citrix™

Citrix SD-WAN Platforms

Contents

Product Datasheet

June 19, 2020

The Citrix SD-WAN product data sheet is available on www.citrix.com. Click **Products**, and in the Networking list, select **Citrix SD-WAN**. In Platforms, select SD-WAN platforms to review the complete list of available SD-WAN platforms.

Platform Editions

July 24, 2020

The various Citrix SD-WAN hardware platforms offer a wide range of features, communication ports, and processing capacities. All Citrix SD-WAN hardware platforms support the Citrix SD-WAN software.

> **Important**:
> The NetScaler SD-WAN product is rebranded to Citrix SD-WAN. All references to the term NetScaler SD-WAN are applicable to the new product term Citrix SD-WAN.

The Citrix SD-WAN Standard appliances include the following editions:

- SD-WAN Standard Edition 110, 210, 400 and 410
- SD-WAN Standard Edition 1000, 1100, 2000, and 2100
- SD-WAN Standard Edition 4000, 4100, 5100, and 6100

The Citrix SD-WAN WANOP appliances include the following editions:

- SD-WAN WANOP 800, 1000, 2000, 2100, and 3000
- SD-WAN WANOP 1000 WS and 2000 WS
- SD-WAN WANOP 4100 and 5100

The Citrix SD-WAN Premium (Enterprise) appliances include the following editions:

- SD-WAN Premium (Enterprise) Edition 1000, 1100, 2000, and 2100
- SD-WAN Premium (Enterprise) Edition 5100, and 6100

Update Password

From 10.2.6 release onwards, the appliance and LOM passwords are set to the Citrix serial number, which is displayed on the rear of the appliance. Change the password on first time logon.

From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.

WANOP

April 8, 2020

> **Important**
>
> The **NetScaler SD-WAN** product is rebranded to **Citrix SD-WAN**. All references to the term **NetScaler SD-WAN** is applicable to the new product term **Citrix SD-WAN**.

The Citrix SD-WAN WANOP appliances include the following editions:

- SD-WAN WANOP 800, 1000, 2000, and 3000
- SD-WAN WANOP 1000 WS and 2000 WS
- SD-WAN WANOP 4100 and 5100

Citrix SD-WAN 800, 1000, 2000 and 3000 WANOP appliances

June 19, 2020

The SD-WAN 800, 1000, 2000 and 3000 appliances are 1U accelerators for use in datacenters and larger branch offices.

The SD-WAN 2000 can be thought of as a faster Repeater 8500 appliance with two accelerated bridges, while the SD-WAN WANOP 3000 can be thought of as a faster Repeater 8800 with three accelerated bridges. The configuration process, however, is not the same. Like the high-end Repeater SDX appliance, SD-WAN 2000 and WANOP 3000 appliances use virtual machines for acceleration and management, running under a XenServer hypervisor.

- SD-WAN 800 Series. A small 1U appliance suitable for medium-sized branch offices, the 800 Series has two accelerated bridges and supports WAN speed of up to 10 Mbps.
- SD-WAN 2000 Series. A full-sized 1U appliance suitable for large branch offices and smaller datacenters, the 2000 Series has two accelerated bridges and supports WAN speed of 10-50 Mbps.
- SD-WAN 3000 Series. A full-sized 1U appliance suitable for the largest branch offices and medium-sized datacenters, the 3000 Series has three accelerated bridges and supports WAN speed of 50-155 Mbps.

The Citrix Compliance Regulatory Models are as follows:

- SD-WAN 800 WANOP: CB 504-2
- SD-WAN 1000 WANOP: CB 504-2
- SD-WAN 2000 WANOP: NS 6xCu
- SD-WAN 3000 WANOP: NS 6xCu 6xSFP

All SD-WAN platforms have similar components and hardware platforms offer a wide range of features, communication ports, and processing capacities. All platforms support the SD-WAN software and have multicore processors. These appliances have similar architectures, run the same release binaries, and are fully supported with release 9.2.

Citrix SD-WAN WANOP 800

May 23, 2019

The Citrix SD-WAN WANOP 800 platform has a dual-core processor and 8 GB of memory. The platform has a bandwidth of up to 6 Mbps and up to 10 Mbps, respectively.

The following figure shows the front panel of an SD-WAN WANOP 800 appliance.

Figure 1. Citrix SD-WAN 800, front panel
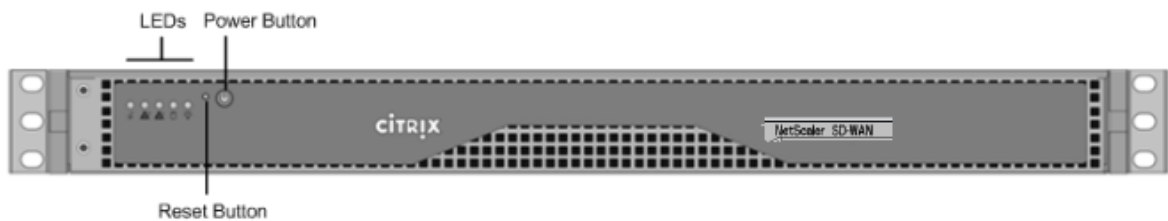
- The front panel of the SD-WAN 800 appliance has a power button and five LEDs.
- The power button switches main power (the power to the power supply) on or off.
- The reset button restarts the appliance.

The LEDs provide critical information about different parts of the appliance.

- Power Fail—Indicates that a power supply unit has failed.
- Information LED—Indicates the following:

Status	Description
Continuously on and red	The appliance is overheated. (This might be a result of cable congestion.)
Blinking red (1 Hz)	Fan failure.
Blinking red (0.25 Hz)	Power failure.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.

Status	Description
Blinking blue (300 m/s)	Remote UID is on. Use this function to identify the server from a remote location.

- NIC1 and NIC2—Indicate network activity on the LAN1 and WAN1 ports.
- HDD—Indicates the status of the hard disk drive.
- Power—When blinking, indicates that the power supply unit is receiving power and operating normally.

The following figure shows the back panel of an SD-WAN 800 appliance.

Figure 2. Citrix SD-WAN 800 appliance, back panel
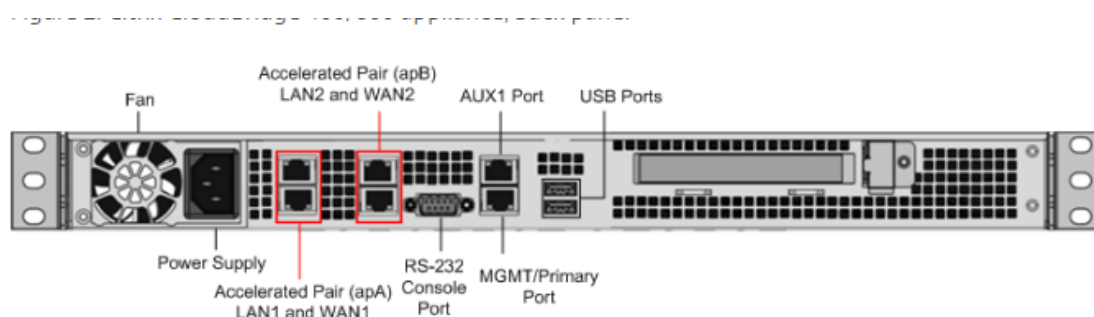
The following components are visible on the back panel of an SD-WAN 800 appliance:

- Cooling fan
- Single power supply, rated at 200 watts, 110–240 volts
- Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges. Individual port assignments: LAN1 is apA.1, WAN1 is apA.2, LAN2 is apB.1, LAN2 is apB.2.
- RS-232 serial console port
- One Aux Ethernet port and one management port
- Two USB ports
- One Solid State Drive (SSD)
  - SD-WAN 800 - 240 GB SSD

For initial configuration of a SD-WAN appliance, perform the following tasks::

- Configure the appliance for use on your site.
- Install the Citrix license.
- Enable acceleration.
- Enable traffic shaping (inline mode only).

You can configure the appliance by connecting the appliance to your computer through either the Ethernet port or the serial console. The following procedure enables you to configure the appliance by connecting it to your computer through the Ethernet port.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your set up appliance by completing the Assigning a Management IP Address through the Serial Console procedure.

Citrix SD-WAN WANOP 1000

June 19, 2020

The Citrix SD-WAN WANOP 1000 platform has 3 models: SD-WAN 1000-06, SD-WAN 1000-010, and SD-WAN 1000-020, with bandwidths of 6Mbps, 10Mbps, and 20Mbps, respectively. Each model is a 1U appliance with one quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of an SD-WAN 1000 appliance.

The front panel of the Citrix SD-WAN WANOP 1000 appliance has a power button and five LEDs.

- The power button switches main power (the power to the power supply) on or off.
- The reset button restarts the appliance.
- The LEDs provide critical information about different parts of the appliance.

Figure 1. Citrix SD-WAN WANOP 1000, front panel

The appliance has the following ports:

- An RS232 serial console port.
- A copper Ethernet (RJ45) management port. The management port is used to connect directly to the appliance for system administration functions.
- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of an SD-WAN 1000 appliance.

Figure 2. Citrix SD-WAN WANOP 1000 appliance, back panel
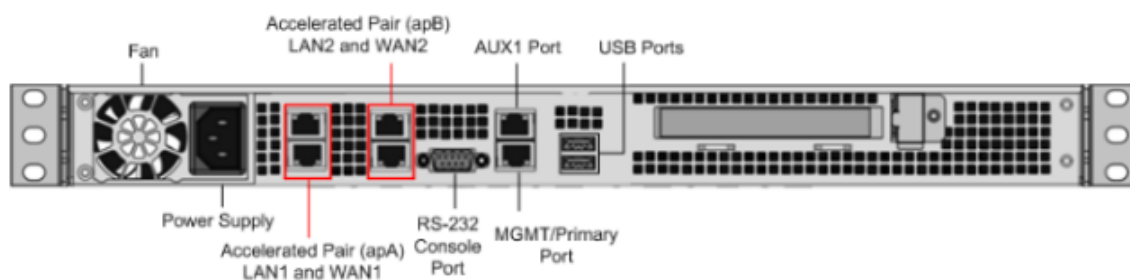
The following components are visible on the back panel of the SD-WAN WANOP 1000 appliance:

- 600 GB removable solid-state drive, which stores the appliance's software and user data.
- USB port (reserved for a future release).
- Single power supply, rated at 300 watts, 100-240 volts.

Power on appliance after a graceful shutdown

To power on the appliance after a graceful shut down:

1. Connect a Serial console cable to the rear of the appliance and to the serial port on a management laptop.

2. On the management laptop, restart a putty session using the following configuration settings:
   - Serial line: COM1
   - Speed: 9600

3. Power on the appliance and as it is booting, press the following key in the Putty session to enter the BIOS configuration screen. Keypress: **DEL**
4. When in the BIOS, navigate to,
   - Advanced Tab > **Select**
   - Boot Feature > **Enter**

5. When in the Boot Feature screen, change the value of the parameter **Restore on AC Power Loss; **from **Last State **> **Power ON**.

6. Navigate to Save and Exit.

   - Select **Save changes** and **Reset**
   - Select **Yes**

   Allow the system to restart. This takes approximately five minutes.

7. After the appliance is powered on, login to the appliance management instance (SVM). The default IP address for the appliance is: 192.168.100.1, user name is: admin/password.

8. In the SD-WAN appliance GUI, navigate to **Configuration** > **Maintenance** > **Reboot Appliance**. Allow the appliance to fully shut down. Ensure that there are no power lights on the appliance when the shut down process has completed.

9. Power on the appliance to confirm that the BIOS configuration change has been applied successfully. This can be either done through the APC intelligent PDU Web Management console or by physically pulling the power cable out of the shut down SD-WAN appliance, waiting for 10 seconds and then plugging it back in again. The appliance power ups automatically from all shut down scenarios.

Citrix SD-WAN WANOP 2000

June 19, 2020

The Citrix SD-WAN WANOP 2000 platform has 3 models: SD-WAN 2000-010, SD-WAN 2000-020, and SD-WAN 2000-050, with bandwidths of 10 Mbps, 20 Mbps, and 50 Mbps, respectively. Each model is a 1U appliance with 1 quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN WANOP 2000 appliance.

Figure 1. Citrix SD-WAN WANOP 2000, front panel

The appliance has the following ports:

- An RS232 serial console port.

- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.

- A copper Ethernet (RJ45) management port, numbered 0/1. The management port is used to connect directly to the appliance for system administration functions.

> **Note**: The LOM port also operates as a management port.

- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN 2000 appliance.

Figure 2. Citrix SD-WAN WANOP 2000 appliance, back panel

The following components are visible on the back panel of the SD-WAN 2000 appliance:

- 600 GB removable solid-state drive, which stores the appliance's software and user data.
- Power switch, which turns off power to the appliance. Press the switch for five seconds to turn off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 100–240 volts.

Citrix SD-WAN WANOP 3000

June 19, 2020

The Citrix SD-WAN WANOP 3000 platform has 3 models: SD-WAN 3000-050, SD-WAN 3000-100, and SD-WAN 3000-155, with bandwidths of 50M bps, 100 Mbps, and 155 Mbps, respectively. Each model is a 1U appliance with 1 quad-core processor and 32 gigabytes (GB) of memory.

The Citrix SD-WAN WANOP 3000 appliance is available in two port configurations:

- Six 10/100/1000 Base-T copper Ethernet ports
- Four 1G SX Fiber ports

The following figure shows the front panel of an SD-WAN 3000 with six 10/100/1000 Base-T copper Ethernet ports.

Figure 1. Citrix SD-WAN WANOP 3000 (6×10/100/1000 Base-T copper Ethernet ports), front panel
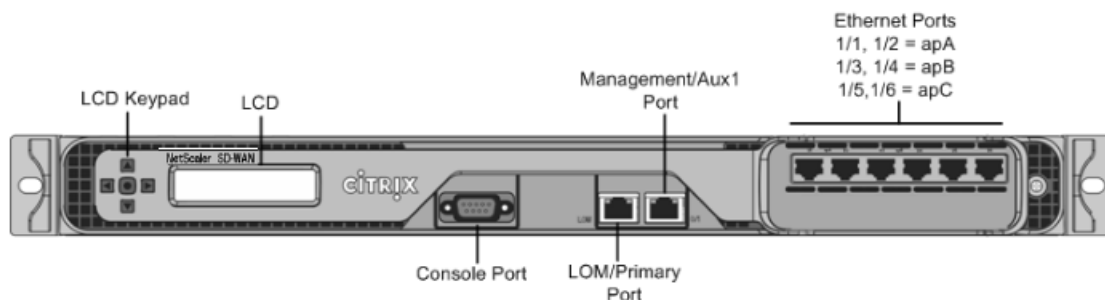
The following figure shows the front panel of an SD-WAN 3000 appliance with four 1G SX fiber ports.

Figure 2. Citrix SD-WAN WANOP 3000 (4×1G SX Fiber ports), front panel
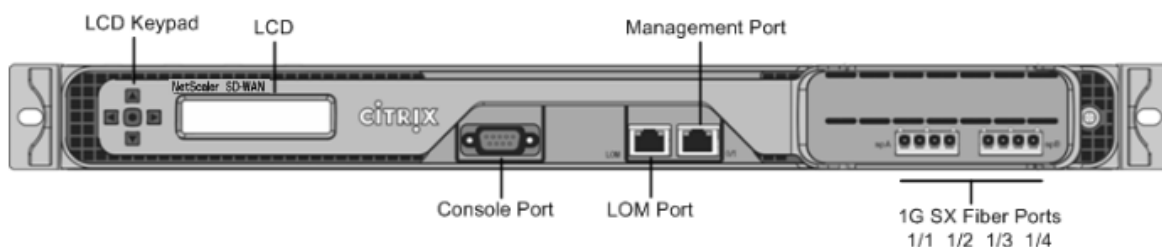
The appliance has the following ports:

- An RS232 serial console port.

- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.

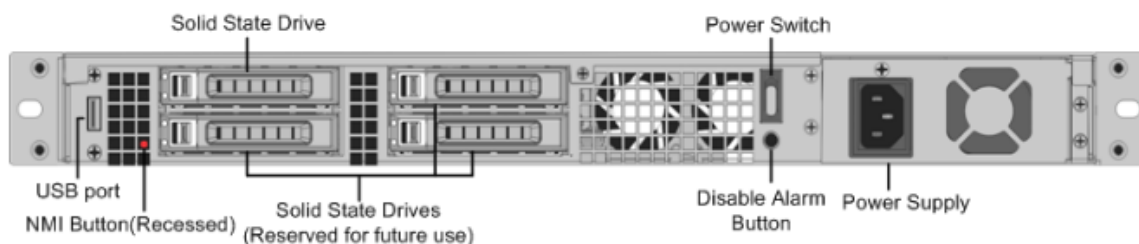- A copper Ethernet (RJ45) management port, numbered 0/1. The management port is used to connect directly to the appliance for system administration functions.

  > **Note**: The LOM port also operates as a management port.

- Network Ports, in one of the following configurations:

    – SD-WAN 3000 (6x10/100/1000 Base-T copper Ethernet ports). Six 10/100/1000 Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 from left to right. The six ports form three accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), 1/3 and 1/4 are accelerated pair B (apB), and 1/5 and 1/6 are accelerated pair C (apC).

    – SD-WAN 3000 (4x 1G SX Fiber ports). Four 1G SX fiber ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA) and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN WANOP 3000 appliance.

Figure 3. Citrix SD-WAN WANOP 3000 appliance, back panel
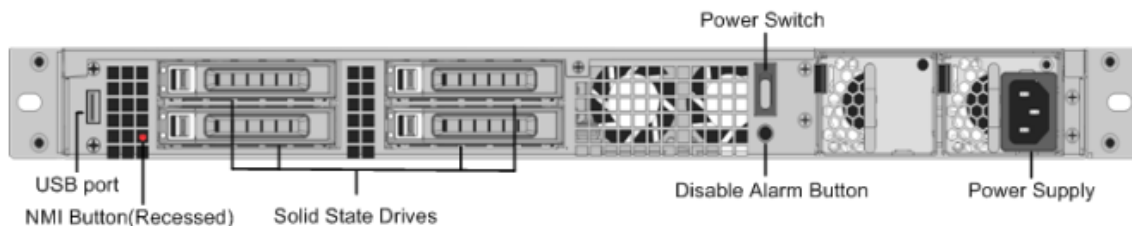
The following components are visible on the back panel of the SD-WAN WANOP 3000 appliance:

- Four 600 GB removable solid-state drives. The top left solid-state drive stores both the appliance's software and the user data. The other three store only user data.
- Power switch, which turns power to the appliance on or off. To turn off the power, press the switch for five seconds.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Disable alarm button, which is nonfunctional unless you install a second power supply. In that case, it disables the alarm that sounds if the appliance is plugged into only one power outlet or one of the power supplies fails.
- Single power supply, rated at 450 watts, 100–240 volts.

Summary of Hardware Specifications

June 22, 2020

The following table summarizes the specifications of the Citrix SD-WAN WANOP 800, 1000, 2000, and 3000 hardware platforms.

Table 1. Citrix SD-WAN WANOP 800, 2000, 1000, and 3000 Platforms Summary

Platform Performance

H/W Specifications	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
Bandwidth	Up to 6 Mbps	Up to 10 Mbps	Model 1000-006: 6 Mbps	Model 2000-010: 10 Mbps	Model 3000-050: 50 Mbps
	Model 400-002: 2Mbps	Model 800-002: 2Mbps	Model 1000-010: 10 Mbps	Model 2000-020: 20 Mbps	Model 3000-100: 100 Mbps
	Model 400-006: 6 Mbps	Model 800-006: 6 Mbps	Model 1000-020: 20 Mbps	Model 2000-050: 50 Mbps	Model 3000-155: 155 Mbps
		Model 800-010: 10 Mbps			
Maximum HDX sessions	Up to 60	Up to 100	200	300	500
Total sessions	500	10,000	10,000	20,000	50,000
Acceleration Plug-in CCUs	NA	NA	NA	750	1,000

Hardware Specifications

H/W Specifications	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
Processor	2 Cores	2 Cores	2 Cores	4 Cores	4 Cores
Total disk space	1 x 160 GB SSD	1 x 240 GB SSD		1 x 600 GB SSD	4 x 600 GB SSD
SSD (dedicated Compression history)	40 GB	80 GB		275 GB	1.5 TB
RAM	8 GB	8 GB	24 GB	32 GB	

H/W Specifications	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
Network Interfaces	2 pair with bypass 10/100/1000	2 pair with bypass 10/100/1000		4 x 10/100/1000 Base-T copper Ethernet	6 x 10/100/1000 Base-T copper Ethernet
Transceiver support	No	No	Yes	Yes	
Power supplies	1	1	1	1	

Physical Dimensions

H/W Specifications	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
Rack Units	1U	1U		1U	1U
System width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks		EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
System depth	10.5" (26.7 cm)	10.5" (26.7 cm)		25.4" (64.5 cm)	25.4" (64.5 cm)
System weight	8 lbs (3.5 kg)	8 lbs (3.5 kg)		32 lbs (14.5 kg)	32 lbs (14.5 kg)
Shipping dimensions and weight	26L x 18.5W x 6.5" H; 14 lbs	26L x 18.5W x 6.5" H; 14 lbs	32L x 23.5W x 7.5" H; 39 lbs	32L x 23.5W x 7.5" H; 39 lbs	

Environmental and Regulatory

H/W Specifications	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
Voltage	100/240 VAC, 50-60 Hz	100/240 VAC, 50-60 Hz		100/240 VAC, 50-60 Hz	100/240 VAC, 50-60 Hz
Power consumption (Max.)	200W	200W		300 W	450 W

H/W Specifications	SD-WAN WANOP 800	SD-WAN WANOP 1000	SD-WAN WANOP 2000	SD-WAN WANOP 3000	
Operating Temperature (degree Celsius)	10–35	10–35		0–40	0–40
Non-operating Temperature (degree Celsius)	-40–+70	-40–+70		-40–+70	-40–+70
Allowed Relative Humidity	8%–90%	8%–90%		5%–95%	5%–95%
Safety certifications	CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)	CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)		CSA	TUV
Electromagneti and susceptibility certifications	FCC (Part 15 Class A), EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A	FCC (Part 15 Class A), EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A	FCC (Part 15 Class A), EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A	FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT	FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT
Environmental certifications	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE

Citrix SD-WAN 800, 1000, 2000 and 3000 WANOP appliances

June 19, 2020

The SD-WAN 800, 1000, 2000 and 3000 appliances are 1U accelerators for use in datacenters and larger

branch offices.

The SD-WAN 2000 can be thought of as a faster Repeater 8500 appliance with two accelerated bridges, while the SD-WAN WANOP 3000 can be thought of as a faster Repeater 8800 with three accelerated bridges. The configuration process, however, is not the same. Like the high-end Repeater SDX appliance, SD-WAN 2000 and WANOP 3000 appliances use virtual machines for acceleration and management, running under a XenServer hypervisor.

- SD-WAN 800 Series. A small 1U appliance suitable for medium-sized branch offices, the 800 Series has two accelerated bridges and supports WAN speed of up to 10 Mbps.
- SD-WAN 2000 Series. A full-sized 1U appliance suitable for large branch offices and smaller datacenters, the 2000 Series has two accelerated bridges and supports WAN speed of 10-50 Mbps.
- SD-WAN 3000 Series. A full-sized 1U appliance suitable for the largest branch offices and medium-sized datacenters, the 3000 Series has three accelerated bridges and supports WAN speed of 50-155 Mbps.

The Citrix Compliance Regulatory Models are as follows:

- SD-WAN 800 WANOP: CB 504-2
- SD-WAN 1000 WANOP: CB 504-2
- SD-WAN 2000 WANOP: NS 6xCu
- SD-WAN 3000 WANOP: NS 6xCu 6xSFP

All SD-WAN platforms have similar components and hardware platforms offer a wide range of features, communication ports, and processing capacities. All platforms support the SD-WAN software and have multicore processors. These appliances have similar architectures, run the same release binaries, and are fully supported with release 9.2.

SD-WAN 1000 Appliance with Windows Server

May 23, 2019

The Citrix SD-WAN 1000 with Windows Server platform has a quad-core processor and 32 GB of memory. This platform has a bandwidth of up to 20 Mbps.

The following figure shows the front panel of a SD-WAN 1000 appliance with Windows Server.

Figure 1. Citrix SD-WAN 1000 with Windows Server, front panel

The front panel of the SD-WAN 1000 with Windows Server appliance has a power button and five LEDs.

The power button is used to switch the appliance on or off.

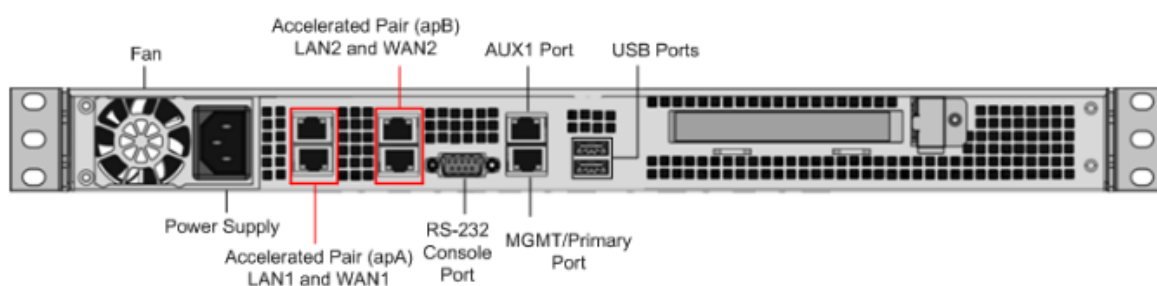The reset button restarts the appliance.

The LEDs provide critical information related to different parts of the appliance.

- Power Fail – Indicates the power supply unit has failed.
- Information LED – Indicates the following:

Status	Description
—	—
Continuously ON and red	The appliance is overheated. (This might be a result of cable congestion.)
Blinking red (1Hz)	Fan failure, check for an inoperative fan.
Blinking red (0.25Hz)	Power failure, check for the non-operational power supply.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Blinking blue (300 m/s)	Remote UID is on. Use this function to identify the server from a remote location.

- NIC1 and NIC2 – Indicate network activity on the LAN1 and WAN1 ports.
- HDD – Indicates the status of the hard disk drive.
- Power – Indicates that the power supply units are receiving power and operating normally.

The following figure shows the back panel of a SD-WAN 1000 appliance with Windows Server.

Figure 2. Citrix SD-WAN 1000 appliance with Windows Server , back panel

The following components are visible on the back panel of a SD-WAN 1000 appliance with Windows Server:

- Cooling fan
- Single power supply, rated at 200 watts, 110-240 volts
- Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges
- RS-232 serial console port
- One AUX Ethernet port and one management port
- Two USB ports

© 1999–2021 Citrix Systems, Inc. All rights reserved.
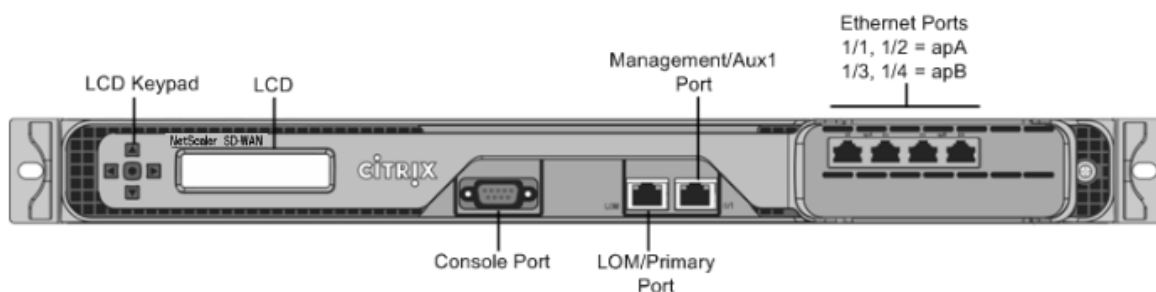
SD-WAN 2000 Appliance with Windows Server

May 23, 2019

The Citrix SD-WAN 2000 with Windows Server platform is a 1U appliance with 1 quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 2000 appliance with Windows Server.

Figure 1. Citrix SD-WAN 2000 appliance with Windows Server, front panel

> **Note**: You cannot assign apA ports to Windows Server. However, you can assign AUX port to Windows Server

SD-WAN 2000 appliance with Windows Server has the following ports:

- An RS232 serial console port.

- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.

- A copper Ethernet (RJ45) management port, numbered 0/1, and named PRI (primary). The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of WAN optimization and Windows Server.

  > **Note**: The LOM port also operates as a management port.

- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two *accelerated pairs*, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN 2000 appliance with Windows Server.

Figure 2. Citrix SD-WAN 2000 appliance with Windows Server, back panel

The following components are visible on the back panel of the SD-WAN 2000 appliance with Windows Server:

- 600 GB removable solid-state drive, which stores the appliance's software and user data, and 1 TB hard disk drive.
- Power switch, which switches power to the appliance on or off. Press the switch for five seconds to switch off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 100–240 volts.

Ethernet Port Names

May 23, 2019

When configuring the appliance, you have to specify IP addresses for various Ethernet ports of the appliance. The Ethernet ports are named differently on the front panel of Citrix SD-WAN 1000 and 2000 appliances with Windows Server, in the Citrix SD-WAN instance, and in the Windows Server, as shown in the following table:

SD-WAN 1000WS	SD-WAN 2000WS	SD-WAN Instance	Windows Server
MGMT (Blue)	0/1 (LOM/PRI)	Primary	Citrix PV Ethernet Adapter #0: 0/1
AUX	0/2 (AUX)	Aux	Citrix PV Ethernet Adapter #1: 0/2
apA LAN1/WCCP (Green)	1/1	apA.1	N/A
apA WAN1	1/2	apA.2	N/A

SD-WAN 1000WS	SD-WAN 2000WS	SD-WAN Instance	Windows Server
apB LAN2	1/3	apB.1*	Double-click the Desktop icon nic_mapping.vbs to display the mapping**
apB WAN2	1/4	apB.2*	Double-click the Desktop icon nic_mapping.vbs to display the mapping**

* Available to the SD-WAN instance only in four-port mode.

** Available to the Windows Server only in two-port mode.

Supported Features

June 22, 2020

The following table lists various features supported on SD-WAN 1000 and 2000 appliances with Windows Server.

Features table for Citrix SD-WAN 1000 and 2000 with Windows Server Series Appliances

	Citrix SD-WAN 1000 with Windows Server series	Citrix SD-WAN 2000 with Windows Server series
AutoConfiguration	Y	Y
SD-WAN Plug-In	N	Y
Compression	Y	Y
RPC over HTTPS	Y	Y
SSL Compression	Y	Y
TCP Acceleration	Y	Y
Traffic Shaping	Y	Y
Video Caching	Y	Y

	Citrix SD-WAN 1000 with Windows Server series	Citrix SD-WAN 2000 with Windows Server series
Windows File System Acceleration	Y	Y
Windows Outlook Acceleration	Y	Y
XenApp/ XenDesktop Acceleration	Y	Y
Group Mode	Y	Y
High Availability Mode	Y	Y
Inline Mode	Y	Y
Virtual Inline Mode	Y	Y
WCCP Mode	Y	Y
VLANs	Y	Y

Summary of Hardware Specifications

May 23, 2019

The following tables summarize the specifications of the SD-WAN 1000 and 2000 with Windows Server hardware platforms.

H/W Specification	SD-WAN 1000 with Windows Server	SD-WAN 2000 with Windows Server
Windows Server version	Windows Server 2012 R2	Windows Server 2012 R2

Platform Performance

H/W Specification	SD-WAN 1000 with Windows Server	SD-WAN 2000 with Windows Server
Bandwidth	Up to 20 Mbps	Up to 50 Mbps
Maximum HDX sessions	Up to 100	300
Total sessions	10,000	20,000

H/W Specification	SD-WAN 1000 with Windows Server	SD-WAN 2000 with Windows Server
Acceleration Plug-in CCUs	N/A	750

Hardware Specifications

H/W Specification	SD-WAN 1000 with Windows Server	SD-WAN 2000 with Windows Server
Processor	4 Cores	4 Cores
Total disk space	1x300 GB SSD and 1x1 TB HDD	1 x 600 GB SSD and 1X1 TB HDD
SSD (dedicated Compression history)	123 GB for Disk-Based Compression (DBC); 25 GB for video caching	225 GB for Disk-Based Compression (DBC); 50 GB for video caching
RAM	32 GB	24 GB
Network Interfaces	2 pair with bypass 10/100/1000; 2 GigE ports for Management and AUX ports	4 x 10/100/1000 Base-T copper Ethernet; 2 GigE ports for Management and AUX ports
Power supplies	1	1

Physical Dimensions

H/W Specification	SD-WAN 1000 with Windows Server	SD-WAN 2000 with Windows Server
Rack Units	1U	1U
System width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
System depth	10" (25.4 cm)	25.4" (64.5 cm)
System weight	8.5 lbs (3.9 kg)	32 lbs (14.5 kg)
Shipping dimensions and weight	26 L x 18.5 W x 6.5" H; 14.5 lbs	32 L x 23.5 W x 7.5" H; 39 lbs

Environmental and Regulatory

H/W Specification	SD-WAN 1000 with Windows Server	SD-WAN 2000 with Windows Server
Voltage	100/240 VAC, 50-60 Hz	100/240 VAC, 50-60 Hz
Power consumption (Max.)	200 W	300 W
Operating Temperature (degree Celsius)	10–35	0-40
Non-operating Temperature (degree Celsius)	-40 – +70	-40 – +70
Allowed Relative Humidity	8% – 90% non-condensing	5%–95%
Safety certifications	CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)	CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)
Electromagnetic and susceptibility certifications	FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM	FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM
Environmental certifications	RoHS, WEEE	RoHS, WEEE

Citrix SD-WAN 4100 and 5100 WANOP Appliances

June 19, 2020

Citrix SD-WAN 4100,5100 WANOP appliances are high-performance WAN accelerators for busy datacenters. These appliances combine multiple virtual accelerator instances with a single virtual instance of the NetScaler load-balancer, providing the performance of multiple SD-WAN WANOP appliances in a single package.

Citrix SD-WAN 4100, 5100 WANOP WAN accelerators are the high end of the Citrix SD-WAN product line. They are designed to accelerate sites with WAN links with speeds more than 1 Gbps, especially busy datacenters that communicate with many branch and regional sites.

A single SD-WAN WANOP 4100, 5100 appliance can support WAN speeds of up to 2 Gbps and up to 5000 XenApp/XenDesktop users.

For datacenters needing even more performance, multiple SD-WAN WANOP 4100/5100 appliances can be deployed as a load-balanced array using the WCCP clustering feature.

Citrix SD-WAN WANOP 4100, 5100 is recommended at the hub of a hub-and-spoke deployment, where

smaller appliances are used at the spokes, whenever the link speed or the number of XenApp/Xen-Desktop users is higher than can be supported by a smaller appliance.

DC to DC Replication

If you require a secondary data center, SD-WAN WANOP 4000, 5000 appliances can provide optimization for Data-Center to Data-Center replication. This optimization improves replication time and reduces bandwidth consumption.

For details on how to configure an SD-WAN WANOP appliance for DC-to-DC replication with NetApp Snap Mirror, see http://support.citrix.com/article/CTX137181.

Architecture

June 25, 2020

Internally, the SD-WAN 4000/5000 appliance contains several virtual machines:

- A Xen hypervisor
- A NetScaler instance
- At least two accelerator instances
- A management server instance that manages the GUI and other tasks
- Internal networking

Figure 2. SD-WAN 4100/5100 virtual machines, internal networks, and external port usage (inline deployment shown)
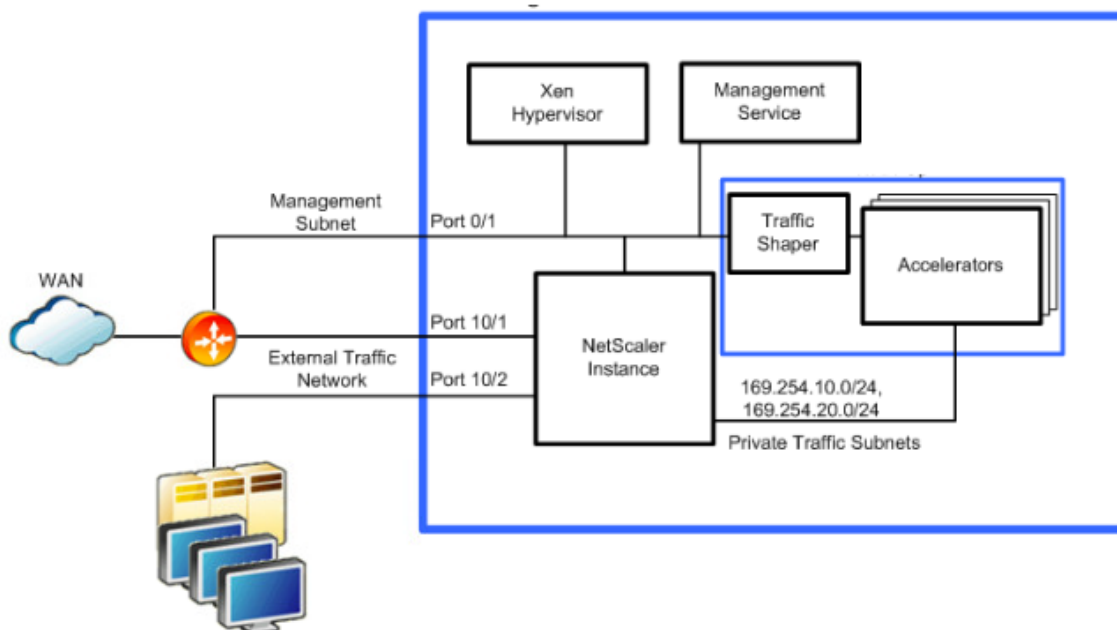
No WAN traffic enters or leaves the accelerators except as configured in the NetScaler instance. When the appliance is first used, the Provisioning Wizard sets up an initial configuration that provides communication and load balancing between the NetScaler instance and the accelerators.

The management service is the management configuration interface for the appliance, and provides access to key operating and monitoring elements of the appliance. The management service displays SD-WAN parameters as if they were from a single accelerator, and all changes made through this interface are applied to all the accelerator instances.

The Xen hypervisor hosts all the virtual machines. The hypervisor is not user-configurable and should not be accessed except at the request of Citrix.

Internal and External Networks

The external network interfaces are divided into two categories: traffic interfaces and management interfaces.

Traffic Interfaces—The traffic interfaces include all the network interfaces except ports 0/1 and 0/2, which are used only for management. Acceleration takes place only on the traffic interfaces.

> **Note**: You must keep the traffic interfaces isolated from the management interface to prevent ARP flapping and other problems. This isolation can be achieved physically or by tagging management interface and traffic interface packets with different VLANs.

Management subnet—The virtual machines connect directly to the external management subnet, with different IP addresses for the management service, NetScaler instance, and XenServer.

> **Note**: You must keep the traffic interfaces isolated from the management interface to prevent ARP flapping and other problems. This isolation can be achieved physically or by tagging management interface and traffic interface packets with different VLANs.

Private Internal traffic subnet—The accelerators' accelerated ports are connected to the NetScaler instance internally in a one-arm mode, using an internal traffic subnet. There is no direct connection between the instances' accelerated ports and the appliance's external ports. All accelerated traffic to the accelerators is controlled by the NetScaler instance.

Since this internal subnet is not accessible from outside the appliance, it uses non-routable subnets in the 169.254.0.0/16 range. The NetScaler instance provides NAT for features that require routable access to the accelerator. Only the following two features of the accelerators require IP addresses that can be reached from the outside world:

- The signaling IP address, used for secure peering and the SD-WAN Plugin.
- IP addresses, used for communication with the router when the WCCP protocol is used.

In both cases, the number of externally visible IP addresses is independent of the number of accelerators the appliance has.

The internal traffic subnet requires two IP addresses per accelerator, plus an address for the NetScaler, plus one or two WCCP VIP addresses if WCCP is used. Since the internal network is private, it has an abundance of address space for these tasks.

Data Flow on the Private Traffic Subnet—The one-arm connection between the NetScaler instance and the accelerators uses the SD-WAN virtual inline mode, in which the NetScaler instance routes packets to the accelerators and the accelerators route them back to the NetScaler instance. Traffic flow over this internal traffic subnet is identical regardless of whether the mode visible to the outside world (on the external interfaces) is inline, virtual inline, or WCCP.

This traffic requires the SD-WAN "Return to Ethernet Sender" option, and the NetScaler MAC Address Forwarding and Use Subnet IP options, which are enabled by the Provisioning Wizard.

Deployment Mode Summary: The differences between WCCP mode, inline mode, and virtual inline mode can be summarized as follows:

- WCCP mode is a one-arm configuration. The accelerators establish WCCP control channels with the router. In WCCP mode, only one or two accelerators manage the WCCP control channel on behalf of all the accelerators. Data traffic is load-balanced across all the accelerators. When GRE encapsulation is used, the NetScaler instance performs GRE encapsulation/decapsulation on the data stream between itself and the router, allowing the data between the NetScaler and the accelerators to use a decapsulated, Level-2 configuration.
- Inline mode operates much the same as WCCP mode internally, but externally the appliance emulates a bridge, and no WCCP control channel is established. A packet that enters the appliance on one bridge port exits through the other bridge port. SD-WAN 4000 and 5000 appliances

have multiple bridges to support multiple inline links.

- In virtual inline mode (used when WCCP and inline modes are not feasible), the appliance is deployed in a one-arm configuration, much like WCCP, but without the WCCP control channel. Traffic is sent to the appliance from the router, using policy-based routing (PBR) rules. The appliance processes the traffic and returns it to the router.

Figure 3. WCCP and virtual inline cabling

WCCP
Appliance
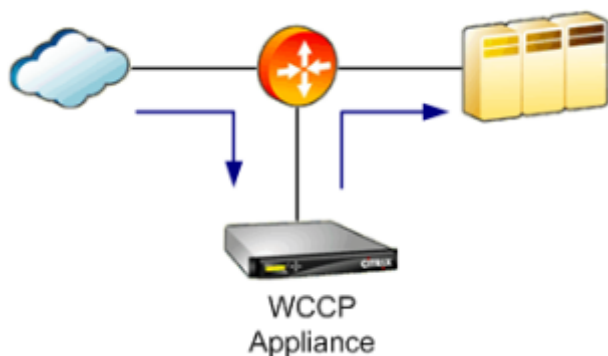
See SD-WAN 4100/5100 virtual machines, internal networks, and external port usage for a diagram of port usage on SD-WAN 4100/5100 appliances. Traffic ports are arranged as a set of accelerated bridges, while the management ports are independent. Typically only one management port is used.

Figure 4. Inline cabling

Inline
Appliance

Accelerated Bridges

SD-WAN 4100/5100 appliances have multiple accelerated bridges. Different models have different numbers and types of bridge ports. The two ports making up such a bridge are called an "accelerated pair." All current models include a built-in network bypass function. (Some older SD-WAN 4100-500 and 4100–1000 units do not include network bypass). The network bypass function (also called "fail to wire") connects pairs of ports together if the appliance fails as a result of either power loss or software failure (as determined by an internal watchdog timer).

Inline deployment. The bypass function allows SD-WAN 4100/5100 to be deployed in line with your WAN, typically between your LAN and your WAN router, without introducing a point of network failure.

The accelerated bridges support either 1 Gbps or 10 Gbps data rates. Ethernet and SFP+ interfaces are supported, depending on model.

One-arm deployment. One-arm deployments are also supported, using WCCP or virtual inline modes. With such deployments, an SD-WAN 4000/5000 traffic port is connected directly to a port on the WAN router. The other port on the bridged pair is left unconnected.

Performance considerations. Inline deployments provide higher performance than the one-arm deployments, because the use of two ports instead of one doubles the peak throughput of the interfaces.

Peak throughput is important with SD-WAN 4100/5100 appliances, because the compressor provides acceleration in proportion to the compression ratio. That is, a connection that achieves 100:1 compression transfers data 100 times faster than an uncompressed connection, as long as the rest of the network path can keep up.

For example, take a datacenter with a 500 Mbps WAN link and a 1 Gbps LAN. The small 2:1 speed ratio between the WAN and LAN allows compression to provide only a 2x speedup on a whole-link basis, because there is no way to get data onto or off of the LAN at speeds above 1 Gbps. A 10 Gbps LAN, which allows a tenfold increase in peak data rates, is recommended for use with SD-WAN 4100/5100 deployments.

When an SD-WAN 4100/5100 appliance is deployed in a one-arm mode, the peak transfer rate is cut in half. An SD-WAN 4100/5100 in one-arm mode, connected to the router with a 1 Gbps LAN interface, saturates this interface when the WAN is running at full speed in both directions. For good performance, SD-WAN 4100/5100 must have a LAN interface that is much faster than the WAN. When the appliance is connected directly to the router in a one-arm mode, use a 10 Gbps router port.

> **Note**
>
> The 10 Gbps ports support 10 Gbps only. They do not negotiate lower speeds. Use the 1 Gbps ports for 1 Gbps networks.

Other ports

An SD-WAN 4100/5100 appliance has atleast two non-accelerated ports. Port 0/1 is typically used for management, Port 0/2 is present but typically not used. A Light Out Management (LOM) port is also provided. An RS-232 port can be used for management.
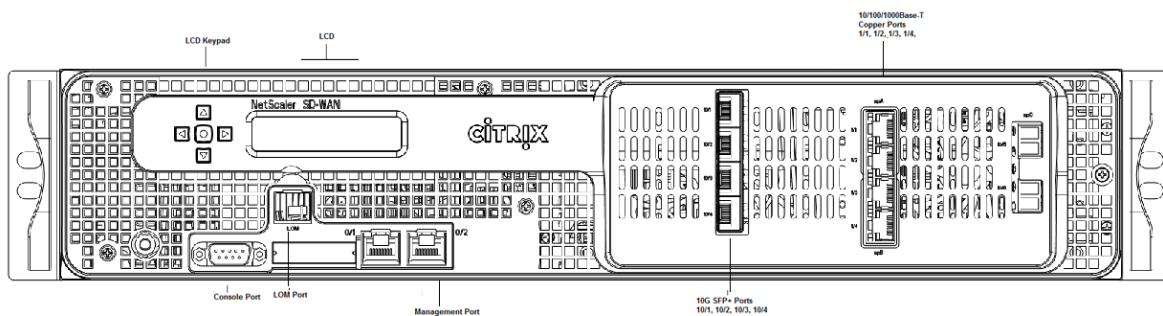
SD-WAN 4100 WANOP

June 19, 2020

Citrix SD-WAN 4100 WANOP are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory. The Citrix SD-WAN 4100 WANOP has a bandwidth of 310 Mbps, 500 Mbps, and 1 Gbps, respectively.

The following figure shows the front panel of the Citrix SD-WAN 4100 appliance.
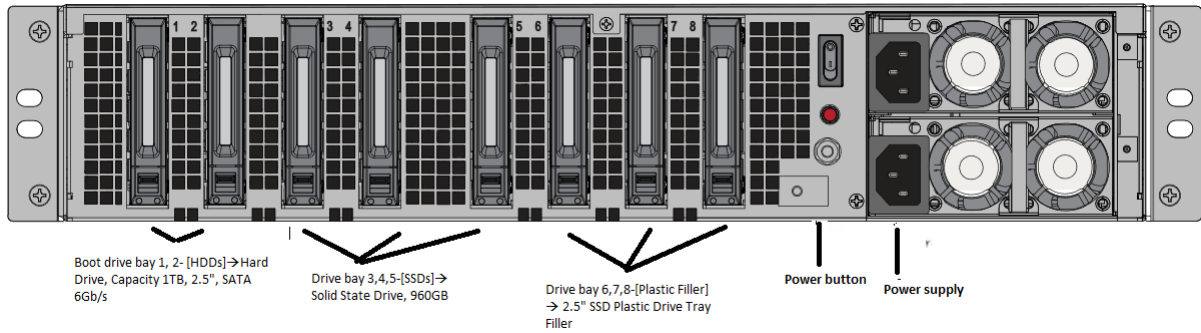
Figure 1.Citrix SD-WAN 4100, front panel

The Citrix SD-WAN 4100 WANOP appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- RS232 serial console port.
- Network Ports
    - 1x 2-port 10/1G Bypass
    - 1x 4-port 1G Bypass
    - 1x 4-port 10G/1G
    - 1x 2-port 10G (Hidden)

The following figure shows the back panel of the Citrix SD-WAN 4100 WANOP appliance.

Figure 2. Citrix SD-WAN 4100 WANOP back panel

The following components are visible on the back panel of the Citrix SD-WAN 4100 WANOP appliance:

- Four 800 GB removable solid-state drives, which store the appliance's compression history.
- Two 1 TB removable hard disk drives.
- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.

- Disable alarm button. This button is functional only when the appliance has two power sup-
plies. Press this button to stop the power alarm from sounding when you have plugged the ap-
pliance into only one power outlet or when one power supply is malfunctioning and you want
to continue operating the appliance until it is repaired.
- Two power supplies (either AC or DC). providing full hot swap redundancy.

SD-WAN 5100 WANOP

June 19, 2020

Citrix SD-WAN 5100 WANOP is a 2U appliance. Each model has 10-core processor with 2.80 GHz and
128 gigabytes (GB) of memory. The Citrix SD-WAN 5100 WANOP appliance has a bandwidth of 2 Gbps.

The following figure shows the front panel of the Citrix SD-WAN 5100 WANOP appliance.

Figure 1. Citrix SD-WAN 5100 WANOP, front panel
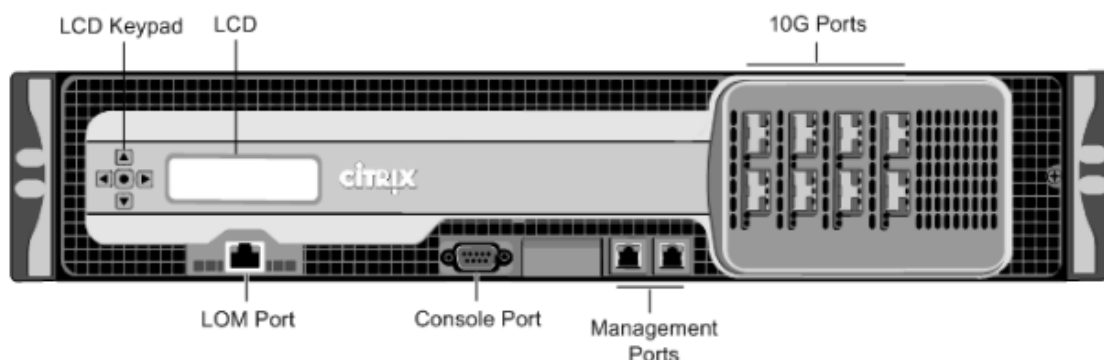
The Citrix SD-WAN 5100 WANOP appliance has the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to re-
motely monitor and manage the appliance independently of the appliance's software.
- RS232 serial console port.
- Ethernet ports:
    - Two 2-port 10/1G bypass, One 4-port 10G/1G, One 2-port 10G.

These ports are used to connect directly to the appliance for system administration functions.

The following figure shows the back panel of the Citrix SD-WAN 5100 WANOP appliance.

Figure 2. Citrix SD-WAN 5100 WANOP, back panel

Boot drive bay 1, 2- [HDDs]→Hard Drive, Capacity 1TB, 2.5", SATA 6Gb/s

Drive bay 3,4,5-[SSDs]→ Solid State Drive, 960GB

Drive bay 6,7,8-[Plastic Filler] → 2.5" SSD Plastic Drive Tray Filler

Power button   Power supply

The following components are visible on the back panel of the Citrix SD-WAN 5100 WANOP appliance:

- Six 800 GB removable solid-state drives, which store the appliance's compression history.
- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Two 1 TB removable hard disk drive.
- Disable alarm button. This button is functional only when the appliance has two power supplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Two power supplies (either AC or DC). providing full hot swap redundancy. Each power supply has an LED indicating its status.

Summary of Hardware Specifications

June 19, 2020

The following tables summarize the specifications of the Citrix SD-WAN 4100/5100 WANOP hardware platforms.

Specifications	4100 WANOP	5100 WANOP
Bandwidth	Up to 1 Gbps	Up to 2 Gbps
Regulatory model number	2U1P1B	2U1P1D
Processors	2 X 6 Core 2.60 GHz	2 X 10 Core 2.80 GHz
HDD	2x 1 TB HDD boot drives in RAID 1 (mirroring) mode	2x 1 TB HDD boot drives in RAID 1 (mirroring) mode
SSD	4x 800 GB	6x 800 GB
Memory	96 GB	128 GB

Specifications	4100 WANOP	5100 WANOP
Number of power supplies	2 power supplies providing full hot swap redundancy	2 power supplies providing full hot swap redundancy
AC power supply	100–240 V ac, 50 Hz to 60 Hz, 2 x 9.0 to 4.5A	100–240 V ac, 50 Hz to 60 Hz, 2 x 9.0 to 4.5A
DC power supply	-36 V dc to -72 V dc, 2 x 25.5 to 13.0A	-36 V dc to -72 V dc, 2 x 25.5 to 13.0A
Maximum AC power consumption	633 W	822 W
Maximum DC power consumption	712 W	895 W
Airflow (front to rear)	65 CFM, typical	65 CFM, typical
Heat Dissipation	137 W/FT 2/FT, typical	144 W/FT 2/FT, typical
Package weight (lbs.) Shipping dimensions and weight	62 lbs (28.1 kgs)	64 lbs (29.10 kgs)
Dimensions	36.5" x 24.5" by 11" (93 cm x 63 cm x 28 cm)	36.5" x 24.5" by 11" (93 cm x 63 cm x 28 cm)
System weight (lbs.)	45 lbs (20.4 kg)	47 lbs (27 kg)
Rack Units	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 SC48D rack 17.25" (44 cm)	EIA 310-D, IEC 60297, DIN 41494 SC48D rack 17.25" (44 cm)
Depth	28" (71.1 cm)	28" (71.1 cm)
Operating temperature	32–104 F (0–40 C)	32–104 F (0–40 C)
Non-operating temperature	14F to 140F (-10C to 60C)	14F to 140F (-10C to 60C)
Humidity range (non-condensing)	5%-95% non-condensing	5%-95% non-condensing
Safety certifications	IEC 60950-1, second Edition; CSA 60950-1, second Edition; UL 60950-1, second Edition; AS/NZS 6050-1	IEC 60950-1, second Edition; CSA 60950-1, second Edition; UL 60950-1, second Edition; AS/NZS 6050-1

Specifications	4100 WANOP	5100 WANOP
EMC & susceptibility	US (FCC (Part 15 Class A)); Europe (CE (EN55022/55024)); Australia (RCM), Japan (VCCI), Korea (KCC), Taiwan (BSMI), China (CCC), India (BIS), Russia (EAC), Saudi Arabia (CITC), Brazil (Anatel), South Africa (ICASA), Mexico (NOM), Egypt (NTRA), Israel (MoC)	US (FCC (Part 15 Class A)); Europe (CE (EN55022/55024)); Australia (RCM), Japan (VCCI), Korea (KCC), Taiwan (BSMI), China (CCC), India (BIS), Russia (EAC), Saudi Arabia (CITC), Brazil (Anatel), South Africa (ICASA), Mexico (NOM), Egypt (NTRA), Israel (MoC)
Environmental compliance	RoHS, REACH, WEEE	RoHS, REACH, WEEE

Lights Out Management Port of the SD-WAN WANOP 4100/5100 Appliance

May 23, 2019

The SD-WAN 4100/5100 appliances have an Intelligent Platform Management Interface (IPMI), also known as the Lights out Management (LOM), port on the front panel of the appliance. By using the LOM, you can remotely monitor and manage the appliance, independently of the SD-WAN 4100/5100 software. You can remotely change the IP address, perform different power operations, and obtain health monitoring information of the appliance by connecting to the appliance through the LOM port.

By connecting the LOM port over a dedicated channel that is separate from the data channel, you can make sure that connectivity to the appliance is maintained even if the data network is down.

Accessing the LOM Port by using a Web Browser

By using a web browser you can remotely log on to the LOM port to obtain information about the appliance and perform different operations on the appliance.

To access the LOM by using a web browser

1. In a web browser, type the IP address of the LOM port. For initial configuration, type the port's default address.
2. In the **User Name** box, type **nsroot**.
3. In the **Password** box, type **nsroot**.

Configuring the LOM Port

You can use the Intelligent Platform Management Interface (IPMI), also known as the Lights Out Management (LOM) port, to remotely monitor and manage the appliance, independently of the NetScaler software. For initial configuration of the lights-out management (LOM) port, connect to the port's default IP address and change it to the address that you want to use for remote monitoring and management. Also specify the administrator credentials and the network settings.

> **Note**: The LEDs on the LOM port are unoperational by design.

To configure the NetScaler LOM Port

1. Connect the LOM port to a management workstation or network.
2. In a web browser, type: http://192.168.1.3.

   > **Note**: The NetScaler LOM port is preconfigured with the IP address 192.168.1.3 and subnet mask 255.255.255.0.

3. In the **User Name** box, type **nsroot**.
4. In the **Password** box, type **nsroot**.
5. On the **Configuration** tab, click **Network** and type values for the following parameters:

   - IP Address—IP address of the LOM port.
   - Subnet Mask—Subnet mask used to define the subnet of the LOM port.
   - Default Gateway—IP address of the router that connects the LOM port to the network.

6. Click **Save**.

Power Cycling the appliance

You can remotely turn off the appliance and turn it back on. The result is similar to pressing the power button on the back panel of the appliance for less than two seconds.

To power cycle the appliance

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click **Remote Control**.
4. Under **Options**, click **Power Control**, and then click **Power Cycle System**.
5. Click **Perform Action**.

Accessing the appliance by using the Access Console

The LOM port allows you to remotely access and manage the appliance by logging on to a redirected console.

To access the appliance by using the access console

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click **Remote Control**.
4. Under **Options**, click Console Redirection.
5. Click **Launch Console**, and then click **Yes**.
6. Type the administrator credentials for the appliance.

Obtaining Health monitoring Information

You can log on to the LOM port to view the health information about the appliance. All system sensor information, such as system temperature, CPU temperature, status of fan and power supplies, appears on the sensor readings page.

To obtain health monitoring information

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click **System Health**.
4. Under **Options**, click **Sensor Readings**.

Power Control Operations using the LOM Port

You can remotely perform different power control operations, such as restarting the appliance, performing a graceful shutdown, and performing a forced shutdown, by using the LOM port.

To perform power control operations

1. In a web browser, log on to the LOM port by using the administrator credentials.
2. In the Menu bar, click **Remote Control**.
3. Under **Options**, click **Power Control**, and then select one of the following options:
   - **Reset System**—Restart the appliance.
   - **Power Off System – Immediate**—Disconnect power to the appliance without shutting down the appliance.
   - **Power On System**—Turn on the appliance.

- **Power Cycle System**—Turn off the appliance, and then turn it back on.
4. Click **Perform Action**.

Troubleshooting Tips

June 19, 2020

While most installations complete smoothly, some installations require knowledge of the appliance's internal structure or the use of little-known features before you can perform more monitoring and troubleshooting. These troubleshooting tips provide information and techniques that allow a more in-depth analysis of the appliance.

Understanding internal addresses

Some reports show addresses on the private subnets within the SD-WAN 4100/5100, so it's good to know what these addresses mean. These subnets connect the virtual machines together, without connecting to external ports.

All these addresses are on the local link subnet 169.254.0.0/16, described in RFC3927. This address space is segmented into three partly overlapping subnets: system management, private traffic, and accelerator management subnets.

Virtual machines in the SD-WAN 4100 and 5100. The system management subnet is not shown in this diagram. The traffic shaper manages traffic from all accelerators and is controlled via the accelerator GUI.
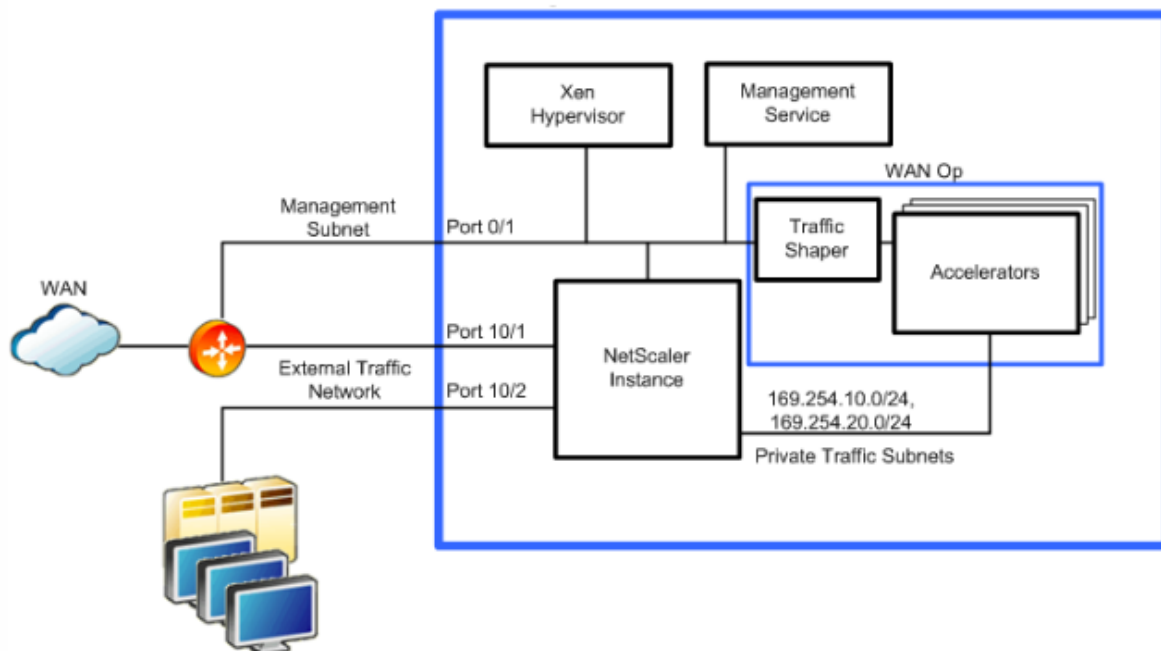
System management subnet

Function	Address
Management Service	169.254.0.10/16
NetScaler Instance	169.254.0.11/16
XenServer	169.254.0.1/16

Private traffic subnet

Function	Address
apA IP, accelerators 1–8	169.254.10.21/24 - 169.254.10.28/24
apA Signaling IP, accelerators 1–8	169.254.10.121/24 - 169.254.10.128/24
NetScaler Instance	169.254.10.11/24

Accelerator management subnet

Function	Address
Accelerator unified management IP (controls all accelerators)	169.254.0.20/24
Primary Port IP, accelerators 1–8	169.254.0.21/24 - 169.254.0.28/24

Checking and correcting accelerator instance status

Sometimes an error message may indicate an issue with one of the virtual machines in the appliance. To check their status, go to the System Configuration page and select an Instance view of either the SD-WAN or NetScaler subsystems. For example, the SD-WAN page.

- A fully active instance shows a green circle for VM State, Instance State, and Licensed.
- Your appliance may have more instances present than are licensed; ignore the unlicensed instances.
- If the VM State or Instance State of the remaining instances is not green, use the "Rediscover" action to attempt to bring these instances back into operation.

You can also get detailed information for each instance:

- Every instance should have a Status of "Inventory from SD-WAN Instance completed.
- Every instance should be running the same version of the software.
- Every instance should have the netmask (255.255.255.0) and gateway (169.254.0.20).
- Instances that show an uptime shorter than other instances have rebooted since the last whole-system reboot.

Logging into the NetScaler instance

Sometimes it is useful to log into the NetScaler instance to check its status or do configuration. You can log into the NetScaler instance from the **NetScaler Instances** page of the view, as shown in the following. Click the **IP Address** link.

You can also log into the NetScaler instance directly from your browser if you know its IP address on the management port (port 0/1).

Once logged in, you can see the NetScaler GUI, which identifies itself as NetScaler VPX at the top of the page.

This is the standard NetScaler user interface. Using monitoring features is safe. Configuration changes should be made with caution, as the SD-WAN 4100/5100 makes undocumented assumptions about how the NetScaler instance is configured.

Using ping and traceroute

The ping and traceroute utilities are not available on the accelerator instances, as they are on other SD-WAN products. Instead, you can use the equivalent features on the NetScaler instance, using the **Diagnostics** page as shown in the following illustration.

These features work over your external network and on the appliance's internal subnets.
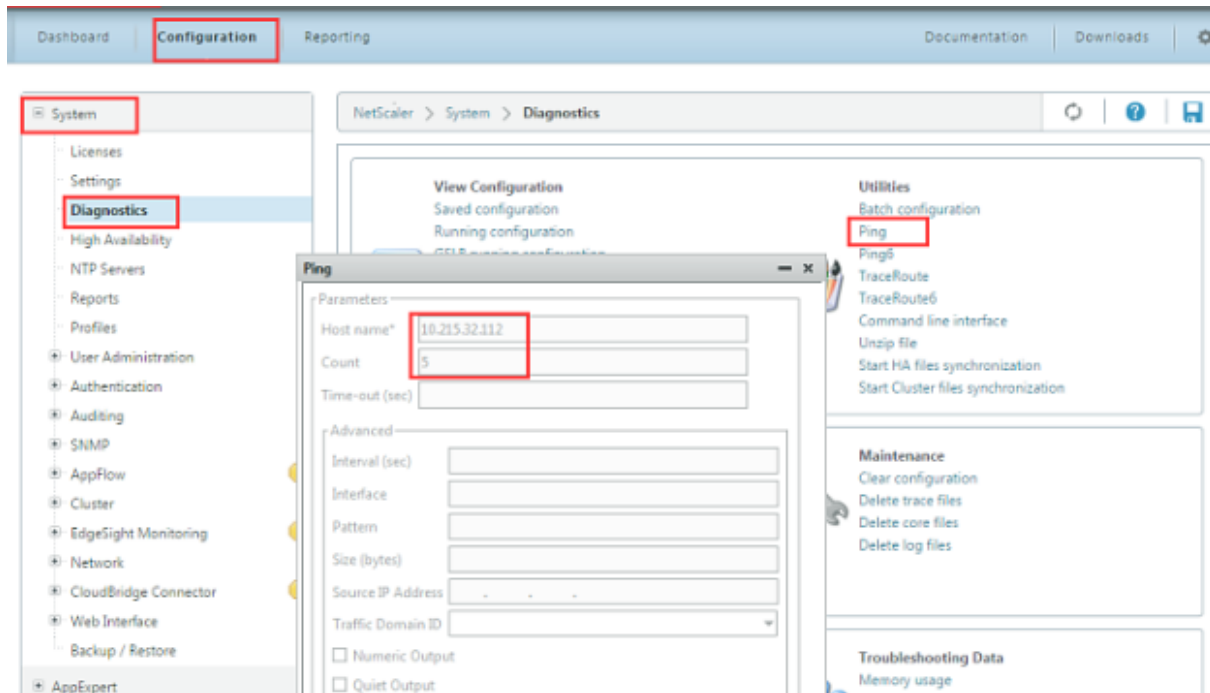
Using the system dashboard

Unlike the SD-WAN Dashboard, the System Dashboard page is devoted largely to hardware monitoring.

- The System Health tables show a status summary, with a Details link for expanded information in graphical form.
- The Events tables show a status summary, with a Show Events link to see the related log entries.
- If several ports are marked as Down, which is only an error if a cable is supposed to be present. Most appliances have several unused ports.
- Fail To Wire lists FTW Disabled for all ports. This means that the network bypassing feature is not enabled on this appliance. Examination of the FTW Events showed that there were no actual events, indicating that the feature is probably disabled.

For each warning or error, more details are available through the **Details links or Show Events** buttons.

Logging in to different instances via SSH

You can log into some of the virtual machines from the management port (port 0/1) using an ssh utility (such as PuTTY on Windows), logging in either as root or nsroot and using the administrative password. This gives you a shell prompt.

The most common use for logging on via SSH is to restore the IP address of an instance, typically the management service, that has become unreachable due to misconfigured network parameters. Otherwise, SSH is not recommended, as configuration changes can render the appliance unstable or unusable.

If neither of the two instances below are accessible over the network, you can log into the XenServer instance using the RS-232 port, which will give you a shell prompt.

Once logged into one of these virtual machines, you can use SSH from the shell prompt to reach the NetScaler instance or the accelerator at the appropriate 169.254.x.x address.

The usual UNIX/Linux commands are available, including the text editor.

Instance	Login	Password	Actual Username
Management Service	nsroot	Admin password	root
Management Service	root	Admin password	root
XenServer	nsroot	Admin password	nsroot
XenServer	root	Admin password	root

Monitoring individual accelerator instances

Logging into the accelerator GUI IP allows you to manage all the accelerator instances as a unit. Changes are automatically propagated to all the accelerator instances.

On rare occasions, you may wish to troubleshoot individual accelerator instances.

The login for the instances is admin. The password is the same admin password as is used on the other instances.

This is recommended for monitoring, not for making permanent changes, since any parameter you set in an instance may be overwritten later by the synchronization process. To do this, use the following URLs:

Accelerator Instance	URL
1	https://<accelerator_ip>:4001
2	https://<accelerator_ip>:4002

Accelerator Instance	URL
8	`https://<accelerator_ip>:4008`

Using individual elements of the update bundle

The update bundles distributed by Citrix are in a simple .tgz format (a tar archive compressed with gzip. It is sometimes useful to extract individual components from the archive, rather than going back to the Citrix Web site and downloading them individually. This is most commonly useful with the management service (build-svm*.tgz) or the accelerator release (orbital*.bin).

The update bundle is managed by tar/gzip or by archiving utilities like 7-zip.

Supported Features

May 23, 2019

Table 1. Features Table for Citrix SD-WAN 4100 and 5100 WANOP Series Appliances

Features	Citrix SD-WAN 4100 series	Citrix SD-WAN 5100 series
Auto Configuration	N	N
SD-WAN Connector	Y	Y
SD-WAN Plug-In	Y	Y
Compression	Y	Y
RPC over HTTPS	Y	Y
SSL Compression	Y	Y
TCP Acceleration	Y	Y
Traffic Shaping	Y	Y
Video Caching	N	N
Windows File System Acceleration	Y	Y
Windows Outlook Acceleration	Y	Y
XenApp/ XenDesktop Acceleration	Y	Y

Features	Citrix SD-WAN 4100 series	Citrix SD-WAN 5100 series
Group Mode	N	N
High Availability Mode	Y	Y
Inline Mode	Y	Y
Virtual Inline Mode	Y	Y
WCCP Mode	Y	Y
VLANs	Y	Y

Standard Edition

April 15, 2021

> **Important**
>
> The **NetScaler SD-WAN** product is rebranded to **Citrix SD-WAN**. All references to the term **NetScaler SD-WAN** are applicable to the new product term **Citrix SD-WAN**.

The Citrix SD-WAN Standard appliances include the following editions:

- SD-WAN Standard Edition 110
- SD-WAN Standard Edition 210
- SD-WAN Standard Edition 400, and 410
- SD-WAN Standard Edition 1000, 2000, and 2100
- SD-WAN Standard Edition 4000, 4100, and 5100
- SD-WAN Standard Edition 6100
- SD-WAN Standard Edition 1100

Installing the hardware

September 27, 2021

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you can use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.

Appliance physical installation instructions and precautions

- Place the appliance indoor along with its associated power connectors, power supply cables, and antennas. Do not expose the appliance and its associated components to external weather.

- Mount the appliance such that it does not vibrate. Use a rack or wall mount to minimize potential vibrations.

- Determine the placement of each component in the rack before you install the rack.

- Install the equipment near an electrical outlet for easy access.

- Mount the appliance with sufficient air ventilation. Do not run the appliance at a location that does not meet the environment specifications. For details on operating temperature, and other environment specifications, see the Citrix SD-WAN Data Sheet.

- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Most appliances can be installed in standard server racks that conform to EIA-310-D specification. The appliances ship with a set of rails, which you must install before you mount the appliance. The only tools that you need for installing an appliance are a Phillips screwdriver and a flathead screwdriver.

Warning: If you are installing the appliance as the only unit in the rack, mount it at the bottom. If the rack contains other units, make sure that the heaviest unit is at the bottom. If the rack has stabilizing devices available, install them before mounting the appliance.

Your appliance requires one or two rack units depending on the height of the appliance.

Cautions

- Electrostatic discharge (ESD) can damage your equipment.
- Do not place any objects on the appliance.
- Do not cover vent holes on the side of the appliance.
- Metal surface of the appliance can get heated up.
- Use caution when touching the metal surface of the appliance.

Electrical safety precautions

During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been designed as electrical insulators.
- Ensure that the power supply cords include grounding plugs and are plugged into grounded electrical outlets.
- Ensure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload.
- A reliable ground must be maintained always. Therefore, the rack should be grounded. Pay particular attention to power supply connections other than the direct connection to the branch circuit (for example, connections to power strips).

Warning

There is a risk of Explosion, if the battery is replaced with an incorrect battery type.

Desktop mount

Citrix SD-WAN appliances can be desktop mounted using the rubber feet shipped in the appliance package.

Rack mount the appliance

The rackmount chassis of for SD-WAN appliances fits a standard rack and takes 1U of racking height. The appliance can be placed on any flat surface, or mounted in any standard rack unit with the provided rack-mount brackets and screws.

To install the appliance into a rack:

1. Ensure that the appliance is placed on a stable surface before rack-mount installation.
2. Attach the provided rack-mount brackets to the sides of the appliance using the provided bracket screws.
    - If you are installing the appliance into a four-post rack, attach the rack-mount brackets with the handles aligned with the front of the appliance.
    - If you are installing the appliance into a two-post rack, attach the rack-mount brackets with the handles aligned with the middle of the appliance.
3. Position the appliance in the rack. Ensure there is enough room around the device to allow for sufficient air flow.
4. Line up the rack-mount bracket holes to the holes on the rack and ensure that the SD-WAN 1100-SE and PE appliance are level.
5. Finger tighten four rack-mount screws to attach the appliance to the rack.

6. Tighten the rack-mount screws with an appropriate screwdriver.

7. Plug the provided power cable.

Rack mount the appliance:

Rack mounted with primary and
secondary (optional) adapters
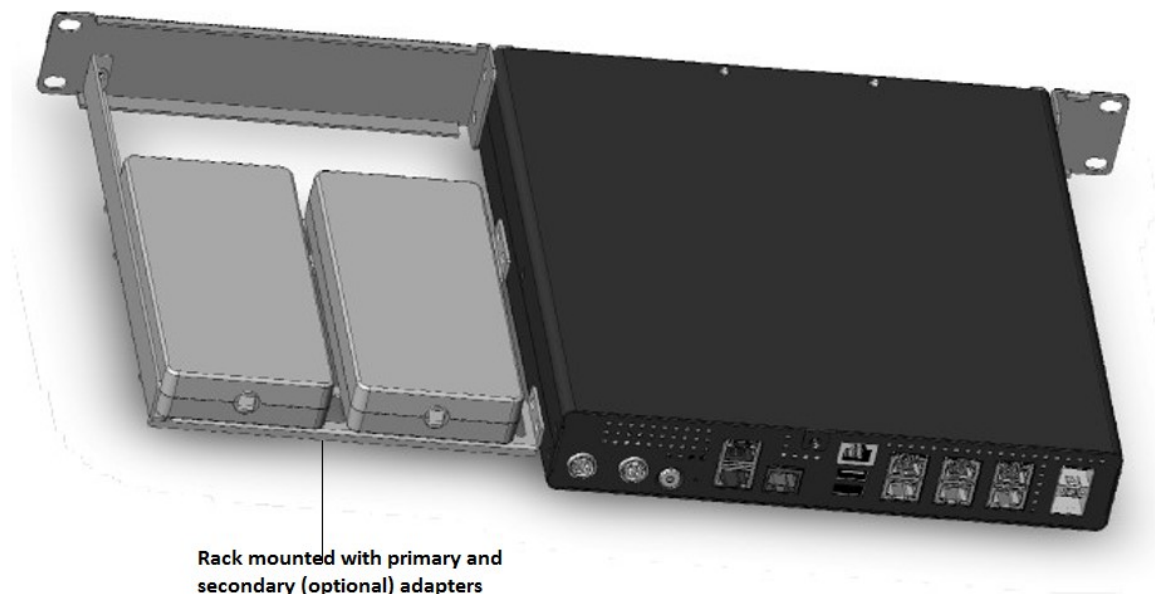
Connecting the appliance to a power source

The number of power cables shipped with an appliance depends on the number of power supplies on the appliance. Appliances that come with two power cables can also operate if only one power cable is connected. Appliances that come with four power cables can also operate if only two power cables are connected. A separate ground cable might not be required, because the three-prong plug provides grounding.

1. Connect the power cable to one of the inlet receptacles on the back of the appliance, and connect the other end of the power cable to a power outlet.

2. If your appliance has more than one power supply, repeat this process. The additional power supply is a redundant, hot-swappable power supply.

3. The Citrix SD-WAN appliance boots up.

Connecting the appliance to the network

1. Verify that the appliance is connected through a console or Ethernet port. This ensures that you can configure the appliance after it is switched on.

2. Press the ON/OFF toggle power switch on the back panel of the appliance.

Connect the interfaces on the appliance to the network ports on the appropriate switches by using Ethernet or fiber optic cables. Connecting multiple network ports to the same switch or VLAN can result in a network loop.

Setting up the appliance

1. If you are configuring the appliance using Zero Touch Deployment (ZTD), refer to the following link on the docs.citrix.com site; Zero Touch Deployment

2. If you are configuring a hardware SD-WAN appliance, physically connect the appliance to a PC. Refer to the following link on the docs.citrix.com site; configuring SD-WAN hardware

To set up your Citrix SD-WAN appliance hardware, do the following:

1. Set up the chassis.

    - Citrix SD-WAN appliances are installed in a standard rack. For desktop installation, place the chassis on a flat surface. Ensure that there is a minimum of 2 inches of clearance at the sides and back of the appliance for proper ventilation.

2. Connect the Power.

    - Ensure that the power switch is set to off.
    - Plug the power cord into the appliance and an AC outlet.
    - Press the power button on the front of the appliance.

3. Connect the appliance Management Port to a PC. Connect the appliance to a PC in preparation for completing the next procedure, setting the Management IP address for the appliance.

    Note: Before you connect the appliance, ensure the Ethernet port is enabled on the PC. Use an Ethernet cable to connect the SD-WAN Appliance Management Port to the default Ethernet port on a PC.

To configure the management IP address for a hardware SD-WAN appliance, do the following:

Note: Repeat the following process for each hardware appliance you want to add to your network.

1. If you are configuring a hardware SD-WAN appliance, physically connect the appliance to a PC.

    - If you have not already done so, connect one end of an Ethernet cable to the Management Port on the appliance, and the other end to the default Ethernet port on the PC.

    Note: Ensure that the Ethernet port is enabled on the PC you are using to connect to the appliance.

2. Record the current Ethernet port settings for the PC you are going to use to set the appliance management IP address. Change the Ethernet port settings on the PC before you can set the appliance management IP address. Record the original settings so you can restore them after configuring the management IP address.

---

3. Change the IP address for the PC. On the PC, open your network interface settings and change the IP address for your PC to the following: 192.168.100.50

4. Change the **Subnet Mask** setting on your PC to the following: 255.255.0.0

5. On the PC, open a browser and enter the default IP address for the appliance. Enter the following IP address in the address line of the browser: 192.168.100.1

   Note: Use Google Chrome browser when connecting to an SD-WAN appliance. Ignore any browser certificate warnings for the Management Web Interface.

The **SD-WAN management web interface login** screen on the connected appliance is displayed.

1. Enter the administrator user name and password, and click **Login**. After you log into the management web interface, the Dashboard page appears.

   - Default administrator user name: `admin`<!--NeedCopy-->
   - Default administrator password: `password`<!--NeedCopy-->

   Note

   Change the default password. Record the password in a secure location, as password recovery might require a configuration reset.

Install Fiber Patch Cable in Ports 10/3 and 10/4

Through release 9.3, on an appliance, SD-WAN ports 10/3 and 10/4 must be connected with the provided cable, as shown in the following figure.

Note

Fiber patch cable for 10/3 and 10/4 port is applicable only to the 4000 and 5000 WANOP series appliances.

Starting with release 9.3, the patch cable is no longer required, and can be omitted if:

- The appliance was shipped from the factory with release 9.3 or later, or
- The appliance was shipped from the factory with release 9.3 or earlier, but you upgrade it to later version and change the default loopback in the management service (on **System > Configuration > System > Configure Loopback Settings**).

If you decide to eliminate the need to use loopback cable, the ports 10/3 and 10/4 are still reserved. These ports are not available for WAN optimization.

To install the patch cable

1. Connect the LC-to-LC cable to the ports as shown in the figures above.
2. Insert one end of the cable into port 10/3.
3. Insert the other end of the cable into port 10/4.

Citrix SD-WAN 110 Standard Edition Appliances

September 8, 2021

The Citrix SD-WAN 110 SE platform is a branch side appliance that can be deployed in micro and small branch offices/ remote sites/ home offices / retail stores, and temporary worksites. A single box-in-branch solution helps to reduce the hardware footprint and eases branch deployment.

The Citrix SD-WAN 110-SE appliance is a desktop form factor appliance. This appliance has 2-core processor with 4 GB memory and 32 GB of storage (SATA-DOM drive).

The Citrix Compliance Regulatory models are:

- SD-WAN 110
- SD-WAN 110-LTE-WiFi
- SD-WAN 110-WiFi

For more information, see the following:

- Citrix SD-WAN platform data sheet
- Citrix SD-WAN 110 SE Quick Start Guide: ZTD via the WAN Interface
- Citrix SD-WAN 110 LTE Wi-Fi Quick Start Guide: ZTD via the LTE Interface
- Citrix SD-WAN 110 LTE Wi-Fi Unboxing and Installation
- Citrix SD-WAN 110 LTE Wi-Fi Compliance
- Citrix SD-WAN 110 Wi-Fi Compliance

Note

The 110-SE appliance cannot be configured as an MCN.

To log in to the SD-WAN 110 SE management web interface, use the following credentials.

- **Default administrator user name**: admin

- **Default administrator password**: The Serial Number of the appliance, found at the bottom of the appliance chassis.

  Note

  On a first time login, you are requested to change the default password to a password of your choice.

Citrix SD-WAN 11.1.0 is the minimum software version required for Citrix SD-WAN 110-SE appliance. Citrix SD-WAN 11.3.0 is the minimum software version that supports Wi-Fi capabilities for Citrix SD-WAN 110-LTE-WiFi and Citrix SD-WAN 110-WiFi-SE model.

LED	Description
Ethernet Copper Ports LED	Active/Link: **Green**
	Speed 1000: **Orange**
	Speed 100: **Green**
	Speed 10: **off**
Power LEDs	Power on: **Solid Green**
	Power off: **Solid Blue**
	Factory Reset: **Flashing blue and green (alternatively)**
	Software power cycle: **Flashing green for ~15 seconds (shutdown time) and then flashing blue for ~25 seconds and then solid green**

Note

Port 1/1 is the default LAN port and port 1/2 is the default WAN port. Port 1/3 is disabled. The default LAN IP on port is 192.168.101.1, it also runs a default DHCP server that provides LAN clients with IP address pool starting from 192.168.0.50 to 192.168.0.250.

Port Labels	Type	Description
1/1, 1/2, and 1/3	Traffic	The data ports are used to carry network traffic.

Port Labels	Type	Description
1/4	Management port	The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of the appliance. From Citrix SD-WAN version 11.1.1 and above you can use the port 1/4 as a data port or a management port per the configuration. For more information, see Configurable Management or Data port.
USB	2 USB ports	USB ports
Serial	RJ-45/RS-232	An RS232 serial console port.
Power	Power button	**Power OFF state**: Press the power button and release it immediately: Power on the appliance.
		Press the power button and hold it for 10+ seconds: Factory resets the appliance. The appliance takes around 7 min for a factory reset.
		Power ON state: Press the power button and release it immediately: Orderly shut down the appliance.
		Press the power button and hold it for 5+ seconds: Force shut down the appliance.
DC 12 V	DC Power Supply	Refer System Specifications for power supply information.

Citrix SD-WAN 110-LTE-WiFi-SE

The Citrix SD-WAN 110-LTE-WiFi-SE platform is a branch side appliance that can be deployed in micro and small branch offices/Remote sites/ retail stores, and temporary worksites. A single box-in-branch solution helps to reduce the hardware footprint and eases branch deployment.

The Citrix SD-WAN 110-LTE-WiFi-SE appliance is a desktop form factor appliance. This appliance has 2-core processor with 4 GB memory and 32 GB of storage (SATA-DOM drive).

> **Note**
>
> - The Citrix SD-WAN 110-LTE-WiFi-SE appliance cannot be configured as an MCN.
>
> - As of March 10,2020, the appliance is shipped as **Wi-Fi Ready**. The Wi-Fi access point functionality can be used with Citrix SD-WAN software version 11.3.0 or higher.
>
> - The Citrix SD-WAN 110-LTE-WiFi-SE appliance can be configured as an access point using SD-WAN Orchestrator. For more details, see Wi-Fi Access Point.

The following figure shows the front panel of the 110-LTE-WiFi-SE appliance.

LED	Description
Ethernet Copper Ports LED	Active/Link: **Green**
	Speed: 1000 **Orange**
	Speed 100: **Green**
	Speed 10: off
Power LEDs	Power on: **Solid Green**
	Power off: **Solid Blue**
	Factory Reset: **Flashing blue and green (alternatively)**
	Software power cycle: **Flashing green for ~15 seconds (shutdown time) and then flashing blue for ~25 seconds and then solid green**

Citrix SD-WAN Platforms

LED	Description
Wi-Fi	OFF: Not using Wi-Fi
	Flashing green: Wi-Fi is configured but not in use
	Solid green: Wi-Fi is actively used
LTE	OFF: **No signal**
	1 bar: **Poor**
	2 bar: **Fair**
	3 bar: **Good**
	4 bar: **Excellent**
SIM Card Slots	Two Mini (2FF) size SIM slots. Use an adapter to use Micro (3FF) and Nano (4FF) size SIMs. Snap the smaller SIM into the adapter. Order the adapter as an FRU.
	Note: At any given time, only one SIM is active. Power ON the appliance and then insert the SIM card.
LTE	LTE antenna male connector

Note

Port 1/1 is the default LAN port and port 1/2 is the default WAN port. Port 1/3 is disabled. The default LAN IP on port 1/1 is 192.168.101.1, it also runs a default DHCP server that provides LAN clients with IP address pool starting from 192.168.0.50 to 192.168.0.250. For LTE appliances, the LTE SIM slot is also the default WAN port. The WAN ports are configured as DHCP clients.

Port Labels	Type	Description
LTE	Antenna male connector	Connector for LTE antenna.
1/1, 1/2, and 1/3	Data ports	The data ports are used to carry Network traffic.

Port Labels	Type	Description
1/4	Management port	The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of the appliance. From Citrix SD-WAN version 11.1.1 and above you can use the port 1/4 as a data port or a management port per the configuration. For more information, see Configurable Management or Data port.
USB	2 USB ports	USB 2.0 ports
Serial	RJ-45/RS-232	An RS232 serial console port
Power	Power button	**Power OFF state**: Press the power button and release it immediately: Power on the appliance
		Press the power button and hold it for 10+ seconds: Factory resets the appliance. The appliance takes around 7 min for a factory reset.
		Power ON state: Press the power button and release it immediately: Orderly shut down the appliance.
		Press power button and hold it for 5+ seconds: Force shut down the appliance.
DC 12 V	DC Power Supply	Refer System Specifications for the power supply information.

Citrix SD-WAN 110-WiFi-SE

The Citrix SD-WAN 110-WiFi-SE platform is a branch side appliance that can be deployed in micro and small branch offices/Remote sites/ retail stores, and temporary worksites. It is a single box in branch solution that helps to reduce hardware foot print and eases branch deployment.

The Citrix SD-WAN 110-WiFi-SE appliance is a desktop form factor appliance. This appliance has 2-core processor with 4 GB memory and 32 GB of storage (SATA-DOM drive).

Note

- The Citrix SD-WAN 110-WiFi-SE appliance cannot be configured as an MCN.
- The Citrix SD-WAN 110-WiFi-SE appliance can be configured as an access point using SD-WAN Orchestrator. For more details, see Wi-Fi Access Point.

LED	Description
Ethernet Copper Ports LED	Active/Link: **Green**
	Speed: 1000 **Orange**
	Speed 100: **Green**
	Speed 10: off
Power LEDs	Power on: **Solid Green**
	Power off: **Solid Blue**
	Factory Reset: **Flashing blue and green (alternatively)**
	Software power cycle: **Flashing green for ~15 seconds (shutdown time) and then flashing blue for ~25 seconds and then solid green**
Wi-Fi	OFF: Not using Wi-Fi
	Flashing green: Wi-Fi is configured but not in use

LED	Description
	Solid green: Wi-Fi is actively used
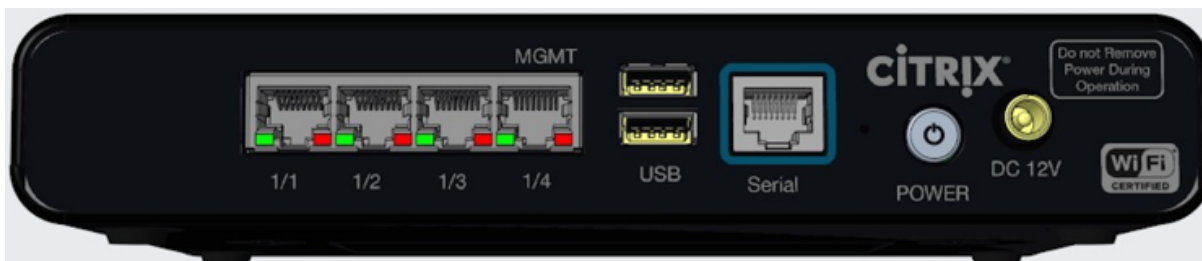
Note

Port 1/1 is the default LAN port and port 1/2 is the default WAN port. Port 1/3 is disabled. The default LAN IP is 192.168.101.1. The WAN port is configured as a DHCP client.

Port Labels	Type	Description
1/1, 1/2, and 1/3	Data ports	The data ports are used to carry Network traffic.
1/4	Management port	The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of the appliance. From Citrix SD-WAN version 11.1.1 and above you can use the port 1/4 as a data port or a management port per the configuration. For more information, see Configurable Management or Data port.
USB	2 USB ports	USB 2.0 ports
Serial	RJ-45/RS-232	An RS232 serial console port
Power	Power button	**Power OFF state**: Press the power button and release it immediately: Power on the appliance

Port Labels	Type	Description
		Press the power button and hold it for 10+ seconds: Factory resets the appliance. The appliance takes around 7 min for a factory reset.
		Power ON state: Press the power button and release it immediately: Orderly shut down the appliance.
		Press power button and hold it for 5+ seconds: Force shut down the appliance.
DC 12 V	DC Power Supply	Refer System Specifications for power supply information.

Mounting the SD-WAN 110 SE appliance

The Citrix SD-WAN 110-SE appliance can be installed in the following installation modes:

- Desk placement
- Wall mount
- Rack mount

Desk placement

The Citrix SD-WAN 110-SE appliance can be placed on a desk using the rubber feet shipped in the appliance package. You can also fix a plastic stand to the side of the appliance, and place it vertically. The front view and the rear view of the appliance are shown below.

Temperature specifications and recommended placement

The Citrix SD-WAN 110 appliance supports desk placement, wall mount, and rack mount. Citrix recommends a vertical placement of the appliance through the stands or through wall mounting, especially in environments that lack air conditioning and good airflow. If placed horizontally, the underside of the appliance may become hot.

The Citrix SD-WAN 110 appliance and its compliance regulatory models are designed to work in home and office environments where the ambient temperature does not exceed 40 degrees C, and where

air flow is not restricted (as it would be in an enclosure without fan cooling). Above 40 degrees C, the appliance may not work as expected. For more information, see Citrix SD-WAN data sheet.

Wall mount

The Citrix SD-WAN 110-SE appliance can be wall mounted by placing and adjusting the appliance screw slots on the wall screws.
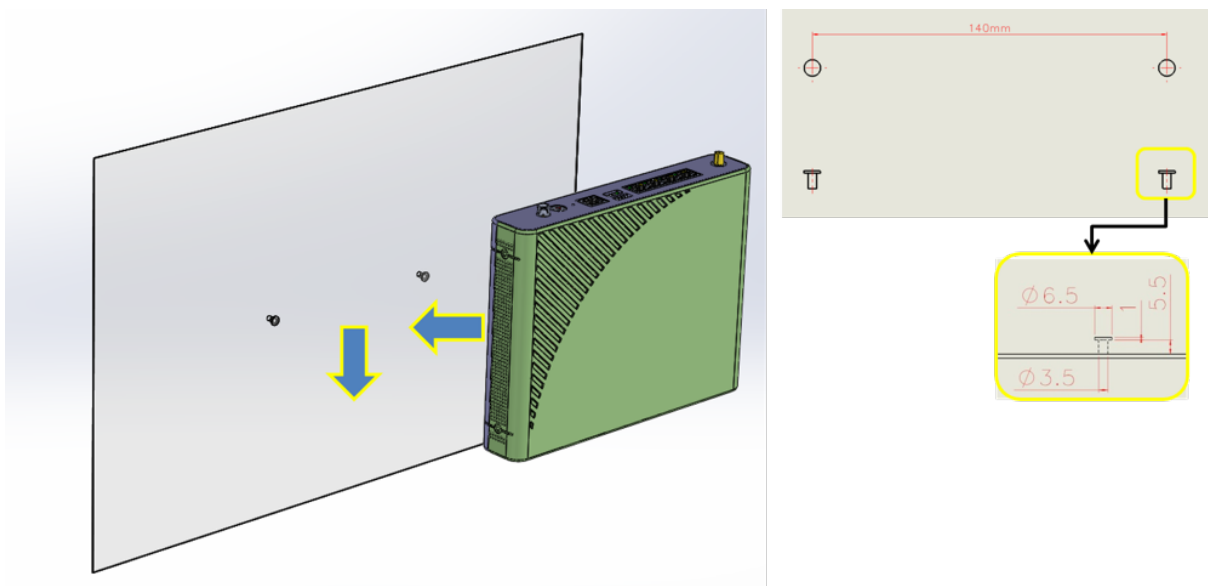
Use two wall mount screws with the following dimensions:

- Screw Length: 12 mm
- Screw out of wall: 5.5 mm
- Screw head: ⌀6.0 mm ~ ⌀7.5 mm
- Screw body: 3.5 mm
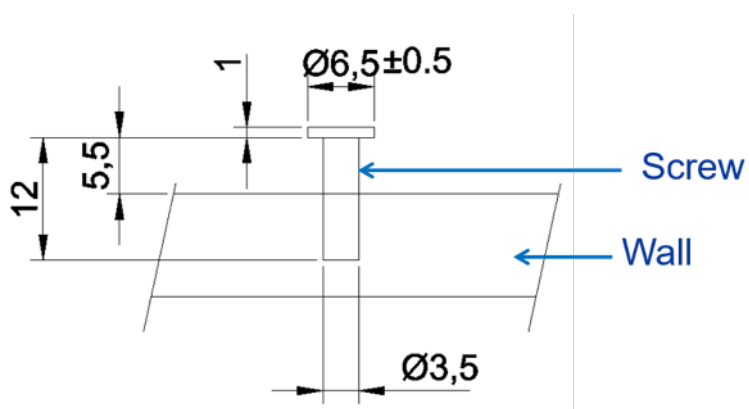
Rack mount

1. Fix the shelf to the rack with the provided screws.

2. Install the chassis. Place the appliance screw slots on the positioning screws on the shelf and slide it, to lock it into position.
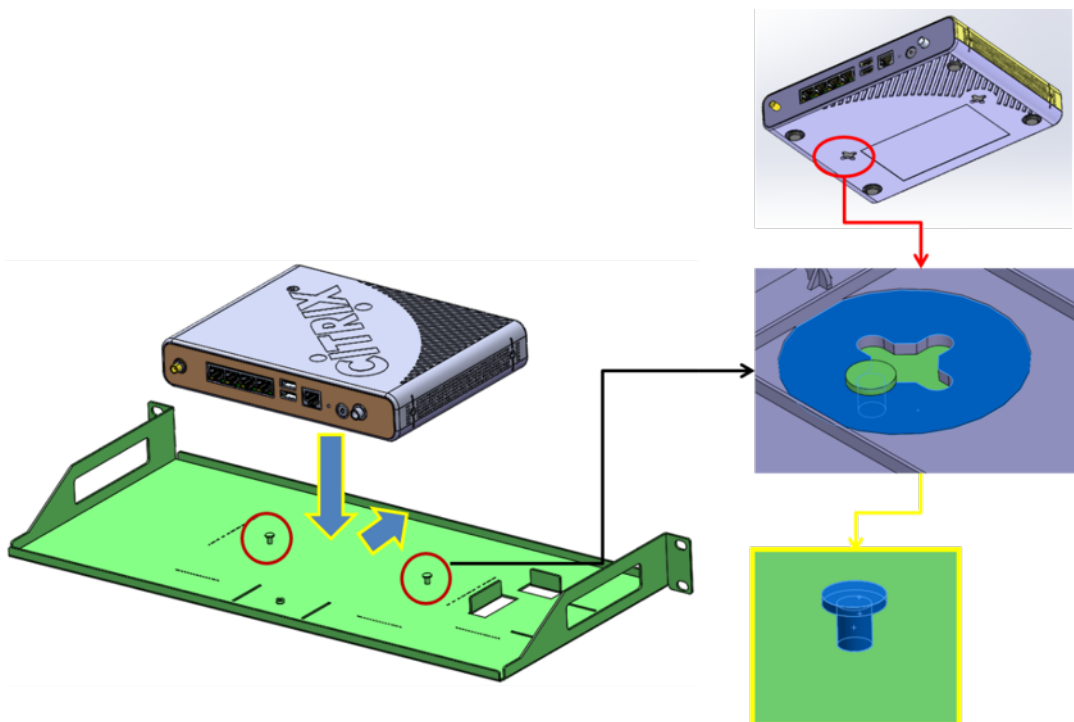
3. Install the chassis fix bracket to hold the appliance in position. Place the chassis fix bracket on the slot and fix it with a screw.
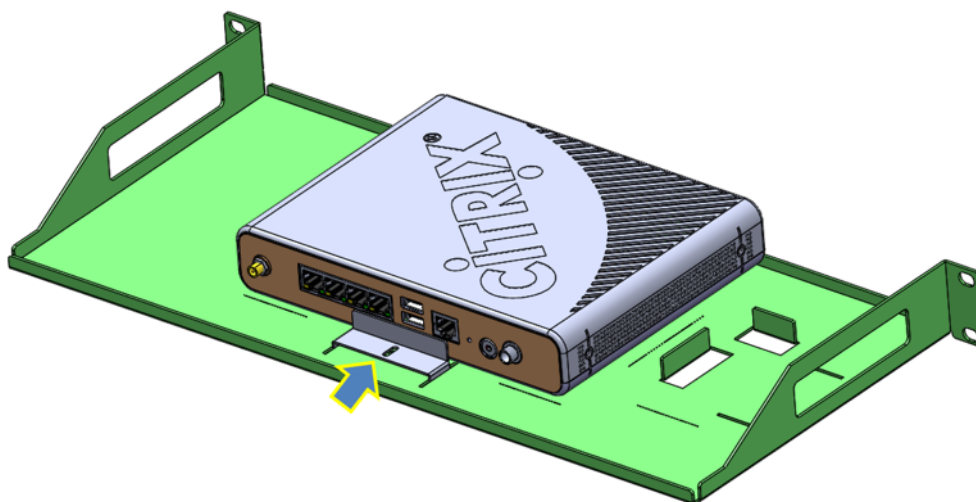
4. Install the power adapter. Place the power adapter on the adapter slot.
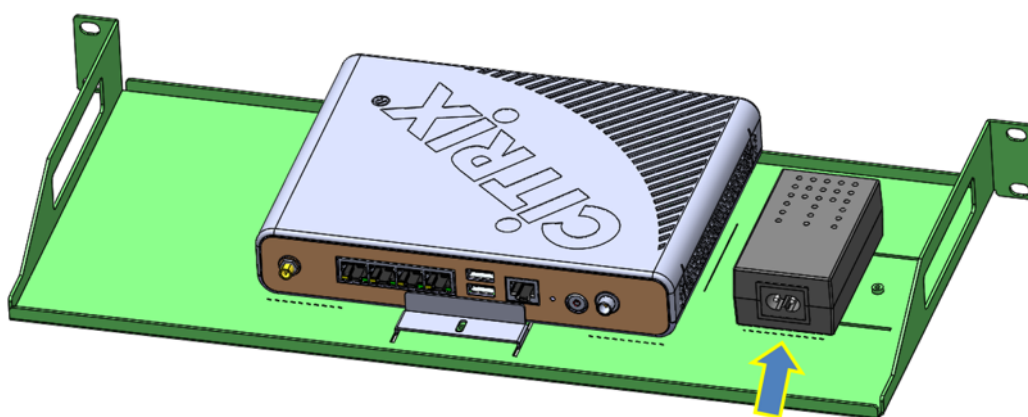
5. Install the adapter fix bracket to hold the power adapter in position. Place the adapter fix bracket on the slot and fix it with a screw.
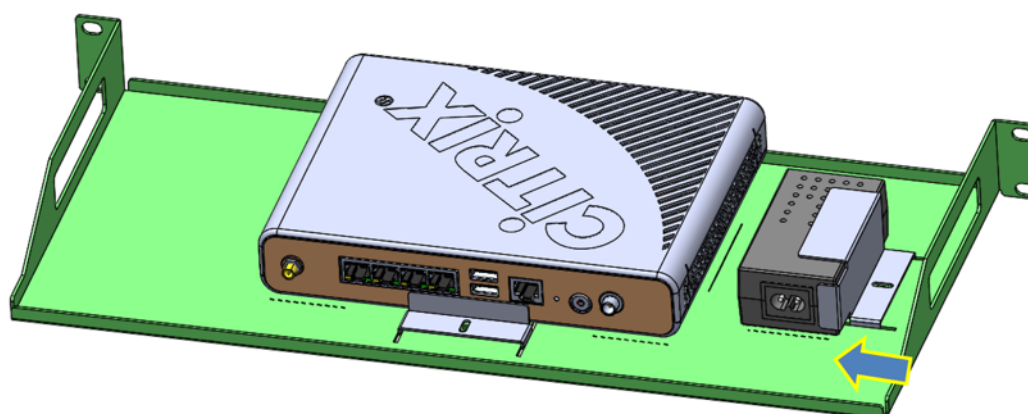
Installing the LTE antennas

To use the Citrix SD-WAN 110-LTE-WiFi-SE appliance as an LTE modem, install the antennas to the appliance. The antennas are included in the appliance package. The Citrix SD-WAN 110-LTE-WiFi-SE appliance has two SMA coax male connectors at the front and rear of the appliances. The antennas have independent rotating SMA female connectors.

Note

Ensure that both the LTE antennas are installed for better LTE cellular connectivity.

To install the antennas to the appliance:

1. Place the antenna SMA coax connector (F) on the appliance SMA coax connector (M) and rotate the antenna connector clockwise, until the connector is tight.

   Note

   The recommended torque is 0.20–0.28 newton meters (N m)
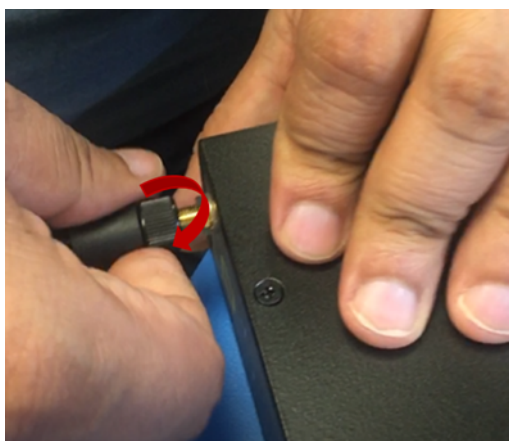
---

2. Adjust the antenna orientation and direction.

3. Similarly connect the other antenna to the rear SMA coax connector (M) of the appliance.

For more information on configuring the LTE functionality using the GUI and CLI, see Configure LTE functionality on 110 SE LTE appliance.

