

NetWitness[®] Platform

Version 12.3.0.0

AWS Installation Marketplace Guide

Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

December, 2023

Contents

- Getting Started with NetWitness Platform for AWS Marketplace 4**
 - About NetWitness Platform for AWS Marketplace 4
 - Prerequisites 4
- Deploy NetWitness Platform from AWS Marketplace 5**
 - Deployment Overview 5
 - Subscribe to AWS NetWitness Marketplace Product 7
 - Deploy EC2 Instance from AWS Marketplace and Configure a Host 11
- Getting Help with NetWitness Platform 19**
 - Contact NetWitness Support 19
 - Feedback on Product Documentation 19

Getting Started with NetWitness Platform for AWS

Marketplace

This document describes how to get started with NetWitness Platform 12.3 using AMI from AWS Marketplace and configure it.

About NetWitness Platform for AWS Marketplace

NetWitness Platform delivers uncompromised threat detection, investigation, and response, across network, logs, and endpoint, whether deployed on-premises, in the cloud, or hybrid. The NetWitness Platform allows security analysts to prioritize, respond, reconstruct, survey, investigate and confirm information about threats in their environment and take the appropriate response, optimizing their security posture and protecting against the impacts of attacks.

Core platform modules include network detection and response (NDR), security information and event management (SIEM) and endpoint detection and response (EDR). Additional modules are available for UEBA, SOAR, and asset analytics to reduce the attack surface. NetWitness features market-leading SASE integrations (both packets and logs), and over 400 integrations with general-purpose and industry-specific security tools, with the ability to instantly parse new sources. NetWitness Platform is utilized continuously in the field by NetWitness Incident Response/Cyber Defense Services, where new detections and methods cycle back into product development.

Prerequisites

Ensure the following before you begin the installation:

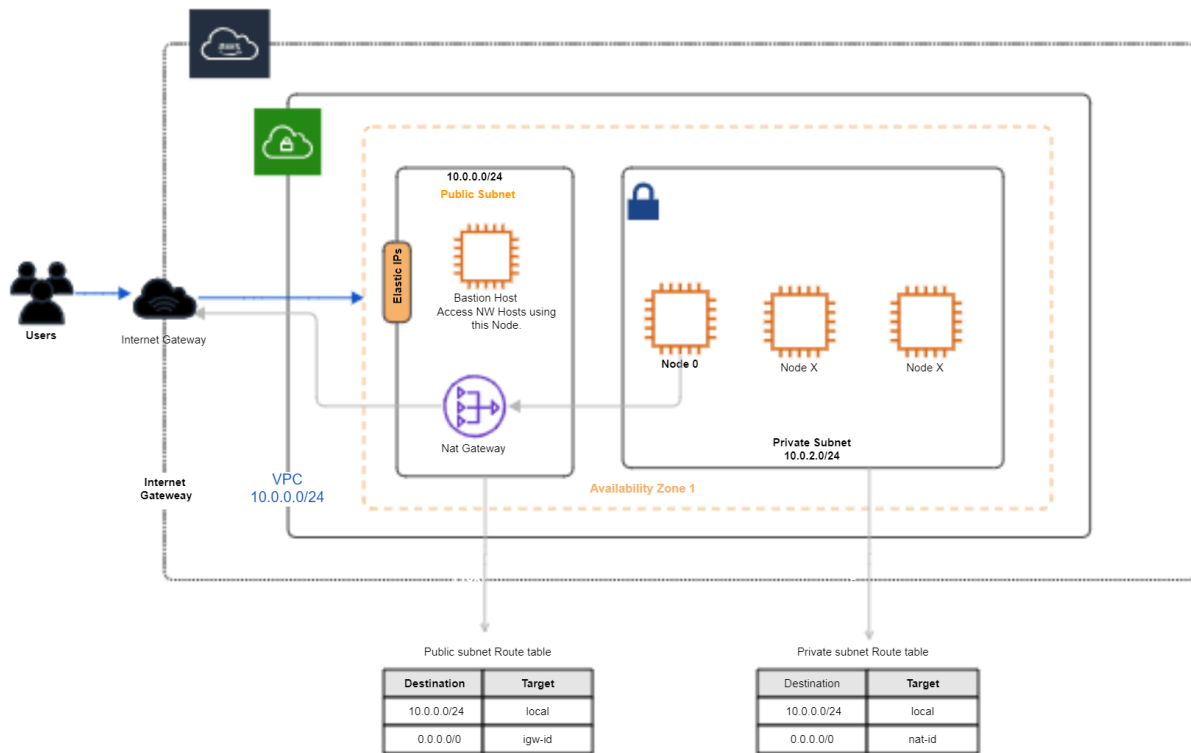
- Access to the AWS console with the appropriate permissions to set up the network and launch an EC2 instance.
- Subscribe to NetWitness 12.3 Product from Marketplace

