



a Hewlett Packard
Enterprise company

HPE Synergy and Aruba CX 10000 Networking Deployment Guide

Contents

Introduction.....	3
Overview.....	4
Prerequisites.....	5
Detailed Topology.....	6
Task 1: AOS-CX Switches.....	7
Task 2: Aruba Fabric Composer.....	8
Guided Setup	8
Switch to Fabric Association	10
VSX Configuration	11
Persona Configuration	17
VSX LAG Configuration	18
VRF and SVI Configuration	22
PVLAN Configuration	28
PSM Integration.....	31
VMware vCenter Integration	33
Task 3: HPE Synergy Networking	37
Networks	37
Logical Interconnects	38
Server Profiles.....	40
Task 4: VMware vDS.....	43
Task 5: Distributed Services	50
Distributed Firewall Configuration	52
Task 6: Security Policy Validation & FW Logging.....	65
Appendix.....	70
CX10000-1 Configs and Verification Commands	70
CX10000-2 Configs and Verification Commands	77

Introduction

The Aruba CX 10000 Series Switch with Pensando represents a new category of data center switches that combines best-of-breed Aruba data center L2/3 switching with the industry's only, fully programmable data-processing unit (DPU). The Pensando Elba DPU is able to deliver stateful software-defined services inline, at scale, with wire-rate performance and orders of magnitude scale and performance improvements over traditional data center L2/3 switches at a fraction of their TCO.

The Pensando Policy and Services Manager (PSM) is a distributed system, leveraging an intent-based model that delivers network and security policy to CX 10000 DPUs at the edge.

Aruba Fabric Composer is an intelligent, API-driven, software-defined orchestration solution that simplifies and accelerates network provisioning, security management and day-to-day operations across rack-scale compute and storage infrastructure. PSM integration allows network security policies to be configured directly from Aruba Fabric Composer.

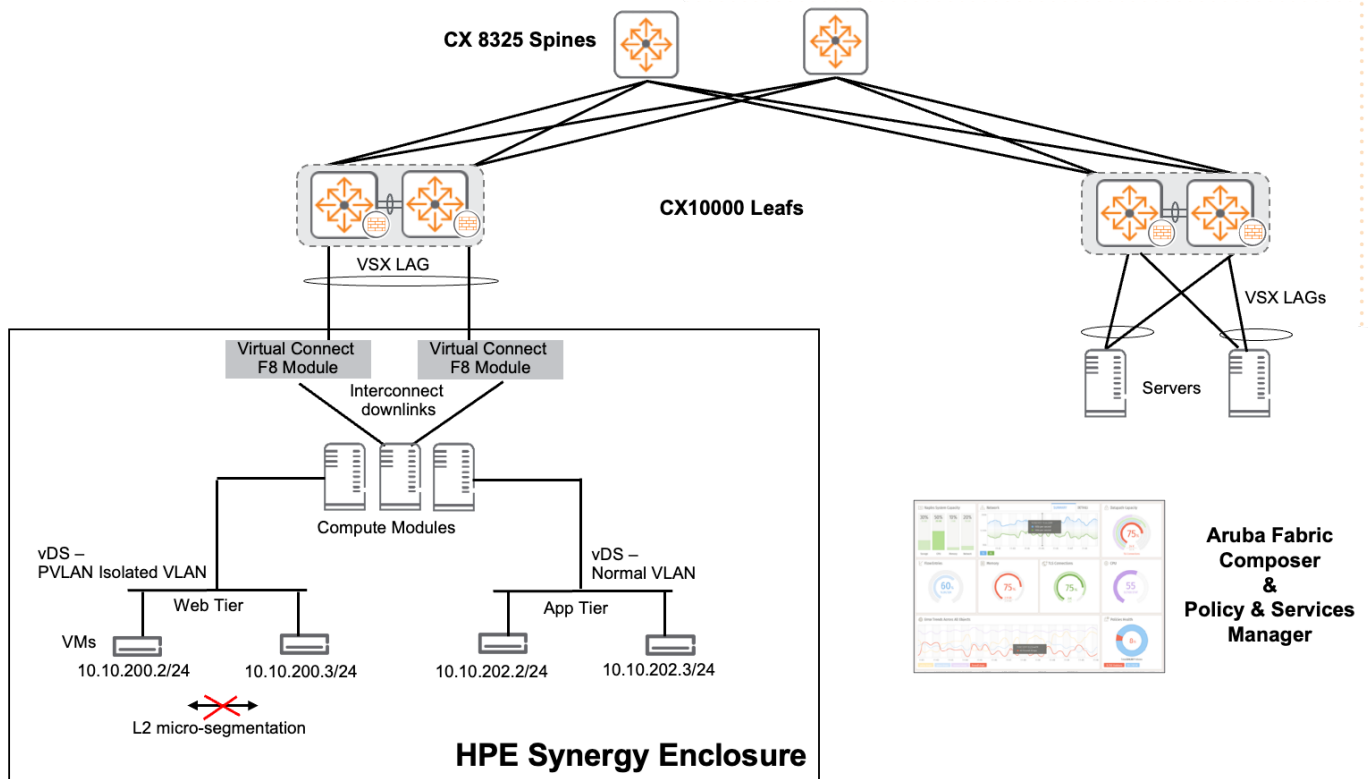
Aruba Fabric Composer together with the Pensando Policy and Services Manager (PSM) provides a distributed system, leveraging an intent-based model that delivers network and security policy to Aruba CX 10000 DPUs at the edge.

This document provides networking guidance when building out a solution that leverages an HPE Synergy enclosure connected to an Aruba CX 10000 network managed by Aruba Fabric Composer and PSM.

Overview

As shown in Figure 1, Aruba Fabric Composer provides underlay and overlay automation for the Data Center fabric comprising Aruba CX 8325 Spines and CX 10000 Leafs which connect to rack mount servers and blade server enclosures such as HPE Synergy.

Figure 1. Data Center with CX 8325 Spines, CX 10000 Leafs and HPE Synergy



For network redundancy and traffic load sharing, HPE Synergy Virtual Connect modules connect to the Aruba CX 10000s via a Virtual Switching Extension (VSX) Link Aggregation Group (LAG). “Tunnel” mode would be used on Virtual Connect to simplify and minimize network configuration within HPE OneView.

In addition, when Aruba Fabric Composer (AFC) is integrated with VMware vCenter, you can easily create vSphere Distributed Switches (vDS), PVLAN, port groups and visualize those network connections between the physical switches, Virtual Connect ports, vSwitches, Virtual Machines (VMs).

The Aruba CX 10000 network security policies provide east/west firewall capabilities between Servers, Virtual Machines (VMs) or Containers within a VLAN or across different network VLAN/subnets. If micro-segmentation within the same hypervisor or across different hypervisors and within the same subnet is required for network isolation and security policies, Private VLAN (PVLAN) can be utilized. This guide uses VMware vSphere Distributed Switch on HPE Synergy compute modules as an example.

Prerequisites

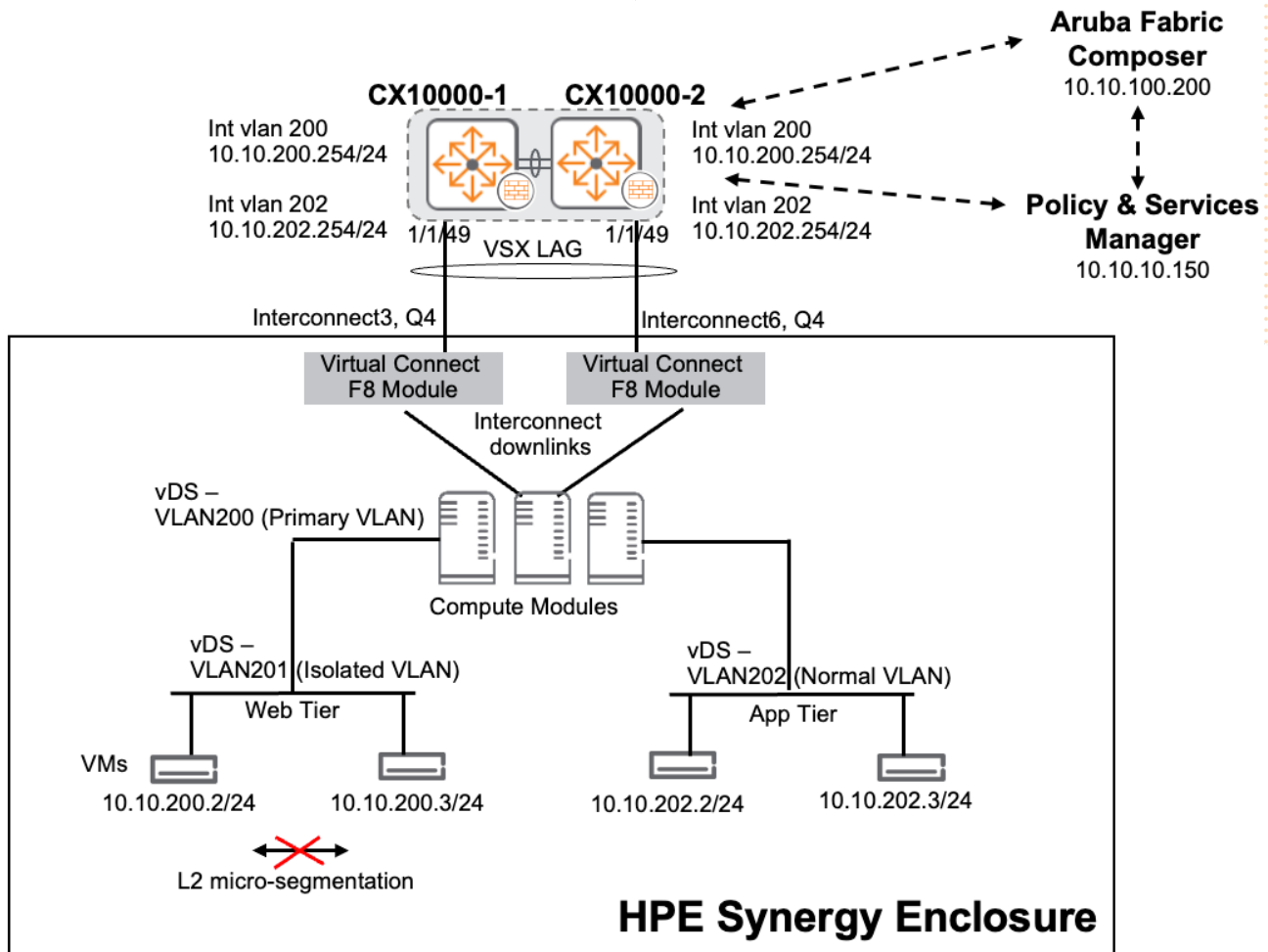
Before connecting and configuring an HPE Synergy enclosure to the Aruba CX 10000 network, the following are recommended:

- Aruba CX 10000s loaded and booted up with code version 10.09.0010 (minimum)
- Ports between devices should be cabled up and connected without errors
- A separate Out Of Band (OOB) network for management
 - Aruba CX 6300 switches are suitable for the OOB network
 - Mgmt ports of the Aruba CX 8325/10000 switches, Aruba Fabric Composer and PSM should be connected to the OOB network and have IP reachability between each other
- Aruba Fabric Composer 6.2 (minimum) should be functional, refer to [Aruba Support Portal](#)
 - This guide is focused on HPE Synergy with Aruba CX 10000 switches, refer to Aruba Fabric Composer documentation for Aruba Fabric Composer high availability deployment recommendations
- PSM 1.29.2-T-11 (minimum) should be functional, refer to [Aruba Support Portal](#)
 - This guide is focused on HPE Synergy with Aruba CX 10000 switches. Please refer to PSM documentation for PSM high availability deployment recommendations
- HPE OneView and HPE Synergy should be functional, refer to [HPE Synergy Documentation Quick Links for more information on HPE Synergy networking](#)
 - For reference, this guide used firmware 1.7.1.1001 for interconnects, firmware 6.4.00 for Oneview and enclosure bundles
- For flow-logging to appear properly within PSM, make sure that the time set within the attached PC/VM is set to the same time as PSM.

Detailed Topology

As this guide is focused on HPE Synergy with Aruba CX 10000 switches, the detailed topology as shown in Figure 2 will be used and referenced for the rest of this guide.

Figure 2. Data Center rack with Aruba CX 10000 Leafs and HPE Synergy



3 VLANs are used in this guide:

- VLAN 200 – Primary PVLAN
 - Int VLAN 200 (10.10.200.254/24) on Aruba CX 10000s will function as default gateways for VLAN 200 and VLAN 201.
 - Suitable for VMs that do not require L2 micro-segmentation on the 10.10.200.0/24 subnet.
- VLAN 201 – Isolated PVLAN
 - Suitable for VMs that require L2 micro-segmentation on the 10.10.200.0/24 subnet.
- VLAN 202 – Normal VLAN (Non PVLAN)
 - Interface VLAN 202 (10.10.202.254/24) on Aruba CX 10000s will function as default gateways for VLAN

202.

- Suitable for VMs that do not require L2 micro-segmentation on the 10.10.202.0/24 subnet.

For network redundancy and traffic load sharing, 1 x 40G uplink on each HPE Synergy Virtual Connect module connects to a pair of Aruba CX 10000s via VSX LAG. LACP is only required between Aruba CX 10000s and the Virtual Connect modules. The vDS doesn't require LACP to Virtual Connect modules. When "Tunnel" mode is configured on Virtual Connect, there is no requirement to create VLANs or PVLANS in OneView.

Note that connectivity options from the Synergy enclosure to the Aruba CX 10000 switches will vary based on the VC module in use and the constraints of the environment. Depending on the VC module chosen users could use 40G or 100G interfaces, but they could also use 4x10G or 4x25G interfaces to connect to each ToR switch.

Please refer to the Synergy site for more details on VC modules available - <https://www.hpe.com/us/en/integrated-systems/synergy.html>

To implement east/west firewall capabilities between VMs on different subnets, security policies configured on Aruba Fabric Composer are pushed down via PSM to the Aruba CX 10000 DPUs to permit or deny desired traffic.

The remainder of this guide walks through the tasks required for this deployment to be successful and should be done sequentially.

Task 1: AOS-CX Switches

Using console access, enter the base configuration below required on AOS-CX switches for Aruba Fabric Composer management, modify hostnames and IPs as required.

```
configure
hostname CX10000-R1RU33-SW1
interface mgmt
ip static 10.251.X.5/24
default-gateway 10.251.X.254
```

If you need ports changed from 25g to 10g, you will need to modify the interface-group as required.

```
system interface-group 1 speed 10g
!interface group 1 contains ports 1/1/1-1/1/4
system interface-group 5 speed 10g
!interface group 5 contains ports 1/1/17-1/1/20
```

When managed by Aruba Fabric Composer, the majority of Aruba CX 10000 features can be configured from the Aruba Fabric Composer GUI.

To ensure all traffic is inspected by the security policy, this should also be added at the global level.

