🖏 Tools	> BR-IACITY02	(6)		
🛍 Reports	> BR-SAC01 (2) 📐		
- Launch	> BR-SJC01 (8)			
Launen	> BR-TME (2)			
Here and the second sec	> BR-WDSM02	2 (1)		
— Maintain ————	> BR-WHE01 (5)		
Firmware	> BR-WHE02 (1)		
	> BR-WHE03 (1)	0	
Granization	BR-WHE03-0	lone (0)		

Configure Switch Hostname

Step 1 On the left navigation menu, click **Global** and select the data center core switch group.

HPE GreenLake	
aruba Central	
Customer: Orange TME	
🛱 Global	
 	
[▼ dc-	
ជGroups	
DC-RSVACCESS DC-RSVCORE	
DC-RSVCORE	

Step 2 On the left navigation menu, select Devices.

HPE GreenLake				
	orubo Central			
Cu	stomer: Orange TME			
ä	DC-RSVCORE	\bigcirc		
— Ma	anage			
88	Overview			
0	Devices			
Ĺ	Clients			
0	Guests			

Step 3 Scroll horizontally to view the identifying serial number and click the name of the recently added switch.

HPE GreenLake							88
Central		Q Search or ask Aruba			۹	(ව
Customer: Orange TME	En Switzbor				li. Summary	i List	ැටි Config
ជ dc-rsvcore 이	Switches					_	
— Manage ————	SWITCHES • ONLINE 2 2	• OFFLINE 0					
B Overview							
Devises	SWITCHES						\odot
Devices		Last Seen	Usage	Firmware Version	♀ Serial/Stack ID		
🗖 Clients	• 8325	-	5 kbps	10.10.1010	TW00KM300P		
😩 Guests	* 8325	-	80 gbps	10.10.1010	TW00KM301K	U	PLINKS

Step 4 On the left navigation menu, click **Device**.

HPE GreenLake					
(aruba Central				
Cu	stomer: Orange TME				
(+ I	···· 8325	\oslash			
— Ma	inage	_			
88	Overview				
	Clients				
格	LAN				
٥	VSX				
0	Device				

Step 5 In the System tile, click Properties.

HPE GreenLake				
Orubo Central	Search or			
Customer: Orange TME				
← 📼 8325 📀	Switch MultiEdit			
— Manage ———	Access to AOS-CX search and custom configuration (editor & expr			
🗄 Overview	System			
🗖 Clients	Properties Contact, location, time zone and VRF			
ය 사	HTTP Proxy			
IO VSX	HTTP proxy server integration			
	SNMP			
Device	SNMPv2 communities, SNMPv3 users and trap destinations			
Analyze	Logging			
	Log server and event severity classification			
Д Alerts & Events	Administrator			
🛛 Audit Trail	Local device administration			
🔦 Tools	Source Interface			

Step 6 On the **Edit Properties** page, enter a hostname for the switch in the **Name** field, then click **SAVE**.
Name	- VRF	Administrator username
RSVDC-CORE1-1	VRF	admin
Contact	Management 🗸	- Administrator password
netadmin@orangetme.local	DNS servers	Automistrator password
	10.2.120.98	
Location	10.2.120.99	-
DC01, Roseville, CA	+	-
Timozono	NTP servers	
Los Angeles (UTC-08:00) V	10.2.120.98	-
	10.2.120.99	_
	+	

Step 7 To return to the device list, at the top of the left navigation menu, click ← (left arrow) next to the switch name.

HPE GreenLake							
aruba Central							
Customer: Orange TME							
← 8325	\oslash						
— Manage —							
B Overview							

Step 8 Repeat this procedure to assign a hostname for each switch in both data center groups.

NOTE:

It may take several minutes for a newly assigned name to display in the Central device list.

Configure Data Center Site

Step 1 At the top of the left navigation menu, click the current switch, then click the **Sites** column heading.

HPE GreenLake		
aruba Central		
Customer: Orange TME	=	0
← 📼 8325 🤇	Summary	Hardware
요 Global		
Filter lists		
ជGroups	勖 Sites 錄	
BR-BHAM-01 BR-ECMBR	BHAM-01 BR-SAC01	

Step 2 At the bottom left of the Network Structure pane, click New Site.

HPE GreenLake					
Orubo Central		Q Sear	ch or ask Aruba		
Customer: Orange TME	د Network Structure				
🕸 Global 💦					
a Guests	♥ Site Name	✓ Address	Device		
Applications	All Devices		109		
Security	Unassigned		19		
🗞 Network Services	BHAM-01	1030 Lakeway Dr	2		
— Analyze ———	BR-SAC01	3535 Elverta Rd	2		
🇘 Alerts & Events	DSM-DC-01	4090 Westown Pkwy	0		
🛛 Audit Trail	ESP-MB01	4199 Campus Dr	1		
La Tools	ESP-RS01	8501 foothills blvd	6		
	ESP-RS02	6280 America Center Dr, CA	2		
ш. Reports	ESP-RS03	27816 Jones Rd	0		
App Catalog	ESP-VPNC	3333 Scott Blvd	2		
			20 Sitor		
Firmware	Bulk upload		20 Siles		

Step 3 In the **CREATE NEW SITE** window, enter the site location information, then click **Add**.

CREATE NEW SITE
SITE NAME
RSVDC
STREET ADDRESS
8000 Foothills Blvd
СІТҮ
Roseville
United States
California 🗸
ZIP/POSTAL CODE
95747
LATITUDE (OPTIONAL)
LONGITUDE (OPTIONAL)
Add

Step 4 Click the **Site Name** column heading in the left table and enter search criteria to limit the site names displayed.

aruba Central		Q Search or ask Aruba							?
Customer: Orange TME	د Network Structure	Platform Integration	2						
🗟 Global 🛛 🔅		Hattorin integration							
— Manage —	¬ RSVD [®]	∀Address	Device C		∀Name	∀ Group	∀туре		
田 Overview	All Devices		113		SJCBR1-AC1-AC2	BR-SJC01	SWITCH		L
	Unassigned		14		Aruba-2930F-8	BR-BHAM-01	SWITCH		
	RSVDC	8000 Foothills Blvd	6		BR-IACITY01-S	BR-IACITY01	SWITCH		
					RSVCP-AC3-AP33	CP-RSVWLAN	IAP		

Step 5 Click the **Name** column heading in the right table and enter search criteria to limit the switch names displayed.

HPE GreenLake							
aruba Central	Q Sea	arch or ask Aruba				Q	@
Customer: Orange TME	Network Structure	ation					
ର୍ଦ୍ଧୁ Global 🛛 🔅							
🙁 Guests	SITE NAME RSVDC Y Address	Device		∑ RSVDC ×	∀ Group	∀туре	
Applications	All Devices	109		RSVDC-CORE1-2	DC-RSVCORE	SWITCH	
Security	Unassigned	19		RSVDC-CORE1-1	DC-RSVCORE	SWITCH	
🗞 Network Services	RSVDC 8000 Foothills Blvd	0		RSVDC-ACCESS2-1	DC-RSVACC	SWITCH	
— Analyze ———				RSVDC-ACCESS2-2	DC-RSVACC	SWITCH	
🇘 Alerts & Events				RSVDC-ACCESS1-1	DC-RSVACC	SWITCH	
🛛 Audit Trail			+	RSVDC-ACCESS1-2	DC-RSVACC	SWITCH	

Step 6 In the device list, select all data center core and access switches.

HPE GreenLake									
aruba Central		Q Sea	rch or ask Aruba					Q	¢
Customer: Orange TME	ې ۱								
🕸 Global 💦	Network Structure	Platform integra	luon						
🙁 Guests	▼ SITE NAME ▼ RSVDC	Address	Device		▼ RSVDC	×	ƳGroup	∀туре	
Applications	All Devices		109		RSVDC-CORE1-2	2	DC-RSVCORE	SWITCH	
Security	Unassigned		19		RSVDC-CORE1-		DC-RSVCORE	SWITCH	
🗞 Network Services	RSVDC 8	000 Foothills Blvd	0		RSVDC-ACCESS	2-1	DC-RSVACC	SWITCH	
— Analyze —					RSVDC-ACCESS	2-2	DC-RSVACC	SWITCH	
🇘 Alerts & Events					RSVDC-ACCESS	1-1	DC-RSVACC	SWITCH	
🛛 Audit Trail				+	RSVDC-ACCESS	1-2	DC-RSVACC	SWITCH	

Step 7 Click and hold on one device name and drag it to the group name on the left. When the group name is highlighted in blue, release the mouse button.

HPE GreenLake								
orubo Central		Q Sea	arch or ask Aruba				۹ 🔅	G
Customer: Orange TME	٤							
ର୍ଦ୍ଧ Global 📀	Network Structure	Platform Integration						
Applications	∑ rsvdc ×	√ Address	Device C		√ rsvdc ×	∀Group	∀туре	
 Security 	All Devices		109		RSVDC-CORE1-2	DC-RSVCORE	SWITCH	
🞖 Network Services	Unassigned		19		RSVDC-CORE1-1	DC-RSVCORE	SWITCH	
- Analyze	RSVDC	8000 Foothills Blvd	0		RSVDC-ACCESS2-1	DC-RSVACCESS	SWITCH	
Alerts & Events					RSVDC-ACCESS2-2	DC-RSVACCESS	SWITCH	
Audit Trail				-	RSVDC-ACCESS1-1	DC-RSVACCESS	SWITCH	
) Tasla					RSVDC-ACCESS1-2	DC-RSVACCESS	SWITCH	
- 100IS								
🗓 Reports							•	
— Launch ————							N-	
App Catalog								

Step 8 In the CONFIRMATION ACTION window, click Yes.



Step 9 In the site list, click the name of the data center site.

HPE GreenLake								
aruba Central		Q Sear	rch or ask Aruba				Q	\$?
Customer: Orange TME	ສໍ		t					
🗟 Global 💦	Network Structure	Platform Integra	tion					
थ Guests	▼ SITE NAME RSVDC ▼ A	ddress	Device		∇Name	𝕂 Group	∀туре	
Applications	All Devices		109		RSVDC-CORE1-2	DC-RSVCORE	SWITCH	
Security	Unassigned		13		RSVDC-CORE1-1	DC-RSVCORE	SWITCH	
🗞 Network Services	RSVDC 80	00 Foothills Blvd	6 🖍		RSVDC-ACCESS2-1	DC-RSVACC	SWITCH	
— Analyze ———					RSVDC-ACCESS2-2	DC-RSVACC	SWITCH	
✿ Alerts & Events					RSVDC-ACCESS1-1	DC-RSVACC	SWITCH	
🗷 Audit Trail				+	RSVDC-ACCESS1-2	DC-RSVACC	SWITCH	

Step 10 Verify that the complete list of data center switches appears in the device list on the right.

Verify Data Center Cabling

Step 1 At the top of the left navigation menu, click **Global**, then click the data center site name in the **Sites** column.

HPE GreenLake	
aruba Central	
Customer: Orange TME	្តែ
🛱 Global	Network Structure PI
요 Global	
[▼ rsv	×
ជGroups	∎Sites
CP- RSV ACC CP- RSV AGG CP- RSV CORE CP- RSV WLAN	RSVCP RSVDC RSVDC

Step 2 On the left navigation menu, click Tools.

	HPE GreenLake	
	orubo Central	
Cu	stomer: Orange TME	
	RSVDC	\oslash
— Ma	anage	—
88	Overview	
Q	Devices	
Lo	Clients	
	Applications	
0	Security	
) 0	Guests	
— Ar	alyze	
Ċ	Alerts & Events	
Ċ	Live Events	
Z	Tools	
Ĺ.	Reports	

Step 3 On the Tools menu at the top, click the Commands tab.

HPE GreenLake							
Central	Central Q Search or ask Aruba						
Customer: Orange TME	8		(F			
■ RSVDC	Network Check	Device Check	Commands	Console			
	Select a Device Typ	e, Select Devices, Add	the Commands and	d Run them			

Step 4 Click the Available Devices dropdown, then select all data center switches.

HPE GreenLake							
aruba Central		uba					
Customer: Orange TME	Network Check Device Check	ck Commands	Console				
🗈 RSVDC 🛛 📀	Network check Device chec	communus	console				
— Manage ————	Select a Device Type, Select Device	s Add the Commands and	Runthem				
🗄 Overview	Device Type Switch	SEARCH					
Devices	Select commands from one or mor	RSVDC-ACCESS1-1					
	Categories	RSVDC-ACCESS1-2					
Lo Clients	All Category	RSVDC-ACCESS2-1					
Applications		RSVDC-ACCESS2-2					
Security		RSVDC-CORE1-1					
9 Guests		RSVDC-CORE1-2					
- Analyze		* - Supports addition	al mandatory filters				

Step 5 In the **Categories** list, click **All Category**, enter *lldp* in the commands list filter, click **show lldp neighbor**, and click **Add** >.

HPE GreenLake						
aruba Central			Q Search or as	sk Aruba		٩
Customer: Orange TME	oc Natural Charle	Davies Chask	((annala		
B RSVDC		Device Check	Commands	Console		
— Manage —	Select a Device Ty Device Type	vpe, Select Devices, Ad	ld the Commands ar Available Devices	nd Run them		
B Overview	Select commands	from one or more ca	tegories	¥	h -	
Devices	Categories		γ Commands	5		Selected Commands
Clients	All Category				Add >	
Applications			F	No data to display	< Remove < Remove All	No data to display
Security						
🙁 Guests						
 Analyze △ Alerts & Events 			* - Supports addit + - Supports addit ^ - Cannot run wit	tional mandatory filters tional optional filters th other commands		This list of commands will run in the order of its sequence (Maximum is 20)

Step 6 At the lower left of the Commands pane, click RUN.