Summary of hardware specifications

Specifications	110-SE, 110-LTE-WiFi-SE, and 110-WiFi-SE
Regulatory Model Number	SD-WAN 110, SD-WAN 110-LTE-WiFi, SD-WAN 110-WiFi
Memory	4 GB
Non-Volatile Storage	32 GB

Specifications	110-SE, 110-LTE-WiFi-SE, and 110-WiFi-SE
LTE	3G, 4G. For Citrix SD-WAN 110-LTE-WiFi-SE appliance only.
LAN Ports	4x GbE RJ45
USB 2.0	2
SIM Slot	X2 2FF. Adaptors for 3FF and 4FF to be ordered as an FRU. For Citrix SD-WAN 110-LTE-WiFi-SE appliance only.
LTE Module	Quectel EG25-G. For Citrix SD-WAN 110-LTE-WiFi-SE appliance only.
Power Supply Ratings	
Power Supplies	Single (External)
Input Voltage / Frequency Ranges (normal)	100–240 VAC, 50–60 Hz
Input Current	0.6 A
Wattage (max)	24 W
Appliance Ratings	
Input Voltage	12 VDC
Input current	2.0 A
Wattage (typical)	10 W
Wattage (max)	15.5 W
Thermal Dissipation	
Airflow (front to rear)	n/a: fan-less
Typical Heat Dissipation	34BTU
Max Heat Dissipation	53BTU
Mechanical	
Package Weight (kg)	0.9 kg
Package Dimensions	38.5 cm L x 25.4 cm W x 9.01 cm H
System Weight (kg)	0.62 kg
System Dimensions	21.59 cm L x 15.87 cm W x 3.81 cm H
Environmental and Regulatory	
Operating Temperature	0–40 degree C

Specifications	110-SE, 110-LTE-WiFi-SE, and 110-WiFi-SE
Humidity Range	5–90%, Non-condensing
Industry Standards	GCF, PTCRB, Wi-Fi CERTIFIED™
Safety Certifications	CB, UL
Regulatory Compliance	CE, FCC, ISED (IC), RCM, VCCI & MIC, Anatel, BTK, BSMI & NCC (Taiwan), CITC, CCC, ENACOM, ICASA, IFT, SRRC, WPC, DWLFM & TRA (Bahrain), TRA (UAE), SUBTEL, SDPPI, CAK, MCINET, NCC (Nigeria), CRA
Environmental Compliance	RoHS 3, WEEE, REACH

EG25-G TX (Transmit) output power (dBm) for Quectel EG25-G (LTE)

Frequency	Maximum Value (in dBm)
WCDMA B1/B2/B4/B5/B6/B8/B19	24+1/-3dB
LTE-FDD B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28	23+/-2dB
LTE-TDD B38/B39/B40/B41	23+/-2dB

EG25-G RX receiving sensitivity (dBm) for Quectel EG25-G (LTE)

Frequency	Primary (in dBm)
WCDMA B1	-108.2
WCDMA B2	-109.5
WCDMA B4	-108.5
WCDMA B5	-109.2
WCDMA B6	-109
WCDMA B8	-109.5
WCDMA B19	-109
LTE-FDD B1 (10M)	-97.3
LTE-FDD B2 (10M)	-98

Frequency	Primary (in dBm)
LTE-FDD B3 (10M)	-97.5
LTE-FDD B4 (10M)	-97.8
LTE-FDD B5 (10M)	-98
LTE-FDD B7 (10M)	-97.3
LTE-FDD B8 (10M)	-98
LTE-FDD B12 (10M)	-98
LTE-FDD B13 (10M)	-98
LTE-FDD B18 (10M)	-98
LTE-FDD B19 (10M)	-98
LTE-FDD B20 (10M)	-98
LTE-FDD B25 (10M)	-98
LTE-FDD B26 (10M)	-98
LTE-FDD B28 (10M)	-98.1

Antenna gain for Quectel EG25-G (LTE)

Ethertronics LTE antenna 1004112-C003			
Part No. 1004112 - Broadband External LTE / Cellular antenna			
Frequency	690–960	1710–2220	2500–2700
Peak Gain	1.18 dBi	4.5 dBi	4.0 dBi

Wireless WAN (LTE) Specifications

Specifications	110-SE and 110-LTE-WiFi-SE
Modem	Quectel EG25-G
Geography	Global

Specifications	110-SE and 110-LTE-WiFi-SE
LTE Category	Cat4 (Theoretical 150 Mbps DL; 50 Mbps UL)
Carrier Aggregation	No
SIM Slots	2 (only 1 active)
LTE Bands	B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28/
Output Power	Class 3 (23 dBm±2 dB)
Theoretical Speeds	150 Mbps downlink/50Mbps uplink

Wireless LAN (Wi-Fi) Specifications

Wi-Fi capabilities		110-WiFi-SE and 110-LTE-WiFi	Antenna peak gain
Wi-Fi standards		802.11 a/b/g/n/ac	
Frequency bands*		2412 MHz, 2417 MHz, 2422 MHz, 2427 MHz, 2432 MHz, 2437 MHz, 2442 MHz, 2447 MHz, 2452 MHz, 2457 MHz, 2462 MHz, 2467 MHz, 2472 MHz	2.6 dBi
	Channel width: 20 MHz	5180 MHz, 5200 MHz, 5220 MHz, 5240 MHz, 5745 MHz, 5765 MHz, 5785 MHz, 5805 MHz, 5825 MHz	5.0 dBi
	Channel width: 40 MHz	5190 MHz, 5230 MHz, 5755 MHz, 5795 MHz	5.0 dBi
	Channel width: 20 MHz	5180 MHz, 5200 MHz, 5220 MHz, 5240 MHz, 5745 MHz, 5765 MHz, 5785 MHz, 5805 MHz, 5825 MHz	5.0 dBi
	Channel width: 80 MHz	5210 MHz, 5775 MHz	5.0 dBi

Wi-Fi capabilities	110-WiFi-SE and 110-LTE-WiFi	Antenna peak gain
Max simultaneous SSIDs	4	

*- Some frequency bands/channels and channel widths are not available for some countries, depending on the supported bands per country. Output power of the device is configured to operate within the regulatory limit set by the host country/domain.

The Wi-Fi CERTIFIED™ Logo is a certification mark of Wi-Fi Alliance®.

Troubleshooting Citrix SD-WAN 110 SE network issue

The Citrix SD-WAN 110 SE appliance fails to establish network connectivity under the following conditions.

- Appliance is managed by SD-WAN Orchestrator and/or brought up by zero touch deployment (ZTD).
- Appliance is in factory state and ZTD/SD-WAN Orchestrator agents are not installed.
- Appliance time (CMOS or hardware) is ahead of the actual time.
- Appliance time is set backwards by the NTP daemon before download/installation of the ZTD/SD-WAN Orchestrator agents.

Workaround

After initial installation (or after resetting the unit to its original factory configuration), the end-user installing SD-WAN 110 must verify that the appliance is successfully connected to the organizational network. The end-user must be provided with organization-specific instructions along with the appliance (for example, dial tone on the VoIP phone) to verify network connectivity. If the appliance does not connect to the network, the end-user can follow the instructions provided below:

1. Leave the appliance powered on and wait for 30 minutes or longer.
2. Briefly but firmly press the Power button (1–2 seconds) to shut it down.
3. After the lights on the appliance go dark, press the Power button again to turn the appliance back on. The SD-WAN 110 appliance now restarts and connects to the network.

Citrix SD-WAN 210 Standard Edition Appliances

October 6, 2021

The Citrix SD-WAN 210-SE appliance is a 1U appliance for use in small branch offices. This appliance has 2-core processor with 4 GB memory and 64 GB of storage.

The Citrix Compliance Regulatory models are:

- SD-WAN 210-SE (non-LTE) - NS-SDW-210
- SD-WAN 210-SE LTE - NS-SDW-210-LTE-R1, NS-SDW-210-LTE-R2, NS-SDW-210-LTE-RC

For more information, see the Citrix SD-WAN platform data sheet.

> **Note**
>
> - You can configure Citrix SD-WAN 210-SE and Citrix SD-WAN 210-SE LTE as an MCN only in the SD-WAN Orchestrator managed networks.
> - You can configure the Citrix SD-WAN 210-SE appliance using the new user interface. For more information, see User interface for SD-WAN appliances. Provisioning the Citrix SD-WAN 210-SE as an MCN, redirects you to the legacy user interface.

The following figure shows the front panel of the 210 SE appliance.

Figure 1. SD-WAN 210-SE front panel

LED	Description
Ethernet Copper Ports LED	Active/Link: **Green**
	Speed 1000: **Orange**
	Speed 100: **Green**
	Speed 10: **off**
SIM Card Slot	Two Mini (2FF) size SIM slots. Use an adapter to use Micro (3FF) and Nano (4FF) size SIMs. Snap the smaller SIM into the adapter. Order the adapter as an FRU.

LED	Description
	Note: At any given time, only one SIM is active. Power ON the appliance and then insert the SIM card.
Bypass LEDs	Normal Mode: **Green**
	Bypass Mode: **Orange**
Ethernet Fiber Ports	Active/Link: **Green**
	Speed: 1000: **Orange**
Power LEDs	Power on: **Green**
	Power off: **off**

Figure 2. SD-WAN 210 SE back panel
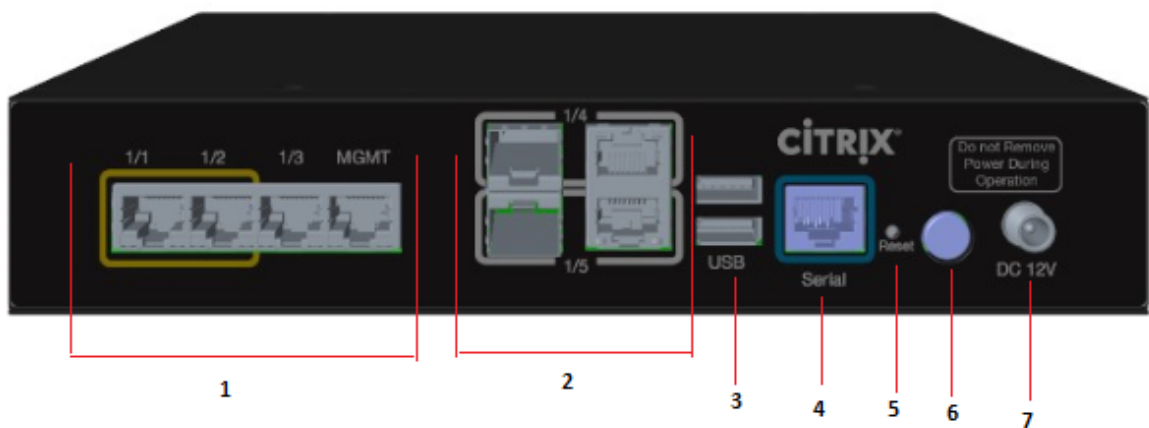
The following components are visible on the back panel of the 210 SE appliance:

Interface	Port Labels	Type	Description
1	1/1 and 1/2	Bypass/FTW	Fail-to-Wire
	1/3	Traffic	Network traffic

Interface	Port Labels	Type	Description
	Management	RJ-45	A copper Ethernet (RJ45) management port. The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of Virtual WAN.
2	1/4 and 1/5	SFP and Ethernet (combination ports)	Used as a combination of SFP and Ethernet one each on the top and bottom. Supported speeds: 100 Mbps and 1000 Mbps.
3	USB	2	USB ports
4	Console	RS-232 serial	An RS232 serial console port.
5	Reset	Reset button	Consult Citrix technical support for more information.
6	Power	Power button	Power button to power on or off the appliance. Press the switch for five seconds to switch off the power.
7	Power Supply	DC Power Supply	Single power adapter. Power rating: 40 W, voltage: 12 V, and current: 3.33 A.

Citrix SD-WAN 210-SE LTE

The 210 SE LTE appliance is a 1U appliance. This appliance has 2-core processor with 4 GB memory and 64 GB of storage.

The following figure shows the front panel of the 210 SE LTE appliance.

Figure 3. 210 SE (LTE) front panel with antenna
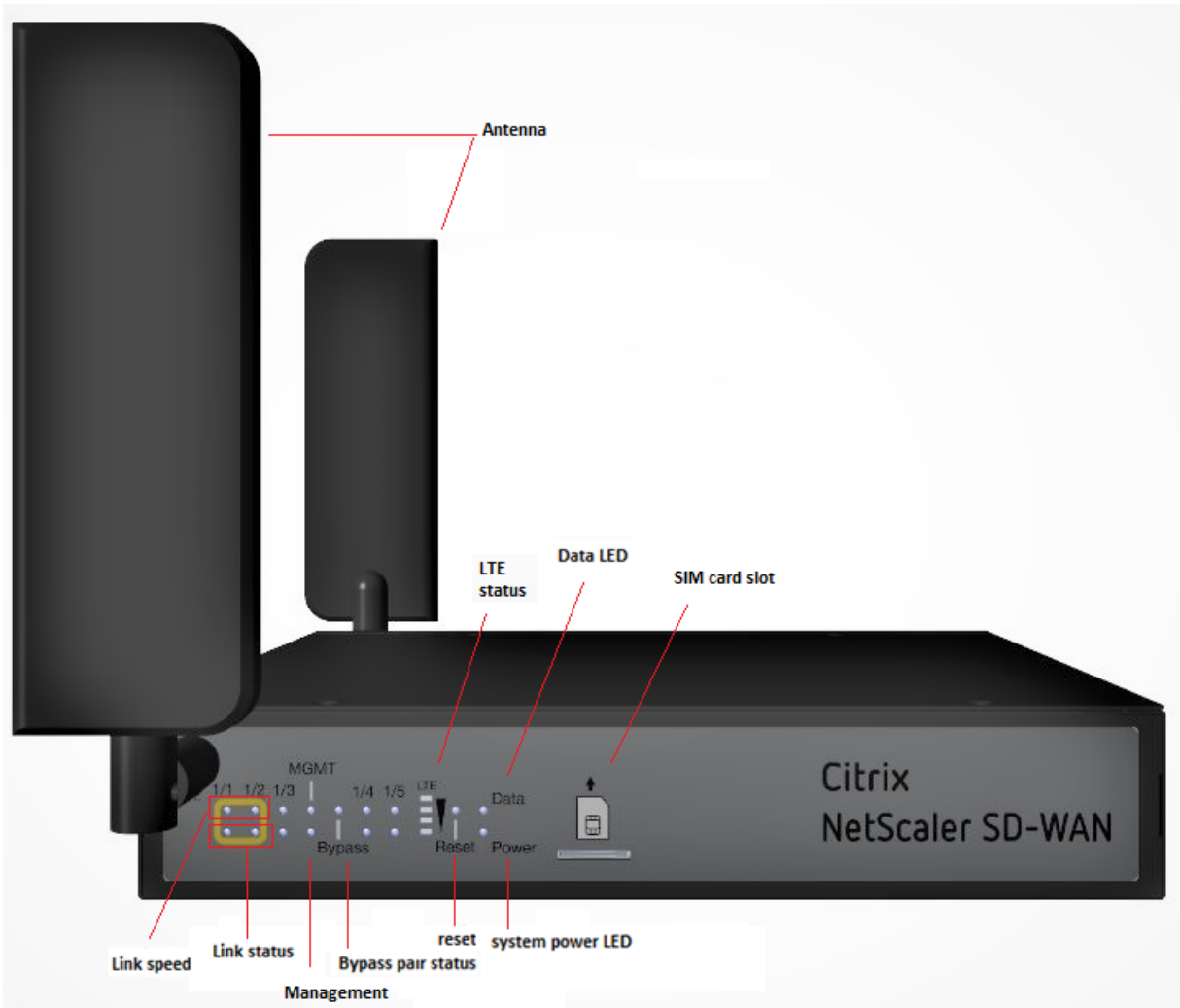
LED	Description
Ethernet Copper Ports LED	Active/Link: **Green**
	Speed: 1000 **Orange**
	Speed 100: **Green**
	Speed 10: off

LED	Description
Bypass LEDs	Normal Mode: **Green**
	Bypass Mode: **Orange**
Ethernet Fiber Ports	Active/Link: **Green**
	Speed: 1000: Orange**
System and Data LEDs	Sys: Power on: **Green**
	Sys: Power off: off
	Data access storage: Blue

Figure 4. 210 SE (LTE) back panel with antenna

The following components are visible on the back panel of the 210 SE LTE appliance:

Interface	Port Labels	Type	Description
1	1/1 and 1/2	Bypass/FTW	FTW ports
	1/3	Traffic	Traffic port
	Management	RJ-45	A copper Ethernet (RJ45) management port. The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of Virtual WAN.
2	1/4 and 1/5	SFP and Ethernet (combination ports)	Used as a combination of SFP and Ethernet one each on the top and bottom.
3	USB	2	USB ports
4	Console	RS-232 serial	An RS232 serial console port
5	Reset	Reset button	Consult Citrix technical support for more information.
6	Power	Power button	Power button to power on or off the appliance. Press the switch for five seconds to switch off the power.
7	Power supply	DC Power supply	Single power adapter. Power rating: 40 W, voltage: 12 V, and current: 3.33 A.

Interface	Port Labels	Type	Description
8	Antenna connectors	Male connectors	Connectors for antenna
9	Two antennas	LTE antennas	Antennas shipped with the appliance.

Installing the LTE antennas

To use the Citrix SD-WAN 210 SE LTE appliance as an LTE modem, install the antennas to the appliance. The antennas are included in the appliance package. The 210 SE LTE appliance has two SMA coax male connectors at the front and rear of the appliances. The antennas have independent rotating SMA female connectors.

> **Note**
>
> Ensure that both the LTE antennas are installed for better LTE cellular connectivity.

To install the antennas to the appliance:

1. Place the antenna SMA coax connector (F) on the appliance SMA coax connector (M) and rotate the antenna connector clockwise, until the connector is tight.

   > **Note**
   >
   > The recommended torque is 1.8–2.5 Lbs force-inch.

2. Adjust the antenna orientation and direction.

3. Similarly connect the other antenna to the rear SMA coax connector (M) of the appliance.

For more information on configuring the LTE functionality using the GUI and CLI, see Configure LTE functionality on 210 SE LTE appliance.

Citrix SD-WAN 210 platform support for MiRiC-E1T1 FE/GBE SFP

The following two types of MiRiC SFPs are supported on the 210 appliance for SFP ports 1/5 and 1/6.

1. MiRiC-E1T1 FE SFPs.
2. MiRiC-E1T1 GBE SFPs.

MiRiC-E1T1 FE SFPs must configure with speed as 100 Mbps and duplex as full. MiRiC-E1T1 GBE SFPs must configure with speed as 1 Gbps and duplex as full.

To configure, go to SD-WAN appliance GUI, navigate to **Configuration > Network Adapters > Ethernet page**.
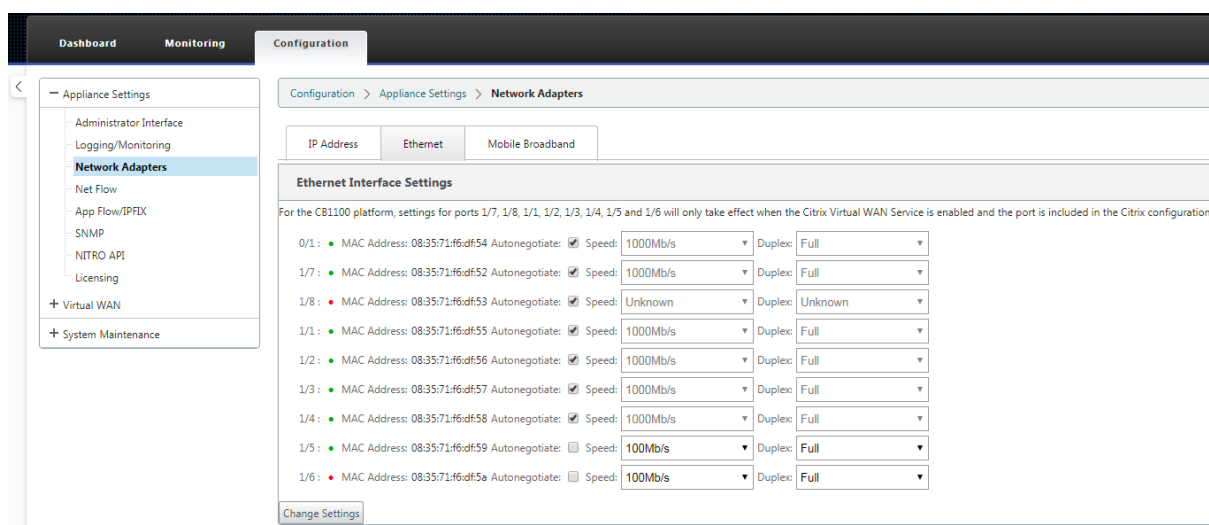
Access MiRiC SFP web service

1. The SFP transceivers have a default management IP address of 192.168.205.1, which can be used for the SFP web service to configure relevant configurations, for example; T1 or E1. The IP address can be modified other than 192.168.205.1. However ensure that you avoid IP address conflicts.

2. To enable SFP access to the management:

   - Log into the appliance CLI via **ssh admin@(ip address)**

   - Run: sfp_access

   - To enable access on 1/5, run one of the following commands.

     – enable 1/5 # Works for GBE transceivers only if already configured.
     – enable 1/5 100 # - Works only for FE transceivers
     – enable 1/5 1000 # - Works only for GBE transceivers
     – enable 1/5 100 172.217.43.2 # - For FE transceivers and assumes a user changes the default IP to an IP in 172.217.43.0/24

   - enable 1/5 1000 172.217.43.2 # - For GBE transceivers and assumes a user changes the default IP to an IP in 172.217.43.0/24

     > **Note:**
     >
     > Enabling management access on 1/5 automatically disables management access on 1/6, and conversely.

   - To disable access to the management:

     – Log in appliance CLI via ssh admin@(IP address)
     – Run: sfp_access

- Run: disable

- To show the status:

    - Log in appliance CLI via ssh admin@(IP address)
    - Run: sfp_access
    - Run: status

- Ensure that you disable the management access once configuration is done.

- When the appliance is rebooted, the management access is disabled automatically.

- When virtual service is restarted, the management access remains configured until enable or disable operation is done.

- When the appliance is disabled, the management access to the SFPs is lost.

- When the appliance is re-enabled, the management access is regained.

3. To configure E1 or T1 type for SFP transceiver:

    - The client machine must be in the same IP subnet as the appliance management subnet.
    - The client machine must have a route to the subnet of SFP transceiver IP address, 192.168.205.0/24, with the appliance management IP as the gateway.
    - Open a browser and visit SFP transceiver management
    - Default user name: su
    - Default password: 1234
    - To configure Interface Type (E1 or T1), navigate to **Configuration > Physical Ports** and choose **E1 or T1** from the drop down menu, and click **Save** button.

Summary of hardware specifications

January 24, 2021

Specifications	210-SE and 210-SE LTE
Regulatory Model Number	NS-SDW-210, NS-SDW-210-LTE-R1, NS-SDW-210-LTE-R2
Processors	Intel C3338
Memory	4 GB DDR4 PC4-2400 SODIMM
Number of Power Adapters	1
AC Power Supply (adapter) Voltage, Frequency and Current	115–230 V 50–60 Hz 1.5A

Specifications	210-SE and 210-SE LTE
Maximum AC Power Consumption	18.9 W
Maximum DC Power Consumption	13.2 W
Airflow (front to rear)	Fan-less
Heat Dissipation	45.0384 BTU
Package Weight (lbs.)	5 lbs
System Weight (lbs.)	2.9 lb
Width	175 mm
Height	42 mm
Depth	232 mm
Operating Temperature	0–40°C
Humidity Range (non-condensing)	5% to 90% RH
Safety Certifications	UL
Regulatory Certifications	FCC, CE
Environmental Compliance	RoHS/REACH/PFOS/CoM/WEEE
Safety Certifications	c UL us listed
LTE Advanced Module (CAT6)	Sierra Wireless™ EM7455, Sierra Wireless™ EM7430, Taoglas TG.30.8113 (Theoretical 300 Mbps DL; 50 Mbps UL with DUAL carrier aggregation)
LTE Advanced Bands (CAT6)	1, 2, 3, 4, 5, 7, 8, 12, 13, 20, 25, 26, 29, 30, 41; 1, 3, 5, 7, 8, 18, 19, 21, 28, 38, 39, 40, 41
Regulatory Compliance	FCC, IC, CE, ICASA, ENACOM, IFETEL, ANATEL, RCM, BIS
Industry Certifications	PTCRB, GCF

RX Receiving Sensitivity (dBm) for Sierra Wireless™ EM7455, Sierra Wireless™ EM7430

LTE Bands	AirPrime EM7455 (SD-WAN-210-LTE-R1)	LTE Bands	AirPrime EM7430 (SD-WAN-210-LTE-R2)
Band 1	-97.5	Band 1	-97.5
Band 2	-97.0	Band 3	-97.1

LTE Bands	AirPrime EM7455 (SD-WAN-210-LTE-R1)	LTE Bands	AirPrime EM7430 (SD-WAN-210-LTE-R2)
Band 3	-97.0	Band 5	-99.3
Band 4	-97.5	Band 7	-96.4
Band 5	-98.5	Band 8	-99.3
Band 7	-96.5	Band 18	-98.9
Band 8	-99.0	Band 19	-99.3
Band 12	-97.5	Band 21	-98.2
Band 13	-97.0	Band 28	-97.3
Band 20	-98.5	Band 38	-97.2
Band 25	-97.0	Band 39	-98.4
Band 26	-98.5	Band 40	-96.0
Band 29	n/a	Band 41	-97.0
Band 30	-95.5		
Band 41	-97.5		

UMTS Bands	AirPrime EM7455 (SD-WAN-210-LTE-R1)	UMTS Bands	AirPrime EM7430 (SD-WAN-210-LTE-R2)
Band 1	-110.5	Band 1	-110.1
Band 2	-110.0	Band 5	-111.4
Band 3	-109.5	Band 6	-112.0
Band 4	-110.0	Band 8	-112.0
Band 5	-111.0	Band 9	-110.2
Band 8	-111.5	Band 19	-111.7

TX (Transmit) Output Power (dBm) for Sierra Wireless™ EM7455, Sierra Wireless™ EM7430

LTE Bands	AirPrime EM7455 (SD-WAN-210-LTE-R1)	LTE Bands	AirPrime EM7430 (SD-WAN-210-LTE-R2)
Band 1, 2, 3, 4, 5, 8, 12, 13, 20, 25, 26	+23 dBm +/- 1 dB	Band 1, 3, 5, 8, 18, 19, 21, 28, 29	+23 dBm +/- 1 dB
Band 7, 30, 41	+22 dBm +/- 1 dB	Band 7, 38, 40, 41	+22 dBm +/- 1 dB

UMTS Bands	AirPrime EM7455 (SD-WAN-210-LTE-R1)	UMTS Bands	AirPrime EM7430 (SD-WAN-210-LTE-R2)
Band 1 (IMT 2100 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)	Band 1 (IMT 2100 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)
Band 2 (UMTS 1900 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)	Band 5 (UMTS 850 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)
Band 3 (UMTS 1800 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)	Band 6 (UMTS 850 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)
Band 4 (UMTS 1700/2100 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)	Band 8 (UMTS 900 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)
Band 5 (UMTS 850 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)	Band 9 (UMTS 1700 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)
Band 8 (UMTS 900 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)	Band 19 (UMTS 850 12.2 kbps)	+23 dBm +/- 1 dB, **Note:** Connectorized (Class 3)

Antenna gain (dB) for Taoglas

Specifications	Details
Part No.	TG.30.8113
Product Name	Apex Hinged TG.30 Ultra-Wideband 4G LTE antenna

Specifications	Details
Frequency Range	698 MHz to 960 MHz, 1575.42 MHz, 1710 MHz to 2700 MHz (typical 70%+ Efficiency and 3 dBi+ Peak Gain)
Other Features	Dipole Swivel Terminal antenna
	Hinged 90° termination with SMA(M) Connector
	RoHS Compliant

Citrix SD-WAN 400 and 410 Standard Edition Appliances

June 19, 2020

The Citrix SD-WAN 400 SE and 410 SE are 1U appliances for use in small branch offices. The SD-WAN 410 SE Series is the next generation of SD-WAN Standard Edition appliances with Virtual WAN functionality.

- SD-WAN 400 Series: A small, affordable 1U appliance suitable for smaller branch offices. The SD-WAN 400 SE Series has two accelerated bridges and supports WAN speeds of up to 50 Mbps.
- SD-WAN 410 Series: A small, affordable 1U appliance suitable for smaller branch offices. The SD-WAN 410 SE Series supports WAN speeds of up to 150 Mbps.

The 400-SE platform is Hypervisor based and 410-SE is a bare metal appliance.

Within a given series, all models use the same hardware, and the different WAN speed ratings are obtained through different licensing options. For example, the SD-WAN 410 SE models (the 410-20, 410-50, 410–100, and 410–150) use the same hardware, and an appliance can be licensed as either a 20 Mbps, 50 Mbps, 100 Mbps, or 150 Mbps appliance.

The licensed bandwidth applies only to the sending direction, so an SD-WAN 410 SE-20, rated at 20 Mbps in the sending direction, is appropriate for Virtual Path (fixed/dynamic) with a 16 Mbps/8 Mbps download/upload bandwidth.

In addition to differences in WAN bandwidth capabilities, the different series vary in CPU power, installed RAM, and installed disk capacity.

All models use solid-state drives instead of conventional hard drives for increased speed and reliability.

The Citrix Compliance Regulatory models for SD-WAN 400-SE and 410-SE are:

- SD-WAN 400-SE: CB 504-2
- SD-WAN 410-SE: 512-2

For more information, see the Citrix product platform datasheet.

Citrix SD-WAN 400 SE

June 25, 2020

The SD-WAN 400 SE platform has a dual-core processor and 8 GB of memory. This platform has a bandwidth of up to 50 Mbps.

The following figure shows the front panel of an SD-WAN 400 SE appliance.

Figure 1.SD-WAN 400 SE, front panel

- The front panel of the SD-WAN 400 SE appliance has a power button and five LEDs.

- The power button switches main power (the power to the power supply) on or off.

- The reset button restarts the appliance.

The LEDs provide critical information about different parts of the appliance.

- Power Fail—Indicates that a power supply unit has failed.

- Information LED—Indicates the following:

Status	Description
Continuously on and red	The appliance is overheated.
Slow blink - 1 blink per second	Fan failure.
Fast blink - 4 blinks per second	Power failure.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Fast blink - 3–4 blinks per second	Remote UID is on. Use this function to identify the server from a remote location.

- NIC1 and NIC2—Indicate network activity on the LAN1 and WAN1 ports.

- HDD—Indicates the status of the hard disk drive.

- Power—When blinking, indicates that the power supply unit is receiving power and operating normally.

The following figure shows the back panel of an SD-WAN 400 SE appliance.

Figure 2. SD-WAN 400 SE appliance, back panel
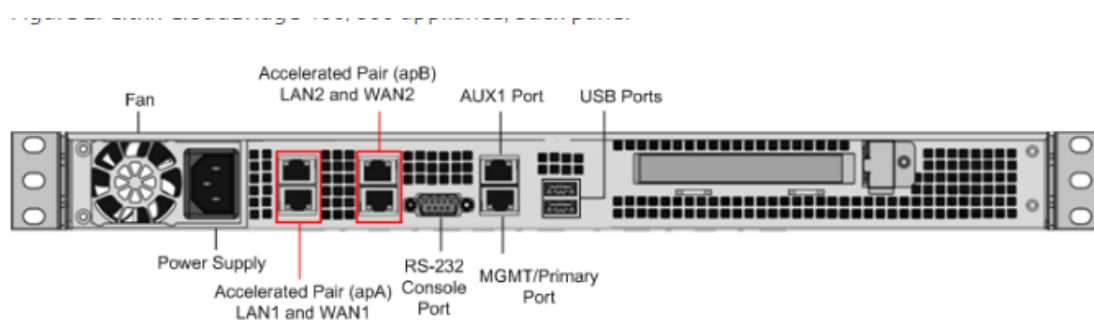
The following components are visible on the back panel of an SD-WAN 400 SE appliance:

- Cooling fan
- Single power supply, rated at 200 watts, 110–240 volts
- Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges. Individual port assignments: LAN1 is apA.1, WAN1 is apA.2, LAN2 is apB.1, LAN2 is apB.2.
- RS-232 serial console port
- One Aux Ethernet port and one management port
- Two USB ports
- One Solid State Drive (SSD)
- SD-WAN 400 - 160 GB SSD

Citrix SD-WAN 410 SE

June 25, 2020

The SD-WAN 410 SE platform has a dual-core processor and 8 GB of memory. This platform has a bandwidth of up to 150 Mbps.

The following figure shows the front panel of an SD-WAN 410 SE appliance.

The power button switches main power (the power to the power supply) on or off. Press the switch for two seconds to turn off the power.

The reset button restarts the appliance.

- apA, apB, and apC -Indicate network activity on the LAN and WAN ports.

- Bypass port— Indicates the status of the third pair of bypass ports.

- Power— When blinking, indicates that the appliance is doing factory reset.

The LEDs provide critical information about different parts of the appliance.

- Power indicator —Indicates that a power supply unit has failed.
- Information LED—Indicates the following:

Status	Description
Continuously on orange	Data ports are in bypass mode (FTW)
Continuously ON and red.	The appliance is overheated. (This might be a result of cable congestion.)
Slow blink - 1 blink per second	Fan failure.
Fast blink- 4 blinks per second	Power failure.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Fast blink - 3–4 blinks per second	Remote UID is on. Use this function to identify the server from a remote location.
Solid Green	Appliance is operational.

> **Note**
>
> The terms FTW and bypass are inter-exchangeable. The bypass port is the FTW port.
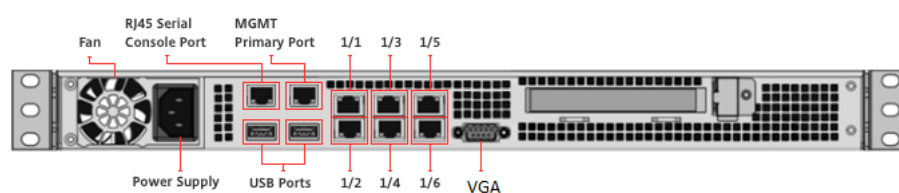
The above figure shows the back panel of an SD-WAN 410 SE appliance.

The following components are visible on the back panel of an SD-WAN 410 SE appliance:

- Cooling fan - This platform is intended for use in a branch typically desktop mounted with ambient air temperature.
- Single power supply, rated at 200 watts, 110–240 volts. Power supply has an LED that indicates the status of the power supply, as described in hardware-common-components-con1.html
- One RJ45 management port.
- One RJ45 console port.
- 6X1 GigE Copper (1000BASE-TX).
- VGA port.
- Two USB ports.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

Port labeling for SD-WAN 410

All data ports are labeled in the order they are enumerated by the Operating System. The ports use odd port numbers for LAN ports and even port numbers for WAN ports. 1/1 is used for the first LAN port, 1/2 for the first WAN port, 1/3 for the second LAN Port, 1/4 for the second WAN port, 1/5 for the third LAN Port, and 1/6 for the third WAN Port.

Summary of Hardware Specifications

May 23, 2019

The following table summarizes the specifications of the SD-WAN 400 SE and 410 SE hardware platforms.

Citrix SD-WAN 400 and 410 platforms specification summary

Hardware specifications

Feature	SD-WAN 400 SE	SD-WAN 410 SE
Processor	2 Cores	4 Cores
Total disk space	1 x 160 GB SSD	64 GB SATADOM
Total SSD and Compression history (SSD)	40 GB	60 GB (compression history (SSD) - N/A)
RAM	8 GB	8 GB
Network Interfaces (Fail-to-wire, Non-fail-to-wire, Management)	2 pair with bypass 10/100/1000	6 x 1000Base-TX, N/A, 1 x 1000Base-TX
Transceiver support	No	No. The FTW ports are pre-installed with Transceivers.
Power supplies	1	1

Physical dimensions

Feature	SD-WAN 400 SE	SD-WAN 410 SE
Rack Units	1U	1RU (1.75 inches/4.45 cm)
System depth	10.5" (26.7 cm)	14" (35 cm)
System weight	8 lbs (3.87 kg)	8.5 lbs (3.87 kg)
Shipping dimensions and weight	26" x 6.5" x 18.5" (66.1 x 16.6 x 47.0 cm), 13.5 lbs (6.14 kg)	26" x 6.5" x 18.5" (66.1 x 16.6 x 47.0 cm), 13.5 lbs (6.14 kg)

Environmental and regulatory

Feature	SD-WAN 400 SE	SD-WAN 410 SE
Wattage	200 W	200 W
Voltage	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)
Operating altitude	0–4921 ft (0-1500M)	0–4921 ft (0-1500M)
Storage temperature	14–140°F (-10–60°C)	14–140°F (-10–60°C)

Feature	SD-WAN 400 SE	SD-WAN 410 SE
Allowed Relative Humidity	8%–90%	Operating: 20% to 80% (noncondensing)
Safety certifications	CSA/EN/IEC/UL 60950-1 Compliant, UL, or CSA Listed (USA and Canada), CE Marking (Europe)	CSA/EN/IEC/UL 60950-1 Compliant, UL, or CSA Listed (USA and Canada), CE Marking (Europe)
Electromagnetic and susceptibility certifications	FCC (Part 15 Class A), CCC, KCC, NOM, CITC, EAC, DoC, CE, VCCI, RCM	FCC (Part 15 Class A), CCC, KCC, NOM, CITC, EAC, DoC, CE, VCCI, RCM
Environmental certifications	RoHS, WEEE	RoHS, WEEE, REACH (optional)

Citrix SD-WAN 4000, 4100, and 5100 Standard Edition Appliances

June 19, 2020

Citrix SD-WAN Standard Edition 4000, 4100, 5100 appliances are high-performance appliances for busy datacenters. These platform editions are designed for Virtual WAN links with speeds more than 1 Gbps, especially for busy datacenters that communicate with many branch and regional sites. These appliances are recommended at the hub of a hub-and-spoke deployment, where smaller appliances are used at the spokes, whenever the link speed or the number of XenApp/XenDesktop users is higher than that can be supported by a smaller appliance.
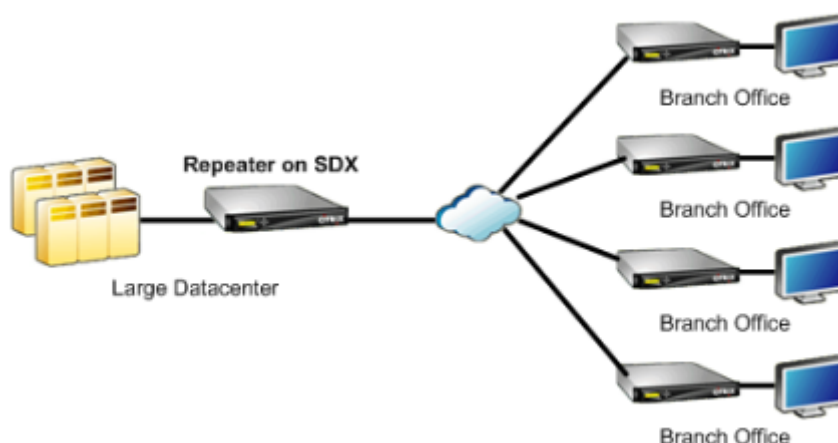
Citrix SD-WAN 4000 SE

June 25, 2020

The SD-WAN 4000 is a 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 GB (GB) of memory. The SD-WAN 4000 SE has a bandwidth of 300 Mbps, 500 Mbps, 1 Gbps, and 2 Gbps respectively.

The following figures shows the front panel of the SD-WAN 4000 SE appliance.

Figure 1.SD-WAN 4000 SE, front panel
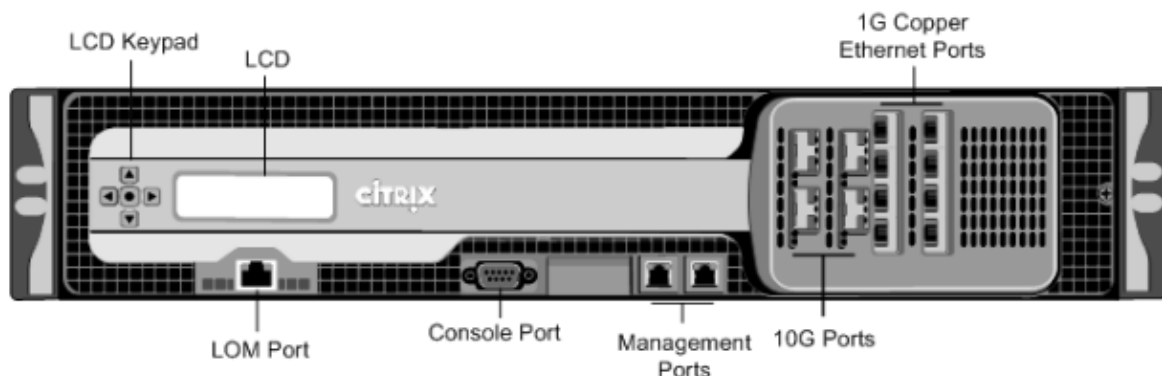
The Citrix SD-WAN 4000 SE appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.

  Note: The LEDs on the LOM port are not operational by design.

- RS232 serial console port.

- Two 10/100/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.

- Network Ports

  - SD-WAN 4000 SE (without FTW cards). Eight 1G SFP ports and four 10G SFP+ ports.
  - SD-WAN 4000 SE (with FTW cards). Eight 1G copper Ethernet ports and four 10G ports.

The following figure shows the back panel of the SD-WAN 4000 SE appliance.

Figure 2. SD-WAN 4000 SE, back panel
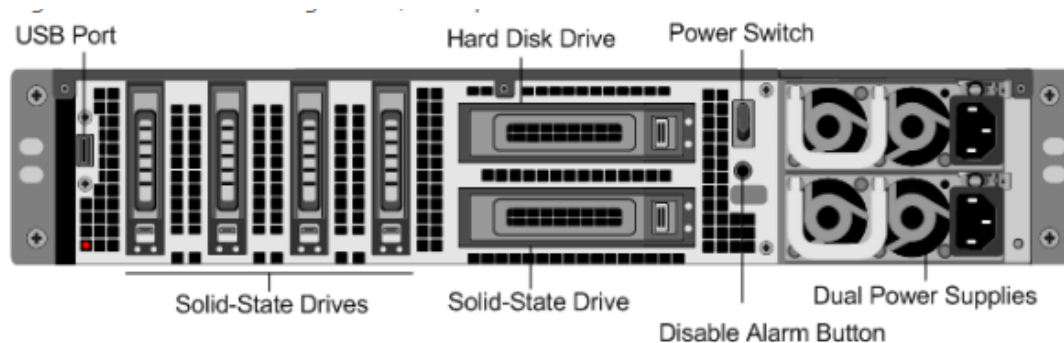
The following components are visible on the back panel of the 4000 SE appliance:

- Four 600 GB removable solid-state drives. The 256 GB solid-state drive below the hard disk drive stores the appliance's software. Newer editions of 4000-SE have 800 GB removable SSD and 240 GB SSD.
- USB port (reserved for a future release).
- A 1 TB removable hard disk drive.
- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable alarm button. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies (either AC or DC), each rated at 850 watts, 100–240 volts.

Citrix SD-WAN 4100 SE

July 7, 2020

Citrix SD-WAN 4100 is a 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 96 GB (GB) of memory. The SD-WAN 4100 SE has a virtual WAN bandwidth of 4 Gbps and 6 Gbps.

The following figures shows the front panel of the SD-WAN 4100 SE appliance.

Figure 1. SD-WAN 4100 SE, front panel
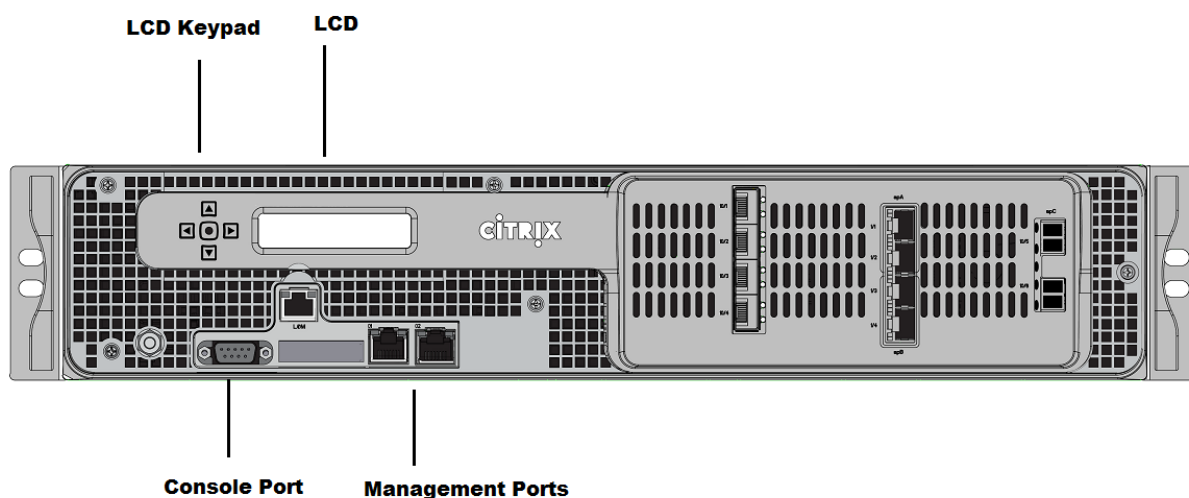
The SD-WAN 4100 SE appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software. The LEDs on the LOM port are not operational by design.
- RS232 serial console port.
- Two 10/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.
- 2 port 10G FTW
- 4 port 10G/1G SFP+
- 4 port 10/100/1000 FTW RJ 45

The following figure shows the back panel of the SD-WAN 4100 SE appliance.

Figure 2. SD-WAN 4100 SE, back panel

The following components are visible on the back panel of the SD-WAN 4100 SE appliance:
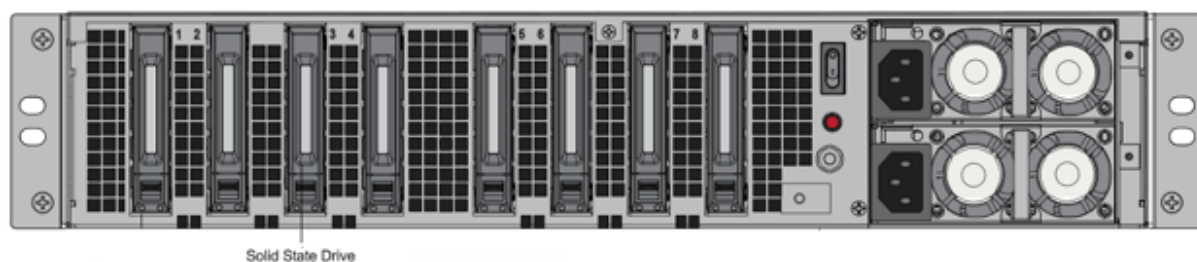
- 2 X 1 TB HDD in RAID 1.
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable alarm button. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.

- Dual power supplies (either AC or DC), each with max power of 850 watts, 100–240 volts.

Citrix SD-WAN 5100 SE

June 25, 2020

The SD-WAN 5100 SE is a 2U appliance. Each model has two 10-core processors for a total of 20 physical cores (40 cores with hyper-threading), and 128 GB (GB) of memory. For latest performance and bandwidth capacity details, please see also the latest datasheet that gets updated more regularly at: citrix.com; datasheet.

The SD-WAN 5100 SE appliance front panel has the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called lights out management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.
- Eight 10G ports: 4 LC fiber ports with bypass, 4 SFP+ ports (no bypass).
- Two USB ports (reserved for a future release).

The following components are visible on the back panel of the SD-WAN 5100 SE appliance:

- 2 X 1 TB removable hard disk drive.
- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable PS alarm button. This button is functional only when the appliance has two power supplies. Press this button to mute the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual redundant, hot-swappable power supplies.

Upgrade 5100 SE appliance to 5100 PE appliance

Insert solid state drive (SSD)

1. Insert the required SSD in the standard edition appliance. For instructions about how to insert SSD, see Solid State Drive (Field Replaceable Unit).

    a) 5100 SE appliance requires 800 GB more SSD. Insert the SSD into the third bay.
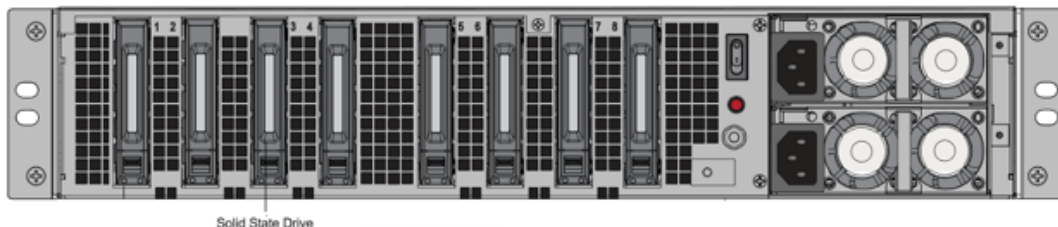
Solid State Drive

2. Restart the appliance through the SD-WAN web management interface.

3. Ensure that the software release version installed on the appliance is SD-WAN release version 10.0. Follow the steps provided here; upgrade new appliance.

4. Install the Premium (Enterprise) Edition platform license. For license information, see the Citrix SD-WAN product downloads site.

5. Upgrade the network using single step upgrade to software release version 10.0 or later.

Note: Citrix SD-WAN 5100-SE is a bare metal platform. You can login directly to the appliance console using admin/password and then into shell prompt.

Configure Management IP address using serial Console

1. Access serial console of the appliance.
2. Log in using the **root/nsroot** credentials.
3. Type the **ssh admin@169.254.0.60 -l admin** command.
4. Type password: **password**.
5. Type the **management_ip** command.
6. Type the **set interface 192.168.100.1 255.255.255.0 192.168.100.254** command.
7. Type the **apply** command.

Summary of Hardware Specifications

June 19, 2020

The following table summarizes the specifications of Citrix SD-WAN 4000, 4100, and 5100 SE hardware platforms.

Specifications	SD-WAN 4000 SE	SD-WAN 4100 SE	SD-WAN 5100 SE
Regulatory Model Number	4x10GE SFP+ 8xSFP	2U1P1B	2U1P1D
Processors	Two 6-core	Two 6-core	Two 10-core
Memory	96 GB	96 GB	128 GB
Number of power supplies	Dual power supplies	Dual power supplies	Dual power supplies
AC power supply, input voltage, frequency and current	100-240 V AC, 47-63 hz	100-240 V AC, 47–63 hz; 7.0-3.5 A	100-240 V AC, 47–63 hz; 9.0-4.5 A
Maximum AC power consumption	650 W	850 W	850 W
Package weight	69 lbs	69 lbs	69 lbs
Shipping dimensions	36.5' L X 24.5' W X 11' H	36.5' L X 24.5' W X 11' H	36.5' L X 24.5' W X 11' H
System weight	60 lbs	60 lbs	60 lbs
Rack unit	2RU	2RU	2RU
Rack options - Width	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting bracket
Depth	28" (72 cm)	28" (72 cm)	28" (72 cm)
Operating temperature	32–104 F (0–40 C)	32–104 F (0–40 C)	32–104 F (0–40 C)
Humidity (non-condensing)	20% - 80%	20% - 80%	20% - 80%
Safety certifications	CSA	CSA	CSA

Specifications	SD-WAN 4000 SE	SD-WAN 4100 SE	SD-WAN 5100 SE
EMC and susceptibility	USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC), Taiwan (BSMI), Brazil (Anatel), Israel (MoC)	USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC), Taiwan (BSMI), Brazil (Anatel), Israel (MoC)	USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC), Taiwan (BSMI), Brazil (Anatel), Israel (MoC)
Environmental compliance	ROHS, WEEE	ROHS, WEEE	ROHS, WEEE

Citrix SD-WAN 1000, 2000, and 2100 Standard Edition Appliances

June 25, 2020

The SD-WAN Standard Edition 1000, 2000, and 2100 appliances combine virtualized instances of the SD-WAN appliance.

The SD-WAN Standard Edition 1000, 2000, and 2100 appliances are based on the Citrix branch architecture, which supports multiple virtual machines. All branch appliances contain an SD-WAN Standard Edition instance and management service instance.

The SD-WAN instance is typically used in inline mode, with the SD-WAN instance interposed between the WAN router and the LAN. The SD-WAN instance can also be deployed in virtual inline mode.

The appliance has two modes. Two-port mode and four-port mode, which determine how ports 1/3 and 1/4 are used.

Citrix SD-WAN 1000 SE

June 19, 2020

The SD-WAN 1000-SE with platform has a quad-core processor and 32 GB of memory. This platform has a bandwidth of up to 100 Mbps.

The following figure shows the front panel of an SD-WAN 1000-SE appliance.

Figure 1. Citrix SD-WAN 1000-SE front panel

The front panel of the SD-WAN 1000-SE appliance has a power button and five LEDs. The power button is used to switch the appliance on or off. The reset button restarts the appliance.

The LEDs provide critical information related to different parts of the appliance.

- Power Fail – Indicates the power supply unit has failed.
- Information LED – Indicates the following:

Status	Description
Continuously ON and red	The appliance is overheated. (This might be a result of cable congestion.)
Blinking red (1Hz)	Fan failure, check for an inoperative fan.
Blinking red (0.25Hz)	Power failure, check for the non-operational power supply.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Blinking blue (300 m/s)	Remote UID is on. Use this function to identify the server from a remote location.

- NIC1 and NIC2 – Indicate network activity on the LAN1 and WAN1 ports.
- HDD – Indicates the status of the hard disk drive.
- Power – Indicates that the power supply units are receiving power and operating normally.

The following figure shows the back panel of an SD-WAN 1000-SE appliance.

Figure 2. Citrix SD-WAN 1000-SE appliance, back panel

The following components are visible on the back panel of an SD-WAN 1000-SE appliance:

- Cooling fan.
- Single power supply, rated at 200 watts, 110–240 volts.
- Accelerated pairs of Ethernet ports (apA and apB).
- RS-232 serial console port.
- One AUX Ethernet port and one management port.
- Two USB ports.

Power on Appliance After a Graceful Shut Down

To power on the appliance after a graceful shut-down:

1. Connect a Serial console cable to the rear of the appliance and to the serial port on a management laptop.

Console Port
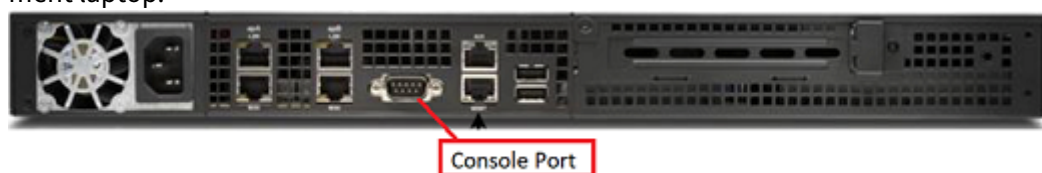
2. On the management laptop, restart a putty session using the following configuration settings:

- Serial line: COM1
- Speed: 9600

3. Power on the appliance and as it is booting, press the following key in the Putty session to enter the BIOS configuration screen. Keypress: **DEL**

4. When in the BIOS, navigate to,

   a) Advanced Tab > **Select**

   b) Boot Feature > **Enter**
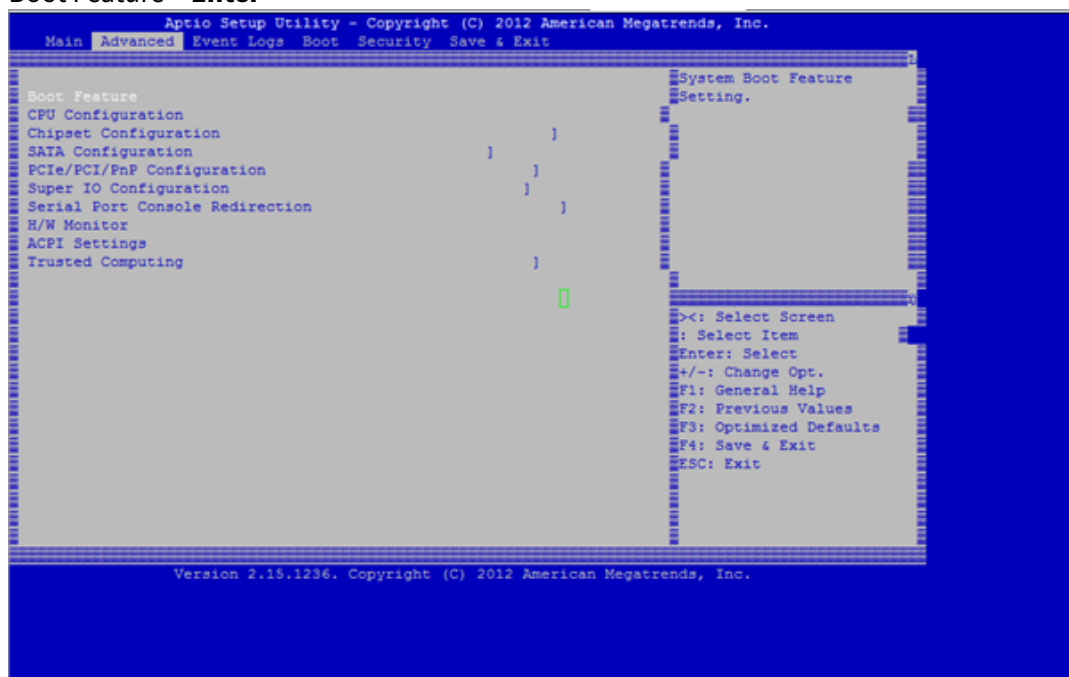
5. When in the Boot Feature screen, change the value of the parameter **Restore on AC Power Loss**; from **Last State** > **Power ON**.
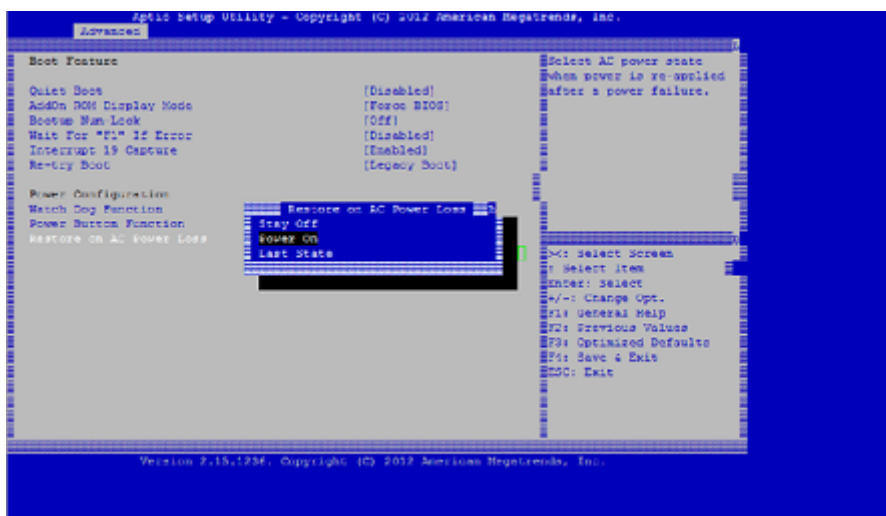
6. Navigate to Save and Exit.

   a) Select **Save changes** and **Reset**

   b) Select **Yes**

   Allow the system to restart. This takes approximately five minutes.
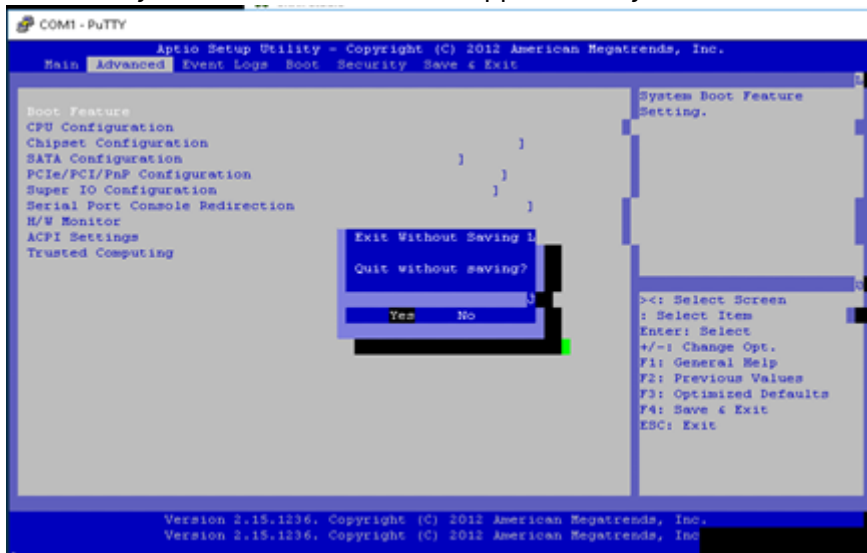
7. After the appliance is powered on, login to the appliance management instance (SVM). The default IP address for the appliance is: 192.168.100.1, user name is: admin/password.
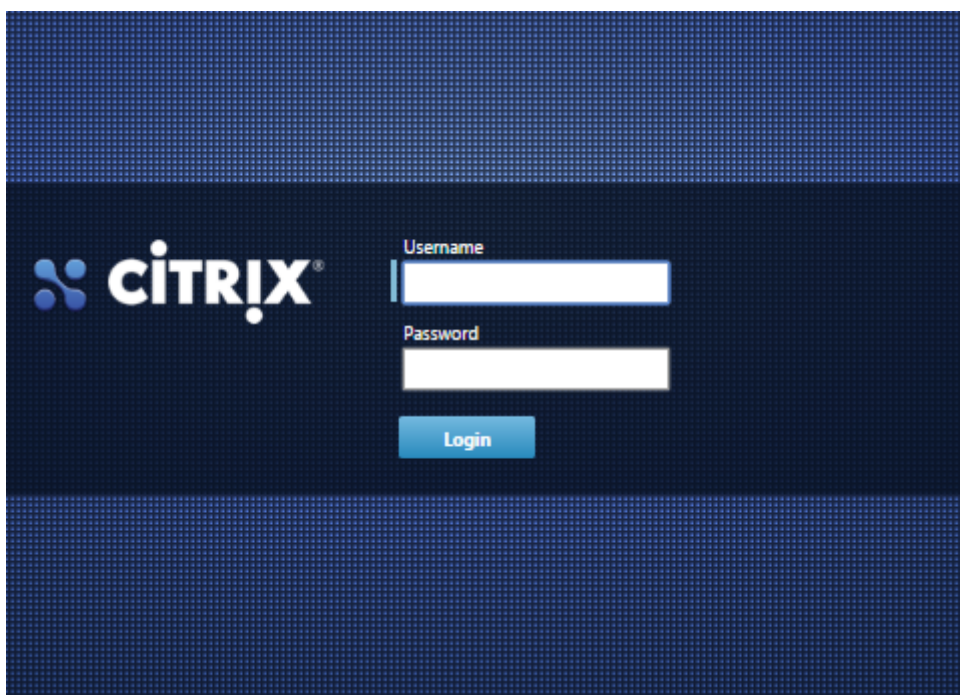
8. In the SD-WAN appliance GUI, navigate to **Configuration** > **System Maintenance** > **Restart System** and click **Reboot**. Allow the appliance to fully shut down. Ensure that there are no power lights on the appliance when the shut-down process has completed.

9. Power on the appliance to confirm that the BIOS configuration change has been applied successfully. This can be either done through the APC intelligent PDU Web Management console or by physically pulling the power cable out of the shut-down SD-WAN appliance, waiting for 10 seconds and then plugging it back in again. The appliance power ups automatically from all shut-down scenarios.

Citrix SD-WAN 2000 SE

May 23, 2019

The Citrix SD-WAN 2000-SE platform is a 1U appliance with one quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 2000-SE appliance.

Figure 1. Citrix SD-WAN 2000-SE appliance, front panel
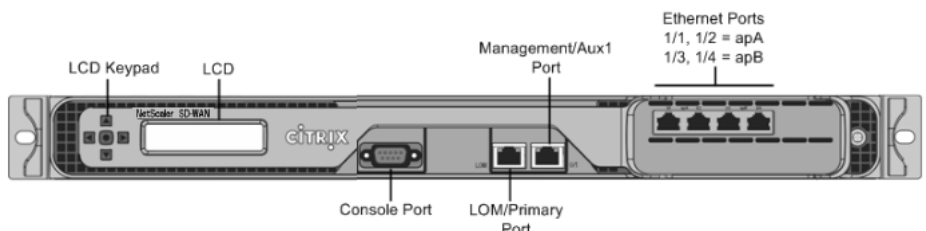
SD-WAN 2000-SE appliance has the following ports:

- An RS232 serial console port.
- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, numbered 0/1, and named PRI (primary). The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of Virtual WAN. The LOM port also operates as a management port.
- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two *accelerated pairs*, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

Figure 2. Citrix SD-WAN 2000-SE appliance,back panel
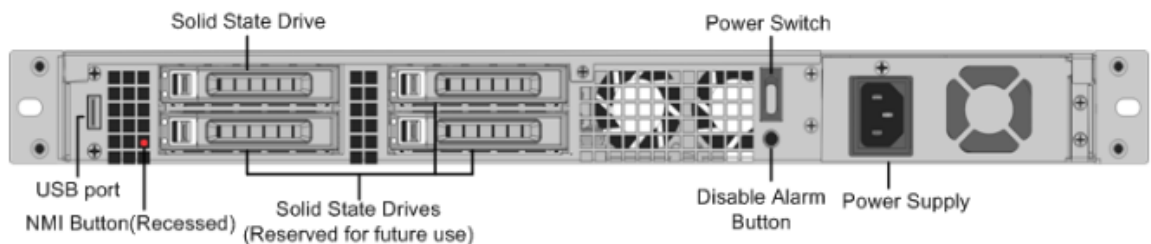
The following components are visible on the back panel of the SD-WAN 2000-SE appliance:

- 600 GB removable solid-state drive, which stores the appliance's software and user data, and 1 TB hard disk drive.
- Power switch. Press the switch for five seconds to switch off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.

- Single power supply, rated at 300 watts, 100-240 volts.

Citrix SD-WAN 2100 SE

June 25, 2020

The Citrix SD-WAN 2100-SE platform is a 1U appliance with 8 core processor and 32 GB (GB) of memory.

The following figure shows the front panel of the SD-WAN 2100-SE appliance.

Figure 1. Citrix SD-WAN 2100-SE appliance, front panel

SD-WAN 2100-SE appliance has the following ports:

- An RS232 serial console port.
- 10/100/1000 Base-T copper Ethernet management port (RJ45) called the Lights out Management (LOM) port labeled LOM, and management port labeled 0/1. You can use these ports to remotely monitor and manage the appliance independently of the appliance's software.
- USB ports.
- Four 1000 Base-TX copper Ethernet ports.
- Four 1GE SFP ports.

Port Labels - old 2100-SE Front Bezel	Description
LOM	Lights out management Port
0/1	Management Port
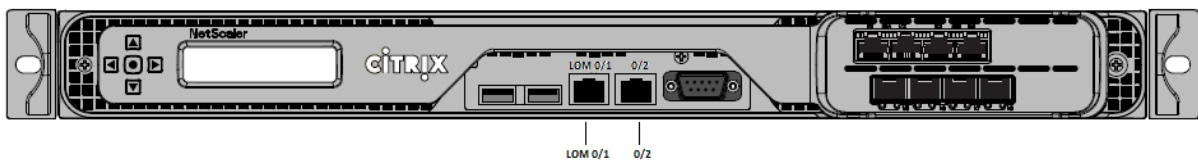
Port Labels - new 2100-SE Front Bezel	Description
LOM 0/1	Lights out management and Management Port
0/2	Management port that is reserved for future use (Management)

- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port labeled lights out management and 0/1. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, labeled 0/2. This management port cannot be used for system administration functions. This port is reserved for future use.

Figure 2. Citrix SD-WAN 2100-SE appliance, back panel
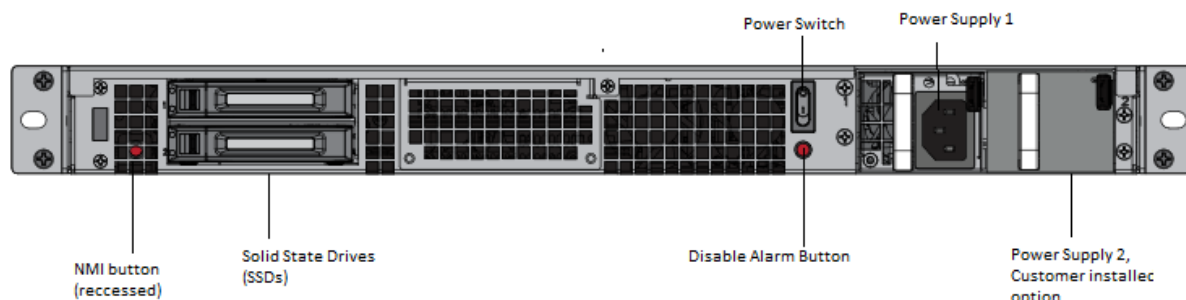
The following components are visible on the back panel of the SD-WAN 2100-SE appliance:

- 240 GB removable solid-state drive and 1 blank slot.
- Power switch, which switches power to the appliance on or off. Press the switch for five seconds to switch off the power.
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. Use a pen, pencil, or other pointed object to press the red button, which is required to prevent unintentional activation.
- Single power supply, rated at 450 watts, 100–240 volts.

Convert 2100 SE Appliance to 2100 PE Appliance

Important

To use PE functionality, the 2100 appliance needs to have SD-WAN release 9.3 or higher software version. The SD-WAN release 9.3 and higher software release versions support 2100 PE.

- 2100 SE ships with only one SSD (240 GB) and one blank carrier.
- If you want to upgrade to a PE appliance, you can order the kit. The kit includes an extra SSD (480 GB) and appropriate license for PE.
- Upon receiving the kit, install the new 480 GB drive in the empty slot (leaving original SSD as is). Upgrade to SD-WAN release 10.0, and apply new PE license.

Note

You can also convert a 2100 SE appliance to 2100 PE appliance using the USB reimage utility.

108

Insert Solid State Drive (SSD)

1. Insert the required SSD in the standard edition appliance. For instructions about how to insert SSD, see Solid State Drive (Field Replaceable Unit).
    a) 2100 SE appliance requires 480 GB or more SSD.
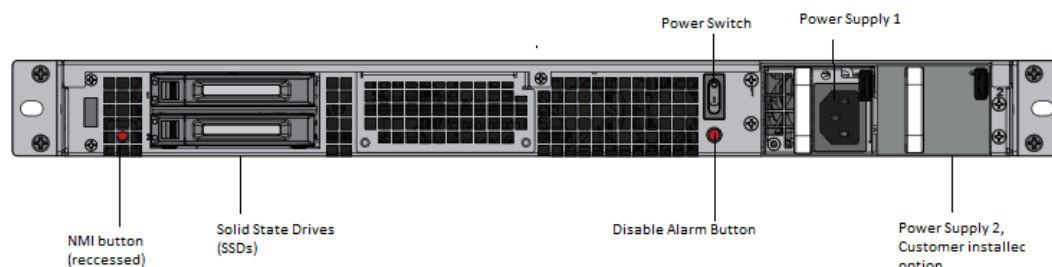
2. Restart the appliance through the SD-WAN web management interface.
3. Ensure that the software release version installed on the appliance is SD-WAN release version 10.0. Follow the steps provided here; upgrade new appliance.
4. Install the Enterprise Edition platform license. For license information, see the Citrix SD-WAN product downloads.
5. Upgrade the network using single step upgrade to software release version 10.0 or later.

Configure Management IP address using serial Console

1. Access serial console of the appliance.
2. Log in using the **root/nsroot** credentials.
3. Type the **ssh admin@169.254.0.60 -l** administrator command.
4. Type password: **password**.
5. Type the **management_ip** command.
6. Type the **set interface 192.168.100.1 255.255.255.0 192.168.100.254** command.
7. Type the **apply** command.

Summary of Hardware Specifications

August 18, 2020

The following table summarizes the specifications of the SD-WAN 1000-SE, 2000-SE, and 2100-SE hardware platforms.

Specifications	SD-WAN 1000-SE	SD-WAN 2000-SE	SD-WAN 2100-SE
Bandwidth	Up to 100 Mbps	Up to 300 Mbps	Up to 2 Gbps
Total sessions, Max Virtual Paths (Static/Dynamic)	10,000	20,000	256/32
Processor	4 Cores	4 Cores	8-Core 2.1 GHz
Total Disk Space	1X480 GB SSD	1X800 GB SSD	1X240 GB SSD
RAM	16 GB	24 GB	32 GB
Network Interfaces	2 pair with bypass 10/100/1000; 2 GigE ports for Management and AUX ports	2 pair with bypass 10/100/1000	2 pair with bypass of 1G; 4 x 1GE SFP; 2 GigE ports for Management and AUX ports
Power Supplies	1	1	1 module and 1 optional FRU
Rack Units	1U	1U	1U
System Width	EIA 310-D for 19-inch (482.6 mm) racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
System Depth	10" (25.4 cm)	23.5" (60 cm)	24" (61 cm)
System Weight	8.5 lbs (3.9 kg)	32 lbs (14.5 kg)	32 lbs (14.5 kg)
Shipping dimensions and weight	26 L x 18.5 W x 6.5" H; 14.5 lbs	32 L x 23.5 W x 7.5" H; 39 lbs	33" L x 24" W x 8" H; 40 lbs
Voltage	100/240 VAC, 50–60 Hz	100/240 VAC, 50–60 Hz	100/240 VAC, 50–60 Hz
Power consumption (Max.)	200 W	300 W	450 W
Operating Temperature (degree Celsius)	10–35	0–40	0–40
Non-operating Temperature (degree Celsius)	-40 to +70	-40 to +70	-10C to +60C
Allowed Relative Humidity	8% – 90% non-condensing	5%–95% non-condensing	20%-80% non-condensing

Specifications	SD-WAN 1000-SE	SD-WAN 2000-SE	SD-WAN 2100-SE
Safety certifications	CSA/EN/IEC/UL 60950-1 Compliant, UL, or CSA Listed (USA and Canada), CE Marking (Europe)	CSA/EN/IEC/UL 60950-1 Compliant, UL, or CSA Listed (USA and Canada), CE Marking (Europe)	CSA/EN/IEC/UL 60950-1 Compliant, UL, or CSA Listed (USA and Canada), CE Marking (Europe)
Electromagnetic and susceptibility certifications	FCC Class A, EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A	FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT	FCC (Part 15 Class A), CCC, KCC, NOM, CITC, EAC, DoC, CE, VCCI, RCM
Environmental certifications	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE

6100 Standard Edition and Premium Edition appliance

March 4, 2021

The Citrix SD-WAN 6100 Standard Edition (SE)/ Premium Edition (PE) is a 2U appliance. Each model has two 14-core processors for a total of 28 physical cores (with hyper-threading enabled), and 256 GB of memory. For latest performance and bandwidth capacity details, see the Citrix SD-WAN data sheet.

The following Citrix SD-WAN software versions are supported on the 6100 appliance editions:

- Citrix SD-WAN 6100 SE – Citrix SD-WAN 10.2.3 and above.
- Citrix SD-WAN 6100 PE - Shipped with Citrix SD-WAN 10.2.7 image, upgrade the software to Citrix SD-WAN 11.2.1 and above to enable PE functionality.

The Citrix SD-WAN 6100 SE/PE appliance front panel has the following ports:

Port	Description
0/1, 0/2	10/100/1000 Base-T copper Ethernet management ports (RJ45)
1/1, 1/2, 1/3, 1/4	1000 Base-TX Fail-To-Wire
10/1, 10/2, 10/3, 10/4	10G Base-SR Fail-To-Wire
10/5, 10/6, 10/7, 10/8	10G SFP+

The following components are visible on the back panel of the Citrix SD-WAN 6100 SE/PE appliance:

For Citrix SD-WAN 6100 SE [SSD Configuration]

- Drive bay 3 - 2.5" Boot drive SSD with 480 GB capacity
- Drive bay 1, 2, 4 - 2.5" SSD Plastic Drive Tray "Fillers- Dummy"

For Citrix SD-WAN 6100 PE [SSD Configuration]

- Drive bay 3 - 2.5" Boot drive SSD with 480 GB capacity
- Drive bay 1, 2, 4 - 2.5" 960 GB SSD.

Power Switch and back end Button functionalities:

- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.

- Disable PS alarm button is functional only when the appliance has two power supplies.

  Press this button to mute the power alarm from sounding:

  - When you have plugged the appliance into only one power outlet.
  - When one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.

- Dual redundant, hot-swappable power supplies (100–240 VAC standard 1,000 W, 48 V DC optional).

Convert the Citrix SD-WAN 6100 SE appliance to the Citrix SD-WAN 6100 PE appliance

1. Insert the required SSD in the Citrix SD-WAN SE appliance.

- Drive bay 3-Insert 2.5" Boot drive SSD with 480 GB capacity.
- Drive bay 1, 2, and 4- Insert 2.5" 960 GB SSD.
  For instructions about how to insert SSD, see Solid State Drive.

1. Restart the appliance through the SD-WAN web management interface.

2. Ensure that the software release version installed on the appliance is Citrix SD-WAN 11.2.1 or above. If the appliance is running a version lower than 11.2.1, upgrade the software to 11.2.1 and perform a local change management. For upgrade instructions, see Upgrade paths.

3. Install the Premium Edition platform license. For license information, see Citrix SD-WAN product downloads.

Summary of hardware specifications

The following table summarizes the specifications of Citrix SD-WAN 6100 SE hardware platform.

Specifications	Citrix SD-WAN 6100 SE/PE
Compliance Regulatory Model number	2U1P1A
Processors	2x 14 Core processor (Intel E5-2680 v4 14-core, 2.4 GHz)
Memory	256 GB 2,400 MHz, 8x 32 GB RDIMM

Specifications	Citrix SD-WAN 6100 SE/PE
Number of power supplies	2 (Each 1,000 W; Dual Redundant Hot swappable)
AC power supply, input voltage, frequency, and current	100–240 V AC, 50–60 Hz, 5.5-2.8A
DC input voltage and Current	-36 V DC to -72 V DC, 15.4-7.7A
Typical AC power consumption	357 W
Maximum AC power consumption	480 W
Typical Heat Dissipation	1251 BTU/Hr
Max Heat Dissipation	1218 BTU/Hr
Typical Airflow (front to rear)	65 CFM
Max Airflow (front to rear)	125 CFM
Altitude Range	Max 5,000 m (Up to 16,000 ft)
Solid State Drives (SSD)	1x480GB and 3x960GB SSD (1.2GB DBC, applicable for PE only)
Package weight	69 (lbs) (31.3 Kg)
Shipping dimensions	36.5' L X 24.5' W X 11' H (94 x 63 x 28 cm)
System weight (lbs)	60 (lbs) (27.2 Kg)
Rack Height	2U
Rack Width	EIA 310-D for 19 (inch) racks
Rack Depth	28 inches (71.1 cm)
Operating temperature	0–45°C (32–113°F)
Humidity (non-condensing)	5% - 95%
Safety certifications	IEC 60950-1, second Edition
	CSA 60950-1, second Edition
	UL 60950-1, second Edition
	AS/NZS 60950-1

Specifications	Citrix SD-WAN 6100 SE/PE
EMC and susceptibility	US (FCC (Part 15 Class A)), Europe (CE (EN55032/55024)), Australia (RCM), Japan (VCCI), Korea (KCC), Taiwan (BSMI), China (CCC), India (BIS), Russia (CUTR), Russia (EAC), Saudi Arabia (CITC), Brazil (Anatel), South Africa (ICASA), Mexico (NOM), Egypt (NTRA), Israel (MoC)
Environmental compliance	ROHS, WEEE, REACH

Citrix SD-WAN 1100 Standard Edition and Premium Edition

October 5, 2021

The Citrix SD-WAN 1100 standard and premium edition appliance is a desktop form factor appliance. Each model has 8-core processor with 24 GB memory and 480 GB of storage (SSD drive).

The following figure shows the front panel of the 1100 SE and PE appliance.

Figure 1. Citrix SD-WAN 1100 SE and PE, front panel

Table 1. LED power supply indicators

LED Color	LED Indicates
Ethernet ports	Active/Link: Green, Speed -1000 Orange, Speed-100: Green, Speed-10: off
Bypass LEDs	Normal Mode: Green, Bypass Mode: Orange
Small Form-factor Pluggable (SFP) Port LEDs	Active/Link: Green, Speed- 1000: Orange
Power LEDs	Power on: Green, Power off: off

The appliance has the following ports:

- Serial console port.
- One 10/100/1000 Base-T copper Ethernet management port (RJ45). The management port is used to connect directly to the appliance for system administration functions.
- Two como ports (1/5 and 1/6). One can use RJ45 or SFP port at a time.
- 480 GB solid-state drive, which is used to store the Citrix SD-WAN software and the user data.
- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Two Power over Ethernet (POE) ports (1/7 and 1/8). Each port has <30 watts output.
- Two sets of FTW ports, (1/1, 1/2), and (1/3, 1/4).
- USB ports.
- Single power supply. Second power supply (optional) for redundancy, each rated at 150 W.

Accessory FRUs:

- Rackmount Kit
- Extra power adapter and power cord – connected to DC Jack 2

- SFP transceiver and cable (s)

Citrix SD-WAN 1100 SE and PE back panel:

Citrix SD-WAN 1100 SE and PE back panel labeled:

For information about installing the rails, rack mounting the hardware, and connecting the cables, see
[Installing the Hardware](#).

Ports	Supported speeds
1/1-1/4	100/1000

Ports	Supported speeds
1/5-1/6	RJ45: 1000 only, SFP: 100 (certain SFPs)/1000
1/7-1/8	100/1000

Citrix SD-WAN 1100 enhancement on SFP to support High Availability with Y-Cable

The available SFP ports on 1100 appliances can be used with fiber optic Y-Cables to enable high availability feature for Edge Mode deployment. On the 1100 SE/PE appliance the splitter cable split end connects to fiber ports of two 1100 appliances that are configured in high availability pair. For more information, see Enable Edge Mode High Availability Using Fiber Optic Y-Cable.

Citrix SD-WAN 1100 platform support for MiRiC-E1T1 FE/GBE SFP

The following two types of MiRiC SFPs are supported on the 1100 appliance for SFP ports 1/5 and 1/6.

1. MiRiC-E1T1 FE SFPs.
2. MiRiC-E1T1 GBE SFPs.

MiRiC-E1T1 FE SFPs must configure with speed as 100 Mbps and duplex as full. MiRiC-E1T1 GBE SFPs must configure with speed as 1 Gbps and duplex as full.

To configure, go to SD-WAN appliance GUI, navigate to **Configuration > Network Adapters > Ethernet page**.

Access MiRiC SFP web service

1. The SFP transceivers have default management IP address of 192.168.205.1, which can be used for the SFP web service to configure relevant configurations, for example; T1 or E1. The IP ad-

dress can be modified other than 192.168.205.1. However ensure that you avoid IP address conflicts.

2. To enable SFP access to the management:

- Log into the appliance CLI via **ssh admin@(ip address)**

- Run: sfp_access

- To enable access on 1/5, execute one of the following commands.

  - enable 1/5 # Works for GBE transceivers only if already configured.
  - enable 1/5 100 # - Works only for FE transceivers
  - enable 1/5 1000 # - Works only for GBE transceivers
  - enable 1/5 100 172.217.43.2 # - For FE transceivers and assumes a user changes the default IP to an IP in 172.217.43.0/24

- enable 1/5 1000 172.217.43.2 # - For GBE transceivers and assumes a user changes the default IP to an IP in 172.217.43.0/24

  > **Note:**
  >
  > Enabling management access on 1/5 automatically disables management access on 1/6, and vice versa.

- To disable access to the management:

  - Log in appliance CLI via ssh admin@(IP address)
  - Run: sfp_access
  - Run: disable

- To show the status:

  - Log in appliance CLI via ssh admin@(IP address)
  - Run: sfp_access
  - Run: status

- Ensure that you disable the management access once configuration is done.

- When the appliance is rebooted, the management access is disabled automatically.

- When virtual service is restarted, the management access remains configured until enable or disable operation is done.

- When the appliance is disabled, the management access to the SFPs is lost.

- When the appliance is re-enabled, the management access is regained.

3. To configure E1 or T1 type for SFP transceiver:

- The client machine must be in the same IP subnet as the appliance management subnet.

- The client machine must have a route to the subnet of SFP transceiver IP address, 192.168.205.0/24, with the appliance management IP as the gateway.
- Open a browser and visit SFP transceiver management
- Default user name: su
- Default password: 1234
- To configure Interface Type (E1 or T1), navigate to **Configuration > Physical Ports** and choose **E1 or T1** from the drop-down menu, and click **Save** button.

Factory Reset

November 4, 2019

Factory Reset via button pushes

You can restore factory default settings on Citrix SD-WAN 210, 410 and 1100 appliances by performing a reset via button pushes.

To perform factory reset on Citrix SD-WAN 410 appliance:

1. Power OFF the appliance using the power button.

   > **Note**
   >
   > Ensure that the appliance is powered up, but is in OFF state.

2. Using a paper-clip, press and hold the NMI reset button for 5+ seconds or until the power LED starts flashing.

3. While the power LED is flashing, press and release the power button to trigger the factory reset process.

To perform factory reset on Citrix SD-WAN 210 and 1100 appliance:

1. Power OFF the appliance using the power button.

   > **Note**
   >
   > Ensure that the appliance is powered up, but is in OFF state.

2. Using a paper-clip, press and release the NMI button, the power LED starts flashing.

3. Press and release the power button within 3 seconds to trigger the factory reset process.

Tip

- Pressing the NMI reset button even number of times cancels the reset action and results in normal appliance reboot.
- Pressing the reset button odd number of times performs a factory reset.
- Power LED flash indicates that the appliance is being reset.

The appliance restarts and the CLI is displayed. The appliance may reboot 4–5 times as it extracts, copies, and initializes the boot process. At the login prompt, you can start configuring the appliance using CLI or the web management interface.

Factory Reset via Internal USB

You can restore factory default settings on Citrix SD-WAN 210, 410, 1100, 2100, 4100, 5100, and 6100 appliances by performing a reset via the internal USB. These appliances have an internal USB drive that stores the factory default settings.

To reset an appliance via Internal USB:

1. Connect a computer to the serial console of the Citrix SD-WAN appliance.
2. Reboot the appliance.
3. While the appliance boots when you see a cursor moving across the screen, perform the following steps:
   a) Press and hold the ESC key.
   b) Press and hold the SHIFT key.
   c) Press the number 1 key (SHIFT +1 = !) and release all keys.
   d) Repeat steps a, b, and c until the cursor stops moving.
4. Select the internal USB option that is displayed on the boot menu.

Note

The internal USB name may vary for different platforms. There may be similar option with UEFI as well on the boot menu, ignore that and select the one with no UEFI.

Premium (Enterprise) Edition

July 26, 2019

> **Important**
>
> The **Enterprise Edition** appliance is rebranded to **Premium**. All references to the term **Enterprise** is applicable to the new product term **Premium**.
>
> Also, the **NetScaler SD-WAN** product is rebranded to **Citrix SD-WAN**. All references to the term **NetScaler SD-WAN** is applicable to the new product term **Citrix SD-WAN**.

The Citrix SD-WAN Premium
(Enterprise) appliances include the following editions:

- SD-WAN Premium (Enterprise) Edition 1000, 2000, and 2100

Citrix SD-WAN 1000, 2000, and 2100 Premium (Enterprise) Edition Appliances

June 19, 2020

The SD-WAN Premium (Enterprise) edition 1000, 2000, and 2,100 appliances combine virtualized instances of WAN optimization and Virtual WAN functionality installed on the appliance. It offers a combination of Virtual WAN and WAN Optimization capabilities.

The SD-WAN 1000 PE, 2000 PE, and 2100 appliances are based on the Citrix branch architecture, which supports multiple virtual machines. All branch appliances contain an SD-WAN instance, a management service instance, and a Xenserver hypervisor.

The SD-WAN instance is typically used in inline mode, with the SD-WAN instance interposed between the WAN router and the LAN, so WAN traffic flows through the accelerated bridge. The SD-WAN instance can also be deployed in virtual inline mode, using a single accelerated bridge port.

In addition to the accelerated bridges and the Windows **LAN port**, a management port connects to all virtual machines (instances) and the hypervisor.

The appliance has two modes, two-port mode and four-port mode, which determine how ports 1/3 and 1/4 are used.

Citrix SD-WAN 2100 PE (EE) Appliance

December 14, 2020

The Citrix SD-WAN 2100 PE (EE) appliance is a 1U appliance. This appliance has 8-core processor with 2.1 GHz and 32 GB of memory.
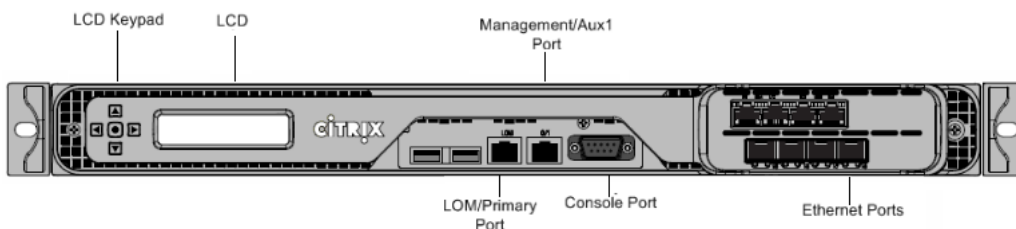
The SD-WAN 2100 PE (EE) appliance has the following ports on the front panel:

- An RS232 serial console port.

- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port for initial provisioning of Virtual WAN. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.

- Two USB ports.

- Four 1000Base-TX copper Ethernet ports (fail-to-wire).

- Four 1GE SFP ports.

Citrix SD-WAN 2100 PE (EE) back panel
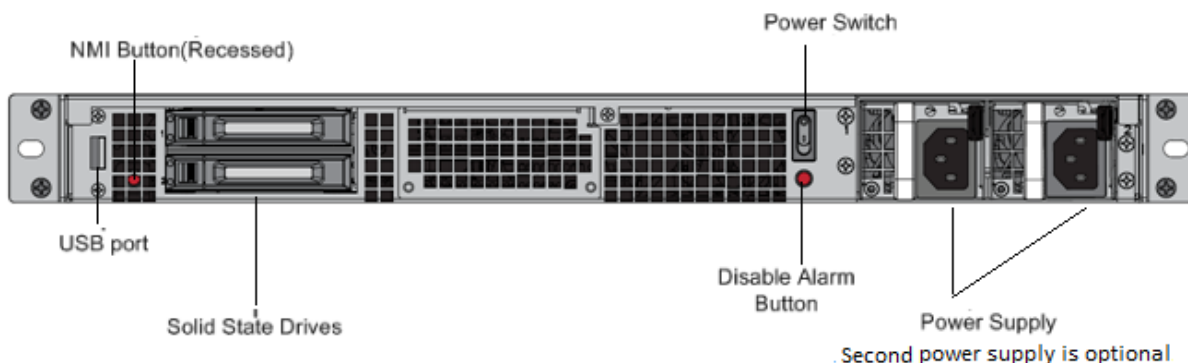
The following components are visible on the back panel of the 2100 PE (EE) appliance:

- 240 GB and 480 GB removable solid-state drives that store the appliance's software and user data.
- Power switch, which switches power to the appliance on or off. Press the switch for five seconds to switch off the power.
- Single power supply, rated at 450 watts, 100–240 volts. Each power supply has an LED indicating its status, as described below. A second power supply is available as an extra accessory (optional Field Replaceable Unit (FRU).

2100 PE has two disks, Drive Bay1 holds 240 GB SSD (boot disk) and Drive Bay2 holds 480 GB SSD. In a case of replacing the old boot disk with a new 240 GB SSD boot disk, it is required to remove both the 240 GB and 480 GB SSDs prior to plugging in the new 240 GB SSD in Bay1 and following it up with

plugging back 480 GB SSD. This is required for the BIOS to refresh the boot order sequence to normal state and ensure it boots from the 240GB SSD (boot disk).

> **Important**
>
> To use PE functionality, you need SD-WAN release 10.0 on the 2100 PE appliances and install PE licenses.

SD-WAN 2000 PE (EE) Appliance

May 23, 2019

The Citrix SD-WAN 2000 PE (EE) platform is a 1U appliance with 1 quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 2000 PE (EE) appliance.

Figure 1. Citrix SD-WAN 2000 PE (EE) appliance, front panel

SD-WAN 2000 PE (EE) appliance has the following ports:

- An RS232 serial console port.

- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.

- A copper Ethernet (RJ45) management port, numbered 0/1, and named PRI (primary). The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of WAN optimization and Windows Server.

  > **Note**: The LOM port also operates as a management port.

- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two *accelerated pairs*, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN 2000 PE appliance.

Figure 2. Citrix SD-WAN 2000 PE appliance, back panel
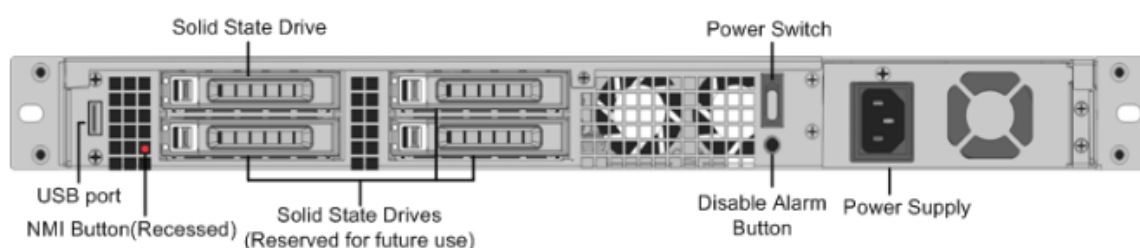
The following components are visible on the back panel of the SD-WAN 2000 PE appliance:

- 600 GB removable solid-state drive, which stores the appliance's software and user data, and 1 TB hard disk drive.
- Power switch, which switches power to the appliance on or off. Press the switch for five seconds to switch off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. Use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 100–240 volts.

Citrix SD-WAN 1000 PE (EE) Appliance

June 19, 2020

The SD-WAN 1000 PE (EE) platform has a quad-core processor and 32 GB of memory. This platform has a bandwidth of up to 100 Mbps.

The following figure shows the front panel of an SD-WAN 1000 PE (EE) appliance.

Figure 1. Citrix SD-WAN 1000 PE (EE), front panel

- The front panel of the SD-WAN 1000 PE (EE) appliance has a power button and five LEDs.
- The power button is used to switch the appliance on or off.
- The reset button restarts the appliance.

The LEDs provide critical information related to different parts of the appliance.

- Power Fail – Indicates the power supply unit has failed.

- Information LED – Indicates the following:

Status	Description
Continuously ON and red	The appliance is overheated.
Slow blink - 1 blink per second	Fan failure, check for an inoperative fan.
Fast blink - 4 blinks per second	Power failure, check for the non-operational power supply.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Fast blink - 3–4 blinks per second	Remote UID is on. Use this function to identify the server from a remote location.

- NIC1 and NIC2 – Indicate network activity on the LAN1 and WAN1 ports.
- HDD – Indicates the status of the hard disk drive.
- Power – Indicates that the power supply units are receiving power and operating normally.

The following figure shows the back panel of an SD-WAN 1000 EE appliance.

Figure 2. Citrix SD-WAN 1000 PE (EE) appliance, back panel

The following components are visible on the back panel of an SD-WAN 1000 PE (EE) appliance:

- Cooling fan
- Single power supply, rated at 200 watts, 110–240 volts
- Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges
- RS-232 serial console port
- One AUX Ethernet port and one management port
- Two USB ports

Power on appliance after a graceful shutdown

1. Connect a Serial console cable to the rear of the appliance and to the serial port on a management laptop.

2. On the management laptop, restart a putty session using the following configuration settings:

   - Serial line: COM1
   - Speed: 9600

3. Power on the appliance and as it is booting, press the following key in the Putty session to enter the **BIOS configuration** screen.
   Keypress: **DEL**

4. When in the BIOS, navigate to,

   - Advanced Tab > **Select**
   - Boot Feature > **Enter**

5. When in the **Boot Feature** screen, change the value of the parameter **Restore on AC Power Loss;** from **Last State** > **Power ON**.

6. Navigate to Save and Exit.

   - Select **Save changes** and **Reset**
   - Select **Yes**

   Allow the system to restart. This takes approximately five minutes.

7. After the appliance is powered on, login to the appliance management instance (SVM). The default IP address for the appliance is: 192.168.100.1, user name is: admin/password.

8. In the SD-WAN appliance GUI, navigate to **Configuration** > **Maintenance** > **Reboot Appliance**. Allow the appliance to fully shut down. Ensure that there are no power lights on the appliance when the shutdown process has completed.

9. Power on the appliance to confirm that the BIOS configuration change has been applied successfully. This can be either done through the APC intelligent PDU Web Management console or by physically pulling the power cable out of the shutdown SD-WAN appliance, waiting for 10 seconds, and then plugging it back in again. The appliance power ups automatically from all shutdown scenarios.

Summary of Hardware Specifications

June 19, 2020

The following tables summarize the specifications of the SD-WAN 1000 PE, 2000 PE, and 2100 PE platforms.

Specifications	SD-WAN 1000 PE	SD-WAN 2000 PE	SD-WAN 2100 PE
Bandwidth	Up to 100 Mbps	Up to 250 Mbps	Up to 1 Gbps
Regulatory model number	NS 6xCu	NS 6xCu	1U1P1A
Processors	4 Core	4 Core	8 Core, 2.1 GHz
Solid State Drives (SSD)	123 GB for Disk-Based Compression (DBC); 25 GB for video caching	225 GB for Disk-Based Compression (DBC); 50 GB for video caching	1X240 GB and 1X480 GB
Memory	32 GB	24 GB	32 GB
Number of power supplies	1 power supply	1 power supply	1 power supply, 1 optional FRU

Specifications	SD-WAN 1000 PE	SD-WAN 2000 PE	SD-WAN 2100 PE
AC power supply input voltage, frequency, and current	100 V ac to 240 V ac, 50–60 Hz, 1.7–3.4 A	100 V ac to 240 V ac, 50–60 Hz, 1.7–3.4 A	100 V ac to 240 V ac, 50–60 Hz, 1.7–3.4 A
DC power supply input voltage and current	-40 to -70 V DC, 4.8 to 8.6A	-40 to -70 V DC, 4.8 to 8.6A	-40 to -72 V DC, 4.8 to 8.6A
Maximum AC power consumption	200 W	300 W	450 W
Airflow (front to rear)	22.1 CFM, Full: 76.2 CFM	22.1 CFM, Full: 76.2 CFM	22.1 CFM, Full: 76.2 CFM
Package weight (lbs.) Shipping dimensions and weight	26 L x 18.5 W x 6.5" H; 14.5 lbs	32 L x 23.5 W x 7.5" H; 39 lbs	33" L x 24" W x 8" H; 40 lbs
System weight (lbs.)	8.5 lbs (3.9 kgs)	32 lbs (14.5 kgs)	32 lbs (14.5 kgs)
Rack Units	1U	1U	1U
Width	EIA 310-D, 19"	EIA 310-D, 19"	EIA 310-D, 19"
Depth	10" 25.4 cm	25.4" (64.5 cm)	28" (71.1 cm)
Operating temperature	10–35 C	0–40 C	32–104 F (0–40 C)
Non-operating temperature	-40 to +70 C	-40 to +70 C	14F to 140F (-10C to 60C)
Humidity range (non-condensing)	8%-90%	5%-95%	20%-80%
Safety certifications	CSA/EN/IEC/UL 60950-1 Compliant, UL, or CSA Listed (USA and Canada), CE Marking (Europe)	CSA/EN/IEC/UL 60950-1 Compliant, UL, or CSA Listed (USA and Canada), CE Marking (Europe)	IEC 60950-1, second Edition, CSA 60950-1, second Edition, UL 60950-1, second Edition, AS/NZS 6050-1

Specifications	SD-WAN 1000 PE	SD-WAN 2000 PE	SD-WAN 2100 PE
EMC & susceptibility	FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM	FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM	US (FCC (Part 15 Class A)), Europe (CE (EN55032/ CISPR32), Australia (RCM), Japan (VCCI), Korea (KCC), Taiwan (BSMI), China (CCC), India (BIS), Russia (EAC), Saudi Arabia (CITC), Brazil (Anatel), South Africa (ICASA), Mexico (NOM), Egypt (NTRA), Israel (MoC)
Environmental certifications	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE

Ethernet Port Names

May 23, 2019

Specify IP addresses for various Ethernet ports of the appliance when configuring the appliance. The Ethernet ports are labeled differently on the front panel of SD-WAN 1000 PE and 2000 PE appliances in the SD-WAN instance, as shown in the following table:

Front Panel		SD-WAN Instance
SD-WAN 1000 PE	**SD-WAN 2000 PE**	
MGMT (Blue)	0/1 (LOM/PRI)	Primary
AUX	0/2 (AUX)	Aux
apA LAN1/WCCP (Green)	1/1	apA.1
apA WAN1	1/2	apA.2
apB LAN2	1/3	apB.1*
apB WAN2	1/4	apB.2*

Available to the SD-WAN instance only in four-port mode.

Installing the Appliance

May 23, 2019

After you have determined that the location where you install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. You can also connect the appliance to a computer through Ethernet port for initial configuration. On SD-WAN 1000 PE appliance, this port is labeled as MGMT (management) port and on SD-WAN 2000 PE, the port is labeled as PRI (primary) port. To complete the installation, you switch on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.

Rack Mount the Appliance

May 23, 2019

An SD-WAN 1000 PE (EE) or 2000 PE (EE) appliance requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.

Rack Mount the Appliance

May 23, 2019

An SD-WAN 1000 PE (EE) or 2000 PE (EE) appliance requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.

Connecting the Cables

June 19, 2020

When the appliance is securely mounted on the rack, determine which ports you should use. You are then ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

> **Warning**: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Ports

A typical installation using a single accelerated bridge uses four Ethernet ports (the Primary port and apA) and six IP addresses (four on the Primary port's subnet and two on apA's subnet).

The appliance has two motherboard ports and two accelerated bridges.

- The motherboard ports are labeled as MGMT (management) and AUX1 (auxiliary) ports in SD-WAN 1000 appliance and PRI (primary) and AUX (auxiliary) in SD-WAN 2000 appliance. You use MGMT port of the SD-WAN 1000 appliance and PRI port of the SD-WAN 2000 appliance for initial configuration.
- Accelerated bridge ports are apA and apB are available on the back panel of SD-WAN 1000 appliance and the front panel of SD-WAN 2000 appliance. On SD-WAN 1000 appliance, these ports are labeled as LAN1 and WAN1, and LAN2 and WAN2, respectively. However, on SD-WAN 2000 appliance, these ports are labeled as 1/1 and 1/2, and 1/3 and 1/4, respectively.

Connecting the ethernet cables

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

To connect an ethernet cable to a 10/100/1000BASE-T port

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port. **On SD-WAN 1000 appliance**, the ports are available on the back panel and labeled as LAN1 and WAN1 for apA bridged port for LAN and WAN links, respectively. **On SD-WAN 2000 appliance**, the ports are available on the front panel. The ports on SD-WAN 2000 are labeled as 1/1 and 1/2 for the apA bridged port. You can use 1/1 for LAN and 1/2 for WAN link.
2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

Connecting the console cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port. **On SD-WAN 1000 appliance**, the port is on the back panel. **On SD-WAN 2000 appliance**, the port is on the front panel.

   > **Note**: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the power cable

An SD-WAN appliance has one power supply. A separate ground cable is not required, because the three-prong plug provides grounding. Provide power to the appliance by installing the power cord. Connect the other end of the power cable to a standard 110V/220V power outlet.

Switch on the Appliance

June 19, 2020

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port, so that you can configure the appliance after it is switched on.
2. Press the **ON/OFF toggle power switch** on the appliance.
3. On SD-WAN **2000** appliance, verify that the LCD on the front panel is backlit and the start message appears

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs, you can quickly remove power from the appliance.

Initial Configuration

May 23, 2019

After checking the connections, you are ready to deploy the SD-WAN 1000 and 2000 appliances on the network.

The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

To perform initial configuration:

- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Perform more configuration for Windows.
- Assign management IP address through the serial console.
- Troubleshoot initial configuration issues.

By default, the initial configuration deploys the appliance in inline mode.

Prerequisites

May 23, 2019

Before you begin configuring the appliance, make sure that the following prerequisites have been met:

- You should have physical access to the appliance.
- In the Worksheet, record all IP addresses and other values you would use to configure the appliance. Preferably, print the worksheet before you start the configuration process.
- You should already have an SD-WAN license key from Citrix, sent in an email. If you are using remote licensing, you need the IP address of the licensing server.
- WAN Send and Receive Speeds.

Configuring the Appliance by Connecting a Computer to the Ethernet Port

June 19, 2020

For initial configuration of an SD-WAN appliance, perform the following tasks:

- Configure the appliance for use on your site.
- Install the Citrix license.
- Enable acceleration.
- Enable traffic shaping (inline mode only).

With inline deployments, this configuration might be all you need, because most acceleration features are enabled by default and require no additional configuration.

You can configure the appliance connecting the appliance to your computer through either the Ethernet port or the serial console. The following procedure enables you to configure the appliance by connecting it to your computer through the Ethernet port.

