

cPacket Cloud Suite

# **Quick Start Guide for AWS cClear-V Control Center**

*Version 24.2.1*

## Revision History

| Document Version | Date      | Notes   |
|------------------|-----------|---|
| 1                | 13Aug2024 | <ul style="list-style-type: none"><li>• The original release of this document.</li></ul>                  |
| 2                | 03Dec2024 | <ul style="list-style-type: none"><li>• Document title/naming modifications.</li></ul>                    |
| 3                | 10Jan2025 | <ul style="list-style-type: none"><li>• Minor document reference edits.</li></ul>                         |
| 4                | 15Apr2025 | <ul style="list-style-type: none"><li>• Added license server information</li><li>• Title update</li></ul> |

# Table of Contents

*Introduction..... 3*

*Getting started.....3*

*Before you begin.....4*

*Installation using AWS Marketplace cClear-V AMI.....5*

*Installation using the cPacket cClear-V Shared AMI..... 7*

*After Installation and Launching..... 8*

    Log In and License..... 8

    Verifying Operation..... 9

*On-Prem to Cloud Requirements.....12*

*IAM Policy to install cClear-V..... 14*

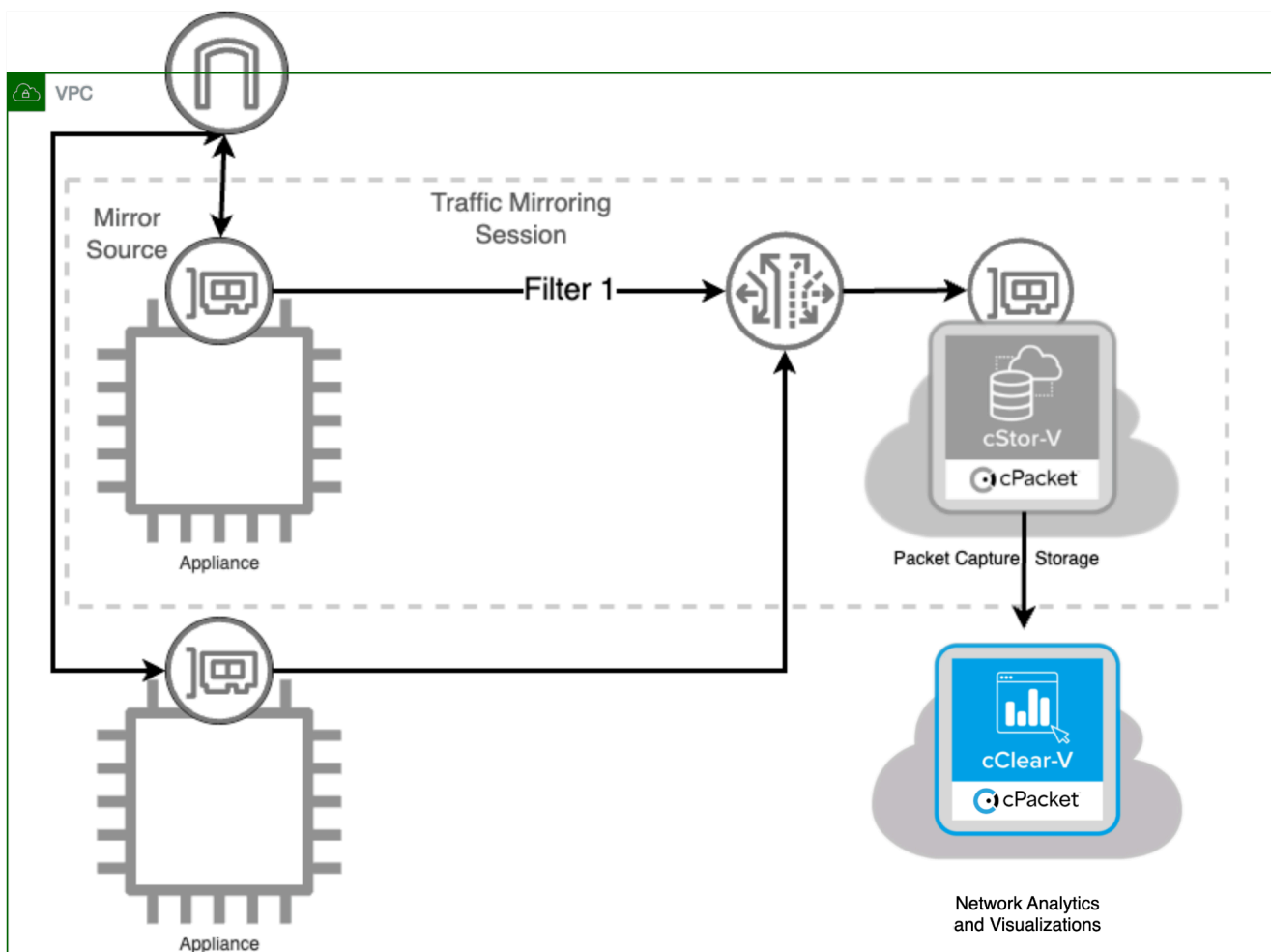
*Troubleshooting..... 15*

## 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. See the **Quick Start Guide for AWS cVu-V Packet Broker** to setup cVu-V packet mirroring and the **Quick Start Guide for AWS cStor-V Packet Capture** to setup cStor-V packet capture.



## 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   |
|---|--|
| <b>AWS User ID</b>  | You will need a user ID in an AWS account, permissions for the user are listed below.  |
| <b>AWS Account and Region</b>                                     | 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, ...   |
| <b>cPacket License Key</b>  | cPacket will provide you with a license key used to activate the cClear-V appliance.   |
| <b>AWS Organization Tagging Policies</b>                          | 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.  |
| <b>Identity and Access Management (IAM) User/Permissions/Role</b> | <p>In the account used for installation, the user needs to have permissions granted to setup the cClear-V virtual appliance. See <a href="#">IAM Policy to install cClear-V</a> for the minimum permissions.</p> <p>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:</p> <ul style="list-style-type: none"><li>- AmazonEC2FullAccess</li><li>- AmazonEC2RoleforSSM</li><li>- IAMFullAccess</li></ul> |

|                                    |  |
|------------------------------------|--|
|                                    | <ul style="list-style-type: none"> <li>- AWSMarketplaceManageSubscriptions (for marketplace access)</li> </ul>   |
| <b>Network Bandwidth</b>           | <p>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.</p>  |
| <b>Virtual Private Cloud (VPC)</b> | <p>You will need a <b>VPC</b> 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.</p>        |
