IoT sensor dashboard

Deployment Guide

De Silva, Akalanka

7-25-2023

1. Introduction

This is an accelerator for creating an IoT solution to view data from sensors, predominantly LoRaWAN sensors, using AWS IoT services. It should be noted that since this is an accelerator, it is designed to be a starting point of your solution build journey rather than a complete solution. However, this accelerator does create all the AWS resources required to interface with LoRaWAN gateways, ingest, decode & store LoRaWAN messages, along with template dashboards for the supported types of sensors. It also supports ingesting data from any MQTT sensor which can connect and publish to IoT Core directly. Therefore, it can be used to cater to certain basic use cases with minimal customization.

This accelerator utilizes the following key AWS services:

- AWS IoT Core – IoT Core acts as the connection point for your MQTT based sensors to the AWS cloud. IoT Core for LoRaWAN provides a fully managed LoRaWAN Network Server (LNS) that enables customers to connect wireless devices that use the LoRaWAN protocol
- AWS Lambda – There are 2 Lambda functions in this accelerator
    - Decoder function – this function decodes the uplink data from the sensors based on the sensor's vendor and the model. This is to decode uplink messages from LoRaWAN sensors.
    - Sensor list update function – this function updates the database table with IoT thing create and delete events to maintain a table of provisioned sensors
- Amazon Timestream – this is where the timeseries data transmitted from the sensors are stored. It also contains a separate table to maintain the list of provisioned sensors along with vendor and model information for dashboarding purposes.
- Amazon Managed Grafana – this is used as the dashboarding layer. Users can consume the prebuilt dashboards for each model of sensor or build their own dashboards while using the given dashboards as a reference.

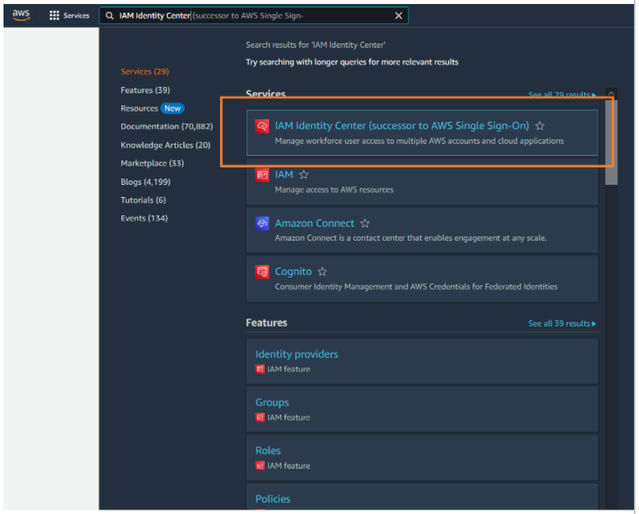
In the background, AWS IAM Identity Center provides the single sign on for the Amazon Managed Grafana, thus allowing the administrator the flexibility to segregate the dashboard logins from AWS account logins. It also allows the end user to utilize the same single sign on that the user might be already using on other AWS services.

2. Deployment guide

Step 1 – Enable IAM Identity Center and create a user

Important: This step can be skipped if IAM Identity Center is enabled and users already exist. If this is a fresh AWS account, follow the instructions below.

1.1 Open IAM Identity Center



Search results for 'IAM Identity Center'

Try searching with longer queries for more relevant results

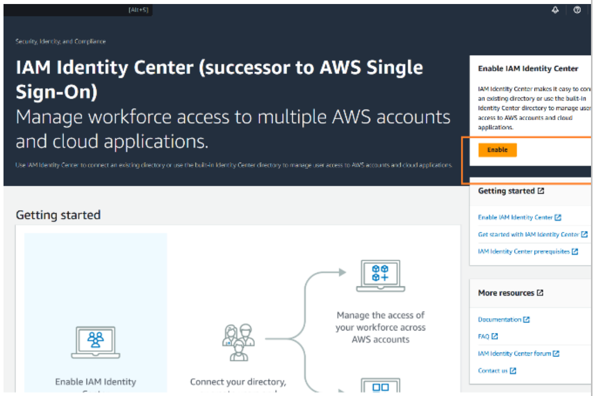
IAM Identity Center (successor to AWS Single Sign-On)
Manage workforce user access to multiple AWS accounts and cloud applications

IAM
Manage access to AWS resources

Amazon Connect
Amazon Connect is a contact center that enables engagement at any scale.