> **Note**: On an SD-WAN 1000 appliance, you use the Ethernet port labeled as MGMT. However, on SD-WAN 2000 appliance, you use the Ethernet port labeled as PRI or LOM.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your Worksheet by completing the Assigning a Management IP Address through the Serial Console procedure, and then run steps 4 through 25 of the following procedure.

> **Note**: Make sure that you have physical access to the appliance.

To configure the appliance by connecting a computer to the SD-WAN appliance Ethernet port 0/1

1. Set the Ethernet port address of a computer (or other browser-equipped device with an Ethernet port), to 192.168.100.1, with a network mask of 255.255.0.0. On a Windows device, this is done by changing the Internet Protocol Version 4 properties of the LAN connection, as shown below. You can leave the gateway and DNS server fields as blank.
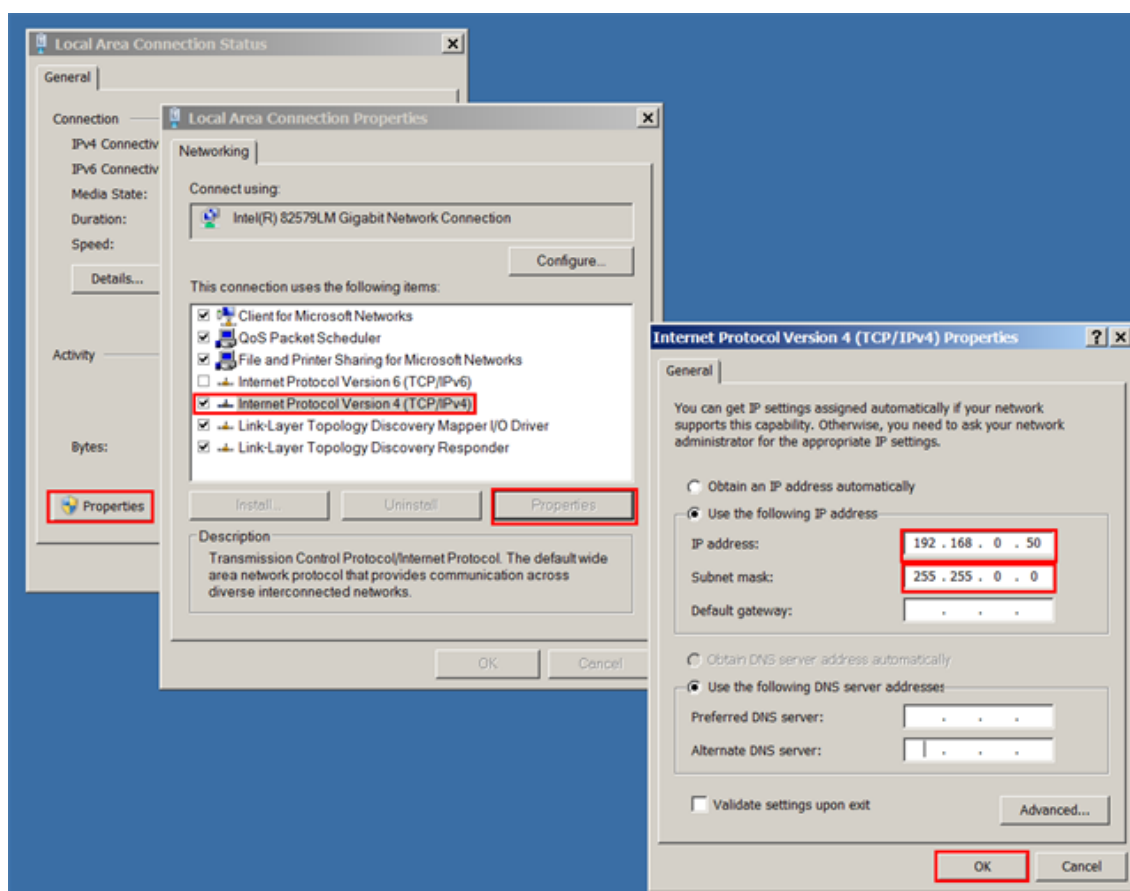
2. Using an Ethernet cable, connect this computer to the port labeled MGMT on an SD-WAN 1000 appliance, or to the port labeled PRI on an SD-WAN 2000 appliance.

3. Switch on the appliance. Using the web browser on the computer, access the appliance by using the default management service IP address http://192.168.100.1.

4. On the login page, use the following default credentials to log on to the appliance.

5. Start the configuration wizard by clicking **Get Started**.

6. On the Platform Configuration page, enter the respective values from your worksheet, as shown in the following example:

> **Note**: If, for SD-WAN configuration, you want to use the same network mask and gateway as those for Network Configuration, select the **Use System Netmask and Gateway** option.

7. Click **Done**. A screen showing the Installation in Progress… message appears. This process takes approximately 2 to 5 minutes, depending on your network speed.

   > **Note**: If you are configuring the appliance by connecting it to your computer through the serial console port, skip step 8 through step 14.

8. A Redirecting to new management IP message appears.

9. Click **OK**.

10. Unplug your computer from the Ethernet port and connect the port to your management network.

11. Reset the IP address of your computer to its previous setting.

12. From a computer on the management network, log on to the appliance by entering the new Management Service IP address, such as `https://<Managemnt_IP_Address>`, in a web browser.

13. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.

14. Log on to the appliance.

15. The Configuration wizard starts again. In this wizard, some of the values which you have already provided, appear by default. Specify rest of the values you have recorded in your worksheet.

16. In **System Services** section, update the values if necessary.

17. In the **Licensing** section, select the appropriate license type. You can either select a local license or a remote license server to apply a license to the appliance.

     a) If you opt for a local license, you must generate a license by using the host ID of the appliance. To generate a local license for the appliance, see http://support.citrix.com/article/ctx131110. To apply the license, you can navigate to the SD-WAN > **Configuration** > **Appliance Settings** > **Licensing** page, after completing the Configuration wizard.

     b) If you opt for a remote licensing server, you must select a remote appliance model and provide the IP address of the licensing server in the **Licensing Server Address** field.

18. In the **WAN Link Definition** section, specify receive and send speeds for the WAN link in the respective fields. Citrix recommends values 10% lower than the WAN bandwidth, to avoid network congestion.

19. By default, **WAN-side adapter** settings are configured on the appliance. Accept the default settings.

20. Click **Install**. After the Installation process is complete, the appliance restarts.

21. When the appliance restarts, the Dashboard page appears.
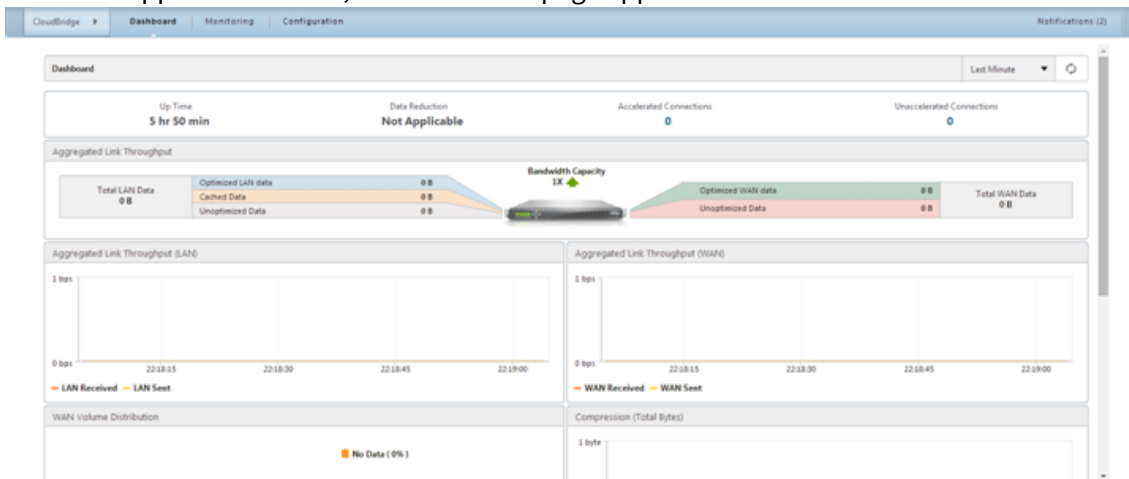
22. To configure the appliance to accelerate the network traffic, open navigate to the **Configuration** tab.

> **Note**: Make sure that you have already applied the appropriate license to the appliance.

23. On the Network Adapters page of the Appliance Settings node, verify and, if necessary, assign IP addresses, subnet masks, and gateways to the accelerated bridges (apA and apB) to be used. Applying these changes restarts the appliance.

> **Note**: You need to assign IP addresses to apA and apB adapters only if you intended to configure WCCP mode, virtual inline mode, or the Video Caching feature on the appliance.

24. The Initial Configuration is complete. Traffic now flows through the appliance. The Dashboard page shows this traffic.
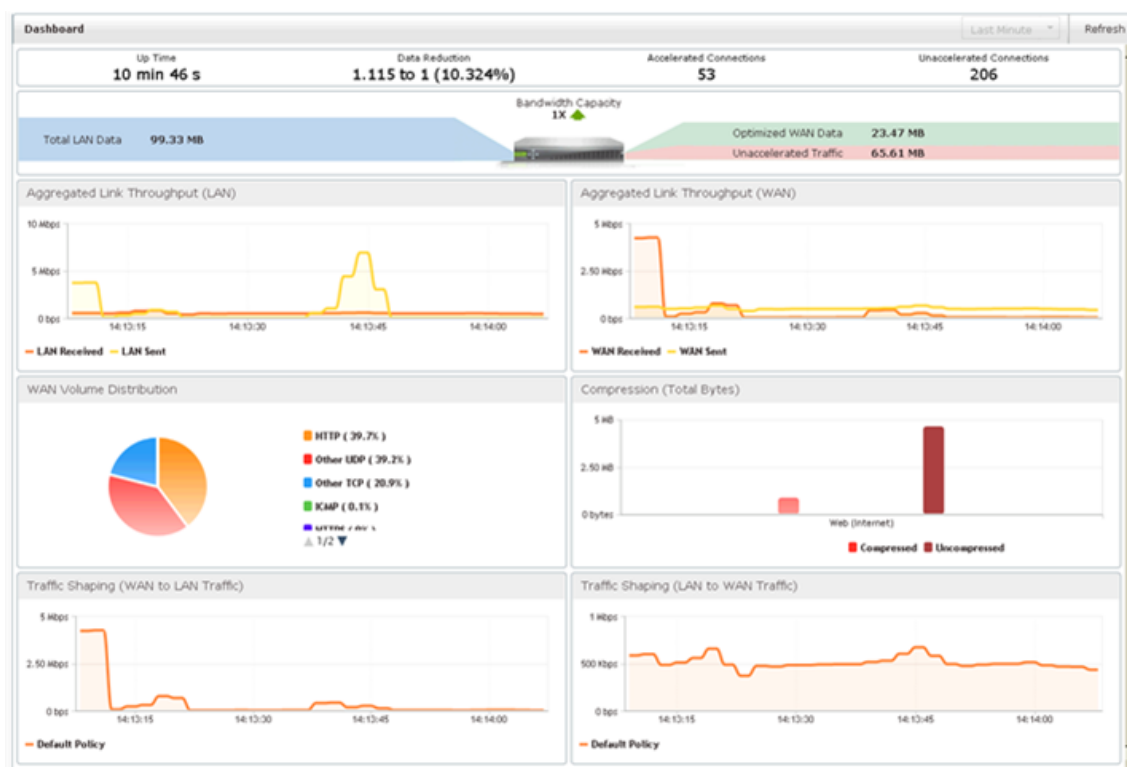
25. You need more configuration on the appliance if you intend to use some of the modes and features, such as, virtual inline mode, video caching, secure peering, high availability, encrypted CIFS/MAPI acceleration, AppFlow monitoring, or SNMP monitoring.

Note:

- Inline installations place the appliance between your LAN and WAN routers, using both ports of the accelerated bridge, such as ports LAN1 and WAN1 on an SD-WAN 1000 appliance with Window Server or ports 1/1 and 1/2 on SD-WAN 2000 appliance with Windows Server, for the apA accelerated bridge port.
- WCCP and virtual inline installations connect a single accelerated bridge port to your WAN router.
- Virtual inline installations require that you configure your router to forward WAN traffic to the appliance. See Router Configuration.
- WCCP installations require configuration of your router and the appliance. See WCCP Mode.

Assigning a Management IP Address through the Serial Console

May 23, 2019

If you do not want to change the settings of your computer, you can perform initial configuration by

---

connecting the appliance to your computer with a serial null modem cable. Make sure that you have physical access to the appliance.

To configure the appliance through the serial console

1. Connect a serial null modem cable to the appliance's console port.

2. Connect the other end of the cable to the serial COM port of a computer running a terminal emulator, such as Microsoft HyperTerminal, with settings 9600, N,8,1, p.

3. On the **HyperTerminal output**, press **Enter**. The terminal screen displays the Logon prompt.

   > **Note**: You might have to press **Enter** two or three times, depending on the terminal program you are using.

4. At the logon prompt, log on to the appliance with the following default credentials:

   - **Username**: nsroot
   - **Password**: nsroot.

5. At the **$** prompt, run the following command to switch to the shell prompt of the appliance:
   `$ ssh 169.254.0.10`

6. Enter **Yes** to continue connecting to the management service.

7. Log on to the shell prompt of the appliance with the following default credentials:

   - **Password**: nsroot.

8. At the logon prompt, run the following command to open the **Management Service Initial Network Address Configuration** menu: `## networkconfig`

9. Type **1** and press **Enter** to select option 1, and specify a new management IP address for the management service.

10. Type **2** and press **Enter** to select option 2, and specify a new management IP address for the XenServer server.

11. Type **3** and press **Enter** to select option 3, and then specify the network mask for the management service IP address.

12. Type **4** and press **Enter** to select option 4, and then specify the default gateway for the management service IP address.

13. Type **8** and press **Enter** to save the settings and exit.

14. Access the SD-WAN appliance by entering the new management service IP address of the appliance, such as `https://<Management_Service_IP_Address>`, in a web browser of a computer on the management network.

---

15. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.

16. Run steps 4 through 25 of the Configuring the Appliance by Connecting a Computer to the Ethernet Port procedure to complete the configuration process.

Setting up the SD-WAN Appliance

June 19, 2020

To set up the SD-WAN appliance hardware, see the instructions documented in the Setting up the appliance hardware section.

Citrix SD-WAN 5100 Premium (Enterprise) Edition Appliance

June 19, 2020

Citrix SD-WAN Premium (Enterprise)Edition 5100 appliances are high-performance appliances for busy datacenters.

This appliance is designed to operate Virtual WAN links with speeds more than 1 Gbps for busy datacenters that communicate with many branch and regional sites.

SD-WAN 5100 PE (EE) is recommended at the hub of a hub-and-spoke deployment, where smaller appliances are used at the spokes, whenever the link speed or the number of XenApp/XenDesktop users is higher than that can be supported by a smaller appliance.

Citrix SD-WAN 5100 PE

June 26, 2020

The SD-WAN 5100 PE is a 2U appliance. Each model has two 10-core processors for a total of 20 physical cores (40 cores with hyper-threading), and 128 GB (GB) of memory. For latest performance and bandwidth capacity details, see the latest datasheet that gets updated more regularly at: citrix.com; datasheet.

The SD-WAN 5100 PE appliance front panel has the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called lights out management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.
- Eight 10G ports - 4 LC fiber ports with bypass, 4 SFP+ ports (no bypass).
- Two USB ports (reserved for a future release).

The following components are visible on the back panel of the SD-WAN 5100 PE appliance:

- 2 X 1 TB removable hard disk drive.
- Requires 960 GB more SSD. Insert the SSD into the third, fourth, and fifth drive bays.
- Boot drive bay 1, 2- [HDDs] - Hard Drive, Capacity 1TB, 2.5", SATA 6Gb/s.
- Drive bay 3,4,5-[SSDs]- Solid State Drive, 960GB.
- Drive bay 6,7,8-[Plastic Filler] - 2.5" SSD Plastic Drive Tray Filler.
- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable PS alarm button. This button is functional only when the appliance has two power supplies. Press this button to mute the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual redundant, hot-swappable power supplies (100-240VAC standard, -48VDC optional).

The power supplies used for 5100 appliance is two power supplies each 1000W.

Upgrades from Standard Edition to Premium Edition use 960G SSDs, three of the SSDs installed in bays 3, 4 & 5.

Upgrade 5100 SE appliance to 5100 PE appliance

Insert solid state drive (SSD)

1. Insert the required SSD in the standard edition appliance. For instructions about how to insert SSD, see Solid State Drive (Field Replaceable Unit).
   a) 5100 SE appliance requires 960 GB more SSD. Insert the SSD into the third, fourth, and fifth drive bays.
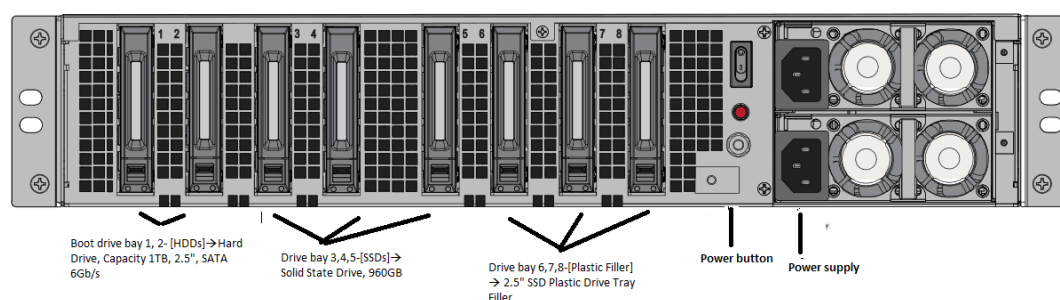
Boot drive bay 1, 2- [HDDs]→Hard Drive, Capacity 1TB, 2.5", SATA 6Gb/s   Drive bay 3,4,5-[SSDs]→ Solid State Drive, 960GB   Drive bay 6,7,8-[Plastic Filler] → 2.5" SSD Plastic Drive Tray Filler   Power button   Power supply

2. Restart the appliance through the SD-WAN web management interface.

3. Ensure that the software release version installed on the appliance is SD-WAN release version 10.0. Follow the steps provided here; upgrade new appliance.

4. Install the Premium (Enterprise) Edition platform license. For license information, see the Citrix SD-WAN product downloads site.

5. Upgrade the network using single step upgrade to software release version 10.0 or later.

Summary of Hardware Specifications

June 19, 2020

The following table summarizes the specifications of Citrix SD-WAN 5100 PE hardware platforms.

Specifications	SD-WAN 5100 PE
Regulatory Model Number	2U1P1D
Processors	Two 10-core
Memory	128 GB
Number of power supplies	1 (optional second power supply for redundancy)
AC power supply, input voltage, frequency and current	100-240 V AC, 47–63 hz; 9.0-4.5 A
Maximum AC power consumption	850 W
Package weight	69 lbs
Shipping dimensions	36.5' L X 24.5' W X 11' H
System weight	60 lbs
Rack unit	2RU
Rack options - Width	EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting bracket

Specifications	SD-WAN 5100 PE
Depth	28" (72 cm)
Operating temperature	32–104 F (0–40 C)
Humidity (non-condensing)	20% - 80%
Safety certifications	CSA
EMC and susceptibility	USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC), Taiwan (BSMI), Brazil (Anatel), Israel (MoC)
Environmental compliance	ROHS, WEEE

6100 Standard Edition and Premium Edition appliance

March 4, 2021

The Citrix SD-WAN 6100 Standard Edition (SE)/ Premium Edition (PE) is a 2U appliance. Each model has two 14-core processors for a total of 28 physical cores (with hyper-threading enabled), and 256 GB of memory. For latest performance and bandwidth capacity details, see the Citrix SD-WAN data sheet.

The following Citrix SD-WAN software versions are supported on the 6100 appliance editions:

- Citrix SD-WAN 6100 SE – Citrix SD-WAN 10.2.3 and above.
- Citrix SD-WAN 6100 PE - Shipped with Citrix SD-WAN 10.2.7 image, upgrade the software to Citrix SD-WAN 11.2.1 and above to enable PE functionality.

The Citrix SD-WAN 6100 SE/PE appliance front panel has the following ports:

Port	Description
0/1, 0/2	10/100/1000 Base-T copper Ethernet management ports (RJ45)
1/1, 1/2, 1/3, 1/4	1000 Base-TX Fail-To-Wire
10/1, 10/2, 10/3, 10/4	10G Base-SR Fail-To-Wire
10/5, 10/6, 10/7, 10/8	10G SFP+

The following components are visible on the back panel of the Citrix SD-WAN 6100 SE/PE appliance:

For Citrix SD-WAN 6100 SE [SSD Configuration]

- Drive bay 3 - 2.5" Boot drive SSD with 480 GB capacity
- Drive bay 1, 2, 4 - 2.5" SSD Plastic Drive Tray "Fillers- Dummy"

For Citrix SD-WAN 6100 PE [SSD Configuration]

- Drive bay 3 - 2.5" Boot drive SSD with 480 GB capacity
- Drive bay 1, 2, 4 - 2.5" 960 GB SSD.

Power Switch and back end Button functionalities:

- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.

- Disable PS alarm button is functional only when the appliance has two power supplies.

  Press this button to mute the power alarm from sounding:

    - When you have plugged the appliance into only one power outlet.
    - When one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.

- Dual redundant, hot-swappable power supplies (100–240 VAC standard 1,000 W, 48 V DC optional).

Convert the Citrix SD-WAN 6100 SE appliance to the Citrix SD-WAN 6100 PE appliance

1. Insert the required SSD in the Citrix SD-WAN SE appliance.

- Drive bay 3-Insert 2.5" Boot drive SSD with 480 GB capacity.
- Drive bay 1, 2, and 4- Insert 2.5" 960 GB SSD.
  For instructions about how to insert SSD, see Solid State Drive.

1. Restart the appliance through the SD-WAN web management interface.

2. Ensure that the software release version installed on the appliance is Citrix SD-WAN 11.2.1 or above. If the appliance is running a version lower than 11.2.1, upgrade the software to 11.2.1 and perform a local change management. For upgrade instructions, see Upgrade paths.

3. Install the Premium Edition platform license. For license information, see Citrix SD-WAN product downloads.

Summary of hardware specifications

The following table summarizes the specifications of Citrix SD-WAN 6100 SE hardware platform.

Specifications	Citrix SD-WAN 6100 SE/PE
Compliance Regulatory Model number	2U1P1A
Processors	2x 14 Core processor (Intel E5-2680 v4 14-core, 2.4 GHz)
Memory	256 GB 2,400 MHz, 8x 32 GB RDIMM

Specifications	Citrix SD-WAN 6100 SE/PE
Number of power supplies	2 (Each 1,000 W; Dual Redundant Hot swappable)
AC power supply, input voltage, frequency, and current	100–240 V AC, 50–60 Hz, 5.5-2.8A
DC input voltage and Current	-36 V DC to -72 V DC, 15.4-7.7A
Typical AC power consumption	357 W
Maximum AC power consumption	480 W
Typical Heat Dissipation	1251 BTU/Hr
Max Heat Dissipation	1218 BTU/Hr
Typical Airflow (front to rear)	65 CFM
Max Airflow (front to rear)	125 CFM
Altitude Range	Max 5,000 m (Up to 16,000 ft)
Solid State Drives (SSD)	1x480GB and 3x960GB SSD (1.2GB DBC, applicable for PE only)
Package weight	69 (lbs) (31.3 Kg)
Shipping dimensions	36.5' L X 24.5' W X 11' H (94 x 63 x 28 cm)
System weight (lbs)	60 (lbs) (27.2 Kg)
Rack Height	2U
Rack Width	EIA 310-D for 19 (inch) racks
Rack Depth	28 inches (71.1 cm)
Operating temperature	0–45°C (32–113°F)
Humidity (non-condensing)	5% - 95%
Safety certifications	IEC 60950-1, second Edition
	CSA 60950-1, second Edition
	UL 60950-1, second Edition
	AS/NZS 60950-1

Specifications	Citrix SD-WAN 6100 SE/PE
EMC and susceptibility	US (FCC (Part 15 Class A)), Europe (CE (EN55032/55024)), Australia (RCM), Japan (VCCI), Korea (KCC), Taiwan (BSMI), China (CCC), India (BIS), Russia (CUTR), Russia (EAC), Saudi Arabia (CITC), Brazil (Anatel), South Africa (ICASA), Mexico (NOM), Egypt (NTRA), Israel (MoC)
Environmental compliance	ROHS, WEEE, REACH

Citrix SD-WAN 1100 Standard Edition and Premium Edition

October 5, 2021

The Citrix SD-WAN 1100 standard and premium edition appliance is a desktop form factor appliance. Each model has 8-core processor with 24 GB memory and 480 GB of storage (SSD drive).

The following figure shows the front panel of the 1100 SE and PE appliance.

Figure 1. Citrix SD-WAN 1100 SE and PE, front panel

Table 1. LED power supply indicators

LED Color	LED Indicates
Ethernet ports	Active/Link: Green, Speed -1000 Orange, Speed-100: Green, Speed-10: off
Bypass LEDs	Normal Mode: Green, Bypass Mode: Orange
Small Form-factor Pluggable (SFP) Port LEDs	Active/Link: Green, Speed- 1000: Orange
Power LEDs	Power on: Green, Power off: off

The appliance has the following ports:

- Serial console port.
- One 10/100/1000 Base-T copper Ethernet management port (RJ45). The management port is used to connect directly to the appliance for system administration functions.
- Two como ports (1/5 and 1/6). One can use RJ45 or SFP port at a time.
- 480 GB solid-state drive, which is used to store the Citrix SD-WAN software and the user data.
- Power switch, which turns off power to the appliance, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Two Power over Ethernet (POE) ports (1/7 and 1/8). Each port has <30 watts output.
- Two sets of FTW ports, (1/1, 1/2), and (1/3, 1/4).
- USB ports.
- Single power supply. Second power supply (optional) for redundancy, each rated at 150 W.

Accessory FRUs:

- Rackmount Kit
- Extra power adapter and power cord – connected to DC Jack 2

- SFP transceiver and cable (s)

Citrix SD-WAN 1100 SE and PE back panel:

Citrix SD-WAN 1100 SE and PE back panel labeled:

For information about installing the rails, rack mounting the hardware, and connecting the cables, see
Installing the Hardware.

Ports	Supported speeds
1/1-1/4	100/1000

Ports	Supported speeds
1/5-1/6	RJ45: 1000 only, SFP: 100 (certain SFPs)/1000
1/7-1/8	100/1000

Citrix SD-WAN 1100 enhancement on SFP to support High Availability with Y-Cable

The available SFP ports on 1100 appliances can be used with fiber optic Y-Cables to enable high availability feature for Edge Mode deployment. On the 1100 SE/PE appliance the splitter cable split end connects to fiber ports of two 1100 appliances that are configured in high availability pair. For more information, see Enable Edge Mode High Availability Using Fiber Optic Y-Cable.

Citrix SD-WAN 1100 platform support for MiRiC-E1T1 FE/GBE SFP

The following two types of MiRiC SFPs are supported on the 1100 appliance for SFP ports 1/5 and 1/6.

1. MiRiC-E1T1 FE SFPs.
2. MiRiC-E1T1 GBE SFPs.

MiRiC-E1T1 FE SFPs must configure with speed as 100 Mbps and duplex as full. MiRiC-E1T1 GBE SFPs must configure with speed as 1 Gbps and duplex as full.

To configure, go to SD-WAN appliance GUI, navigate to **Configuration > Network Adapters > Ethernet page**.

Access MiRiC SFP web service

1. The SFP transceivers have default management IP address of 192.168.205.1, which can be used for the SFP web service to configure relevant configurations, for example; T1 or E1. The IP ad-

dress can be modified other than 192.168.205.1. However ensure that you avoid IP address conflicts.

2. To enable SFP access to the management:

   - Log into the appliance CLI via **ssh admin@(ip address)**

   - Run: sfp_access

   - To enable access on 1/5, execute one of the following commands.

     – enable 1/5 # Works for GBE transceivers only if already configured.
     – enable 1/5 100 # - Works only for FE transceivers
     – enable 1/5 1000 # - Works only for GBE transceivers
     – enable 1/5 100 172.217.43.2 # - For FE transceivers and assumes a user changes the default IP to an IP in 172.217.43.0/24

   - enable 1/5 1000 172.217.43.2 # - For GBE transceivers and assumes a user changes the default IP to an IP in 172.217.43.0/24

     Note:

     Enabling management access on 1/5 automatically disables management access on 1/6, and vice versa.

   - To disable access to the management:

     – Log in appliance CLI via ssh admin@(IP address)
     – Run: sfp_access
     – Run: disable

   - To show the status:

     – Log in appliance CLI via ssh admin@(IP address)
     – Run: sfp_access
     – Run: status

   - Ensure that you disable the management access once configuration is done.

   - When the appliance is rebooted, the management access is disabled automatically.

   - When virtual service is restarted, the management access remains configured until enable or disable operation is done.

   - When the appliance is disabled, the management access to the SFPs is lost.

   - When the appliance is re-enabled, the management access is regained.

3. To configure E1 or T1 type for SFP transceiver:

   - The client machine must be in the same IP subnet as the appliance management subnet.

- The client machine must have a route to the subnet of SFP transceiver IP address, 192.168.205.0/24, with the appliance management IP as the gateway.
- Open a browser and visit SFP transceiver management
- Default user name: su
- Default password: 1234
- To configure Interface Type (E1 or T1), navigate to **Configuration > Physical Ports** and choose **E1 or T1** from the drop-down menu, and click **Save** button.

Factory Reset

November 4, 2019

Factory Reset via button pushes

You can restore factory default settings on Citrix SD-WAN 210, 410 and 1100 appliances by performing a reset via button pushes.

To perform factory reset on Citrix SD-WAN 410 appliance:

1. Power OFF the appliance using the power button.

   > **Note**
   >
   > Ensure that the appliance is powered up, but is in OFF state.

2. Using a paper-clip, press and hold the NMI reset button for 5+ seconds or until the power LED starts flashing.

3. While the power LED is flashing, press and release the power button to trigger the factory reset process.

To perform factory reset on Citrix SD-WAN 210 and 1100 appliance:

1. Power OFF the appliance using the power button.

   > **Note**
   >
   > Ensure that the appliance is powered up, but is in OFF state.

2. Using a paper-clip, press and release the NMI button, the power LED starts flashing.

3. Press and release the power button within 3 seconds to trigger the factory reset process.

Tip

- Pressing the NMI reset button even number of times cancels the reset action and results in normal appliance reboot.
- Pressing the reset button odd number of times performs a factory reset.
- Power LED flash indicates that the appliance is being reset.

The appliance restarts and the CLI is displayed. The appliance may reboot 4–5 times as it extracts, copies, and initializes the boot process. At the login prompt, you can start configuring the appliance using CLI or the web management interface.

Factory Reset via Internal USB

You can restore factory default settings on Citrix SD-WAN 210, 410, 1100, 2100, 4100, 5100, and 6100 appliances by performing a reset via the internal USB. These appliances have an internal USB drive that stores the factory default settings.

To reset an appliance via Internal USB:

1. Connect a computer to the serial console of the Citrix SD-WAN appliance.
2. Reboot the appliance.
3. While the appliance boots when you see a cursor moving across the screen, perform the following steps:
    a) Press and hold the ESC key.
    b) Press and hold the SHIFT key.
    c) Press the number 1 key (SHIFT +1 = !) and release all keys.
    d) Repeat steps a, b, and c until the cursor stops moving.
4. Select the internal USB option that is displayed on the boot menu.

Note

The internal USB name may vary for different platforms. There may be similar option with UEFI as well on the boot menu, ignore that and select the one with no UEFI.

VPX models

July 26, 2019

> **Important**
>
> The **NetScaler SD-WAN** product is rebranded to **Citrix SD-WAN**. All references to the term **NetScaler SD-WAN** is applicable to the new product term **Citrix SD-WAN**.

The Citrix SD-WAN VPX (Virtual) appliances include the following editions:

- SD-WAN VPX-SE
- SD-WAN VPX-WANOP
- SD-WAN VPX-L

Citrix SD-WAN VPX Standard Edition

June 19, 2020

Citrix SD-WAN Standard Edition is a virtual Citrix SD-WAN appliance that can be hosted on Citrix XenServer, VMware ESX or ESXi, Microsoft Hyper-V, and Amazon AWS-virtualization platforms. An SD-WAN VPX appliance supports most of the features of a physical Standard Edition or WANOP appliances.

Because SD-WAN SE Edition VPX is a virtual machine, you can deploy your choice of hardware, exactly where you need it, and in combination it with other virtual machines – servers, VPN units, or other appliances – to create a unit that precisely suits your needs.

SD-WAN Standard Edition VPX software is available as:

- A Xen virtual machine running under XenServer 6.5 SP1.
- A VMware vSphere virtual machine running under ESX/ESXi 5.5, 6.0, and 6.5.

When a newly installed SD-WAN SE VPX virtual machine is up and running, you configure as you would configure a physical SD-WAN SE appliance, using the same configuration screens.

Differences between WANOP VPX and Physical SD-WAN WANOP Appliances

An SD-WAN WANOP VPX virtual appliance is similar to an SD-WAN Repeater 8500 series appliance, including support for the
SD-WAN Plug-in and links of up to 45 mbps. Following are the key differences:

- Except for Amazon EC2 instances, licensing via remote license servers is mandatory for retail licenses. Local licensing is available for non-retail licenses, such as evaluation and VPX Express licenses. For Amazon EC2 instances, you can use either Citrix licensing or select a product with built-in licensing for the bandwidth limit you desire (2, 10, 20, or 45 Mbps).
- SD-WAN VPX obtains its SD-WAN Plug-in licenses from the remote license server (except for SD-WAN VPX for Amazon Web Services, which does not support Plug-ins). Plug-ins connecting to

multiple virtual appliances consume only a single Plug-in license, not one license per appliance, as long as all virtual appliances use the same license server.

- The SD-WAN LCD front-panel display is not supported.
- The **RS-232 serial** command interface is not supported.
- Multiple accelerated bridges are not supported.
- Ethernet bypass cards are not supported.
- Group mode is not supported.
- SD-WAN High-availability mode is not supported. (XenServer high availability and vSphere high availability are supported.)
- Three ports are supported (apA.1, apA.2, and Primary), except for Amazon Web Services instances, which support only a single port.

For step-by-step instructions on installing and deploying an SD-WAN VPX-SE, see the following:

- Installing VPX-SE on VMware ESXi – See Installing and Deploying an SD-WAN VPX-SE on ESXi.
- Installing SD-WAN VPX-SE on XenServer – The procedures for installing an SD-WAN Virtual WAN (Standard Edition) VPX (SD-WAN VPX-SE) and an SD-WAN WAN Optimization appliance (WANOP VPX) are similar. However, there are some critical differences, as outlined in Differences Between an SD-WAN VPX-VW and WAN OP VPX Installation.

Prerequisites

January 21, 2021

This section outlines the hardware and software requirements for Citrix SD-WAN Virtual Appliance (SD-WAN VPX-SE), and defines the platform dependencies.

> **NOTE**
>
> - From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.
>
> - A system maintenance account - CBVWSSH, exists for development and debugging and has no external login permissions. The account can only be accessed through a regular administrative user's CLI session.

With 10.2.6 release, the default password is the serial number of the SD-WAN appliance and is mandated to change on first time logon. The LOM access will also be disabled.

Hardware requirements

The SD-WAN VPX-SE hardware requirements for the hosting platform are as follows:

- Virtual CPUs: 4 Core, 2.7 GHz (or equivalent) processor or better.
- Memory: 4 GB RAM
- Management Interface: 1 (default)

Disk space requirements

Virtual path count	MCN/RCN	Branch
Less than 128	120 GB	40 GB (Default)
Greater or equal to 128	240 GB	120 GB

Software requirements

This section outlines the software requirements for the SD-WAN VPX-SE, and basic information on acquiring and downloading the SD-WAN VPX-SE software.

Operating system requirements

SD-WAN VPX-SE Virtual Appliance supports the following server platforms:

- XenServer Hypervisor 6.5 SP1
- VMware Hypervisor ESXi server, version 5.5.0 or higher
- Microsoft Azure
- AWS
- Linux-KVM

Browser requirements

Browsers must have cookies enabled, and JavaScript installed and enabled.

The SD-WAN VPX-SE Management Web Interface supports the following browsers:

- Google Chrome 49.0.2623112 m+
- Mozilla Firefox 43.0.4+
- Microsoft Internet Explorer 11.0.9600.18163+

Downloading the installation files

Before beginning the installation, you must download or copy the SD-WAN VPX-SE OVF template (.ova file) to the local PC you are using to connect to the ESXi server that will host your SD-WAN VPX-SE.

> **Note**
>
> Remote licenses are supported for SD-WAN VPX-VW. For additional information on licensing and downloading SD-WAN software, see the sections, Licensing and Acquiring the SD-WAN Software Packages.

To download the SD-WAN VPX-SE installation files, go to the following URL:

http://www.citrix.com/downloads.html

Instructions for downloading the software are provided on this site.

Download the appropriate file, as follows:

- To install SD-WAN VPX-SE on XenServer, download this file: cb-vw-vpx-<version>.xva

- To install SD-WAN VPX-SE on VMware ESXi Server, download this file: cb-vw-vpx-<version>_vmware.ova, where <version> is the current SD-WAN SE version number.

The following section provides a summary of the steps and procedures involved in installing and configuring an SD-WAN VPX-SE Virtual Appliance.

Interface specifications

The SD-WAN VPX-SE interface specifications are as follows:

- SD-WAN VPX-SE supports a maximum number of five interfaces.
- The first interface is reserved for use as the Management IP Address for the Virtual Appliance.
- Before powering up the new VM for the SD-WAN VPX-SE Virtual Appliance, you must configure and assign more interfaces (one each) for the LAN and WAN.
- For SD-WAN VPX-SE, bridges are not created by default for the data interface (for example, eth1 and eth2).

Supported topology deployments

Deployments that are supported for hardware SD-WAN Appliances are also supported for SD-WAN VPX-SE. SD-WAN VPX-SE supports both 1-arm and In-line deployments. WCCP is not supported.

Checklist

June 19, 2020

Gather the following information:

> • **Note** the IP Address of the ESXi server that will host the SD-WAN VPX-SE Virtual Machine (VM).

- Select a unique name to assign to the SD-WAN VPX-SE VM.

- Determine the amount of memory to allocate for the SD-WAN VPX-SE VM.

- Determine the amount of disk capacity to allocate for the virtual disk for the VM (default disk space requirement is 39.1 GB).

- If you are not using DHCP, note the IP Address you intend to assign as the static Management IP Address for the SD-WAN VPX-SE. (By default, SD-WAN VPX-SE uses DHCP).

- Determine the Gateway IP Address the SD-WAN VPX-SE will use to communicate with external networks.

  > • **Note** the subnet mask for the network in which the SD-WAN VPX-SE will reside.

Citrix SD-WAN VPX-SE Versus VPX-WANOP

June 19, 2020

This section outlines the essential differences between installing a SD-WAN VPX (VPX-SE) for deployment in your SD-WAN network, as compared to a SD-WAN VPX for WAN Optimization.

The primary differences when installing and configuring a SD-WAN VPX-SE virtual appliance from SD-WAN WANOP VPX, are as follows:

- Download the following installation files from the Citrix SD-WAN downloads site (http://www. citrix.com/downloads.html).

> **Note**
>
> Remote licenses are supported for SD-WAN VPX-SE.

- To install SD-WAN VPX-SE on XenServer, download this file: `*cb-vw-vpx-\<version\>.xva*`
- To install SD-WAN VPX-SE on VMware ESXi Server, download this file: `*cb-vw-vpx-\<version \>\\_vmware.ova*`

Where *<version>* is the current SD-WAN version number.

> **Note**
>
> For additional information on licensing and downloading SD-WAN software, see the sections, Licensing and Acquiring the SD-WAN Software Packages.

- SD-WAN VPX-SE Virtual Appliance supports the following server platforms:
  - XenServer Hypervisor 6.5 SP1

- VMware Hypervisor ESXi server, version 5.5.0 or higher
- SD-WAN VPX-SE supports both Inline and PBR deployments; however, WCCP deployments are not supported for VPX-SE.
- The Virtual Machine for the SD-WAN VPX-SE Virtual Appliance must be installed manually, on either the XenServer or VMware ESXi Server platform. Currently, there is no installation wizard for this procedure.
- The minimum configuration requirements for the Virtual Machine are as follows:
  - **Virtual CPUs: 4**
  - **Memory**: 4GB RAM
  - **Virtual Datastore**: 40 GB disk
  - **Management Interface**: 1 (default)
- SD-WAN VPX-SE interface specifications are as follows:
  - SD-WAN VPX-SE supports a maximum number of five interfaces.
  - The first interface is reserved for use as the Management IP Address for the Virtual Appliance.
  - Before powering up the new VM for the SD-WAN VPX-SE Virtual Appliance, you must configure and assign additional interfaces (one each) for the LAN and WAN.
  - For VPX-SE, bridges are not created by default for the data interface (for example, eth1 and eth2).
- If you are not using DHCP, you must configure a static Management IP Address for the SD-WAN VPX-SE Virtual Appliance.

Note

DHCP is enabled by default for the SD-WAN VPX-SE Management IP Address.

To configure a static Management IP Address for a SD-WAN VPX-SE Virtual Appliance, do the following:

1. Open the vSphere Client or XenServer Client where you created the SD-WAN VPX-SE Virtual Machine (VM).

2. Open the vSphere or XenServer Console for the new SD-WAN VPX-SE, and log into the Administrator account for the VM.

   - Default Administrator user name: **admin**
   - Default Administrator password: **password**

3. Enter the following command lines at the console CLI prompt:

   ```
   pre codeblock management_ip set_management_ip set interface <ip> <
   subnetmask> <gateway> <!--NeedCopy-->
   ```

   Where:

   - <ip> is the Management IP Address for the SD-WAN VPX-SE Virtual Appliance.*
   - <subnetmask>* is the subnet mask used to define the network in which the SD-WAN VPX-SE

Virtual Appliance resides.

- <gateway>* is the Gateway IP Address of the SD-WAN VPX-SE Virtual Appliance will use to communicate with external networks.

4. Restart the SD-WAN VPX-SE Virtual Appliance VM.

Note

See also the section, Setting the Management IP Addresses for the Appliances.

Overview of VPX Installation and Deployment

June 19, 2020

This section provides a summary of the steps involved for installing and deploying a SD-WAN VPX-SE Virtual Appliance.

You can install SD-WAN VPX-SE on the following platforms:

- **VMware ESXi** – For instructions, see Installing and Deploying a SD-WAN VPX-SE on ESX.
- **XenServer** – The procedures for installing a SD-WAN VPX (VPX-SE) and a SD-WAN (WAN Optimization) VPX are very similar. For instructions on installing a SD-WAN WANOP VPX on XenServer, see the chapter entitled, "CloudBridge VPX," in the document entitled, Citrix CloudBridge 7.4 Product Documentation, available on the Citrix Documentation Portal (http://docs.citrix.com/). See also, Differences Between a SD-WAN VPX-SE and WANOP VPX Installation.

Summary of Procedures for Deploying a SD-WAN VPX-VW on ESXI

The following list summarizes the steps and procedures involved in deploying a SD-WAN VPX-SE on a VMware ESXi server.

1. Gather your SD-WAN VPX-SE installation and configuration information. For instructions, see SD-WAN VPX-SE Installation and Configuration Checklist.
2. Install the VMware vSphere Client. For instructions, see Installing the VMware vSphere Client.
3. Install and deploy the SD-WAN VPX-SE OVF Template. For instructions, see Installing and Deploying the SD-WAN VPX-SE OVF Template.
4. Configure the SD-WAN VPX-SE Management IP Address. For instructions, see Configuring the Management IP Address for the SD-WAN VPX-SE
5. Connect to the SD-WAN VPX-SE and test the deployment. For instructions, see Connecting to the SD-WAN VPX-SE and Testing the Deployment.

Virtual Ethernet Ports Per VPX-SE/VPXL-SE Platforms

June 19, 2020

In SD-WAN 9.3 release, the VPX-SE/VPXL-SE platforms support 4 Virtual Ethernet interface only. This leads to deployment issues when multiple VLANs are mapped to the same interface (debuggability). In SD-WAN 10.0, support for additional ports for VPX-SE high availability deployments between servers is added. This support would enable customers to map high availability interfaces one-to-one to real ports to avoid any hypervisor misconfiguration that would separate the virtual appliances and cause both virtual appliance to become active. Not all Hypervisors support nine Virtual Ports which is required to support the maximum configuration. If more ports are configured in the SD-WAN appliance than available, SD-WAN supports the current configuration that has more SD-WAN ports than Hypervisor ports.

VPX Standard Edition on ESXi

May 23, 2019

This chapter provides step-by-step instructions for installing, configuring, and deploying the SD-WAN VPX-SE. This includes basic instructions for installing the VMware vSphere Client, which you use to create and deploy the SD-WAN VPX-SE Virtual Machine.

> **Note**
>
> VMware vSphere Client operation details might change with new releases of the vSphere software. For the most complete and current vSphere Client installation and operation instructions, please refer to your VMware documentation. The instructions in this chapter are intended to provide the most basic and essential guidelines, only, for installing an SD-WAN VPX-SE Virtual Machine on the ESXi platform.

The following summarizes the top-level steps for installing and deploying an SD-WAN VPX-SE. Perform these procedures in the exact order listed.

1. Install the VMware vSphere Client.
2. Install and deploy the SD-WAN VPX-SE OVF Template.
3. Configure the SD-WAN VPX-SE Management IP Address.
4. Connect and test the deployment.

Install Client

June 19, 2020
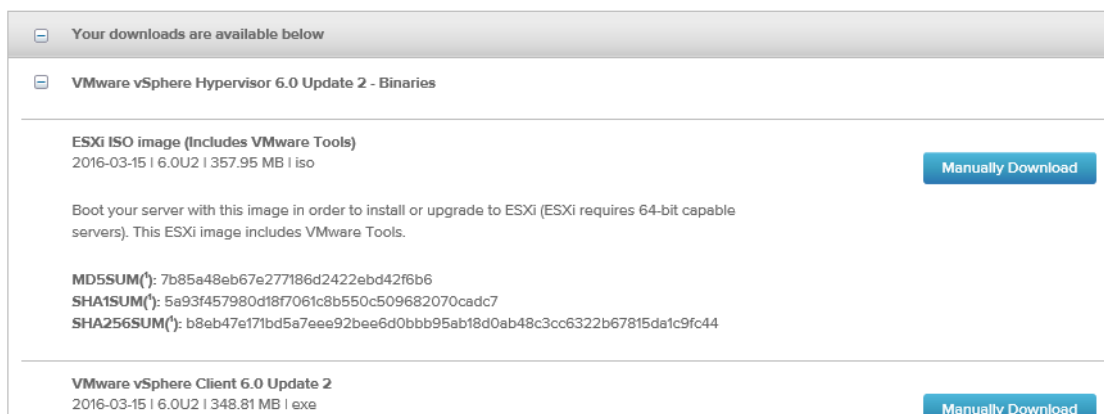
This section provides basic instructions for downloading and installing the VMware vSphere client you use to create and deploy the SD-WAN VPX-SE Virtual Machine.

> **Note**
>
> Please refer to your VMware vSphere Client documentation for additional information. SD-WAN can be deployed in vShpere Client version 5.5 or later.

1. Open a browser and navigate to the ESXi server that will host your vSphere Client and VPX-SE Virtual Machine (VM) instance at: https://my.vmware.com/group/vmware/evalcenter?p=free-esxi6 The **VMware ESXi downloads** page displays,

2. lick the **Download vSphere Client** link to download the vSphere Client installation file.
3. Install the vSphere Client. Run the vSphere Client installer file that you downloaded, and accept each of the default options when prompted.
4. After the installation completes, start the vSphere Client program. The **VMware vSphere Client** login page displays, prompting you for the ESXi server login credentials.

5. Enter the **ESXi server login credentials**. Enter the following:

- **IP address / Name**: Enter the **IP Address** or Fully Qualified Domain Name (FQDN) for the ESXi server that hosts your SD-WAN VPX-SE VM instance.
- **User name:** Enter the server Administrator account name. The default is root.
- **Password**: Enter the password associated with this Administrator account.

6. Click **Login.** This displays the **vSphere Client** main page.
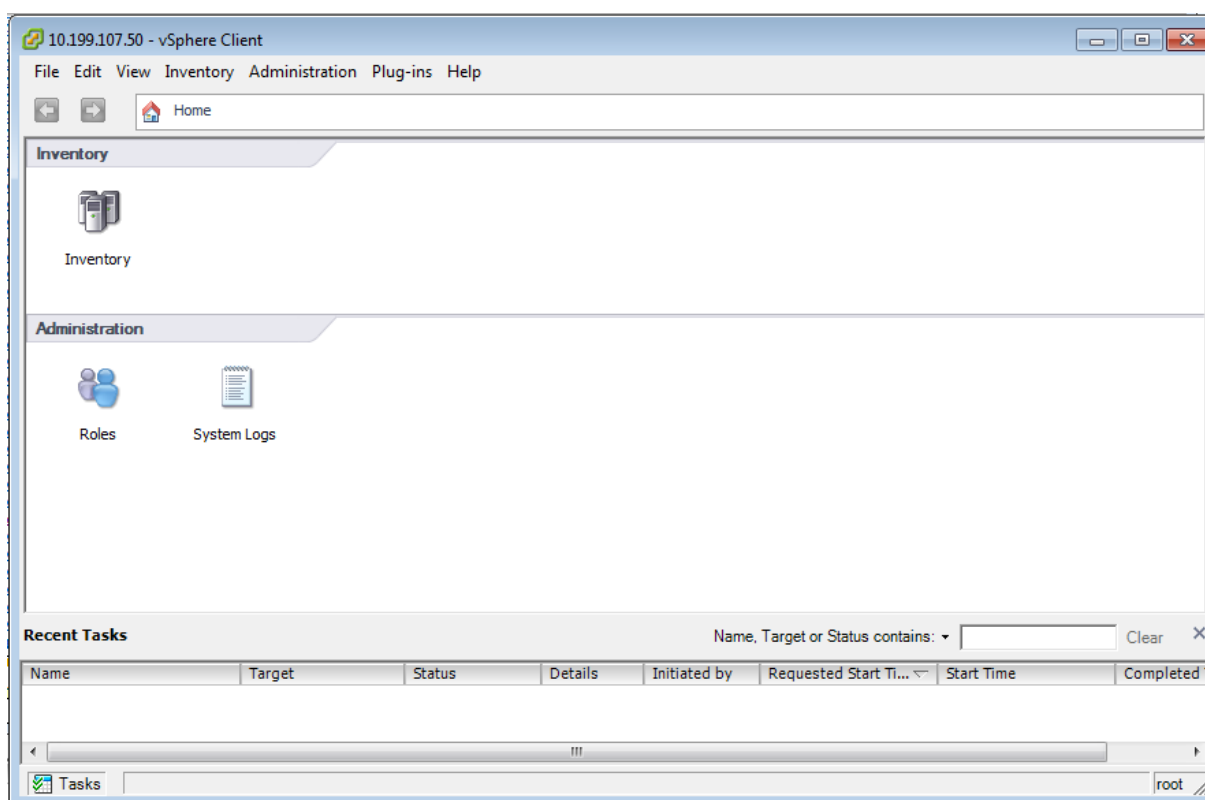
The next step is to install and deploy the SD-WAN VPX-SE OVF template and set up the Virtual Machine. The following section provides instructions for these procedures.

Deploy SD-WAN VPX

June 25, 2020

This section provides instructions for installing the SD-WAN VPX OVF template and creating the SD-WAN VPX Virtual Machine.

1. If you have not already done so, download the SD-WAN VPX OVF template file (.ova file) to the local PC. Download or copy the SD-WAN VPX OVF template to the local PC you are using to connect to the ESXi server that will host your SD-WAN VPX. The OVF template file has a file name using the following naming convention: *cb-vw-vpx-version_number-vmware.ova*, where:

   - *version_number* is the SD-WAN VPX release version number.

   - *.ova* is the file name suffix indicating that this is an OVF template file.

     > **Note**
     >
     > For additional information, see Downloading the Software Packages.

---

2. Continuing in the vSphere Client, click **File** and then select **Deploy OVF Template...** from the drop-down menu. This displays the first page of the **Deploy OVF Template** wizard, the **Source** page.
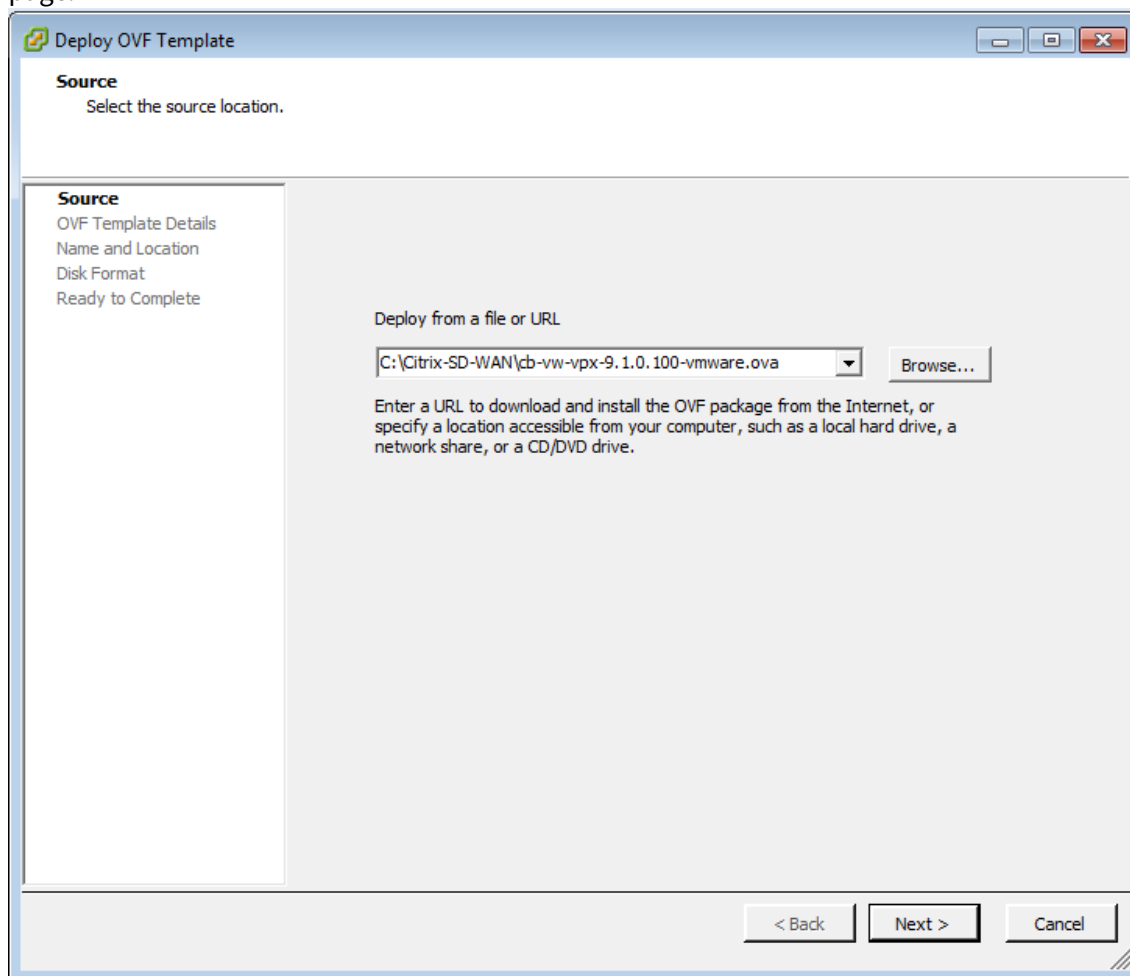
3. Select the CB VPX-VW OVF template *(.ova* file) you want to install. Browse to the location of the *.ova* file you downloaded earlier to the local PC, and select it.

4. Click **Next**. This imports the selected *.ova* file and displays the **OVF Template Details** page.

168
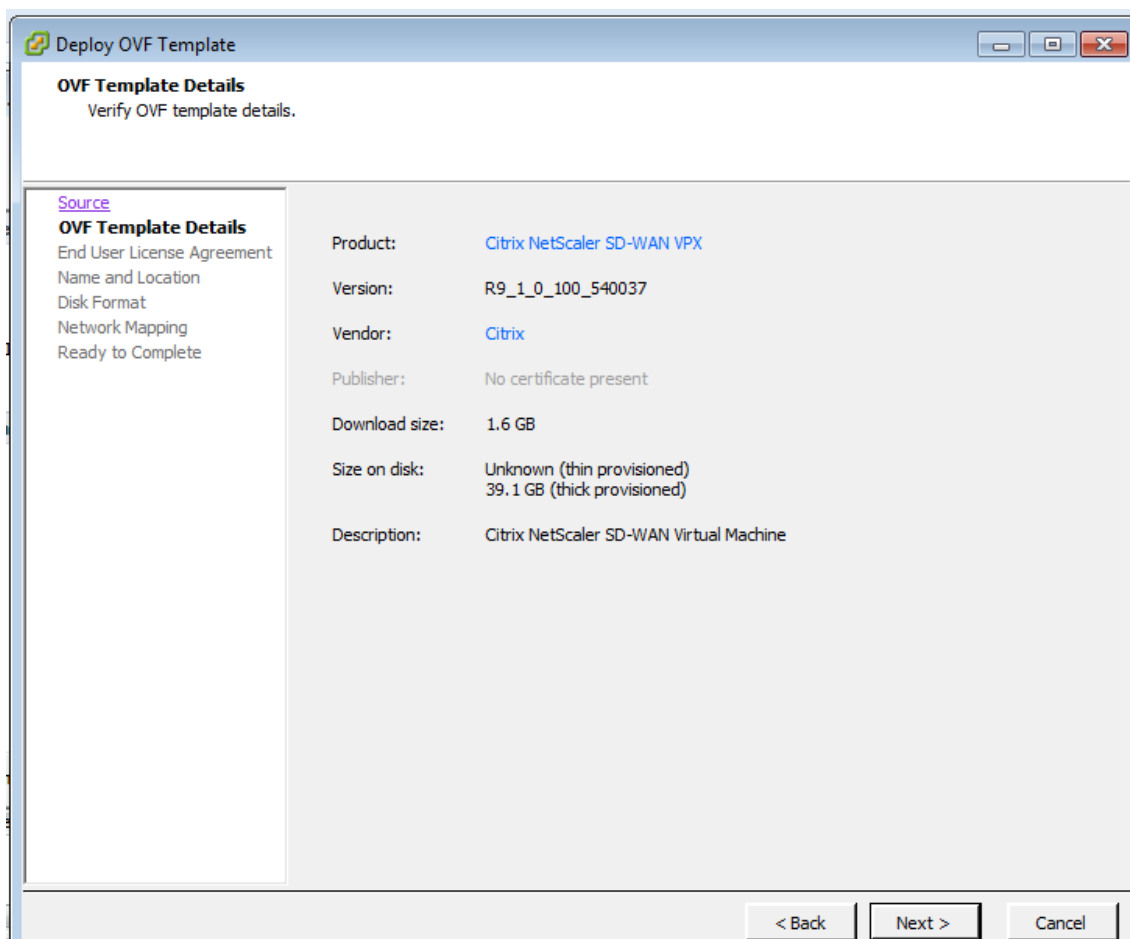
5. This page displays some basic information regarding the OVF template you imported.

6. Click **Next**. This proceeds to the **End User License Agreement** page.
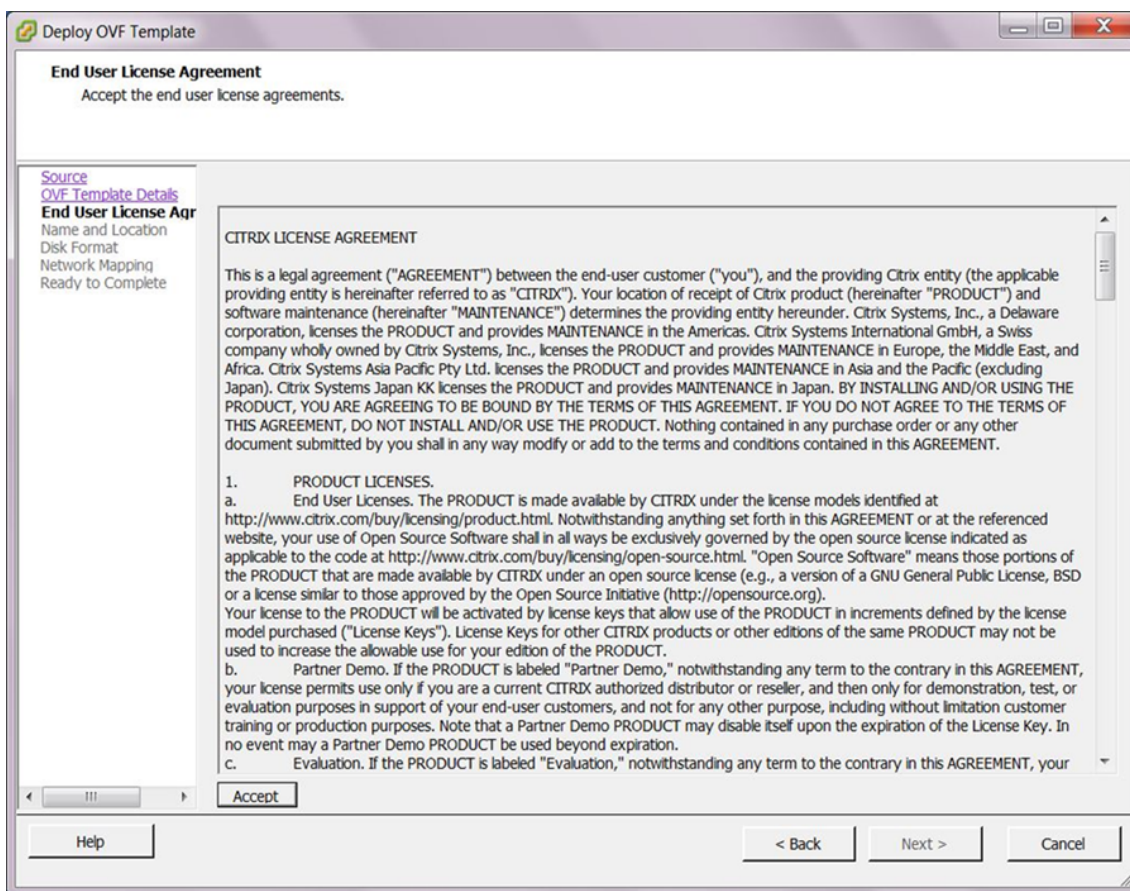
7. Click **Accept**, and then click **Next**. This proceeds to the **Name and Location** page.

170
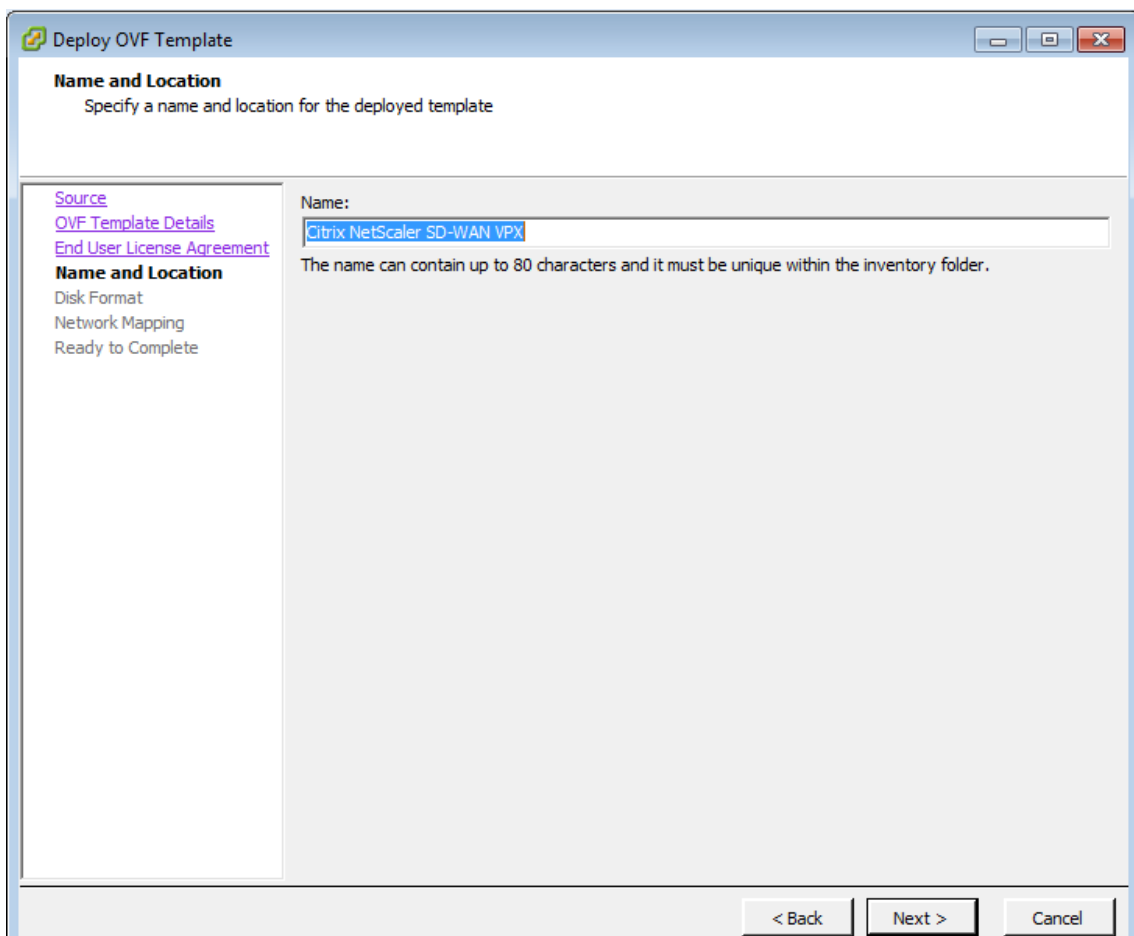
8. Enter a unique name for the new VM (or accept the default). The name must be unique within the current **Inventory** folder, and can be up to 80 characters in length.

9. Click **Next**. This displays the Disk Format page. The SD-WAN VPX-VW Virtual Machine requires 39.1 GB of disk space.
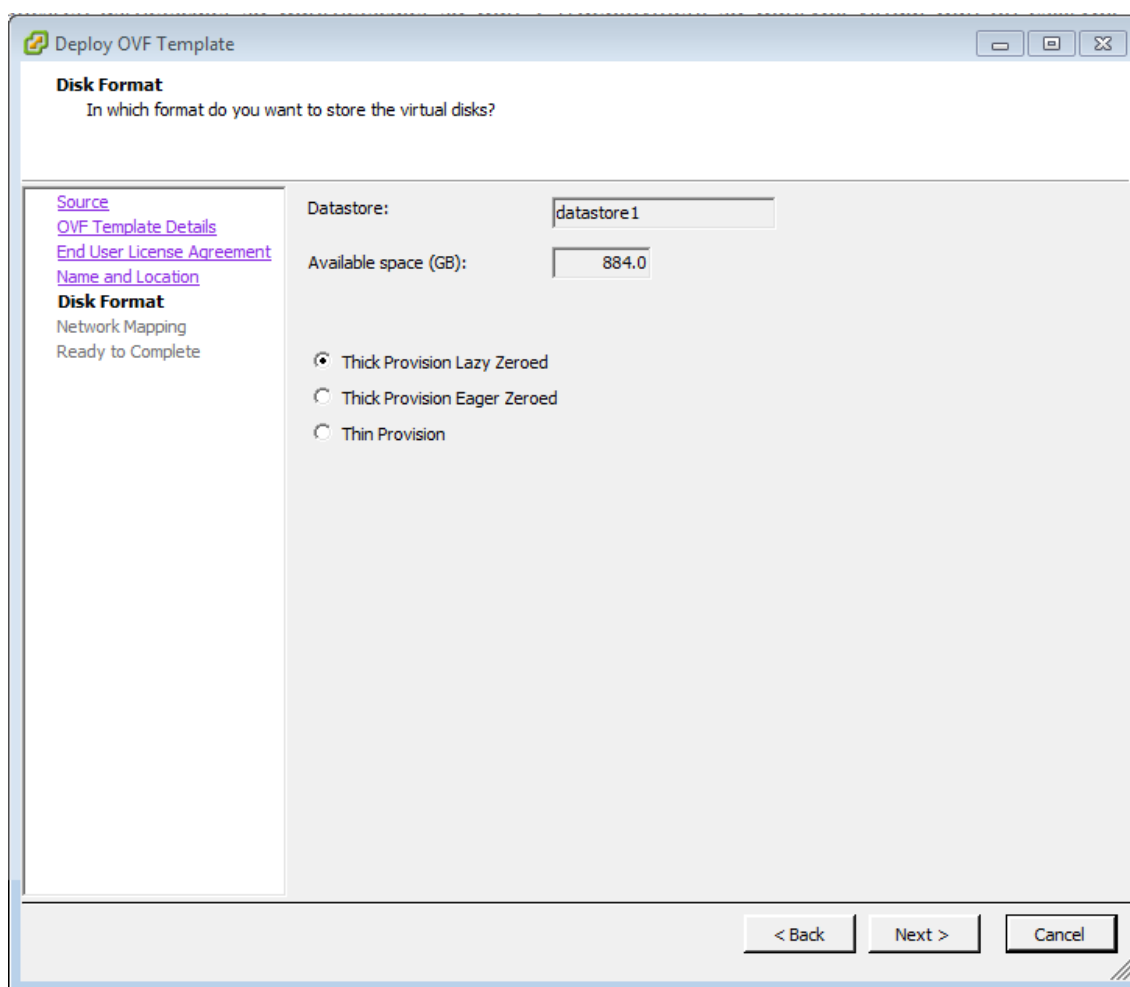
10. Accept the default settings, and click **Next**. This proceeds to the **Network Mapping** page.
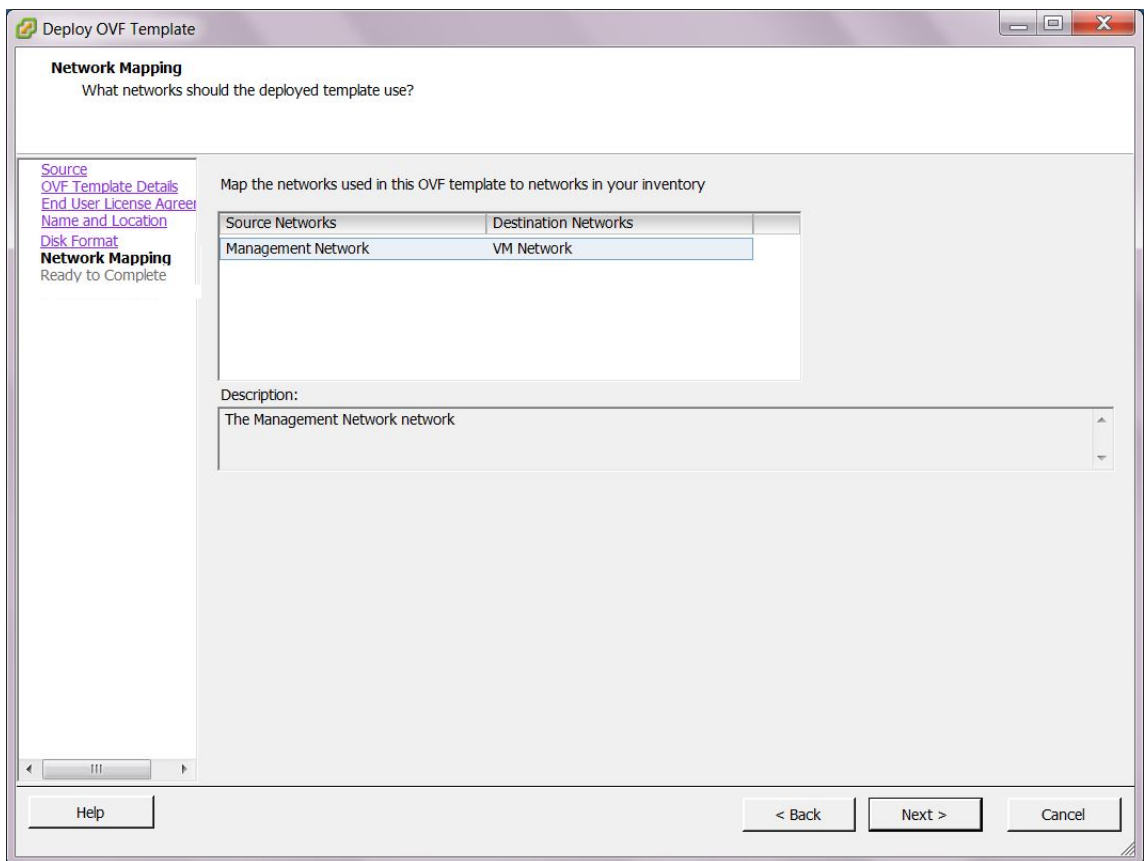
11. Accept the default (**VM Network**) and click **Next**. This proceeds to the Ready to Complete page.
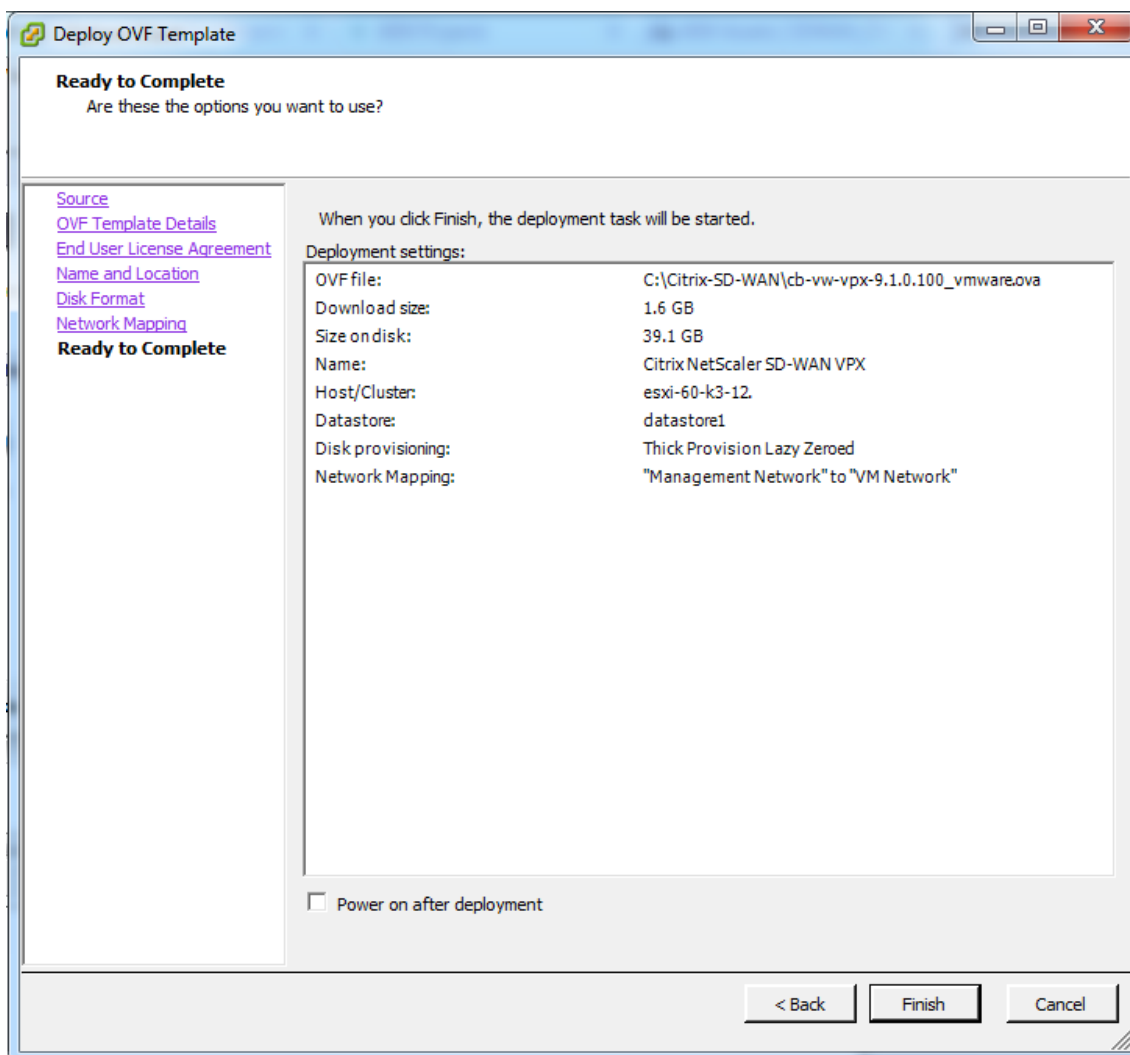
12. Click **Finish** to create the VM.

> **Note**
>
> Decompressing the disk image onto the server could take several minutes.

This displays the **Deploying Citrix SD-WAN VPX** status dialog box.
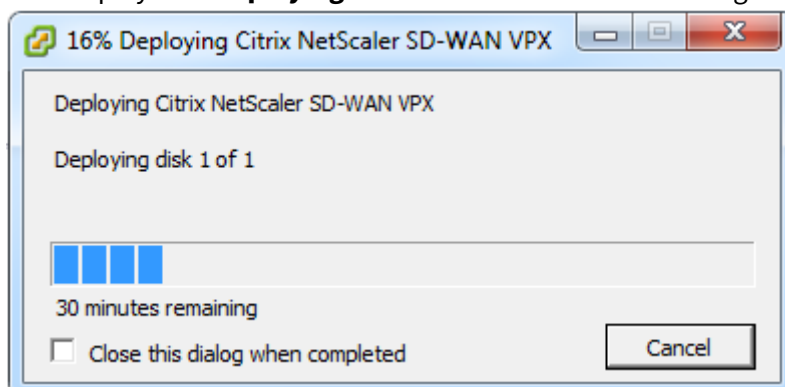
Depending on the conditions present on your server, the deployment can take from several minutes to a few hours to complete. When the SD-WAN VPX Virtual Machine has been successfully created, a success message displays.
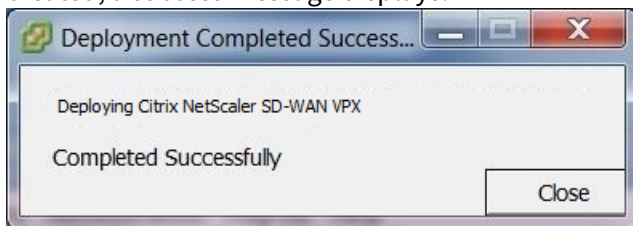
13. Click **Close**. This closes the **Deploy OVF Template** wizard and returns to the vSphere Client main window. If this is the first VM you have created using this vSphere Client, the vSphere Client **Home** page displays. If you have previously created one or more VMs, the **Inventory** page displays.

The next step is to configure the SD-WAN VPX Management IP Address. The following section provides instructions for this procedure.

Configure Management IP

December 15, 2020

There are two methods for assigning the Management IP Address to the SD-WAN VPX Virtual Machine:

- **Automatic**: By default, all SD-WAN VPX Virtual appliances use the Dynamic Host Control Protocol (DHCP) to automatically acquire the Management IP Address. To use DHCP, the DHCP server must be present and available in the SD-WAN. For acquiring the IPv6 addresses automatically, the appliances can use DHCP or Stateless Address Auto Configuration (SLAAC). For instructions on identifying the acquired Management IP Address, see Displaying the DHCP assigned Management IP Address for the VPX.
- **Manual**: If you are not using DHCP or SLAAC, you must manually assign a static Management IP Address for the SD-WAN VPX Virtual Appliance. For instructions, see Manually Configuring a Static Management IP Address for the VPX.

Manually configuring a static Management IP address for the VPX

If you are not using DHCP or SLAAC, you must configure a static Management IP Address for the SD-WAN VPX Virtual Appliance VM manually. To configure, use the console of the Virtual Machine you created, in the vSphere Client.

Note

DHCP is enabled by default for the SD-WAN VPX Management IP Address.

1. Continuing in the vSphere client **Inventory** page, select the new SD-WAN VPX VM in the **Inventory** tree (left pane). This displays the **Inventory** page for the new VM, with the **Getting Started** tab preselected.
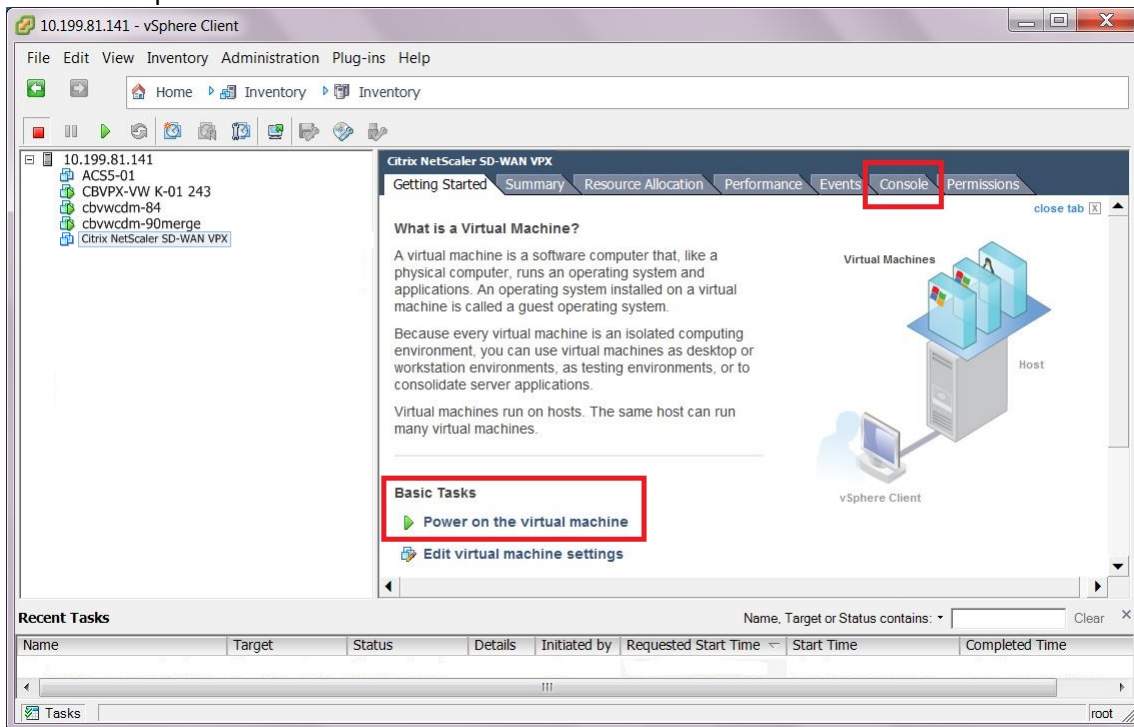
2. Power on the new Virtual Machine. In the **Basic Tasks** section of the **Getting Started** tab page, click **Power on the virtual machine** (green play button) to power on the new SD-WAN VPX-SE VM.

3. Select the **Console** tab in the **Inventory** page tab bar. The Console tab is located in **Inventory** page tab bar at the top of the main page area. Selecting this tab displays and enables access to the CLI console for the VM.
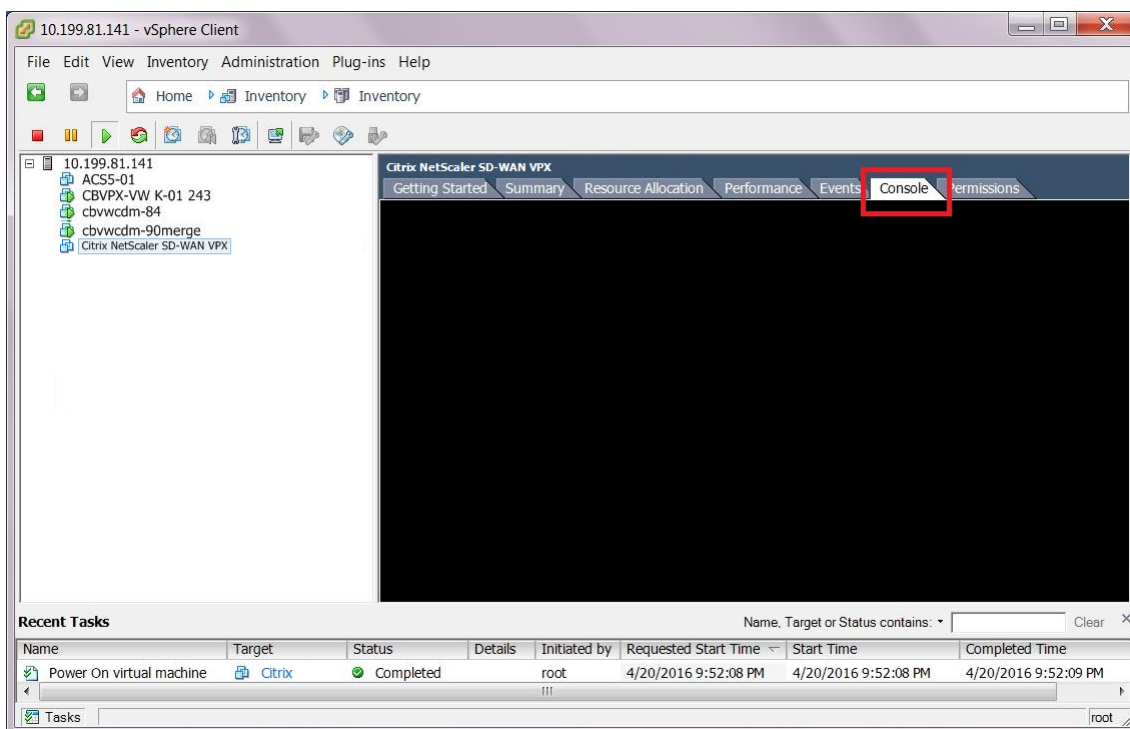
As the new VM starts up, a series of status messages display in the console.

When the startup process completes, the console login prompt displays.

4. Click anywhere inside the console area to enter console mode. This turns control of your mouse cursor over to the VM console, and enables console mode.

> **Note**
>
> To release console control of your cursor, press the **Ctrl and Alt** keys simultaneously.

5. Log into the VM console. The default login credentials for the new SD-WAN VPX-SE VM are as follows:

   - **Login**: *admin*
   - **Password**: *password*

   This displays the console **Welcome** screen.

6. Enter the following command line at the console prompt:

   - To configure an IPv4 address:

   management_ip

This switches to the *management_ip* CLI in the console, and displays the *set_management_ip* prompt.

```
Console to Citrix acquired

MCN_DC-MCN_DC-VPX>management_ip

Which would you like to do?
        "set interface <ip address> <subnet mask> <gateway>" - Stage New Setting
s for IP Address, Subnet Mask, and Gateway IP Address
        "address" - Stage New IP Address
        "mask" - Stage New Subnet Mask
        "gateway" - Stage New Gateway IP Address
        "clear" - Clear Settings
        "disable" - disable IPv4 address on the interface
        "apply" - Apply Staged Settings
        "cancel" - Cancel Staged Settings
        "main_menu" - Return to the Main Menu

set_management_ip>
```

- To configure an IPv6 address:

  `management_ipv6`

  This switches to the *management_ipv6* CLI in the console, and displays the *set_management_ipv6* prompt.

```
[BANLSREEJITHS:~ sri    $ ssh admin@10.    .56
[admin@10.    3.56's password:

Console to Citrix acquired

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter
 "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>
```

7. Configure the interface settings for the VM. Enter the following command line at the *set_management_ip* prompt:

   - For an IPv4 address:

     `set **interface** <ip address> <subnet mask> <gateway>`

     Where:

     - <IP address> is the Management IP Address for the SD-WAN VPX-SE Virtual Appliance.
     - <subnet mask> is the subnet mask used to define the network in which the CB VPX-VW Virtual Appliance resides.
     - <gateway> is the Gateway IP Address the SD-WAN VPX-SE Virtual Appliance uses to communicate with external networks.

     This stages but does not apply the interface settings.

```
Console to Citrix acquired


[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

[MCN_DC-MCN_DC-VPX>management_ip                                             ]

Which would you like to do?
        "set interface <ip address> <subnet mask> <gateway>" - Stage New Setting
s for IP Address, Subnet Mask, and Gateway IP Address
        "address" - Stage New IP Address
        "mask" - Stage New Subnet Mask
        "gateway" - Stage New Gateway IP Address
        "clear" - Clear Settings
        "disable" - disable IPv4 address on the interface
        "apply" - Apply Staged Settings
        "cancel" - Cancel Staged Settings
        "main_menu" - Return to the Main Menu

set_management_ip>set interface 10.          255.255.255.0 10.        1
```

- For an IPv6 address:

  set **interface** <IPv6 address> <prefix>

  where:

  - <IPv6 address> is the Management IP Address for the SD-WAN VPX-SE Virtual Appli-
    ance.

  - <prefix> represents a block of address space or a network.

  Enter one of the following:

  - **SLAAC**: Enables SLAAC for automatically assigning an IPv6 address to each device on
    the network. SLAAC enables an IPv6 client to generate its own addresses.

    ```
    Console to Citrix acquired


    [WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

    MCN_DC-MCN_DC-VPX>
    [WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

    [MCN_DC-MCN_DC-VPX>management_ipv6
    set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
    disable. Enter "main_menu" to return to the main menu.

    set_management_ipv6>SLAAC

    set_management_ipv6_slaac>Please enter "enable" to enable slaac. To disable, please go to management_ipv6

    menu.  Enter "main_menu" to return to the main menu.

    set_management_ipv6_slaac>enable
    Management interface settings have been enabled for V6. Applying settings to take effect.
    Applied changes, duplicate address detection is in progress!! Please wait.

    No conflicts detected!! The IPv6 address is applied to tn-mgt0!!

    set_management_ipv6_slaac>
    ```

  - **DHCP**: Enables DHCP for assigning IP addresses automatically. Select stateful or
    stateless based on your need.

```
Console to Citrix acquired


[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>DHCP

set_management_ipv6_dhcp>Please enter "enable" to enable DHCPv6. To disable, please go to
management_ipv6 menu.  Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>enable
set_management_ipv6_dhcp>Which mode of DHCP do you like to enable? Please select "stateful" or
["stateless".  Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>stateful
Management interface settings have been enabled for V6. Applying settings to take effect.

set_management_ipv6_dhcp>█


======================================================================
Console to Citrix acquired


[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>DHCP

set_management_ipv6_dhcp>Please enter "enable" to enable DHCPv6. To disable, please go to
management_ipv6 menu.  Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>enable
set_management_ipv6_dhcp>which mode of DHCP do you like to enable? Please select "stateful" or
["stateless".  Enter "main_menu" to return to the main menu.

set_management_ipv6_dhcp>stateless
Management Interface settings have been enabled for V6. Applying settings to take effect.

set_management_ipv6_dhcp>█
```

- **Static**: Enter the IP address is manually.

```
======================================================================
Console to Citrix acquired


[MCN_DC-MCN_DC-VPX>management_ipv6
set_management_ipv6>Configuring IPv6: Enter "SLAAC" or "DHCP" or "static". Enter "disable" to
disable. Enter "main_menu" to return to the main menu.

set_management_ipv6>static

IPv6 Address:           (Not configured)
IP Prefix:              (Not configured)


Which would you like to do?
        "set interface <ip address> <IPv6 prefix>" - Stage New Settings for IP Address and prefix
        "main_menu" - Return to the Main Menu

set_management_ipv6_static>set interface fd73:          ::4 64
The following management Interface settings have been staged
[IP Address:            fd73:2039:5849:26::4
IP Prefix:              64

Which would you like to do?
        "apply" - Apply Staged Settings
        "cancel" - Cancel Staged Settings
        "main_menu" - Return to the Main Menu

set_management_ipv6_static>█
```

8. Apply the staged settings for the VM interface. Do the following:

   a) Enter the following command at the *set_management_ip* prompt (for IPv4) or

---

set_management_ipv6 prompt (for IPv6): `apply`

b) When prompted to confirm the *apply* operation, enter *Y*.

This applies the staged interface settings for the VM, and displays the results.

9. Enter exit and press **Return** at the prompt to exit the management_ip CLI.

10. Exit the console. Enter **exit and press Return** at the console prompt, and then press **Ctrl+Alt to regain control of the cursor.**

11. Shut down and restart the VM. Do the following:

a) Select the **Getting Started** tab to display the **Basic Tasks** options.
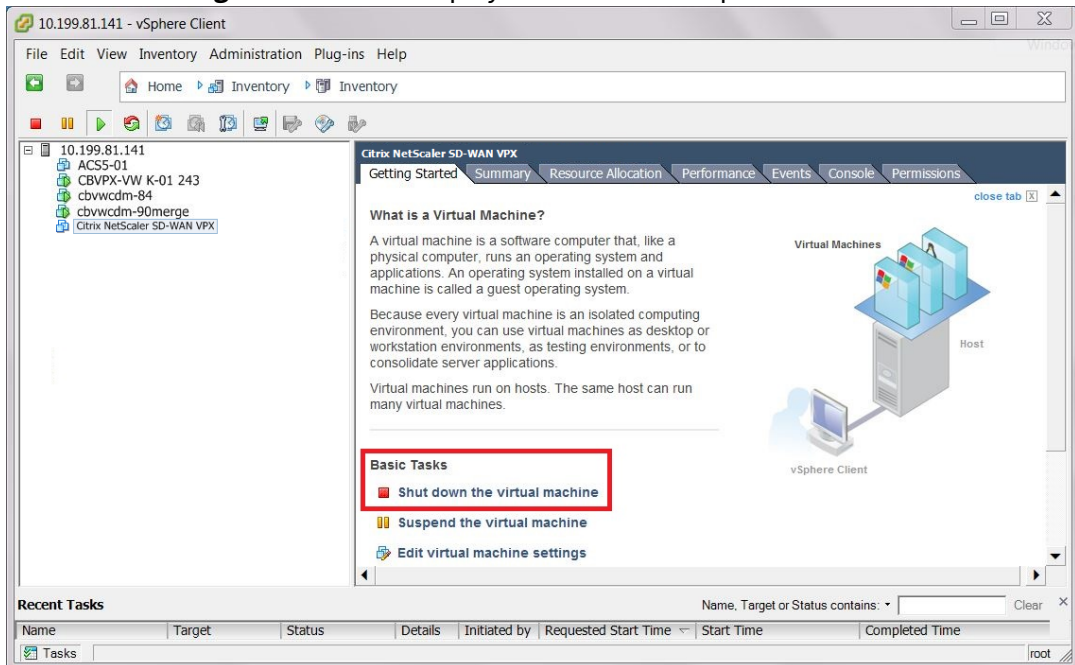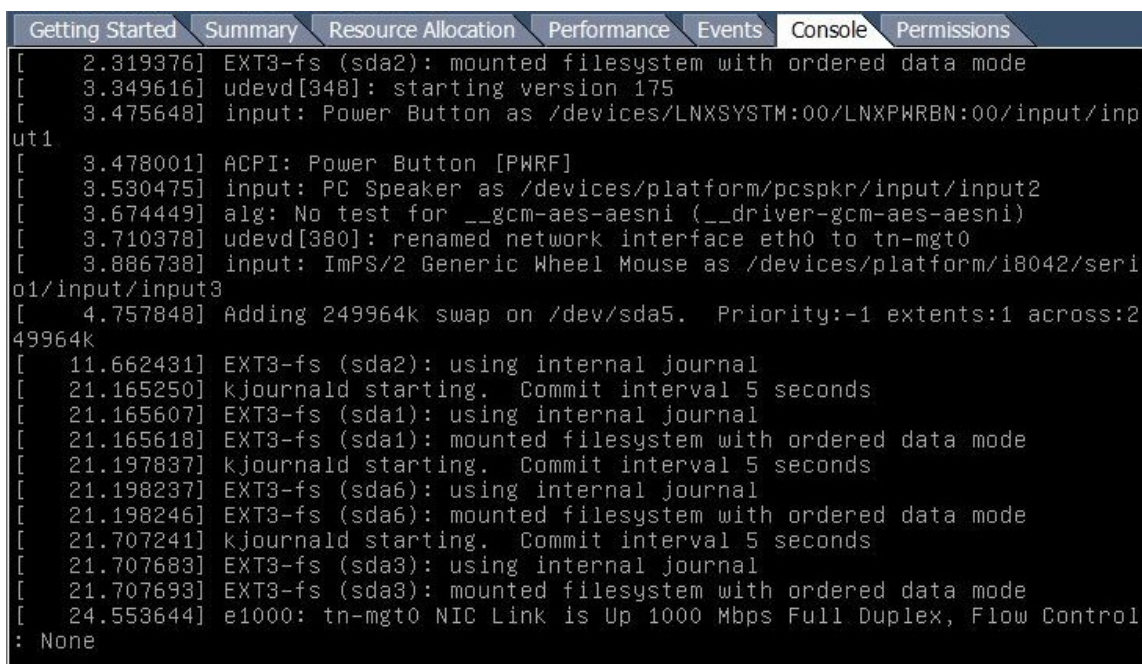
b) In the **Basic Tasks** section, click **Shut down the virtual machine** (red box icon).

You are prompted to confirm that you want to shut down the guest operating system for the VM.
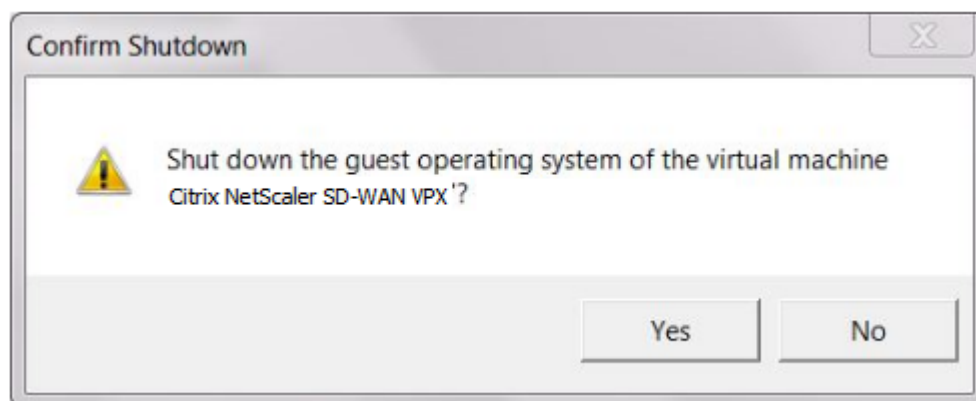
c) Click **Yes** to confirm. This shuts down the guest operating system and powers off the VM. When the shutdown completes, the **Power on the virtual machine** option (green play button) becomes available.
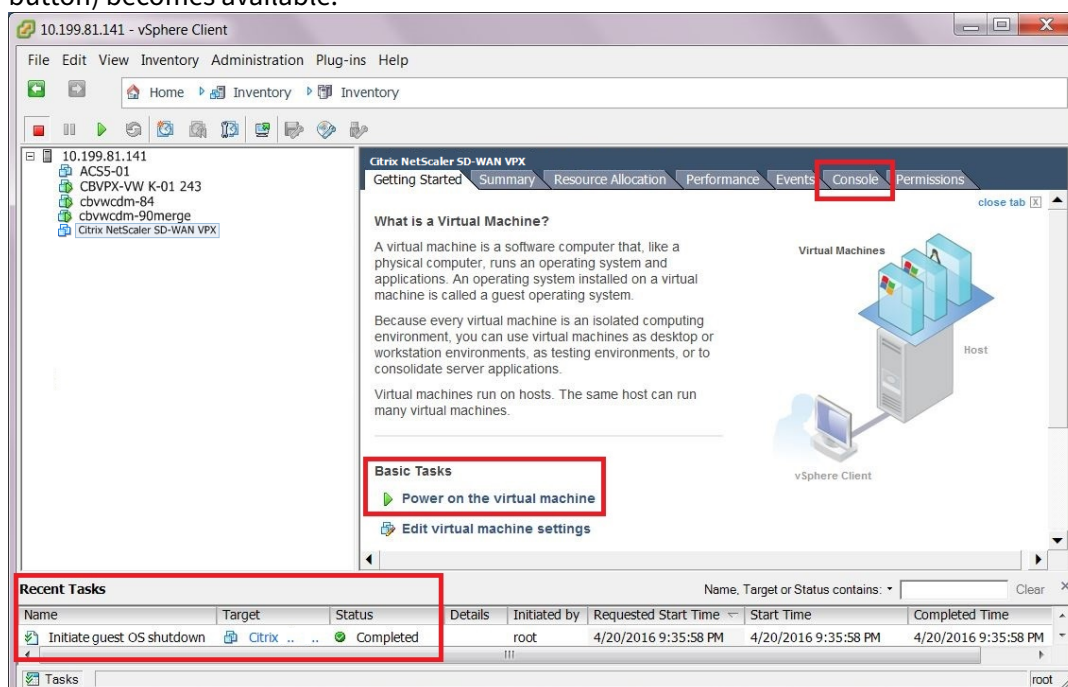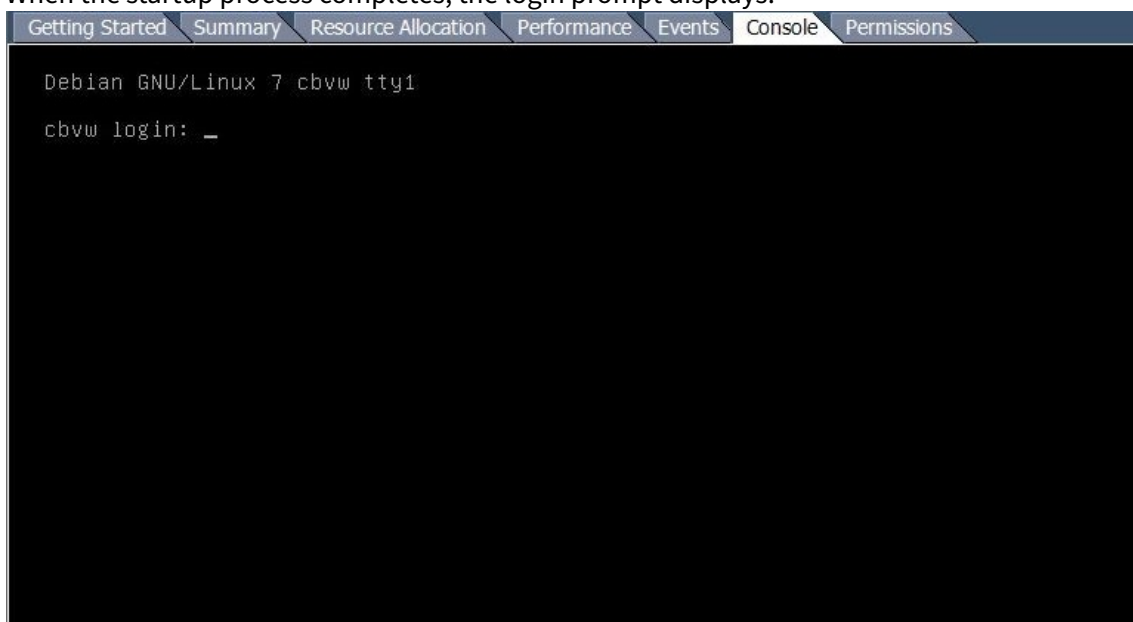
12. Restart the Virtual Machine. Click **Power on the virtual machine** (green right-arrow) to restart the VM. You can view the progress of the start-up process in the **Console** tab page for the VM.

183

When the startup process completes, the login prompt displays.

You can now proceed to the final step, Connecting to the SD-WAN VPX-SE and Testing the Deployment

Displaying the DHCP assigned Management IP address for the VPX

This section provides instructions for displaying and recording the DHCP-assigned Management IP Address for the new SD-WAN VPX-SE Virtual Appliance VM.

Note

By default, all SD-WAN VPX-SE Virtual Appliances use DHCP. If you are not using DHCP, or have assigned a static IP Address for the Virtual Appliance, you can skip this step. If you are using DHCP, the DHCP server must be present and available in the SD-WAN before you can complete this step.

