

クラウド基礎誤植等訂正表

下記の誤りにつきまして、お詫び申し上げますとともに、訂正させていただきます。

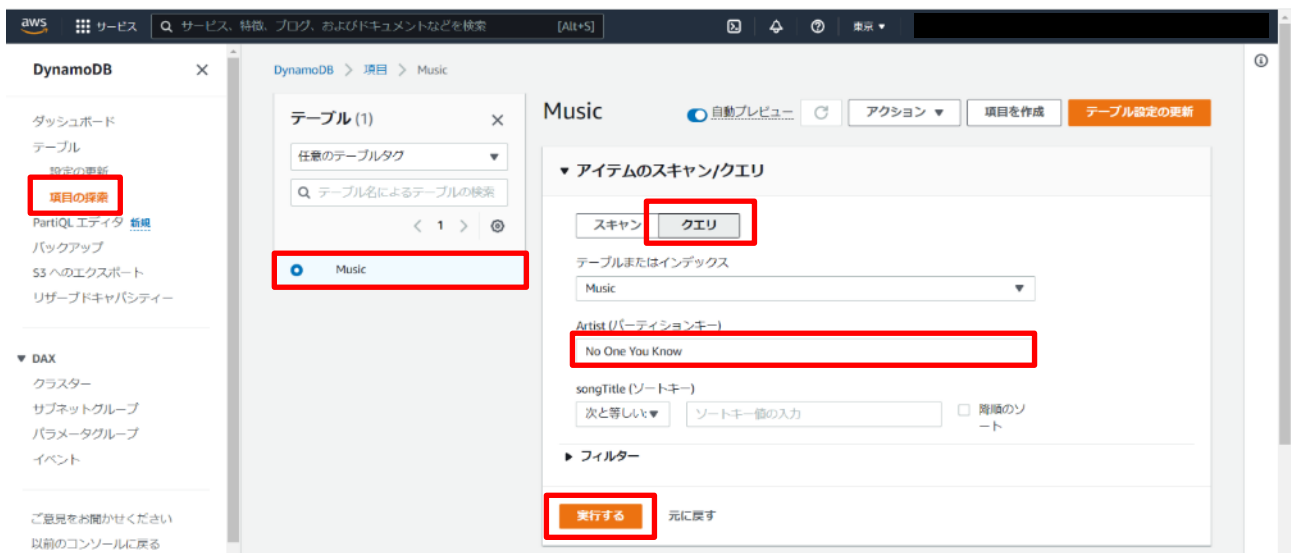
【クラウド基礎 2-1_講義資料 P26、P28】 コンソール変更

マネジメントコンソールの表示変更に伴い、講義資料と相違している画面を記載します。

【P26】



【P28】



【クラウド基礎 2-2_講義資料 P6】

テキスト内の設定画面と、現在の AWS の設定画面が異なるため以下に記載いたします。
以下、読み替えてご利用ください。

① VPC の作成

1. マネジメントコンソールでリージョンが [アジアパシフィック(東京)] になっていることを確認し、VPC の作成を行うためにサービスの一覧から [VPC] をクリックします。
2. [VPC の作成] をクリックして VPC の作成画面へ遷移したら、以下の通りに設定を行って [VPC の作成] をクリックします。
 - 作成するリソース : [VPC のみ]
 - 名前タグ : [YYYYMMDDDeployHandsOnVPC] (YYYYMMDD は本日の日付)
 - IPv4 CIDR ブロック : [10.0.0.0/16]

The screenshot shows the AWS Management Console 'Create VPC' page. The breadcrumb navigation at the top reads 'VPC > お使いの VPC > VPC を作成'. The main heading is 'VPC を作成' with a '情報' (Info) link. Below this is a descriptive sentence: 'VPC は、Amazon EC2 インスタンスなどの AWS のオブジェクトによって使用される AWS クラウドの分離された部分です。'.

The 'VPC の設定' (VPC Settings) section contains the following options:

- 作成するリソース** (Create resources): Radio buttons for 'VPC のみ' (selected) and 'VPC など' (VPC and others).
- 名前タグ - オプション** (Name tag - optional): A text input field containing '20221031DeployHandsOnVPC'.
- IPv4 CIDR ブロック** (IPv4 CIDR block): Radio buttons for 'IPv4 CIDR の手動入力' (selected) and 'IPAM 割り当ての IPv4 CIDR ブロック'.
- IPv4 CIDR**: A text input field containing '10.0.0.0/16'.
- IPv6 CIDR ブロック** (IPv6 CIDR block): Radio buttons for 'IPv6 CIDR ブロックなし' (selected), 'IPAM 割り当ての IPv6 CIDR ブロック', 'Amazon 提供の IPv6 CIDR ブロック', and 'IPv6 CIDR 所有 (ユーザー所有)'.
- テナンシー** (Tenancy): A dropdown menu set to 'デフォルト' (Default).

The 'タグ' (Tags) section includes a description: 'タグは、AWS リソースに割り当てられるラベルです。各タグはキーとオプションの値で構成されています。タグを使用してリソースを検索およびフィルタリングしたり、AWS のコストを追跡したりできます。' Below this is a table with two columns: 'キー' (Key) and '値 - オプション' (Value - optional). The 'キー' column has a search input with 'Name' and a close button. The '値 - オプション' column has a search input with '20221031DeployHandsOnVPC', a close button, and a '削除' (Delete) button. A '新しいタグを追加' (Add new tag) button is at the bottom left of the table, with a note 'さらに 49 個のタグを追加できます。' (You can add up to 49 more tags).

At the bottom right of the console, there are two buttons: 'キャンセル' (Cancel) and 'VPC を作成' (Create VPC).

【クラウド基礎 2-2_講義資料 P9】

ルートテーブルの作成

10. 続いて[ルートテーブルの作成] ボタンをクリックしてルートテーブルの作成画面に遷移したら、以下の通りに設定を行って画面下部の [ルートテーブルを作成] をクリックします。

- 名前タグ : [YYYYMMDDDeployHandsOnRouteTable] (YYYYMMDD は本日の日付)
- VPC : [YYYYMMDDDeployHandsOnVPC] (先ほど作成した VPC)

VPC > ルートテーブル > ルートテーブルを作成

ルートテーブルを作成 情報

ルートテーブルは、VPC、インターネット、および VPN 接続内のサブネット間でパケットがどのように転送されるかを指定します。

ルートテーブル設定

名前 - オプション
「Name」というキーと、指定した値を使用してタグを作成します。

20221031DeployHandsOnRouteTable

VPC
このルートテーブルに使用する VPC。

VPC を選択

Q |

vpc-093b03d3ae66308ac (20221031DeployHandsOnVPC)

vpc-0dece5d6e9174d094 (デフォルト)

タグは、AWS リソースに割り当てられるラベルです。各タグはキーとオプションの値で構成されています。タグを使用してリソースを検索およびフィルタリングしたり、AWS のコストを追跡したりできます。

キー

値 - オプション

Q Name X

Q 20221031DeployHandsOnRoute X

削除

新しいタグを追加

さらに 49 個のタグを追加できます。

キャンセル

ルートテーブルを作成

11. ルートテーブルの作成が完了したら、作成したルートテーブルを選択して [サブネットの関連付け] タブから [サブネットの関連付けの編集] をクリックします。