Cognito
Consumer Identity Management and AWS Credentials for Federated Identities

1.2 Enable IAM Identity Center


[Alt+S]
Security, Identity, and Compliance
Enable
Getting started
Enable IAM Identity Center
Get started with IAM Identity Center
IAM Identity Center prerequisites
More resources
Documentation
FAQ
IAM Identity Center forum
Contact us
Enable IAM Identity
Connect your directory,
Manage the access of your workforce across AWS accounts

IAM Identity Center (successor to AWS Single Sign-On)

Manage workforce access to multiple AWS accounts and cloud applications.

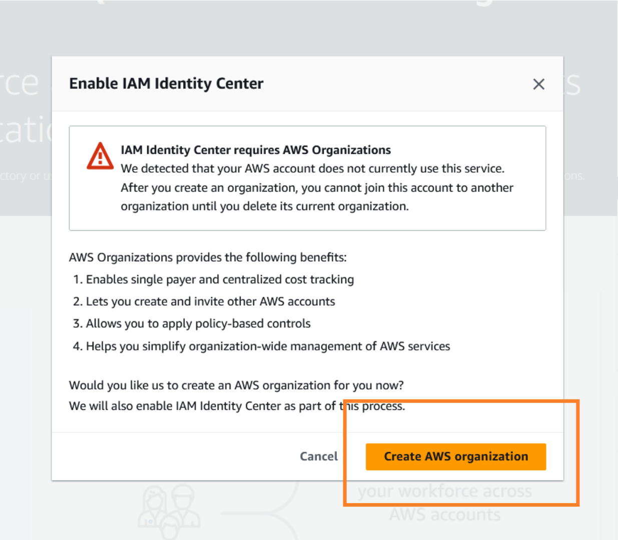
Use IAM Identity Center to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.

Enable IAM Identity Center

IAM Identity Center makes it easy to con an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.

Getting started

1.3 Confirm that you want to create an AWS Org.



Enable IAM Identity Center

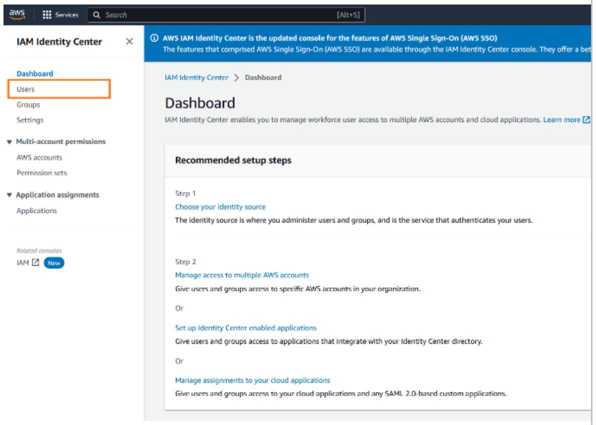
IAM Identity Center requires AWS Organizations
We detected that your AWS account does not currently use this service. After you create an organization, you cannot join this account to another organization until you delete its current organization.

AWS Organizations provides the following benefits:

1. Enables single payer and centralized cost tracking
2. Lets you create and invite other AWS accounts
3. Allows you to apply policy-based controls
4. Helps you simplify organization-wide management of AWS services

Would you like us to create an AWS organization for you now?
We will also enable IAM Identity Center as part of this process.

1.4 Navigate to Users



AWS IAM Identity Center is the updated console for the features of AWS Single Sign-On (AWS SSO)
The features that comprised AWS Single Sign-On (AWS SSO) are available through the IAM Identity Center console. They offer a bet

Dashboard

IAM Identity Center enables you to manage workforce user access to multiple AWS accounts and cloud applications. Learn more

Recommended setup steps

Step 1
Choose your identity source
The identity source is where you administer users and groups, and is the service that authenticates your users.

Step 2
Manage access to multiple AWS accounts
Give users and groups access to specific AWS accounts in your organization.