HPE GreenLake								
aruba Central			Q Search or ask	Aruba				۹
Customer: Orange TME	လို Network Check	စြ Device Check	() Commands	Console				
🗈 RSVDC 🛛 📀								
	Select a Device Type	e, Select Devices, Ac	dd the Commands an	id Run them				
— Manage —	Device Type Switch		Available Devices	~				
日 Overview	Select commands fi	rom one or more ca	tegories					
Devices	Categories		→ Commands				Selected Commands	
Lo Clients	All Category		show lacp aggre	gates		Add >	show lldp neighbor	
Applications			show lldp local	aces		< Remove		
Security			show loop-prote	ect		< Remove All		
🙁 Guests			show mac-addre	ess-table				
— Analyze ————			show module 144 Commands * - Supports addition	0 sele onal mandatory filters	cted		1 Commands This list of commands will run in th	0 selected
🗘 Alerts & Events			+ - Supports addition ^ - Cannot run with	onal optional filters other commands			its sequence (Maximum is 20)	
♪ Live Events	Repeat							
🔦 Tools	Devices which are Output history of	e already running co device with buffer s	mmands shall not exe pace issues shall be a	ecute newly added com utomatically cleared	nmands			
🔝 Reports	Few commands n	equire the log level t	o be set as debug to s	see the output				
- Maintain								
Firmware	RUN	RESET						

Step 7 Scroll down to the command output. Review the results for each switch to ensure that LLDP neighbor relationships are consistent with planned cabling.

HPE GreenLake								C	10
aruba Central		Q Search or ask	Aruba		(۹	٩	0	ሐ
Customer: Orange TME	Network Check	Commands	Console						
🗈 RSVDC 🛛 🔗	Network check Device check	commands	console						
— Manage ———	Output history of device with buffer	ommands shall not exec space issues shall be au	ute newly added commi tomatically cleared	ands					
🗄 Overview	Few commands require the log level	to be set as debug to se	e the output						
Devices									
🗖 Clients	RUN RESET								
Applications	DEVICE OUTPUT								
Security	DEVICE	i≡ Output for the o	levice: RSVDC-CORE1-	1		Q	☑ .	↓ , ;	0
🙁 Guests	Ø RSVDC-CORE1-2	 	0:28:fc:2b:00 1/1	/53	1/1/53	120	CLEA	\R	
- Analyze	⊘ RSVDC-CORE1-1	RSVDC-ACCESS1-1 1/1/2 54:8	0:28:fc:ca:00 1/1,	/53					
Alerts & Events	⊘ RSVDC-ACCESS2-1	1/1/3 b8:c RSVDC-ACCESS2-1	4:e7:d5:49:00 1/1.	/53					
Live Events	⊘ RSVDC-ACCESS2-2	1/1/4 b8:d RSVDC-ACCESS2-2	4:e7:d5:29:00 1/1.	/53	1/1/53	120			
Ļ LIVE LVEIKS	⊘ RSVDC-ACCESS1-1	RSVDC-FW1-1 1/1/6 04:9	0:81:00:5e:f6 1/1.	/52	Leaf Spine RPI to RSVDC				
🖏 Tools	⊘ RSVDC-ACCESS1-2	RSVDC-FW1-2 1/1/31 90:2 RSVDC-COPF1-2	0:c2:c3:d4:00 1/1.		VSX_ISL				
🛍 Reports		1/1/32 90:2 RSVDC-CORE1-2	0:c2:c3:d4:00 1/1,	/32	VSX_ISL				
— Maintain ————		mgmt bc:c RSVDC-POD1-OOBM	7:a5:d4:c0:80 1/1.	/14	1/1/14	120			
Firmware		=== Troubleshoot	ing session complet	ted ===					

NOTE:

To reduce line wrapping, click the three dots/dashes icon to the left of "*Output for the device:*" to toggle **Device** column visibility and expand the the output window. The output also can be expanded to fill the web browser page by clicking the fill screen icon ([]) at the upper right of the window header.

Two-Tier Core

Configure Two-Tier core switches as a VSX pair for Layer 2 aggregation of the data center access switches, IP data center services, and routing to the main campus.

Configure Core VSX ISL Interface

To establish a VSX relationship between the core switches, create a link aggregation (LAG) interface for assignment as the VSX data plane's inter-switch link (ISL). The LAG can be defined at the Central UI group level when using the same ports for the VSX ISL on both core switches.

Step 1 On the left **Aruba Central** menu, click the current context, then click the data center core switch group name in the **Groups** column.

HPE GreenLake	
aruba Central	
Customer: Orange TME	
🕺 Global	0
요 Global	
⟨∇ dc-	
ជGroups	Π
DC-RSVACCESS	
DC-RSVCORE	
DC-RSVCORE	
NOTE:	

The current context in the screenshot above is **Global**.



Step 2 On the left navigation menu, click Devices.

Step 3 At the upper right of the Switches pane, click Config.

HPE GreenLake			88			
Central	Search or ask Aruba	Q 🤵	• 🔿 🙈			
Customer: Orange TME	Switches	II. ∷⊟ Summary List	<mark>ැලි</mark> Config			
법 DC-RSVCORE	MultiEdit 🖜					
— Manage ————	Access to AOS-CX search and custom configuration (editor & express configuration).	ess to AOS-CX search and custom configuration (editor & express configuration).				

Step 4 In the Interfaces tile, click Ports & Link Aggregations

HPE GreenLake						
aruba Central	Q Search or	r ask Aruba				
Customer: Orange TME						
다. a dc-rsvcore	switches					
— Manage ———	Access to AOS-CX search and custom configuration (editor & expres	s configuration).				
🗄 Overview	System	Interfaces				
Devices	Properties Contact, location, time zone and VRF	Ports & Link Aggregations Specific ports, LAGs and VLAN assignments				

Step 5 Scroll to the right of the **Ports & Link Aggregations** table, and click the **+** (plus sign) at the upper right.

HPE GreenLake									88
Central			Q Search or a	ask Aruba			Q	٩	() ଲ
Customer: Orange TME	Switches						II. Summary	:≡ List	Config
법 DC-RSVCORE 이	MultiEdit								
— Manage ————	Access to AOS-0	CX search and cus	stom configuration (editor & express	configuration).			Confi	gurati	on Status
🗄 Overview								Q	+ 💬
Devices	Admin Up		Speed Duplex	IP Address	VLAN Mode	Native VLAN	Access VLAN		
	Enabled								

Step 6 On the Add LAG page, enter the following values and click ADD:

- Name: lag256
- **Description:** VSX-ISL-LAG
- Port Members: 1/1/31, 1/1/32
- Speed Duplex: <no value> (default)
- VLAN Mode: trunk
- Native VLAN: 1 (default)
- Allowed VLANs: <no value> (default)
- Admin Up: checked
- Aggregation Mode: LACP Active

Name lag256		Routing	Admin Up
		VLAN Mode	
Description		trunk 🗸	
VSX-ISL-LAG		Netice MI AN	Aggregation Mode
			1551 c54 don mode
Port Members		<u> </u>	
1/1/31, 1/1/32	\sim		
		Allowed VLANs	
Speed Duplex	~		

Step 7 In the **Ports & Link Aggregations** table's title row, click ← (left arrow) to return to the main configuration page.

HPE GreenLake							
Orubo Central				Q S			
Customer: Orange TME							
다 DC-RSVCORE	Switches						
— Manage —	Access to AOS-0	CX search and	custom configurat	ion (editor			
🗄 Overview	← Port	s & Link A	ggregations	(54)			
Devices	Number		Description				
	lag1		RACK-1				
	lag2		RACK-2				

Configure Routing VLAN

In this topology, a VLAN is created for routing traffic to upstream external networks. The same VLAN is used to establish a routed transit path between the core switches using the VSX ISL. If one of the core switches loses its external network peering, external reachability information is learned from the ISL and external hosts are still reachable from the other core switch.

NOTE:

When more than one VRF is present, a VLAN per VRF is created. This sample topology uses only the default VRF, so only one VLAN is created.

Step 1 In the Bridging tile, click VLANs.

HPE GreenLake				00
aruba Central	Q Sea	rch or ask Aruba	۹	🌻 🕐 🔒
Customer: Orange TME	Switches		ii. Summary	:⊟ 👸 List Config
법 DC-RSVCORE 이	MultiEdit			
— Manage —	Access to AOS-CX search and custom configuration (ed	litor & express configuration).	Con	iguration Status
🗄 Overview	System	Interfaces	Bridging	
Devices	Properties Contact, location, time zone and VRF	Ports & Link Aggregations Specific ports, LAGs and VLAN assignments	VLANs Virtual subnet management	
Clients	HTTP Proxy	Security	Loop Prevention	
🙁 Guests	ni re proxy server integration	becancy	Loop protection and spanning tree	

Step 2 In the upper right of the **VLANs** table, click the **+** (plus sign).

HPE GreenLake								88
aruba Central			Q Search or ask Aruba			Q	٩	0 A
Customer: Orange TME	Switches					II. Summary	List	Config
ជ dc-rsvcore 이	MultiEdit	•						_
— Manage —	Access to AOS-	CX search and	custom configuration (editor & express configuration	on).		Confi	gurati	on Status
B Overview	← VLA	Ns (3)					Q	+ 💬
Devices	ID		Name	Description	Admin Up	Voice		
	1		DEFAULT_VLAN_1		Enabled	Disabled		

Step 3 On the Add VLAN page, enter the following field values, then click ADD.

- ID: 4000
- Name: CORE-ROUTING
- Description: <no value> (default)
- Admin Up: checked (default)
- Voice: unchecked (default)

ID			
4000			
Name			
CORE-ROUTING			
Description			
🗸 Admin Up			
Voice			

Step 4 In the **VLANs** table's title row, click ← (left arrow) to return to the main configuration page.

HPE GreenLake	
aruba Central	
Customer: Orange TME	
다 DC-RSVCORE	Switches
– Manage –	Access to AOS-CX search and
🗄 Overview	← VLANs (6)
Devices	ID
🗖 Clients	1 101

Spanning Tree

Multi-chassis link aggregations (MC-LAGs) provide the primary loop prevention mechanism in a Two-Tier architecture. When configured on both core and access switches, MC-LAGs allow loop-free forwarding on all inter-switch links simultaneously in both directions, .

MC-LAGs provide efficient, hash-based load balancing with better performance than individually mapped VLANs to Multiple Spanning-Tree (MST) instances.

Spanning-tree (STP) is configured as a backup loop prevention mechanism in case of operator cabling errors when connecting hosts to top of rack switches.

Setting the spanning-tree priority to 0 ensures that the core VSX pair of switches is the STP root.

Step 1 In the Bridging tile, click Loop Prevention.

HPE GreenLake			88
aruba Central	Q Search or	r ask Aruba	۾ 🧔 🕏
Customer: Orange TME			II. ∷≣ 🚱
다 dc-rsvcore	Switches MultiEdit		
— Manage ————	Access to AOS-CX search and custom configuration	n (editor & express configuration).	Configuration Status
🗄 Overview	System	Interfaces	Bridging
Devices	Properties Contact, location, time zone and VRF	Ports & Link Aggregations Specific ports, LAGs and VLAN assignments	VLANS Virtual subnet management
□ Clients	HTTP Proxy	Security	Loop Prevention
😩 Guests	HTTP proxy server integration	Security	Loop protection and spanning tree

Step 2 In the **Loop Prevention** window, set the following **Spanning Tree** values, then click **SAVE**. - **Priority:** *0* - **Region:** *RSVDC*

👓 Switches				ll. ∷≣ Summary List	<mark>ැරිා</mark> Config
MultiEdit Access to AO	t OD DS-CX search and custom configurati	ion (editor & express configuration).		Configura	ition Status
← Lo	oop Prevention				
- Sp	panning Tree 💶				_
Moc MS	de ITP 💙	Priority Region 0 ✓ RSVDC			
P	orts (55)				Q
Nu	ımber	Description	LAG Members	Loop Protection	
lagi	256	VSX_ISL_LAG	1/1/31, 1/1/32	Disabled	
1/1	1/1			Disabled	
1.14	10			Disabled	_
		O Changes wi	ll be deployed on all CX switches in the group	CANCEL	SAVE

Enter MultiEdit Configuration

The Central UI interface provides simplified access to most common switch configuration features. MultiEdit is a tool in the Central UI for CX switches that enables configuration of any CX feature using CLI syntax. MultiEdit provides syntax checking, colorization, and command completion.

For complete details on using MultiEdit, refer to the Editing Configuration on AOS-CX section of Central online help.

The text configuration snippets in the following steps are intended for copying and pasting into MultiEdit. To prevent potential copy/paste errors, scroll to the bottom of the configuration, create a new line, then paste the new configuration lines. MultiEdit automatically positions new lines in the correct configuration context.

Step 1 At the upper left of the Switches pane, click the MultiEdit enable slider.

HPE GreenLake	
aruba Central	C
Customer: Orange TME	
다 DC-RSVCORE	Switches MultiEdit
– Manage –	Access to AOS-CX search and custom

Step 2 Click both core switches in the Devices lists, then click EDIT CONFIG.

HPE GreenLake									
Central			Q Searc	h or ask Aruba				Q	۵ 🤹
Customer: Orange TME								ll. Summary	i≣ 👸 List Config
ជ dc-rsvcore 이	MultiEdit								
— Manage —	Access to AOS-C	< searc	h and custom configu	iration (editor & exp	oress configura	ation).		Configu	ration Status
🗄 Overview	Device-Lev	/el Co	onfiguration	er of the methods h		a configuration for	he colosted do is		
Devices	Contextual Search	h Engine	nces and choose eithe	er of the methods t		e configuration for	ne selected devic	.es.	
Lo Clients	Enter Search	Query	(e.g. nae-status:Crit	ical AND label:	SEARCH 8	FILTER Che	ck Search Doo	cumentation	
😩 Guests	Devices	(2)							\odot
Applications	Name	↓≞.	Firmware	Con	Status	Config	NAE	MAC A	IP A
Security	RSVDC-CORE	-1 -2	10.10.1030 10.10.1030	Jan 27, 2023 Jan 27, 2023	OnlineOnline	Sync Sync	Normal Normal	9020c2-c31400 9020c2-c3d400	172.16.104 172.16.104
Analyze							2 item(s)) selected Clea	Ir PRESS CONFIG
Audit TrailTools								Edit Config	

NOTE:

When using the Central MultiEditor, it is beneficial to save small sets of configuration at a time. This reduces the volume of configuration that must be inspected when errors occur and makes troubleshooting configuration elements faster.

Configure Core Switch VSX

The core switches are configured as a VSX pair to support Layer 2 multi-chassis link aggregation (MC-LAG) to the access layer switches. The previously defined LAG is assigned as the VSX data path inter-switch link (ISL). The out-of-band (OOB) *mgmt* interface is used for VSX keepalives to maximize the number of ports available to connect access switches.

