cPacket Networks, Inc.

Capture in AWS Quick Start

Deploying the cPacket cStor-V virtual appliance in AWS

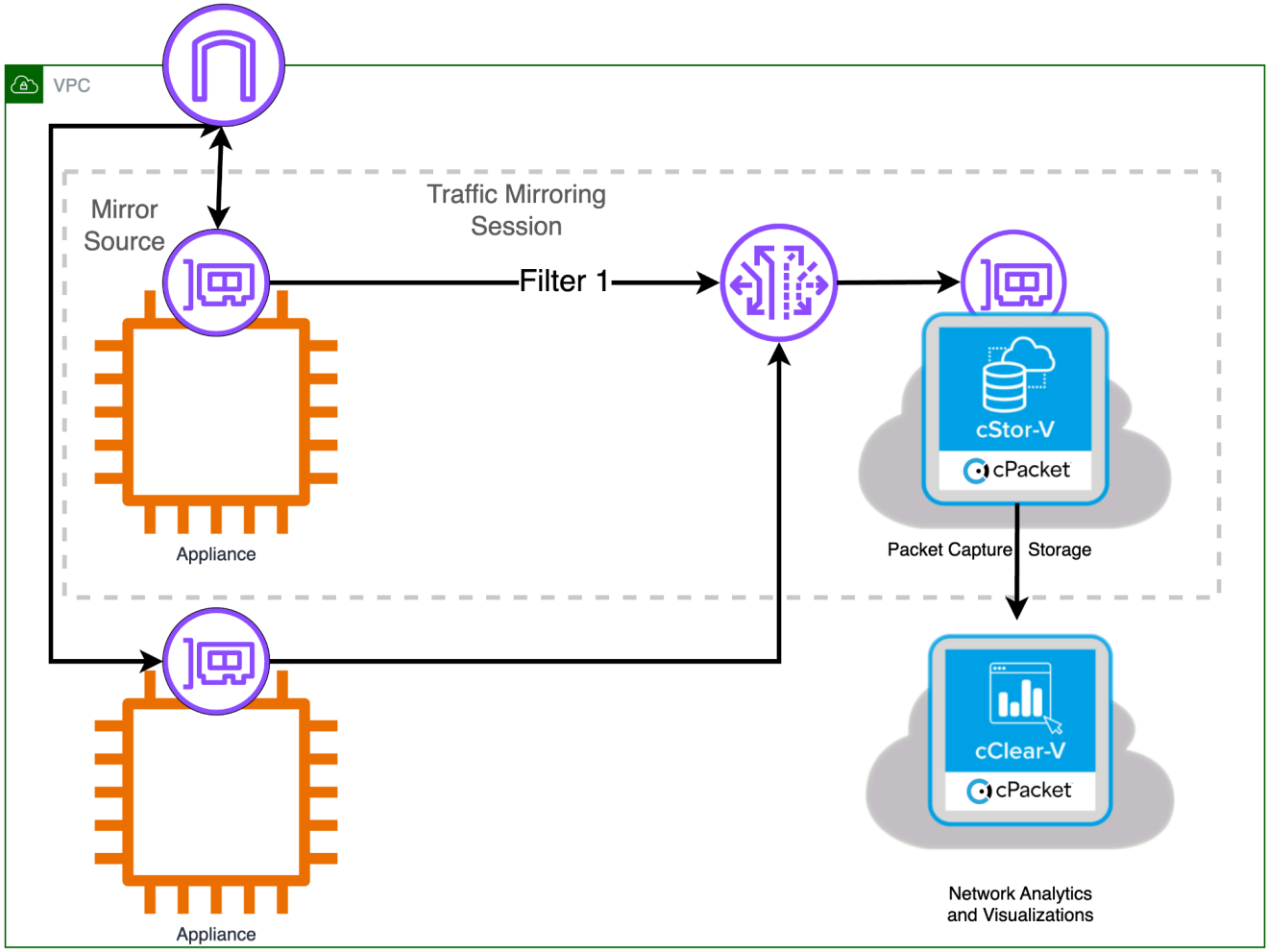
Table of Contents

Introduction

In this guide you will learn how to launch a cPacket cStor-V virtual appliance in your Amazon Web Services (AWS) environment to capture packets using Virtual Private Cloud (VPC) Traffic Mirroring. 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 AWS.

