Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER – PROVISION NITRO COMPUTE NODES USING AWS MARKETPLACE

Version 1.0

Fortanix Inc. | 3910 Freedom Circle | Suit 104 | Santa Clara, CA 95054 | United States of America | ☎ +1 (650) 943-2484
✉ info@fortanix.com | 🌐 www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION 2

2.0 FORTANIX OFFERINGS ON AWS MARKETPLACE 2

2.1 Direct Search 2

2.2 Filtred Search 3

2.3 Navigating the Landing Screen 4

2.4 Configuring the Software 5

3.0 PROVISIONING THE COMPUTE NODE USING AWS MARKETPLACE 10

4.0 REVIEWING THE COMPUTE NODE 11

5.0 REFERENCES 13

6.0 DOCUMENT INFORMATION 14

6.1 Document Location 14

6.2 Document Updates 14

1.0 INTRODUCTION

Fortanix Confidential Computing Nitro Compute Node Agent software is deployed on an Amazon Web Services (AWS) Nitro EC2 instance to manage the compute node and applications running in Nitro enclaves. The node agent ensures that a valid Nitro-enabled virtual machine is enrolled into a Fortanix Confidential Computing Manager (CCM) account for running containerized applications in the AWS Nitro secure enclaves, while also providing hardware pre-registration and application-node policy restrictions.

The solution orchestrates critical security policies such as identity verification, data access control, and code attestation for enclaves that are required for confidential computing. Unlike other approaches, Fortanix provides the flexibility to run and manage the broadest set of applications, including existing applications, new enclave-native applications, and pre-packaged applications.

The Fortanix CCM enables applications to run in confidential computing environments, verifies the integrity of those environments, and manages the enclave application lifecycle.

This document describes how to provision an EC2 instance and enroll a Fortanix Nitro Node Agent using the Amazon Web Services (AWS) Marketplace.

2.0 FORTANIX OFFERINGS ON AWS MARKETPLACE

You can use either of the following two methods to explore Fortanix offerings on the AWS Marketplace:

- **Direct Search:** Simply enter "Fortanix" into the Search bar.

  OR
- **Filtered Search:** Refine your search by selecting specific categories.

2.1 DIRECT SEARCH

Perform the following steps:

1. Log in to the AWS Marketplace Console using your AWS account credentials.
2. Type Fortanix in the Search bar to list Fortanix marketplace offerings.

3. Select the **Fortanix Confidential Computing Nitro Compute Node** option from the Marketplace section. This action opens a new tab on the screen.

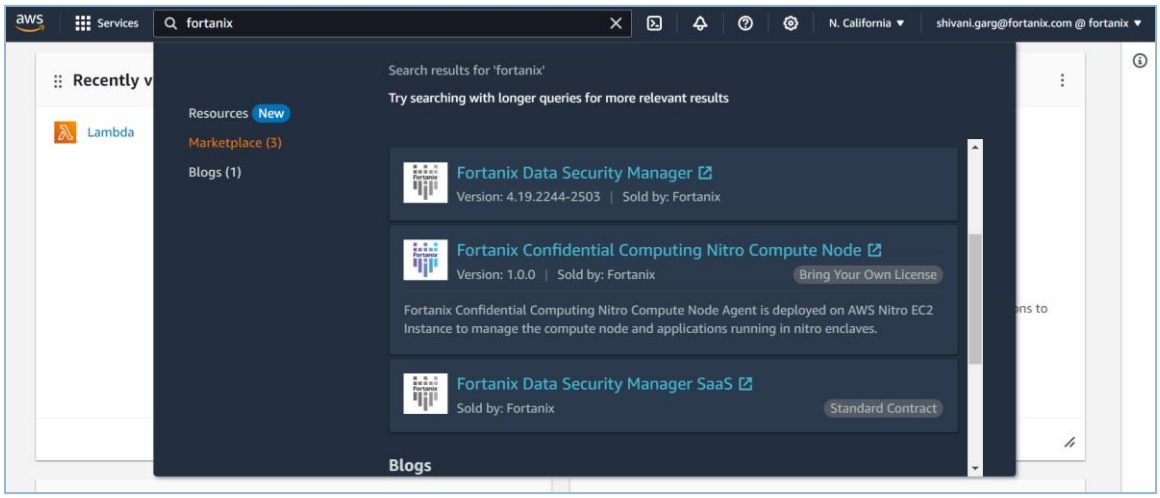


FIGURE 1: SEARCH RESULTS

2.2 FILTRED SEARCH

Perform the following steps:

1. Access the AWS Marketplace login page at https://aws.amazon.com/marketplace and enter your credentials to log in.
2. On the landing page, scroll to the "Find AWS Marketplace products that meet your needs" section.

