

# Versa Workflows and Templates

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify the functions of the main Versa Director tabs
- Navigate through the Versa Director environment to accomplish some basic tasks

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through a remote desktop connection. The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 5 other students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these hints to help you in the labs This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment. At the end of the lab guide you can find additional help on to how to complete the tasks, so if you have trouble with a task, please refer to the help section. If you still cannot accomplish the task, ask your instructor for assistance. In addition, you will see **hints** placed throughout the lab guide to help you along.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

# Lab Topology



Versa Director Login: labuserXYZ (e.g. labuser110, lab Versa Director Password: Versa@123

Branch OoB Login: **versa** Branch OoB Password: **versa123** 

Remember

use it a lot!

this! You will

Testing Host Login: labuserXYZ (e.g. labuser110, labuser111, etc.) Testing Host Password: versa123

©Copyright 2021 Versa Networks

# Interface Addresses

CPE	vni-0/0	vni-0/1	vni-0/2
Branch110	192.168.19.110/24	192.168.20.110/24	172.16.110.1/24
Branch111	192.168.19.111/24	192.168.20.111/24	172.16.111.1/24
Branch112	192.168.19.112/24	192.168.20.112/24	172.16.112.1/24
Branch113	192.168.19.113/24	192.168.20.113/24	172.16.113.1/24
Branch114	192.168.19.114/24	192.168.20.114/24	172.16.114.1/24
Branch115	192.168.19.115/24	192.168.20.115/24	172.16.115.1/24
MPLS Gateway	192.168.19.3		
INET Gateway		192.168.20.3	

# **Controller Addresses**

MPLS	MPLS Gateway	INET	INET Gateway
192.168.17.3/24	192.168.17.1	192.168.18.3/24	192.168.18.1



# Exercise 1: Connect to the remote lab environment

The first lab exercise is to become familiar with how to connect to the remote lab environment. Your instructor should have reviewed the following information with you prior to starting:

- Branch/Node/CPE Assignment
- Remote Lab Access

If you have not yet been assigned a branch device, please contact the instructor as this is a shared environment, and each student will configure and monitor a specific branch node.

Question: What node is assigned to you in the lab topology?

Follow the instructions provided by your instructor to connect to the remote lab environment.

Once you have started your remote desktop session, you will be presented with the remote desktop:

Recycle Bin		Î	Refresh remote desktop session	
MTPuTTY	Multi-Tabbed Putty			
README.bd	Access Instructions for lab components			
Remote Desktop	Remote Desktop to testing hosts			
	Google Chrome for Versa Director access			
	Multi-Tabbed Putty			
				Rg 🔁 👍 ENG

h



CPE	Username	Password
Branch110	labuser110	Versa@123
Branch111	labuser111	Versa@123
Branch112	labuser112	Versa@123
Branch113	labuser113	Versa@123
Branch114	labuser114	Versa@123
Branch115	labuser115	Versa@123



# Exercise 2: Examine the Workflow Environment

In the following lab exercises, you will:

- Identify the types of workflows available in Versa Director
- Examine the structure of a Controller workflow
- Examine the structure of an Organization workflow

Open the Workflows dashboard. On the left-side menu there are 3 main categories of workflows. Expand all 3 categories so that the sub-components are visible. Fill in the sub-components in the diagram below.

Infrastructure	$\sim$	
	lame	
Template	ontroller01	
Template	· · · · · · · · · · · · · · · · · · ·	
Devices	~	

Each of these categories of objects or components is related to a type of object within Versa Director:

- Infrastructure Workflows are used to help create controllers and organizations.
- Template Workflows are used to create different template-based components.
- Device Workflows are used to create branch device (CPE) components.

There are already a few workflows saved in Versa Director that were used to create components in the lab environment. These include:

- A Controller workflow
- A Template workflow for each of the preconfigured templates
- A Spoke Group workflow for each of the preconfigured spoke groups that are used in the hub-andspoke labs
- A Device workflow for each of the preconfigured devices in the lab environment.

Again, it is important to remember that these are saved processes, not the templates, controllers, or devices that the processes create. We will examine this concept as you complete the lab.



Deploy Controller - Controller01			×
General Location Information 0	Control Network WAN Interfaces		
Controller			
Name*	Provider Organization	Global Controller ID	
Controlerot	+ Create Organization	V 1	
Peer Controller	+ - Sub Organizations	🕂 📃 🔽 Staging Controller	Post Staging Controller
Docourco			
Nesource			
Baremetal     Create Virtual Machin	ne		
192.168.99.102			
Analytics Cluster	$\sim$		
+ Analytics Cluster			
			Cancel Continue

Note that the dialog title is "Deploy Controller – Controller01". This is because the end result of completing the workflow is the creation and deployment of a controller.

Question: What organization owns and manages this controller?

Question: What is the IP Address of the controller?

Question: To what analytics cluster will this controller forward log and statistics information?

Question: What are the 2 roles that this controller will perform in the SD-WAN?

This controller is managed by the SP organization. We'll see later in the lab that sub-organizations that fall under the SP organization can use this controller. When multiple sub-organizations use a parent controller, the controller acts as a multi-tenant controller and maintains separate control plane functionality for each tenant.

The IP address listed is the out-of-band management interface that is used for initial communication between the Versa Director and the Versa Controller. It is only used for the creation and onboarding process. Once the controller is provisioned, a separate interface associates with the Control Network is used for further communication between the head-end components.

This controller will be configured as a Staging controller and as a Post Staging controller. The Staging Controller function allows devices to be onboarded through this controller. The Post Staging Controller function allows this controller to act as a BGP route reflector, and SD-WAN CPEs will be able to establish BGP sessions with the controller for control plane information.

Continue to the Location Information tab. The Location Information tab can be used to indicate where the controller is physically located.

