

EC2インスタンスとIPアドレス

まりお

@*satensi3103*

目次

- 0. 目的
- 1. EC2インスタンスのIPアドレス割り当ての仕組み
- 2. EC2インスタンスを作る
- 3. インスタンスとENIの確認
- 4. リンク集

0. 目的

- 前章ではVPC領域の中にサブネットを作成した
- 本章はサブネットの中にEC2インスタンスを配置する
- 配置したインスタンスと、ENIの確認を行う
- (marp for vscodeを使ってみる)

1. EC2インスタンスのIPアドレス割り当ての仕組み

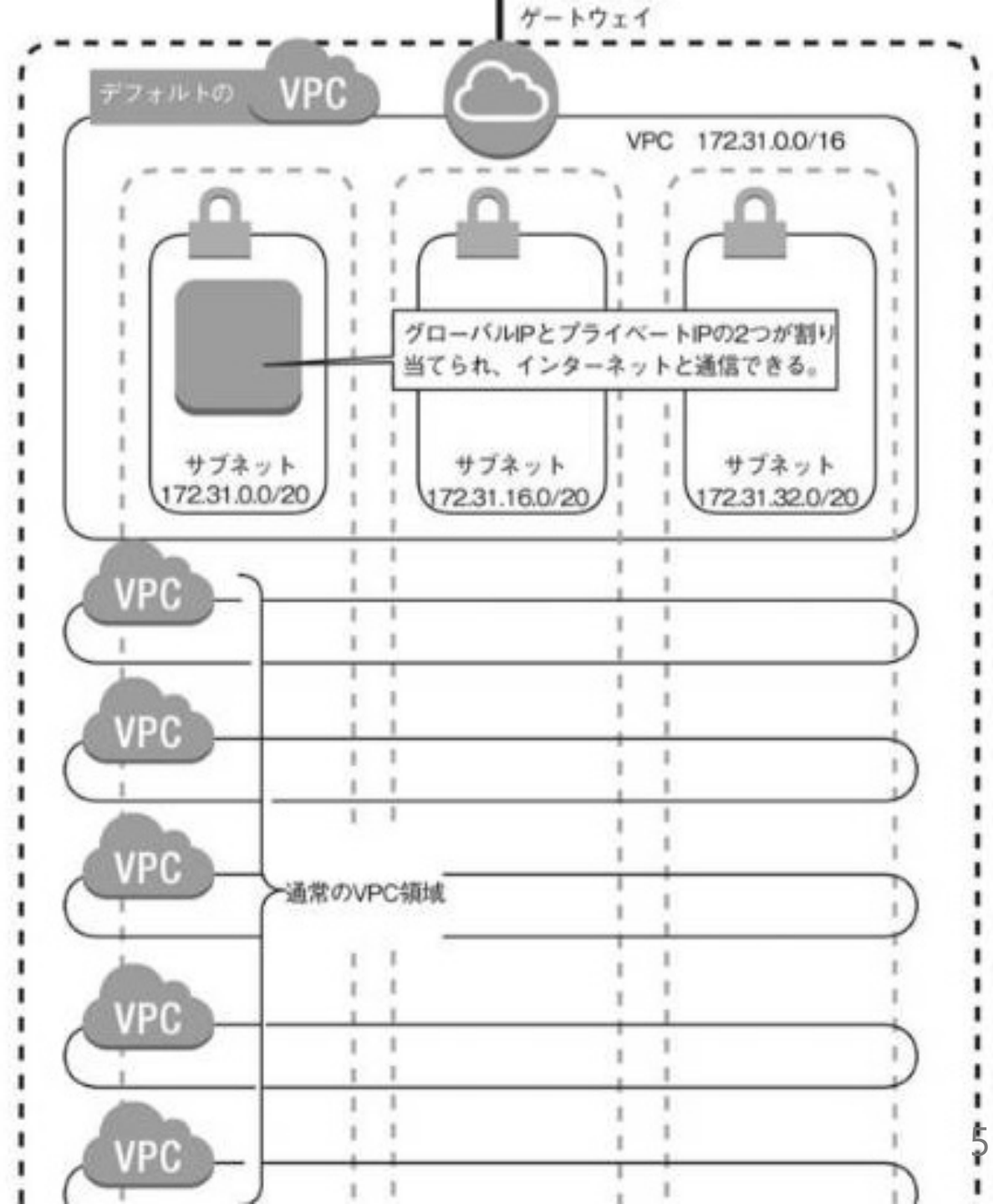
1.1 VPC領域とサブネット

VPC領域

- ネットワークを作る場所
- 利用するIPアドレスの範囲をプライベートIPアドレスとして指定

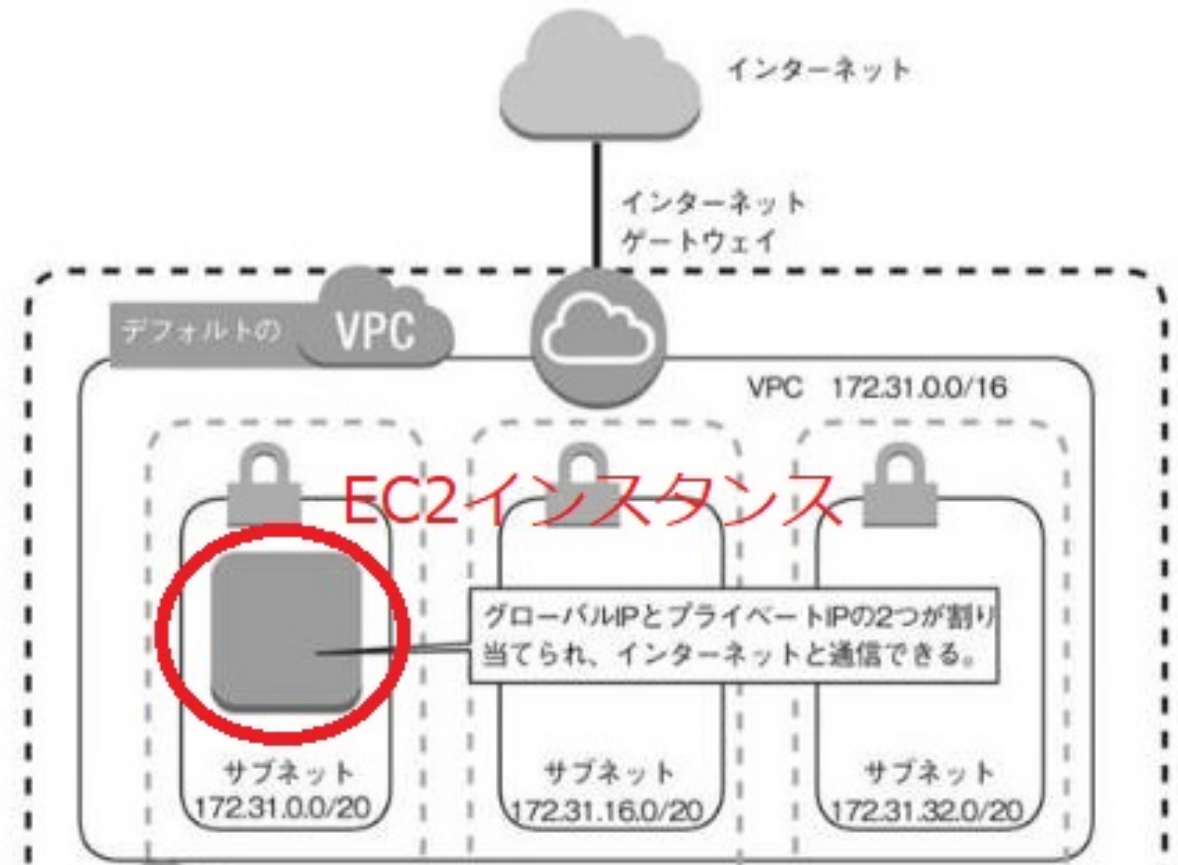
サブネット

- VPC領域を分割して、アベイラビリティゾーンに配置したもの



