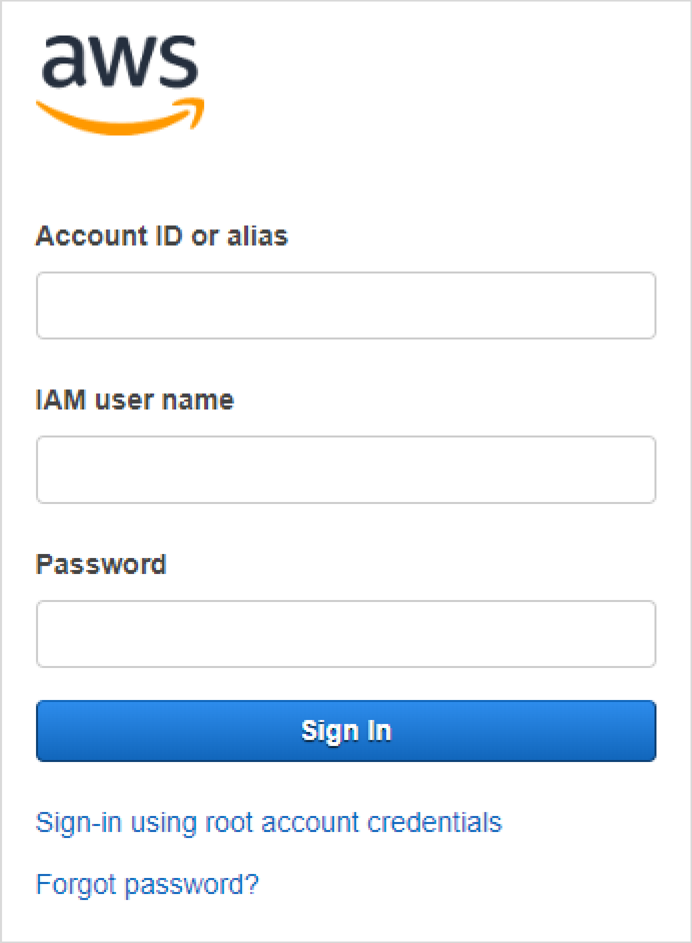
Deploying CyFIR Investigator from AWS Marketplace

Table of Contents

Deploying CyFIR Investigator from AWS Marketplace

Step 1: Sign in

Sign in or create an AWS account on Amazon Web Services Portal.



Account ID or alias

IAM user name

Password

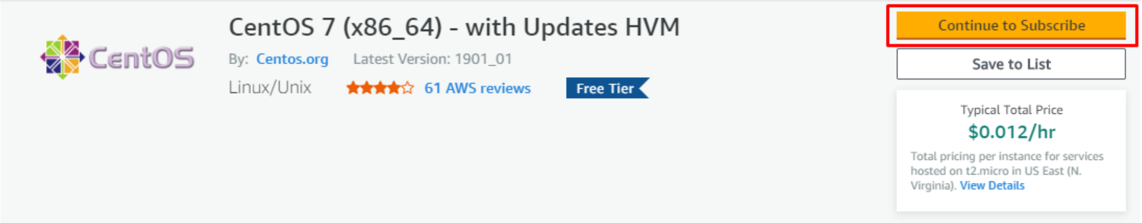
Step 2: Select the AMI

Before you select the AMI, check if you are subscribed to CentOS 7.

As the CyFIR AMI configuration is based on CentOS 7, the free subscription to CentOS 7 is required.

If you have not subscribed to CentOS 7, then follow the link and create the subscription:

1. Click **Continue to Subscribe**.



CentOS 7 (x86_64) - with Updates HVM

By: Centos.org Latest Version: 1901_01

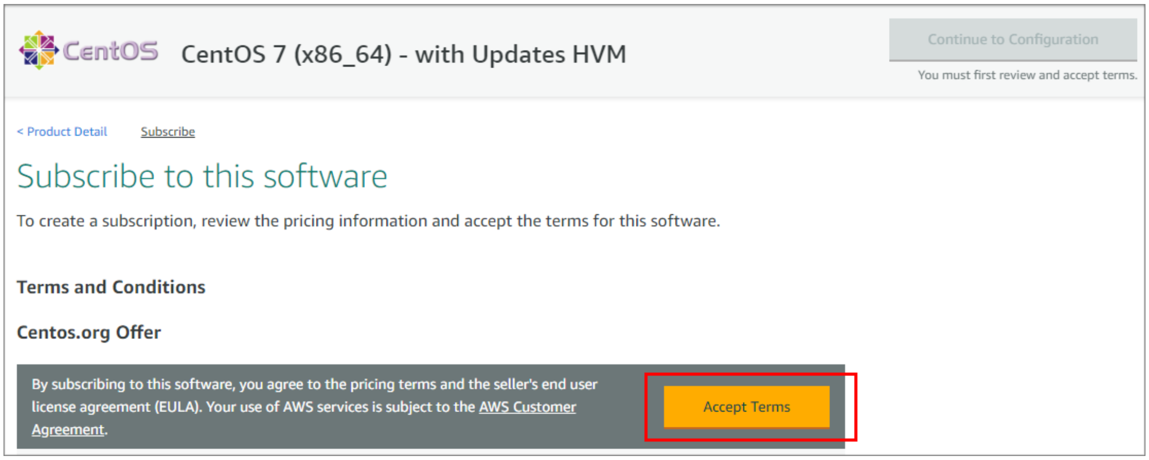
Linux/Unix ★★★★☆ 61 AWS reviews Free Tier

Typical Total Price

$0.012/hr

Total pricing per instance for services hosted on t2.micro in US East (N. Virginia). View Details

2. Read the **AWS Customer Agreement** and click the **Accept Terms** button.



CentOS 7 (x86_64) - with Updates HVM

You must first review and accept terms.

Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

Terms and Conditions

Centos.org Offer

By subscribing to this software, you agree to the pricing terms and the seller's end user license agreement (EULA). Your use of AWS services is subject to the AWS Customer Agreement.

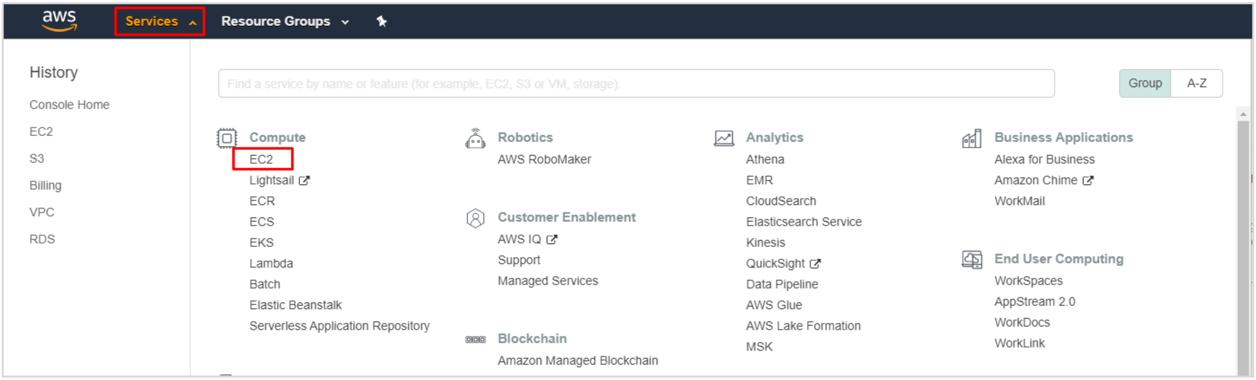
3. The subscription is created.