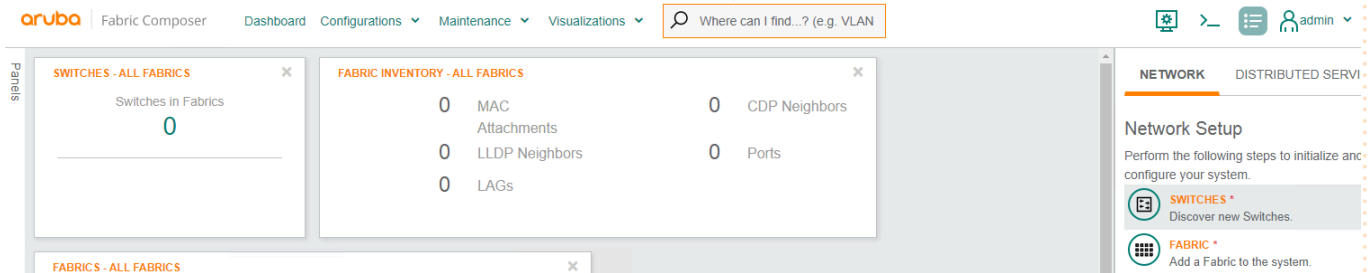
```
no ip icmp redirect
```

Task 2: Aruba Fabric Composer

This section provides guidance on automating the network fabric, validating connectivity to the Aruba CX switches, PSM, and integration with vSphere/PSM.

Guided Setup

After logging into Aruba Fabric Composer, click the guided network setup (green icon with 3 ...) on the right.



Click on “SWITCHES” to discover new switches, enter IPs and desired passwords to be pushed down to the switches.

Discover Switches

Enter the details of the Switches to be discovered.

Switches *
10.10.10.212-10.10.10.213

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

admin Switch Password *

The switches admin account password for switch access. If the switches have no password, this password will be set on them. Any non empty string, example: thing.red.7

Confirm admin Switch Password *

Must match the admin Switch Password

afc_admin Account Password *

A password to be used for the afc_admin account creation for switch access. Any non empty string, example: car.top-2

Confirm afc_admin Account Password *

Must match the afc_admin Account Password

(* = Required)

CANCEL
APPLY

The switches should be added but unassigned.

aruba | Fabric Composer | Dashboard | Configurations ▾ | Maintenance ▾ | Visualizations ▾ |

Switches
Audits
Support Bundles
Device Firmware
Backups

Maintenance / Switches

	Health	Status	Name
<input type="checkbox"/>	Select Health...	Select Status...	Enter Regex for Name...
<input type="checkbox"/>	HEALTHY, BUT...	Unassigned	10000-RU33-SW1
<input type="checkbox"/>	HEALTHY, BUT...	Unassigned	10000-RU34-SW2

Click on “FABRIC” on the guided network setup to add a fabric, enter desired info and click “APPLY”.

Fabric

Enter a required Fabric Name and an optional Description and Time Zone. A time zone will be applied to all switches in the fabric.

Name *
Any non empty string, example: fabric01

Description
Example: My New Fabric

Type * × ▾
Select Data for your network traffic, Management for out of band management traffic.

Time Zone ▾

Auto Save Interval min
A value between 600 seconds (10 minutes) and 43200 seconds (12 hours) for the system to automatically copy the running config to startup config for each switch in fabric. 0 disables Auto Save.

(* = Required)

CANCEL

APPLY

Switch to Fabric Association

After the switches are discovered, you can assign switches to the fabric by clicking on “ASSIGN SWITCH TO FABRIC” in the guided setup workflow on the right.

Configuration / System / Fabrics & Switches

Name	Health	Type
Enter Regex for Name...	Select Health...	Enter Regex for Typ...
CX10000	HEALTHY	Data
Unassigned		

Network Setup
Perform the following steps to initialize and configure your system.

- SWITCHES**
Discover new Switches.
- FABRIC**
Add a Fabric to the system.

Selected Fabric:
CX10000

ASSIGN SWITCH TO FABRIC *
Assign Switch To Fabric

Add the switches, select a fabric, desired role, initialize the ports and click “ADD” and then “APPLY”.

Select a role for the selected Switches.

☒ Force LLDP Discovery

☒ Initialize Ports
Enable ports, routing, and set default MTU values.

☐ Exclude this switch from association to any Distributed Services Manager

Switch	Role	Force LLDP Discovery	Initialize Ports	Exclude this switch from...
10000-RU33-SW1	Leaf	Yes	Yes	No
10000-RU34-SW2	Leaf	Yes	Yes	No

(* = Required)

After a minute or so, the switches should appear healthy and synced with the assigned fabric.

Maintenance / Switches

Health	Status	Name	Fabric
Select Health...	Select Status...	Enter Regex for Name...	Enter Regex for Fab...
HEALTHY	Synced	10000-RU33-SW1	CX10000
HEALTHY	Synced	10000-RU34-SW2	CX10000

Users can continue to follow the workflow on the right and now add NTP/DNS configurations. The configs are straight forward so this guide continues to the VSX setup portion of the workflow.

VSX Configuration

Click “VSX CONFIGURATION” in the guided setup workflow on the right.

Maintenance / Switches

	Health	Status	Name	Fabric
<input type="checkbox"/>	× Healthy ×	Select Status...	Enter Regex for Name...	Enter Regex for Fabric...
<input type="checkbox"/>	HEALTHY	Synced	10000-RU33-SW1	CX10000
<input type="checkbox"/>	HEALTHY	Synced	10000-RU34-SW2	CX10000

ACTIONS ▾

NETWORK DISTRIBUTED SE

Network Setup

Perform the following steps to initialize configure your system.

- SWITCHES**
Discover new Switches.
- FABRIC**
Add a Fabric to the system.

Selected Fabric:

CX10000

- ASSIGN SWITCH TO FABRIC**
Assign Switch To Fabric
- NTP CONFIGURATION**
Configure Switch NTP.
- DNS CONFIGURATION**
Configure Switch DNS.
- VSX CONFIGURATION**
Configure VSX Switch Pairing.

Select “Automatically generate VSX Pairs” and click “NEXT”.

VSX (CX10000) ? ×

Create Mode Name Inter-Switch Link Settings Keep Alive Interfaces Keep Alive Settings Options Summary

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

NEXT

Add desired name and click “NEXT”.

VSX (CX10000) ? ×

✓

Create Mode

✓

Name

?

Inter-Switch Link Settings

?

Keep Alive Interfaces

?

Keep Alive Settings

?

Options

?

Summary

Enter a required Name Prefix and an optional Description.

Name Prefix *

Any non empty string, example: MyVsxPair

Description

Example: VSX Pair

(* = Required)

CANCEL

BACK

NEXT

Use default values and click “NEXT”.

VSX (CX10000) ? ×

✓

Create Mode

✓

Name

✓

Inter-Switch Link Settings

?

Keep Alive Interfaces

?

Keep Alive Settings

?

Options

?

Summary

Specify the required Hello and Peer Detect Intervals as well as the Hold Time and Timeout. This will be applied to the automatically generated Inter-Switch Links.

Hello Interval *

A number of seconds between 1 and 5, example: 1

Peer Detect Interval *

A number of seconds between 60 and 600, example: 300

Hold Time *

A number of seconds between 0 and 3, example: 0

Timeout *

(* = Required) Scroll for more options

CANCEL

BACK

NEXT

Enter desired keepalive interface mode and add an address pool.

✓

✓

✓

?

?

?

?

Create Mode

Name

Inter-Switch Link Settings

Keep Alive Interfaces

Keep Alive Settings

Options

Summary

Specify the required Keep Alive Interface attributes. This will be used to automatically generate and associate IP Interfaces of the selected type to the VSX Switch members.

Interface Mode Point-to-Point

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 Select ... ADD

IPv4 Subnetwork Address
A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24

(* = required)

CANCEL
BACK
NEXT

Click “ADD” to provide a name for the address pool, and then click “NEXT”.

✓

?

?

Name

Settings

Summary

Enter a required Name and an optional Description.

Name * Pool1
Any unique non empty string, example: ResourcePool-1

Description
Example: ResourcePool-1 description

(* = required)

CANCEL
BACK
NEXT

Add a subnet range and then click “NEXT” and then “APPLY”.

Resource Pool

✓

✓

?

Name
Settings
Summary

Select a required resource type and a set/range of resources.

Resource Type

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: 192.168.1.10, 192.168.1.100-192.168.1.200, 192.168.10.0/24

Resource Count 254

(* = required)

CANCEL
BACK
NEXT

Click “NEXT”.

VSX (CX10000)

✓

✓

✓

✓

?

?

?

Create Mode
Name
Inter-Switch Link Settings
Keep Alive Interfaces
Keep Alive Settings
Options
Summary

Specify the required Keep Alive Interface attributes. This will be used to automatically generate and associate IP Interfaces of the selected type to the VSX Switch members.

Interface Mode

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

IPv4 Subnetwork Address

A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24

(* = required)

CANCEL
BACK
NEXT

For Keepalive setting, keep as default values, and click "NEXT".

VSX (CX10000) ? ×

✓

Create Mode

✓

Name

✓

Inter-Switch Link Settings

✓

Keep Alive Interfaces

✓

Keep Alive Settings

?

Options

?

Summary

Specify the required Hello and Dead Intervals as well as the UDP Port to be used for the Keep Alive Interfaces.

Hello Interval * A number of seconds between 1 and 5, example: 1

Dead Interval * A number of seconds between 2 and 20, example: 3

UDP Port * A number between 1024 and 65535, example: 7678

(* = Required)

CANCEL BACK NEXT

Leave the Linkup timer as default and click "ADD" to add a MAC Address Resource Pool, or simply add the desired MAC Address range needed. Click "NEXT".

VSX (CX10000) ? ×

✓

Create Mode

✓

Name

✓

Inter-Switch Link Settings

✓

Keep Alive Interfaces

✓

Keep Alive Settings

✓

Options

?

Summary

Set the required Linkup Delay Timer, and System MAC Address.

Linkup Delay Timer * A number of seconds between 0 and 600, example: 180

Set the System MAC Address Range. Select or add a MAC Address Resource Pool or specify a range.

MAC Address Resource Pool

MAC Address Range A hyphen-separated range of valid MAC Addresses, example: 02:00:00:00:01:00-02:00:00:00:01:FF

(* = Required)

CANCEL BACK NEXT

Review the parameters and click “APPLY”.

VSX (CX10000)

✓

Create Mode

✓

Name

✓

Inter-Switch Link Settings

✓

Keep Alive Interfaces

✓

Keep Alive Settings

✓

Options

✓

Summary

Name Prefix	Synergy
Description	
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	Pool1 (192.168.10.0/24)
Keep Alive Hello Interval	1
Keep Alive Dead Interval	3
Keep Alive UDP Port	7678

CANCEL

BACK


APPLY

VSX should now be operational (you may need to click refresh for AFC to reflect that). Make sure that parameters are operational, in_sync, and peer_established.

Configuration / Network / VSX

Fabric		CX10000	
		FACILITIES	
		ACTIONS	
Primary Switch Keep Alive Int...	Primary Switch Overall State	Primary Switch ISL State	Primary Switch Device State
Enter Regex for Primary Switc	Enter Regex for Primary Switc	Enter Regex for Primary Switc	Enter Regex for Primary Switc
VSX Keep alive interface - 10000- RU34-SW2 - 192.168.10.2/31	operational	in_sync	peer_established

Persona Configuration

Click on “Configurations” > “Ports” > “Ports” >  con > select desired switch on top right drop down menu. Users can select multiple switches, if desired – in this example select both Aruba CX 10000 switches.

Select the ports facing the server (both 1/1/49 in this example) and click > Actions > Port Type

Configuration / Ports / Ports

Fabric Switch



×

 10000-RU33-SW1

×

 10000-RU34-SW2

SELECT ALL

2 selected  

☒ Selected
☐ Not Available

LAG LINK AGGREGATION GROUP

UPLINK

☐ Enabled
☐ Disabled
☐ No Transceiver
☐ Filtered
☐ Port has a health issue

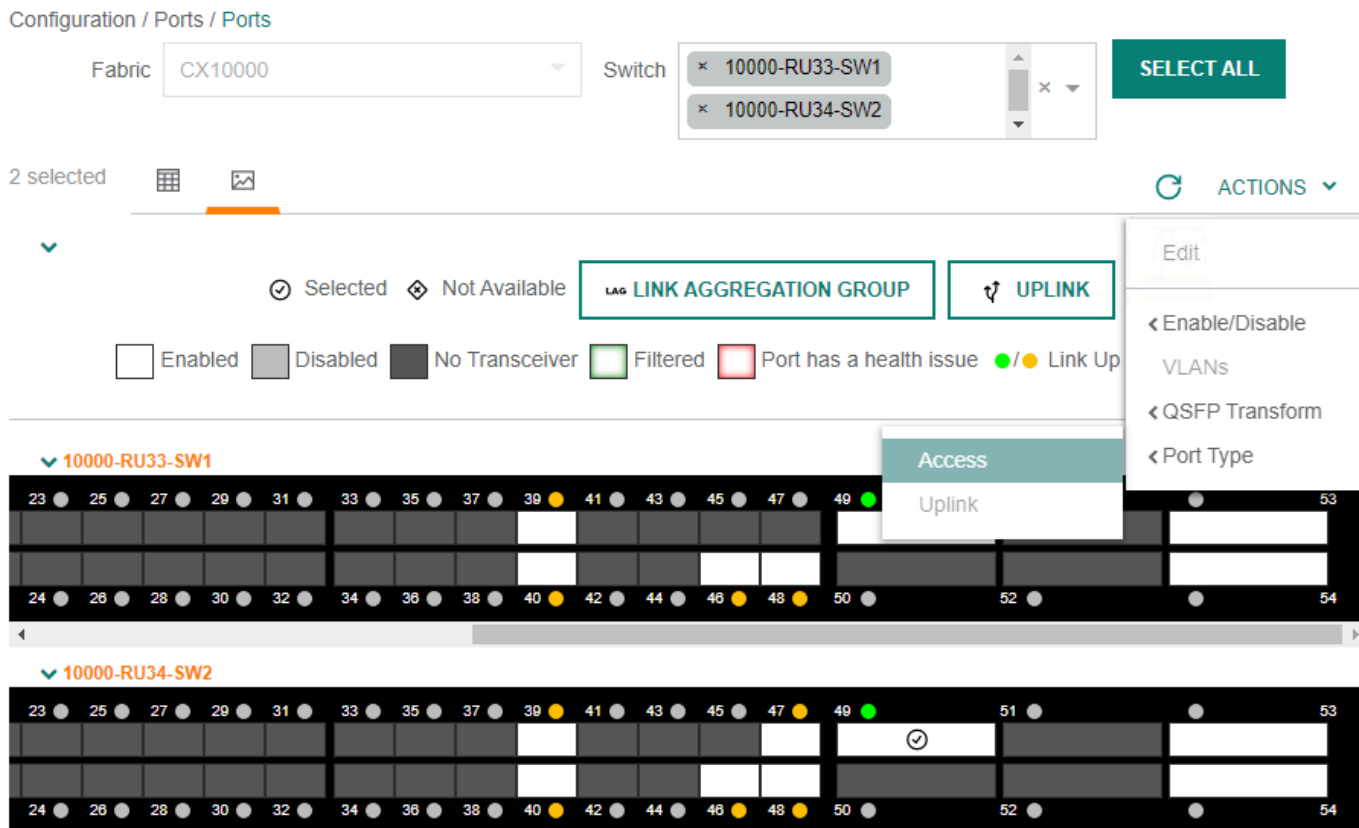
●/● Link Up

10000-RU33-SW1

Access

Uplink

10000-RU34-SW2



Select the “Access” port type and then click “OK”.