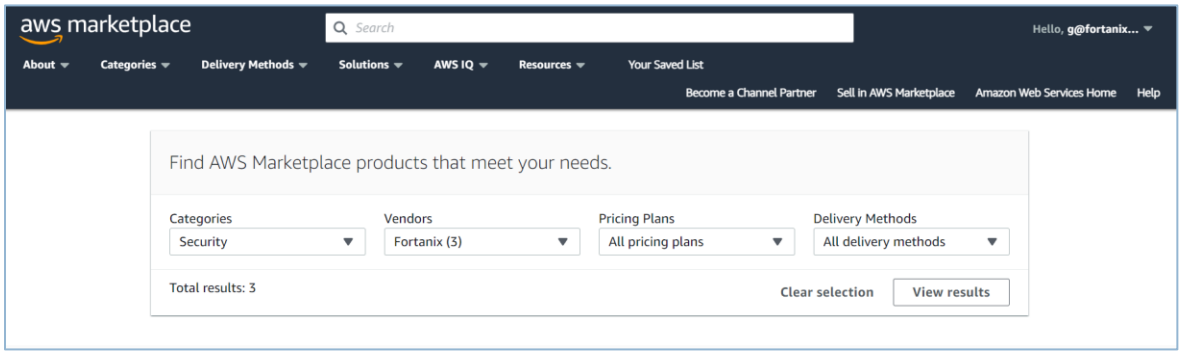


FIGURE 2: FILTERS

In this section, select the following criteria:

- **Categories:** Select the **Security** option under infrastructure software, observe dynamic changes in the available options for vendors, pricing plans, and delivery methods.
- **Vendors:** Select **Fortanix** from the drop down menu, dynamically refining your search.

- **Pricing Plans:** Select the **Bring Your Own License (BYOL)** option from the drop down menu.
- **Delivery Methods:** Select **CloudFormation** from the drop down menu.

Once you have selected the required specifications, out of the available marketplace offers from Fortanix, select the **Fortanix Confidential Computing Nitro Compute Node** option.

2.3 NAVIGATING THE LANDING SCREEN

The following is the landing screen for Fortanix Confidential Computing Nitro Compute Node:

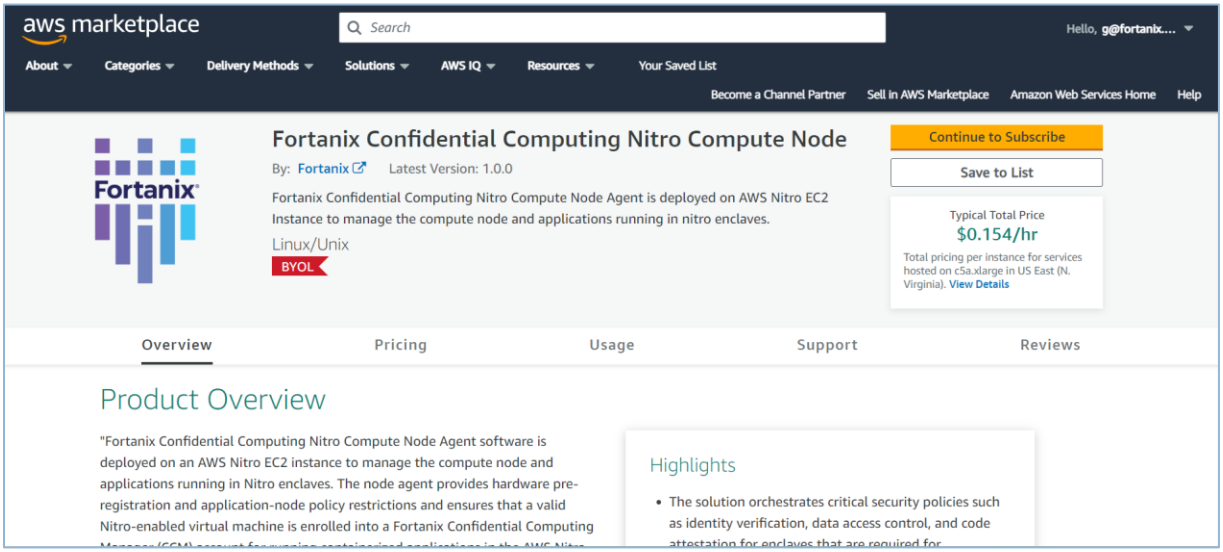


FIGURE 3: LANDING SCREEN

The following are the components on the screen:

- **Continue to Subscribe:** Progress through the subscription process for the Fortanix Confidential Computing Nitro Compute Node.
- **Overview:** Fortanix Nitro Compute Node seamlessly integrates with AWS Nitro EC2 instances, managing compute nodes and applications securely. Start a free trial at https://ccm.fortanix.com/.
- **Pricing:** Fortanix Nitro Compute Node offers a free tier.
    - **Free Tier:** No charges for the software.
    - **Bring Your Own License (BYOL):** Available for customers with existing licenses.
- **Usage:** Deploy the Fortanix Nitro Compute Node Agent on AWS Nitro EC2 instances to manage the compute node and applications running in Nitro enclaves. Fortanix CCM

enables applications to run in confidential environments. You can enroll a compute node agent at https://ccm.fortanix.com/.

- **Support:** A 24/7 support using Slack and email at support@fortanix.com is available. The refunds are not supported, but cancellations are accepted at any time.
- **Reviews:** Share your thoughts by writing a customer review. Your feedback contributes to the community's understanding of this product.

2.4 CONFIGURING THE SOFTWARE

Perform the following steps to configure the software on your system:

1. On the **Configure this software** page, enter the following:
   - **Fulfillment Option:** Select the **Deploy Confidential Computing Node Agent** option.
   - **Software Version:** Select the required version from the drop down menu, ensuring compatibility with your preferences.
   - **Region:** Select the desired region for deployment, for example, "US East (N. Virginia)."
2. Click the **Continue to Launch** button.

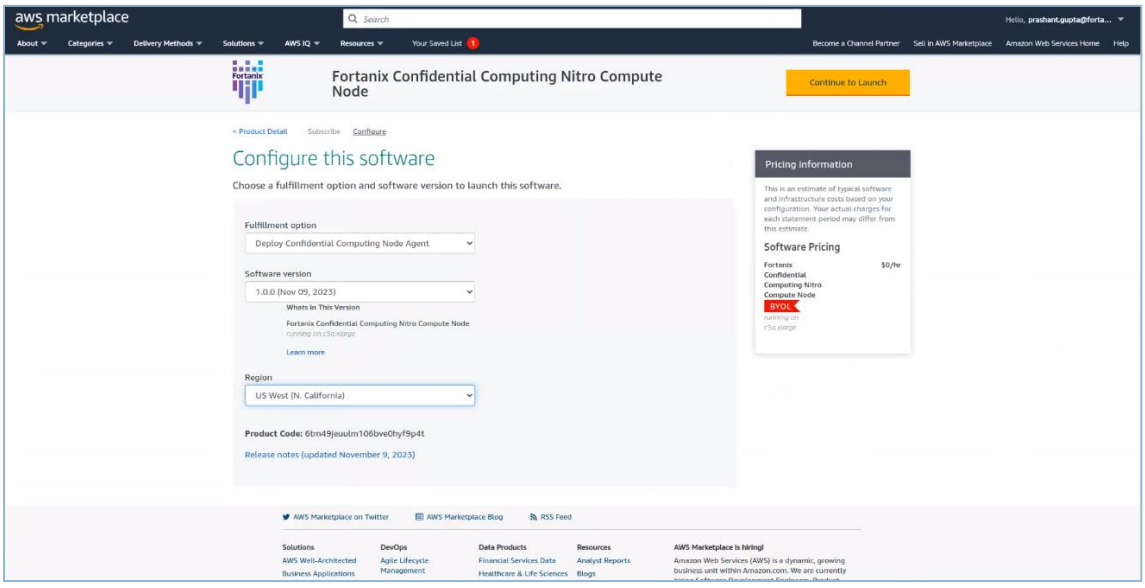


FIGURE 4: CONFIGURE THE SOFTWARE

3. On the **Launch this software** page, enter the following:
   - Select the **Launch CloudFormation** option from the Choose Action drop down menu.
   - Click the **Launch** button. This will redirect you to the "Create Stack" page.