新しい VPC エクス
ペリエンス
ご意見をお聞かせください

VPC ダッシュボード
EC2 グローバルビュー
新規
VPC でフィルタリング:
VPC を選択

▼ 仮想プライベートクラ
ウド
お使いの VPC
サブネット
ルートテーブル
インターネットゲート
ウェイ
Egress-only インターネ
ットゲートウェイ
キャリアゲートウェイ
DHCP オプションセッ
ト
Elastic IP
マネージドプレフィッ
クスリスト
エンドポイント
エンドポイントサービ
ス
NAT ゲートウェイ
ピアリング接続

ルートテーブル rtb-0d5edf48f24ec3d | 20221031DeployHandsOnRouteTable は正常に作成されました。

VPC > ルートテーブル > rtb-0d5edf48f24ec3d

rtb-0d5edf48f24ec3d / 20221031DeployHandsOnRouteTable

アクション ▼

① Reachability Analyzer でネットワーク接続を確認できるようになりました Reachability Analyzer の実行 X

詳細 情報

ルートテーブル ID rtb-0d5edf48f24ec3d	メイン いいえ	明示的なサブネットの関連付 け -	Edge の関連付け -
VPC vpc-093b03d3ae66308ac 20221031DeployHandsOnVPC	所有者 ID 8626666861849		

ルート サブネットの関連付け Edge の関連付け ルート伝播 タグ

明示的なサブネットの関連付け (0)

サブネットの関連付けの検索

サブネットの関連付けを編集

サブネット ID	IPv4 CIDR
----------	-----------

12. [サブネットの関連付けを編集]画面では先ほど作成した [YYYYMMDDDeployHandsOnPublicSubnet] を選
択して、画面下部の[関連付けを保存] をクリックします。

VPC > ルートテーブル > rtb-0d5edf48f24ec3d > サブネットの関連付けを編集

サブネットの関連付けを編集

このルートテーブルに関連付けられているサブネットを変更

利用可能なサブネット (1/1)

サブネットの関連付けをフィルタリング

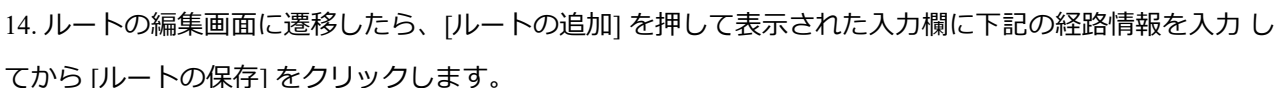
<input checked="" type="checkbox"/>	名前	サブネット ID	IPv4 CIDR	IPv6 CIDR	ルートテーブル ID
<input checked="" type="checkbox"/>	20221031DeployHandsOnPublicSubnet	subnet-072746d29e9596681	10.0.1.0/24	-	メイン (rtb-056761c6099)

選択されたサブネット

subnet-072746d29e9596681 / 20221031DeployHandsOnPublicSubnet X

キャンセル 関連付けを保存

13. サブネットの関連付けの編集が完了したら、今度は [ルート] タブより [ルートの編集] をクリックします。



- VPC > ルートテーブル > rtb-0d5edfbc48f24ec3d > ルートを編集

ルートを編集

送信先	ターゲット	ステータス	伝播済み
10.0.0.0/16	Q local	アクティブ	いいえ
Q 0.0.0.0/0	<div>Q </div> <ul style="list-style-type: none"> キャリアゲートウェイ コアネットワーク Egress Only インターネットゲートウェイ ゲートウェイロードバランサーのエンドポイントインスタンス インターネットゲートウェイ ローカル NAT ゲートウェイ ネットワークインターフェイス Outpost Local Gateway ピアリング接続 Transit Gateway 仮想プライベートゲートウェイ 	-	いいえ

ルートを追加

キャンセル プレビュー 変更を保存

インターネットゲートウェイを選択すると、自分の作成した IGW が表示されるので
クリックし、以下と同じような画面になれば問題ありません。そのまま[変更を保存]を押しましょう。

VPC > ルートテーブル > rtb-0d5edfbe48f24ec3d > ルートを編集

ルートを編集

送信先	ターゲット	ステータス	伝播済み
10.0.0.0/16	<input type="text" value="local"/>	🟢 アクティブ	いいえ
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-0cbe8714c9a761986"/>	-	いいえ

キャンセル

【クラウド基礎 2-2_講義資料 P14~P17】

ステップ 3. EC2 インスタンス（Web/AP）を作成する

3. EC2 インスタンスの作成ウィザードで以下の通りに設定を行います。

① ステップ 1: インスタンスの名前を設定。

Name : [YYYYMMDDDeployHandsOnWebInstance] (YYYYMMDD は本日の日付)

② ステップ 2: Amazon マシンイメージ (AMI) [Amazon Linux 2 AMI (HVM), SSD Volume Type]を選択

EC2 > インスタンス > インスタンスを起動

インスタンスを起動

Amazon EC2 では、AWS クラウドで実行される仮想マシン (インスタンス) を作成できます。以下の簡単なステップに従って、すばやく開始できます。

名前とタグ

名前
20221031DeployHandsOnWebInstance [さらにタグを追加](#)

▼ アプリケーションおよび OS イメージ (Amazon マシンイメージ)

AMI は、インスタンスの起動に必要なソフトウェア設定 (オペレーティングシステム、アプリケーションサーバー、アプリケーション) を含むテンプレートです。お探しのものが以下に表示されない場合は、AMI を検索または参照してください。

Q 何千ものアプリケーションイメージと OS イメージを含むカタログ全体を検索します。

最新 | **クイックスタート**

Amazon Linux macOS Ubuntu Windows Red Hat

Amazon マシンイメージ (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0de5311b2a443fb89 (64 ビット (x86)) / ami-082dd9d89994d3690 (64 ビット (Arm))
仮想化: hvm ENA 有効: true ルートデバイスタイプ: ebs

説明
Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2

アーキテクチャ
64 ビット (x86)

AMI ID
ami-0de5311b2a443fb89 [快速読みプロバイダー](#)

③ ステップ 3:インスタンスタイプの選択 [t2,micro]を選択

④ ステップ 4:キーペアの作成

表示された画面で[新しいキーペアの作成]というリンクを押下しましょう。

その後下記の名前を入力し、[キーペアを作成]をクリックします。

作成後は、キーペア名の箇所に作成したキーペアの名前が表示されるようになります。

- キーペア：[新しいキーペアの作成]
- キーペア名：[YYYYMMDDDeployHandsOnKeyPair]（YYYYMMDD は本日の日付）
※ダウンロードしたキーペアは EC2 インスタンスへの接続時に使いますので、
適切に保管しておいてください。

▼ インスタンスタイプ 情報

インスタンスタイプ

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB メモリ
オンデマンド Linux 料金: 0.0152 USD 1 時間あたり
オンデマンド Windows 料金: 0.0198 USD 1 時間あたり

Compare instance types

▼ キーペア (ログイン) 情報

キーペアを使用してインスタンスに安全に接続できます。インスタンスを起動する前に、選択したキーペアにアクセスできることを確認してください。

キーペア名 - 必須

20221031DeployHandsOnKeyPair

新しいキーペアの作成

キーペアを作成

キーペアを使用すると、インスタンスに安全に接続できます。

以下にキーペアの名前を入力します。指示が表示されたら、ご使用のコンピューターの安全でアクセス可能な場所に、そのキーペアを保存します。後でインスタンスに接続するときに必要になります。 [詳細はこちら](#)