VSX LAG Configuration

Click on “Configurations” > “Ports” > “Link Aggregation Groups” > “ACTIONS” > “Add”

aruba | Fabric Composer | Dashboard | Configurations | Maintenance | Visualizations | Where can I find...? (e.g. VLAN)

Ports

Link Aggregation Groups

VLAN Groups

PVLANS

Transceivers

Configuration / Ports / Link Aggregation Groups

Fabric: CX10000

	Name	Type	LAG Number
<input type="checkbox"/>	<input type="text" value="Enter Regex for Name..."/>	<input type="text" value="Select Type..."/>	<input type="text" value="Enter Regex for LAG Number..."/>
> <input type="checkbox"/>	ISL-10000-RU33-SW1	Inter-Switch Link	256
> <input type="checkbox"/>	ISL-10000-RU34-SW2	Inter-Switch Link	256

ACTIONS: Add, Edit, Delete, VLANs

Select a single LAG option and click “NEXT”.

Link Aggregation Group

Create Mode Settings Ports LACP Settings Summary

Select an option to create the LAG(s). Choose to create multiple MLAGs or to configure a single LAG.

☐ Create multiple MLAGs for selected VSX Pairs.

☒ Create a single Link Aggregation Group.

(* = required)

CANCEL BACK NEXT

Enter a desired name, LAG number and then click “NEXT”.

Link Aggregation Group

?

×

✓

Create Mode

✓

Settings

?

Ports

?

LACP Settings

?

VLANs

?

Summary

Enter a required Name and optional Description and LAG Number.

Name *

Any non empty string, example: LAG-1

Description

Example: Link Aggregation Group 1

LAG Number

A number between 1 and 256, example 1

☐ Inter-Switch Link

(* = Required)

CANCEL

BACK

NEXT

Select the VSX switches/ports connected to Synergy Virtual Connect and click “NEXT”.

Link Aggregation Group

?

×

✓

Create Mode

✓

Settings

✓

Ports

?

LACP Settings



?

VLANs

?

Summary

LAG Switch Member

2 selected  

	Switch	Port	Enabled	Link State	Routed	Current Speed
<input type="checkbox"/>	<input type="text" value="Enter Regex for Switch..."/>	<input type="text" value="49"/>	<input type="text" value="Select Enable..."/>	<input type="text" value="Select Link St..."/>	<input type="text" value="Select Routed..."/>	<input type="text" value="Select Current..."/>
<input checked="" type="checkbox"/>	10000-RU33-SW1	1/1/49	Yes	up	Yes	40Gbps
<input checked="" type="checkbox"/>	10000-RU34-SW2	1/1/49	Yes	up	Yes	40Gbps

(* = Required) Scroll for more options

CANCEL

BACK

NEXT

Select the switches and enter the desired values and click "NEXT".

Link Aggregation Group

?

✕

✓

✓

✓

✓

?

?

Create Mode

Settings

Ports

LACP Settings

VLANs

Summary

☒ ENABLE LACP Falldack

<input checked="" type="checkbox"/>	Switch	Ports	LACP Mode	LACP Interval	Priority
<input checked="" type="checkbox"/>	CX10000-R1RU33-SW1	1/1/49	Active	Slow	1
<input checked="" type="checkbox"/>	CX10000-R1RU34-SW2	1/1/49	Active	Slow	1

LACP Mode

Active

LACP Interval

Slow

✕

Priority

1

A number between 1 and 32768, example 1

(* = Required)

Scroll for more options

CANCEL

BACK

NEXT

Enter a native VLAN, desired VLANs to be allowed, and click "NEXT" and "APPLY".

Link Aggregation Group

?

✕

✓

✓

✓

✓

✓

?

Create Mode

Settings

Ports

LACP Settings

VLANs

Summary

Assign Native VLAN, VLANs, VLAN Groups, and PVLAN Port Type to the LAG. At least one VLAN must be configured for an MLAG.

Native VLAN

1

A VLAN between 0 and 4094, example: 1. Empty or 0 disables the Native VLAN.

VLANs

200-202

'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

Select PVLAN Port Type...

(* = Required)

CANCEL

BACK

NEXT

VSX LAG info can be seen if you expand it out.

Configuration / Ports / Link Aggregation Groups

Fabric

CX10000

ACTIONS ▾

	<div>Name</div> <div><div>Enter Regex for Name...</div></div>	<div>Type</div> <div><div>Select Type...</div></div>	<div>LAG Number</div> <div><div>Enter Regex for LAG Number.</div></div>	<div>Switch</div> <div><div>Enter Regex for</div></div>
>	<input type="checkbox"/> ISL-10000-RU33-SW1	Inter-Switch Link	256	10000-RU33-SW1
>	<input type="checkbox"/> ISL-10000-RU34-SW2	Inter-Switch Link	256	10000-RU34-SW2
✓	<input type="checkbox"/> Synergy	Provisioned	10	10000-RU33-SW1 10000-RU34-SW2

<div>Switch</div> <div><div>Enter Regex for Switch...</div></div>	<div>Port</div> <div><div>Enter Regex for Port...</div></div>	<div>Speed</div> <div><div>Select Speed...</div></div>	<div>LACP Mode</div> <div><div>Select LA</div></div>
10000-RU33-SW1	1/1/49	Auto	Active
10000-RU34-SW2	1/1/49	Auto	Active

VRF and SVI Configuration

Click on “Configurations” > “Routing” > “VRF” > “ACTIONS” > “Add”.

aruba | Fabric Composer | Dashboard | Configurations ▾ | Maintenance ▾ | Visualizations ▾ | Where can I find...? (e.g. VLAN)

VRF

Configuration / Routing / VRF

Fabric: CX10000

	Name	Type	Switches	
	<input type="text" value="Enter Name..."/>	<input type="text" value="Select Type..."/>	<input type="text" value="Enter Switches..."/>	
...	default	Default		
...	mgmt	Management		

ACTIONS ▾

- Add
- Edit
- Delete
- Reapply VRF

Enter the desired name and click “NEXT”.

Virtual Routing & Forwarding

Progress: **Name** (✓) | Scope (?) | Routing (?) | Route Targets (?) | Summary (?)

Enter a required Name and an optional Description.

Name *

Any non empty string between 1 and 92 characters, example: VRF1

Description

Example: New Virtual Routing and Forwarding

(* = required)

CANCEL **BACK** **NEXT**

You can either “Apply” the config to all switches or select specific switches and click “NEXT”.

Virtual Routing & Forwarding

✓

Name

✓

Scope

?

Routing

?

Route Targets

?

Summary

Set the scope of the VRF. The VRF may be applied to the entire Fabric or to a specific set of Switches within the Fabric.

☐ Apply the VRF to the entire Fabric and all Switches contained within it.

Switches

× CX10000-R1RU33-SW1 / CX10000-R1RU34-SW2 (VSX)

DESELECT ALL

(*) = required

CANCEL

BACK

NEXT

“L3 VNI” and “Route Targets” are not required if VXLAN is not used, so for this example click “NEXT” on both screens to proceed.

Virtual Routing & Forwarding

✓

Name

✓

Scope

✓

Routing

?

Route Targets

?

Summary

Set the optional L3 VNI.

L3 VNI

A number between 1 and 16777214, example 1

(*) = required

CANCEL

BACK

NEXT

Virtual Routing & Forwarding

Enter the optional Route Target Mode and Ext-Community. Enter both or none of the fields.

Route Target Mode:

Route Target Ext-Community:
A valid Autonomous System Number, example: 65001:101

Address Family:

Route Target Mode	Route Target Ext-Community	Address Family
There is no data to display		

(* = required)

Review the parameters and click “APPLY”.

Virtual Routing & Forwarding

Name: Synergy
 Description:
 Switches: 10000-RU34-SW2 / 10000-RU33-SW1 (VSX)

After the desired VRF is created, select that VRF and then click on “ACTIONS” > “IP Interfaces”

aruba | Fabric Composer | Dashboard | Configurations | Maintenance | Visualizations | Where can I find...? (e.g. VLAN)

VRF

Configuration / Routing / VRF

Fabric: CX10000

Name	Type	Switches	
Enter Name...	Select Type...	Enter Switches...	
...	default	Default	...
...	mgmt	Management	...
...	Synergy	User	10000-RU33-SW1,10000-RU34-SW2

ACTIONS

- Add
- Edit
- Delete
- Reapply VRF
- IP Interfaces
- IP Static Routes

Under “IP Interfaces”, click on “ACTIONS” > “Add”

aruba | Fabric Composer | Dashboard | Configurations | Maintenance | Visualizations | Where can I find...? (e.g. VLAN)

VRF

Configuration / Routing / VRF / Synergy

Fabric: CX10000

Name	Type	Switches	Route Distinguisher	L3 VNI
Enter Name...	Select Type...	Enter Switches...	Enter Regex for Route Disting	En
Synergy	User	10000-RU33-SW1,10000-RU34-SW2		0

IP INTERFACES | IP STATIC ROUTES | NETWORKS | ARP TABLES | IP ROUTE TABLES

Type	Enabled	Switch	VLAN	
Select Type...	Select Enable...	Enter Switch...	Enter Regex for VL	

ACTIONS

- Add
- Edit
- Delete

Enter your desired VLAN, switches, and subnet.

IP Interface

?

Interface Type

?

Name

?

Summary

Select the IP Interface Type and set the appropriate attributes.

☒ Enable this IP Interface

Type

VLAN *
A VLAN between 1 and 4094, example: 1.

Switches *

IPv4 Subnetwork Address *
A valid IPv4 Subnet in CIDR format. Example: 192.168.1.0/24

(* = Required) [Scroll for more options](#)

Enter your desired SVI IP range, active gateway IP and MAC.

“Enable Local Proxy ARP” should be selected for primary PVLAN SVI (VLAN 200) to allow VMs on the same isolated PVLAN to communicate if desired via the security policy. “Enable Local Proxy ARP” is not required for normal VLAN 202.

Click “NEXT”.

IP Interface

✓

Interface Type

?

Name

?

Summary

IPv4 Addresses *
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: 00:00:00:00:00:01. Both Active Gateway values must be defined if using Active Gateway.

☐ Enable VSX Shutdown on Split

☒ Enable Local Proxy ARP

(* = Required) [Scroll for more options](#)

Enter an optional name, description and then click “NEXT”.

IP Interface

✓

Interface Type

✓

Name

?

Summary

Enter an optional Name and Description.

Name

A string, up to 42 characters. example: ipinterface1

Description

Example: My New IP Interface

(* = required)

CANCEL
BACK
NEXT

Review the parameters and then click “APPLY”.

IP Interface

✓

Interface Type

✓

Name

✓

Summary

Name	
Description	
Type	SVI
Enabled	Yes
VLAN	200
Switches	10000-RU34-SW2 / 10000-RU33-SW1 (VSX)
Active Gateway IP Address	10.10.200.254
Active Gateway MAC Address	00:00:00:00:00:01
IPv4 Addresses	10.10.200.250-10.10.200.254
VSX Shutdown on Split	No
Local Proxy ARP Enabled	Yes

CANCEL
BACK
APPLY

SVIs should now be operational, repeat for other desired SVIs.

In this guide, only VLANs 200 and 202 require SVIs. VLAN 201 is an isolated PVLAN and uses VLAN 200 primary PVLAN as the SVI for the 10.10.200.0/24 subnet.

aruba Fabric Composer Dashboard Configurations Maintenance Visualizations Where can I find...? (e.g. VLAN)

VRF

BGP

OSPF

EVPN

Configuration / Routing / VRF / Synergy

Fabric CX10000

ACTIONS

Name	Type	Switches	Route Distinguisher	LS
Enter Name...	Select Type...	Enter Switches...	Enter Regex for Route Disting	
Synergy	User	10000-RU33-SW1,10000-RU34-SW2		0

IP INTERFACES IP STATIC ROUTES NETWORKS ARP TABLES IP ROUTE TABLES

ACTIONS

Type	Enabled	Switch	VLAN	Port/LA
Select Type...	Select Enable...	Enter Switch...	Enter Regex for VLAN...	Enter
<input type="radio"/> SVI	Yes	10000-RU34-SW2	200	
<input type="radio"/> SVI	Yes	10000-RU33-SW1	200	
<input type="radio"/> SVI	Yes	10000-RU34-SW2	202	
<input type="radio"/> SVI	Yes	10000-RU33-SW1	202	

PVLAN Configuration

Click on “Configurations” > “Ports” > “PVLANS” > “ACTIONS” > “Add”

Give the PVLAN config a name and then click “NEXT”.

PVLAN (CX10000)

Name **Switches** **Primary VLAN** **Secondary VLANs** **Secondary Ports** **Summary**

Enter a required Name and an optional Description.

Name Prefix * Synergy
Any non empty string, example: PVLAN-1

Description
Any non empty string, example: My PVLAN

(* = Required)

CANCEL

BACK

NEXT

Select the desired switches and then click “NEXT”.

PVLAN (CX10000)

✓

Name

✓

Switches

?

Primary VLAN

?

Secondary VLANs

?

Secondary Ports

?

Summary

Select required Switches for this PVLAN configuration to be applied to. The Primary and Secondary VLANs will be configured on these switches. Promiscuous and Secondary Ports can be chosen from these switches.

Switches *

x
10000-RU34-SW2 / 10000-RU33-SW1 (VSX)
x

SELECT ALL

(* = Required)

CANCEL

BACK

NEXT

Enter the Primary VLAN 200 and then click “NEXT”.

PVLAN (CX10000)

✓

Name

✓

Switches

✓

Primary VLAN

?

Secondary VLANs

?

Secondary Ports

?

Summary

Configure a required Primary VLAN and select optional Promiscuous Ports to be associated with the VLAN.

Primary VLAN *

200

A VLAN between 2 and 4094, example: 2.

Promiscuous Ports

SELECT PORTS

Switch	Port
There is no data to display	

(* = Required)

CANCEL

BACK

NEXT

Enter the Isolated VLAN 201 and then click “NEXT”.

PVLAN (CX10000)

✓

✓

✓

✓

?

?

Name
Switches
Primary VLAN
Secondary VLANs
Secondary Ports
Summary

Configure optional Isolated VLANs and Community VLANs.

Isolated VLANs

A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102.

Community VLANs

A number, set, or range of VLANs between 2 and 4094, example: 5, 10-45, 102.

(* = Required)

CANCEL
BACK
NEXT

Click “NEXT” on the “Secondary Ports” screen. Review and click “APPLY”.

PVLAN (CX10000)

✓

✓

✓

✓

✓

?

Name
Switches
Primary VLAN
Secondary VLANs
Secondary Ports
Summary

Configure optional Secondary VLAN and Port entries.

