napatech

Software Installation Guide

SmartNIC

# Getting started with Napatech FPGA Cloud Crypto

Use this information to launch Napatech FPGA-based cloud cryptography on AWS and use the step-by-step guide to run AES encryption in the cloud.

DN-1170 Rev. 2

# Contents

# Modification history

This document has been updated as follows:

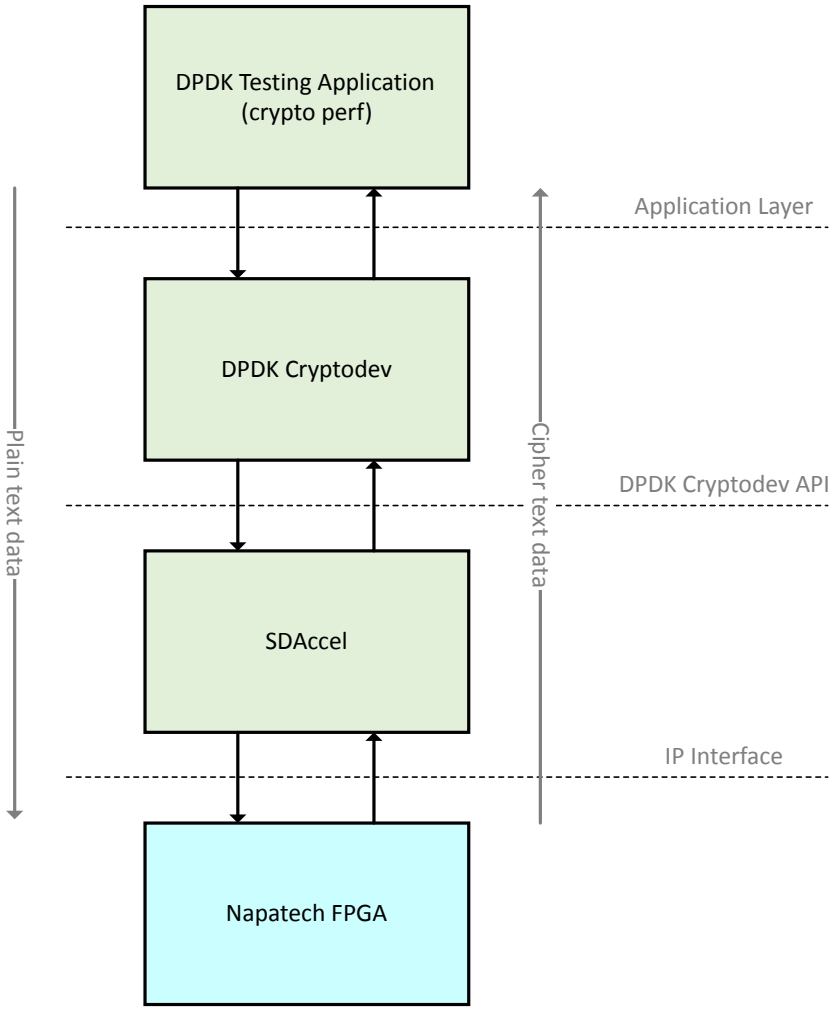
| Rev. | Date | Comment |
|---|---|---|
| 1 | 2018-10-31 | First version. |
| 2 | 2019-03-14 | Updates to sample: Run the FPGA Cloud Crypto sample on page 9 |

# 1 Introduction

Use this guide to get you up and running with Napatech FPGA Cloud Crypto on Amazon Elastic Compute Cloud (Amazon EC2).

Napatech FPGA Cloud Crypto provides cloud-based encryption and decryption. The solution uses the DPDK Cryptodev API to encrypt and decrypt all data using AES-GCM.

The sample uses a Cryptodev application (DPDK crypto perf) to send data through the DPDK Cryptodev API to the Napatech FPGA, controlled by the SDAccel Xilinx Development Environment. The sample runs within one EC2 F1 instance.




For background information about Amazon EC2, see the AWS online documentation at: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html.

# 2 Create an AWS account

Create an Amazon Web Services account, if you don't have an account already.