You can select the CyFIR AMI in one of the following ways:

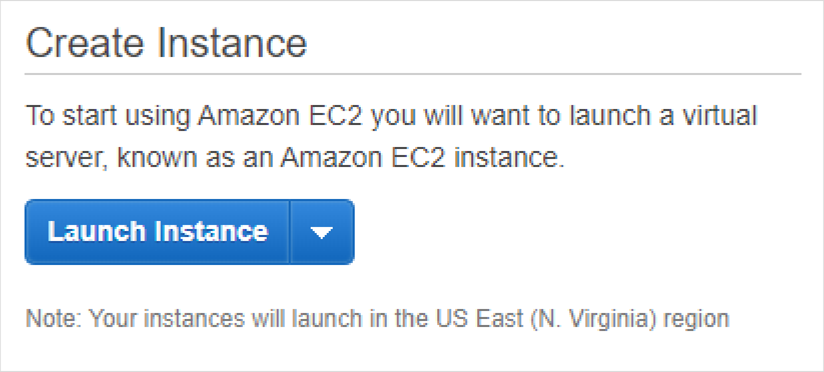
- On the Amazon Web Services Marketplace
- Via the AWS Management Console

When selecting the CyFIR AMI via the AWS Management Console, do the following:

1. On the **Services** page, select **EC2**.



2. In the **Create Instance** group, click **Launch Instance**.



Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

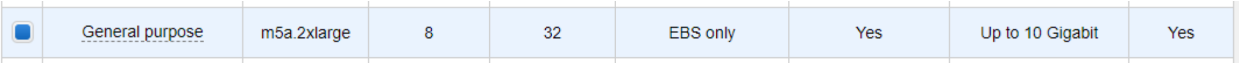
Note: Your instances will launch in the US East (N. Virginia) region

3. The **Choose the Amazon Machine Image (AMI)** page opens.
4. Click the **AWS Marketplace** item in the left pane and select the CyFIR AMI. You can enter the **CyFIR** in the search box and press **Enter** or click the search icon.

5. After the CyFIR AMI is selected, review the information and click **Continue**.

Step 3: Choose instance type

It is recommended to select the **m5a.2xlarge** instance type.



■	General purpose	m5a.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes

Also, you can select any other instance type to fit your use case. Make sure the selected instance meets the following requirements:

- Two 4-Core Xeon 2.1 GHz processors
- 32 GiB RAM
- Network 10 Gbit/s

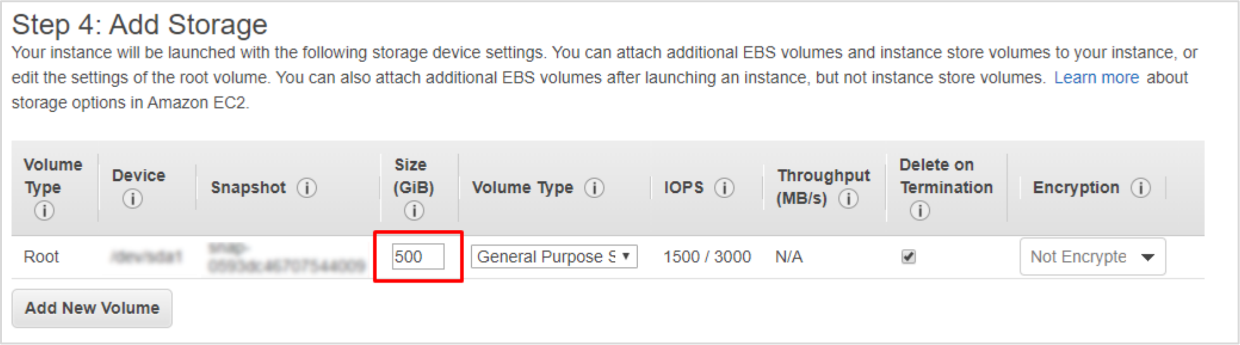
After the instance is selected, click **Next: Configure instance details**.

Step 4: Configure instance

After reviewing the instance details, click **Next: Add Storage**.

Step 5: Add storage

Define the storage settings. It is recommended to have minimum 500 GiB of free hard disk space.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	[redacted]	[redacted]	500	General Purpose S ▾	1500 / 3000	N/A	☑	Not Encrypte ▾

After the storage settings are defined, click **Next: Add Tags**.