To display the DHCP-assigned Management IP Address for the Virtual Appliance, do the following:

1. Continuing in the vSphere client **Inventory** page, select the new SD-WAN VPX-SE VM in the **Inventory** tree (left pane). This displays the Inventory page for the SD-WAN VPX-SE VM.
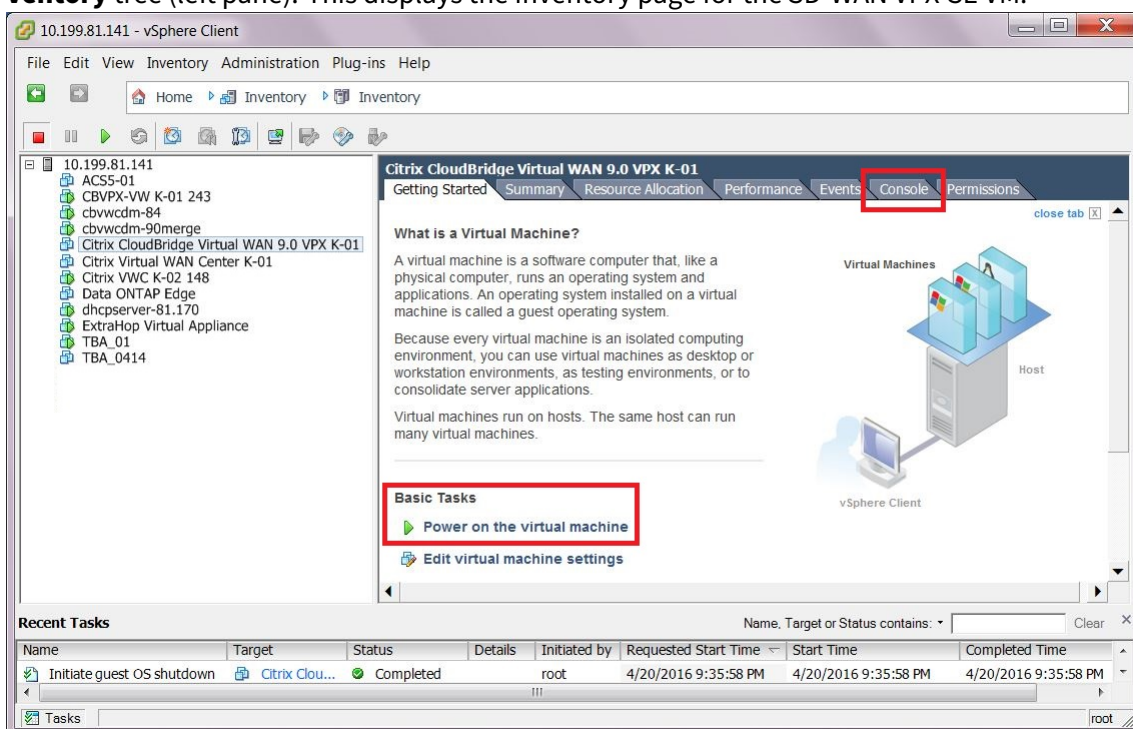
2. If you have not already done so, power on the new Virtual Machine. In the **Basic Tasks** section, click the **Play** icon (green arrow) to power on the new SD-WAN VPX-SE VM.

3. Select the **Console** tab in the **Inventory** page tab bar. The **Console** tab is located in **Inventory** page tab bar at the top of the main page area. Selecting this tab displays and enables access to the CLI console for the VM.

---
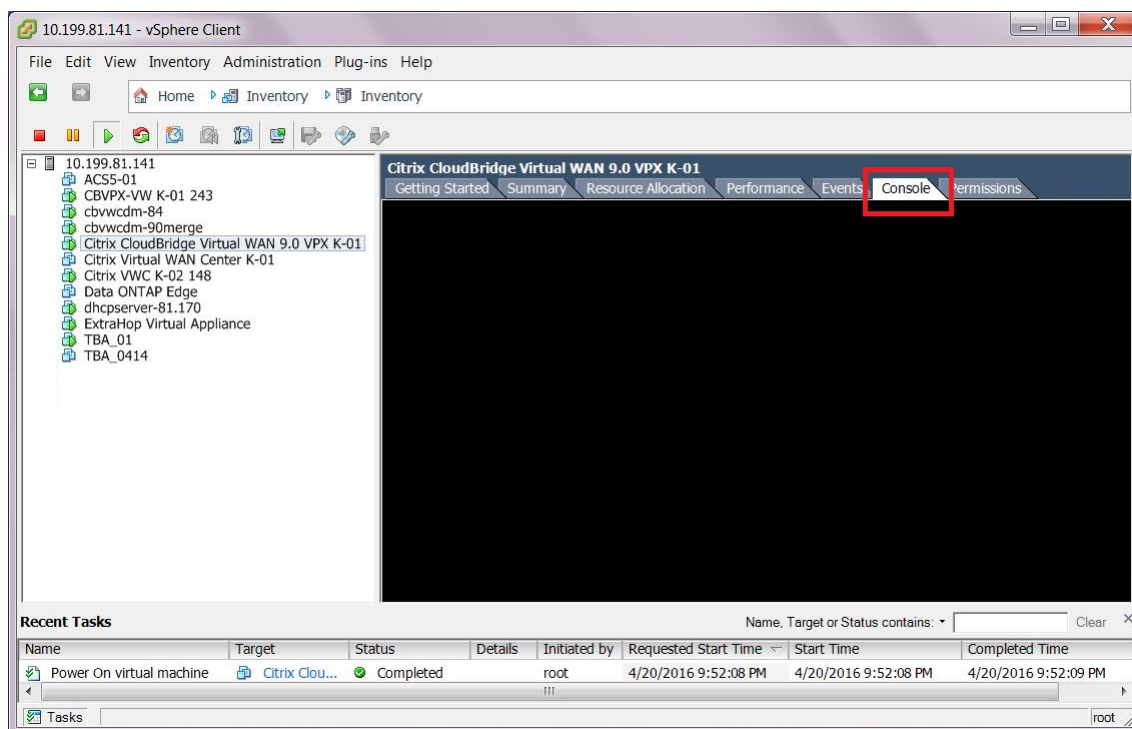
4. Click anywhere inside the console area to enter console mode. This turns control of your mouse cursor over to the VM console, and enables console mode.

> **Note**
>
> To release console control of your cursor, press the **Ctrl** and **Alt** keys simultaneously.

5. Press **Enter** to display the console **login** prompt. Press **Enter** once or twice to display the console l**ogin** prompt.

186
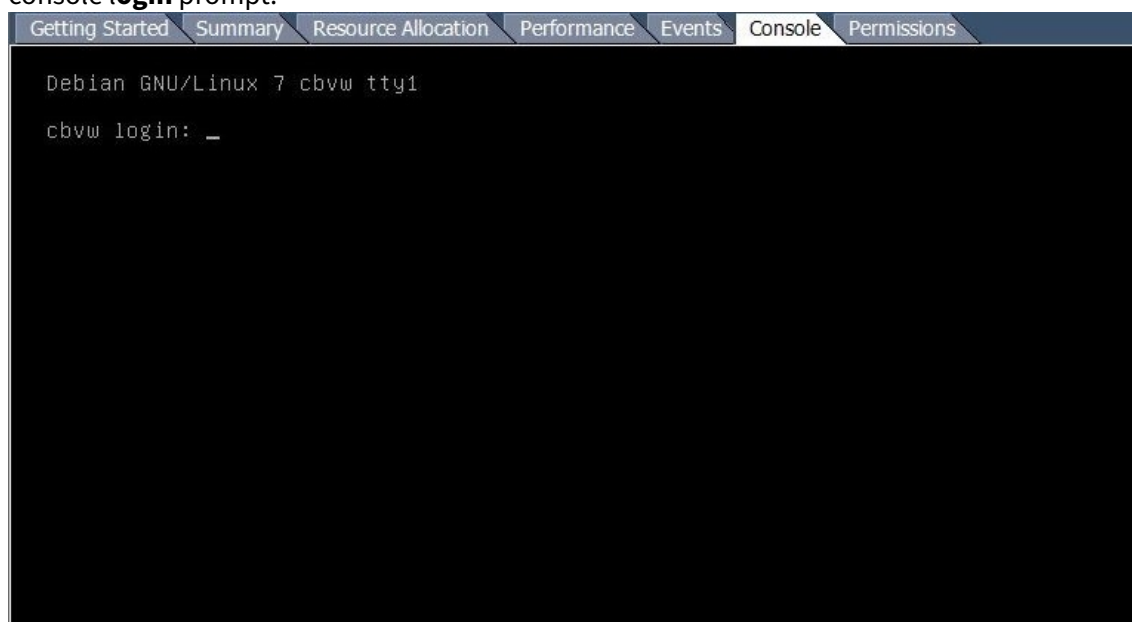
6. Log into the VM console. The default login credentials for the new SD-WAN VPX-SE VM are as follows:

- **Login**: *admin*
- **Password**: *password*

This displays the console **Welcome** message, which includes the **Host IP Address**.

```
Last login: Tue Dec  1 17:15:16 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[BANLSREE        :~ sri    $ ssh admin@10.    3.56                           ]
[admin@10.    .56's password:                                               ]
    ==================================================================

            Operating System 5.1 on CBVPXv1
            Host IPV4 = 10.    .56
            Host IPv6 = fd73:                              :bcf1

    ==================================================================
Console to Citrix acquired


[WARNING] RADIUS server is unreachable. This may cause slowness in the CLI.

MCN_DC—MCN_DC—VPX>
```

7. Record the Management IP Address for the SD-WAN VPX-SE VM.

Note

The DHCP server must be present and available in the SD-WAN, or this step cannot be completed.

After logging into the console, the Welcome message displays the *Last login* information and the *Host IP Address*. This IP Address is the Management IP Address for this new SD-WAN VPX-SE VM.

This completes the deployment of the SD-WAN VPX-SE Virtual Machine. The final step is to connect to the new SD-WAN VPX-SE and test the deployment. Instructions are provided in the next section.

Connecting to the SD-WAN VPX and Testing the Deployment

June 25, 2020

The next step is to connect to the new SD-WAN VPX-SE Virtual Appliance, to confirm that the deployment was successful.

To test the deployment, do the following:

1. On a connected PC, open a browser and enter the **Management IP Address** for the SD-WAN VPX-SE Virtual Appliance. You can use any PC connected to your network (for example, the local PC you used to deploy the SD-WAN VPX-SE Virtual Machine in the vSphere Client). If you have successfully assigned the Management IP Address for the SD-WAN VPX-SE, the Management Web Interface **Login** page displays.
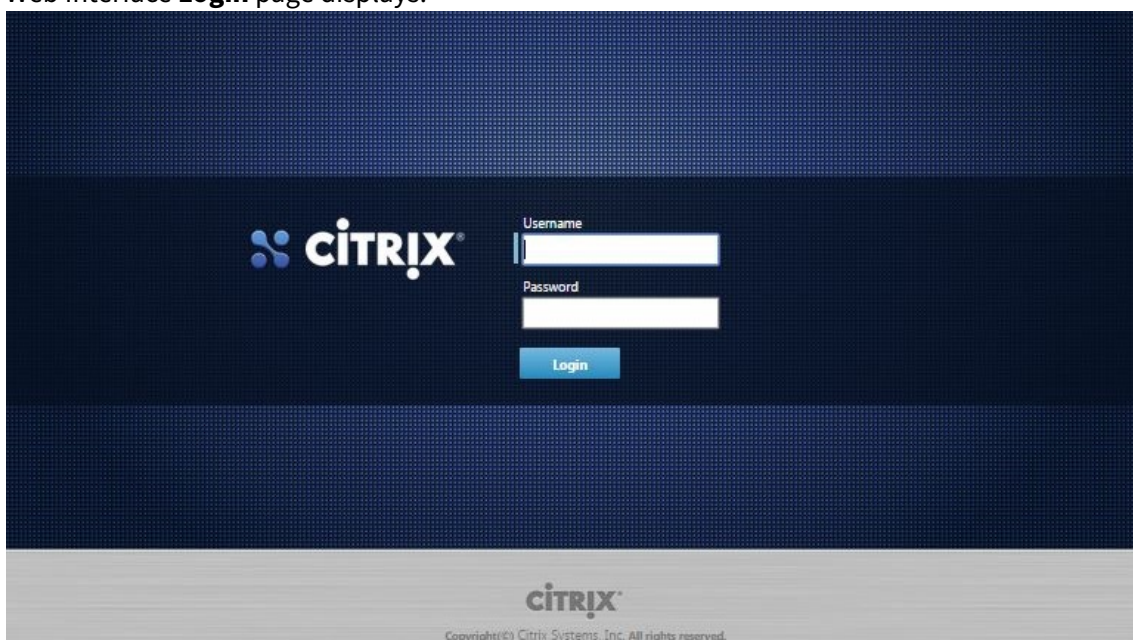
2. Enter the **Administrator user name** and password, and click **Login**.
   - Default Administrator user name: *admin*
   - Default Administrator password: *password*

Note

It is recommended that you change the default password as soon as possible. Be sure to record the password in a secure location, as password recovery might require a configuration reset.

After you have logged into the Management Web Interface, the **Dashboard** page displays.
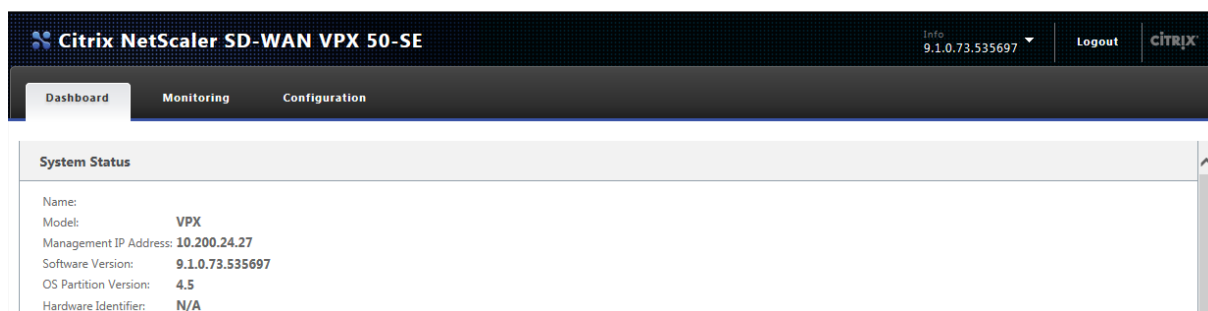
The first time you log into the Management Web Interface on an appliance, the **Dashboard** displays an Alert icon (goldenrod delta) and alert message indicating that the Virtual WAN Service is disabled, and the license has not been installed. For now, you can ignore this alert. The alert will be resolved

automatically after you have installed the license, and completed the configuration and deployment process for the appliance.

You have now completed the initial installation and deployment of the SD-WAN VPX-SE Virtual Appliance. However, there are some remaining steps to complete the set-up process for the Virtual Appliance before adding it to your SD-WAN network. For instructions on completing the next step, please proceed to the section, Initial setup.

SD-WAN VPX Usage Scenarios

June 22, 2020

You can deploy VPX to accelerate the traffic to or from a branch office, to and from a particular server, or in the cloud. In the data center, you can create a flexible and powerful configuration by assigning a separate VPX instance to each server. Or, at any location, you can assign multiple VPX instances to one server, for different types or levels of acceleration services within the same server.

For employees connecting through VPNs, VPX can accelerate their connections.

As with a physical appliance, inline mode is the most common type of configuration, but WCCP and virtual inline modes can provide an effective deployment.

VPX usage scenarios

You can deploy VPX to accelerate the traffic to or from a branch office, or to and from a particular server. In the data center, you can create a flexible and powerful configuration by assigning a separate VPX instance to each server. Or, at any location, you can assign multiple VPX instances to one server, for different types or levels of acceleration services within the same server.

For employees connecting through VPNs, VPX can accelerate their connections.

As with a physical appliance, inline mode is the most common type of configuration, but WCCP mode can provide an effective failover mechanism.

Branch-office accelerator

A VPX image can be installed on the server of your choice and deployed just like a SD-WAN/SD-WAN appliance. VPX has all the functionality of a SD-WAN/SD-WAN appliance, and in addition has advantages provided by virtualization. Group mode and high-availability modes are not supported.

Figure 1.VPX use case #1: Branch-office accelerator
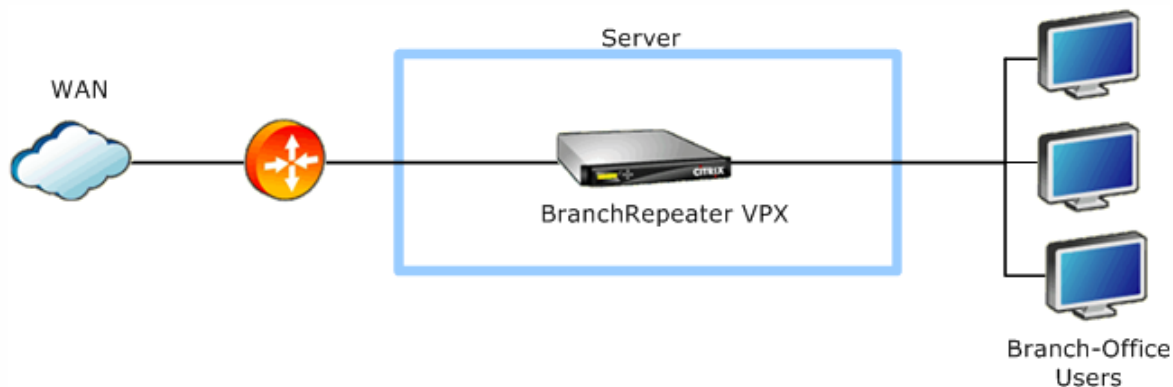
Accelerated branch-office server

If you add a virtual server to the simple branch-office accelerator configuration, you have an accelerated branch-office server, as shown in the figure below. If you assign the virtual networks within the appliance hosting the virtual machines so that the path to the WAN passes through the virtual SD-WAN/SD-WAN, all WAN traffic is accelerated automatically. For example, all web traffic, backups, remote applications, database queries, and operations that require network-file-system access are accelerated.

The virtual environment allows you to add the desired functionality to the server unit, including the operating system and features of your choice. This configuration accelerates all the WAN traffic from every system in the branch office. You can even deploy multiple virtual servers on the same machine, consolidating your branch-office rack down to a single unit running multiple virtual machines.

Figure 2. VPX use case #2: Accelerated branch-office server
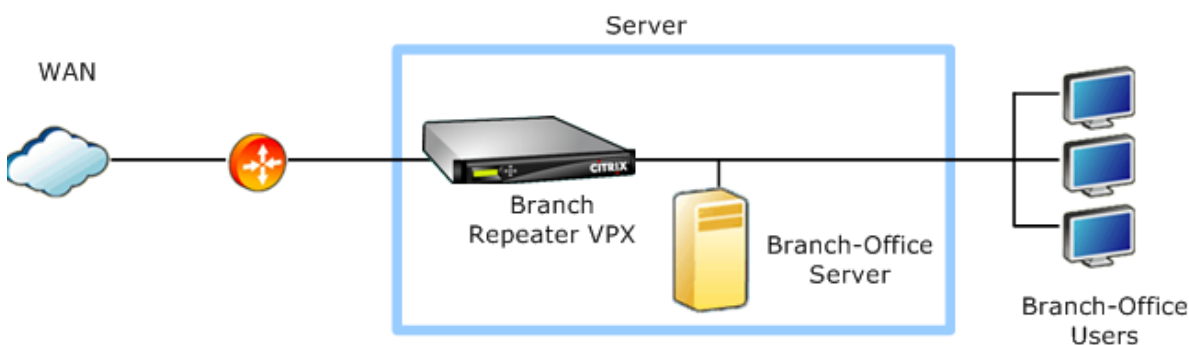
Accelerated datacenter servers

Installing VPX VMs on every server in the data center creates a solution that scales perfectly as you add server capacity, while minimizing the number of servers by adding acceleration to the servers

themselves. Once you have more than a few accelerated servers, the aggregate acceleration provided by multipleVPX VMs exceeds anything that can be provided with a single appliance.

VPX accelerates all types of network applications, including XenApp, XenDesktop, Citrix Merchandising Server, network file systems, databases, web servers, and more.

Figure 3. VPX use case #3: Accelerated Datacenter Servers
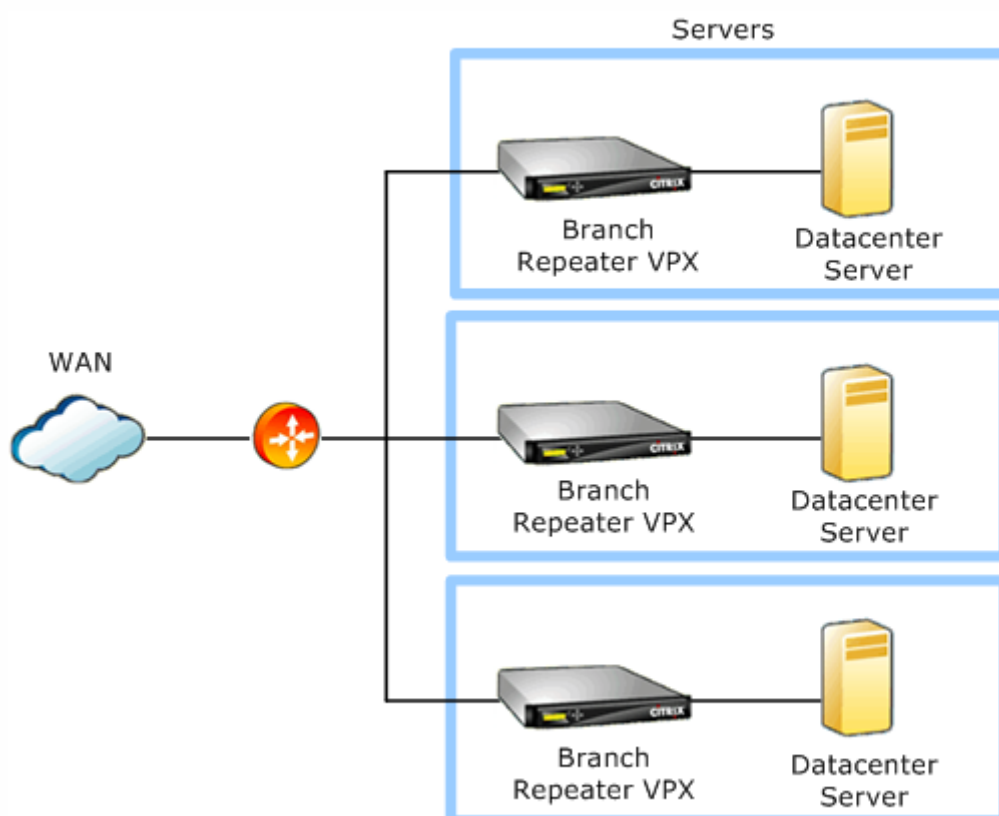
VPN accelerator

By installing the VPN of your choice with VPX, you have an accelerated VPN.

> **Note**: Unlike other configurations, the VPN virtual machine is on the WAN side and the VPX virtual appliance is on the LAN side, because the VPN traffic must be decrypted for compression and application acceleration.

Figure 4. VPX use case #4: VPN accelerator
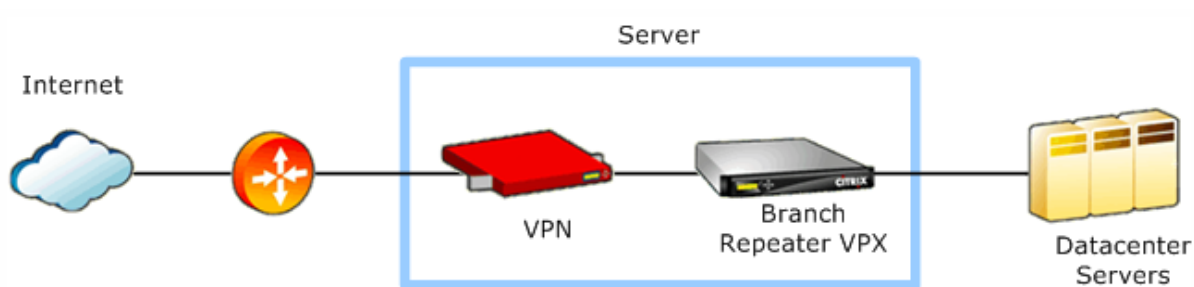
Multiple VPX Instances on the same server

By putting multiple VPX VMs on the same server, you can create different types or levels of acceleration services within the same unit. One VPX instance might be dedicated to a critical application, or each instance dedicated to an individual remote site or customer. Use VLAN switches to direct traffic to the appropriate VPX instance.

Figure 5. VPX use case #5: Multiple Instances for Dedicated Acceleration Resources
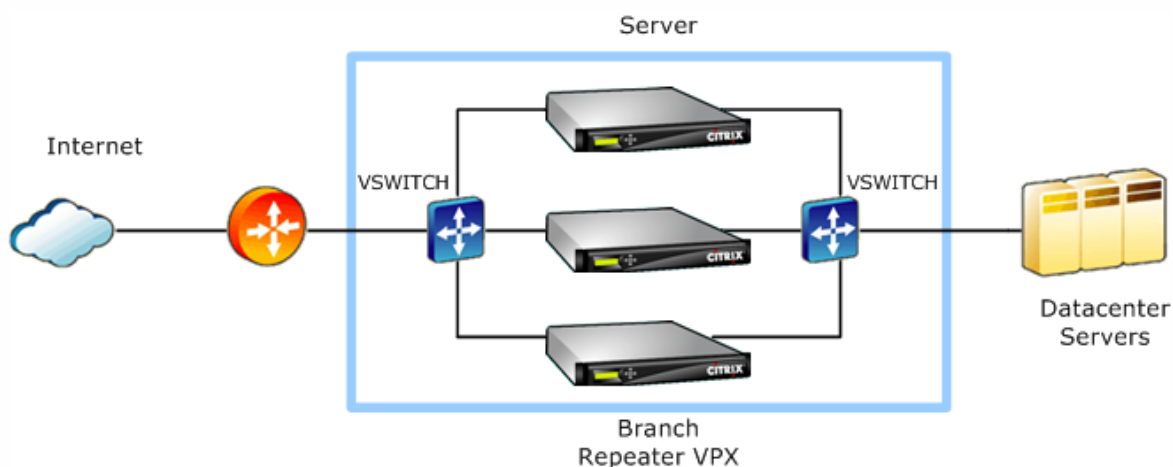
WCCP and virtual inline deployment

WCCP and virtual inline modes are suitable for one-arm deployments, which use only one port. The Amazon AWS version of VPX uses only a single port, and is thus always deployed in a one-armed mode.

Figure 6. VPX use case #6: WCCP or virtual inline deployment
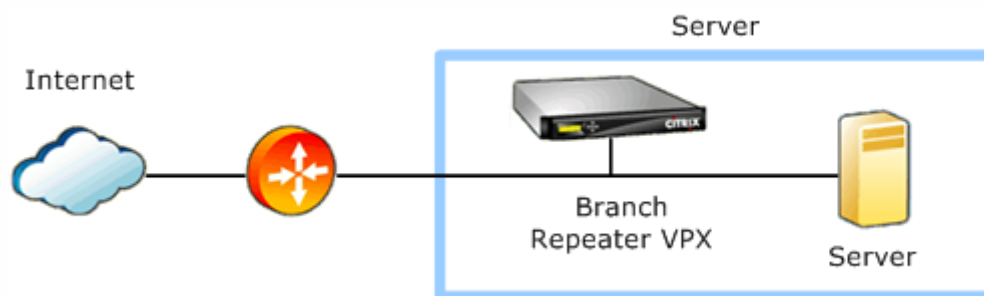
In cases where an Ethernet bypass card would be desirable, using WCCP instead of inline mode provides effective fault-tolerance, because WCCP has built-in health-checking. Instead of forwarding traffic through an unresponsive WCCP device, the routers send the traffic directly to the end point.

Branch-office accelerator SD-WAN/SD-WAN VPX can be installed on the server of your choice and deployed just like any other SD-WAN/SD-WAN appliance. VPX has the same functionality as the SD-WAN/SD-WAN appliance along with the additional features provided by virtualization. The group mode and high-availability mode are not supported.

SD-WAN VPX features

VPX supports Citrix Command Center release 4.0 or later. SD-WAN also supports SD-WAN/SD-WAN VPX Express licenses, which support a maximum accelerated sending rate of 512 kbps, 10 accelerated connections, and 5 SD-WAN/SD-WAN Plug-ins.

- VPX for XenServer special features includes:
    - XenServer Essentials Support
    - XenMotion Live Migration
    - XenServer High Availability
    - Workload Balancing
    - Performance Monitoring and Alerts
- VPX for VMware vSphere special features include:
    - VMware vCenter Server (remote management).
    - VMware vSphere high availability (high availability).
    - VMware vSphere vMotion (migrate SD-WAN VPX to a different server with identical processors).
    - VMware Guest Customization (replicate VPX with different per-instance parameters).

System Requirements and Provisioning

October 8, 2021

SD-WAN VPX runs on XenServer 5.5 or later, VMware vSphere ESX/ESXi 4.1 or later, Hyper-V under 64-bit Windows Server 2008 R2 SP1, and AWS. SD-WAN VPX supports four configurations, from 2 GB to 8 GB of RAM and 100 GB to 500 GB of disk space. The intermediate, 4 GB RAM/250 GB disk configuration is similar to the Repeater 8500 series appliance.

Supported configurations

The following tables list all supported SD-WAN VM configurations. (AWS configurations are preselected and are different.)

Type	vCPUs	RAM	Disk	Maximum WAN Speed	Maximum Accelerated Connections	Maximum SD-WAN/SD-WAN Plug-ins
2 GB production config.	2	2 GB	100 GB	2 Mbps	1,000	50
4 GB production config.	2	4 GB	250 GB	10 Mbps	10,000	250
4 GB production config. (With 45mbps license)	2	4 GB	250 GB	45 Mbps	15,000	400
8 GB production config.	4	8 GB	500 GB	45 Mbps	25,000	500

Other configurations (not for production networks)

Type	vCPUs	RAM	Disk	Maximum WAN Speed	Maximum Accelerated Connections	Maximum SD-WAN/SD-WAN Plug-ins
VPX Express	2	1 GB	60 GB	512 kbps	10	5
Min. evaluation config.	2	1 GB	60 GB	2 Mbps	1,000	5

Minimum resource requirements

An SD-WAN VPX virtual machine has the following minimum hardware requirements for a production environment:

- 2 GB RAM
- 100 GB disk (local disks provide the best performance)
- 2 virtual NICs (Ethernet ports), except for AWS, which requires only one virtual NIC
- 2 virtual CPUs
- A modern CPU (Intel Nehalem or newer or AMD Family 10 h or newer, both of which were introduced in 2008). Older CPUs can run at reduced performance due to the use of emulated x86 TSC (timestamp counter) functionality. When clock states higher than C1 are not used and Speed-Step/PowerNow modes are disabled in the BIOS of older processors, TSC emulation will not be used and the system runs at normal speed.

The server hosting VPX must have RAM, CPU, and disk resources greater than those required by the VPX VM. (VPX does not support VMware hardware over-commit.) The server must have enough resources to run the hypervisor in addition to the virtual appliance. However, having as many physical Ethernet ports as virtual ones is not mandatory when one of a VPX VM's Ethernet ports is connected to another virtual machine on the same server. Possible Ethernet options include:

- Mapping the VPX VM's two virtual ports to two physical ports, rendering its operation equivalent to that of a stand-alone SD-WAN.
- Mapping one of the VPX VM's virtual ports to a physical port, and the other to a virtual network containing one or more virtual machines on the same server, thus creating an accelerated server.
- Mapping each of the VPX VM's virtual ports to a virtual network, thus chaining the VPX VM between two sets of VMs on the same server.

The following figure shows a VPX VM in a one-arm deployment for traffic that ends on another virtual machine on the same server. Only one physical port is required in this case, but both virtual ports are

used.
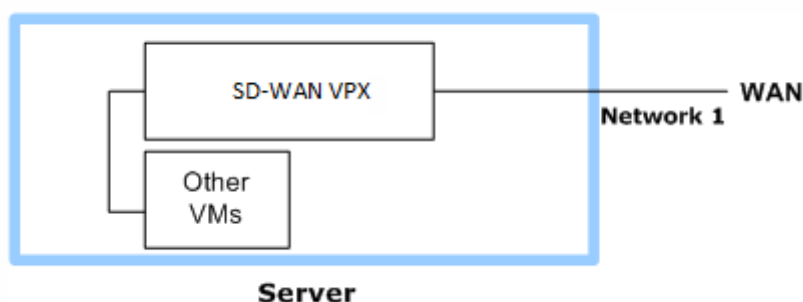
For VPX VM requirements for cloud deployments, see the following links:

- AWS
- Azure
- GCP

Maximum usable resources

Following are the maximum amount of resources that a single VPX virtual machine can use effectively:

- 4 virtual CPUs
- 8 GB RAM
- 500 GB disk
- 4 virtual NICs (Release 9.x)
- 8 virtual NICs (Release 10.x)

  Server resources not allocated to VPX VMs are available to other VMs on the same server, but be careful to avoid overcommitting resources.

Disk and RAM

While the amounts of RAM and disk space are increased, the additional resources are allocated primarily to the compression subsystem. Increased memory also allows more connections and acceleration partners to be supported.

The SD-WAN compression system makes heavy demands on the disk subsystem. In general, local disk storage outperforms network disk storage and reduces resource contention on both the LAN and the network disk.

The relationship between disk or memory resources and link speed is indirect. Memory and disk sizes have no effect on the speed at which packets are sent more than the link (bps). Providing more memory and disk space improves compression performance by increasing the amount of compression history that can be used for pattern matching.

Virtual NICs

Except for AWS, two virtual network interfaces are required. They are bridged and used for both acceleration and the browser based user interface. These interfaces must be attached to different virtual networks. For one-arm operation, the second interface can be a stub, attached only to a VPX VM.

A third virtual network interface provides an independent interface to the VPX VM, which is the equivalent to the Primary port on a physical appliance. It can be used for the browser based interface, but not for acceleration.

Other virtual machines

- Server resources beyond those allocated to VPX are available for other virtual machines on the same server.
- Resource usage by other VMs effects VPX performance, and conversely. Acceleration makes intensive use of CPU, memory, disk, and network.

Virtual network routing can be used to connect other VMs on the server to VPX VMs, but the simplest method of connecting such VMs is to attach them to the server's LAN-side Ethernet port. WAN-bound packets then pass through the VPX VM's bridge and are accelerated automatically, if they originate inside or outside the server hosting VPX.

Figure 2. An Inline Deployment that Accelerates External Traffic and Traffic from Local VMs
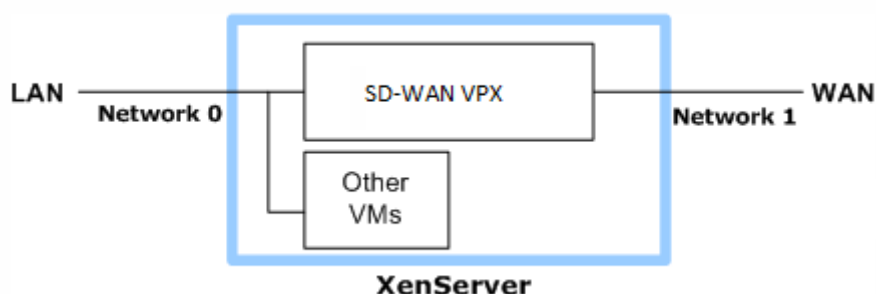
Installing SD-WAN Virtual Appliances on XenServer

June 19, 2020

To install NetScaler SD-WAN virtual appliances on Citrix XenServer, you must first install XenServer on a machine with adequate system resources. To perform the SD-WAN VPX installation, you use Citrix XenCenter, which must be installed on a remote machine that can connect to the XenServer host through the network.

Before you begin installing a virtual appliance, do the following:

- Install a supported version of XenServer® on hardware that meets the minimum requirements. See the SD-WAN release notes for the supported versions of XenServer.
- Install XenCenter® on a management workstation that meets the minimum system requirements.
- Obtain VPX license files.

With the prerequisites met, you are ready to import the virtual appliances and configure them.

To import an SD-WAN virtual appliance to XenServer by using XenCenter

1. Start XenCenter on your workstation.
2. On the **Server** menu, click **Add**.
3. In the **Add New Server** dialog box, in the **Hostname** text box, type the IP address or DNS name of the XenServer server that you want to connect to.
4. In the User Name and Password text boxes, type the administrator credentials, and then click **Connect**. The XenServer name appears in the navigation pane with a green circle, which indicates that the XenServer is connected.
5. In the navigation pane, click the name of the XenServer server on which you want to install SD-WAN VPX.
6. On the **VM** menu, click **Import**.
7. In the **Import** dialog box, in Import file, browse to the location at which you saved the SD-WAN VPX.xva image file. Make sure that the Exported VM option is selected, and then click **Next**.
8. Select the **XenServer server** on which you want to install the virtual appliance, and then click **Next**.
9. Select the local storage repository in which to store the virtual appliance, and then click **Import** to begin the import process.
10. Add, modify, or delete virtual network interfaces as required. Attach virtual network interfaces, interface 0, and interface 1 to the two different virtual adapters (called Networks on this screen). These two interfaces are used as the accelerated bridge of the virtual appliance. If virtual network interface 2 exists, it can be assigned as well, and used as a management interface (equivalent to the Primary port). When finished, click **Next**.
11. Clear the **Start the VM after Import** check box.
12. Click **Finish** to complete the import process. To view the status of the import process, click the **Log** tab. The newly created virtual machine appears under the server list in the XenCenter interface.

> Important
>
> Do not attach both virtual adapters to the same network. Doing so creates forwarding loops, which can cause network outages. Also, do not attach the two physical Ethernet ports associated

with SD-WAN VPX to the same Ethernet switch.

To configure the virtual SD-WAN appliance

1. In XenCenter, select the icon for the SD-WAN VPX virtual machine. Then, on the **Storage** tab, select **Properties** and, in the **Properties** dialog box, adjust the disk allocation to the desired level.

   Note:

   - Changing the disk allocation on the SD-WAN VPX virtual machine resizes and reinitializes the compression history. Any accumulated history is lost.
   - Do not attempt to change resource allocation while SD-WAN VPX is running.
   - Do not use the **Force Shutdown or Force Reboot** commands. They might not work and can cause problems. Use the **Shutdown and Reboot** commands instead.

2. Right-click the **SD-WAN VPX** icon and select the Properties option. Under CPU and Memory, select the number of VCPUs and the amount of VM memory corresponding to a supported configuration.

3. In the **SD-WAN VPX Properties** dialog box, click **Startup Options**, and then select the **Auto-start** on server boot check box. (The OS Boot Parameters are not used).

4. Set the basic network parameters. Depending on which release you are running, do one of the following:

   a) After the virtual machine starts, go to the virtual machine console, log into the command-line interpreter, and set the IP parameters for the accelerated bridge, using the following example as a guide:

   ```
   pre codeblock Login: admin Password: password admin> set adapter
    apa -ip 172.16.0.213 -netmask 255.255.255.0 -gateway 172.16.0.1
   admin> restart <!--NeedCopy-->
   ```

   b) When an SD-WAN VPX virtual machine is started for the first time, it automatically runs the Deployment Wizard. Follow the wizard to set the IP parameters.

5. After the SD-WAN VPX has restarted, log on to the browser-based UI (Default credentials: admin and password) at the IP address that you assigned to apA

6. From the **Command** menu, select **Quick Installation**.

7. On the Quick Installation page, perform a quick installation as you would for a physical SD-WAN appliance.

8. Complete the configuration.

> **NOTE**
>
> - From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.
>
> - A system maintenance account - CBVWSSH, exists for development and debugging and has no external login permissions. The account can only be accessed through a regular administrative user's CLI session.

XenServer 6.5 Upgrade for SD-WAN Standard Edition Appliances

June 19, 2020

> **Important**
>
> To upgrade to XenServer version 6.5, the appliances must be running SD-WAN software release 9.0.x or later.
>
> **Note**
>
> Do not attempt upgrading, if the appliance is running on software version lower than release 9.0.x to prevent upgrade issues.

How to upgrade to XenServer 6.5

To upgrade to XenServer 6.5 on SD-WAN Standard Edition appliances, ensure that the appliance is running software release version 9.0.x or later. If the appliances are running older software release version, upgrade to the latest software release version first.

1. Upgrade SD-WAN Standard Edition software through the change management procedure. See, the Change Management procedure.

    a) In SD-WAN SE GUI, go to **Configuration** > **System Maintenance** > **Update Software**. Download the *cb-vw-<Platform_Model>-<Build_No>.tar.gz* file. Then, download *ns-sdw-*

    vw-<Build_No>.upg file to update operating system software.

    b) Follow Single-Step Upgrade work flow to upgrade SD-WAN software.

2. Perform steps a or b as outlined in step 1 before upgrading to Citrix XenServer 6.5.

---
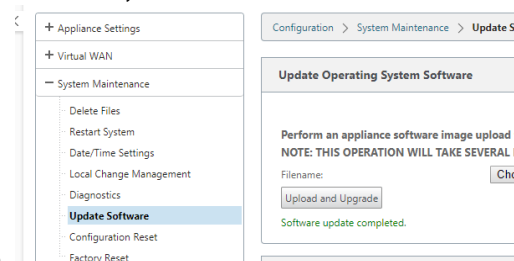
3. Navigate to **Update Software** in the SD-WAN GUI.

4. Upload Citrix XenServer6.5 bundle which has been download from download server to **Update Operating System Software** by selecting the downloaded file location.
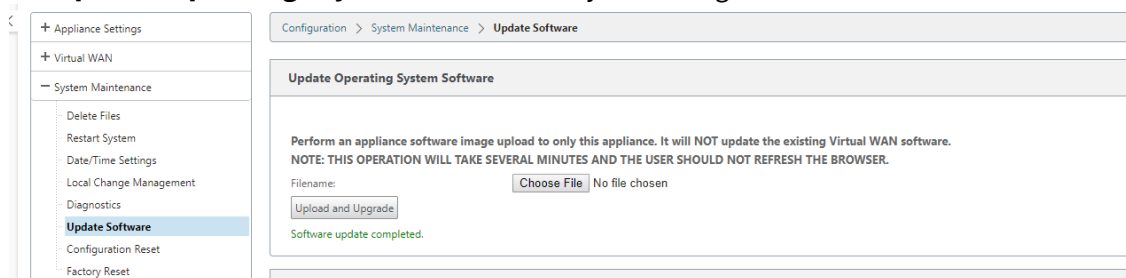
5. Click **Upload and Upgrade**. Wait for approximately 20 mins for the upgrade to complete. The appliance restarts after the upgrade is successfully completed.

Installing SD-WAN Virtual Appliances on VMware ESX

September 29, 2021

> Warning
>
> Ensure that you enable the promiscuous mode on VM Network only. Do not enable the promiscuous mode on the **Virtual Switch** setting.
>
> **Note**
>
> VMware vSphere Client operation details might change with new releases of the vSphere software. For the most complete and current vSphere Client installation and operation instructions, also see your VMware documentation. The instructions in this chapter are intended to provide the most basic and essential guidelines, only, for installing an SD-WAN VPX-SE Virtual appliance on the ESXi platform.

The following summarizes the top-level steps for installing and deploying an SD-WAN VPX-SE. Perform these procedures in the exact order listed.

1. Install the VMware vSphere Client.
2. Install and deploy the SD-WAN VPX-SE OVF Template.
3. Configure the SD-WAN VPX-SE Management IP Address.
4. Connect and test the deployment.

This chapter provides step-by-step instructions for installing, configuring, and deploying the SD-WAN VPX-SE. This includes basic instructions for installing the VMware vSphere Client, which you use to create and deploy the SD-WAN VPX-SE virtual machine.

Before you begin installing a virtual appliance, do the following:

- Install VMware ESX version 5.5 or ESXi 6.0, or later, on hardware that meets the minimum requirements.
- Install the VMware vSphere client on a management workstation that meets the minimum system requirements.
- Download the SD-WAN VPX-SE set up files.
- Obtain SD-WAN VPX-SE license files.

Also, before installing an SD-WAN VPX-SE virtual appliance, label all the interfaces that you plan to assign to VPX virtual appliances, in a unique format. In large deployments, labeling these interfaces in a unique format helps in quickly identifying them between other interfaces used by other virtual machines, such because Windows and Linux virtual machines. Such labeling is especially important if different types of virtual machines share interfaces.

SD-WAN VPX-SE requires non-default networking options. Between other things, you create two new virtual switches (vswitch0 and vswitch1) for the accelerated bridge, which must be assigned to two different virtual switches.

Installing the VMware vSphere Client

This section provides basic instructions for downloading and installing the VMware vSphere client you use to create and deploy the SD-WAN VPX-SE virtual machine.

> **Note**
>
> See also your VMware vSphere Client documentation for additional information.

1. Open a browser and navigate to the ESXi server that hosts your vSphere Client and SD-WAN VPX-SE virtual machine (VM) instance. The **VMware ESXi Welcome** page displays.

2. Choose the **Download vSphere Client** link to download the vSphere Client installation file.
3. Install the vSphere Client. Run the vSphere Client installer file that you downloaded, and accept each of the default options whether prompted.
4. After the installation completes, start the vSphere Client program. The **VMware vSphere Client** login screen displays, prompting you for the ESXi server login credentials.
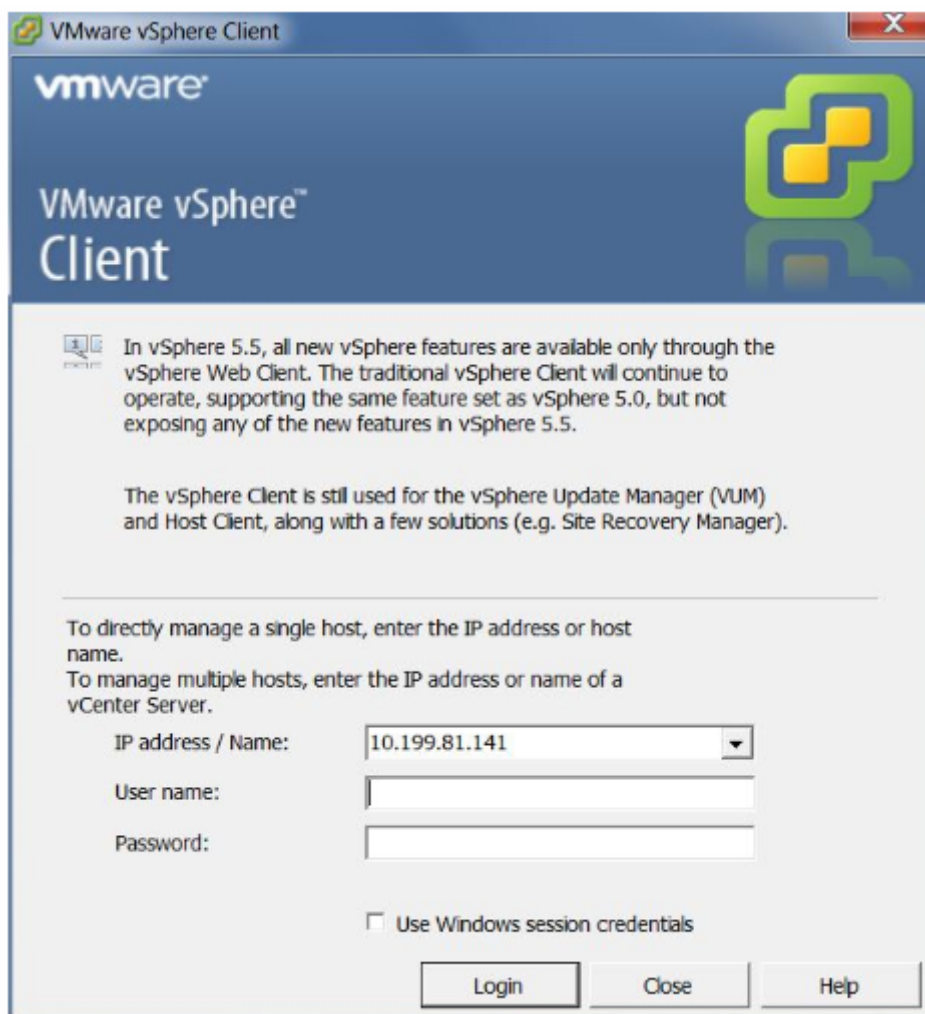
5. Type the ESXi server login credentials. Type the following:
   - **IP address / Name**: Type the IP Address or Fully Qualified Domain Name (FQDN) for the ESXi server that hosts your SD-WAN VPX-SE VM instance.
   - **User name:** Type the server administrator account name. The default is root.
   - **Password**: Type the password associated with this administrator account.
6. Choose **Login.** This appears the **vSphere Client** main page.
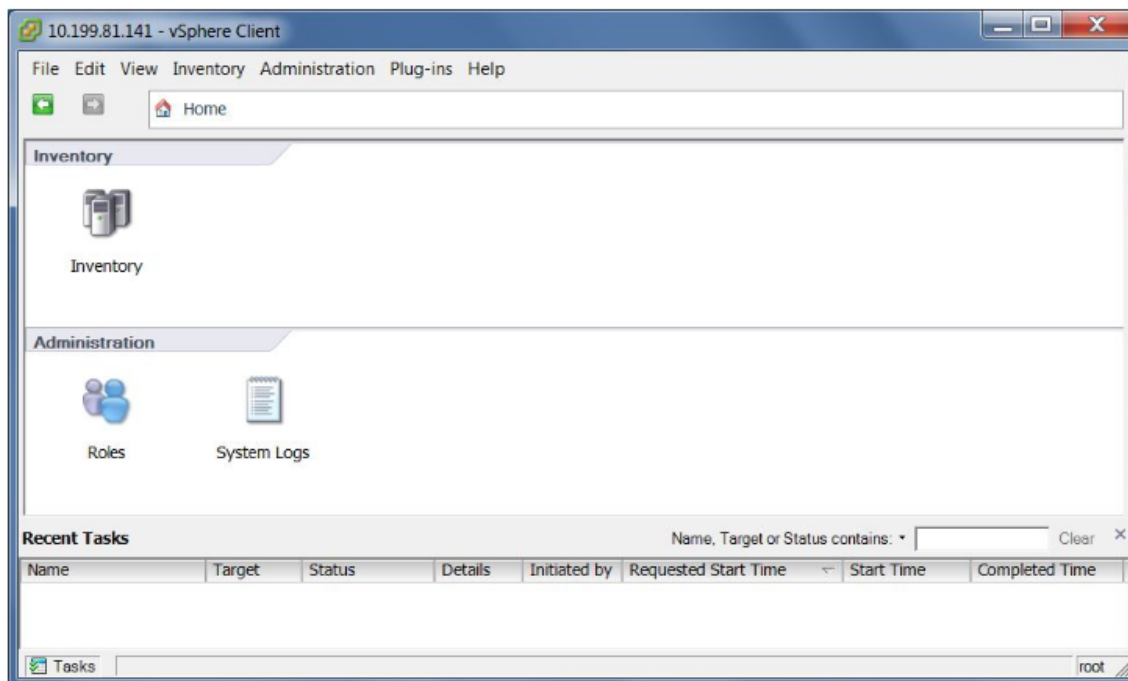
The next step is to install and deploy the SD-WAN VPX-SE OVF template and set up the virtual machine. The following section provides instructions for these procedures.

Installing and deploying the SD-WAN VPX-SE OVF Template

This section provides instructions for installing the SD-WAN VPX-SE OVF template and creating the SD-WAN VPX-SE virtual machine.

1. When you have not already done so, download the SD-WAN VPX-SE OVF template file (.ova file) to the local PC. Download or copy the SD-WAN VPX-SE OVF template to the local PC you are using to connect to the ESXi server that hosts your SD-WAN VPX-SE. The OVF template file has a file name using the following naming convention: **cb-vwc-version_number-vmware.ova**
Where:

   version_number is the SD-WAN VPX-SE release version number.

   .ova is the file name suffix indicating that this is an OVF template file.

   > **Note**
   >
   > For additional information, please see Downloading the Software Packages section.

2. Continuing in the vSphere Client, choose **File** and then choose **Deploy OVF Template...** from the drop-down menu. This appears the first page of the **Deploy OVF Template** wizard, the **Source** page.

3. Choose the SD-WAN VPX-SE OVF template *(.ova* file) you want to install. Browse to the location of the *.ova* file you downloaded earlier to the local PC, and choose it.

---

4. Choose **Next**. This imports the selected *.ova* file and appears the **OVF Template Details** page.

5. The next page appears some basic information regarding the OVF template you imported.

6. Choose **Next**. This proceeds to the **EULA** page.

7. Choose **accept**, and then choose **Next**. This proceeds to the **Name and Location** page.

8. Type a unique name for the new VM (or accept the default). The name must be unique within the current **Inventory** folder, and can be up to 80 characters in length**.**

9. Choose **Next**. This proceeds to the **Storage** page.

10. Choose a datastore that has sufficient space available for the VM. The SD-WAN VPX-SE virtual machine requires 39.1 GB of disk space.

11. Choose **Next**. This appears the **Disk Format** page.

12. Accept the default settings, and choose **Next**. This proceeds to the **Network Mapping** page.

13. Accept the default (**VM Network**) and choose **Next**. This proceeds to the Ready to Complete page.

14. Choose **Finish** to create the VM. This appears the **Deploying NetScaler SD-WAN VPX-SE** status dialog box. Depending on the conditions present on your server, the deployment can take from several minutes to a few hours to complete. When the SD-WAN VPX-SE virtual machine has been successfully created, a success message displays.

15. Choose **close**. This closes the **Deploy OVF Template** wizard and returns to the vSphere Client main window. When this is the first VM you have created using this vSphere Client, the vSphere Client **home page** displays. When you have previously created one or more VMs, the **Inventory** page displays.

The next step is to configure the SD-WAN VPX-SE Management IP Address. The following section provides instructions for this procedure.

Configuring the Management IP address for the SD-WAN VPX-SE

There are two methods for assigning the Management IP Address to the SD-WAN VPX-SE virtual machine:

- When you are not using DHCP: You must manually assign a static Management IP Address for the SD-WAN VPX-SE Virtual Appliance.
- When you are using DHCP: By default, all SD-WAN -VW Virtual Appliances use DHCP to acquire the Management IP Address. To use DHCP, the DHCP server must be present and available in the Virtual WAN.

For more information see, Configuring the management IP.

Manually configuring a static Management IP address for the VPX

When you are not using DHCP, or want to set a static Management IP Address for the SD-WAN VPX-SE Virtual Appliance VM, you must do this manually. To do so, you use the console for the virtual machine you created, in the vSphere Client.

Also see, Setting up the SD-WAN Virtual WAN Appliances.

To set the Management IP Address manually, do the following:

> **Note**
>
> DHCP is enabled by default for the SD-WAN VPX-SE Management IP Address.

1. Continuing in the vSphere client **Inventory** page, choose the new SD-WAN VPX-SE VM in the **Inventory** tree (left pane). This appears the **Inventory** page for the new VM, with the **Getting Started** tab preselected.
2. Power on the new virtual machine. In the **Basic Tasks** section of the **Getting Started** tab page, choose **Power on the virtual machine** (green play mouse button) to power on the new SD-WAN VPX-SE VM.
3. Click the **Console** tab in the **Inventory** page tab bar. The Console tab is located in **Inventory** page tab bar at the top of the main page area. Selecting this tab appears and enables access to the CLI console for the VM. Because the new VM starts up, a series of status messages are displayed in the console. When the startup process completes, the console login prompt displays.
4. Choose anywhere inside the console area to type console mode. This turns control of your pointing device cursor more than to the VM console, and enables console mode.
5. Log into the VM console. The default login credentials for the new SD-WAN VPX-SE VM are because follows:
   Login: *Admin*
   Password: *password*
   This appears the console **Welcome** screen.
6. Type the following command line at the console prompt: `management_ip` This switches to the `management_ip` CLI in the console, and appears the `set_management_ip` prompt.
7. Configure the interface settings for the VM. Type the following command line at the *set_management_ip* prompt:
   `set` **`interface`** `<ipaddress> <subnetmask> <gateway>`
   Where:
   - `<ip>` is the Management IP Address for the SD-WAN VPX-SE Virtual Appliance.
   - `<subnetmask>` is the subnet mask used to define the network in which the SD-WAN VPX-SE Virtual Appliance resides.
   - `<gateway>` is the Gateway IP Address the SD-WAN VPX-SE Virtual Appliance uses to communicate with external networks.
     This stage but does not apply the interface settings.

8. Apply the staged settings for the VM interface. Do the following:

    a) Type the following command at the *set_management_ip* prompt:

       Apply

    b) When prompted to confirm the *apply* operation, type *Y*. This applies the staged interface settings for the VM, and appears the results.

9. Type exit and press **Return** at the prompt to exit the management_ip CLI.

10. Exit the console. Type **exit** and press **Return** at the console prompt, and then press **Ctrl+Alt to regain control of the cursor.**

11. Shutdown and start the VM. Do the following:

    a) Choose the **Getting Started** tab to display the **Basic Tasks** options.

    b) In the **Basic Tasks** section, choose **shutdown the virtual machine** (red check box icon). You are prompted to confirm that you want to end the guest operating system for the VM.

    c) Choose **Yes** to confirm. This shuts down the guest operating system and powers off the VM. When the shutdown completes, the **Power on the virtual machine** option (green play mouse button) becomes available.

12. Start the virtual machine. Choose **Power on the virtual machine** (green right-arrow) to start the VM. You can view the progress of the start-up process in the **Console** tab page for the VM.

When the startup process completes, the login prompt displays. You can now proceed to the final step, Connecting to the SD-WAN VPX-SE and Testing the Deployment.

> **NOTE**
>
> • From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.
>
> • A system maintenance account - CBVWSSH, exists for development and debugging and has no external login permissions. The account can only be accessed through a regular administrative user's CLI session.

SD-WAN Standard Edition Virtual Appliance (VPX) in Hypervisor on HyperV 2012 R2 and 2016

January 12, 2021

To install SD-WAN VPX-SE in the hypervisor on HyperV 2012 R2 and 2016:

1. Install **HyperV Manager**. For more information, see documentation at Microsoft.com.
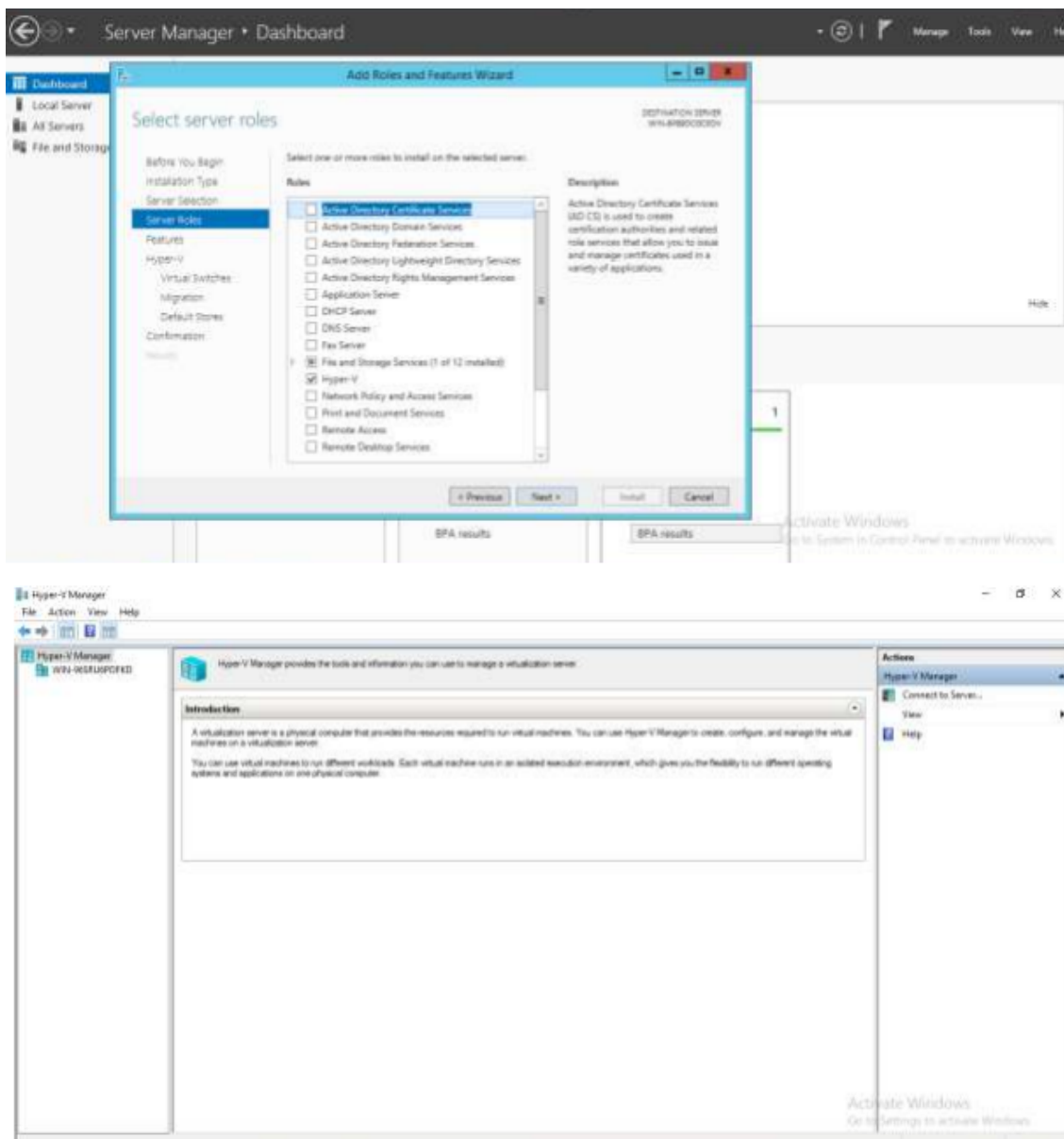
2. Unzip the SD-WAN distribution that you downloaded from **My Citrix**.

3. Start **Hyper-V Manager**.

There are two methods to create the virtual machine.

- **Method 1**: Import virtual machine

    1. In the navigation pane, under **Hyper-V Manager**, select the server on which you want to install **SD-WAN VPX**.

    2. On the Actions menu, click **Import Virtual Machine**.

    3. In the **Import Virtual Machine** dialog box, in **Location** box, specify the path to the folder that contains the SD-WAN VPX files.

        > **Note**
        >
        > If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.

    4. Click **Import**.

    5. Verify that the virtual appliance that you created is listed under **Virtual Machines**.

    6. Right-click the virtual machine, and then click **Settings**.

    7. In the **Settings** window's navigation pane, under Hardware, select the first network adapter in the list.

    8. In the **Network** drop-down menu, select apA1 Network. This is the LAN interface for apA1.

    9. Make sure the **Enable MAC address spoofing** box is selected. If it is not, select it and apply the changes.

    10. In the **Settings** window's navigation pane, under Hardware, select the second network adapter in the list. Repeat the step 10 and step 11, and assign the adapter to apA2 Network. This is the WAN interface for apA2. Important: Do not configure the same Network for both the network adapters. Incorrect configuration creates packet loops, which can bring down the network.

    11. Optionally, change the virtual hard disk size:

        – In the **Settings** window navigation pane, under IDE Controller 0, select **Hard Drive**.
        – Click **Edit**.
        – Follow the steps in the Edit Virtual Hard Disk Wizard to increase the allocation to one of the supported sizes, using the Expand option in the wizard.

    12. Optionally, change the memory size.

        – In the **Settings** window's navigation pane, under **Hardware**, select **Memory**.
        – Allocate the RAM space by adjusting the memory to one of the supported sizes.
        – Click **OK**.

    13. Optionally, define the management port.

        – Right-click the virtual machine, and then click **Settings**.

- In the **Settings** window navigation pane, under **Hardware**, select **Add Hardware**.
- Select **Network Adapter** from the list of devices, and then click **Add**.
- Name the new virtual network as Primary Network 3.
  * Make sure the **Enable spoofing of MAC addresses** check box is selected.
  * Click **OK** to apply the changes.

14. Right-click the **SD-WAN VPX virtual machine** and select **Connect**.

15. In the file menu, click **Action**, and then click **Start** to start the virtual machine.

16. When an SD-WAN VPX virtual machine is started for the first time, it automatically starts the Deployment Wizard. This wizard asks questions about the deployment mode. Select **Setup Using Web UI**. On the next screen, enter the **IP address**, netmask, and gateway for the apA interface, and click **Finish**.

17. After SD-WAN VPX has restarted, log on to the browser based UI ((user name: admin, password: password) at the IP address that you assigned to apA, for example: `https://172.16.0.213`

18. In the **HyperV Manager** window, go to **Virtual Switch Manager,** and configure interfaces in the following order; management, LAN, and WAN.
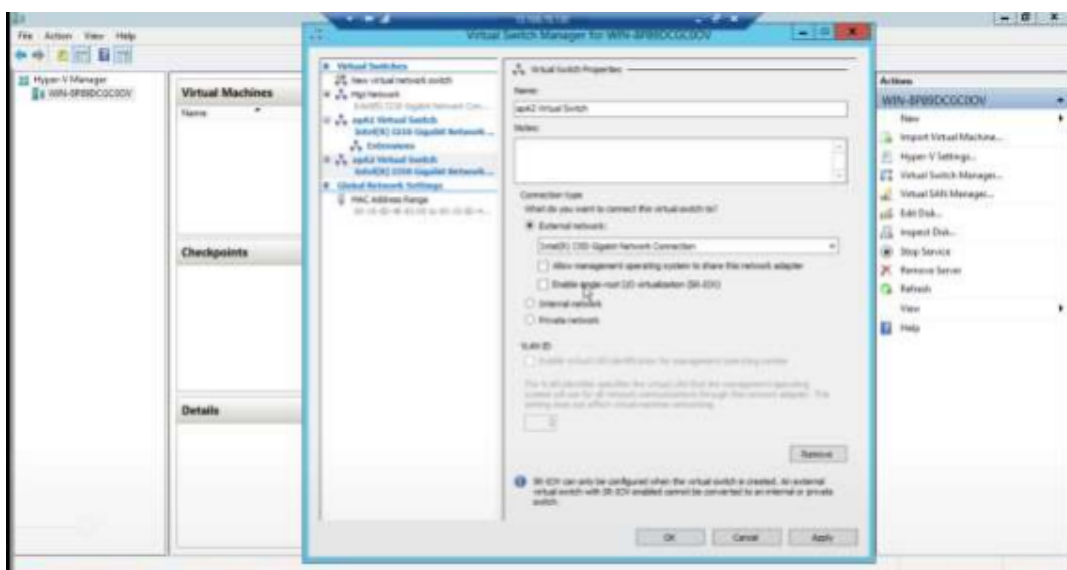
19. Download the ***hyperv.tgz*** file and untar it.

20. Import VM using the extracted *VHD* and assign the number of CPUs and memory accordingly. Add interfaces in the order (management, LAN, and WAN). Enable Mac spoofing on LAN and WAN interfaces. Go to **Settings** > **Interface** >**Advanced features**.

- **Method 2**: New virtual machine wizard

    > **NOTE**
    >
    > Select method 2 if the Hyper-V virtual machine has to connect to orchestrator.

    1. Open the SD-WAN Hyper-V setup file and select **Virtual Hard Disks** folder.

    2. Copy the hard disk image and paste it in a freshly created folder outside of the Hyper-V setup file.

    3. Open the **Hyper-V Manager > select the Hyper-V ID >** right click and select **New > Virtual Machine**.

    4. The **Virtual Machine Wizard** opens, Click **Next**.

5. Provide the name and you can also specify a location for the virtual machine. Select the check box to provide a different location to store the virtual machine. Click **Next**.

6. Select the generation for the virtual machine and click **Next**.

7. Specify the amount of memory to allocate to the virtual machine and click **Next**.

8. Select a connection from the drop-down list and click **Next**. The connection being selected here is for Management port.

9. To connect VHD, select the **Use an existing virtual hard disk** radio button, browse, and select the VHD file from the extracted zip file and click **Next**. The virtual hard disk can be found in below location:

** > ctx-sdw-se-vpx > Virtual Hard Disks**

10. Verify the details on the **Summary** page and click **Finish** to complete the creation of the virtual machine.

By default, the virtual machine is in **Off** sate. The virtual machine created so far has only 1 Interface and 1 core, you have to increase the number of cores and add 2 more Interfaces for SD-WAN to work. Perform the following procedure:

1. Verify that the virtual appliance that you created is listed under **Virtual Machines**.

2. Right-click the virtual machine, and then click **Settings**.

3. In the **Settings** window's navigation pane, under Hardware, select the first network adapter in the list.

4. In the **Network** drop-down menu, select apA1 Network. This is the LAN interface for apA1.

5. Make sure the **Enable MAC address spoofing** box is selected. If it is not, select it and apply the changes.

6. In the **Settings** window's navigation pane, under Hardware, select the second network adapter in the list. Repeat the step 10 and step 11, and assign the adapter to apA2 Network. This is the WAN interface for apA2. Important: Do not configure the same Network for both the network adapters. Incorrect configuration creates packet loops, which can bring down the network.

7. Increase Number of Virtual CPU cores.

   - In the **Settings** window navigation pane, select **Processor**.
   - Increase **Number of virtual processors** to at least 4.

- Click **Apply**.

8. Optionally, change the virtual hard disk size:

   - In the **Settings** window navigation pane, under IDE Controller 0, select **Hard Drive**.
   - Click **Edit**.
   - Follow the steps in the Edit Virtual Hard Disk Wizard to increase the allocation to one of the supported sizes, using the Expand option in the wizard.

9. Optionally, change the memory size.

   - In the **Settings** window's navigation pane, under **Hardware**, select **Memory**.
   - Allocate the RAM space by adjusting the memory to one of the supported sizes.
   - Click **OK**.

10. Right click and select **start**. Once the state is changed to **Running**, your virtual machine is now ready to use.

Adding interfaces
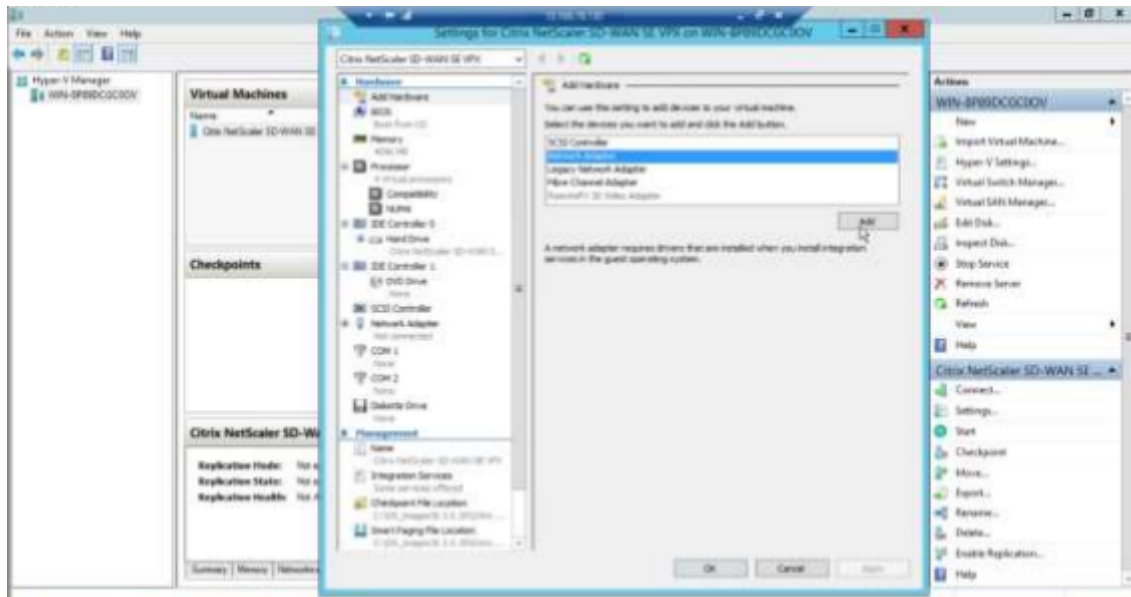
Enabling Mac spoofing on the interfaces (LAN and WAN)
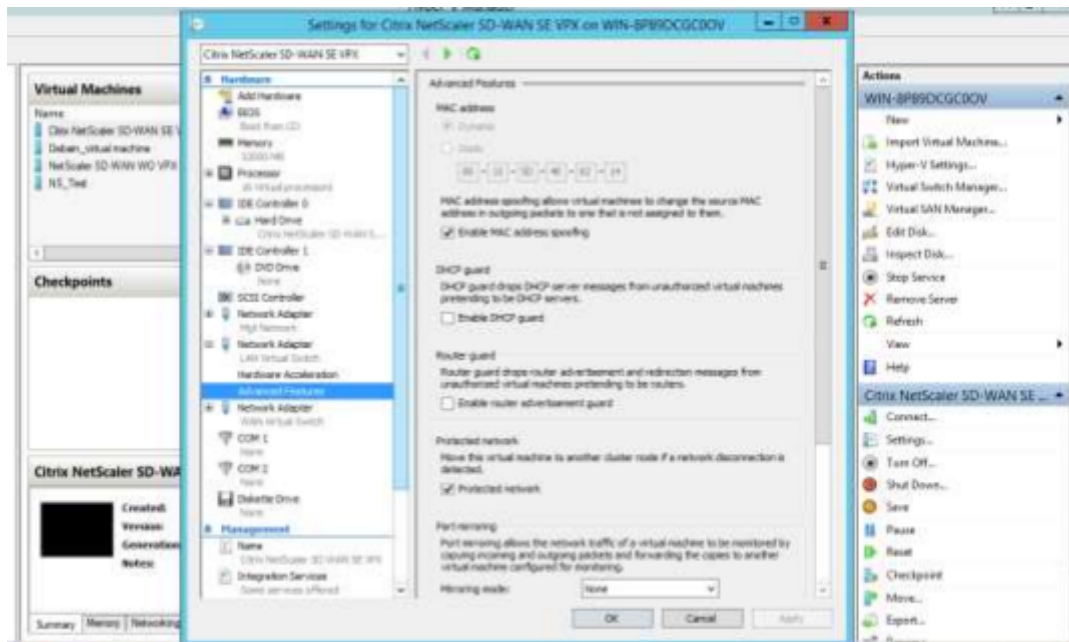
After the VM is up, assign free IP address. The VM can be accessed after assigning the IP address.
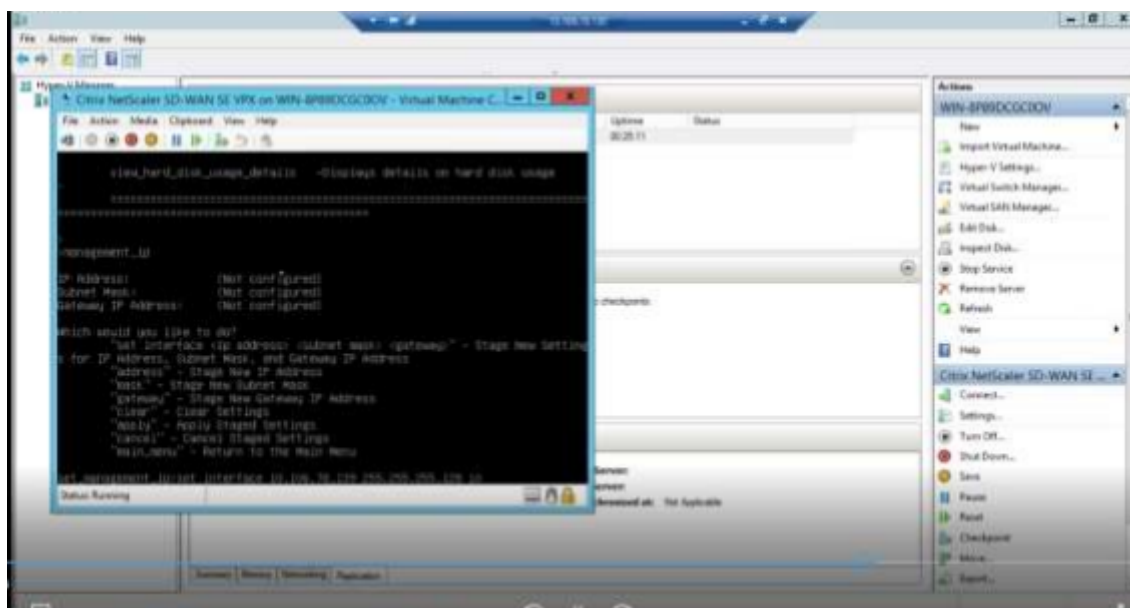
Note

The qcow image downloaded must be present under the default folder /var/lib/libvirt/images. If this image is downloaded, and used in different folder in **KVM**, there can be issues when disk size expansion is performed.

Limitations for deploying SD-WAN VPX-SE in HyperV 2012 R2 and 2016

- VLAN Tagged Trunk Deployment is not supported.

Installing SD-WAN Appliances on the Microsoft Hyper-V Platform

July 19, 2021

To install NetScaler SD-WAN virtual appliances on Microsoft Windows Server, you must first install Windows Server, with the Hyper-V role enabled, on a machine with adequate system resources. While installing the Hyper-V role, be sure to specify the network interface cards (NICs) on the server that Hyper-V uses to create the virtual networks. You can reserve some NICs for the host. Use the **Hyper-V Manager** to perform the SD-WAN VPX installation.

SD-WAN VPX for Hyper-V is delivered in virtual hard disk (VHD) format. It includes the default configuration for elements such as CPU, network interfaces, and hard-disk size and format. After you install an SD-WAN VPX instance, you can configure its network adapters, add virtual NICs, assign the SD-WAN IP address, subnet mask, and gateway, and complete the basic configuration of the virtual appliance.

Microsoft Server Hardware Requirements

- The server's processor must support Intel Virtualization Technology.
- The server must run 64-bit Windows 2008 R2 SP1 (Standard, Enterprise, or data center Editions), or 2012 (Standard or data center Editions) with a full installation (not a Core installation), and the Hyper-V component enabled.
- Minimum system configuration is 4 GB RAM, 200 GB hard drive, and 2 physical CPU.
- Two physical Ethernet NICs are required. Three are recommended.

Note

The procedure below uses three NICs.

For more information about Windows Server 2008 R2 system requirements, see http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx (the exact location is subject to change by Microsoft at any time).

For information about installing Microsoft Server 2008 R2, see Installing Windows Server 2008 R2 (the exact location is subject to change by Microsoft at any time).

Prerequisites for Installing SD-WAN virtual appliances on the Microsoft Hyper-V platform

Before you begin installing a virtual appliance, do the following:

- Enable the Hyper-V role on Windows Server 2008 R2 or 2012. For more information, see Hyper-V Installation (the exact location is subject to change by Microsoft at any time).
- Download the VPX setup files. If you do not have a My Citrix account, access the home page at http://www.mycitrix.com, click the **New Users link**, and follow the instructions to create a new My Citrix account.

To download the SD-WAN VPX setup files

1. In a web browser, go to http://www.citrix.com/ and click **My Citrix**.
2. Type your user name and password.
3. Click **Downloads**.
4. In **Search Downloads by Product**, select **NetScaler SD-WAN**.
5. Under **Virtual Appliances**, select and download the required SD-WAN VPX distribution.
6. Copy the compressed file to your server.

To configure virtual NICs on the SD-WAN VPX

1. Log on to the Windows **Server as an Administrator**, either at a keyboard or VGA console, or through a NIC that you plan to use for managing the virtual appliance (not at one of the ports

that you use for the accelerated bridge).

2. To start Hyper-V Manager, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager.**

3. In the navigation pane, under **Hyper-V Manager**, select the server on which you want to install SD-WAN VPX.

4. On the **Actions** menu, click **Virtual Network Manager**…

5. In the **Virtual Network Manager** window, in the navigation pane, under **Virtual Networks**, click **New virtual network**.

6. Choose **External** as type of virtual network, and then click **Add**.

7. Name the new virtual network as apA Network 1 and select the physical NIC to map it to.

8. Click **OK** to apply the changes.

9. The **Apply Networking Changes** popup displays a caution indicating that pending changes might disrupt network connectivity. Click **Yes**.

10. Repeat steps 5–9 for the second accelerated bridge port. Name it as apA Network 2 and connect it to a different physical port.

11. Click **Apply** to apply the networking changes.

Installing SD-WAN VPX on Microsoft Server with Hyper-V Manager

After you have enabled the Hyper-V role on Microsoft Server and extracted the VPX files, you can use Hyper-V Manager to install SD-WAN VPX. After you import the virtual machine, you must configure the virtual NICs by associating them with the virtual networks created by Hyper-V. Based on the Microsoft server you are using, see the procedures in the following links to complete the installation.

- Microsoft Server 2008 R2

- Microsoft Server 2012

- Microsoft Server 2012 and 2016

  NOTE

  – From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.

  – A system maintenance account - CBVWSSH, exists for development and debugging and has no external login permissions. The account can only be accessed through a regular administrative user's CLI session.

Create a Virtual Machine on the Microsoft Hyper-V Platform using Virtual Hard Disk file

You need to download the SD-WAN Hyper-V setup files:

1. In a web browser, go to http://www.citrix.com/ and click **My Citrix**.
2. Type your user name and password.
3. Click **Downloads**.
4. In **Search Downloads by Product**, select **Citrix SD-WAN**.
5. Under **Virtual Appliances**, select and download the required SD-WAN Hyper-V distribution.
6. Copy the compressed file to your server and extract it.

To create a new virtual machine by using Hyper-V Manager:

1. Open the SD-WAN Hyper-V setup file and select **Virtual Hard Disks** folder.

2. Copy the hard disk image and paste it in a freshly created folder outside of the Hyper-V setup file.

3. Open the **Hyper-V Manager > select the Hyper-V ID >** right click and select **New > Virtual Machine**.

4. The **Virtual Machine Wizard** opens, Click **Next**.

5. Provide the name and you can also specify a location for the virtual machine. Select the check box to provide a different location to store the virtual machine. Click **Next**.

6. Select the generation for the virtual machine and click **Next**.

7. Specify the amount of memory to allocate to the virtual machine and click **Next**.

8. Select a connection from the drop-down list and click **Next**. The connection being selected here is for Management port.

9. To connect VHD, select the **Use an existing virtual hard disk** radio button, browse, and select the VHD file from the extracted zip file and click **Next**. The virtual hard disk can be found in below location:

** > ctx-sdw-se-vpx > Virtual Hard Disks**

10. Verify the details on the **Summary** page and click **Finish** to complete the creation of the virtual machine.

By default, the virtual machine is in **Off** sate. The virtual machine created so far has only 1 Interface and 1 core, we have to increase number of cores and add 2 more Interfaces for SD-WAN to work. Perform the following procedure:

1. Verify that the virtual appliance that you created is listed under **Virtual Machines**.

2. Right-click the virtual machine, and then click **Settings**.

3. In the **Settings** window's navigation pane, under Hardware, select the first network adapter in the list.

4. In the **Network** drop-down menu, select apA1 Network. This is the LAN interface for apA1.

5. Make sure that the Enable MAC address spoofing box is selected. If it is not, select it and apply the changes.

6. In the **Settings** window's navigation pane, under Hardware, select the second network adapter in the list. Repeat the step 10 and step 11, and assign the adapter to apA2 Network. This is the WAN interface for apA2. Important: Do not configure the same Network for both the network adapters. Incorrect configuration creates packet loops, which can bring down the network.

7. Increase Number of Virtual CPU cores.

   - In the **Settings** window navigation pane, select **Processor**.

- Increase **Number of virtual processors** to at least 4.
- Click **Apply**.

8. Optionally, change the virtual hard disk size:

   - In the **Settings** window navigation pane, under IDE Controller 0, select **Hard Drive**.
   - Click **Edit**.
   - Follow the steps in the Edit Virtual Hard Disk Wizard to increase the allocation to one of the supported sizes, using the Expand option in the wizard.

9. Optionally, change the memory size.

   - In the **Settings** window's navigation pane, under **Hardware**, select **Memory**.
   - Allocate the RAM space by adjusting the memory to one of the supported sizes.
   - Click **OK**.

10. Right click and select **start**. Once the state is changed to **Running**, your virtual machine is now ready to use.

Installing SD-WAN VPX on Microsoft Server 2008 R2

June 19, 2020

Performing the installation procedures

After you have enabled the Hyper-V role on Microsoft Server 2008 R2 and extracted the VPX files, you can use Hyper-V Manager to install SD-WAN VPX. After you import the virtual machine, you must configure the virtual NICs by associating them with the virtual networks created by Hyper-V.

> **Note**: You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

To install SD-WAN VPX on Microsoft Server 2008 R2 by using Hyper-V Manager

1. Unzip the SD-WAN distribution that you downloaded from My Citrix.

2. Start **Hyper-V Manager**.

3. In the navigation pane, under **Hyper-V Manager**, select the server on which you want to install SD-WAN VPX.

4. On the **Actions** menu, click **Virtual Switch Manager**.

5. In the **Import Virtual Machine** dialog box, in **Location**, specify the path to the folder that contains the Branch VPX SD-WAN files.

   > **Note**: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.

6. Click **Import**.

7. Verify that the virtual appliance that you imported is listed under **Virtual Machines**.

8. Right-click the imported virtual machine, and then click **Settings**.

9. In the **Settings** window's navigation pane, under **Hardware**, select the first network adapter in the list.

10. In the **Network** drop-down menu, select apA Network 1. This is the LAN interface for apA1.

11. Make sure the **Enable spoofing of the MAC addresses** box is selected. If it is not, select it and apply the changes.

12. In the **Settings** window's navigation pane, under **Hardware**, select the second network adapter in the list. Repeat the step 10 and step 11, and assign the adapter to apA Network 2. This is the WAN interface for apA2.
    Important: Do not configure the same Network for both the network adapters. Incorrect configuration creates packet loops, which can bring down the network.

13. Optionally, change the virtual hard disk size:

    - In the **Settings** window navigation pane, under IDE Controller 0, select **Hard Drive**.
    - Click **Edit**.

- Follow the steps in the Edit Virtual Hard Disk Wizard to increase the allocation to one of the supported sizes, using the Expand option in the wizard.

14. Optionally, change the memory size.

- In the **Settings** window's navigation pane, under **Hardware**, select **Memory**.
- Allocate the RAM space by adjusting the memory to one of the supported sizes.
- Click **OK**.

15. Optionally, define the management port.

- Right-click the virtual machine, and then click **Settings**.
- In the **Settings** window navigation pane, under **Hardware**, select **Add Hardware**.
- Select **Network Adapter** from the list of devices, and then click **Add**.
- Name the new virtual network as Primary Network 3.
- Make sure the **Enable spoofing of MAC addresses** check box is selected.
- Click **OK** to apply the changes.

16. Right-click the **Branch Repeater VPX virtual machine** and select **Connect**.

17. In the file menu, click **Action**, and then click **Start** to start the virtual machine.

18. When an SD-WAN VPX virtual machine is started for the first time, it automatically starts the Deployment Wizard. This wizard asks questions about the deployment mode: Inline, WCCP, or PBR (virtual inline), or Setup Using Web UI. Select **Setup Using Web UI**. On the next screen, enter the **IP**, netmask, and gateway for the apA interface, and click **Finish**.

19. After SD-WAN VPX has restarted, log on to the browser based UI ((user name: admin, password: password) at the IP address that you assigned to apA, for example: `https://172.16.0.213`

More configuration

For more configuration instructions, see the documentation for physical SD-WAN and SD-WAN appliances.

Upgrading to a previous release

The software upgrade mechanism built into physical SD-WAN appliances is also supported by SD-WAN VPX. Alternatively, you can install a new virtual machine running the desired release.

Installing SD-WAN VPX on the Microsoft Server 2012

May 23, 2019

Performing the installation procedures

After you have enabled the Hyper-V role on Microsoft Server and extracted the VPX files, you can use Hyper-V Manager to install SD-WAN VPX. After you import the virtual machine, you must configure the virtual NICs by associating them with the virtual networks created by Hyper-V.

> **Note**: You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

To install SD-WAN VPX on Microsoft Server 2012 by using Hyper-V Manager

1. Unzip the SD-WAN distribution that you downloaded from My Citrix.

2. Start Hyper-V Manager.

3. In the navigation pane, under **Hyper-V Manager**, select the server on which you want to install SD-WAN VPX.

4. On the **Actions** menu, click **Import Virtual Machine.

5. In the **Import Virtual Machine** dialog box, in **Location** box, specify the path to the folder that contains the SD-WAN VPX files.

   > **Note**: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.

6. Click **Import**.

7. Verify that the virtual appliance that you imported is listed under **Virtual Machines**.

8. Right-click the imported virtual machine, and then click **Settings**.

9. In the **Settings** window's navigation pane, under **Hardware**, select the first network adapter in the list.

10. In the **Network** drop-down menu, select apA1 Network. This is the LAN interface for apA1.

11. Make sure the **Enable MAC address spoofing** box is selected. If it is not, select it and apply the changes.

12. In the **Settings** window's navigation pane, under **Hardware**, select the second network adapter in the list. Repeat the step 10 and step 11, and assign the adapter to apA2 Network. This is the WAN interface for apA2.
    Important: Do not configure the same Network for both the network adapters. Incorrect configuration creates packet loops, which can bring down the network.

13. Optionally, change the virtual hard disk size:

    - In the **Settings** window navigation pane, under IDE Controller 0, select **Hard Drive**.
    - Click **Edit**.

- Follow the steps in the Edit Virtual Hard Disk Wizard to increase the allocation to one of the supported sizes, using the Expand option in the wizard.

14. Optionally, change the memory size.

   - In the **Settings** window's navigation pane, under **Hardware**, select **Memory**.
   - Allocate the RAM space by adjusting the memory to one of the supported sizes.
   - Click **OK**.

15. Optionally, define the management port.

   - Right-click the virtual machine, and then click **Settings**.
   - In the **Settings** window navigation pane, under **Hardware**, select **Add Hardware**.
   - Select **Network Adapter** from the list of devices, and then click **Add**.
   - Name the new virtual network as Primary Network 3.
     - Make sure the **Enable spoofing of MAC addresses** check box is selected.
     - Click **OK** to apply the changes.

16. Right-click the **SD-WAN VPX virtual machine** and select **Connect**.

17. In the file menu, click **Action**, and then click **Start** to start the virtual machine.

18. When an SD-WAN VPX virtual machine is started for the first time, it automatically starts the Deployment Wizard. This wizard asks questions about the deployment mode. Select **Setup Using Web UI**. On the next screen, enter the **IP address**, netmask, and gateway for the apA interface, and click **Finish**.

19. After SD-WAN VPX has restarted, log on to the browser based UI ((user name: admin, password: password) at the IP address that you assigned to apA, for example: `https://172.16.0.213`

Extra configuration

For more configuration instructions, see the documentation for physical SD-WAN/SD-WAN appliances.

Downgrading to a previous release

The software upgrade mechanism built into physical SD-WAN/SD-WAN appliances is supported by SD-WAN/SD-WAN VPX. Alternatively, you can install a new virtual machine running the desired release.

Installing SD-WAN SE Virtual Appliances (VPX) in Linux-KVM Platform

June 19, 2020

1. To set up SDWAN VPX-SE for the Linux-KVM platform:
   - Use the graphical Virtual Machine Manager (Virtual Manager) application. Or,
   - Use the virsh program Linux-KVM command line.
2. The host Linux operating system must be installed on suitable hardware by using virtualization tools such as KVM Module and QEMU. The number of virtual machines (VMs) that can be deployed on the hypervisor depends on the application requirement and the chosen hardware.
3. The.qcow2 file has to be unique for each of the NetScaler VPX instance provisioned. It is a virtual hard disk (VHD) that is attached to VM.

Prerequisites:

- Install Ubuntu 16.04 on the bare metal appliance which supports Virtualization. The following are the steps to check if the bare metal appliance supports Virtualization.
- 64-bit x86 processors with the hardware virtualization feature included in the AMD-V and Intel VT-X processors.
  - To test whether your CPU of Linux host supports virtualization, enter the following command at the host Linux shell prompt: `egrep -c '(vmx|svm)'/proc/cpuinfo`, this output must be more than 0.
  - Alternative to step 2, install a package/tool called "cpu-checker" (sudo apt-get install cpu-checker), enter the following command: `kvm-ok`, the output must be "KVM acceleration can be used."
- On the hosting hypervisor, run `cat /proc/cpuinfo | grep flags` command and verify whether the following CPU flags are present: `popcnt`, `sse`, `sse2`, `pni`, `ssse3`, `sse4_1`, `and sse4_2`.
- Minimum hardware requirements: As the SDWAN-Virtual WAN (guest OS) requires 4 vCPUs, 4 GB RAM and 40 GB (VHD). You must have a host with these specifications which can satisfy this.
- Software requirements: Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-78-generic x86_64)

Install qemu-kvm, libvirt-bin, virt-manager: sudo apt-get install qemu-kvm libvirt-bin virt-manager bridge-utils. Execute this command to obtain all the required packages/software.

Provisioning the SD-WAN VPX appliances by using Virtual Machine Manager (VMM):

1. Open the **Virtual Machine Manager**. Go to **Application** > **System Tools** > **Virtual Machine Manager**, and provide the logon credentials in the **Authenticate** window.
2. Once the VMM opens, you must see QEMU/KVM which indicates that the VMM is not connected to the QEMU Virtualization. NIC ordering for SD-WAN VPX-SE provisioning must be in the following order; Management, LAN, and **WAN**.
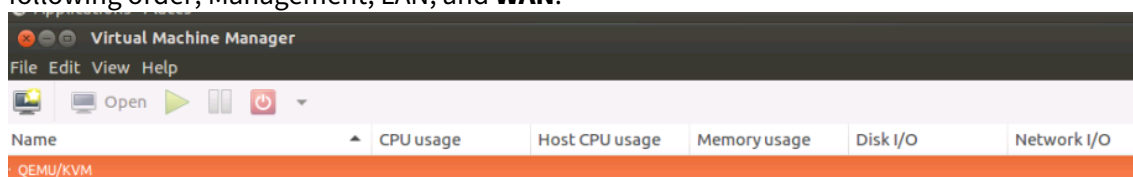
3. Select **New Virtual Machine**.

   Add new VMM

4. Select the **VHD**, the VHD used by one machine cannot be shared. Unique VHD is required for every Virtual Machine. Browse the image and select the path where it is downloaded.
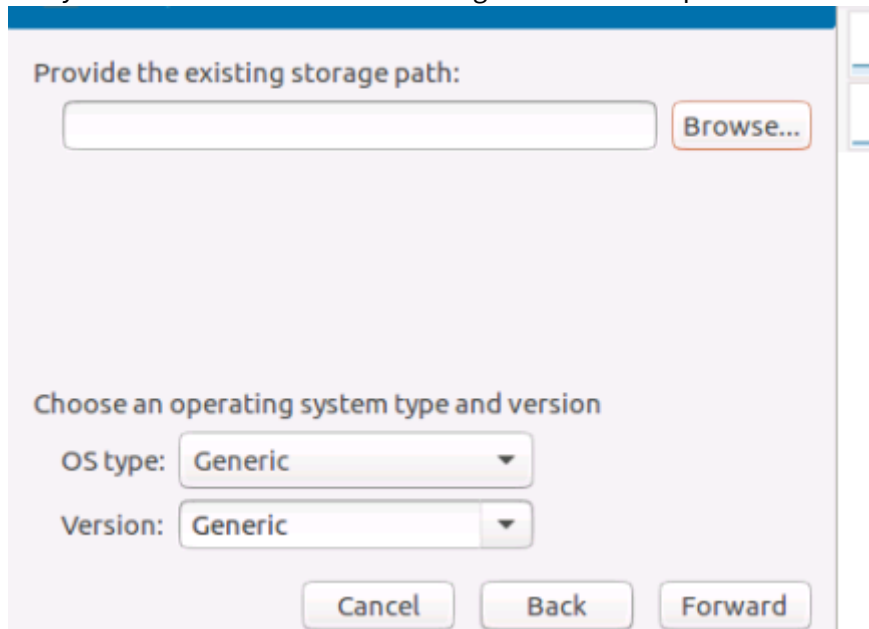
5. Provide RAM as 4,096 MB and CPU as 4.
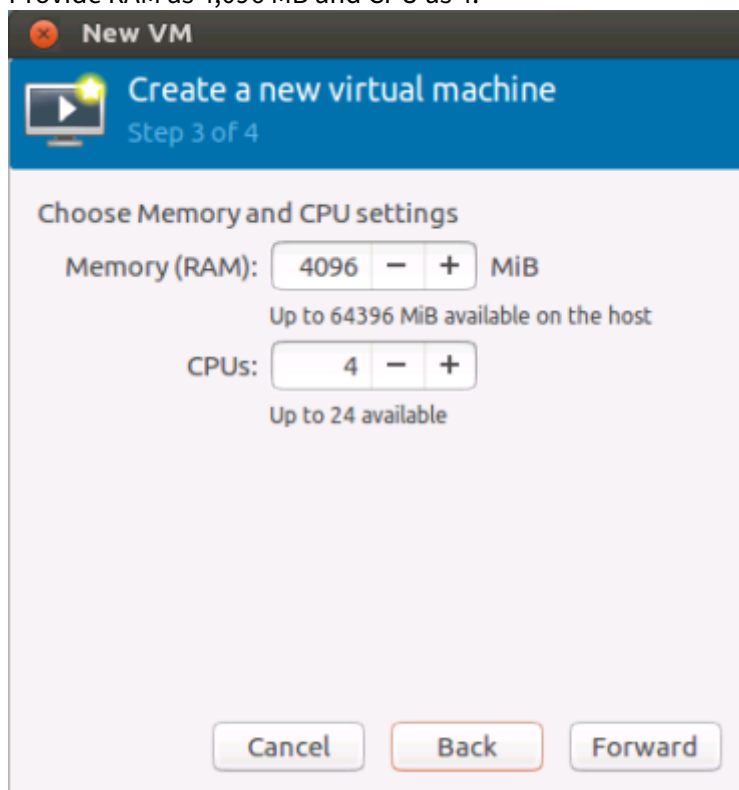
6. Name the VM as needed and select **Customize configuration before Install**. As by default one

NIC gets selected to the Virtual Machine, you can see the **Network selection** option. In this setup **enp4s0f0** is the Management Network for the Host machine, and if you want to use this NIC, sharing same NIC between guests and host for Management access. Source Mode is Bridge since it is shared between VMs.
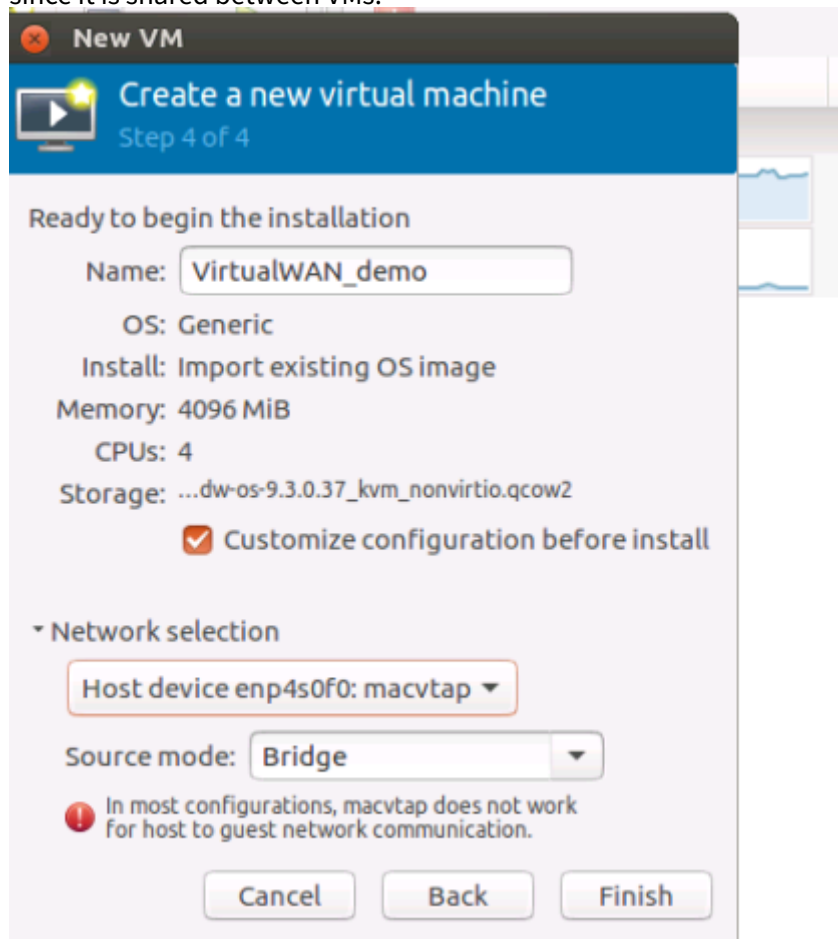
7. After clicking **Finish**, ensure you select **customize configuration before install** for further configuration. For the NIC that is assigned, in this example "enp4s0f0: MacVTap" select the **Device model as** "virtio." The model that is supported for communication.
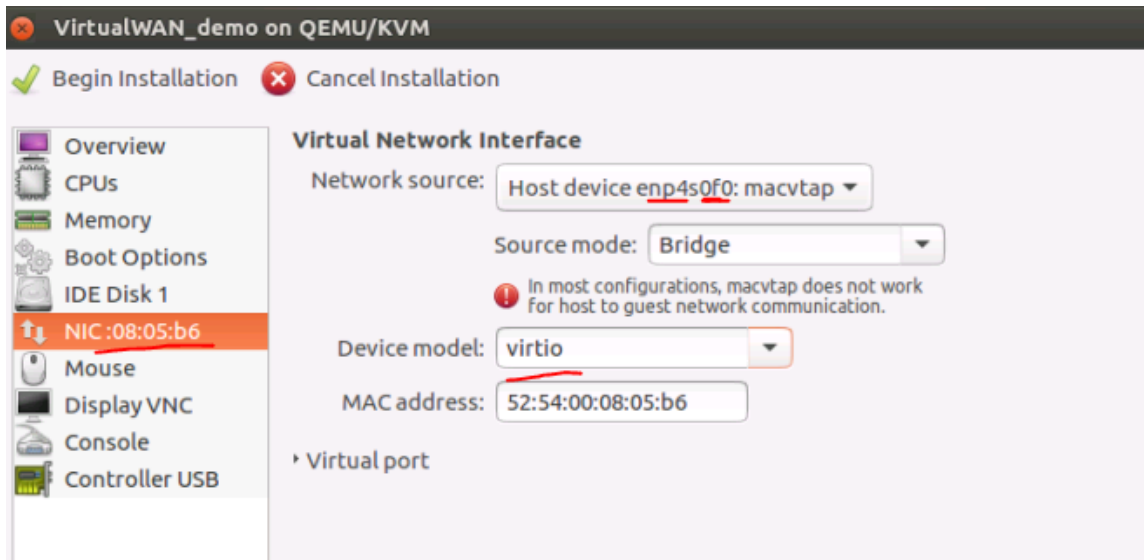
8. Add more NICs for LAN and WAN with **Add Hardware** at the bottom left side corner. For good Performance, it is recommended to use Source Mode as Pass-through (Only one VM can use the Lower NIC and hence it cannot be shared across VMs). For LAN and WAN interfaces use "Pass-through" Mode and Device Model must be "virtio."
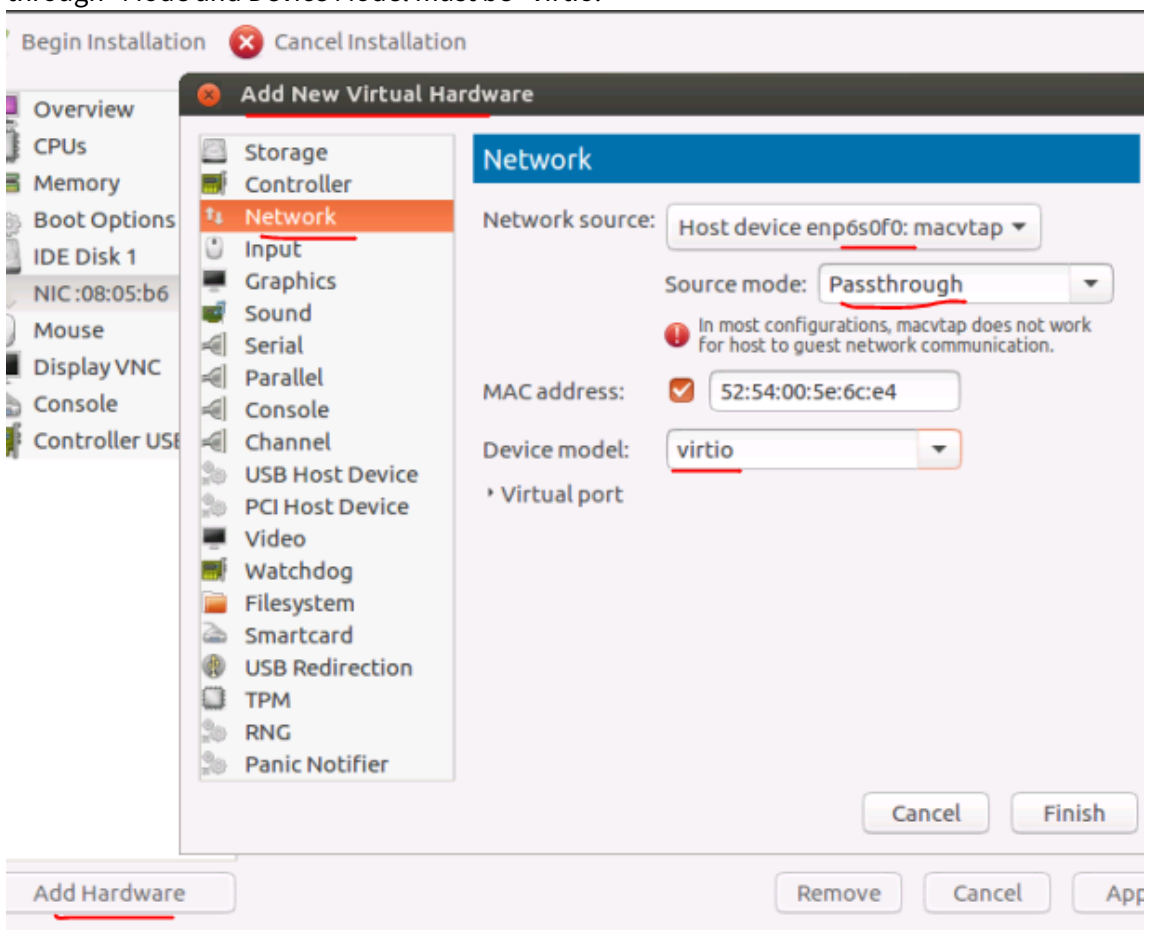
9. Select **Begin Installation** for the installation process to start and you can see the console of the

appliance.