Deploy Controller - Controller01				×
General Location Information	Control Network WAN In	terfaces		
Control Network				
Network Name	Interface	VLAN ID	IP Address/Prefix	
Control	vni-0/0	V 0	172.16.0.3/24	
Gateway Routing Protocol ○ None ● BGP ● OSPF ● St	atic			
Back				Cancel

Continue to the Control Network tab.

The Control Network tab is where you define the North-Bound interface that is normally used to communicate with Versa Director and Versa Analytics. If the Versa Controller or Versa Analytics nodes are not on the same broadcast domain as the north-bound interface, routing can be configured on the north-bound interface to enable reachability.

Continue to the WAN Interfaces tab.

	VLAN	Network		IPv4				IPv	6		Public IP	
rface	ID	Name	Address	Gateway	DHCP	FQDN	Address	Gateway	DHCP	FQDN	Address	
-0/0		Select										÷
-0/1	0	MPLS	192.168.17.1/	192.168.17.3								+
i-0/2	0	INET	192.168.18.1/	192.168.18.3								+
	0/0 0/1 0/2	ID           0/0         0           0/1         0           0/2         0	ID         Name           0/0         0         +-Select+           0/1         0         MPLS           0/2         0         INET	ID         Name         Address           0/0         0        Select         0           0/1         0         MPLS         192.168.17.1/           0/2         0         INET         192.168.18.1/	ID         Name         Address         Gateway           0/0         0        Select         1         1           0/1         0         MPLS         192.168.17.17         192.168.17.3           0/2         0         INET         192.168.18.17         192.168.18.3	ID         Name         Address         Gateway         DHCP           0/0         0        Select <td>ID         Name         Address         Gateway         DHCP         FQDN           0/0         0        Select         0</td> <td>ID         Name         Address         Gateway         DHCP         FQDN         Address           0/0         0        Select         0</td> <td>IAD         Name         Address         Gateway         DHCP         FQDN         Address         Gateway           0/0         0        Select         0         0         0         Gateway         0         0         0         Gateway         0<!--</td--><td>ID         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP           0/0         0        Select         0         <td< td=""><td>IAD         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN           0/0         0        Select         0</td><td>ID         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN         Address           0/0         0        Select         Image: Comparison of the select         <t< td=""></t<></td></td<></td></td>	ID         Name         Address         Gateway         DHCP         FQDN           0/0         0        Select         0	ID         Name         Address         Gateway         DHCP         FQDN         Address           0/0         0        Select         0	IAD         Name         Address         Gateway         DHCP         FQDN         Address         Gateway           0/0         0        Select         0         0         0         Gateway         0         0         0         Gateway         0 </td <td>ID         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP           0/0         0        Select         0         <td< td=""><td>IAD         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN           0/0         0        Select         0</td><td>ID         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN         Address           0/0         0        Select         Image: Comparison of the select         <t< td=""></t<></td></td<></td>	ID         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP           0/0         0        Select         0 <td< td=""><td>IAD         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN           0/0         0        Select         0</td><td>ID         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN         Address           0/0         0        Select         Image: Comparison of the select         <t< td=""></t<></td></td<>	IAD         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN           0/0         0        Select         0	ID         Name         Address         Gateway         DHCP         FQDN         Address         Gateway         DHCP         FQDN         Address           0/0         0        Select         Image: Comparison of the select <t< td=""></t<>

The WAN interfaces are the south-bound interfaces that connect to the SD-WAN environment. It is over these interfaces that CPEs will communicate with the controller.



Click Cancel to exit the workflow dialog.

In the Infrastructure menu, select *Organizations*. The primary organization (SP in this example) is created during the initial Versa Director configuration process. Subsequent organizations (sub-organizations) are created using the Organizations workflow.

Open the Tenant1 organization workflow.

VERSA							10	1	labus
a chi	Monitor	Configuration	Workflows	Administration	Analytics			Commit	Templa
astructure 🗸 🗸	-								
Controllers	Create Orga	nization							
Organizations	Organizatio	0							
olate 🗸 🗸	Nemek			Tabal Organization ID t		Descent			
Templates	Topport1			o organization iD*		cn			
Application Steering	Tenanci			6					
Spoke Groups		tication							
Service Chains	IKE Authent	ucation							
ies 🗸 🗸	I PSK () I	PKI	S	taging CA Agent		Post Staging CA Agent			
Devices									
	SCP				CPE Deployment Typ	ie .			
	Shared C	ontrol Plane			SDWAN	<u>×</u>			
	Controllers	CMS Connectors	Analytics Cluster	Routing Instances	Supported User Role	es			
	Available			Add All	Selected			Remo	ove All
	Search				Search				
					Controller01				×

Controllers and Organizations are usually only created at the initial SD-WAN deployment phase The Organization workflow allows you to define a sub-organization and its associated parameters. Note that the controller Controller1 is listed in the Controllers tab. This configuration allows the Tenant1 sub-organization to use the Controller1. If another sub-organization under the SP domain is created, it could also be allowed to use the Controller1 controller. Other tenant-specific configuration parameters can be configured as well, including tenant-specific Analytics connectors, the default routing instances that will be created for devices within the sub-organization, and the supported user roles available to users within the sub-organization, which allows the parent organization to manage and control what type of access users within the sub-organization are allowed to be assigned.



### IMPORTANT! Do not change any of the organization parameters!

Take a few minutes to explore the configuration parameters included in the organization workflow, then click Cancel to exit out of the workflow.

# Exercise 3: Examine Template Workflows

It's common for the Controllers and Organizations workflows to be used only once or twice in an entire deployment, as those components are normally defined and deployed in the initial stages of the SD-WAN deployment. The workflows that are used frequently are the Template and Devices workflows.

In the following exercises you will:

• Examine the structure of a Device Template workflow

In the Template workflow menu, select Templates. This opens the Device Template workflow table. Device Template workflows are used to build the base configuration template that a group of devices will inherit when a device is created in a later step. There are multiple workflows saved that were created during the initial lab setup. Device Templates that are created using the Device Template workflow are placed in the *Configuration > Templates > Device Templates* table in Versa Director, and are stored in the local Versa Director database.