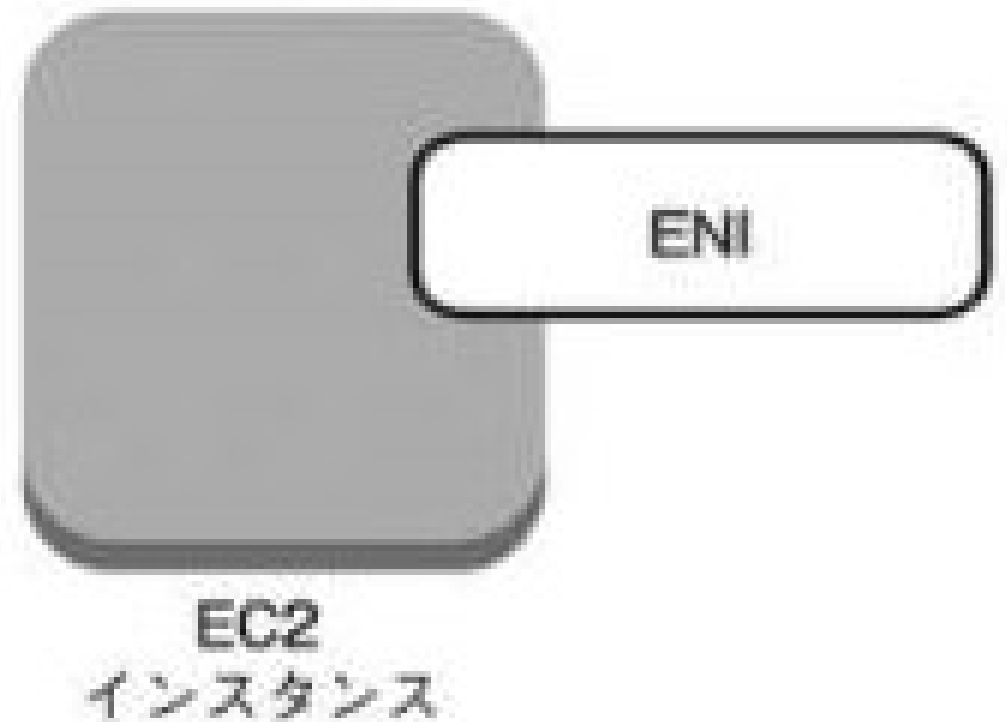
1.2 EC2インスタンスとは

- EC2で起動された仮想サーバー
- サブネットの中に配置される



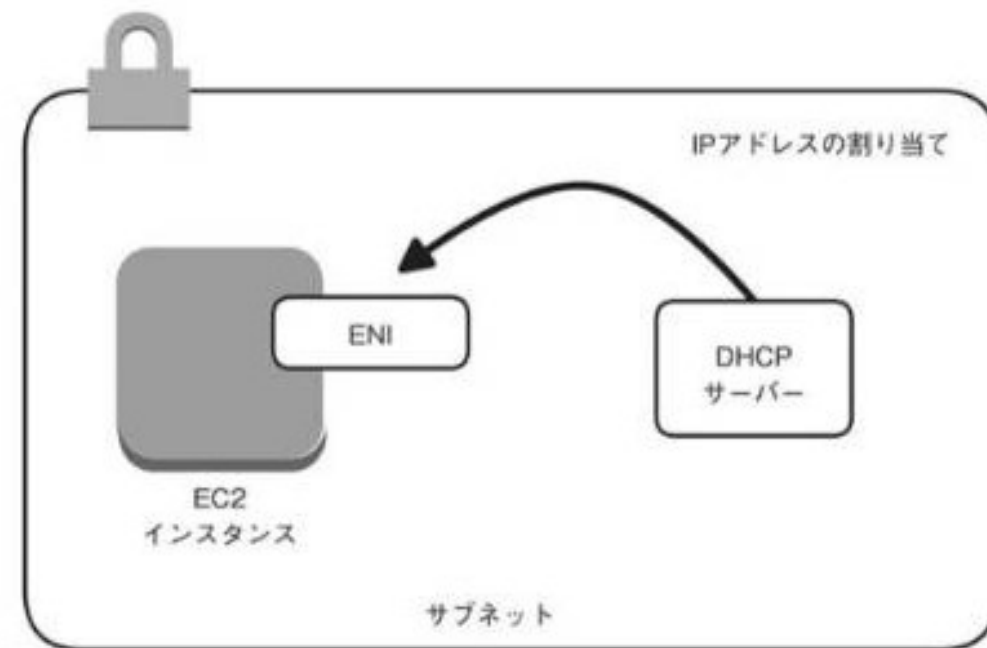
1.3 ネットワークインターフェイス ENI

- AWSにおいてNIC(ネットワークインターフェイスカード)に相当する
- EC2をネットワークに繋ぐためのもの、インスタンスと同時に作成



1.4 DHCPサーバー

- AWSではサブネット上でDHCPサーバー機能が動作
- DHCP：IPv4で通信用の基本設定を自動で行うためのプロトコル



1.4 DHCPサーバー

- 予約されたIPアドレス以外を起動時に動的に割り当てる
- 右図に示すものの以外のIPが対象
- 今回のサブネットだと10.0.0.4～10.0.0.254

IP アドレス	用途
先頭	ネットワークアドレスとして使用
先頭+1	VPC ルーターで使用