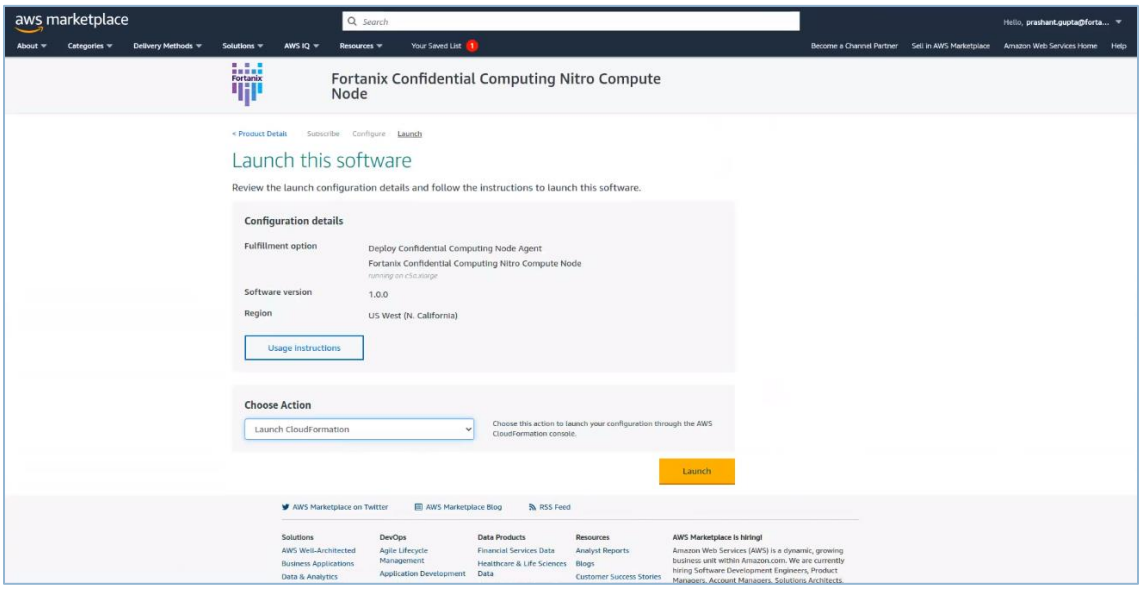


FIGURE 5: LAUNCH THE SOFTWARE

4. On the **Create Stack** page, enter the following:
   - **Prerequisite:** Select the default option, **Template is Ready** radio button.
   - **Specify Template:**
     - **Template Source:** Select the default option, **Amazon S3 URL** radio button.
     - **Amazon S3 URL:** Enter the default Amazon S3 URL in the field.
     - **S3 URL:** Enter the default S3 URL.