Getting started

A mirror session is a connection between a mirror source and a mirror target. In the following diagram, the mirror sources on the left are EC2 instances and the mirror target on the right is the cPacket cStor-V virtual appliance. The mirror filter determines which network packets are mirrored. This setup guide describes how to deploy cStor-V to be used in conjunction with cClear-V. Please see the cPacket *Analytics in AWS Quick Start* to set up cClear-V.



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 cStor-V. Currently only the cStor-V appliance is available in the AWS Marketplace, which is the easiest way to install the virtual appliance. 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 cStor-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 cStor-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 cStor-V virtual appliance. See IAM Policy to install cStor-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

<table>
<tr><td></td><td>- AWSMarketplaceManageSubscriptions (for marketplace access)</td></tr>
<tr><td>Network Bandwidth</td><td>The network bandwidth to be captured will determine the size of the instance for the cStor-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.</td></tr>
<tr><td>Virtual Private Cloud (VPC)</td><td>You will need a VPC to install the cStor-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 cStor-V will be installed into the same VPC.</td></tr>
<tr><td>Security Groups/Policies</td><td>The following ports will be opened on the cStor-V for inbound and outbound traffic.

Inbound:
<table><tr><td>TCP 22</td><td>SSH traffic</td></tr><tr><td>TCP 443</td><td>Encrypted HTTP traffic</td></tr><tr><td>UDP 4789</td><td>UDP port to receive VxLAN mirrored traffic</td></tr></table>
Outbound ports:
- All TCP/UDP ports</td></tr>
<tr><td>SSH Key Pair</td><td>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.</td></tr>
<tr><td>AWS Cloud Shell Access</td><td>The account and use you are using must have permission to use the AWS Console.</td></tr>
</table>

Installation Steps using AWS Marketplace cStor-V AMI

The following steps describe how to install the cStor-V image from the AWS Marketplace. This is the easiest and simplest way to install a basic cStor-V appliance. 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 cStor-V - Cloud Packet Capture and Network Analytics**.
3. Select **Continue to Subscribe**.
4. Accept the Terms and Conditions for the **cPacket cStor -V** and select **Continue to Configuration**.
5. Select the options on the **Configure this software** page to launch the cStor-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 use a **Name** and **owner** tag.
Instance type	Leave **c5.2xlarge** 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**.
Configure storage	Specify the size of the cStor-V virtual appliance storage volume. The size of your storage volume corresponds to your ability to store packets and capture data on the cStor-V. **Note:** Review Appendix A: AWS Storage Configuration or 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.

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 cStor-V appliance. Users may need to wait up to 10 minutes after deploying before all services are fully operational. You can now continue to test your installation and setup packet mirroring, proceed to After Installation and Launching.

Installation using the cPacket cStor-V Shared AMI

The following steps describe how to install the cStor-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 cStor-V (CSTOR) AMI and then press ENTER.
6. Select the checkbox next to the cPacket cStor-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 tags such as Owner or CreatedBy. Make sure you select the Resource Types to apply the tags to, for cStor-V you can select **Instances**, **Network Interfaces**, and **Volumes**.
8. Select one of the following supported instance types:

Instance Type	Total Volumes	Details
m5n.2xlarge	4	Recommended for proof of concepts with analytics enabled
m5n.8xlarge	8	For 5Gbps capture with analytics enabled
m5n.16xlarge	10	For 10Gbps capture with analytics enabled

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 cStor-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 cStor-V from the Internet
13. You can select an existing security group used by your organization or create one when you launch this cStor-V. The following security rules and protocols are needed for the cStor-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
UDP	4789	Select 0.0.0.0/0 – VXLAN port to receive mirrored traffic **

** Note: In production deployments this CIDR should be limited to subnets that will be mirroring traffic.

14. Configure **storage**.
15. Leave the Size (GiB) field for the root volume at its default value (32 GiB). The cStor-V database will be placed on the smallest volume. Leave the second volume at its default value (8 GiB) for this deployment. Change the third volume to 256 GiB.
16. Click Add new volume. Change the fourth volume to 256 GiB.