Click on the Base-Template-NGFW workflow to open the workflow.

The template that is created by a workflow inherits the name of the workflow. Continue to the next page in the lab guide to answer some questions and fill in some details related to this example workflow.

Edit Template - Base-Template-NGFW					×
Basic Interfaces Routing Tunnels I	nbound NAT Services Management Servers				
Name*	Туре*			Organization*	
Base-Template-NGFW	SDWAN Post Staging			Tenant1	~
Device Type		Redundant Pa	air 😨		
SDWAN	1	Enable	VRRP	Template Name	
O Full Mesh ● Hub ● Hub Controller	Spoke		Cloud CPE		
Sub Organizations	€ Controllers*		<b>+</b> -	Analytics Cluster	~
	Controller01			+ Analytics Cluster	
				Preferred Software	Version
				Select	~
Subscription 📀					
Solution Tier		Custom Par	ameters		E Drimont
Senice Bandwidth	Solution Addon Tier	+ − Name ⇒	value		Primary
25 Mbps	<b>~</b>				Z Analytics Enabled
Aggregate Bandwidth	_		No Records to Dis	splay	
25 Mops					
					Cancel Continue Recreate



What organization will have access to this workflow and the template that this workflow creates?

To what controller(s) will devices that use this template connect?

This is the inherited subscription profile, which can be overridden by a more specific subscription profile on a device if desired. What subscription information will be inherited by devices that use the template created by this workflow?

Open the Interfaces tab of the workflow.

The Interfaces tab allows you to define the common interface layout of the devices that will share the template configuration created by the workflow. Note that the device *Port Configuration* diagram is a logical diagram and does not represent the actual physical device – it is only used for port mapping purposes and basic port parameters.

Edit Temp	Edit Template - Base-Template-NGFW X													
Basic	Interfaces	Routing	Tunnels	Inbound NAT	Services Man	iagement Servei	15							
Device Po Numb Ports 6	Device Port Configuration       Number of     0     1     2     3     4     5       Ports     0     1     2     3     4     5       6     V     Mgmt WAN WAN LAN     LTE     WIFI													
WAN Inter	rfaces 🔋				_		_	1D-14		<b>P</b> -6				
Port #	Interface	VLAN ID	)	Network Name		Priority	Static	DHCP	Static	DHCP	Allow SSH To CPE	Nexthop	Remote IP	Sub Interfaces
0	vni-0/0	•		MPLS	~	\$		0		0	0		•	Ð
1	vni-0/1	•		INET	~	\$							۰	Đ
LAN Inter	faces 🔋		-											-
Port #	Interface	VLAN ID	Networ	k Name	Organization		Zones		Routing	Instance	St	IPv4	IPv6	Sub Interfaces
2	vni-0/2	\$	Tenant	1-LAN	Tenant1	~]	Tenant1-LA	N-Zone $\sim$	Tenant	1-LAN-VR	~			Đ
Back												G	ancel	Recreate

The LAN interfaces are the customer site facing interfaces at the local site. The *Network Name* is a userdefined name, the *Organization* determines which sub-organization owns the port, the *Zones* allows the user to define a specific security zone associated with the interface, and the Routing Instance is autopopulated based on the routing instance name configured for the organization. The method that devices will acquire address is specified in the template. However, the actual addressing is configured during the device creation process, as addressing is device specific.

To assign a port to a role, click on the port and select the role from the popup window. You can also change the assignment of a port by clicking on a port that already has an assignment.

Open the Routing tab of the workflow.

The Routing template allows you to define base routing protocol parameters if desired. When routing protocol information is configured in the workflow, the workflow process automatically creates the route redistribution policies required to advertise the local routing information – and routes learned through the workflow-created routing processes – to remote sites in the SD-WAN.

Edit Temp	olate - Base-Ter	mplate-NGFW						×				
Basic	Interfaces	Routing Tunnels	Inbound NAT Services Man	agement Servers								
BGP												
Network	k <b>* ≑</b>	iBGP	Local AS*	Neighb	or IP*	Peer AS*	BFD					
Select	t		\$	\$		•		<b>E</b>				
				No Records to	Display							
OSPF /	OSPFv3				Static Routes							
Network	k Name* 🗢	Area*	BFD		Routing Instance* 🕈	Prefix*	Nexthop*					
Select	t	~)≎[		<b>E</b>	Select	~)\$	\$					
					No Reserve to Display							
		No Rec	ords to Display									
Back							Cancel	itinue Recreate				

Open the Tunnels tab of the workflow.

The Tunnels tab allows you to specify direct internet access or SD-WAN gateway functions on devices that use the template created by the workflow. You can also configure site-to-site tunnels for non-SD-WAN tunnels between devices.

Edit Template - Base-Templat	te-NGFW						×
Basic Interfaces Ro	uting Tunnels Inbound NAT Service	es Management Servers					
Split Tunnels 🤋							
VRF Names 🗢		WAN Interfaces		DIA	Gateway		
Select	~	-Select	N				+
Tenant1-LAN-VR		INET					1
					Load Balance		
Site to Site Tunnels							
Name 🗢	Peer Type	WAN/LAN Network	LAN VRF	Vpn Profile		BGP Enabled	
	Select V	Select V	Select V	Select		0	<b>(</b>
		No Records to	Display				
Back					Cancel	Continue	Recreate

Question: According to the preconfigured tunneling configuration, which local VRF will be able to use the INET transport to reach non-SD-WAN destinations (split tunneling and DIA)?

Open the Inbound NAT tab.

The Inbound NAT tab allows you to create static destination-NAT to allow outside resources to reach internal NATed devices.