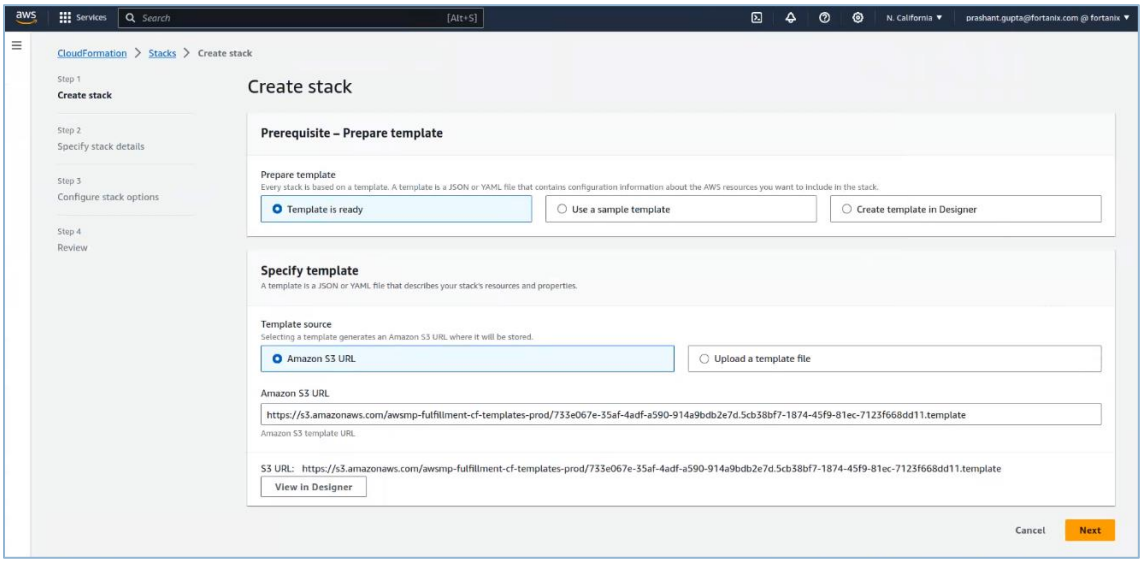


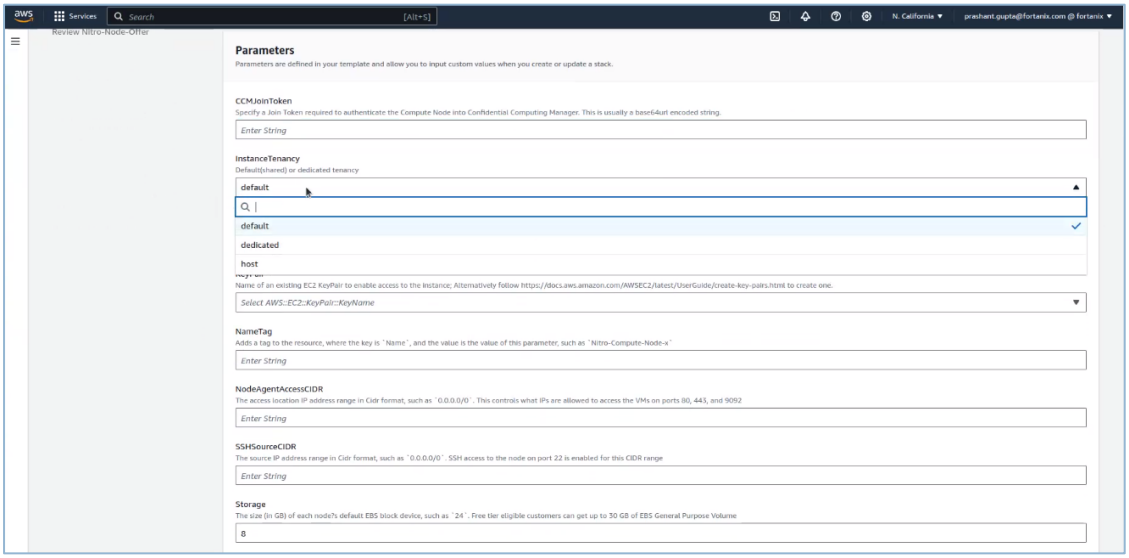
FIGURE 6: CREATE STACK

5. Click the **Next** button.

6. On the **Specify Stack Details** page, enter the following:

PARAMETER NAME	TYPE	DESCRIPTION
CCMJoinToken	String	Refers to a security token used during the process of joining a node to the Fortanix Confidential Computing Manager (CCM). It ensures secure communication and authentication between the node and the manager within the Fortanix ecosystem. *To know more about this token, refer to Section 3.0 - Provision the Compute Node Using AWS Marketplace.*
InstanceTenancy	dedicated or host	Refers to the tenancy model for an Amazon EC2 instance. It determines whether the instance runs on dedicated hardware ("dedicated") or shared hardware (default or "host"). The choice can impact performance isolation and compliance requirements.
InstanceType	String	Specifies the C5a hardware series of Amazon EC2 instances that will be launched. It defines the computing capacity, memory, and networking capabilities of the instance.
KeyPair	KeyPair	Refers to a set of cryptographic keys (public and private) used for secure SSH access to an EC2 instance. During launch, the instance is associated with the public key, while the client uses the private key to authenticate and establish a secure connection. *For more information, refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-key-pairs.html.*
NameTag	String	Refers to a user-defined tag assigned to AWS resources, providing a human-readable identifier. It helps in organizing and managing resources efficiently.
NodeAgentAccessCIDR	String	Specifies the IP address range (CIDR block, such as `0.0.0.0/0`) from which the Fortanix Confidential Computing Node Agent can be accessed. It acts as a security measure, restricting access to a defined set of IP addresses.

PARAMETER NAME	TYPE	DESCRIPTION
SSHSourceCIDR	String	Defines the allowed IP address range (CIDR block, such as `0.0.0.0/0`) from which SSH connections are permitted to access the EC2 instance. This setting enhances security by controlling who can connect to the instance via SSH.
Storage	Integer	Refers to the type and size of storage associated with the EC2 instance. It includes specifications such as the volume type, size, and configuration. Storage options impact the performance and durability of data on the instance.
VpcCIDR	String	Represents the CIDR block assigned to a Virtual Private Cloud (VPC). It defines the range of private IP addresses available within the VPC, facilitating network segmentation and resource isolation.