Deploy NetWitness Platform from AWS Marketplace

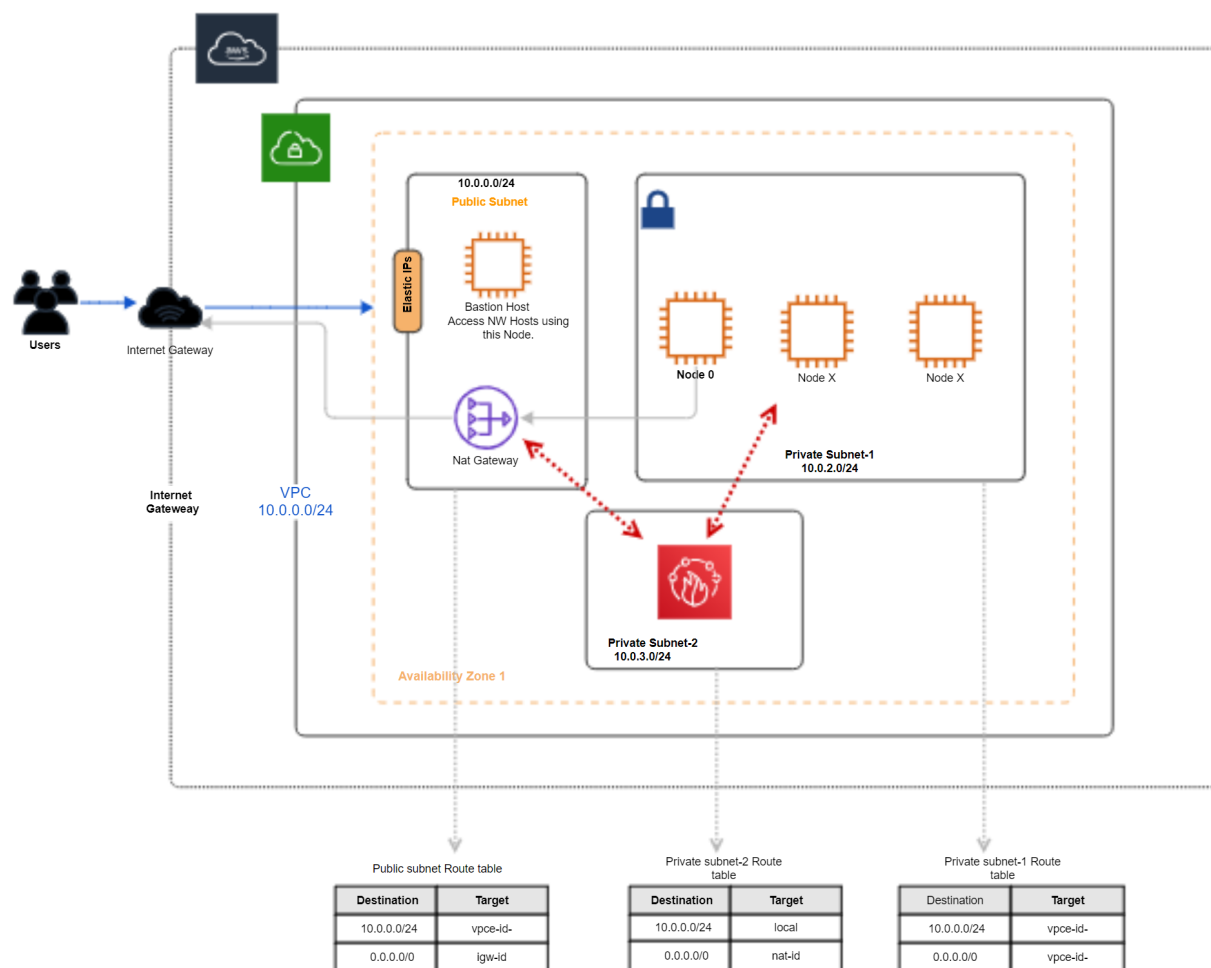
Deployment Overview

The following diagrams show the recommended AWS network architectures for NetWitness deployment.

NetWitness Deployment without Internet Connectivity (Air-Gapped Environment)



NetWitness Deployment with Restricted Internet through Firewall Configuration



1. Set up the NetWitness platform on a dedicated VPC with VPC flow logs enabled to isolate any network issues is recommended. Create a VPC with one Public and Private subnet within the VPC. For more information, see [Create a VPC](#).
2. Specify your own CIDR block for the subnets, which is a subset of the VPC CIDR block.
3. Create two subnets (public and private) and two route tables for NetWitness deployment without Internet connectivity (air-gapped environment).
 - **Set up Public Subnet:** Include the internet gateway in a custom route table. If a subnet is associated with this route table, its traffic will be routed to the internet, making it a public subnet.
 - **Set up a Private Subnet:** Create a custom route table. Keep the default route (same as main table route). The subnet associated to this route table will be the private subnet.

Create two private subnets and three route tables for NetWitness deployment with restricted internet. Additionally, a route table is needed for an additional subnet.
4. Create an internet gateway and attach it to the public subnet to enable communication with the internet.

5. Create a NAT gateway in a public subnet and attach it to the private subnet's route table to allow instances in private subnets to access the Internet.
6. Create two separate security groups is recommended - one for the Bastion instance and another for the private instances as a security best practice.

IMPORTANT:

- If the preferred approach is to set up NetWitness in an air-gapped environment where NW servers have no internet connectivity, a firewall is not required, and all outbound ports can be closed. As a result, the NW Admin server cannot access **CMS.netwitness.com** and must manage content offline. For more information, see the diagram **NetWitness Deployment without Internet Connectivity (Air-Gapped Environment)**.

- To access the NetWitness repo package without a firewall configuration, you must open the outbound ports 80 and 443 in the private security group for the NetWitness instance. This will allow you to access the internet and download the NetWitness repo package. After downloading the package, ensure that you close all outbound ports.

- If customers want to provide internet access to specific domains or URLs in private instances, they can limit outbound traffic by using a firewall. This can be done by whitelisting the URLs in the firewall group and opening ports 80 and 443 in the outbound rules of a private security group. For more information, see the diagram **NetWitness Deployment with Restricted Internet through Firewall Configuration**.