Step 1 Enter the initial VSX configuration.

```
vsx
system-mac 02:00:00:00:10:00
inter-switch-link lag 256
role primary
keepalive peer 172.16.117.102 source 172.16.117.101 vrf mgmt
```

NOTE:

When the *mgmt* vrf is specified, the keepalive peer addresses are the IPs assigned to the outof-band management interfaces. When using DHCP IP address assignments on the OOB management network, DHCP reservations must be created for VSX paired switches to avoid future keepalive failures.

Step 2 Mouse-over the *role* value of **primary** to display the values for each individual switch, then right-click.

Step 3 In the **Modify Parameters** window, click **primary** under *RSVDC-CORE1-2*, select **secondary** from the menu, then click **SAVE CHANGES**.

Devices	<	Configuration
Selected 2/2		snmp-server system-contact netadmin@orangetme.local
ect single device for line numbers	\$	system-mac 02:00:00:00:10:00
RSVDC-CORE1-2	≥ ‼	inter-switch-link lag 256
		keepalive peer 172.16.104.102 source 172.16.104.101 vrf mgmt
		ip dns domain-name example.local vrf mgmt
		ip dns server-address 10.2.120.98 vrf mgmt
		ipydns server-address 10.2.120.99 vrf mgmt

NOTE:

Hover the mouse over the per-switch values to display a switch's assigned value.

Step 4 Modify the VSX keepalive **peer** and **source** parameters by right-clicking on the values.

Switch	peer	source
RSVDC-CORE1-1	172.16.117.102	172.16.117.101

Switch	peer	source
RSVDC-CORE1-2	172.16.117.101	172.16.117.102

Step 5 Assign a description and maximum MTU value to the VSX ISL physical interfaces.

```
interface 1/1/31
    description VSX-ISL
    mtu 9198
interface 1/1/32
    description VSX-ISL
    mtu 9198
```

Configure Core Switch MC-LAGs

Step 1 Create MC-LAG interfaces for connecting to redundant top-of-rack access switches and upstream firewalls.

```
interface lag 1 multi-chassis
   description RACK-1
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed all
    lacp mode active
    lacp fallback
   spanning-tree root-guard
interface lag 2 multi-chassis
   description RACK-2
   no shutdown
   no routing
   vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    lacp fallback
    spanning-tree root-guard
interface lag 101 multi-chassis
   description EXT-FW1-1
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 4000
    lacp mode active
   lacp fallback
   spanning-tree root-guard
interface lag 102 multi-chassis
   description EXT-FW1-2
   no shutdown
   no routing
    vlan trunk native 1
    vlan trunk allowed 4000
    lacp mode active
    lacp fallback
    spanning-tree root-guard
```

NOTE:

MC-LAG interfaces can scope trunked VLANs only to those required for a specific downstream rack. Tagging all VLANs on all core-to-access MC-LAGs supports ubiquitous host mobility across all racks within the Two-Tier structure and reduces the administrative overhead of maintaining VLAN assignments per rack.

Step 2 Assign physical interfaces to the MC-LAGs..

```
interface 1/1/1
    description RSVDC-ACCESS1-1
    no shutdown
   mtu 9198
   lag 1
interface 1/1/2
    description RSVDC-ACCESS1-2
    no shutdown
   mtu 9198
   lag 1
interface 1/1/3
   description RSVDC-ACCESS2-1
   no shutdown
   mtu 9198
   lag 2
interface 1/1/4
    description RSVDC-ACCESS2-2
    no shutdown
   mtu 9198
   lag 2
interface 1/1/29
    description EXT-FW1-1
   no shutdown
   mtu 9198
   lag 101
interface 1/1/30
    description EXT-FW1-2
    no shutdown
   mtu 9198
   lag 102
```

Step 3 Remove the following configuration line from interfaces configured above: vlan access 1

NOTE:

Interface LAG assignments and VLAN access statements cannot be assigned to an interface simultaneously. An error occurs when saving the MultiEdit configuration if the **vlan access 1** statement is not removed.

Configure Routing Services

In a Two-Tier architecture, the core switches provide IP gateways to downstream hosts, route traffic between data center hosts in different subnets, and route traffic between the data center and external networks.

Configure Routing Components

This sample deployment connects to a campus network via an active/passive pair of upstream firewalls. It is common to place firewalls between the data center and a campus network for granular policy enforcement. When using an active/passive redundant firewall pair, IP assignments are used only by the currently active firewall. Access control lists (ACLs) also can be used to augment firewall policy or in place of a firewall, when policy complexity does not require a dedicated appliance.

OSPF is the most common protocol used between Two-Tier data center core switches and external networks. Alternatively, BGP can be configured.

In the diagram below, OSPF adjacencies are formed between the two core switches and between each core switch and RSVDC-FW1-1, which is the active member of the firewall cluster pair. Under normal operating conditions, RSVDC-FW1-2 does not participate in routing or traffic forwarding. When RSVDC-FW1-2 becomes the active member of the firewall cluster, the OSPF sessions are moved and traffic is forwarded to RSVDC-FW1-2.



When more than one VRF is present, each VRF maintains its own set of OSPF peerings over a unique VLAN on the same physical links.

VSX combines two separate switches into a single, logical Layer 2 switch. Layer 3 functions remain independent. If an external link fails between one of the core switches and the upstream firewall, the same VLAN configured for external network reachability provides a routed transit path over the VSX ISL. An OSPF adjacency is configured between the core switches, which shares external network reachability between them.

Step 1 Set the switch profile.

```
profile l3-agg
```

NOTE:

The available profile options are platform dependent. Selecting a profile optimizes switch hardware resources for its role in the network. It is recommended to assign the *l3-agg* profile to CX 8325 and CX 10000 core switches. CX 8360 switches should use their default *aggregation-leaf* profile. CX 9300 switches should use their default *leaf* profile.

Step 2 Create the OSPF process.

```
router ospf 1
router-id 10.250.12.1
passive-interface default
area 0.0.0.0
```

Step 3 Mouse-over the OSPF router ID values *10.250.12.1*, right-click to set per switch values, set the **router-id** of RSVDC-CORE-1-2 to *10.250.12.2*, and click **SAVE CHANGES**.



Step 4 Create core switch loopback interfaces. The loopback IP should be the same value assigned to the OSPF router-id.

```
interface loopback 0
ip address 10.250.12.1/32
ip ospf 1 area 0.0.0.0
```

Step 5 Mouse-over the loopback 0 **ip address** value of *10.250.12.1*, right-click to set per switch values, set the **ip address** of RSVDC-CORE1-2 to *10.250.12.2/32*, and click **SAVE CHANGES**.

Devices	<		Configuration	Modify Parameters SAVE CHANGES
Selected 2/2			lag 256	Set same value for all devices
ect single device for line numbers			interface 1/1/32	Interface IP address
RSVDC-CORE1-1	\diamond		no shutdown	RSVDCCORET+1
RSVDC-CORE1-2	\diamond		mtu 9198	10.250.12.1/32
	Ť		lag 256	RSVIC CORET 2
			interface loopback 0	10.250.12.2/32
			ip address 10.250.12.1/32	
		**	ip ospf 1 area 0.0.0.0	
			interface vlan101	
			description PROD-WEB-SVI	
			ip mtu 9198	
			ip address A.B.C.D/M	
			active-gateway ip mac 02:00:0a:01:65:01	
			active-gateway ip 10.12.101.1	
			interface #1ap102	

Step 6 Configure the external/transit VLAN SVI.

```
interface vlan4000
description CORE-ROUTING-SVI
ip mtu 9198
ip address 10.255.12.1/29
ip ospf 1 area 0.0.0.0
no ip ospf passive
```

Step 7 Mouse-over the transit VLAN **ip address** value of *10.255.12.1*, right-click to set per switch values, set the **ip address** of RSVDC-CORE1-2 to *10.255.12.2/29*, and click **SAVE CHANGES**.

Devices <	Configuration	Modify Parameters SAVE CHANGES 🗙
Selected 2/2	interface vlan 4000	Set same value for all devices
elect single device for line numbers	description CORE-ROUTING-SVI	Interface IP address
RSVDC-CORE1-1 🛇	ip mtu 9198	RSVDC-CORE1-1
	ip address 10.255.12.1/29	10.255.12.1/29
KSVDC-CORET-2	ip ospf 1 area 0.0.0.0	RSVDC-CORE1-2
	no ip ospf passive	10.255.12.2/29
	snmp-server system-location DC01, Roseville, CA	
	snmp-server system-contact netadmin@orangetme.1	a de la construcción de la constru
	vsx	
	system-mac 02:00:00:00:10:00	

Configure Host VLAN SVIs

Step 1 Configure VLAN switched virtual interfaces (SVIs) for data center host VLANs. Core switches provide the default gateway to downstream data center hosts. An active gateway IP and MAC address are configured for each VLAN to allow both core switches to represent the same IP gateway.

```
interface vlan101
    description PROD-WEB-SVI
    ip mtu 9198
    ip address 10.12.101.2/24
    active-gateway ip mac 02:00:0a:01:65:01
    active-gateway ip 10.12.101.1
    ip ospf 1 area 0.0.0.0
interface vlan102
    description PROD-DB-SVI
    ip mtu 9198
    ip address 10.12.102.2/24
    active-gateway ip mac 02:00:0a:01:65:01
    active-gateway ip 10.12.102.1
    ip ospf 1 area 0.0.0.0
```

NOTE:

The sample active gateway MAC address associated with the virtual IP sets the locally administered bit to "1" and embeds a hexadecimal representation of the active gateway IP in the last four octets.

Step 2 Mouse-over the VLAN 101 **ip address** value of *10.12.101.2*, right-click to set per switch values, set the **ip address** of RSVDC-CORE1-2 to *10.12.101.3*, and click **SAVE CHANGES**.



Step 3 Mouse-over the VLAN 102 **ip address** value of *10.12.102.2*, right-click to set per switch values, set the **ip address** of RSVDC-CORE1-2 to *10.12.102.3*, and click **SAVE CHANGES**.

evices	<	0	Configuration	Modify Parameters SAVE CHANGES
Selected 2/2			lag 256	Set same value for all devices
t single device for line numbers			interface vlan101	Interface IP address
RSVDC-CORE1-1	\diamond		description PROD-WEB-SVI	HSVDC-CORET-1
RSVDC-CORE1-2			ip mtu 9198	10.12.102.2/24
	Ť		ip address A.B.C.D/M	HSVDC-CORE1-2
			active-gateway ip mac 02:00:0a:01:65:01	10.12.102.3/24
			active-gateway ip 10.12.101.1	
			interface vlan102	
			description PROD-DB-SVI	
			ip mtu 9198	
			ip address 10.12.102.2/24	
			active-gateway ip mac 02:00:0a:01:65:01	
			active-gateway ip 10.12.102.1	
			snmp-server system-location DC01, Roseville, CA	

Step 4 At the bottom right of the MultiEdit Configuration window, click **SAVE**.

Devices <	Configuration	
Selected 2/2 ct single device for line numbers RSVDC-CORE1-1	<pre>role SEL keepalive peer SEL source SEL vrf mgmt ip dns domain-name example.local vrf mgmt ip dns server-address 10.2.120.98 vrf mgmt ip dns server-address 10.2.120.99 vrf mgmt router ospf 1 router-id A.B.C.D passive-interface default area 0.0.0.0 https-server vrf mgmt configuration-lockout central managed</pre>	

Two-Tier Multicast

The ESP Two-Tier Data Center uses Protocol Independent Multicast—Sparse-Mode (PIM-SM) to distribute multicast source information and establish interface forwarding state. A centralized Rendezvous Point (RP) registers and distributes multicast sources throughout the network. The data center core switches perform multicast routing and typically point to an RP already established for campus usage to advertise data center sources and learn about campus sources. The Bootstrap Router (BSR) mechanism for PIM elects and learns the active RP. Internet Group Messaging Protocol (IGMP) is enabled on data center host interfaces (routed-only interfaces and VLAN/SVI interfaces) to identify multicast listeners. When a host is interested in received traffic for a multicast group, it sends an IGMP join message.

Step 1 Enable PIM routing on the core switches.

router pim enable active-active

Step 2 Enable PIM-SM on external and data center host VLANs.

Step 3 Enable IGMP on VLAN SVI interfaces for data center hosts.

```
interface vlan 101
ip igmp enable
interface vlan 102
ip igmp enable
```

Verify Operational State

Step 1 On the left navigation menu, click Tools.

	HPE GreenLake	
	aruba Central	
Cu	stomer: Orange TME	
IJ	DC-RSVCORE	0
— Ma	anage	_
88	Overview	
Q	Devices	
Ĺ	Clients	
ð	Guests	
::	Applications	
0	Security	
— An	alyze	-
Ų	Alerts & Events	
X	Audit Trail	
ez,	Tools	
ſ.	Reports	

Step 2 On the Tools menu at the top, click the Commands tab.

HPE GreenLake										
aruba Central			Q Search or asl	k Aruba						
Customer: Orange TME	Notwork Chock	Davise Check	Commands	Consolo						
ជ dc-rsvcore 🛛 🔿	Network Check	Device check	commands	Console						
	Select a Device Type, Select Devices, Add the Commands and Run th									

Step 3 Click the Available Devices dropdown, select both data center core switches, then click else-

	HPE GreenLake		
	orubo Central	Q Search or ask Aruba	
	Customer: Orange TME	کی ا	
	ជ DC-RSVCORE 이	Network Check Device Check	k Commands Console
	— Manage ————	Select a Device Type, Select Devices Device Type Switch	Add the Commands and Run them SEARCH
	🗄 Overview	Select commands from one or mor	RSVDC-CORE1-1
	Devices	Categories	RSVDC-CORE1-2
where on the page.	🗖 Clients	All Category	

Step 4 In the **Categories** list, click **All Category**. Enter *vsx* in the commands list filter, click **show vsx status**, then click **Add** >.

HPE GreenLake				
aruba Central		Q Search or ask Aruba		٩
Customer: Orange TME				
ជ DC-RSVCORE 이	Network Check Device Check	Commands Console		
Manago	Select a Device Type, Select Devices,	Add the Commands and Run them		
	Switch	2 Switches		
CVerview	Select commands from one or more	categories		
Devices	Categories			Selected Commands
Clients	All Category			
2 Guests		No data to display	< Remove	No data to display
Applications				
Security				
- Analyze		 * - Supports additional mandatory filters + - Supports additional optional filters 	Th	iis list of commands will run in the order of its quence (Maximum is 20)
△ Alerts & Events		^ - Cannot run with other commands		

Step 5 Add the following additional commands to the Selected Commands list.

