cPacket Networks, Inc.

Analytics in AWS Quick Start

Deploying the cPacket cClear-V virtual appliance in AWS

Table of Contents

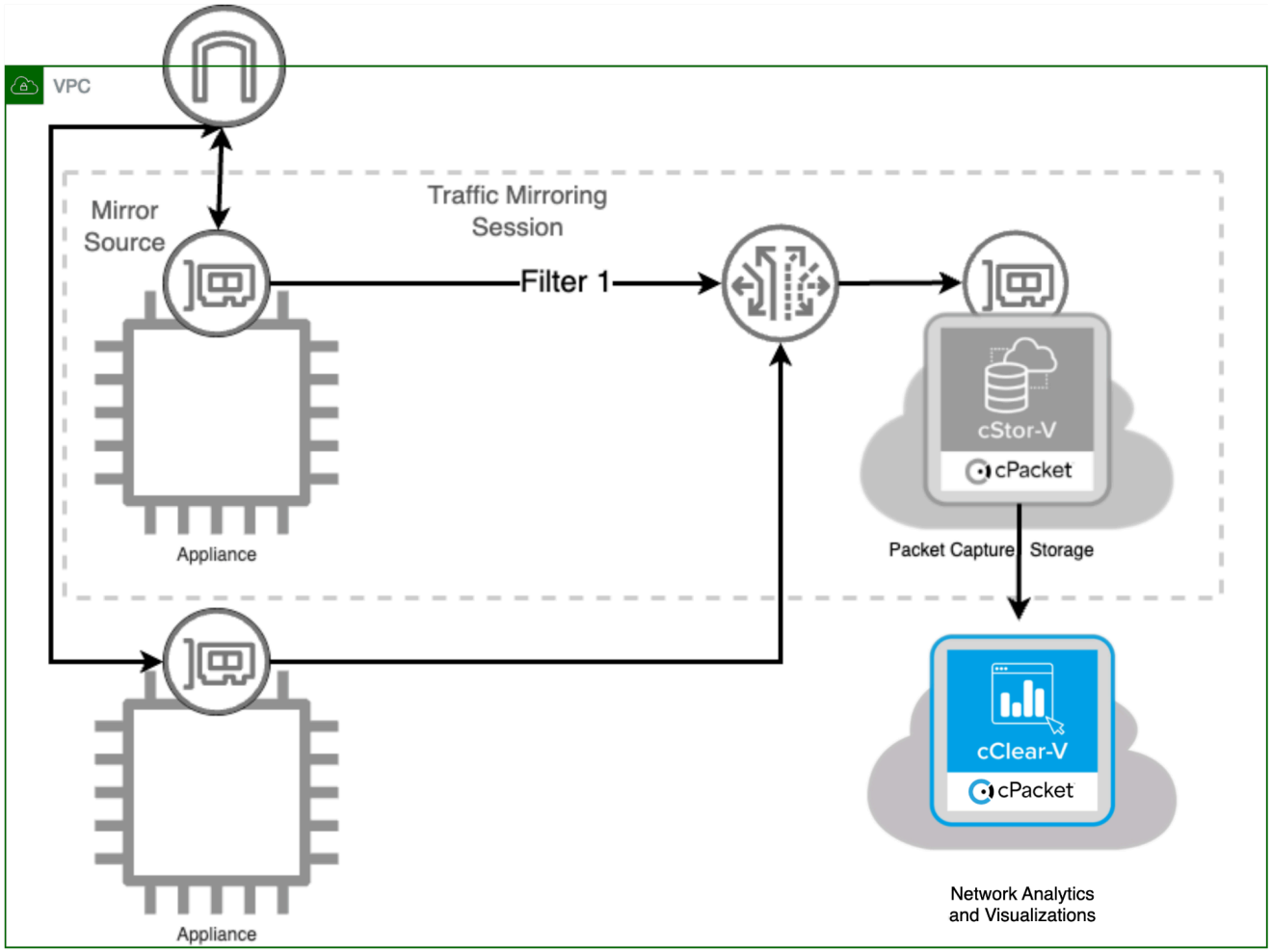
© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

Introduction

In this guide you will learn how to launch a cPacket cClear-V virtual appliance in your Amazon Web Services (AWS) environment to analyze packets from a cPacket cStor-V. We recommend using this guide to set up a basic cClear-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 AWS.