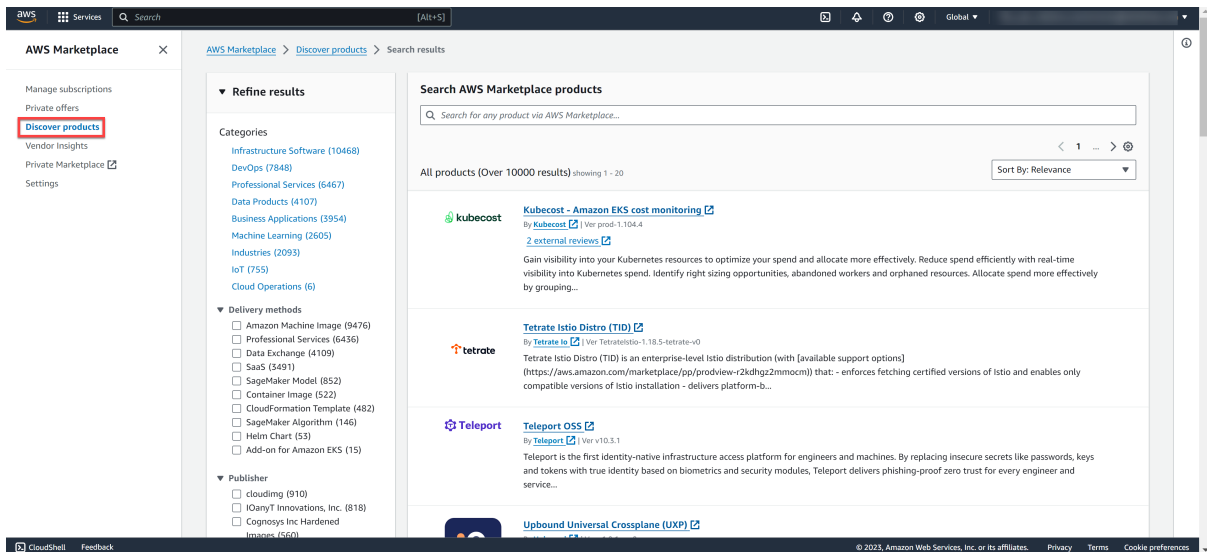
7. Launch the Bastion instance, use the security group created for the Bastion instance in the previous step 6; it's important to allocate an Elastic IP address to ensure communication with the Internet.
8. launch the Bastion instance, generate a key pair and keep it safe. This key pair will be required to SSH into Bastion instance for troubleshooting purposes.
9. Subscribe to NetWitness Product from the AWS Marketplace service. For more information, see [Subscribe to AWS NetWitness Marketplace Product](#).
10. Launch a private NetWitness instance using the NetWitness AMI from AWS Marketplace, within a private subnet and use the security group created in step 6. For more information, see [Deploy EC2 Instance from AWS Marketplace and Configure a Host](#).

Subscribe to AWS NetWitness Marketplace Product

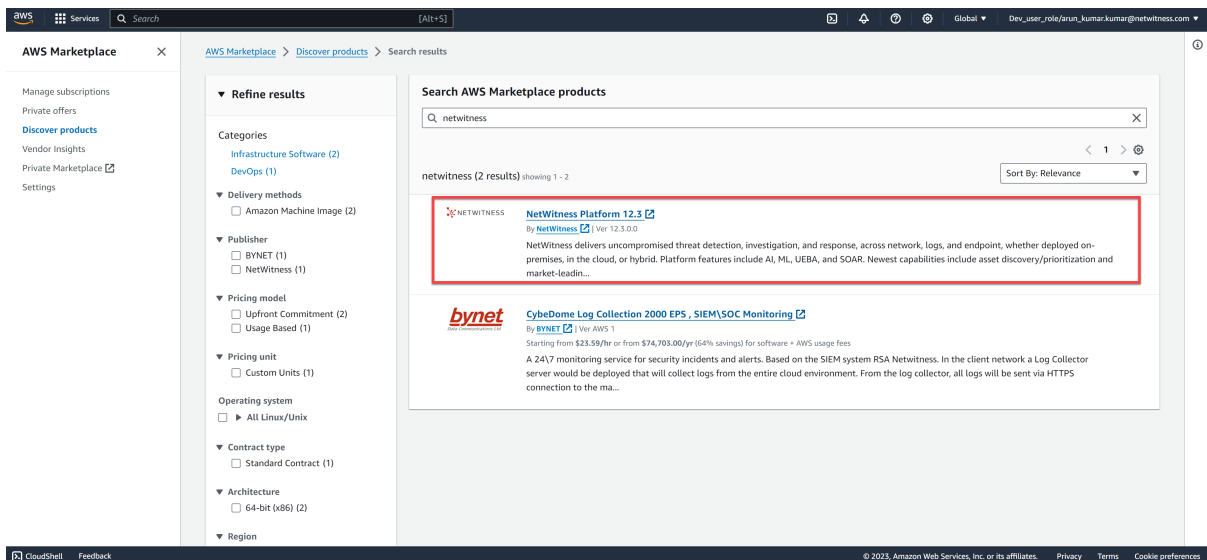
This topic describes the steps required to subscribe to NetWitness through the AWS Marketplace.