- show lacp interfaces
- show ip ospf interface all-vrfs

- show ip route all-vrfs
- show spanning-tree mst detail
- show ip pim
- show ip igmp
- show ntp status

Step 6 At the lower left of the Commands pane, click RUN.

Central		Q Search or ask	Aruba			۹	New Central	(
Customer: Orange TME	ස Network Check	Device Check	() Commands	Console						
Manage	Select a Device Type Device Type Switch	e, Select Devices, Ac	dd the Commands a Available Devices 2 Switches	nd Run them 🗸						
Devices	Categories	oni one or more ca	Comr Comr	Commands			Selected Commands			
Clients	All Category		show n	show ntp associations			show vsx status			
Guests Applications Security			show n	tp servers		Add > < Remove < Remove All	show lacp interfaces show ip ospf interface all-vrfs show ip route all-vrfs show spanning-tree mst deta			
Alerts & Events	Repeat		144 Com * - Suppo + - Suppo ^ - Canno	mands rts additional mandatory rts additional optional filt t run with other comman	0 selected filters ers ds		8 Commands This list of commands will run in sequence (Maximum is 20)	0 selected the order of its		
Tools Reports	Devices which are Output history of Few commands re	already running co device with buffer s equire the log level t	mmands shall not ex pace issues shall be to be set as debug to	ecute newly added con automatically cleared see the output	nmands					

Step 7 Scroll down to review the CLI command output for each switch. Verify key results for each command.

- show vsx status
 - ISL channel: In-Sync
 - ISL mgmt channel: operational
 - Config Sync Status: In-Sync
 - Device Role: set to primary and secondary on corresponding switches
 - Other VSX attributes display equal values for both VSX members

DEVICE OUTPUT				
DEVICE	E Output for the device: RSVDC-CORE1-1	Q	⊠ ±	53
Ø RSVDC-CORE1-1	=== Troubleshooting session started ===		CLEAR	ון
ØRSVDC-CORE1-2	Output Time: 2024-02-22 17:47:50 UTC COMMAND= show vsx status V5X Operational State TSL channel : In-Sync TSL channel : operational Config Sync Status : In-Sync NAE : peer_reachable HTTPS Server : peer_reachable Attribute Local Peer_reachable ISL link lag256 lag256 ISL version 2:00:00:00:10:00 2:00:00:00:10:00 Platform 325 Software Version GL, 10. 13. 1000 Device Role GL, 10. 13. 1000 GL. 10. 13. 1000 secondary			

- show lacp interfaces
 - Both Actor and Partner have corresponding interfaces for each MC-LAG.

- All Actor interfaces have a **Forwarding State** of "up" for all host facing MC-LAGs and the upstream core switch facing MC-LAGs.

DEVICE OUTPUT															
DEVICE	i≣ Output f	or the device:	RSVD	C-CORE	1-1							Q		⊥	0
⊘ RSVDC-CORE1-1 ⊘ RSVDC-CORE1-2	Output Tin COMMAND= s	ne: 2024–02– how lacp in	22 18: terfac	11:10 es	== UTC								CLI	AR	
	State abbn A - Active S - Short- C - Collec X - State Actor deta	abbreviations : P - Passive F - Aggregable I - Individual citive P - Passive F - Aggregable I - Individual hort-timeout L - Long-timeout N - InSync 0 - OutofSync ollecting D - Distributing tate m/c expired E - Default neighbor state details of all interfaces: 													
	Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State						
	1/1/1 1/1/2 1/1/3 1/1/4 1/1/29 1/1/30 1/1/31 1/1/32	lag1(mc) lag1(mc) lag2(mc) lag101(mc) lag102(mc) lag256 lag256	1 2 3 4 29 30 32 33	1 1 1 1 1 1 1	ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD	02:00:00:00:10:00 02:00:00:00:10:00 02:00:00:00:10:00 02:00:00:00:10:00 02:00:00:00:10:00 02:00:00:00:10:00 90:20:c2:c3:14:00 90:20:c2:c3:14:00	65534 65534 65534 65534 65534 65534 65534 65534 65534	1 2 2 101 102 256 256	up up up up up up up up						
	Partner de	tails of al	l inte	rfaces	:	TD									
	INTT	Aggr Name	Id Id	Port Pri	State	System-10 	System Pri	Aggr Key 							
	1/1/1 1/1/2 1/1/3 1/1/4 1/1/29 1/1/30 1/1/31 1/1/32	lag1(mc) lag1(mc) lag2(mc) lag2(mc) lag101(mc) lag102(mc) lag256 lag256	53 1053 53 1053 56 56 32 33	1 1 1 1 1 1	ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD ALFNCD	$\begin{array}{c} 02:00:00:00:10:01\\ 02:00:00:00:10:01\\ 02:00:00:00:10:01\\ 02:00:00:00:10:02\\ 02:00:00:00:10:02\\ 03:00:00:00:10:02\\ 03:00:00:00:10:02\\ 03:00:00:00:10:02\\ 03:00:00:00:00:10\\ 03:00:00:00:00:00\\ 00:20:00:00:00\\ 00:20:00:00:00\\ 00:20:00:00:00\\ 00:20:00:00\\ 00:00:00:00\\ 00:00:00:00\\ 00:00:00:00\\ 00:00:00:00\\ 00:00:00\\ 00:00:00\\ 00:00:00\\ 00:00:00\\ 00:00:00\\ 00:00:00\\ 00:00\\ 00:00:00\\ $	65534 65534 65534 65534 65534 65534 65534 65534 65534	255 255 255 101 102 256 256							×

- All Actor and Partner interfaces have a state of "ALFNCD".

- show ip ospf interface all-vrfs
 - All interfaces display Area "0.0.0.0" and Process "1".
 - VLAN 4000 State/Type is set to a valid value of DR, BDR or DR-other.
 - VLAN 4000 **DR** and **BDR** values are populated with IP addresses on the link.

DEVICE OUTPUT											
DEVICE	:≡ Output for the device: RSVDC-CORE1-1			Q		¥ 0					
Ø RSVDC-CORE1-1	0utput Time: 2024-02-22 18:11:16 UTC				CLE	AR					
⊘ RSVDC-CORE1-2	COMMAND= show ip ospf interface all-vrfs Codes: DR - Designated router BDR - Backup Designat	ed router									
	Interface loopback0 is up, line protocol is up										
	VRF : default IP Address : 10.250.12.1/32 Status : Up Hello Interval : 10 sec Transit Delay : 1 sec EFD : Disabled Cost Configured : NA State/Type : Loopback DR Link LSAs : NO Link LSAs : 0 Authentication : No	Process Area Network Type Dead Interval Retransmit Interval Link Speed Cost Calculated Router Priority BDR Checksum Sum Passive	: 1 : 0.0.0 : Loopback : 40 sec : 5 : NA : 1 : NA : 1 : NO : 0 : Yes								
	Codes: DR - Designated router BDR - Backup Designat	Codes: DR - Designated router BDR - Backup Designated router									
	Interface vlan101 is up, line protocol is up										
	VRF : default IP Address : 10.12.101.2/24 Status : Up Hello Interval : 10 sec Transit Delay : 1 sec BFD : Disabled Cost Configured : NA State/Type : DR DR Link LSAs : 0 Authentication : No	Process Area Network Type Dead Interval Retransmit Interval Link Speed Cost Calculated Router Priority BDR Checksum Sum Passive	: 1 0.0.0.0 : Broadcast : 5 sec : 1000 Mbps : 100 : 1 : No : Yes								
	Codes: DR - Designated router BDR - Backup Designated router										
	Interface vlan102 is up, line protocol is up	Interface vlan102 is up, line protocol is up									
	VRF : default IP Address : 10.12.102.2/24 Status : Up Hello Interval : 10 sec Transit Delay : 1 sec BFD : Disabled Cost Configured : NA State/Type : Po-other Dink LSAs : 0 Authentization : No	Process Area Network Type Dead Interval Link Speed Cost Calculated Router Priority BOR Checksum Sum Passive	: 1 0.0.0.0 : Broadcast : 5 sec : 1000 Mbps : 100 : 1 NO : 0 : Yes								
	Codes: DR - Designated router BDR - Backup Designat	ed router									
	Interface vlan4000 is up, line protocol is up										
	VRF : default IP Address : 10.255.12.1/29 Status : Up Hello Interval : 10 sec Transit Delay : 1 sec BFD : Disabled Cost Configured : NA State/Type : DR DR : 10.255.12.1 Link LSAs : 0 Authentication : No	Process Area Network Type Dead Interval Retransmit Interval Cost Calculated Router Priority BDR Checksum Sum Passive	: 1 9.0.0.0 : Broadcast : 5 sec : 5 sec : 1000 : 100 : 1 : 1 : 10.255.12.2 : 0 : No								

- show ip route all-vrfs
 - Verify that a default route is learned from the OSPF protocol and installed in the route table with the upstream firewall as the next hop.

DEVICE OUTPUT											
DEVICE	;≣ Output for the dev	ice: RSVDC-CORE1-1						Q		↓ :	3
⊘ RSVDC-CORE1-1									CLE	AR I	
RSVDC-CORE1-2	Output Time: 2024 Output Time: 2024 COMMAND show ip r Displaying ipv4 ro Origin Codes: C - R - Type Codes: E - E2 - VAF: default Prefix 0.0.0.0/00 10.0.0.1/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32 10.0.0.100/32	02-22 18:28:12 UTC oute all-wrfs utes selected for forwarding connected, S - static, L - local RTP, B - BCP, O - OSFP, D - OHCP External BGP, I - Internal BGP, V - VPN, OSFF external area, EI - OSPF external ' GSFF external type 2 Nexthop 10.255.12.3 10.2	EV - EVPN ype 1 Interface vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000	VRF (egress) - - - - - - - - - - - - - - - - - -	Origin/ Type 0/E2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Distance/ Metric 110/125 110/110 110/112 110/112 110/112 110/112 110/120 110/120	Age 00h:05m:27s 00h:05m:27s 00h:05m:23s 00h:05m:23s 00h:05m:27s 00h:05m:27s 00h:05m:27s 00h:05m:27s 00h:05m:27s 00h:05m:27s		CLE	<u>AR</u>	
	10.0.6.111/32 10.0.6.112/32 10.1.1.0/24 10.1.2.0/24 10.1.3.0/24 10.1.4.0/24	10,255,12,3 10,255,12,3 10,255,12,3 10,255,12,3 10,255,12,3 10,255,12,3	vlan4000 vlan4000 vlan4000 vlan4000 vlan4000 vlan4000		0 0 0 0 0	[110/116] [110/212] [110/212] [110/212] [110/212] [110/212]	00h:05m:27s 00h:05m:27s 00h:05m:27s 00h:05m:27s 00h:05m:27s 00h:05m:27s				

- Verify that valid campus routes are learned from the OSPF protocol.

- show spanning-tree mst detail
 - Verify that the Bridge Address and Root Address values are the same.
 - Verify that all LAG interfaces have a Role of "Designated" and State of "Forwarding".

DEVICE OUTPUT												
DEVICE	i≡ Output for th	e device: RSVDC-C	ORE1-1							۹	⊠ ±	0
⊘ RSVDC-CORE1-1	Output Time: 2	2024-02-22 18:28	====== :17 UTC								CLEAR	
Ø RSVDC-CORE1-2	COMMAND= show #### MST0 Vlans mapped: Bridge Root Regional Root Operational Configured Root Regional Root	<pre>show spanning-tree mst detail T0 apped: 1-4040 .02:00:00:00:00:00 Address:02:00:00:00:00:00 l Root Hello time(in seconds): 2 ed Hello time(in seconds): 2 Address:02:00:00:00:00:00:00 l Root Address:02:00:00:00:10:00 Internal cost:0</pre>			priority:0 Forward delay(in seconds):15 Max-age(in seconds):20 txHoldCount(in pps): 6 Forward delay(in seconds):15 Max-age(in seconds):20 Max-Hops:20 Priority:0 Priority:0 Rem Hops:20							-
	Port	Role	State	Cost	Priority	Туре	BPDU-Tx	BPDU-Rx	TCN-Tx	TCN-Rx		
	 1/1/5 1/1/6 1/1/6 1/1/8 1/1/10 1/1/10 1/1/10 1/1/11 1/1/12 1/1/12 1/1/15 1/1/15 1/1/15 1/1/15 1/1/15 1/1/15 1/1/16 1/1/17 1/1/22 1/1/22 1/1/22 1/1/22 1/1/26 1/26 1/1/26 1/1/26 1/1/26 1/1/26 1/1/26 1/1/26 1/1/26 1/1/26 1/1/26 1/27 1/	Disabled Dis	Down Down Down Down Down Down Down Down	20000 200000 20000 20000 20000 20000 200000 20000 20000 20000 20000 2000000	128 128 128 128 128 128 128 128 128 128	P2P P2P P2P P2P P2P P2P P2P P2P P2P P2P	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		

- show ip pim
 - Verify that **PIM Status** is "Enabled".

DEVICE OUTPUT		
DEVICE	E Output for the device: RSVDC-CORE1-1	Q 🗹 ± 🖸
Ø RSVDC-CORE1-1	 Output Time: 2024-02-22 18:28:22 UTC	CLEAR
⊘ RSVDC-CORE1-2	COMMAND= show ip pim	
	PIM Global Parameters	
	VRF : default PIM SStatus : Enabled PIM SSM Range ACL : Not Configured Join/Prune Interval (sec) : 60 SPT Threshold : Enabled State Refresh Interval (sec) : 60 State Refresh Interval (sec) : 60 State Refresh Status : Inactive PIM NSF Status : Inactive Shared Border Status : Disabled	

- show ip igmp
 - Verify that each host VLAN has an interface stanza with the **Querier IP** field populated with an IP address of one of the corresponding core switch VLAN SVIs.