先頭+2	Amazon が提供する DNS へのマッピング用に予約
先頭+3	将来のための予約
末尾	ブロードキャストアドレスとして予約

1.5 DHCPサーバーのオプション

- DNSサーバーやデフォルトのドメイン名の指定といったオプション設定が可能

VPC ダッシュボード
VPC でフィルタリング:
🔍 VPC の選択

VIRTUAL PRIVATE CLOUD
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
DHCP オプションセット
Elastic IP
エンドポイント
エンドポイントのサービス
NAT ゲートウェイ
ピアリング接続

セキュリティ
ネットワーク ACL
セキュリティグループ

仮想プライベートネットワーク (VPN)
カスタマーゲートウェイ
仮想プライベートゲートウェイ

DHCP オプションセットの作成 アクション ▾

🔍 タグや属性によるフィルター、またはキーワードによる検索 < 1 中の 1 ~ 1 >

<input type="checkbox"/>	Name ▾	DHCP オプションセット ID	オプション	所有者 ▾
<input type="checkbox"/>		dopt-f01f3597	domain-name = ap-northeast-1.compute.internal; domain-name-se...	281370848616

DHCP オプションセット: dopt-f01f3597

詳細 タグ

DHCP オプションセット ID dopt-f01f3597

所有者 281370848616

オプション domain-name = ap-northeast-1.compute.internal;
domain-name-servers = AmazonProvidedDNS;

1.6 IPアドレス割り当ての注意点

プライマリプライベートIPアドレス

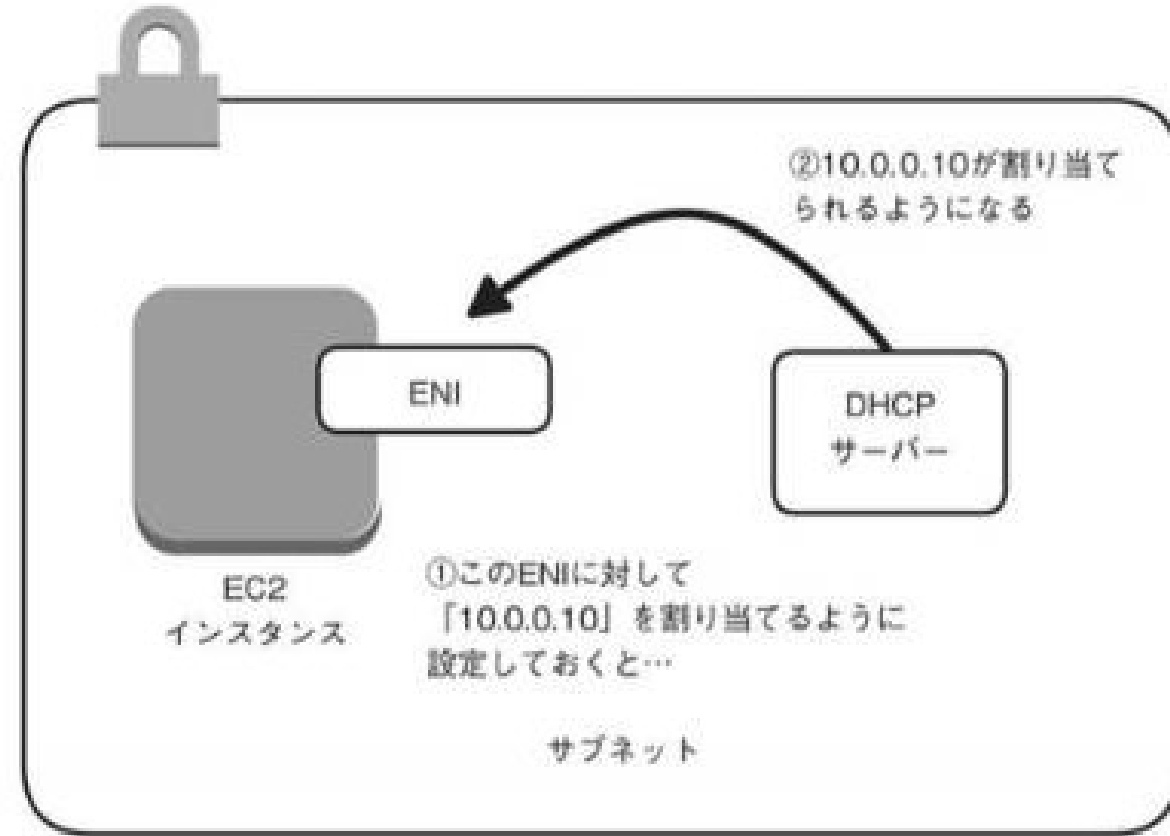
- ENIが必ず1つ持つ
- プライマリプライベートIPアドレスはENI作成時に定まり、固定