To subscribe to NetWitness through the AWS Marketplace

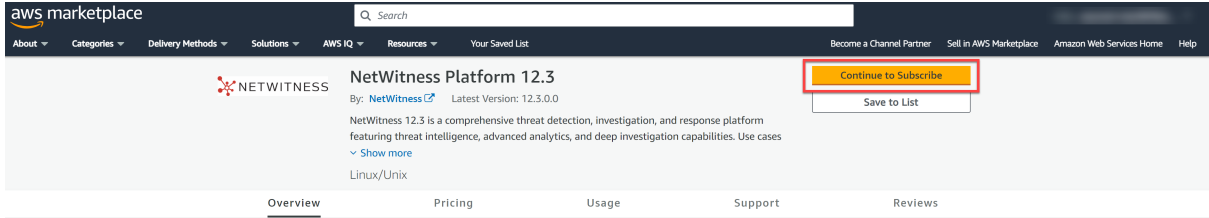
1. Log in to the AWS Management Console.
2. Navigate to **AWS Marketplace Subscriptions** AWS Service and click **Discover Products** in the left panel.



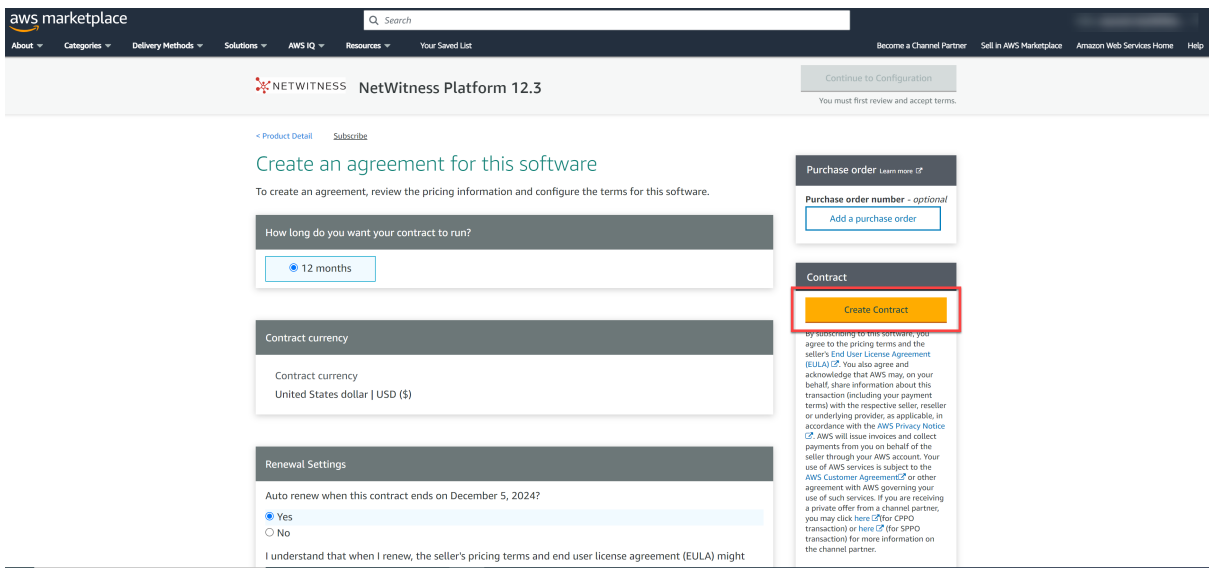
3. Search for NetWitness product and select NetWitness Platform 12.3.