キーペア名

20221031DeployHandsOnKeyPair

名前には最大 255 文字の ASCII 文字を使用できます。先頭または末尾にスペースを含めることはできません。

キーペアのタイプ

☒ RSA
RSA で暗号化されたプライベートとパブリックのキーペア

☐ ED25519
ED25519 で暗号化されたプライベートキーとパブリックのキーペア (Windows インスタンスではサポートされません)

プライベートキーファイル形式

☒ .pem
OpenSSH で使用する場合

☐ .ppk
PuTTY で使用する場合

キャンセル キーペアを作成

⑤ ステップ 4: インスタンスの詳細の設定

ネットワーク設定の[編集]を押し、以下の内容を設定してください。

The screenshot shows the 'Network settings' section of the AWS Management Console. A red box highlights the 'Edit' button in the top right corner. Below the button, the following settings are visible:

- ネットワーク 情報**
vpc-0dece5d6e9174d094
- サブネット 情報**
優先順位なし (アベイラビリティゾーンのデフォルトサブネット)
- パブリック IP の自動割り当て 情報**
有効化
- ファイアウォール (セキュリティグループ) 情報**
セキュリティグループとは、インスタンスのトラフィックを制御する一連のファイアウォールルールです。特定のトラフィックがインスタンスに到達できるようにルールを追加します。

At the bottom, there are two radio buttons: ☒ セキュリティグループを作成する and ☐ 既存のセキュリティグループを選択する. Below these, a note states: 次のルールを使用して、「launch-wizard-1」という新しいセキュリティグループを作成します。

- ネットワーク : [YYYYMMDDDeployHandsOnVPC]
- サブネット : [YYYYMMDDDeployHandsOnPublicSubnet] ※パブリックサブネットを選択
- 自動割り当てパブリック IP : [有効]
- プライマリ IP : [10.0.1.10]

⑥ ステップ 6: セキュリティグループの設定

- セキュリティグループの割り当て : [新しいセキュリティグループを作成する]
- セキュリティグループ名 : [YYYYMMDDDeployHandsOnWebSecurityGroup]
(YYYYMMDD は本日の日付)
- 説明 : [Security Group for YYYYMMDD Deploy Hands On Web Instance]
(YYYYMMDD は本日の日付)
- ルール :
 - タイプ : SSH
 - ソース : [My IP]

※[My IP]とは、操作を行っているパソコンのパブリック IP アドレスのことです。

※自分のパソコンから SSH を使ったアプリケーションで、この EC2 インスタンスにアクセス することを許可するルールです。

▼ ネットワーク設定 情報

VPC - 必須 情報
vpc-093b03d3ae66308ac (20221031DeployHandsOnVPC)
10.0.0.0/16

サブネット 情報
subnet-072746d29e9596681 20221031DeployHandsOnPublicSubnet
VPC: vpc-093b03d3ae66308ac 所属: 862066801049
アベイラビリティゾーン: ap-northeast-1a 利用可能な IP アドレス: 251
CIDR: 10.0.1.0/24

パブリック IP の自動割り当て 情報
有効化

ファイアウォール (セキュリティグループ) 情報
セキュリティグループとは、インスタンスのトラフィックを制御する一連のファイアウォールルールです。特定のトラフィックがインスタンスに到達できるようにルールを追加します。

☒ セキュリティグループを作成する ☐ 既存のセキュリティグループを選択する

セキュリティグループ名 - 必須
20221031DeployHandsOnWebSecurityGroup

説明 - 必須 情報
Security Group for 20221031 Deploy Hands On Web Instance

インバウンドセキュリティグループのルール
▼ セキュリティグループルール 1 (TCP, 22, 39.111.221.119/32) 削除

タイプ 情報	プロトコル 情報	ポート範囲 情報
ssh	TCP	22

Source type 情報
My IP

名前 情報
Add CIDR, prefix list or security group

説明 - optional 情報
例: 管理者のデスクトップの SSH

39.111.221.119/32 X

セキュリティグループルールを追加

▶ 高度なネットワーク設定

⑨ インスタンスの作成

最後に[インスタンスの作成]をクリックします。その後、EC2 インスタンスの作成が始まります。
その後、クラウド基礎 2-2-講義資料_1.2 P17 の記載とおり、IP アドレスを控えておいてください。

【クラウド基礎 2-2_講義資料 P18~21】

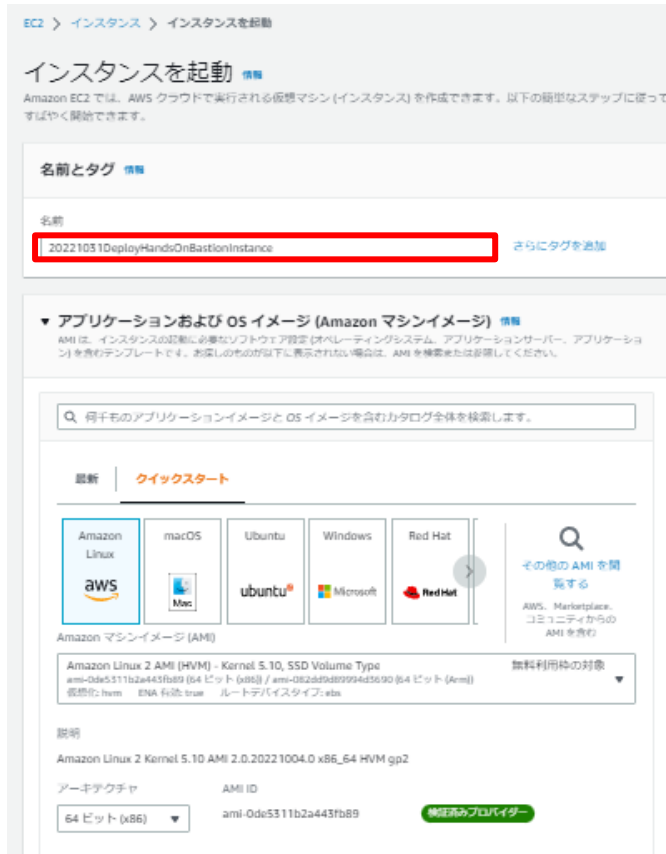
ステップ 4. EC2 インスタンス（踏み台）を作成する

1. 先ほどと同じように、EC2 インスタンスの作成ウィザードで以下の通りに設定を行います。

①ステップ 1:インスタンスの名前を設定。

- Name : [YYYYMMDDDeployHandsOnBastionInstance] (YYYYMMDD は本日の日付)

②ステップ 2: Amazon マシンイメージ (AMI) [Amazon Linux 2 AMI (HVM), SSD Volume Type]を選択



③ ステップ 3:インスタンスタイプの選択 [t2,micro]を選択

④ ステップ 4:キーペアの作成

表示された画面で[新しいキーペアの作成]というリンクを押下しましょう。

その後下記の名前を入力し、[キーペアを作成]をクリックします。

作成後は、キーペア名の箇所に作成したキーペアの名前が表示されるようになります。

- キーペア：[新しいキーペアの作成]
- キーペア名：[YYYYMMDDDeployHandsOnBationKeyPair]（YYYYMMDD は本日の日付）