DEVICE OUTPUT		
DEVICE	:≡ Output for the device: RSVDC-CORE1-1	Q 🖸 🕹
		CLEAR
Ø RSVDC-CORE1-2	Output Time: 2024-02-22 18:28:27 UTC	
	COMMAND= show ip igmp	
	VRF Name : default Interface : vlan101 IGMP Operating Version : 3 Querier State : Querier Querier IP [this switch] : 10.12.101.2 Querier IP [this switch] : 10.12.101.2 Querier Expiration Time : 10d 2h 15m Querier Expiration Time : 1m 30s IGMP Snoop Enabled on VLAN : False	
	Active Group Address Vers Mode Uptime Expires	
	239.1.1.1 3 EXC 5m 38s 3m 46s	
	VRF Name : default Interface : vlan102 IGMP Donraing Version : 3 Querier State : 0uerier Querier IP [this switch] : 10.12.102.2 Querier Uptime : 100 2h 15m Querier Expiration Time : 100 2h 15m Querier Expiration Time : 11m 30s IGMP Snoop Enabled on VLAN : False	

• show ntp status

⊥ C

- Verify that **NTP Server** is populated with a configured NTP server IP address.

DEVICE OUTPUT				
DEVICE	i Output for the device: RS	VDC-CORE1-1	Q	
			ļ	
Ø RSVDC-CORE1-2	======================================	======================================		
	COMMAND= show ntp status NTP Status Information			
	NTP NTP DHCP NTP Authentication NTP Server Connections	: Enabled : Enabled : Disabled : Using the mgmt VRF		
	System time NTP uptime	: Thu Feb 22 10:28:32 PST 2024 : 15 days, 20 hours, 1 minutes, 4 seconds		
	NTP Synchronization Info	rmation		
	NTP Server Poll interval Time accuracy Reference time	: 10.2.120.99 at stratum 4 : 1024 seconds : Within 0.000014 seconds : Thu Feb 22 2024 10:16:46.357 as per America/Los_Angeles		
	=== Troubleshooting sess	ion completed ===		

- Verify that the **Time Accuracy** field is populated.

Two-Tier Server Access

Configure Two-Tier access switches as VSX pairs for redundant multi-chassis link aggregation (MC-LAG) connections to the core and downstream data center hosts.

Configure Access VSX ISL Interface

To establish a VSX relationship between each pair of access switches, a link aggregation (LAG) interface must be created for assignment as the VSX data plane's inter-switch link (ISL). Standardizing the ToR model enables configuring the same ports on all access switches for the VSX ISL link at the UI group level.

Step 1 On the left navigation menu, click **DC-RSVCORE**, then click the data center access switch group name in the **Groups** column.

HPE GreenLake	
aruba Central	
Customer: Orange TME	
ධ DC-RSVCORE	
硷 Global	
(▼ dc-	
ជGroups	
DC-RSVACCESS	
DC-RSVACCESS	


Step 2 On the left navigation menu, click **Devices**.

Step 3 At the upper right of the Switches pane, click Config.

HPE GreenLake			00
Central	Q Search or ask Aruba	Q	¢ ⊘ Å
Customer: Orange TME	Switches	ll. Summary	List
법 DC-RSVACCESS 이	MultiEdit 🌒		
— Manage —	Access to AOS-CX search and custom configuration (editor & express configuration).	Confi	iguration Status

Step 4 In the Interfaces tile, click Ports & Link Aggregations

HPE GreenLake		
aruba Central		Q Search or ask Aruba
Customer: Orange TME		
다 DC-RSVACCESS 이 Manage	Switches MultiEdit Access to AOS-CX search and custo	n configuration (editor & express configuration).
品 Overview	System	Interfaces
Devices	Properties Contact, location, time zone and V	Ports & Link Aggregations Specific ports, LAGs and VLAN assignments

Step 5 Scroll to the right of the **Ports & Link Aggregations** table, and click the **+** (plus sign) in the upper right.

HPE GreenLake								88
Central		Q Se	arch or ask Aruba			Q	٩	⑦
Customer: Orange TME	=== Switchos					II. Summary	:= List	Config
ជ dc-rsvaccess 이	MultiEdit (_
— Manage ————	Access to AOS-C	ccess to AOS-CX search and custom configuration (editor & express configuration).					guratio	on Status
🗄 Overview							Q	+ 💮
Devices		Speed Duplex	IP Address	VLAN Mode	Native VLAN	Access VLAN		_

Step 6 On the Add LAG page, assign the following values:

- Name: lag256
- **Description:** *VSX_ISL_LAG*
- Port Members: 1/1/49, 1/1/50
- **Speed Duplex:** <*no value*> (default)
- VLAN Mode: trunk
- Native VLAN: 1 (default)
- Allowed VLANs: <no value> (default)
- Admin Up: checked
- Aggregation Mode: LACP Active

Name lag256	Routing	Admin Un
Description	VLAN Mode trunk V	
VSX_ISL_LAG	Native VLAN	Aggregation Mode LACP active
Port Members	1	
1/1/49, 1/1/50 🗸		
	Allowed VLANs	
Speed Duplex 💙		

Step 7 In the **Ports & Link Aggregations** table's title row, click ← (left arrow) to return to the main configuration page.

HPE GreenLake					
Orubo Central				Q Se	
Customer: Orange TME					
다 DC-RSVACCESS	Switches MultiEdit				
— Manage ————	Access to AOS-C	X search and	custom configurat	ion (editor	
🗄 Overview	← Port	s & Link A	ggregations	(56)	
Devices	Number		Description		
	lag256		VSX_ISL		
	OOBM				

Spanning Tree

MC-LAGs provide loop prevention in a Two-Tier architecture. Spanning-tree (STP) is configured as a backup loop prevention mechanism in case of host cabling errors to ToR switches.

Step 1 In the Bridging tile, click Loop Prevention.

HPE GreenLake			88
orubo Central	Q Sea	arch or ask Aruba	۹ 🧔 🤹
Customer: Orange TME			II. :⊒ 🔞 Summary List Config
ជ DC-RSVACCESS 이	MultiEdit		Configuration Status
— Manage ———	Access to AOS-CX search and custom configuration	(editor & express configuration).	Configuration status
🗄 Overview	System	Interfaces	Bridging
Devices	Properties Contact, location, time zone and VRF	Ports & Link Aggregations Specific ports, LAGs and VLAN assignments	VLANs Virtual subnet management
🗔 Clients	HTTP Proxy HTTP proxy server integration	Security	Loop Prevention Loop protection and spanning tree
🕰 Guests			

Step 2 In the **Loop Prevention** window, set the Spanning Tree **Region** to **RSVDC**, leave all other settings at their default, then click **SAVE**.

Mode MSTP	~	Priority 32 768 ✓	Region RSVDC			
Ports (55)						
Number		Description		LAG Members	Loop Protection	
lag256		VSX_ISL_LAG		1/1/49, 1/1/50	Disabled	
1/1/1					Disabled	
1./1./2					Dicabled	

Enter MultiEdit Configuration

Step 1 At the upper left of the Switches pane, click the MultiEdit enable slider.

HPE GreenLake		
Central		Search or ask Aruba
Customer: Orange TME	 Switches	
ជ DC-RSVACCESS 〇	MultiEdit	
— Manage ————	Access to AOS-C	X search and custom configuration (editor & express configuration).

Step 2 Select all access switches in the Devices lists, then click EDIT CONFIG.

HPE GreenLake								80
orubo Central		•	Q Search or ask Aruba				Q	🜻 🕐 🖁
Customer: Orange TME							II. Summary	∷≣ 👸 List Config
ជ dc-rsvaccess 이	MultiEdit							_
— Manage ————	Access to AOS-CX se	arch and custom config	uration (editor & express confi	guration).			Confi	guration Status
🗄 Overview	Device-Level	Configuration	or of the methods below to sh	ango configura	tion for the colocted	douicos		
Devices	Contextual Search Eng	gine	ler of the methods below to th	ange conngura	uon for the selected	devices.		
🗖 Clients	Enter Search Que	ery (e.g. nae-status:Cri	tical AND label:access)	SEARCH & F	Check	Search Documenta	ation	
🙁 Guests	Devices (4)							\odot
Applications	Name 🗍	Firmware Ve	Config Modifi	Status	Config St	NAE St	MAC Ad	IP Add
Socurity	RSVDC-ACCESS1-							172.16.104.24
V Security	RSVDC-ACCESS1-							172.16.104.25
— Analyze ———	RSVDC-ACCESS2-							172.16.104.26
Alerts & Events	RSVDC-ACCESS2-	2 10.10.1030	Feb 01, 2023, 01:05:	• Online	Sync	Normal 4 item	(s) selected C	lear
Audit Trail						VIEW COM	NFIG EDIT CONFIG	EXPRESS CONFIG
🖏 Tools							Edit Config	

Configure Access Switch VSX Pairs

The access switches are configured as VSX pairs to support Layer 2 multi-chassis link aggregation to the core layer and downstream data center hosts. A two-port link aggregation is configured and assigned as the VSX data path inter-switch link (ISL). The out-of-band *mgmt* interface is used for VSX keepalives to maximize the number of ports available for connecting access switches.

Step 1 Enter the initial VSX configuration.

```
vsx
system-mac 02:00:00:00:10:01
inter-switch-link lag 256
role primary
keepalive peer 172.16.104.25 source 172.16.104.24 vrf mgmt
```

Step 2 Mouse-over the field values in the table column headings below, right-click, and set the appropriate values for each switch.



Switch	system-mac	role	peer	source
RSVDC-ACCESS1-2	02:00:00:00:10:0 change]	secondary	172.16.104.103	172.16.104.104
RSVDC-ACCESS2-1	02:00:00:00:10:02	2primary[no- change]	172.16.104.106	172.16.104.105
RSVDC-ACCESS1-2	02:00:00:00:10:0	secondary	172.16.104.105	172.16.104.106

Step 3 Assign a description and maximum MTU value for the VSX ISL physical interfaces.

interface 1/1/49
 description VSX-ISL
 mtu 9198
interface 1/1/50
 description VSX-ISL
 mtu 9198

Configure Access to Core MC-LAGs

Step 1 Create the core-facing MC-LAG interface.

```
interface lag 255 multi-chassis
    no shutdown
    description DC-CORE
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
```

NOTE:

Tag all VLANs on all inter-switch MC-LAGs to support ubiquitous host mobility across all racks in the Two-Tier structure.

Step 2 Assign physical interfaces to the core MC-LAG interface.

```
interface 1/1/53
    no shutdown
    mtu 9198
    description RSVDC-CORE1-1
    lag 255
interface 1/1/54
    no shutdown
    mtu 9198
    description RSVDC-CORE1-2
    lag 255
```

NOTE:

The same physical interface on each access switch in the data center should connect to the same upstream core switch. For example, interface 1/1/53 on every ToR access switch can be configured to connect to the primary switch in the VSX core pair. This creates a consistent configuration that is easy to troubleshoot.

Step 3 Remove the following configuration line from interfaces 1/1/53 and 1/1/54: vlan access 1

Configure Access Switch to Host MC-LAGS

Step 1 Configure the host-facing MC-LAG interface.

interface lag 1 multi-chassis
 no shutdown
 description ESXi-01
 no routing
 vlan trunk native 1
 vlan trunk allowed 101-102
 lacp mode active
 spanning-tree root-guard

NOTE:

MC-LAG interfaces to downstream hosts should scope allowed VLANs only to those required for host.

Step 2 Mouse-over the description field, right-click, then modify values appropriately for each switch.

Switch	description
RSVDC-ACCESS1-2	ESXi-01[no-change]
RSVDC-ACCESS2-1	ESXi-02
RSVDC-ACCESS2-2	ESXi-02



NOTE:

Additional field configuration values, such as allowed VLANs on the trunk, also can be modified, when appropriate.

Step 3 Associate physical interfaces with the MC-LAG. The following configuration assigns an interface MTU and associates the interfaces with the previously created MC-LAG interface.

interface 1/1/1 no shutdown mtu 9198 lag 1

NOTE:

Standardize the association of LAG index values to physical interfaces across all access switches for efficient configuration of switch interfaces. The example above assigns LAG index 1 to interface 1/1/1 on all selected switches in MultiEdit.

Step 4 Remove the following configuration line from interfaces 1/1/1: vlan access 1

Step 5 Repeat this process for each host facing MC-LAG.

Configure Multicast

Server Access switches do not perform multicast routing or client services, but IGMP snooping observes IGMP requests from hosts to optimize multicast forwarding at Layer 2. IGMP populates Multicast MAC addresses corresponding to IP multicast groups in the MAC table. This conserves bandwidth by ensuring that multicast traffic is forwarded only to interested receivers.

Step 1 Enable IGMP snooping on all VLAN interfaces.

```
vlan 101
ip igmp snooping enable
vlan 102
ip igmp snooping enable
```

Step 2 At the bottom right of the MultiEdit Configuration window, click SAVE.



Configure Physical Port Speeds

The default port speed on a switch may be different than the supported speed of a connected device. When attached host speeds are not common across racks, MultiEdit can be used to select only the ToR VSX pair of switches to be modified.

Aruba CX 8325 and CX 10000 switches set physical interface speeds in groups. Every non-uplink interface is associated with an interface group. All members of an interface group use the same operational speed. The size of the group depends on the switch model. This sample topology uses a CX 8325, which groups sets of 12 non-uplink physical interfaces to four distinct interface groups.

Step	1 Select switches that	t require interface	group speed setting	zs, then click EDIT CON	FIG.
	I October Stritteries that	eregane miceriace	Si oup opeeu oetting		

ter Search Query (e	e.g. nae-status:Critical AND	label:access)	SEARCH & FILT	TER Check Search	Documentation		
Devices (4)							
ame 🚛	Firmware Version	Config Modified	Status	Config Status	NAE Status	MAC Address	IP Addr
VDC-ACCESS1-1	10.13.1000	Feb 12, 2024, 22:54:58	• Online	Sync	Normal	a0a001-923780	172.16.117.1
VDC-ACCESS1-2 VDC-ACCESS2-1 VDC-ACCESS2-2	10.13.1000 10.13.1000 10.13.1000	Feb 12, 2024, 22:54:58 Feb 12, 2024, 22:54:58 Feb 12, 2024, 22:54:58	OnlineOnlineOnline	Sync Sync Sync	Normal Normal Normal	a0a001-923600 a0a001-92c680 a0a001-929780	172.1 172.1 172.1

Step 2 Set the interface group port speed to 10Gbps.

system interface-group 1 speed 10g

NOTE:

The command above sets physical ports 1/1/1–1/1/4 on an 8360 and ports 1/1/1–1/1/12 on an 8325 to operate at 10 Gbps.