4. Click Continue to Subscribe in the upper right corner of the page.

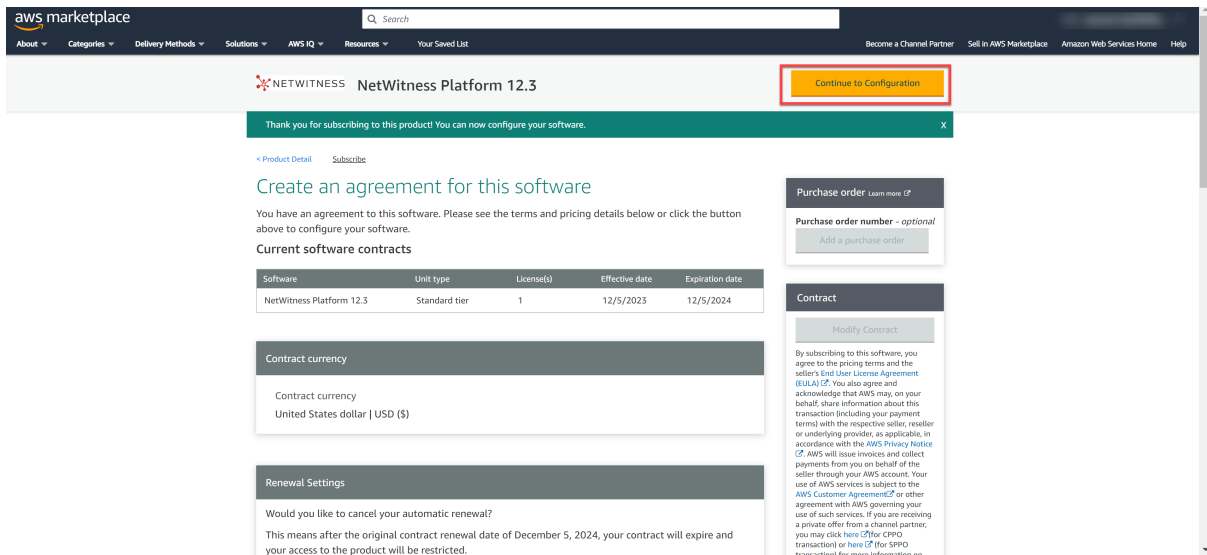


5. Verify the terms and the pricing and click **Create Contract**.

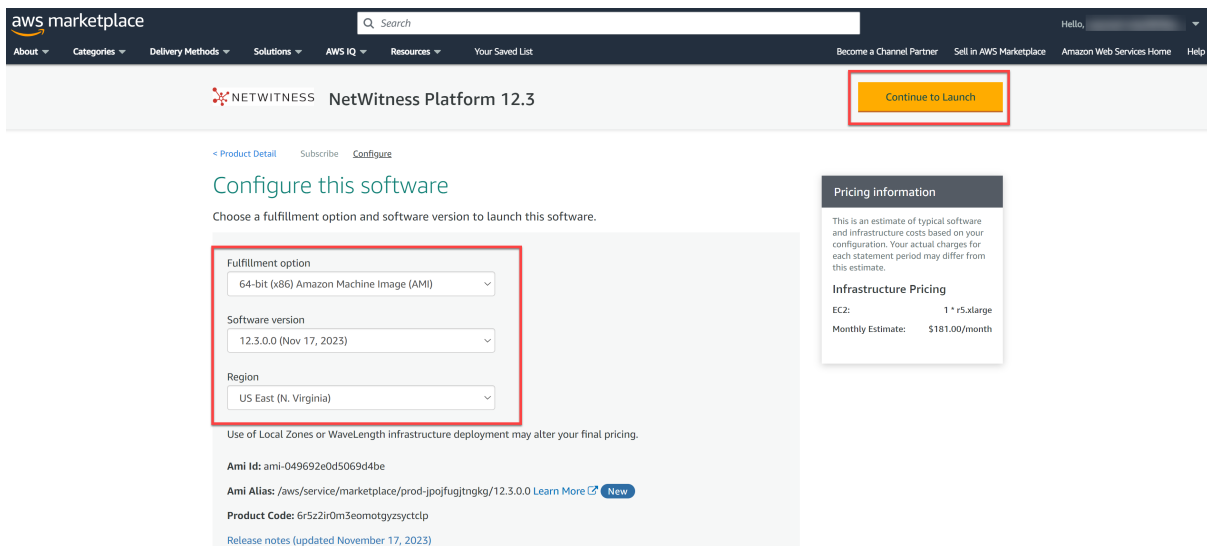


A success message is displayed that you subscribed to the product.

6. Click **Continue to Configuration**.



7. Under **Configure this Software** view, keep the default settings and click **Continue to Launch**.



8. Select **Launch through EC2** from the **Choose Action** drop-down list and click **Launch**.

The screenshot shows the AWS Marketplace interface for launching NetWitness Platform 12.3. The page title is "Launch this software". Below the title, there is a section for "Configuration details" with the following information:

- Fulfillment option:** 64-bit (x86) Amazon Machine Image (AMI) NetWitness Platform 12.3 (running on i5.large)
- Software version:** 12.3.0.0
- Region:** US East (N. Virginia)

Below the configuration details, there is a "Choose Action" dropdown menu with "Launch through EC2" selected. To the right of the dropdown, there is a note: "Choose this action to launch your configuration through the Amazon EC2 console." Below the dropdown and note, there is a yellow "Launch" button.

Next steps, **Launch** button redirects you to the **EC2 > Instances > Launch an instance** setup view to configure and deploy the EC2 instance.

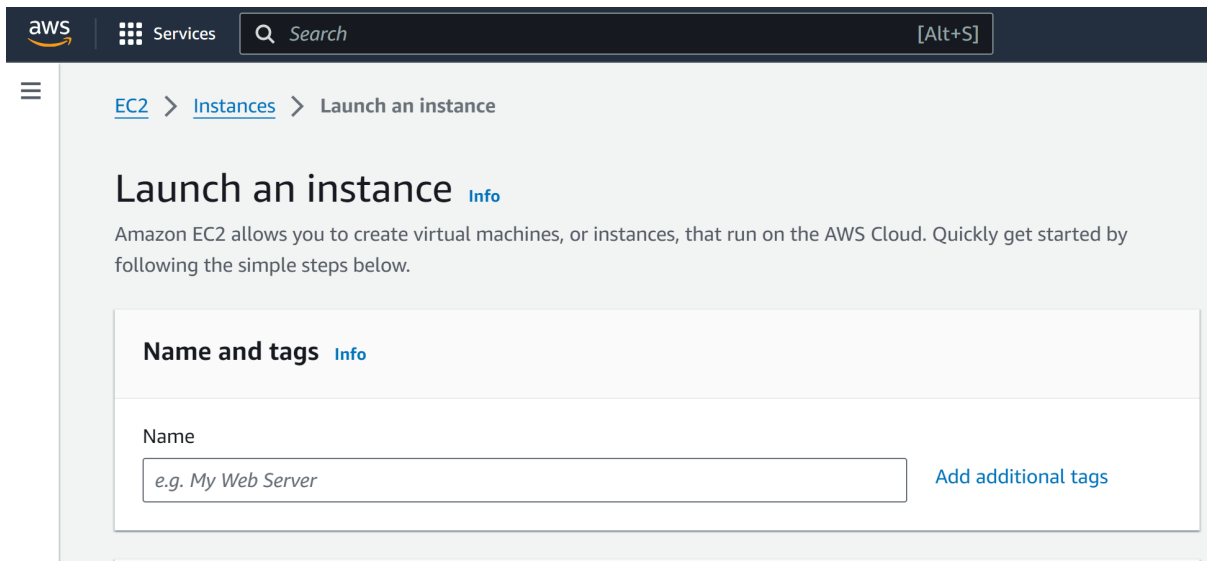
Deploy EC2 Instance from AWS Marketplace and Configure a Host

Configure the NetWitness Platform on an AWS instance by using the provided Amazon Machine Image (AMI).