Edit Templa	late - Base-Temp	late-NGFW										×
Basic	Interfaces	Routing Tunnels	Inbou	nd NAT Services	Mar	nagement Servers						
inbound	d NAT 🔋											
Name* 🕈	\$	WAN Network*		LAN Routing Instance*	6	Protocol		External Addresses*	External Ports	Internal Addresses*	Internal Ports	
		Select	$\sim$	Select	Y	Select	$\sim$	P Address/Range	\$	P Address/Range	\$	
	No Records to Display											
Back										Cance	l Continue	Recreate



### Open the Services tab.

Enabling the services in the template workflow allows you to configure the services in the resulting template. The Services tab allows you to define what services will be active on the device. The services themselves are not created in the Workflow. The services are activated in the workflow, which instructs the workflow to create the configuration hierarchy necessary to add the services later by defining the services within the template that will be created. If you do not enable the services in the workflow, the corresponding configuration hierarchy will not be created in the template.

Edit Template - Base-Te	emplate-NGFW						×
Basic Interfaces	Routing Tunnels In	bound NAT Services M	anagement Servers				
DHCP Server				DHCP Relay			
LAN Interfaces 🗢	DHCF	Options Profile		LAN Interfaces 🗢	IP Address*		
Select	~)		~ 🔳	Select	~)¢[		<b>H</b>
Service Templates 😌	No Record	s to Display	DHCP Options Profile		No Records to Display		
Organization	Security						*
Tenant1	🔿 None	NGFW	⊖ SFV	V			*
4							F.
<u> </u>			 				
Back					Ca	ancel Continue	Recreate

Open the Management Servers tab.

The Management Servers tab allows you to define parameters such as NTP servers, Syslog Servers, and other management server connectivity that will be common among all devices that use the resulting template.

Edit Template - Base-Template-NGFW X											
Basic Interfaces Routing Tunnels Inbound NAT Services Management Servers											
NTP Servers (0) Syslog Servers (0) TACACS+ Servers (0) RADIUS Servers (0) SNMP Managers (0) LDAP Servers (0)											
NTP Servers											
	4 <b>1</b> K										
Reachability via *											
Select	E1										
NO RECORDS ADDED											
Back Clean & Recreate	Cancel Recreate										

## Important! Do not change this workflow!

This workflow is used to reset the Base-Template device template throughout the lab! You will have the opportunity to create your own template workflow next!

Click *Cancel* to close the workflow dialog, then select *Yes* from the popup.



# **Exercise 4: Examine Device Workflows**

After completing this lab exercise, you will be able to:

• Identify the components of a Device workflow

Next you will explore the Devices device template. The Device workflow is used to create the individual devices in the network. Devices created by the Device workflows are added to the *Administration* > *Inventory* > *Hardware* table in Versa Director.

Select *Devices* from the Devices workflow section. You will see several device workflows in the table. These device workflows were used to create the devices in the pre-configured lab environment. In this part of the lab you will examine the properties of one of the pre-configured device workflows.

Select the *Hub105* device workflow in the table. This will open the workflow that was used to create the Hub105 device.

Add Device - Hub105				×
Basic Location Information [	Device Service Template	Bind Data		
Name* Hub105	Global Device	⊧ ID*	Organization* Tenant1	
Deployment Type CPE-Baremetal Device	Serial Numbe	r	Device Groups* DG-Hub105	$\sim$
Admin Contact Information		Subscription	+Device Group	
Email Phone Numb	ber 1) 555-5555	Service Bandwidth Select options	Aggregate Bandwidth	
		C	ancel Save Continue	Redeploy

### IMPORTANT: Do NOT change the parameters in the Hub-105 device workflow!

The Basic tab of the device workflows is used for the base parameters. The device that is created in the *Hardware Inventory* will inherit the name of the device workflow.

In most situations, the *Global Device ID* chosen by Versa Director is used to avoid overlapping device IDs within other organizations, as the Global Device ID must be unique on Versa Director. The Serial Number is the software or hardware serial number of the device. The Subscription properties can be left at the default values, in which case the subscription values in the template to which the device is linked will be used. If you wish to assign different subscription values to the individual device, you may do so here.

The *Device Groups* parameter is used to link the device to a template. If a device group needed to link the device to a template does not exist, the *+Device Group* shortcut will open the Device Group creation dialog, where you can create the desired device group without leaving the Device workflow.



16

#### Open the Location Information tab.

Add Devi	Add Device - Hub105									
Basic	Location Information	Device Service Template	Bind Data							
Locatio	n									
Address	5 1			Address 2						
City		State		Country*	Zip					
San Jos	ie .	CA		USA						
Latitude	e	Longitude								
37.338	208	-121.886329		Get Coordinates						
Back				Cancel	Save C	ontinue Redeploy				

You must enter a Country value. Other values are optional, but the more specific you are, the better. The Location Information tab allows you to enter device location information. The final location is based on Latitude and Longitude values that are calculated from the address information. The more detailed the address information, the more accurate the latitude and longitude values will be. This information is used to display the device on maps in the Monitor and Analytics dashboards.

#### Open the Device Service Template tab of the Device workflow.

Add Devic	dd Device - Hub105 X											
Basic	Location Information	Device Service Template	Bind Data									
			▶         ▼   < 1 >   25									
Tenant		Category	Template									
		NO DE	EVICE SERVICE TEMPLATE ADDED									
Back			Cancel Save Continue Redeploy									

The Device Service Template tab allows you to assign service templates to the device directly. In many instances, the service templates are assigned through the device group. Allowing the administrator to assign a service template directly to a device allows more flexibility for service assignment.



Open the Bind Data tab of the Device workflow.