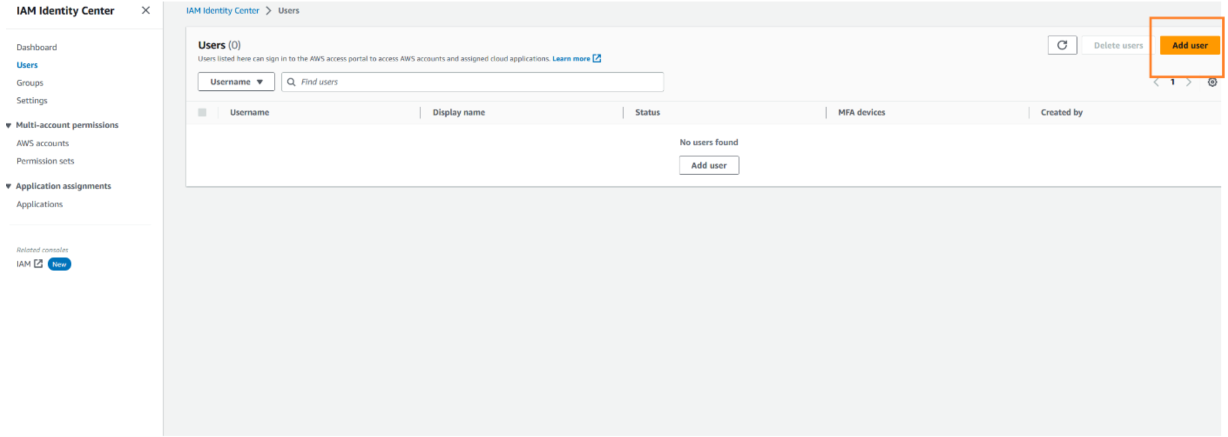
Or

Set up Identity Center enabled applications
Give users and groups access to applications that integrate with your Identity Center directory.

Or

Manage assignments to your cloud applications
Give users and groups access to your cloud applications and any SAML 2.0-based custom applications.

1.5 Add a User



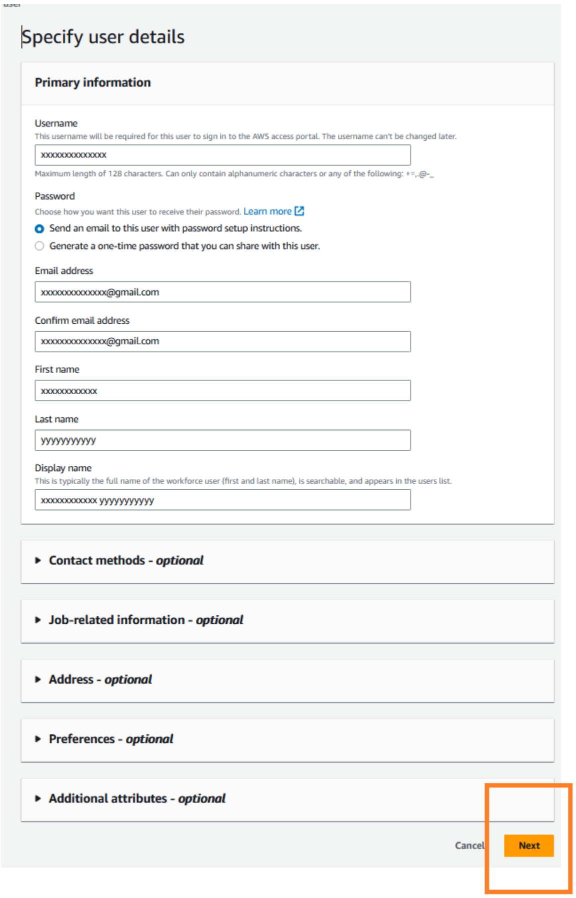
Users (0)

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. Learn more

Username	Display name	Status	MFA devices	Created by

No users found

1.5.1 Add a User (contd.)



Specify user details

Primary information

Username

This username will be required for this user to sign in to the AWS access portal. The username can't be changed later.

xxxxxxxxxxxxxx

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +=,.@-_

Password

Choose how you want this user to receive their password. Learn more

● Send an email to this user with password setup instructions.

○ Generate a one-time password that you can share with this user.

Email address

xxxxxxxxxxxxxx@gmail.com

Confirm email address

xxxxxxxxxxxxxx@gmail.com

First name

xxxxxxxxxxxx

Last name

yyyyyyyyyy

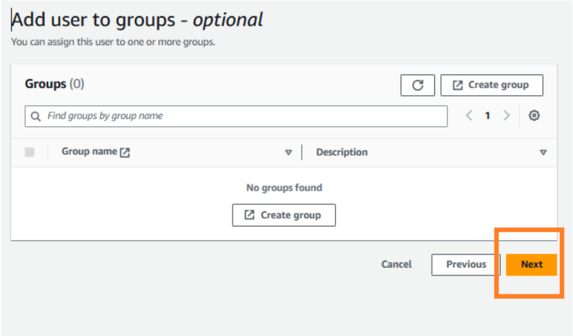
Display name

This is typically the full name of the workforce user (first and last name), is searchable, and appears in the users list.

xxxxxxxxxxxx yyyyyyyyyy

Contact methods - optional
Job-related information - optional
Address - optional
Preferences - optional
Additional attributes - optional
Cancel
Next