Context

| Step | Action |
|---|---|
| 1 | Follow the Amazon instructions on creating an account from its homepage: https://aws.amazon.com/. |

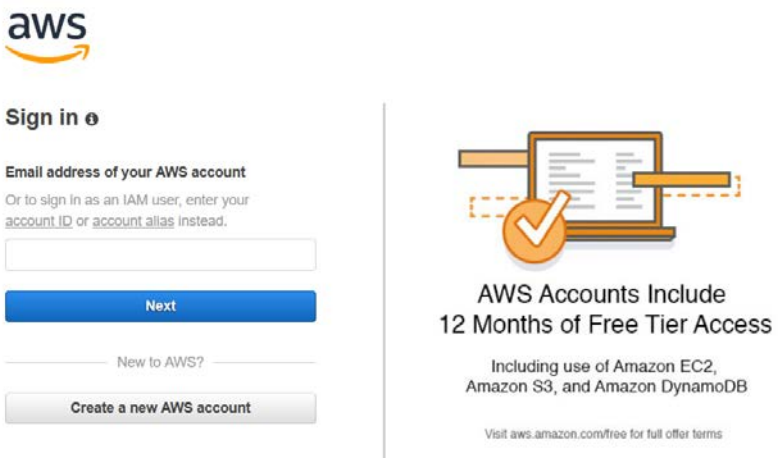
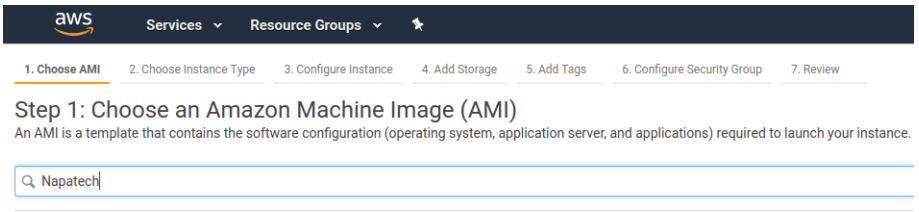

**Note:** When you create an account you are asked for credit card information, but you will not be charged initially. Amazon will only charge you based on your actual use of paid services.

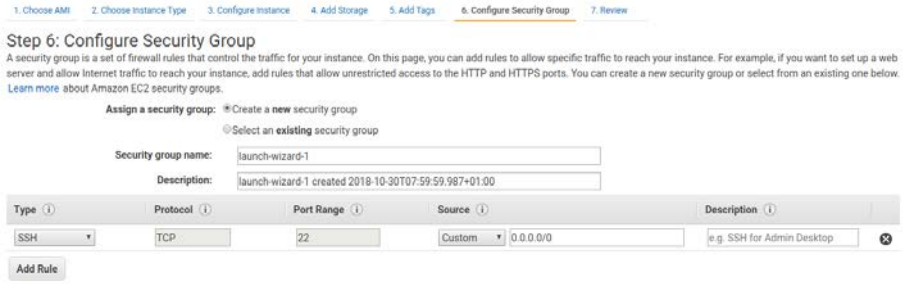
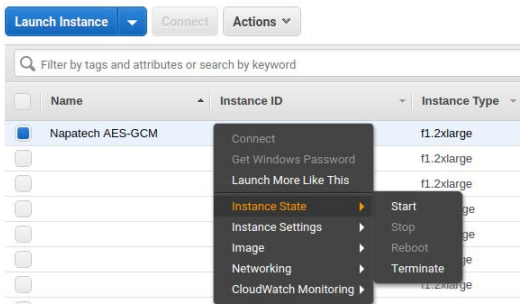
# 3 Setup the Amazon Machine Image (AMI)

Launch an EC2 instance from the AWS Console, and select and configure the Napatech Amazon Machine Image (AMI).

Context

For background information on launching an Amazon EC2 instance, see the Amazon documentation here: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html.

| Step | Action |
|---|---|
| 1 | From a web browser, log on to the AWS Console: https://console.aws.amazon.com/console.<br>  |
| 2 | When you are logged in, from **AWS services**, click **Services** from the toolbar, and **EC2** from **All services** > **Compute**.<br>The **EC2 Dashboard** opens. |
| 3 | Click **Launch Instance** to start a new instance.<br>**Step 1: Choose an Amazon Machine Image (AMI)** opens. |
| 4 | Select **AWS Marketplace** from the menu and enter `Napatech` in the search field.<br>  |
| 5 | Click **Select** to choose the Napatech AMI.<br>**Note:** If you have already set up an AMI, you can click **Continue** to start the AMI that you configured previously. |
| 6 | Scroll to the FPGA instances, and select **f1.2xlarge**.<br>**Note:** **f1.2xlarge** is the smallest FPGA instance, and you do not need anything larger. |

| Step | Action |
|---|---|
| 7 | Click through **Next: Configure Instance Details**, **Next: Add Storage**, **Next: Add Tags**.<br>There is nothing for you to configure on these pages. |
| 8 | Click **Next: Configure Security Group**. Create a new (or use an existing) security group and configure an IP address that can access the instance.<br>This allows access to the instance. Use Port 22 for the **Port Range**:<br>  |
| 9 | Click **Review and Launch**, and then select or create an SSH key pair, to allow access to the instance.<br>The instance will now start up. |
| 10 | When the instance has started, note down the value in **Public DNS (IPv4)**, as you will need this information to access and run the instance.<br>If the instance is powered down, right click the instance for options to restart it:<br>  |

Result

The Napatech FPGA Cloud Crypto instance is launched and you are ready to run the sample.