※ダウンロードしたキーペアは EC2 インスタンスへの接続時に使いますので、適切に保管しておいてください。

▼ インスタンスタイプ 情報

インスタンスタイプ

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GB メモリ

オンデマンド Linux 料金: 0.0152 USD 1 時間あたり

オンデマンド Windows 料金: 0.0198 USD 1 時間あたり

Compare instance types

▼ キーペア (ログイン) 情報

キーペアを使用してインスタンスに安全に接続できます。インスタンスを起動する前に、選択したキーペアにアクセスできることを確認してください。

キーペア名 - 必須

20221031DeployHandsOnBationKeyPair

新しいキーペアの作成

キーペアを作成

キーペアを使用すると、インスタンスに安全に接続できます。

以下にキーペアの名前を入力します。指示が表示されたら、ご使用のコンピューターの安全でアクセス可能な場所に、そのキーペアを保存します。後でインスタンスに接続するときに必要になります。詳細はこちら

キーペア名

20221031DeployHandsOnBationKeyPair

名前には最大 255 文字の ASCII 文字を使用できます。先頭または末尾にスペースを含めることはできません。

キーペアのタイプ

☒ RSA
RSA で暗号化されたプライベートとパブリックのキーペア

☐ ED25519
ED25519 で暗号化されたプライベートキーとパブリックのキーペア (Windows インスタンスではサポートされません)

プライベートキーファイル形式

☒ .pem
OpenSSH で使用する場合

☐ .ppk
PuTTY で使用する場合

キャンセル キーペアを作成

⑤ ステップ 5:インスタンスの詳細の設定

ネットワーク設定の[編集]を押し、以下の内容を設定してください。



▼ ネットワーク設定 情報

編集

ネットワーク 情報
vpc-0dece5d6e9174d094

サブネット 情報
優先順位なし (アベイラビリティゾーンのデフォルトサブネット)

パブリック IP の自動割り当て 情報
有効化

ファイアウォール (セキュリティグループ) 情報
セキュリティグループとは、インスタンスのトラフィックを制御する一連のファイアウォールルールです。特定のトラフィックがインスタンスに到達できるようにルールを追加します。

☒ セキュリティグループを作成する ☐ 既存のセキュリティグループを選択する

次のルールを使用して、「launch-wizard-1」という新しいセキュリティグループを作成します。

- ネットワーク : [YYYYMMDDDeployHandsOnVPC]
- サブネット : [YYYYMMDDDeployHandsOnPublicSubnet] ※パブリックサブネットを選択
- 自動割り当てパブリック IP : [有効]
- プライマリ IP : [10.0.1.10]

⑥ ステップ 6:セキュリティグループの設定

- セキュリティグループの割り当て : [新しいセキュリティグループを作成する]
- セキュリティグループ名 : [YYYYMMDDDeployHandsOnBastionSecurityGroup]
(YYYYMMDD は本日の日付)
- 説明 : [Security Group for YYYYMMDD Deploy Hands On Bastion Instance]
(YYYYMMDD は本日の日付)
- ルール :
 - タイプ : SSH
 - ソース : [My IP]

※[My IP]とは、操作を行っているパソコンのパブリック IP アドレスのことです。

※自分のパソコンから SSH を使ったアプリケーションで、この EC2 インスタンスにアクセス することを許可するルールです。

【クラウド基礎 2-2_講義資料 P25】 誤記

5. [セキュリティグループの作成] をクリックして～の設定内容にてスペルミスが見つかったため、訂正させていただきます。

【誤】

- 説明 : [Secyruity Group for **YYYYMMDD** Deploy Hands On DB Instance]

【正】

- 説明 : [Security Group for **YYYYMMDD** Deploy Hands On DB Instance]

【誤】

- インバウンドルール

ソース 1 : [YYYYMMDDHandsOnWebSecurityGroup のセキュリティグループ ID]

【正】

- インバウンドルール

ソース 1 : [YYYYMMDD**Deploy**HandsOnWebSecurityGroup のセキュリティグループ ID]

【誤】

- インバウンドルール

ソース 2 : [YYYYMMDDHandsOnBastionSecurityGroup のセキュリティグループ ID]

【正】

- インバウンドルール

ソース 2 : [YYYYMMDD**Deploy**HandsOnBastionSecurityGroup のセキュリティグループ ID]

【クラウド基礎 2-2_講義資料 P26】

➤ 接続 ※赤の箇所はテキストに記載がなかった箇所です。

- **コンピューティングリソース** : [EC2 コンピューティングリソースに接続しない]
- VPC : [YYYYMMDDDeployHandsOnVPC]
- サブネットグループ : [deployhandsonsubnetgroup]
- パブリックアクセス可能 : [なし]
- VPC セキュリティグループ : [既存の選択]
- **既存の VPC セキュリティグループ** : [YYMMDDDeployHandsOnDBSecurityGroup]
- アベイラビリティーゾーン : [ap-northeast-1a]

接続 情報

コンピューティングリソース

このデータベースのコンピューティングリソースへの接続を設定するかどうかを選択します。接続を設定すると、コンピューティングリソースがこのデータベースに接続できるように、接続設定が自動的に変更されます。

☒ EC2 コンピューティングリソースに接続しない

このデータベースのコンピューティングリソースへの接続を設定しないでください。後でコンピューティングリソースへの接続を手動で設定できます。

☐ EC2 コンピューティングリソースに接続

このデータベースの EC2 コンピューティングリソースへの接続を設定します。

Virtual Private Cloud (VPC) 情報

VPC を選択します。VPC は、この DB インスタンスの仮想ネットワーク環境を定義します。

20221031DeployHandsOnVPC (vpc-093b03d3ae66308ac)

▼

対応する DB サブネットグループがある VPC のみが表示されます。

☒ データベースの作成後に、VPC を変更することはできません。

DB サブネットグループ 情報

DB サブネットグループを選択します。DB サブネットグループは、選択した VPC で DB インスタンスが使用できるサブネットと IP 範囲を定義します。

deployhandsonsubnetgroup

▼

パブリックアクセス 情報

☐ あり

RDS はデータベースにパブリック IP アドレスを割り当てます。Amazon EC2 インスタンスと VPC 外の他のリソースはデータベースに接続できます。VPC 内のリソースもデータベースに接続できます。データベースに接続できるリソースを設定する VPC セキュリティグループを 1 つ以上選択します。

☒ なし

RDS はデータベースにパブリック IP アドレスを割り当てません。Amazon EC2 インスタンスと VPC 内の他のリソースのみがデータベースに接続できます。データベースに接続できるリソースを設定する VPC セキュリティグループを 1 つ以上選択します。

VPC セキュリティグループ (ファイアウォール) 情報

データベースへのアクセスを許可する VPC セキュリティグループを 1 つ以上選択します。セキュリティグループのルールで適切な受発トラフィックが許可されていることを確認します。