10. Use **management_ip command** to set the IP address.

How to deploy SD-WAN appliances in Linux-KVM hypervisor platform instance on the same host

Deploying SD-WAN appliances in high availability mode on the same host requires sharing physical interface across SD-WAN VPX appliances. For example. The eth3 of physical hypervisor (host) is used for WANLink-1 for Primary VM, the same interface must be used for secondary appliance, so that if primary appliance becomes inactive, the secondary appliance can respond to the ARP requests for shared MAC.
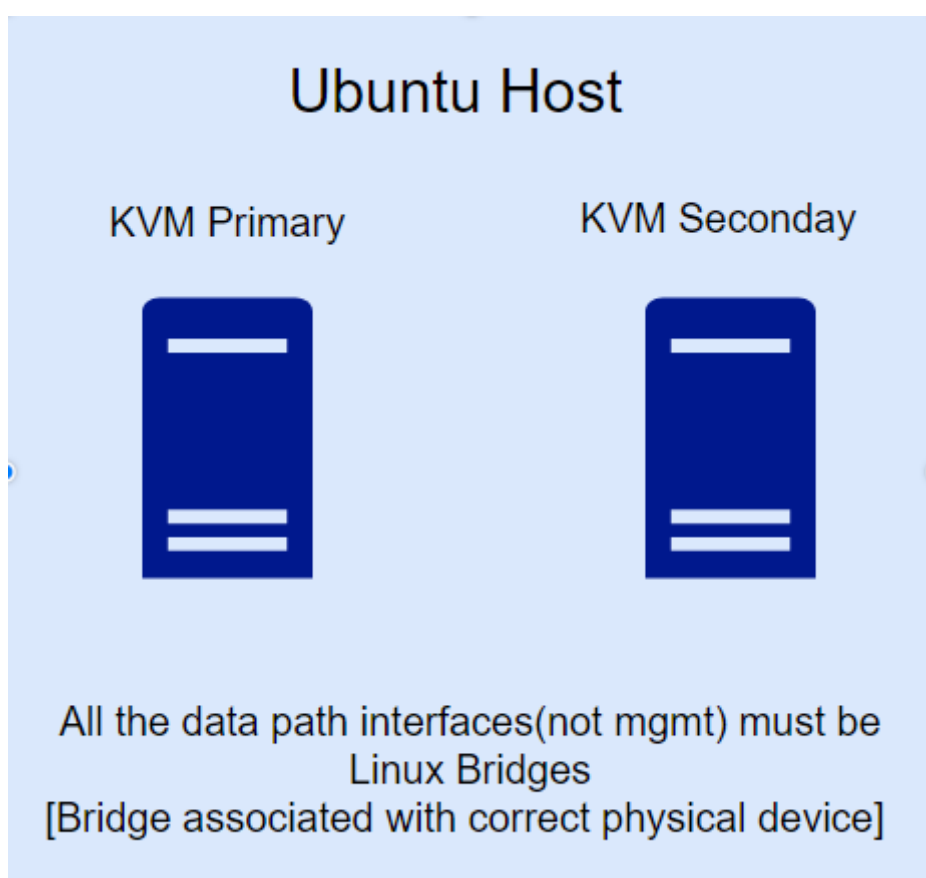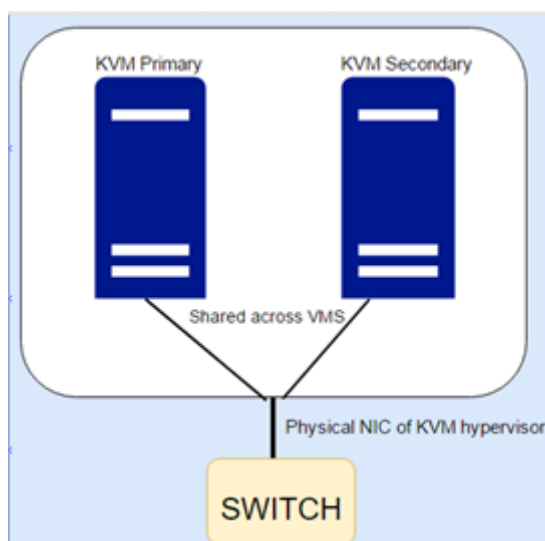
For sharing the Physical NIC between the VMs which are on the same host, the source modes that can be used according to KVM networking is **MACVTAP Bridge** or **Linux Bridge**.

How to use linux bridge

- Create Bridge using *"brctl"* on the Host (KVM Hypervisor level).
- Associate the required Physical NIC to the bridge created (using brctl commands).
- These bridges created at the Hypervisor level must be now associated to the SD-WAN VM.
- Primary and Secondary VMs are now associated with the Linux bridges created.

To create linux bridge and associate it with virtual machine:

- Adding bridge, `brctl addbr ha-brwan1`
- Associating physical NIC to the bridge `ha-brwan1`: `brctl addif ha-brwan1 eth3`
- Associating the bridge "ha-brwan1" to the SD-WAN-SE (Virtual WAN) (both Physical and Secondary)

1. When adding network interface, select **Network source as** "Specify shared device name."
2. Under **Bridge Name**, provide the name of the bridge created.
3. Device Model must always be "virtio."

Create bridges for LAN and WAN interfaces. The following snapshot depicts the way to associate interface to SDWAN-SE using Virtual Machine Manager.

> **Note**
>
> These steps must be followed only when both Primary and Secondary high availability node is present on the same KVM Hypervisor/Host. In case, if high availability nodes are present on different Hypervisors then **MACVTAP: Passthrough source** mode can be used.
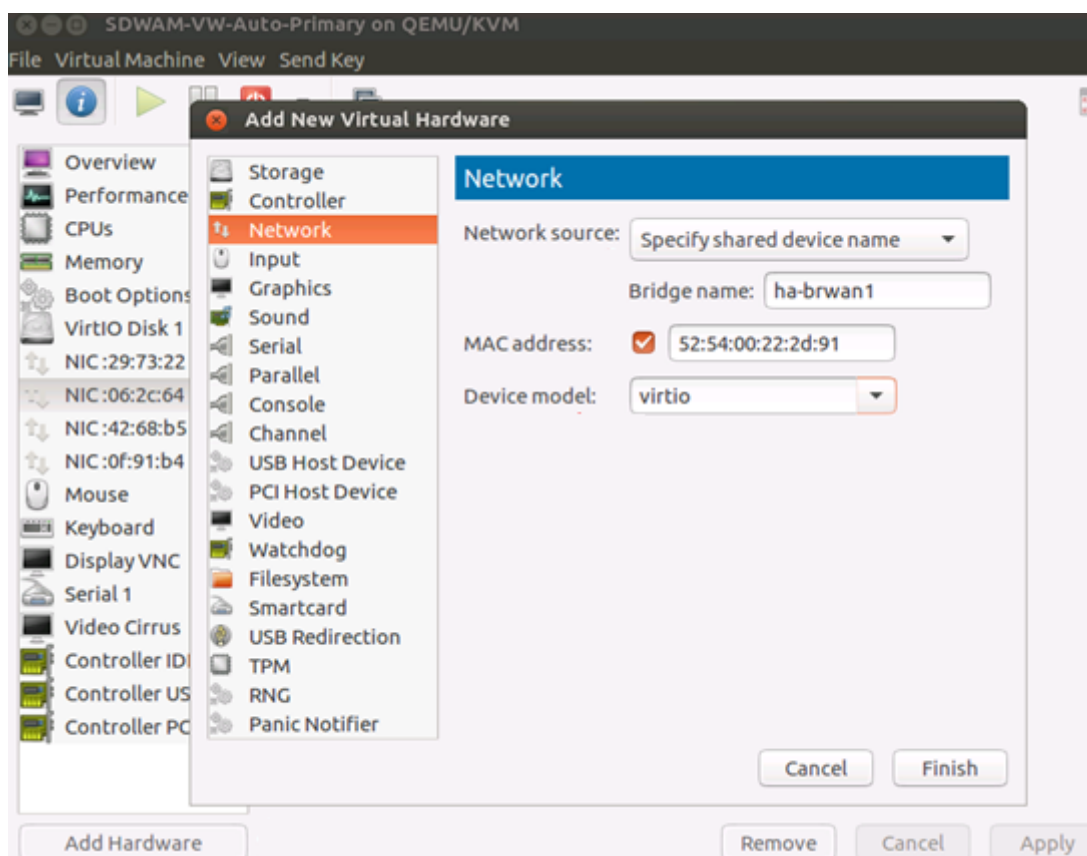
Limitation with MacVTap bridge mode type

With interface associated to Virtual Machines as MacVTap Bridge mode type there are issues with shared MAC communication. SD-WAN Virtual WAN uses shared MAC (AA: AA: AA: 00:00: XX). When MacVTap Bridge mode is used, ARP resolution does not occur for shared Mac. So MacVTap Bridge is not a recommended option.

> **NOTE**
>
> - From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.
>
> - A system maintenance account - CBVWSSH, exists for development and debugging and has no external login permissions. The account can only be accessed through a regular admin-istrative user's CLI session.

Install Citrix SD-WAN SE VPX on Google Cloud Platform

February 15, 2021

Deploying Citrix SD-WAN SE VPX on GCP enables organizations to establish a direct and highly secure connection between branches and applications hosted on GCP. It eliminates the need to backhaul cloud bound traffic through the Data Center. The key benefits of using Citrix SD-WAN on GCP are:

- Create direct connections from every branch site to GCP.

- Ensure an always-on connection to GCP.

- Extend your secure perimeter to the cloud.

- Evolve to a simple and easy to manage the branch network.

Citrix SD-WAN Standard Edition for GCP logically bonds multiple network links into a single secure logical virtual path. The solution enables organizations to use variety of connections from different service providers to get highly resilient virtual WAN paths. These virtual paths function as an overlay to seamlessly aggregate bandwidth capacities across multiple links and deliver consistent user experience even if some of the member links go down or suffer degradation. This is enabled by the per-packet load balancing and monitoring capabilities of Citrix SD-WAN.

Summary of deployment steps

1. Choose a region where you want to deploy the instance and create three VPCs in different subnets. Optionally, you can create another VPC for HA if needed.

NIC	Associated network
NIC 0 (default)	Management subnet
NIC 1	LAN subnet
NIC 2	WAN subnet
NIC 3	HA subnet (optional)

> **Note**
>
> If you are creating a new management subnet, allow port 443 in its firewall rules.

2. Create a Citrix SD-WAN SE instance and associate the interfaces with the VPCs.

3. Create firewall rules on WAN subnet VPC to enable ingress on UDP port 4980. It is used by Citrix SD-WAN instance to create the virtual path.

---

4. Create a route on LAN subnet VPC to intercept all the traffic generated from LAN.

5. Access the Citrix SD-WAN SE VPX using the management IP address.

Create VPC networks

Create VPC networks that will be associated with the management subnet, LAN subnet, and WAN subnet. While creating an image a default interface is available, this can be used as the management interface. Create two VPC network for LAN and WAN subnet.

1. To create a VPC network, in the GCP console navigate to **VPC network** > **VPC networks** > **Create VPC Network**.
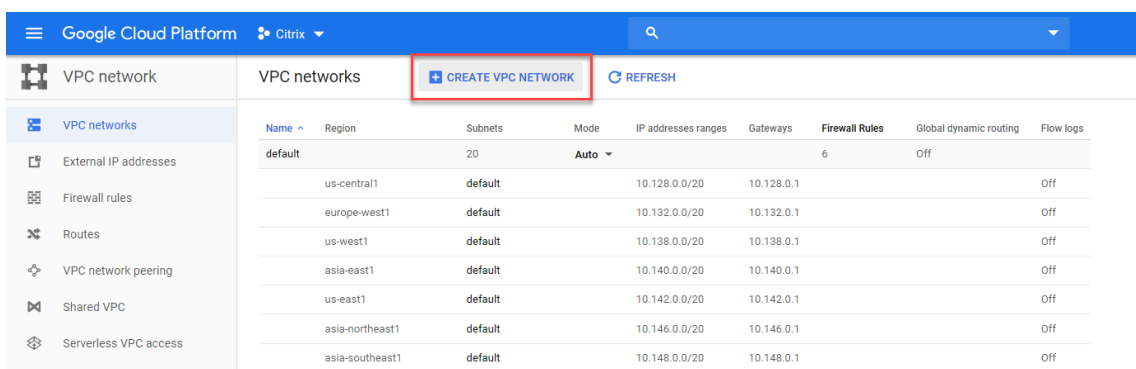
2. Specify the name, description, region subnet IP address and create a LAN VPC network.

3. Similarly create a WAN VPC network.

4. Optionally, for HA deployment create an HA VPC network.

> **Note**
>
> All four VPC networks must be in the same region.

5. Create WAN link public IP.

6. Associate the WAN Public IP to WAN subnet after creating the instance.

> **Note**
>
> For the HA secondary instance you do not have to associate the WAN Public IP.
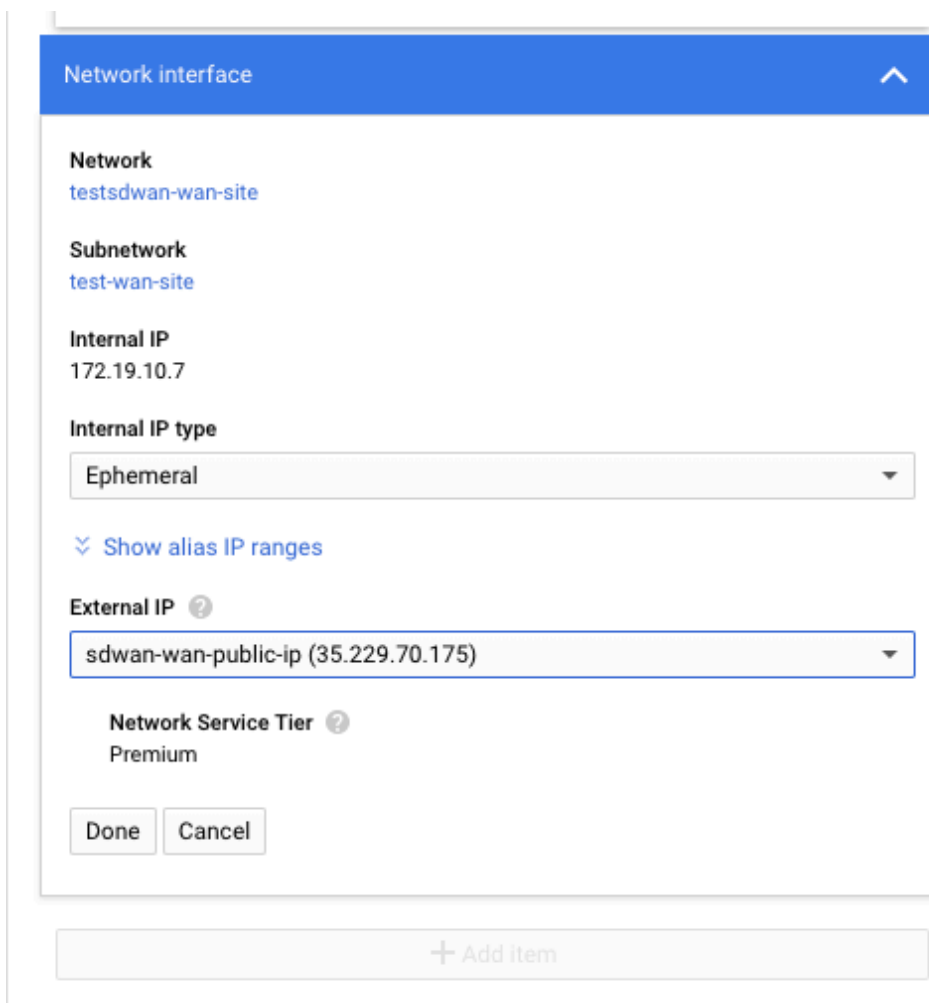
Create the Citrix SD-WAN SE VPX instance

1. In GCP Marketplace search for **Citrix SD-WAN Standard Edition**, open it, and click **LAUNCH ON COMPUTE ENGINE**.

2. The required vCPU's and memory are selected by default. Select the **GCP Region**.

> **Note**
>
> The GCP region must be same as the region of the VPC networks.

3. From **Existing network1** list select default, this is the management interface. Similarly, for **Existing network2** and **Existing network3** select the LAN and WAN subnets respectively. Ensure that **useExNet** is selected for all the three networks and click **Deploy**.

> **Note**
>
> If you are creating a new management subnet, allow port 443 in its firewall rules.

4. Optionally, create another instance for HA as described in the previous steps. Ensure that the LAN and WAN network and subnets are the same for both the HA instances.

5. After the SD-WAN SE VPX instance is deployed, use the default user name and password provided by GCP to log in into the SD-WAN SE VPX.
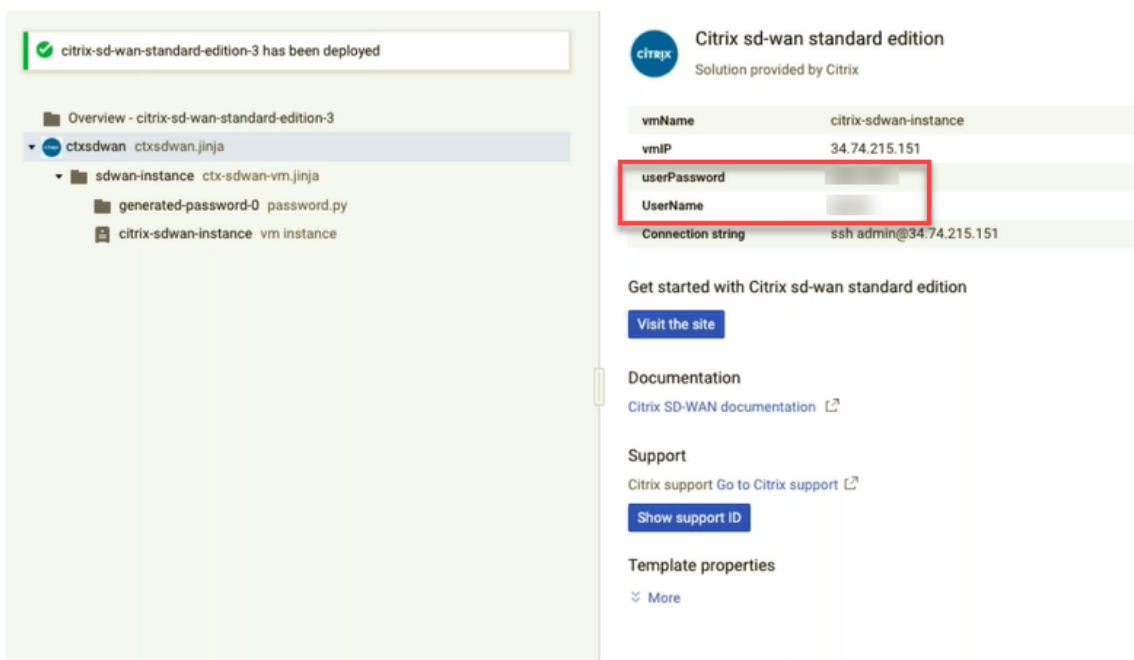
Create firewall rule on WAN subnet VPC

1. Navigate to **VPC Network > VPC Networks > WAN subnet VPC**. In the Firewall rules tab, click **Add firewall rule**.
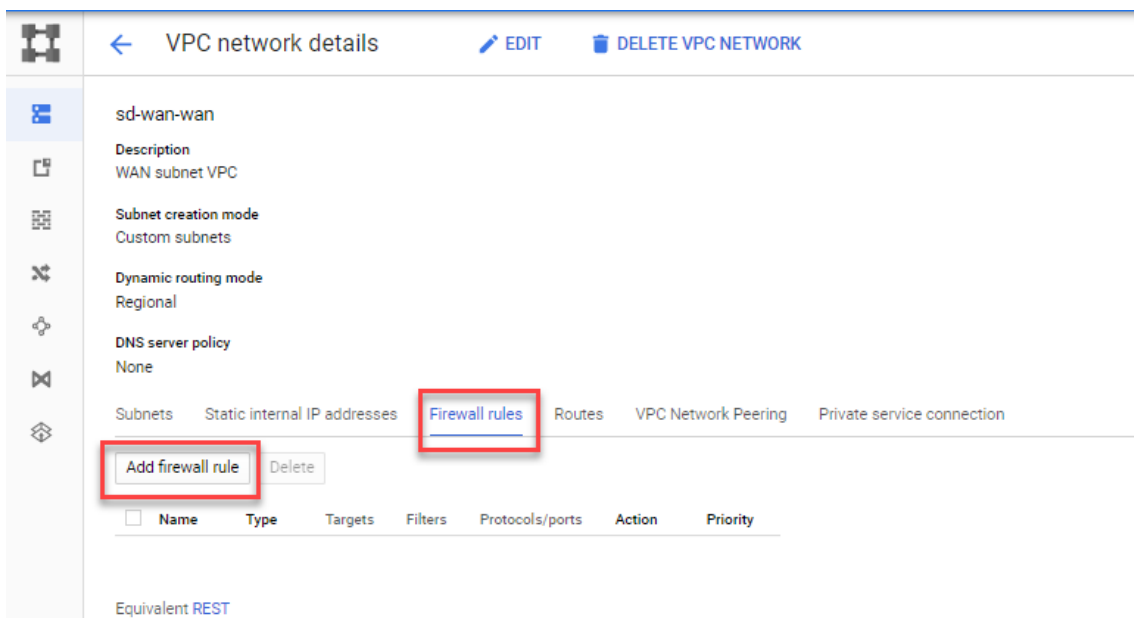
2. Allow ingress for all instances on UDP port 4980. This port is used by the SD-WAN instance to create an overlay network.

Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Name ⃝

server-firewall1

Description (Optional)

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more
- On
- ⦿ Off

Network ⃝

sd-wan-wan ▾

Priority ⃝
Priority can be 0–65535 Check priority of other firewall rules

1000

Direction of traffic ⃝
- ⦿ Ingress
- Egress

Action on match ⃝
- ⦿ Allow
- Deny

Targets ⃝

All instances in the network ▾

Source filter ⃝

IP ranges ▾

Source IP ranges ⃝

0.0.0.0/0 ⊗

Second source filter ⃝

None ▾

Protocols and ports ⃝
- Allow all
- ⦿ Specified protocols and ports
  - ☐ tcp : `20, 50−60`
  - ☑ udp : `4980`
  - ☐ Other protocols
    - `protocols, comma separated, e.g. ah, sctp`

⌄ Disable rule

[Create] [Cancel]
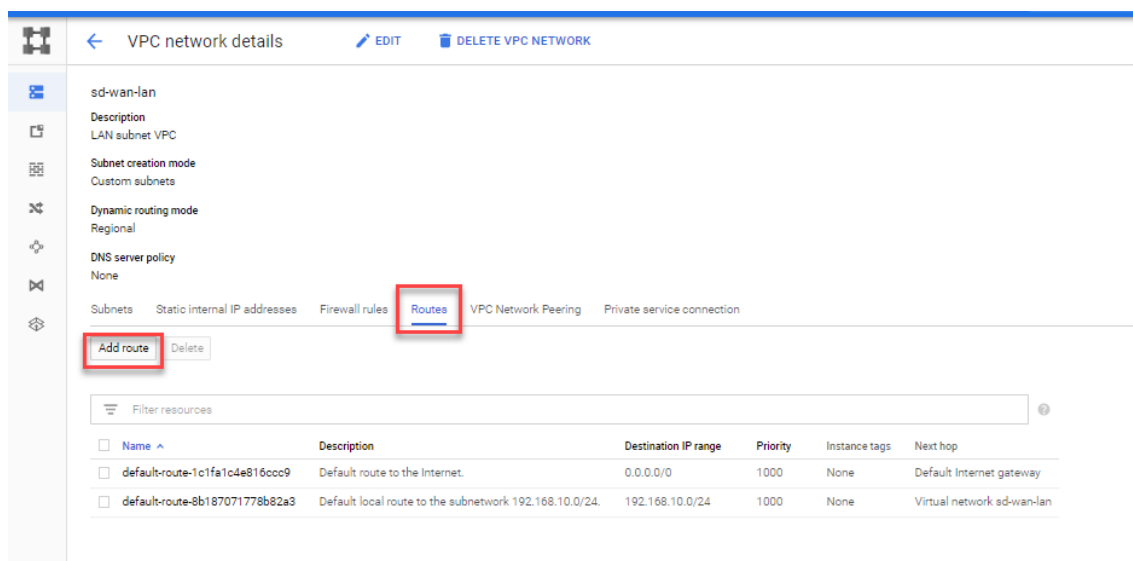
Equivalent REST or command line

3. Optionally, for HA deployment ensure that the same firewall rule is created on HA subnet VPC as well and the UDP port number 4980 is allowed.

Create a route on LAN subnet VPC

Create a route on LAN subnet VPC to intercept all the traffic generated from LAN.

1. Navigate to **VPC Network > VPC Networks > LAN subnet VPC**. In the Routes tab, click **Add route**.

2. Enter the Destination IP range, the LAN network of the other end. In the Next Hop field, select Specify IP address and in the Next hop IP address specify the SD-WAN LAN interface IP.

3. Optionally, for HA deployment, on the primary instance configure the Alias IP. This is used as the LAN interface IP in SD-WAN configuration.

Access the SD-WAN SE VPX instance

Use the management interface IP address to access the GUI of the SD-WAN SE VPX instance. Use the default user name and password provided by GCP to log into the SD-WAN SE VPX.
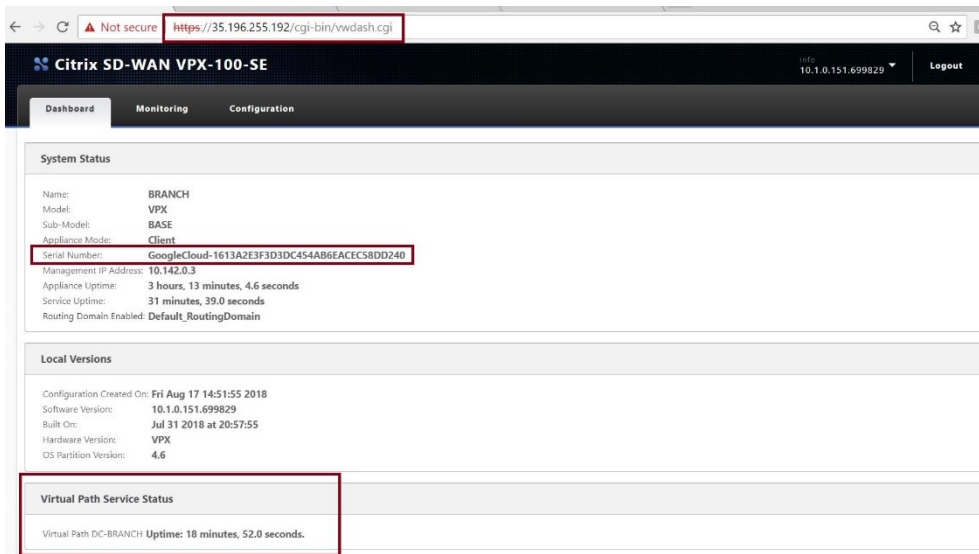
NOTE

- From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.

- A system maintenance account - CBVWSSH, exists for development and debugging and has no external login permissions. The account can only be accessed through a regular administrative user's CLI session.

For HA to work, ensure that in the SD-WAN configuration the WAN interface is configured with DHCP. Use the alias IP to configure the LAN interface.

259
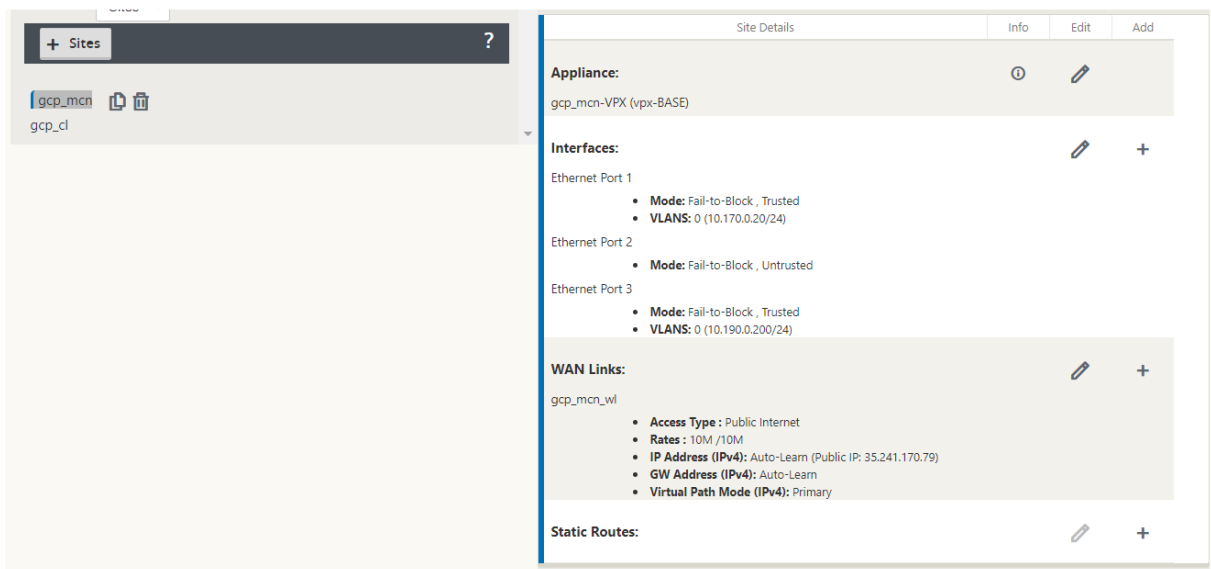
Installing SD-WAN VPX Standard Edition AMI on AWS

December 4, 2020

The Citrix SD-WAN SE appliances bond multiple network paths in the single virtual path. The virtual paths are monitored so that critical application paths are always routed through optimal paths. This solution enables customers to deploy applications in the cloud and utilize multiple service provider networks for seamless delivery of applications to the end-users.

To create an SD-WAN SE-VPX on Amazon Web Services(AWS), you go through the same process as with creating any other instance, setting a few instance parameters to non-default settings.

Instantiating an SD-WAN Virtual Appliance (AMI) on AWS:

To install an SD-WAN virtual appliance in an AWS VPC, you need an AWS account. You can create an AWS account at http://aws.amazon.com/. SD-WAN is available as an Amazon Machine Image (AMI) in AWS Marketplace.

Note: Amazon makes frequent changes to its AWS pages, so the following instructions may not be up-to-date.

To instantiate an SD-WAN virtual appliance (AMI) on AWS:

1. In a web browser, type http://aws.amazon.com/.
2. Click **My Account/Console**, and then click **My Account** to open the **Amazon Web Services Sign** in page.
3. Use your AWS account credentials to sign in. This takes you to the Amazon Web Services page.

Citrix SD-WAN SE appliances offer the following AWS service instances:

- VPC Dashboard - isolated portion of the AWS cloud populated by AWS objects, such as EC2 instances
    - Enabled by creating a VPC in AWS. See the following configuration steps.
- EC2 Dashboard - elastic compute cloud, resizable virtual services / instances
    - Enabled by creating NetScaler SD-WAN AMI. See below for configuration steps.
    - CIDR – Classless Inter-Domain Routing block, consisting of continuous IP address range, used to specify your VPC (cannot be larger than 16 regions).

SD-WAN web interface

- Configure Citrix (formerly NetScaler SD-WAN) SD-WAN AMI

The following are the requirements and limitations for deploying SD-WAN SE-VPX AMI in AWS:

Minimum requirements

- **AWS EC2 Instance Type**: c4.2xlarge, c4.4xlarge, c5.xlarge, c5.2xlarge, c5.4xlarge, m4.2xlarge, m4.4xlarge, M5.2xlarge, m5.4xlarge
- **Virtual CPU**: 8
- **RAM**: 15 GB
- **Storage**: 160 GB
- **Network Interfaces**: minimum of 2 (one management, one for LAN/WAN)
- **BYOL** – bring-your-own-license and subscription

From 11.3 release onwards, Citrix SD-WAN has introduced support for the M5 and C5 instances. The newer AWS regions such as Hong Kong and Paris only support M5 and C5 instances.

The M5 and C5 instances have improved hardware performance and are designed for higher demanding workloads. The M5 and C5 instances deliver better price/performance than the M4 instances on a per-core basis.

NOTE

The M5 and C5 instances are supported from a fresh provision of 11.3 and higher version only. To keep using the M5 and C5 instances, you cannot downgrade from 11.3 version since the M5 and C5 instances are not supported on any firmware version prior to 11.3 release.

Limitations

- AWS does not allow bridging of interface so Fail-to-Wire is not an option for configuring interface groups.
- Instances provisioned with 10.2.4/11.2.1 versions, AMIs cannot change their instance type to M5/C5.

Citrix (formerly NetScaler SD-WAN) SD-WAN with AWS
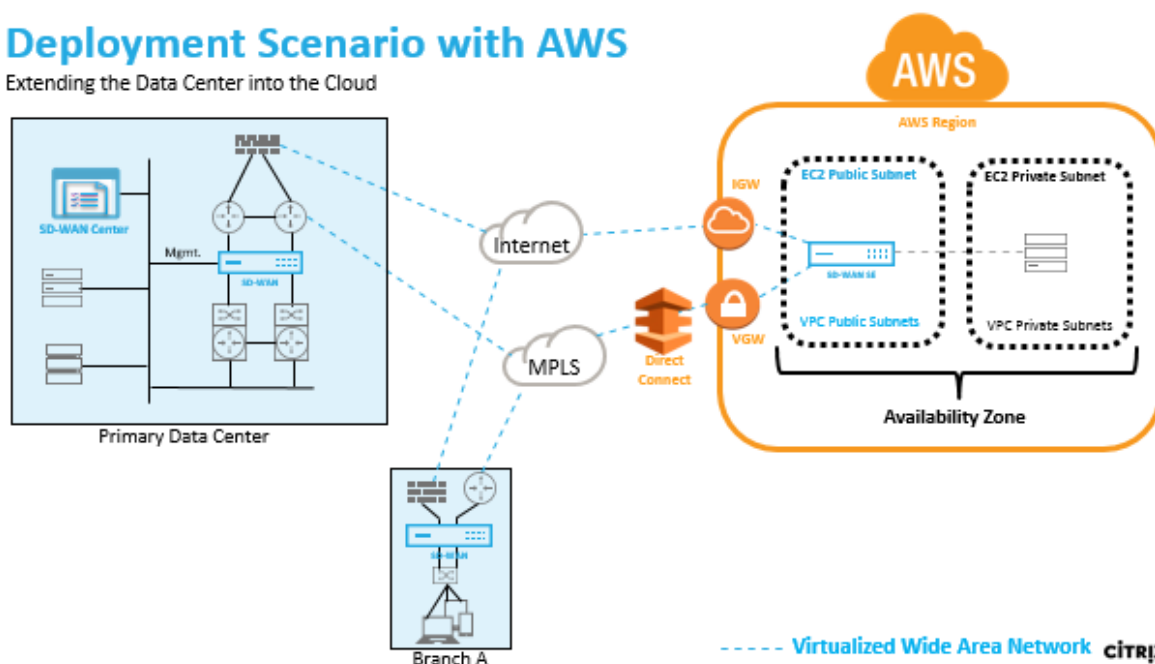
Deploying an AWS region with a specified Availability Zone. Within that Virtual Private Cloud (VPC) infrastructure, SD-WAN Standard Edition AMI (Amazon Machine Image) is deployed as the VPC Gateway.

- The VPC private has routes towards the VPC Gateway.
- SD-WAN instance has a route towards the AWS VGW (VPN Gateway) for direct connect and another route towards IGW (Internet Gateway) for internet connectivity.
- Connectivity between Data Center, Branch, and Cloud applying different transport modes utilizing multiple WAN paths simultaneously.
- Automatic Route Learning with OSPF and BGP.
- Single IPsec tunnel across multiple paths where security renegotiation is not required upon any link failure occurrences.
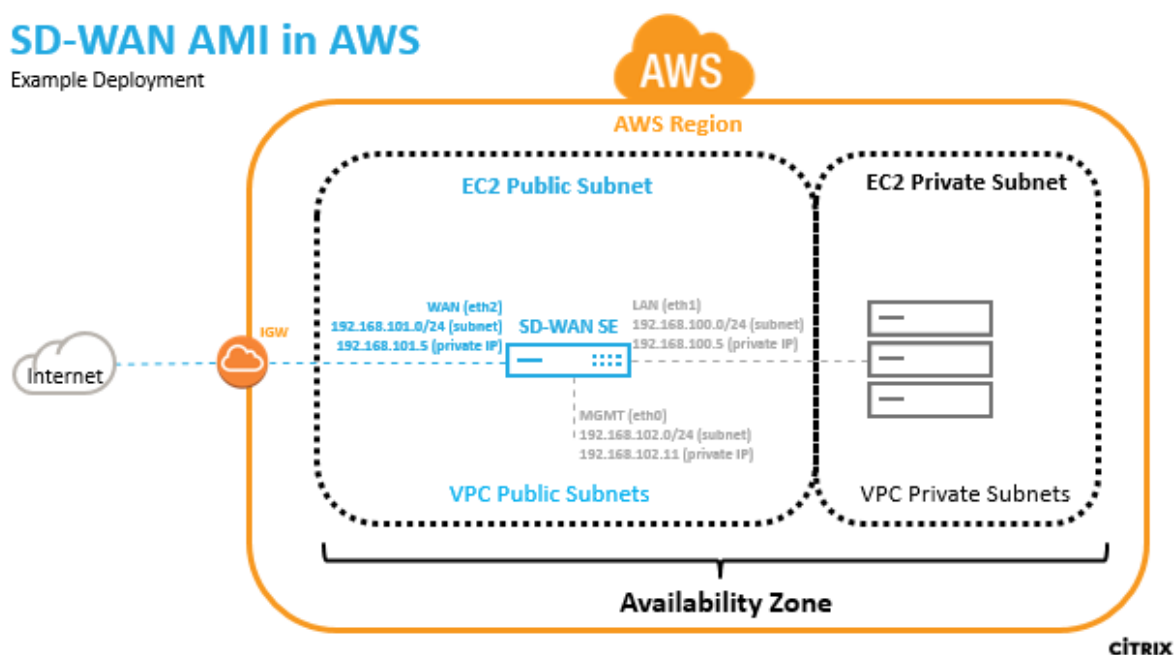
In AWS a subnet and IP address must be defined for each SD-WAN AMI interface. The number of interfaces utilized depends on the deployment use case. If the goal is to reliably access application resources that are on the LAN side of the VPX (inside the same Region), the VPX can be configured with three Ethernet interfaces; one for management on eth0, one for LAN on eth1, and one for WAN on eth2.

Alternatively, if the goal is to hair-pin traffic through the VPX to some other region or to the public internet, the VPX can be configured with two Ethernet interfaces; one for management on eth0, and a second for LAN/WAN on eth1.

SD-WAN SE AMI in AWS overview

1. **Create VPC in AWS using VPC Dashboard**

To get started with the Amazon virtual private cloud you need to create a VPC, which is a virtual network dedicated to your AWS account.

- Define CIDR blocks/Subnets and assign to VPC - for identifying the device in the network. For example. 192.168.100.0/22 is selected for the VPC in the example network diagram encompassing the WAN, LAN, and Management subnets – 192.168.100.0 – 192.168.103.255) - 192.168.100.0/22
- Define an Internet Gateway for the VPC – for communicating with outside the cloud environment
- Define routing for each defined subnet - for communication between the subnets and Internet
- Define Network ACLs (Access Control List) - for controlling the inflow/outflow of the traffic from/to the subnet for security purposes

- Define Security Group - for controlling the inflow/outflow of the traffic from/to each instance of the network device

Create an Citrix SD-WAN AMI:

- For more information,refer to the EBS best practices and Must-know best practices for Amazon EBS encryption

- For defining Security groups the policy must look like the following:

  - Outbound: Allow All traffic
  - Inbound:
  - SSH from all IP addresses / subnets from where management IP will be accessed.
  - All traffic from your AWS VPCs (private IPs)
  - All traffic from the WAN side public IPs of Citrix SD-WAN peer appliances hosted on prem or in cloud.

- Define the Network Interfaces for the EC2 instance

- Create Elastic IP addresses for the EC2 instance

- Define Security for the EC2 instance and network interfaces

Connect to the SD-WAN web interface:

- License
- Install identify using Local Change Management

Create a VPC in AWS - Virtual Private Cloud (VPC)

To create VPC:

1. From the AWS management console tool bar, select **Services** > **VPC** (Networking & Content Delivery).
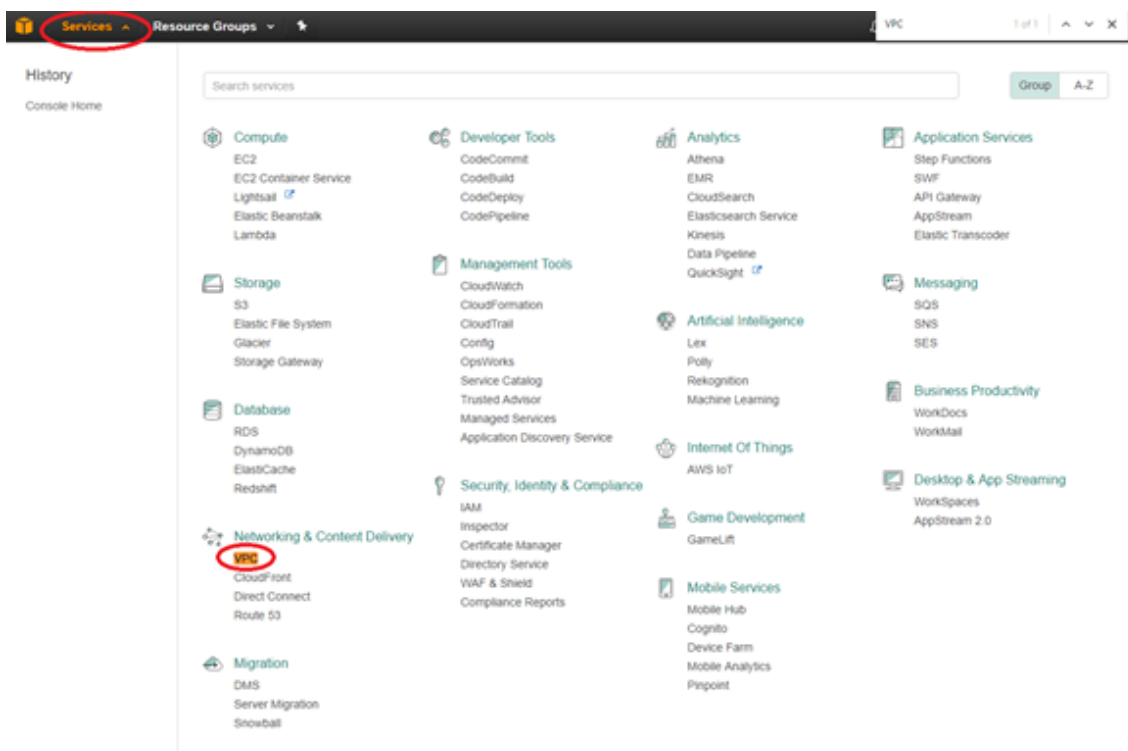
2. Select your **VPCs**, then click the **Create VPC** button.
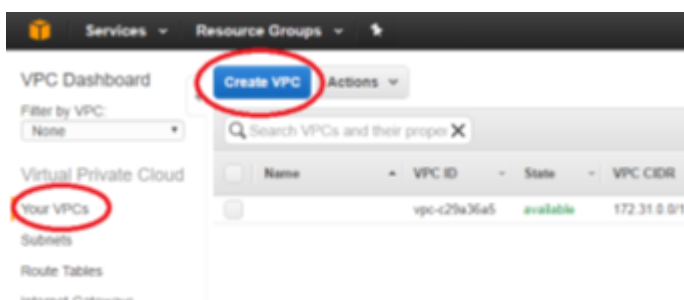
3. Add **Name** tag, CIDR block according to your network diagram and Tenancy = default, and click **Yes, Create**.

265

Define an internet gateway for the VPC

To define the Internet gateway for the VPC:

1. From the AWS management console, select **Internet Gateways** > **Create Internet Gateway**. The Internet Gateway traffic matching the 0.0.0.0/0 route can be configured in the route table. It is also required for external access to the SD-WAN AMI web interface for further configuration.
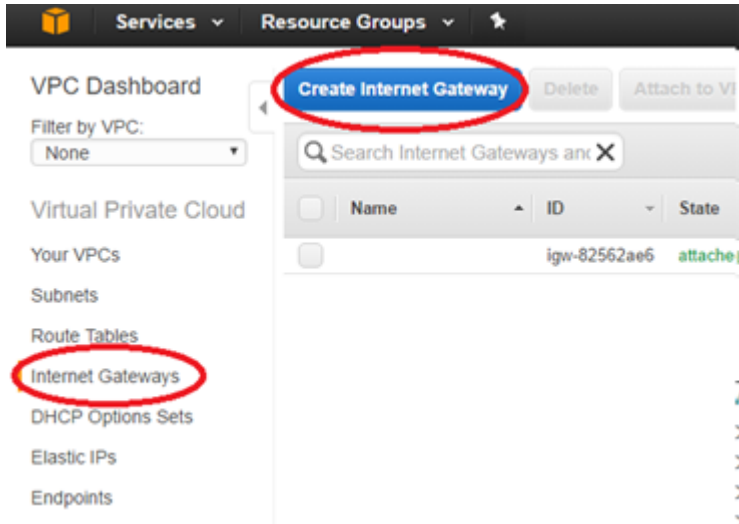
2. Give the IGW a Name tag, and click **Yes, Create**.
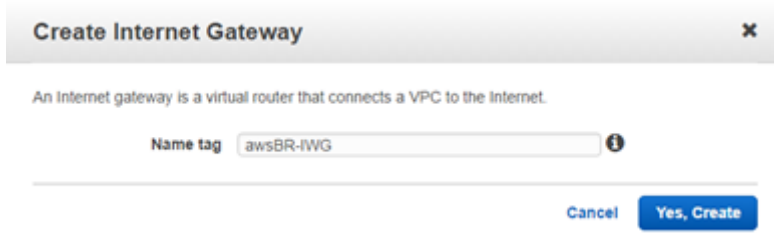
3. Select the newly created IGW and click **Attach to VPC**.
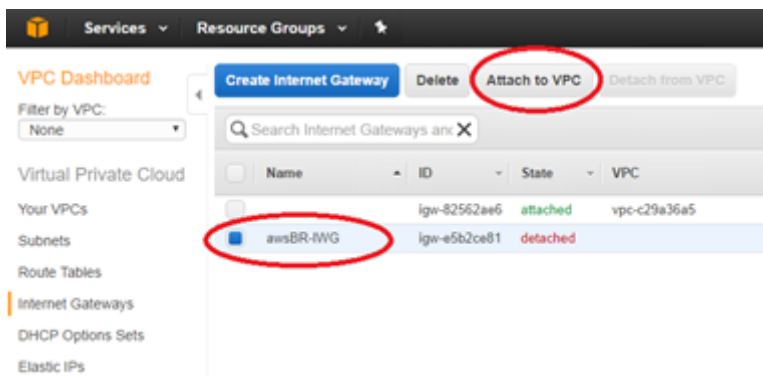
4. Select the previously created VPC and click **Yes, Attach**.

Define subnets for the VPC to differentiate mgmt, LAN, and WAN

To define subnets for VPC:

1. From the AWS management console, select **Subnets** > **Create Subnets** to create Mgmt, LAN, and WAN subnets. Use the defined subnets to distinguish between the LAN, WAN, and Mgmt subnets defined in the SD-WAN configuration.
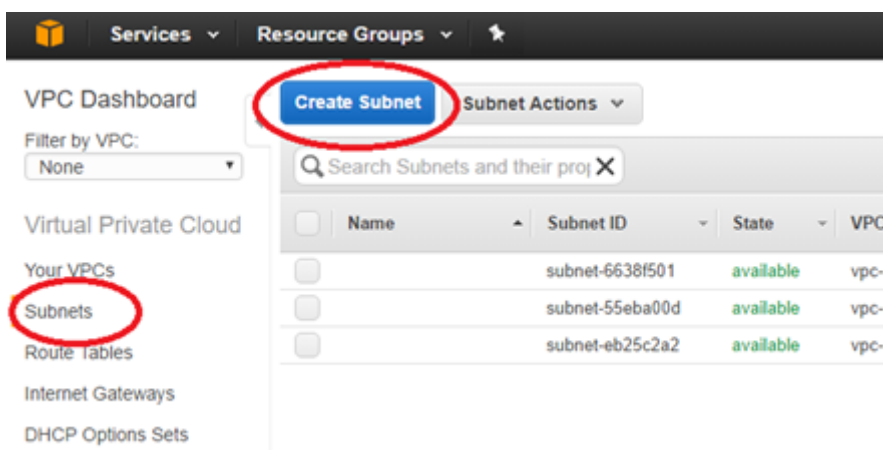
2. Enter the details specific for the Mgmt subnet of the VPX, then create it using the **Yes, Create** button.

   - Name tag: name to identify different subnets (Mgmt, LAN, or WAN)
   - VPC: <the VPC previously created>
   - Availability Zone: <set at discretion>
   - CIDR block: subnet specific to the defined name (Mgmt, LAN, or WAN) that is a smaller subset of the CIDR previously defined

3. Repeat the process until you have created a subnet for the Mgmt, LAN, and WAN networks.

Define route tables for the management subnet

To define route tables:

1. From the AWS management console, select **Route Tables** > **Create Route Table** to create route tables for the Mgmt, LAN, and WAN subnets.
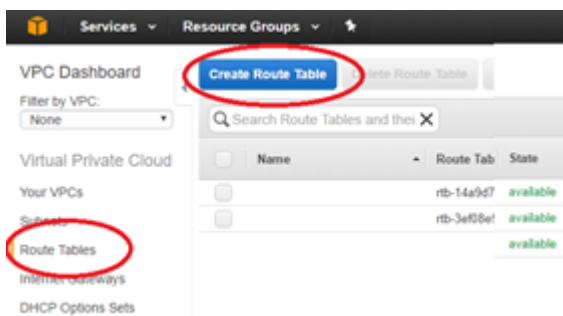
2. Enter the detail for the Mgmt subnet

   - Name tag: name to identify different subnets (Mgmt, LAN, or WAN)
   - VPC: The previously created VPC

3. With the newly created route table still highlighted, select **Subnet Association** > **Edit**.
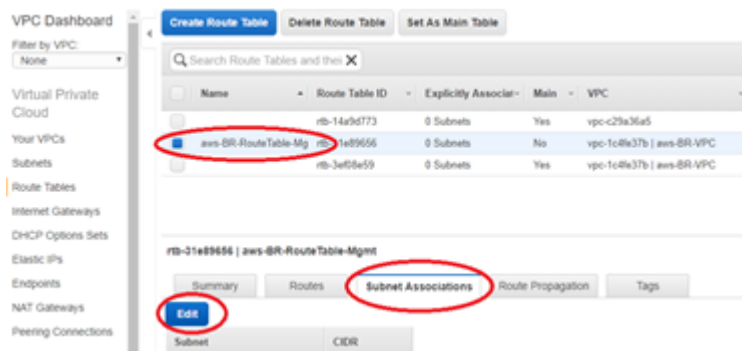
4. Make the association with the desired subnet, then click **Save**.
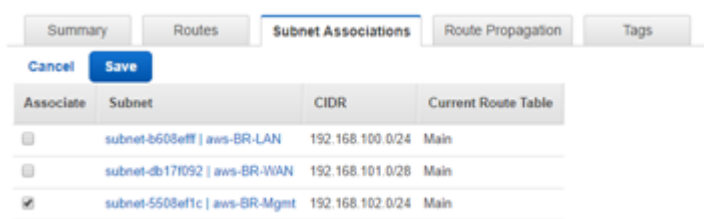
5. With the newly created route table still highlighted, select **Routes** > **Edit**.
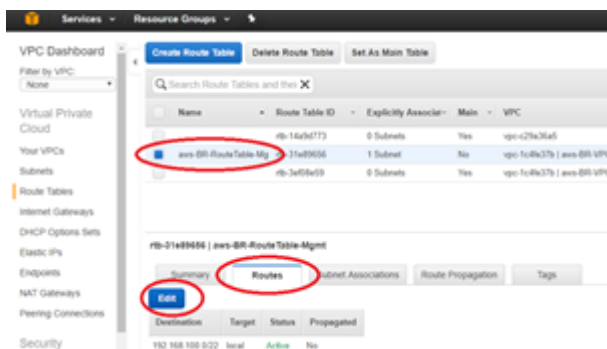
6. Click **Add** another route button (only required for the Mgmt, and WAN subnets), then **Save**.

   - Destination: 0.0.0.0/0
   - Target: The Internet Gateway (igw-xxxxxxx previously defined)
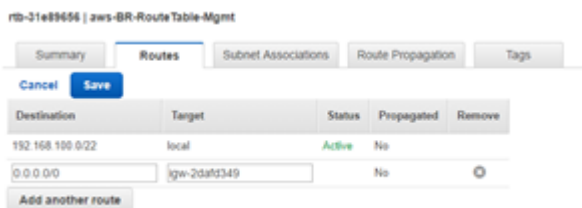
Note

AWS provides a global route table in the EC2 instance but the NetScaler SD-WAN AMI will use local route tables so that the user can control traffic forwarding to the Virtual Path.

Define route tables for the WAN subnet

To define route tables:

1. From the AWS management console, select **Route Tables** > **Create Route Table** to create route tables for the Mgmt, LAN, and WAN subnets.
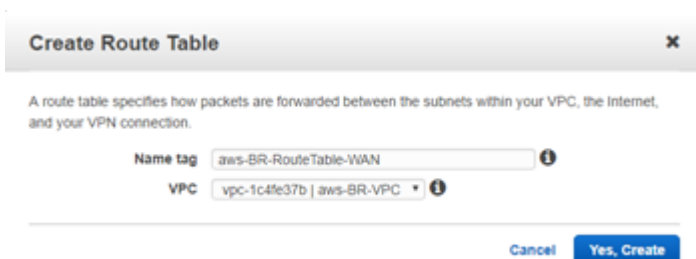
2. Enter the details for the WAN subnet:

   - Name tag: name to identify different subnets (Mgmt, LAN, or WAN)
   - VPC: The previously created VPC

3. With the newly created route table still highlighted, select **Subnet Association** > **Edit**.

4. Make the association with the desired subnet, then click **Save**.

5. With the newly created route table still highlighted, select **Routes** > **Edit**.

6. Click **Add** another route button (only required for the Mgmt, and WAN subnets), then **Save**.

   - Destination: 0.0.0.0/0
   - Target: <The Internet Gateway> (igw-xxxxxxx previously defined)

Define route tables for the LAN subnet

To define route tables for the LAN subnet:

1. From the AWS management console, select **Route Tables** > **Create Route Table** to create route tables for the Mgmt, LAN, and WAN subnets.

2. Enter the details for the LAN subnet:

   - Name tag: name to identify different subnets (Mgmt, LAN, or WAN)
   - VPC: The previously created VPC

3. With the newly created route table still highlighted, select **Subnet Association** > **Edit**.

4. Make the association with the desired subnet, then click **Save**.

> **Note**
>
> To route LAN side traffic through SD-WAN, associate the target destination as the SD-WAN LAN interface id in the SD-WAN LAN route table. The target for any destination can be set to interface id only after creating the instance and attaching network interfaces to that instance.

Create an SD-WAN SE AMI

To create the EC2 instance:

1. From the AWS management console tool bar, select **Services** > **EC2 (Compute)**.
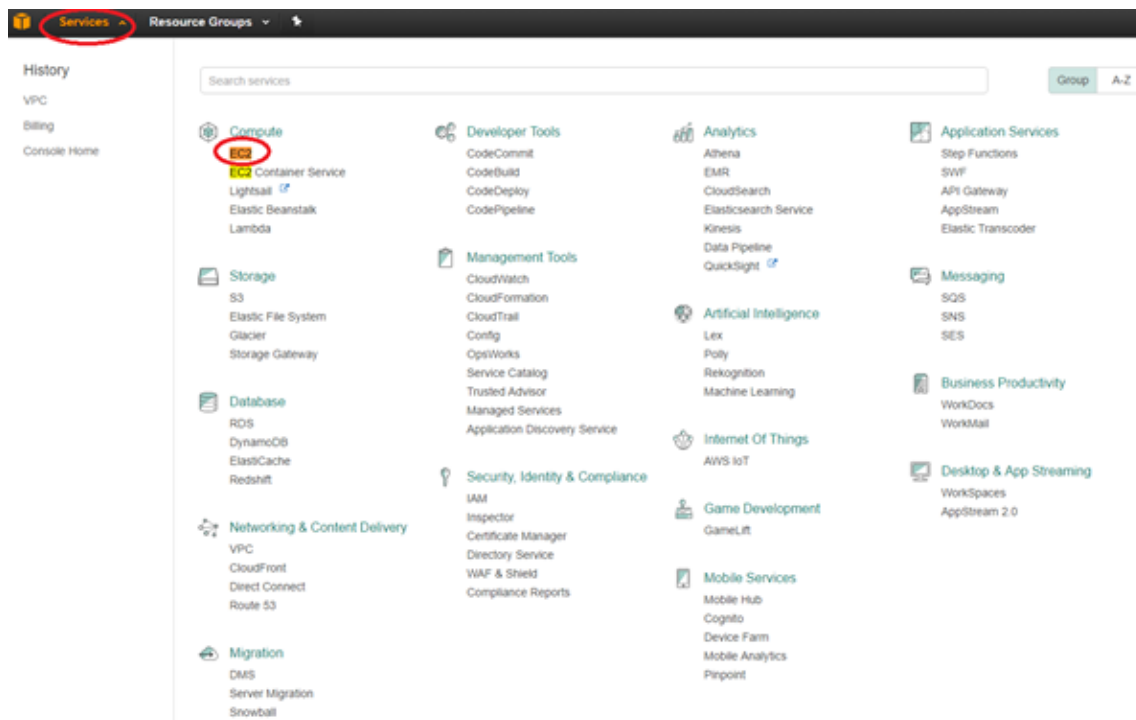
2. Select the **EC2** dashboard tool bar, select **Instances** > **Launch Instance**.
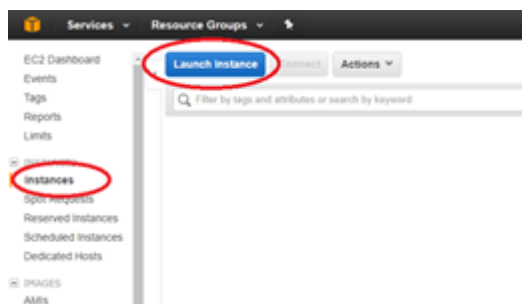
3. Use the **AWS Marketplace** tab to search for the SD-WAN Amazon Machine Image (AMI) or use the **My AMIs** tab to locate an owned or shared SD-WAN AMI, locate **Citrix NetScaler SD-WAN Standard Edition** and then click **Select**.
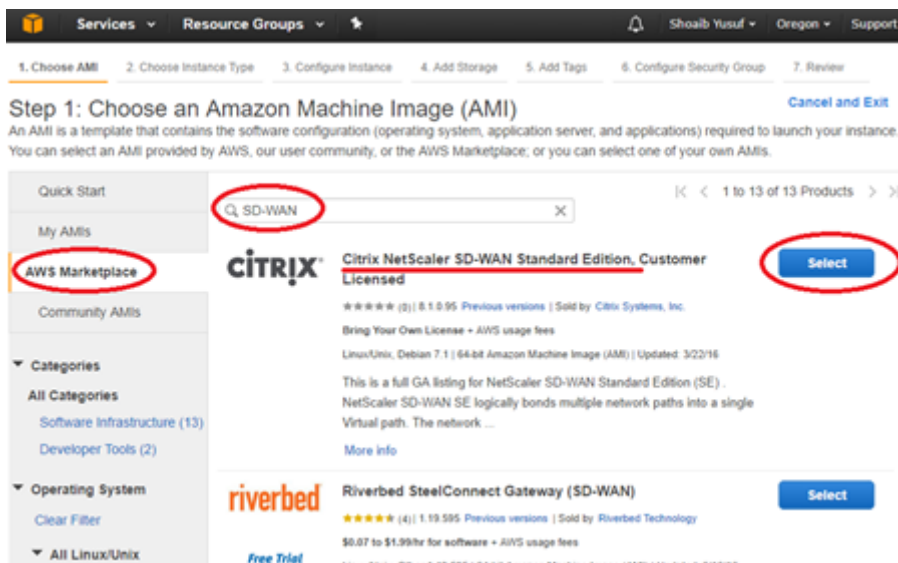
4. Confirm the selection with **Continue**.

5. On the **Choose Instance Type** screen, select the **EC2 Instance Type** that was identified during preparation, then select **Next: Configure Instance Details**.
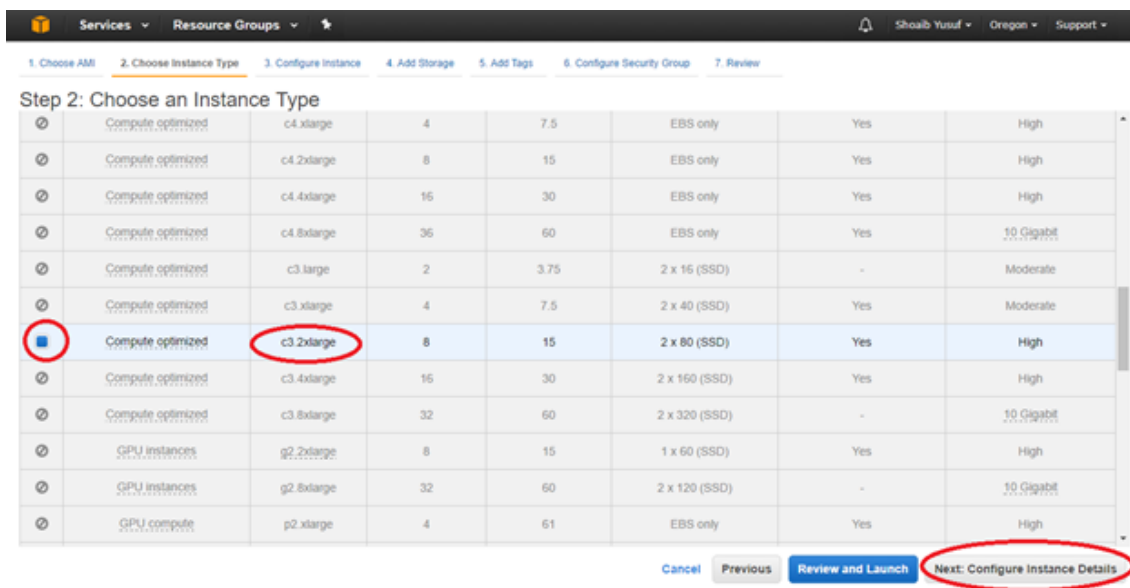
6. Enter instance details (anything not specified must be left unset/default):

   - Number of Instances: 1
   - Network: select VPC previously created>
   - Subnet: select Mgmt Subnet previously defined
   - Auto-assigning Public IP: enabled
   - **Network interfaces > Primary IP**: enter predefined Mgmt IP

273

7. Click **Next: Add Storage**
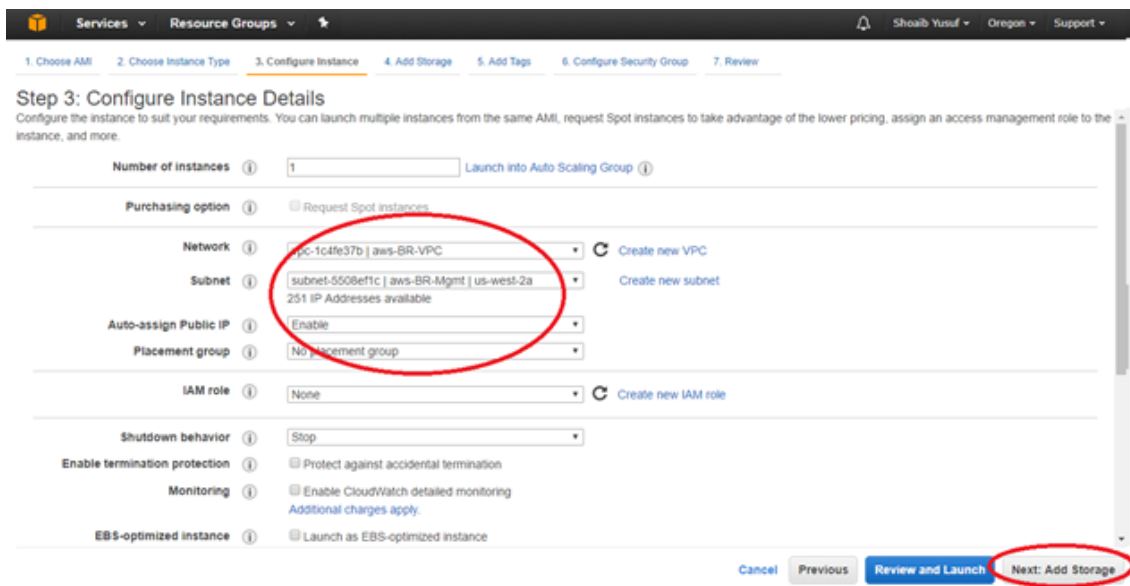
Note

Associate the EC2 instance with the Mgmt Subnet to associate the first EC2 interface (eth0) with the SD-WAN Mgmt interface. If eth0 is not associated with the SD-WAN Mgmt interface, connectivity is lost following a reboot.1.

8. Enter the following information for the Root Storage:

   • Volume Type: General Purpose (SSD) GP2

9. Then select **Next: Tag Instance**
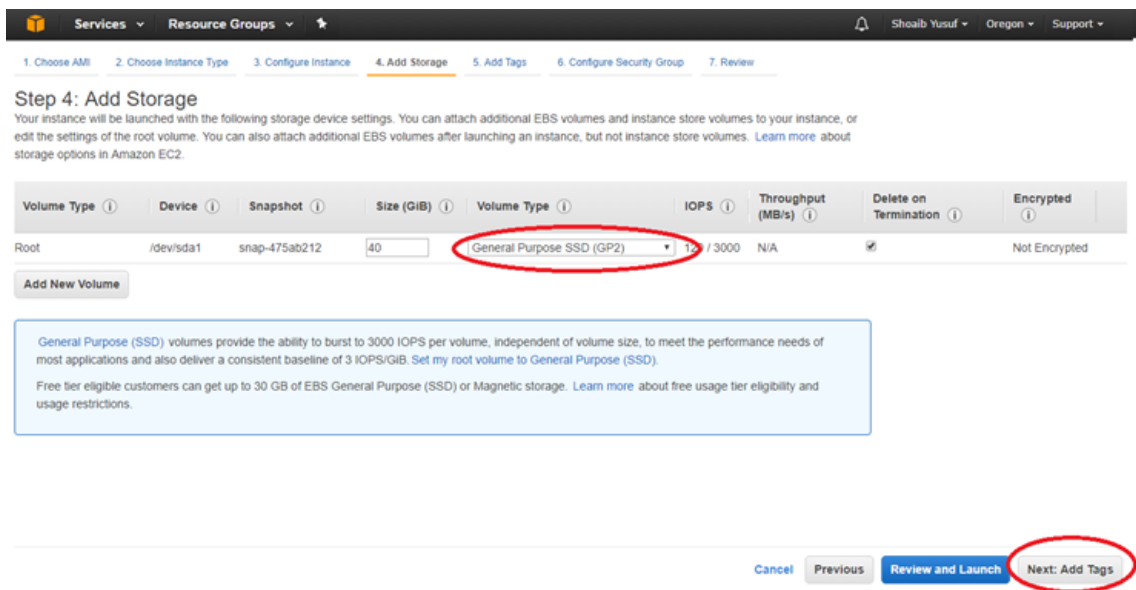
10. Give the EC2 instance a name by specifying a value for the default **Name** Tag. Optionally create other desired Tags.
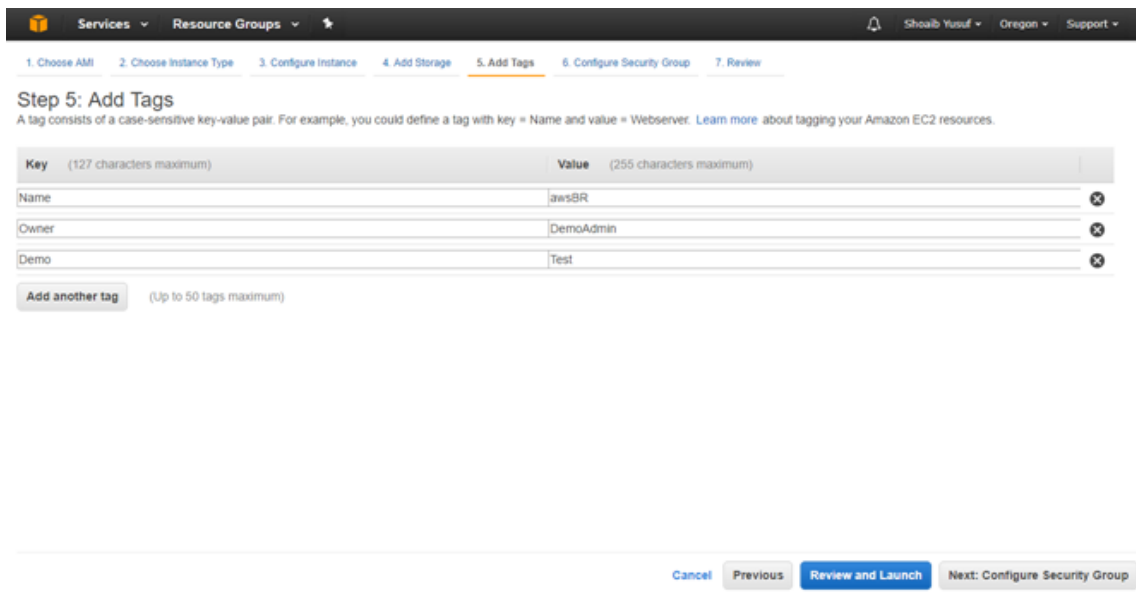
11. Then select **Next: Configure Security Group**.

12. Select an existing **Security Group** or create a Security Group:

    - Default security group generated includes HTTP, HTTPS, SSH, and
      Click the **Add Rule** button to add two more:
    - All ICMP with Source: Custom 0.0.0.0/0
    - Custom UDP Rule with Port Range: 4980 and Source: custom <known IP addresses from partner SD-WAN>

13. Select **Review** and **Launch**.
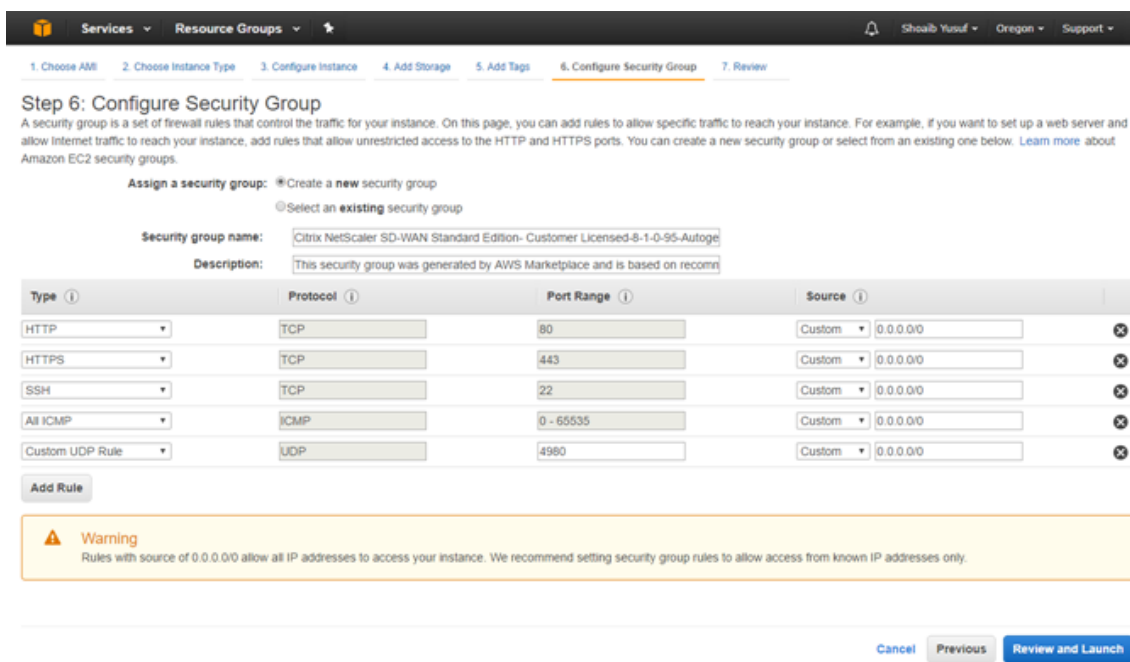
14. After complete with reviewing, select **Launch**.

15. In the **Key Pair** pop-up, either select an existing key pair or create a new key pair, then select **Launch Instance**.

Important

If a new key pair is created, be sure to download and store it in a safe location.

16. Citrix SD-WAN SE AMI must now be launched successfully.
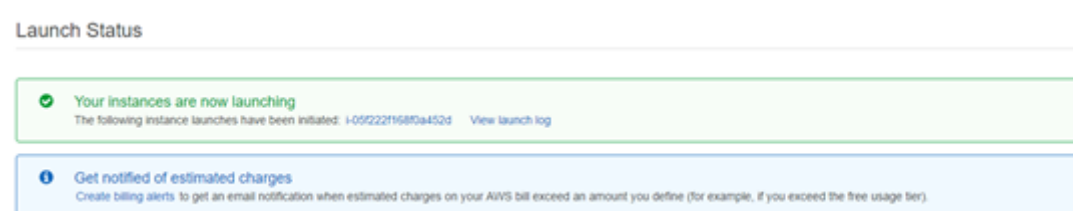
> **Note**
>
> A Security Group is a set of firewall rules that controls traffic for an EC2 Instance. Inbound and outbound rules can be edited during and after EC2 launch. Each EC2 Instance must have a Security Group assigned. Also, each Network Interface must have a Security Group assigned. Multiple Security Groups can be used to apply distinct sets of rules to individual Interfaces. The default Security Group added by AWS only allow traffic within a VPC.
>
> The Security Group assigned to the NetScaler SD-WAN AMI and its interfaces must accept SSH, ICMP, HTTP, and HTTPS. The Security Group assigned to the WAN interface must also accept UDP on port 4980 (for Virtual Path support). Refer to AWS help for more detail on Security Group configuration information.
>
> **Important**
>
> Wait two hours if provisioned from a new account and then retry

17. Navigate back to your **AWS Console: EC2 Dashboard**.

18. From the tool bar, under **Network & Security** select **Network Interfaces**, highlight the Mgmt interface and Edit the Name tag to give the interface a useful name.

19. Then click **Create Network Interface** to create the LAN interfaces:

    - Description: <a user-defined description for the interface>
    - Subnet: <the subnet previously defined for the interface>
    - Private IP: <the private IP for the interface previously defined during preparation>
    - Security Group: <the appropriate security group for the interface>
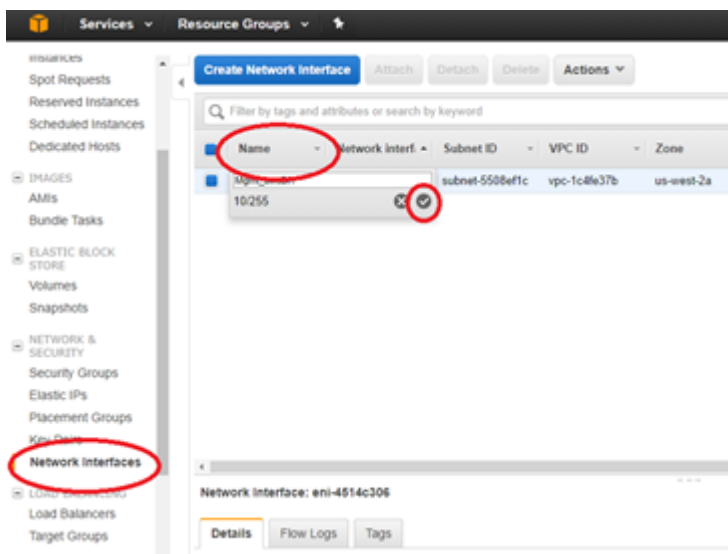
20. Repeat and click **Create Network Interface** to create the WAN interface.
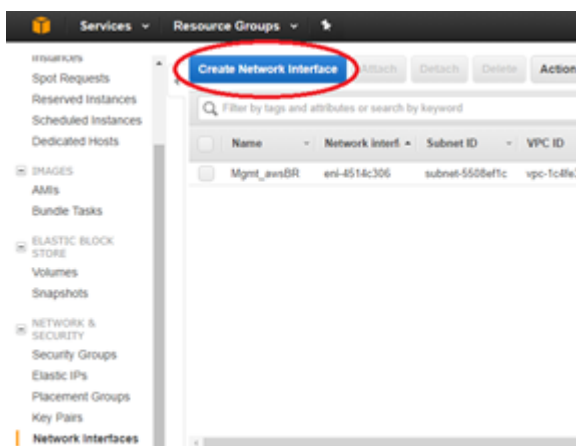
21. Edit the Name tag for each new interface and give a useful name.
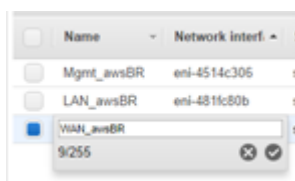
22. Highlight the **Mgmt Interface** and select **Actions** > **Change Source/Dest**. Check to disable **Source/Dest**. Check, then select **Save**.
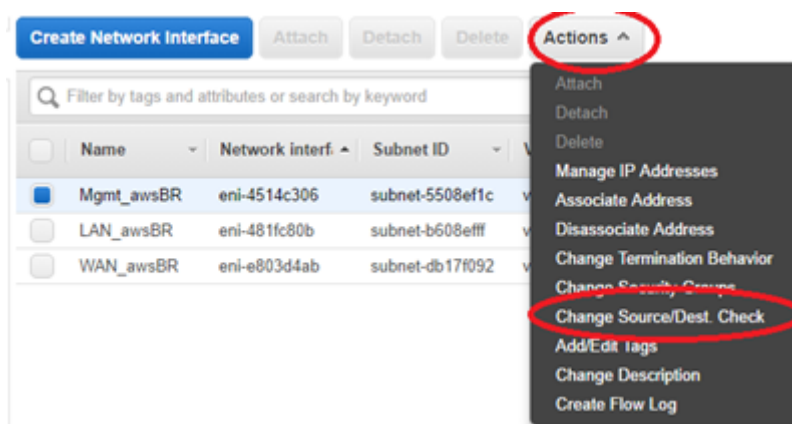
23. Repeat for LAN and WAN interfaces.
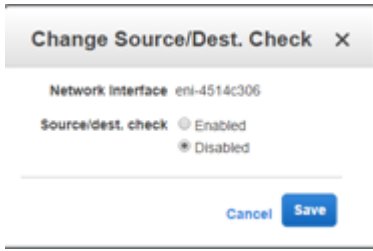
24. At this point all the Network Interfaces: **Mgmt**., **LAN**, and **WAN** each are configured with a **Name**, **Primary private IP**, and disabled for **Source/Dest. Check** attribute. Only the Mgmt. Network Interface has a Public IP associated with it.
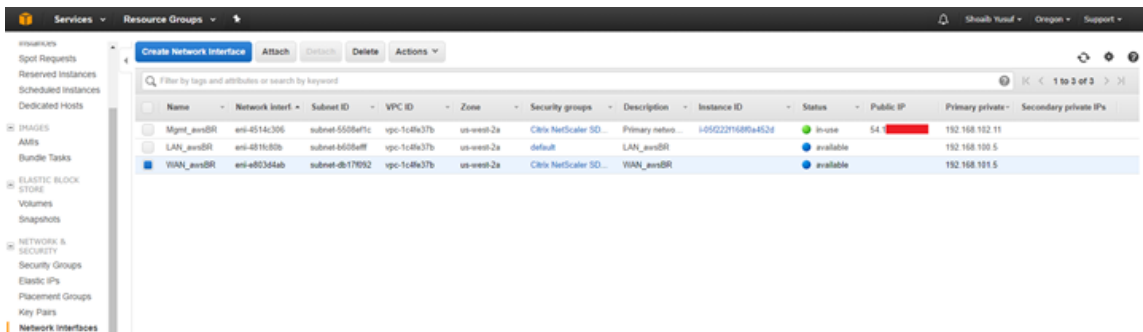
Important

Disabling the Source/Dest. Check attribute enables the interface to handle network traffic that is not destined for the EC2 instance. As the NetScaler SD-WAN AMI acts as a go-between for network traffic, the Source/Dest. Check attribute must be disabled for proper operation.

The Private IPs defined for these Network Interfaces, ultimately, must match the IP addresses in your SD-WAN configuration. It can be necessary to define more than one Private IP for the WAN Network Interface if that interface is associated with more than one WAN Link IP in the SD-WAN configuration for this site node. This can be accomplished by defining Secondary Private IPs for the WAN Interface as needed.

25. From the **EC2 Dashboard** tool bar, select **Instances**.
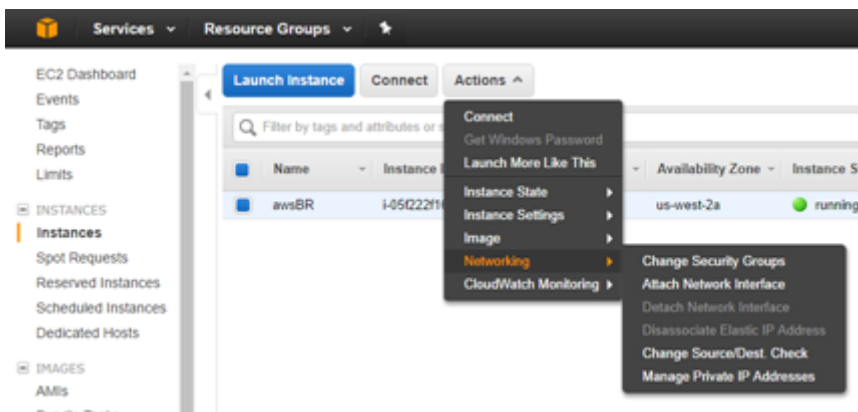
26. Highlight the newly created instance, then select **Actions** > **Networking** > **Attach Network In-terface**.
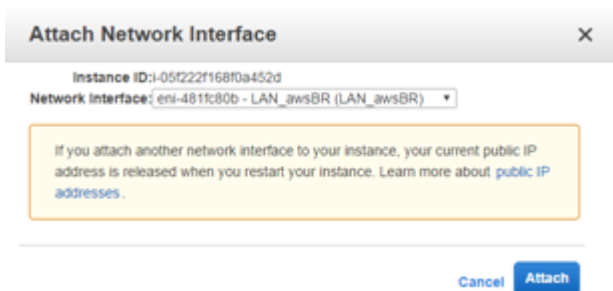
27. Attach first the LAN network interface and then the WAN network interface to the SD-WAN SE AMI.
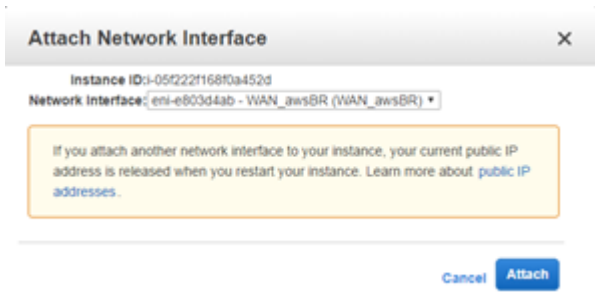
Note

Attaching the Mgmt, LAN, and WAN in that order attaches to eth0, eth1, eth2 in the SD-WAN AMI. This aligns with the mapping of the provisioned AMI and ensures that interfaces are not reassigned incorrectly in the event of AMI reboot.

28. From the **EC2 Dashboard** tool bar, select **Elastic IPs (EIP)**, then click **Allocate new address**.
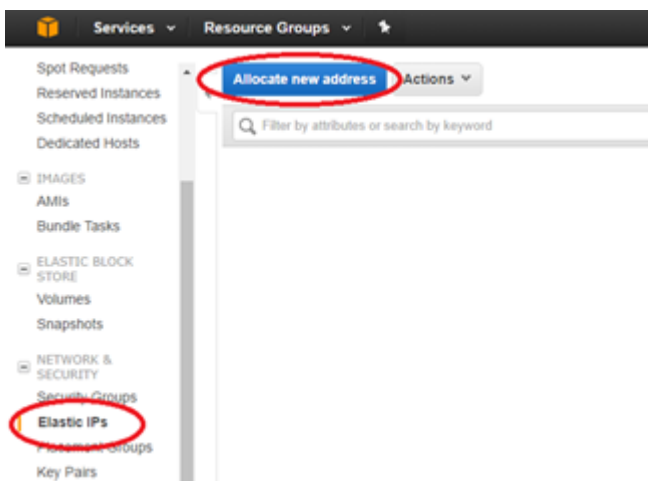
29. Click **Allocate** to allocate a new IP address, then **Close** after the New address request succeeded.

30. Highlight the new EIP and select **Action** > **Associate address** to associate the EIP with the Mgmt.

Interface, then click **Associate**.

- Resource type: <network interface>
- Network interface: <previously created Mgmt. Network Interface>
- Private IP: <previously defined private IP for Mgmt>
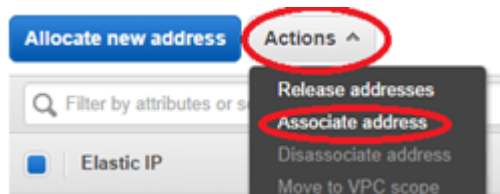
31. Repeat the process to associate another new EIP with the WAN interface.
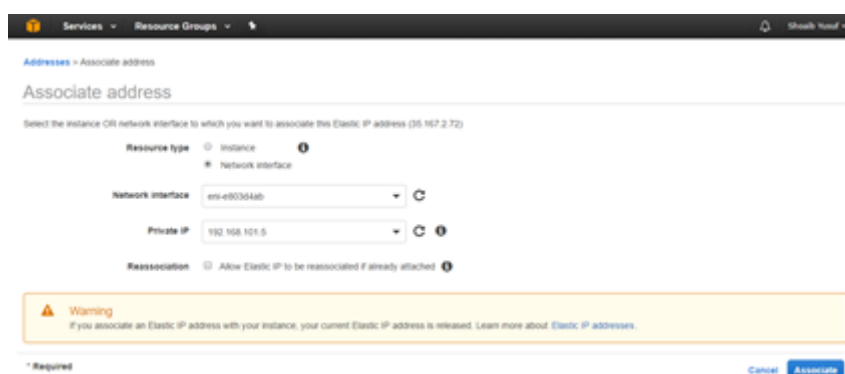
Configure SD-WAN SE AMI - SD-WAN Web management interface

To configure SD-WAN SE AMI:

1. At this point, you must be able to connect to the SD-WAN SE AMI's management interface using a web browser.

2. Enter the **Elastic IP (EIP)** associated with the Mgmt. Interface. You can create a security exception, if the security certificate is not recognized.

3. Log in to the SD-WAN SE AMI using the following credentials:

   - User name: *admin*
   - Password: *<aws-instance-id>* (example; i-00ab111abc2222abcd)
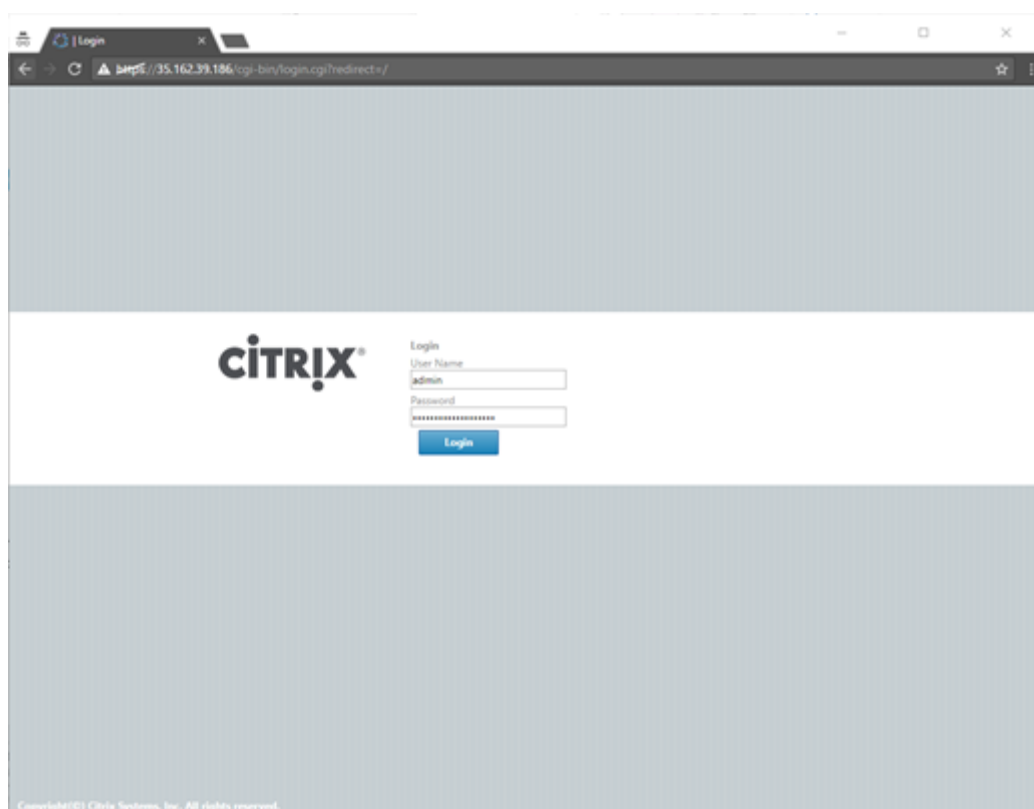
Note

If the Mgmt. Interface cannot be reached, check the following:

- Make sure the EIP is correctly associated with the Mgmt. interface
- Make sure the EIP responds to ping
- Makes sure the Mgmt. interface Route Table includes an Internet Gateway route (0.0.0.0/0)
- Make sure the Mgmt. interface Security Group is configured to allow HTTP/HTTPS/ICM-P/SSH

Starting with release 9.1 SD-WAN AMI, users can also log in to the SD-WAN AMI console using *ssh admin@<Mgmt. EIP>*, assuming that the key pair for the EC2 Instance has been added to the user's SSH key chain.

4. For SD-WAN SE **bring-your-own-license (BYOL) AMI**, a software license must be installed:

- On the SD-WAN web interface, navigate to **Configuration** > **Appliance Settings** > **Licensing**
- From **License Configuration**: **Upload License for this Appliance**, select **Choose File**, browse and open the **SD-WAN SE AWS license**, then click **Upload and Install**
- After successful upload, License Status will indicate State: Licensed
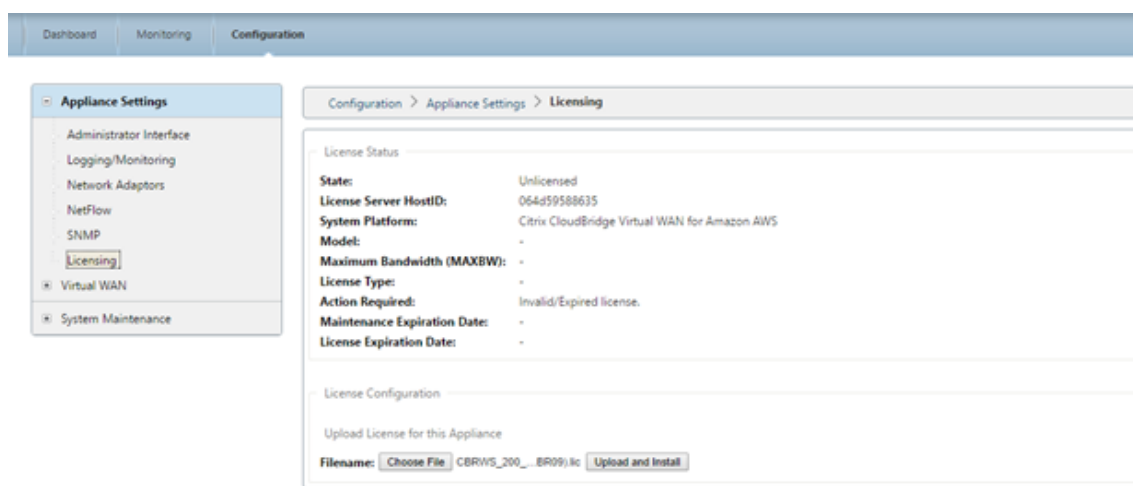
5. Set the appropriate **Data/Time** for the new AMI:

   - On the SD-WAN web interface, navigate to **Configuration** > **System Maintenance** > **Date/-Time Settings**
   - Set the correct date and time using **NTP**, **Date/Time Setting**, or **Timezone**
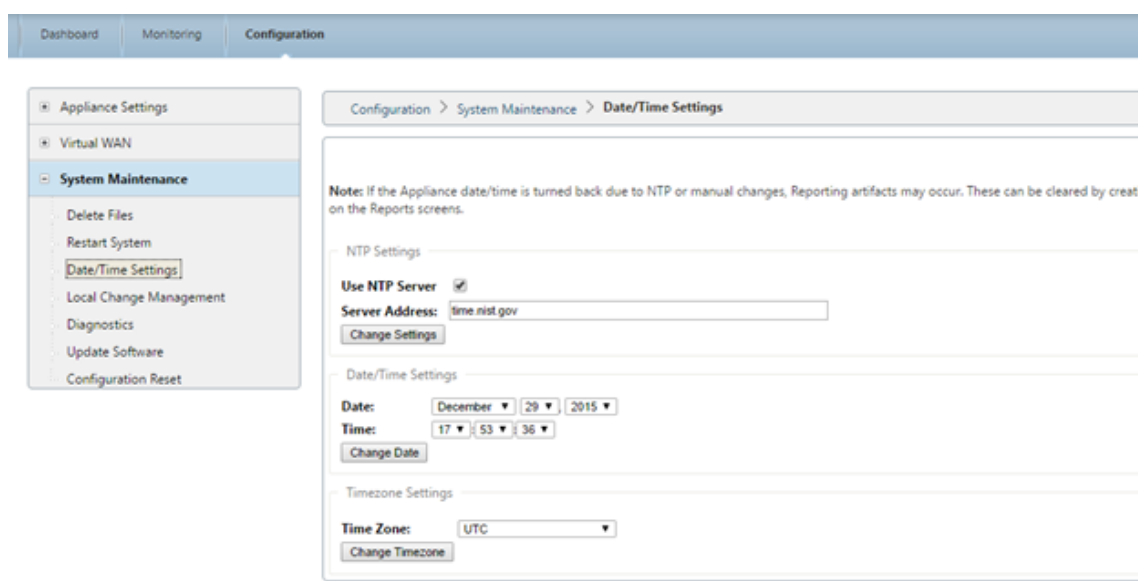
Note

The SD-WAN SE AMI Virtual WAN Service remains disabled until an appliance package (Software + Configuration) is installed on the AMI.

Add SD-WAN SE AMI to your SD-WAN environment

To add SD-WAN AMI to your SD-WAN environment:

1. Navigate to your **SD-WAN Center** or **Master Control Node** for your SD-WAN environment.

2. Add a **new site** node using the **Configuration Editor**:

- Add site: model VPX, Mode: client
- Interface Groups: awsLAN = eth1, awsWAN = eth2 (untrusted)
- Virtual IP Address: 192.168.100.5 = awsLAN, 192.168.101.5 = awsWAN with awsLAN virtual IP address being configured, the SD-WAN advertises the LAN subnet of 192.168.100.5/24 as a local route to the SD-WAN Environment (refer to the **Connections** > <**AWSnode** > **Routes**).
  WAN Links:
- AWSBR-WAN with Access Type Public Internet, Autodetect Public IP if client node or configure the EIC for WAN link if MCN node, Access Interfaces: awsWAN 192.168.101.5 with gateway 192.168.101.1 (#.#.#.1 is typically the AWS reserved gateway).

3. In the Configuration Editor validate the path association under **Connections** > **DC** > **Virtual Paths** > **DC-AWS** > **Paths**.
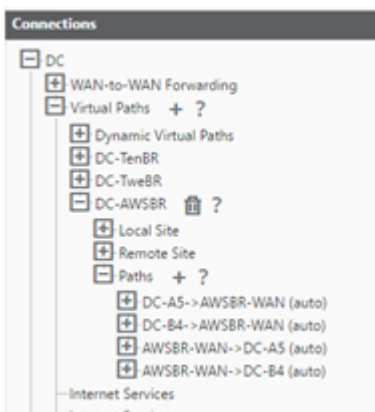
> **Note**
>
> The Virtual Path is used across the AMI WAN interface to push software and configuration updates to the SD-WAN AMI instead of via direct connection to the Mgmt. interface.
>
> Private IP addresses must be defined on the EC2 WAN Network Interface for every WAN

Link IP in the Configuration Editor. This can be accomplished by defining one or more Secondary Private IPs for the Network Interface as necessary.

Important

Recall the assigned mapping in the AWS EC2 dashboard assigning Mgmt. to eth0, LAN to eth1 and WAN as eth2

Amazon reservices the first four IP addresses and the last IP address in each subnet CIDR block and cannot be assigned to an instance. For example, in a subnet with CIDR block 192.168.100.0/24, the following five IP addresses are reserved:

- 192.168.100.0: Network address
- 192.168.100.1: Reserved by AWS for the VPC router
- 192.168.100.2: Reserved by AWS for the DNS server
- 192.168.100.3: Reserved by AWS for future use
- 192.168.100.255: Network broadcast address, which is not supported in a VPC

4. **Save and Export** the newly created SD-WAN configuration and export to the **Change Management Inbox**.

5. Navigate to the MCN **Change Management** and run through the change management process to push the latest configuration to the SD-WAN environment informing all existing SD-WAN nodes of the newly added AWS node and the subnets (virtual interfaces) associated with it. Make sure to upload the software package specific to VPX in the Change Preparation step that matches the current software used by the existing SD-WAN environment.

6. From the **Change Management** page, download the package generated specifically for the new AWS node using the **active** link.

7. Navigate back to the SD-WAN SE AMI's management interface using the assigned EIP for the Mgmt. interface.

8. Navigate to **Configuration** > **System Maintenance** > **Local Change Management**.

9. Click **Choose File** to browse and **Upload** the active AWS software/config package recently downloaded.

10. After successful **Local Change Management**, the web interface must auto-refresh with the latest installed software, with the **Virtual WAN Service** still disabled.
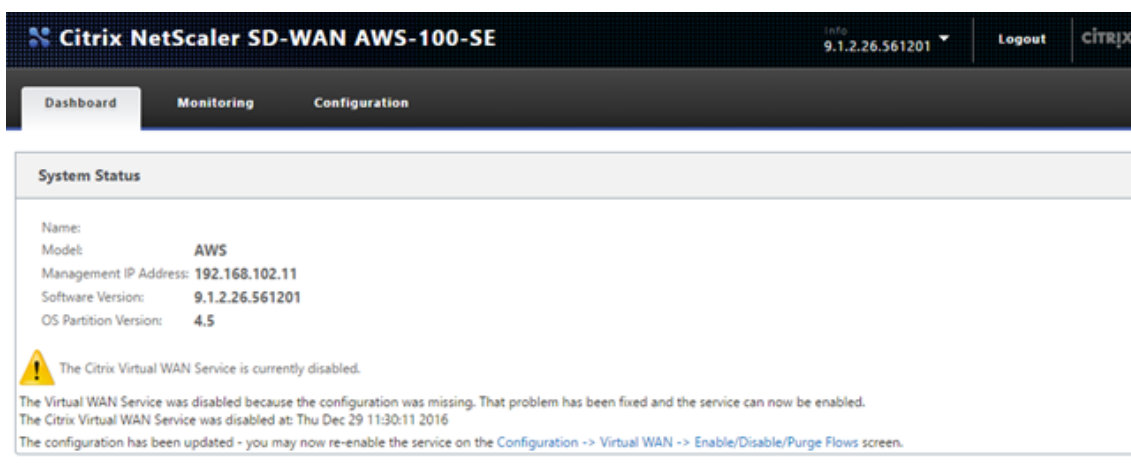
11. On the SD-WAN SE AMI section, navigate to **Configuration** > **Virtual WAN Enable/Disable/Purge Flows** and enable the service using the **Enable** button.

12. Upon successful connectivity on the WAN interface, the SD-WAN reports Good Path State on the **Monitoring** > **Statistics** > **Paths** page.
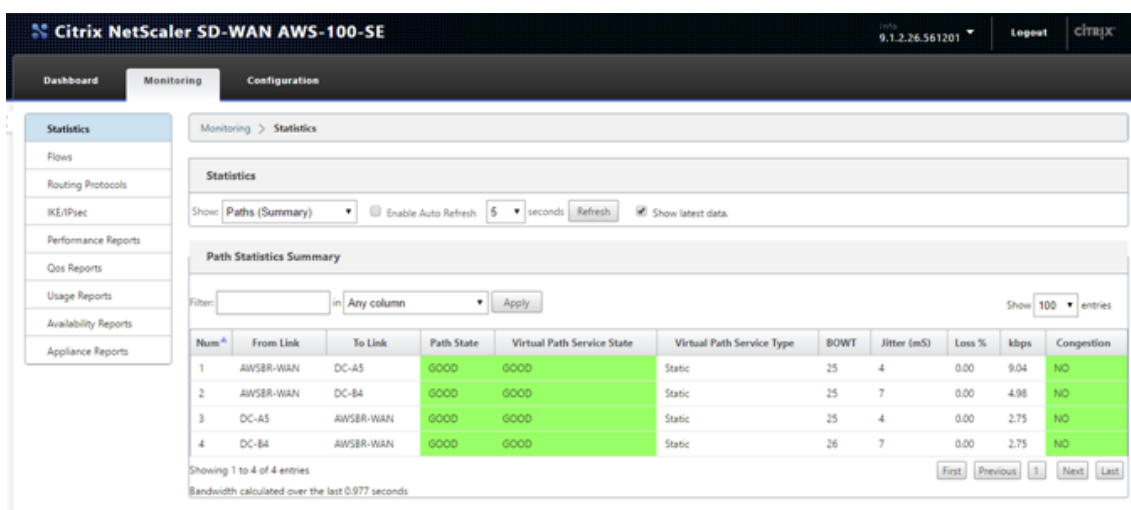
Troubleshooting

The correct private Internet Web Gateway (IWG) IP must be used in the SD-WAN Access Interface con‑
figuration

- If an incorrect IWG is used in the Configuration Editor to define the WAN Link for the AWS Site
  (Virtual IP Address and the correct Gateway) then Virtual Path fails to establish.
- A quick way to check if the IWG is incorrectly configured is to check the **SD-WAN ARP table**.

SD-WAN built in Packet Capture tool can help confirm proper packet flow

1. Navigate to the **Configuration** > **System Maintenance** > **Diagnostic** page of the SD-WMA AMI.
2. Select the **Packet Capture** tab, and set the following settings, then click **Capture**:
    - Interfaces: To capture on eth2 which was associated with the WAN interface.
3. The capture output on the webpage must show the UDP probe packets leaving the SD-WAN SE
   AMI with the WAN VIP / Private IP as the source, with a destination of the Static Public IPs used
   for the MCN, also the returning UDP packet with the source of the MCN Static Public IP and the
   destination of the local VIP/Private IP (which was NAT'd by the IWG).

> **Note**
>
> This can typically occur when an IP address is created outside of the CIDR block assigned to the
> VPC.

NOTE

- From 10.2.6 and 11.0.3 release onwards, it is mandatory to change the default admin user account password while provisioning any SD-WAN appliance or deploying a new SD-WAN SE VPX. This change is enforced using both CLI and UI.

- A system maintenance account - CBVWSSH, exists for development and debugging and has no external login permissions. The account can only be accessed through a regular administrative user's CLI session.

