NetWitness® Platform

Version 12.4.0.0

AWS Installation Marketplace Guide

NETWITNESS

Platform

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 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.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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/.

April, 2024

Contents

Getting Started with NetWitness Platform for AWS Marketplace

This document describes how to get started with Netwitness Platform 12.4 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:

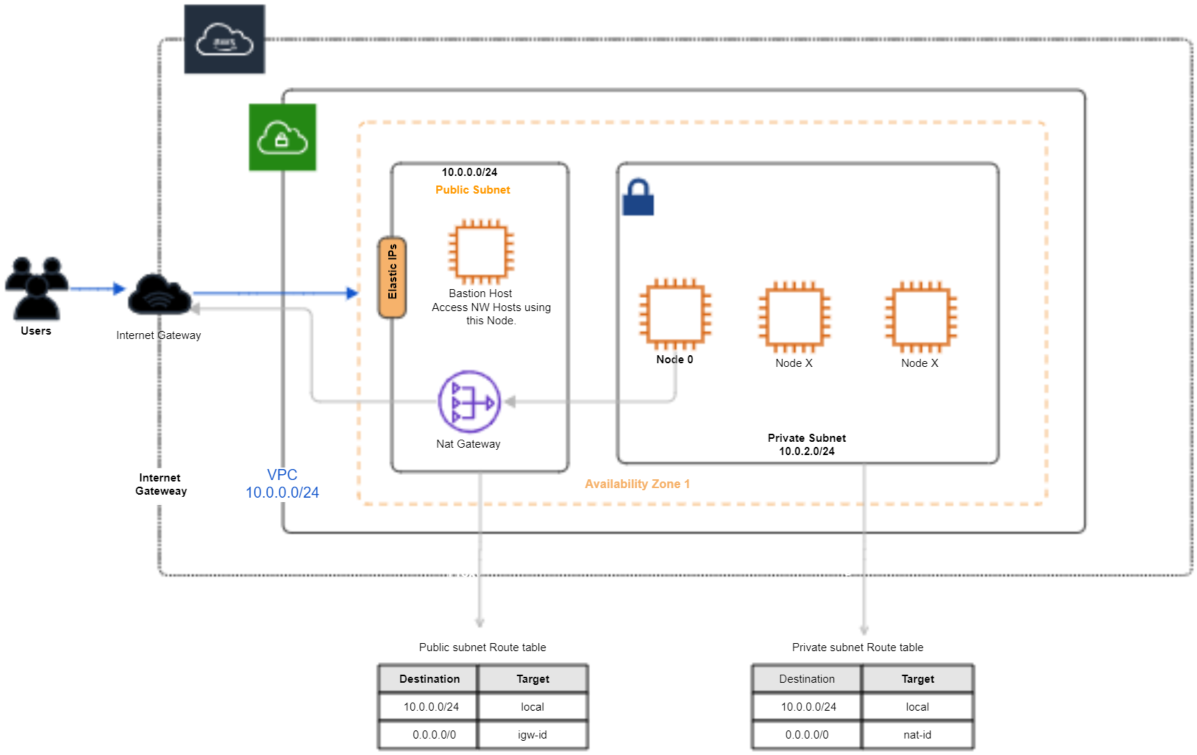
- Access to the AWS console with the appropriate permissions to set up the network and launch an EC2 instance.
- Subscribe to Netwitness 12.4 Product from Marketplace

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)



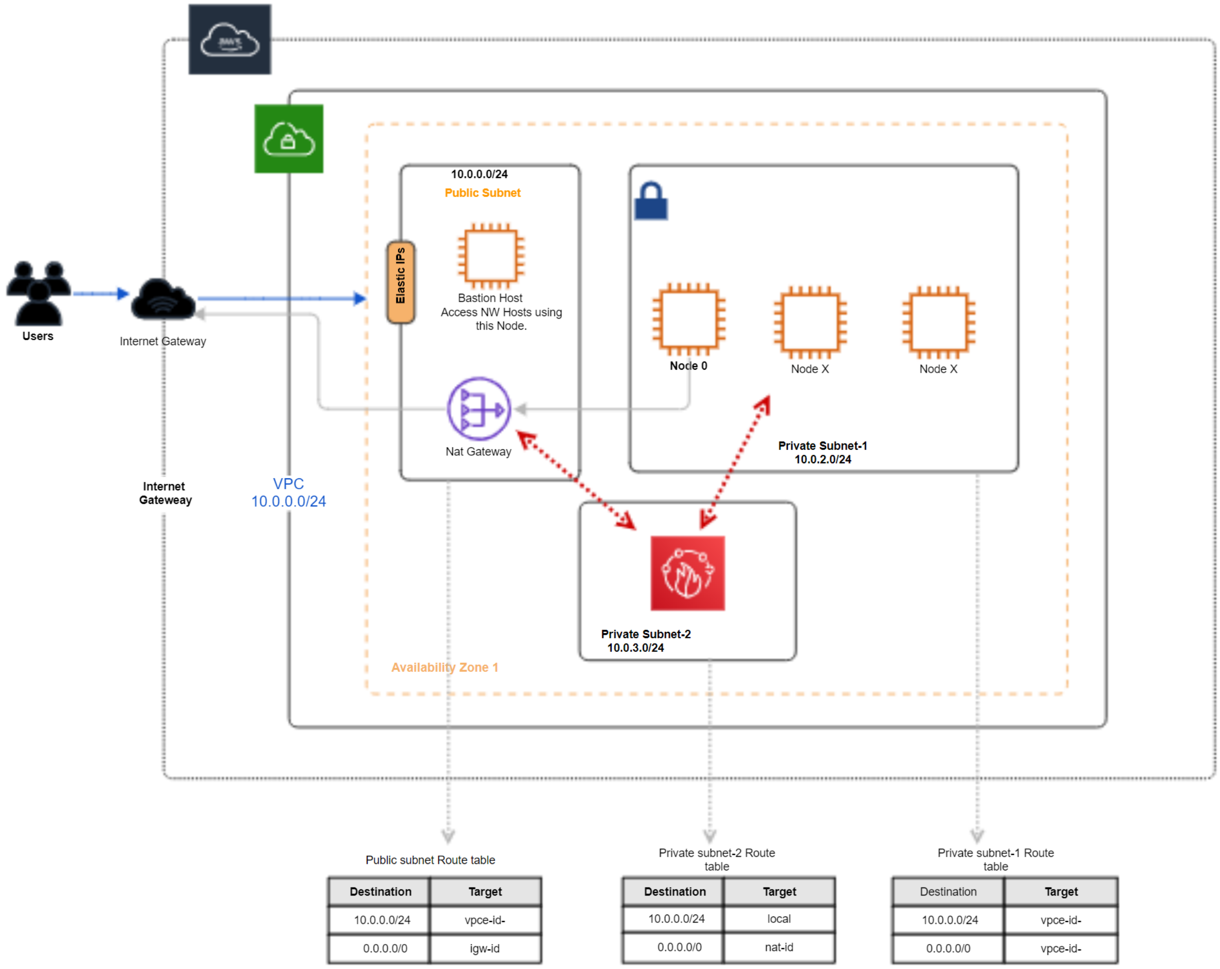
Public subnet Route table

Destination	Target
10.0.0.0/24	local
0.0.0.0/0	igw-id

Private subnet Route table

Destination	Target
10.0.0.0/24	local
0.0.0.0/0	nat-id

NetWitness Deployment with Restricted Internet through Firewall Configuration



Public subnet Route table

Destination	Target
10.0.0.0/24	vpce-id-
0.0.0.0/0	igw-id

Private subnet-2 Route table

Destination	Target
10.0.0.0/24	local
0.0.0.0/0	nat-id

Private subnet-1 Route table

Destination	Target
10.0.0.0/24	vpce-id-
0.0.0.0/0	vpce-id-

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.

