vAPV Administration Guide

For ArrayOS APV 10.4 Release

September 10, 2020

1 Server Hardware Requirements

The server hosting the vAPV must meet the following minimal requirements:

- CPU: One or more 64-bit x86 multi-core CPUs with virtualization assist (Intel-VT or AMD-V) enabled
- RAM: 4 GB available for vAPV
- NIC: 1 x 1 Gbps NIC or 2 x 1 Gbps NICs
- Storage: 40 GB of available hard drive space for vAPV

2 Hypervisor Version Requirement

The following hypervisor versions are supported by vAPV deployment:

- VMware ESXi 5.0 or later (64-bit only)
- Citrix XenCenter 7.4 or later (64-bit only)
- KVM in CentOS 6.0 or later (64-bit only)
- Microsoft Hyper-V (Windows Server 2012/2016/2019 version 64-bits)

3 Hypervisor Guest Environment Requirement

The virtual machine guest environment for the vAPV is recommended to meet the following minimum requirements:

- 2 vCPUs
- 2 GB vRAM (the default and recommended vRAM size is 4 GB)
- 1 virtual network interface (only supports VMXNET3 Ethernet adapters on VMware ESXi)
- 40 GB hard drive space

Note:

1. 4 GB vRAM is recommended for vAPV running many configurations.
2. Array Networks only qualifies the above-mentioned virtual machine configurations. Other configurations of the virtual machine instances are not tested and may or may not work. Please consult with Array Networks Customer Support (support@arraynetworks.com) before altering the configurations.

4 Deploying the vAPV Virtual Machine

4.1 Deploying the vAPV Virtual Machine on VMware ESXi

The first step in deploying the vAPV virtual machine on VMware ESXi is to download the vAPV VMDK file and upload it to the VMware ESXi host machine. Next, run the deployment wizard from within the VMware vSphere client as follows:

1. Please contact Array Networks Customer Support (Email: support@arraynetworks.com) for download instructions.
2. Upload the obtained vAPV compressed package to the VMware ESXi host and decompress it to obtain two VMDK files.
3. In the left column of the vSphere Client, select the host where the vAPV is to be created. Select **File** > **New** > **Virtual Machine** to enter the **Create New Virtual Machine** wizard.
4. In the **Configuration** section, select **Custom** and click **Next**.
5. In the **Name and Location** section, enter a name for the virtual machine, and click **Next**.
6. In the **Resource Pool** section, select resource pool for the virtual machine, and click **Next**.
7. In the **Storage** section, select storage location for virtual machine files, and click **Next**.
8. In the **Virtual Machine Version** section, select **Virtual Machine Version: 8** or higher version, and click **Next**.
9. In the **Guest Operating System** section, select **Linux** and set the **Version** to **Linux (64-bit)**, and click **Next**.
10. In the **CPUs** section, set CPU core number (no less than 2), and click **Next**.
11. In the **Memory** section, set Memory size (no less than 2 GB), and click **Next**.
12. In the **Network** section, configure NIC as required, and click **Next**.
13. In the **SCSI Controller** section, configure SCSI controller as required, and click **Next**.
14. In the **Select a Disk** section, select **Use an existing virtual disk**, and click **Next**.
15. In the **Select an Existing Disk** section, click **Browse** to select the VMDK disk file, and click **Next**.
16. In the **Advanced** section, configure as required, and click **Next**.
17. In the **Ready to Complete** section, double check all the virtual machine configurations, and click **Finish**.
18. Once the virtual machine is deployed, right-click the deployed virtual machine and select **Power** > **Power On** in the pop-up menu to start the vAPV virtual machine.

4.2 Deploying the vAPV Virtual Machine on Citrix XenCenter

The first step in deploying the vAPV virtual machine on Citrix XenCenter is to download the compressed file containing the vmdk image to your local system. Next, run the "**Import**" wizard from within XenCenter.

To enable the communication between the vAPV and other virtual machines, administrators need to disable the Generic Receive Offload (GRO) function on the Xen host machine, and also disable the TCP Segment Offload (TSO) function on the target virtual machine (if co-deployed on the same Xen host machine with the vAPV) for communication purpose.

Note: If the vAPV virtual machine and the real servers are deployed on the same Xen platform, administrators must disable the "tx-checksum-ipv4" option on the real servers. Otherwise, all functions related to the checksum mechanism cannot work properly.