Getting started

cClear is used to analyze packet data from other cPacket products. This setup guide describes how to deploy cClear-V to be used in conjunction with cStor-V. Please see the cPacket *Capture AWS Quick Start* to set up cStor-V packet capture and mirroring.



© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

Before you begin

Access to the Amazon Machine Images (AMI) for cPacket appliances is provided through the AWS Marketplace or alternatively they can be shared to a specific AWS account ID and Region where you will be installing cClear-V. Currently cClear-V and cStor-V virtual appliances are available in the AWS Marketplace, which is the easiest way to install cPacket virtual appliances. This guide will cover both installation processes. If you cannot access the AWS Marketplace, you must provide the AWS account ID and Region where you will be installing cClear-V to your cPacket representative. cPacket will share the latest AMI images for the virtual appliance to this account ID in selected regions.

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

Requirement	Detail
AWS User ID	You will need a user ID in an AWS account, permissions for the user are listed below.
AWS Account and Region	If you cannot access the AWS Marketplace, an AWS account and region must be provided to cPacket so the virtual appliance images (Amazon Machine Image - AMI's) can be shared. Account numbers are 12 digits in length and example regions names are: us-east-1, us-west-2, …
cPacket License Key	cPacket will provide you with a license key used to activate the cClear-V appliance.
AWS Organization Tagging Policies	Your organization may have requirements for tagging resources created in the cloud. Common tag requirements are: Name, Owner, and CreatedBy. If these tags are mandated by your organization, creating a device without them will fail the organizational policy. Remediation is to simply add the required tags at resource creation time.
Identity and Access Management (IAM) User/Permissions/Role	In the account used for installation, the user needs to have permissions granted to setup the cClear-V virtual appliance. See IAM Policy to install cClear-V for the minimum permissions. Your organization may already have roles defined that grant these permissions through their IAM policies, if not there are existing AWS managed policies that can be granted to the user or the group the user is a member of. They are: - AmazonEC2FullAccess - AmazonEC2RoleforSSM - IAMFullAccess

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

	- AWSMarketplaceManageSubscriptions (for marketplace access)
Network Bandwidth	The network bandwidth to be captured will determine the size of the instance for the cClear-V appliance. Recommendation on instance sizing and the number of storage volumes are contained later in this guide and indexed by network bandwidth of Gbps you would like to capture.
Virtual Private Cloud (VPC)	You will need a **VPC** to install the cClear-V into. We recommend working with your organization's AWS cloud support team and request a VPC that has an AWS Internet Gateway already configured, and has EC2 instances generating traffic you would like to capture. The cClear-V will be installed into the same VPC.
Security Groups/Policies	The following ports will be opened on the cClear-V for inbound and outbound traffic. Inbound: - TCP 22 – SSH traffic - TCP 443 – Encrypted HTTP traffic - Outbound ports: - All TCP/UDP ports
SSH Key Pair	A SSH public/private key pair to control access to the virtual appliances and hosts. If you don't currently have an SSH Key Pair you can create one during installation.
AWS Cloud Shell Access	The account and use you are using must have permission to use the AWS Console.

Installation using AWS Marketplace cClear-V AMI

The following steps describe how to install the cClear-V image from the AWS Marketplace. This is the easiest way to install a cClear-V virtual appliance for evaluation purposes. Your user must have permission to install subscriptions from the Marketplace for this installation procedure.

1. Sign in to AWS with your username and password.
2. Search the Amazon Marketplace for cPacket and select **cPacket cClear-V - cPacket Management and Visualization**.
3. Select **Continue to Subscribe**.

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

4. Accept the Terms and Conditions for the **cPacket cClear-V** and select **Continue to Configuration**.
5. Select the options on the **Configure this software** page to launch the cClear-V.

Field	Value
Fulfillment option	Select **64-bit (x86) Amazon Machine Image (AMI)**
Software version	Select the software version to deploy, we recommend using the latest release in the Marketplace.
Region	Use the dropdown to specify the region where the software should be deployed.