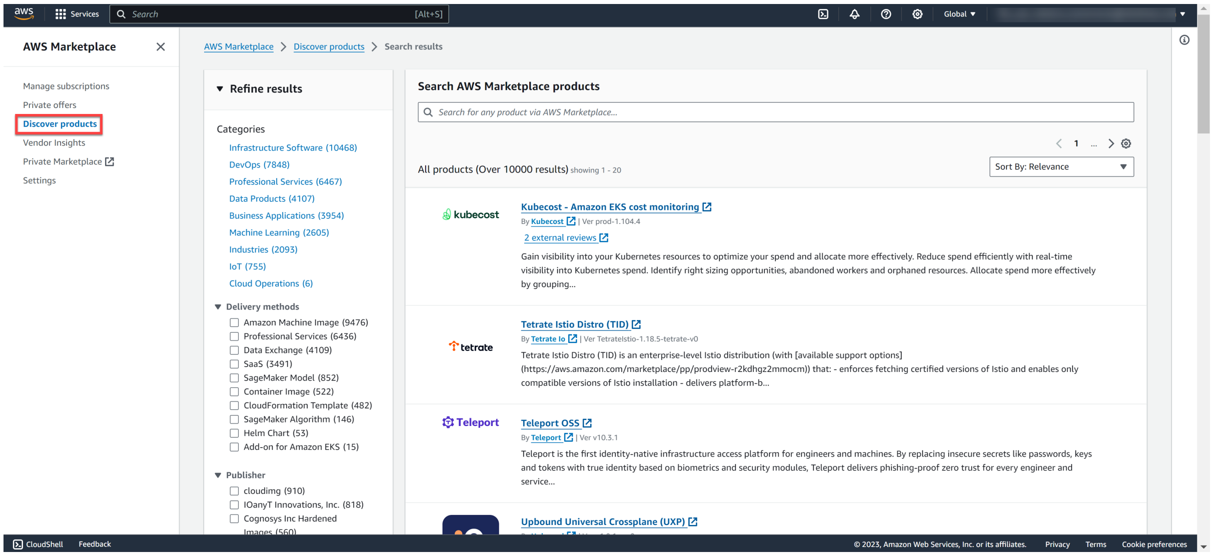
Subscribe to AWS NetWitness Marketplace Product

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.


aws
Services
Search
[Alt+S]
Global ▾
[redacted]
AWS Marketplace
Manage subscriptions
Private offers
Discover products
Vendor Insights
Private Marketplace
Settings
AWS Marketplace > Discover products > Search results
▼ Refine results
Categories
Infrastructure Software (10468)
DevOps (7848)
Professional Services (6467)
Data Products (4107)
Business Applications (3954)
Machine Learning (2605)
Industries (2093)
IoT (755)
Cloud Operations (6)
▼ Delivery methods
□ Amazon Machine Image (9476)
□ Professional Services (6436)
□ Data Exchange (4109)
□ SaaS (3491)
□ SageMaker Model (852)
□ Container Image (522)
□ CloudFormation Template (482)
□ SageMaker Algorithm (146)
□ Helm Chart (53)
□ Add-on for Amazon EKS (15)
▼ Publisher
□ cloudimg (910)
□ IOanyT Innovations, Inc. (818)
□ Cognosys Inc Hardened Images (560)
Search AWS Marketplace products
Search for any product via AWS Marketplace...
< 1 ... >
All products (Over 10000 results) showing 1 - 20
Sort By: Relevance ▾
kubecost
tetrate
Teleport
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

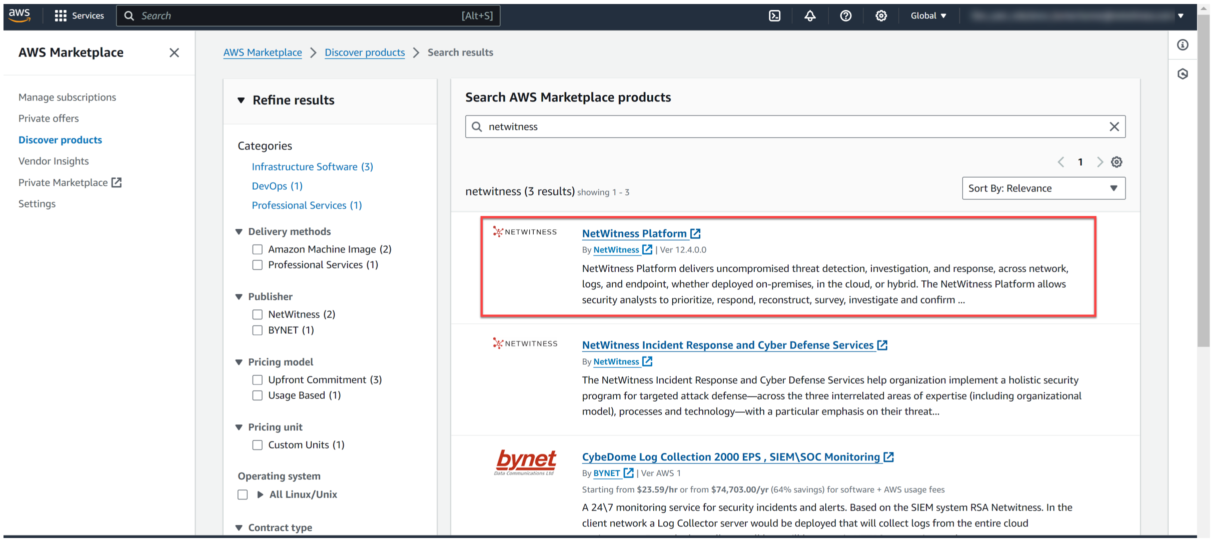
Kubecost - Amazon EKS cost monitoring
By Kubecost | Ver prod-1.104.4
2 external reviews
Gain visibility into your Kubernetes resources to optimize your spend and allocate more effectively. Reduce spend efficiently with real-time visibility into Kubernetes spend. Identify right sizing opportunities, abandoned workers and orphaned resources. Allocate spend more effectively by grouping...

Tetrate Istio Distro (TID)
By Tetrate Io | Ver TetrateIstio-1.18.5-tetrate-v0
Tetrate Istio Distro (TID) is an enterprise-level Istio distribution (with [available support options](https://aws.amazon.com/marketplace/pp/prodview-r2kdhgz2mmocm)) that: - enforces fetching certified versions of Istio and enables only compatible versions of Istio installation - delivers platform-b...