☒ 既存の選択

既存の VPC セキュリティグループの選択

☐ 新規作成

新しい VPC セキュリティグループの作成

既存の VPC セキュリティグループ

Choose one or more options

▼

20221031DeployHandsOnDBSecurityGroup

×

アベイラビリティーゾーン 情報

ap-northeast-1a

▼

▶ 追加設定

16

【クラウド基礎 2-2_講義資料 P27】

➤ モニタリング

チェックを外す



データベース認証

データベース認証オプション 情報

☒ パスワード認証
データベースのパスワードを使用して認証します。

☐ パスワードと Kerberos 認証
承認されたユーザーに、Kerberos 認証を使ってこの DB インスタンスで認証を行うことを許可するディレクトリを選択します。

モニタリング

Performance Insights 情報

☐ Performance Insights をオンにする 情報

▶ 追加設定
拡張モニタリング

【クラウド基礎 2-2_講義資料 P27】 ※赤の箇所はテキストに記載がなかった箇所です。

➤ 追加設定

- 最初のデータベース名：[oracledb]
- DB パラメータグループ：[default.oracle-se2-19]（初期値）
- オプショングループ：[default.oracle-se2-19]（初期値）
- 文字セット：[AL32UTF8]
- 自動バックアップの有効化：[無効]（チェックを外す）
- バックアップの保持期間：[7 日間] ←上記チェックを外すと非表示になる
- バックアップウィンドウ：[設定なし] ←上記チェックを外すと非表示になる
- スナップショットにタグをコピー：[有効] ←上記チェックを外すと非表示になる
- 暗号を有効化：[無効]（チェックを外す）
- ログのエクスポート
 - ・アラートログ : [無効]
 - ・監査ログ : [無効]
 - ・リスナーログ : [無効]
 - ・ Oracle Management Agent ログ : [無効]
 - ・トレースログ : [無効]
- メンテナンス
 - ・マイナーバージョン自動アップグレードの有効化：[無効]
- メンテナンスウィンドウ：[設定なし]
- 削除保護の有効化：[無効]

【実際の画面】

▼ 追加設定

データベースオプション、暗号化をオフにしました、バックアップをオフにしました、バックトラックをオフにしました、メンテナンス、CloudWatch Logs、削除保護をオフにしました。

データベースの選択肢

最初のデータベース名 [情報](#)

oracledb

データベース名を指定しないと、Amazon RDS はデータベースを作成しません。

DB パラメータグループ [情報](#)

defaultoracle-se2-19

オプショングループ [情報](#)

defaultoracle-se2-19

文字セット

AL32UTF8

バックアップ

- ☐ 自動バックアップを有効にします
データベースのポインタインタイムスナップショットを作成します。

暗号化

- ☐ 暗号を有効化
選択すると対象のインスタンスを暗号化します。マスターキー ID とエイリアスは、AWS Key Management Service コンソールを使用して作成した後に、リストに表示されます。 [情報](#)

ログのエクスポート

Amazon CloudWatch Logs に発行するログタイプを選択します。

- ☐ アラートログ
☐ 監査ログ
☐ リスナーログ
☐ Oracle Management Agent ログ
☐ トレースログ

IAM ロール

サービスにリンクされた以下のロールは、CloudWatch Logs にログを発行するために使用されます。

RDS サービスにリンクされたロール

- ④ 全般、スロークエリ、監査ログがオンになっていることを確認してください。デフォルトではエラーログが有効になっています。詳細は [こちら](#)

メンテナンス

マイナーバージョン自動アップグレード [情報](#)

- ☐ マイナーバージョン自動アップグレードの有効化
マイナーバージョン自動アップグレードを有効にすると、新しいマイナーバージョンがリリースされたときに自動的にアップグレードされます。自動アップグレードは、データベースのメンテナンスウィンドウに行われます。

メンテナンスウィンドウ [情報](#)

Amazon RDS によってデータベースに適用されている保留中の変更またはメンテナンスの期間を選択します。

- ☐ ウィンドウを選択
☒ 設定なし

削除保護

- ☐ 削除保護の有効化
データベースが誤って削除されるのを防ぎます。このオプションが有効になっている場合、データベースを削除することはできません。

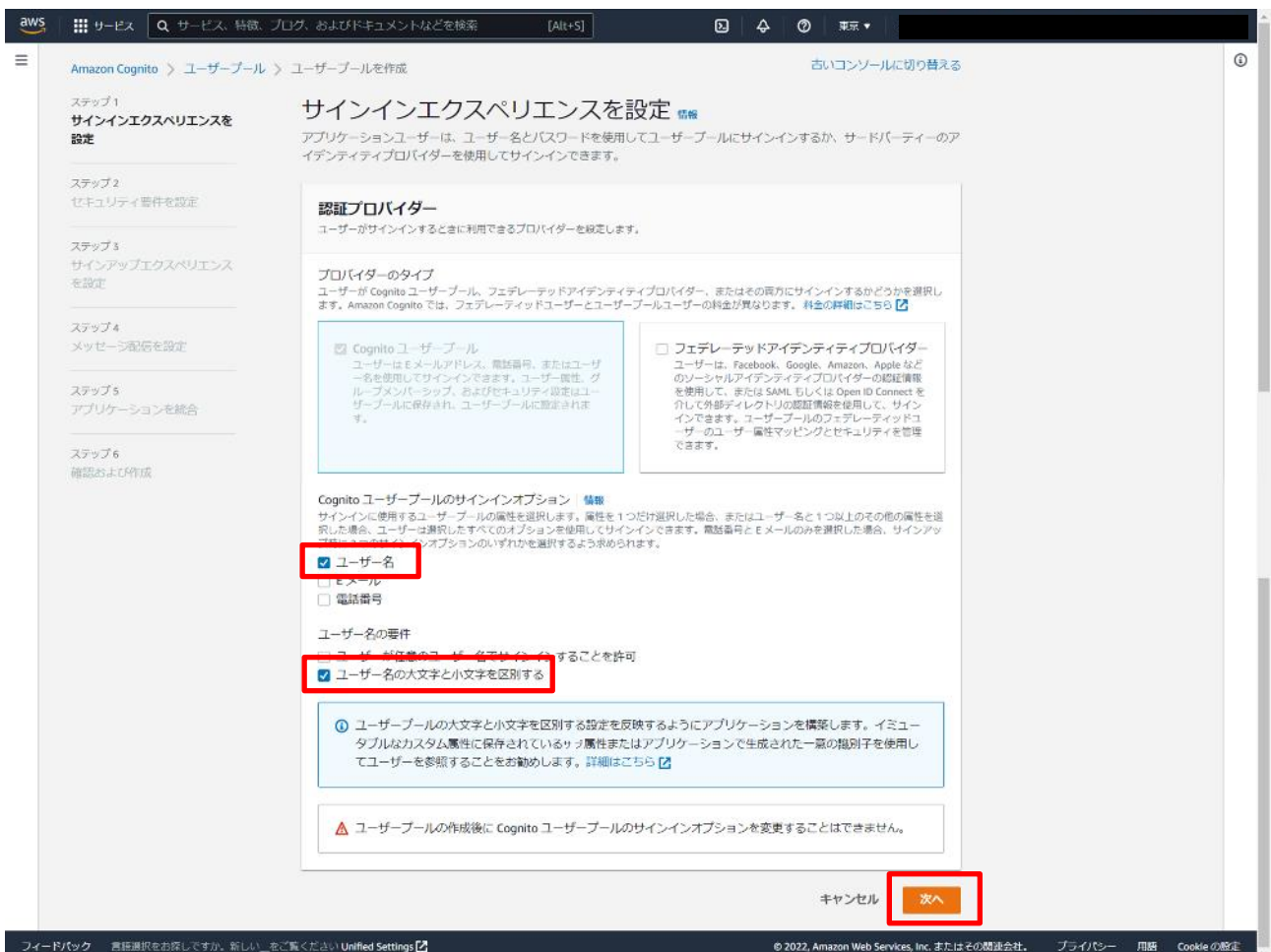
【クラウド基礎 3-7_講義資料 P52～P57】 コンソール変更

マネジメントコンソールの表示変更に伴い、講義資料と相違している画面を記載します。

【P52】



【P54】



【P54】

aws

サービス

サービス、特徴、ブログ、およびドキュメントなどを検索

[Alt+S]