Secondary VLAN

Ports

CLEAR

ADD

UPDATE

Secondary VLAN	Ports
There is no data to display	

(* = Required)

CANCEL
BACK
NEXT

Configuration / Ports / PVLANS

Fabric

	Name	Switch	Primary VLAN	Promiscuous Ports	Isolated VLANs
	<input type="text" value="Enter Regex for Name..."/>	<input type="text" value="Enter Regex for Switch..."/>	<input type="text" value="Enter Regex for Primary VLA"/>	<input type="text" value="Enter Regex for Promiscuous"/>	<input type="text" value="Enter Regex for Isolated VLA"/>
<input type="radio"/>	Synergy-PVLANS-10000-RU-33-SW1-200	10000-RU-33-SW1	200		201
<input type="radio"/>	Synergy-PVLANS-10000-RU34-SW2-200	10000-RU34-SW2	200		201

PSM Integration

The Pensando integration allows you to:

- Configure security policies in Aruba Fabric Composer
- Or configure security policies in PSM
 - This may be required in scenarios where the security and network team are separate entities and the networking team is not allowed to manage the security policies

In the guided setup, select “DISTRIBUTED SERVICES” > “Pensando PSM”

onfiguration / Ports / PVLANS

Fabric

ACTIONS

Name	Switch	Primary VLAN	Promiscuous Ports
<input type="text" value="Enter Regex for Name"/>	<input type="text" value="Enter Regex for Switch"/>	<input type="text" value="Enter Regex for Primary VLA"/>	<input type="text" value="Enter Regex for Promiscuous"/>

NETWORK

DISTRIBUTED SERVICES

Distributed Services Setup
Perform the following steps to initialize and configure distributed services.

PENSANDO PSM *
Configure the Distributed Services Manager

Enter the required values

Pensando PSM
? ×

Host

Settings

Summary

Name *

Any non empty string, example: integration 1

Description

Example: My new Integration.

Host *

A valid Hostname at least two characters long or IPv4 Address, example: hostname.example.com, 198.162.5.4

Username *

Any non empty string, example: IntegrationUser

Click “VALIDATE” and if successful, click “NEXT”.

Password *

Any non empty string, example: tan.boot-13

☐ Validate SSL/TLS certificates for Aruba Fabric Composer

☒ Enable this configuration

VALIDATE

(* = required)

CANCEL BACK NEXT

Select the fabric, then both check box options, click “NEXT”, review and then click “APPLY”.

Pensando PSM

Host Settings Summary

Select a Fabric whose switches will be auto associated with this Pensando PSM.

Fabric CX10000

☒ Enable auto decommissioning for switches deleted from the system

☒ Enable auto VLAN placement on all switches when creating a Network

(* = required)

CANCEL BACK NEXT

The connected status should now be shown.

aruba Fabric Composer Dashboard Configurations Maintenance Visualizations Where can I find...? (e.g. VLAN)

Aruba NetEdit

HPE iLO Amplifier

ODIM™ Plugin Integration

HPE SimpliVity

Nutanix Prism

Pensando PSM

Configuration / Integrations / Pensando PSM

	Status	Host	Username	Enabled
	Select Status...	Enter Regex for Host...	Enter Regex for Username...	Select Enab
<input type="radio"/>	CONNECTED	10.10.10.150	admin	Yes

You can verify REST API connectivity between the Aruba CX 10000 switch and PSM is operational by clicking on “CLI Commands” next to “Guide Setup” icon.



Select your fabric or switches, type your desired “show” command, hit enter and click “RUN”.

The Aruba CX 10000 switches should be shown as “admitted” into PSM.

CLI Command Processor

Select Fabrics or Switches, enter Show Commands and press Run for results.

Fabrics

CX10000

Switches

Not applicable when a Fabric is selected.

Commands

show psm

Results

```

Switch : 10000-RU34-SW2 Command : show psm

Policy and Services Manager Information

Operational Status : admitted
Host Addresses      : 10.10.10.150
VRF                  : mgmt

Switch : 10000-RU33-SW1 Command : show psm

Policy and Services Manager Information

Operational Status : admitted
Host Addresses      : 10.10.10.150

```

Download Options
Download Results
Download JSON Data

(* = Required)

CANCEL


RUN

VMware vCenter Integration

The vSphere integration will allow you to view vSphere hosts in Aruba Fabric Composer, automatically deploy network configurations based on VM deployment on vSphere and visualize network connections between physical switches, Virtual Connect ports, vSwitches and VMs.

Click on “Configurations” > “Integrations” > “VMware vSphere” > “ACTIONS” > “Add”.

Enter the required values.

 VMware vSphere

?

?

?

?

HostAruba FabricvSphereSummary

Configure an integration between Aruba Fabric Composer and VMware vSphere

Name *
Any non empty string, example: integration 1

Description
Example: My new Integration.

Host *
A valid Hostname at least two characters long or IPv4 Address, example: hostname.example.com, 198.162.5.4

Username *

(* = required)

CANCELBACKNEXT

Click "Validate" and if successful, then click "NEXT".

Password *
Any non empty string, example: tan.boot-13

☐ Validate SSL/TLS certificates for Aruba Fabric Composer
☒ Enable this configuration

VALIDATE

(* = required)

CANCELBACKNEXT

Select all 3 options and then click “NEXT”.

VMware vSphere

✓

Host

✓

Aruba Fabric

?

vSphere

?

Summary

☒ Automated VLAN provisioning for ESX hosts directly connected to the fabric.

VLAN Range

1-4094

Enter the VLAN range Aruba Fabric Composer is allowed to modify 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 provisioning for ESX hosts connected through intermediate switches.

Intermediate VLAN Range

1-4094

Enter the VLAN range Aruba Fabric Composer is allowed to modify 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 provisioning for ESX hosts directly connected to the fabric.

PVLAN Range

1-4094

(*) = Required Scroll for more options

CANCEL

BACK

NEXT

Select “Discovery protocols” and then click “NEXT”.

VMware vSphere

✓

Host

✓

Aruba Fabric

✓

vSphere

?

Summary

Enable or disable discovery settings for this VMware vSphere configuration.

☒ Discovery protocols
☐ Use CDP when configuring distributed vSwitches

If automatic discovery (Discovery Protocols) is enabled, automatically enable CDP on vSwitches and Distributed vSwitches. Leaving this field unchecked enables LLDP.

(*) = Required

CANCEL

BACK

NEXT

Review the parameters and then click “APPLY”.

VMware vSphere

Host Aruba Fabric vSphere **Summary**

Host	10.10.100.100
Username	administrator@vsphere.local
Password	*****
Validate SSL/TLS server certificate when communicating with this system (self-signed and private CA-signed server certificates not supported)	No
Enabled	Yes
Name	vCenter
Description	
Discovery protocols	Yes
Use CDP when configuring distributed vSwitches	No
Automated VLAN provisioning for ESX hosts directly connected to the fabric.	Yes

CANCEL BACK APPLY

The connected status should be shown.

aruba | Fabric Composer | Dashboard | Configurations | Maintenance | Visualizations | Where can I find...? (e.g. VLAN)

Aruba NetEdit
HPE iLO Amplifier
ODIM™ Plugin Integration
HPE SimpliVity
Nutanix Prism
Pensando PSM
VMware NSX-T
VMware vSphere

Configuration / Integrations / VMware vSphere

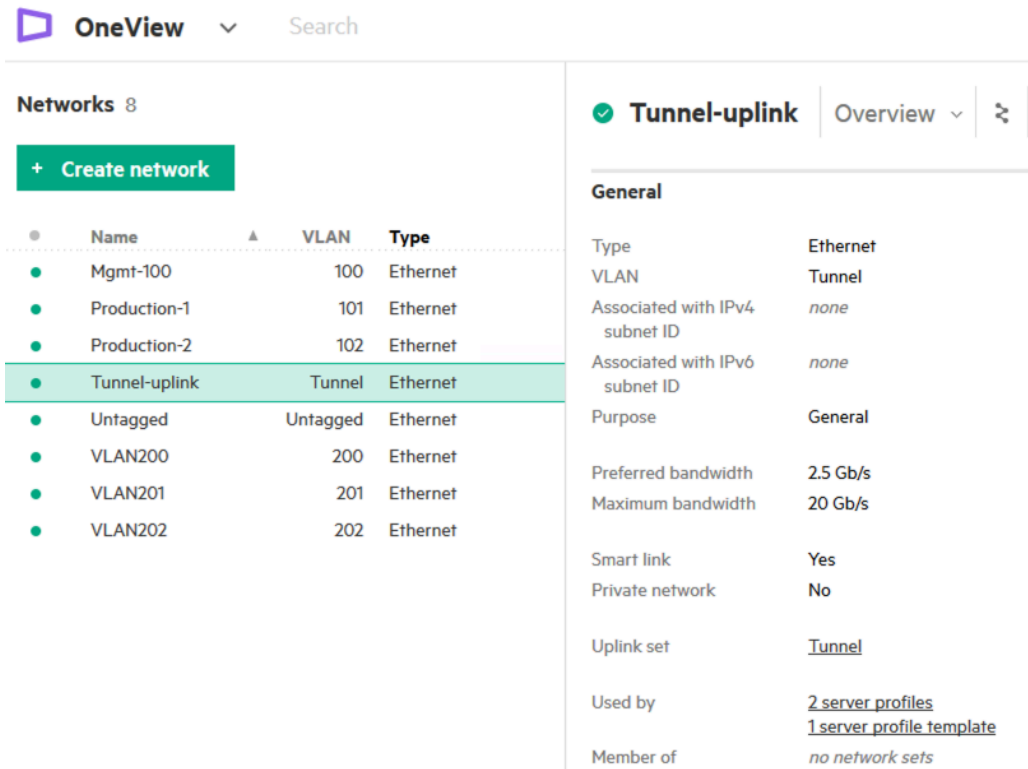
	Status	Host	Username	Enabled	Provisioning
<input type="radio"/>	CONNECTED	10.10.100.100	administrator@vsphere.local	Yes	VLAN (
					VLAN (
					PVLAN

Task 3: HPE Synergy Networking

This section provides guidance on networks, logical interconnects, and server profiles to connect to the Aruba CX 10000 switches.

Networks

From OneView, select “NETWORKING” > “Networks” and create a network with VLAN set to “Tunnel”.



The screenshot shows the HPE OneView interface. At the top, there is a search bar and a 'OneView' logo. Below the search bar, the 'Networks' section is active, showing a list of 8 networks. A green button labeled '+ Create network' is visible. The network list includes 'Mgmt-100', 'Production-1', 'Production-2', 'Tunnel-uplink' (highlighted), 'Untagged', 'VLAN200', 'VLAN201', and 'VLAN202'. The 'Tunnel-uplink' network is selected, and its configuration details are shown on the right. The configuration includes a 'General' tab with various settings.

Name	VLAN	Type
Mgmt-100	100	Ethernet
Production-1	101	Ethernet
Production-2	102	Ethernet
Tunnel-uplink	Tunnel	Ethernet
Untagged	Untagged	Ethernet
VLAN200	200	Ethernet
VLAN201	201	Ethernet
VLAN202	202	Ethernet

Tunnel-uplink	
Overview	
General	
Type	Ethernet
VLAN	Tunnel
Associated with IPv4 subnet ID	none
Associated with IPv6 subnet ID	none
Purpose	General
Preferred bandwidth	2.5 Gb/s
Maximum bandwidth	20 Gb/s
Smart link	Yes
Private network	No
Uplink set	Tunnel
Used by	2 server profiles 1 server profile template
Member of	no network sets

Logical Interconnects

Within “Networking” > “Logical Interconnect Groups”, click “Edit”, then select “Add uplink set”.

OneView Search

Logical Interconnect Groups 2

+ Create logical interconnect group

Name

Synergy_MLAG

Synergy_SAS

Edit Synergy_MLAG General

General

Name Synergy_MLAG

Redundancy Redundant

Logical Interconnect Group

Internal no networks	Productio... 3 networks 2 uplink ports	Synergy_... 3 networks 2 uplink ports
-------------------------	--	---

Add uplink set

Create an uplink set with the “Type” set to “Tunnel” and add the desired uplink ports.

Create Uplink Set ?

General

Name Tunnel

Consistency checking Exact match

Type Tunnel

Connection mode Automatic

LACP timer Short (1s)

LACP load balancing Source & Destination MAC Address

LACP failover trigger All active uplinks transition to offline

LACP distribute uplink ports ☒

Networks

Network Tunnel-uplink

Uplink Ports

Interconnect Module	Enclosure	Bay	Port	Capability	Speed	
Virtual Connect SE 40Gb F8 Module for Synergy	1	3	Q4	Ethernet + FCoE	Auto	×
Virtual Connect SE 40Gb F8 Module for Synergy	1	6	Q4	Ethernet + FCoE	Auto	×

Add uplink ports

Remove uplink ports

Remove all

Create

Create +

Cancel

From “Networking” > “Logical Interconnects”, you will notice an inconsistency error. Select “Actions” > “Update from group” to fix it.

The screenshot shows the HPE OneView interface. On the left, under "Logical Interconnects", there is a list with two items: "Steve_Synergy_LE-Synergy_MLAG" (highlighted in green) and "Steve_Synergy_LE-Synergy_SAS-1". The main panel displays details for "Steve_Synergy_LE-Synergy_MLAG". A yellow warning banner at the top states: "The logical interconnect is inconsistent with the logical interconnect group Synergy_MLAG. Active". Below this, the "Logical Interconnect" section shows a table with columns: Internal, Production..., Synergy_..., and Tunnel. The "Internal" column is currently selected. On the right, an "Actions" dropdown menu is open, showing options: Edit, Update from group (highlighted), Update firmware, Configure port monitoring, Refresh, and Reapply configuration.

If VSX LAG is configured on the Aruba CX 10000s from the previous section, you can validate the LACP LAG is operational between Virtual Connect and the CX 10000s under the “Uplinks Sets” section. The interconnects should be green with “Linked active” state, “LACP activity” and the attached switch neighbor info should also be seen.

OneView Search

Logical Interconnects 2

- Steve_Synergy_LE-Synergy_MLAG
- Steve_Synergy_LE-Synergy_SAS-1

Steve_Synergy_LE-Synergy_MLAG Uplink Sets

Update from group Completed 4m37s Daryl 12/14/21

Uplink Sets [Edit](#)

Synergy_MLAG_CX10000

▼ Tunnel

Connection mode Automatic
 LACP timer Short (1s)
 LACP load balancing Source & Destination MAC Address
 LACP fallover trigger All active uplinks transition to offline
 LACP distribute uplink ports Enabled
 Native network none

Networks (1)
[Tunnel-uplink](#) Tunnel

Uplinks

Uplink	State	Operational Speed	Requested Speed	Auto-negotiation	LAG	LAG State	Connected To
MXQ7300BTY, interconnect 3, Q4	Linked active	40 Gb/s	Auto	Enabled	21	LACP activity	04:90:81:00:33:4a 1/1/49
MXQ7300BTY, interconnect 6, Q4	Linked active	40 Gb/s	Auto	Enabled	21	LACP activity	04:90:81:00:36:56 1/1/49

Server Profiles

Edit your “Server Profile Template” and “Add Connection” with “Network” set to “Tunnel-uplink”.

OneView Search

Server Profile Templates 1

+ Create server profile template

BL480

Add Connection ?

