

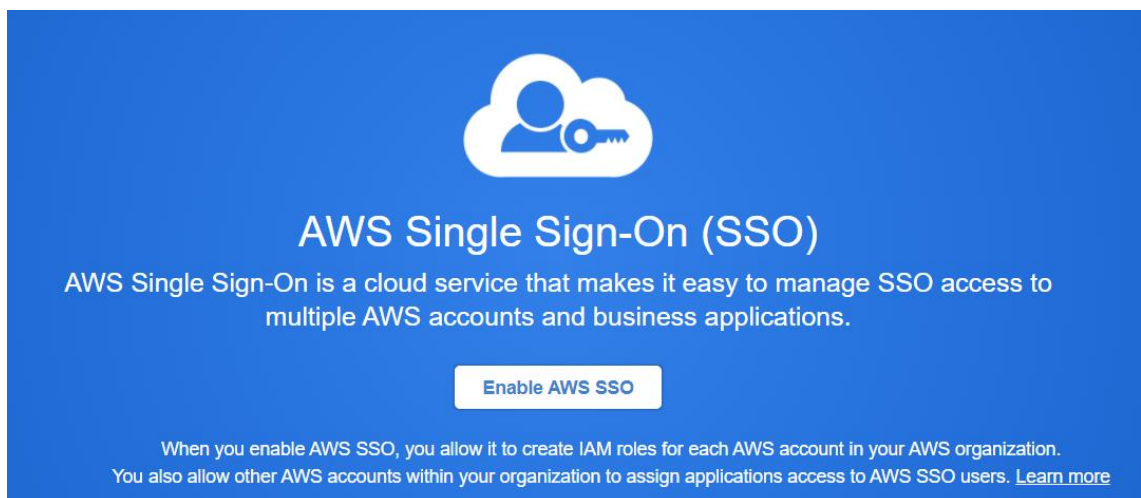
[認証のセットアップ]

AMG はスタンドアロンの ID/Password 認証をサポートしておらず、Idp を利用した SAML 認証か AWS SSO を用いることになります。このワークショップでは AWS SSO を用います。AWS SSO は、AWS 上でアイデンティティを作成、または接続し、AWS 組織全体のアクセスを一元的に管理するものです。自分の AWS アカウントやクラウドアプリケーションだけのアクセスを管理することも可能です。ユーザー ID は、AWS SSO で直接作成することもできますし、Microsoft アクティブディレクトリや、Okta Universal Directory や Azure AD などの標準ベースの ID プロバイダーから持ってくることもできます。

AWS SSO を AWS アカウントで設定するためには、AWS Organizations との連携が必須です。AWS Organizations は、AWS リソースの増加やスケーリングに合わせて、環境を一元的に管理し、統制を実現するサービスです。AWS Organizations を使って、新しい AWS アカウントを作成しリソースを割り当てたり、アカウントをグループ化してワークフローを整理したり、ガバナンスのためにアカウントまたはグループにポリシーを適用したり、すべてのアカウントに単一の支払い方法を利用することで請求を簡素化したりできるようになります。

既に AWS Organization で管理されている AWS アカウントで本ワークショップを行う場合、AWS SSO を利用する権限が付与されている必要がありますので注意してください。

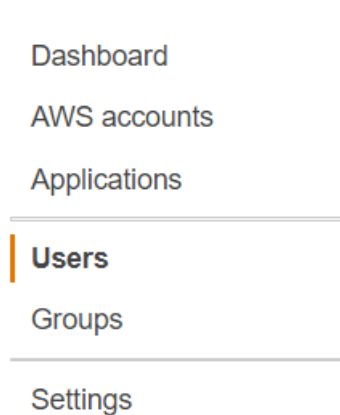
1. AWS SSO のマネージメントコンソールに移動します



2. [Enable AWS SSO]のボタンをおします。AWS アカウント上で Organization がまだ有

効化されていない場合、Organization を有効化する指示が出ますが、画面に従って有効化してください。

3. 左のペインから[Users]をクリックします



4. [Add user]をおします
5. 以下のように情報を入力し[Next:Groups]ボタンをおします。AWS の管理者と同じメールアドレスでも可能ですが、ややこしくなるので可能であれば別のメールアドレスをお勧めします。