東京

Amazon Cognito ユーザープール ユーザープールを作成

古いコンソールに切り替える

ステップ 1
サインインエクスペリエンスを設定

ステップ 2
セキュリティ要件を設定

ステップ 3
サインアップエクスペリエンスを設定

ステップ 4
メッセージ配信を設定

ステップ 5
アプリケーションを統合

ステップ 6
確認および作成

セキュリティ要件を設定

多要素認証に加えて強力なパスワード要件を設定し、アプリケーションユーザーが誤って認証情報を漏えいするのを防ぎます。

パスワードポリシー

パスワードポリシーを作成して、ユーザーが設定できるパスワードの長さや複雑さを定義します。

パスワードポリシーモード

☐ Cognito のデフォルト
デフォルトのパスワード要件を使用します。

☒ カスタム
ユーザーが定義するパスワード要件を使用します。

パスワードの最小文字数

8 文字

6〜99 の数字に必要があります。パスワードの長さが 8 文字以上であることを必須化することを強くお勧めします。

パスワード要件

☐ 少なくとも 1 つの数字を含む

☐ 少なくとも 1 つの特殊文字 (! \$ % ' () * + , - . : ; = < > ? [\] ^ _ { | } ~ ` ' +) を含む

☐ 少なくとも 1 つの大文字を含む

☐ 少なくとも 1 つの小文字を含む

管理者によって設定された仮パスワードの有効期限:

7 日

0〜365 の数字に必要があります。

多要素認証

ユーザーのサインインプロセス中に多要素認証 (MFA) を強制することで、アプリケーションへの安全なアクセスを設定します。タイムベースドワンタイムパスワード (TOTP) を使用した MFA 要素は、Cognito のホストされた UI と統合されておらず、API を使用して実装する必要があります。MFA 設定は、すべてのアプリケーションクライアントに適用されます。

MFA の強制

☐ MFA を必須にする - 推奨
ユーザーは、サインイン時に追加の認証要素を指定する必要があります。

☐ オプションの MFA
ユーザーは 1 つの認証要素でサインインでき、追加の認証要素を追加することもできます。

☒ MFA なし
ユーザーは 1 つの認証要素でのみサインインできます。これは、最も安全性が低いオプションです。

ユーザーアカウントの復旧

ユーザーがパスワードを忘れた際にアカウントを復旧する方法を設定します。受信者のメッセージとデータレートが適用されます。

セルフサービスのアカウントの復旧

☒ セルフサービスのアカウントの復旧を有効化 - 推奨
ユーザープールでパスワードを忘れた場合のオペレーションを許可します。ホストされた UI サインインページで、「パスワードを忘れた場合」のリンクが表示されます。この機能が有効になっていない場合、管理者は Cognito API を使用してパスワードをリセットします。

ユーザーアカウントの復旧メッセージの配信方法

ユーザーがアカウントの復旧コードをリクエストしたときに、ユーザープールがメッセージを配信する方法を選択します。SMS メッセージは Amazon SNS によって個別に課金されます。E メールメッセージは Amazon SES によって個別に課金されます。料金の詳細については、こちらを参照してください。

☐ E メールのみ

☐ SMS のみ

☐ 使用できる場合は E メール、それ以外の場合は SMS

☒ 使用可能な場合は SMS、それ以外の場合は E メール

使用可能な場合は SMS、それ以外の場合は E メール、そして、MFA にも使用している場合は、SMS でパスワードをリセットすることを許可します

ユーザーが電話番号をパスワード回復メカニズムと多要素認証要素の両方として使用できるため、選択されたオプションは推奨されません。

キャンセル

戻る

次へ

フィードバック

言語選択をお探しのですか。新しい UI をご覧ください Unified Settings

© 2022, Amazon Web Services, Inc. またはその関連会社。

プライバシー

用語

Cookie の設定

20

aws サービス Q サービス、特徴、ブログ、およびドキュメントなどを検索 [Alt+S]

Amazon Cognito ユーザープール ユーザープールを作成 古いコンソールに切り替える

ステップ 1 サインインエクスペリエンスを設定

ステップ 2 セキュリティ要件を設定

ステップ 3 **サインアップエクスペリエンスを設定**

ステップ 4 メッセージ配信を設定

ステップ 5 アプリケーションを統合

ステップ 6 確認および作成

サインアップエクスペリエンスを設定 情報

新しいユーザーがサインアップ時に自分のアイデンティティを検証する方法と、ユーザーのサインアップフロー中に必須にする属性とオプションにする属性を決定します。

セルフサービスのサインアップ 情報

アプリケーションの新規ユーザーが自らアカウントに登録できるかどうかを選択します。

自己登録 情報

☒ 自己登録を有効化

ホストされた UI のサインインページに [サインアップ] リンクを表示し、新しいユーザーアカウントを作成するために /v2 API を使用することを許可します。この機能が有効になっていない場合、フェデレーションおよび管理 API オペレーションがユーザープロファイルを作成します。

属性検証とユーザーアカウントの確認

Cognito アシスト型とセルフマネージド型のユーザー属性の検証およびアカウントの確認から選択します。サインイン、アカウントの復旧、および MFA に使用できるのは、検証済みの属性のみです。ユーザーによるサインインが許可される前に、属性検証またはユーザープール管理の検証によってユーザーアカウントが確認されている必要があります。

Cognito アシスト型の検証および確認 情報

☒ Cognito が検証と確認のためにメッセージを自動的に送信することを許可 - 推奨

Cognito は、ユーザーが入力する必要があるコードを含む検証メッセージを送信します。新しいユーザーの場合、これにより、属性が検証され、アカウントが確認されます。この機能が有効になっていない場合、管理 API オペレーションと Lambda トリガーによってユーザーの検証と確認が行われます。

検証する属性 情報

Cognito による検証メッセージの送信先となるユーザーの連絡先属性を選択します。SMS の使用時に受信者メッセージの料金およびデータの料金が適用されます。

☐ SMS メッセージを送信、電話番号を検証

ユーザーがサインイン、MFA、およびアカウントの復旧のために電話番号を使用することを許可するため、SMS で検証します。SMS メッセージは Amazon SNS によって別途課金されます。

☒ Eメールのメッセージを送信、Eメールアドレスを検証

ユーザーがサインイン、MFA、およびアカウントの復旧のために Eメールアドレスを使用することを許可するため、Eメールで検証します。Eメールメッセージは Amazon SES によって別途課金されます。