General

Name Tunnel

Function type Ethernet

Network Tunnel-uplink

Port Auto

Link aggregation group None

Requested bandwidth (Gb/s) 2.5

Requested virtual functions ☒ None ☐ Custom ☐ Auto

Boot managed manually

Local

Add Add + Cancel

“Tunnel-uplink” connection should be created.

OneView Search

Server Profile Templates 1

+ Create server profile template

Name
BL480

Edit BL480 Connections

Connections

Requested virtual functions	None
Requested bandwidth	2.5 Gb/s
Link aggregation group	None
Isolated trunk	No

2	B-side	<u>Production</u> (network set)	Mezzanine 3:2-a	Not bootable	edit	x
Type	Ethernet					
MAC address	Auto					
Requested virtual functions	None					
Requested bandwidth	2.5 Gb/s					
Link aggregation group	None					
Isolated trunk	No					
3	CX10000	<u>CX10000</u> (network set)	Mezzanine 3:1-c	Not bootable	edit	x
Type	Ethernet					
MAC address	Auto					
Requested virtual functions	None					
Requested bandwidth	2.5 Gb/s					
Link aggregation group	None					
Isolated trunk	No					
4	Tunnel	<u>Tunnel-uplink</u> Tunnel	Mezzanine 3:2-c	Not bootable	edit	x
Type	Ethernet					
MAC address	Auto					
Requested virtual functions	None					
Requested bandwidth	2.5 Gb/s					
Link aggregation group	None					

From “Server Profiles”, you will see it is inconsistent with its “server profile template”, you can fix it by clicking on “Update from template”.

OneView Search

Server Profiles 2 All statuses All labels All resources

+ Create profile

Name
Bay 1-BL480 Gen9
Bay 2 - BL480 Gen9

Bay 2 - BL480 Gen9 Overview

▲ The server profile is inconsistent with its server profile template. Active 12/6/21 3:37:00 pm

The following automatic updates are required to restore consistency:

Create a connection to network Tunnel-uplink with id 4 on port Mezzanine (Mezz) 3:2-c.

The server profile needs to be powered off to be updated from the server profile template.

Resolution

The profile can be made consistent with its template by updating it from the template. The profile or template may also be edited to manually restore consistency. If consistency is not desired, this alert can be cleared.

[Update from template](#)

[Edit](#)

[Details](#)

You can update it by selecting “Update from template after power is off” and “Momentary press”.

If desired, VMs should be migrated to another hypervisor before powering the compute module off.

Power off Bay 1-BL480 Gen9

Bay 1-BL480 Gen9 is assigned to server hardware. Consider shutting down the applications and operating system gracefully.

☒ Update from template after power is off

Bay 1-BL480 Gen9 will be updated from BL480 after the server hardware is powered off.

Momentary press

Mimics a physical momentary press of the power button.

Press and hold

Forcefully power off server.

Close

Repeat this step for all server profiles that require the “Tunnel” uplink.

Once the server profile update is complete, you will be able to check the MAC address of the “Tunnel” uplink by clicking on “Edit” > “Connections”. This MAC will show up in vSphere as a physical NIC.

OneView

Search

Server Profiles 2

+ Create profile

Name
Bay 1-BL480 Gen9
Bay 2 - BL480 Gen9

Edit Bay 1-BL480 Gen9

Connections

Connections	Requested bandwidth	Link aggregation group	Isolated trunk
	2.5 Gb/s	None	No

2	<u>Production</u> (network set)	Mezzanine 3:1-a	Not bootable		
Type	Ethernet				
MAC address	3A:B6:6C:C0:00:17 (v)				
Requested virtual functions	None				
Requested bandwidth	2.5 Gb/s				
Link aggregation group	None				
Isolated trunk	No				
3	<u>CX10000</u> (network set)	Mezzanine 3:1-c	Not bootable		
Type	Ethernet				
MAC address	3A:B6:6C:C0:00:27 (v)				
Requested virtual functions	None				
Requested bandwidth	2.5 Gb/s				
Link aggregation group	None				
Isolated trunk	No				
4	<u>Tunnel-uplink</u> Tunnel	Mezzanine 3:2-c	Not bootable		
Type	Ethernet				
MAC address	3A:B6:6C:C0:00:28 (v)				
Requested virtual functions	None				
Requested bandwidth	2.5 Gb/s				
Link aggregation group	None				

Task 4: VMware vDS

After Aruba Fabric Composer is integrated with VMware vSphere, from Aruba Fabric Composer you will be able to:

- Create VMware vDS and assign VMNICs
- Create PVLANS in vDS

In Aruba Fabric Composer, click on “Visualizations” > “Hosts” > select your desired hypervisors in the bottom selection window and unselect undesired hypervisors.

You should see the new VMNIC with mac address matching the previous screenshot in OneView, that is the VMNIC that should be assigned into the vDS.

The screenshot displays the 'Hosts Visualization' section of the Aruba Fabric Composer. On the left, there are settings for 'Displaying' (2 of 8 Hosts, 13 of 72 Virtual Machines) and 'Settings' (Show Hosts, Show Selection Table, Hide Disconnected NICs). A 'Name Truncation' section allows specifying the truncation position (Start, Middle, End, None) and length (17 Characters). The main area shows a network diagram with hosts, vSwitches, and VMNICs. A table at the bottom lists selected VMNICs and their IP addresses. A tooltip for vmnic3 shows its details.

IP Address	VMNIC
10.10.100.2	vmnic0
	vmnic1
	vmnic2
	vmnic3

Physical Network Interface Details:

Name	vmnic3
Admin Status	up
MAC Addresses	3a:b6:6c:c0:00:28
Neighbor Status	Disconnected

To create the vDS, click on the desired hypervisor > “Create Microsegmentation”

The screenshot shows a dropdown menu with the following options: Actions, Create Microsegmentation, and Update Microsegmentation. The 'Create Microsegmentation' option is highlighted.

Input the desired names and select desired NICs. Multiple VMNICs on the same host can be selected if available. Only the

VMNIC MAC assigned to the “tunnel uplink” is required. Click “NEXT”.

Distributed Virtual Switch

✓

Settings

?

PVLAN

?

Summary

Enter a required name and NICs from the selected host, and configure an optional Portgroup Name Prefix.

Name *

Any non empty string, example: DVS-1

NICs *

✕ vmnic3

▼

Portgroup Name Prefix

Any non empty string, example: Portgroup-1

(* = Required)

CANCEL

BACK

NEXT

Enter the Primary PVLAN (200), Isolated PVLAN (201), and click “ADD”, click NEXT” and then “APPLY”.

Distributed Virtual Switch

✓

Settings

✓

PVLAN

?

Summary

Configure optional Primary and Isolated VLANs.

Primary VLAN

A VLAN between 2 and 4094, example: 2.

Isolated VLAN

A VLAN between 2 and 4094, example: 2.

CLEAR

ADD

Primary VLAN	Isolated VLAN	
200	201	<div>✕</div>

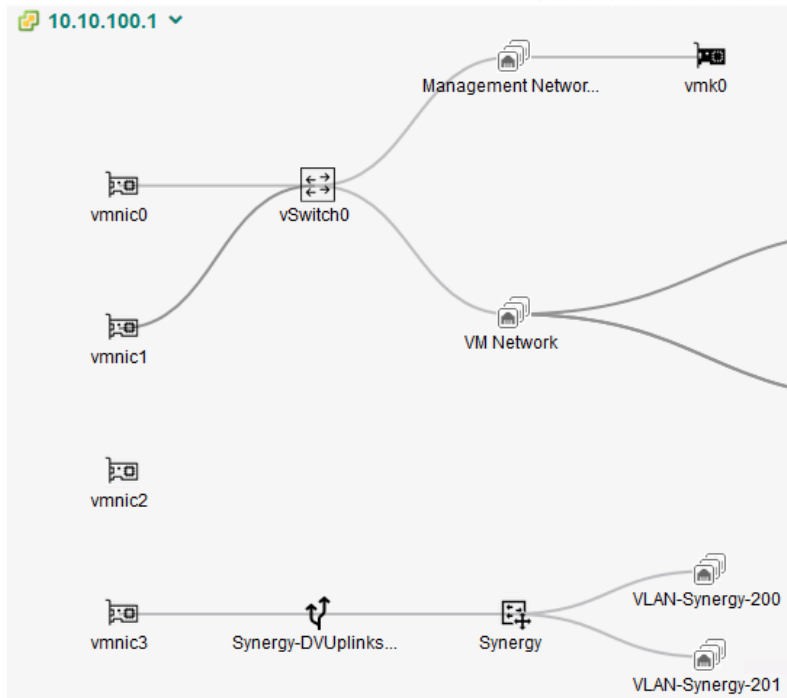
(* = Required)

CANCEL

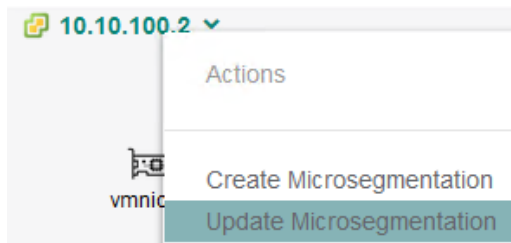
BACK

NEXT

Once done, you should be able to see the vDS, VMNIC and port group.



On other desired hypervisors, select “Update Microsegmentation” to add additional hypervisors and VMNICs to the vDS.



Update Microsegmentation

Select a required DVS and NICs from the selected host.

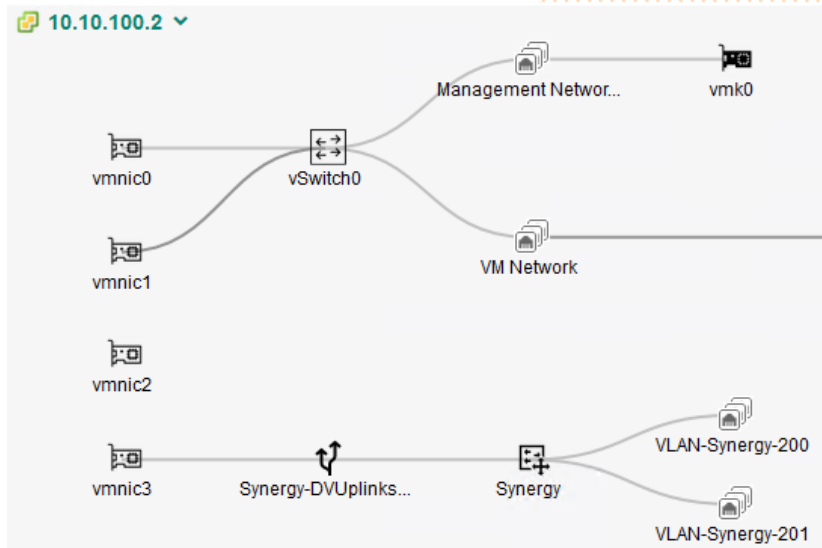
Distributed Virtual Switch *

NICs *

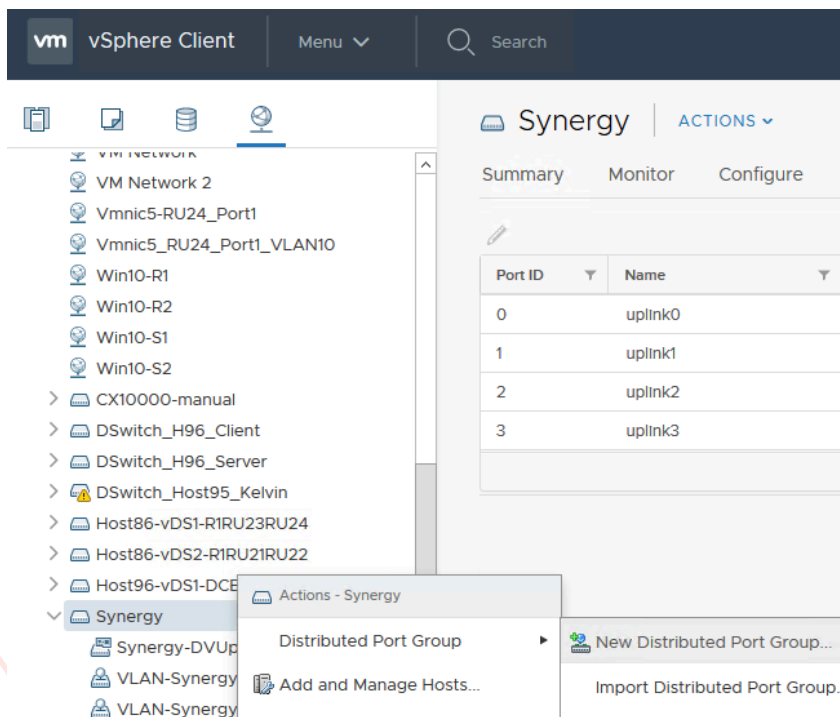
(* = Required)

CANCELAPPLY

Once done, you should be able to see the vDS, VMNIC and port group.



You will need to create non PVLAN port groups directly in vCenter by clicking on the “Networking” icon > right click desired vDS > “Distributed Port Group” > “New Distributed Port Group”.



Enter the desired values, click "NEXT" and then "FINISH".

New Distributed Port Group

- ✓ 1 Select name and location
- ✓ 2 Configure settings
- 3 Ready to complete**

Ready to complete

Review the changes before proceeding.

Distributed port group name	VLAN-Synergy-202
Port binding	Static binding
Number of ports	8
Port allocation	Elastic
Network resource pool	(default)
VLAN ID	202

[CANCEL](#)[BACK](#)[FINISH](#)

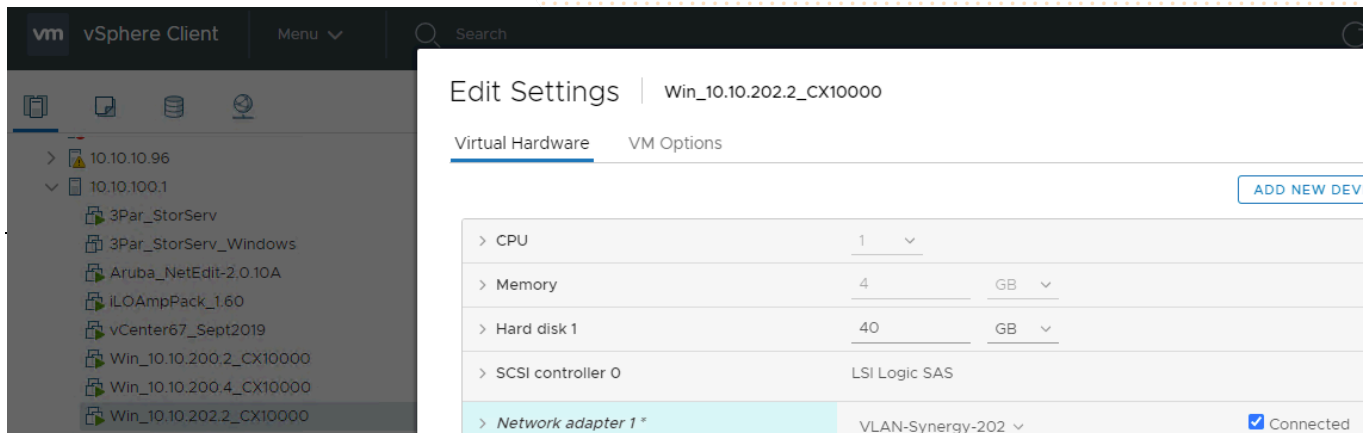
The next step is to update the VM network adapters to the desired port group in vCenter.