6. Select **Continue to Launch** to continue.
7. On the **Launch this software** page, select **Launch through EC2** for the **Choose Action** field.
8. On the **Launch an instance** page, enter or select the following information:

Field	Value
Name and tags	Add any tags you'd like. As a best practice, we recommend a **Name** and **owner** tag.
Instance type	Leave **m5a.2xlarge** as the default.
Key pair (login)	You can use an existing key pair or create a new one.
Network	Select the VPC you want to launch your instance into.
Subnet	Select the subnet you want to use from the dropdown or select **Create a new subnet**.
Auto-assign public IP	Leave Auto-assign public IP enabled.
Security Group	For quickest installation we recommend creating a new security group as it will include the default ports required. If users wish to utilize an existing security group, ensure inbound ports TCP 22 (SSH) and TCP 443 (HTTPS) are open.
Configure storage	Leave the Size (GiB) field for the root volume at its default value (40 GiB). Change the second volume to meet your storage requirements. 200 GiB can hold approximately one week of analytics for a 5 Gbps network traffic rate. **Note:** You can contact your sales representative for assistance choosing a volume size that balances expenses with your need to preserve data based on expected traffic types and load.

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

9. Select **Launch instance** when ready to continue.

A Success message confirms the launch of the instance and displays the instance ID. You will need the instance ID in order to login to the cClear-V appliance as it is the default password. Even though the Instance will now indicate it is **Running**, users may need to wait up to 15 minutes after deploying before all services are fully operational. You can now continue to test your installation, proceed to After Installation and Launching.

Installation using the cPacket cClear-V Shared AMI

The following steps describe how to install the cClear-V image shared to your AWS account and region. You only need to follow these steps if your organization and user do not have access to the AWS Marketplace.

1. Sign in to AWS with your username and password.
2. Select **EC2**.
3. In the left navigation panel, under Images, select **AMIs**.
4. Above the table of AMIs, change the Filter from Owned by Me to Private Images.
5. Using the filter box, find the cPacket cClear-V (CCLEAR) AMI and then press ENTER.
6. Select the checkbox next to the cPacket cClear-V AMI and select **Launch Instance from AMI**.
7. Adding any tags required by your organization. The “Name” tag becomes the instance’s name and you can add any other tags that your organization may require. Make sure you select the Resource Types to apply the tags to, for cClear-V you can select Instances, Network Interfaces, and Volumes.
8. Select one of the following supported instance types:

Instance Type	Details
m5n.2xlarge	**Recommended for proof of concepts**
m5n.4xlarge	For 5Gbps packet traffic
m5n.8xlarge	For 10Gbps packet traffic

9. Select or create a SSH Key pair. This key is used to access the instance remotely over SSH. If you create a new one it will download the .PEM file to your Downloads folder.
10. Select the **Edit** button on the Network Settings to edit VPC and network policies for the cClear-V appliance.
11. Select the VPC to run from the VPC drop down menu.

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

12. Make sure the **Auto-assign public IP** is enabled, this will allow access to the web UI on the cClear-V from the Internet

13. You can select an existing security group used by your organization or create one when you launch this cClear-V. The following security rules and protocols are needed for the cClear-V, you can add additional protocols by selecting **Add security group rule**.

Type	Port	Source Type
SSH	22	Select My IP for restricted or Anywhere for unrestricted access
HTTPS	443	Select My IP for restricted or Anywhere for unrestricted access

14. Configure storage.

15. Leave the Size (GiB) field for the root volume at its default value (40 GiB). Change the second volume to 200 GiB. 200GiB can hold approximately one week of analytics for a 5 Gbps network traffic rate.

16. (Optional) Edit each EBS volume to switch their encryption status to “Encrypted” if you select the Advanced and show details option.

17. From the **Shutdown behavior** drop-down list, select **Stop**.

18. Select **enable** in the Termination protection drop down list.

19. Select **Launch Instance**.

After Installation and Launching

It will take up to 15 minutes for the cClear-V to be accessible. To access the cClear-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

cClear-V requires you to enter the activation key to manage cStor-V and use analytics. To manage cStor-V the cClear-V must have a network path to the cStor-V. To add an activation key to cClear-V follow the steps below:

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

At the cClear-V login page use the default admin username: cpacket

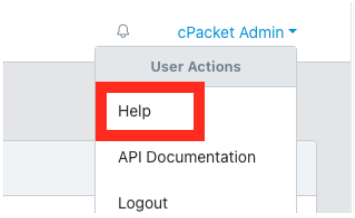
1. The password will be :
    a. For AWS Marketplace Deployment: [insert-ec2-instance-id]
    b. For Shared AMI Deployment: cpacketpw
2. After you login on the left pane select **Administration -> Software.**
3. Under **Licenses**, enter the license key provided to you from cPacket.