Teleport OSS
By Teleport | Ver v10.3.1
Teleport is the first identity-native infrastructure access platform for engineers and machines. By replacing insecure secrets like passwords, keys and tokens with true identity based on biometrics and security modules, Teleport delivers phishing-proof zero trust for every engineer and service...

Upbound Universal Crossplane (UXP)

3. Search for **NetWitness** product and select **NetWitness Platform 12.4**.

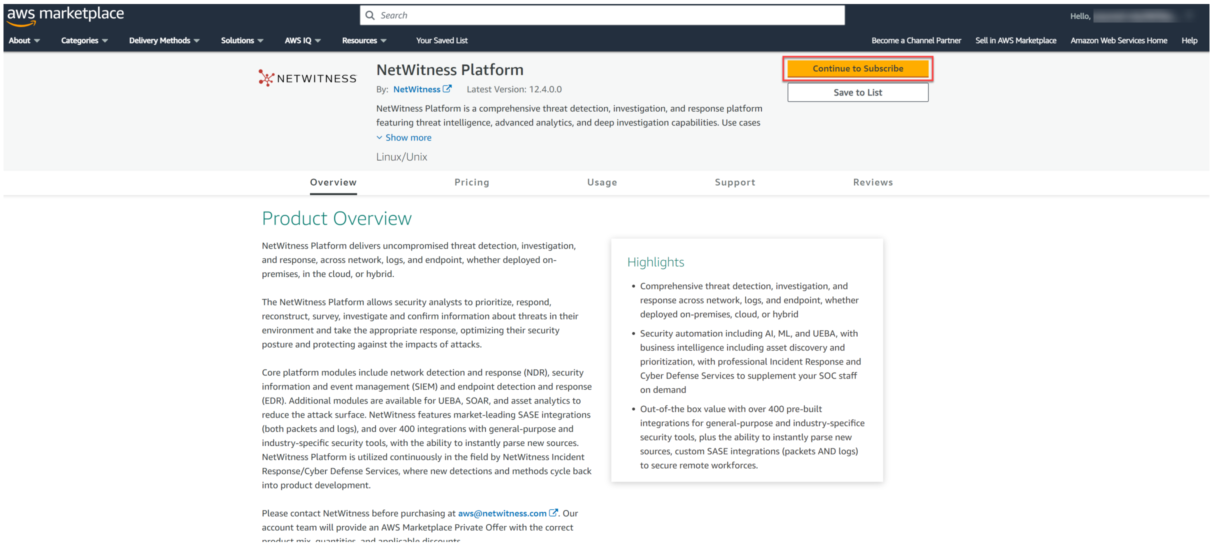


NetWitness Platform
By NetWitness | Ver 12.4.0.0
NetWitness Platform delivers uncompromised threat detection, investigation, and response, across network, logs, and endpoint, whether deployed on-premises, in the cloud, or hybrid. The NetWitness Platform allows security analysts to prioritize, respond, reconstruct, survey, investigate and confirm ...

NetWitness Incident Response and Cyber Defense Services
By NetWitness
The NetWitness Incident Response and Cyber Defense Services help organization implement a holistic security program for targeted attack defense—across the three interrelated areas of expertise (including organizational model), processes and technology—with a particular emphasis on their threat...

CybeDome Log Collection 2000 EPS , SIEM\SOC Monitoring
By BYNET | Ver AWS 1
Starting from $23.59/hr or from $74,703.00/yr (64% savings) for software + AWS usage fees
A 24\7 monitoring service for security incidents and alerts. Based on the SIEM system RSA Netwitness. In the client network a Log Collector server would be deployed that will collect logs from the entire cloud

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



NetWitness Platform

By: NetWitness Latest Version: 12.4.0.0

NetWitness Platform is a comprehensive threat detection, investigation, and response platform featuring threat intelligence, advanced analytics, and deep investigation capabilities. Use cases

Linux/Unix

Product Overview

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.

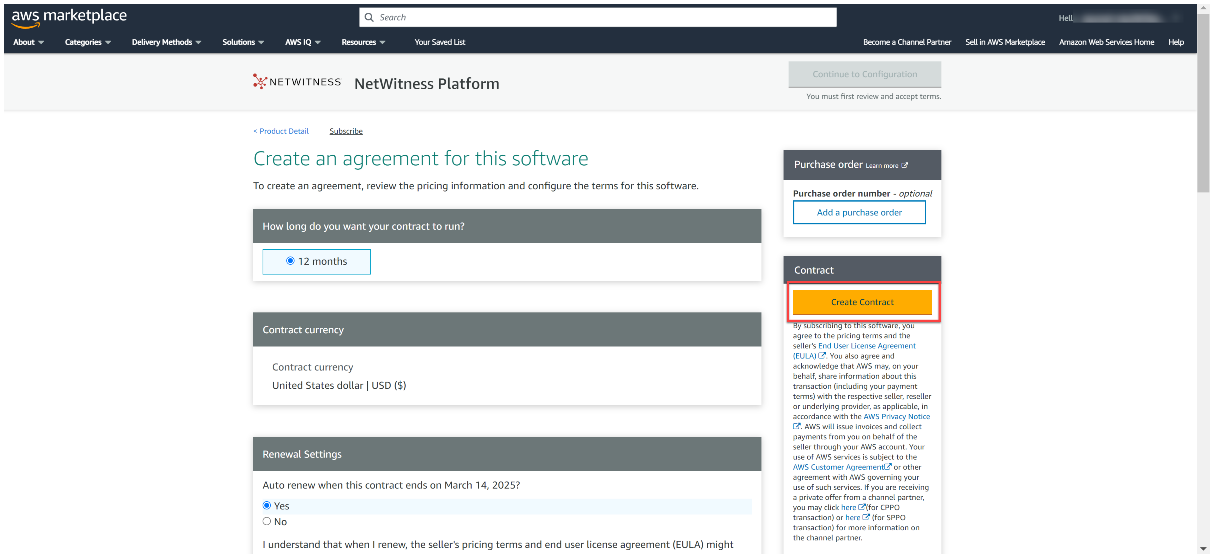
Core platform modules include network detection and response (NDR), security information and event management (SIEM) and endpoint detection and response (EDR). Additional modules are available for UEBA, SOAR, and asset analytics to reduce the attack surface. NetWitness features market-leading SASE integrations (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.

Please contact NetWitness before purchasing at aws@netwitness.com. Our account team will provide an AWS Marketplace Private Offer with the correct product mix, quantities, and applicable discounts.

Highlights

- Comprehensive threat detection, investigation, and response across network, logs, and endpoint, whether deployed on-premises, cloud, or hybrid
- Security automation including AI, ML, and UEBA, with business intelligence including asset discovery and prioritization, with professional Incident Response and Cyber Defense Services to supplement your SOC staff on demand
- Out-of-the box value with over 400 pre-built integrations for general-purpose and industry-specifice security tools, plus the ability to instantly parse new sources, custom SASE integrations (packets AND logs) to secure remote workforces.

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



NetWitness Platform

You must first review and accept terms.

Create an agreement for this software

To create an agreement, review the pricing information and configure the terms for this software.

How long do you want your contract to run?

● 12 months

Contract currency

Contract currency
United States dollar | USD ($)

Renewal Settings

Auto renew when this contract ends on March 14, 2025?