セカンダリプライベートIPアドレス

- 任意追加
- セカンダリプライベートIPアドレスは手動設定、変更可能

1.6 IPアドレス割り当ての注意点

- プライマリプライベートIPアドレスに固定IPアドレスを割り当てることも可能(以降は変更不可)
- 勝手なIPアドレスを利用してはいけない、常にサブネット下のDHCPサーバーの割り当てるIPアドレスを使用する



2. EC2インスタンスを作る

2.1 インスタンスの画面を開き、インスタンスの作成をクリック



2.2 AMI(Amazon マシンイメージを選択)

- AMIはAmazon Linuxを選択
- Amazon Linux 2はRHEL7がベース
- 相違点はリンク集を参考

1. AMI の選択 2. インスタンスタイプの選択 3. インスタンスの設定 4. ストレージの追加 5. タグの追加 6. セキュリティグループの設定 7. 確認

ステップ 1: Amazon マシンイメージ (AMI)

[キャンセルして終了](#)

AMI は、インスタンスの作成に必要なソフトウェア構成 (OS、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。AMI は、AWS が提供するもの、ユーザーコミュニティが提供するもの、または AWS Marketplace に掲載されているものを選択できます。独自の AMI のいずれかを選択することもできます。

🔍 検索用語を入力して AMI を検索します (「Windows」など)。

クイックスタート

マイ AMI

AWS Marketplace

コミュニティ AMI

☐ 無料利用枠のみ ⓘ



Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0f310fcd6141e627 (64 ビット x86) / ami-08360a37d07f61f88 (64 ビット Arm)

Amazon Linux
無料利用枠の対象

Amazon Linux 2 には 5 年間のサポートが含まれます。Amazon EC2、systemd 219、GCC 7.3、Glibc 2.26、Binutils 2.29.1 で最適なパフォーマンスを発揮できるように調整された Linux カーネル 4.14、および、追加の最新のソフトウェアパッケージを提供します。

ルートデバイスタイプ: ebs 仮想化タイプ: hvm ENA 有効: はい

選択

☒ 64 ビット
(x86)

☐ 64 ビット
(Arm)



Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0318ecd6d05daa212

Amazon Linux
無料利用枠の対象

Amazon Linux AMI は、AWS がサポートする EBS-backed イメージです。デフォルトのイメージには、AWS コマンドラインツール、Python、Ruby、Perl、および Java が含まれます。レポジトリには、Docker、PHP、MySQL、PostgreSQL、およびその他のパッケージが含まれます。

ルートデバイスタイプ: ebs 仮想化タイプ: hvm ENA 有効: はい

選択

64 ビット (x86)