The vAPV deployment steps are as follows:

1. Please contact **Array Networks Customer Support** (Email: support@arraynetworks.com) for download instructions.
2. Download the compressed file (for example, Rel_APV_10_4_0_x_xen.tar.gz) containing the Array vAPV vmdk image file.
3. Open the ".tar.gz" file by using the WinRAR archiver and extract the Array vAPV file package ending with ".vmdk".

4. From the "**File**" menu in XenCenter, select "**Import**" to start the "**Import**" wizard.
5. In the "**Import Source**" pane, locate the image file using the "**Browse**" button. For example, "\MyDocuments\Work\Virtualization\<vAPV_filename>".
6. Click "**Next**" to open the "**VM Definition**" pane, enter the VM name and specify memory size and the number of CPUs.
7. Click "**Next**" to open the "**Location**" pane, and select the home server on which the Virtual Machine should be run.
8. Click "**Next**" to open the "**Storage**" pane, and select the storage repository to store the virtual disks for the new Virtual Machine.
9. Click "**Next**" to open the "**Networking**" pane, and select the target network to which the VM virtual network interface will map.
10. Click "**Next**" to open the "**OS Fixup Settings**" pane, and select "**Don't use Operating System Fixup**" option.
11. Click "**Next**" to open the "**Transfer VM Settings**" pane, and in the "**Network Settings**" area, select the "**Automatically obtain network settings using DHCP**" option when a DHCP server has already configured. Otherwise, please choose "**Use these network settings**" to specify "**IP address**", "**subnet mask**" and "**Gateway**" parameters.
12. Click "**Next**" to open the "**Finish**" screen.
13. Select the check box at the bottom of the "**Finish**" pane to start the vAPV Virtual Machine as soon as the import process is over.
14. The vAPV Virtual Machine will be deployed and started automatically.

4.3 Deploying the vAPV Virtual Machine on KVM

The first step in deploying the vAPV virtual machine on KVM is to download the compressed file containing the bootable hard disk of the virtual machine. Next create a virtual machine by using these files. Detailed steps are as follows:

1. Please contact Array Networks Customer Support (Email: support@arraynetworks.com) for download instructions.
2. Download the compressed file (for example, Rel_APV_10_4_0_x_kvm.tar.gz) containing the Rel_APV_10_4_0_x.qcow2 disk image file. Please make sure that you have more than 40 GB of free space after the download.
3. Decompress the tar.gz file by using the "**tar -xvzf <vAPV_image>.tar.gz**" command to obtain the Rel_APV_10_4_0_x.qcow2 disk image file.
4. Edit the XML configuration file as follows and move it to the "/etc/libvirt/qemu/" directory:
   - Specify the appropriate bridge name that you want the interfaces to be connected to. Then use the "**ifconfig** <*bridge_name*>" command to enable the bridge.
   - Specify the NIC type to "virtio" or "e1000".
   - Specify the disk, CPU, and memory in the vAPV configuration file if required.

   Please do not change any other fields as it might lead to licensing conflicts.
5. Create a virtual machine from the XML configuration file by using the "**virsh define /etc/libvirt/qemu/vAPV.xml**" command.
6. Start the virtual machine by using the "**virsh start vAPV**" command.

Note: The deployment steps of vAPV on KVM are based on the CentOS 7.0 environment. The deployment steps on other Linux environments are similar. For any questions on the deployment, please contact Array Networks Customer Support (Email: support@arraynetworks.com).

4.4 Deploying the vAPV Virtual Machine on Microsoft Hyper-V

The first step in deploying the vAPV virtual machine on Microsoft Hyper-V is to download the compressed file containing the vhd image to your local system. Detailed steps for deploying vhd file are as follows:

1. Please contact **Array Networks Customer Support** (Email: support@arraynetworks.com) for download instructions.
2. Download the compressed file (for example, Rel_APV_10_4_0_x_HyperV.tar.gz) containing the Array vAPV vhd image.
3. Open the compressed file by using the WinRAR archiver and extract the compressed file.
4. Access the Microsoft Hyper-V server using the Microsoft Hyper-V Manager. In Hyper-V Manager, click **Action** > **New** > **Virtual Machine** to bring up the New Virtual Machine Wizard.
5. Click "**Next**" on the wizard and input a virtual machine name such as "**vAPV**".
6. In the "**Specify Generation**" pane, select "**Generation 1**" and click "**Next**".
7. In the "**Assign Memory**" pane, input the startup memory of vAPV and click "**Next**".
8. In the "**Configure Networking**" pane, select a network adapter to use as a virtual switch.
9. In the "**Connect Virtual Hard Disk**" pane, select "**use an existing virtual hard disk**", and enter the vAPV vhd image file location. Click "**Next**" when ready.
10. Verify that all deployment settings are correct and click "**Finish**".
11. Once the virtual machine is deployed, it can be started.