Deploy Citrix SD-WAN Standard Edition Instance on Azure - Release Version 10.2 and above

July 12, 2021

Citrix SD-WAN Standard Edition for Azure logically bonds multiple network links into a single secure logical virtual path. The solution enables organizations to use connections from different service providers including Broadband, MPLS, 4G/LTE, Satellite, and point-to-point links to get high resiliency virtual WAN paths. Citrix SD-WAN for Azure enables organizations to have a direct secure connection from each branch to the applications hosted in Azure eliminating the need to backhaul cloud bound traffic through a data center. Some of the benefits of using Citrix SD-WAN in Azure are:

- Create direct connections from every location to Azure.
- Ensure an always on connection to Azure.
- Extend your secure perimeter to the cloud.
- Evolve to a simple, easy to manage branch network.

> **Note**
>
> Earlier, 128 virtual paths were supported in Azure. With 11.2 release onwards, 256 virtual parts are supported with SD-WAN SE in Azure.

Topology - SD-WAN in Azure

Citrix SD-WAN Standard Edition can only be deployed in Gateway deployment mode in Azure. A Public IP address (Static/Dynamic) is assigned to the WAN facing interface of SD-WAN and one public IP is assigned to the management interface to access the management interface in Azure.
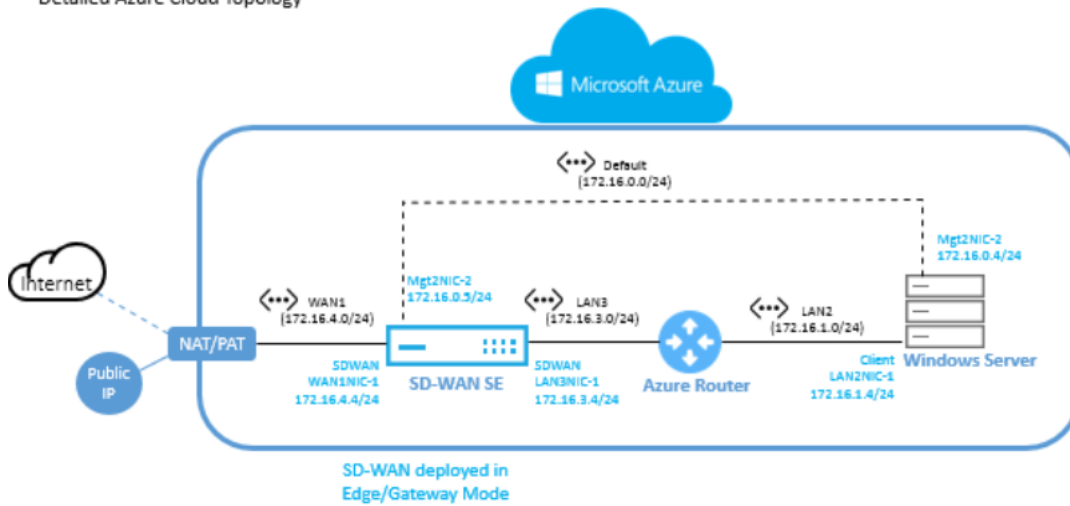
Use case

An Azure VM is deployed within a specified region and can be connected to multiple branch locations through MPLS, Internet, or 4G/LTE. Within a Virtual Network (VNET) infrastructure, SD-WAN Standard Edition VM is deployed in Gateway mode. The VNET has routes towards the Azure Gateway. The SD-WAN instance has a route towards the Azure Gateway for internet connectivity.

Connectivity between Data Center, Branch, and Cloud is achieved by using different transports methods utilizing multiple WAN paths simultaneously.
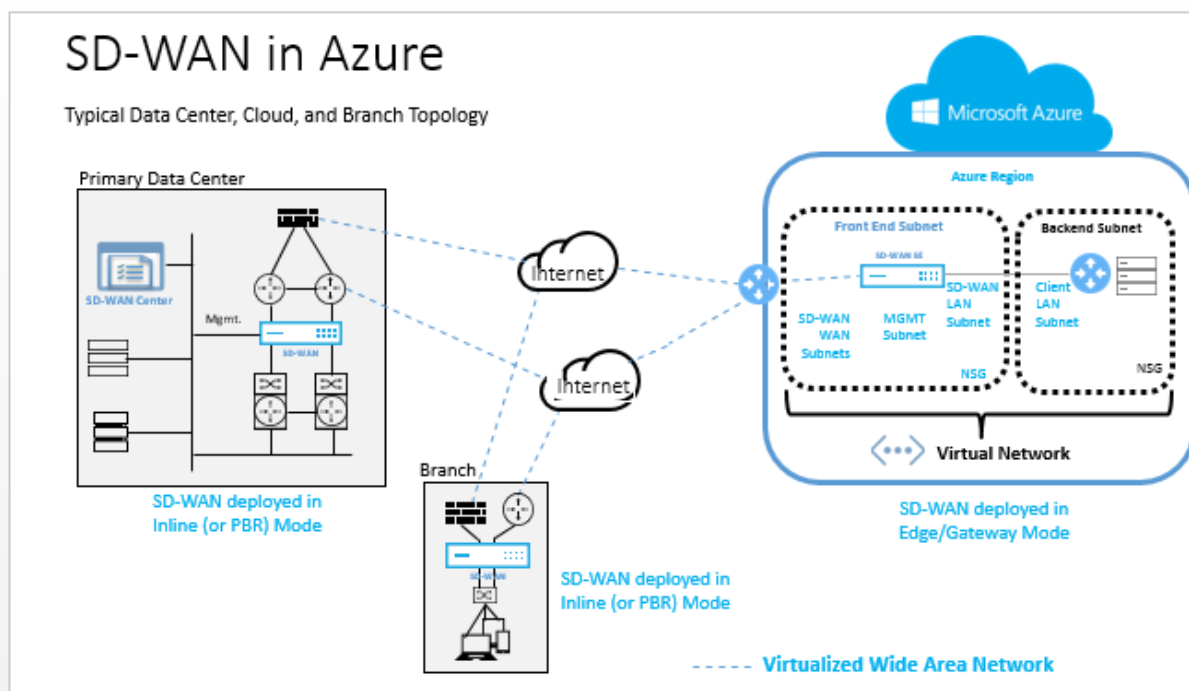
To deploy Citrix SD-WAN standard edition in Microsoft Azure

1. In a web browser, type https://portal.azure.com/. Log into Microsoft Azure account. Search for Citrix SD-WAN Standard Edition.
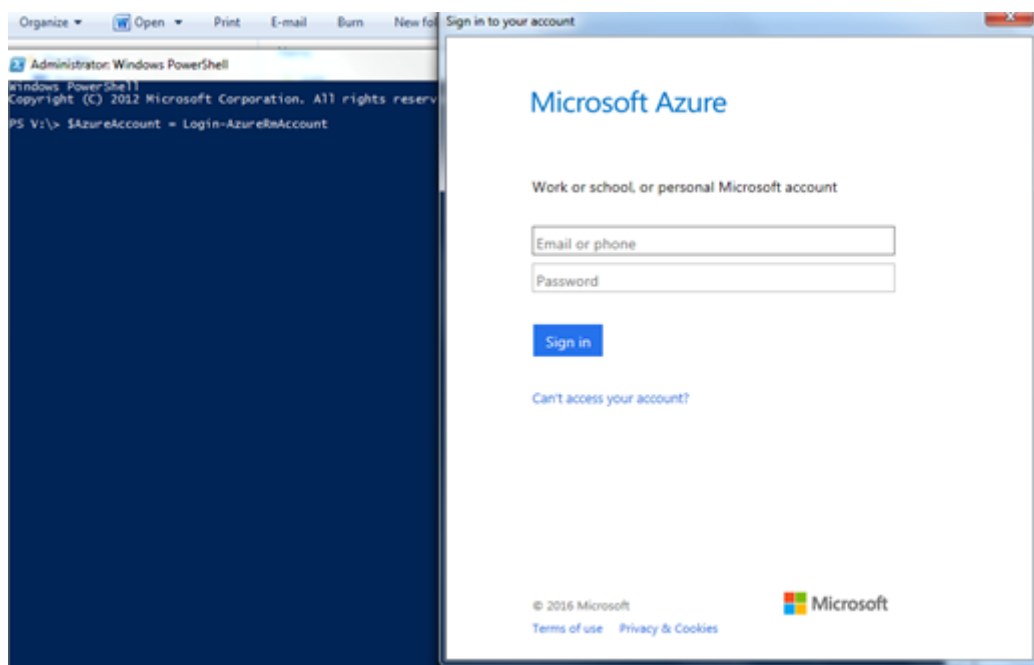
2. In the search results window, choose the following solution. Click **create** after going through the description and making sure the solution chosen is correct.

---
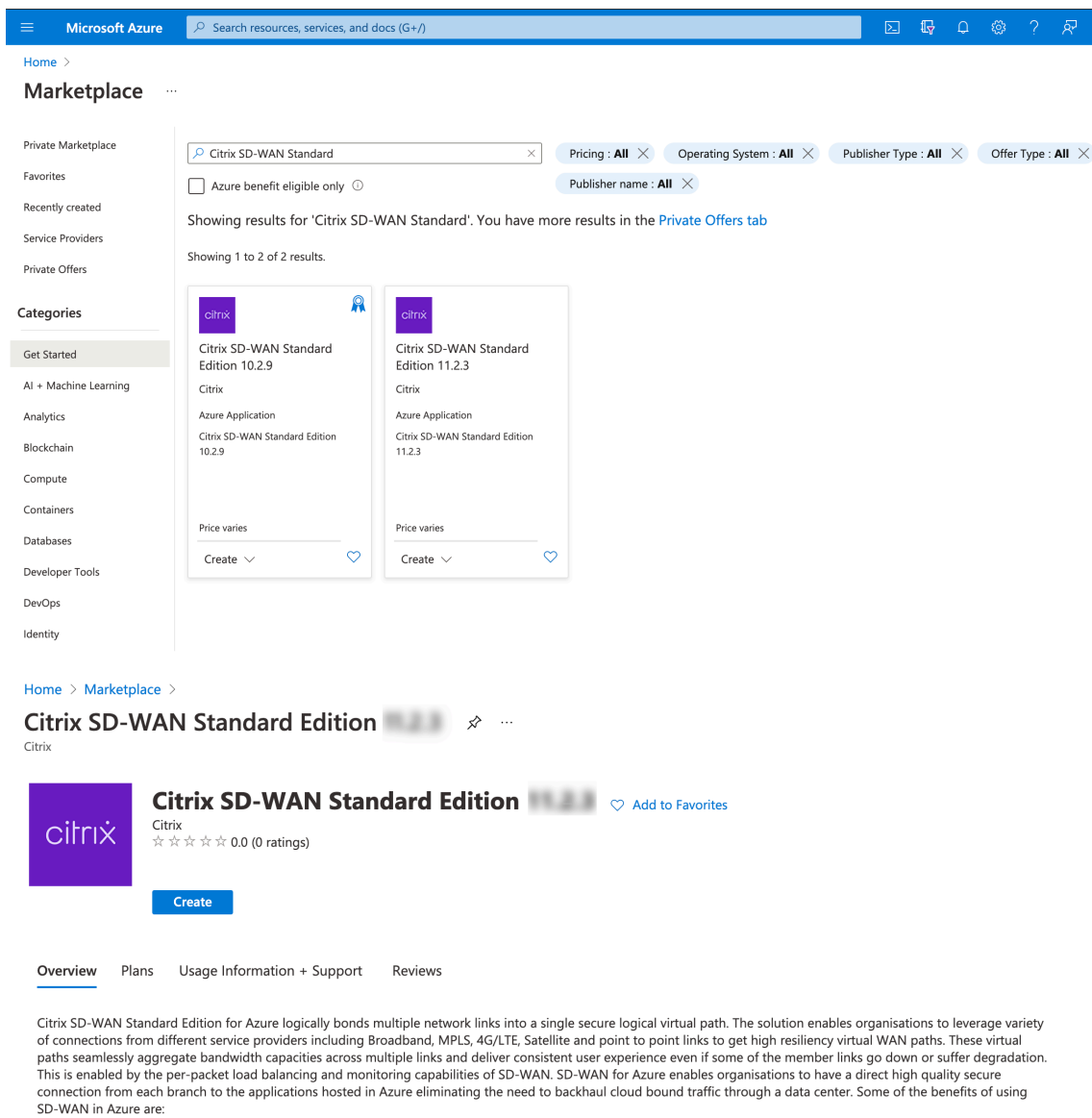
3. After you click **Create,** a wizard prompting for details necessary to create the virtual machine in Azure appears. In the first step, choose the resource group in which you like to deploy the solution. A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You can decide how you want to allocate resources to resource groups based on your deployment. Some important points to consider when defining your resource group are:

- If one resource, such as a database server must exist on a different deployment cycle, then it can be in another resource group.
- Each resource can only exist in one resource group.
- You can add or remove a resource to another resource group at any time.
- You can move a resource from one resource group to another resource group

- A resource group can contain resources that reside in different regions.
- A resource group can be used to scope access control for administrative actions.
- A resource can interact with resources in other resource groups. This interaction is common when the two resources are related but do not share lifecycle (for example, web apps connecting to a database).

In the following image, choose **Create New**.

Under **Location**, choose the region in which you want to deploy the solution. When creating a resource group, you must provide a location for that resource group. The resource group stores metadata about the resources that you are creating. Therefore, when you specify a location for the resource group, you are specifying where that metadata is stored.
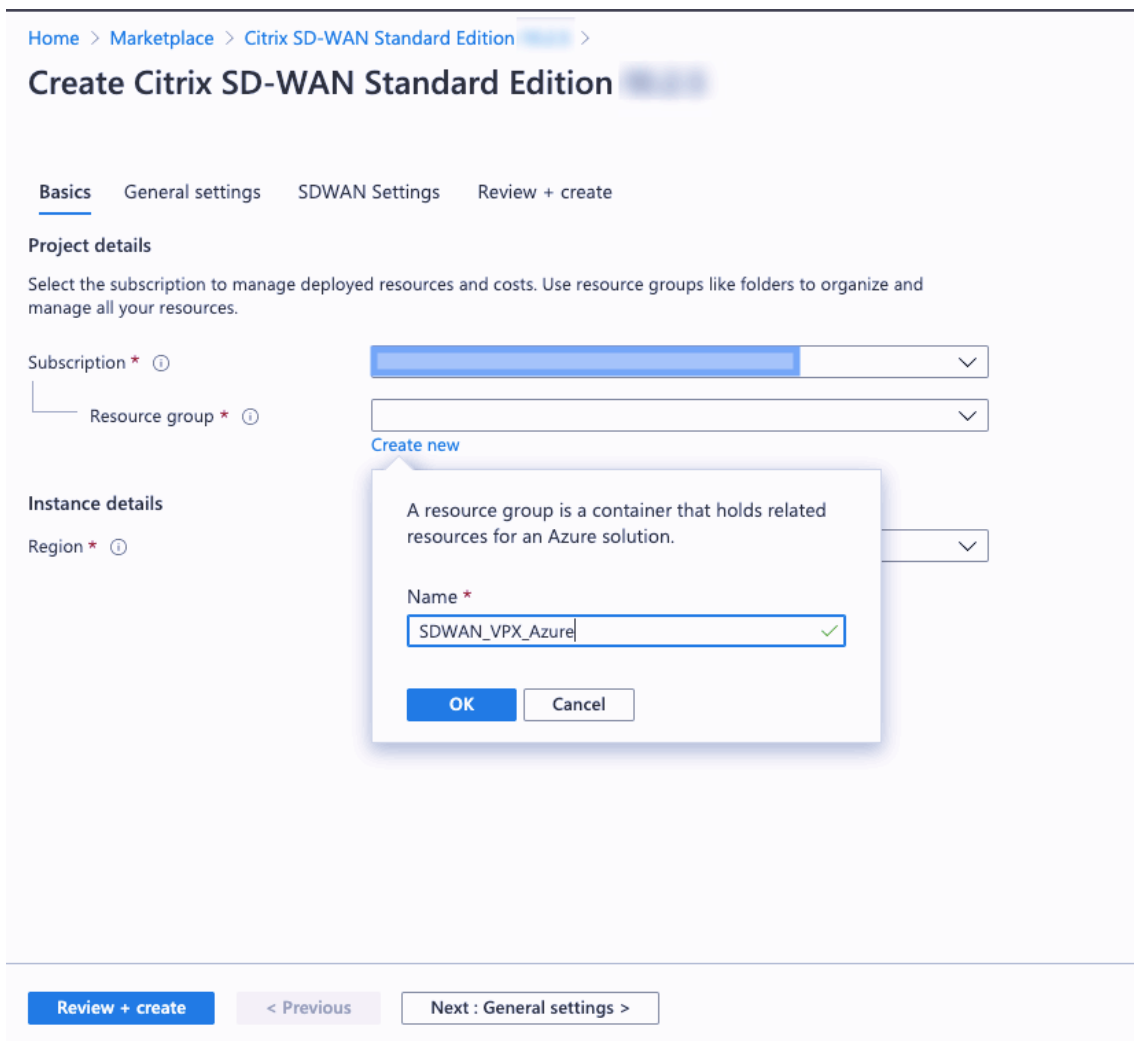
> **Note**
>
> Azure mandates creating a resource inside either a new resource group or an empty resource group, you won't be able to deploy the SD-WAN instance in a non-empty resource group.

Citrix SD-WAN Platforms

4. Provide a name for the Virtual Machine. Choose a user name and strong password. The password must consist of an upper case letter, special character and must be more than nine characters. Click **OK**. This password is required to log in to the management interface of the instance.

> **Note**
>
> You cannot provision the instance with the user name *admin* as it is a reserved name. However, to get admin access after provisioning the instance, use *admin* as the user name and the password created while provisioning the instance. If you use the user name created while provisioning the instance, you get read only access.

5. Choose the instance in which you want to run the image. Choose the instance type depending on your requirement as shown in the following.

- Instance type D3_V2 for max uni-directional throughput of 200 Mbps with 16 max virtual paths/branches.
- Instance type D4_V2 for max uni-directional throughput of 500 Mbps with 16 max virtual paths/branches.
- Instance type F8 standard for max uni-directional throughput of 1 Gbps with 64 max virtual paths/branches.
- Instance type F16 standard for max uni-directional throughput of 1 Gbps with 128 max virtual paths/branches.

6. From Citrix SD-WAN 11.0.3 release onwards, by default 120 GB of OS Disk Size is allocated. If necessary, you can modify the disk size to a value between 40 GB to 999 GB.
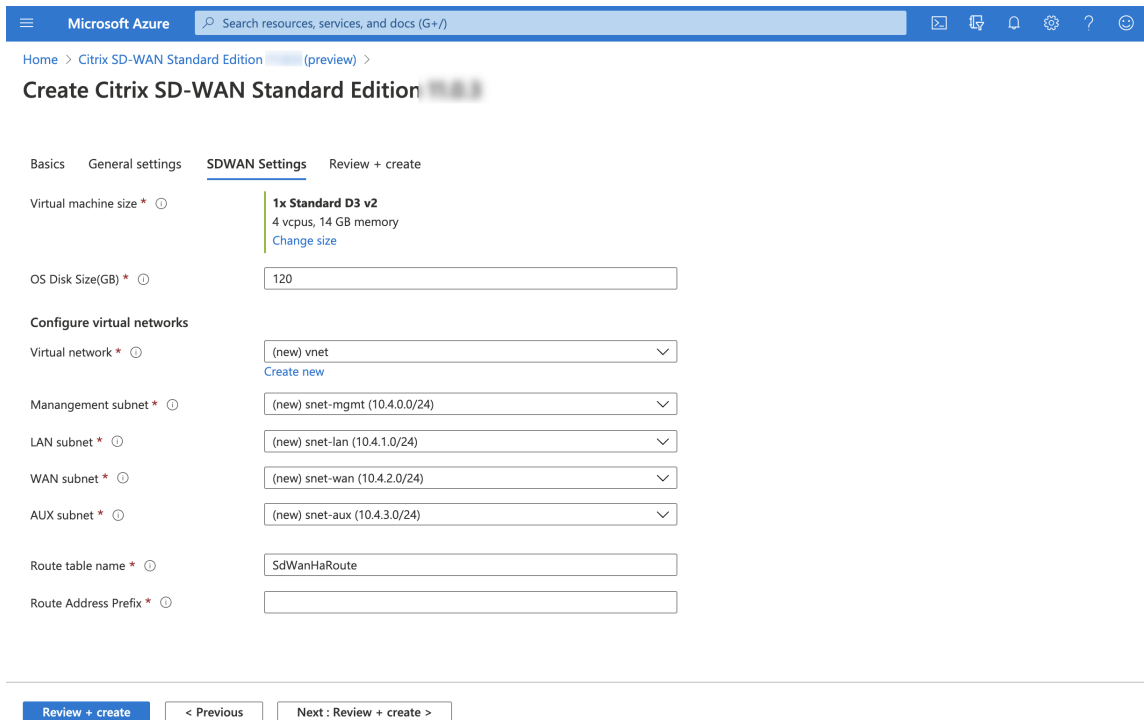
7. Create a new Virtual Network (VNET) or use an existing VNET. It is the most critical step for deployment as this step chooses the subnets to be assigned to the interfaces of the SD-WAN VPX VM.
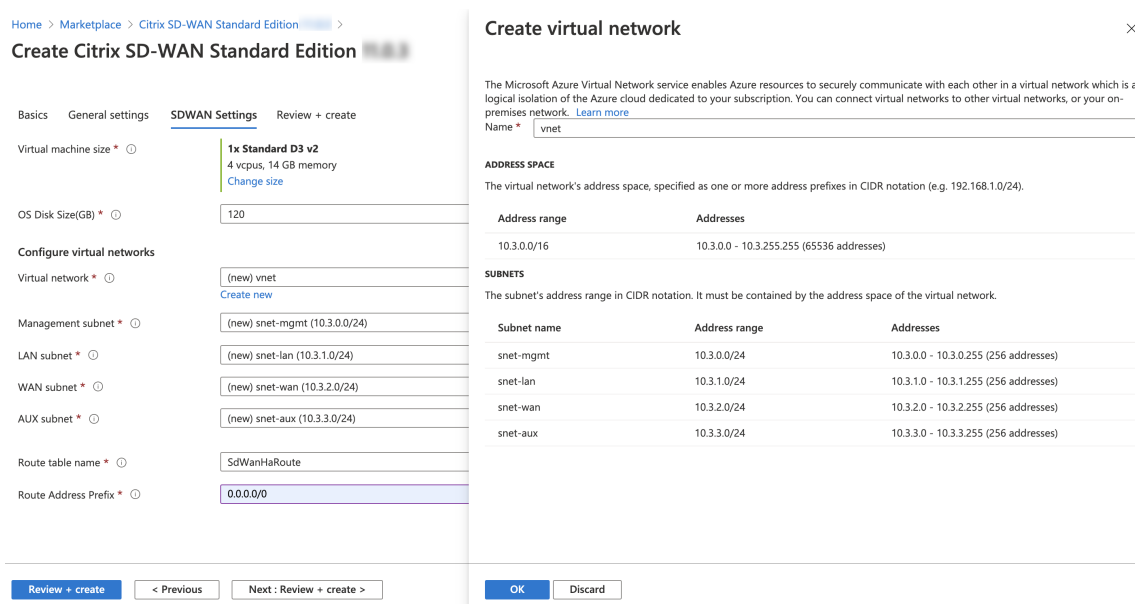
8. You can assign the required subnets to each of the interfaces in the VM. The ordering for assigning subnets is Management, LAN, WAN, and AUX respectively. Choose as required and click **OK**. In the following image, you are assigning the subnets to each of the interfaces.

NIC	Associated network
NIC 0 (default)	Management subnet
NIC 1	LAN subnet
NIC 2	WAN subnet

9. Click **Review+Create** and ensure the validation is passed.

The deployment starts and you can view the status in the notifications section.

10. You can get more details of your deployment by going to the resource group in which you are creating the deployment.
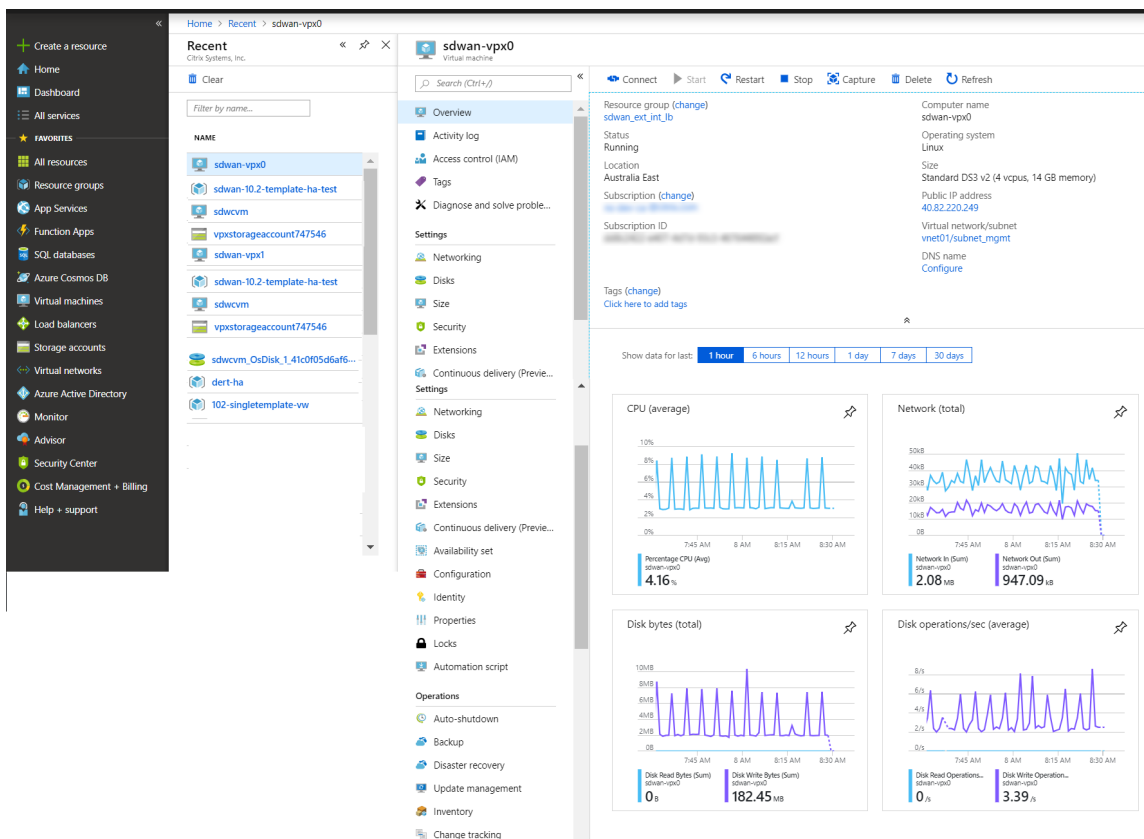
11. After provisioning, a public IP address for the management interface is auto created. Use the Public IP address to access the SD-WAN GUI.
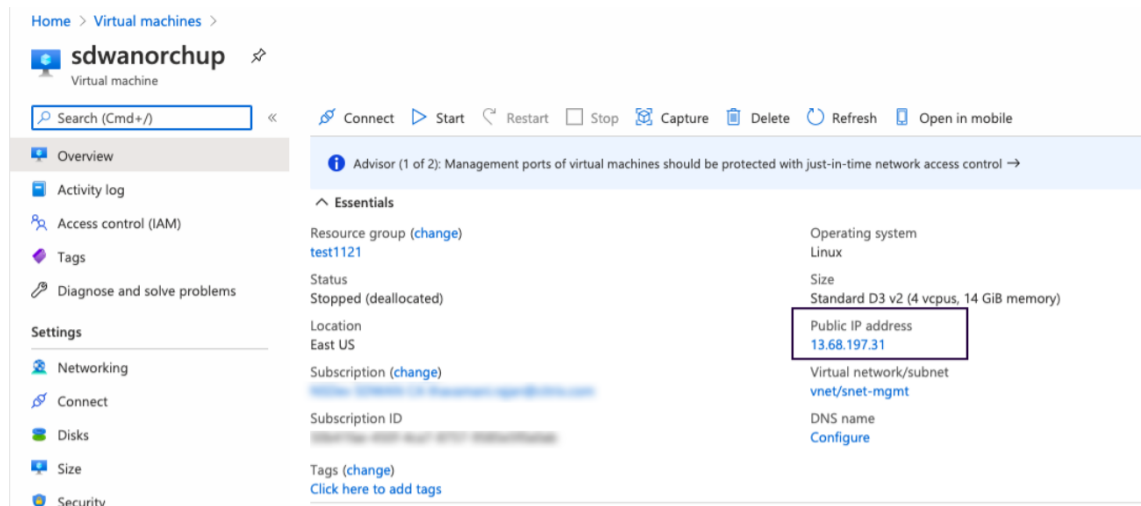
12. To get admin access to the instance, use *admin* as the user name and the password created in the first step.
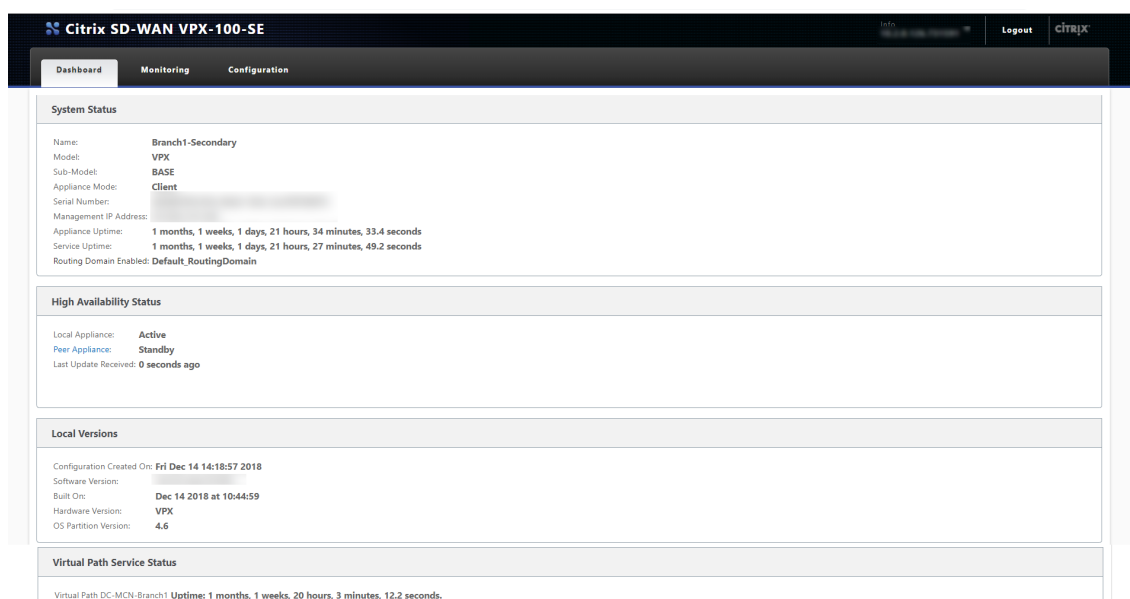
13. After you log into the GUI, notice that the virtual service is disabled because SD-WAN on Azure works on a BYOL (Bring Your Own License) model. Apply the license through the licensing tab, if you have the license already or order a new one by going to Citrix store.
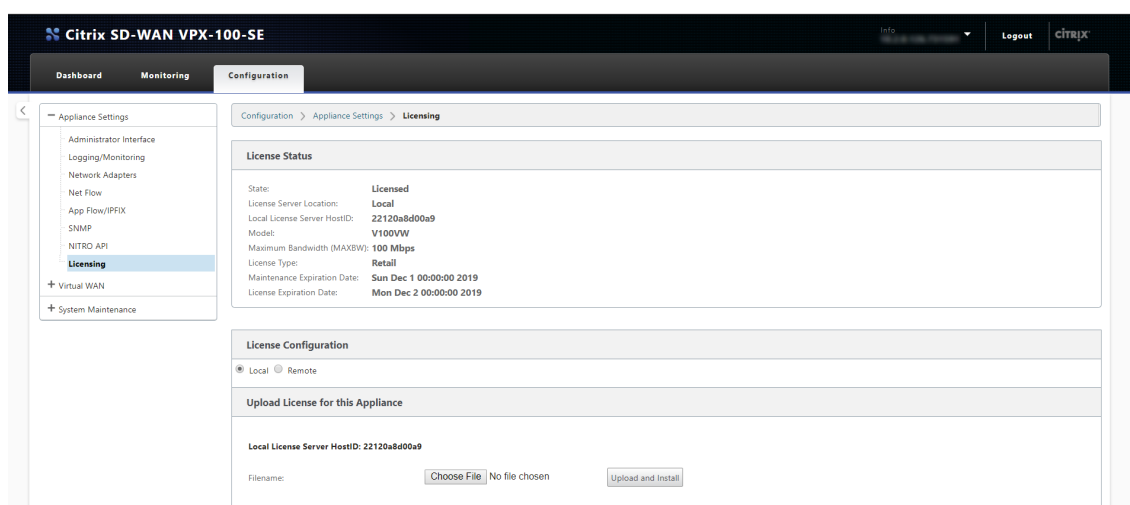
14. After the license is applied, you can apply configuration to the appliance and use it like any other branch. For more information on configuring the appliance, refer to: SD-WAN licensing

Internet breakout for Azure MCN

To configure internet breakout for Azure MCN:

1. In the MCN appliance configure DHCP IP on the WAN interface with Public IP configured for the WAN link.

2. Configure Internet service on the MCN.

3. Add an Outbound Dynamic port restricted NAT with the inside service as Internet.

4. Add a firewall policy on the MCN to allow Azure load balancer health probes on port number 500.

5. Add another load balancing rule on the Azure external load balancer for TCP on port number 80, with direct server return disabled.

6. On the end client machine that must breakout to the internet, set the route next hop IP address to the Internal Load Balancer private IP address. The load balancer IP is configured as LAN VIP in the MCN.

Troubleshooting

1. **Issue**: After logging in to a freshly provisioned Citrix SD-WAN VM created using the Azure deployment template for 11.2.3, the UI displays the following warning message:

```
Disk usage for the Active OS partition usage is at 70%
```
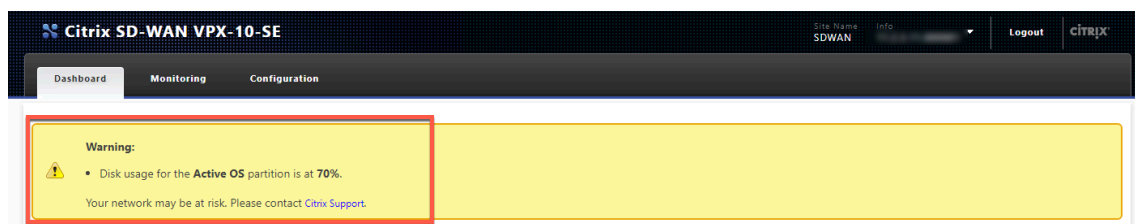

Resolution: Azure subscriptions can have a few default extensions enabled for security purposes. When an image is freshly created, `waagent` installs these plug-ins in the default path which increases the Active OS partition usage. Upgrading the software to Citrix SD-WAN 11.3 or later releases removes the warning message from the UI.

2. **Issue**: When logged into Citrix SD-WAN UI using the user name from the Azure deployment template, you get logged in as a read-only user. You can only view configuration and cannot modify any settings on the VM.

    Resolution: If you use the user name created while provisioning the instance, you get read-only access. To get admin access after provisioning the instance, use admin as the user name and the password created while provisioning the instance.

Limitations - Microsoft Azure VMs

- After a VM is created and booted in Azure, the interfaces cannot be added or deleted. The VM profile (RAM/HD/CPUs) can be changed.
- Routes are added in the Virtual WAN configuration file directing all Virtual WAN data traffic coming from the WAN to the Client/Server LAN Subnet.

Microsoft Azure supports only gateway mode for deployments. For more information about gateway mode, see gateway mode.

Citrix SD-WAN Standard Edition Virtual Appliance (VPX) high availability Support for AWS

December 4, 2020

The following procedure describes how to deploy SD-WAN virtual (VPX) appliances in high-availability mode on the AWS cloud.

Points to consider when deploying SD-WAN VPX high availability appliances in the AWS Cloud.

---

1. AWS does not support GARP (Generic Attribute Registration Protocol), VLAN or L2 related functionality, such as promiscuous mode and bridging. This is because two VMs belonging to different customers can be scheduled on the same host sharing NICs.
2. L2 requires the switch appliance to be configured and these are not exposed to AWS users.
3. SD-WAN appliance high availability model depends on GARP. When failover occurs, the new primary appliance sends GARPS out for VIP addresses.
4. AWS takes a new approach for high availability failover. A new concept of ENI (Elastic Network Interface) is introduced. ENI is an entity which stands for Network Interface which has attributes like the IP address, MAC address, Security Group, and Port Rules.
5. You can move ENIs from active or inactive Instance to another active or inactive Instance.
6. The Instance must be capable to handling the hot plug of interfaces.
7. Each Instance type has limitations on the number of ENIs associated and number of IPs per ENI.
8. AWS design for high availability failover involves Instances communicating with the external server to call Query API AWS servers.
9. The AWS servers are traditional HTTP servers. A request is sent from an instance to the Query API server to get or post information regarding an Instance/subnet/VPC or any other attribute on the AWS.
10. For the cloud platform setup, the shared base MAC address configuration is ignored and has no significance.

Deploy Citrix SD-WAN standard edition VPX in high availability mode using cloud template

For more information,refer to the EBS best practices and Must-know best practices for Amazon EBS encryption

- For defining Security groups the policy must look like the following:
  - Outbound: Allow All traffic
  - Inbound:
  - SSH from all IP addresses / subnets from where management IP will be accessed.
  - All traffic from your AWS VPCs (private IPs)
  - All traffic from the WAN side public IPs of Citrix SD-WAN peer appliances hosted on prem or in cloud.
    From 11.3 release onwards, Citrix SD-WAN has introduced support for the M5 and C5 instances. The newer AWS regions such as Hong Kong and Paris only support M5 and C5 instances.

The M5 and C5 instances have improved hardware performance and are designed for higher demanding workloads. The M5 and C5 instances deliver better price/performance than the M4 instances on a per-core basis.

> **NOTE**
>
> - The M5 and C5 instances are supported from a fresh provision of 11.3 and higher version only. To keep using the M5 and C5 instances, you cannot downgrade from 11.3 version since the M5 and C5 instances are not supported on any firmware version prior to 11.3 release.
>
> - Instances provisioned with 10.2.4/11.2.1 versions, AMIs cannot change their instance type to M5/C5.

Deploy SD-WAN standard edition VPX in high availability mode using cloud template

SD-WAN high availability solution template is published in the AWS marketplace, you can subscribe and use the **CloudFormation** template to deploy the HA setup.

Prerequisites

Before launching the **CloudFormation** template, you need to have VPC, subnets, route tables created for Management, LAN, and WAN network. To create and define the subnets and route tables (if not created), refer Installing SD-WAN VPX Standard Edition AMI on AWS topic.

To deploy SD-WAN standard edition VPX in high availability mode using cloud template:

1. Go to AWS marketplace and click **Pricing** tab. Select the **Region** from the drop-down list and specify the **Fulfillment Option** as **High Availability Mode** deployment. Click **Continue** to Subscribe.
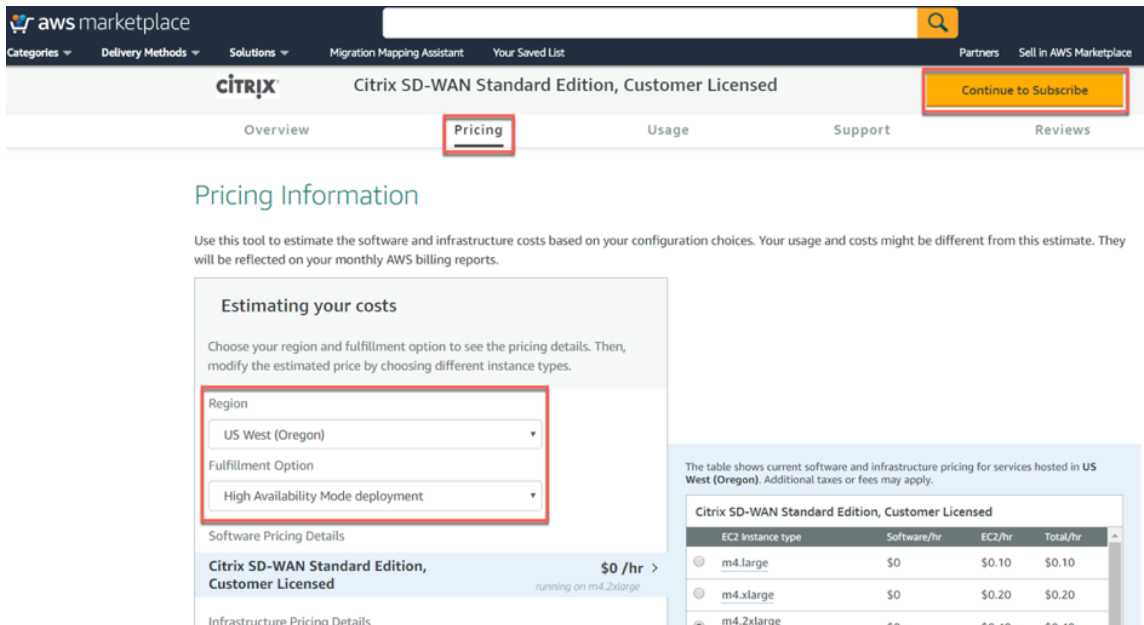
2. Click **Continue to Configuration**.

---

3. Specify **Fulfillment Option** as **CloudFormation Template** and **High Availability Mode Deployment** from the drop-down list. Select **Region** and click **Continue to Launch**.

4. Choose action as **Launch CloudFormation** in the launch software window and click **Launch**.
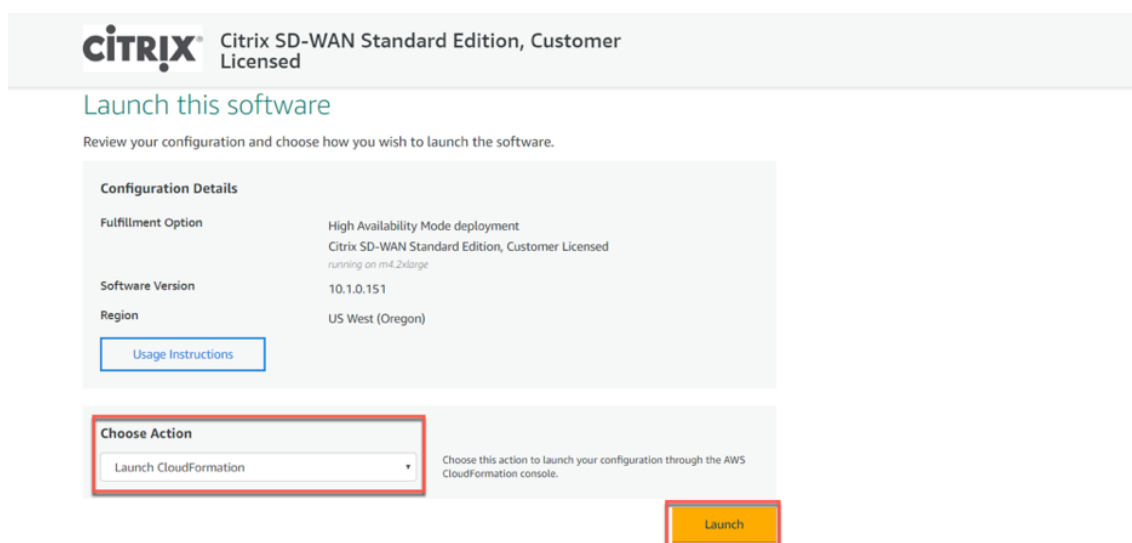
5. In the **Create Stack** window, the predefined **S3 template URL** appears during the **CloudFormation**. Click **Next**.
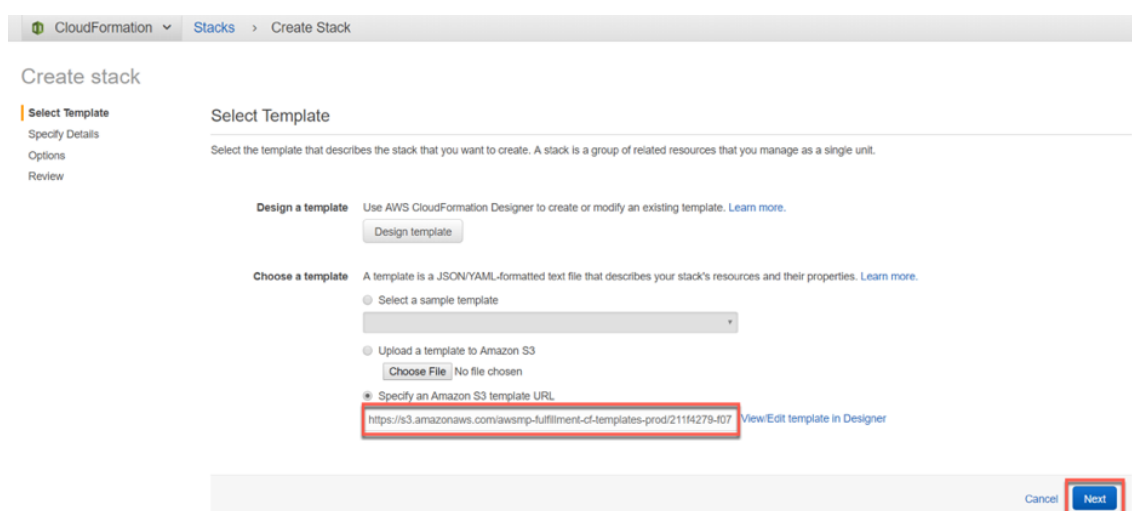
6. Specify a **Stack** name in the **Specify Details** section.

7. Configure **Virtual Private Network Configuration**. Fill in the following parameter details:

   - **VPC ID**: Provide the virtual private cloud ID.

   - **Remote SSH CIDR IP**: Provide the IP address range that can SSH to the EC2 instance (port 22).

> **Note**
>
> It is recommended to allow SSH only from the known IP addresses.

- **Remote HTTP CIDR IP**: Provide the IP address range that can HTTP to the EC2 instance (port80).

- **Remote HTTPS CIDR IP**: Provide the IP address range that can HTTPS to the EC2 instance (port 443).

- **Key Pair**: Provide a name of an existing EC2 KeyPair to enable SSH access to the instances.

Parameters

Virtual Private Network Configuration

VPC ID		
	Vpcld of your existing Virtual Private Cloud (VPC)	
Remote SSH CIDR IP		The IP address range that can SSH to the EC2 instance (port: 22).
Remote HTTP CIDR IP	0.0.0.0/0	The IP address range that can HTTP to the EC2 instance (port: 80).
Remote HTTPS CIDR IP	0.0.0.0/0	The IP address range that can HTTPS to the EC2 instance (port: 443).
Key Pair		Name of an existing EC2 KeyPair to enable SSH access to the instances

8. Configure **Network Interfaces** which must be attached to the instances created. Note that the Primary IPs are for the primary instance of the high availability pair and Secondary IPs are configured for the secondary instance of the high availability pair.

Network Interface Configuration

Management Subnetwork		
	SubnetId of an existing subnet in your Virtual Private Cloud (VPC) dedicated for management IP	
Primary Management IP		Private IP assigned to the Management ENI of Primary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.
Secondary Management IP		Private IP assigned to the Management ENI of Secondary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.
LAN Subnetwork		
	SubnetId of an existing subnet in your Virtual Private Cloud (VPC) dedicated for LAN side	
Primary LAN IP		Private IP assigned to the LAN ENI of Primary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.
Secondary LAN IP		Private IP assigned to the LAN ENI of Secondary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.
WAN Subnetwork		
	SubnetId of an existing subnet in your Virtual Private Cloud (VPC) dedicated for WAN side.	
Primary WAN IP		Private IP assigned to the WAN ENI of Primary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.
Secondary WAN IP		Private IP assigned to the WAN ENI of Secondary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.
HA Subnetwork		
	SubnetId of an existing subnet in your Virtual Private Cloud (VPC) dedicated for HA side	
Primary HA IP		Private IP assigned to the HA ENI of Primary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.
Secondary HA IP		Private IP assigned to the HA ENI of Secondary Instance. Last octet has to be between 5 and 254. Leave empty for automatic assignment.

9. Configure other Parameters such as **Instant Type** and **Tenancy Type** and click **Next**.

> **NOTE**
>
> If any validations fail, AWS notifies you and would not let you proceed until the errors are resolved.

10. Set Tags. These tags are AWS-specific options which are user configurable.

11. Configuring the IAM role is not recommended. This is already created by the customized IAM role, which is done through the **Cloud Formation** template.

12. After clicking next, Review the template and acknowledge the custom IAM role which has been created by **Cloud Formation** template. Proceed with **Create**.

13. The new stack that you created appears on the **Cloud Formation Stacks** page. After successful template upload, Monitor the status of the template.

14. Monitor the events of all the resources created by the **Cloud Formation** template. If there is any failure, detailed descriptions of events are generated by AWS which helps in debugging the issue. The Events appear as follows:

15. After successful stack creation, the status of the template appears as **Create_Complete**.

16. Navigate from AWS console to **Services > EC2 > Instances**. You can see two instances **SDWAN-Primary** and **SDWANSecondary** instances created, up and running with Elastic IPs associated with the instances.

17. Select **SDWANPrimary** instance. You can notice all the resources rightly assigned to the instance, Security groups, Elastic IP, IAM role, and four Network Interfaces. Failed to create any high availability functionality might not work as expected.

18. Similarly select **SDWANSecondary** instance and verify the above resources.

Secondary floating IPs for LAN and WAN links

You need a secondary floating IPs for LAN and WAN links for the high availability to work. Once the stack is created, assign new secondary private IPs to the LAN and WAN interfaces of the active EC2 instance. These secondary configured IPs are used while configuring virtual IP addresses in VPX.

Perform the following procedure to attach the secondary LAN IPs to the active instance:

> **Note**
>
> Once the HA solution is deployed, we have to assign secondary floating IP only to the primary instance.

1. Navigate to Services > EC2 > Instances.

---
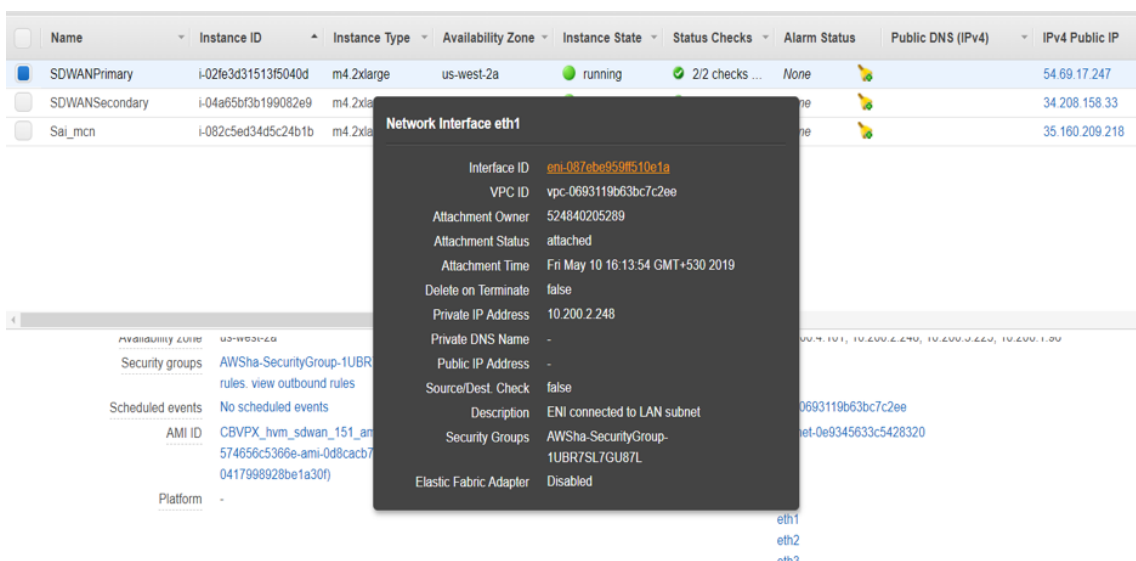
2. Navigate to **Services > EC2 > Network interfaces** and select the LAN/WAN Elastic Network Interfaces (ENI) of the primary instance.

3. Assign new secondary IP.

4. Click **Yes, Update**.

5. Similarly create secondary private IP for the WAN interface as well.

Public IP on WAN link

A public IP required on the WAN link to communicate with the external world. Perform the following steps to associate elastic IP to the WAN ENI interface:

1. Navigate to **Addresses > Allocate new address**.

2. Select the elastic IP created, and click **Action > Associate** address and associate the public to the secondary private WAN IP which we just created.

3. Verify final interfaces and IPs are expected as below:

   • Primary Instance:

- Secondary Instance:

Now the instance provisioning is completed. Configuring SD-WAN high availability appliance is almost similar to configuring standalone appliance. Differences are listed below:

- While creating LAN and WAN Virtual IP interfaces, specify the secondary private IPs created. And for the high availability virtual IP interface, specify a dummy IP in the high availability network.
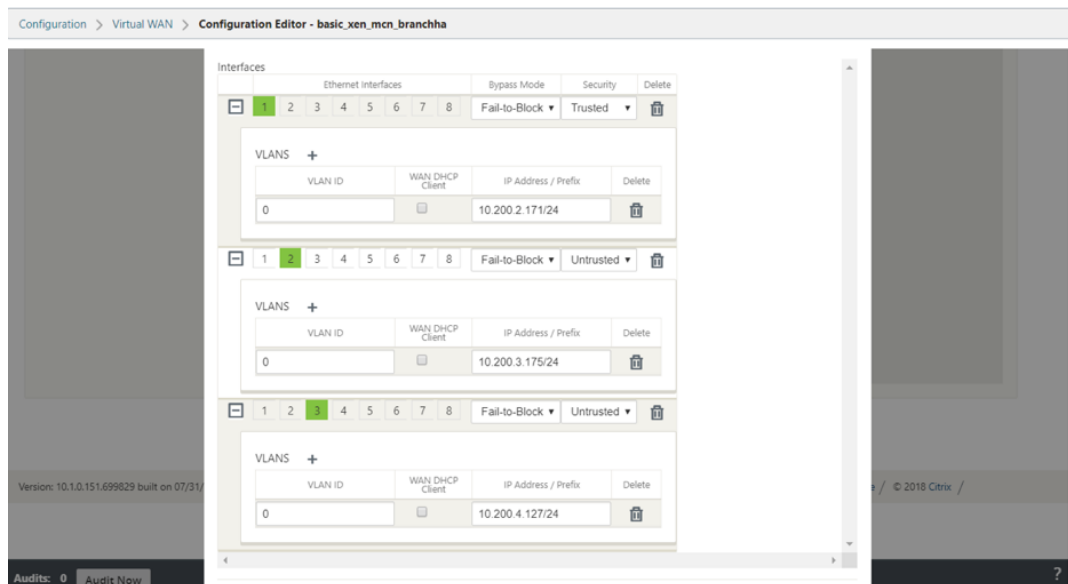
- Enable high availability and specify the high availability interface IPs of the active and secondary instance.
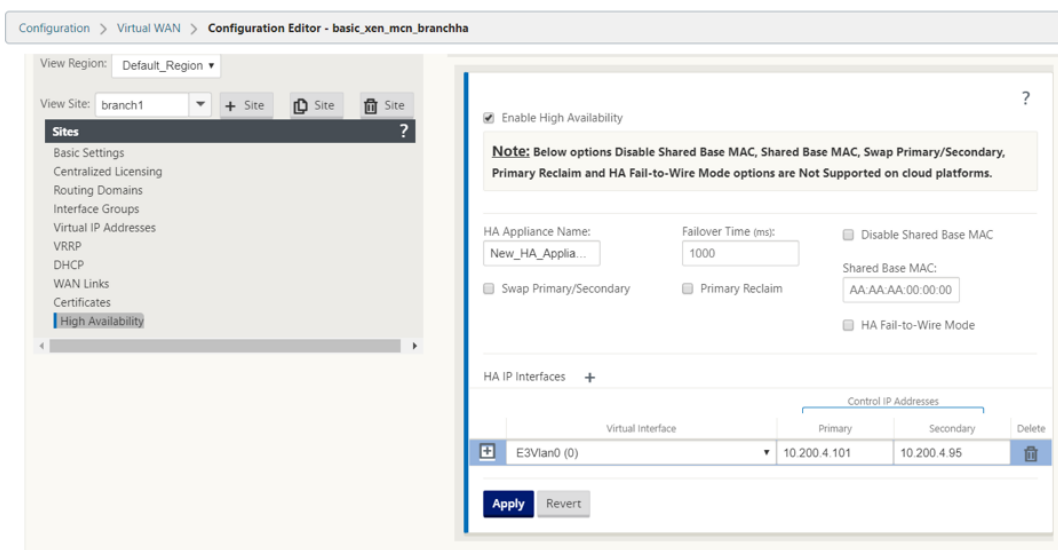
You can verify the high availability status.

How to configure high availability Fail-Over for any SD-WAN instance running on AWS

Set up high availability peers with one high availability peer with three or more ENIs, and 1 high availability peer with an equal number of ENIs. In both Peers, the first ENI is dedicated to Management. One high availability peer owns all Traffic ENIs. During a Failover, the traffic ENIs move from the failing instance to the new Primary instance.

For example, it can take up to or more than 20 secs to move two traffic ENIs. AWS do not have SLAs on API response and you cannot have one for high availability fail-over time.

Note

The AWS design has a limitation of instances dependent on the AWS servers to respond for attach and detach. The fail-over time is unpredictable.

Configuration steps

1. Acquire information about your high availability Peer Instance about information on the number of ENIs associated and details of ENIs associated using the REST API.
2. Detect the condition of the failing instance.
3. Call Detach of ENIs from failing instance using REST APIs.
4. Ensure all ENIs associated are detached.
5. Attach ENIs to the current Primary instance.
6. Ensure All ENIs are attached.
7. Trigger upper layers to detect that new ENIs are in place.
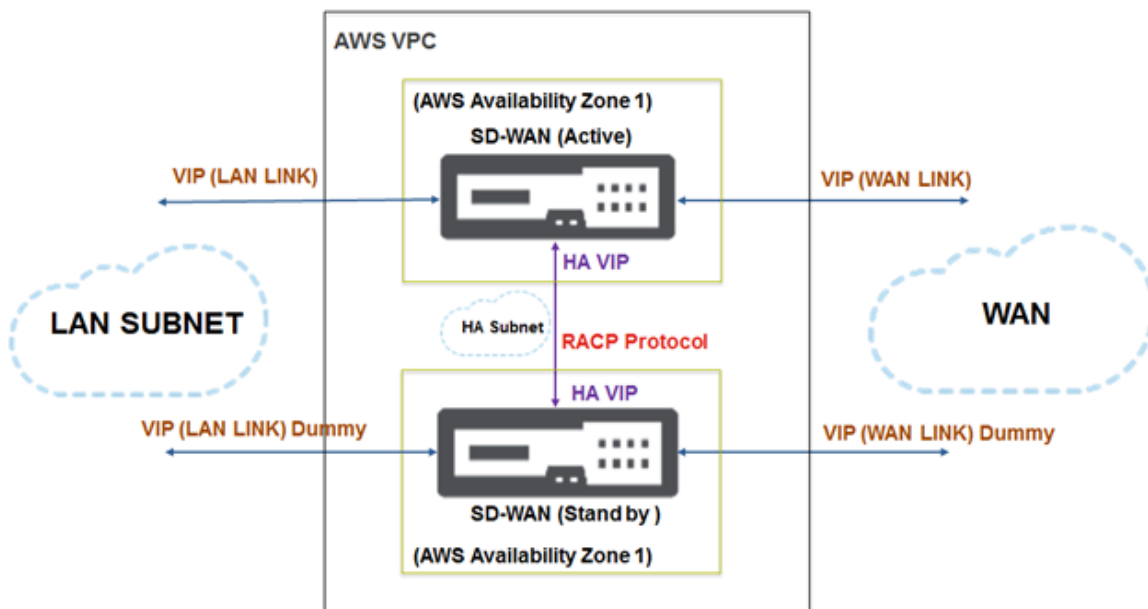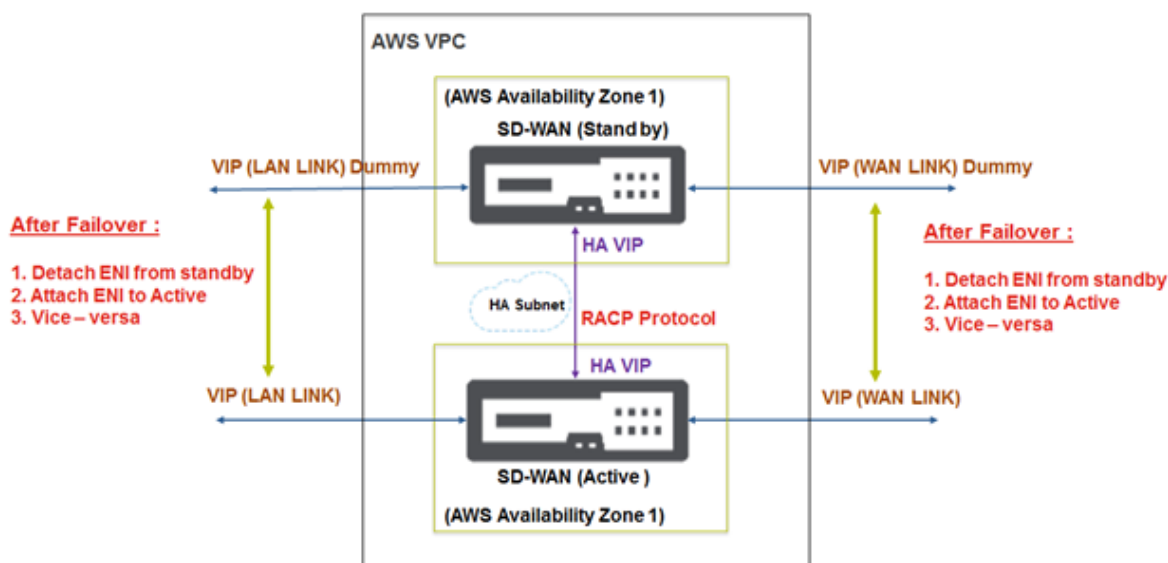
How to configure SD-WAN VPX-SE in a single AWS Virtual Private Cloud (VPC) Subnet or between regions with Public WAN link IP address

In AWS VPC, for an active SD-WAN instance, another high available SD-WAN instance running in the same VPC is released.

1. The links configured are the same between active and stand-by SD-WAN appliances.
2. For AWS, you can create a subnet and a dedicated link for the RACP protocol to communicate between the SD-WAN appliances.
3. In the SD-WAN GUI, configure the following:
   - Create an interface group. Name it as high availability-LINK. Add the interface used for high availability.
   - Create a Virtual IP address for the Interface group.
   - In High Availability Node, Enable high availability and add control Virtual IPs which the RACP protocol uses for communication. Ensure that the IP addresses are same as the configured IP addressed while creating network interfaces in AWS.
   - Perform Change Management and download the active configuration for the stand-by SD-WAN appliance.
   - After applying configuration through local change management on the stand-by SD-WAN appliance, you will see heartbeats exchanged between active and stand-by SD-WAN high availability appliances.
   - When failover occurs, you see SD-WAN appliance transitioning from stand-by to active modes and/or conversely without any configuration loss.

Note

1. AWS supports high availability mode with features such as Elastic Load balancing and auto-scaling where the challenge is to sync configuration within the SD-WAN appliances. In this deployment, you apply the existing RACP protocol for efficient high availability.

2. Both MCN and branch site appliances can be made available in the cloud environment.

Deploy Citrix SD-WAN on AWS Outposts

November 17, 2020

AWS Outposts is a fully managed service that offers the AWS infrastructure, AWS services, APIs, and tools to virtually any data center, co-location space, or on-premises facility for a consistent hybrid cloud experience. AWS services such as compute, storage, database, and other services run locally on Outposts, and you can access the full range of AWS services available in the Region to build, manage, and scale your on-premises applications using familiar AWS services and tools.

With the addition of AWS Outposts to the AWS offering, Citrix SD-WAN customers now can use Citrix SD-WAN's hybrid-cloud solution to easily connect AWS Outposts instances to their existing WAN infrastructure. With this integration customers will be able to manage SD-WAN connectivity from branches to the
AWS cloud and Outposts using Citrix SD-WAN management tools.

- A BYOL license for Citrix SD-WAN VPX
- Minimum 40 GB storage for VPX and minimum 200 GB for VPX-L configuration
- Availability of m5 & c5 instances
- A couple of elastic IPs (for WAN interface and management interface respectively)

NOTE

You might choose not to host the management interface over a public IP.

Solution validation topology/network architecture
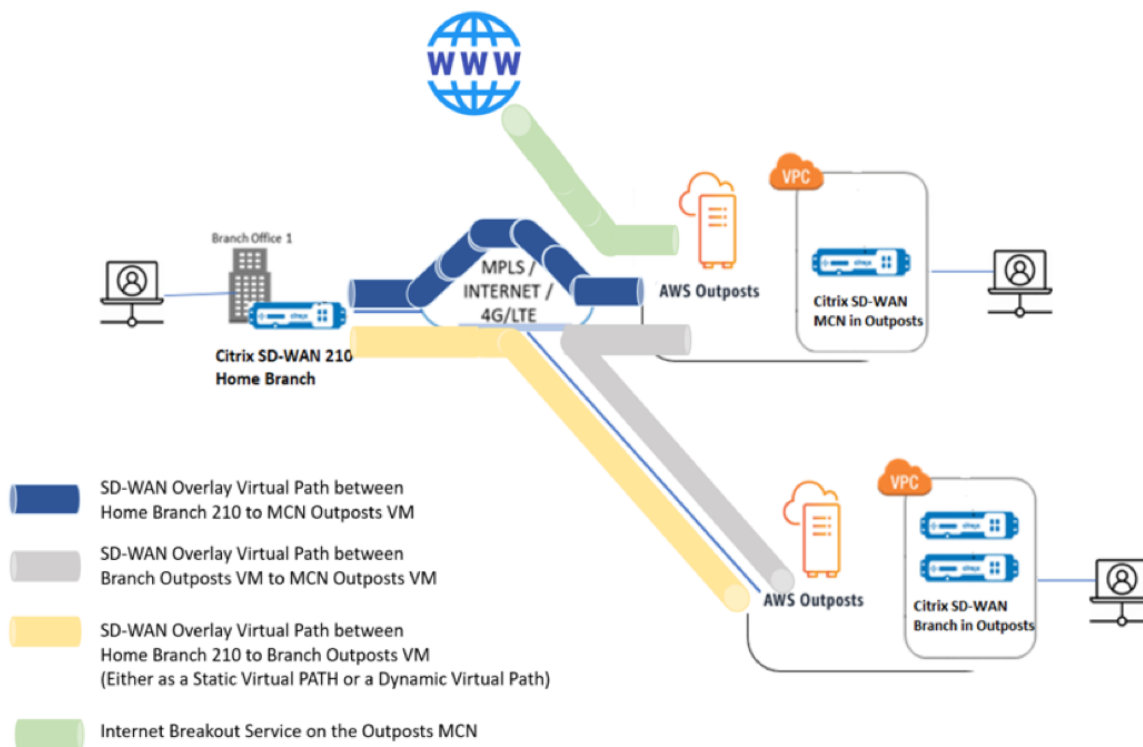
Below is the step-by-step configuration guide to provision an SD-WAN appliance in AWS Outposts.

Prerequisites

1. Log into the Outposts AWS Account.
2. Have access to the Citrix SD-WAN AMI from the market place of AWS Outposts.

NOte

All the snapshots of AWS Outpost console provided in the configuration guide are done with the new console launched by AWS and may not be looking exactly the same, if a legacy UI is selected.

Creation of VPC on Outposts for Citrix SD-WAN appliance (VPXL type)

1. Provide a CIDR block for the AWS Outpost VPC. For this configuration we use a CIDR of 192.168.100.0/22.

2. Leave all other attributes as default.

3. Provide the tag names as necessary to identify the appliance from the instance list for future.
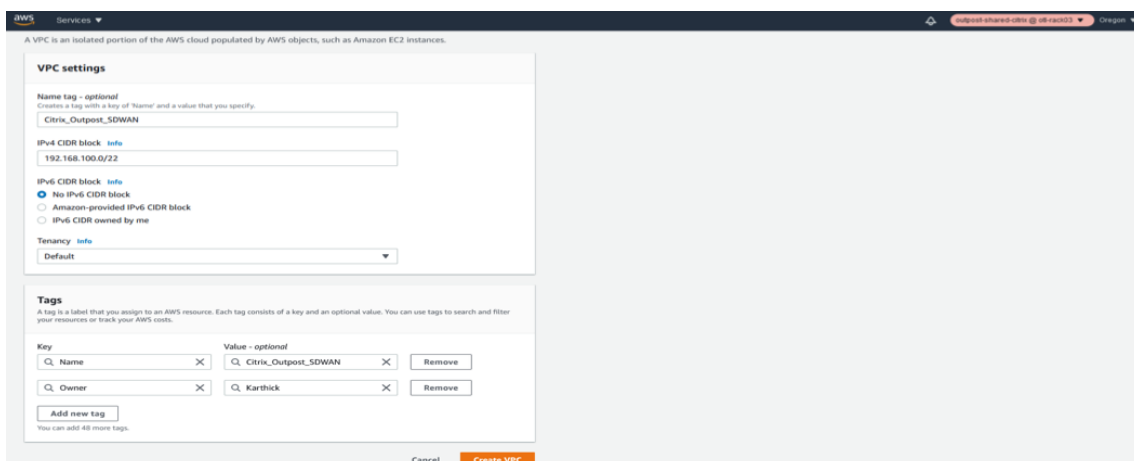
4. Verify that the VPC is created and the IPv4 CIDR details are updated and a VPC ID is obtained for the resource created.

5. The status should be **associated**.
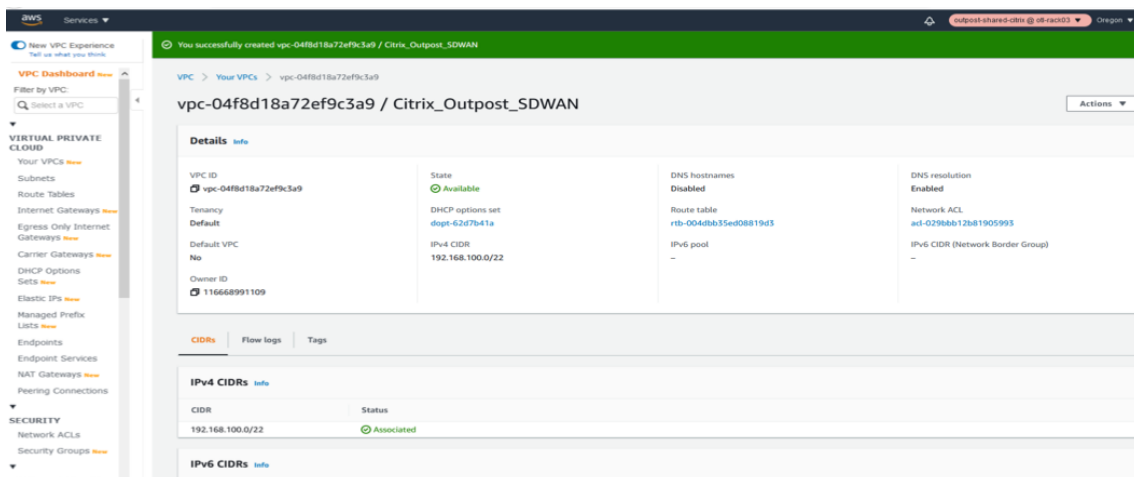
6. Once the VPC is created, the VPC list should show up the new VPC created with the CIDR details in the **Your VPCs** section of VPC AWS outposts service.
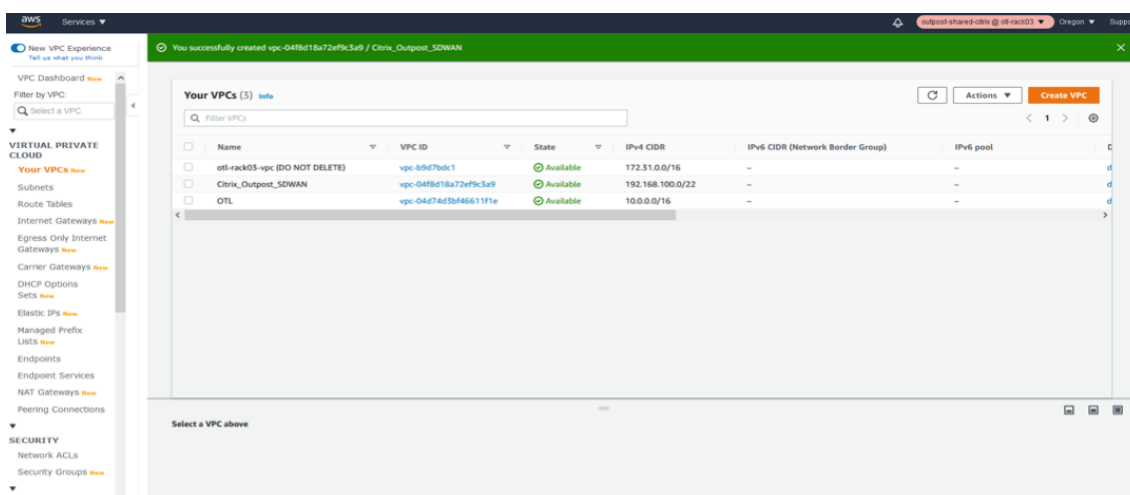
Creation of Internet Gateway and associate to VPC (Internet access for WAN and MANAGEMENT Interface of SD-WAN)

The Internet Gateway is created for the SD-WAN VPC to ensure that we have the management connectivity over the Internet and also for the WAN Link of the SD-WAN appliance to be able to form the virtual path over the Internet (Since the Azure instance hosts an Internet link)

- We create a single Internet Gateway instance for the VPC using "Internet Gateways" section of the VPC AWS Outpost service.

- Click **Create Internet Gateway**.

Create the Internet Gateway for the VPC
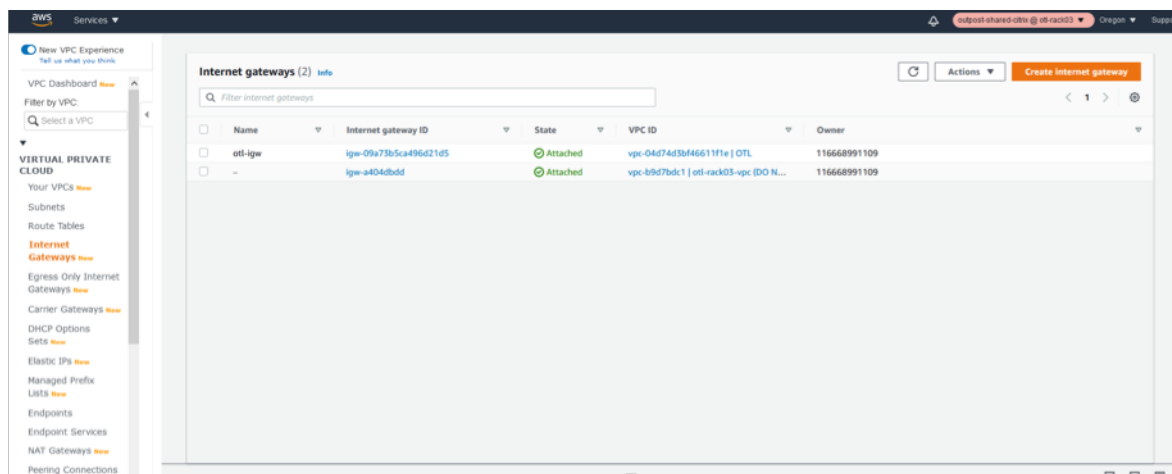
- The Internet gateway is just a resource creation and has nothing special to be configured. If needed, ensure to configure the name tag and the relevant resource tags to search for the resource among the IGW's in the list in future.

- Click **Create Internet gateway**.
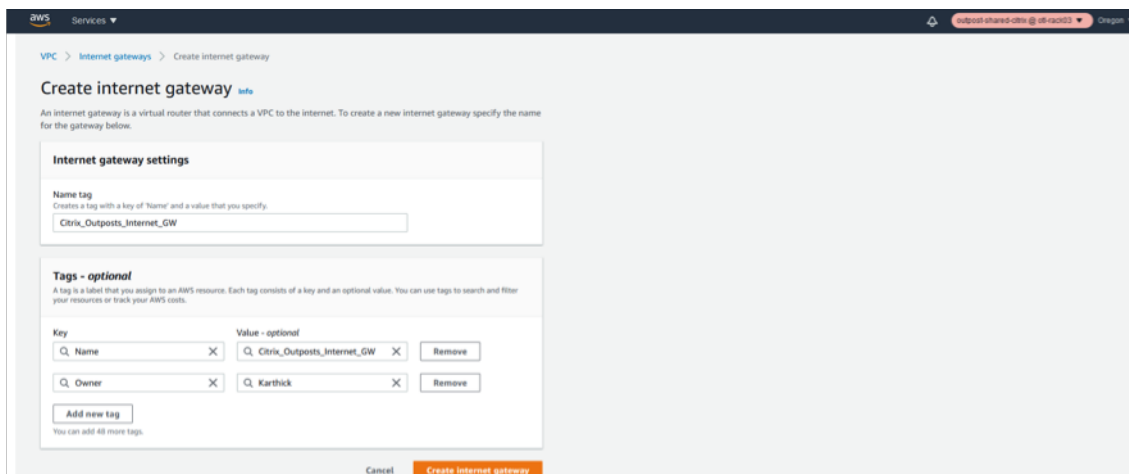
Once the Internet Gateway is created, associate the Internet gateway to a specific VPC we just created.

- Click the IGW resource and in the actions field **select Attach to VPC**.
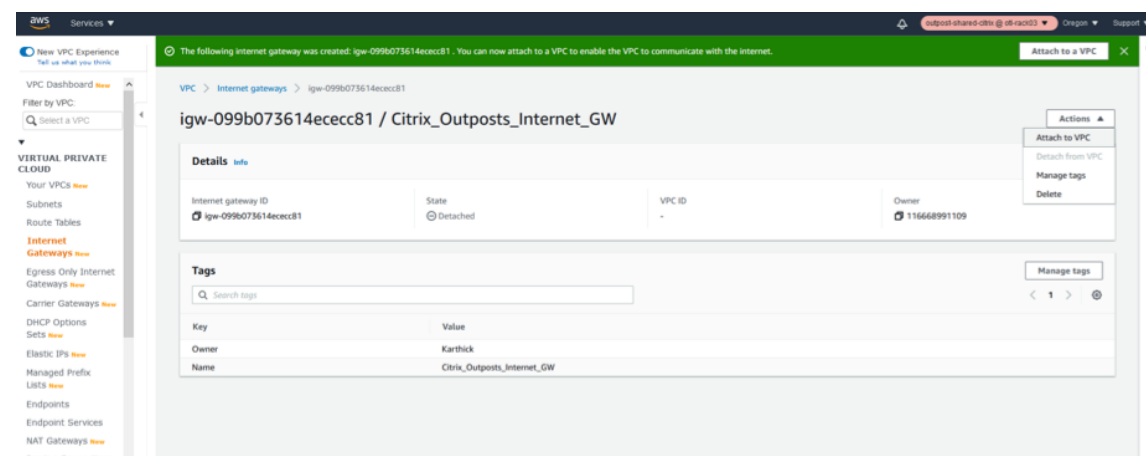
- Once the attach to VPC is clicked, select the VPC we created in step 1 which is for the SD-WAN.

- Click the Available VPC's drop-down list and select the SD-WAN VPC created.

- Click **Attach Internet Gateway**.

Associate the VPC to the Internet Gateway

319
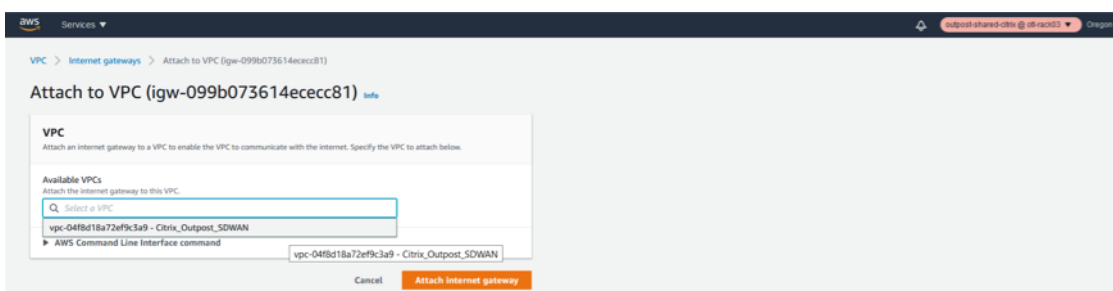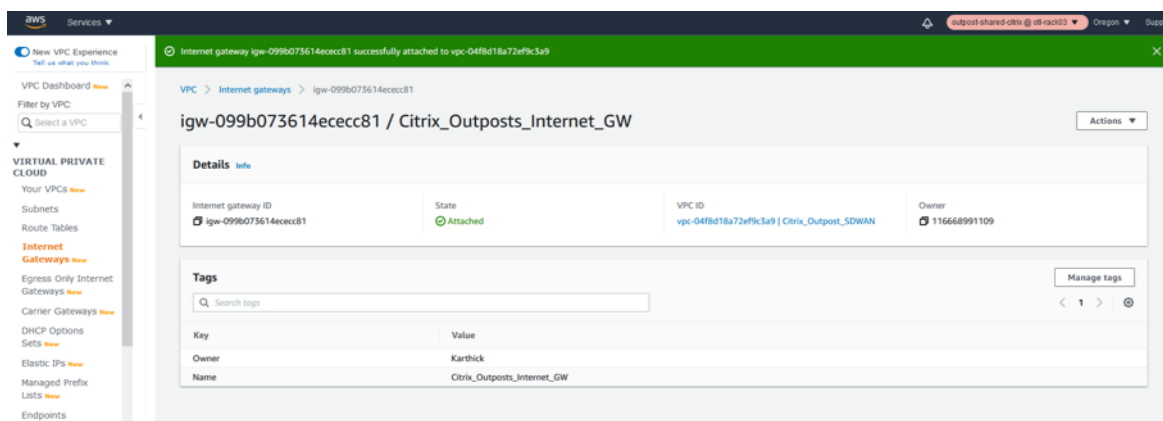
Creation of LAN, WAN and MGMT Subnets for Citrix SD-WAN VPXL appliance

The SD-WAN standalone appliance hosts 3 Interfaces in general.

1. Management Interface
2. LAN Interface
3. WAN Interface

The order of association of the interfaces also are important and the first interface that is associated is the management, followed by LAN and then the WAN subnet.

Management subnet

- Click Subnets under VPC
- Click Create subnet
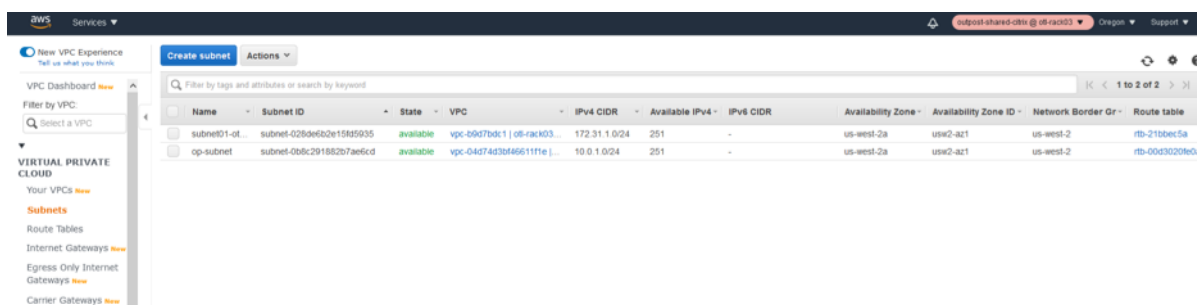
- In the subnet creation window, select the VPC created for SD-WAN as in step 1 and associate.
- Select any availability zone of your choice.
- Provide the management interface a subnet prefix from the VPC CIDR.
- For this configuration guide, the management interface will be configured with 192.168.102.0/24.
- Click create.
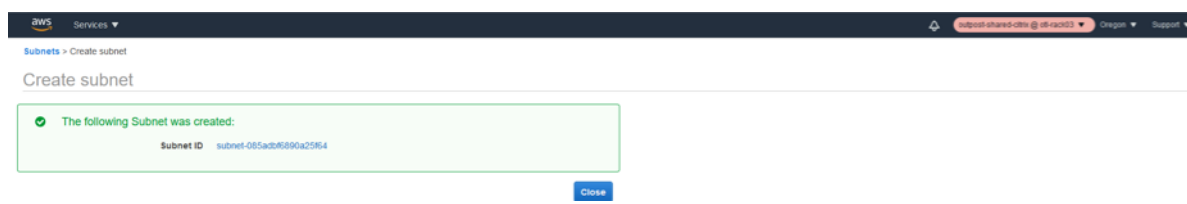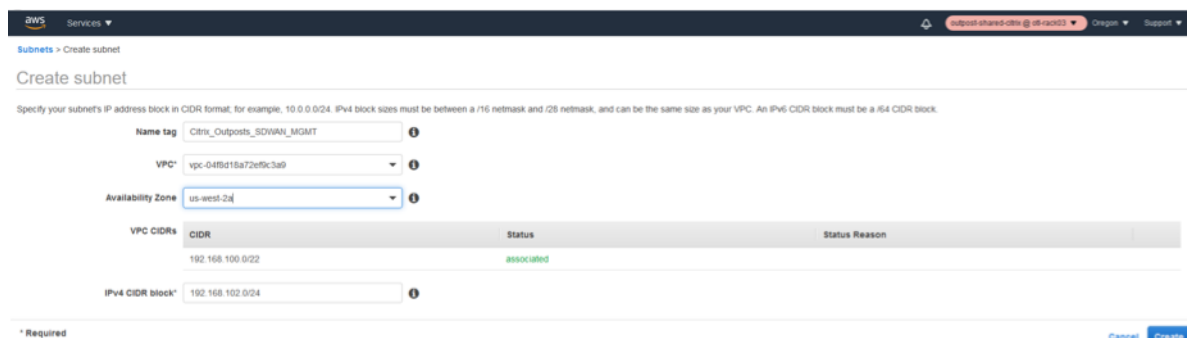
LAN subnet

1. In the subnet creation window, select the VPC created for SD-WAN as in step 1 and associate.

2. Select any availability zone of your choice.

3. Provide the LAN interface a subnet prefix from the VPC CIDR.

4. For this configuration guide, the LAN interface will be configured with 192.168.100.0/24.

5. Click **Create**.
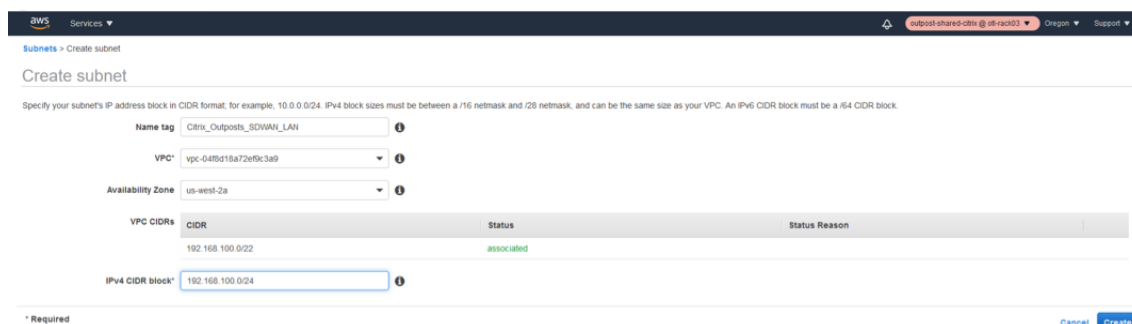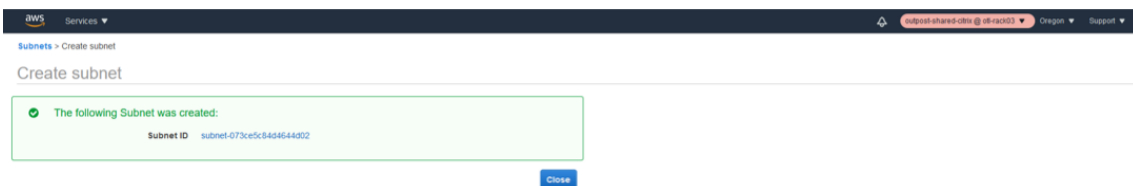
WAN subnet

1. In the subnet creation window, select the VPC created for SD-WAN as in step 1 and associate.

2. Select any availability zone of your choice.

3. Provide the LAN interface a subnet prefix from the VPC CIDR.

4. For this configuration guide, the WAN interface will be configured with 192.168.101.0/24.

5. Click **Create**.
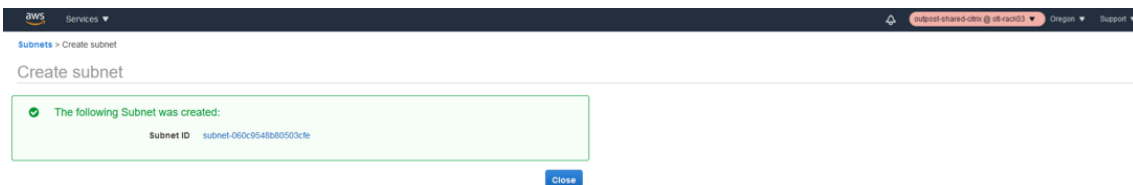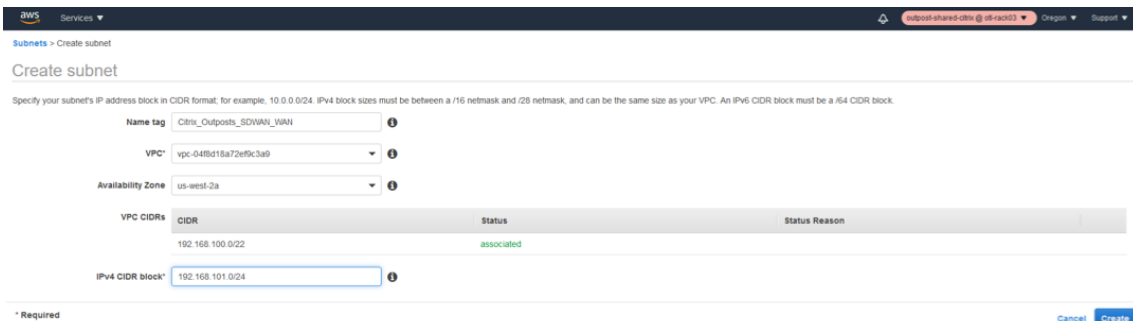
Define route tables for the LAN/WAN/MGMT Subnet

Route tables are helpful to signify routing for each subnet and we need to create the route tables for Management and WAN table so that the Internet access and the other related routes can be configured with the Internet Gateway configured.

Management subnet route table

- Click Route tables under VPC.
- Click create route table.
- Select the VPC created for SD-WAN in step 1.
- Click **Create**.

1. Create the Management route table.
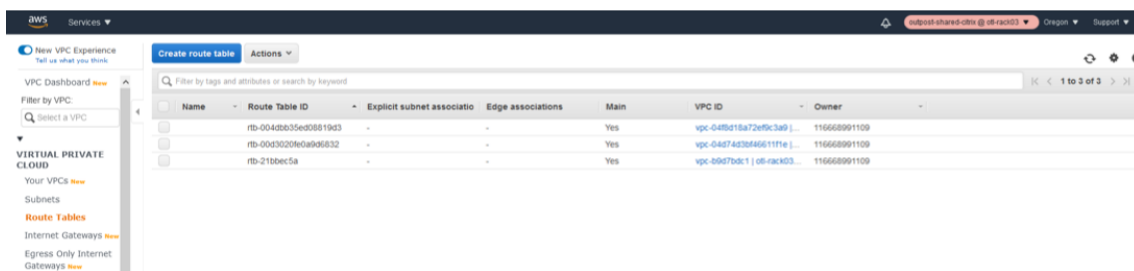
2. Associate the VPC to the management Route Table.
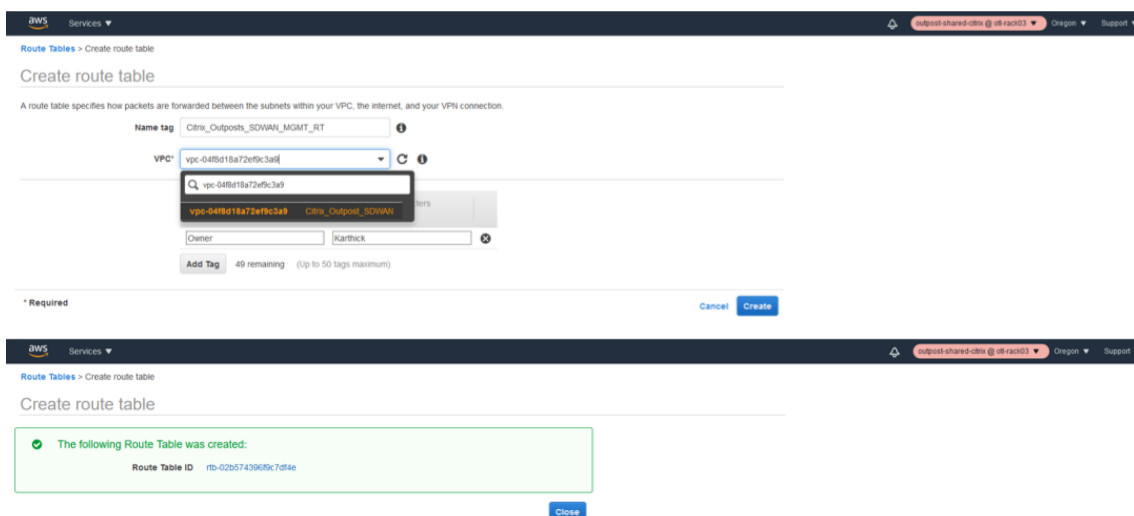
The next step is to associate the route table to the Management subnet created.

- Select the Management route table from the list.
- Click the Actions drop-down list.
- Select **Edit Subnet associations**.
- Associate the Management Subnet to the route table which hosts the IP **192.168.102.0/24**.

3. Edit Subnet Associations for management Route Table.
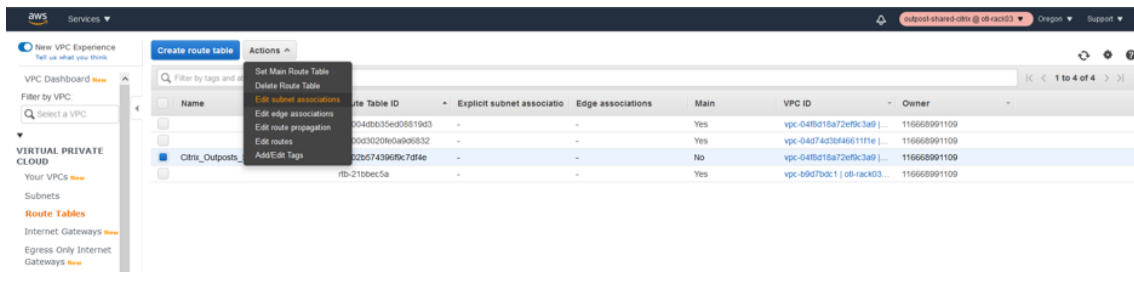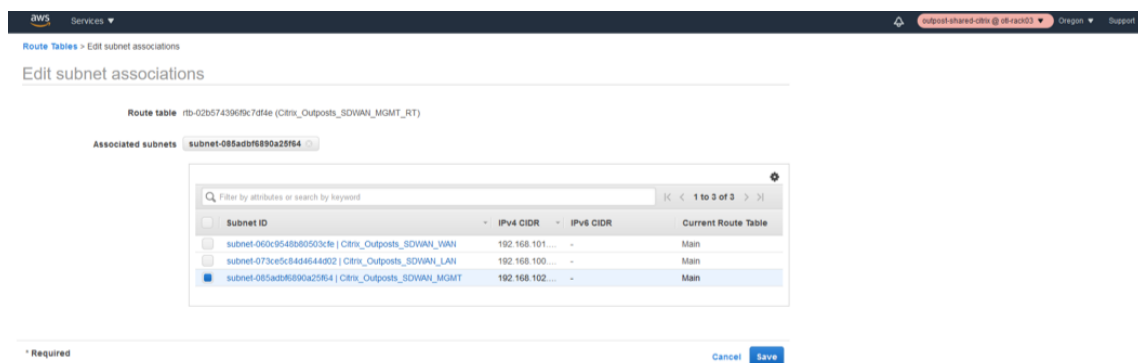
4. Add Routes for management Subnet (Default via IGW).

   Next step is to add the route to the management to reach the Internet for public Access.

   - Select the management route table.
   - Click Edit routes.
   - Provide a new DEFAULT route 0.0.0.0/0 via the IGW instance we created in step 2.
   - Save Routes.
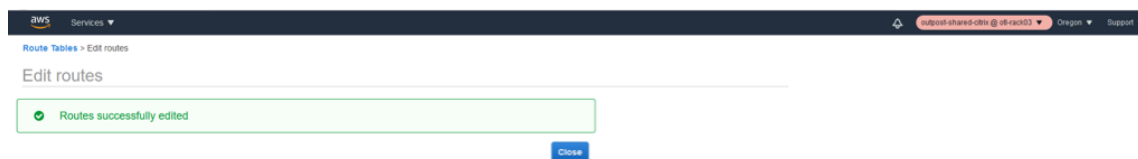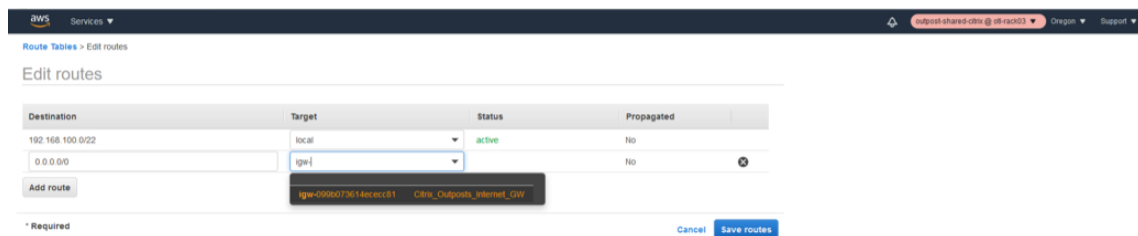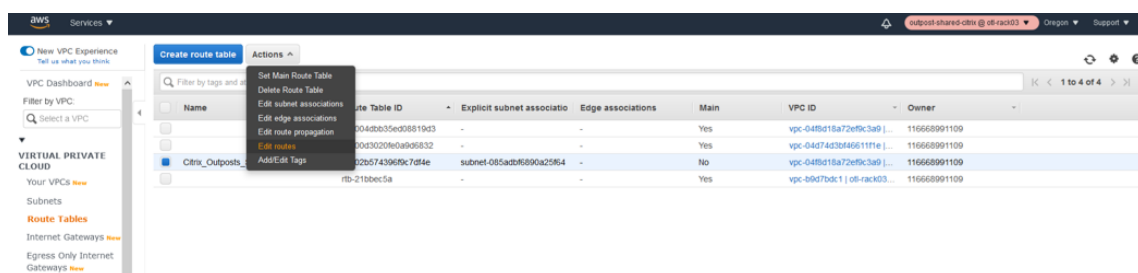
Define route tables for the WAN subnet

1. Create the Route table for WAN Interface

   - Click Route tables under VPC.
   - Click create route table.
   - Select the VPC created for SD-WAN in step 1.

324
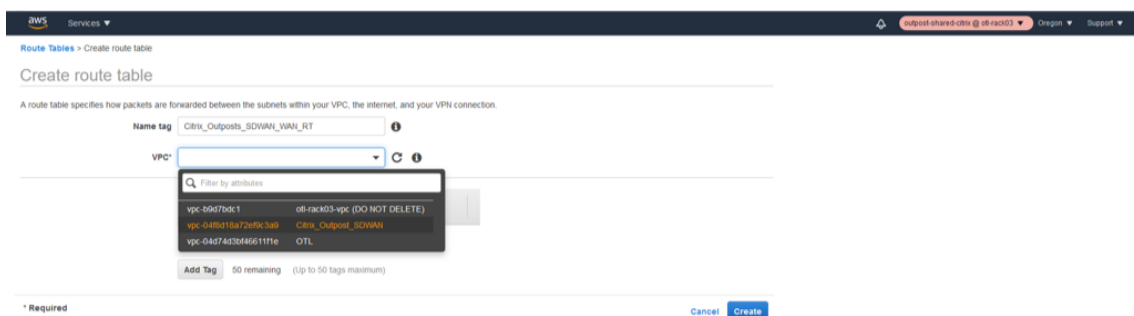
- Click **create**.

2. Associate the VPC to the WAN routing table.
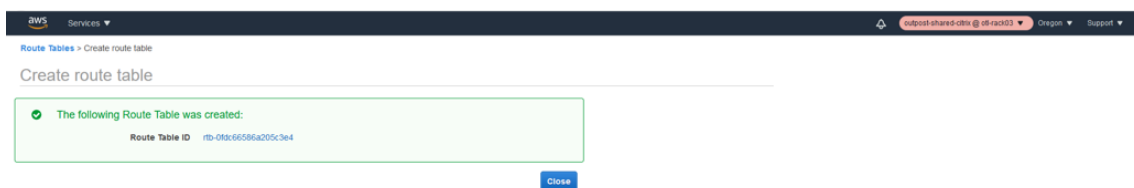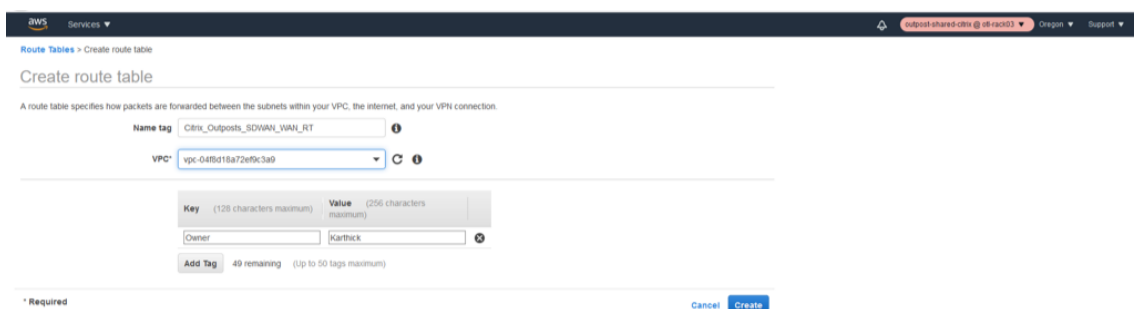
3. Edit Subnet Associations for WAN Route Table.

The next step is to associate the route table to the WAN subnet created.

- Select the WAN route table from the list.
- Click the Actions drop-down list.
- Select **Edit Subnet associations**.
- Associate the WAN Subnet to the route table which hosts the IP **192.168.101.0/24**.
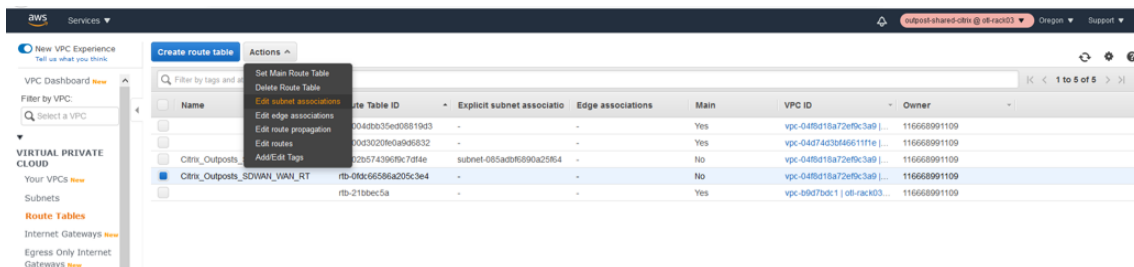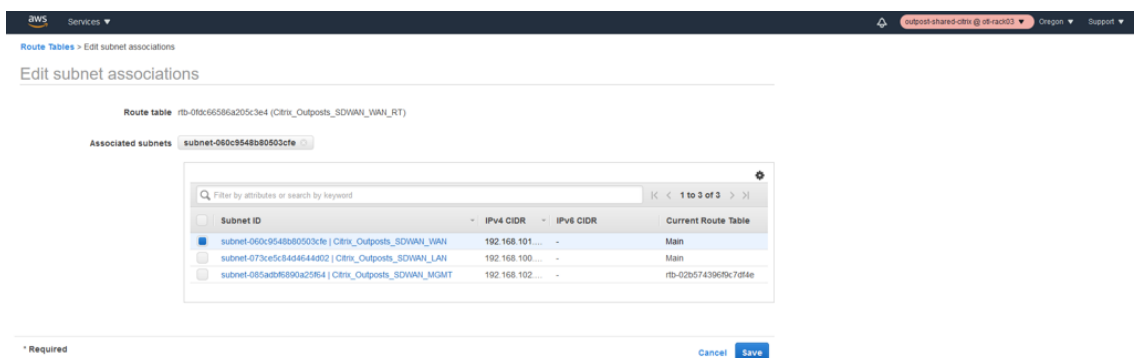
4. Add Routes for WAN Subnet (Default via IGW).