1.5.3 Add a User (contd.)



Add user to groups - *optional*

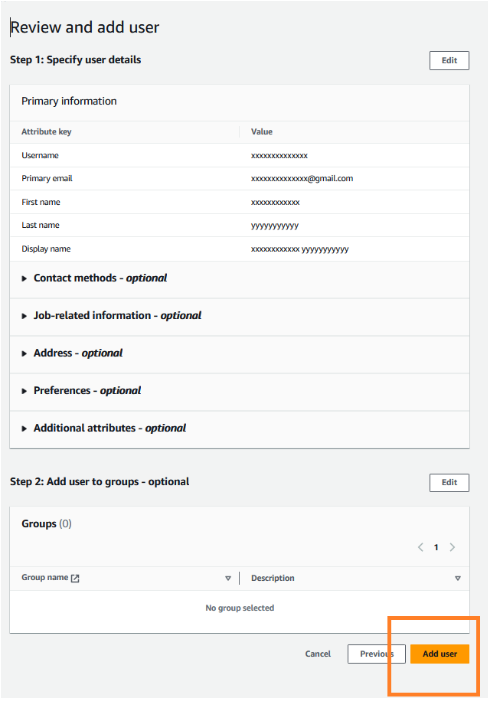
You can assign this user to one or more groups.

Groups (0)

Group name	Description

No groups found

1.5.3 Add a User (contd.)



Review and add user

Step 1: Specify user details

Primary information

Attribute key	Value
Username	xxxxxxxxxxxxxx
Primary email	xxxxxxxxxxxxxx@gmail.com
First name	xxxxxxxxxxxx
Last name	yyyyyyyyyy
Display name	xxxxxxxxxxxx yyyyyyyyyy

Edit
Contact methods - optional
Job-related information - optional
Address - optional
Preferences - optional
Additional attributes - optional
Edit

Step 2: Add user to groups - optional

Groups (0)

Group name	Description

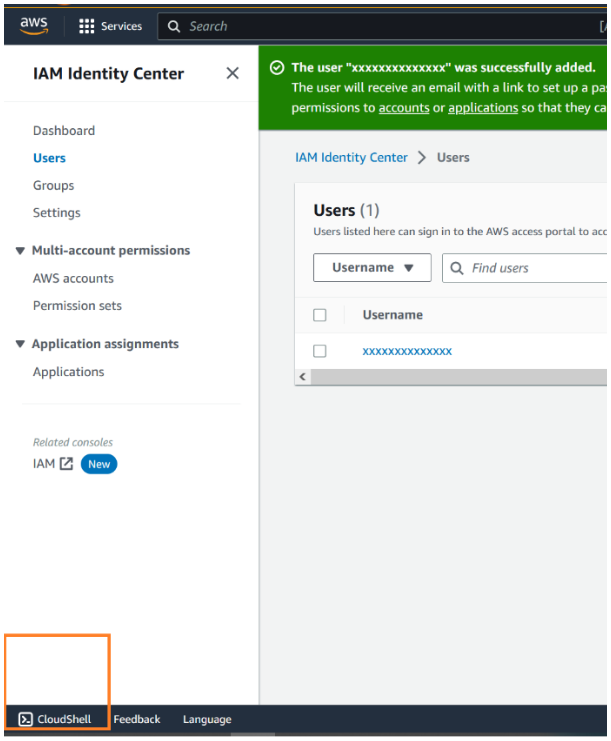
No group selected

1
Cancel
Previous
Add user

Step 2 – Create stack

This step will create the entire stack in your AWS account with a single command in the AWS cloud shell

2.1 Open AWS Cloud Shell



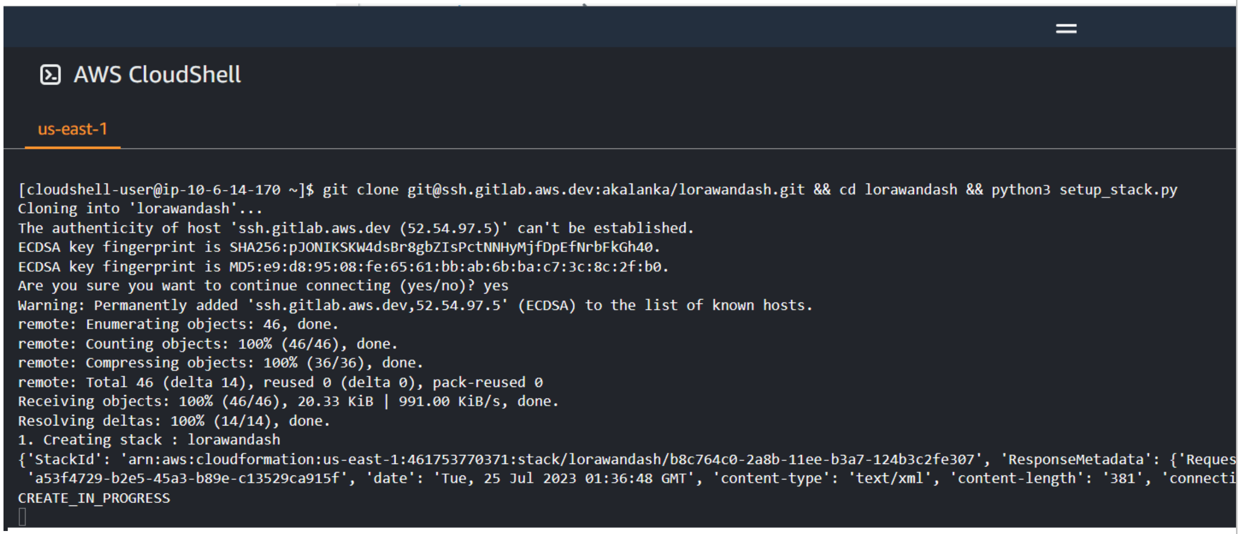
The user "xxxxxxxxxxxxx" was successfully added.
The user will receive an email with a link to set up a pa
permissions to accounts or applications so that they ca