● Yes
○ No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might

Purchase order

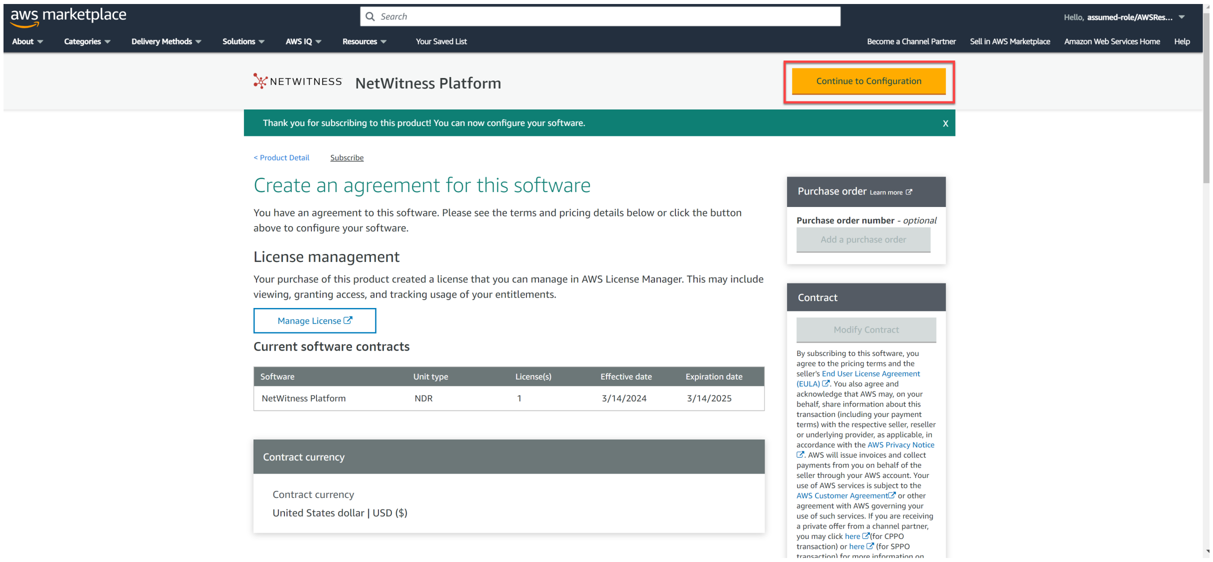
Purchase order number - *optional*

Contract

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may, on your behalf, share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services. If you are receiving a private offer from a channel partner, you may click here (for CPPO transaction) or here (for SPPO transaction) for more information on the channel partner.

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

6. Click **Continue to Configuration**.



NetWitness Platform

Thank you for subscribing to this product! You can now configure your software.

Create an agreement for this software

You have an agreement to this software. Please see the terms and pricing details below or click the button above to configure your software.

License management

Your purchase of this product created a license that you can manage in AWS License Manager. This may include viewing, granting access, and tracking usage of your entitlements.

Current software contracts

Software	Unit type	License(s)	Effective date	Expiration date
NetWitness Platform	NDR	1	3/14/2024	3/14/2025

Contract currency

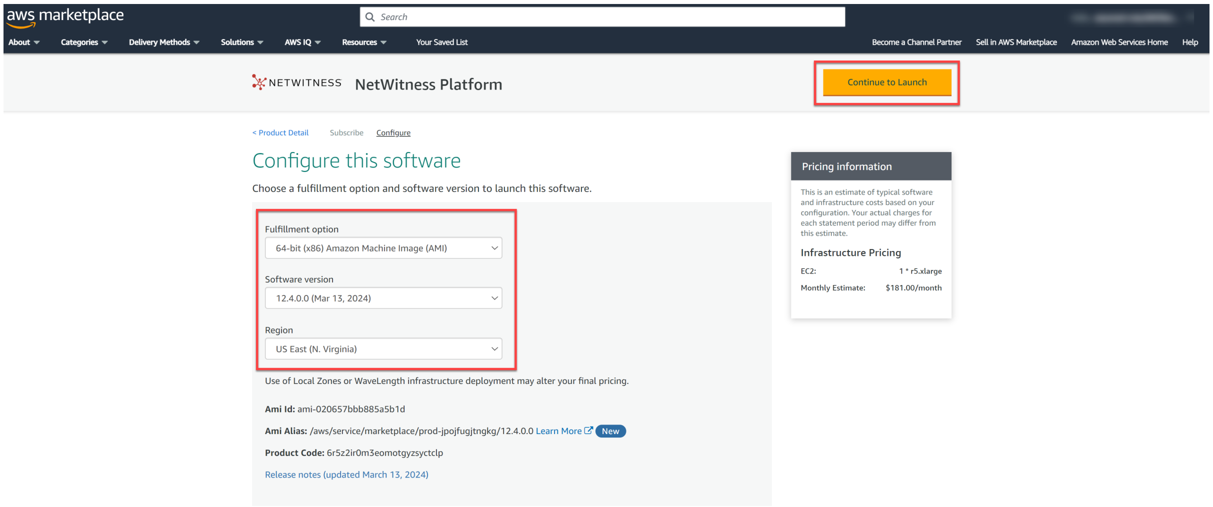
Contract currency
United States dollar | USD ($)

Purchase order number - *optional*

Contract

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may, on your behalf, share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services. If you are receiving a private offer from a channel partner, you may click here (for CPPO transaction) or here (for SPPO transaction) for more information on

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



NetWitness Platform

Configure this software

Choose a fulfillment option and software version to launch this software.

Fulfillment option
64-bit (x86) Amazon Machine Image (AMI)

Software version
12.4.0.0 (Mar 13, 2024)

Region
US East (N. Virginia)

Use of Local Zones or WaveLength infrastructure deployment may alter your final pricing.

Ami Id: ami-020657bbb885a5b1d

Ami Alias: /aws/service/marketplace/prod-jpojfugjtngkg/12.4.0.0

Product Code: 6r5z2ir0m3eomotgyzsyctclp

Release notes (updated March 13, 2024)

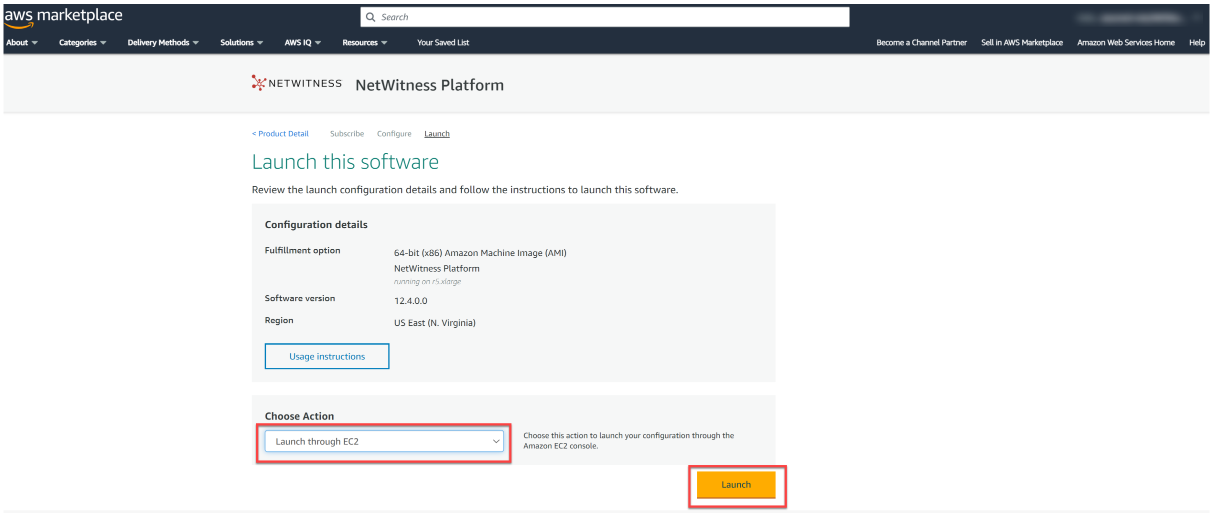
Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Infrastructure Pricing

