cPacket Networks, Inc.

Packet Broker (cVu-V) Quick Start Guide for Azure

Deploying the cPacket cVu-V virtual appliance in Azure Cloud

Revision History

Document Version	Date	Notes
1	02Sep2024	• The original release of this document.
2	03Dec2024	• Added Azure Marketplace instructions

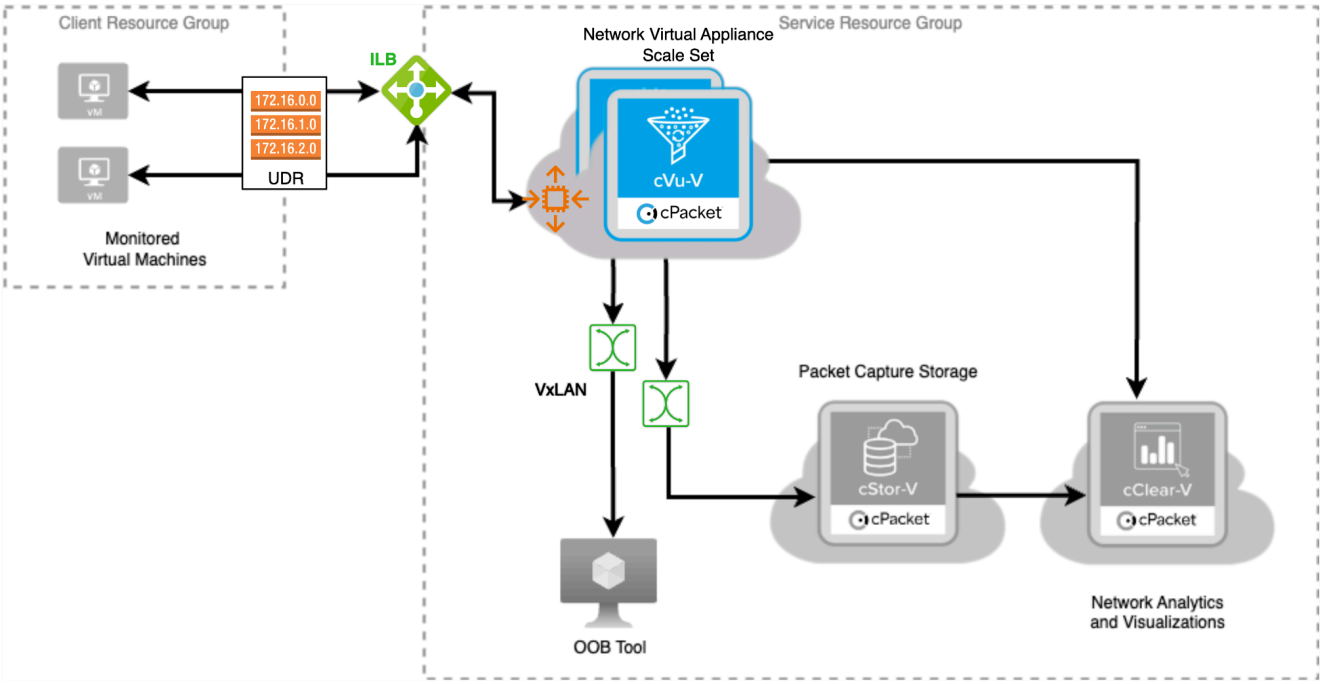
Table of Contents

Introduction

In this guide you will learn how to launch a cPacket cVu-V virtual appliance in your Microsoft Azure environment to capture packets and create flow data from a cPacket cVu-V and cPacket cStor-V. We recommend using this guide to set up a basic cVu-V deployment in accounts that are primarily used for testing and evaluation. cPacket Solutions Engineering will work with you to set up cPacket solutions at scale using deployment scripting when you are ready to deploy the solutions more broadly in Azure.

Getting started

Traffic is mirrored to the cPacket cVu-V by deploying a cPacket cVu-V inline with the network traffic to be monitored and a cVu-V to capture packets and create flow data. This setup guide describes how to deploy cVu-V to be used in conjunction with cStor-V and cClear-V. Please see the cPacket *Capture in Azure Quick Start* to setup cStor-V network mirroring and the cPacket *Analytics in Azure Quick Start* to setup cClear-V packet capture.