Users (1)
Users listed here can sign in to the AWS access portal to acc

2.2 Enter the following command:

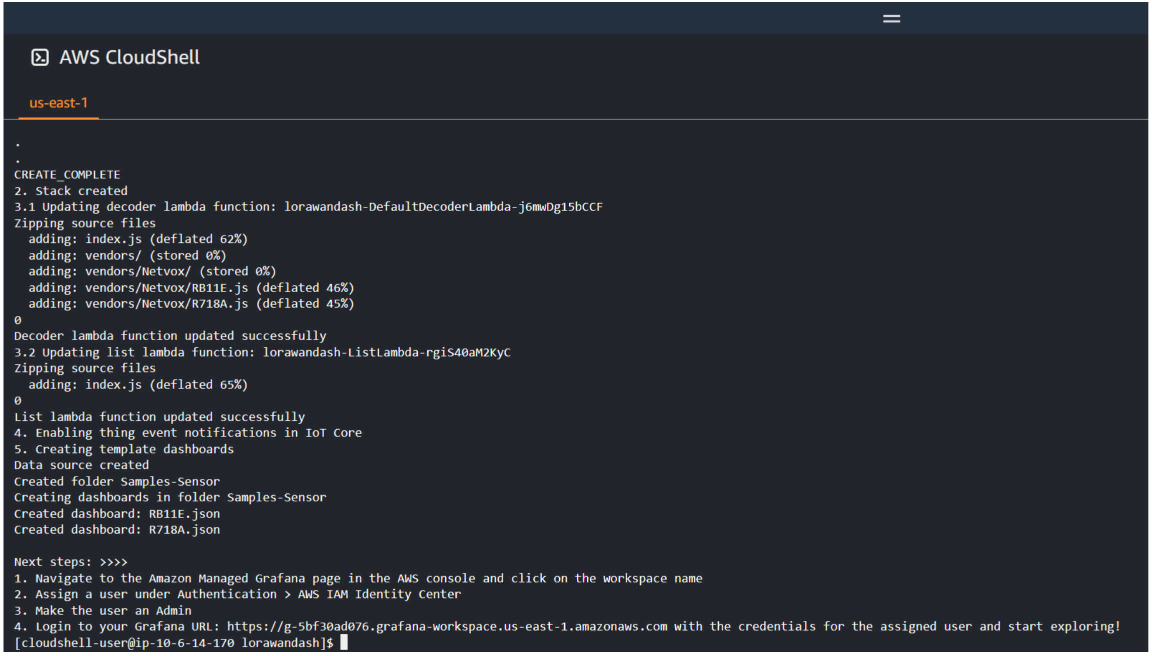
```
git clone https://github.com/aws-samples/iot-x-sensordash.git  && cd iot-x-sensordash && python3 setup_stack.py
```

2.3 Stack creation in progress



```
[cloudshell-user@ip-10-6-14-170 ~]$ git clone git@ssh.gitlab.aws.dev:akalanka/lorawandash.git && cd lorawandash && python3 setup_stack.py
Cloning into 'lorawandash'...
The authenticity of host 'ssh.gitlab.aws.dev (52.54.97.5)' can't be established.
ECDSA key fingerprint is SHA256:pJONIKSKW4dsBr8gbZIsPctNNHyMjfDpEfNrbFkGh40.
ECDSA key fingerprint is MD5:e9:d8:95:08:fe:65:61:bb:ab:6b:ba:c7:3c:8c:2f:b0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ssh.gitlab.aws.dev,52.54.97.5' (ECDSA) to the list of known hosts.
remote: Enumerating objects: 46, done.
remote: Counting objects: 100% (46/46), done.
remote: Compressing objects: 100% (36/36), done.
remote: Total 46 (delta 14), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (46/46), 20.33 KiB | 991.00 KiB/s, done.
Resolving deltas: 100% (14/14), done.
1. Creating stack : lorawandash
{'StackId': 'arn:aws:cloudformation:us-east-1:461753770371:stack/lorawandash/b8c764c0-2a8b-11ee-b3a7-124b3c2fe307', 'ResponseMetadata': {'Reques
 'a53f4729-b2e5-45a3-b89e-c13529ca915f', 'date': 'Tue, 25 Jul 2023 01:36:48 GMT', 'content-type': 'text/xml', 'content-length': '381', 'connecti
CREATE_IN_PROGRESS
```