EC2:	1 * r5.xlarge
Monthly Estimate:	$181.00/month

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



NetWitness Platform

Launch this software

Review the launch configuration details and follow the instructions to launch this software.

Configuration details

Fulfillment option: 64-bit (x86) Amazon Machine Image (AMI)
NetWitness Platform
running on r5.xlarge

Software version: 12.4.0.0

Region: US East (N. Virginia)

Choose Action: Launch through EC2

Choose this action to launch your configuration through the Amazon EC2 console.

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

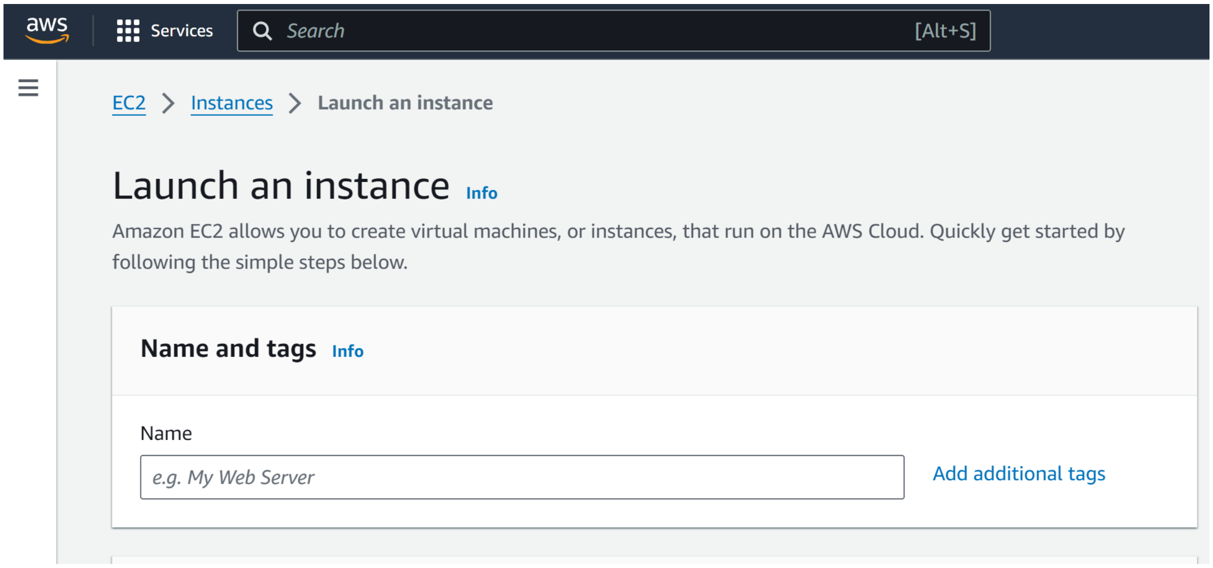
Deploy EC2 Instance from AWS Marketplace and Configure a Host

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**.

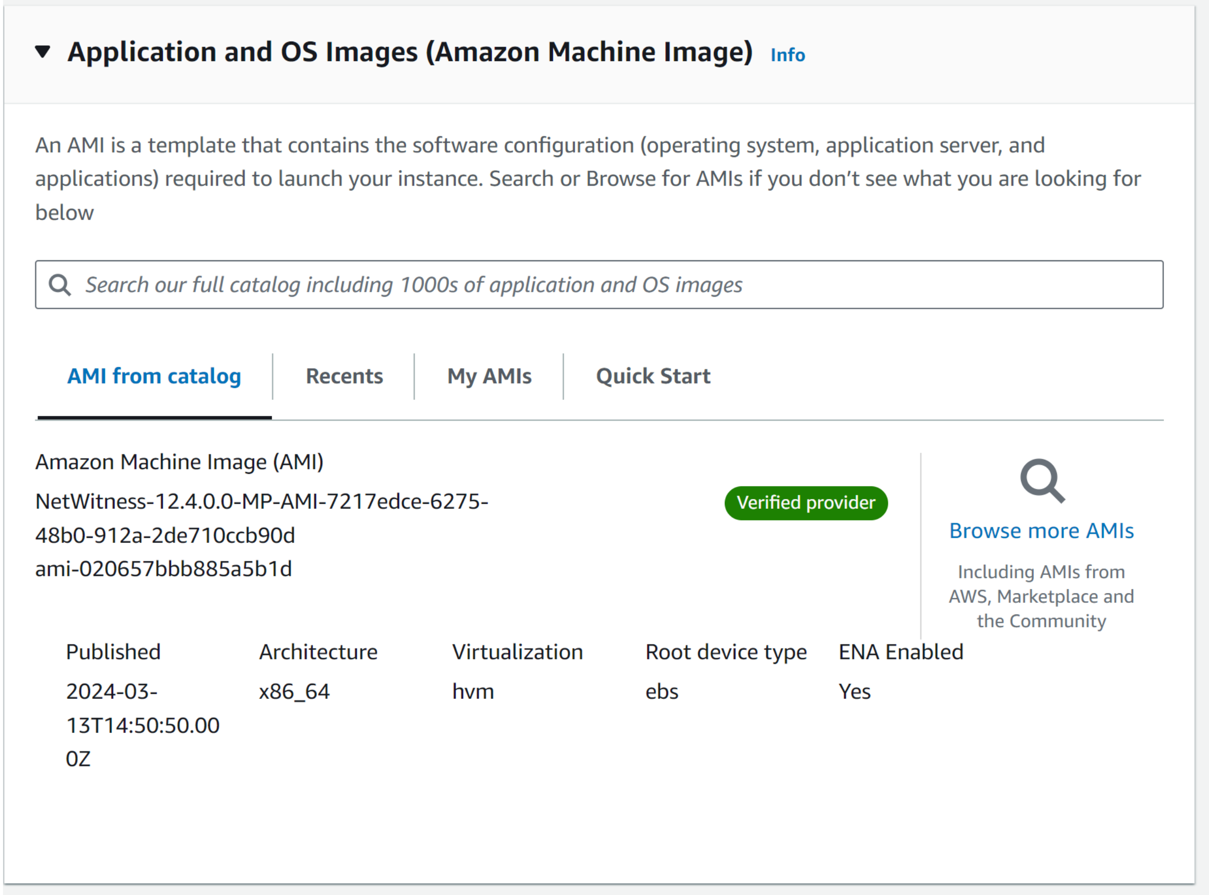


Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

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.