Add Device - Hub105 X											
Basic Location Information Device Service Template Bind Data											
User Input Auto-Generated											
Post Staging Template - T-Hub105											
		Interfaces with Mask									
Device Name	Serial Number	INET_IPv4staticaddress	LAN_IPv4staticaddress	MPLS_IPv4staticaddress	INE						
Hub105	SR105	192.168.20.105/24	172.16.105.1/24	192.168.19.105/24	19						
Service Template Variable	e	{\$v_INET_IPv4_staticaddress}		Device Group · DG-H	ub105						
Service Templates :	Tenant1-DataStore										
User Input Auto-Genera	ated			Clone Cl	ear						
Device Name		Serial N	umber								
Hub105		SR105									
		I									
Validate Template											
Back			Car	ncel Save Rede	ploy						

The Bind Data tab is where you enter device-specific information. When the Bind Data tab is opened, the template associated with the Device Group (in the Basic tab) is scanned for any variables or values that the user needs to enter. If the Bind Data tab is empty when you open it, this is usually because the Device Group configured in the Basic tab is not properly configured, and does not have a corresponding device template configured. When there is a problem with the device group template assignment, the Bind Data tab tries to look for template information, but can't find a related template.

There are 2 ways to enter user-defined information in the Bind Data fields. The first is to enter them directly in the fields listed in the Device Name field. The scroll bar at the bottom of the Post Staging Template window allows you to scroll for additional values.

Another common method of entering the bind data is to click on the device name in the table. This will open a new dialog window that displays all of the required fields.

<sup>L</sup> Click the Hub105 device name in the table to examine the pre-configured bind data for the device.

## IMPORTANT: Do NOT change the bind data information for the Hub105 device!

Click *Cancel* to close the bind data dialog when you are finished examining the data, then click *Cancel* again to close the Device Workflow dialog.



# Exercise 5: Practice

In the next lab exercises you will perform the following tasks:

- Create a Template workflow that is named after your user-id and branch-id (e.g. Template-labuser110-branch110, Template-labuser111-branch111, etc.)
- Create a new device group that links to your newly created template
- Re-assign your existing device to the new device group
- Commit the template in order to re-configure the existing device in the network (using the new template configuration)

Because this course does not cover deployment of devices, you will not deploy the new device that you create. However, you will examine the objects created in Versa Director, and you will re-assign your existing device to the new device group that references the template that you create. You will then commit the template so that you are familiar with the process of creating a template using Workflows and applying the template to a device.

#### 5.1

#### **Create a new Device Template**

In this exercise you will create a new Device Template using a Template workflow. Use a template workflow to create the template with the following parameters:

Workflow Name:	Template-[user-id]-[branch-id]-SFW
Туре:	SDWAN Post Staging
Organization:	Tenant1
Device Type:	SDWAN Full Mesh
Controllers:	Controller01
Analytics Cluster:	van1
Solution Tier:	Premier-Elite-SDWAN
Bandwidth:	25 Mbps

### Basic Tab:

Example: Template-labuser110-branch110



#### Example Output

### **Interfaces Tab**

Assign the following interface parameters in the Interfaces tab:

Port 1 (WAN Interface 0, vni-0/0)	Port Type: WAN Network Name: MPLS IPv4 Address: Static
Port 2 (WAN Interface 1, vni-0/1)	Port Type: WAN Network Name: INET IPv4 Address: Static
Port 3 (LAN Interface 2, vni-0/2)	Network Name: Tenant1-LAN Organization: Tenant1 Zones: Tenant-1-LAN-Zone Routing Instance: (Auto-populate) IPv4 Address: Static

•



Edit Temp	Edit Template - Template-labuser110-branch110																
Basic Interfaces Routing Tunnels Inbound NAT Services Management Servers																	
Device Po	Device Port Configuration																
Numb Ports 6	Number of Ports 6 V Mgmt WAN WAN LAN																
WAN Interfaces 🕄			Dringing		IPv4		IPv6		Allow S	SH	Link Monitor			Cub Interferen			
Port #	Interrace	VLAN	ID	Network Name		Priority	Static	DHCP		Static	DHCP	To CF	E Ne	xthop	Remote	IP	Sub interfaces
0	vni-0/0	•		MPLS	$\sim$	\$			)						\$		÷
1	vni-0/1	•		INET	~	\$			)						\$		+
LAN Inter	faces 🥹													Pv4	1	Pv6	Sub
Port #	Interface	VLAN ID	Networ	'k Name	Organization		Zones			Routing	Instance		Static	DHCP	Static	DHCP	Interfaces
2	vni-0/2	\$	Tenan	t1-LAN	Tenant1	enant1 $\checkmark$		LAN-Zone	$\sim$	Tenant1	Tenant1-LAN-VR 🗸		2				•
Back	Back Cancel Continue Recreate																

### **Routing Tab**

Do not configure any Routing parameters.

### **Tunnels Tab**

Configure Split Tunnels. In the Split Tunnels, link the VRF Tenant1-LAN-VR with the WAN interface INET. Make the Split Tunnels a DIA type, which allows traffic sourced from the Tenant1-LAN-VR and destined to a non-SD-WAN destination to use the INET routing instance to forward traffic (Direct Internet Access).

Be sure to click the 🕂 button to add the DIA configuration .

							,
Create Template							×
Basic Interfaces Routing	Tunnels Inbound NAT Services	Management Servers					
Split Tunnels 🔋							
VRF Names 🗢		WAN Interfaces		DIA	Gateway		
Select	~	Select	~				<b>E</b>
Tenant1-LAN-VR		INET			-		ī
					Load Balance		
Site to Site Tunnels							
Name 🗢	Peer Type	WAN/LAN Network	LAN VRF	Vpn Profile	E	GP Enabled	
	Select V	Select V	Select V	Select			<b>•</b>
		No Records to	Display				
Back					Cancel	Save	Continue



### **Inbound NAT Tab**

Do not configure any Inbound NAT properties.

### Services Tab

Enable the SFW services under the Services tab.

Service Templates 🔋	]		
Organization	Security		
Tenant1	🔿 None	SFW	
4			

### Management Servers Tab

Do not configure any Management Servers properties.



