Vertiv™ Next Connect

Quick Installation Guide for Next Connect Local Agent on Windows and Ubuntu Linux, or a Virtual Appliance

Overview

This Quick Installation Guide provides step-by-step instructions to install the Vertiv™ Next Connect Local Agent on Windows 11, Server 2019, Server 2022, or Ubuntu Linux 22.04 LTS Desktop, or by deploying the Virtual Appliance (Hyper-V, VMware ESXi 8.0, and Nutanix Prism Central).

Prerequisites

- **Network and Firewall:** Ensure the required ports are open and the necessary cloud endpoints are accessible through the organization's firewall. For more details, refer to the Network and Firewall Configuration on page 1.
- **Internet Access:** Required for downloading, installing, registering, updating the agent, and for Vertiv Next Connect connectivity.
- **Vertiv Next Connect Account:** Make sure you have a Vertiv Next Connect account and a customer created for agent registration.

System Requirements

Requirement	Windows 11 or Server 2019/2022	Ubuntu Linux 22.04 LTS Desktop
Minimum free memory	2 GB (4 GB recommended)	2 GB (4 GB recommended)
Total memory	4 GB (8 GB recommended)	4 GB (8 GB recommended)
Total VM memory required (where applicable)	OS specified minimum + Agent minimum	
Minimum free disk space	27 GB (60 GB recommended)	27 GB (60 GB recommended)
Total disk space	60 GB (100 GB recommended)	60 GB (100 GB recommended)
CPU	2+ cores, Intel Xeon E5-2673 v3 or equivalent	2+ cores, Intel Xeon E5-2673 v3 or equivalent

Network and Firewall Configuration

The following table lists the inbound and outbound ports required for communication between the monitored devices and the Local Agent:

Port	Protocol	Transport	Description
0	ICMP	ICMP	Open to allow network connectivity verification over ICMP.
161	SNMP	UDP	Open to allow connectivity to SNMP based targets and clients.
162	SNMP	UDP	Open to send and receive SNMP traps.
22	SSH	TCP	Open to allow SSH sessions to the appliance.
80	HTTP	TCP	• Open to allow internet access to the Vertiv Next Connect portal. • Open to allow monitoring device discovery. • Open to allow communication to the monitoring device communication card. • Open to allow provisioning of the monitoring device card firmware. • REST-HTTPS for sending commands.
443	HTTPS	TCP	• Open to allow a web user interface. • REST-HTTPS for sending commands.
21000	HTTP	TCP	Local web application.
21001	HTTPS	TCP	Local web application.

Port	Protocol	Transport	Description
5671	AMQP	TCP	• Open for Azure IoT Hub. • Open for sending device data. • Open for Blob Storage Connection for device configuration.
8883	MQTT	TCP	• Device provisioning and communication with Azure IoT Hub. • Azure provision certificate. • Receiving commands. • Sending results. • Heartbeats.
6687	Geist™ Discovery Protocol	UDP	Geist™ device discovery protocol.

The following table lists the outbound endpoints required for the Local Agent to communicate securely with Vertiv™ Next Connect. These endpoints must be configured for outbound communication on your organization's firewall.

Service	Endpoint	Transport	Port Number	Description
IoT Hub MQTT / AMQP / HTTPS	*.azure-devices.net	TCP	8883, 5671, 443	Used for all IoT Hub communications.
Device provisioning service (DPS)	*.azure-devices-provisioning.net	TCP	443	Used during initial registration / reprovisioning.
Azure edge agent/hub updates	mcr.microsoft.com and *.data.mcr.microsoft.com	TCP	443	Microsoft container registry (MCR)—IoT Edge runtime modules.
Azure container registry	*.azurecr.io	TCP	443	Used for pulling custom container images.
Application specific API's	https://stfdtnpublicprdeastus002.blob.core.windows.net https://stfoundationprdeastus002.blob.core.windows.net https://next-connect.vertiv.com/* https://next-connect-api.vertiv.com/*			

Downloading the Agent Installer

1. Log in to the Vertiv™ Next Connect platform.
2. Select the *Local Agents* menu under the Equipment menu.
3. Click the *Add* icon to open the New Agent dialog.
4. Click the *DOWNLOAD AGENT INSTALLER* button and select the appropriate installer for your OS:
   - **Windows:** Choose either the standard Windows Agent or the bundled version. The standard version does not come bundled with Eflow and will download Eflow during the installation process.
   - **Ubuntu 22.04 Linux LTS Desktop:** Download the Linux Agent AppImage installer.
   - **Virtual Appliance:** Download the Virtual Appliance OVA file for supported hypervisors.