Username*	<input type="text" value="hkameda"/>
This username will be required to sign in to the user portal. This cannot be changed later.	
Password	<input checked="" type="radio"/> Send an email to the user with password setup instructions. Learn more <input type="radio"/> Generate a one-time password that you can share with the user. Learn more
Email address*	<input type="text" value="harunobukameda@gmail.com"/>
Confirm email address*	<input type="text" value="harunobukameda@gmail.com"/>
First name*	<input type="text" value="Harunobu"/>
Last name*	<input type="text" value="Kameda"/>
Display name*	<input type="text" value="Harunobu Kameda"/>

6. グループの設定は行わず、そのまま[Add user]ボタンをおします
7. ユーザーが作成されたら、登録したメールアドレスにパスワード初期設定を促すメールが届いていますので確認をします

✓

The user "Harunobu Kameda" has been added successfully.

The user will receive an email with a link to set up a password and instructions to connect to user portal. The link will be valid for up to 7 days. You can now grant this user permissions to accounts or applications so that they can access their assigned accounts and applications when they sign in to the user portal. [Learn more](#)

Add user

Delete users

↺

⚙


Display name

Search criteria

<input type="checkbox"/> Display name	Username	Status	MFA devices
<input type="checkbox"/> Harunobu Kameda	hkameda	Enabled	None

◀▶

8. [Accept Invitation]をおします



Hello Harunobu Kameda,

Your AWS Organization (AWS Account #294963776963) uses AWS Single Sign-On (SSO) to provide access to AWS accounts and business applications.

Your administrator has invited you to access the AWS Single Sign-On (SSO) user portal. Accepting this invitation activates your AWS SSO user account so that you can access assigned AWS accounts and applications. Click on the link below to accept this invitation.

Accept invitation

This invitation will expire in 7 days.

9. パスワードを設定します



新規ユーザーのサインアップ

ユーザー情報を入力

ユーザー名: hkameda

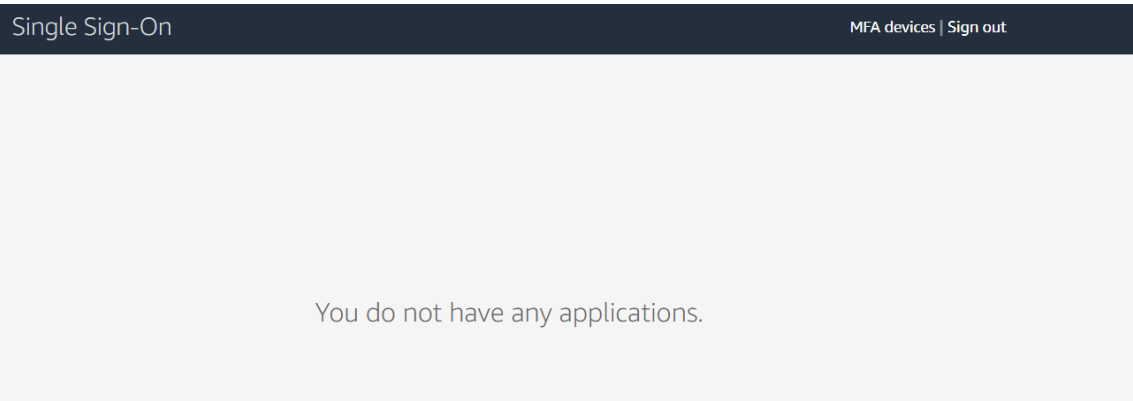
新規パスワード

パスワードを確認

☐ パスワードの表示

新しいパスワードの設定

10. テストでログインしてみます。ユーザー名はメールアドレスではなく、SSO マネージメントコンソールで表示されるユーザー名なので注意してください。
11. 以下の画面が表示されたら成功です



[AMG の起動]

12. AMG のマネージメントコンソールに移動します



13. [Create Workspace] ボタンをおします
14. 適当な名前を入力し [Next] をおします

15. SSO の利用にチェックをつけます

16. [Permission type] はそのまま [Next] をおします
17. [Current account] を選び、Data Source は [Amazon CloudWatch] を選びます。画面に表示されているその他サービスをご利用の場合は、選んでも大丈夫です。

IAM permission access settings

Select how you would like to specify account access.