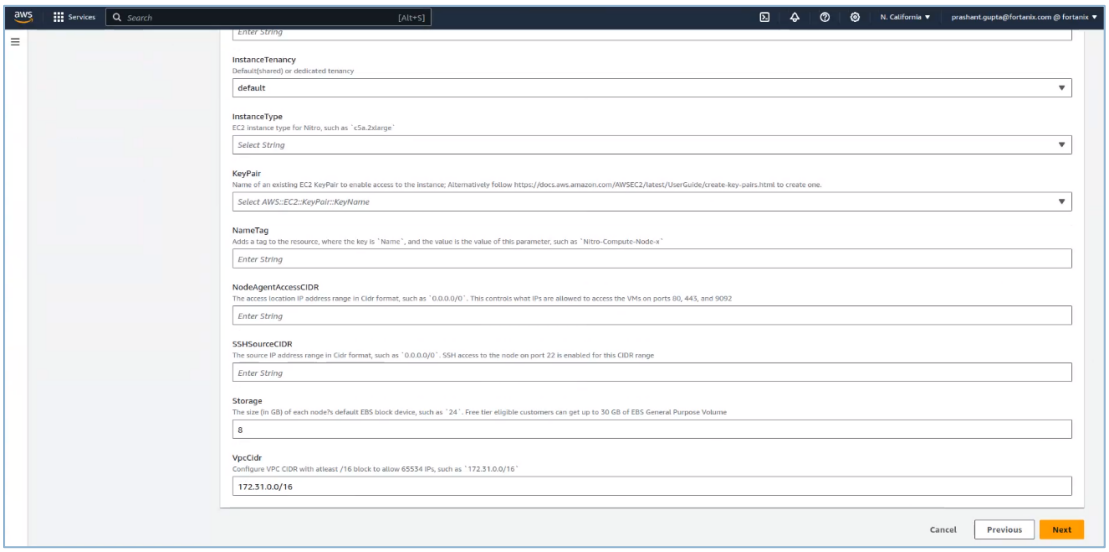


FIGURE 7: SPECIFY STACK DETAILS

7. On the **Configure Stack Options** page, enter the following:

PARAMETER NAME	DESCRIPTION
Tags	Apply tags to categorize stacks based on attributes such as purpose, ownership, or environment.
Permissions	Assign appropriate permissions to individuals or services to govern stack management activities.
Stack failure options	Configure these options to manage failures in a controlled manner, maintaining the integrity of the stack.
Rollback configuration	Tailor rollback behavior to ensure a consistent state and mitigate potential issues resulting from unsuccessful updates.
Notification options	Utilize notification options to stay informed about the progress and status of stack operations, facilitating proactive management.
Stack creation options	Customize creation options to align with specific requirements, ensuring the creation of stacks with desired attributes and behaviours.