NOTE: *Vertiv recommends the use of Ubuntu for all installations whenever feasible.*

Virtual Appliance Deployment

The Vertiv™ Next Connect Local Agent is available as a Virtual Appliance for supported hypervisors. Use the appropriate deployment workflow below, then complete agent registration in the Vertiv Next Connect platform.

VMware ESXi 8.0

Prerequisites: Access to vCenter Server or ESXi Host Client with permissions to deploy OVF templates, and the Vertiv Next Connect Virtual Appliance OVA file. Ensure required network and firewall ports and outbound endpoints in Network and Firewall Configuration are permitted.

1. Log into the VMWare ESXi Host of from vCenter select the target cluster/host.
2. From the Virtual Machines (VM) Menu Select *Create/Register VM*.
3. Select *Deploy OVF Template*.
4. Browse to and select the Next Connect Virtual Appliance **.OVA** file, then continue.
5. Follow the wizard to select a compute resource, datastore, and network/port group.
6. When prompted in the OVF deployment workflow, specify the network configuration parameters as required by your environment (for example, static IP or DHCP).
7. Complete the wizard and power on the virtual machine.
8. Determine the virtual appliance IP address from the VM summary or from your DHCP server.
9. Proceed to the Post-deployment Validation and Registration section of this guide.

Nutanix Prism Central

Prerequisites: Access to Nutanix Prism Central and Prism Element with permissions to import images and create virtual machines, and the Vertiv Next Connect Virtual Appliance OVA file. Ensure required network and firewall ports and outbound endpoints in Network and Firewall Configuration are permitted.

1. Log in to Prism Central.
2. From the Application Switcher, select the *Infrastructure* application.
3. Navigate to *Compute > OVAs*.
4. Upload the Vertiv Next Connect Virtual Appliance **.OVA** file if it is not already available on the OVAs page.
5. Select the target *OVA* and choose *Deploy as VM* from the Actions dropdown menu.
6. In the Deploy as VM window, complete the Configuration step:
   a. Enter a VM name (and description, if desired).
   b. Select the target cluster.
7. Review the CPU and memory values populated from the OVA. Update the values if required by your environment, then click *Next*.
8. In the resources step, review or configure:
   - Boot configuration (UEFI or Legacy BIOS, as required by your environment).
   - Network/subnet for the VM NIC.
   - Any additional disks (optional).
9. Complete the deployment wizard and power on the virtual machine.
10. Determine the virtual appliance IP address from the VM console/VM details or from your DHCP server.
11. Proceed to the Post-deployment Validation and Registration section of this guide.

OVA to VHDX Conversion Guide (for Hyper-V)

This section describes two supported methods to convert a **.ova** image into a Hyper-V compatible **.vhdx**.

Option 1 Using qemu-img (QEMU)

1. Install *QEMU*. Download the installer from https://qemu.weilnetz.de/w64 and run the installer with default options.
2. Add *QEMU* to *PATH*. Go to *System > Advanced system settings > Environment Variables* Path and add:
   C:\Program Files\qemu
3. Extract the OVA. From PowerShell, run:
   tar -xvf C:\ova\ubuntu-ova-20260427.02.ova
4. Convert VMDK VHDX. From PowerShell, run:
   qemu-img convert -f vmdk -O vhdx C:\ova\ubuntu-24.04.3-hardened-disk1.vmdk C:\ova\ubuntu-24.04.3-hardened-disk1.vhdx
5. Sanitize the VHDX (critical for Hyper-V). Hyper-V requires disks to NOT be sparse, compressed, or encrypted. From PowerShell, run:
   fsutil sparse setflag C:\ova\ubuntu-24.04.3-hardened-disk1.vhdx 0
   compact /u C:\ova\ubuntu-24.04.3-hardened-disk1.vhdx
   cipher /d C:\ova\ubuntu-24.04.3-hardened-disk1.vhdx