| <b>Security Groups/Policies</b>    | <p>The following ports will be opened on the cClear-V for inbound and outbound traffic.</p> <p>Inbound:</p> <ul style="list-style-type: none"> <li>- TCP 22 – SSH traffic</li> <li>- TCP 443 – Encrypted HTTP traffic</li> <li>-</li> </ul> <p>Outbound ports:</p> <ul style="list-style-type: none"> <li>- All TCP/UDP ports</li> </ul> |
| <b>SSH Key Pair</b>                | <p>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.</p>  |
| <b>AWS Cloud Shell Access</b>      | <p>The account and use you are using must have permission to use the AWS Console.</p>  |

## 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**.

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  |
|---------------------------|--|
| <b>Fulfillment option</b> | Select <b>64-bit (x86) Amazon Machine Image (AMI)</b>  |
| <b>Software version</b>   | Select the software version to deploy, we recommend using the latest release in the Marketplace. |
| <b>Region</b>             | 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   |
|------------------------------|---|
| <b>Name and tags</b>         | Add any tags you'd like. As a best practice, we recommend a <b>Name</b> and <b>owner</b> tag.   |
| <b>Instance type</b>         | Leave <b>m5a.2xlarge</b> as the default.  |
| <b>Key pair (login)</b>      | You can use an existing key pair or create a new one.   |
| <b>Network</b>               | Select the VPC you want to launch your instance into.   |
| <b>Subnet</b>                | Select the subnet you want to use from the dropdown or select <b>Create a new subnet</b> .  |
| <b>Auto-assign public IP</b> | Leave Auto-assign public IP enabled.  |
| <b>Security Group</b>        | 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.  |
| <b>Configure storage</b>     | <p>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.</p> <p><b>Note:</b> 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.</p> |

**[Optional]  
Advanced  
details**

- Optional - If you want to use automatic cVu-V and cStor-V registration, populate the "User data" text field with the text below, substituting the following 4 fields with the relevant values for your deployment:
  - `${cclear_license}` - the cPacket provided license
  - `${name}` - the Auto Scaling group name
  - `${region}` - the region of the deployment

```
#cloud-config

write_files:
- path: /etc/cclear/cirrus/cclear.lic
  permissions: '0644'
  content: |
    ${cclear_license}
- path: /etc/cclear/cirrus/db.json
  permissions: '0644'
  content: |
    {
      "autoscaling_clusters": {
        "bcc3052a4d8bd95a04603e5a2": {
          "cloud_service_provider": "aws",
          "cpacket_device_type": "cvu",
          "autoscaling_cluster": {
            "region": "${region}",
            "name": "${asg_name}"
          }
        }
      }
    }

runcmd:
- systemctl enable --now auto-licensing.service
%{ if managed_registration }
- systemctl enable --now
managed-device-registration.service
%{ endif }
```