Note: Adding VLAN interface to the default port is currently not supported on Microsoft Hyper-V.

5 Post-Installation Configuration

1. Please finalize all virtual machine configurations before requesting a new license.
2. Please contact the Array Networks Customer Support (Email: support@arraynetworks.com) to obtain a license key after you have finalized the configuration.

Note: Any virtual machine configuration change may invalidate the current license.

To take maximum advantage of system resources, administrators are highly recommended to allocate vCPU/vNIC resources according to the assigned memory size as shown in the table below.

If the vCPU/vNIC resource amount surpasses the recommended maximum number, the vAPV instance can still function well, but its performance may not boost as expected due to the bottleneck of insufficient memory resource.

Assigned Memory Size	Recommended Maximum vCPU Number	Maximum Maximum vNIC Number
Size < 2GB (Not support)	N/A	N/A
2GB ⩽ Size < 4GB	4 vCPUs	4 vNICs
4GB ⩽ Size < 8GB	8 vCPUs	4 vNICs

Assigned Memory Size	Recommended Maximum vCPU Number	Maximum Maximum vNIC Number
8GB ⩽ Size < 16GB	16 vCPUs	8 vNICs
16GB ⩽ Size < 32GB	32 vCPUs	16 vNICs
Size ⩾ 32GB	No limit	No limit

Note: When configuring vCPU resource, please remember not to set the number of "vCPU sockets" larger than 2. Currently, only 1 or 2 "vCPU sockets" can be supported.

6 Array vAPV Series Installation Guide

Once the virtual machine starts, the login shell will appear on the console tab of the vAPV virtual machine, for example, on the VMware vSphere client or virtual machine Manager. Please note that it may take a couple of minutes for the login shell to appear.

The initial username/password is array/admin.

7 Minimum Initial Configuration

Three ways are available to connect to the vAPV to begin configuration:

1. Console (recommended)
2. SSH
3. Web browser

To set up the vAPV via SSH or a Web browser, first you need to complete the network settings of the vAPV through the Console connection.

Please configure the vAPV initial settings like IP address via Console, and then connect to the vAPV through recommended method provided by related hypervisor. Once you login into the vAPV, the vAPV will prompt you for a User Privilege Password. A prompt like "Array Networks Login (AN):" may appear. If this is the first time you have connected to the vAPV, or if you have not changed the default password, then enter the user name "array" and the password "admin".

Now enter "**enable**" and press "**Enter**" to switch to the enable mode. You will be prompted to enter an enable password. The default enable password is null. Therefore, just press "**Enter**". The prompt "AN#" will appear.

Now enter "**config terminal**" and press "**Enter**" to switch to the configuration mode. The prompt "AN(config)#" will appear. At this point, the administrator will have full access to the vAPV CLI.

The CLI commands required for minimum configuration are listed below. It is recommended that you set port1, the default route, and WebUI IP address and port.

ip address *{system_ifname|mnet_ifname|vlan_ifname|bond_ifname} <ip_address> {netmask|prefix} [overlap]*

Allows the user to set each interface IP address and netmask or prefix length.

ip route default *<gateway_ip>*

Allows the user to set the default gateway IP address.

webui ip *<ip_address>*

Allows the user to set the IP address at which that the vAPV will accept Web User Interface commands via the Web browser. It is recommended that a management IP address be used for configuring the WebUI IP address.

webui port *<port>*

Allows the user to set the port from which the vAPV will accept WebUI commands. The port must be designated within the range from 1024 to 65,000. The default port is 8888.

webui {on|off}

Enables or disables the WebUI.

