Fortanix[®]

User Guide

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

VERSION 4.0

TABLE OF CONTENTS

1.0		2
2.0	ENROLL NODE USING AWS NITRO ON AMAZON LINUX	2
2.1	Setting Up the Environment	2
2.2	Installing Nitro Node Agent	3
3.0	DOCUMENT INFORMATION	6
3.1	Document Location	6
3.2	Document Updates	6

Fortanix[®] ENROLL COMPUTE NODES USING AWS NITRO ON AMAZON LINUX

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):

Step 1: Choose an An AMI is a template that contain	Amazon Machine Image (AMI) is the software configuration (openating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Markeplace; or you can select one of your own A	Cancel and Exit AMIs.
Q. Search for an AMI by entering	ng a search term e.g. "Windows"	×
	Search by System	ems Manager parameter
Quick Start	K < 11043	3 of 43 AMIs \rightarrow >
My AMIs	Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-007/85c52c0f43726 (64-bit x86) / ami-0c8ae7b6508ef834 (64-bit Arm)	Select
AWS Marketplace	Amazon Linux Amazon Linux 2 comes with five years support. It provides Linux kernels 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Bizulis 2.29 1, and the latest software packages through extras. This grows the macro Linux AMI that is now under maintenance only mode and has been removed from this wizard.	64-bit (x86)
Community AMIs	Root device type: ets Virtualization type: hom ENA Enabled: Yes	



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-regs)

St Am res	Step 2: Choose an Instance Type Amazon EC2 provides a web selection of instance types and how they can meet your computing needs. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn mere addo instance types and how they can meet your computing needs.												
Filter by: Cda v Current generation v Showhide Columns													
с	Currently selected: c5a.xlarge (- ECUs, 4 vCPUs, 3.3 GHz, -, 8 GiB memory, EBS only)												
	Family - Type - VCPUs () - Memory (GB) - Instance Storage (GB) () - EBS-Optimized Available () - Network Performance () - Privé Support ()												
E	c5a	c5a.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes					
	c5a	c5a.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes					
0	c5a	c5a.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes					
C5a C5a.6darge 16 22 EBS only Yes Up to 10 Gigabit							Up to 10 Gigabit	Yes					
0	c5a	c5a.8xlarge	32	64	EBS only	Yes	10 Gigabit	Yes					
0	c5a	c5a.12xlarge	48	96	EBS only	Yes	12 Gigabit	Yes					
	c5a	c5a.16xlarge	64	128	EBS only	Yes	20 Gigabit	Yes					
	c5a	c5a.24xlarge	96	192	EBS only	Yes	20 Gigabit	Yes					



c. Click Configure Instance and enable enclave support (Advanced Details: Enclave).



ENROLL COMPUTE NODES USING AWS NITRO ON AMAZON LINUX

Step 3: Configure Instan	ce D	etails												
Shutdown behavior	0	Stop	4											
Enable termination protection	۲	Protect against accidental termination												
Monitoring	۲	Enable CloudWatch detailed monitoring Additional charges apply.												
EBS-optimized instance	٢	Launch as EBS-optimized instance												
Tenancy	•	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenar	4) ncy.											
Elastic Inference	٢	Add an Elastic Inference accelerator Additional charges apply.												
File systems	•	add the system C Create new file syst	em											
Enclave	١	Enable AWS Nitro Enclaves enables you to create is data within your Amazon EC2 instrument and	olated con	ute environment	ts to further p	protect and	securely pr	ocess highly	sensitive					
Metadata accessible	æ	Enabled	3											
Metadata version	(1)	V1 and V2 (token optional)	4											
Metadata token response hop limit	Ð	1	4											
User data	1	● As text () As file [] Input is already base64	encoded											
		(Optional)			4									
											Cancel	Previous	Review and Launch	Next: Add Stora

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



ENROLL COMPUTE NODE	×
Get a join token to register a compute node	
•••••	
COPY DOWNLOAD Please download or copy the token. For the next steps, please refer to the detailed process documented on our support portal.	

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.



ENROLL COMPUTE NODES USING AWS NITRO ON AMAZON LINUX

CONFIDENTIAL	Fortanix Demo					
MANAGER	Nitro_Workflows / Infrastructure / Compute nodes					
	Infrastructure					
Compute Nodes						
Compute Clusters	INTEL SGX AZURE SEV CONTAINER	AWS NITRO ENCL	AVES			
	AWS Nitro Enclaves - Co	ompute Nodes				+ ENROLL NODE
	Q. Search					
	NAME 🗠	STATUS 🗸	LABELS	СРИ	EPC SIZE	
	Compute.internal	Active	fortanik.cloudihodeiL_172.312.307 fortanik.cloudiho Nitro.encleve fo c24762b062e6c33e35006925d fortanik.cloudiho Nitro.encleve	2	N/A	Oct 5th, 2023 🖗 🗄 🚦

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

Fortanix[®] ENROLL COMPUTE NODES USING AWS NITRO ON AMAZON LINUX

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

© 2016 – 2023 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc. All other trademarks are the property of their respective owners.

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform <u>info@fortanix.com</u> immediately.