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   | <b>Recommended for proof of concepts</b> |
| m5n.4xlarge   | For multiple cStor-V deployments         |

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.
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

#### Firewall Configuration for Online Licensing

To utilize an online license with cClear-v, your network must allow outbound internet access to our license servers. Please ensure that your firewall is configured to permit connections to the following IP addresses:

- **34.250.134.210** (effective from June 19th, 2023, 09:00 GMT)
- **34.251.49.36** (effective from June 19th, 2023, 09:00 GMT)

This configuration is necessary for cClear-v to communicate with the license servers and validate your license.

### License Activation

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:

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

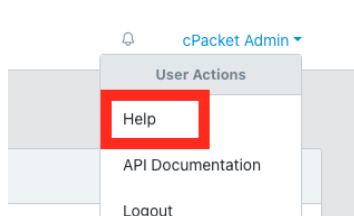
1. The password will be :
  - a. For AWS Marketplace Deployment: [insert-ec2-instance-id]
  - b. For Shared AMI Deployment: cpacketpw
2. After you login on the left pane select **Administration -> Software**.
3. Under **Licenses**, enter the license key provided to you from cPacket.

**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.

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

The screenshot shows the cClear web interface. The left sidebar has a menu with 'cStors' highlighted. The main content area is titled 'cStors' and contains a table with the following data:

| Status | Device Name   | Type    | Traffic Rate  | Storage | cVu, Port | Version | Metrics | Actions |
|--------|---------------|---------|---------------|---------|-----------|---------|---------|---------|
| On     | cstorv-c55603 | cStor-V | 928.02 Mbit/s | 6 min   | Not Set   | 22.3.3  | On      |         |

A red dashed box highlights the 'Traffic Rate' column. Below the table are 'Add cStor' and 'Delete' buttons.

3. In cClear add a network monitor

The screenshot shows the cClear web interface. The left sidebar has a menu with 'Network Monitors' highlighted. The main content area is titled 'Network Monitors' and contains a table with the following data:

| Monitor Name           | Type | Target | Sources | Active | Actions |
|------------------------|------|--------|---------|--------|---------|
| No Monitor to display. |      |        |         |        |         |

Below the table are 'Add New' and 'Delete' buttons. The 'Add New' button is highlighted with a red box.

a. Click **Add New**

b. Enter a name and select **Collect all data**.

The screenshot shows the 'Create Network Monitor' dialog box in the cClear application. The 'Name' field is set to 'alltcp'. The 'Description' field is empty. The 'Monitoring' dropdown is set to 'TCP Analytics (4 Tuple)'. The 'On' dropdown is set to 'CIDR'. The 'CIDR' field is set to '0.0.0.0 / 0'. The 'Collect all data' checkbox is checked. The background shows the cClear interface with a sidebar and a 'Network Monitors' table.

| Monitor Name | 0 Monitors |
|--------------|------------|
|--------------|------------|

Buttons: Add New, Delete

Application Labeling

Setup Steps

1. Fill out the template based on your environment, or export a CSV from your IPAM tool
2. Upload the Application labels

Buttons: Set Labels, Download Template

c. Select the cStor to use for the Network Monitor and click **Create**.

The screenshot shows the 'Create Network Monitor' dialog box in the cClear application. The 'Name' field is set to 'alltcp'. The 'Description' field is empty. The 'Monitoring' dropdown is set to 'TCP Analytics (4 Tuple)'. The 'CIDR' field is set to '0.0.0.0/0'. The 'Data Sources' section shows 'cStor-V' selected. The 'Create' button is highlighted. The background shows the cClear interface with a sidebar and a 'Network Monitors' table.

| Monitor Name | 0 Monitors |
|--------------|------------|
|--------------|------------|