☐ 電話番号が利用可能な場合は SMS メッセージを送信し、それ以外の場合は Eメールメッセージを送信する

ユーザーアカウントの作成時に Eメールと電話番号の両方を検証する場合は、カスタムコードを構築する必要があります。

属性変更の確認 情報

☐ 未完了の更新があるときに元の属性値をアクティブに保つ - 推奨

Eメールまたは電話番号属性の値を更新する場合、ユーザーは新しい値を確認する必要があります。ユーザーは新しい値を確認するまで、メッセージを受信し、元の値でサインインできます。この機能を有効にしないと、ユーザーは新しい値を確認するまでその属性でサインインできなくなります。

必須の属性 情報

新しいユーザーの作成時に必要な属性を選択します。Cognito は、OpenID Connect (OIDC) 標準に基づいて一連の標準属性をすべてのユーザーに割り当てます。

以前の選択に基づく必須属性

追加の必須属性

属性を選択

email X

⚠ このユーザープールの作成後に、必須属性を変更することはできません。

カスタム属性 - オプション

最大 50 個のカスタム属性を追加してサインアップエクスペリエンスをパーソナライズします。ユーザープールの作成後にカスタム属性名を変更することはできません。

キャンセル 戻る **次へ**

フィードバック 言語選択をお探しますが、新しい...をご覧ください Unified Settings

© 2022, Amazon Web Services, Inc. またはその関連会社。 プライバシー 用語 Cookie の設定

【P54】

aws サービス 🔍 サービス、特徴、ブログ、およびドキュメントなどを検索 [Alt+S] 東京

Amazon Cognito > ユーザーグループ > ユーザーグループを作成 古いコンソールに切り替える

ステップ 1
サインインエクスペリエンスを設定

ステップ 2
セキュリティ要件を設定

ステップ 3
サインアップエクスペリエンスを設定

ステップ 4
メッセージ配信を設定

ステップ 5
アプリケーションを統合

ステップ 6
確認および作成

メッセージ配信を設定 情報

Amazon Cognito は、Amazon SES と Amazon SNS を使用して、E メールや SMS メッセージをアプリケーションユーザーに送信します。メッセージについては、追加の SES および SNS コストが発生する場合があります。

E メール

ユーザーグループがユーザーに E メールメッセージを送信する方法を設定します。

E メールプロバイダー 情報

- ☐ Amazon SES で E メールを送信 - 推奨
アカウントの Amazon SES 検証済みアイデンティティを使用して E メールを送信します。Eメールの量が多く、本番ワークロードの場合は、このオプションをお勧めします。
- ☒ Cognito で E メールを送信
Cognito のデフォルトの E メールアドレスは、開発を開始するに際しての 一時的なものとして使用します。1 日に最大 50 通の E メールを送信するために使用できます。

SES の機能を使用するには、Amazon SES で検証済み送信者が設定されている必要があります。詳細はこちら

SES リージョン 情報

アジアパシフィック (東京)

送信元 E メールアドレス 情報

デフォルトでは、「no-reply@verificationemail.com」が使用されます。Amazon SES で検証済みの場合は、別のメールアドレスを選択することもできます。

no-reply@verificationemail.com

返信先 E メールアドレス - オプション 情報

無効な返信アドレスを設定すると、アカウントに送信制限が適用される場合があります。

メールアドレスを入力

キャンセル 戻る **次へ**

フィードバック 言語選択をお探しのようですが、新しいUIをご覧ください Unified Settings

© 2022, Amazon Web Services, Inc. またはその関連会社。 プライバシー 用語 Cookie の設定

aws

サービス

検索

サービス、特徴、ブログ、およびドキュメントなどを検索

[Alt+S]

表示

Amazon Cognito > ユーザープール > ユーザープールを作成

古いコンソールに切り替える

ステップ 1
サインインエクスペリエンスを設定

ステップ 2
セキュリティ要件を設定

ステップ 3
サインアップエクスペリエンスを設定

ステップ 4
メッセージ配信を設定

ステップ 5
アプリケーションを統合

ステップ 6
確認および作成

アプリケーションを統合 情報

Cognito の組み込みの認証および承認フローを使用して、ユーザープールのためにアプリケーション統合を設定します。

ユーザープール名

ユーザープールのわかりやすい名前を作成します。

ユーザープール名

20220401serverless

ユーザープール名は 128 文字以下である必要があります。名前には、英数字、スペース、+、=、@、といった特殊文字のみを使用できます。

このユーザープールを作成すると、ユーザープール名を変更できなくなります。

ホストされた認証ページ

ユーザーのサインアップおよびサインインフローのために Cognito のホストされた UI と OAuth 2.0 サーバーを使用するかどうかを選択します。

☐ Cognito のホストされた UI を使用

ホストされたサインアップ、サインイン、および OAuth 2.0 サービスエンドポイントを使用する Amazon Cognito で構築します。この機能が有効になっていない場合は、Cognito API オペレーションを使用してサインアップとサインインを実行します。

最初のアプリケーションクライアント

アプリケーションクライアントを設定します。アプリケーションクライアントは、認証されていない API オペレーションを呼び出すための許可を持つユーザープール内の単一アプリケーションプラットフォームです。ユーザープールは複数のアプリケーションクライアントを持つことができます。

アプリケーションタイプ 情報

アプリケーションタイプを選択すると、一般的なデフォルト設定が自動的に入力されます。ユーザープールの作成後にアプリケーションクライアントをさらに追加できます。

☒ パブリッククライアント
ネイティブアプリケーション、ブラウザアプリケーション、またはモバイルデバイスアプリケーション。
Cognito API リクエストは、クライアントのシークレットで保護されていないユーザーシステムから実行されます。

☐ 秘密クライアント
クライアントのシークレットを安全に保存できるサーバー側のアプリケーション。
Cognito API リクエストは中央サーバーから実行されます。

☐ その他
カスタムアプリケーション、独自の許可、認証フロー、およびクライアントのシークレットの設定を選択します。

アプリケーションクライアント名 情報

JavaScript App

アプリケーションクライアントの名前は 128 文字以下にする必要があります。名前には、英数字、スペース、+、=、@、といった特殊文字のみを使用できます。

クライアントのシークレット 情報

アプリケーションクライアントがクライアントのシークレットを持つかどうかを選択します。クライアントのシークレットは、API リクエストを認証するためにアプリケーションのサーバー側のコンポーネントによって使用されます。クライアントのシークレットを使用すると、第三者がクライアントになりますことを防ぐことができます。

☐ クライアントのシークレットを生成する

☒ クライアントのシークレットを生成しない

Amazon Cognito がアプリケーションクライアント用にクライアントのシークレットを生成することを許可した後で、当該シークレットを変更または削除することはできません。

高度なアプリケーションクライアントの設定

以前の選択内容に基づいて、推奨される認証フロー、OAuth 2.0 許可タイプ、および OIDC スコープが入力されています。

属性の読み取りおよび書き込み許可 情報

このアプリケーションが読み書きできる標準属性とカスタム属性を選択します。必須の属性は書き込み可能としてロックされます。イミュータブルなカスタム属性を書き込み可能に設定して、サインアップ中にアプリケーションクライアントが初期値を設定できるようにすることをお勧めします。