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

AMI from catalog | Recents | My AMIs | Quick Start

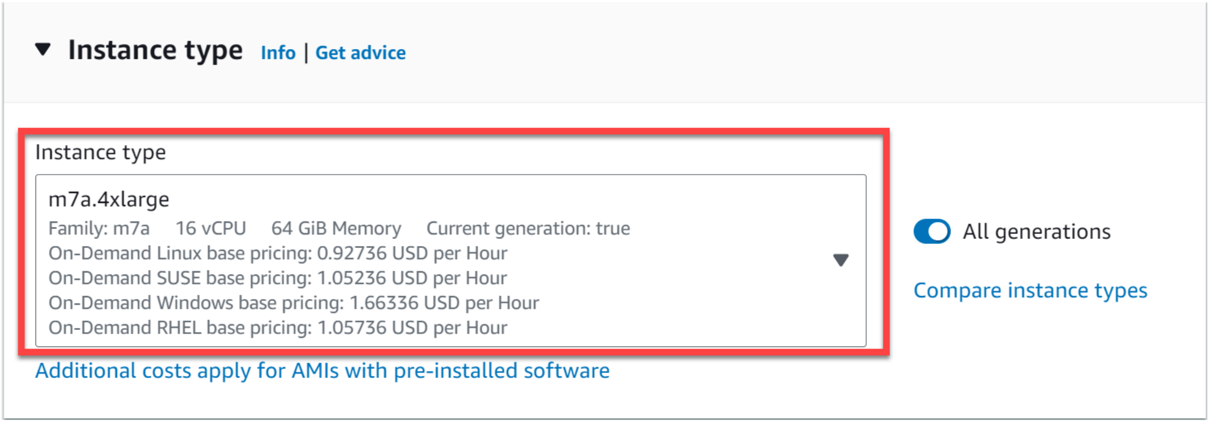
Amazon Machine Image (AMI)
NetWitness-12.4.0.0-MP-AMI-7217edce-6275-48b0-912a-2de710ccb90d
ami-020657bbb885a5b1d

Verified provider

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Published	Architecture	Virtualization	Root device type	ENA Enabled
2024-03-13T14:50:50.000Z	x86_64	hvm	ebs	Yes

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

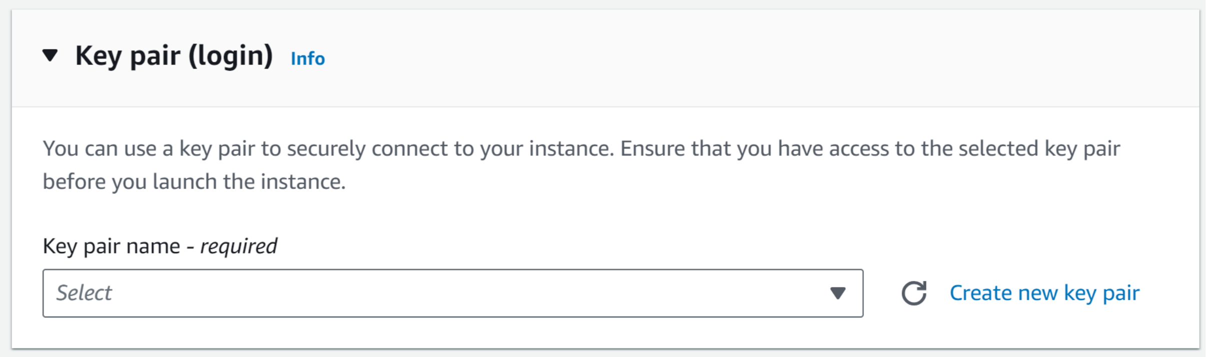
Compare instance types

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 12.4.

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

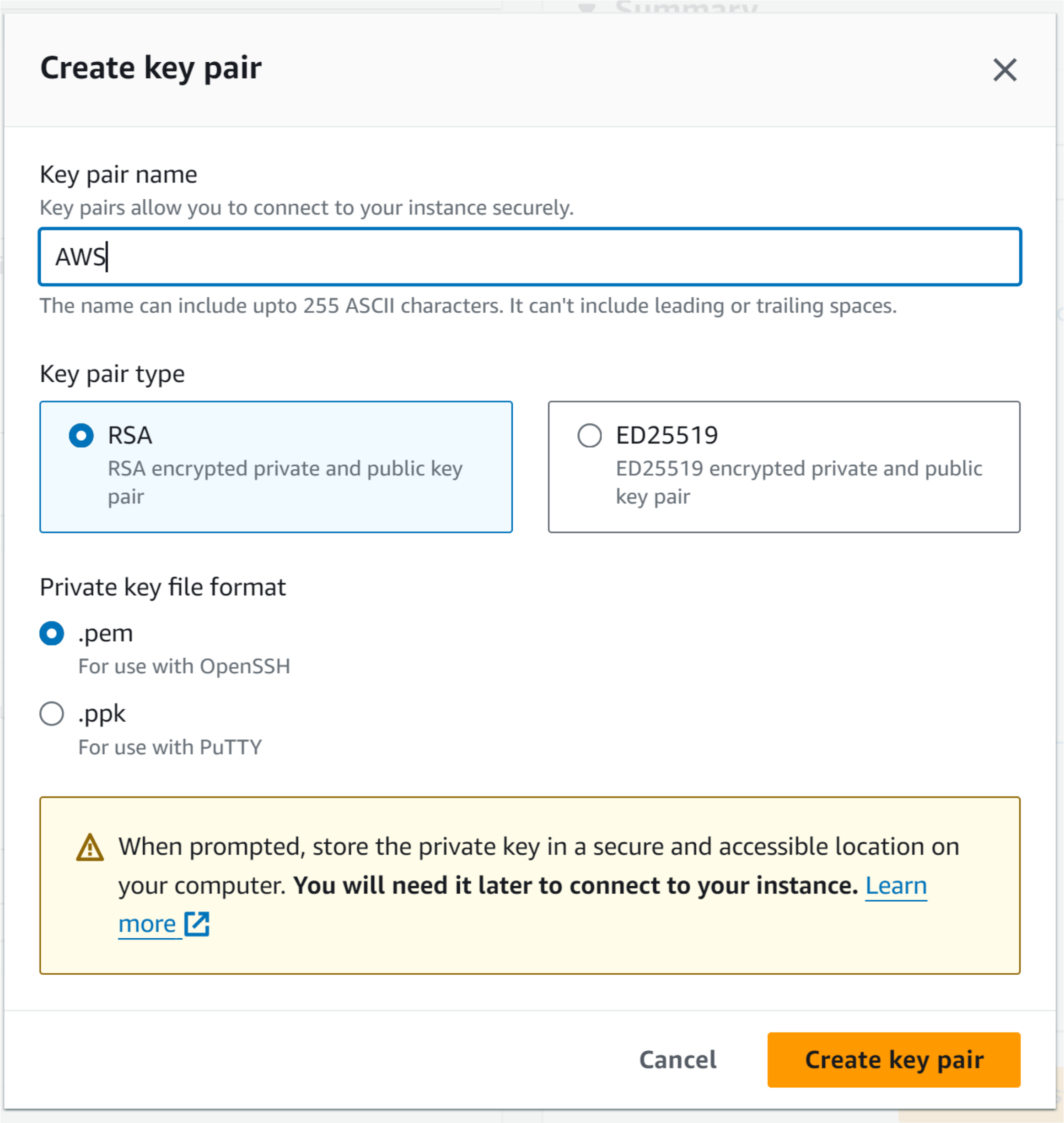
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

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

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.