Buttons: Add New, Delete

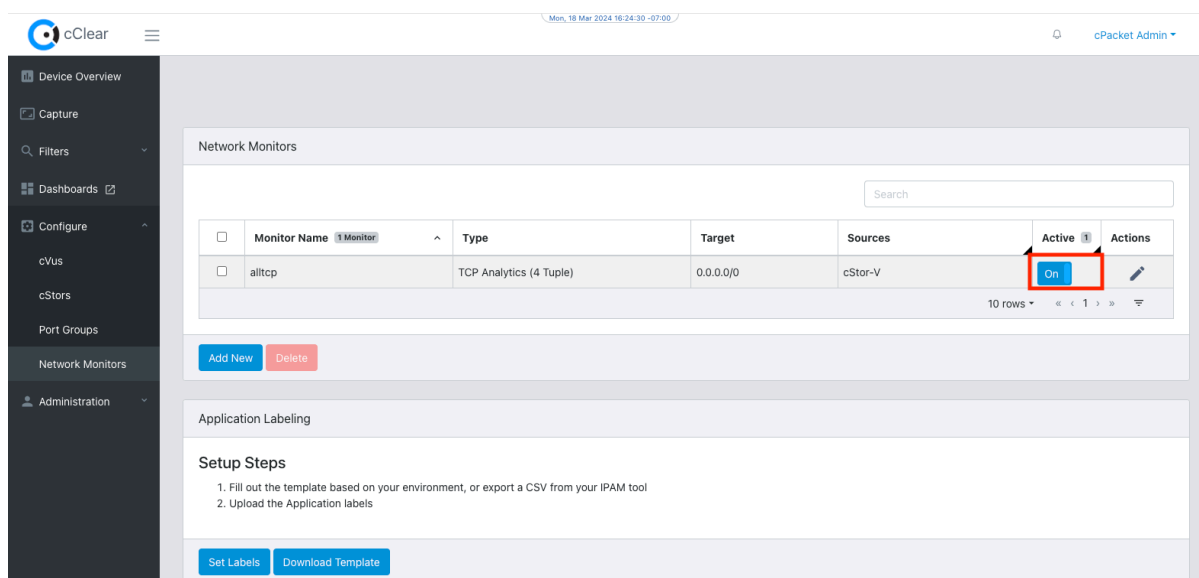
Application Labeling

Setup Steps

1. Fill out the template based on your environment, or export a CSV from your IPAM tool
2. Upload the Application labels

Buttons: Set Labels, Download Template

d. To activate the new Network Monitor you just created, turn on the **Active** toggle.



4. Click **Dashboards** in the left menu to go 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  |
|----------------------------------|--|--|
| <b>Encrypted data on drive</b>   | SED  | Elastic Block Store (EBS)<br>Volume Encryption (AES-256) |
| <b>Secure key management</b>     | Secret platform specific key.<br>Key management WIP. | Key Management Service (KMS)                             |
| <b>Drives destruction</b>        | Secure erase   | On instance termination                                  |
| <b>Protected data in-transit</b> |  |  |
| <b>Download interface</b>        | Authenticated HTTPS API                              | Authenticated HTTPS API                                  |
| <b>Masking</b>                   | Through API and roles                                | Through API and roles                                    |
| <b>Truncation</b>                | Through API and roles                                | Through API and roles                                    |
| <b>Replay</b>                    |  |  |
| <b>Encryption standard</b>       | AES 128  | AES 128  |
| <b>Cookies management</b>        |  |  |
|                                  |  |  |

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

|   |  |  |
|---|--|--|
| <b>Time sync</b>                        | NTP, PTP   | AWS Time Sync (NTP)                                |
| <b>SW Update</b>                        | Through APIs and UI                                    | Through API's and scripts                          |
| <b>Configuration backup and restore</b> | Through APIs and UI                                    | Through APIs and UI and scripts.                   |
| <b>Personal information</b>             | All encrypted  | All encrypted                                      |
| <b>Ports</b>                            |  |  |
| <b>Access ports</b>                     | SSH – controlled by admin<br>HTTPS (80 forward to 443) | SSH-TCP-22<br>HTTPS-TCP-443                        |
| <b>Vulnerabilities management</b>       | Qualys outside scans                                   | Qualys outside scans                               |
| <b>Host access</b>                      |  | SSH<br>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"
      ],
      "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.

The screenshot shows the cStor web interface. The left sidebar contains navigation links: Capture, Capture Settings, Reports, and an ADMINISTRATION section with links for Auth, Software, Security, Utilities, Metrics, and Storage. The main content area is titled 'Home / Capture Settings'. It features three panels: 'Device Information' (IP: 10.0.1.11, Model: cStor-V, Serial: N/A, Version: 23.3.1), 'Device Settings' (with 'Analytics' set to 'On', 'Port Mode' as 'N/A', and 'Retention' as '7' days), and 'Ports' (showing a single port with status 'On'). A red box highlights the 'Analytics' toggle in the 'Device Settings' panel.