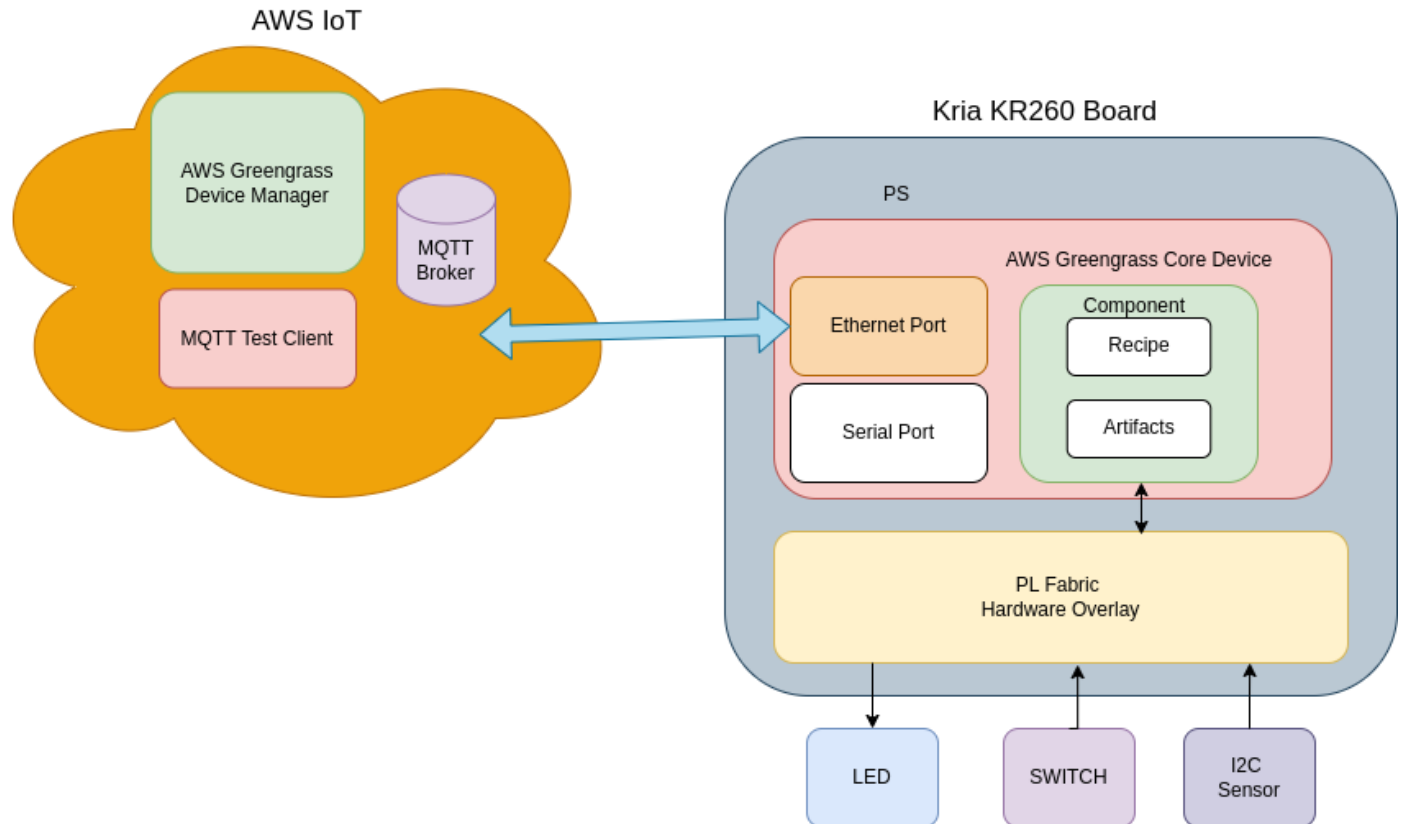


KR260 to AWS IoT Greengrass Architecture



This diagram shows the software and hardware architecture used in this tutorial. Kria KR260 board consists of PL Fabric(FPGA) hardware overlay for interfacing LED, switch and I2C sensor. Further it runs AWS Greengrass Core Device Application which publish and subscribe message topics for actuating LED and monitoring sensors and switches. From AWS IoT MQTT Test Client KR260 LED will be controlled through subscribed topic and also publish Switch pressed event to AWS IoT cloud.

Creating Petalinux Project

Create Petalinux from BSP

In host machine, create the petalinux project using provided BSP:

BSP feature:

- Petalinux version 2022.2
- Added meta-aws layer for installing required dependencies required for running greengrass core device in KR260
- Rootfs packages : packagegroup-buildessential, git, libgpiod, libgpiod-dev, libgpiod-tools
- Enabled FPGA-manager

Run following commands to create petalinux project:

```
petalinux-create -t project -s xilinx-kr260-starterkit-aws-iot.bsp -n kr260-aws-iot
cd kr260-aws-iot
```

Here “kr260-aws-iot” is the directory created by petalinux-create command, you can change the name according to your need. This directory is the petalinux-project base directory, which we will be using in further steps.

Next build the project after sourcing the Petalinux 2022.2 environment:

```
source <Path to Petalinux 2022.2>/settings.sh
petalinux-config --silentconfig
petalinux-build
```

Here is the console log after running the petalinux-build.

```
sanam@sanam-tytton: ~/kr260-p2022-2-default$ petalinux-build
[INFO] Sourcing buildtools
[INFO] Building project
[INFO] Sourcing build environment
[INFO] Generating workspace directory
INFO: Stbake petalinux-image-minimal
NOTE: Started PRServer with DBfile: /media/sanam/workspace2/sanam/kr260-p2022-2-default/build/cache/prserv.sqlite3, Address: 127.0.0.1:46633, PID: 558748
loading cache: 100% | ETA: --:--:--
loaded 0 entries from dependency cache.
Parsing recipes: 100% | ETA: 0:02:02
Parsing of 4532 .bb files complete (0 cached, 4532 parsed), 6025 targets, 620 skipped, 1 masked, 0 errors.
NOTE: Resolving any missing task queue dependencies
initializing tasks: 100% | ETA: 0:00:28
Checking state error object availability: 100% | ETA: 0:00:39
state summary: wanted 100% Local 29 Network 653 Missed 404 Current 2726 (62% match, 89% complete)
moving 2 state objects for arch xilinx_k26_kr: 100% | ETA: 0:00:00
NOTE: Executing tasks
NOTE: Tasks Summary: Attempted 9498 tasks of which 9481 didn't need to be rerun and all succeeded.
INFO: Failed to copy built images to tftp dir: /tftpboot
[INFO] Successfully built project
sanam@sanam-tytton: ~/kr260-p2022-2-default$
```

Next create the SD card image with the following commands:

```
petalinux-package --boot --u-boot --force
petalinux-package --wic --images-dir images/linux/ --bootfiles
"ramdisk.cpio.gz,u-boot,boot.scr,Image,system.dtb,system-zynqmp-sck-kr-g-revB.dtb"
--disk-name "sda"
```

This will create the petalinux-sdimage.wic image at <petalinux project directory>/image/linux folder. Copy the created wic image to SD card using tools like Balena Etcher.