2.4 Stack Creation complete



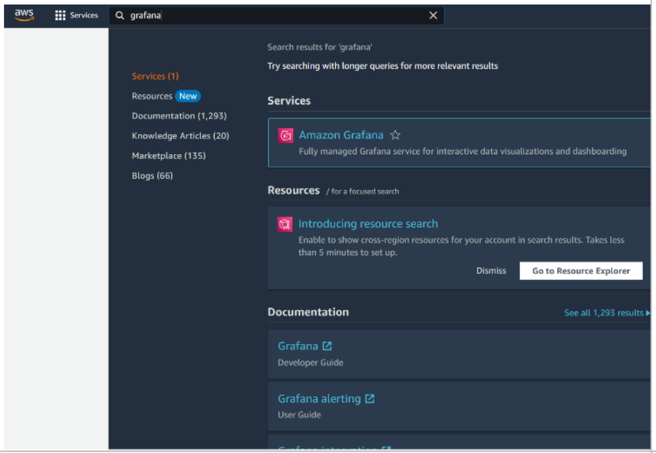
```
.
.
CREATE_COMPLETE
2. Stack created
3.1 Updating decoder lambda function: lorawandash-DefaultDecoderLambda-j6mwDg15bCCF
Zipping source files
  adding: index.js (deflated 62%)
  adding: vendors/ (stored 0%)
  adding: vendors/Netvox/ (stored 0%)
  adding: vendors/Netvox/RB11E.js (deflated 46%)
  adding: vendors/Netvox/R718A.js (deflated 45%)
0
Decoder lambda function updated successfully
3.2 Updating list lambda function: lorawandash-ListLambda-rgiS40aM2KyC
Zipping source files
  adding: index.js (deflated 65%)
0
List lambda function updated successfully
4. Enabling thing event notifications in IoT Core
5. Creating template dashboards
Data source created
Created folder Samples-Sensor
Creating dashboards in folder Samples-Sensor
Created dashboard: RB11E.json
Created dashboard: R718A.json

Next steps: >>>>
1. Navigate to the Amazon Managed Grafana page in the AWS console and click on the workspace name
2. Assign a user under Authentication > AWS IAM Identity Center
3. Make the user an Admin
4. Login to your Grafana URL: https://g-5bf30ad076.grafana-workspace.us-east-1.amazonaws.com with the credentials for the assigned user and start exploring!
[cloudshell-user@ip-10-6-14-170 lorawandash]$
```

At the end of the stack creation it will provide the next steps to assign a user to the Grafana instance which is described int step 3.

Step 3 – Assign Users to Grafana

This step will assign users to the Grafana workspace. Ensure that the users are created in IAM Identity Center by following Step 1. Furthermore ensure that the email for newly created users are verified and the password is set.

3.1 Navigate to Amazon Managed Grafana



Search results for 'grafana'

Try searching with longer queries for more relevant results

Services

Amazon Grafana ☆

Fully managed Grafana service for interactive data visualizations and dashboarding

Resources / for a focused search

Introducing resource search

Enable to show cross-region resources for your account in search results. Takes less than 5 minutes to set up.