Click on the template that you created with your workflow to open the template and use the values in the lab to fill in the information below.

Interface Name:	Address associated with the interface
vni-0/0	
vni-0/1	
vni-0/2	

Question: Why do you think that there are variable names in the interface IP Address field of the interfaces instead of actual IP addresses?

Network Name	Interface associated with the network
MPLS	
INET	
LAN-Network	

Virtual Routers	Networks associated with the Virtual Router
MPLS-Transport-VR	
INET-Transport-VR	
Tenant1-Control-VR	
Tenatn1-LAN-VR	

Open the Services tab of the template and fill in the following information:

Home Template-labuser	110-branch110	$\sim$
* 🗘 🔹 %		
∎-{ <b>I</b> CGNAT		
<u> </u>		
<b>G</b>		
8 <sup>2</sup>		
Web Proxy		



Location	Values
Stateful Firewall > Security > Policies	What 2 policies are automatically created?
Stateful Firewall > IPsec	What 2 VPN profiles are automatically created?
SDWAN > Controllers	What controller is listed?

Open the *Objects & Connectors* tab of the template.

Expand the *Objects* menu and fill in the following information:

	Hor	me labuser110	0-branch
-	¥	۰ 🔅	\$8
٢	0	bjects	$\sim$
	9		
	Q,		
	æ	Persistent Action	ns
	Ē		
	<b>@</b>	Cloud Profiles	
	5	Pre-defined	>
	\$	Custom Objects	>
	•	SNAT Pool	
0,	Co	onnectors	>



In the next lab parts you will:

• Compare the newly created Device Template to the running configuration on your device

#### Steps:

- Open your device in Appliance Context mode (by using the Monitor tab, the Configuration > Devices table, or through the Administration > Appliances table.)
- Identify the security features configured on your device and compare them with the security features configured in the device template you just created.

#### Step by Step Guide

Navigate to the *Administration > Appliances* dashboard. Locate your device in the Appliances table. Click on your device to open the Appliance Context mode of your device.

V	VERSA		M	lonitor	Configuration	Workflows	Administr	ation Ar	nalytics	
2 0	Organizations		Total	Appliances : 9						10
🕴 C	ystem	>		Name	Mgmt. Address	Туре	Time Created	Service Start	Software Version	Si
D N	otification Config ntitlement Manager	>	0	Branch110	10.1.64.102	Branch	Tue, Sep 22 2	Thu, Mar 04 2	20.2.2-GA	1
L D	)irector User Mana iventory	>		Name	Branch110		Tue, Mar 09 2	Tue, Mar 09 2	20.2.2-GA	11
erest Barrier Barrier Barrier	DWAN	>		Location	Bend,OR, USA		Tue, Mar 09 2 Tue, Mar 09 2	Tue, Mar 09 2 Tue, Mar 09 2	20.2.2-GA 20.2.2-GA	1(
0 .	10.0	2		Services	sdwan,nextgen-fi	irewall,cgnat	Tue, Mar 09 2 Tue, Aug 11 2	Tue, Mar 09 2 Thu, Mar 04 2	20.2.2-GA 20.2.2-GA	10
				Router	192.168.99.130	Service-vnf	Tue, Aug 11 2 Tue, Sep 17 2	Thu, Mar 04 2 Thu, Mar 04 2	20.2.2-GA 20.2.2-GA	10

From Appliance Context mode, navigate to the Configuration > Services dashboard and fill in the configured service below:

25

١		A.	Monitor	Analytics	Configuration	Administration
	lome Branc	h110		$\sim$	Organization: Tenant1	~
3	6 <b>0</b> 6	8				
-	CGNAT					
6	IPsec	>				
824 (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	SDWAN Web Proxy Captive Portal	>				Select a service from left menu.

Question: What type of security services are currently configured (and configurable) on the device?

Question: Are these services the same services that are available under the template that you created?

Click the Home button to exit device configuration mode.

In the next lab parts you will:

- Create a device group named DG-[branched] (e.g. DG-branch110, DG-branch111, etc.);
- Assign the template you created to the device group;
- Re-assign your branch device to the new device group; and
- Commit the template you created in order to re-configure your branch device.

#### Steps:

- Create a new device group with the name DG-[branch-name] (e.g. DG-branch110, DG-branch111, etc.).
- Assign the template that you created to the device group.
- Reassign your device to the new device group (either through the Devices > Device Group dashboard or through the Device Workflow for your device)
- Commit the changes
- Verify that the services changed on your device from Next Gen Firewall to Stateful Firewall services.

#### Step by Step Guide

From the main Versa Director dashboard, navigate to *Configuration > Devices > Device Groups*.

In the Device Groups dashboard, click the + button to create a new device group.

VERSA							🔎 🗐 🕕 labuser 🗸
W NETWORKS	N	Ionitor Configuration	m Workflows A	dministration	Analytics		Commit Template
						Configuration >	> Tenant1 > Device Groups C
Search	Temp	lates 👻 Devices 👻 Objects	•				
sp (G	Q	Search					Ⅱ   ▼   < 1 of 1 ▶   25 ∨
A Tenant1	0				Contact Information	Add	Members
		Name	Organizations	Email Address	Phone Number	Appliances	Devices
		DG-Hub105	Tenant1				Hub105
		DG-NGFW	Tenant1				Branch111 Branch114 Branch110 <u>View More</u>
		DG-SFW	Tenant1				

Name the device group DG-[branch-id] (e.g. DG-branch110, DG-branch111, etc.)

Assign the template you created earlier to the Post Staging Template field, then click OK to create the device group.