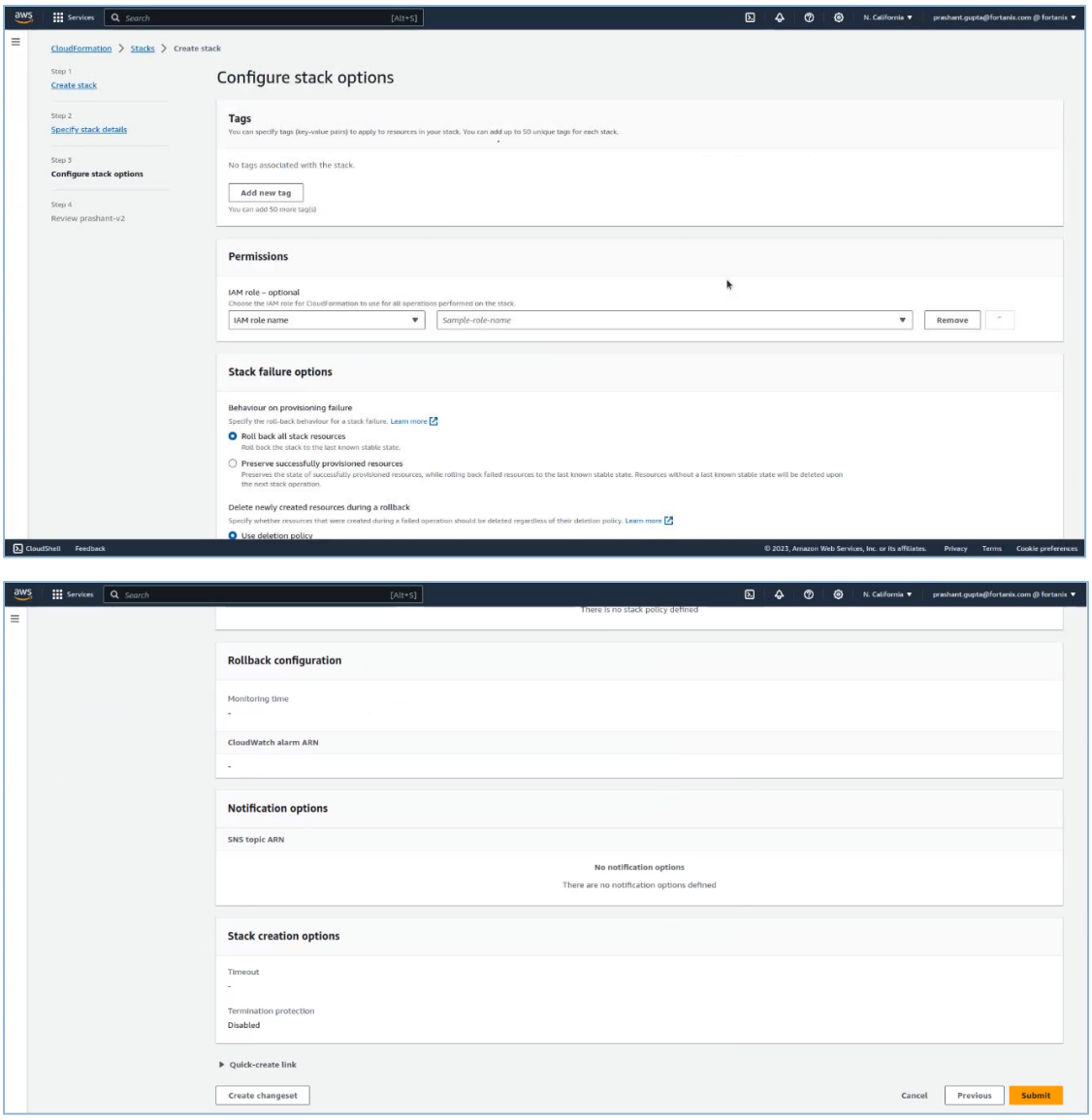


FIGURE 8: CONFIGURE STACK OPTIONS

8. Click the **Submit** button.

3.0 PROVISIONING THE COMPUTE NODE USING AWS MARKETPLACE

Perform the following steps:

1. First, generate a Join Token using the CCM UI. To generate your Join Token, log in to https://ccm.fortanix.com.
2. Navigate to **Infrastructure** → **Compute Nodes** → **AWS NITRO ENCLAVES** tab and click **+ ENROLL NODE**.

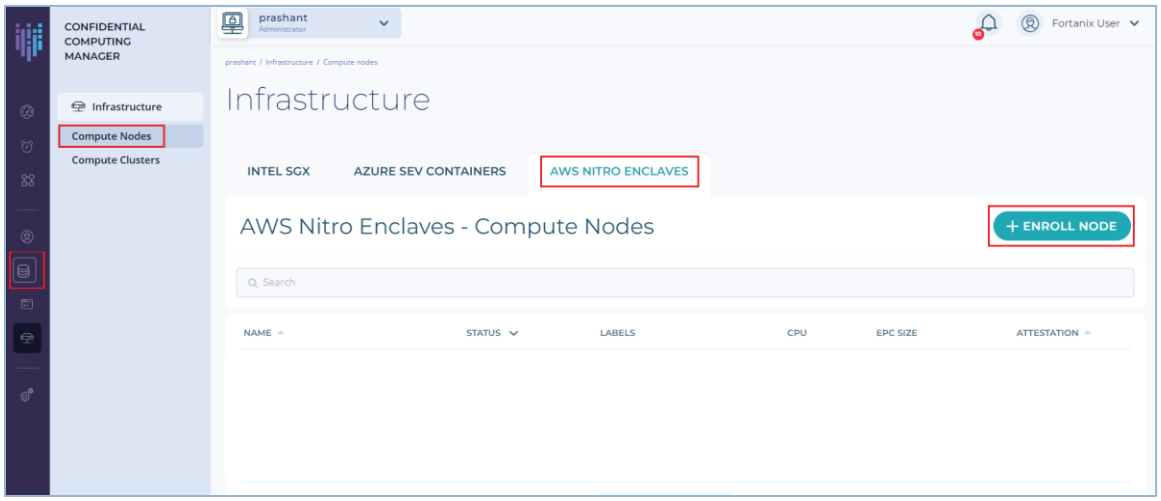


FIGURE 9: ENROLL COMPUTE NODE

3. Click the **COPY** button to copy the Join Token. This Join Token is used by the compute node to authenticate itself.

FIGURE 10: GENERATE TOKEN

4. In the **Create Fortanix Confidential Computing Node Agent** form, fill all the necessary.
5. Click the **Submit** button.