キャンセル

戻る

次へ

【P56】

aws

サービス

サービス、特徴、ブログ、およびドキュメントなどを検索

[Alt+S]

🔍 🔔 ⌂ 表示 ▼

Amazon Cognito > ユーザープール > ユーザープールを作成

古いコンソールに切り替える

ステップ 1
サインインエクスペリエンスを設定

ステップ 2
セキュリティ要件を設定

ステップ 3
サインアップエクスペリエンスを設定

ステップ 4
メッセージ配信を設定

ステップ 5
アプリケーションを統合

ステップ 6
確認および作成

確認および作成 情報

選択内容を確認し、問題がなければ [作成] を選択して確定します。

ステップ 1: サインインエクスペリエンスを設定 編集

認証プロバイダー

プロバイダーのタイプ
Cognito ユーザープール

Cognito ユーザープールのサインインオプション
ユーザー名
フェデレーテッドサインインのオプション
-

⚠ ユーザープールの作成後に Cognito ユーザープールのサインインオプションを変更することはできません。

ステップ 2: セキュリティ要件を設定 編集

パスワードポリシー 情報

パスワードの最小文字数
8 文字

パスワード要件
-

管理者によって設定された仮パスワードの有効期限:
7 日

多要素認証 情報

MFA の強制
MFA なし

ユーザーアカウントの復旧 情報

セルフサービスのアカウントの復旧
有効

復旧メッセージの配信方法
使用可能な場合は SMS、それ以外の場合は E メール。そして、MFA にも使用している場合は、SMS でパスワードをリセットすることを許可します

ステップ 3: サインアップエクスペリエンスを設定 編集

セルフサービスのサインアップ 情報

自己登録
有効

属性検証とユーザーアカウントの確認 情報

Cognito アシスト型の検証および確認
Cognito が検証と確認のためにメッセージを自動的に送信することを許可
有効
検証する属性
Eメールのメッセージを送信、Eメールアドレスを検証

属性変更の確認
未完了の更新があるときに元の属性値をアクティブに保つ
無効

必須の属性 情報

必須の属性
email

次ページへ続く

24

ステップ 4: メッセージ配信を設定

編集

E メール 情報

E メールプロバイダー
Cognito で E メールを送信

SES リージョン
アジアパシフィック (東京)

送信元 E メールアドレス
no-reply@verificationemail.com

返信先 E メールアドレス
-

ステップ 5: アプリケーションを統合

編集

ユーザープール名

ユーザープール名
20220401serverless

⚠ このユーザープールを作成すると、ユーザープール名を変更できなくなります。

アプリケーションクライアントのメイン設定

アプリケーションタイプ
パブリッククライアント

クライアントのシークレット
-

アプリケーションクライアント名
JavaScript App

▼ 高度なアプリケーションクライアントの設定

認証フロー
ALLOW_REFRESH_TOKEN_AUTH
ALLOW_CUSTOM_AUTH
ALLOW_USER_SRP_AUTH

更新トークンの有効期限
30 日と 0 分

アクセストークンの有効期限
0 日と 60 分

ID トークンの有効期限
0 日と 60 分

高度なセキュリティ設定
トークンの取り消しを有効化
ユーザー存在エラーの防止を有効化

▼ 属性の読み取りおよび書き込みの許可 (このアプリケーション用)

このアプリケーションが読み書きできる標準属性とカスタム属性を選択します。必須の属性は書き込み可能としてロックされます。イミュータブルなカスタム属性を書き込み可能に設定して、サインアップ中にアプリケーションクライアントが初期値を設定できるようにすることを勧めます。

属性	読み取り	書き込み
address	🟢 読み取り	🟢 書き込み
birthdate	🟢 読み取り	🟢 書き込み
email	🟢 読み取り	🟢 書き込み
email_verified	🟢 読み取り	🔴 書き込み不可
family_name	🟢 読み取り	🟢 書き込み
gender	🟢 読み取り	🟢 書き込み
given_name	🟢 読み取り	🟢 書き込み
locale	🟢 読み取り	🟢 書き込み
middle_name	🟢 読み取り	🟢 書き込み
name	🟢 読み取り	🟢 書き込み
nickname	🟢 読み取り	🟢 書き込み
phone_number	🟢 読み取り	🟢 書き込み
phone_number_verified	🟢 読み取り	🔴 書き込み不可
picture	🟢 読み取り	🟢 書き込み
preferred_username	🟢 読み取り	🟢 書き込み
profile	🟢 読み取り	🟢 書き込み
updated_at	🟢 読み取り	🟢 書き込み
website	🟢 読み取り	🟢 書き込み
zoneinfo	🟢 読み取り	🟢 書き込み

キャンセル

戻る

ユーザープールを作成

【P57】

Amazon Cognito > ユーザープール

ユーザープール (1) 情報

ユーザープールを表示および設定します。ユーザープールは、フェデレーテッドおよびローカルユーザープロファイルのディレクトリであり、ユーザーのために認証オプションを提供します。

削除 ユーザープールを作成

名前または ID でユーザープールを検索

ユーザープール名	ユーザープール ID	作成時刻	最終更新時刻
20220401serverless	ap-northeast-1_SUep9qaCT	5 秒前	5 秒前

Amazon Cognito > ユーザープール > 20220401serverless

20220401serverless 情報

削除

ユーザープールの概要

ユーザープール名 20220401serverless	ARN arn:aws:cognito-idp:ap-northeast-1:484856368:397:userpool/ap-northeast-1_SUep9qaCT	作成時刻 2022年5月26日 9:51 JST
ユーザープール ID ap-northeast-1_SUep9qaCT	推定ユーザー数 0	最終更新時刻 2022年5月26日 9:51 JST

Amazon Cognito > ユーザープール > 20220401serverless

20220401serverless 情報

削除

ユーザープールの概要

ユーザープール名 20220401serverless	ARN arn:aws:cognito-idp:ap-northeast-1:484856368:397:userpool/ap-northeast-1_SUep9qaCT	作成時刻 2022年5月26日 9:51 JST
ユーザープール ID ap-northeast-1_SUep9qaCT	推定ユーザー数 0	最終更新時刻 2022年5月26日 9:51 JST

開始方法

ユーザー グループ サインインエクスペリエンス サインアップエクスペリエンス メッセージング **アプリケーションの統合** ユーザー

Amazon Cognito > ユーザープール > 20220401serverless

20220401serverless 情報

削除

高度なセキュリティ 情報

疑わしいユーザーアクティビティへの Cognito の自動応答など、高度なセキュリティ機能を設定します。高度なセキュリティについては、追加の料金が請求されます。料金を参照してください

有効化

ステータス

無効

アプリケーションクライアントのリスト

アプリケーションとユーザープールを統合するアプリケーションクライアント。ユーザープールのデフォルト設定に対するクライアントの上書きを設定し、Amazon Pinpoint分析を設定します。

アプリケーションクライアントと分析 (1) 情報

アプリケーションクライアントを設定します。アプリケーションクライアントは、アプリケーションにアタッチされたユーザープールの認証リソースです。アプリケーションクライアントを選択して、アプリケーション用に許可される認証アクションを設定します。

削除 アプリケーションクライアントを作成

アプリケーションクライアントの名前または ID で検索

アプリケーションクライアント名	クライアント ID
JavaScript App	1u01131v3tkquk78f65b3rq1