Name I 440		
DG-branch110		
Description		
Tags		
Organization	Capital Two Factor Auth	CA In Data Contar
Charles Terralate	Enable Two Factor Auth	
Staging Template	Post Staging Template	General del Soloct
Email	Phone (201) 555-5555	
Post Staging Template Ass	sociation(2) Devices(0) URL Based ZTP	
Post Staging Template Ass	sociation(2) Devices(0) URL Based ZTP	₽   III   ▼   < 1 >   2
Post Staging Template Ass	Sociation(2) Devices(0) URL Based ZTP	E   III   ▼   < 1 >   2     Template
Post Staging Template Ass Tenant Tenant1	Category DataStore	Image: Base of the second
Post Staging Template Ass Tenant Tenant1 Tenant1	Category DataStore Main	
Post Staging Template Ass Tenant Tenant1 Tenant1	Category DataStore Main	Image: Constraint of the second se
Post Staging Template Ass Tenant Tenant1 Tenant1	Category DataStore Main	Template Template-labuser110-branch110



Question: Does your new device group appear in the Device Group table?

Question: Does your branch device appear in your device group Members list?

#### Assign Device to a New Device Group

In the next steps, you will use the Device workflow to assign your branch device to the new device group.

Navigate to the Workflows > Devices > Devices dashboard and locate your device in the Device Workflow list. Click your device to open the workflow.

Locate your new device group in the Device Groups drop-down menu, and assign your new device group to the device.

Add Device - Branch110				×
Basic Location Information Devic	e Service Template Bind Data			
Name*	Global Device ID*		Organization*	
Branch110	102		Tenant1	
Deployment Type	Serial Number		Device Groups*	
CPE-Baremetal Device	SN-Branch110		DG-branch110	1
			+Device Group	
Admin Contact Information		Subscription		
Email Phone Number		Service Bandwidth	Aggregate Bandwidth	
(201) 555	5-5555	Select options		
		Can	cel Save Continue Redeploy	



Click the Redeploy button to apply the changes to the Device workflow.

You have successfully update the device information in Versa Director. The next step is to apply the changes made in Versa Director to your appliance by committing the template.

Click the Commit Template link in the top-right corner of Versa Director.

In the Commit dialog:

- 1. Select the Tenant1 organization
- 2. Select your newly created template from the Select Template drop-down
- 3. Locate your device in the Device Groups table and select the box next to your device
- 4. Ensure that the Overwrite option is selected
- 5. Click the OK button to apply the changes to the device.

Comm	llt						3	×
Organ Tenar	ization*	1) ~	O Template O	Service Template		$\sim$		
Select Temp	Template* late-labuser110-bran	ich110 2 ~	Reboot		Auto Me	erge Overwrite	0	
Device	Groups							
	Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association	
	DG-branch110							
	Branch110	Branch	OUT_OF_SYNC	IN_SYNC	0	•	ů.	
(3)								
$\sim$								
						5	Cancel	J



In the next lab steps you will:

- Verify that the changes have been applied to your device (security services changed from Next Gen Firewall to Stateful Firewall)
- Change your template services from SFW to NGFW services using the Template Workflow
- Re-deploy your template with the new services definition
- Apply the template changes to your device
- Verify that the security services changed from SFW to Next Gen Firewall services.

In the Versa Director dashboard, navigate to Administration > Appliances and locate your device in the appliances table.

Click your appliance in the Appliance table to open the Appliance Context mode of your device.

In the Appliance Context mode of your device, navigate to the Configuration > Services dashboard and fill in the diagram below:

1	VE	RSA		Monitor	Analytics	Configuration	Administration
	lome	Branch11	0		~	Organization: Tenant1	
3	6 <b>Q</b>	٢	\$				
-4 A	CGNAT						
3	IPsec		>				
82	SDWAN		>				Select a service from I
•	Web Pro	оху					

Question: What types of security services are configurable on the device?

Question: Were the changes you made applied to the device?

Next you will change the services available on your device back to Next Gen Firewall services by changing your template using the Template workflow.

Click the Home button next to your device name to exit Appliance Context mode. This returns you to the main Versa Director user interface.

In the main Versa Director user interface, navigate to Workflows Template > Templates to display the saved Device Template workflows.



In your Template workflow, navigate to the Services tab.

Edit Tem	emplate - Template-labuser110-branch110 X													
Basic	Interfaces	Routing	Tunnels	Inbound NAT	Services	Managemer	nt Servers							
DHCP	Server								DHCP Relay					
LAN Int	terfaces 🗢		[	OHCP Options Prot	file				LAN Interfaces 🗢		IP Address*			
Selec	:t		$\sim$			$\sim$	+		Select		✓ Q			+
			No Re	cords to Display							No Records to Disp	blay		
						+DHCP Op	tions Profile							
Service	e Templates 🔞				(1)	)								
Organ	ization	Secur	rity		تے م	5								<b>^</b>
Tenan	t1		Non	e	NGF	N	0	SFW						Ŧ
•														$\rightarrow$
														(2)
Back												Cancel	Continue	Recreate

In the Services tab:

- 1. Change the services to NGFW
- 2. Click Recreate

When an existing template is changed by updating the Template workflow, Versa Director will prompt you to confirm/validate the changes by doing a Difference (diff and merge) validation. The changes to the template will be displayed, and the administrator is required to verify and deploy the changes:

Diff and Merge					×
Active Template					
Current ∳ (Read         ()         238         239         240         services [ "cgnat" "sdwan" "stateful         241         traffic-identification (         242         using [ "ptvi2" "tvi-0/4.0" "tvi-0         ()         786         service-node-group "default-sng" (         787         id "0";         788         services [ "cgnat" "sdwan" "stateful         789         type "internal";         790         ()	-firewall" ];	~111-> ~111->	() 238 239 240 () 786 787 787 789 790 ()	Newly Generated ↓ } convices [ "ogac ] "nextgen-fire traffic-identification { using [ "ptvi2" "tvi-0/4.0" "t service-node-group "default-sng" { id "0"; convices [ "ogac ] "nextgen-fire type "internal"; }	Auto-merged (Recommended) (Editable) well" "sdwan" ]; vi-0/5.0" "tvi-0/602.0" "tvi-0/603.0" ]; well" "sdwan" ];
	You changed the se nextgen firewall – template con	ervices the as figurat ⇒∉	from sociate	stateful-firewall to ed changes to the e highlighted	
					Deploy Cancel

Click Deploy to apply the workflow changes to the template, and to re-write the template data.