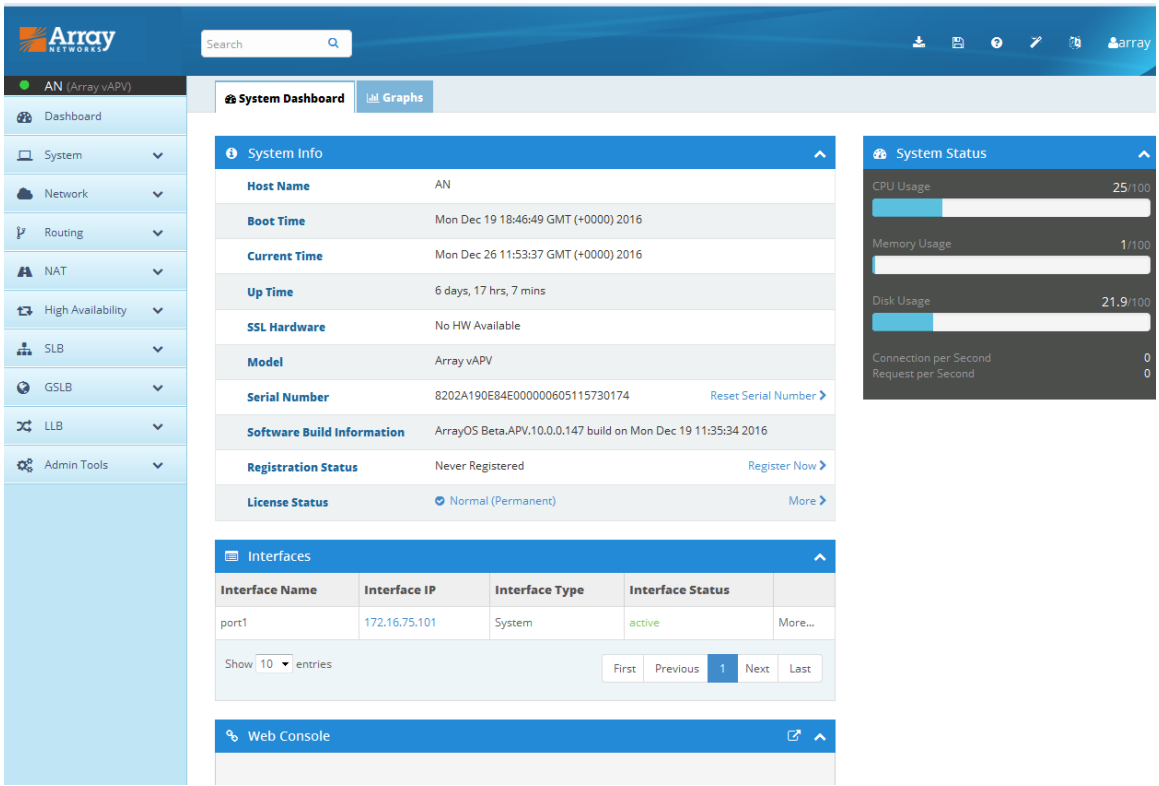
With the above network settings completed for the vAPV, you may set up the vAPV via SSH or a Web browser. You may use a Web browser to connect to the WebUI IP address assigned to the vAPV (with WebUI enabled) or establish an SSH connection to the IP address of the vAPV.

Note: If you change the settings of the vAPV port1 IP address and WebUI IP address, the connection to the vAPV will be terminated and you will have to enter the new WebUI address in the browser to reconnect to the vAPV WebUI.

Configuration Example

```
AN(config)#ip address port1 10.8.6.50 255.255.255.0
AN(config)#ip route default 10.8.6.1
AN(config)#webui ip 10.8.6.50
AN(config)#webui port 8888
AN(config)#webui on
```

After completing these steps, administrators may continue to configure the vAPV via the CLI or WebUI. To access and configure vAPV via WebUI, enter the URL **https://10.8.6.50:8888** in the address bar of a browser. Then follow the prompts to log in the vAPV and enter the password for the “enable” mode. After you enter the “enable” mode, the following window will be displayed.



For more detailed configuration information, please refer to the User Guide and CLI Handbook of the APV series products.

8 Resizing a vAPV Virtual Machine on Hypervisors

Resizing the vAPV virtual machine such as adjusting the system resources vCPUs, vNICs, RAM and bandwidth, might cause the license to become invalid, and therefore administrators must be very cautious when resizing a virtual machine. Before any resizing operation, please check the resizing scenario and be aware of the potential effects caused by your operation, as shown in the following table:

Resizing Scenario	Influence
Downgrade the VM size	The license will still be valid.
Upgrade the VM size within the licensed limits	The license will still be valid.
Upgrade the VM size beyond the licensed limits	The license will become invalid. Please repurchase the vAPV license by providing the following information to Array Networks Support (Email: support@arraynetworks.com): • Serial number • New Capacity you wish to purchase

You can use "**show version**" command to check the "**Licensed Limits**" item which displays the system resources authorized by the license.