Before you begin

Access to the virtual hard disk (VHD) for cPacket cVu-V is available using the Azure Marketplace or by leveraging Shared Access Signature (SAS) URLs provided by cPacket. These installation instructions will cover both methods. If you prefer to use SAS URL's, please contact your cPacket representative to obtain the requisite SAS URL file.

You will need access to an Azure account with permissions to create and update Azure Resource Groups, VNET (Virtual Network) and Virtual Machines.

The following table lists all the requirements necessary to begin installation in Azure.

Requirement	Detail
Azure account	Provides access to your Azure subscriptions.
Resource Group	A container that holds related resources for the cPacket cVu-V.
Location	The geographic region where the Azure resources are located to sustain your virtual cVu-V.
Storage account	The Azure storage account contains all of your Azure Storage data objects, including blobs and disks.
Blob storage container	The storage container where the cPacket cVu-V image is stored as a blob.
Managed disk	The disk required for cPacket cVu-V data storage.
Network security group	The network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from the cPacket cVu-V.
Azure CLI	Provides extra configuration needed.

Accessing Marketplace Images

To install from the Azure Marketplace using these instructions, search for the cVu-V image during the image selection step when creating your Virtual Machine Scale Set. You do not need to subscribe to the Marketplace offer ahead of time. To locate the image, search for 'cPacket' and select 'cPacket cVu-V - Cloud Packet Broker'. See the **Create Virtual Machine Scale Set** section below for more information.

Obtain the cVu-V image via SAS URL

If you are installing from the Marketplace you can skip the SAS URL steps. If you are using the cCLoud Azure SAS URLs perform the following:

1. Login to the desired Azure account and open Azure Cloud Shell.
2. Upload the SAS URL ccloud-urls.txt file to Azure Cloud Shell.
3. Download the ccloud-azure-images script from the public GitHub repository.
4. Execute the script using the detailed instructions provided in the repository. After executing the script, you will have new image resources in your resource group.

Installation

Create a client resources group and virtual machines (Optional)

You may monitor an existing resource group/VNET/subnet or create a new one. Use the following procedure to create a new client network that will contain the traffic to be inspected by the service resource group.

1. Select **Resource groups**.
2. Select **Create**.
3. Enter the following values:
    a. **Subscription**: Select your Azure subscription.
    b. **Resource group**: Enter a new resource group name.
    c. **Region**: Select an Azure location, such as Central US.
4. Select **Next: Tags >** and add any tags desired for your resource group
5. Select **Next: Review + Create**
6. Select **Create**. It takes a few seconds to create a resource group.
7. Select **Refresh** from the top menu to refresh the resource group list, and then select the newly created resource group to open it. Or select **Notification**(the bell icon) from the top, and then select **Go to resource group** to open the newly created resource group.
8. Click **+Create**.
9. Type **Virtual network** in the search box. In the results, under **Marketplace**, select **Virtual network**. Select **Create** on the **Virtual network** page, which opens **Create a Virtual network** page.
10. In the **Basics** tab, under **Create virtual network**, make sure the correct subscription is selected and select the service resource group that you just created.
11. Type **vnet** as the name for the virtual network name.

12. Select **Next** to go to the **Security** tab. Leave the default settings.
13. Select **Next** to go to the **IP addresses** tab.
14. Select **+ Add a subnet**. Leave the default settings which will give you a default2 subnet and click add.
15. Select **+ Add a subnet** again. Leave the default settings which will give you a default3 subnet and click add.
16. Select **Next** to go to the **Tags** tab. Add any tags desired for the VNET.
17. Select **Next** to go to the **Review + Create** tab.
18. Select **Create**. It takes a few seconds to create the VNET.
19. Navigate to the resource group.
20. Click +**Create**.
21. Type **Virtual machine** in the search box. In the results, under **Marketplace**, select **Virtual Machine**. Select **Create** on the **Virtual Machine** page, which opens the **Create a Virtual Machine** page.
22. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and select the service resource group that you just created.
23. Type ***ubuntu-0*** as the name for your virtual machine.
24. Select an Ubuntu image that meets your company requirement, for example **Ubuntu Server 22.04 LTS - x64 Gen2**
25. For **Authentication type,** choose **SSH public key.** For **SSH public key source** choose **Use existing public key** and paste in your public key. Only provide your public key, such as ~/.ssh/id_rsa.pub. You can use the Azure Cloud Shell from the portal to create and use SSH keys.
26. Select **Next: Disks >** Leave the defaults.
27. Select **Next: Networking >**.
28. Under **Subnet** select **default2.**
29. Select **Next: Management >** Leave the defaults.
30. Select **Next: Monitoring >** Leave the defaults.
31. Select **Next: Advanced >** Leave the defaults.
32. Select **Next: Tags >**. Add any tags desired.
33. When you're done, select **Review + create**.
34. After it passes validation, select **Create** to deploy the virtual machine.
35. Repeat steps 20-34 for a second Virtual machine. Change the name on step 23 to **ubuntu-1**. Change the subnet on step 29 to **default3**.