Step 6: Add tags

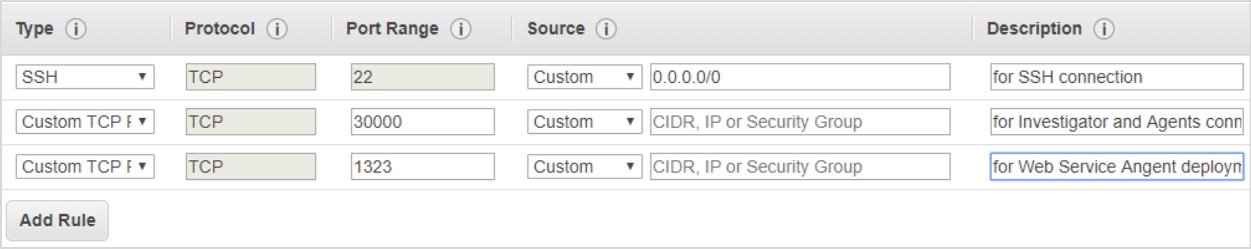
Optionally, define tag settings. Click **Next: Configure Security Group**.

Step 7: Configure security group

Select the security group you would like to use for this instance. The default settings contain all the ports you would need in order to configure and access your instance. If you are using a custom security group, please ensure that all the ports are listed properly so access can be granted appropriately.

The following ports must be specified:

- 22 – The port is used for SSH connection;
- 30000 – The port is used for CyFIR Investigator and Agents connection;
- 1323 – The port is used for Web Service Agents deployment.



Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ		Description ⓘ
SSH ▾	TCP	22	Custom ▾	0.0.0.0/0	for SSH connection
Custom TCP F ▾	TCP	30000	Custom ▾	CIDR, IP or Security Group	for Investigator and Agents conn
Custom TCP F ▾	TCP	1323	Custom ▾	CIDR, IP or Security Group	for Web Service Angent deployn

Make sure IP addresses for your security group are specified in the **Source** column.

After the rules are added, click **Review and Launch**.

Step 8: Review instance launch

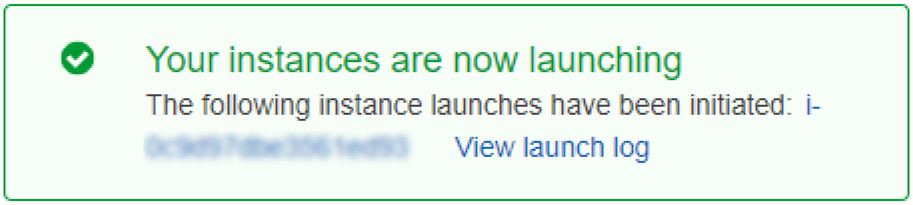
Review your instance details and click **Launch**.

Step 9: Select an existing key pair or create a new key pair

Select an existing key pair or create a new key pair. This key will be used to ensure a secure connection to your instance.

Step 10: Launch your instance

After the Key pair settings are configured, click **Launch Instances**.



Your instances are now launching

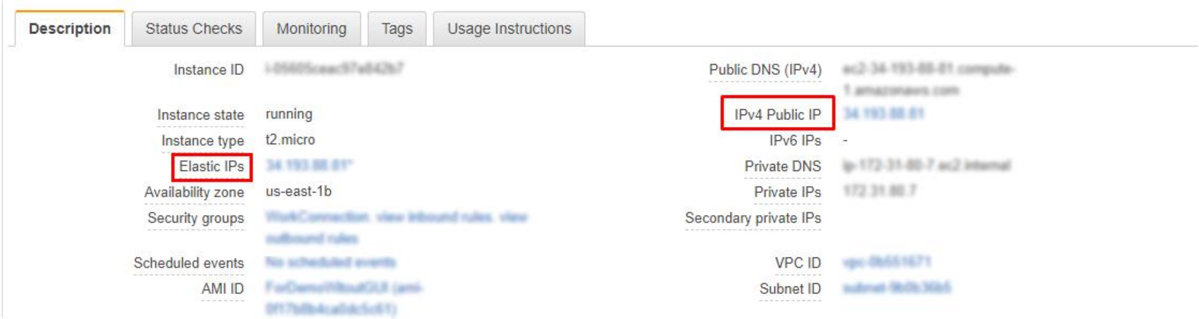
The following instance launches have been initiated: i-[redacted] View launch log

To view your instance, click **View Instances** at the bottom of the page.