	Devices	<	Configuration
	Selected 2/2		ssh server vrf mgm vlan 1
	RSVDC-ACCESS1-1	\$	vlan 101 name PROD-WEB
	KSVDC-ACCESS1-2	~	vlan 102 name PROD-DB
			spanning-tree conf
			no shutdown ip dhcp
			system interface-g
			interface lag 1 mu
Step 3 At the lower right of the MultiEdit Configuration window, click SAVE.			

Verify Configuration



	HPE GreenLake	
	Central	
	Customer: Orange TME	
Step 2 On the Tools menu at the top, click the Commands tab.	ස් DC-RSVACCESS ා	Network Check

Step 3 Click the **Available Devices** dropdown, select all access switches, then click elsewhere on the page.

HPE GreenLake				
Central			Q Search or as	sk Aruba
Customer: Orange TME	8		(
법 DC-RSVACCESS 이	Network Check	Device Check	Commands	Console
— Manage — .	Select a Device Typ Device Type Switch	e, Select Devices Ado SE	d the Commands an ARCH	d Run them
Devices	Select commands f	rom one or mor	RSVDC-ACCESS1-1 RSVDC-ACCESS1-2	
🗖 Clients	All Category		RSVDC-ACCESS2-1	
😩 Guests				No data to display
Applications				

Step 4 In the **Categories** list, click **All Category**. Enter *vsx* in the commands list filter, click **show vsx status**, then click **Add** >.

HPE GreenLake				
aruba Central		Q Search or ask Aruba		Q
Customer: Orange TME				
ជ DC-RSVACCESS 이	Network Check Device Check	commands Console		
— Manage ———	Select a Device Type, Select Devices, Device Type	Add the Commands and Run them Available Devices		
E Overview	Select commands from one or more	categories		
Devices	Categories	♀ Commands		Selected Commands
🗔 Clients	All Category		Add >	
🙁 Guests		TP	< Remove	1 PP
Applications		No data to display	< Remove All	No data to display
Security				
- Analyze	<u> </u>	 * - Supports additional mandatory filters + - Supports additional optional filters 		This list of commands will run in the order of its sequence (Maximum is 20)

Step 5 Add the following additional commands to the Selected Commands list.

• show lacp interfaces

- show spanning-tree mst detail
- show ntp status

Step 6 At the lower left of the Commands pane, click RUN.

Select a Device Type, Select Device	es, Add the Commands and Run them		
Device Type	Available Devices		
Switch	4 Switches 🗸		
Select commands from one or mor	re categories		
Categories	Commands V ntp	Selected Commands	
All Category	show ntp associations	show vsx status	
	show ntp servers	Add > show lacp interfaces	
		< Remove show spanning-tree mst detail	
		show ntp status	
	144 Commands		
	* - Supports additional mandatory filters	4 Commands This list of commands will run in the order of its sequence (Maximum is 20)	
	 - Supports additional optional inters - Cannot run with other commands 	sequence (manification as)	
Repeat			
Devices which are already runnin	or commands shall not execute newly added commands		
Output history of device with huf	for space issues shall be automatically cleared		
Output history of device with but	Ther space issues shall be automatically cleared		
Few commands require the log le	evel to be set as debug to see the output		
-			
RUN RESE	T		

Step 7 Scroll down to review the CLI command output for each switch. Verify key result data for each command.

- show vsx status
 - ISL channel: In-Sync
 - ISL mgmt channel: operational
 - Config Sync Status: In-Sync
 - Device Role: set to primary and secondary on corresponding switches
 - Other VSX attributes display equal values for both VSX members

DEVICE OUTPUT										
DEVICE	⋮ Output for the device: RSVDC-ACCESS1-1								₹	::
⊘ RSVDC-ACCESS2-1	=== Troubleshooting session started ===							CLE	AR	
⊘ RSVDC-ACCESS1-1										
	Output Time: 2024-	02-23 16:22:08 UTC								
⊘ RSVDC-ACCESS2-2	UMMANU= snow VSX Status VSX Operational State ISL channel : In-Sync ISL mgmt channel : operational Config Sync Status : In-Sync NAE : peer_reachable HTTPS Server : peer_reachable									
	Attribute	Local	Peer 							
	ISL link ISL version System MAC Platform Software Version Device Role	lag256 2 02:00:00:00:10:01 8360 LL.10.13.1000 primary	lag256 22 02:00:00:00:10:01 8360 LL.10.13.1000 secondary							

- show lacp interfaces
 - Both Actor and Partner have a corresponding interface for each MC-LAG.
 - All Actor interfaces have a State of "ALFNCD".
 - All Actor interfaces have a **Forwarding State** of "up" for all host facing MC-LAGs and the upstream core switch facing MC-LAGs.
 - All Partner interfaces have a state of "PLFNCD" or "ALFNCD".



NOTE:

"(mc)" in the **Aggr Name** column indicates an MC-LAG. The switch on which the *show lacp interfaces* command is run is considered the Actor. The other VSX member switch is considered the Partner.

- show spanning-tree mst detail
 - Verify that the **Root Address** value is the virtual VSX MAC address on the core switches.
 - Verify that the Role for LAG 255 connected to the core switches is "Root" with a State of "Forwarding".
 - Verify that the Role for all other LAGs and ports with connections is "Designated" with a State of "Forwarding".

EVICE := Output fo	r the device: RSVDC	-ACCESS1-1							Q		⊥
RSVDC-ACCESS2-1										CLE	AR
RSVDC-ACCESS1-1 Output Time	2024-02-23 16:2	22:18 UTC									
COMMAND= s RSVDC-ACCESS1-2 #### MST0 Vlans mapp RSVDC-ACCESS2-2 0perationa	now spanning-tree ed: 1–4094 Address:02:00 L Hello time(in	mst detail 0:00:00:10:01 n seconds): 2	prior: Forward	ity:32768 delay(in se	conds):15 Ma	x-age(in second	ls):20 txHc	oldCount(in p	ps):		
6 Configured Root Regional R	Hello time(in Address:02:00 Port:lag255 Dot Address:02:00 Internal cost	n seconds): 2 0:00:00:10:00 0:00:00:10:00 t:200	Forward Priority Path cos Priority Rem Hops	delay(in se y:0 st:0 y:0 s:19	conds):15 Ma	x-age(in second	ls):20 Max-	-Hops:20			
Port TCN-Rx	Role	State	Cost	Priority	Туре	BPDU-Tx	BPDU-Rx	TCN-Tx			
	Designated Dissbled	Forwarding Down Down Down Down Down Down Down Down	20000 20000	128 128 128 128 128 128 128 128 128 128		675976 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0				

- show ntp status
 - Verify that **NTP Server** is populated with a configured NTP server IP address
 - Verify that the **Time Accuracy** field is populated.

DEVICE OUTPUT		
DEVICE	⋮ Output for the device: RSVDC-ACCESS1-1	< 🖂 🕂 🔅
⊘ RSVDC-ACCESS2-1		CLEAR
⊘ RSVDC-ACCESS1-1	Output Time: 2024-02-23 16:22:22 UTC	
⊘ RSVDC-ACCESS1-2	COMMAND= show ntp status NTP Status Information	
Ø RSVDC-ACCESS2-2	NTP : Enabled NTP DHCP : Enabled NTP Authentication : Disabled NTP Server Connections : Using the mgmt VRF	
	System time : Fri Feb 23 08:22:22 PST 2024 NTP uptime : 15 days, 15 hours, 32 minutes, 21 seconds	
	NTP Synchronization Information	
	NTP Server: 10.2.120.98 at stratum 3Poll interval: 1024 secondsTime accuracy: Within -0.000825 secondsReference time: Fri, Feb 23 2024 8:03:13.545 as per America/Los_Angeles	
	=== Troubleshooting session completed ===	

Ansible Two-Tier Data Center

HPE Aruba is committed to providing effective, flexible network automation strategies tailored to customer needs. In addition to workflow-based automations provided by Aruba Central and Aruba Fabric Composer, the HPE Aruba Networking Developer Hub provides comprehensive tooling to support CX switch configuration using Ansible.

Overview

Ansible is an open-source orchestration framework maintained by Red Hat. It automates provisioning, configuration management, and application deployment.

An Ansible playbook automates CX switches using the AOS-CX Ansible Collection that configures switches using multiple REST API calls and CLI commands via SSH.

The Ansible workflow in this guide provides turnkey automation of an AOS-CX Two-Tier Data Center. The zipped version of the project can be downloaded from the Github repository into your Ansible control machine using the following **git clone** command:

\$ git clone https://github.com/aruba/aoscx-ansible-dcn-workflows.git

NOTE:

HPE Aruba's Getting Started with Ansible and AOS-CX guide provides additional information on how to use the AOS-CX Ansible Collection.

Ansible Project Prerequisites

This project assumes a working knowledge of Ansible. If you are new to Ansible automation, please review HPE Aruba's Getting Started with Ansible and AOS-CX guide on the Developer Hub.

An automation server or VM in the networking environment with SSH reachability to the IP addresses assigned to the Aruba CX out-of-band management interfaces is required.

The Ansible control machine requires **Python3.5+** and **Ansible 2.13.1+**, which can be installed using Ansible's Installing Ansible guide.

This project requires HPE Aruba's AOS-CX Ansible Collection, which can be installed by executing the **ansible-galaxy** command using the requirements.yml file in the HPE Ansible data center repository.

```
$ cd aoscx-ansible-dcn-workflows
$ ansible-galaxy install -r requirements.yml
```

The following Python libraries are required for this project.

• Jinja2 2.10+

- paramiko 2.1.1+
- pip 6.0+
- requests 2.2.0+
- netaddr 0.7.5+
- pyaoscx 2.5.1+
- openpyxl

The Python libraries can be installed by running **pip** with the requirements.txt file in the HPE Ansible data center repository.

```
$ cd aoscx-ansible-dcn-workflows
$ pip install -r requirements.txt
```

Ansible Project Structure

The Ansible files for the Two-Tier Data Center project are maintained in a general data center workflow repository on Github. The repository also contains files for additional projects. Visit the AOS-CX Data Center Automation with Ansible Developer Hub for details on the other workflows hosted within the data center repository.

The files necessary for the Two-Tier Data Center workflow are listed in the repository structure below.

```
configs
                                        # Directory for generated configurations
|- sample_configs
                                        # Sample Final Configurations for all
   workflows
templates
                                        # Place to hold Jinja templates for config
   generation
                                        # Jinja2 configuration Templates for Two-
|- 2TierV2
   Tier DCN V2
                                        # Access switch Jinja2 template for
  - access.j2
   Architecture II version 2
                                        # Core switch Jinja2 template for
  |- core.j2
   Architecture II version 2
deploy_2tierv2_dcn.yml
                                        # Playbook for Architecture II version 2
inventory_2tierv2_dcn.yml
                                        # Inventory for Architecture II version 2
                                        # Python library requirements for project
requirements.txt
requirements.yml
                                        # Galaxy collection requirements for
   project
```

The inventory and template files are critical for running the Two-Tier Data Center playbook, as described in separate chapters in this guide.

Two-Tier Data Center Topology

The Ansible workflow deploys the same sample topology used in the Aruba Central Two-Tier Data Center guide. Some information from the Aruba Central guide is repeated here for reference and readability.

HPE Aruba Two-Tier data centers meet the requirements of small- and medium-size data centers. For network resiliency, multi-chassis link aggregations (MC-LAGs) are used at both switch tiers. The diagram below summarizes the physical topology configured in this deployment guide and the relationship between components.



Two-Tier Core Layer

The core layer provides redundant Layer 2 connectivity to downstream access switches. A VSX pair of core switches is configured with an MC-LAG to each downstream rack. All links from the core layer to the access layer for a single rack are members of the same MC-LAG, whether the rack is populated with a single switch or with a VSX-pair of access switches. MC-LAG provides network resiliency and load-balancing. It also mitigates the need for loop avoidance mechanisms between the core and access layer switches.

Layer 3 services for the data center are provided by the core layer. VLAN switched virtual interfaces (SVIs) define data center subnets, and Aruba Active Gateway provides redundant IP gateways to data center hosts. The core layer also provides redundant IP connectivity to upstream external networks. Typically, firewalls are placed between a data center and external networks for policy enforcement. The redundancy strategies between the data center core and external networks can vary, depending on device features and organizational requirements. In this guide, a traditional active/passive redundant pair of firewalls is connected to the core switch pair using MC-LAGs.

Two-Tier Access Layer

The access layer provides Layer 2 connectivity to downstream data center hosts.

When a single access switch is at the top-of-rack (ToR) position, the access layer connects to the core layer using a standard LAG. A single ToR switch can provide physical link redundancy using a standard LAG, but host connectivity is lost when performing firmware upgrades or when the ToR switch fails.

This example deployment uses a VSX pair of ToR switches at the access layer, which provides physical switch redundancy to directly attached hosts. This model supports uninterrupted host connectivity, even when one of the ToR switches fails or a firmware upgrade is performed. Each access layer switch also is connected to each core switch using an MC-LAG for redundancy, load balancing, and loop avoidance.

Ansible Two-Tier Inventory

An Ansible inventory file serves two primary functions for AOS-CX automation: it defines the set of switches to apply automated configuration, and it defines a set of variables that provide configuration values for those switches.

YAML Inventory File

Ansible inventory files are formatted using YAML data structures. The Two-Tier data center inventory file provides a reference for formatting host, group, and variable data in an Ansible automation.

Red Hat's How to build your inventory guide provides a general reference on creating inventory files.

The example inventory variable values must be modified to align with the organization's environment. This includes customizing the host IP addresses, DNS servers, port assignments, etc. This chapter provides background information and the variable names needed to modify the example inventory file successfully for individual needs.

Inventory Hosts

Hosts are the targets for an Ansible playbook automation. They are defined in one or more **hosts** sections in the inventory file.

An **ansible_host** variable is assigned to each switch with a fully-qualified DNS name (FQDN), IPv4 address, or IPv6 address value. The playbook uses this value for SSH and API communication with switch management interfaces.

Additional variables are associated with each host that represent the desired configuration state of the target switch. Variable values can be assigned directly to an individual host or inherited through the group structure described in this chapter.

Inventory Variables

Variables defined in the Ansible inventory file serve two general purposes: they specify switch configuration and Ansible playbook behavior. Most variables in the Ansible inventory file represent values assigned to switch configuration statements when the playbook builds a switch configuration file.

All the variables in the example inventory file are necessary for the Two-Tier data center playbook to run properly.