#### Verify the Template Changes, and Apply the Update to your Device

Navigate to *Configuration > Templates > Device Templates*. Ensure that the *Tenant1* organization is selected in the left-side menu.

31

Locate and open the device template that you just updated through the Device Template workflow.

In the *Services* tab of the template configuration, verify that the Next Gen Firewall services are present in the template.

1					
			Monitor	Configuration	Workflows
	Home Template-	labuser11	0-branch110	× 1	Organization: Ter
4	0 0	\$			
•	CGNAT				
0	Next Gen Firewall	>			
6	IPsec	>			
82	SDWAN	>			
	Web Proxy				
	Captive Portal				

Navigate to the Monitor > Devices dashboard. Ensure that the Tenant1 organization is selected in the left-side menu.

Locate your device in the Devices table, and open your device. This places you in Appliance Context mode for your device (in the same way that clicking your device in the Administration > Appliances table places you in Appliance Context mode).

From Appliance Context mode, navigate to the *Configuration > Services* dashboard.

Question: What security services do you think will be available on the device (answer is on the next page):



32

The Stateful Firewall services are still present on the device. Although you modified the template and verified the changes, the template changes haven't been committed to the devices that reference the template.

Click the Home button next to your appliance name to exit Appliance Context mode.

From the main Versa Director user interface, click Commit Template.

From the Commit dialog:

r

- 1. Select the Tenant1 organization
- 2. Select your template from the Select Template drop-down menu
- 3. Select your device from the device list
- 4. Ensure that Overwrite is selected
- 5. Click OK to commit the changes to the device.

	Comn	nit						×		
	Organ Tenar	iization* nt1	~	🛛 Template 🌑	• Template • Service Template					
(2)	Select Temp	Template* blate-labuser110-bran	nch110 🗸 🗸	Reboot	Reboot • Auto Merge • Overv					
		Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association		
	• 🔽	DG-branch110								
(3		Branch110	Branch	OUT_OF_SYNC	IN_SYNC	0	0	L)		
								DK Cancel		



### Verify the Changes on the End Device

Now that you have committed the template changes to your device, you will verify the changes one more time.

From the Versa Director user interface, navigate to Administration > Appliances and locate you device in the appliance list. Click your appliance to open the Appliance Context dashboard.

In the Appliance Context dashboard, navigate to Configuration > Services.

Question: Did the available services change from Stateful Firewall to Next Gen Firewall?

# Exercise 6: Reset the Lab Environment

In this lab part you will:

- Re-assign your device to the Base-Template-NGFW template by re-assigning the Device Group in your Device workflow
- Commit the changes to reset your device configuration to the base configuration
- Delete your user-created Device Template Workflow (which will delete the template associated with the workflow)
- Delete the user-created Device Group that you created during this lab.
- 1. Navigate to the Workflows > Devices > Device hierarchy to display the saved Device workflows.
- 2. Locate your device workflow in the Device Workflow table and click the workflow to open it.
- 3. In the Device workflow, set the Device Group to DG-NGFW.
- 4. Click Redeploy to update your device workflow and save the changes.

Add Device - Branch110		×
Basic Location Information Device Serv	ice Template Bind Data	
Name*	Global Device ID*	Organization *
Branch110	102	Tenant1
Deployment Type	Serial Number	Device Groups*
CPE-Baremetal Device $\lor$	SN-Branch110	DG-NGFW V
		+Device Group
Admin Contact Information	Subscription	
Email Phone Number	Service Bandwi	dth Aggregate Bandwidth
(201) 555-5555	Select options	
		Cancel Save Continue Redeploy



Navigate to the *Configuration > Devices > Device Groups* dashboard.

In the Device Groups table:

- 1. Check the box next to your user-defined device group
- 2. Click the button to remove your user-defined device group.
- 3. Confirm the device group deletion

				• d			↓ Iabuser ✓	
	IVI	conigura	uon worknows	Administration	nalytics	Configurat	on > Tenant1 > Device Groups	
Search	Temp	lates 👻 Devices 👻 Objec	its 👻			(2		
SP 🔘		earch			Y   < 1 of 1 >   25 >			
Tenant1	-	-				Contact Information		Members
$\sim$		Name	Organizations	Email Address	Phone Number	Appliances	Devices	
(1)		DG-branch110	Tenant1					
$\cup$		DG-Hub105	Tenant1				Hub105	
		<u>DG-NGFW</u>	Tenant1				Branch111 Branch114 Branch112 View More	
		DG-SFW	Tenant1					

Navigate to the *Workflows > Template > Templates* dashboard.

In the Templates workflow table:

- 1. Check the box next to your user-defined template
- 2. Click the button to remove your user-defined template.
- 3. Confirm the wokflow deletion

	N	Ionitor Config	uration	Workflows	Administration	Analytics			<b>1</b> 9	Commi	labuser ∽ it Template
Organization:Select			~					( 2			C
Infrastructure >	Q	Search						) <b>+</b>   E	) <b>( () () ()</b>	1 of 1	25 🗸
Templates		Name		Status		La	ast Modified Time	De	elete Template By		
Application Steering		Base-Template-NGFW		Deployee	t	W	ed, Sep 23 2020, 21:24	-	lapuser		
Spoke Groups		Base-Template-SFW		Deployee	i .	Tu	ie, Aug 11 2020, 20:37		Administrator		
Service Chains		Template-labuser110-	branch110	Deployee	i .	Th	nu, Mar 11 2021, 20:25		labuser		
Devices		<u>T-Hub105</u>		Deployee	i	Tu	ie, Sep 01 2020, 02:11		Administrator		
- Concer											