Step 11: Connect to CyFIR Deployment

1. Copy the IP address of your instance.
   It is highly recommended to use the Elastic IP address for your instance. For more details on configuring elastic IP, see the Elastic IP Addresses section in the AWS Documentation.

NOTE: Public IP address can be used as well but each time the instance is stopped, its public IP changes, as a result the Agents stop connect to the Proxy and CyFIR must be reconfigured.



Instance ID [redacted]
Instance state running
Instance type t2.micro
Elastic IPs [redacted]
Availability zone us-east-1b
Security groups [redacted]
Scheduled events [redacted]
AMI ID [redacted]

Public DNS (IPv4) [redacted]
IPv4 Public IP [redacted]
IPv6 IPs -
Private DNS [redacted]
Private IPs [redacted]
Secondary private IPs
VPC ID [redacted]
Subnet ID [redacted]

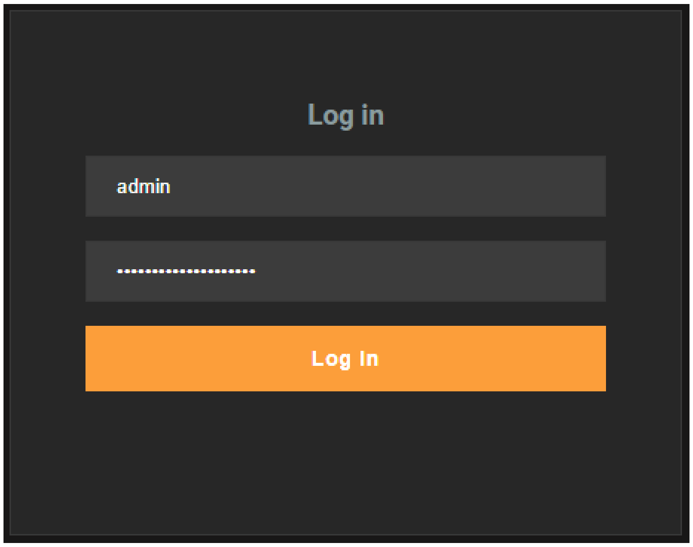
2. Connect to the instance using an SSH client with the username 'centos' and the ssh-key you selected during launch (no password required with ssh-key). See Connection via Putty instruction here.
3. Run the command-line terminal and navigate to the **CyFIR** folder using the **cd /opt/CyFIR/** command.
4. To prepare the system, run the script using one of the following commands:
    - to install Agents in the security mode: **sudo /opt/CyFIR/deploy_script.sh -security=yes**
    - to install Agents in the non-security mode: **sudo /opt/CyFIR/deploy_script.sh -security=no**

In case you use the **sudo /opt/CyFIR/deploy_script.sh** command without the **-security** parameter, Agents will be installed in the non-security mode.

After the successful script execution, the system is ready for use.

Step 12: Log in to CyFIR Deployment

1. Open your web browser and paste the link *https://<your instance IP or hostname>:1323/download* to access CyFIR Deployment. The **Login** page is displayed.



Log in

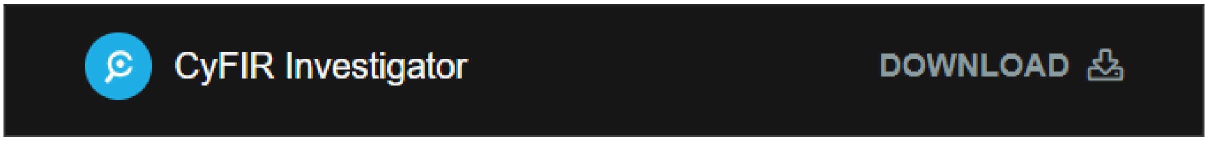
admin

••••••••••••••••••••

2. In the **User** box, enter **admin.**
3. In the **Password** box, enter your instance ID.
4. Click **Log In.**

Step 13: Download CyFIR Investigator

In the opened CyFIR Deployment page, click **Download** to download CyFIR Investigator.