   Next step is to add the route to the WAN to reach the Internet for public Access.

   - Select the WAN route table.
   - Click Edit routes.
   - Provide a new DEFAULT route 0.0.0.0/0 via the IGW instance we created in step 2.
   - Save Routes.
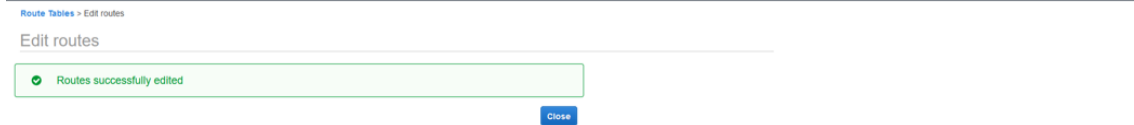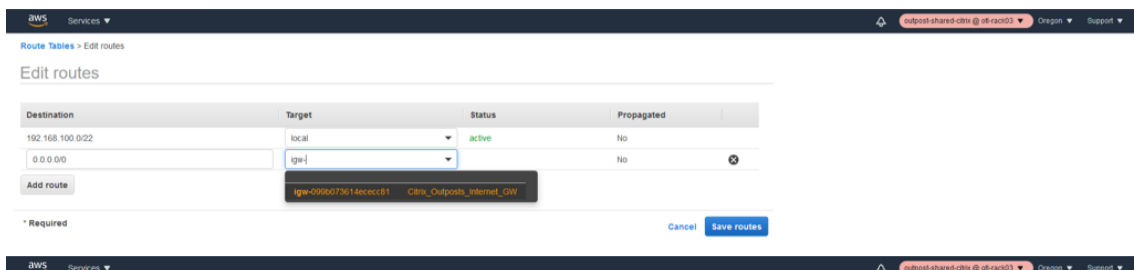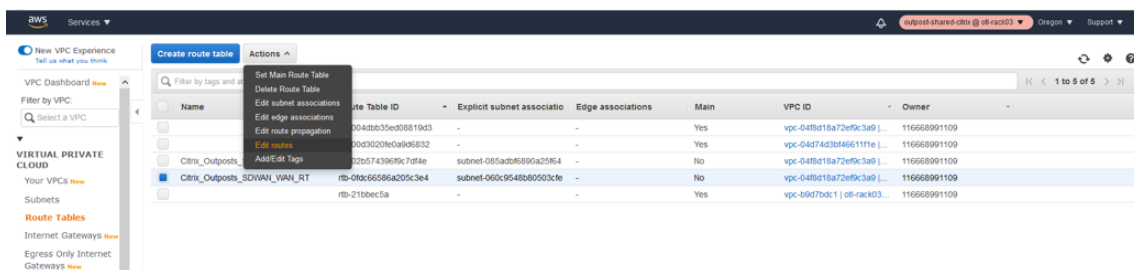
Define route tables for the LAN subnet

1. Create the Route table for LAN Interface

   - Click Route tables under VPC.
   - Click create route table.
   - Select the VPC created for SD-WAN in step 1.
   - Click **create**.
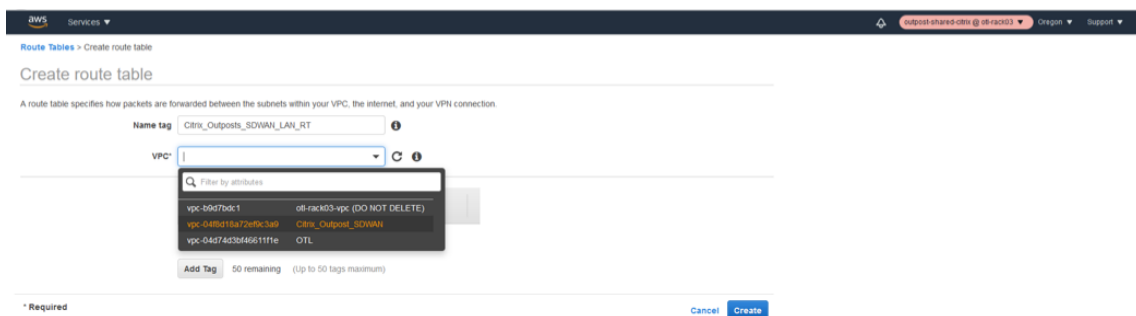
2. Associate the LAN routing table to the VPC.
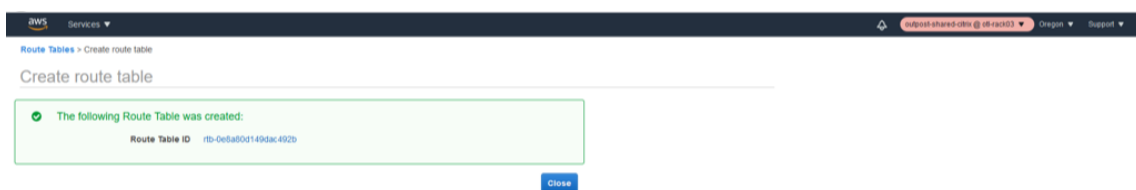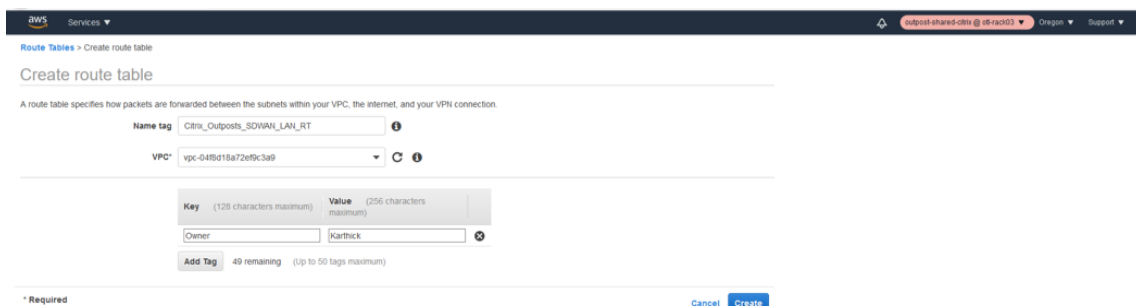
3. Edit Subnet Associations for LAN Route Table.

The next step is to associate the route table to the LAN subnet created.

- Select the WAN route table from the list.
- Click the Actions drop-down list.
- Select **Edit Subnet associations**.
- Associate the LAN Subnet to the route table which hosts the IP 192.168.100.0/24.

327
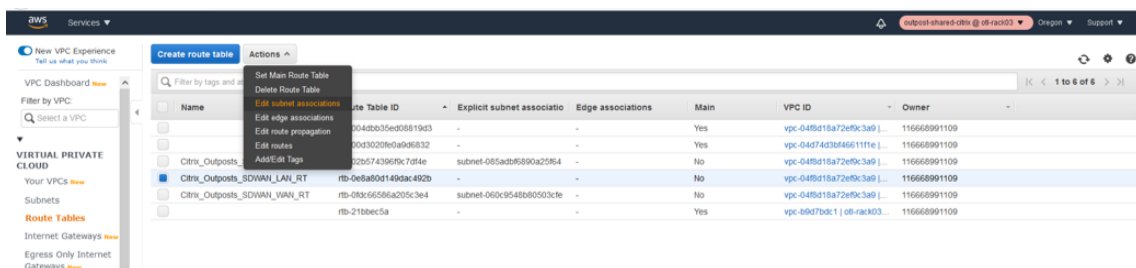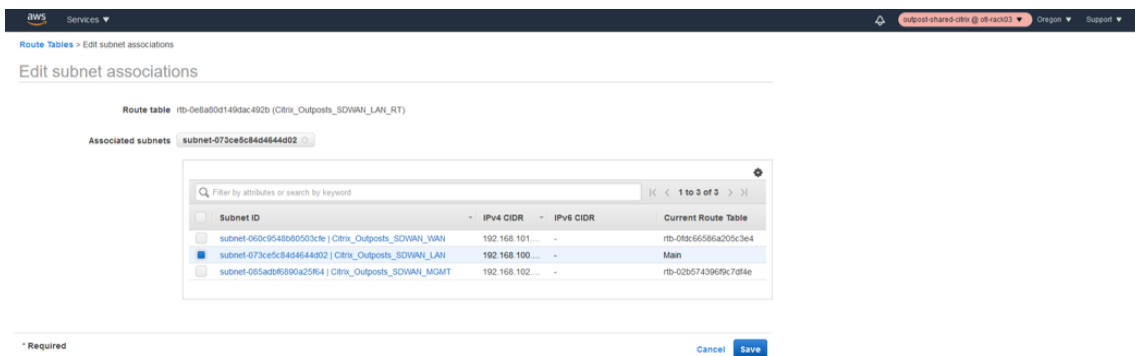
Outpost AMI Instance Provisioning/Deployment

Launch AMI Instance (Private)

1. Choose the Private AMI by uploading the shared AMI into outposts (If not published in Marketplace yet).
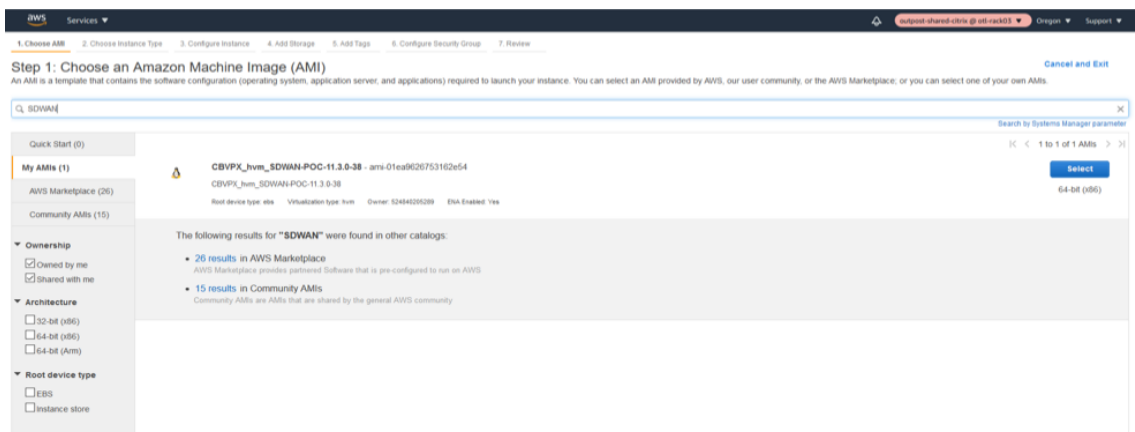
2. Select the right type of instance (VPXL – M5.2xlarge).
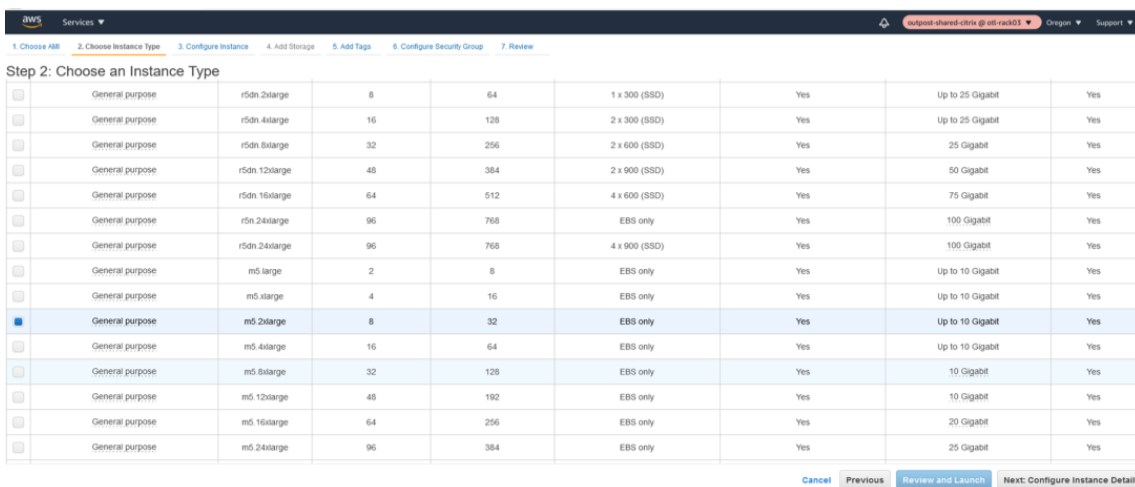
- Configure the Instance Details like the VPC network, Subnet.

- Select the VPC created for the instance in the Network.
- Select the MGMT subnet as the primary interface.
- Select **Enabled** for Auto assign public IP.
- Provide a custom Private IP as well for the management interface in the bottom of the instance details page.
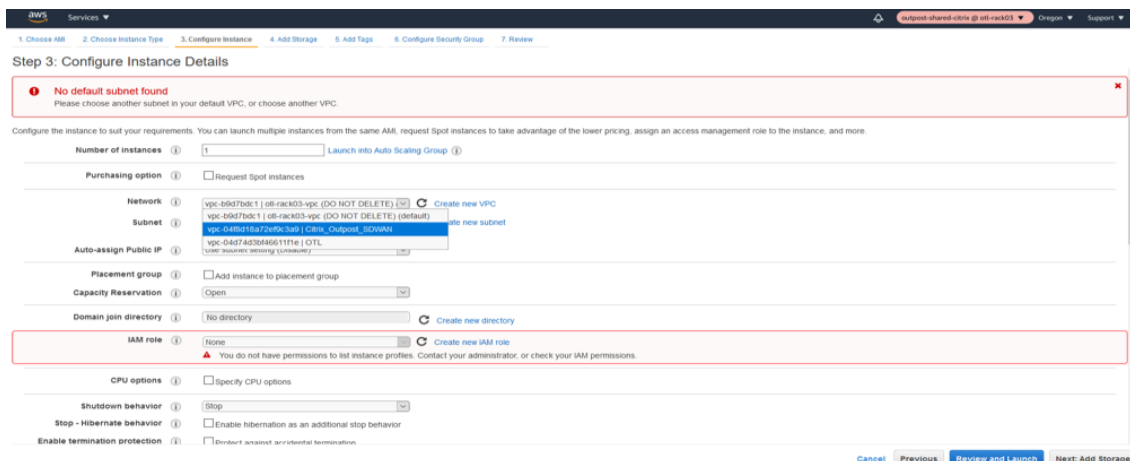
3. Select default Storage.
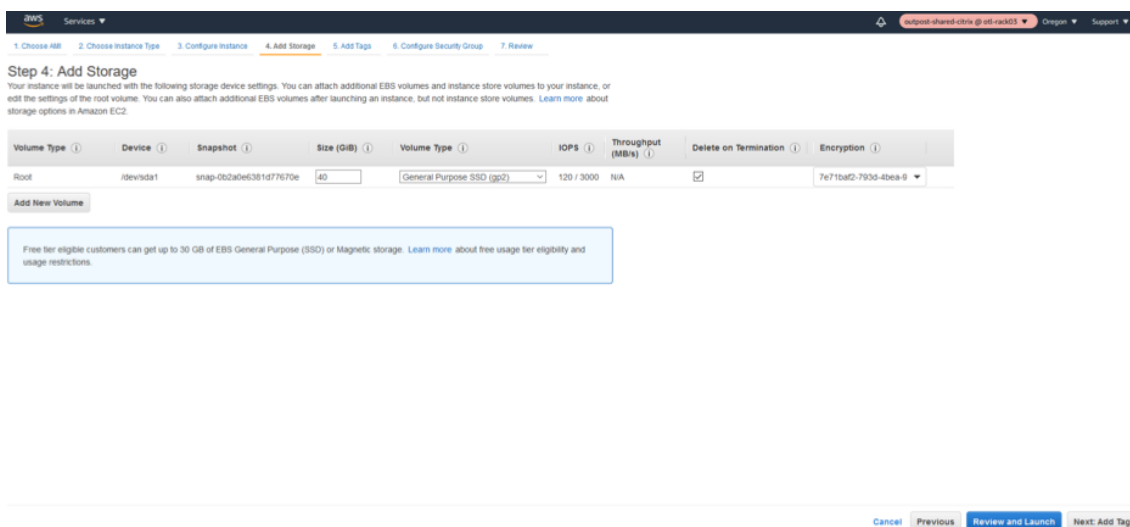
4. Add relevant tags for instance search/indexing later.
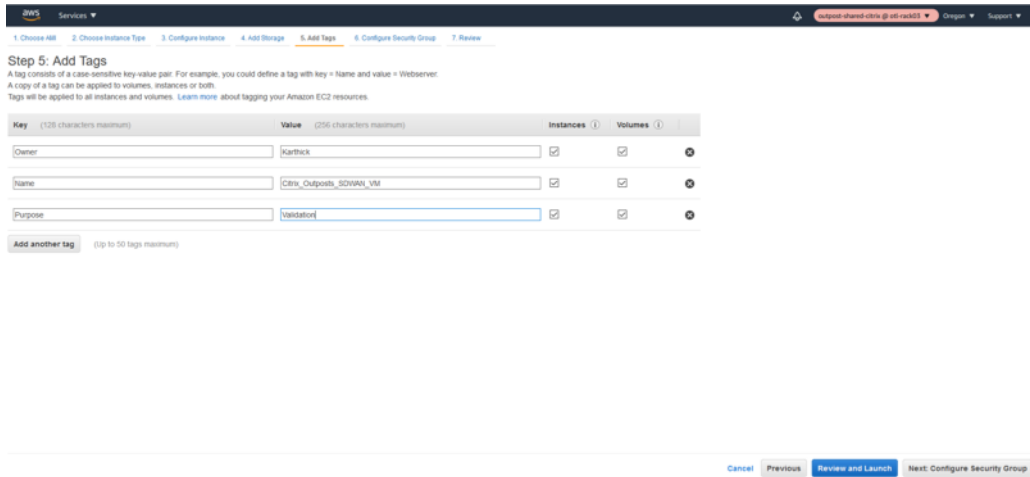
5. Define the relevant Security Group for the instance.
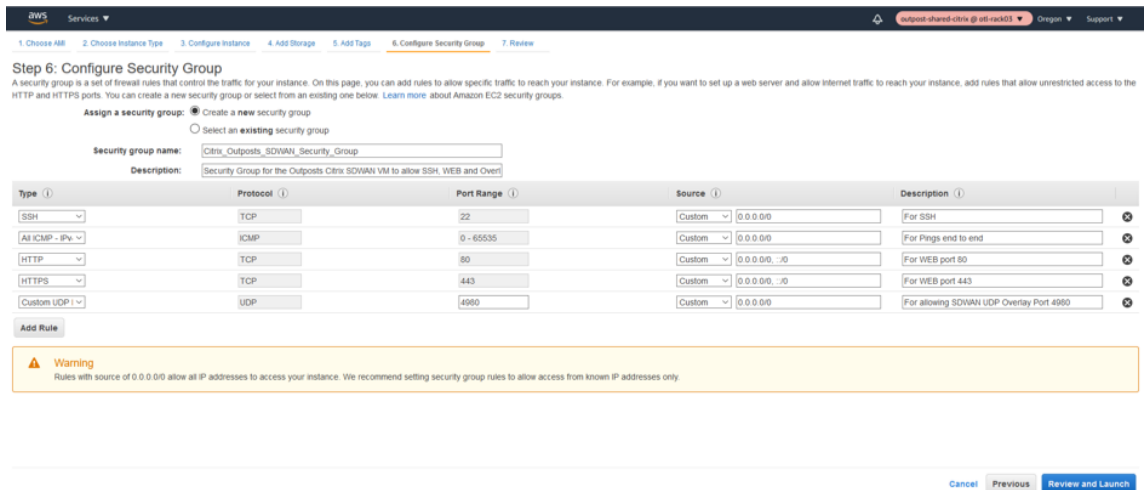
6. Summary of the Network Security Group of the Citrix SD-WAN Outpost Instance.
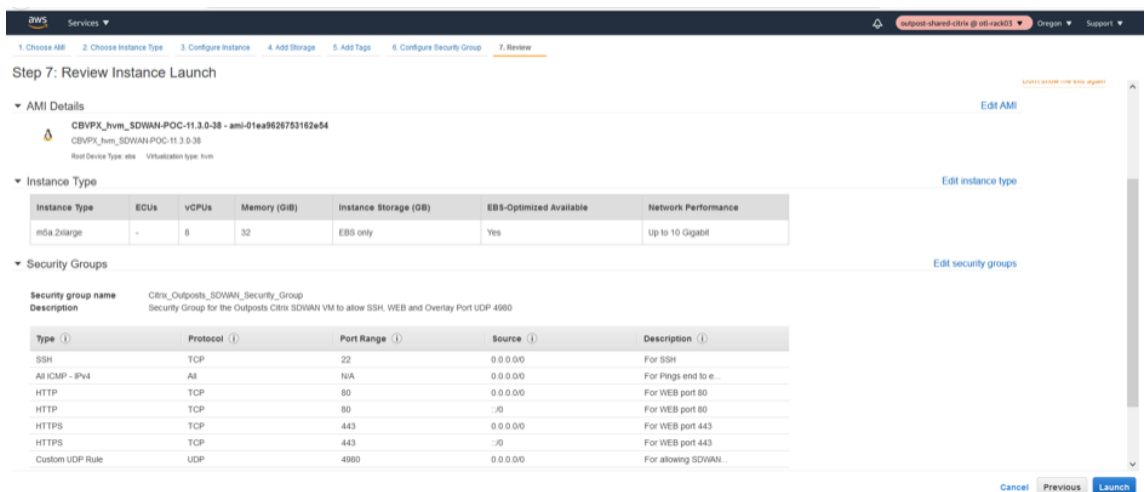
7. Download the Keypair for the instance launch via SSH for later use.

8. Initiate the LAUNCH of the instance.

9. Verify the Instance status and its health check in the EX2 Dashboard post launch.

331
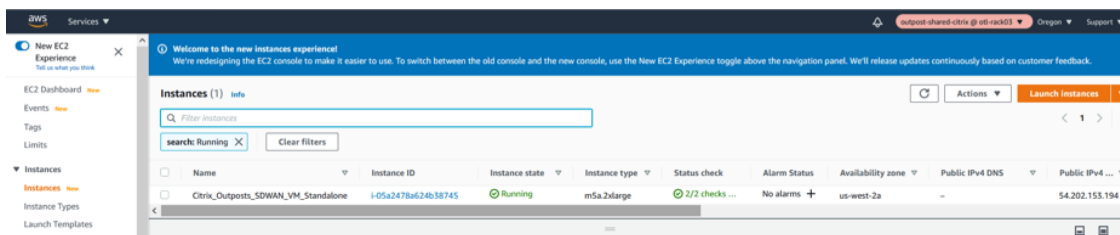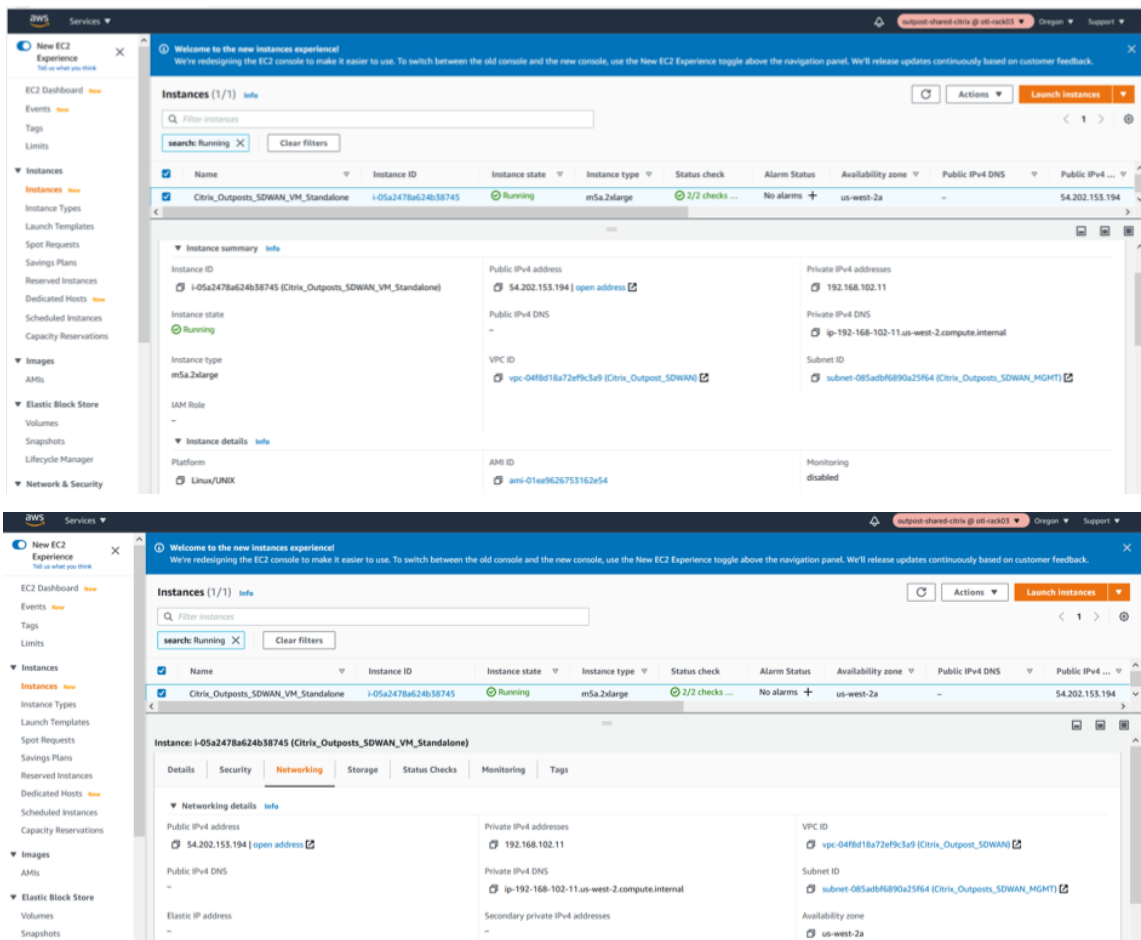
Creation of LAN/WAN Network Interfaces and Association

LAN Network Interface

1. Create the LAN Network Interface.
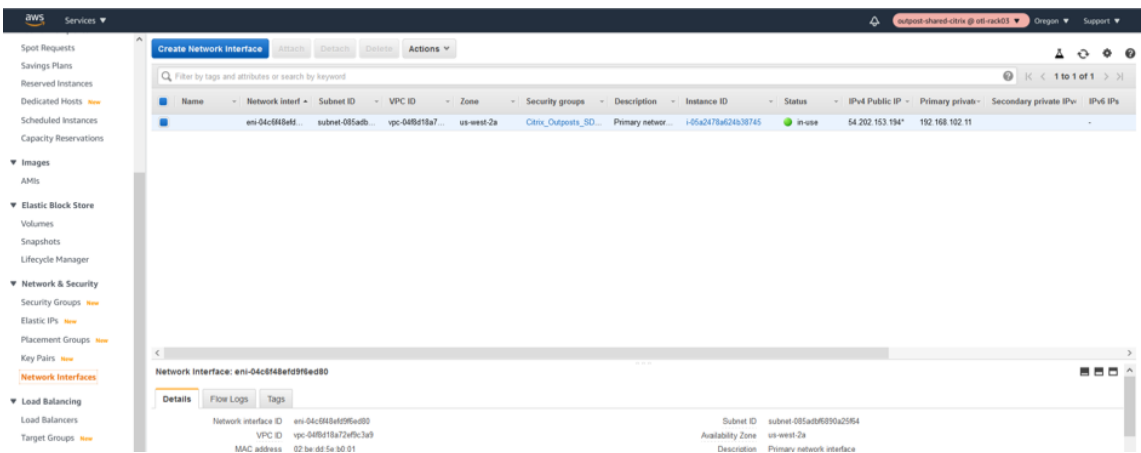
2. Associate the Subnet related to LAN Interface.
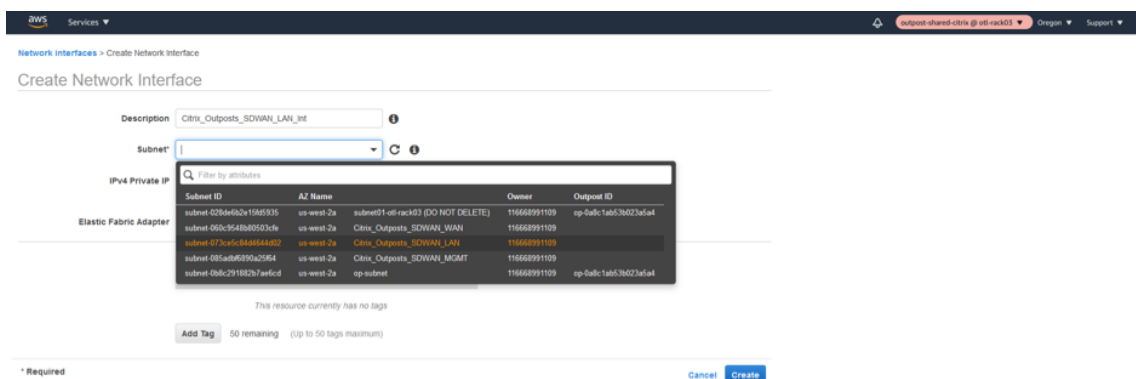
3. Associate a custom LAN Private IP 192.168.100.5 and associate the NSG (Network Security Group).
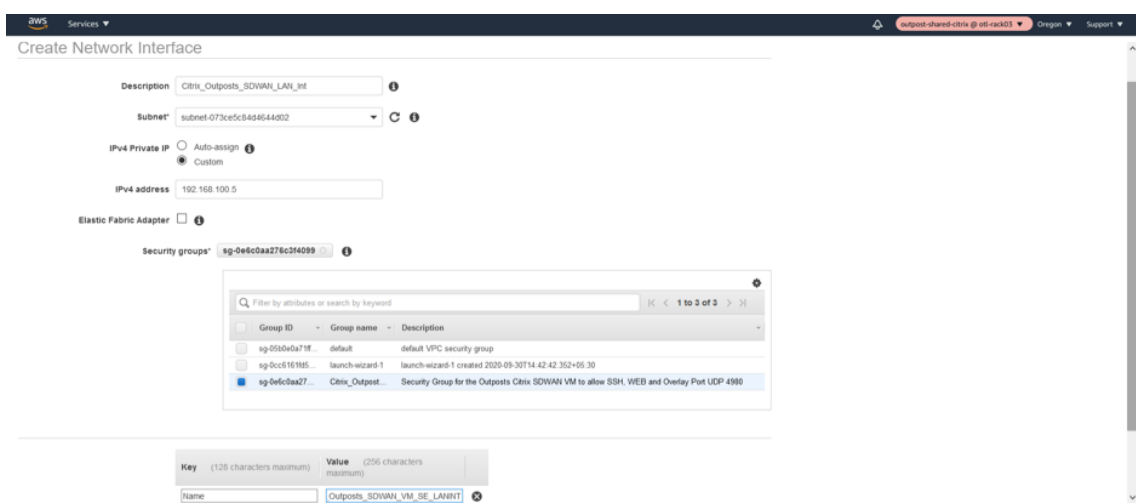
WAN Network Interface

1. Create the WAN Network Interface.
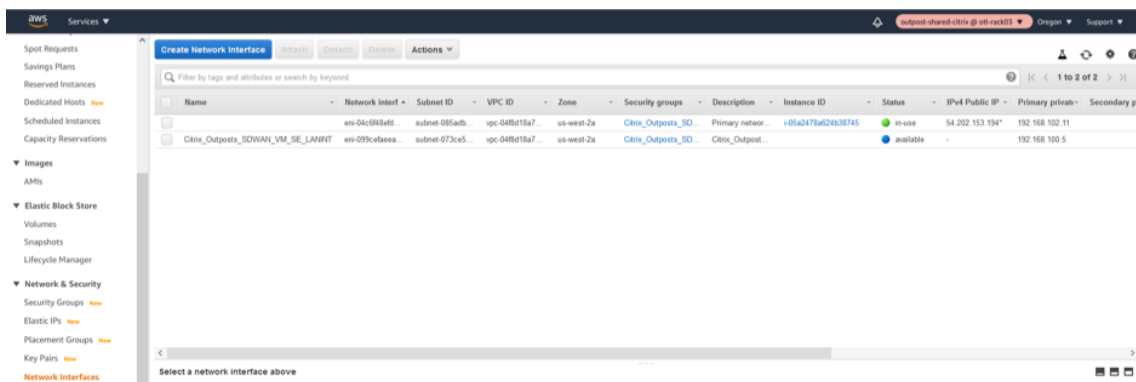
2. Associate the WAN Subnet to the network interface.
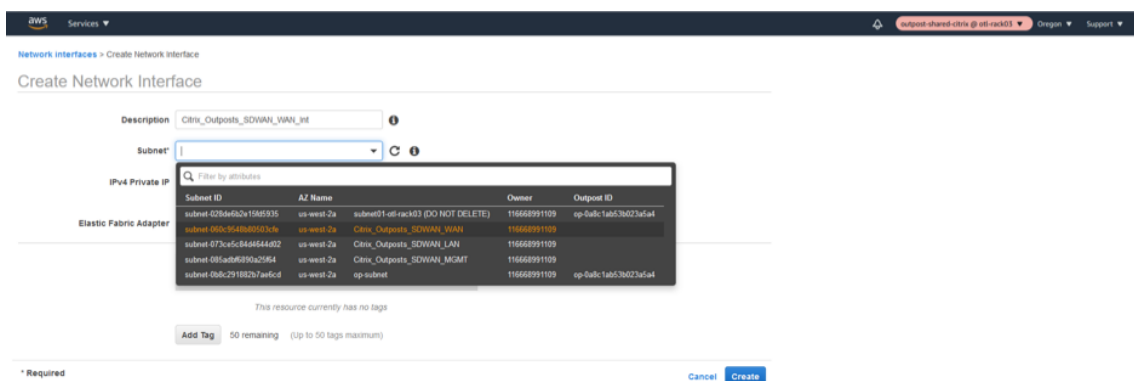
3. Provide a private custom WAN IP as 192.168.101.5 and associate the Network Security Group.
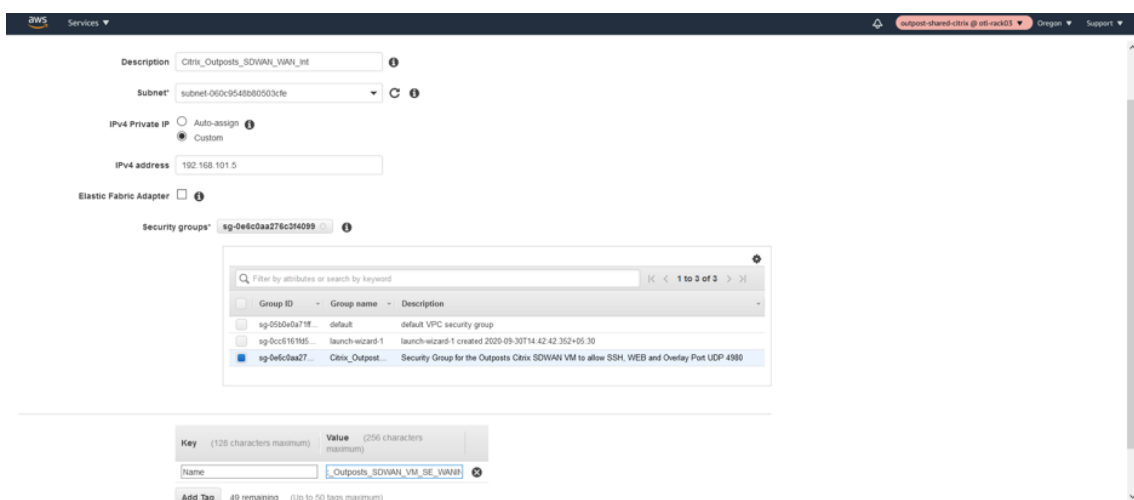
Change SOURCE/DEST Check on LAN/WAN/Management Interfaces

Disabling the Source/Dest. Check attribute enables the interface to handle network traffic that is not destined for the EC2 instance. As the NetScaler SD-WAN AMI acts as a go-between for network traffic, the Source/Dest. Check attribute must be disabled for proper operation.

Management Interface disable SRC/DEST check
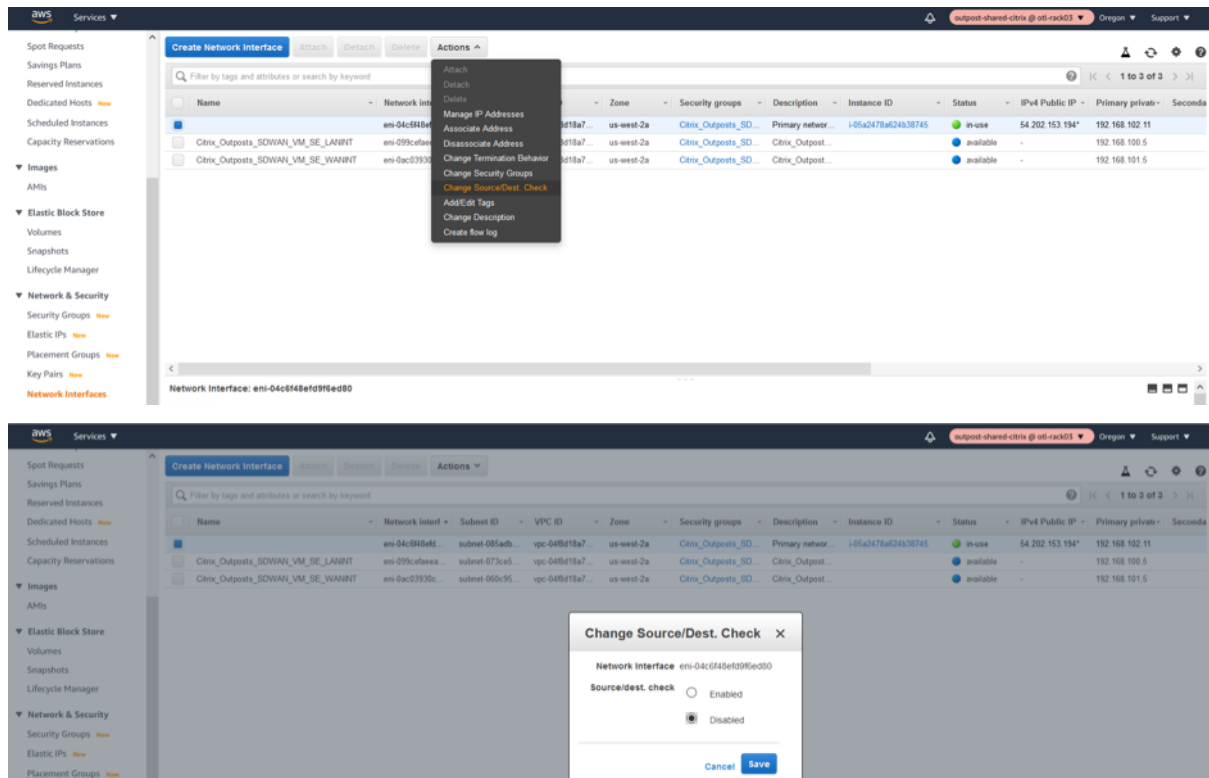
LAN Interface disable SRC/DEST check

335
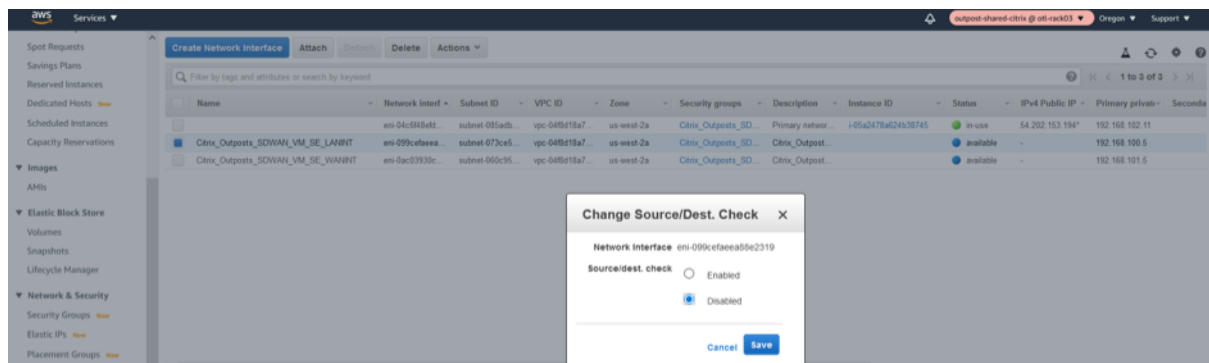
WAN Interface disable SRC/DEST check
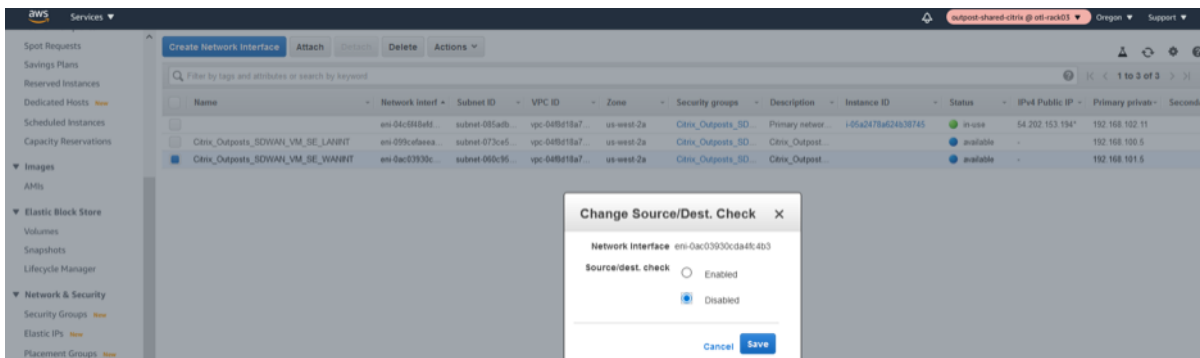
Attach the LAN/WAN Network Interfaces to Outpost Citrix SD-WAN

LAN Interface Association

1. Attach the LAN Network Interface to the SD-WAN.
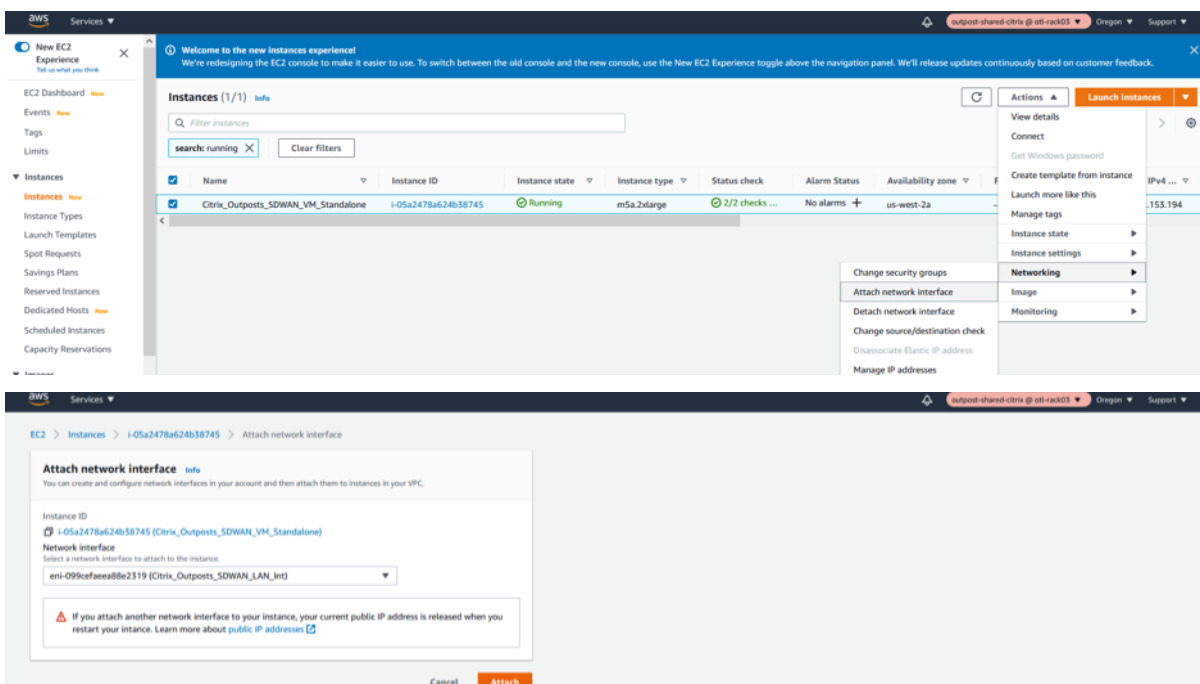
WAN Interface Association

1. Attach the WAN Network Interface to the SD-WAN.
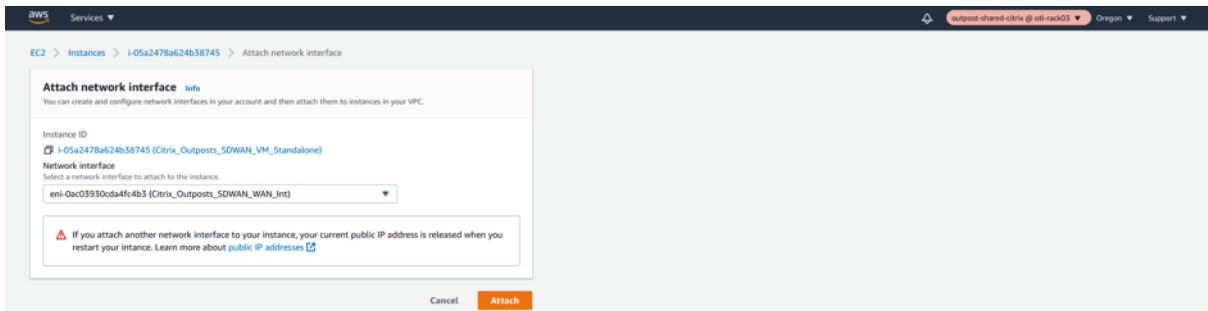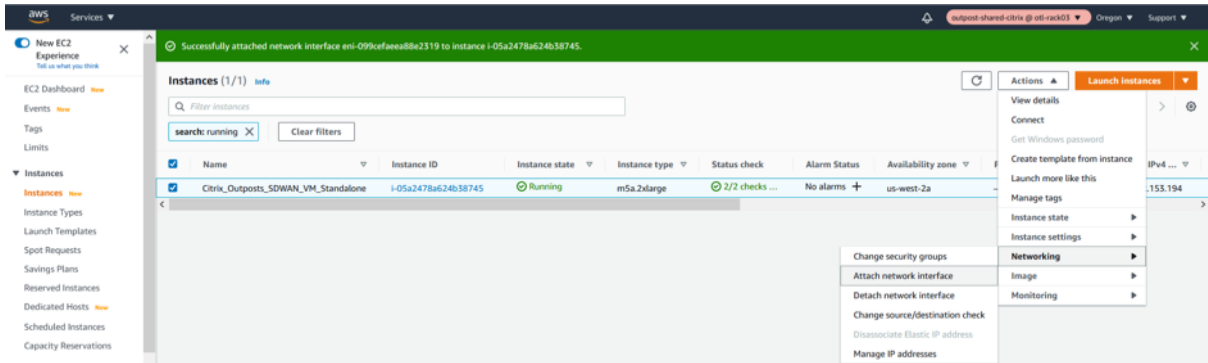
Note

Attaching the Mgmt, LAN, and WAN in that order attaches to eth0, eth1, eth2 in the SD-WAN AMI. This aligns with the mapping of the provisioned AMI and ensures that interfaces are not reassigned incorrectly in the event of AMI reboot.

Create and Associate ELASTIC IPs to MGMT and WAN Interfaces of Outpost Citrix SD-WAN

Management IP Elastic IP

1. Allocate a new ELASTIC IP for MGMT Interface.
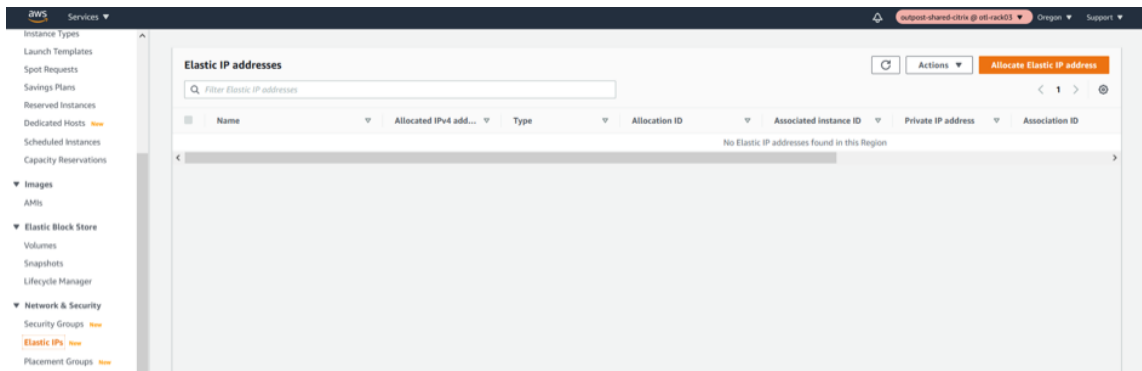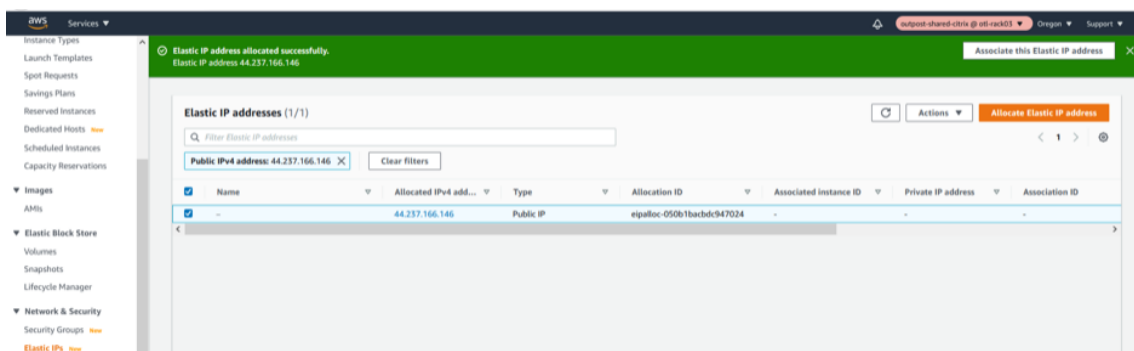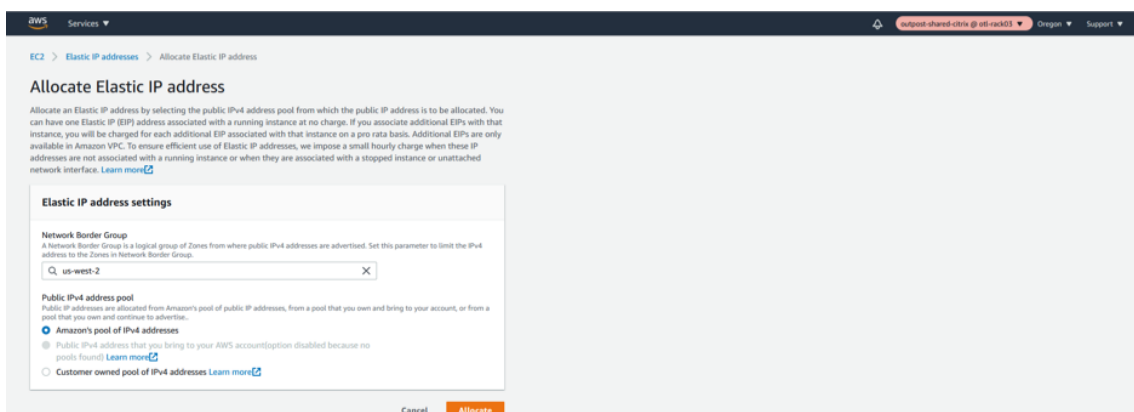
2. Associate the newly created ELASTIC IP to Management Interface.

The Management Elastic IP is needed for SSH/UI browsing over 80/443 of the Outpost based Citrix SD-WAN appliance. This makes management simpler.

We will be specifically linking the elastic IP to the Management Network Interface and further specifically to th private IP associated with the management subnet which is "192.168.102.11".

- Select Network Interface
- Select the Management network interface
- Assign a private IP Address "192.168.102.11"
- Associate
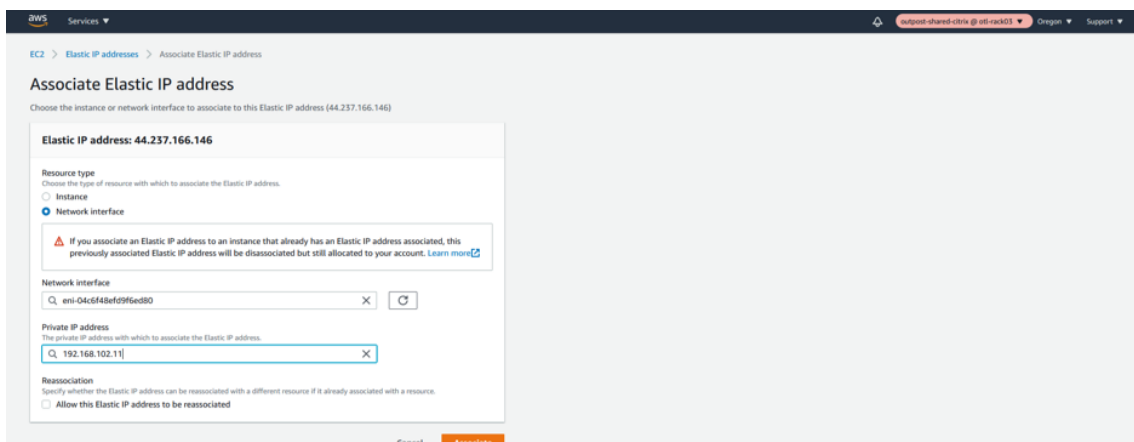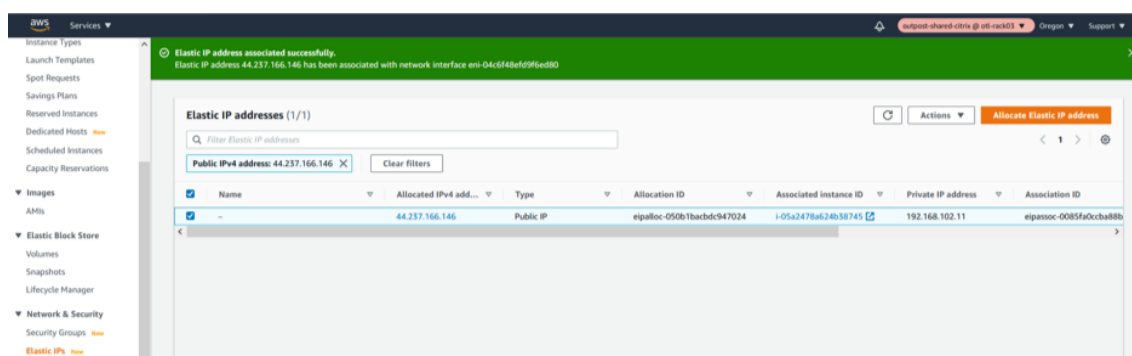
WAN Interface Elastic IP

1. Allocate a new ELASTIC IP for WAN Interface
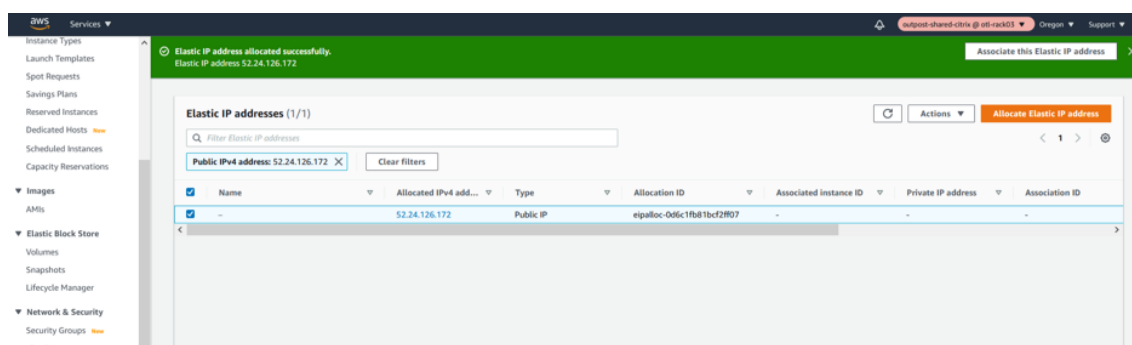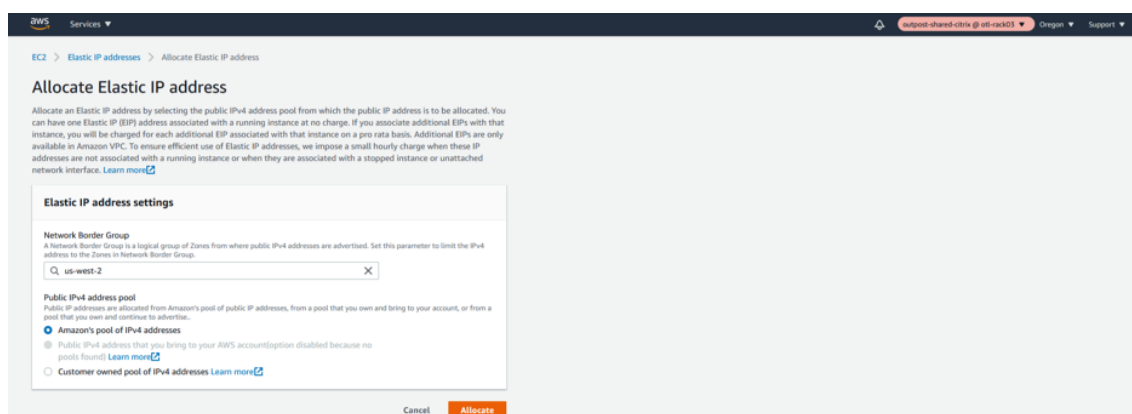
2. Associate the newly created ELASTIC IP to WAN Interface.

   The WAN Elastic IP is needed for enabling the overlay communication between different sites to the Outpost based Citrix SD-WAN appliance and have the IP connectivity to the external world. This would be the Public IP of the WAN Link that we will provide for an MCN or a Branch. This IP is essentially to be known by all the remote appliances/peers to help have an overlay control/data channel establishment.
   We will be specifically linking the elastic IP to the WAN Network Interface and further specifically to the private IP associated with the WAN subnet which is "192.168.102.11".

- Select Network Interface
- Select the WAN network interface
- Assign a private IP Address "192.168.101.5"
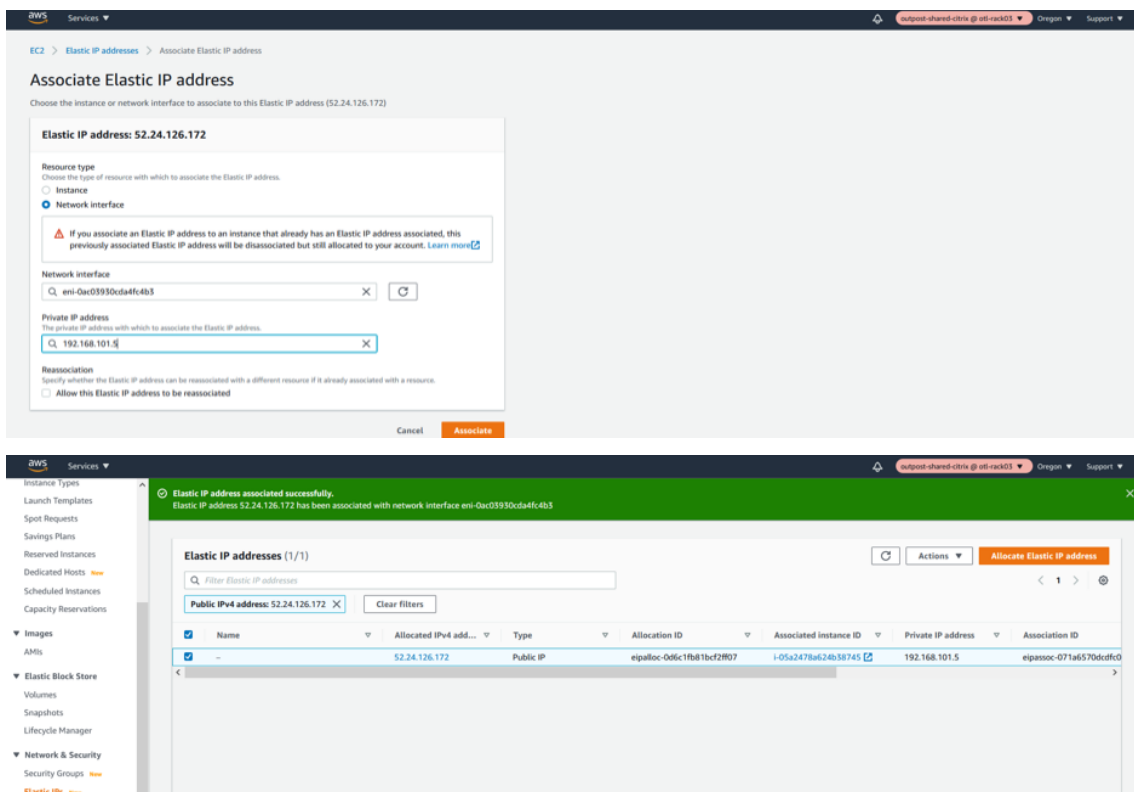
Outpost VPXL SD-WAN VM as an MCN

Access/Configure the Outpost Citrix SD-WAN as an MCN

1. Access MGMT Interface IP.

   Note down the elastic IP of the Management interface and type in `https://<elastic_ip_mgmt_interfac` `>` to access the SD-WAN UI.
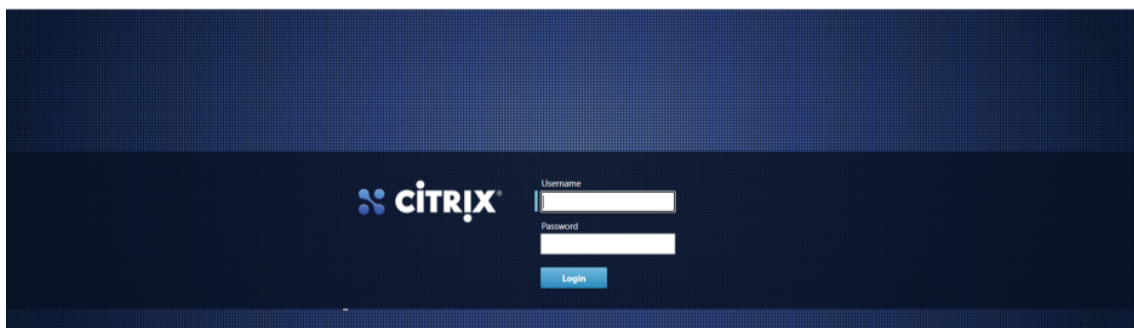
2. Authenticate with admin credentials.

User name is admin and password is the INSTANCE ID (Highlighted below)
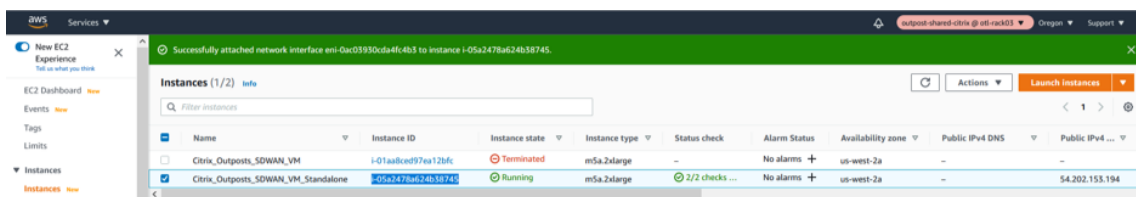
3. Make the role of the Outpost Citrix SD-WAN VM as an MCN (Master Control Node)
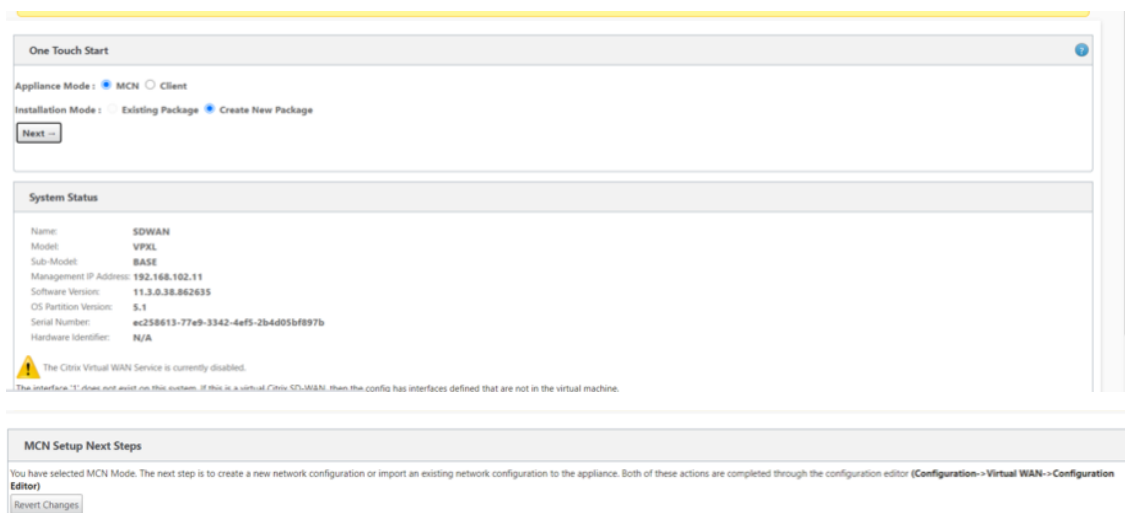
4. Add a new site for the MCN (Outpost SD-WAN).
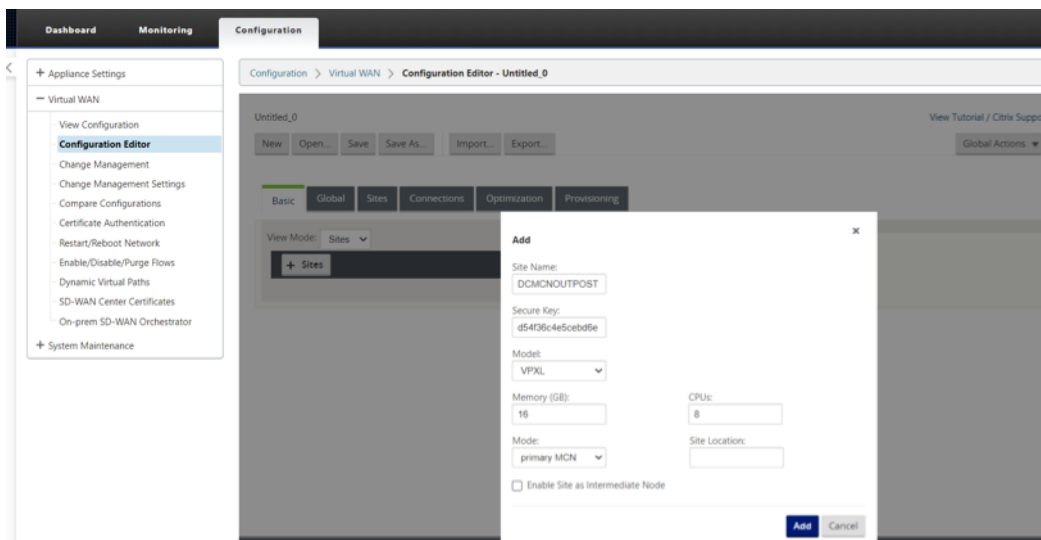
5. Configure the Outpost VM (MCN) Network Interface Groups for LAN and WAN.
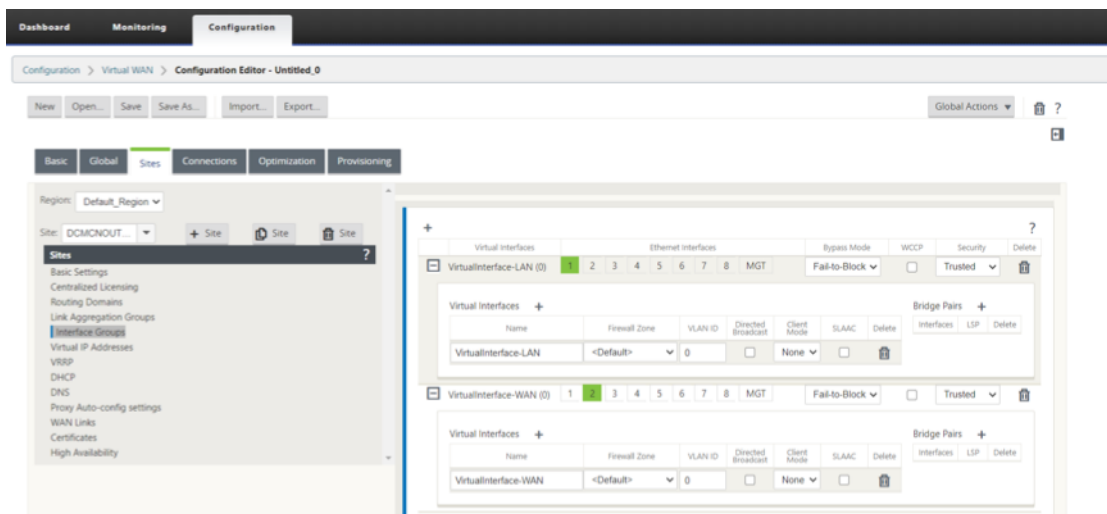
6. Configure the Outpost VM (MCN) Virtual IP Addresses (VIPs) for LAN and WAN.
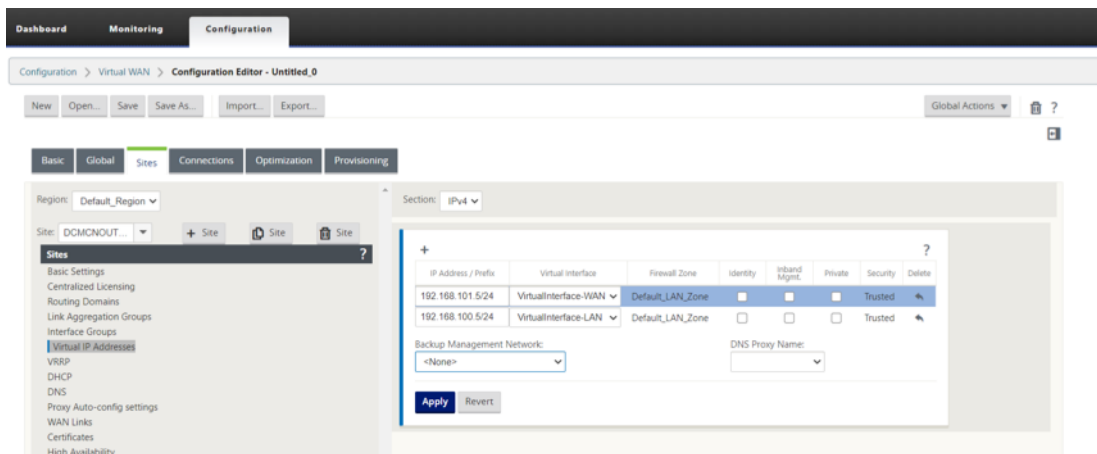
7. Configure the Outpost VM (MCN) WAN Link.

- DOWNLOAD/UPLOAD capacity definitions on the WAN link.
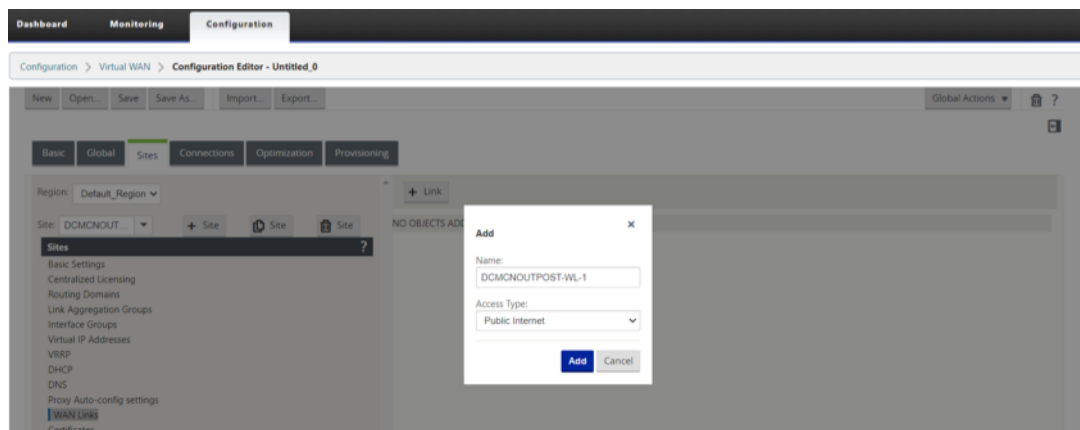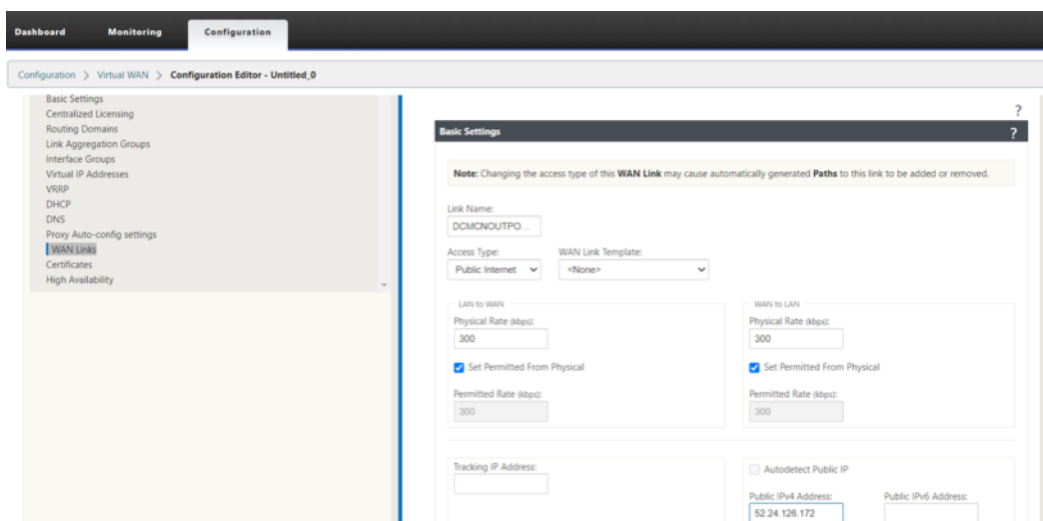
- Configure the Access Interface and the Gateway IP of the WAN Link.
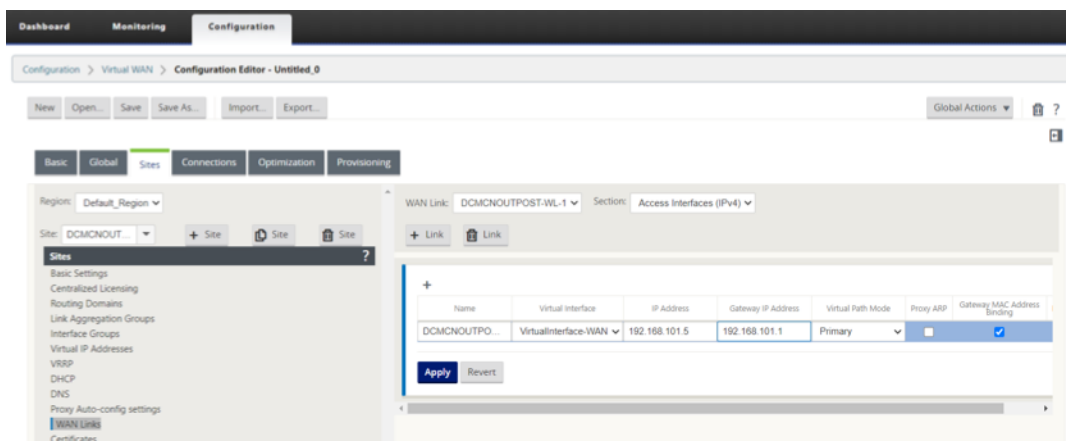
Citrix SD-WAN 210 as a HOME USER BRANCH SD-WAN

Configure the 210 Citrix SD-WAN as a BRANCH

1. Add a 210 site as a Branch in Client mode.
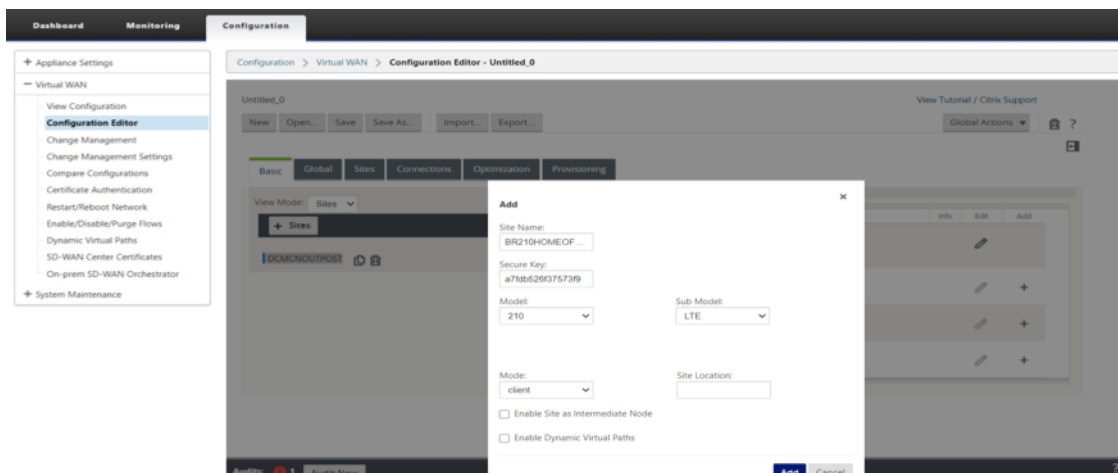
2. Configure the 210 HOME OFFICE Branch Network Interface Groups for LAN and WAN.
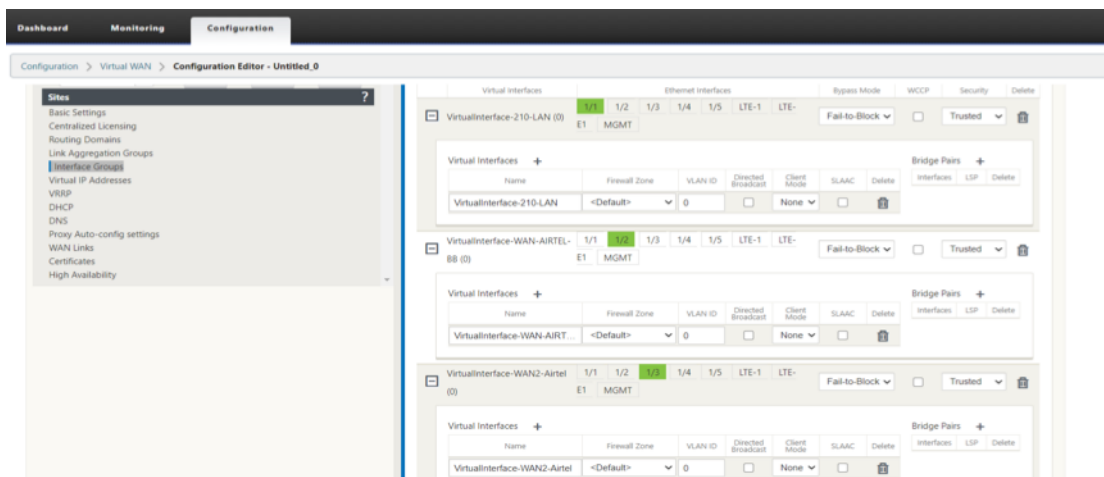
3. Configure the 210 HOME OFFICE Branch Virtual IP Addresses (VIPs) for LAN and WAN.
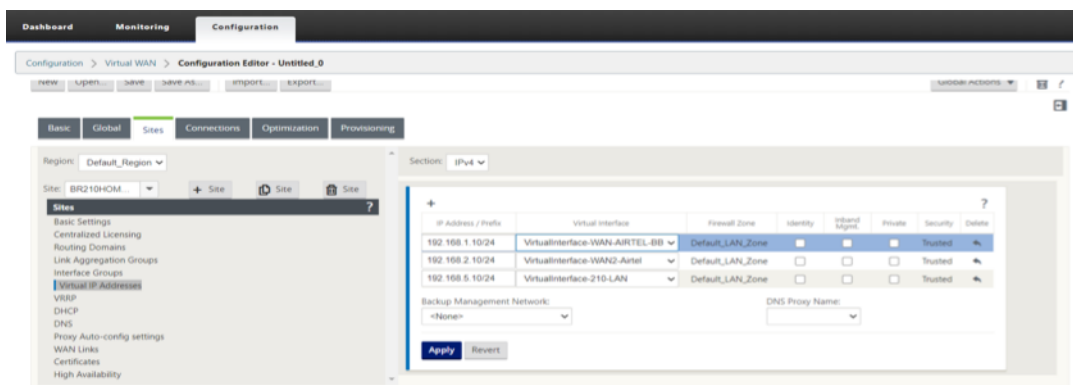
4. Configure the 210 HOME OFFICE Branch WAN Link.

- DOWNLOAD/UPLOAD capacity definitions on the WAN link.

Citrix SD-WAN Platforms
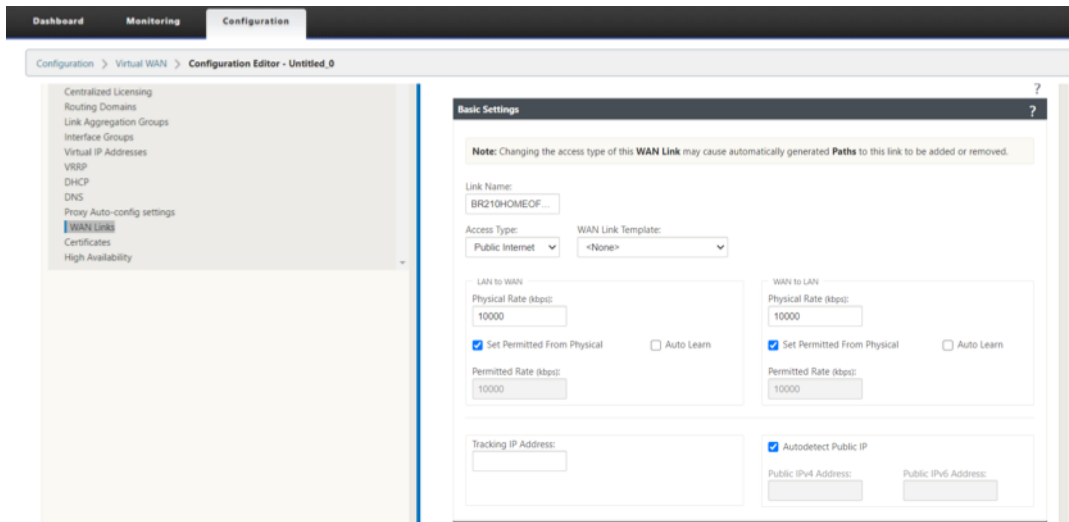
- Configure the Access Interface and the Gateway IP of the WAN Link.

Perform Change Management and Stage the configuration to the appliances
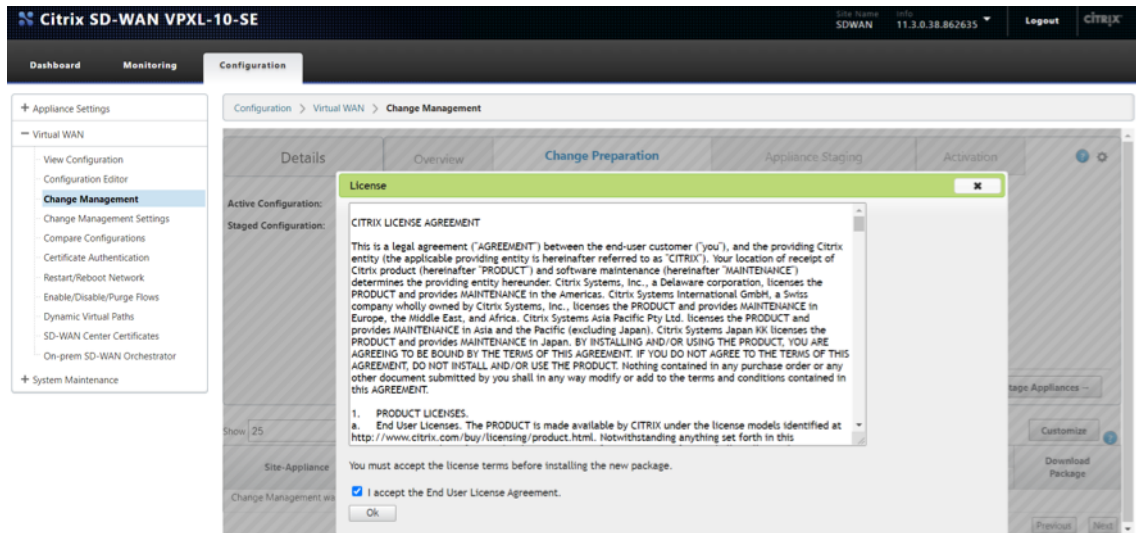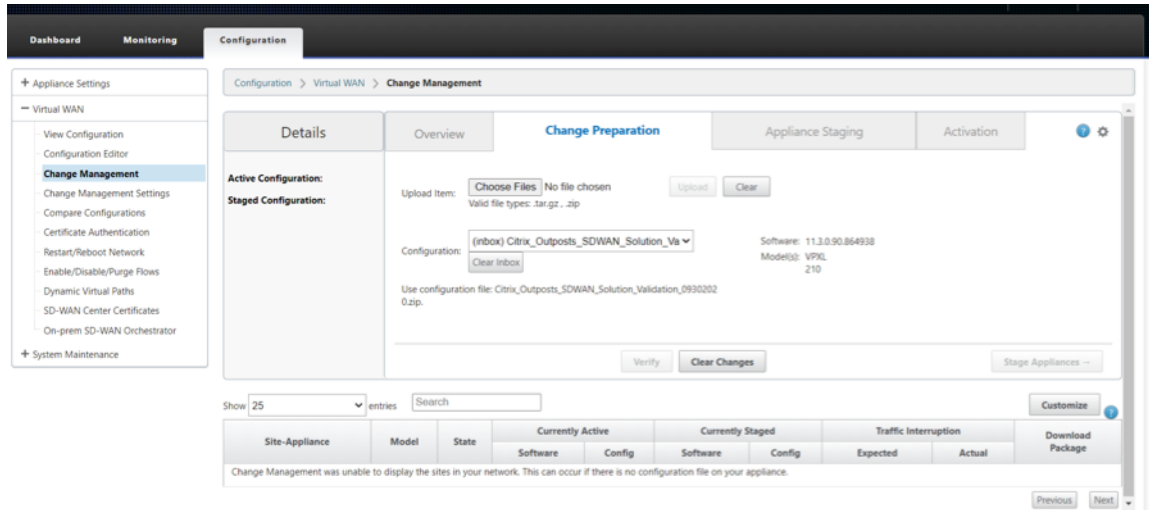
Activate the Configuration
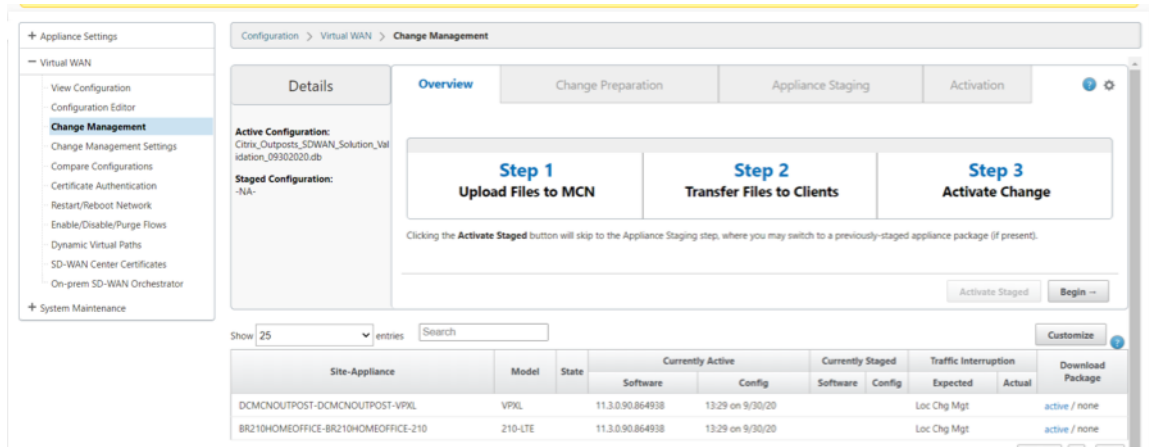
Verify the Virtual PATH creation

On the Outpost MCN VM

On the 210 HOME Branch

Validate Traffic over Virtual PATH between Outpost VM and 210 Branch.

- **Step 1** – Initiate Ping between the 210 Branch and the Outposts MCN
- **Step 2** – Check Flows on both 210 and MCN VM on Upload/Download direction and verify the SIP, DIP, IP Protocol and the Service used for processing traffic
- **Step 3** – Check firewall connection on the Outpost MCN and the 210 for the ICMP traffic between the 2 sites
- Verify that Ping traffic initiated between the 210 Branch and the Outposts MCN is processed via Virtual Path
    - Flows should indicate flows via right service type as Virtual Path
        * Check Flows on Outpost MCN – SIP, DIP, IP Protocol should match including Service as Virtual Path
        * Check the paths in the flow for best path used – Should be one of the best paths in the list of paths available
    - Check flows on the 210 Branch - SIP, DIP, IP Protocol should match including Service as Virtual Path
        * Check the paths in the flow for best path used – Should be one of the best paths in the list of paths available
    - Check Firewall to check the connection
        * Check Firewall on the Outpost MCN should have the connection information with the Application as ICMP for response. Should have SIP-SPORT (MCN), DIP-DPORT (210) including Source Service and Dest service as Local and Virtual Path respectively
        * Source
        * Check Firewall on the 210 Branch should have the connection information with the Application as ICMP for request. Should have SIP-SPORT (210), DIP-DPORT (MCN) including Source Service and Dest service as Local and Virtual Path respectively

Initiate PING from the end laptop to 192.168.100.5 (LAN side VIP of the Outposts SD-WAN)

- **Command** – ping 192.168.100.5
- **Source Ip address of initiating laptop** – 192.168.5.160
- This traffic is intended to traverse the Virtual path due to the routing table installed on the branch with the 192.168.100.0/24 installed as a prefix reachable over VP

Initiate PING from the end laptop to 192.168.100.5 (LAN side VIP of the SD-WAN)

Verify Flows that the LAN to WAN and WAN to LAN direction entries are seen in both the MCN (Outpost VM) and the 210 Branch

Verify FLOWS on the 210 Home Branch

On the Home Branch

LAN to WAN (From Branch towards MCN)

- Source IP – 192.168.5.160
- Dest IP – 192.168.100.5
- Proto/IPP – ICMP

WAN to LAN (From MCN towards Branch)
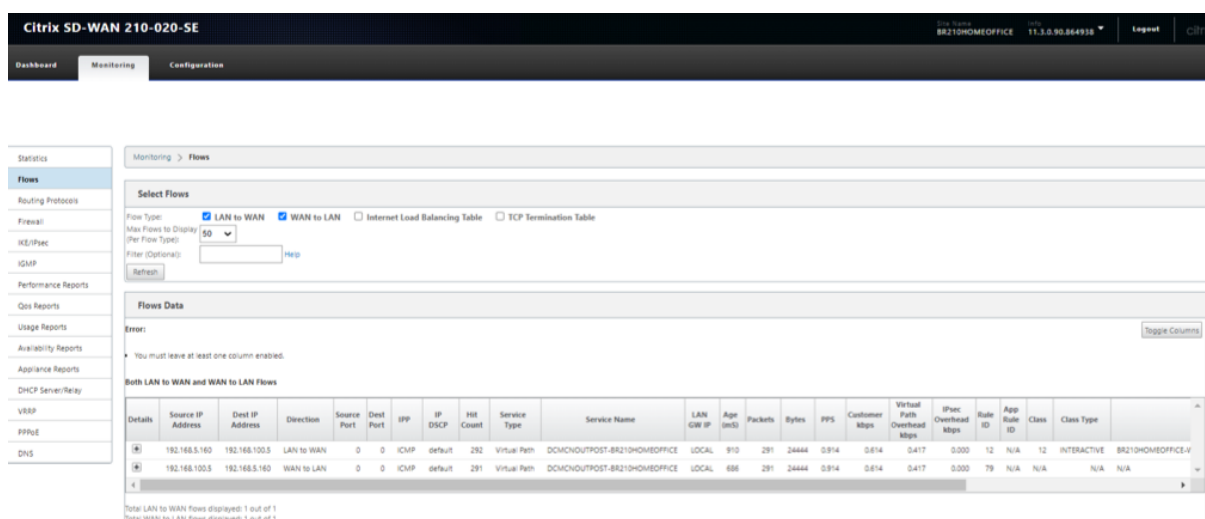
- Dest IP – 192.168.5.160
- Source IP – 192.168.100.5
- Proto/IPP – ICMP

- Verify that the service used is Virtual Path and the service name is that if between the MCN (Outpost VM) to the Branch 210

- Also check the path will display the current best path that is taking the ICMP traffic through the Virtual Path (Which is WL1 on the 210 to the only existing link at the MCN side)

> **Note**
>
> Check the current path in the "Path" Column in the below snapshot.
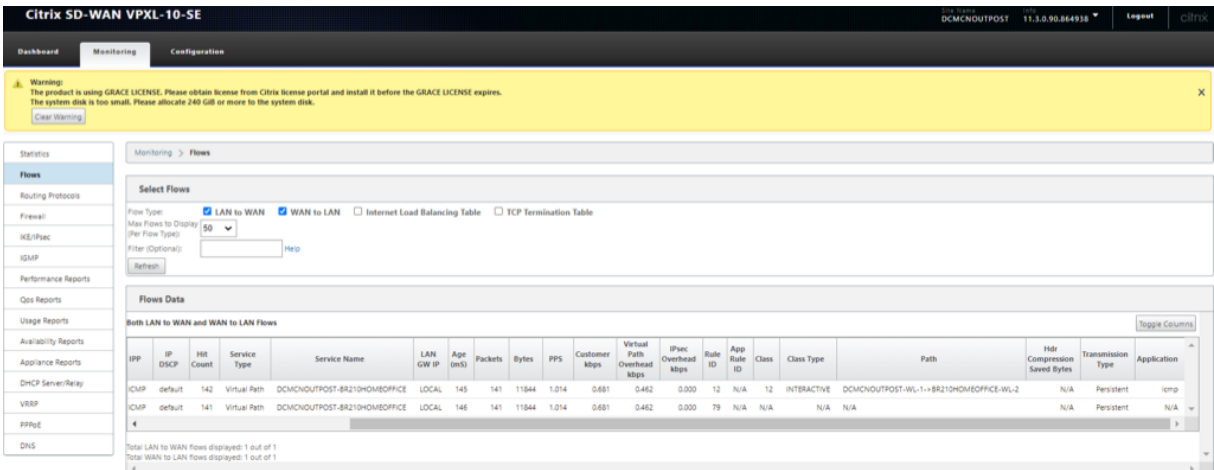
Verify on the MCN (Outposts VM)

On the MCN Outpost VM side

WAN to LAN (From Branch towards MCN)

- **Source IP** – 192.168.5.160
- **Dest IP** – 192.168.100.5
- **Proto/IPP** – ICMP

LAN to WAN (From MCN towards Branch)
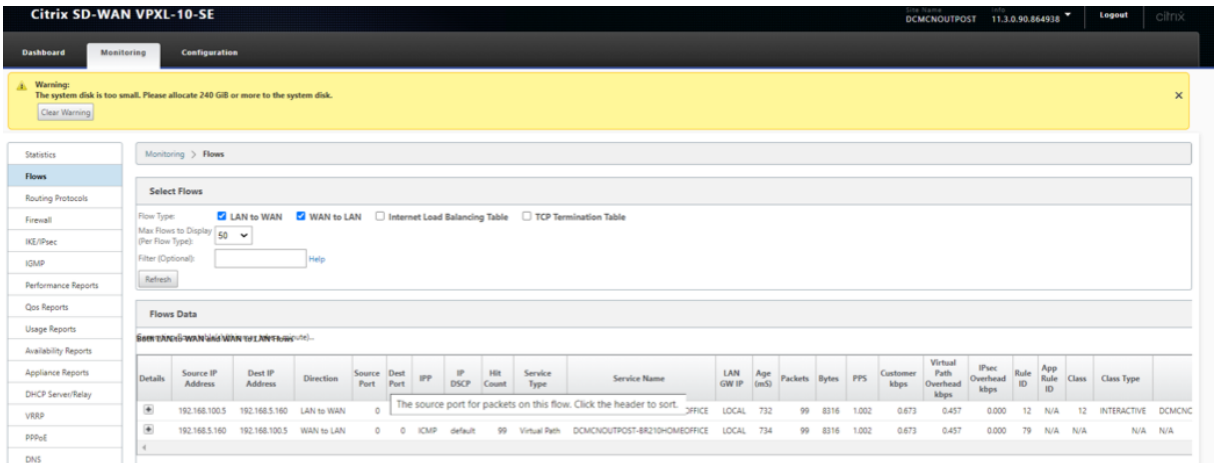
- **Dest IP** – 192.168.5.160
- **Source IP** – 192.168.100.5
- **Proto/IPP** – ICMP

- Verify that the service used is Virtual Path and the service name is that if between the MCN (Outpost VM) to the Branch 210

- Also check the path will display the current best path that is taking the ICMP traffic through the Virtual Path (Which is WL1 on the 210 to the only existing link at the MCN side)

Verify Firewall details on the MCN (Outposts VM)

Below details are validated for the flow at the MCN (Outposts VM)

- Application – ICMP
- Source Service – Virtual PATH (Traffic came via VP from the Branch side)
- Destination Service – IPHOST (Because we are pinging to the IP of the SD-WAN and is intended to the device)
- State - Established

For information on support policies, see support and services

Verify Firewall details on 210 Home Branch

Below details are validated for the flow at the 210 Branch side.

- Application – ICMP
- Source Service – Local (Initiated from a host behind the 210 Branch)
- Destination Service – Virtual Path (Because we are pinging to the IP of the SD-WAN and is intended to the device and is carried via Virtual Path)
- State - Established

For information on support policies see support and services
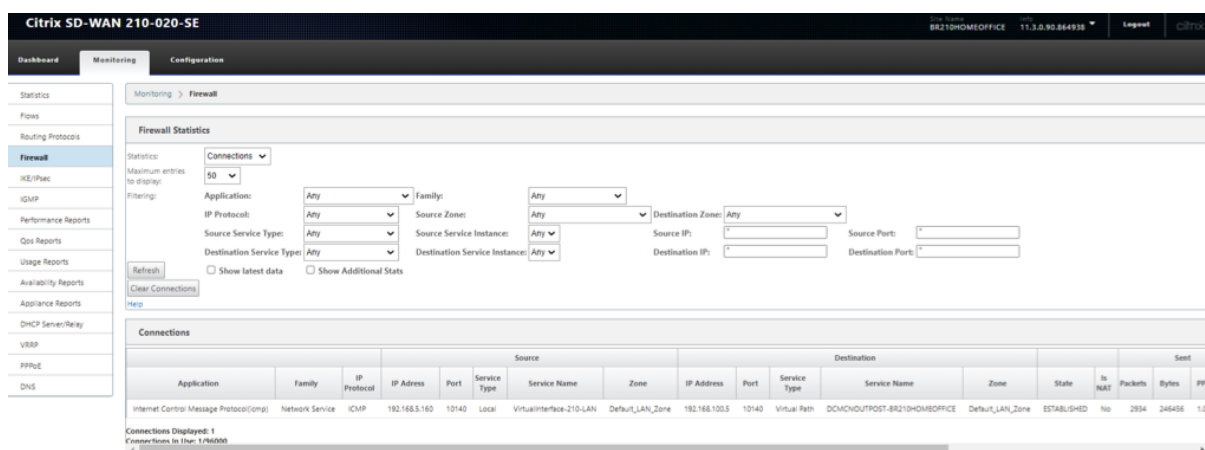
Deploy SD-WAN Standard Edition instances in High Availability mode in Azure - Release Version 10.2 and above

February 10, 2021

The Citrix SD-WAN Azure solution deploys Citrix SD-WAN in Edge Gateway Mode as a single instance, or a cluster pair for High Availability (HA). In an HA deployment, an Azure Load Balancer (ALB) controls the failover between the WAN interfaces of the Citrix SD-WAN appliances.

You can use the Azure load-balancer (ALB) on the LAN side to control failover on the LAN side of the SD-WAN appliances. The Citrix SD-WAN Azure solution in HA creates two separate ALBs (each one on LAN and WAN).

The following diagram illustrates the Citrix SD-WAN Azure HA deployment:
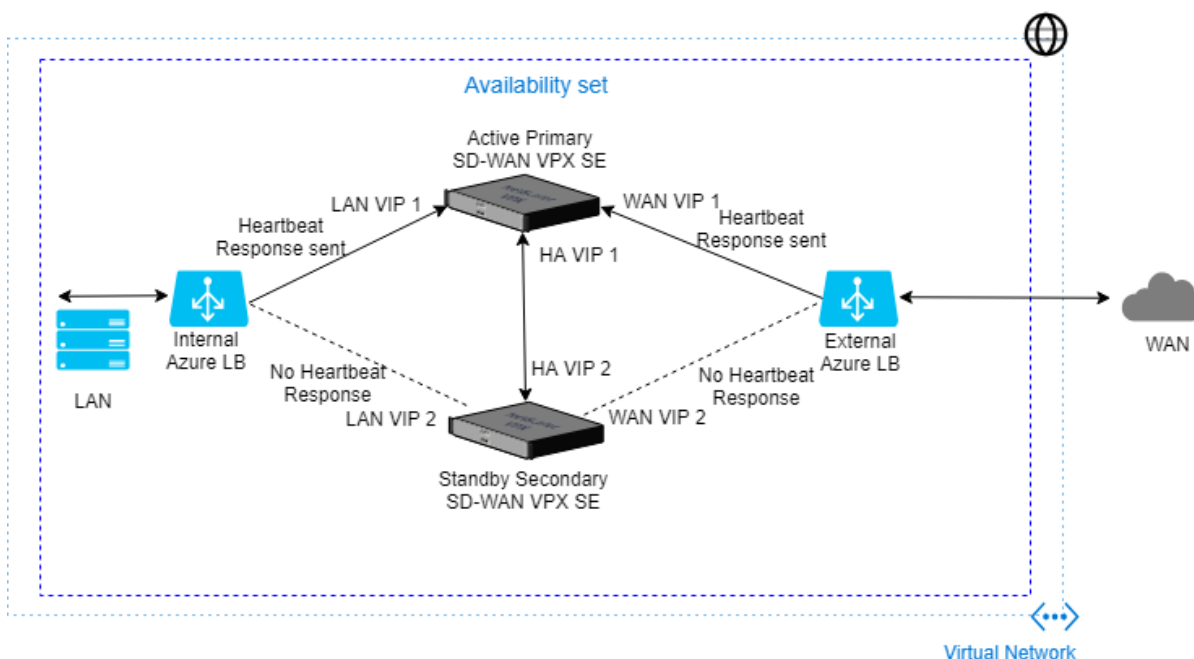
The SD-WAN Standard Edition deployment in Azure is required to be deployed in Edge or Gateway mode deployment where the SD-WAN instance acts as the gateway for the LAN environment. For more information, see Gateway mode.