Note: Before resizing the vAPV virtual machine, please shut it down first.

9 Loading the vAPV License

The vAPV currently only support Bring Your Own License (BYOL) model. Therefore, you will need to purchase a license from Array Networks and load the license to the system to unlock its feature. Please perform the following steps to generate a serial number and import a new valid license:

1. Contact the **Array Networks Customer Support** (support@arraynetworks.com) to apply for a new license based on the serial number in the output of the command "**show version**"
2. Import the new license by executing the command "**system license**".

For example:

```
AN(config)#system license "be99af00-ef53d5fd-e21501ad-9eee8179-3dd843b3-1108c600-1505fdab-20130108-99999999"
```

10 Known Limitations

- Fast Failover (FFO) is not supported.
- Software SSL can run only on Intel CPUs.
- If the Network Interface Card (NIC) type is "i82545em_copper" or "i82545em_fiber", the system will not perform hardware checksums even if the command "**system tune hwcksum on**" is configured.

11 vAPV FAQ

11.1 General

- How is the vAPV software upgraded?

  For vAPV running as a virtual appliance, the system update is the same as APV, that is, use the command "**system update** …" for the ArrayOS update.

- How many vCPUs are supported?

  A maximum of 32 vCPUs are supported.

- Is SSL offload supported?

  Yes. SSL offload (software only solution) is supported on the Intel CPUs only.

- Can I use a third-party hardware SSL accelerator?

  No. You cannot install any third party hardware accelerator and expect it to work with vAPV.

- Can I put vAPV in a cluster/HA configuration with a physical APV?

  No, vAPV clustering with a physical APV is not supported.

- Why does a vAPV as an HA unit remain active when its port becomes “DOWN”?

  Because vAPV uses virtual NICs, hypervisors do not provide the physical port status to our virtual device. For HA to work, the condition of the gateway health check (using the command “**monitor network gateway**”) should be used instead of port status condition, for which the port status is always “UP”.

- Why there is no default IP address assigned like the APV appliance offers?

  The default IP address assignment is removed from vAPV to avoid potential IP address conflicts in the case that multiple instances of vAPV are first installed on the same hypervisor.

- Is VMware vMotion supported?

  Yes. Because vMotion operates on VMware using generic interfaces, it requires no GuestOS support. vAPV is proven to work with vMotion. Array Networks will work with customers if any issues are found while vAPV is working with vMotion.

- Is VMware HA supported?

  Yes. vAPV supports VMware HA. Array Networks will work with customers if any issues are found while vAPV is running VMware HA.

- Is VMware Tools supported?

  Yes. vAPV integrates VMware Tools, with which the following buttons besides the power button can work properly for vAPV:

  - Shutdown
  - Reset
  - Suspend
  - Resume

- Are the virtio NIC and disk supported on KVM?

  Yes. The virtio NIC and disk are supported on KVM.

- Why can’t I ping successfully after changing the MAC address of vAPV port?

  Enabling the “MAC Address Spoofing” option on the hypervisor can help avoid this issue.

- Why does vAPV fail to correctly display network interface information in some scenarios?

  If the network card driver used by the vAPV host is net_vmxnet3, net_virtio or net_af_packet, regardless of the specific network card type, the network interface information displayed by the vAPV “**show version**” command will be 10G optical port. This may not match the actual situation.

11.2 Configuration

- **How do I configure bond interfaces on VMware ESXi?**

Configuring bond interfaces on vAPV will cause duplicate packets. Thus, it is recommended to use the VMware ESXi NIC teaming function to configure bond interfaces for vAPV. Detailed steps are as follows:

1. Select the target VMware ESXi host.
2. Click "**Configure** > **Network** > **Add Network**". Select the physical interfaces for bonding while creating the vSphere standard switch (vSwitch), and complete the operation as prompted.
3. Select the vAPV that requires interface bonding, and click "**Edit Virtual Machine Setting**". Then, associate the network adapter (vAPV's virtual network interface) with the vSwitch just created.

- **How do I configure the trunk VLAN on VMware ESXi?**

1. Edit the virtual machine portgroup associated with the vAPV by setting the VLAN ID as 4095. Thus, VMware ESXi will not untag the VLAN.
2. Configure VLAN on the vAPV and the peer physical switch respectively.

- **How do I limit the interface speed on vAPV?**

On vAPV, the interface speed setting only supports the "auto" mode, indicating that the interface automatically negotiates the speed. Even if you set the interface speed manually on vAPV, the setting will not work.