Single Value Assignments

Simple variables assign a single value to the right of the variable name with a colon separator.

```
mtu: 9198
vsx_role: primary
vsx_system_mac: 02:00:00:00:10:01
```

List and Dictionary Assignments

It can be advantageous to assign multiple values to a single variable for automating switch configuration.

Lists can be defined using two methods in the inventory file. The first method assigns a set of comma delimited values in square brackets to a variable name. The second method assigns each list member on a new line preceded by a dash.

The second method provides an easily understandable visual structure for creating dictionaries (multidimensional arrays), where each dictionary member contains its own set of nested variables. A dictionary is analogous to an employee record, where each employee is assigned a set of values such as name, address, and phone number.

Array Definition Method	Array Syntax
Method 1: comma delimited simple list in square brackets	variable_name: [value1, value2, value3]
Method 2: simple list with dash-delimited lines	variable_name: - value1 - value2 - value3
Method 2: dictionary entries containinga subset list of variable assignments	<pre>dictionary_variable_name: - dict1_var1: dict1_var1_value dict1_var2: dict1_var2_value dict1_var3: dict1_var3_value - dict2_var1: dict2_var1_value dict2_var2: dict2_var3_value - dict3_var3: dict3_var1_value dict3_var3: dict3_var3_value</pre>

Example lists from the inventory file are shown below:

ntp_servers: [10.2.120.98, 10.2.120.99]
dns_servers: [10.2.120.98, 10.2.120.99]
vsx_isl_ports: ['1/1/49', '1/1/50']

The following example illustrates how to assign sets of variables in dictionary form to the **host_vlans** variable. Grouping sets of values in this manner facilitates AOS-CX config automation in the template file.

```
host_vlans:
- id: 101
name: PROD-WEB
ip_address: 10.12.101.2
active_gateway_mac: 02:00:0a:01:65:01
active_gateway_ip: 10.12.101.1
- id: 102
name: PROD-DB
ip_address: 10.12.102.2
active_gateway_mac: 02:00:0a:01:65:01
active_gateway_ip: 10.12.102.1
```

AOS-CX Ansible Collection Variables

AOS-CX Ansible Collection variables are reserved names that modify playbook behavior and connectivity to automated hosts.

Some AOS-CX Ansible Collection variables require a specific value, such as the following connection variables.

```
ansible_connection: arubanetworks.aoscx.aoscx  # D0 NOT CHANGE
ansible_network_os: arubanetworks.aoscx.aoscx  # D0 NOT CHANGE
ansible_httpapi_use_ssl: True  # D0 NOT CHANGE
```

Inventory Groups

Groups provide a hierarchical structure for the inventory file. Ansible hosts and variables can be defined at any group level in the hierarchy.

In the example deployment, six groups are defined to organize the inventory file into a four-level hierarchy.



Groups enable efficient organization of common configuration elements, similar to Aruba Central. Each host inherits the variables assigned to groups in its path hierarchy. This enables assigning common configuration elements on multiple affinities, such as data center location, functional role, or rack.

Core switch hosts are defined in the **core** group. Server access switches are defined in their respective rack group to accommodate configuration common to each VSX pair. For example, server access switches in rack 1 are defined in the **rack1** group.

AOS-CX Ansible Collection variables that apply to all switches are defined once in the **aoscx_switches** group. Configuration values common to all data center switches are defined once in the **DC-RSV** group. The **core** and **access** groups assign configuration common to switches in those respective roles. Configuration values common to access switches in the same rack are defined at the rack level. The rack groups are defined primarily to apply VSX and MC-LAG configuration to redundant top-of-rack switches. Variables that have unique values at each host are defined at the host level for both core and access switches.

The following diagram illustrates a sample variable at each group level inherited by a host and a unique host variable assignment:



When the same variable exists in multiple contexts, the assignment nearest the host in the hierarchy is used by the Ansible playbook. A host variable assignment takes precedence over all group assignments.

The example Ansible group organization is just one approach for categorizing switches with common configuration elements. Organizations should use a grouping methodology that best meets their needs.

Specify a Template File

The playbook uses inventory variables in conjunction with a configuration template to build AOS-CX configuration statements.

When automating more than one switch model or role, some configuration elements may be unique to the model or role. Two examples include: - Assigning switch profiles to optimize hardware resources with a switch's network functions. Switch profile names are not consistent across all switch models. - In the Two-Tier data center, OSPF routing is configured on core switches, but not on server access switches.

A separate template file for core and access switches is used in our example deployment. Standardizing a consistent switch platform for each role can simplify template creation, although additional scripting logic can be applied in a template file to accommodate model differences.

It is best practice to use different configuration templates for each switch role for efficient template file administration.

The configuration templates are assigned to a host with the **config_template** inventory variable. In this project, the **config_template** variable is assigned in the **core** and **access** group contexts.

config_template: templates/2TierV2/access.j2

Configuration templates are described further in the Ansible Template chapter.

Planning Inventory File Values

This section provides sample values and rationale for naming and numbering schemes. Adjust values and formats as needed to accommodate specific requirements. Use a consistent approach in the physical and logical configurations to improve network management and troubleshooting.

Naming Conventions

Establish a switch naming convention that indicates the switch type, role, and location to simplify identification and increase operating efficiency.

Example values used in this guide:

Switch Name	Role	Description
RSVDC-CORE1-1	Core	Roseville Data Center Core Switch, VSX Pair Member 1 (primary)
RSVDC-CORE1-2	Core	Roseville Data Center Core Switch, VSX Pair Member 2 (secondary)
RSVDC-ACCESS1-1	Acces	Top-of-Rack Access Switch in Rack 1, VSX Pair Member #1 (primary)
RSVDC-ACCESS1-2	Access	sTop-of-Rack Access Switch in Rack #1, VSX Pair Member 2 (secondary)

In the Ansible inventory file, the switch name is defined as an Ansible inventory name in the **hosts** stanza. For example, the inventory name **RSVDC-ACCESS-1-1** is created in the hosts stanza in the **DC-RSV > access > rack1** group context. Each link in the table above references the location in the inventory file for a specific switch's inventory name.

When executing the playbook, the hostname in the configuration file is set based on the current iterated switch inventory name.

IP Address Planning

Plan a consistent IP numbering scheme with values that can accommodate the current deployment size and leave room for growth. Define a range that can represent loopback addresses, IP addresses used in supporting protocols, and a range for data center hosts. It is beneficial to assign data center host subnets from a larger range of maskable IP addresses that summarizes all host subnets in the data center.

Example IP address ranges used in this guide:

Subnet	Functional Description
10.255.12.0/24	Routed interface IP addresses
10.250.12.0/24	Loopback IP addresses
10.12.0.0/16	Summary range of all data center host subnets
10.12.101.0/24	Example of a specific data center host subnet

The Ansible inventory statically defines all the IP addresses needed, including loopback addresses and routed interfaces. Each link in the table above references the location in the inventory file of an example IP address assigned from the pool. Some values and variables are repeated for devices. Be sure to review all entries in the inventory file before execution.

MAC Address Planning

A Locally Administered Address (LAA) should be used when defining virtual MAC addresses for VSX and active gateway functions. This is required when configuring an Active Gateway for an SVI on a VSX pair and when configuring the system MAC address of VSX. An LAA is a MAC in one of the four formats shown below:

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

The *x* positions can contain any valid hex value. It is helpful to create a hexadecimal representation of the associated IP address or VLAN ID using the hex positions. For more details on the LAA format, see the IEEE tutorial guide.

In this guide, VSX system MAC addresses are set to 02:00:00:10:xx, where xx is replaced with the rack number of the VSX pair and the core switches use a value of 00.

Active Gateway MAC addresses are set in the format 02:00:0a:xx:xx:xx.

The **host_vlans** variable defined in the **RSV-DC** group is redefined for each core switch at the host level. Be mindful to use consistent **vlan_id** and **name** values in the inventory file at both levels.

NOTE:

A variable's value may be reassigned at a different level in the inventory file's hierarchy for several reasons. In our example, the dictionary values assigned to the **host_vlans** variable in the **DC-RSV** group are inherited by all access switches. The core switches require additional variables in the dictionary for their roles in the network, where some values are unique to the host. Redefining the **host_vlans** variable at each core switch's host level overwrites the dictionary values defined in the higher group, so it is necessary to include the previously defined **vlan_id** and **name** variables in the new dictionary list assignment at the host level.

Inventory Variable Reference

This section describes inventory variables included in this example Ansible AOS-CX playbook automation. The example inventory file provides a complete reference for the Two-Tier data center automation.

The top level **aoscx_switches** group assigns variables associated to all switch hosts focused on script execution.

Variable Name	Value	Notes
ansible_user	[switch username]	Login user for switch. This value can be changed. It is best practice to define an automation user account.
ansible_password	[switch password]	Password for the ansible_user account on the switch.
ansible_connection	arubanetworks.ac	This value is used by the AOS-CX Ansible Collection and must not be changed.
ansible_network_os	arubanetworks.ac	งร ัโห่เลงระไม ่e is used by the AOS-CX Ansible Collection and must not be changed.

Variable Name	Value	Notes
ansible_httpapi_use_ssl	True	This value enables HTTPS communication and should not be changed.
ansible_httpapi_validate_certs	False	Change this value to True to perform certificate validation using the host's certificate store.
ansible_acx_no_proxy	True	
ansible_aoscx_validate_certs	False	
ansible_aoscx_use_proxy	False	

The **DC-RSV** group assigns AOS-CX configuration variables common to all data center switches.

Variable Name	Sample Value	Notes
hostname	"{{inventory_name}}"	The playbook iterates over each host entry in the inventory file, and the <i>inventory name</i> is the name of the host entry currently being iterated.
group	RSVDC	This value is referenced by another variable to assign the MST instance name.
config_path	"configs/"	The directory that playbook generated configurations will be stored.
timezone	"america/los_angeles"	Value used to assign the time zone for all switches at this data center location.
mtu	9198	Value used to assign the Layer 2 interface MTU. AOS-CX defines the Layer 2 MTU value as the acceptable Layer 3 payload size, not the Ethernet frame size directly.
stp_config_name	"{{group}}"	Value used to assign the MST instance name to the value of the group variable.

Variable Name	Sample Value	Notes
ntp_servers	[10.2.120.98, 10.2.120.99]	List of NTP servers used to assign multiple NTP servers.
ntp_vrf	mgmt	Value used to assign source VRF for NTP queries.
dns_servers	[10.2.120.98, 10.2.120.99]	List of DNS servers used to assign multiple DNS servers.
dns_domain	example.local	Value used to assign DNS domain.
system_location	DC01, Roseville, CA	Value used to assign SNMP server system location
system_contact	netadmin@orangetme.lo	oc øå lue used to assign SNMP server system contact
opsf_area	0.0.0.0	Value used to assign the OSPF area on core switches. The server access switches do not participate in OSPF. Although the ospf_area inventory variable is associated with access switches by its inclusion in the DC-RSV group, it is not applied to server access switch configurations, because it is not referenced by the access switch configuration template when building configuration files.
tacacs_servers		This defines the start of a dictionary containing multiple variables for each TACACS server entry.
tacacs_servers.host	10.2.120.94	Value used to assign the IP address of an individual TACACS server. Each tacacs_server dictionary entry has its own unique IP assignment.
tacacs_server.ciphertext	[shared secret]	Value used to assign the encrypted shared key for an individual TACACs server.

Variable Name	Sample Value	Notes
host_vlans		This defines the start of a dictionary containing multiple variables for each server VLAN. The host_vlans dictionary defined at the DC-RSV level is inherited by server access switches, but it is overwritten by host-level variables for each core switch.
host_vlans.id	101	Value used to assign VLAN ID for each VLAN in the data center. A unique value is assigned to each dictionary entry.
host_vlans.name	PROD-WEB	Value used to assign VLAN name. A unique value is assigned to each dictionary entry.
vsx_isl_lagid	256	Value used to assign the LAG ID used as the ISL in a VSX pair.
vsx_keepalive_vrf	mgmt	Value used to assign the VRF used for VSX keepalive messages.

The **core** group assigns AOS-CX configuration variables common to data center core switches.

Variable Name	Sample Value	Notes
config_template	templates/2TierV2	Assigns the core switch configuration template to both core switches. The playbook uses the configuration template and inventory variables in combination to generate switch configuration files.
vsx_system_mac	02:00:00:00:10:00	Value used to assign VSX system MAC address to both VSX core switches.

Variable Name	Sample Value	Notes
vsx_keepalive_ip_primary	172.16.117.101	Value used to identify the VSX primary switch IP address for VSX keepalive configuration, but not assignment to an interface. The switches used in this deployment example use DHCP to obtain a mgmt interface IP assignment. The IP address assignments for the VSX primary and secondary switches are identified through the use of DHCP reservations.
vsx_keepalive_ip_secondary	172.16.117.102	Value used to identify the VSX secondary switch IP address for VSX keepalive configuration.
vsx_isl_ports	[1/1/31, "1/1/32"]	Value used to identify the physical interfaces assigned to the VSX ISL. The same interfaces are used on both switches.
mclags		This defines the start of a dictionary containing multiple variables for each switch VSX/MC-LAG.
mclags.id	1	Value used to assign MC-LAG interface IDs. A unique value is assigned to each dictionary entry.
mclags.interfaces	["1/1/1", "1/1/2"]	Value used to assign physical interfaces for a specific MC-LAG ID. Unique values are assigned to each dictionary entry.
mclags.allowed_vlans	["all"]	Value used to assign VLAN IDs for a specific MC-LAG ID. This example is a simple list containing only one element. The all keyword allows all VLANs between core and access switches.
mclags.mtu	9198	Value used to assign the Layer 2 MTU for MC-LAG member interfaces. It is best practice to set the Layer 2 MTU to its highest value.

Variable Name	Sample Value	Notes
mclags.description	RACK-1	Value used to assign the description for a specific MC-LAG ID. Unique values are assigned to each dictionary entry.

Each core switch is assigned a set of variables at the host level. The variables and lists assigned at the host level contain unique values not shared by other switches. The following table shows sample values for the RSVDC-CORE1-1 switch.