Installing hardware overlay

After booting the previously used SD card into KR260.
Login to KR260 serial terminal using login name: petalinux
For the first login one has to update the new password.

```
xilinx-kr260-starterkit-20222 login: petalinux
You are required to change your password immediately (administrator enforced).
New password:
Retype new password:
xilinx-kr260-starterkit-20222:~$
```

Next copy the KR260 firmwares to KR260 using network tools like scp or manually copying the firmware files at /home/petalinux directory of SD card.

Get the KR260 firmware folder. It contains:

- kr260_i2c.bit.bin
- kr260_i2c.dtbo
- shell.json

Copy these file to the KR260 board. For firmware to be loaded using xmutil (FPGA manager), one has to copy these file at "/lib/firmware/xilinx".

For this, create the folder at "kr260-i2c" at "/lib/firmware/xilinx" and copy the files in "kr260-i2c" folder.

```
cd /lib/firmware/xilinx
sudo mkdir kr260-i2c
sudo cp <kr260-firmware directory>/kr260_i2c* ./
sudo cp <kr260-firmware directory>/shell.json ./
```

Next, check the available fpga firmware using `xmutil listapps` command. `kr260-i2c` will be available in the list.

```
xilinx-kr260-starterkit-20222:~$ sudo xmutil listapps
Accelerator      Accel_type      Base      Base_type      #slots(PL+AIE)      Active_slot
k26-starter-kits XRT_FLAT        k26-starter-kits XRT_FLAT        (0+0)                0,
kr260-i2c        XRT_FLAT        kr260-i2c      XRT_FLAT        (0+0)                -1
xilinx-kr260-starterkit-20222:~$
```

Next load the `kr260-i2c` firmware, which contains necessary hardwares(gpio) and interfaces. In our Greengrass Demo, we will be using these gpio to trigger the publishing data to AWS Greengrass IoT cloud server and also actuate GPIO on the message received from AWS cloud.

```
sudo xmutil unloadapp
sudo xmutil loadapp kr260-i2c
```

```
xilinx-kr260-starterkit-20222:~$ sudo xutil loadapp kr260-i2c
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /fpga-full/firmware-name
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /fpga-full/pid
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /fpga-full/resets
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /fpga-full/uid
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/overlay0
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/overlay1
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/afi0
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/clocking0
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/clocking1
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/overlay2
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/axi_gpio_0
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/misc_clk_0
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/misc_clk_1
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/axi_iic_0
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/axi_iic_1
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/axi_intc_0
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: OF: overlay: WARNING: memory leak will occur if overlay removed, property: /_symbols_/axi_intc_1
Nov 19 09:35:53 xilinx-kr260-starterkit-20222 kernel: irq: type mismatch, failed to map hwirq-0 for interrupt-controller@80000000!
kr260-i2c: loaded to slot 0
xilinx-kr260-starterkit-20222:~$
```

Now to access GPIO in user application, we will be using `gpiod` library.

Installing gpiod python modules

GPIOD packages are required to access the GPIO channels. It also provides python binding for accessing GPIO in python programming. Install the gpiod python modules:

```
sudo pip3 install gpiod
```

Now we can check the available gpio using gpiod applications:

Using `gpiodetect` to get available gpio:

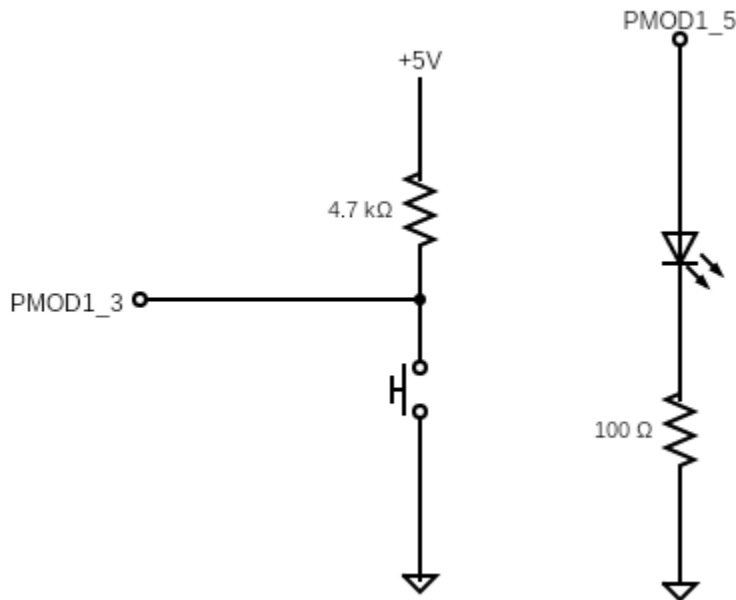
```
xilinx-kr260-starterkit-20222:~$ sudo gpiodetect
gpiochip0 [firmware:zynqmp-firmware:gpio] (4 lines)
gpiochip1 [zynqmp_gpio] (174 lines)
gpiochip2 [slg7xl45106] (8 lines)
gpiochip3 [80010000.gpio] (6 lines)
xilinx-kr260-starterkit-20222:~$
```

Here `gpiochip3` is the device corresponding to gpio in FPGA and it consists of 6 lines. Further these gpio lines are connected to PMOD 1 such that:

PMOD1-> 1 - gpiochip3 line 0

PMOD1-> 3 - gpiochip3 line 1

PMOD1-> 5 - gpiochip3 line 2



Schematic for LED and Switch Connection

11	9	7	5	3	1	PMOD UPPER
12	10	8	6	4	2	PMOD LOWER
V _{CC}	GND	I/O	I/O	I/O	I/O	

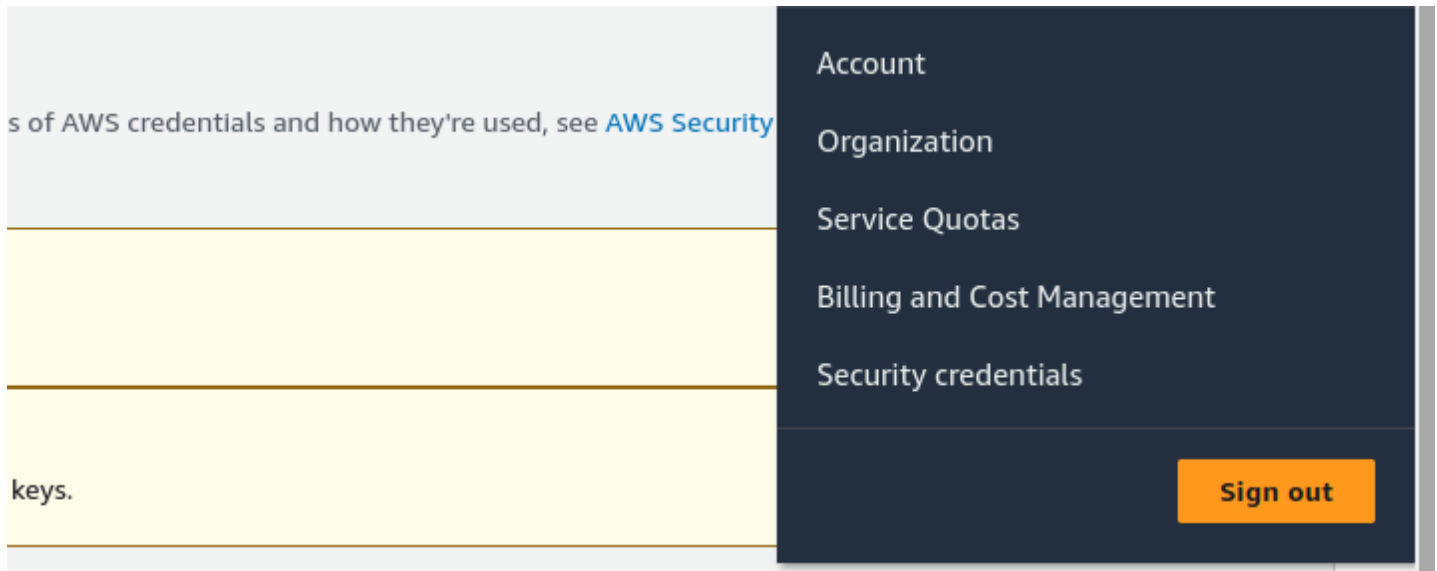
PMOD port numbering

We will be using these gpios while creating component of Greengrass AWS core device in KR260.

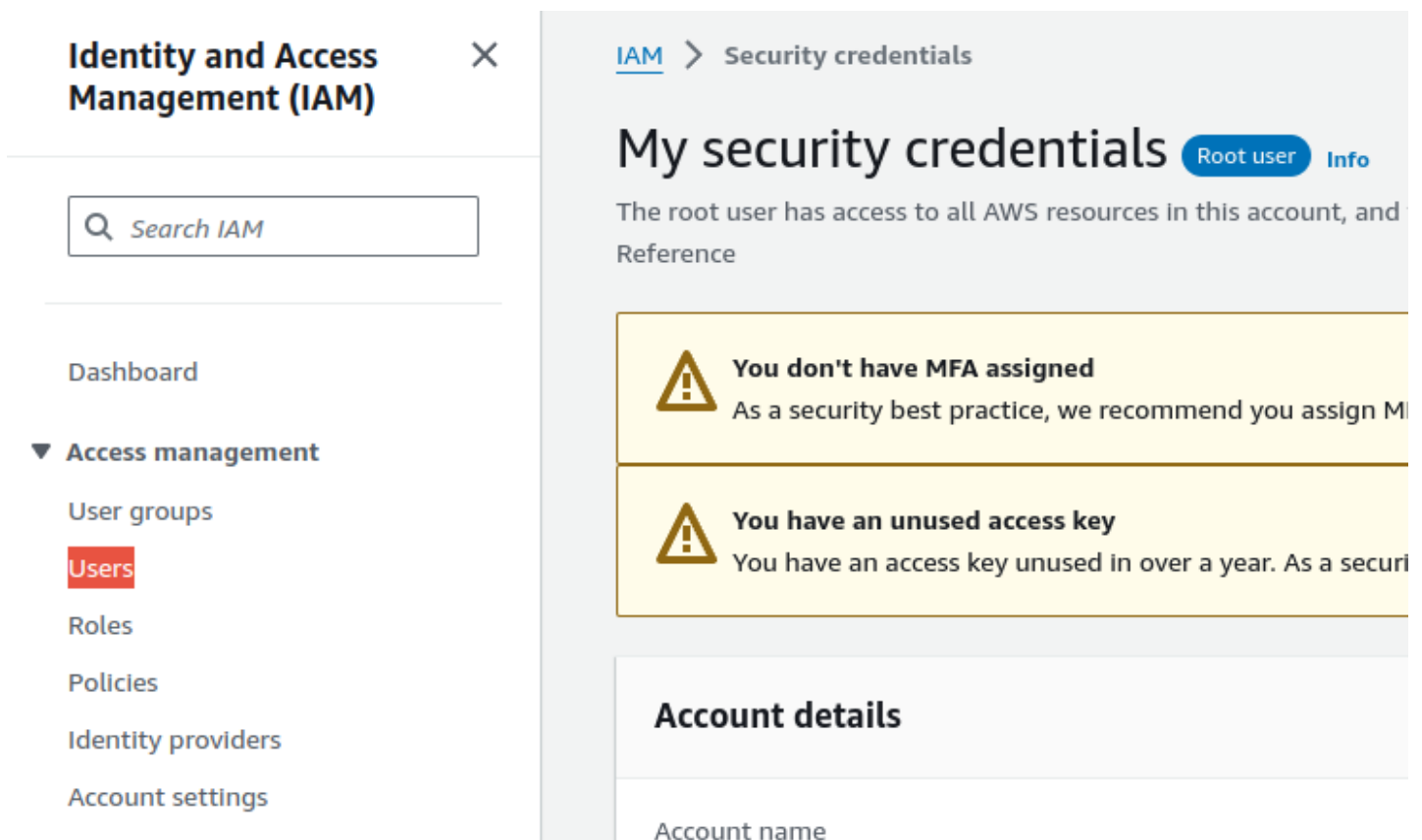
AWS IoT user creation

For an non human access to AWS services one has to create a user with required permissions. Follow following steps to create the user for IoT end devices.

