



cPacket Cloud Suite

Quick Start Guide for Azure cStor-V Packet Capture

Version 24.2.1

Revision History

Document Version	Date	Notes
1	13Aug2024	<ul style="list-style-type: none">• The original release of this document.
2	10Sep2024	<ul style="list-style-type: none">• Clarify license delete steps.
3	03Dec2024	<ul style="list-style-type: none">• Added Azure Marketplace instructions.
4	10Jan2025	<ul style="list-style-type: none">• Minor document reference edits.
5	15Apr2025	<ul style="list-style-type: none">• Title update

Table of Contents

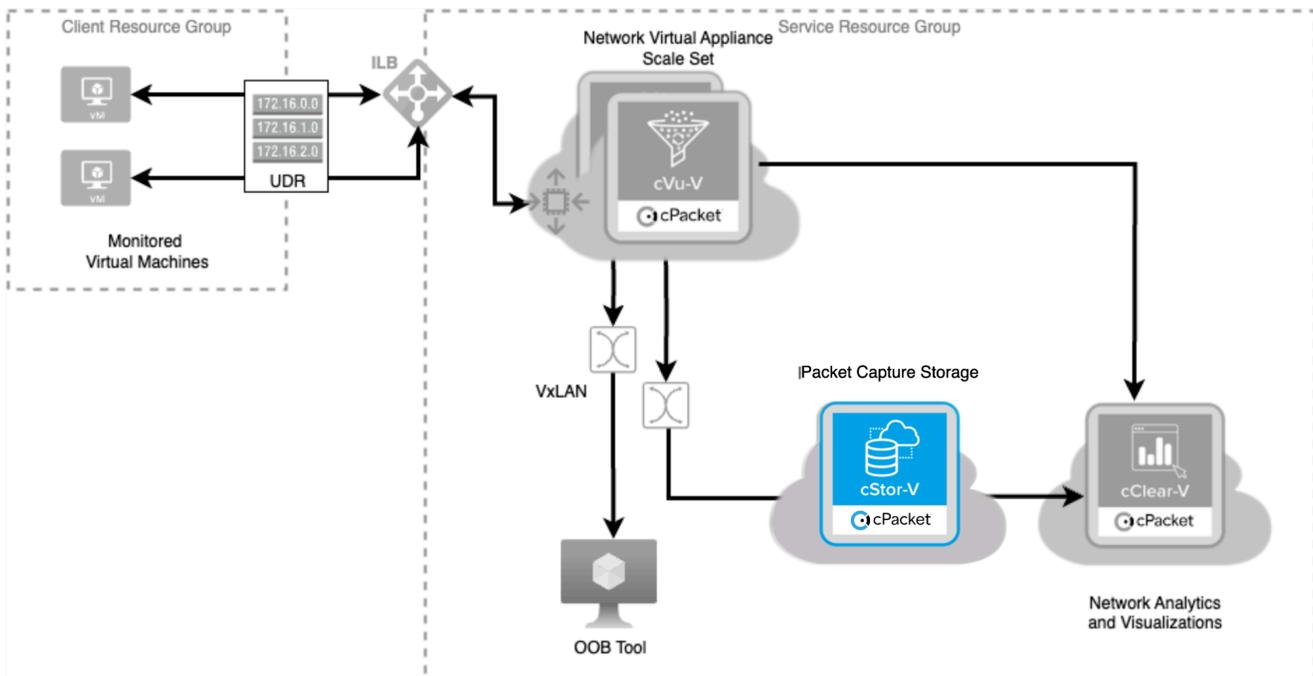
Revision History	1
<i>Introduction</i>	3
<i>Getting started</i>	3
<i>Before you begin</i>	3
Accessing Marketplace Images	4
Obtain the cStor-V image via SAS URL	4
<i>Installation</i>	5
<i>After Installation and Launching</i>	6
Log In and License	6
Verifying Operation	7
Appendix A: Azure Storage Configuration	7
Disk Volumes	7
Calculating Storage Needs	8
Example	8
Troubleshooting	8

Introduction

In this guide you will learn how to launch a cPacket cStor-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 cStor-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 cStor-V by deploying a cPacket cVu-V inline with the network traffic to be monitored and a cStor-V to capture packets and create flow data. This setup guide describes how to deploy cStor-V to be used in conjunction with cVu-V and cClear-V. See the **Quick Start Guide for Azure cVu-V Packet Broker** to setup cVu-V packet mirroring and the **Quick Start Guide for Azure cClear-V Control Center** to setup cClear-V packet capture.



Before you begin

Access to the virtual hard disk (VHD) for cPacket cStor-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.

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 cStor-V.
Location	The geographic region where the Azure resources are located to sustain your virtual cStor-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 cStor-V image is stored as a blob.
Managed disk	The disk required for cPacket cStor-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 cStor-V.

Accessing Marketplace Images

To install from the Azure Marketplace follow these steps:

1. Login to the Azure Portal
2. [Navigate to the cStor-V Marketplace offer](#) and select the 'Get It Now' button.
3. Select 'Continue' to proceed past the pop-up to agree to share information with cPacket.
4. Select 'Create' which will take you to the 'Create a Virtual Machine' page.
5. Jump to the [Installation](#) section below to continue the process.