Note: The smallest volume is always used for the cStor-V database volume. This volume is used to store configuration and reports (packet captures for viewing) and may be increased to support more or larger reports.

The remaining volumes are used for packet capture. 512 GiB will retain approximately one hour of packet data at 1Gbps. The size of these volumes can be increased or decreased depending on the traffic and storage requirements.

See Appendix A: AWS Storage Configuration for more details.

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

Note: 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.

18. From the **Shutdown** behavior drop-down list, select **Stop**.
19. Select **enable** in the **Termination protection** drop down list.
20. Select **Launch Instance**.

After Installation and Launching

It will take up to 10 minutes for the cStor-V to be accessible using a browser. 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 have a valid license to capture packets and use analytics. 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 AWS Marketplace, the password will be the EC2 Instance ID found on the EC2 Instance page for the cStor-V. (looks like i-*0b351d27f546e3367* where the letters and numbers are unique for your instance). If you have deployed using a cPacket shared AMI, 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 using the steps below:

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, you've confirmed your cStor-V is operational.

Traffic Mirroring

Once you have completed the installation and activated the license, your cStor-V is ready to receive mirrored traffic from EC2 Instances. The AWS guide for Traffic Mirroring can be found here (AWS Traffic Mirroring). This guide will walk you through the necessary steps to receive mirrored traffic from an EC2 instance.

There are three resources to create for Traffic Mirroring

1. Traffic Mirror Target – This is the cStor-V's Elastic Network Interface (ENI)
2. Traffic Mirror Filter – Rules to determine which traffic to mirror from the source(s)
3. Traffic Mirror Session – Session that identifies the mirrored source and target

Create a traffic mirror target

To set up a Traffic Mirror Target you will need the identifier for the Elastic Network Interface (ENI) on the cStor-V.

1. In the AWS Management Console select **EC2**.
2. From the EC2 menu select **Instances** to locate the cStor-V.
3. Select the cStor-V Instance ID to access the Instance Summary.
4. Select the **Networking** tab from the Instance Summary page.
5. The Network Interface tab will list the Network interfaces for the cStor-V, it will look like eni-0c90b129e1f5fc6d7 with unique digits for your ENI.
6. Copy the Interface ID.
7. In the AWS Management Console, in the top menu, select **Services**.
8. Select **VPC**.

9. In the left pane, under Traffic Mirroring, select **Mirror Targets**.
10. Select **Create Traffic Mirror Target**.
11. In the **Name** tag field, type a descriptive name for the target.
12. In the **Description** field, type a description for the target.
13. From the **Target** type drop-down list, select **Network Interface**.
14. From the **Target** drop-down list, select the cStor-V ENI.
15. Select **Create**.

> **Note:** The Traffic Mirror Target ID that is created, it will look like tmt-01421338b23ede911 with unique digits for your ID.

Create a traffic mirror filter

You must create a filter to allow or restrict traffic sent from the mirroring sources to cStor-V. For the purposes of this guide we will mirror all inbound and outbound traffic from EC2 instances.

1. In the AWS Management Console, in the left pane under Traffic Mirroring, select **Mirror Filters**.
2. Select **Create traffic mirror filter**.
3. In the Name tag field, type a name for the filter.
4. In the Description field, type a description for the filter.
5. Under Network services, select the **amazon-dns** checkbox.
6. In the Inbound rules section, select **Add rule**.
7. Configure an inbound rule:
    1. In the Number field, type a number for the rule, such as 100.
    2. From the Rule action drop-down list, select accept.
    3. From the Protocol drop-down list, select All protocols.
    4. In the Source CIDR block field, type 0.0.0.0/0.

5. In the Destination CIDR block field, type 0.0.0.0/0.
6. In the Description field, type a description for the rule.

8. In the Outbound rules section, select **Add rule**.

9. Configure an outbound rule:
    1. In the Number field, type a number for the rule, such as 100.
    2. From the Rule action drop-down list, select accept.
    3. From the Protocol drop-down list, select All protocols.
    4. In the Source CIDR block field, type 0.0.0.0/0.
    5. In the Destination CIDR block field, type 0.0.0.0/0.
    6. In the Description field, type a description for the rule.
10. Select **Create**.