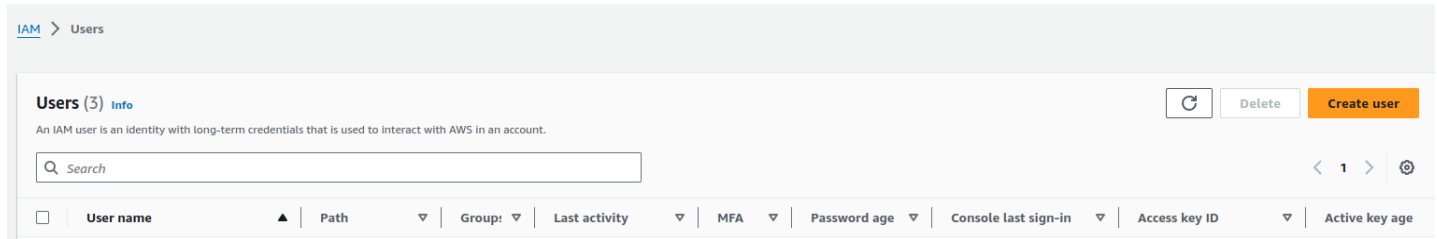
- Login to AWS console
- Next go to `Security credentials` link available at root user drop down at top right corner of the AWS console



- Next Go to User management page by clicking at the User link at IAM sidebar. This will list the available users.



- Now create a new user for KR260 device by clicking the "Create User" button.

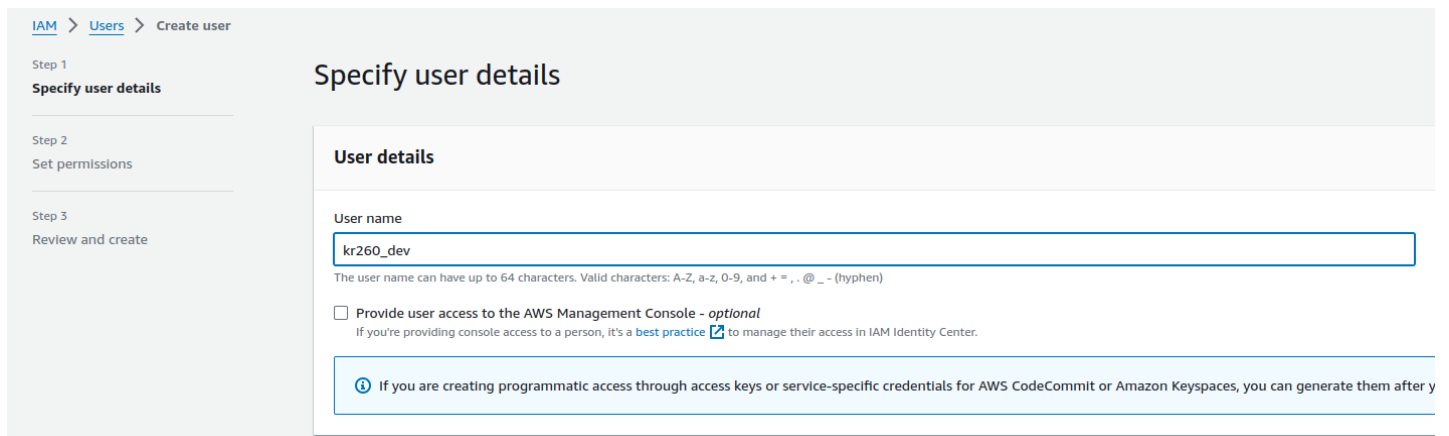


The screenshot shows the AWS IAM console 'Users' page. At the top, there's a breadcrumb 'IAM > Users'. Below it, a header shows 'Users (3)' with an 'Info' link. A description states: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' There are buttons for 'Refresh', 'Delete', and 'Create user'. A search bar is present. Below the search bar is a table with columns: 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', 'Access key ID', and 'Active key age'. The table is currently empty.

This will lead to step wise User creation forms. So fill the User details,

This will lead to step wise User creation forms.

So fill the User details, leave the console access unchecked as user does not have to access the AWS console through web.



The screenshot shows the 'Specify user details' form in the AWS IAM console. The breadcrumb is 'IAM > Users > Create user'. On the left, there's a sidebar with 'Step 1: Specify user details' (active), 'Step 2: Set permissions', and 'Step 3: Review and create'. The main form area has a title 'Specify user details' and a section 'User details'. It contains a 'User name' field with the value 'kr260_dev'. Below the field, a note says: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)'. There is an unchecked checkbox labeled 'Provide user access to the AWS Management Console - optional' with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' At the bottom, there's a blue box with an information icon and text: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after y'.

Next, update the Permissions options by attaching following policies:

- AWSGreengrassFullAccess
- IAMFullAccess
- AWSIoTFullAccess
- AmazonS3FullAccess

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (3/1167)

Choose one or more policies to attach to your new user.



[Create policy](#)

Filter by Type

All types

1 match

< 1 > ⚙

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	AWSIoTFullAccess	AWS managed	1

► Set permissions boundary - optional

Cancel

Previous

Next

After finishing the above steps click "Create User" to finish the user creation.

[IAM](#) > Users

Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="checkbox"/>	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in
<input type="checkbox"/>	dev-user	/	0	✓ 2 days ago	-	-	-
<input type="checkbox"/>	kr260_dev	/	0	-	-	-	-

Permissions
Groups
Tags (1)
Security credentials
Access Advisor





Permissions policies (4)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

All types

< 1 > ⚙

<input type="checkbox"/>	Policy name ↗	Type
<input type="checkbox"/>	 AmazonS3FullAccess	AWS managed
<input type="checkbox"/>	 AWSGreengrassFullAccess	AWS managed
<input type="checkbox"/>	 AWSIoTFullAccess	AWS managed
<input type="checkbox"/>	 IAMFullAccess	AWS managed

Next get the access token and access key for the user. For this open the user details by clicking on the user link in the above table.

And go to "Security credentials" for creating the Access Key for the user.

Permissions
Groups
Tags
Security credentials
Access Advisor

Console sign-in

Select access key for command line based access control for user.

Use case



Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.



Local code

You plan to use this access key to enable application code in a local development environment to access your AWS account.



Application running on an AWS compute service

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.



Third-party service

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.



Application running outside AWS

You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.



Other

Your use case is not listed here.



Alternatives recommended

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

Confirmation



I understand the above recommendation and want to proceed to create an access key.