	Sample	
Variable Name	Values	Notes
ansible_host	172.16.117.101	Value used by the AOS-CX Ansible playbook to connect to this specific switch host.
vsx_role	primary	Value used to assign the VSX role. The template file uses this variable in a conditional statement to generate proper VSX keepalive IP configuration.
loopback0_ip	10.250.12.1	Value used to assign an IP address to the loopback0 interface.
routing_vlans		This defines the start of a dictionary for VLANs used to route to external networks. In this example deployment, only a single external routing VLAN is defined with a single dictionary entry. This dictionary is assigned at the host level for each core switch, because unique IP address assignments exist per host that cannot be inherited from a higher level group.
routing_vlans.id	4000	Value used to assign VLAN ID for the VLAN used to connect to external networks.
routing_vlans.name	CORE- ROUTING- SVI	Value used to assign VLAN name.
routing_vlans.ip_address	10.255.12.1	Value used to assign a unique VLAN SVI for this specific switch.

	Sample	
Variable Name	Values	Notes
host_vlans		This defines the start of a dictionary containing multiple variables for each server VLAN. This dictionary is assigned at the host level for each core switch, because unique IP address assignments exist per host that cannot be inherited from a higher level group.
host_vlans.id	101	Value used to assign VLAN ID for each VLAN in the data center. A unique value is assigned to each dictionary entry.
host_vlans.name	PROD- WEB	Value used to assign VLAN name. A unique value is assigned to each dictionary entry.
host_vlans.ip_address	10.12.101.2	Value used to assign unique VLAN SVI for this specific switch.
host_vlans.active_gateway_mac	02:00:0a:01:6	5 5/0l ue used to assign the Active Gateway MAC address shared by the VLAN on both VSX members.
host_vlans.active_gateway_ip	10.12.101.1	Value used to assign the Active Gateway IP address shared by the VLAN on both VSX members.

The **access** group assigns AOS-CX configuration variables common to data center access switches.

Variable Name	Sample Values	Notes
config_template	templates/2TierV2,	Assigns the access switch configuration template to all server access switches. The playbook uses the configuration template and inventory variables in combination to generate switch configuration files. It may be necessary to assign the config_template variable at the host level, when differences between hardware models do not support the same features.

Variable Name	Sample Values	Notes
speed_interface_group_10g	[1]	A list of switch interface groups to set to 10 Gbps operation. The example list contains only a single element.
vsx_isl_ports	["1/1/49", "1/1/50"]	Value used to identify the physical interfaces assigned to the VSX ISL. The same interfaces are used on both switches. The same VSX interfaces can be assigned to all server access switches, because the same switch model and port layout are used for all access switches.

A rack group assigns AOS-CX configuration variables common to a VSX redundant pair of rack switches. In this example deployment, MC-LAGS are defined at the rack level to accommodate unique description and VLAN assignments per LAG. It is possible to define MC-LAGs for all host-facing ports just once in the **access** group, when assigning all VLANs to the MC-LAGs without unique descriptions.

Variable Name	Sample Values	Notes
vsx_system_mac	02:00:00:00:	Value used to assign VSX system MAC address to both VSX core switches.
vsx_keepalive_ip_primary	172.16.117.103	Value used to identify the VSX primary switch IP address for VSX keepalive configuration, but not assignment to an interface. The switches used in this deployment example use DHCP to obtain a mgmt interface IP assignment. The IP address assignments for the VSX primary and secondary switches in all redundant top-of-rack server access pairs are identified through the use of DHCP reservations.
vsx_keepalive_ip_secondary	172.16.117.104	Value used to identify the VSX secondary switch IP address for VSX keepalive configuration.
mclags		This defines the start of a dictionary containing multiple variables for each server access switch VSX/MC-LAG to physical servers.

Variable Name	Sample Values	Notes
mclags.id	1	Value used to assign MC-LAG interface IDs. A unique value is assigned to each dictionary entry.
mclags.interfaces	[1/1/1]	Value used to assign physical interfaces for a specific MC-LAG ID. Unique values are assigned to each dictionary entry.
mclags.allowed_vlans	[101, 102]	Value used to assign VLAN IDs for a specific MC-LAG ID. This example is a simple list containing two allowed VLANs.
mclags.mtu	9198	Value used to assign the Layer 2 MTU for MC-LAG member interfaces. It is best practice to set the Layer 2 MTU to its highest value.
mclags.description	ESXi-01	Value used to assign the description for a specific MC-LAG ID. Unique values are assigned to each dictionary entry.

Each access switch is assigned a set of variables at the host level. The variables and lists assigned at the host level contain unique values that are not shared by other switches. The following table shows sample values for the RSVDC-ACCESS1-1 switch.

Variable Name	Sample Values	Notes
ansible_host	172.16.117.10	Value used by the AOS-CX Ansible playbook to connect to this specific switch host.
vsx_role	primary	Value used to assign VSX role. The template file uses this variable in a conditional statement to generate proper VSX keepalive IP configuration.
Ansible Two-Tier Template

When executing an AOS-CX Ansible playbook, Jinja2-based template files are used to create AOS-CX switch configurations.

Overview

Template files are called by the playbook to build a complete AOS-CX configuration file for each target switch. The template file's Jinja2 syntax in combination with variables defined in the inventory file support the building of dynamic and complex switch configurations.

Multiple template files can be used to build configurations based on switch roles or other criteria. The playbook selects the template assigned to a switch host in the inventory file using the **config_template** variable's value. The variable can be assigned directly to a host or it can be inherited from a group.

Template Syntax

Jinja2 syntax supports the use of variable replacement values, loops, and conditional statements.

This chapter describes basic formatting of the Jinja2-based template file. The sample template can be modified or used as a reference to build new templates.

The core and access template files in this example deployment can be used unmodified when deploying CX 8325-32C core switches and any 83xx-series CX model as access switches.

Standard CLI Statements

Any standard AOS-CX switch configuration statement can be added to a template file. The configuration line is copied to the switch exactly as it appears in the file. Strict adherence to AOS-CX syntax is required, and it is best practice to use a full and complete configuration statement. Configuration statements should be placed in the correct context in the file. AOS-CX indentation uses four spaces.

The following example uses standard AOS-CX CLI configuration statements in a template file:

```
profile l3-agg
router pim
enable
active-active
https-server vrf mgmt
```

Simple Variable Substitution

The template file can substitute a single variable value in place of a static value in a configuration statement. Variable values are assigned in the inventory file. To use a variable's value in the template file, place the inventory file's variable name inside two curly braces: {{variable_name}}.

By substituting static values with a variable, the same template file can be used to configure multiple switches that require different values in config statements. In addition to applying unique values such as IP addresses, variables enable the same template to be used across different administrative and geographic boundaries. For example, inventory variables can be defined for timezones, SNMP information, DNS servers, NTP servers, and other configuration components that may have different values based on location.

The flexibility of a template file is increased as you increase the number of variables. Each administrator must balance the additional complexity of inventory and template files when increasing the number of variables for added flexibility.

Variable values can be assigned directly to a host in the inventory file, or they can be inherited from a parent group. The following example of AOS-CX configuration statements uses simple variable substitutions in a template file.

hostname {{hostname}} clock timezone {{timezone}} interface lag {{vsx_isl_lagid}}

NOTE:

A playbook error will occur if a template references a variable name that is not defined in the inventory file.

Iteration Over a List of Values

When an inventory variable is assigned a list of values, the template file can iterate over each member of the list using a **for** loop to generate multiple AOS-CX configuration lines.

Iteration over a simple list is helpful when generating multiple lines of configuration that contain a single modified value. For example, generating multiple AOS-CX configuration statements to define a set of NTP or DNS servers. Iteration over a dictionary enables more complex configuration, such as creating a set of VLAN interfaces, where each interface requires a set of additional information to build the configuration, such as VLAN ID, IP address and, active gateway assignments.

Examples of a simple list and dictionary-based iteration are provided below.

Example 1: Iteration Over a Simple List

The example inventory file defines a simple comma-delimited list for DNS servers at the **DC-RSV** group level as follows:

dns_servers: [10.2.120.98, 10.2.120.99]

The playbook calls upon the template file which iterates over this list and generates the proper AOS-CX config using the following syntax:

p{% for server in dns_servers %} ip dns server-address {{server}} vrf mgmt {% endfor %} p

In the above example, the **for** statement reads one list member at a time from the **dns_servers** variable, and assigns it to the local **server** variable. The **server** variable value is used to complete the AOS-CX configuration statement located between the beginning and end of the for loop, by replacing the variable name with its assigned value on each iteration. This process is repeated until all list members are read and each configuration line is written to the switch config file. In this example, the first list value of **10.2.120.98** is assigned to the **server** variable to generate the first configuration line from the loop. After the second list value of **10.2.120.99** is read and another configuration line is generated, the **for** loop is complete, since no additional list members are present.

The following AOS-CX configuration lines are generated from the above **for** loop:

```
ip dns server-address 10.2.120.98 vrf mgmt
ip dns server-address 10.2.120.99 vrf mgmt
```

Example 2: Iteration Over a Dictionary

The example inventory file defines a dictionary at the RSVDC-CORE1-1 host level to assign VLAN interface values (**DC-RSV > core > RSVDC-CORE1-1**). In the example below, there are two entries in the **host_vlans** dictionary, and each entry contains a list of associated variable values that are required to define a VLAN interface such as **id**, **name**, **ip_address**, etc.

```
host_vlans:
- id: 101
name: PROD-WEB
ip_address: 10.12.101.2
active_gateway_mac: 02:00:0a:01:65:01
active_gateway_ip: 10.12.101.1
- id: 102
name: PROD-DB
ip_address: 10.12.102.2
active_gateway_mac: 02:00:0a:01:65:01
active_gateway_ip: 10.12.102.1
```

The playbook calls upon the template file to iterate over the host_vlans dictionary and generate the proper AOS-CX VLAN interface config using the following syntax:

{% for vlan in host_vlans %} interface vlan {{vlan.id}} {% endfor %}

In the above example, the **for** statement reads one dictionary member at a time from the **host_vlans** array. Each array entry is read as a set of variables and assigned to the local **vlan** variable. The individual sub-variable values are referenced by concatenating the parent variable (**vlan**) and one of the sub-variable names (i.e., **id**, **name**, **ip_address**, etc.) with a dot separator. For example, **vlan.name** references the VLAN name value of the current dictionary entry read into the **vlan** variable.

This method supports writing complex configuration, where multiple variable values are associated with a single logical AOS-CX configuration area.

When the first dictionary entry is read, the following variable value assignments are made: - **vlan.id**: 101

- vlan.name: *PROD-WEB* - vlan.ip_address: 10.12.101.2 - vlan.active_gateway_mac: 02:00:0a:01:65:01 - vlan.active_gateway_ip: 10.12.101.1

- vian.active_gateway_ip: 10.12.101

NOTE:

The **for** loop contains additional logic, where if no **vlan.mask** variable is defined, the default value of **24** is substituted. It also contains reference to the **ospf_area** variable that is an inherited value of **0.0.0.0** for all hosts assigned at the **DC-RSV** group level.

The following AOS-CX configuration is generated by the template using the example **for** loop:

```
interface vlan 101
   description PROD-WEB
   ip mtu 9198
   ip address 10.12.101.2/24
   active-gateway ip mac 02:00:0a:01:65:01
    active-gateway ip 10.12.101.1
    ip ospf 1 area 0.0.0.0
    ip igmp enable
    ip pim-sparse enable
interface vlan 102
   description PROD-DB
   ip mtu 9198
    ip address 10.12.102.2/24
    active-gateway ip mac 02:00:0a:01:65:01
    active-gateway ip 10.12.102.1
   ip ospf 1 area 0.0.0.0
    ip igmp enable
    ip pim-sparse enable
```

Conditional Statements

Jinja2 supports evaluating conditional if/then/else statements, which can be used when generating configuration statements.

The example below contains two conditional statements, a second nested inside the first:

{% if vsx_keepalive_int is defined %} interface {{vsx_keepalive_int}} {% if vsx_role == "primary" %} {% else %} {% endif %}

In the example above, the conditional statement **{% if vsx_keepalive_int is defined %}** checks if the **vsx_keepalive_int** variable is defined for the current host for which the configuration is being generated. If not, the entire stanza above is ignored and no VSX keepalive interface configuration is generated for the switch. If the variable is defined, the configuration is generated using variable substitution.

The second conditional evaluation is designed to assign the correct IP address to the VSX keepalive interface based on the role of the switch in the VSX pair. Both the primary and secondary keepalive IP addresses are defined in the inventory file. If the current switch processed by the playbook is the primary switch, then the **vsx_keepalive_ip_primary** variable value is assigned. If the switch is not the primary, then the **vsx_keepalive_ip_secondary** variable value is assigned.

Run the Two-Tier Playbook

Execute the following command from the root level of the cloned repository:

ansible-playbook deploy_2tierv2_dcn.yml -i inventory_2tierv2_dcn.yml

The playbook performs the following actions on every device in the inventory file:

Step 1 Generate switch configuration files. The switch configurations are based on inventory file variable values and Jinja2 configuration templates assigned in the inventory file.

NOTE:

The **core** group in the inventory file assigns the templates/2TierV2/core.j2 template file to the **config_template** variable. Both core switches are configured using this template.The **access** group in the inventory file is assigned the templates/2TierV2/access.j2 template file to the **config_template** variable. All access switches are configured using this template.

Step 2 Push the generated configurations to each switch using the AOS-CX Ansible SSH module **aoscx_config**.

Step 3 Enable 10g speed interface groups, if defined in the inventory file. In the example, the access switches have interface groups defined that operate at the non-default value of 10 Gbps .

Aruba Validated Hardware and Software

The following hardware and software versions are used for the creation of this guide.

Features have been independently validated. Interoperability validation of the combined feature set in this guide is pending.

EVPN-VXLAN Fabric

Wired Switching

Product Name	Software Version
Aruba CX 8325	10.11.1050
Aruba CX 10000	10.11.1050
Aruba CX 8360	10.11.1050
Aruba CX 6300	10.11.1050
Aruba CX 6400v2	10.10.1010

Management and Orchestration

Product Name	Software Version
Aruba Fabric Composer	6.5.3-13069
Pensando Policy and Services Manager	1.54.5-T-2

Layer 2 Two-Tier

Switching Products

Product Name	Software Version
Aruba CX 8325	10.13.1000
Aruba CX 8360	10.13.1000

Management and Orchestration

Product Name	Software Version
Aruba Central	2.5.8

© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to: www.arubanetworks.com/assets/legal/EULA.pdf



www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054 1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550

See Confluence for Correct Doc Title