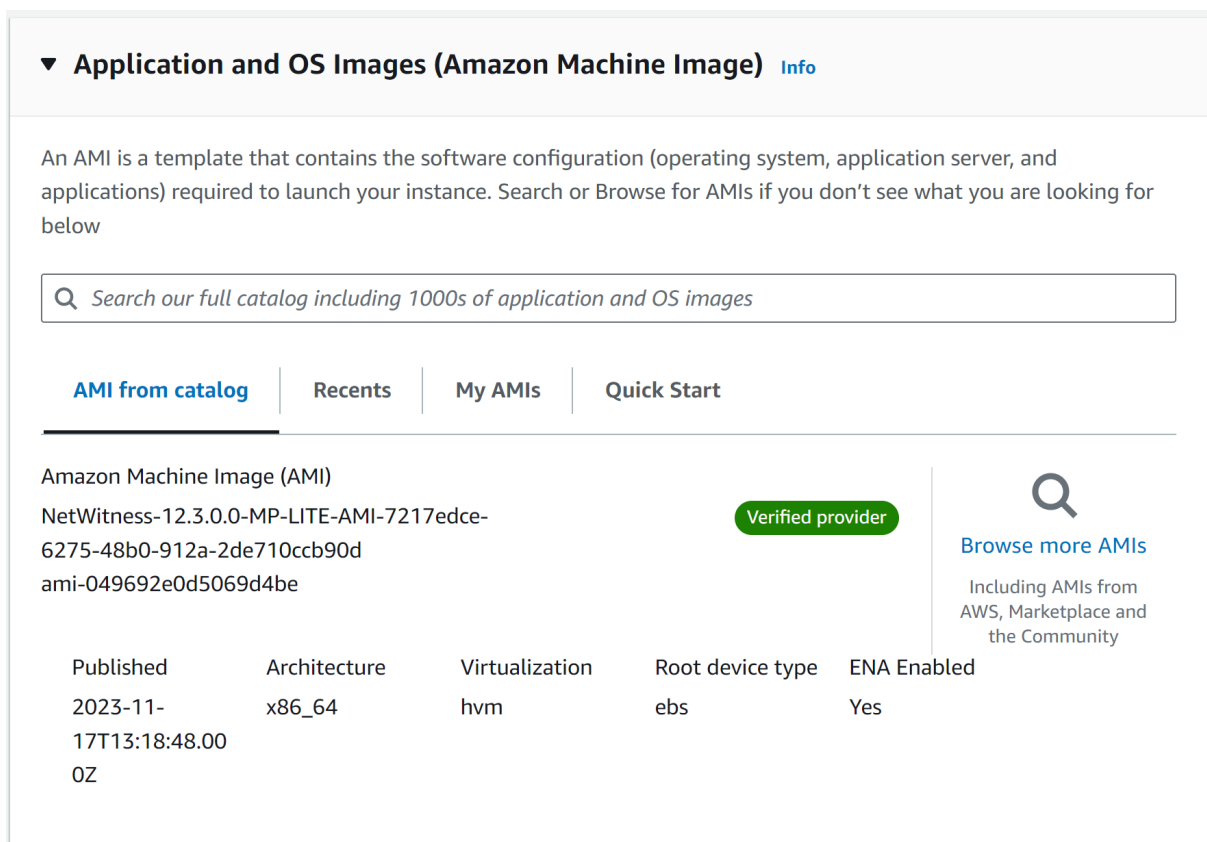
1. Enter the name under the **Name and tags** for your instance

(Optional) To add other tags, click **Add additional tags**. Then, for each tag, click **Add tag** and enter the Key, Value, and Resource Types.

Note: For Resource Types, add **Instances** and **Volume**.



2. Under **Application and OS Images (Amazon Machine Image)**, the AMI is pre-selected by default from the **AMI from catalog** section as you have subscribed.



3. Select an instance size from the **Instance** type drop-down list.

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

m7a.4xlarge

Family: m7a 16 vCPU 64 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.92736 USD per Hour

On-Demand SUSE base pricing: 1.05236 USD per Hour

On-Demand Windows base pricing: 1.66336 USD per Hour

On-Demand RHEL base pricing: 1.05736 USD per Hour

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

NetWitness recommends creating an **m7a.4xlarge** instance type with 16 CPUs and 64 GB of RAM for NW Server (node-0) and suggests choosing the appropriate instance type based on specific requirements. For further guidance on selecting the recommended instance type for each NW Service, please refer to the [Storage Guide for NetWitness® Platform 12.3](#).

4. Under **Key pair (login)**, create or select the key pair for SSH authentication.

Note: If you are creating an instance for the first time, you need to generate a key pair. For subsequent instances, you can reuse the same key pair.

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼

- a. To create a new key pair, select **Create new key pair**.
The Create key pair dialog is displayed.

Create key pair ✕

Key pair name
Key pairs allow you to connect to your instance securely.

AWS|

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Cancel **Create key pair**

- b. In the **Key pair name** text box, type a name for the new key pair and keep other values as default.
- c. Click **Create key pair**.
The .PEM file that contains the private key is downloaded.
- d. Save the private key to a location that is secure and accessible. You cannot download the private key file again.

Note: AWS EC2 instances are accessed with the help of key pairs and do not proceed without selecting a key pair.