# 4 Run the FPGA Cloud Crypto sample

The sample application encrypts data using the Napatech FPGA, offloading processing to the cloud.

Prerequisite

Make sure that you have the Public IP address of the instance (see Launch the instance).

Context

You can find instructions on how to run the sample on the AMI at: `/home/centos/readme.md`.

The sample uses a Cryptodev application (DPDK crypto perf) to send data through the DPDK Cryptodev API to the Napatech FPGA, controlled by the SDAccel Xilinx Development Environment. The sample runs within one EC2 F1 instance.

The results returned confirm that the traffic was encrypted and transmitted successfully.

| Step | Action |
|---|---|
| 1 | Log in to the Napatech instance using the **Public DNS (IPv4)** of the instance, in the format:<br>`-ssh centos@<Public_IP_address> -i . ssh/<public_key>.pem`<br>where `<Public_IP_address>` is the instance public IP address, and `<public_key>` is the public key that allows access to the instance. For example:<br>`-ssh centos@10.10.10.10 -i . ssh/key.pem` |
| 2 | If this is the first time you are running the sample application, install the runtime:<br>`sudo su`<br>`source /opt/runtime_install.sh`<br>The script can take around five minutes to complete, and you might see no progress at intervals. You will see an Installation successful message when the script has completed.<br>**Note:** You only need to run this script the first time you use the sample. |
| 3 | Run the setup script:<br>`sudo su`<br>`source /opt/runtime_setup.sh` |
| 4 | Run the sample:<br>`cd /opt/dpdk/x86_64-native-linuxapp-gcc/app`<br>`./dpdk-test-crypto-perf -l 0-1 --vdev crypto_napatech -w 0000:00:00.0 -- --devtype crypto_napatech --aead-algo aes-gcm --aead-key-sz 16 --aead-iv-sz 16 --aead-op encrypt --aead-aad-sz 16 --digest-sz 16 --optype aead --silent --ptest throughput --total-ops 100 --buffer-sz 128000`<br>**Note:** You can edit the number of buffers to be encrypted using the `--total-ops` flag. The larger the number of buffers, the greater the performance and reduction in overhead. You can also edit `--buffer-sz`, which specifies the amount of data you want to encrypt. |

Result

When you run the sample, the final entry is a table of results that includes listings for buffer size, burst size, Gbps, and cycles per buffer. In this example, the number of buffers to be encrypted is set at 1000 (`--total-ops`) and the buffer size is 64 bytes (`--buffer-sz`):

```
sh-4.2# sudo -E LD_LIBRARY_PATH=/home/centos/lib:${LD_LIBRARY_PATH} ./dpdk-test-crypto-perf -l 0-1 --vdev crypto_napatech -w 0000:00:00.0 -- --devtype crypto_napatech --aead-algo a
es-gcm --aead-key-sz 16 --aead-iv-sz 16 --aead-op encrypt --aead-aad-sz 16 --digest-sz 16 --optype aead --silent --ptest throughput --total-ops 1000 --buffer-sz 64
EAL: Detected 8 lcore(s)
EAL: Detected 1 NUMA nodes
EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
EAL: No free hugepages reported in hugepages-1048576kB
EAL: Probing VFIO support...
CRYPTODEV: [crypto_napatech] - Creating cryptodev crypto_napatech

CRYPTODEV: [crypto_napatech] - Initialisation parameters - name: crypto_napatech,socket id: 0, max queue pairs: 8, max sessions: 2048
xclProbe found 0 FPGA slots with xocl driver running
[0]user:0xf000:0x1d51:[xocl:2017.4.5:128]
xclProbe found 1 FPGA slots with xocl driver running
Found Platform
Platform Name: Xilinx
XCLBIN File Name: aes_gcm
INFO: Importing ./aes_gcm.hw.xilinx_aws-vu9p-f1_dynamic_5_0.awsxclbin
Loading: './aes_gcm.hw.xilinx_aws-vu9p-f1_dynamic_5_0.awsxclbin'
AFI not yet loaded, proceed to download.
AFI load complete.
Allocated session pool on socket 0
    lcore id    Buf Size  Burst Size    Enqueued    Dequeued  Failed Enq  Failed Deq        MOps        Gbps  Cycles/Buf

           1          64          32        1000        1000           0      331913      0.0060      0.0031   380493.76

WARNING: Profiling may contain incomplete information. Please ensure all OpenCL objects are released by your host code (e.g., clReleaseProgram()).
sh-4.2#
```

This output shows that the data has been encrypted as expected.