For VPC and subnets that contain application instances that will be mirrored, we recommend the following filtering rules to help avoid mirroring duplicate frames from peer EC2 instances that are in a single VPC to the cStor-V.

- All outbound traffic is mirrored to the cStor-V, whether the traffic is sent from one peer device to another on the subnet or if the traffic is sent to a device outside of the subnet.
- Inbound traffic is only mirrored to the cStor-V when the traffic is from an external device. For example, this rule ensures that an app server request is not mirrored twice: once from the sending app server and once from the database that received the request.
- Rule numbers determine the order in which the filters are applied. Rules with lower numbers, such as 100, are applied first.

Important: These filters should only be applied when mirroring all the instances in a CIDR block including app servers.

Create a traffic mirror session

You must create a session for each AWS resource that you want to monitor.

Note: To prevent mirror packets from being truncated, set the traffic mirror source interface MTU value to 54 bytes less than the traffic mirror target MTU value for IPv4 and 74 bytes less than the traffic mirror target MTU value for IPv6. For more information about configuring the network MTU value, see the following AWS documentation: Network Maximum Transmission Unit (MTU) for Your EC2 Instance.

1. In the AWS Management Console, in the left pane, under Traffic Mirroring, select **Mirror Sessions**.
2. Select **Create traffic mirror session**.
3. In the **Name** tag field type a descriptive name for the session.
4. In the **Description** field type a description for the session.
5. From the **Mirror source** drop-down list, select the source **ENI** to mirror, this is typically attached to the EC2 instance that you want to monitor.
6. From the **Mirror target** drop-down list, select the traffic mirror target ID generated for the target ENI that was created in the previous step.
7. In the **Session number** field, type 1.
8. For the VNI field, leave this field empty and the system assigns a random unique VNI.
9. For the **Packet length** field, leave this field empty, this will mirror the entire packet.
10. From the **Filter** drop-down list select the ID for the traffic mirror filter you created in the previous step.
11. Select **Create.**

The traffic from the ENI you selected should now be mirrored to the cStor-V. You can verify operation by running a packet capture in the cStor-V and verifying the source address in the packet capture includes the IP address of the ENI being mirrored.

IAM Policy to Install cStor-V

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

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "cStorMinInstall",
           "Effect": "Allow",
           "Action": [
               "iam:ListInstanceProfiles",
               "ec2:*"
           ],
           "Resource": "*"
       },
       {
           "Sid": "cStorMinSSHKey",
           "Effect": "Allow",
           "Action": [
               "iam:GetSSHPublicKey",
               "iam:ListSSHPublicKeys",
               "iam:UpdateSSHPublicKey",
               "iam:UploadSSHPublicKey"
           ],
           "Resource": [
               "arn:aws:iam::*:user/${aws:username}"
           ]
       },
       {
           "Sid": "cStorMinCloudWatch",
           "Effect": "Allow",
           "Action": [
               "cloudwatch:GetMetricData",
               "cloudwatch:DescribeAlarms"
           ],
           "Resource": "*"
       }
   ]
}
```


Appendix A: AWS Storage Configuration

Disk Volumes

Our product requires the following disk volumes:

1. **OS Volume (Root volume) :** This volume should be 32 GiB.
2. **Database Volume (Smallest EBS 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:

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

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

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

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

3. **Determine Capture Volume Sizes:** Each capture volume should be equal in size. Sizing should be based on the table in the Installation using the cPacket cStor-V Shared AMI section.

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: $2 / 8 * 3600 = 900\ GiB$
- Database Volume: $2 * 10 = 20\ GiB$ (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.

Appendix B: 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
Protected data at-rest		
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		
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 or	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 **cStor-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
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
Other ports	SNMP, DNS, PTP	DNS, HTTP-TCP-80, VxLAN-UDP-4789, GENEVE-UDP-6081, ICMP-subnet limited (port access controlled through EC2 Security Groups)
Vulnerabilities management	Qualys outside scans	Qualys outside scans
Host access		SSH AWS System Session Manager (SSM - Optional)