☒ **Current account**
 Use Grafana to monitor resources in your current account.

☐ **Organization**
 Use Grafana to monitor resources in your Organizational Units (OUs).

▼ **Data sources and notification channels - optional**

Data sources

Selecting an AWS data source below creates an IAM role that enables Amazon Grafana access to those resources in your current account. It does not set up the selected service as a data source. Note that all resources will be accessible by default.

<input type="checkbox"/>	Data source name
<input type="checkbox"/>	AWS IoT SiteWise
<input type="checkbox"/>	AWS X-Ray
<input checked="" type="checkbox"/>	Amazon CloudWatch
<input type="checkbox"/>	Amazon OpenSearch Service (successor to Amazon Elasticsearch Service)

18. [Next]をおします
19. 最後に[Create Workspace]をおします
20. 構築中のステータスになりますので数分間待ちます

Creating workspace grafanatest

Amazon Grafana > Workspaces > grafanatest

grafanatest Delete

Summary [Info](#)

Description ✎	Date created	IAM role ✎
-	2021-10-07	arn:aws:iam::294963776963:role/service-role/AmazonGrafanaServiceRole-USEvnlHg
Grafana workspace URL	Authentication access	Enterprise license
⊖ Creating	AWS SSO	-
Status		Grafana version
⊖ Creating		8.0

Workspace grafanatest successfully created.

Amazon Grafana > Workspaces > grafanatest

grafanatest Delete

Summary [Info](#)

Description ✎	Date created	IAM role ✎
-	2021-10-07	arn:aws:iam::294963776963:role/service-role/AmazonGrafanaServiceRole-USEvnlHg
Grafana workspace URL	Authentication access	Enterprise license
g-1dda7d574b.grafana-workspace.ap-northeast-1.amazonaws.com ✎	AWS SSO	Upgrade to Grafana Enterprise
Status		Grafana version
⊕ Active		8.0

21. [Assign new user or group]をおします

Authentication | Data sources | Notification channels

AWS Single Sign-On (SSO) ⓘ Pending user input

You can enable AWS SSO by creating a user or connect AWS SSO to an external identity provider (IdP) to enable users to log in to the workspace with their existing credentials. Note that when you enable SSO by creating a new user, you will need to assign this user access to the workspace before they can log in to the workspace.

[Assign new user or group](#)

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

22. SSO のユーザーが表示されていますので先程作成したユーザーを選んで[Assign users and groups]をおします

Users (0) | **Groups (0)**

Users (1)

< 1 > ⓘ

<input type="checkbox"/>	Display name	Email
<input type="checkbox"/>	Harunobu Kameda	harunobukameda@gmail.com

[Cancel](#) [Assign users and groups](#)