# 5 Additional resources

Use these links to find out more about Napatech FPGA Cloud Crypto.

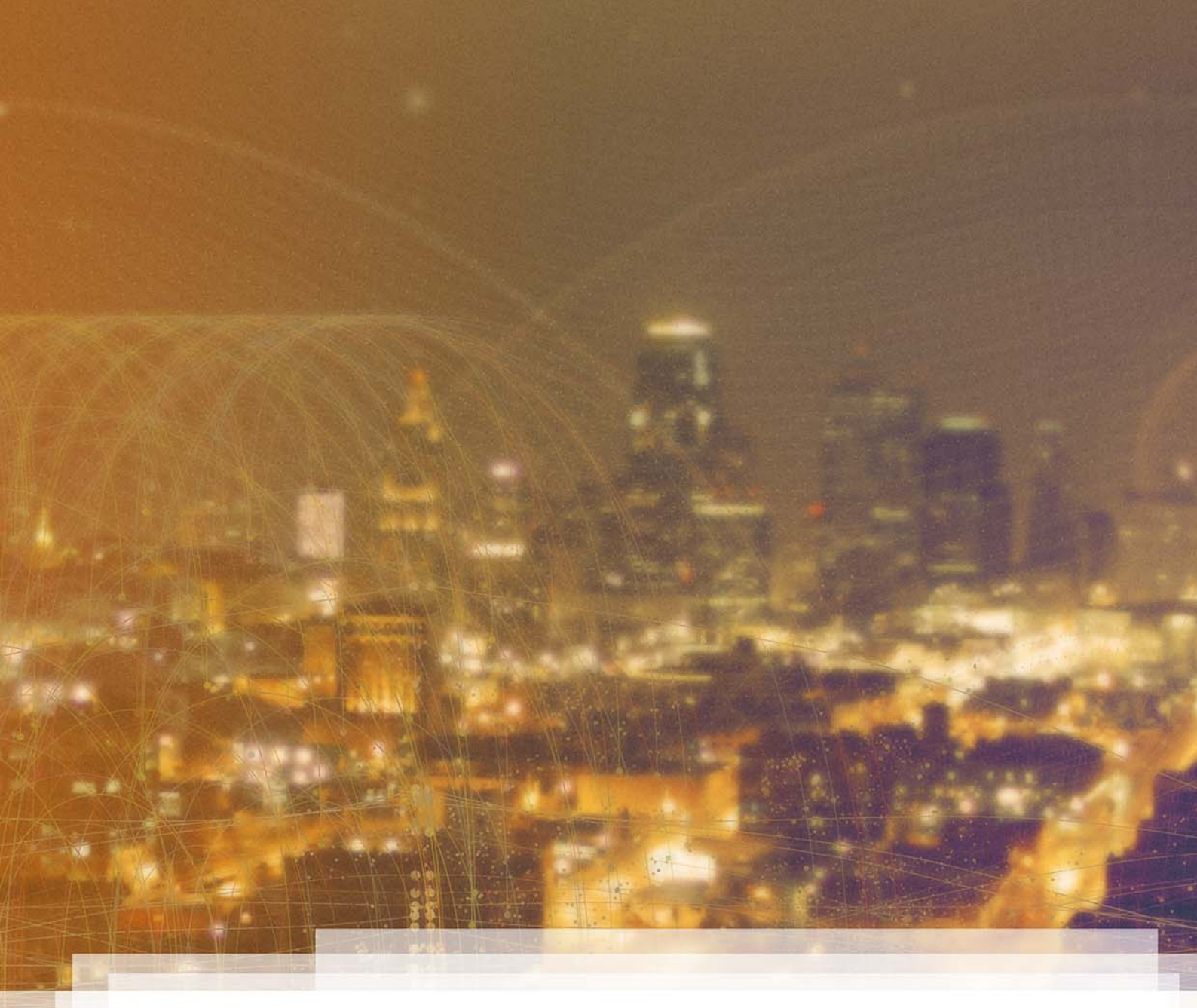
Context

Napatech on AWS Marketplace: Napatech FPGA Cloud Crypto

Napatech website: Napatech website

Napatech Support: support@napatech.com

AMI information: `/home/centos/readme.md`



# Back Matter

The back matter contains these sections:

# Index