5. Under **Network Settings**, select a VPC, Subnet, and Security group.
To select or create, click **Edit** and configure the details:

- a. Select a virtual private cloud (VPC) from the **VPC** drop-down list.
- b. Select a private subnet for your VPC from the **Subnet** drop-down list.
- c. Select **Disable** from the **Auto-assign public IP** drop-down menu.
- d. Under **Firewall (security groups)**, Choose the **Select existing security group** option and under **Common security groups** drop-down list, select an existing private instance security group that allows ports for the NetWitness, to create an allowlist of trusted IP addresses that can access your NetWitness deployment. In the security group you must add the inbound and outbound rules. For more information on the ports used by NetWitness components, see the topic [Network Architecture and Ports](#) topic in the *Deployment Guide for NetWitness Platform 12.3*.

▼ Network settings [Info](#)

VPC - *required* [Info](#)

[↻](#)

Subnet [Info](#)

[↻](#) [Create new subnet](#) [↗](#)

Auto-assign public IP [Info](#)

[▼](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Common security groups [Info](#)

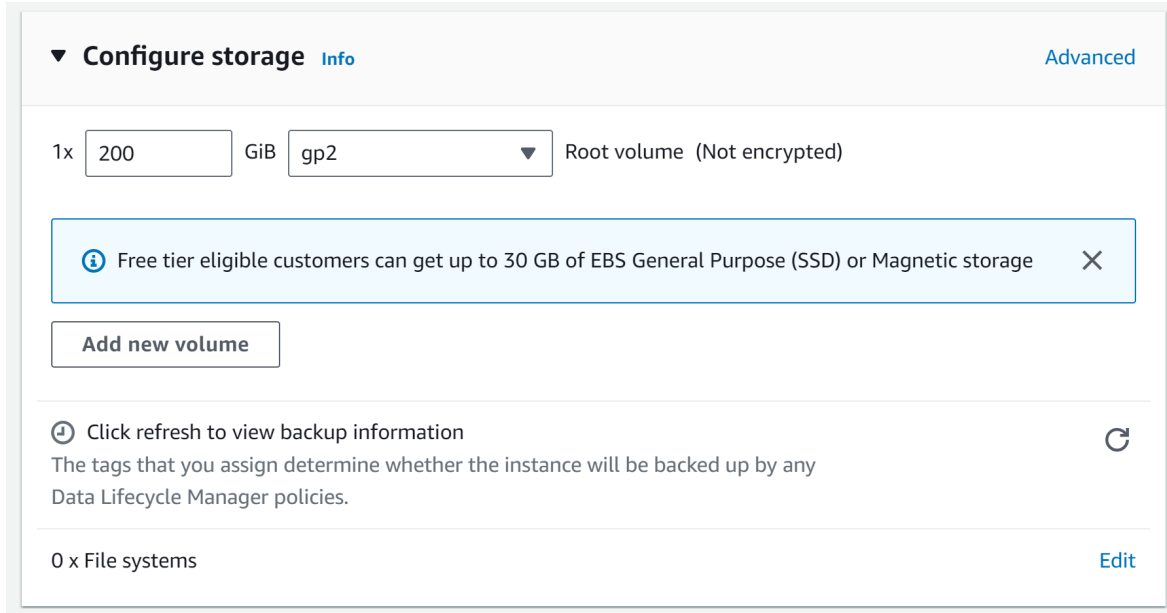
[▼](#)

[✕](#) [↻](#) [Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

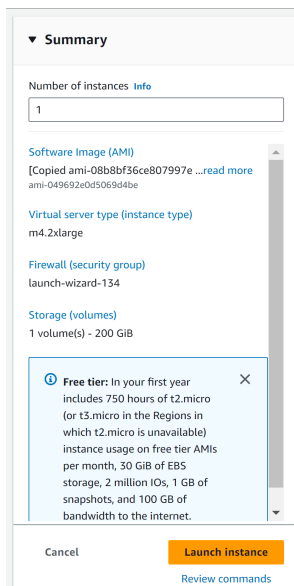
▶ **Advanced network configuration**

6. Under **Configure storage**, specify the size and type of the volume.
 - (Optional) Click **Add new volume** if you need more storage and configure the details. For information about available disk options, see [AWS Volume Types](#).

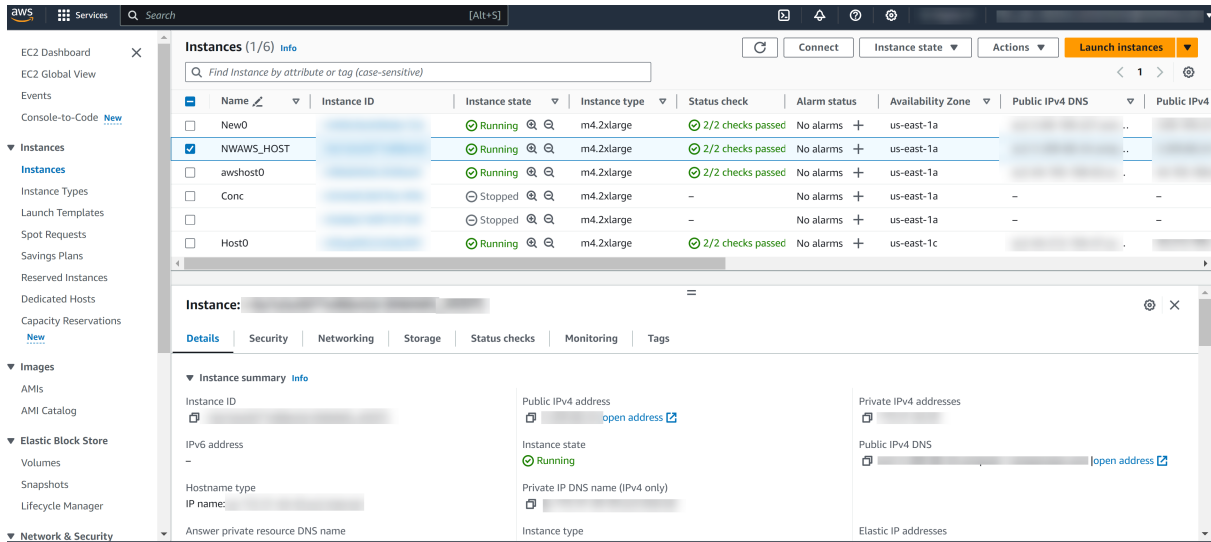


For more information, see the [Storage Guide for NetWitness® Platform 12.3](#) for guidelines on how to configure storage based on based on the requirements of the NetWitness component (that is, service) for which you are launching an instance.