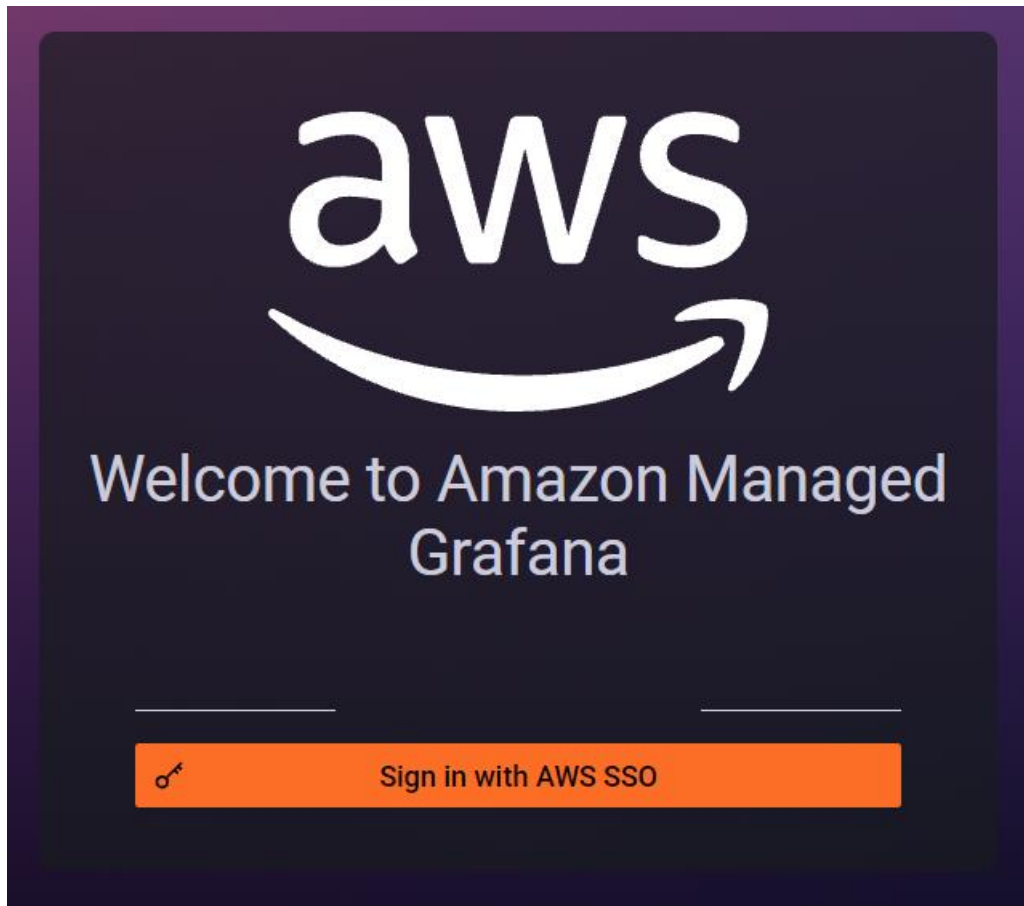
23. 作成した Workspace の詳細画面に遷移し、URL をクリックします

grafanatest [Delete](#)

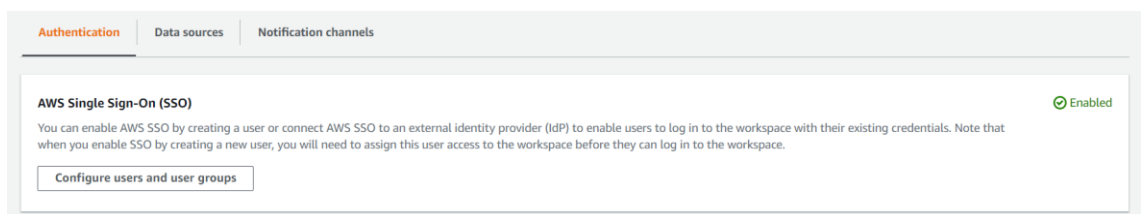
Summary [Info](#)

Description ⓘ - Grafana workspace URL g-1dda7d574b.grafana-workspace.ap-northeast-1.amazonaws.com ⓘ Status ✔ Active	Date created 2021-10-07 Authentication access AWS SSO	IAM role ⓘ arn:aws:iam::294963776963:role/service-role/AmazonGrafanaServiceRole-USEvnLhg Enterprise license Upgrade to Grafana Enterprise Grafana version 8.0
--	--	---