Create service resource group (Optional)

If you do not already have a service resource group with cClear-V and/or cStor-V, use the following procedure to create a service resource group plus the additional resources that you need to run cVu-V, such as subnets and route tables.

1. Select **Resource groups**.
2. Select **Create**.
3. Enter the following values:
    - **Subscription**: Select your Azure subscription.
    - **Resource group**: Enter a new resource group name.
    - **Region**: Select an Azure location, such as Central US.
4. Select **Next: Tags >** and add any tags desired for your resource group
5. Select **Next: Review + Create**
6. Select **Create**. It takes a few seconds to create a resource group.
7. Select **Refresh** from the top menu to refresh the resource group list, and then select the newly created resource group to open it. Or select **Notification**(the bell icon) from the top, and then select **Go to resource group** to open the newly created resource group.

Create Load Balancer

1. Navigate to the resource group with your cClear-V and/or cStor-V.
2. Click **+Create.**
3. Type **load balancer** in the search box. In the results, under **Marketplace**, select **Load Balancer**. Select **Create** on the **Load Balancer** page, which opens the **Create load balancer page**.
4. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and select the service resource group that you just created or an existing resource group where cClear-v has been deployed.
5. Type ***cvu-lb*** as the name for the load balancer.
6. Select **Next: Frontend IP configuration >**
7. Click **+ Add a frontend IP configuration.** Type **cvu-lb-fe** as the name. Select the virtual network and subnet you will be placing the **cVu-V scale set.** If you created a client resource (above) then it should be **vnet** and **default**. **Click Save.**
8. Select **Next: Backend pools >** Leave the defaults.
9. Select **Next: Inbound rules >** Leave the defaults.

10. Select **Next: Outbound rules >** Leave the defaults.
11. Select **Next: Tags >** and add any desired tags.
12. Select **Next: Review + create >**
13. After it passes validation, select **Create** to deploy the load balancer.

Create Virtual Machine Scale Set

1. Navigate to the resource group with your cClear-V and/or cStor-V.
2. Click +**Create.**
3. Type **Scale set** in the search box. In the results, under **Marketplace**, select **Virtual Machine Scale Sets**. Select **Create** on the **Virtual Machine Scale Sets** page, which opens the **Create a Virtual Machine Scale Set** page.
4. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and select the service resource group that you just created or an existing resource group where cClear-v has been deployed.
5. Type ***cvuScaleSet*** as the name for your scale set.
6. Under **Orchestration**, ensure the **Uniform** option is selected for **Orchestration mode**.
7. Locate and select the cVu-V image for **Image**. This can be either the image located in the Marketplace or the one installed into your resource group using SAS URL's.
8. Under **Size** select **Standard_D4s_v5**.
9. Under **Username** type **ubuntu.**
10. Choose **SSH public key**. Only provide your public key, such as ~/.ssh/id_rsa.pub. You can use the Azure Cloud Shell from the portal to create and use SSH keys.
11. Under **Licensing** select Other.
12. Select **Next: Spot >** Leave the defaults.
13. Select **Next: Disks >** Leave the defaults.
14. Select **Next: Networking >**
15. In **Virtual network**, select the client virtual network or the virtual network your traffic is on. If you did the **Create a client resources group and virtual machines (Optional)** step at the beginning of this document, choose that virtual network which you should have named **vnet**
16. In **Network interface**, verify the NIC is in a separate network than your traffic. If you created a client resource (above) then it should be default.
17. In **Load balancing options**, select **Azure load balancer**.
18. In **Select a load balancer** select **cvu-lb** that you created above.
19. in **Select a backend pool** select **Create new**

a. In **Name** type **cvu-lb-bepool**.

b. Select **Create**.