Option 2 Using StarWind V2V Converter

1. Install *StarWind Converter*. Download it from https://www.starwindsoftware.com/starwind-v2v-converter#download and install with default settings.
2. Extract the OVA. From PowerShell, run:
   tar -xvf C:\ova\ubuntu-ova-20260427.02.ova
3. Convert using the graphical user interface (GUI). Open StarWind V2V Converter, then:
   a. Select the source image (***.vmdk**).
   b. Choose destination format: **VHDX file**.
   c. Select the destination image format option (VHDX) as needed for your environment.
   d. Start conversion.

Hyper-V

Prerequisites: A Windows system with Hyper-V Manager and permissions to create virtual machines, the Vertiv™ Next Connect Virtual Appliance OVA file, and a tool to extract TAR archives (for example, 7-Zip). Ensure required network and firewall ports and outbound endpoints in Network and Firewall Configuration are permitted.

1. Convert the downloaded Virtual Appliance **.OVA** to a Hyper-V compatible **.vhdx** by following the OVA to VHDX Conversion Guide (for Hyper-V) above.
2. Open *Hyper-V Manager* and select *New > Virtual Machine*.
3. Set the *VM Name* and *Location* as desired.
4. Select *Generation 2*.
5. Assign hardware resources according to the appliance requirements (memory, CPU, and disk).
6. Select the appropriate virtual switch for networking.
7. When prompted for the virtual hard disk, select *Use an existing virtual hard disk* and browse to the converted **.vhdx** file.
8. Complete the New Virtual Machine Wizard.
9. Disable Secure Boot: Right-click the *VM > Settings > Security*, clear *Enable Secure Boot*, then click *OK*.
10. Start the *VM* and open *Connect*.
11. Validate that the kernel loads, the NIC initializes, and an IP address is assigned (DHCP or static).
12. Proceed to the Post-deployment Validation and Registration section of this guide.

Post-deployment Validation and Registration

1. Open a browser and navigate to the virtual appliance Web UI using **https://<appliance-ip>:21001**.
2. In the Web UI, generate a temporary registration code. The registration code is valid for 15 minutes by clicking *Register a new agent*.
   a. **Add the Local Agent in Vertiv™ Next Connect:** From the agent webpage, click *Connect* to Register. This will prompt you to log into Vertiv™ Next Connect and will direct you to the add Agent page with the code auto populated. Enter an agent name and click *Save*.
   b. **Verify status and device polling:** Confirm the agent appears Online in the Local Agents view and that device polling starts as expected.

Windows Installation Steps

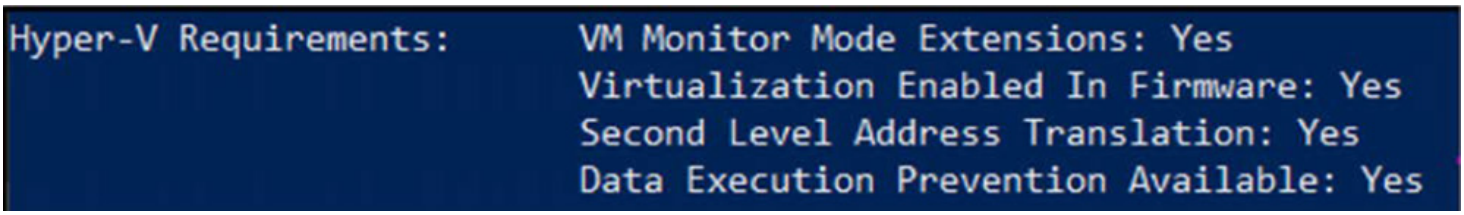
Preparation

IMPORTANT: *This section is only intended for physical Windows Machines. For Agents being deployed into Virtual Environments it is recommended that you use the virtual appliance.*

1. Ensure Hyper-V compatibility. From an elevated PowerShell terminal, run the following command:

   systeminfo

2. This generates a report on the system's capabilities. The Hyper-V section is near the bottom of the report and appears as shown below.