Important: If you want to reinstall a different configuration and reuse the same license key, make sure you delete the license from the cClear-V using the steps below:

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

Verifying Operation

1. In cClear-V, add an available cStor-V instance. For detailed instructions, please refer to the cClear User Guide which can be accessed from the help menu.



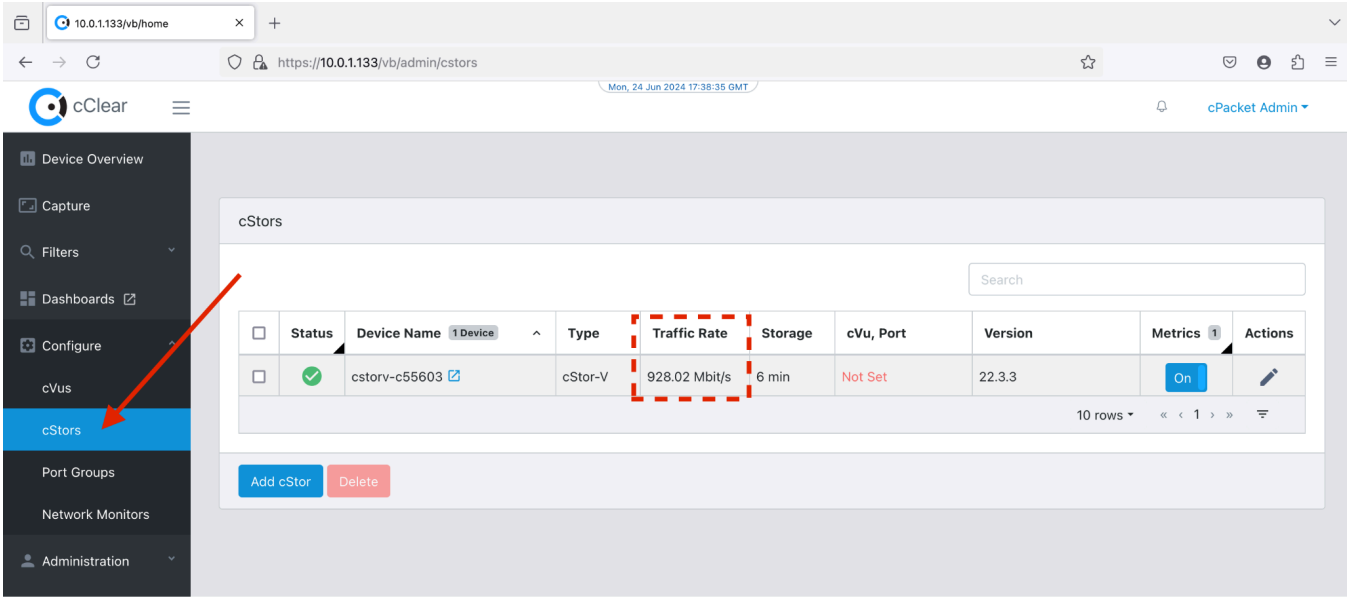
    a. Go to Configure > cStors.
    b. Click Add cStor.

    For Auth Type, select User Login.

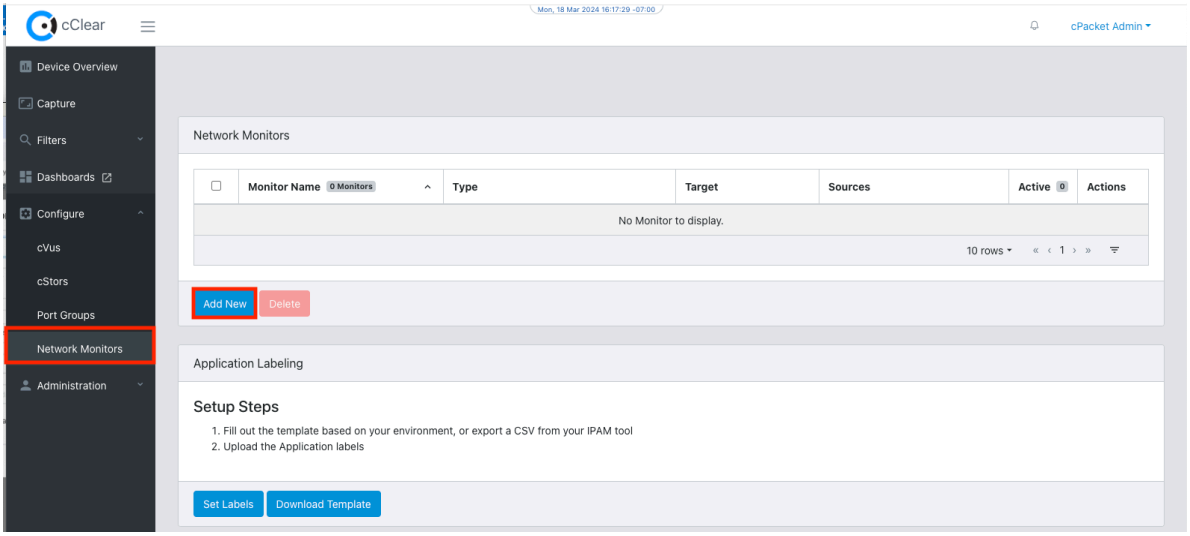
        i. Enter the cStor name, IP address, and login credentials. Selecting an associated cVu and port is optional.
        ii. Click Save to add the cStor.