The compute node is now successfully created.

4.0 REVIEWING THE COMPUTE NODE

After the node agent is created, the node will be enrolled in CCM, you will see it under the **Compute Nodes** overview table.

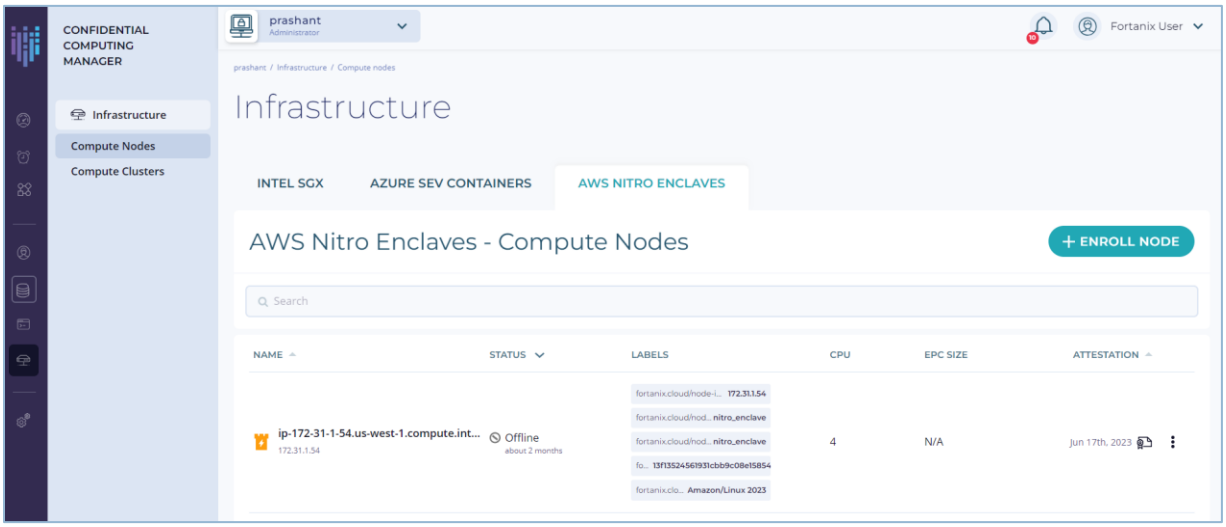


FIGURE 11: ENROLLED NODE

The following are the components on the screen:

- **Name:** Represents the DNS name of the compute node.
- **Status:** Indicates the current state of the compute node, such as active, inactive, online or offline.
- **Labels:** Contains descriptive tags for each compute node. Labels are used to provide additional information or group similar items together for organizational purposes.
- **CPU:** Displays information related to the Central Processing Unit (CPU) of the corresponding item. This information may include details such as the CPU type, usage, or other relevant metrics.
- **EPC Size:** Specifies the size or capacity of the Enclave Page Cache (EPC) associated with the item. However, this is not applicable for AWS Nitro Enclaves instances.
- **Attestation:** Provides information about the attestation status of the compute node. The validity of the compute node certificate is one year.
    - Click the ⋮ icon to perform the following actions:
        - **View Certificate:** View the details of the certificate associated with the compute node. You can also click icon to directly view the NITRO_ENCLAVE certificate.
        - **Copy Compute Node ID:** Copy the unique identifier (ID) of the compute node to the clipboard, facilitating easy reference in configurations or troubleshooting.

- **Delist Compute Node:** Remove the compute node from an active or trusted nodes list. This action may revoke the node's access or privileges within the Fortanix environment.

5.0 REFERENCES

Refer to the following documents for more details:

- *https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html#nitro-enclave-considerations*
- *https://support.fortanix.com/hc/en-us/articles/4412575587732-Fortanix-Node-Agent-Software-AWS-Nitro-Platform*

NOTE: *Refer to https://support.fortanix.com/hc/en-us/articles/4414195448980-User-s-Guide-Enroll-a-Compute-Node-Using-AWS-Nitro-on-Amazon-Linux to know the manual steps for installing the Fortanix Nitro Node Agent on a pre-created EC2 instance.*

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/18093708125460-User-s-Guide-Provision-a-Compute-Nodes-Using-AWS-Marketplace

6.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com