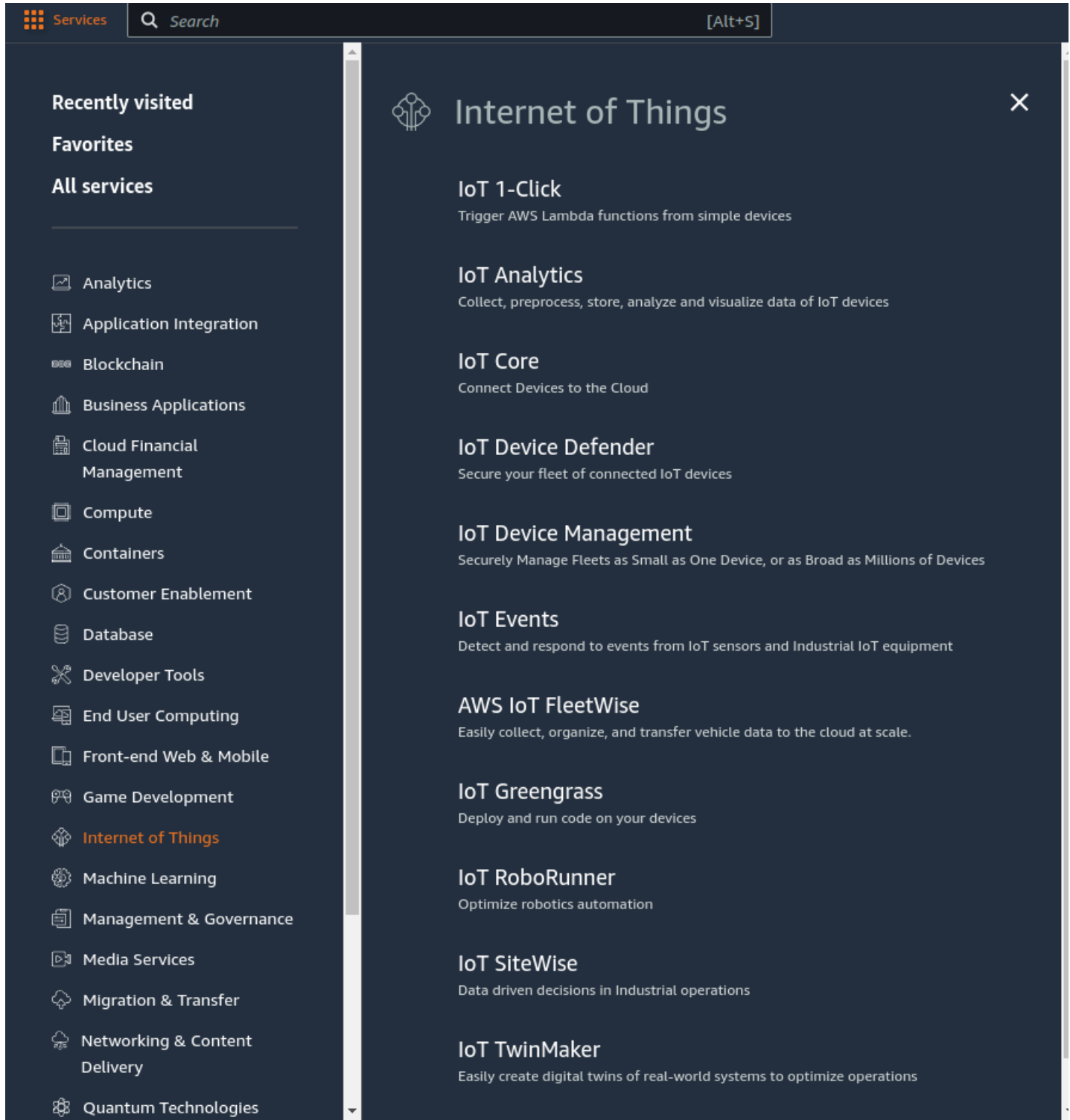
Cancel

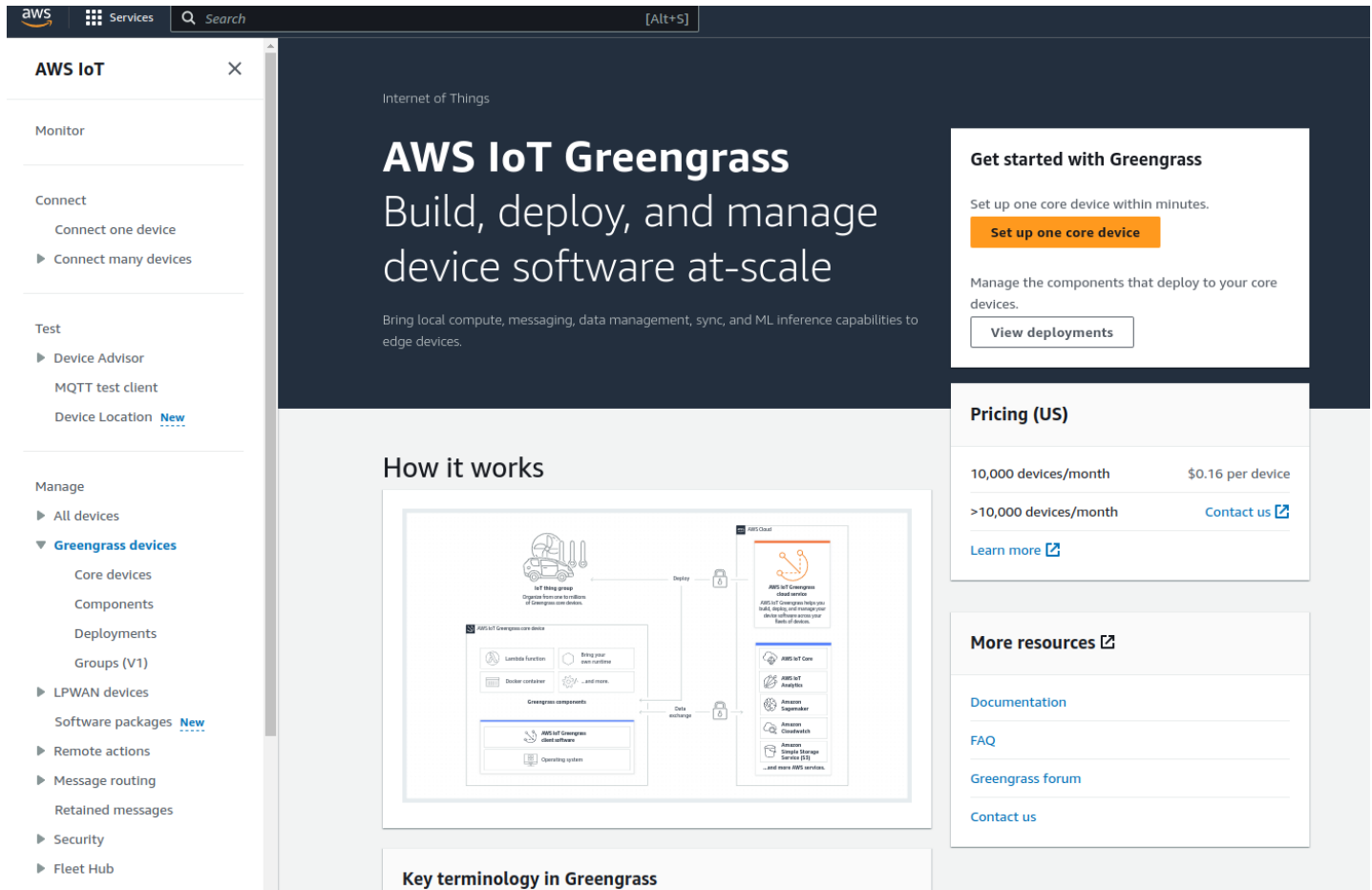
Next

Next save the "Access Key" and "Secret Access Key". We will need this later while using greengrass CLI in KR260 console or downloading the csv file.

Installing Greengrass CLI in KR260 board

Steps and scripts for installing greengrass device is provided by AWS Greengrass dashboard in AWS web console. So first access the AWS Greengrass IoT page, go to AWS Services -> Internet of Things -> IoT Greengrass link





Get started with Greengrass

Set up one core device within minutes.

[Set up one core device](#)

Manage the components that deploy to your core devices.

[View deployments](#)

Pricing (US)

10,000 devices/month	\$0.16 per device
>10,000 devices/month	Contact us

[Learn more](#)

More resources

- [Documentation](#)
- [FAQ](#)
- [Greengrass forum](#)
- [Contact us](#)

How it works

The diagram shows an IoT thing group (represented by a truck icon) sending data to an AWS IoT Greengrass core device. The core device then interacts with various AWS services (Lambda, S3, etc.) through a data exchange.

Key terminology in Greengrass

Now click on “Set up one core device” button

This will open the Greengrass core device setup page:

Here you can change the Core device name like `kr260-dev`

[AWS IoT](#) > [Greengrass](#) > [Core devices](#) > Set up one Greengrass core device

Set up one Greengrass core device

Step 1: Register a Greengrass core device

Greengrass core devices are AWS IoT things. Enter a thing name to be used to create a Greengrass core device.

Core device name

The name of the AWS IoT thing to create. We generated the following name for you.

kr260-peta-dev1

The name can be up to 128 characters. Valid characters: a-z, A-Z, 0-9, underscore (_), and hyphen (-).

Step 2: Add to a thing group to apply a continuous deployment

Add your Greengrass core device to an AWS IoT thing group. If the thing group has an active Greengrass deployment, your new core device receives and applies the deployment when you finish the setup process. To deploy to only the core device, select No group.

Thing group

- ☒ Enter a new group name
- ☐ Select an existing group
- ☐ No group

Thing group name

The name of the AWS IoT thing group to create.

kr260PetaGroup

The name can be up to 128 characters. Valid characters: a-z, A-Z, 0-9, underscore (_), and hyphen (-).

Now in KR260 terminal console run following commands and scripts:


```
export AWS_ACCESS_KEY_ID=<AWS_ACCESS_KEY_ID>
export AWS_SECRET_ACCESS_KEY=<AWS_SECRET_ACCESS_KEY>
```

Download and install Greengrass core software by running the script available in AWS greengrass core device setup page:

Download the installer

Run the following command on the device to download the AWS IoT Greengrass Core software.

```
curl -s https://d2s8p88vqu9w66.cloudfront.net/releases/greengrass-nucleus-latest.zip > greengrass-nucleus-latest.zip && unzip greengrass-nucleus-latest.zip -d GreengrassInstaller
```

 Copy

Next install the Greengrass core device by running the script available in AWS greengrass core device setup page:

Run the installer

The AWS IoT Greengrass Core software is a JAR file that installs the software when you run it for the first time. Run the following command on the device.

```
sudo -E java -Droot="/greengrass/v2" -Dlog.store=FILE -jar ./GreengrassInstaller/lib/Greengrass.jar
--aws-region us-east-1 --thing-name kr260-peta-dev1 --thing-group-name kr260PetaGroup --component
--default-user ggc_user:ggc_group --provision true --setup-system-service true --deploy-dev-tools
true
```

 Copy

Here is the console log after running above command:

```
xilinx-kr260-starterkit-20222:~$ sudo -E java -Droot="/greengrass/v2" -Dlog.store=FILE -jar ./GreengrassInstaller/lib/Greengrass.jar
s.jar --aws-region us-east-1 --thing-name kr260-peta-dev1 --thing-group-name kr260PetaGroup --component-default-user ggc_user:g
gc_group --provision true --setup-system-service true --deploy-dev-tools true
Password:
Provisioning AWS IoT resources for the device with IoT Thing Name: [kr260-peta-dev1]...
Found IoT policy "GreengrassV2IoTThingPolicy", reusing it
Creating keys and certificate...
Attaching policy to certificate...
Creating IoT Thing "kr260-peta-dev1"...
Attaching certificate to IoT thing...
Successfully provisioned AWS IoT resources for the device with IoT Thing Name: [kr260-peta-dev1]!
Adding IoT Thing [kr260-peta-dev1] into Thing Group: [kr260PetaGroup]...
Successfully added Thing into Thing Group: [kr260PetaGroup]
Setting up resources for aws.greengrass.TokenExchangeService ...
Attaching TES role policy to IoT thing...
No managed IAM policy found, looking for user defined policy...
IAM policy named "GreengrassV2TokenExchangeRoleAccess" already exists. Please attach it to the IAM role if not already
Configuring Nucleus with provisioned resource details...
Downloading Root CA from "https://www.amazontrust.com/repository/AmazonRootCA1.pem"
Created device configuration
Successfully configured Nucleus with provisioned resource details!
Creating a deployment for Greengrass first party components to the thing group
Configured Nucleus to deploy aws.greengrass.Cli component
Successfully set up Nucleus as a system service
xilinx-kr260-starterkit-20222:~$
```

Now in Greengrass set up page, one can view the Greengrass core devices and find above `kr260-dev` in the list.