20. Select **Next: Management >** leave defaults.
21. Select **Next: Health >** leave defaults.
22. Select **Next: Advanced >**.
23. Enter the following **custom data** into the text box.

```
#!/bin/bash
set -ex

downstream_tool_ip="<cstor_ip_addr>"
capture_nic_name="$(ip -o link show | awk -F': ' '/^[0-9]+: e/{print $2}' | sed -n
'1p')"
capture_nic_ip="$(ip -o -4 addr show | awk -F '[: ]+' '/global/ { print $4 }' | cut
-d'/' -f1 | sed -n '1p')"

config_file="/home/cpacket/boot_config.toml"
touch "$config_file"
chmod a+w /home/cpacket/boot_config.toml

cat >/home/cpacket/boot_config.toml <<EOF_BOOTCFG
vm_type = "azure"
cvuv_mode = "inline"
cvuv_mirror_eth_0 = "$capture_nic_name"
cvuv_vxlan_id_0 = 1337
cvuv_vxlan_srcip_0 = "$capture_nic_ip"
cvuv_vxlan_remoteip_0 = "$downstream_tool_ip"
web_hash = "$2b$12$HDtoaDtI5V.DGiREeuY2yeqjvSM3Y1UxS1b.8Te/5ynSzefSRvAZW"
EOF_BOOTCFG
```

24. Change the **<cstor_ip_addr>** to the IP address of the cStor-V you deployed or change to no characters if there is not a downstream tool.
25. Click **Next:Tags >** and add any desired tags.
26. When you're done, select **Review + create**.
27. After it passes validation, select **Create** to deploy the scale set.
28. Navigate to the resource group with your cVu-V scale set.
29. Select the **cvu-lb** from the list of resources.
30. Select **Settings > Health probes.**
31. Select **+Add.**
32. In **Name** type **cvu-lb-hp.**
33. Verify the **Protocol** is TCP

34. Verify the **Port** is 80.
35. Select **Save.**
36. Select **Settings > Load balancing rules.**
37. Select **+Add.**
38. In **Name** type **cvu-lb-rule.**
39. In **Frontend IP address** select **cvu-lb-fe.**
40. In **Backend pool** select **cvu-lb-bepool.**
41. Select **High availability port.**
42. in **Health probe** select **cvu-lb-hp.**
43. Select **Enable TCP Reset.**
44. Select **Save.**
45. Navigate to the resource group with your cVu-V scale set.
46. Select **cvuScaleSet** from the list of resources.
47. Select **Operations > Health and repair.**
48. Select **Enable application health monitoring.**
49. In **Application health monitor** select **Load balancer probe**.
50. Verify **Use existing** is selected.
51. Verify **Load balancer health probe** is set to **cvu-lb-hp**.
52. Select **Save**. Wait for update to complete.
53. Select **Instances**.
54. Select all instances and select **Upgrade**. Select **Yes**. Wait for the upgrade to complete. If Latest model says “Yes”, click refresh or wait until they no longer show that they are the Latest model before upgrading.
55. Select **Operations > Upgrade policy**.
56. In **Upgrade mode,** select **Rolling…,** leave the defaults. Select **Apply**. Note: It may take a few minutes to be able to apply **Rolling…**
57. Check to make sure the instances are healthy by going to cvuScaleSet > Instances.

Enable IP forwarding

To route traffic through the cVu-V, turn on IP forwarding in Azure. When IP forwarding is enabled, any traffic received by the cVu-V that's destined for a different IP address, isn't dropped and is forwarded to the correct destination.

Get started with Azure Command-Line Interface (CLI)

1. Run the following command. Be sure to change the <resource_group> to your resource group.

```
az vmss update \
--name cvuScaleSet \
--resource-group <resource_group> \
--set
"virtualMachineProfile.networkProfile.networkInterfaceConfigurations[
0].enableIpForwarding=true"
```

2. Wait until the cVu scale set has been updated by the rolling updates. You can check the health in the scale set instance page.