Obtain the cStor-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.
5. Use the search bar to find 'Azure Compute Galleries' and select the service.
6. Locate and select 'cStor-V'.
7. Click the 'Create VM' button to initiate the VM creation process.

Installation

The steps required for installation from the Azure Marketplace and using SAS URLs are similar with a few differences called out below.

Fill in the following details on the Create a virtual Machine page:

Field	Value
Subscription	Use the dropdown to specify the subscription where the software should be deployed.
Resource Group	Create a new resource group or select the existing resource group where cStor-V should be deployed.
Name	Assign a unique name for your machine

1. Select a machine size. The standard machine size recommendation for cStor-V is **Standard_D8s_v5**. Additional options are provided below.

Instance Type	Capture Volumes	Details
Standard_D8s_v5	2	Recommended for proof of concepts with analytics enabled (1 Gbps)
Standard_D32s_v5	10	For 5 Gbps capture with analytics enabled
Standard_D64s_v5	16	For 10 Gbps capture with analytics enabled

2. Fill in the following required fields:
 - SSH Key Username: ubuntu
 - SSH public key source: Allow Azure to generate a new key or use an existing one.
 - Key pair name: Use the generated name or assign a new one.

- **For SAS URL Deployment:** Selected inbound ports: HTTPS (443), SSH (22) (Marketplace images are configured with these ports automatically enabled).
3. Click **Next: Disks**.
 4. Create and attach a data disk for the database volume.
 - Click **Create and attach a new disk**.
 - Select a 32 GiB drive.
 - Check the **Delete disk with VM** option.
 5. Create and attach two disks for the capture volumes. The cost will increase with the size of the disks.
 - Click **Create and attach a new disk**.
 - Select a 256 GiB drive or a size that suits your needs (See [Appendix A: Azure Storage Configuration](#)). 256 GiB x 2 volumes can store approximately an hour of capture and analytics data for a 1 Gbps traffic rate.
 - Check the **Delete disk with VM** option.
 - Repeat these steps to add a second disk. The second disk **must** be the same size as the first disk. Note that all capture volumes must be of the same size.
 6. Click **Next: Networking**
 7. Retain the default networking settings. This will provide you with a new Virtual Network, Subnet, and Public IP. Confirm that the allowed inbound ports are HTTPS (443) and SSH (22). Enable the '**Delete public IP and NIC when VM is deleted**' option.
 8. Skip the **Management, Monitoring, and Advanced** sections and proceed directly to 'Tags'. Add an 'owner' tag with your email address as its value.
 9. Click **Review + create**, then **Create**.
 10. Once your resource is created, retrieve the public IP for login purposes.
 - Click on **Virtual Machines** from the left-side menu.
 - Select the specific virtual machine for which you want to find the public IP address.
 - On the **Overview** page of the virtual machine, you will find the Public IP address listed.
 11. Please allow up to 10 minutes for cStor-V instances to launch. Navigate to 'https://<your_public_ip>' to log in to the UI.

After Installation and Launching

It will take several minutes for the cStor-V to be accessible. To access the cStor-V use the public IP address that is displayed on the EC2 Instances page, enter the IP address into a browser to login. You will need to accept the certificate to access the login page.

Log In and License

cStor-V requires you to enter the activation key to capture packets and use analytics. Alternatively, if you have an existing cClear or cClear-V with an active cStor-V license you can add this cStor-V to it and refresh the license. The cClear-V must have a network path to the cStor-V.

For stand-alone cStor-V deployments, add a license key to the cStor-V follow the steps below.

1. At the cStor-V login page use the default admin username: cpacket
2. If you have deployed from Azure Marketplace, the password will be the vmlid found in the JSON view for the running virtual machine. The JSON viewer can be accessed by navigating to the Overview tab for the running VM and selecting 'JSON View' located on the right-hand side of the screen. This vmlid looks like *09fd42196-74a6-46dc-a6d4-29ec13ee138d*, where the letters and numbers are unique to your instance. If you have deployed using a cPacket SAS URL's, the password will be: cpacketpw
3. After you login on the left pane select Software.
4. Enter the license key provided to you from cPacket.

Important: If you want to reinstall a different configuration and reuse the same license key, make sure you delete the license from the cStor-V before destroying the instance using the following steps.

1. On the left panel, select Software.
2. Select Delete to release the license and confirm the delete.

Verifying Operation

This cStor-V installation has a single interface that is used for both management and packet capture which make it easy to verify that the cStor-V is operating correctly.

1. After you are logged in, select Capture from the left pane on the cStor
2. In the Range Settings parameters, set the capture length for 15 seconds

3. Select **Download** in the Capture settings and a packet capture will be downloaded
4. Open the packet capture file using Wireshark and you will see the TLS session between your browser and the cStor-V.

If you see a TLS session in the packet capture your cStor-V is operational.