How to deploy Citrix SD-WAN

To create Citrix SD-WAN Standard Edition (SE) instance:

1. Search for **Citrix SD-WAN** in the Azure Marketplace and select **Citrix SD-WAN Standard Edition 10.2.X**.
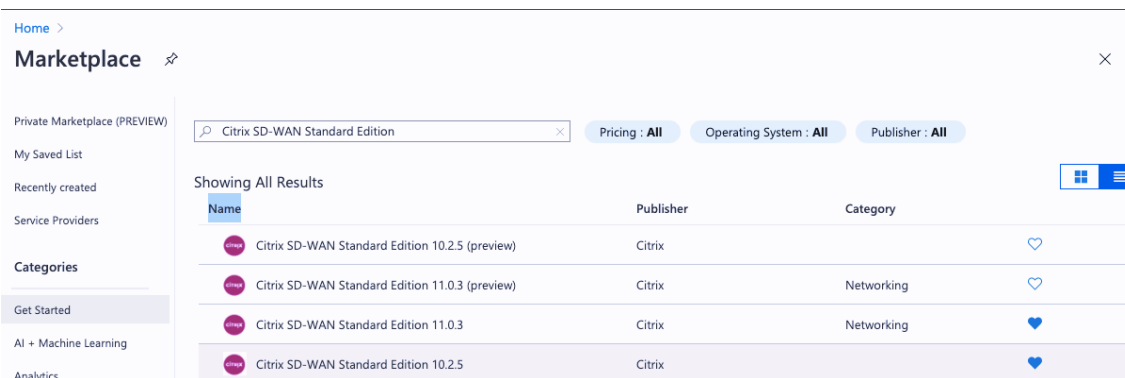
2. Click **Create** button to create the **Citrix SD-WAN SE 10.2.X Instance**.

3. Configure **Basic** settings page and provide the **Resource group** name with the appropriate **Location**.

Note

To create an instance either a new resource group must be created or the resource group must be empty to be reused.

4. Name the Virtual Machine, select **Enabled for HA Deployment Mode**, and create a **Username** and **Password**.

Note

Use **admin** as a user name for the provisioned instance with the same password that was given during provisioning to get the admin access. In the previously mentioned screen-shot, the provisioned user has the guest privilege.

5. Select the **Virtual Machine** size based on the requirement.

6. From Citrix SD-WAN 11.0.3 release, by default 120 GB of OS Disk Size is allocated. If necessary, you can modify the disk size to a value between 40 GB to 999 GB.

7. Use an existing VNet in the location specified or create a new.

8. Once the **Vnet** is created, confirm the auto-populated subnets for **Management, LAN, WAN,** and **AUX,** then click **OK**.

9. Validate the configuration before the **Instance** creation.

10. Click **Create**.

How to configure Citrix SD-WAN HA in Azure

1. Determine the IP addresses assigned to the SD-WAN interfaces. Navigate to **Virtual Machines** > **SDWSEA** (or as appropriate)> **Networking**, and examine the IP of each Azure Network Interface.

   - In this deployment, SDWSEA Interface 0 for Management is 10.100.254.4/13.67.93.144.
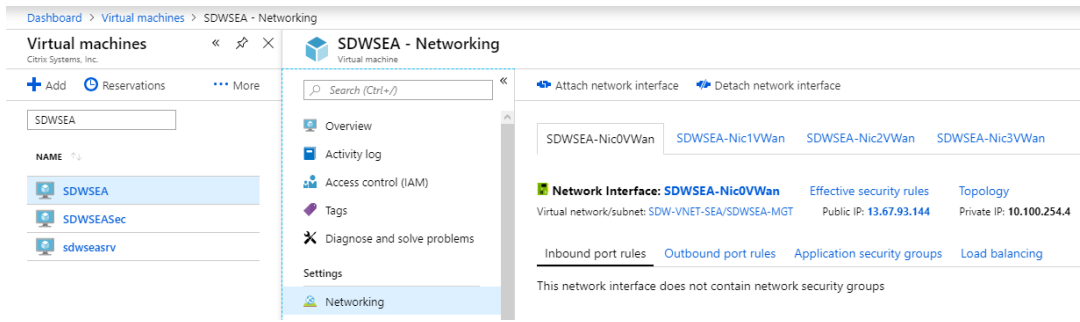
- The SDWSEA Interface 1 LAN VIP is 10.100.1.4.
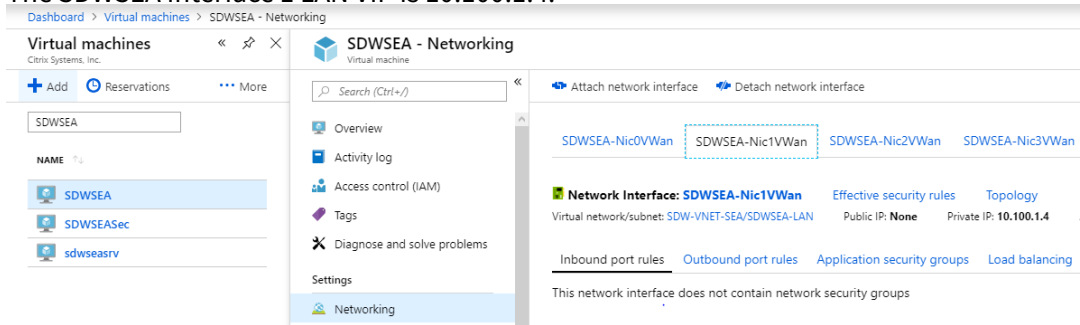
- The SDWSEA Interface 2 WAN VIP is 10.100.0.4.
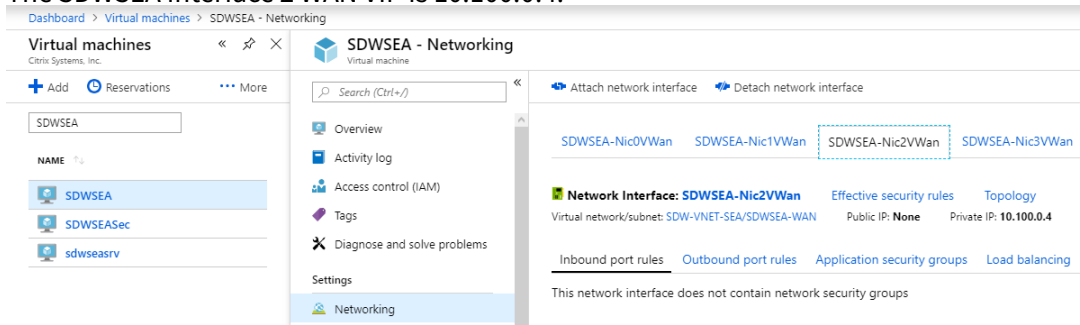
- The SDWSEA Interface 3 HA Tracking IP (not VIP) is 10.100.253.4:
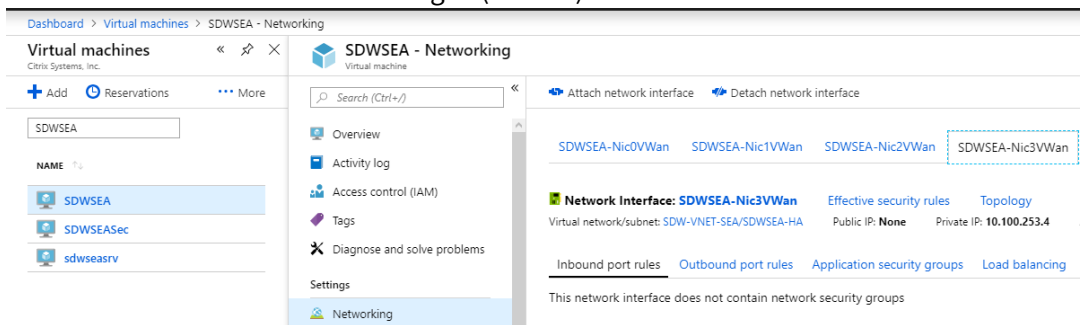
- Repeat the procedure for the secondary Citrix SD-WAN appliance.

2. Determine the SD-WAN ALB Public IP. Navigate to **Load Balancers > sdwanha-external**. Select the correct ALB based on the Resource Group created during the deployment.
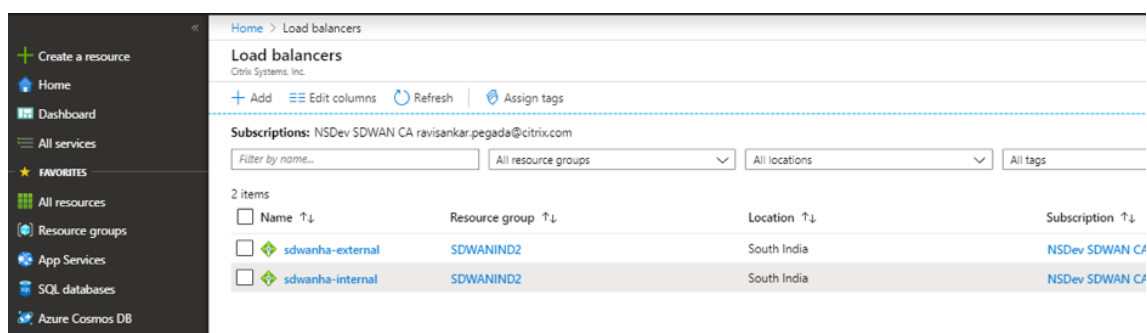
You can see 2 load balancer as following:

- **External**: External LB contains the public IP that you configure in the WAN link configuration.
- **Internal**: Internal LB contains private IP. All LAN side traffic comes to the internal LB. So you can configure the route table with Internal LB IP as a next hop.

3. Proceed to the SD-WAN MCN appliance or SD-WAN Center to configure the SD-WAN HA site. In this topic, the SDWSWEA and SDWSEASec appliances are the MCN appliances.

   > **Note**
   >
   > You can configure Citrix SD-WAN HA in Azure through SD-WAN Orchestrator as well.

4. The SDWANSEA and SDWANSEASec Interface Group Configuration is provided as follows. Bypass mode is set to fail-to-block since only one Ethernet/physical interface is used per virtual interface. The WAN Interface must be set to **Trusted** to accept connections from the ALB.
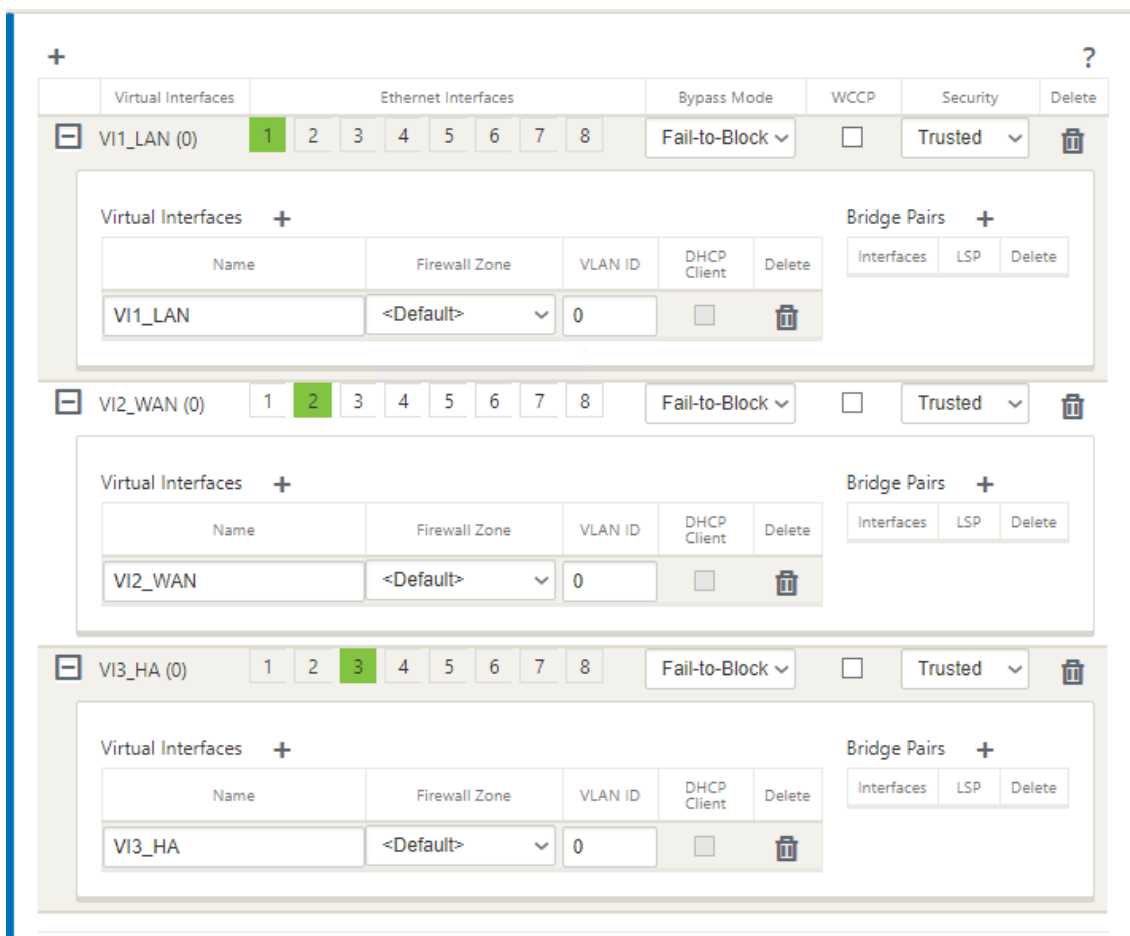
5. The Virtual IP configuration is provided as follows. Note the HA VIP is not the IP addressed assigned to Interface three. Use an available IP address in the appropriate subnet (the subnet assigned to the AUX interface) and not the IP assigned to the Citrix SD-WAN appliances. Note only one VIP in each subnet is the Identity IP.

Two virtual IPs are assigned for both LAN and WAN Virtual Interfaces. One IP belongs to **Primary SD-WAN Virtual Machine** and the other IP belongs to **Secondary SD-WAN Virtual Machine** both on LAN and WAN respectively. Only the **Primary IP** is enabled with Identity.

6. The SDWANSEA WAN Link Settings are provided as follows. Note to configure **External load balancer Public IP Address** as part of **WAN link Public IP Address** setting. The SD-WAN license determines the bandwidth settings.

7. The **Access Interface** settings are as follows. The 10.100.0.1 IP is an Azure reserved IP.

8. HA settings are as follows. The primary and secondary IP address as part of this HA setting must be configured with the AUX Interface IP address of both **Primary and Secondary Virtual Machines** respectively.

9. Click **Apply**.

10. To have LAN traffic go through SD-WAN, add a route table on Azure with a route whose next hop points to Azure Internal Load-balancer IP. And associate the LAN subnet to the route table created.

   If at all you must route all the traffic through SD-WAN, create a default route whose next-hop is pointing to Internal Load balancer IP.

Deploy a Citrix SD-WAN VPX instance on a Citrix ADC SDX appliance

June 27, 2019

Citrix SD-WAN technology applies software-defined networking (SDN) concepts to WAN connections. The technology abstracts traffic management and monitoring from network hardware and applies them to individual applications. The result is improved performance, high-quality user experiences over geographically dispersed locations, and simplified deployment of wide-area and cloud-access networks. For more information, see Citrix SD-WAN.

From release 12.1 49.xx, you can deploy a Citrix SD-WAN VPX instance on Citrix ADC SDX 14XXX and SDX 115XX appliances. For more information, see the following documents:

- Citrix ADC SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080, and SDX 14100

- Citrix ADC SDX 11515, SDX 11520, SDX 11530, SDX 11540, and SDX 11542

Note

Only SD-WAN VPX Standard edition is supported. For more information, see SD-WAN VPX edi-

---

tions.

Deploying a Citrix SD-WAN VPX instance on an SDX appliance includes the following tasks:

- Installing the hardware: ensure the SDX hardware is properly installed. For more information, see Installing the Hardware.
- Setting up and configuring the SDX Management Service. For more information, see Getting Started with the Management Service User Interface and Configuring the Management Service.
- Provisioning the SD-WAN VPX instance on the SDX appliance. For more information, see Provision the Citrix SD-WAN VPX instance on a Citrix ADC SDX.
- Configuring the SD-WAN VPX instance. For more information, see the Configuration documentations and Configuring the virtual path service between the MCN and client sites.

Prerequisites

Ensure you've the following licenses:

- Citrix SD-WAN VPX license
- Citrix ADC SDX platform license

Citrix SD-WAN VPX requirements

The Citrix SD-WAN VPX on SDX platform can act both as a site and MCN. The MCN can handle 1 Gb/s bidirectional throughput and 64 sites.

Supported throughput for MCN and site

- 250 Mb/s to 1 Gb/s bidirectional throughput
- MCN supports 64 sites

Hardware requirement for supported throughput

Site

- 4 CPUs to 16 CPUs
- 4 GB to 16 GB RAM
- 60 GB to 250 GB disk storage
- Minimum 4 NICs: one for management and remaining minimum 3 for data path

Master control node (MCN)

- 4,8, and 16 CPUs
- 16 GB RAM
- 250 GB disk storage

- Minimum 4 NICs: one for management and remaining 3 for data path, with dedicated NICs for data path

Data center topology

You can deploy a Citrix SD-WAN VPX appliance on a Citrix ADC SDX in policy-based route (PBR) mode or in inline mode. See scenario 1 and 2 for topologies for these two supported modes. For more information, see Deploying SD-WAN in PBR mode (Virtual Inline Mode).

Scenario 1. Data center topology: PBR mode or virtual inline mode
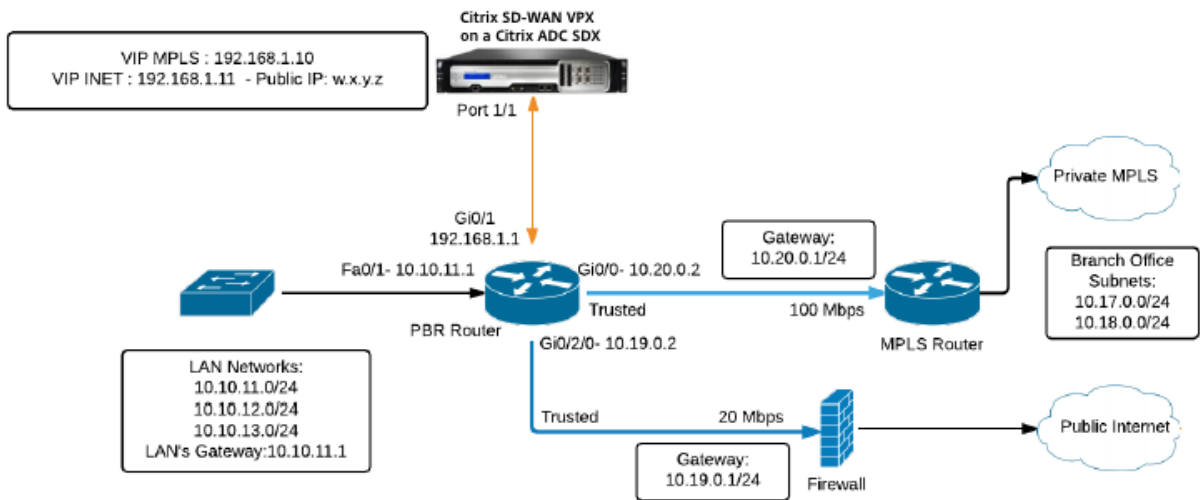
Scenario 2. Branch topology: Inline mode
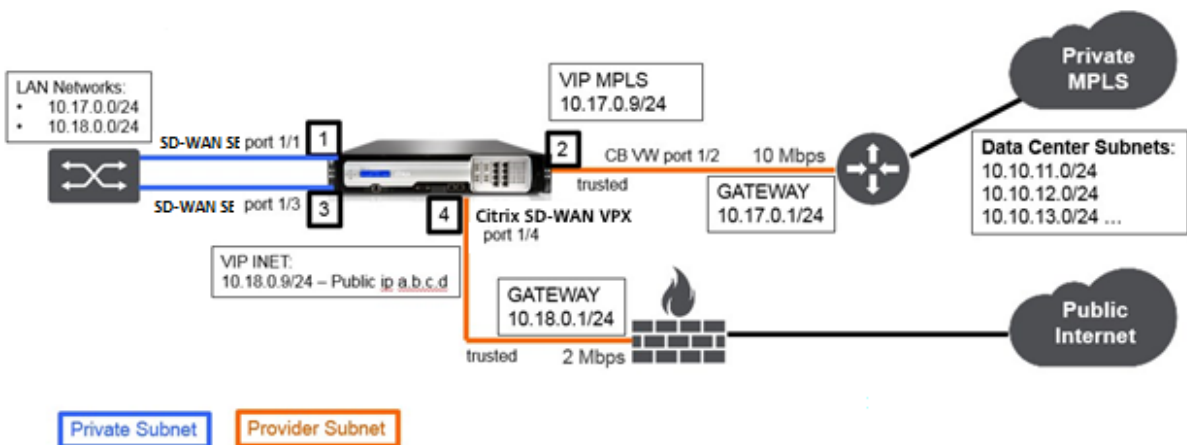
Provision the Citrix SD-WAN VPX instance on a Citrix ADC SDX

Before you provision the Citrix SD-WAN VPX appliance, download the SD-WAN VPX image from the Citrix product download site.

Follow these steps to provision the Citrix SD-WAN VPX appliance.

1. Log on to the Citrix ADC SDX appliance.

2. Navigate to **Configuration > SD-WAN > Instances**.

3. Select **Software Images > Upload** and upload the SD-WAN XVA file.

4. Select Instances > Add. The Provision SD-WAN Instance page appears.

5. In the Provision SD-WAN Instance page, enter the following:

   - Name
   - IP address
   - Netmask
   - Gateway address
   - Upload the XVA file
   - Under **Resource Allocation**, allocate resources.
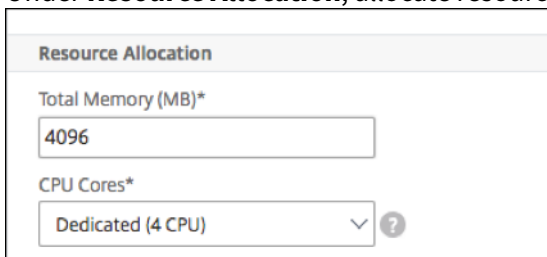
   - Under **Network Settings**, provision management interfaces and select **OK** to create to provision the SD-WAN VPX instance on the SDX appliance.
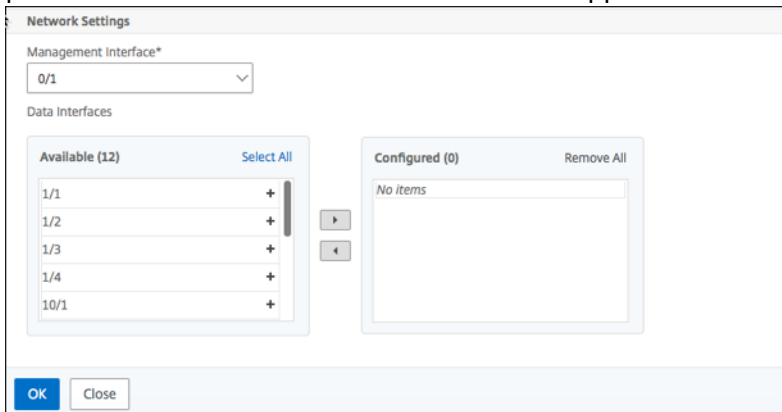
> **Note**
>
> The SDX Management Service binds interfaces to the VPX instance in ascending sequence of interface names. For example, if you add 1/4, and 1/1, Management Service arranges them as 1/1, 1/4. When you add new interfaces, the existing sequence is retained and a new sequence is created. For example, you add interfaces 1/2, 10/1, 1/3.The new sequence would be 1/1, 1/4; 1/2, 1/3, 10/1.

6. The SD-WAN VPX instance appears under the **Instance page**. Here's an example.

To edit the instance, navigate to **Configuration > SD-WAN > Instances**. Select and click the instance. Once you've completed editing, click **OK** to save the changes.

Configuring the Citrix SD-WAN VPX instance

After you've created an SD-WAN instance on the SDX appliance, configure the SD-WAN instance by completing these two tasks:

1. Apply configuration for both MCN and site appliances.

2. Configure virtual path and transmit traffic.

For more information, see the following topics:

- Configuration
- Configuring the virtual path service between the MCN and client sites

Related information

For more information about getting started with a Citrix SD-WAN appliance, see Citrix SD-WAN.

For more about Citrix ADC SDX appliance, see Citrix ADC SDX.

Standard Edition in AWS for Cloud watch Support

May 23, 2019

Citrix SD-WAN Standard Edition in AWS now supports basic CloudWatch for monitoring your SD-WAN instance running on AWS infrastructure. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring. Under basic monitoring, seven pre-selected metrics at five minute frequency and three status check metrics at one minute frequency are available for your SD-WAN instance for no additional charge. You can view the following metrics for your SD-WAN image.

- CPU Utilization - The percentage of allocated compute units that are currently being used for the instance. This metric identifies the processing power required to run an application upon a selected instance.
- Disks read operations - Read operations from all instance volumes available for the specified period.
- Disk Write operations – Write operations for all instance store volume available for the instance in a specified duration of time.
- DiskReadBytes – Bytes written to all instance store volumes available to the running instance
- Networking – This metric identifies the volume of incoming traffic for a single instance.
- Network Out - This metric identifies the volume of outgoing traffic for a single instance.
- Networkpacketsout – Number of packets sent out on all network interfaces by the instance, this is only available for basic monitoring.

Citrix SD-WAN VPX WANOP

June 19, 2020

Citrix SD-WAN WANOP VPX is a virtual Citrix SD-WAN appliance that can be hosted on Citrix XenServer, VMware ESX or ESXi, Microsoft Hyper-V, and Amazon AWS-virtualization platforms. An SD-WAN WANOP VPX appliance supports most of the features of a physical SD-WAN WANOP appliances.

Because SD-WAN WANOP Edition VPX is a virtual machine, you can deploy your choice of hardware, exactly where you need it, and in combination with other virtual machines, servers, VPN units, or other appliances to create a unit that precisely suits your needs.

Citrix SD-WAN WANOP VPX software is available as:

- A Xen virtual machine running under XenServer 5.5 and later.
- A VMware vSphere virtual machine running under ESX/ESXi 4.1–6.0.
- A Hyper-V virtual machine under 64-bit Windows 2008 R2 SP1 - 2012.
- An Amazon AWS instance.
- A Microsoft Azure Instance.

> **Note**
>
> XenServer and VMware vSphere support VLAN trunking, but Hyper-V does not.

For information on configuring SD-WAN WANOP VPX on XenServer, VMware ESX, Microsoft Hyper-V, and Amazon AWS, see Pages 691 - 749 in CloudBridge 7.4 PDF.

When a newly installed SD-WAN WANOP VPX virtual machine is up and running, you can configure it as you would configure a physical SD-WAN WANOP appliance. For more information, see Citrix SD-WAN WANOP documentation.

Installing SD-WAN WANOP Edition AMI on Amazon AWS

May 23, 2019

The Citrix SD-WAN VPX for Amazon AWS brings acceleration support to the Amazon cloud.

> **Note**: At the time of the 7.1.0 software release, the newest supported release of SD-WAN (now SD-WAN) WANOP-VPX for Amazon AWS is 7.0.1. Use this version along with release 7.1.0 on other appliances.

Five variations are supported, four of which have hardwired licensing, and one of which uses ordinary SD-WAN licensing:

- 2 Mbps
- 10 Mbps
- 20 Mbps
- 45 Mbps
- "Bring your own license," which uses a standard Citrix license to determine the licensed bandwidth.

Besides the hardwired licensing, the major difference between SD-WAN WANOP-VPX for Amazon AWS is that it supports only a single port for both management and acceleration. This means that the appliance cannot be used in inline mode.

To create an SD-WAN WANOP-VPX on Amazon AWS, you go through the same process as with creating any other instance, setting a few instance parameters to non-default settings.

Instantiating an SD-WAN virtual Appliance (AMI) on AWS

To install an SD-WAN virtual appliance in an AWS VPC, you need an AWS account. You can create an AWS account at http://aws.amazon.com/. SD-WAN is available as an Amazon Machine Image (AMI) in AWS Marketplace.

> **Note**: Amazon makes frequent minor changes to its AWS pages, so the following instructions may not be exact.

To instantiate an SD-WAN virtual appliance (AMI) on AWS

1. In a web browser, type http://aws.amazon.com/.

2. Click **My Account/Console**, and then click **My Account** to open the **Amazon Web Services Sign in** page.

3. Use your Amazon AWS account credentials to sign in. This takes you to the Amazon Web Services
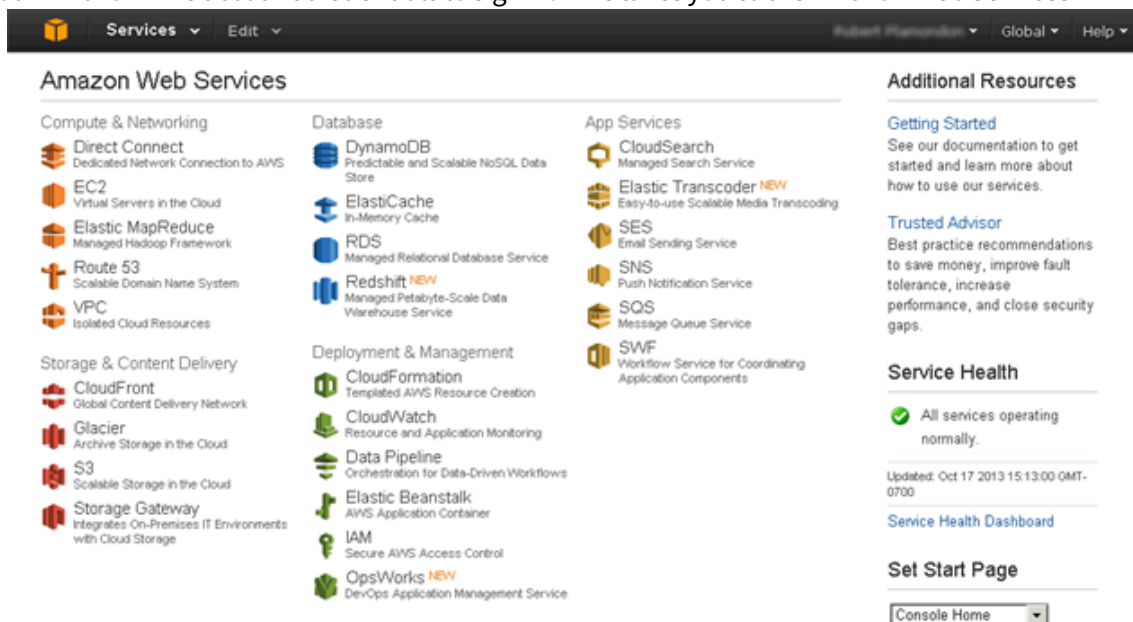
   page.

4. Click EC2 in the Compute & Networking section, then click **Launch Instance**.
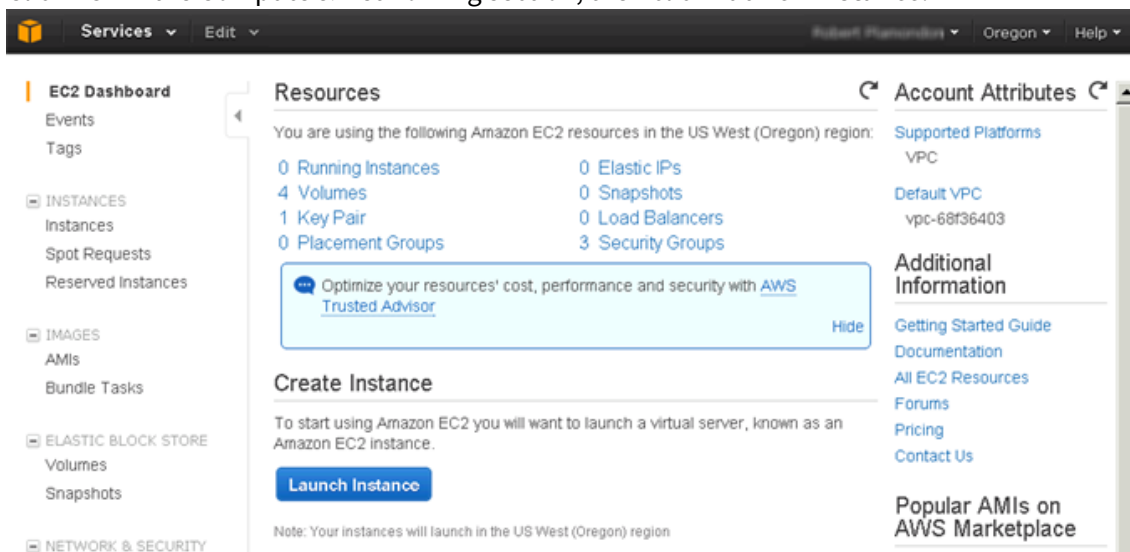
5. In the **Create a New Instance** dialog box, select **AWS Marketplace**, and then click **Continue** to open the **Request Instance Wizard**.

6. In the **Request Instance Wizard** dialog box, click **AWS Marketplace** tab.

7. In the Search text field, type SD-WAN to search for the SD-WAN AMI, and click **Search**.
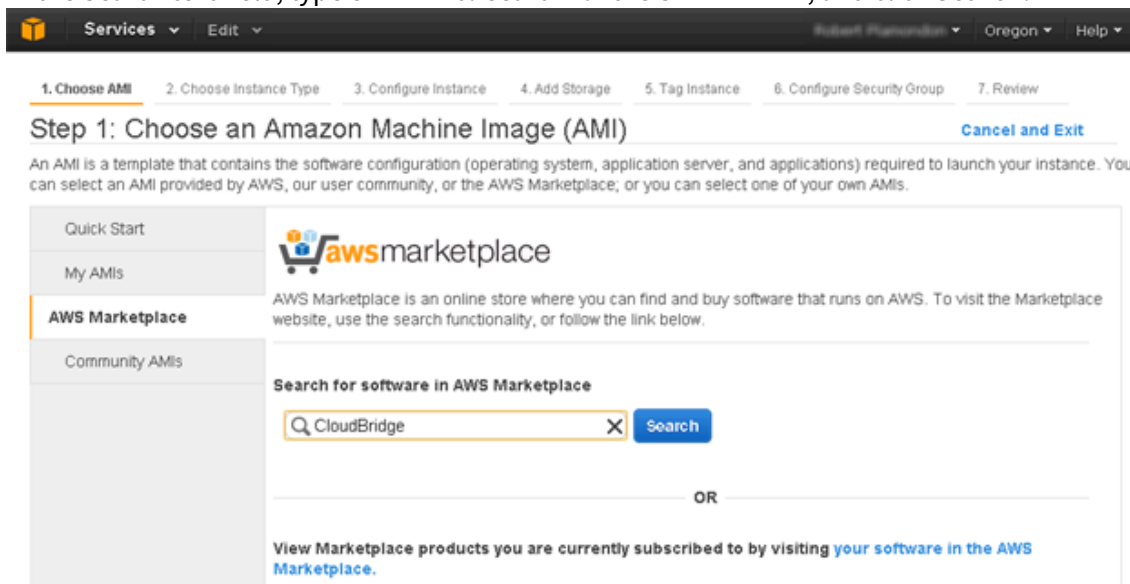
On the search result page, select one of the Citrix SD-WAN offerings On the Citrix SD-WAN page, click **Continue**.

8. On the Launch with EC2 Console tab, click the **Accept Terms** button, if present, then click **Launch** with EC2 Console for the region where you want to launch Citrix SD-WAN AMI.

9. On the Request Instance Wizard page, type 1 in the **Number of Instances** text box, and from the **Instance Type** drop-down list, select Large (m1.large, 7.5GIB).

10. From the **Subnet** drop-down list, select the private network subnet, and then click **Continue**.

11. On the next page, in the **Advanced Instance Options** section, you can change values from their defaults if you choose, and then click **Continue**.

    > **Note**: SD-WAN AMI is not supported with more than one network interface. Therefore, the value of Number of Network Interfaces fields is set to 1.!localized image

12. On the Request Instances Wizard page, enter a name for the EC2 instance in the **Value** text box, and then click **Continue**.

    On the Request Instances Wizard page, select one of the three Kay Pair options and then click **Continue**.
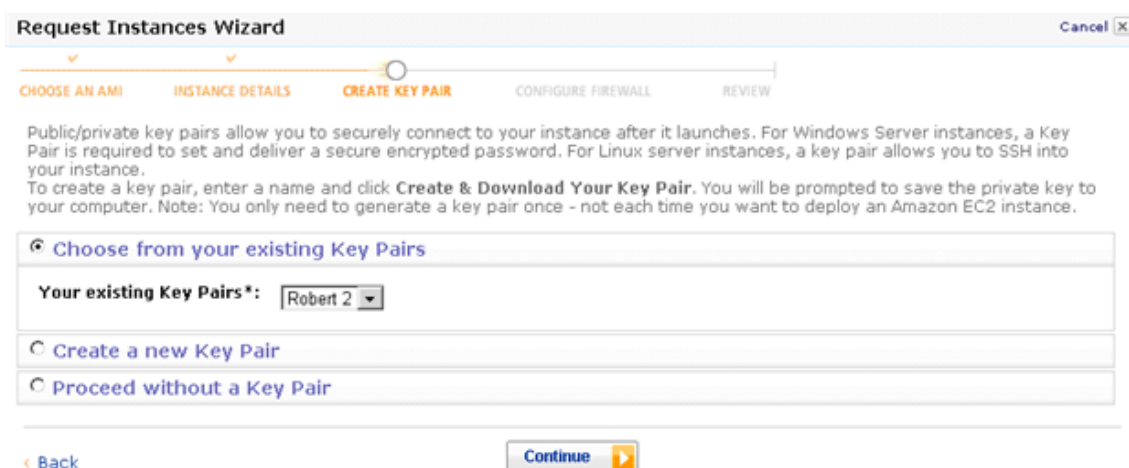
13. Verify the EC2 instance configuration details, and then click **Launch** to launch the EC2 instance.
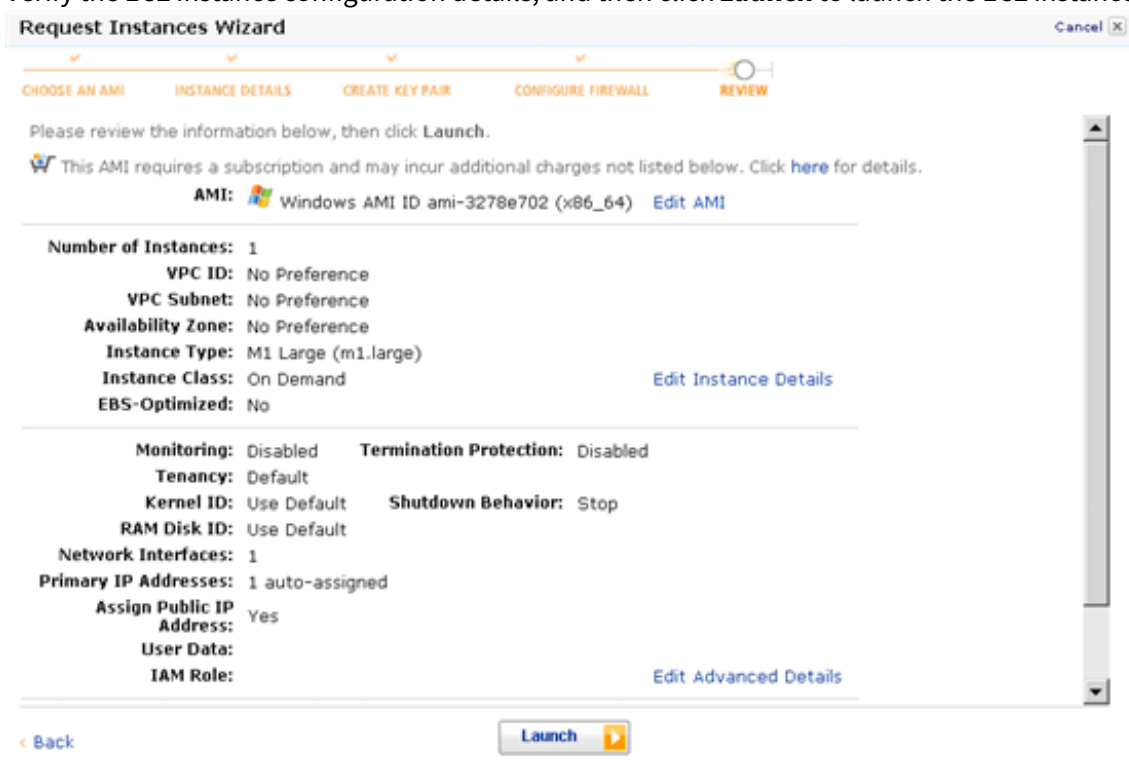
14. Click **Close** to close the **Launch Instance Wizard** dialog box. The new EC2 instance is launched successfully.
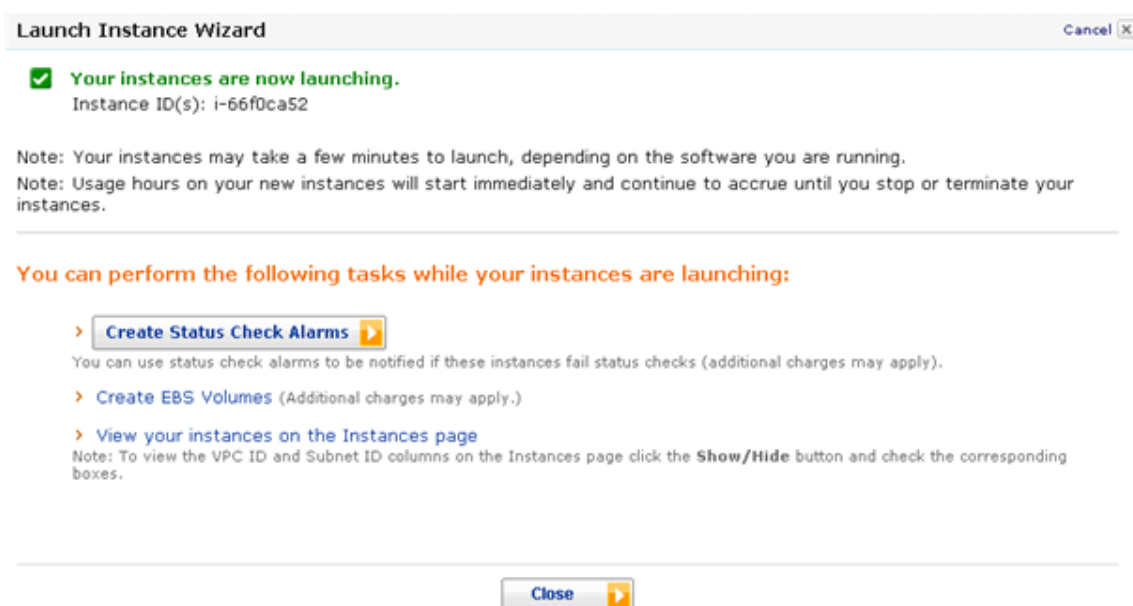
Disabling the Source/Destination Check Feature

May 23, 2019

You must disable the Source/Destination check feature of SD-WAN AMI instance for it to work properly on AWS.

To disable the Source/Destination check feature

1. On the Amazon EC2 Console Dashboard page, in the navigation pane, click instances. The new EC2 instance should appear in the My Instances list.
2. Select the new EC2 instance. The instance details appear in the EC2 Instances pane.
3. Right-click the new EC2 instance and then select **Change Source/Dest Check** from the popup menu.
4. In the Change Source / Dest. Check dialog box, click **Yes**, Disable to disable the feature.

Configuring SNMP Monitoring for the SD-WAN WANOP Edition AMI on AWS

May 23, 2019

You must enable SNMP monitoring on the SD-WAN AMI on AWS. Also, you must grant SNMP monitoring access to the paired NetScaler VPX or SD-WAN Connector on AWS by adding its NSIP on the SD-WAN AMI instance.

To configure SNMP monitoring on the SD-WAN Connector AMI by using the SD-WAN graphical user interface

1. In the navigation pane, expand **Configuration**, and then click **Logging/Monitoring**.
2. In the details pane, click the **SNMP** tab.
3. In the **System Information** section, in the **SNMP Status row**, click **Enable**. This action enables SNMP monitoring on the SD-WAN AMI instance.
4. In the **Access Configuration** section, add SNMP monitoring access to **SD-WAN VPX appliance by** setting the following parameters:
   - Community String (set to the string public)
   - Management Station IP (set to the NSIP of the SD-WAN VPX on AWS)

5. Click **Add**.

Limitations and Usage Guidelines for the SD-WAN WANOP Edition AMI Instances on AWS

May 23, 2019

- High Availability setup for SD-WAN AMI instances is not supported.
- SD-WAN AMI instance in Group Mode is not supported.
- SD-WAN plug-ins are not supported.
- Tagged VLAN is not supported because of the inherent limitation of AWS.
- Traffic shaping is not supported.
- You may create only an m1.large SD-WAN AMI instance on AWS.
- IP address/gateway/subnet assignment using the SD-WAN management user interface is not supported.
- Console access is not available for SD-WAN AMI instance on AWS.
- While configuring the SD-WAN instance, you may not change the disk size, which has a default value of 250 GB. A higher capacity disk does not increase the available Disk Based Compression (DBC) cache size.

Deploy SD-WAN WANOP VPX on Microsoft Azure

June 19, 2020

Citrix SD-WAN WANOP Edition is now available in the Azure Marketplace, enabling WAN optimization between enterprise datacenter/branch and Azure cloud. Since L2 mode support is not available on cloud infrastructures, you cannot deploy Citrix SD-WAN WANOP as a standalone VPX in Azure Cloud. However, you can deploy Citrix SD-WAN WANOP VPX along with Citrix ADC VPX in Azure cloud infrastructure. The Citrix ADC VPX uses cloud connector to create an IPsec tunnel, while the SD-WAN WANOP VPX accelerates the connections, providing LAN-like performance for applications.

Citrix SD-WAN WANOP in Azure cloud topology
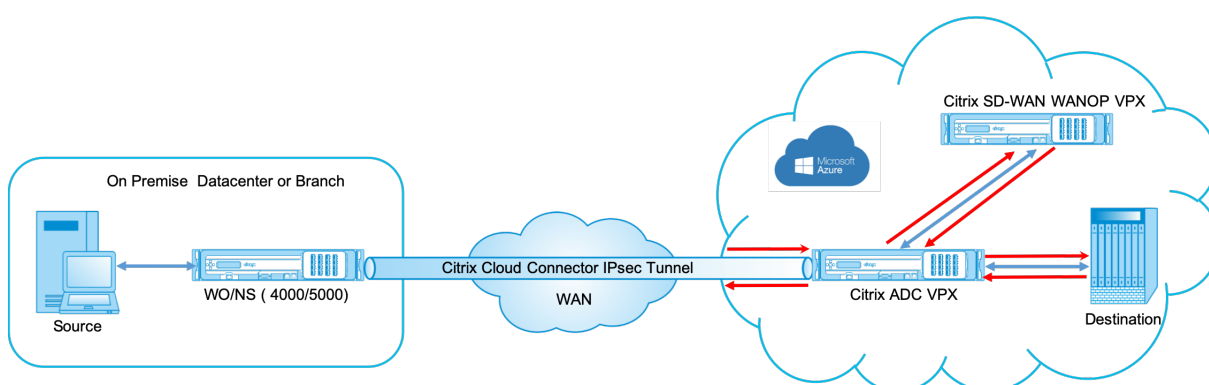
The topology diagram shows an SD-WAN 4000 or 5000 appliance deployed in the data center or branch premises. You can also deploy SD-WAN WANOP and SD-WAN SE appliances in two-box mode or it can both be VPX. On the Azure cloud VNET, the SD-WAN WANOP VPX is deployed in one-arm (PBR) mode with the Citrix ADC VPX.

Deployment overview

To deploy SD-WAN WANOP on Microsoft Azure:

1. Deploy a Citrix ADC VPX instance on the Azure cloud. For more information, see Deploy a Citrix ADC VPX instance on Microsoft Azure. Configure four network interfaces in four different subnets and enable IP forwarding on all the network interfaces. The four network interfaces are used as:

   - Management interface
   - WAN side interface, for IPsec tunnel
   - LAN side interface, to connect to the server
   - WANOP communication interface, to communicate with the Citrix SD-WAN WANOP VPX on the Azure cloud.

2. Deploy a Citrix SD-WAN WANOP VPX on Azure cloud. For more information, see the deployment procedure below.

   > **Note**: Enable IP forwarding on WANOP interface.

3. Configure an IPsec tunnel between the on-premises appliance and the Citrix ADC VPX on Azure cloud, using the public IP address of Citrix ADC WAN interface. For more information on configuring IP tunnels see, IP Tunnels.

4. Configure Citrix ADC VPX to redirect the packets to Citrix SD-WAN WANOP VPX. Use the private IP address of WANOP communication interface and create a load balancing virtual server. For more information, see Create a load balancing virtual server

5. Configure the following route tables on Azure:

   - Route table for WANOP facing interface on Citrix ADC VPX – Route table entries must have source and destination address as client and server subnets respectively. The Citrix ADC VPX's WANOP facing interface IP address is the next hop.
   - Route table for Citrix SD-WAN WANOP interface - Route table entries must have source and destination address as client and server subnets respectively. The Citrix SD-WAN WANOP interface IP address is the next hop.

In the above example, when the source tries to access an application on the cloud destination, the packets flow through the established IPsec tunnel. At the Azure cloud VNET end, the Citrix ADC VPX receives the packets, decrypts, and forwards it to the Citrix SD-WAN WANOP VPX. The Citrix SD-WAN WANOP VPX processes the packets, optimizes it, and sends it back to Citrix ADC VPX. The Citrix ADC VPX sends the packet to the destination. On the return path, the Citrix ADC VPX forwards the packets to Citrix SD-WAN WANOP VPX for optimization. The optimized packets are transmitted back to the source through the established IPsec tunnel.

Deploy Citrix SD-WAN WANOP VPX on Microsoft Azure

To deploy Citrix SD-WAN WANOP VPX on Microsoft Azure:

1. In Microsoft Azure, navigate to **Home** > **Marketplace** > **Networking**, search for **Citrix SD-WAN WANOP** and install it.

2. On the Citrix SD-WAN WAN OP page, from the drop-down list select **Resource Manager** and click **Create**. The **Create Citrix SD-WAN WAN Optimization** page appears.

3. In the **Basics** section, select the subscription type, resource group, and location. Click **OK**.

   Note: You can choose to create a resource group. A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group.
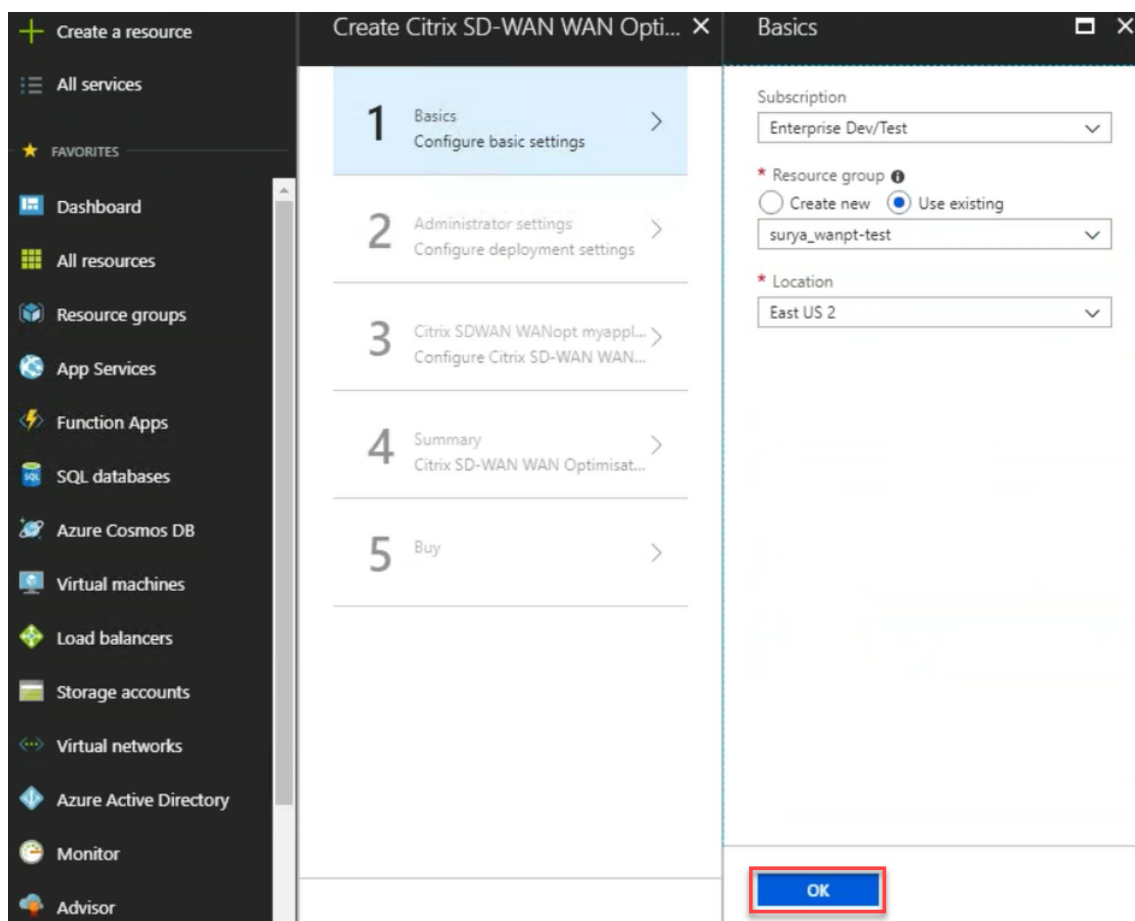
4. In the **Administrator** section, enter the name and credentials for the Citrix SD-WAN WANOP virtual machine. Click **OK**.

Citrix SD-WAN Platforms
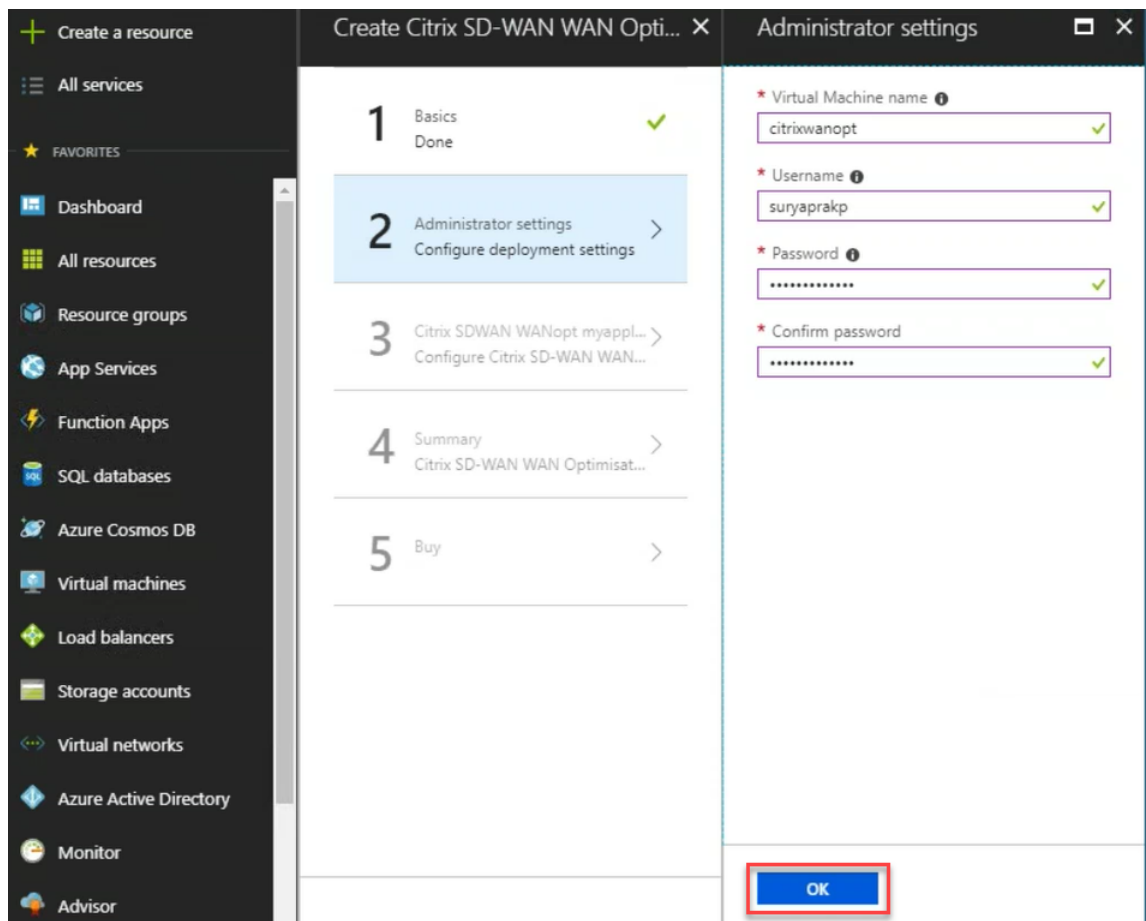
5. In the **Citrix SD-WAN WANOP settings section**, configure the setting for the Citrix SD-WAN WANOP VPX as per your requirements. Click **OK**.
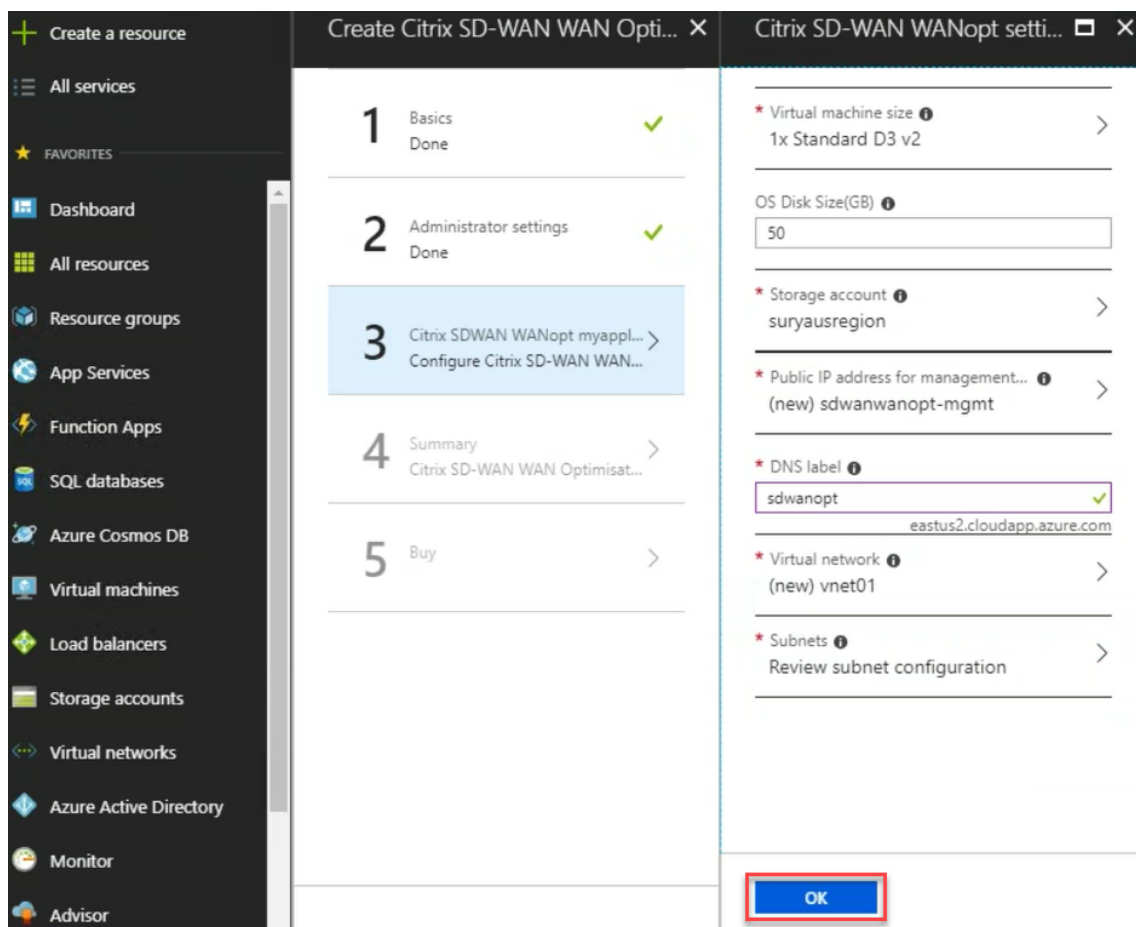
6. The configuration that you provided in previous steps is validated and applied. If you have configured correctly, the validation passed message appears. Click **OK**.
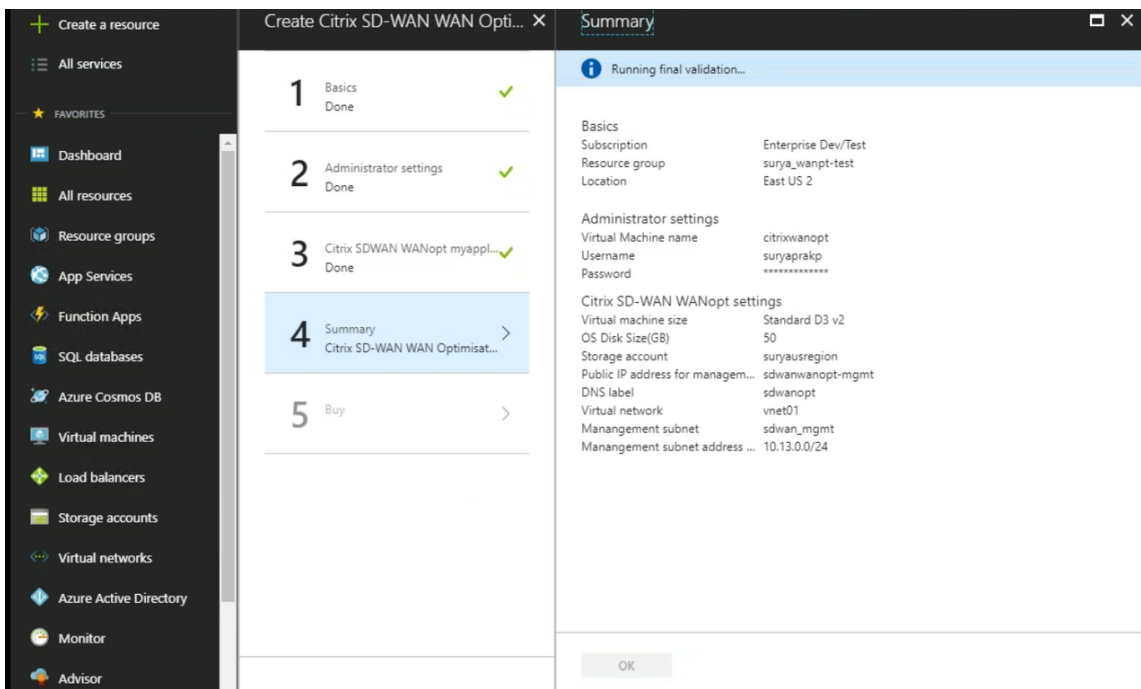
7. After successful deployment, navigate to **Virtual Networks** to view the Citrix SD-WAN WANOP VPX. You can further configure the virtual machine parameters using the settings option.
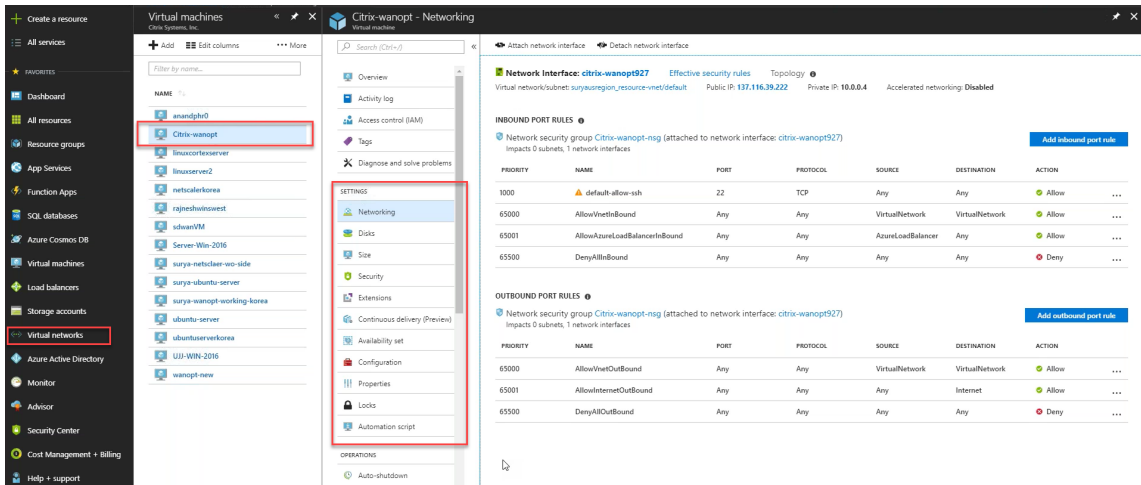
Citrix SD-WAN VPXL

October 8, 2021

Citrix SD-WAN VPXL-SE is an enhanced version of the SD-WAN VPX-SE platform. Depending on the RAM/CPU/Disk configuration, the VPX platform can be operated either as VPX-SE or VPXL-SE. It is available on all VPX-SE platforms including Azure and AWS.

The Citrix SD-WAN VPXL-SE platform can handle up to 256 virtual paths when provisioned as an MC-N/RCN.

Following are the configuration requirements for the VPXL-SE platform.

- 16 GB memory and 16 CPU cores.
- 250 GB of HDD.

The number of virtual paths and dynamic virtual paths that the SD-WAN VPXL-SE platform can handle, irrespective of the appliance role (MCN, RCN, or Client) is as follows:

Memory	Less than 16 GiB	More than 16 GiB
Virtual Path	16	256
Dynamic Virtual Path	8	32

Interface specifications

The SD-WAN VPXL-SE interface specifications are as follows:

- SD-WAN VPXL-SE supports a maximum number of eight interfaces.
- The first interface is reserved to be used as the Management IP Address for the Virtual Appliance.
- Before powering up the new VM for the SD-WAN VPXL-SE Virtual Appliance, you must configure and assign more interfaces (one each) for the LAN and WAN.
- For SD-WAN VPXL-SE, bridges are not created by default for the data interface (for example, eth1 and eth2).

Configuring Citrix SD-WAN VPXL-SE

To configure SD-WAN VPXL-SE:

1. Import the SD-WAN VPX-SE base image (.ova or.xva template). Do not **Power ON** the Virtual machine.
2. Modify the VM resources for Memory to 16 GB RAM, CPU to 16vCPUs and hard disk size to 250 GB.
3. Add the required NIC interfaces to the VM (for LAN and WAN interfaces).
4. **Power ON** the VM.
5. Now, SD-WAN VPX-SE would operate as a VPXL-SE platform model.
6. In case the VM is already Powered ON, before modifying the VM resources, you must perform **Reimage Virtual WAN Appliance Software** under **Configuration** > **System Maintenance**> **Update Software**, and use the **cb-vw_CBVPXL_version.tar.gz** image file.

> **Note**
>
> Ensure to clear options that mention to Power on the Virtual machine, after the VM provisioning/import process is complete.

How to upgrade VPX-SE to VPXL-SE

To upgrade VPX-SE to VPXL-SE:

1. The VPX-SE should have been installed with an SD-WAN base release version of 9.3.0 or higher.
2. Backup and save your existing configuration, if the VPX-SE you are upgrading is an MCN.

> **Important**
>
> A VPX-SE appliance provisioned with an SD-WAN release version 9.2 image cannot be upgraded to a VPXL-SE appliance.
>
> To use the VPXL-SE platform, upgrade SD-WAN release version 9.2. to 9.3 using the change management procedure in the SD-WAN web GUI.
>
> For more information, see upgrading to SD-WAN 9.3.

Deploying VPXL-SE in Microsoft Azure and AWS

The steps to configure and deploy VPXL-SE in Microsoft Azure are similar to the steps to deploy the VPX-SE appliance in Azure. The only difference in the configuration steps is to choose hard disk space as 250 GB and instance as F8 for the VPXL-SE appliance to be successfully deployed in Azure.
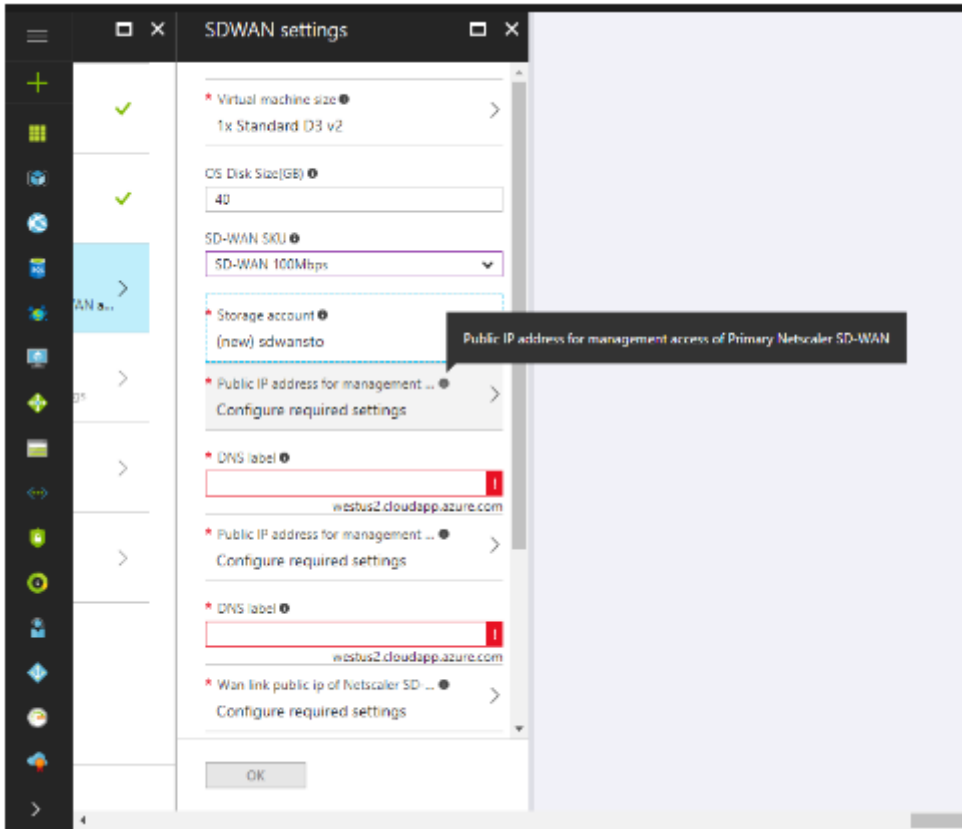
Similarly, the steps to configure and deploy VPXL-SE in AWS is similar to the steps for deploying VPX-SE appliance in AWS with the only difference of selecting disk size of 40 GB and instance of m4.4x large.
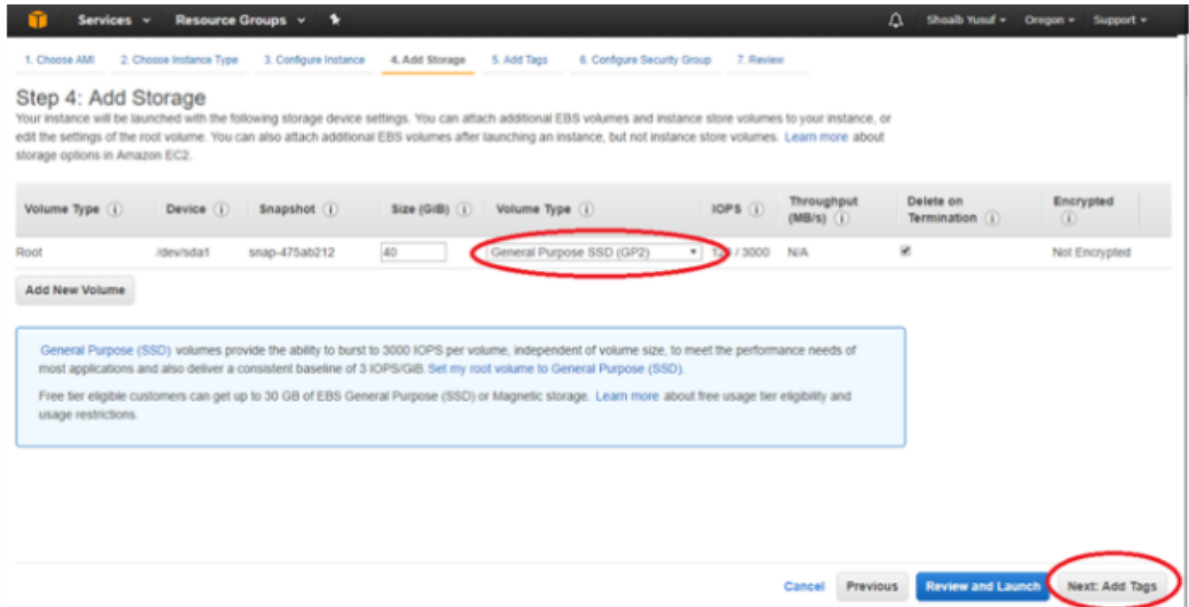
Related information

- [Installing SD-WAN Virtual Appliances on VMware ESXi](#)
- [Installing SD-WAN Virtual Appliances on Microsoft Hyper-V Platform](#)
- [Installing SD-WAN Virtual Appliances on Amazon Web Services](#)
- [Installing SD-WAN Virtual Appliances on Microsoft Azure](#)
- [SD-WAN Standard Edition Virtual Appliance (VPX) high availability Support for AWS](#)
- [SD-WAN Standard Edition Virtual Appliance (VPX) high availability Support for Microsoft Azure](#)

Common hardware components

June 19, 2020

Each platform has front panel and back panel hardware components. The front panel has an LCD display and serial console port. The number, type, and location of ports vary by hardware platform for the following transceivers: copper Ethernet, copper and fiber 1G SFP, and 10GSFP+. The back panel provides access to the fan and the field replaceable units (power supplies, and solid-state and hard-disk drives).

LCD display and LED status indicators

The LCD display on the front of every appliance displays messages about the current operating status of the appliance. These messages communicate whether your appliance has started properly and is operating normally. If the appliance is not operating normally, the LCD displays troubleshooting messages.

The LCD displays real-time statistics, diagnostic information, and active alerts. The dimensions of the LCD limit the display to two lines of 16 characters each, causing the displayed information to flow through a sequence of screens. Each screen shows information about a specific function.

The LCD has an LED backlight. Normally, the backlight glows steadily. When there is an active alert, it blinks rapidly. If the alert information exceeds the LCD screen size, the backlight blinks at the beginning of each display screen. When the appliance shuts down, the backlight remains on for one minute and then automatically turns off.

The system status LEDs indicate the overall status of the appliance. The following table describes the indicators of the system status LED.

System status LEDs

LED Color	LED Indicates
OFF	No power.
Green	Appliance is receiving power.
Red	Appliance has detected an error.

The port LEDs show whether a link is established and traffic is flowing through the port. The following table describes the LED indicators for each port. There are two LED indicators for each port type.

Note: This section applies to all the appliances.

LED port-status indicators

Port Type	LED Location	LED Function	LED Color	LED Indicates
Ethernet (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Yellow	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.
Management (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).

Port Type	LED Location	LED Function	LED Color	LED Indicates
			Green	Traffic rate of 100 Mbps.
			Amber	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid yellow	Link is established but no traffic is passing through the port.
			Blinking yellow	Traffic is passing through the port.

On each power supply, a bicolor LED indicator shows the condition of the power supply. The LEDs of the AC power supplies for each appliance are different from the LEDs of the other appliances.

Table 2. LED Power Supply Indicators

Power Supply Type	LED Color	LED Indicates
AC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing GREEN	Power supply is in standby mode.
	GREEN	Power supply is functional.
	RED	Power supply failure.
DC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing BLUE	Power supply is in standby mode.

Power Supply Type	LED Color	LED Indicates
	BLUE	Power supply is functional.
	RED	Power supply failure.

Ports

Ports are used to connect the appliance to external devices. Citrix SD-WAN appliances support RS232 serial ports, 10/100/1000Base-T copper Ethernet ports, 1-gigabit copper and fiber 1G SFP ports, 10-gigabit fiber SFP+, and 10G Base-T, ports. All Citrix SD-WAN appliances have a combination of some or all of these ports. For details on the type and number of ports available on your appliance, see the section describing that platform.

RS232 serial port

The RS232 serial console port provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

All hardware platforms ship with an appropriate serial cable used to connect your computer to the appliance. For instructions on connecting your computer to the appliance, see Installing the Hardware.

Copper Ethernet ports

The copper Ethernet ports installed on many models of the appliance are standard RJ45 ports.

There are two types of copper Ethernet ports that may be installed on your appliance:

- 10/100BASE-T port

  The 10/100BASE-T port has a maximum transmission speed of 100 megabits per second (Mbps). Most platforms have at least one 10/100BASE-T port.

- 10/100/1000BASE-T port

  The 10/100/1000BASE-T port has a maximum transmission speed of 1 gigabit per second, 10 times faster than the other type of copper Ethernet port.
  Most platforms have at least one 10/100/1000Base-T port.

To connect any of these ports to your network, you plug one end of a standard Ethernet cable into the port and plug the other end into the appropriate network connector.

Management ports

Management ports are standard copper Ethernet ports (RJ45), which are used for direct access to the appliance for system administration functions.

1G SFP and 10G SFP+ ports

A 1G SFP port can operate at a speed of 1 Gbps. It accepts either a copper 1G SFP transceiver for operation as a copper Ethernet port, or a fiber 1G SFP transceiver for operation as a fiber optic port.

The 10G SFP+ and Base-T 10G are high-speed ports. You need a fiber optic cable to connect to a port. If the other end of the fiber optic cable is attached to a 1G SFP port, the 10G SFP+ port automatically negotiates to match the speed of the 1G SFP port.

Ports compatibility:

On some appliances, the 10G slot supports copper 1G transceivers, which can operate at up to 1 Gbps in a 10 Gbps slot.

Notes:

- Certain platforms have 10G slots that do not support copper transceivers. Check with your account representative for support details.
- You cannot insert a fiber 1G transceiver into a 10G slot.
- You cannot insert a 10G transceiver into a 1G slot.

The following tables list the maximum distance specifications for Citrix SD-WAN pluggable media (1G SFP and 10G SFP+ transceivers).

The 10G SFP+, modules are dual-speed capable and support both 1 Gbps and 10 Gbps, depending on the peer switch that the model connects to.

Most tables have the following columns:

- Description: The price list description of the part.
- Transmit Wavelength: The nominal transmit wavelength.
- Cable/Fiber Type: Fiber characteristics affect the maximum transmit distance achievable. This is especially true with 10G on multi-mode fiber (MMF), where various dispersion components become dominant. For more information, see http://www.thefoa.org/tech/ref/basic/fiber.html.
- Typical Reach: Maximum transmit distance.
- Products: Some chassis are available with different media options. Use the appropriate data sheet to confirm that your particular chassis type supports the media.

1G pluggable media

The following table lists the maximum distance specifications for 1G transceivers.

Copper 1G SFP distance specifications

Description: 1G SFP Ethernet copper (100 m) - 4 pack

Transmitter wavelength (nm): Not applicable

Cable type: Category 5 (Cat-5) copper cable

Typical reach (m): 100m

Applicable platforms:

- SD-WAN 1100 SE and PE

Short reach fiber 1G SFP distance specifications

Description: 1G SFP Ethernet SX (300 m) - 4 pack

Transmitter wavelength (nm): 850 nm (nominal)

Fiber type: 50/125um MMF, 2000MHz-km (OM3)
Typical Reach (m): 550 m

Fiber type: 50/125um MMF, 500MHz-km (OM2)
Typical Reach (m): 550m

Fiber type: 50/125um MMF, 400MHz-km
Typical Reach (m): 550m

Fiber type: 62.5/125um MMF, 200MHz-km (OM1)
Typical Reach (m): 300m

Fiber type: 62.5/125um MMF, 160MHz-km
Typical Reach (m): 300m

Applicable platforms:

- SD-WAN 1100 SE and PE

Short reach fiber 1G SFP distance specifications

Description: 1G SFP Ethernet short range (300 m) - Single

Transmitter wavelength (nm): 850 nm (nominal)

Fiber type: 50/125um MMF, 2000MHz-km (OM3)
Typical Reach (m): 550m

Fiber type: 50/125um MMF, 500MHz-km (OM2)
Typical Reach (m): 550m

Fiber type: 50/125um MMF, 400MHz-km

Typical Reach (m): 550m

Fiber type: 62.5/125um MMF, 200MHz-km (OM1)

Typical Reach (m): 275m

Fiber type: 62.5/125um MMF, 160MHz-km

Typical Reach (m): 220m

Applicable platforms:

- SD-WAN 1100 SE and PE

Long reach fiber 1G SFP distance specifications

Description: 1G SFP Ethernet LX - Single

Transmitter wavelength (nm): 1310 nm (nominal)

Fiber type: 9/125um SMF

Typical reach (m): 10 km

Applicable platforms:

- SD-WAN 1100 SE and PE

Long reach fiber 1G SFP distance specifications

Description: 1G SFP Ethernet long range (10 km) - Single

Transmitter wavelength (nm): 1310 nm (nominal)

Fiber type: 9/125um SMF

Typical reach (m): 10 km

Applicable platforms:

- SD-WAN 1100 SE and PE

10 GE pluggable media

The following table lists the maximum distance specifications for 10G transceivers.

Short reach fiber 10G SFP+ distance specifications

Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)
10G SFP+, Ethernet Short Range (300 m) - Single	850 nm (nominal)	50/125um MMF, 2000MHz- km (OM3)	300 m
		50/125um MMF, 500MHz-km (OM2)	82 m
		50/125um MMF, 400MHz-km	66 m
		62.5/125um MMF, 200MHz-km (OM1)	33 m
		62.5/125um MMF, 160MHz-km	26 m

Long reach fiber 10G SFP+ distance specifications

Description: 10G SFP+ Ethernet long range (10 km) - Single

Transmitter wavelength (nm): 1310nm (nominal)

Fiber type: 9/125um SMF

Typical reach (m): 10km

Citrix direct attached (DAC) copper TwinAx 10G SFP+ passive cables

Description: 1m DAC SFP+ cable for up to 1m distance

Description: 3m DAC SFP+ cable for up to 3m distance

Description: 5m DAC SFP+ cable for up to 5m distance

Field Replaceable Units

June 19, 2020

Citrix SD-WAN field replaceable units (FRU) are components that can be quickly and easily removed from the appliance and replaced by the user or a technician at the user's site. The FRUs for a Citrix SD-WAN appliance include DC or AC power supplies, solid-state or hard-disk drives, and a direct attach cable (DAC).

> Note: The solid-state or hard-disk drive stores your configuration information, and it must be restored from a backup after the unit is replaced.

Power supply

For appliances containing two power supplies, the second power supply is optional but recommended . Some appliances can accommodate four power supplies, and require two power supplies as a bare minimum for proper operation. As a best practice, plug in all the power supplies for redundancy.

The appliance ships with a standard power cord that plugs into the appliance's power supply and a NEMA 5-15 plug on the other end for connecting to the power outlet on the rack or in the wall.

If you suspect that a power-supply fan is not working, please see the description of your platform. On some platforms, what appears to be the fan does not turn, and the actual fan turns only when necessary.

On each power supply, a bicolor LED indicator shows the condition of the power supply.

Electrical safety precautions for power supply replacement

Make sure that the appliance has a direct physical connection to earth ground during normal use. When installing or repairing an appliance, always connect the ground circuit first and disconnect it last.

Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even if the power switch is turned off.

Replace an AC power supply

Most Citrix SD-WAN platforms can accommodate two power supplies. Some platforms can accommodate four power supplies. All Citrix SD-WAN appliances function properly with a single power supply, except the appliances that can accomodate four power supplies. These appliances need two power supplies for proper operation. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

> Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working , and if the appliance has four power supplies, you can replace one or two power supplies without shutting down the appliance, provided the other two power supplies are working.

To install or replace an AC power supply on a Citrix SD-WAN appliance:

1. Align the semicircular handle perpendicular to the power supply. Loosen the thumbscrew and press the lever toward the handle and pull out the existing power supply.
2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.
5. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: Citrix SD-WAN appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Replace a DC power supply

Most Citrix SD-WAN platforms can accommodate two power supplies. Some platforms can accommodate four power supplies. All Citrix SD-WAN appliances function properly with a single power supply, except the appliances that can accomodate four power supplies. These appliances need two power supplies for proper operation. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working , and if the appliance has four power supplies, you can replace one or two power supplies without shutting down the appliance, provided the other two power supplies are working.

To install or replace a DC power supply on a Citrix SD-WAN appliance:

1. Loosen the thumbscrew and press the lever towards the handle and pull out the existing power supply.
2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot while pressing the lever towards the handle. Apply firm pressure to insert the power supply firmly into the slot.
5. When the power supply is completely inserted into its slot, release the lever.
6. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Solid-state drive

A solid-state drive (SSD) is a high-performance device that stores data in solid-state flash memory. The MPX solid-state drives contain the boot loader configuration file, configuration file (ns.conf), licenses, and for some models, the Citrix SD-WAN software and the user data.

All platforms store the Citrix SD-WAN software on the SSD. The SSD is mounted as /flash.

Replacement solid-state drives (SSDs) contain a pre-installed version of the Citrix SD-WAN software and a generic configuration file (conf), but they do not contain SSL-related certificates and keys, or custom boot settings. Configuration files and customized settings must be restored to a replacement drive from a backup storage location at the customer site, if available.

To replace a solid-state drive:

1. At the Citrix SD-WAN command prompt, exit to the shell prompt. Type:

   shell

2. Shut down the Citrix SD-WAN appliance by typing the following command at the shell prompt:

   shutdown –p now

3. Locate the SSD on the back panel of the appliance. Push the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

4. Verify that the replacement SSD is the correct type for the platform.

5. Pick up the new SSD, open the drive handle fully to the left or up, and insert the drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the drive locks securely into the slot.

Important: When you insert the drive, make sure that the Citrix product label is at the top if the drive is inserted horizontally or at the right if the drive is inserted vertically.

1. Turn on the Citrix SD-WAN appliance. When the appliance starts, it no longer has the previous working configuration. Therefore, the appliance is reachable only through the default IP address of 192.168.10.1, or through the console port.

2. Perform the initial configuration of the appliance, as described in Initial Configuration. Log on to the default IP address by using a web browser, or connect to the serial console by using a console cable, to perform the initial configuration.

3. Upload a platform license and any optional feature licenses, including universal licenses, to the Citrix SD-WAN appliance.

4. Once the correct Citrix SD-WAN software version is loaded, you can restore the working configuration.

Hard disk drive

A hard disk drive (HDD) stores logs and other data files. Files stored on the HDD include the newnslog files, dmesg and messages files, and any core/crash files. The HDD comes in various capacities, depending on the Citrix SD-WAN platform. Hard drives are used for storing files required at runtime. An HDD is mounted as /var.

Replace a hard disk drive

A hard disk drive (HDD) stores log files and other user files. Collection of new log files begins upon boot-up with the new HDD.

To install a hard disk drive:

1. At the Citrix SD-WAN command prompt, exit to the shell prompt. Type:

   shell

2. Shut down the Citrix SD-WAN appliance by typing one of the following commands at the shell prompt.

   shutdown –p now

3. Locate the hard disk drive on the back panel of the appliance.

4. Verify that the replacement hard disk drive is the correct type for the Citrix SD-WAN platform.

5. Disengage the hard disk drive by pushing the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

6. Pick up the new disk drive, open the drive handle fully to the left, and insert the new drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the hard drive locks securely into the slot.

   Important: When you insert the drive, make sure that the Citrix product label is at the top.

7. Turn on the Citrix SD-WAN appliance. The appliance starts the Citrix SD-WAN software and reads the configuration file.

Note

SD-WAN Standard Edition 400 and 410 appliances do not have field replaceable units. The field replaceable SSD and power supplies are not required.

SD-WAN WANOP/SE 4000 and WANOP 5000 field replaceable units (FRU) are components that can be quickly and easily removed from the appliance and replaced by the user or a technician at the user's site. The FRUs in an SD-WAN WANOP/SE 4000 and WANOP 5000 appliance can include DC or AC power supplies, and solid-state and hard-disk drives.

Ports

June 19, 2020

> **Note**
>
> Some Citrix SD-WAN appliances do not require SFP transceivers.

Ports are used to connect the appliance to external devices. The Citrix SD-WAN appliances support RS232 serial ports, 10/100/1000Base-T copper Ethernet ports, fiber 1G SFP ports, and 10-gigabit fiber SFP+ ports. All SD-WAN appliances have a combination of some or all of these ports. For details on the type and number of ports available on your appliance, see the section describing that platform.

RS232 serial port

The RS232 serial console port provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

All hardware platforms ship with an appropriate serial cable used to connect your computer to the appliance. For instructions on connecting your computer to the appliance, see Installing the Hardware.

Copper ethernet ports

The copper ethernet ports installed on many models of the appliance are standard RJ45 ports.

There are two types of copper Ethernet ports that may be installed on your appliance:

- 10/100BASE-T port. The 10/100BASE-T port has a maximum transmission speed of 100 megabits per second (Mbps). Most platforms have at least one 10/100BASE-T port.

- 10/100/1000BASE-T port. The 10/100/1000BASE-T port has a maximum transmission speed of 1 gigabit per second, 10 times faster than the other type of copper Ethernet port. Most platforms have at least one 10/100/1000Base-T port.

To connect any of these ports to your network, you plug one end of a standard Ethernet cable into the port and plug the other end into the appropriate network connector.

Management ports

Management ports are standard copper Ethernet ports (RJ45), which are used for direct access to the appliance for system administration functions.

1G SFP and 10G SFP+ ports

- A 1G SFP port can operate at a speed of 1 Gbps. It accepts either a copper 1G SFP transceiver, for operation as a copper Ethernet port, or a fiber 1G SFP transceiver for operation as a fiber optic port.

- The 10G SFP+ ports are high-speed ports that can operate at speeds of up to 10 Gbps. You need a fiber optic cable to connect to a 10G SFP+ port. If the other end of the fiber optic cable is attached to a 1G SFP port, the 10G SFP+ port automatically negotiates to match the speed of the 1G SFP port.

Note

The SD-WAN 410-SE appliance can be used as a WAN optimization device, the first port pair has an apA labeled.

The motherboard port is labeled MGMT for port Eth0.

Power Supply

January 28, 2020

Citrix SD-WAN appliances are configured with a single power supply. For an SD-WAN 3000 WANOP appliance, you can order a second power supply.

Citrix SD-WAN 4000, 5000 WANOP/SE, 4100, and 5100 SE appliances are configured with dual power supplies but can operate with only one power supply. The second power supply serves as a backup.

For an SD-WAN Standard Edition 410 appliance, a single chassis power switch is supplied. The device has an external power brick instead of an internal power supply if a desktop form factor is chosen.

Table 1. LED Power Supply Indicators

Power Supply Type	LED Color	LED Indicates
AC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing GREEN	Power supply is in standby mode.
	GREEN	Power supply is functional.
	RED	Power supply failure.

Power Supply Type	LED Color	LED Indicates
DC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing BLUE	Power supply is in standby mode.
	BLUE	Power supply is functional.
	RED	Power supply failure.

Electrical safety precautions for Power Supply replacement

- Make sure that the appliance has a direct physical connection to earth ground during normal use. When installing or repairing an appliance, always connect the ground circuit first and disconnect it last.
- Always unplug any appliance before performing repairs or upgrades.
- Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even if the power switch is turned off.

Replacing an AC Power Supply

Replace an AC power supply with another AC power supply. All power supplies must be of the same type (AC or DC).

> **Note**: You can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace an AC power supply on a Citrix SD-WAN 4000/5000 appliance

1. Align the semicircular handle perpendicular to the power supply. Loosen the thumbscrew and press the lever toward the handle and pull out the existing power supply, as shown in the following figure.
   Figure 1. Removing the Existing AC Power Supply
   localized image
2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.

Figure 2. Inserting the Replacement AC Power Supply

5. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

> **Note**: SD-WAN 4000/5000 appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Replacing a DC Power Supply

Replace a DC power supply with another DC power supply. All power supplies must be of the same type (AC or DC).

> **Note**: You can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace a DC power supply on a Citrix SD-WAN 4000/5000 appliance

1. Loosen the thumbscrew and press the lever towards the handle and pull out the existing power supply, as shown in the following figure.
    Figure 3. Removing the Existing DC Power Supply

2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.

4. Insert the power supply into the slot while pressing the lever towards the handle. Apply firm pressure to insert the power supply firmly into the slot.

Figure 4. Inserting the Replacement DC Power Supply

5. When the power supply is inserted into its slot, release the lever.
6. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: SD-WAN 4000/5000 appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

An SD-WAN 2000 appliance can accommodate only one power supply, which is not field replaceable. An SD-WAN 3000 appliance has only one power supply, but you can order and install a second power supply.

To install or replace an AC power supply in an SD-WAN 3000 appliance

1. If replacing an existing power supply, align the semicircular handle, so that it is perpendicular to the power supply, loosen the thumbscrew, press the lever toward the handle and pull out the existing power supply.
2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.
5. Connect the power supply to a power source.

Note

You can replace one power supply without shutting down the appliance, provided the other power supply is working.

Solid-State Drive

May 23, 2019

A solid-state drive (SSD) is a high-performance device that stores data in solid-state flash memory.

Replace solid-state drive

The SD-WAN 4000/5000 software is stored on the solid-state drive (SSD).

For Citrix SD-WAN 410 appliance, the on-board SATA disk controller must support at least two devices. Support for SATAv3 (6 Gbps) is available.

To replace a solid-state drive

1. Shut down the appliance.

2. Locate the SSD on the back panel of the appliance. Push the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.
   Figure 1. Removing the Existing Solid-State Drive
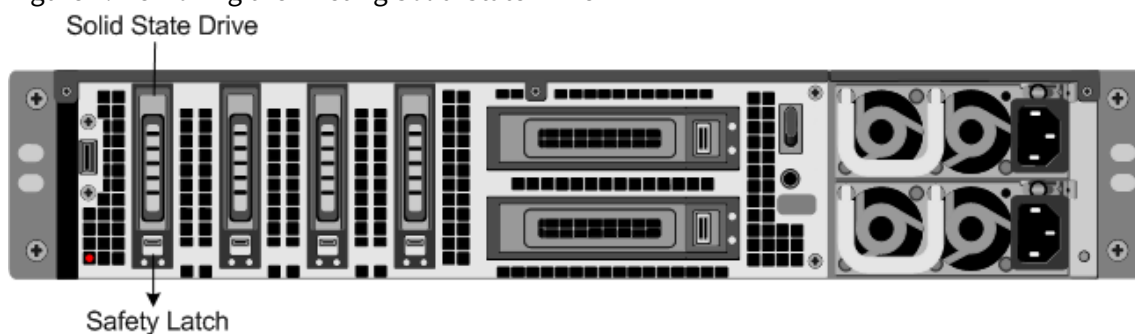
3. Verify that the replacement SSD is the correct type for the platform.

4. Pick up the new SSD, open the drive handle fully to the left or up, and insert the drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the drive locks securely into the slot.
   Important: When you insert the drive, make sure that the Citrix product label is at the top if the drive is inserted horizontally or at the right if the drive is inserted vertically.

   Figure 2. Inserting the Replacement Solid-State Drive

---

5. Turn on the appliance.

6. Log on to the default IP address by using a web browser, or connect to the serial console by using a console cable, to perform the initial configuration.

Hard Disk Drive

June 19, 2020

The Citrix SD-WAN virtual machines are hosted on the hard-disk drive.

Replace hard disk drive

Verify that the replacement hard disk drive is the correct type for the SD-WAN 4000/5000 platform.

To install a hard disk drive

1. Shut down the appliance.

2. Locate the hard disk drive on the back panel of the appliance.

3. Disengage the hard disk drive by pushing the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

   Figure 1. Removing the Existing Hard Disk Drive
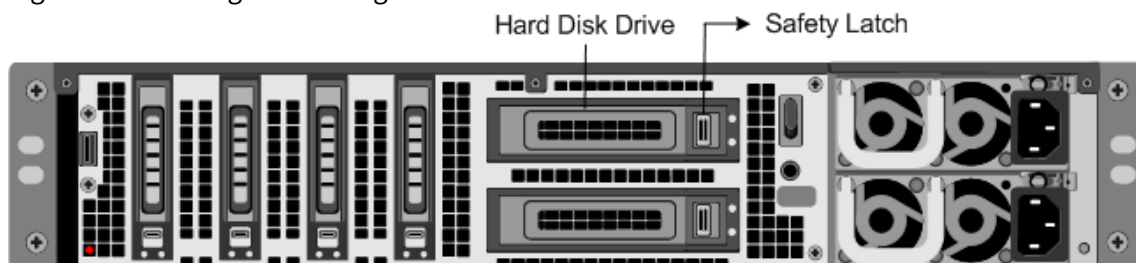
4. Pick up the new disk drive, open the drive handle fully to the left, and insert the new drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the hard drive locks securely into the slot.

   Important: When you insert the drive, make sure that the Citrix product label is at the top.

   Figure 2. Inserting the Replacement Hard Disk Drive

5. Turn on the appliance.

Install and Remove 1G SFP Transceivers

May 23, 2019

> **Note**: Some SD-WAN 4000/5000 appliances do not require SFP transceivers.

A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit per second and is available in both copper and fiber types. Inserting a 1G SFP copper transceiver converts the 1G SFP port to a 1000BASE-T port. Inserting a 1G SFP fiber transceiver converts the 1G SFP port to a 1000BASE-X port. Auto-negotiation is enabled by default on the 1G SFP port into which you insert your 1G SFP transceiver. When a link between the port and the network is established, the speed and mode are matched on both ends of the cable.

Insert 1G SFP transceivers into the 1G SFP ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the 1G SFP transceiver or the appliance.

> Warning: SD-WAN 4000/5000 appliances do not support 1G SFP transceivers from vendors other than Citrix Systems. Attempting to install third-party 1G SFP transceivers on your SD-WAN 4000/5000 appliance voids the warranty. Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.
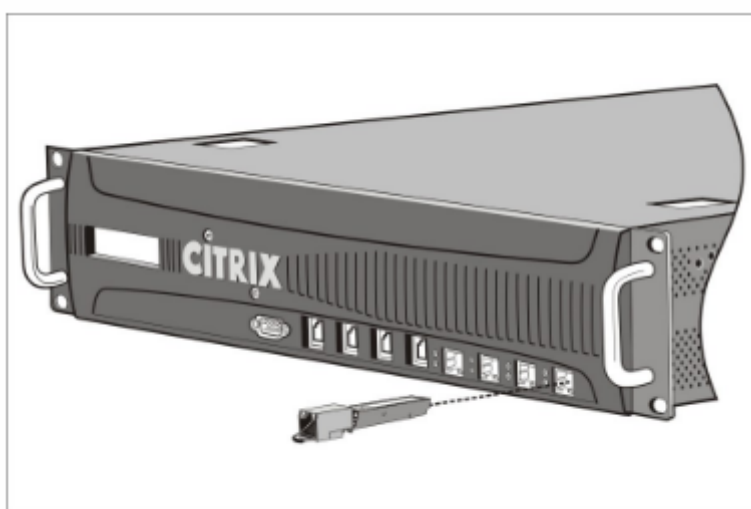
To install a 1G SFP transceiver

1. Remove the 1G SFP transceiver carefully from its box.
   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that

can damage your eyes.

2. Align the 1G SFP transceiver to the front of the 1G SFP transceiver port on the front panel of the appliance, as shown in the following figure.

3. Hold the 1G SFP transceiver between your thumb and index finger and insert it into the 1G SFP transceiver port, pressing it in until you hear the transceiver snap into place.

4. Lock the transceiver.

5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.

6. If you are using a fiber 1G SFP transceiver, do not remove the dust caps attached to the transceiver and the cable until you are ready to insert the cable.

Note

The illustration in the following figures might not represent your actual appliance.

To remove a 1G SFP transceiver

1. Disconnect the cable from the 1G SFP transceiver. If you are using a fiber optic cable, replace the dust cap on the cable before putting it away.
   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Unlock the 1G SFP transceiver.

3. Hold the 1G SFP transceiver between your thumb and index finger and slowly pull it out of the port.

4. If you are removing a fiber 1G SFP transceiver, replace the dust cap before putting it away.

5. Put the 1G SFP transceiver into its original box or another appropriate container.

Install and Remove 10G SFP+ Transceivers

May 23, 2019

Warning

Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

Note

Some SD-WAN 4100/5100 appliances do not require SFP+ transceivers.

A 10-Gigabit Small Form-Factor Pluggable (SFP+) is a compact optical transceiver that can operate at speeds of up to 10 gigabits per second. Autonegotiation is enabled by default on the 10G SFP+ ports into which you insert your 10G SFP+ transceiver. When a link between the port and the network is established, the mode is matched on both ends of the cable and for 10G SFP+ transceivers, the speed is also autonegotiated.

Insert the 10G SFP+ transceivers into the 10G SFP+ ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the transceiver or the appliance.

Important

SD-WAN 4100/5100 appliances do not support 10G SFP+ transceivers provided by vendors other than Citrix Systems. Attempting to install third-party 10G SFP+ transceivers on your SD-WAN 4100/5100 appliance voids the warranty.

To install a 10G SFP+ transceiver

1. Remove the 10G SFP+ transceiver carefully from its box.
2. Align the 10G SFP+ transceiver to the front of the 10G SFP+ transceiver port on the front panel of the appliance.
3. Hold the 10G SFP+ transceiver between your thumb and index finger and insert it into the 10G SFP+ transceiver port, pressing it in until you hear the transceiver snap into place.
4. Move the locking hinge to the DOWN position.
5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
6. Do not remove the dust caps attached to the transceiver and cable until you are ready to insert the cable.

Warning

Do not look directly into fiber optic transceivers and cables. They emit laser beams that can

damage your eyes.

To remove a 10G SFP+ transceiver

1. Disconnect the cable from the 10G SFP+ transceiver. Replace the dust cap on the cable before putting it away.
2. Unlock the 10G SFP+ transceiver by moving the locking hinge to the UP position.
3. Hold the 10G SFP+ transceiver between your thumb and index finger and slowly pull it out of the port.
4. Replace the dust cap on the transceiver before putting it away.
5. Put the 10G SFP+ transceiver into its original box or another appropriate container.

Regulatory compliance

November 17, 2020

Supplier's declaration of conformity

The FCC Compliance Statements listed on this page apply to all Citrix SD-WAN hardware models.

Responsible Party – U.S. Contact Information:

```
1  Citrix Systems, Inc.
2  4988 Great America Parkway
3  Santa Clara, CA
4  95054 USA
5
6  compliance.prime@citrix.com
7  <!--NeedCopy-->
```

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device might not cause harmful interference.
2. This device must accept any interference received, including interference that might cause undesired operation.

> **Note**
>
> This equipment has been tested and found to comply with the limits for a Class A digital device, according to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If not installed and

> used in accordance with the instruction manual, this equipment might cause harmful interference to radio communications. Operation of this equipment in a residential area might cause harmful interference. Users are required to correct the interference at their own expense.

Citrix SD-WAN 110-LTE-WiFi-SE compliance

For information on Citrix SD-WAN 110-LTE-WiFi-SE compliance and declaration of conformity see the following links:

- Citrix SD-WAN 110-LTE-WiFi-SE Compliance
- EU Declaration of Conformity

Citrix SD-WAN 110-WiFi-SE compliance

For information on Citrix SD-WAN 110-WiFi-SE compliance and declaration of conformity see the following links:

- Citrix SD-WAN 110-WiFi-SE Compliance
- EU Declaration of Conformity

Taiwan BSMI RoHS statement

May 23, 2019

The following tables are a declaration of the presence condition of restricted substances in Citrix SD-WAN hardware appliances.

限用物質含有情況標示聲明書

Declaration of the Presence Condition of Restricted Substances

設備名稱：網路負載均衡設備(服務器)						
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
金屬外殼	○	○	○	○	○	○
印刷電路板	○	○	○	○	○	○
電源供應器	○	○	○	○	○	○
風扇	○	○	○	○	○	○
外殼前面板	○	○	○	○	○	○
配件(電源線、傳輸線)	○	○	○	○	○	○

備考1. "超出0.1 wt %"及"超出0.01 wt %"係指限用物質之百分比含量超出百分比含量基準值。

Note 1 : "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. "○"係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2 : "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. "—"係指該項限用物質為排除項目。

Note 3 : The "—" indicates that the restricted substance corresponds to the exemption.

設備名稱：網路負載均衡設備						
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
金屬外殼	○	○	○	○	○	○
印刷電路板	○	○	○	○	○	○
電源供應器	○	○	○	○	○	○
風扇	○	○	○	○	○	○
外殼前面板	○	○	○	○	○	○
配件(電源線、傳輸線)	○	○	○	○	○	○