Fortanix®

User Guide

FORTANIX CONFIDENTIAL COMPUTING MANAGER – ENROLL COMPUTE NODES USING AWS NITRO ON AMAZON LINUX

VERSION 4.0

TABLE OF CONTENTS

1.0   INTRODUCTION

Welcome to the Fortanix Confidential Computing Manager (CCM) User Guide. This document describes how to enroll a compute node using AWS Nitro on Amazon Linux.

2.0   ENROLL NODE USING AWS NITRO ON AMAZON LINUX

2.1   SETTING UP THE ENVIRONMENT

1. Create a new VM:

    a. Select **Amazon Linux 2 Machine Image (AMI):**
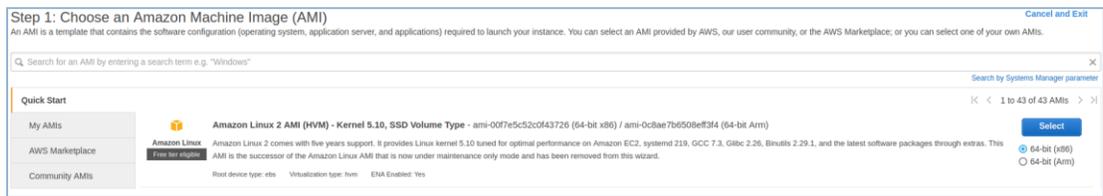
FIGURE 1: SELECT AMI

    b. Select **Instance Type:** Choose an adequate instance. The `c5a.xlarge` type is the minimum option that supports Nitro enclaves (see

https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html#nitro-enclave-reqs)

FIGURE 2: INSTANCE TYPE

    c. Click **Configure Instance** and enable enclave support (**Advanced Details**: **Enclave**).
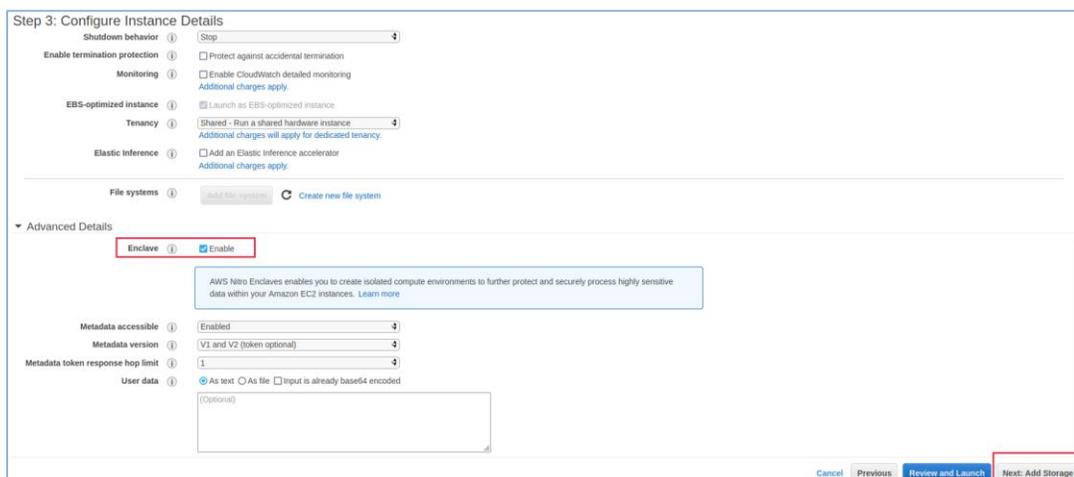
FIGURE 3: CONFIGURE INSTANCE

d.   Click **Add Storage:** The default storage is 8GiB. Increase the storage to a reasonable value.

e.   Optional: Add **Inbound ports** under Security Group to connect to the VM to install the node agent and launch the Nitro containers. You can use port 22 (for SSH) or any out-of-band mechanism to connect to the VM. You can also add any additional port required by the application.

f.   Configure the rest of the parameters as needed and launch the enclave.

2.   Install Nitro Driver and Utilities: Follow the instructions in

https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave-cli-install.html

2.2   INSTALLING NITRO NODE AGENT

1.   Obtain the join token from Fortanix CCM. To generate your Join Token, log in to https://ccm.fortanix.com/.

2.   Click the **Infrastructure → Compute Nodes** menu item in the CCM UI left navigation bar and click the **+ENROLL NODE** on the Compute Nodes page.

3.   In the **ENROLL NODE** window, a Join Token will be generated in the text box for "**Get a join token to register an SGX compute node**". This Join Token is used by the compute node to authenticate itself.

FIGURE 4: COPY JOIN TOKEN

4. Click **Copy** to copy the Join Token (**Figure 4**).

5. Download the *Amazon Nitro node agent installer*.

6. Extract the contents of the package and open the folder.

7. Open the readme file which contains the steps to enroll the compute node in Fortanix CCM.

8. To enroll the compute node:

    a. Copy the file `installer.sh` to your VM.

    b. Run the `installer.sh` with the join token copied in *Step 3*. This will enroll the compute node in Fortanix CCM.

    ```
    sudo bash ./installer.sh <join-token>
    ```

9. After the compute node is enrolled in Fortanix CCM, you will see it under the Compute Nodes overview table.
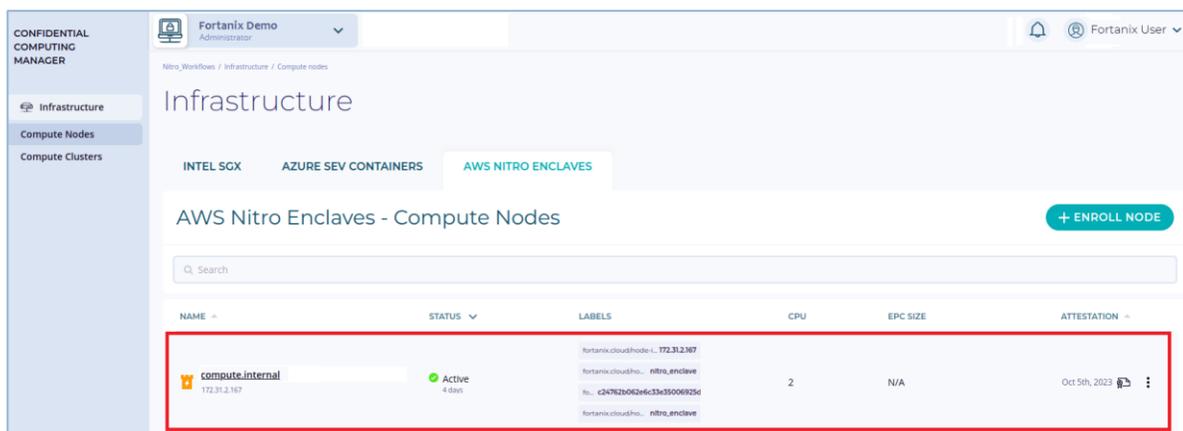
FIGURE 5: NODE ENROLLED

10. Debug:

    a. To view the logs, run the following command:

    ```
    journalctl -xe | grep em-agent
    ```

    b. To view the status, run the following command:

    ```
    systemctl status em-agent-nitro
    ```

3.0 DOCUMENT INFORMATION

3.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/4414195448980-User-s-Guide-Enroll-a-Compute-Node-Using-AWS-Nitro-on-Amazon-Linux

3.2 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

Confidential