Step 14: Install CyFIR Investigator

1. Start CyFIR Investigator installation wizard (run **CyFIRInvestigator.exe**).
2. The Setup wizard **Welcome** page opens. Click **Next**.
3. Carefully read and accept the License agreement. Click **Next**.
4. Select the folder to which CyFIR Investigator will be installed. Click **Next**.
5. Click **Install** to start the installation.
6. When CyFIR Investigator installation completes, the final page of the CyFIR Investigator installation wizard opens. Click **Finish**.

Step 15: Connect CyFIR Investigator and CyFIR Proxy

1. Start CyFIR Investigator.

2. In the **Login** window, in the **Password** box, enter your instance ID. It is your default account password that can be changed after you log in CyFIR Investigator.

3. In the **Proxy Host** box, enter your instance IP address.

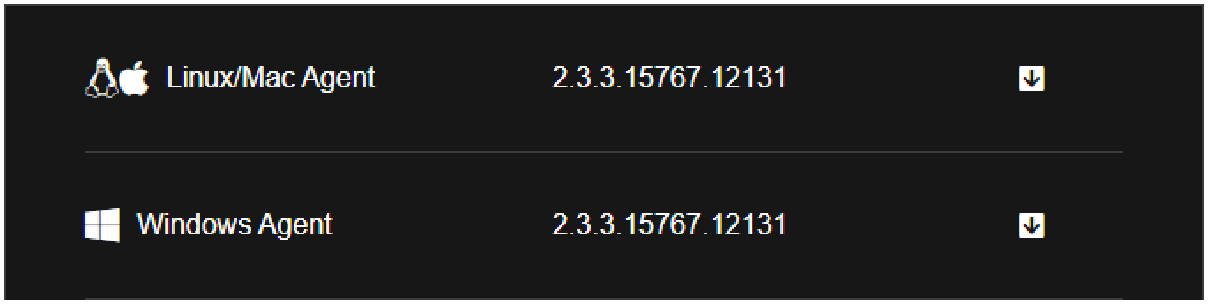
NOTE: It is highly recommended to use the Elastic IP address for your instance. For more details on configuring elastic IP, see the Elastic IP Addresses section in the AWS Documentation.
Public IP address can be used as well but each time the instance is stopped, its public IP changes, as a result the Agents stop connect to the proxy and CyFIR must be reconfigured.

4. Click **OK**.
5. In the opened **Warning** window, consider Proxy certificate as trusted.
6. CyFIR Investigator welcome window opens.
7. Click **Create Case** and define the **Case Name** and **Description** and **Permissions** of users in this case or click **Open Case** and select an existing case.
8. CyFIR Investigator starts.

Step 16: Download CyFIR Agent

Once CyFIR Investigator is installed, you need to download the CyFIR Agent.

Click the Agent from the Agents list depending on your OS.



Linux/Mac Agent	2.3.3.15767.12131	⬇
Windows Agent	2.3.3.15767.12131	⬇

Step 17: Install CyFIR Agent

If you want to install the CyFIR Windows Agent, run the Agent installation package as a user with administrative privileges on the target PC.

If you want to install the CyFIR Linux/Mac Agent, do the following:

1. Copy the installation package to the computer.

2. Run the command-line terminal on the investigated computer.

3. Navigate to the folder with the installation package.

4. Unpack the installation package using the **$ tar zxvf <installation package name>** command.

5. Go to the unpacked folder using the **$ cd <folder name>** command.

6. Run the Agent installation script: **$ sudo ./install_cyfir.sh**

7. If requested, enter the password of the current Linux/Mac user.

8. CyFIR Agent installation begins.

Now, you can begin working in CyFIR Investigator. For more details, see CyFIR Documentation.

Appendix – Additional User Credentials

Proxy and Server Certificates

It is highly recommended to save Proxy and Server certificates on your machine in case there is a need to reconfigure CyFIR. The **.pfx** certificates can be found in the **/opt** directory.

The password for both certificates is your instance ID.

PostgreSQL Database Account

After the system is successfully configured, the PostrgreSQL user account is created with the following credentials:

- **Login**: postgres
- **Password**: <your instance ID>