NOTE: *If all requirements show Yes, you can install Hyper-V on the system. If not, review the additional setup requirements in the System Requirements section, refer to the SL-71242 Vertiv™ Next Connect User Manual.*

3. Set PowerShell execution policy with the following PowerShell command:

   Set-ExecutionPolicy -ExecutionPolicy AllSigned

Run the Installer

1. Start the installation by double clicking the downloaded installer file.
2. As part of the installation process, the installer will check prerequisites and install dependencies. This includes Hyper-V and EFlow. During installation, your machine may restart as needed. After restarting, the installer will automatically launch and pick up the installation from the previous place.

Network Configuration

1. Select One NIC if your devices and internet are on the same network. Select Two NICs if you have separate devices and internet networks.
2. Choose to Assign static or DHCP IPv4 addresses as appropriate. Each NIC must have a unique IP.
3. By default, the broadcast discovery scan is enabled. You can disable it by unselecting the *Enable Broadcast Discovery Scans* option. Vertiv recommends leaving this enabled whenever feasible. This functionality is used for discovering factory-fresh Vertiv Equipment and only performs a broadcast during a device search when broadcast discovery is selected by the user.
4. Confirm default gateway and DNS settings.

Agent Registration

1. The installer generates a temporary registration code that is valid for 15 minutes, which will allow you to register with Vertiv™ Next Connect.
2. Click the link provided during installation, or enter the code manually in the New Agent dialog on the Vertiv Next Connect platform.
3. Select your customer, and name the agent. Click *Save* to register.

Installer Completion and Post-Installation

1. The agent will download additional components and updates so allow 10 to 15 minutes.
2. Check the agent status in the Local Agents menu under Equipment. The agent may take a few minutes to show that it is communicating with the cloud.

NOTE: *Vertiv Next Connect Agent, EFlow, and Edge versions auto-update as needed.*

Ubuntu 22.04 Linux LTS Desktop Installation Steps

Preparation

1. Right-click on the *Installer*, select *Properties*, then select the *Permissions* header, and enable Allow executing file as a program, or from a terminal run:

   chmod a+x linux--local-agent-installer_ <Version>.AppImage
2. Edit the sudoers file to allow passwordless execution for your admin user. From a terminal run the following command:

   sudo nano /etc/sudoers
3. Append the following line at the end of the sudoers file:

   <<adminuser>> ALL=(ALL) NOPASSWD:ALL
4. Install libfuse2 if your Ubuntu uses FUSE3, from the terminal:

   sudo add-apt-repository universe

   sudo apt install libfuse2
5. Optionally, install net-tools for network commands:

   sudo apt-get install net-tools
6. Update your operating system (OS) before installing the agent.

Run the Installer and Register the Agent

1. Double-click or execute the AppImage installer in a terminal.
2. The installer generates a temporary registration code that is valid for 15 minutes, that will allow you to register with Vertiv Next Connect.
3. Click the provided link during installation or manually enter the code in the New Agent dialog on the Vertiv Next Connect platform.
4. Select your customer, and name the agent. Click *Save* to register.

Installer Completion and Post-Installation

1. The agent downloads components and updates. Allow 10 to 15 minutes for this to take place.
2. Remove the passwordless execution from the sudoers file added in step 3 above for security purposes.
3. Check the agent status in the Local Agents menu under Equipment. The agent may take a few minutes to show that it is communicating with the cloud.

Troubleshooting and Additional Notes

- Broadcast device discovery may not be supported in all environments.
- Wi-Fi adapters are not supported.
- If the registration code expires, restart the installer to generate a new one.
- Refer to the User Manual for advanced troubleshooting, supported hypervisors, and optional configurations.

Support

For further assistance, contact your Vertiv support contact at 1-800-543-2378 or refer to the SL-71242 Vertiv™ Next Connect User Manual.

To contact Vertiv Technical Support: visit www.Vertiv.com