Documentation

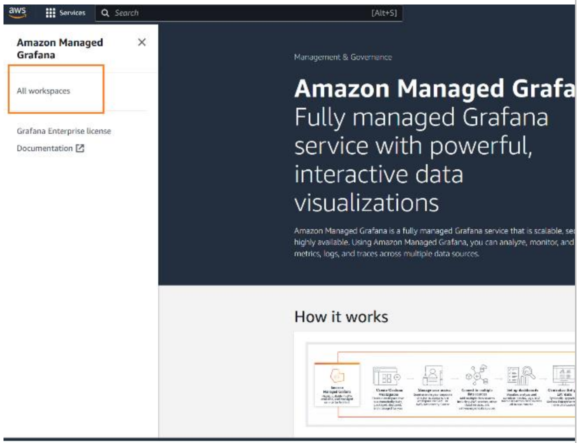
Grafana

Developer Guide

Grafana alerting

User Guide

3.2 Open All Workspaces



Management & Governance

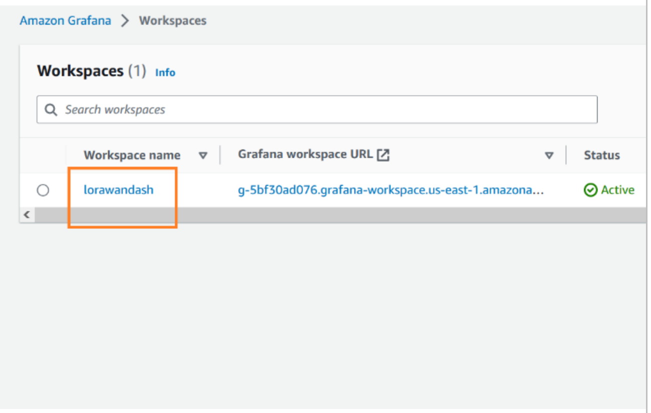
Amazon Managed Grafa

Fully managed Grafana service with powerful, interactive data visualizations

Amazon Managed Grafana is a fully managed Grafana service that is scalable, se
highly available. Using Amazon Managed Grafana, you can analyze, monitor, and
metrics, logs, and traces across multiple data sources.

How it works

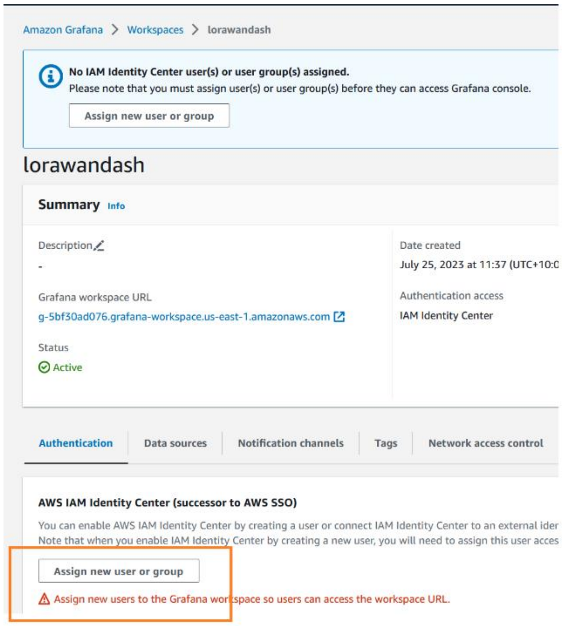
3.3 Open the workspace created in step 2.



Workspaces (1) Info

	Workspace name	Grafana workspace URL	Status
○	lorawandash	g-5bf30ad076.grafana-workspace.us-east-1.amazona...	Active

3.4 Assign a user



No IAM Identity Center user(s) or user group(s) assigned.

Please note that you must assign user(s) or user group(s) before they can access Grafana console.

lorawandash

Summary Info

Description -

Date created: July 25, 2023 at 11:37 (UTC+10:0

Grafana workspace URL: g-5bf30ad076.grafana-workspace.us-east-1.amazonaws.com

Authentication access: IAM Identity Center

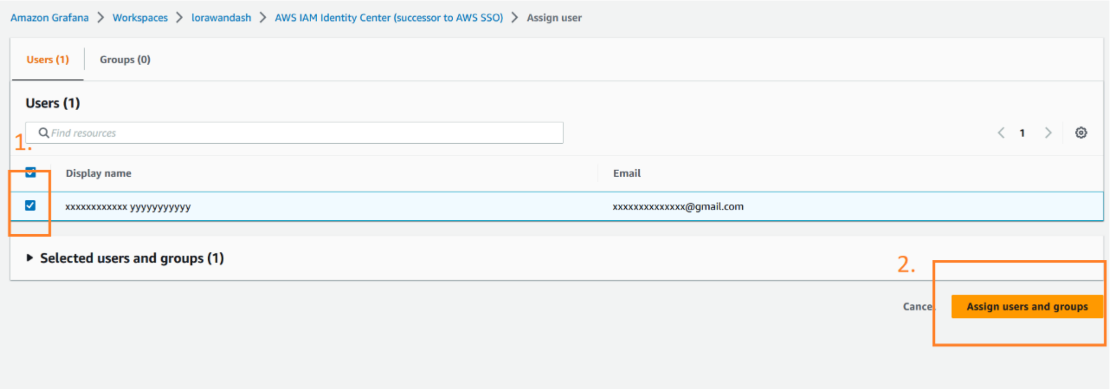
Status: Active

AWS IAM Identity Center (successor to AWS SSO)

You can enable AWS IAM Identity Center by creating a user or connect IAM Identity Center to an external ider
Note that when you enable IAM Identity Center by creating a new user, you will need to assign this user acces

Assign new users to the Grafana workspace so users can access the workspace URL.