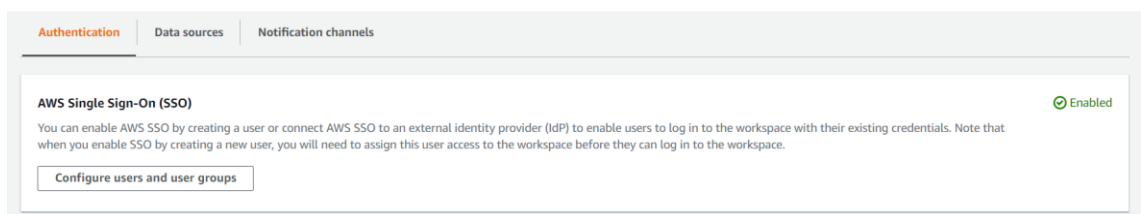
24. ログインをおこないます



25. ログインができれば、一度ブラウザを閉じて、再度 Grafana の Workspace 詳細画面から、[Configure users and user groups]をおして、Admin に昇格させます



26. ユーザーを選んで、[Make admin]ボタンをおします



27. [User Type]が Viewer から Admin に変更になったら完了です

Users (1 of 1) [Info](#)

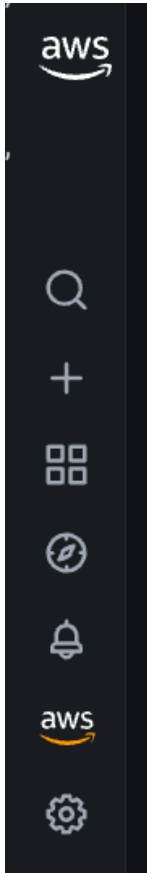
The following users have already been assigned access to Grafana.

[Make admin](#) [Unassign user](#) [Assign user](#)

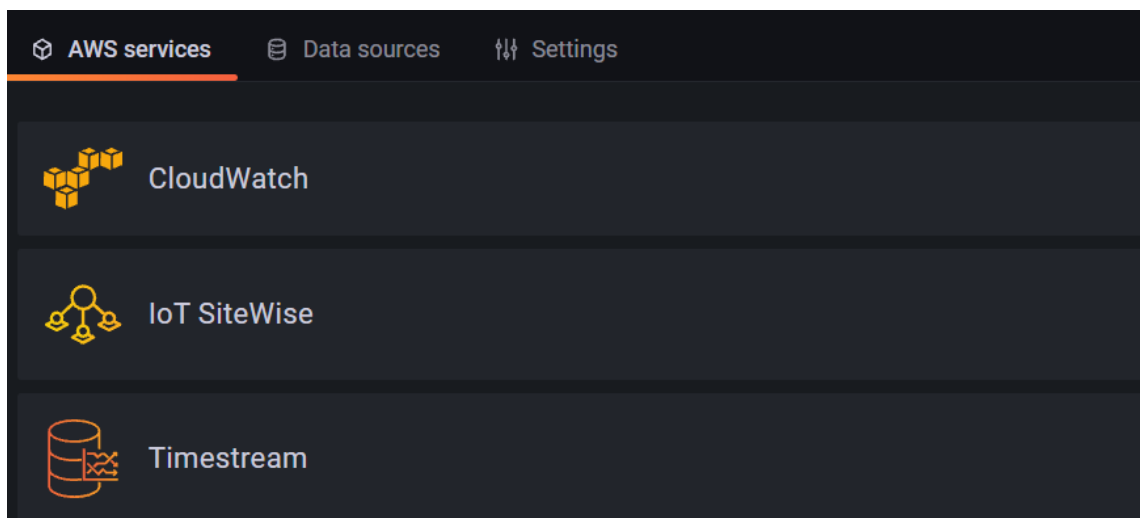
< 1 >

<input checked="" type="checkbox"/>	Full name	User type
<input checked="" type="checkbox"/>	Harunobu Kameda	Admin