Appendix A: Azure Storage Configuration

Disk Volumes

Our product requires the following disk volumes:

1. **OS Volume (Root volume)** : This volume should be 30 GiB.
2. **Database Volume (Uses smallest volume)**: This volume should be twice the size needed to store packet capture reports.
3. **Capture Volumes (Other volumes)** : These volumes store packet captures. The number and size of these volumes depend on the network traffic being captured and the amount of time you want to retain the data.

Calculating Storage Needs

Here is a step-by-step guide to calculate your storage needs:

1. **Determine Database Volume Size:** Decide how much storage you wish to allocate for reports. The size of the database volume should be:

$$2 * (\text{for reports in GiB}) = < \text{Database Volume Size} > \text{ GiB}$$

2. **Calculate Total Capture Storage:** Use this formula:

$$< \text{Number of Gb per second} > / 8 * < \text{Storage Time (in seconds)} > = \text{Total Capture GiB.}$$

This will give you the total storage needed for the packet captures.

Example

If the network traffic is 2Gb per second, and you would like to retain data for 1 hour (3600 seconds). You also plan to allocate 10 GiB for packet capture reports.

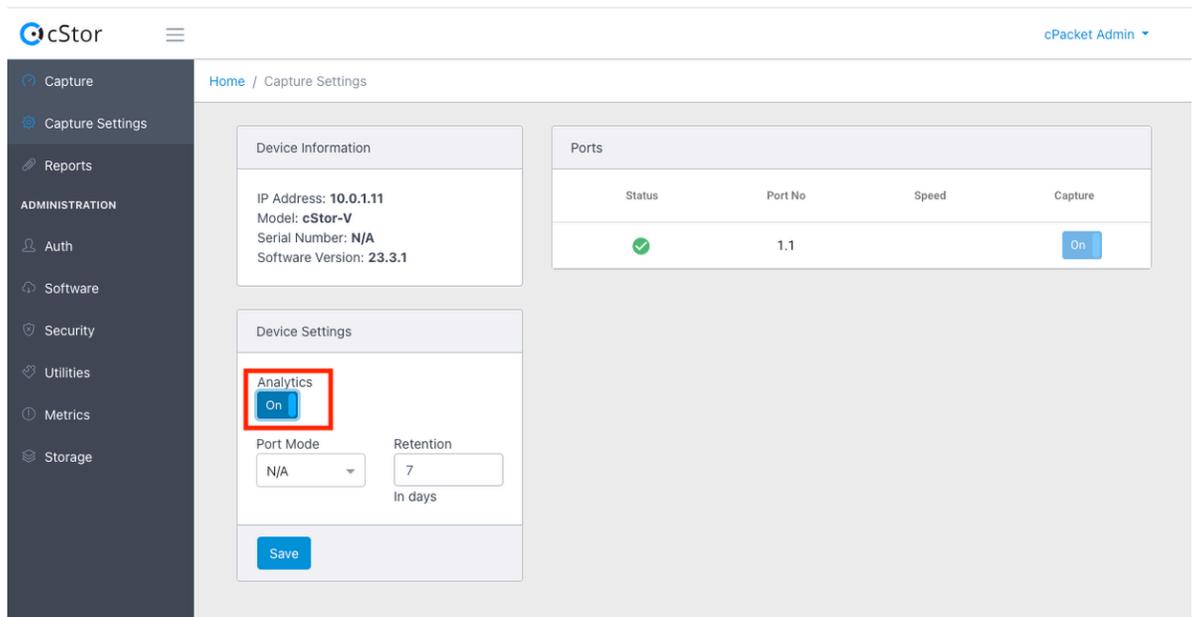
- Total Capture Storage: $2 / 8 * 3600 = 900 \text{ GiB}$
- Database Volume: $2 * 10 = 20 \text{ GiB}$ (Minimum size cannot be less than 8GiB)

In this case, you would need 1 OS volume (32 GiB), 1 database volume (20 GiB), and 4 capture volumes (256 GiB each).

Remember, these numbers will depend on your specific network traffic and storage time requirements.

Troubleshooting

- If no traffic is seen on cStor-V, verify that the green checkmark is shown for the connected cStor in the 'Ports' panel in the Capture Settings tab.
- If no capture statistics are visible in the cStor-V dashboards, verify that Analytics is enabled on your cStor-V in the Capture Settings tab.



The screenshot displays the cStor Capture Settings interface. The left sidebar contains navigation options: Capture, Capture Settings, Reports, and ADMINISTRATION (Auth, Software, Security, Utilities, Metrics, Storage). The main content area is titled 'Home / Capture Settings' and is divided into three panels:

- Device Information:** IP Address: 10.0.1.11, Model: cStor-V, Serial Number: N/A, Software Version: 23.3.1.
- Device Settings:** Analytics is set to 'On' (highlighted with a red box). Port Mode is 'N/A' and Retention is '7' days.
- Ports:** A table with columns Status, Port No, Speed, and Capture. The Status column shows a green checkmark, and the Capture column shows an 'On' button.