7. Under **Summary**, you can specify the number of instances required and review your instance configuration.
8. Click **Launch Instance**.

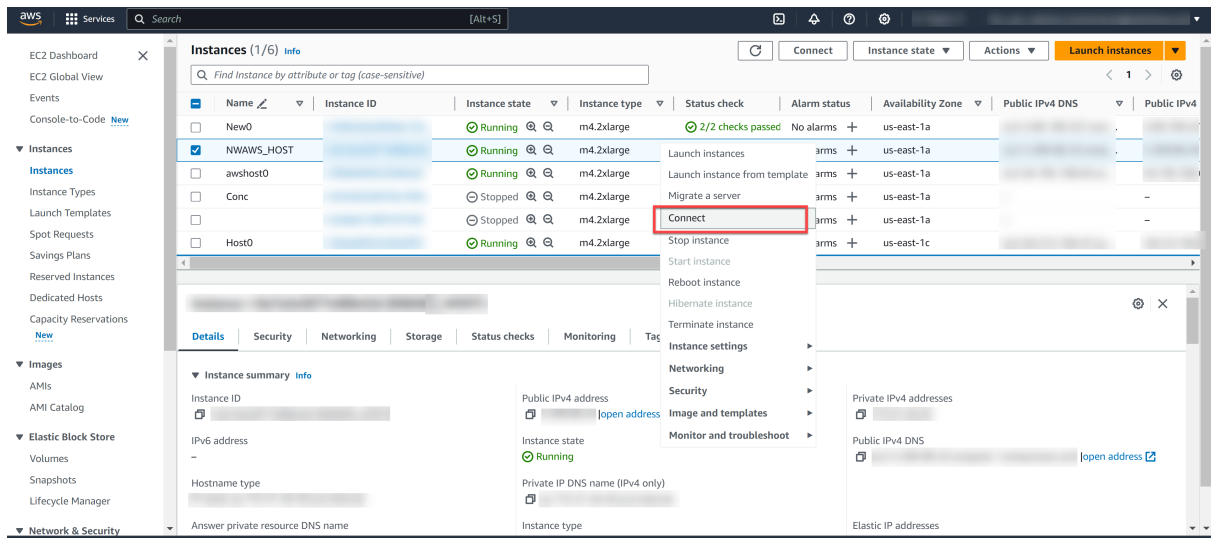


9. Wait a few minutes for the provisioning and initialization to finish.
10. Click **Connect to instance**, which navigates you to the instances tab where you can see all information about our instance.



Note: Wait at the Instances view until the **Instance State** shows **Running** and **Status checks** shows **2/2 checks passed**.

11. Select the instance, right-click, and click **Connect**.



IMPORTANT: You must contact [NetWitness Customer Support](#) to procure NetWitness repositories to continue orchestrating the software. Please provide the **NAT gateway IP address (not the Bastion host IP)** to whitelist, which allows access to the NetWitness repository package.

12. On your computer, open a terminal program, then navigate to the location where the .pem file is stored to open an SSH connection using the aws user account.

13. Enter the following command to connect to the Bastion instance:

```
ssh -i <.pem file> ec2-user@<Public IP>
```

For example: `ssh -i aws.pem ec2-user@150.0.0.0`

14. Enter the following command to connect to your private (NW server) instance from the Bastion instance:

Note: Make sure to copy the downloaded .pem key of the private NetWitness instance to the Bastion instance to connect to the NetWitness private instance.

```
ssh -i <.pem file> ec2-user@<Private IP>
```

For example: `ssh -i aws.pem ec2-user@10.0.0.0`

15. Enter the following command to set the root privileges for the aws user:

```
sudo su
```

16. Enter the following command to copy the NetWitness 12.3.0.0 package to this location:

```
wget -m -nH --no-parent https://repo.netwitness.com/12.3.0.0/
```

Caution: Do not proceed with the installation until the ports on your firewall are configured.

17. Install the NetWitness Platform. For more information, see **Installation Tasks** section under the topic [Launch an Instance and Configure a Host](#).

To configure the other Component hosts, for example, **Packet Decoder Host**, you must repeat the steps 1-11 to launch a new EC2 instance and perform the **Installation Tasks** procedure and then log in to the NetWitness Platform and follow the procedure **Install Component Services on Hosts** under the topic [Launch an Instance and Configure a Host](#).

18. If you use the Enterprise network to access AWS resources such as EC2 instances, you can access the NetWitness Platform UI using the private IP address of the NetWitness instance (node-0). However, suppose you are not connected to an Enterprise network. In that case, you must set up port forwarding within your Bastion instance to access the NetWitness Platform UI from your local system using the public IP of the Bastion instance.

Getting Help with NetWitness Platform

Contact NetWitness Support

If you contact NetWitness Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the NetWitness Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click Support > Case Portal > View My Cases .
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW Update	https://update.netwitness.com/
LiveUI	https://live.netwitness.com

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.