This example shows a VM with 10.10.200.2/24 IP assigned to an isolated PVLAN VLAN 201 port group.

The screenshot displays the vSphere Client interface. On the left, a list of VMs is shown, including 'Win_10.10.200.2_CX10000'. The main pane shows the 'Edit Settings' dialog for this VM. The 'Virtual Hardware' tab is selected, and the 'Network adapter 1' is configured with 'VLAN-Synergy-201' and is checked as 'Connected'.

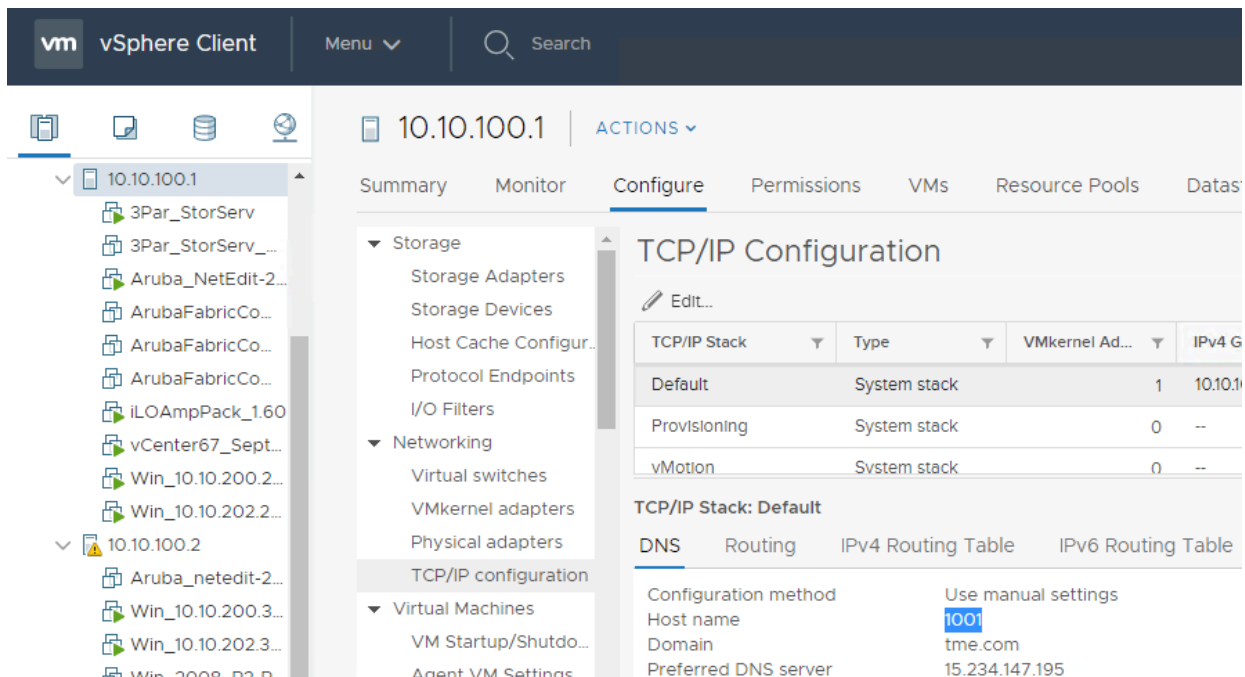
Setting	Value
CPU	1
Memory	4 GB
Hard disk 1	40 GB
SCSI controller 0	LSI Logic SAS
Network adapter 1 *	VLAN-Synergy-201

This example shows a VM with 10.10.202.2/24 IP assigned to the normal VLAN 202 port group.

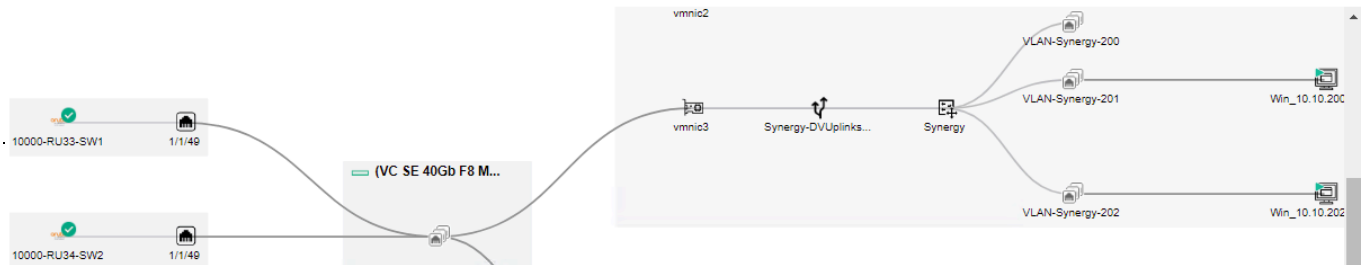


Repeat and assign other VMs to their desired port group.

For visualizations in Aruba Fabric Composer to display correctly, the ESXi hypervisors should have unique host names, DNS domain and DNS server configured under host > Networking > TCP/IP Configuration > Edit > Default.

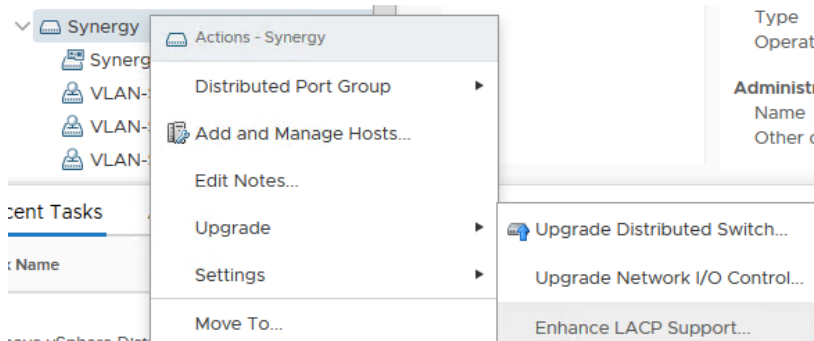


After the VMs are attached to port groups, the “Visualizations” pane should be updated with VMNIC/vDS/port group/VM links.



In addition, the VMNIC links to the VC module and the Aruba CX 10000 switchports should also be shown.

If LACP is required on the Aruba Fabric Composer created vDS pointed towards the switches, you can enable LACP support by selecting the vDS > “Upgrade” > “Enhance LACP Support” > “Next” > “Finish”



This is only applicable if the vDS is used on rack mount servers, if the vDS is only used within a Synergy enclosure, LACP is not required as LACP is enabled at the Virtual Connect level.

Task 5: Distributed Services

This section provides guidance on deploying distributed services on Aruba Fabric Composer, PSM and the Aruba CX 10000 switches.

Network Configuration

Next step is to add VLANs to be redirected/inspected by the Aruba CX 10000 DPUs.

Click on guided setup icon > “DISTRIBUTED SERVICES” > select the desired VRF > “CONFIGURE NETWORKS” > “ACTIONS” > “Add”.

The screenshot shows the Aruba Fabric Composer interface. The top navigation bar includes 'aruba', 'Fabric Composer', 'Dashboard', 'Configurations', 'Maintenance', 'Visualizations', and a search bar. The left sidebar shows 'VRF' with options for BGP, OSPF, and EVPN. The main content area is titled 'Configuration / Routing / VRF / Synergy'. It shows a table for adding networks. The table has columns for Name, Type, Switches, Route Distinguisher, and L3 VRF. A row is added with Name 'Synergy', Type 'User', Switches '10000-RU33-SW1, 10000-RU34-SW2', and Route Distinguisher '0'. The 'ACTIONS' menu is open, showing 'Add' and 'Delete' options. The right sidebar shows the 'DISTRIBUTED SERVICES' setup steps: 'PENSANDO PSM', 'CONFIGURE VRFs', 'CONFIGURE NETWORKS', and 'CONFIGURE POLICY'. The 'CONFIGURE NETWORKS' step is active, showing a dropdown for 'Selected VRF' with 'CX10000/Synergy' selected. Below the dropdown are buttons for 'CONFIGURE NETWORKS' and 'CONFIGURE POLICY'. A legend at the bottom right indicates that '*' means Required, a green dot means Completed, and a blue circle means Incomplete.

Add desired name and click “NEXT”.

The screenshot shows the 'Network' configuration dialog. At the top, there is a progress bar with three steps: 'Name' (completed, indicated by a checkmark), 'Settings' (in progress, indicated by a question mark), and 'Summary' (pending, indicated by a question mark). Below the progress bar, there is a text input field for 'Name' with a red asterisk indicating it is required. The field contains 'VLAN200'. Below the 'Name' field is a text input field for 'Description'. Below the 'Description' field, there is a legend: '(* = required)', 'CANCEL', 'BACK', and 'NEXT' buttons. The 'NEXT' button is highlighted in green.

Add desired VLAN, click “NEXT” and “APPLY”.

Network

Name

Settings

Summary

Set the required VLAN.

VLAN *

A VLAN between 1 and 4094, example: 1.

(* = required)

CANCEL

BACK

NEXT

Repeat for all desired VLANs with SVIs.

VLANs 200 and 202 are configured with SVIs used in this guide. VLAN 201 is an isolated PVLAN that utilizes SVI 200 and doesn't need to be created here.

Fabric Composer

Dashboard
 Configurations
 Maintenance
 Visualizations
 Where can I find...? (e.g. VLAN)

VRF

BGP
 OSPF
 EVPN

Configuration / Routing / VRF / Synergy

Fabric tme-dcn-pod1

ACTIONS

Name	Type	Switches	Route Distinguisher	L3 Vt
<input type="text" value="Enter Name..."/>	<input type="text" value="Select Type..."/>	<input type="text" value="Enter Switches..."/>	<input type="text" value="Enter Regex for Route Disting"/>	<input type="text" value="En"/>
Synergy	User	10000-RU33-SW1,10000-RU34-SW2		0

IP INTERFACES
IP STATIC ROUTES
NETWORKS
ARP TABLES
IP ROUTE TABLES

ACTIONS

	Name	VLAN
<input type="radio"/>	<input type="text" value="Enter Name..."/>	<input type="text" value="Enter Regex for VLAN..."/>
<input type="radio"/>	VLAN200	200
<input type="radio"/>	VLAN202	202

Distributed Firewall Configuration

Click on guided setup icon > “DISTRIBUTED SERVICES” > select desired VRF > “CONFIGURE POLICY” > “ACTIONS” > “Add”.

The screenshot shows the Aruba Fabric Composer interface. The top navigation bar includes the Aruba logo, 'Fabric Composer', and tabs for 'Dashboard', 'Configurations', 'Maintenance', and 'Visualizations'. A search bar is present with the placeholder text 'Where can I find...? (e.g. VLAN)'. The left sidebar lists 'Policy Groups', 'Policies', 'Rules', 'Endpoint Groups', 'Applications', and 'Service Qualifiers'. The main content area is titled 'Configuration / Policy / Policies' and displays a table with columns for 'Name', 'Policy Groups', and 'Health'. A context menu is open over the table, showing 'Add', 'Edit', and 'Delete' options. On the right, the 'DISTRIBUTED SERVICES' section is active, showing a 'Distributed Services Setup' wizard with steps: 'PENSANDO PSM', 'CONFIGURE VRFs', 'CONFIGURE NETWORKS', and 'CONFIGURE POLICY'. The 'CONFIGURE POLICY' step is currently selected.

Enter the desired policy name and then click “NEXT”.

The screenshot shows the 'Policy' configuration wizard. The wizard has five steps: 'Name', 'Settings', 'Rules', 'Enforcers', and 'Summary'. The 'Name' step is currently active, indicated by a checkmark icon. Below the steps, there is a text input field for 'Name' with the value 'Synergy' and a red asterisk indicating it is required. Below the 'Name' field is a text input field for 'Description'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A legend at the bottom left indicates that an asterisk (*) denotes a required field.

(* = Required)

Select “Distributed Firewall” and then click “NEXT”.

Policy

✓

✓

?

?

?

Name

Settings

Rules

Enforcers

Summary

Select a required type. The Policy type will determine the applicable Rules and Enforcers.

Type

(* = Required)

CANCEL BACK NEXT

Select “ACTIONS” > “Add” > “New”

Policy

✓

✓

✓

?

?

Name

Settings

Rules

Enforcers

Summary

Set one or more Rules on the Policy.

	Policies	Index	Name	
<input type="checkbox"/>	<input type="text" value="Enter Regex for Policies..."/>	<input type="text" value="Enter Regex for Index..."/>	<input type="text" value="Enter Regex for Name..."/>	<div> <div>New</div> <div>Existing</div> </div> <div> <div>< Add</div> <div>Remove</div> <div>Move</div> </div>

(* = Required) Scroll for more options

CANCEL BACK NEXT

This example permits RDP traffic from Web Tier to App Tier, e.g. VM (10.10.200.3/32) to VM (10.10.202.2/32). Click “NEXT”.

Rule

✓

?

?

?

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Enter a required Name and an optional Description.

Name ^{*}

Any non-empty string, example: Rule-1

Description

Example: Rule-1 Description

(^{*} = Required)

CANCEL

BACK

NEXT

Select the desired action and click “NEXT”.

Rule

✓

✓

?

?

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Select the required Action.

Action


(^{*} = Required)

CANCEL

BACK

NEXT

Select "ADD" to add new source endpoint group.

 Rule

✓

✓

✓

?

?

NameActionEndpoint GroupsApplications and Service QualifiersSummary

Select one or more Source and Destination Endpoint Groups.

Source Endpoint Group

Select...

ADD

Destination Endpoint Group

Select...

ADD


(* = Required)

CANCEL

BACK

NEXT

Enter the desired name and click next.

 Endpoint Group

✓

?

?

NameEndpointsSummary

Enter a required Name and an optional Description.

Name *

WebTier

Any non-empty string, example: EndpointGroup-1.

Description

Example: EndpointGroup-1 Description.

(* = Required)

CANCEL

BACK

NEXT

Select, “ADD” desired VM, click “NEXT” and then “APPLY”.

Endpoint Group

✓

✓

?

Name
Endpoints
Summary

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/VMMKernel	
10.10.200.3/32	Win_10.10.200.3_CX10000 (10.10.100.2) - Network adapter 1	

(*) = Required
Scroll for more options

CANCEL

BACK

NEXT

Click “ADD” on the destination endpoint group.

Rule

✓

✓

✓

?

?

Name
Action
Endpoint Groups
Applications and Service Qualifiers
Summary

Select one or more Source and Destination Endpoint Groups.

Source Endpoint Group

× WebTier

×

ADD

Destination Endpoint Group

Select...

▼

ADD

(*) = Required

CANCEL

BACK

NEXT

Name the endpoint group and then click “NEXT”.

Endpoint Group

✓

Name

?

Endpoints

?

Summary

Enter a required Name and an optional Description.