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

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



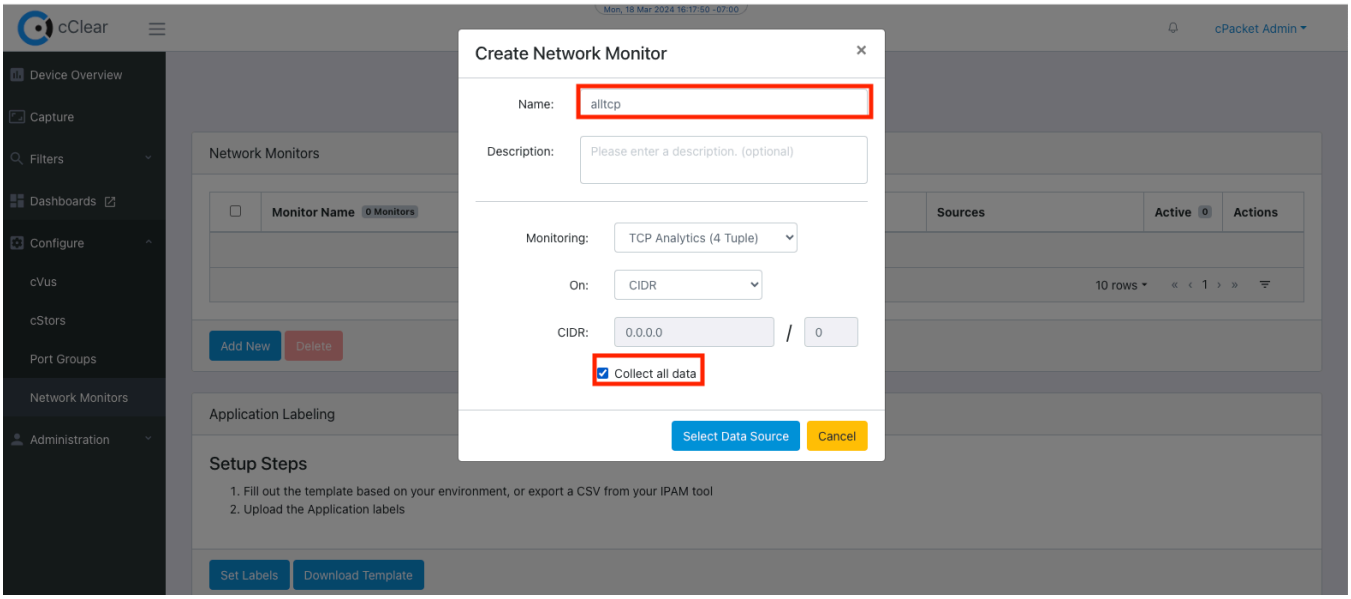
3. In cClear add a network monitor



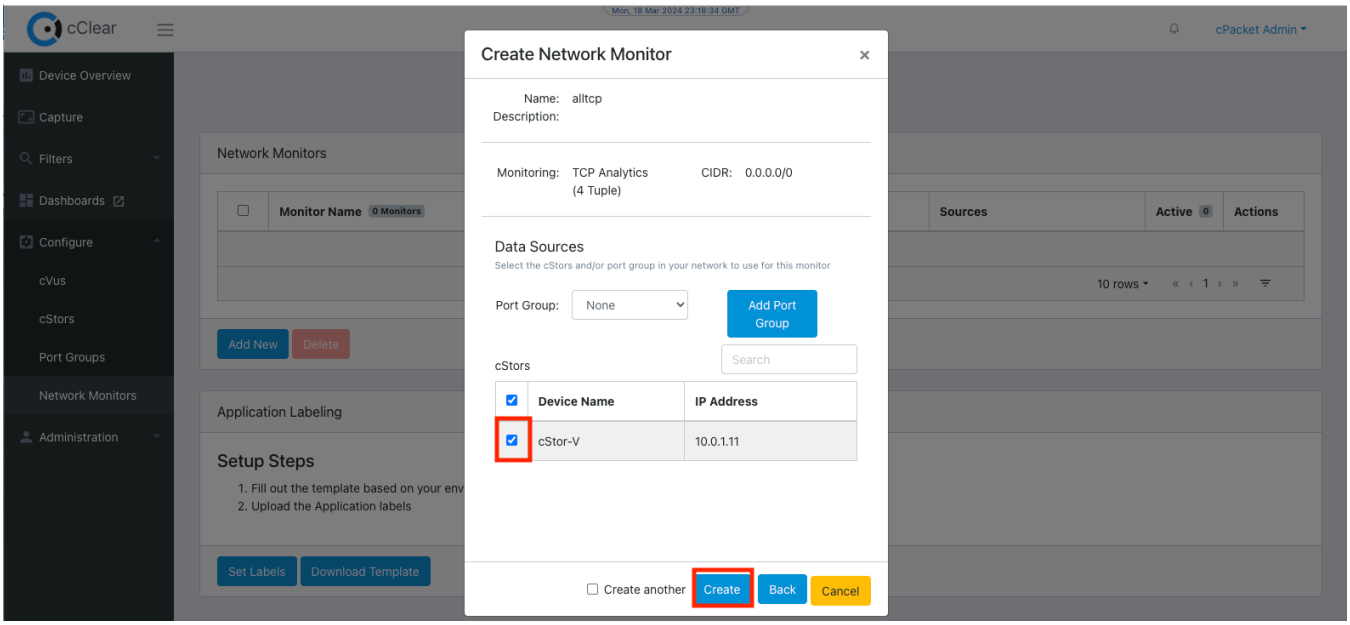