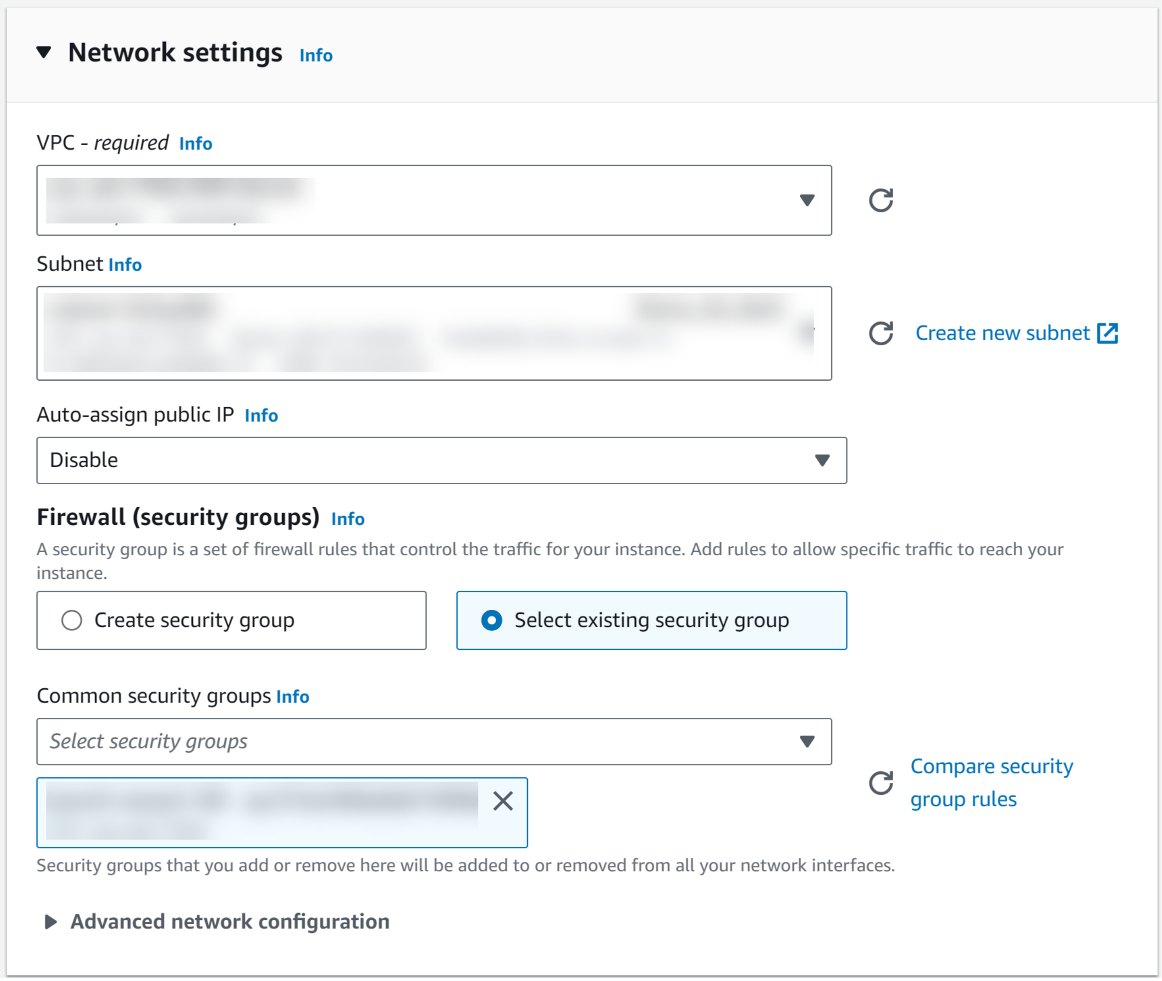
To select or create, click **Edit** and configure the details:

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 12.4*.



▼ **Network settings** Info

VPC - *required* Info

[redacted]

Subnet Info

[redacted]

Auto-assign public IP Info

Disable

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

Select security groups

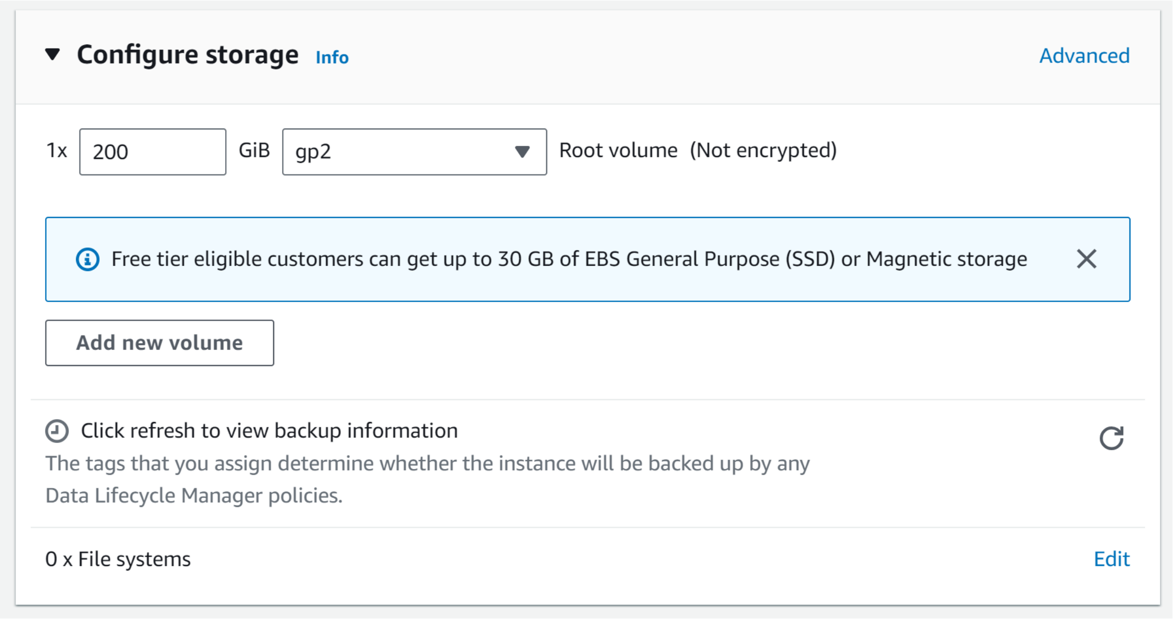
[redacted]

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

Create new subnet
Compare security group rules
▶ 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.