Name *

AppTier

Any non-empty string, example: EndpointGroup-1.

Description

Example: EndpointGroup-1 Description.

(* = Required)

CANCEL

BACK

NEXT

Select, add desired VM (this example shows you can add multiple endpoints), click “NEXT” and then “APPLY”.

Endpoint Group

✓

Name

✓

Endpoints

?

Summary

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/VMMKernel	
10.10.202.2/32	Win_10.10.202.2_CX10000 (10.10.100.1) - Network adapter 1	🗑
10.10.202.3/32	Win_10.10.202.3_CX10000 (10.10.100.2) - Network adapter 1	🗑

(* = Required)

Scroll for more options

CANCEL

BACK

NEXT

Click “NEXT” once both desired source and destination endpoint groups are added.

Rule

✓

✓

✓

?

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Select one or more Source and Destination Endpoint Groups.

Source Endpoint Group

× WebTier

×

ADD

Destination Endpoint Group

× AppTier

×

ADD

(* = Required)

CANCEL

BACK

NEXT

Select existing “Service Qualifier” if applicable, or click “ADD” to add a new service qualifier and then click “NEXT”.

Rule

✓

✓

✓

✓

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Select or add either Applications or Service Qualifiers.

Applications

↓

ADD

Service Qualifiers

× rdp

×

ADD

(* = Required)

CANCEL

BACK

NEXT

Review and click “APPLY”.

Rule

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Name

Description

Type

Action

Source Endpoint Groups

Destination Endpoint Groups

Service Qualifiers

RDP-permit

Layer 3

Allow

WebTier

AppTier

rdp

CANCEL

BACK

APPLY

Take note there is an implicit deny at the end of the policy. You can add more rules to permit traffic by clicking on “Actions” > “Add” > “New”.

Policy

✓

✓

✓

?

?

Name

Settings

Rules

Enforcers

Summary

Set one or more Rules on the Policy.

	Index	Name	Action	Source	Target
<input type="checkbox"/>	<input type="text" value="Enter Regex for Index..."/>	<input type="text" value="Enter Regex for Name..."/>	<input type="text" value="Select Action..."/>	<input type="text" value="Enter Source..."/>	<input type="text" value="Enter Target..."/>
↑ ↓ <input type="checkbox"/>	1	RDP-permit	Allow	WebTier	10

ACTIONS

New

Existing

< Add

Remove

Move

(* = Required)

Scroll for more options

CANCEL

BACK

NEXT

An “ICMP-permit” rule is used in this example to allow VMs to check network connectivity.

Rule

✓

?

?

?

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Enter a required Name and an optional Description.

Name *

Any non-empty string, example: Rule-1

Description

Example: Rule-1 Description

(* = Required)

CANCEL

BACK

NEXT

Select the desired action and then click “NEXT”.

Rule

✓

✓

?

?

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Select the required Action.

Action

(* = Required)

CANCEL

BACK

NEXT

Leave the endpoint groups empty to match on “any”, and then click “NEXT”.

Rule

×

✓

✓

✓

?

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Select or add one or more Source and Destination Endpoint Groups. No specified Endpoint Groups implies any IP Addresses.

Source Endpoint Groups

Select an Endpoint Group or leave empty for any...

ADD

Destination Endpoint Groups

Select an Endpoint Group or leave empty for any...

ADD

(* = Required)

CANCEL

BACK

NEXT

Select the desired service qualifier, click “NEXT”, review and then click “APPLY”.

Rule

×

✓

✓

✓

✓

?

Name

Action

Endpoint Groups

Applications and Service Qualifiers

Summary

Select or add either Applications or Service Qualifiers.

Applications

ADD

Service Qualifiers

× icmp ×

ADD

(* = Required)

CANCEL

BACK

NEXT

Review, add additional rules, e.g. allow Web to App desired traffic and then click “NEXT”.

Policy

Name

Settings

Rules

Enforcers

Summary

Set one or more Rules on the Policy.

ACTIONS

	Index	Name	Action	Source Endpoint Groups	Source Endpoint Gro...	Sou...
<div><div></div><div></div><div></div></div>	<div>Enter Regex for Index...</div>	<div>Enter Regex for Name...</div>	<div>Select Ac...▼</div>	<div>Enter Regex for Source I</div>	<div>Enter Regex for Sou</div>	<div>E</div>
<div><div></div><div></div><div></div></div>	1	RDP-permit	Allow	WebTier	10.10.200.3/32	
<div><div></div><div></div><div></div></div>	2	ICMP-permit	Allow	Any		

(* = Required) Scroll for more options

CANCEL

BACK

NEXT

Take note the policy is applied to the entire network fabric (all Aruba CX 10000 switches), you will not be able to select only specific CX 10000s.

Select

- Desired Fabric
- Desired direction
 - o Egress refers to policy applied from workload perspective, we are trying to permit outbound traffic egress from Web Tier to App Tier, e.g. VM (10.10.200.3/32) to VM (10.10.202.2/32)
- Desired VRF
- Desired Networks

Click on “ADD”.

Policy

✓

✓

✓

✗

?

Name

Settings

Rules

Enforcers

Summary

Fabric

CX10000

×

Direction

Egress

▼

VRF

Synergy

×

Networks

×

VLAN200 - VLAN: 200

×

VLAN202 - VLAN: 202

↑

↓

×

ADD

CLEAR

ADD

Network	Direction	
There is no data to display		

(*) = Required

Scroll for more options

CANCEL

BACK

NEXT

Click "NEXT" and then "APPLY".

Policy

✓

✓

✓

✓

?

Name

Settings

Rules

Enforcers

Summary

Direction

Select...

▼

VRF

Select...

▼

Networks

Select...

▼

ADD

CLEAR

ADD

Network	Direction	
VLAN200 - VLAN: 200	Egress	✕
VLAN202 - VLAN: 202	Egress	✕

(*) = Required

Scroll for more options

CANCEL

BACK

NEXT

The configured policy should be seen as healthy.

Configuration / Policy / Policies

Policy Groups	Health	Type	Enforcer Direction	Enforcer Type	Enforcer
<input type="text" value="Enter Regex for Policy Groups"/>	<input type="text" value="Select Health..."/>	<input type="text" value="Select Type..."/>	<input type="text" value="Select Enforcer Direction..."/>	<input type="text" value="Select Enforcer Type..."/>	<input type="text" value="Enter Enforcer..."/>
	HEALTHY	Distributed Firewall	Egress	Network	VLAN202 - VLAN: 202
			Egress	Network	VLAN200 - VLAN: 200

You can validate the security policy is pushed down to PSM and CX 10000 DPUs in PSM GUI > “Tenants” > “Security Policies” > policy name

Network Security Policies > Synergy

Security Policy

Security Policy Details

Policy Name: Synergy
 Tenant: default
 Created on: 2022-01-27 01:28:50 GMT+00:00
 Propagation: Propagation Complete. Updated on 2 DSSs.

Attach-tenant: true
 Last Modified: 2022-01-27

Policy Rules (2) Search:

<input type="checkbox"/>	Number	Rule Name	Source IPs	Destination IPs	Action	Protocol Port	Applica
<input type="checkbox"/>	1	Synergy..RDP-permit	10.10.200.3/32	10.10.202.2/32, 10.10.20	Permit	tcp/3389	
<input type="checkbox"/>	2	Synergy..ICMP-permit	any	any	Permit	icmp	

And the policy is attached to desired networks in PSM > “Tenants” > “Networks”

Networks

Networks Overview

Networks (2) 7 Columns Search

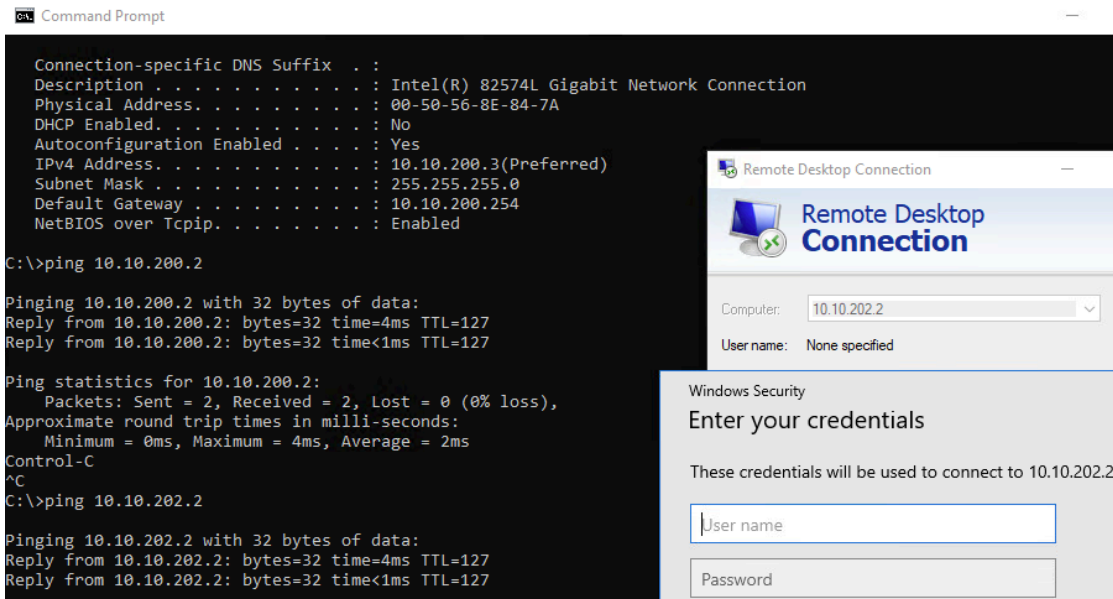
<input type="checkbox"/>	Name	VRF	VLAN	Ingress Policy	Egress Policy	Propagation Status
<input type="checkbox"/>	VLAN202	Synergy	202		Synergy	Propagation Complete. Updated .
<input type="checkbox"/>	VLAN200	Synergy	200		Synergy	Propagation Complete. Updated .

Task 6: Security Policy Validation & FW Logging

VMs on the same isolated PVLAN normally do not have network connectivity between each other.

However, with local proxy arp enabled on VLAN 200, traffic between VMs on the same isolated PVLAN can be subjected to a security policy for traffic to be allowed or denied.

With the security policy in place, we can verify 10.10.200.3 VM in WebTier is able to ping to VMs in the same subnet (10.10.200.0/24) and in the AppTier (10.10.202.0/24) subnet due to the “ICMP-permit” rule. It is also able to connect via RDP to the 10.10.202.2 VM due to the “RDP-permit” rule.



Due to the implicit deny rule, RDP between VMs on the same subnet are denied as expected.



You can view hitcounts towards each rule in Aruba Fabric Composer by clicking on “Configurations” > “Policy” > “Policies” > “...” > “Rules”

aruba | Fabric Composer | Dashboard | Configurations | Maintenance | Visualizations | Where can I find...? (e.g. VLAN)

Policy Groups

Policies

Rules

Endpoint Groups

Applications

Service Qualifiers

Configuration / Policy / Policies

	Name	Policy Groups	Health
<input type="checkbox"/>	<input type="text" value="Enter Regex for Name..."/>	<input type="text" value="Enter Regex for Policy Groups"/>	<input type="text" value="Select Health..."/>
...	<input type="checkbox"/> Synergy		HEALTHY

Rules

Expand each rule out to view hitcount.

aruba | Fabric Composer | Dashboard | Configurations | Maintenance | Visualizations | Where can I find...? (e.g. VLAN)

Policy Groups

Policies

Rules

Endpoint Groups

Applications

Service Qualifiers

Configuration / Policy / Policies / Synergy

Name	Policy Groups	Health	Type
<input type="text" value="Enter Regex for Name..."/>	<input type="text" value="Enter Regex for Policy Groups"/>	<input type="text" value="Select Health..."/>	<input type="text" value="Select Type..."/>
Synergy		HEALTHY	Distributed Firewall

RULES

Any active rule modifications may temporarily disrupt the policy enforcement operation.

	<input type="text" value="Enter Regex for Index..."/>	<input type="text" value="Enter Regex for Name..."/>	<input type="text" value="Enter Regex for Total Hits..."/>
...	<input type="checkbox"/> 1	RDP-permit	1

Time

January 26, 2022 @ 5:47:54 pm PST

Hits

1

ICMP-permit 2

Time	Hits
Enter Regex for Time...	Enter
January 26, 2022 @ 5:47:54 pm PST	2

You can view hitcounts towards each rule in PSM by clicking on “Tenants” > “Security Policies” > “Policy” > hover over a rule.

This example shows 2 hits to RDP-permit in DSM 1/2.

Network Security Policies > Synergy

Security Policy

Security Policy Details

Policy Name: Synergy
 Tenant: default
 Attach-tenant: true
 Created on: 2022-01-27 01:28:50 GMT+00:00
 Last Modified: 2022-01-27 01:28:54 GMT+00:00
 Propagation: Propagation Complete. Updated on 2 DSSs.

Policy Rules (2) Search: Rule Name Source IP Destination IP <Protocol>/<Port> App X Action X 9 Columns

Number	Rule Name	Source IPs	Destination IPs	Action	Protocol Port	Applications	Description	Total Connection Hits
1	Synergy..RDP-permit	10.10.200.3/32	10.10.202.2/32, 10.10.202.3/32	Permit	tcp/3389			10000-RU33-SW1 DSM 1/1: 0 10000-RU33-SW1 DSM 1/2: 2
2	Synergy..ICMP-permit	any	any	Permit	icmp			10000-RU33-SW1 DSM 1/1: 0 10

To enable Firewall logging, from within Aruba Fabric Composer, click on Configuration > System > Firewall Log

Then select “ACTIONS”, and then click “Add”. The Firewall Log Configuration wizard will open up.

Provide a name for the new Firewall Log Policy and then click “NEXT”.

Firewall Log Configuration

Enter a required Name

Name *

Log1

Any non empty string, example: firewall-log

(* = Required)

CANCEL BACK NEXT

You can now either choose to deploy this Firewall Log Policy to the whole fabric, or if desired, you can select specific switches to apply the Firewall Log Policy. Click “NEXT”.

Firewall Log Configuration

Select the Fabric or Switches in which to apply this configuration. A Fabric implies all Switches contained within it.

Fabrics

CX10000

Switches

Not applicable when a Fabric is selected.

(* = Required)

CANCEL BACK NEXT

Next you can now choose the Site Facility, the Severity (All, Allow, Deny), and the preferred Format. When desired parameters have been chosen click “NEXT”, and then “Apply”.

Firewall Log Configuration

Specify the Settings options.

Facility *

Severity *

Format *

☒ Enable PSM Target

(* = Required)

[CANCEL](#) [BACK](#) [NEXT](#)

Firewall Log Configuration

Name Application Settings Summary

Name Log1
Fabrics CX10000
Switches
Facility SYSLOG
Severity all
Format syslog-rfc5424
Enable PSM Target Yes

[CANCEL](#) [BACK](#) [APPLY](#)

If you log into the PSM GUI directly and click on Tenants > Firewall Export Policies, you will now see the new logging policy that was just created.