AWS IoT > Greengrass > Core devices

Greengrass core devices [info](#)

Greengrass core devices (1)

Configure cloud discovery
Set up one core device

< 1 >

Name	Status	Status reported
kr260-peta-dev1	Healthy	3 minutes ago

In KR260 terminal one can get the device components by using `greengrass-cli`:

```
sudo /greengrass/v2/bin/greengrass-cli component list
```

```
xilinx-kr260-starterkit-20222:~$ sudo /greengrass/v2/bin/greengrass-cli component list
Password:
AWS libcrypto resolve: searching process and loaded modules
AWS libcrypto resolve: found static aws-lc HMAC symbols
AWS libcrypto resolve: found static aws-lc libcrypto 1.1.1 EVP_MD symbols
Dec 08, 2023 12:24:38 AM software.amazon.awssdk.eventstreamrpc.EventStreamRPCConnection$1 onConnectionSetup
INFO: Socket connection /greengrass/v2/ipc.socket:8033 to server result [AWS_ERROR_SUCCESS]
Dec 08, 2023 12:24:39 AM software.amazon.awssdk.eventstreamrpc.EventStreamRPCConnection$1 onProtocolMessage
INFO: Connection established with event stream RPC server
Components currently running in Greengrass:
Component Name: TelemetryAgent
  Version: 0.0.0
  State: RUNNING
  Configuration: null
Component Name: DeploymentService
  Version: 0.0.0
  State: RUNNING
  Configuration: null
Component Name: UpdateSystemPolicyService
  Version: 0.0.0
  State: RUNNING
  Configuration: null
Component Name: aws.greengrass.Nucleus
  Version: 2.4.0
  State: FINISHED
  Configuration: {"awsRegion":"us-east-1","componentStoreMaxSizeBytes":"10000000000","deploymentPollingFrequency":8443,"httpClient":{"},"iotCredEndpoint":"cluwyavs4wpvxg.credentials.iot.us-east-1.amazonaws.com","iotDataEndpoint":{"},"mqtt":{"spooler":{"},"networkProxy":{"proxy":{"}}},"platformOverride":{"},"runWithDefault":{"posixUser":"gg
Component Name: aws.greengrass.Cli
  Version: 2.4.0
  State: RUNNING
  Configuration: {"AuthorizedPosixGroups":null}
Component Name: FleetStatusService
  Version: null
  State: RUNNING
  Configuration: null
xilinx-kr260-starterkit-20222:~$
```

We will be adding component to publish and subscribe the topic to the AWS cloud Broker.

Installing the component

Get the `components` folder and copy in the KR260 home directory.

It contains:

artifacts

- com.example.mqtt
- 1.0.0
- mqtt.py (This python code published the data on button press and actuates gpio on receiving the data in subscribed topic)

recipe

- com.example.mqtt-1.0.0.json

To install the above component run the following in the KR260 terminal:

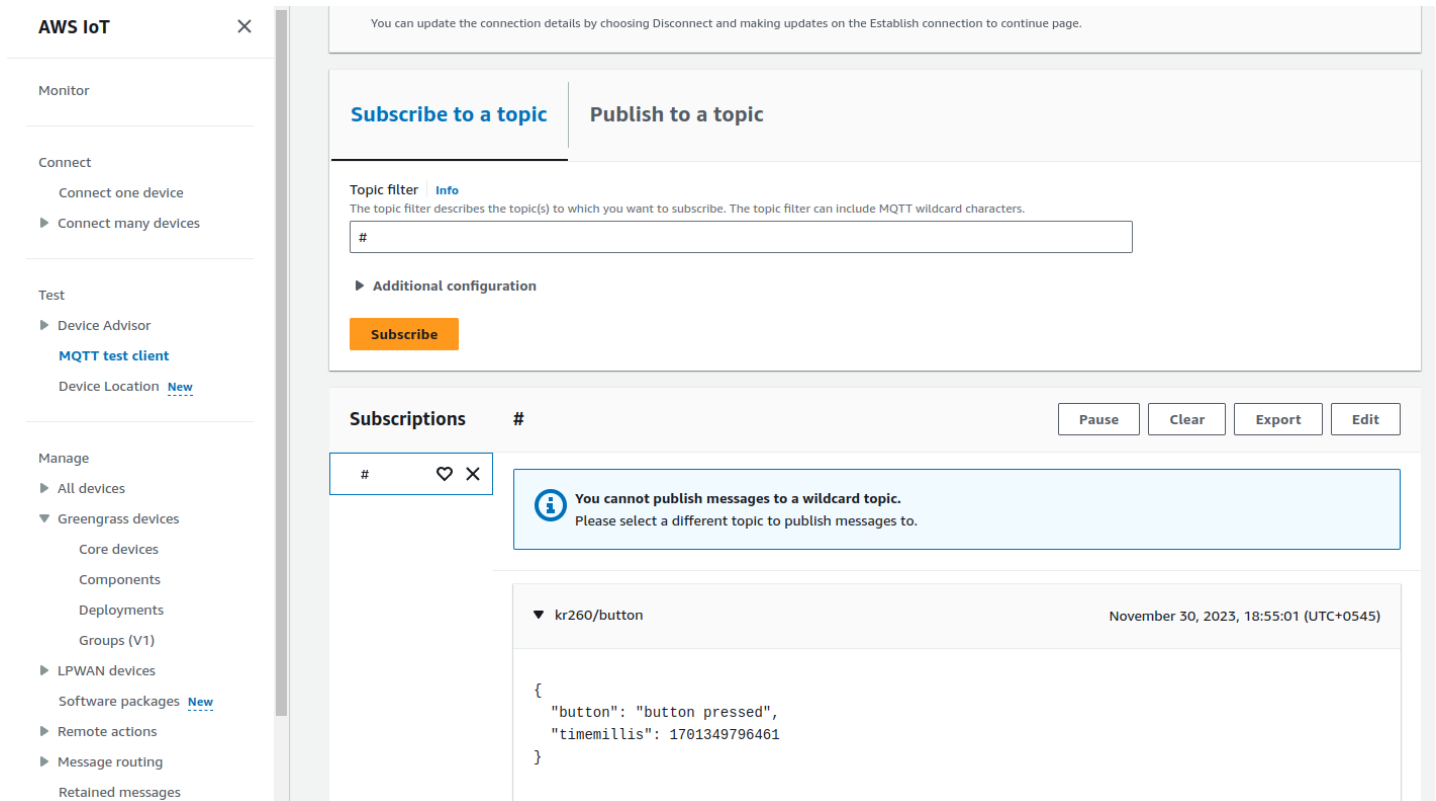
```
sudo /greengrass/v2/bin/greengrass-cli deployment create \  
--recipeDir ~/components/recipe \  
--artifactDir ~/components/artifacts \  
--merge "com.example.mqtt=1.0.0"
```

```
xilinx-kr260-starterkit-20222:~$ sudo /greengrass/v2/bin/greengrass-cli deployment create --recipeDir ~/components/r  
ecipe --artifactDir ~/components/artifacts --merge "com.example.mqtt=1.0.0"  
AWS libcrypto resolve: searching process and loaded modules  
AWS libcrypto resolve: found static aws-lc HMAC symbols  
AWS libcrypto resolve: found static aws-lc libcrypto 1.1.1 EVP MD symbols  
Dec 08, 2023 1:23:18 AM software.amazon.awssdk.eventstreamrpc.EventStreamRPCConnection$1 onConnectionSetup  
INFO: Socket connection /greengrass/v2/ipc.socket:8033 to server result [AWS ERROR SUCCESS]  
Dec 08, 2023 1:23:18 AM software.amazon.awssdk.eventstreamrpc.EventStreamRPCConnection$1 onProtocolMessage  
INFO: Connection established with event stream RPC server  
Local deployment submitted! Deployment Id: 89867086-fe40-45fa-b994-3d4d65036ae5
```