▼ Configure storage Info

Advanced

1x 200 GiB gp2 ▼ Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

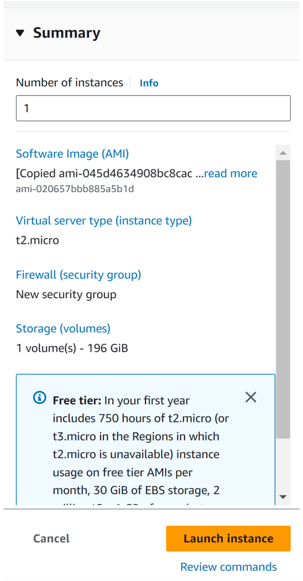
0 x File systems

Edit

For more information, see the Storage Guide for NetWitness® Platform 12.4 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**.



▼ Summary

Number of instances Info

1

Software Image (AMI)
[Copied ami-045d4634908bc8cac ...read more
ami-020657bbb885a5b1d

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 196 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2

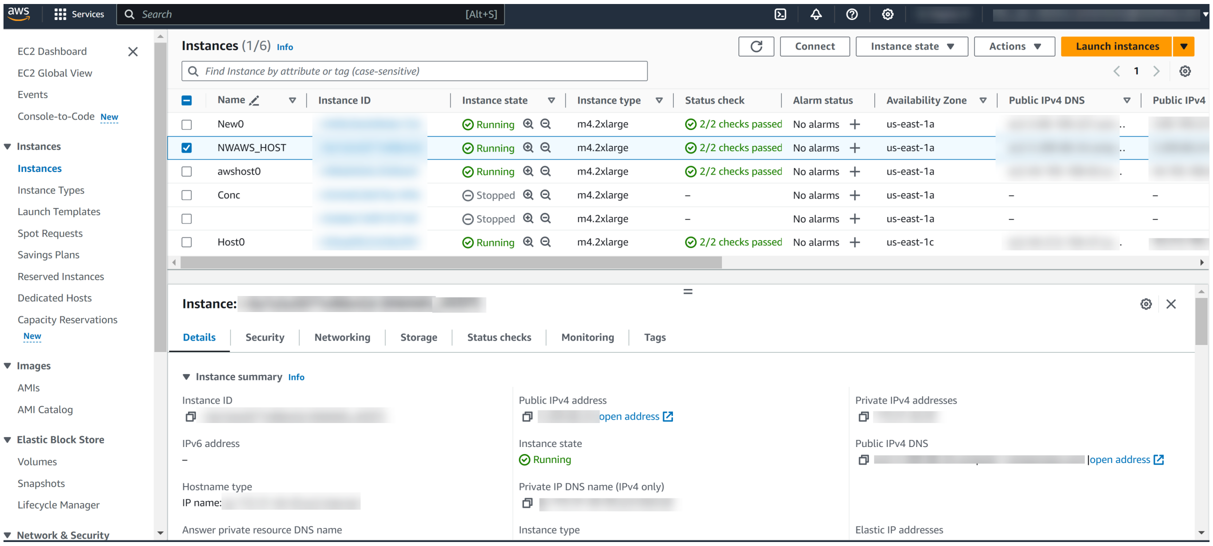
Cancel

Launch instance

Review commands

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.



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
☐	New0	[redacted]	Running	m4.2xlarge	2/2 checks passed	No alarms	us-east-1a	[redacted]	[redacted]
☑	NWAWS_HOST	[redacted]	Running	m4.2xlarge	2/2 checks passed	No alarms	us-east-1a	[redacted]	[redacted]
☐	awshost0	[redacted]	Running	m4.2xlarge	2/2 checks passed	No alarms	us-east-1a	[redacted]	[redacted]
☐	Conc	[redacted]	Stopped	m4.2xlarge	–	No alarms	us-east-1a	–	–
☐		[redacted]	Stopped	m4.2xlarge	–	No alarms	us-east-1a	–	–
☐	Host0	[redacted]	Running	m4.2xlarge	2/2 checks passed	No alarms	us-east-1c	[redacted]	[redacted]

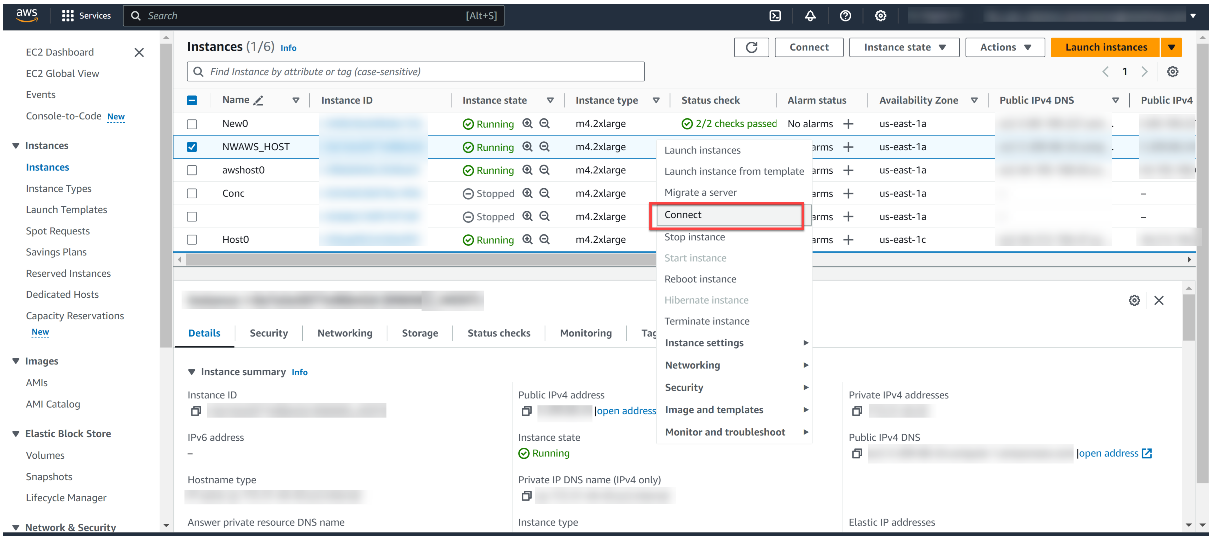
Instance: [redacted]

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
[redacted]	[redacted] open address	[redacted]
IPv6 address	Instance state	Public IPv4 DNS
–	Running	[redacted] open address
Hostname type IP name: [redacted]	Private IP DNS name (IPv4 only) [redacted]	
Answer private resource DNS name	Instance type	Elastic IP addresses

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**.



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
☐	New0	[redacted]	Running	m4.2xlarge	2/2 checks passed	No alarms	us-east-1a	[redacted]	[redacted]
☑	NWAWS_HOST	[redacted]	Running	m4.2xlarge		arms	us-east-1a	[redacted]	[redacted]
☐	awshost0	[redacted]	Running	m4.2xlarge		arms	us-east-1a	[redacted]	[redacted]
☐	Conc	[redacted]	Stopped	m4.2xlarge		arms	us-east-1a		–
☐		[redacted]	Stopped	m4.2xlarge		arms	us-east-1a		–
☐	Host0	[redacted]	Running	m4.2xlarge		arms	us-east-1c	[redacted]	

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 12.4.0.0 package to this location:

    ```
    wget -m -nH --no-parent https://repo.netwitness.com/12.4.0.0/
    ```

    > **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.