Dashboard

System

Tenants

Overview

VRF

Networks

Security Policies

Apps

Firewall Export Policies

Firewall Log Export Policies

Firewall Log Export Policies (4)

Name	Enabled PSM Targets	Exports	Facility Override	Format	Targets
Log1	true	All Logs	Syslog	RFC5424	
AFC	true	All Logs	User	BSD	
New	true	All Logs	User	BSD	
Synergy	true	All Logs	Syslog	RFC5424	

Appendix

CX10000-1 Configs and Verification Commands

You can use these commands to verify desired VLANs are redirected to DSM, LACP is functional and MACs, ARPs are learnt as expected, full configs are provided for reference.

```
10000-RU33-SW1# sh dsm 1/1 redirect
Distributed Services Modules 1/1
=====
```

Filter information

No VLAN redirect configured to Distributed Services module

```
10000-RU33-SW1# sh dsm 1/2 redirect
Distributed Services Modules 1/2
=====
```

Filter information

VLANs: **200-202**

```
10000-RU33-SW1# sh lacp int
```

State abbreviations :

A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state

Actor details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State
1/1/49	lag10(mc)	1049	1	ALFNCD	02:00:00:00:01:00	65534	10	up
1/1/48	lag256	49	1	ALFNCD	04:90:81:00:36:56	65534	256	up

Partner details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key
1/1/49	lag10(mc)	250	128	ASFNCD	f4:03:43:60:a4:d8	32768	21
1/1/48	lag256	49	1	ALFNCD	04:90:81:00:33:4a	65534	256

```
10000-RU33-SW1# sh mac-ad
```

MAC age-time : 300 seconds

Number of MAC addresses : 14

MAC Address	VLAN	Type	Port
00:50:56:8e:30:05	10	dynamic	1/1/17
00:50:56:a2:10:a8	20	dynamic	lag256
00:50:56:8e:d0:4f	20	dynamic	lag256
00:50:56:8e:1e:cb	20	dynamic	1/1/17
00:50:56:8e:92:30	20	dynamic	lag256

```

04:90:81:00:33:4a    200    dynamic    lag256
00:50:56:8e:7c:e7    200    dynamic pv  lag10
00:50:56:8e:84:7a    200    dynamic pv  lag10
04:90:81:00:33:4a    201    dynamic    lag256
00:50:56:8e:7c:e7    201    dynamic    lag10
00:50:56:8e:84:7a    201    dynamic    lag10
04:90:81:00:33:4a    202    dynamic    lag256
00:50:56:8e:b9:48    202    dynamic    lag10
00:50:56:8e:36:8f    202    dynamic    lag10

```

```
10000-RU-33-SW1# show arp vrf Synergy
```

IPv4 Address	MAC	Port	Physical Port	State	VRF
10.10.202.2	00:50:56:8e:b9:48	vlan202	lag10	reachable	Synergy
10.10.202.3	00:50:56:8e:36:8f	vlan202	lag10	reachable	Synergy
10.10.200.240	04:90:81:00:33:4a	vlan200	lag256	reachable	Synergy
10.10.202.240	04:90:81:00:33:4a	vlan202	lag256	reachable	Synergy
10.10.200.3	00:50:56:8e:84:7a	vlan200	lag10	reachable	Synergy
10.10.200.2	00:50:56:8e:7c:e7	vlan200	lag10	reachable	Synergy

```
Total Number Of ARP Entries Listed: 6.
```

```

10000-RU33-SW1# sh run
Current configuration:
!
!Version ArubaOS-CX DL.10.09.0010
!export-password: default
hostname 10000-RU-33-SW1
user admin group administrators password ciphertext
AQBapYYxwdkONC4Sev+y+b04Fd0cjpyMGqn1CM3LhbDcWe3qYgAAABX19SsYxNtZG+srlqp3cbElDSoow9j3gCfvJDfHB
hrvHMipUH9e1HgOlG9JdpqZksDdVrM0Pj01zikAKATkOWTdST+bvBjD2+4GQHgefUJw1PlZkh5S7kFEea+geJIwN63d
user afc_admin group administrators password ciphertext
AQBapTpF3DW4Dzf95Cn2ycp7tQxBzppatqV12DYzpB3py+hKYgAAA0uKA2gWHrCe3Kc1LIleiPzyeZR7eWEaZf0ZwImpP
SmINdJDz9kKcTcjZpZgK6/u0IAAn8qni4+iBgE/3xgMPXn0yEJXCQ07LFJ2R+UsVgxLsbWvf6LCETGvPrvLhfnYX3UJv
no ip icmp redirect
profile leaf
vrf Synergy
!
!
!
!
ssh server vrf mgmt
psm
  host 10.10.10.150 vrf mgmt
vlan 1,10,20
vlan 200
  private-vlan primary
vlan 201

```

```
private-vlan isolated primary-vlan 200
vlan 202
interface mgmt
    no shutdown
    ip static 10.10.10.213/24
    default-gateway 10.10.10.254
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/4
system interface-group 5 speed 10g
    !interface group 5 contains ports 1/1/17-1/1/20
system interface-group 10 speed 10g
    !interface group 10 contains ports 1/1/37-1/1/40
system interface-group 12 speed 10g
    !interface group 12 contains ports 1/1/45-1/1/48
interface lag 10 multi-chassis
    no shutdown
    description provisioned
    no routing
    vlan trunk native 1
    vlan trunk allowed 1,200-202
    lacp mode active
    lacp fallback
    lacp rate slow
interface lag 256
    no shutdown
    description ISL
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    lacp rate slow
    qos trust cos
interface 1/1/1
    no shutdown
    mtu 9198
    ip mtu 9198
interface 1/1/2
    no shutdown
    mtu 9198
    ip mtu 9198
interface 1/1/3
    no shutdown
    mtu 9198
    ip mtu 9198
interface 1/1/4
    no shutdown
    mtu 9198
    ip mtu 9198
interface 1/1/5
    no shutdown
    mtu 9198
    ip mtu 9198
interface 1/1/6
    no shutdown
    mtu 9198
    ip mtu 9198
interface 1/1/7
    no shutdown
    mtu 9198
    ip mtu 9198
```



```
interface 1/1/8
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/9
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/10
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/11
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/12
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/13
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/14
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/15
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/16
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/17
  no shutdown
  mtu 9198
  no routing
  vlan trunk native 1 tag
  vlan trunk allowed 10,20
interface 1/1/18
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/19
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/20
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/21
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/22
  no shutdown
```

```
mtu 9198
ip mtu 9198
interface 1/1/23
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/24
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/25
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/26
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/27
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/28
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/29
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/30
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/31
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/32
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/33
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/34
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/35
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/36
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/37
no shutdown
```

```
mtu 9198
ip mtu 9198
interface 1/1/38
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/39
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/40
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/41
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/42
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/43
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/44
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/45
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/46
no shutdown
persona access
mtu 9198
qos trust cos
ip mtu 9198
ip address 192.168.10.2/31
interface 1/1/47
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/48
no shutdown
persona access
mtu 9198
lag 256
interface 1/1/49
no shutdown
persona access
mtu 9198
lag 10
interface 1/1/50
no shutdown
persona uplink
mtu 9198
ip mtu 9198
```

```
interface 1/1/51
  no shutdown
  persona uplink
  mtu 9198
  ip mtu 9198
interface 1/1/52
  no shutdown
  persona uplink
  mtu 9198
  ip mtu 9198
interface 1/1/53
  no shutdown
  persona uplink
  mtu 9198
  ip mtu 9198
interface 1/1/54
  no shutdown
  persona uplink
  mtu 9198
  ip mtu 9198
interface vlan 200
  vrf attach Synergy
  ip mtu 9198
  ip address 10.10.200.241/24
  active-gateway ip mac 00:00:00:00:00:01
  active-gateway ip 10.10.200.254
  ip local-proxy-arp
interface vlan 202
  vrf attach Synergy
  ip mtu 9198
  ip address 10.10.202.241/24
  active-gateway ip mac 00:00:00:00:00:02
  active-gateway ip 10.10.202.254
  ip local-proxy-arp
vsx
  system-mac 02:00:00:00:01:00
  inter-switch-link lag 256
  role secondary
  keepalive peer 192.168.10.3 source 192.168.10.2
  no split-recovery
  vsx-sync vsx-global
!
!
!
!
https-server vrf mgmt
```

CX10000-2 Configs and Verification Commands

You can use these commands to verify desired VLANs are redirected to DSM, LACP is functional and MACs, ARPs are learnt as expected, full configs are provided for reference.

```
10000-RU34-SW2# sh dsm 1/1 redirect
Distributed Services Modules 1/1
=====
```

Filter information

No VLAN redirect configured to Distributed Services module

```
10000-RU34-SW2# sh dsm 1/2 redirect
Distributed Services Modules 1/2
=====
```

Filter information

VLANs: **200-202**

```
10000-RU34-SW2# sh lacp int
```

State abbreviations :

A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state

Actor details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State
1/1/49	lag10(mc)	49	1	ALFNCD	02:00:00:00:01:00	65534	10	up
1/1/48	lag256	49	1	ALFNCD	04:90:81:00:33:4a	65534	256	up

Partner details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key
1/1/49	lag10(mc)	112	128	ASFNCD	f4:03:43:60:a4:d8	32768	21
1/1/48	lag256	49	1	ALFNCD	04:90:81:00:36:56	65534	256

```
10000-RU34-SW2# sh mac-ad
```

MAC age-time : 300 seconds

Number of MAC addresses : 13

MAC Address	VLAN	Type	Port
00:50:56:a2:10:a8	20	dynamic	1/1/18
00:50:56:8e:d0:4f	20	dynamic	1/1/17
00:50:56:8e:1e:cb	20	dynamic	lag256
00:50:56:8e:92:30	20	dynamic	1/1/17
04:90:81:00:36:56	200	dynamic	lag256
00:50:56:8e:7c:e7	200	dynamic pv	lag10
00:50:56:8e:84:7a	200	dynamic pv	lag10
04:90:81:00:36:56	201	dynamic	lag256

00:50:56:8e:7c:e7	201	dynamic	lag10
00:50:56:8e:84:7a	201	dynamic	lag10
04:90:81:00:36:56	202	dynamic	lag256
00:50:56:8e:36:8f	202	dynamic	lag10
00:50:56:8e:b9:48	202	dynamic	lag10

```
10000-RU34-SW2# sh arp vrf Synergy
```

IPv4 Address	MAC	Port	Physical Port	State	VRF
10.10.202.3	00:50:56:8e:36:8f	vlan202	lag10	reachable	Synergy
10.10.200.251	04:90:81:00:36:56	vlan200	lag256	reachable	Synergy

```
Total Number Of ARP Entries Listed: 2.
```

```
10000-RU34-SW2# sh run
Current configuration:
!
!Version ArubaOS-CX DL.10.09.0010
!export-password: default
hostname 10000-RU34-SW2
user admin group administrators password ciphertext
AQBapfGrz5kq6he5ykpcx4YR1KlJh13fWgVDCSdybQvHf5UhYgAAAE5u3cuwvp8FBs8yTvJLEDGTBi5uGjrQo22ur/4G5
7yjX6K5yhmcK33PG/g+hLs1NqozFFRx+S52ozvyKegnCXjs3piV4D/D5EKd01P8YeEZbv920GcoXPLau6Ws8MiFKgk
user afc_admin group administrators password ciphertext
AQBapS0Y4qS+NoaDC7C/qqGXB832EdF1A3/pSbsyx9RV1IhYYgAAAKHMMJ1XZ0JTwal8hvnFzMn52WtloGsB0+wRQNEF+
1Fz04nnJuvGUy5zDtm/9dBLqg3ExgKxJIn4N1cHHHVWDy/7+upkCgY70LgGE7mEVFEC4wCqh596BZiN1HmTUq661vZo
no ip icmp redirect
profile leaf
vrf Synergy
!
!
!
!
!
ssh server vrf mgmt
psm
    host 10.10.10.150 vrf mgmt
vlan 1,10,20-21
vlan 200
    private-vlan primary
vlan 201
    private-vlan isolated primary-vlan 200
vlan 202
interface mgmt
    no shutdown
    ip static 10.10.10.212/24
    default-gateway 10.10.10.254
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/4
system interface-group 5 speed 10g
    !interface group 5 contains ports 1/1/17-1/1/20
system interface-group 10 speed 10g
    !interface group 10 contains ports 1/1/37-1/1/40
system interface-group 12 speed 10g
    !interface group 12 contains ports 1/1/45-1/1/48
```

```
interface lag 10 multi-chassis
  no shutdown
  description provisioned
  no routing
  vlan trunk native 1
  vlan trunk allowed 1,200-202
  lacp mode active
  lacp fallback
  lacp rate slow
interface lag 256
  no shutdown
  description ISL
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
  lacp rate slow
  qos trust cos
interface 1/1/1
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/2
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/3
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/4
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/5
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/6
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/7
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/8
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/9
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/10
  no shutdown
  mtu 9198
  ip mtu 9198
interface 1/1/11
  no shutdown
```

```
mtu 9198
ip mtu 9198
interface 1/1/12
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/13
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/14
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/15
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/16
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/17
no shutdown
mtu 9198
no routing
vlan trunk native 1 tag
vlan trunk allowed 10,20
interface 1/1/18
no shutdown
mtu 9198
no routing
vlan trunk native 1 tag
vlan trunk allowed 20-21
interface 1/1/19
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/20
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/21
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/22
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/23
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/24
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/25
no shutdown
```



```
mtu 9198
ip mtu 9198
interface 1/1/26
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/27
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/28
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/29
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/30
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/31
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/32
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/33
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/34
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/35
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/36
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/37
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/38
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/39
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/40
no shutdown
```

```
mtu 9198
ip mtu 9198
interface 1/1/41
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/42
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/43
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/44
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/45
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/46
no shutdown
mtu 9198
qos trust cos
description Keep alive Interface 10000-RU34-SW2
ip mtu 9198
ip address 192.168.10.3/31
interface 1/1/47
no shutdown
mtu 9198
ip mtu 9198
interface 1/1/48
no shutdown
mtu 9198
lag 256
interface 1/1/49
no shutdown
persona access
mtu 9198
lag 10
interface 1/1/50
no shutdown
persona uplink
mtu 9198
ip mtu 9198
interface 1/1/51
no shutdown
persona uplink
mtu 9198
ip mtu 9198
interface 1/1/52
no shutdown
persona uplink
mtu 9198
ip mtu 9198
interface 1/1/53
no shutdown
persona uplink
```

```
mtu 9198
ip mtu 9198
interface 1/1/54
no shutdown
persona uplink
mtu 9198
ip mtu 9198
interface vlan 200
vrf attach Synergy
ip mtu 9198
ip address 10.10.200.240/24
active-gateway ip mac 00:00:00:00:00:01
active-gateway ip 10.10.200.254
ip local-proxy-arp
interface vlan 202
vrf attach Synergy
ip mtu 9198
ip address 10.10.202.240/24
active-gateway ip mac 00:00:00:00:00:02
active-gateway ip 10.10.202.254
ip local-proxy-arp
vsx
system-mac 02:00:00:00:01:00
inter-switch-link lag 256
role primary
keepalive peer 192.168.10.2 source 192.168.10.3
no split-recovery
vsx-sync vsx-global
!
!
!
!
!
https-server vrf mgmt
```