3.4 Assign a user (contd.)


Amazon Grafana > Workspaces > lorawandash > AWS IAM Identity Center (successor to AWS SSO) > Assign user

Users (1) | Groups (0)

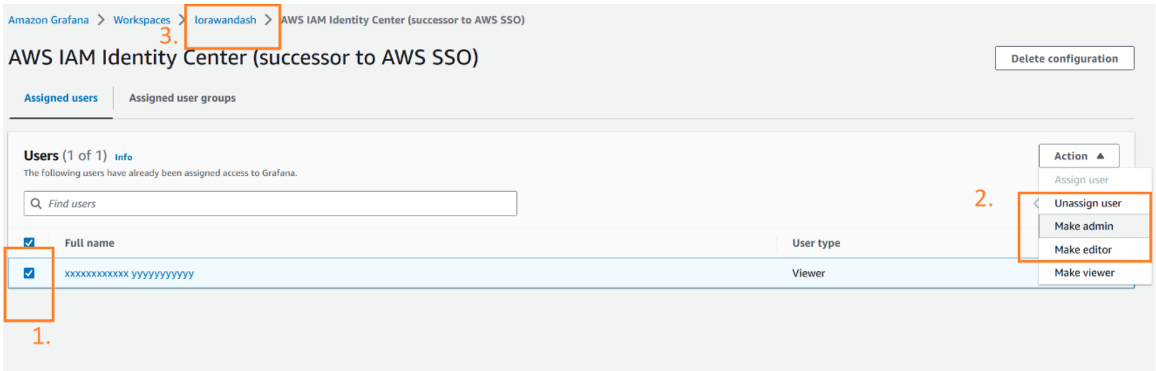
Users (1)

Find resources

☑	Display name	Email
☑	xxxxxxxxxxxx yyyyyyyyyy	xxxxxxxxxxxxxx@gmail.com

▸ Selected users and groups (1)

3.5 Make the user and admin/viewer/editor as desired and go back to the workspace


Amazon Grafana > Workspaces > lorawandash > AWS IAM Identity Center (successor to AWS SSO)

AWS IAM Identity Center (successor to AWS SSO)

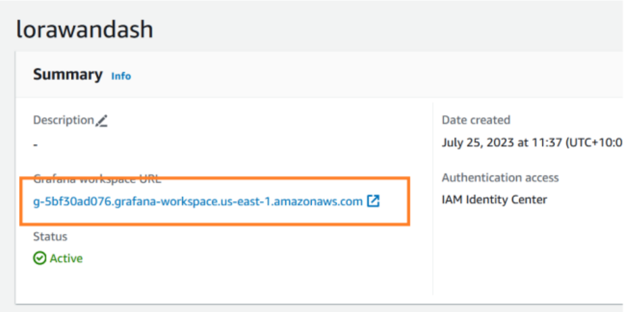
Users (1 of 1) Info

The following users have already been assigned access to Grafana.

Find users

☑	Full name	User type
☑	xxxxxxxxxxxx yyyyyyyyyy	Viewer

3.6 Click to open the Grafana workspace


lorawandash

Summary Info

Description: -

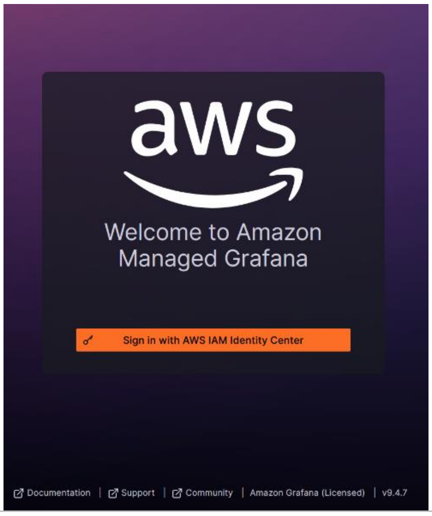
Grafana workspace URL: g-5bf30ad076.grafana-workspace.us-east-1.amazonaws.com

Status: Active

Date created: July 25, 2023 at 11:37 (UTC+10:0

Authentication access: IAM Identity Center

3.7 Login with the created user credentials


aws
Welcome to Amazon Managed Grafana
Sign in with AWS IAM Identity Center
Documentation | Support | Community | Amazon Grafana (Licensed) | v9.4.7

This concludes the stack creation process. For further details on the operational aspects, please refer to the user guide.