Now check the installed component is in “running state”

```
ubuntu@xilinx-kr260-starterkit-20222:~$ sudo /greengrass/v2/bin/greengrass-cli component list  
Components currently running in Greengrass:  
Component Name: aws.greengrass.Nucleus  
Version: 2.12.0  
State: FINISHED  
Configuration: {"awsRegion":"us-east-1","componentStoreMaxSizeBytes":"1000000000","deploymentPollingFrequencySeconds":"15","envStage":"prod","fltpMode":"false","fleetStatus":{"periodicStatusPublishIntervalsSeconds":"60400.0"},"greengrassDataPlaneEndpoint":"","greengrassDataPlanePort":"8443","httpClient":{"},"lotCredEndpoint":"ciwys4v4p4v4g.credentials.lot.us-east-1.amazonaws.com","lotDataEndpoint":"a9jc3obcutfav-ats.lot.us-east-1.amazonaws.com","lotRoleAlias":"GreengrassV2TokenExchangeRoleAlias","jvmOptions":"","log.store=FILE","logging":{"},"mqtt":{"spooler":{"},"networkProxy":{"proxy":{"},"platformOverride":{"},"runWithDefault":{"posixShell":"sh","posixUser":"ggc user:ggc group"},"s3EndpointType":"GLOBAL","telemetry":{"}}}  
Component Name: com.example.mqtt  
Version: 1.0.0  
State: RUNNING  
Configuration: {"accessControl":{"aws.greengrass.ipc.mqttproxy":{"com.example.mqtt:mqttproxy:1":{"operations":["aws.greengrass#PublishToIoTCore","aws.greengrass#SubscribeToIoTCore"],"policyDescription":"Allow access to pub/sub to mqtt/mqtt."},"resources":["kr260/mqtt","kr260/button"]},"message":"hello"}  
Component Name: TelemetryAgent  
Version: 0.0.0  
State: RUNNING  
Configuration: null  
Component Name: DeploymentService  
Version: 0.0.0  
State: RUNNING  
Configuration: null  
Component Name: UpdateSystemPolicyService  
Version: 0.0.0  
State: RUNNING  
Configuration: null  
Component Name: FleetStatusService  
Version: 0.0.0  
State: RUNNING  
Configuration: null  
Component Name: aws.greengrass.Cli  
Version: 2.12.0  
State: RUNNING  
Configuration: {"AuthorizedPosixGroups":null,"AuthorizedWindowsGroups":null}  
Component Name: aws.greengrass.LocalDebugConsole  
Version: 2.4.1  
State: RUNNING  
Configuration: {"bindHostname":"localhost","httpsEnabled":"true","port":"1441","websocketPort":"1442"}
```

Now in aws IoT console, open “MQTT test client” and subscribe to “#”



AWS IoT X

Monitor

Connect

Connect one device

▶ Connect many devices

Test

▶ Device Advisor

MQTT test client

Device Location **New**

Manage

▶ All devices

▼ Greengrass devices

Core devices

Components

Deployments

Groups (V1)

▶ LPWAN devices

Software packages **New**

▶ Remote actions

▶ Message routing

Retained messages

You can update the connection details by choosing Disconnect and making updates on the Establish connection to continue page.

Subscribe to a topic **Publish to a topic**

Topic filter **Info**

The topic filter describes the topic(s) to which you want to subscribe. The topic filter can include MQTT wildcard characters.

#

▶ Additional configuration

Subscribe

Subscriptions # **Pause** **Clear** **Export** **Edit**

×

You cannot publish messages to a wildcard topic.
Please select a different topic to publish messages to.

▼ kr260/button November 30, 2023, 18:55:01 (UTC+0545)

```
{
  "button": "button pressed",
  "timemillis": 1701349796461
}
```

You can see the “button pressed” message once the button is pressed.

Now to control the LED, publish the message to “kr260/mqtt” topic. Here is the screenshot of the message which switch on the LED.

AWS IoT

Monitor

Connect

Connect one device

Connect many devices

Test

Device Advisor

MQTT test client

Device Location New

Manage

All devices

Greengrass devices

Core devices

Components

Deployments

Groups (V1)

LPWAN devices

Software packages New

Remote actions

Message routing

You can update the connection details by choosing Disconnect and making updates on the Establish connection to continue page.

Subscribe to a topic

Publish to a topic

Topic name
The topic name identifies the message. The message payload will be published to this topic with a Quality of Service (QoS) of 0.

kr260/mqtt

Message payload

```
{
  "ledon": true
}
```

Additional configuration

Publish

Subscriptions #

Pause Clear Export Edit

#

You cannot publish messages to a wildcard topic.
Please select a different topic to publish messages to.

kr260/mqtt November 30, 2023, 18:57:32 (UTC+0545)

Now to switch off the LED send "false" message in the "kr260/mqtt" topic.

AWS IoT

Monitor

Connect

Connect one device

Connect many devices

Test

Device Advisor

MQTT test client

Device Location New

Manage

All devices

Greengrass devices

Core devices

Components

Deployments

Groups (V1)

LPWAN devices

Software packages New

Remote actions

Message routing

You can update the connection details by choosing Disconnect and making updates on the Establish connection to continue page.

Subscribe to a topic

Publish to a topic

Topic name
The topic name identifies the message. The message payload will be published to this topic with a Quality of Service (QoS) of 0.

kr260/mqtt

Message payload

```
{
  "ledon": false
}
```

Additional configuration

Publish

Subscriptions #

Pause Clear Export Edit

#

You cannot publish messages to a wildcard topic.
Please select a different topic to publish messages to.

kr260/mqtt November 30, 2023, 18:59:36 (UTC+0545)