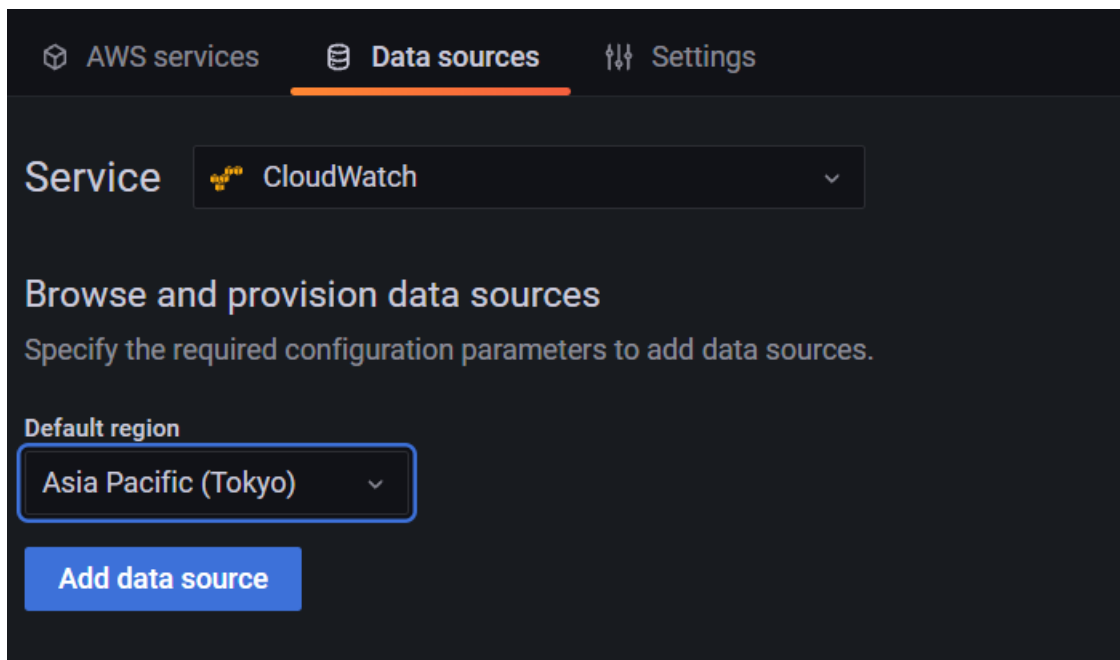
28. 今度は Grafana の左ペインから、AWS アイコンが確認できます



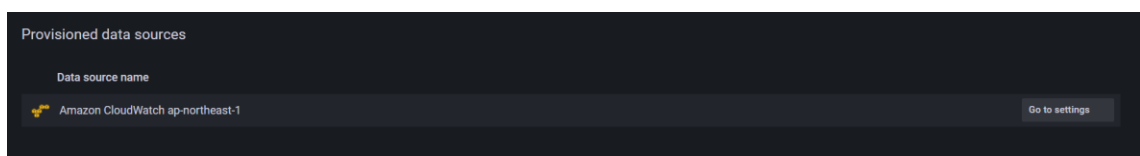
29. AWS アイコンをクリックして、[CloudWatch]をクリックします



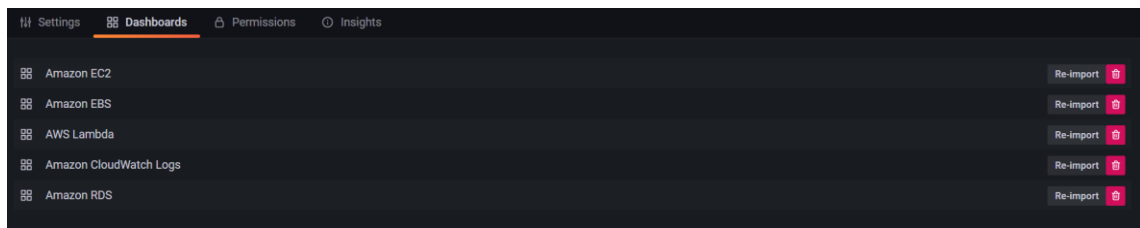
30. 作業中のリージョンを選んで[Add data source]をおします



31. [Go to settings]をおします



32. [Dashboards]タブを選んで、画面右の[import]をおします



33. EC2 や EBS をクリックすると Dashboard が出てきます