   a. Click Add New

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

b. Type in a name and check “Collect all data”

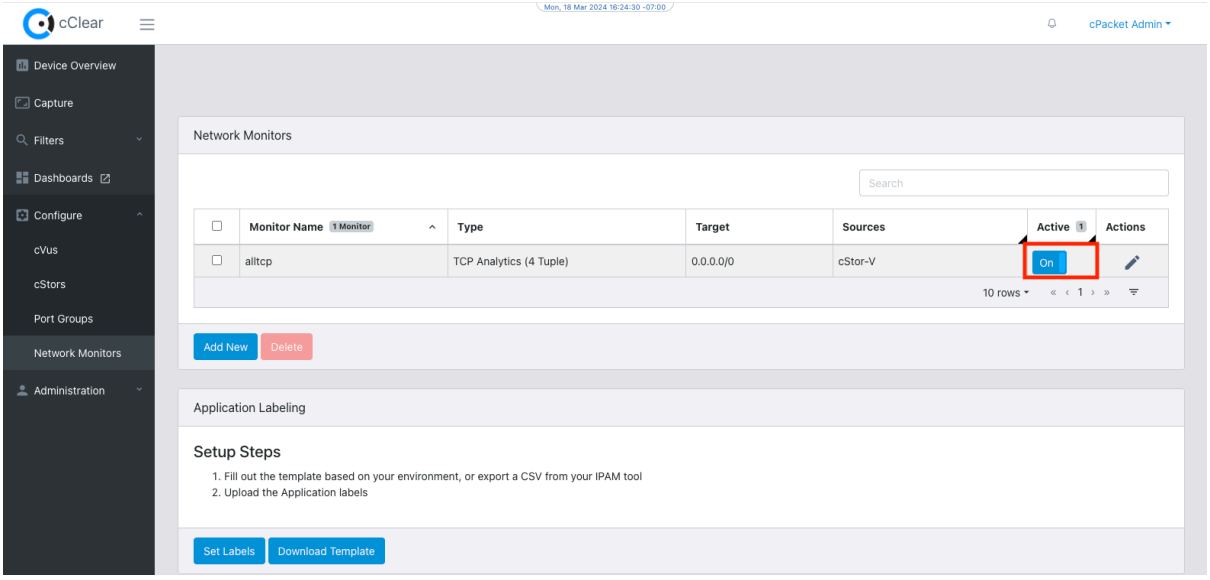


c. Check the cStor device and click “Create”



© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

d. For the new network monitor you just created, make it active by clicking the “On” button



4. Click on the Dashboards in the left menu to take you to the Grafana UI.

On-Prem to Cloud Requirements

The following table maps the requirements for on-prem capture device to cloud capture device, it is meant as a reference for customers familiar with the cPacket on premises cStor appliances.

Requirement	On-Prem	AWS
Encrypted data on drive	SED	Elastic Block Store (EBS) Volume Encryption (AES-256)
Secure key management	Secret platform specific key. Key management WIP.	Key Management Service (KMS)
Drives destruction	Secure erase	On instance termination
Protected data in-transit		
Download interface	Authenticated HTTPS API	Authenticated HTTPS API
Masking	Through API and roles	Through API and roles
Truncation	Through API and roles	Through API and roles
Replay		
Encryption standard	AES 128	AES 128
Cookies management		

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

Authentication & authorization		
Authentication options	TACACS, LDAP, SSO ()	TACACS, LDAP, SSO AWS System Session Manager (SSM)
Authentication servers' management	API	API Identity and Access Management
Password update	API	API Identity and Access Management
Roles and access	Download, restricted packet download, admin and management	Download, restricted packet download, admin and management
Cloud IAM Policies		**cVu-v**: AmazonEC2ReadOnlyAccess AmazonS3ReadOnlyAccess AmazonSSMFullAccess ElasticLoadBalancingReadOnly **cClear-V**: AmazonEC2ReadOnlyAccess AmazonS3ReadOnlyAccess AmazonSSMFullAccess **cClear-V:** AmazonEC2ReadOnlyAccess AmazonS3ReadOnlyAccess AmazonSSMFullAccess
Debug logs		
Log retention	Controlled on the device	Controlled on the virtual device
Audit logs		
Access	Yes	Yes
Accounting	Yes	Yes
Operations	Yes	Yes
Device access control		
Jump box access	Local ACL	EC2 Security Groups
Device management		
Capture failure alerts	SNMP	
Drive failure	SNMP	EBS Status Checks
Other HW failures	SNMP	EC2 System Status Checks EC2 Instance Status Checks

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

SYSLOG	Yes	Yes
Time sync	NTP, PTP	AWS Time Sync (NTP)
SW Update	Through APIs and UI	Through API's and scripts
Configuration backup and restore	Through APIs and UI	Through APIs and UI and scripts.
Personal information	All encrypted	All encrypted
Ports		
Access ports	SSH – controlled by admin HTTPS (80 forward to 443)	SSH-TCP-22 HTTPS-TCP-443
Vulnerabilities management	Qualys outside scans	Qualys outside scans
Host access		SSH AWS System Session Manager (SSM - Optional)

IAM Policy to install cClear-V

The following policy is used to install and operate the cClear-V appliance. It is a very restricted policy and defines the minimum permissions necessary. To install cClear-V from the AWS marketplace, user or role used will need to attach the AWSMarketplaceManageSubscriptions policy.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "cClearMinInstall",
           "Effect": "Allow",
           "Action": [
               "iam:ListInstanceProfiles",
               "ec2:*"
           ],
           "Resource": "*"
       },
       {
           "Sid": "cClearMinSSHKey",
           "Effect": "Allow",
           "Action": [
               "iam:GetSSHPublicKey",
               "iam:ListSSHPublicKeys",
               "iam:UpdateSSHPublicKey",
               "iam:UploadSSHPublicKey"
           ],
```

© cPacket Networks, Inc. | Confidential | Unauthorized reproduction or distribution, in whole or in part, is prohibited without explicit written consent.

```
            "Resource": [
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid": "cClearMinCloudWatch",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "cloudwatch:DescribeAlarms"
            ],
            "Resource": "*"
        }
    ]
}
```

Troubleshooting

- If no traffic is seen in cClear-V, verify that the green check is shown for the connected cStor in the cStor table in cClear-V.

- If no analytics are seen in the cClear-V dashboards, verify that analytics are enabled in your cStor.