Create a route table

In this section, create a route table to define the route of the traffic through the cVu-V virtual machine. The route table is associated with the subnet where the client virtual machines are deployed.

1. Navigate to the resource group you are using for cVu.
2. Click +**Create.**
3. Type **Route table** in the search box. In the results, under **Marketplace**, select **Route table**. Select **Create** on the **Route table** page, which opens the **Create Route table** page.
4. In **Create Route table** enter or select the following information:

Field	Value
Project details	
Subscription	Select your subscription.
Resource group	Select the cVu resource group used
Instance details	
Region	Select the region the client virtual network is in.
Name	Enter route-table-ubuntu-0.
Propagate gateway routes	Leave the default of Yes.

5. Select **Next** to go to the **Tags** tab. Add any tags desired for the VNET.
6. Select **Next** to go to the **Review + Create** tab.

7. Select **Create**.
8. Repeat steps 1-7 for a second Route table. Change the name on step 4 to **route-table-ubuntu-1**.

Create a route

In this section, create a route in the route tables that you created in the previous steps.

1. Navigate to the resource group you are using for cVu.
2. Select route-table-ubuntu-0.
3. In **Settings** select **Routes**.
4. Select **+ Add** in **Routes**.
5. Enter or select the following information in **Add route:**

Field	Value
Route name	Enter route-table-ubuntu-0-route.
Destination type	Select IP Addresses.
Destination IP addresses/CIDR ranges	Enter 10.0.2.0/24.
Next hop type	Select Virtual appliance.
Next hop address	Enter 10.0.0.4. This is the IP address of cvu-lb frontend you created in the earlier steps.

6. Select **Add**.
7. Select **Subnets** in **Settings**.
8. Select **+ Associate**.
9. Enter or select the following information in **Associate subnet**:

Field	Value
Virtual network	Select vnet.
Subnet	Select default2.

10. Select **OK**.
11. Repeat steps 1-10 for **route-table-ubuntu-1** to create a second Route table. Change the name on step 5 to **route-table-ubuntu-1-route**, Destination IP to **10.0.1.0/24**. In step 9, change Subnet to **default3**

After Installation and Launching

Please allow up to 10 minutes for the cVu-V to become accessible. To reach the cVu-V, a jump box connection needs to be established. This connection can be created using the cClear-V. In case your cClear-V does not already have a public IP address, it is necessary to assign one. Associate a public IP address to a virtual machine.

Log In and License

1. Create a tunnel using SSH local port forwarding. In your terminal, enter:

```
ssh -N -L 127.0.01:8443:<cvu_private_ip_address>:443 \
ubuntu@<cclear_public_ip_address> -i <privatekey>
```

- 8443 is the local port that is forwarded to the VM instance via SSH.
- <cvu_private_ip_address> is the cCur-V instance private IP address.
- <cclear_public_ip_address> is the cClear-V instance public IP address.
- <privatekey> is the SSH key pair used as a prerequisite.

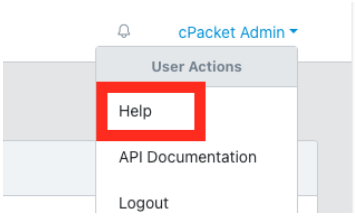
2. Set a manual proxy in your web browser for a SOCKS host: **localhost** and Port: **8443**
3. Enter https://127.0.0.1:8443 in your web browser to reach the cVu login page.

NOTE: You may need to add the **8443** into your URL if it is removed.

cVu-V requires you to have a valid license to replicate traffic to downstream tools. You should connect this cVu-V to an existing cClear-V with an active cVu-V license. The cClear-V must have a network path to the cVu-V.

Verifying Operation

1. In cClear add your cVu. For detailed instructions, please refer to the cClear User Guide which can be accessed from the help menu.



a. Go to Configure > cVus.

b. Click Add cVu.

   For Auth Type, select User Login.

   i. Enter the cVu name, IP address, and login credentials.

   ii. Click Save to add the cVu.

2. Verify that cClear-V is indicating that traffic is flowing to your cVu-V packet capture appliance.