2.3 インスタンスタイプを選択

- 用途に合わせて、様々な種類のインスタンスが用意されている
- 今回は最初から選択されている「t2.micro」を選ぶ

1. AMI の選択 2. インスタンスタイプの選択 3. インスタンスの設定 4. ストレージの追加 5. タグの追加 6. セキュリティグループの設定 7. 確認

ステップ 2: インスタンスタイプの選択

Amazon EC2 では、異なるユースケースに合わせて最適化されたさまざまなインスタンスタイプが用意されています。インスタンスとは、アプリケーションを実行できる仮想サーバーです。インスタンスタイプはさまざまな CPU、メモリ、ストレージ、ネットワークキャパシティの組み合わせによって構成されているため、使用するアプリケーションに合わせて適切なリソースの組み合わせを柔軟に選択できます。インスタンスタイプおよびそれをコンピューティングのニーズに適用する方法に関する [詳細はこちら](#)。

フィルター条件: すべてのインスタンスタイプ 現行世代 列の表示/非表示

現在選択中: t2.micro (可変 ECU, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GiB メモリ, EBS のみ)								
	ファミリー	タイプ	vCPU ⓘ	メモリ (GiB)	インスタンス ストレージ (GB) ⓘ	EBS 最適化利用 ⓘ	ネットワークパフォーマンス ⓘ	IPv6 サポート ⓘ
<input type="checkbox"/>	汎用	t2.nano	1	0.5	EBS のみ	-	低から中	はい
<input checked="" type="checkbox"/>	汎用	t2.micro 無料利用枠の対象	1	1	EBS のみ	-	低から中	はい
<input type="checkbox"/>	汎用	t2.small	1	2	EBS のみ	-	低から中	はい
<input type="checkbox"/>	汎用	t2.medium	2	4	EBS のみ	-	低から中	はい
<input type="checkbox"/>	汎用	t2.large	2	8	EBS のみ	-	低から中	はい
<input type="checkbox"/>	汎用	t2.xlarge	4	16	EBS のみ	-	中	はい
<input type="checkbox"/>	汎用	t2.2xlarge	8	32	EBS のみ	-	中	はい

[キャンセル](#)[戻る](#)[確認と作成](#)[次のステップ: インスタンスの詳細の設定](#)

2.4 インスタンスの詳細の設定

- ネットワークの部分で、配置先のVPC領域を選択
- 配置先のサブネットは前章で作成した「mysubnet01」を選択
- 他はそのまま

1. AMI の選択 2. インスタンスタイプの選択 3. インスタンスの設定 4. ストレージの追加 5. タグの追加 6. セキュリティグループの設定 7. 確認

ステップ 3: インスタンスの詳細の設定

要件に合わせてインスタンスを設定します。同じ AMI から複数のインスタンス作成や、より低料金を実現するためのスポットインスタンスのリクエスト、インスタンスへのアクセス管理ロール割り当てなどを行うことができます。

インスタンス数 ① Auto Scaling グループに作成する ①

購入のオプション ① ☐ スポットインスタンスのリクエスト

ネットワーク ① 新しい VPC の作成

サブネット ① 新しいサブネットの作成
251 個の IP アドレスが利用可能

自動割り当てパブリック IP ①

配置グループ ① ☐ インスタンスをプレイズメントグループに追加します。

キャパシティの予約 ① 新しいキャパシティ予約の作成

IAM ロール ① 新しい IAM ロールの作成

シャットダウン動作 ①

停止・休止動作 ① ☐ 停止動作に休止動作を追加する

終了保護の有効化 ① ☐ 誤った終了を防止します

モニタリング ① ☐ CloudWatch 詳細モニタリングを有効化

キャンセル 戻る 確認と作成 次のステップ: ストレージの追加

2.5 ストレージの設定

- ストレージとして、どのようなEBSを割り当てるか指定
- デフォルトの8GBのストレージ(汎用SSD(gp2))でよい

1. AMI の選択 2. インスタンスタイプの選択 3. インスタンスの設定 **4. ストレージの追加** 5. タグの追加 6. セキュリティグループの設定 7. 確認

ステップ 4: ストレージの追加

インスタンスは次のストレージデバイス設定を使用して作成されます。インスタンスに追加の EBS ボリュームやインスタンスストアボリュームをアタッチするか、ルートボリュームの設定を編集することができます。また、インスタンスを作成してから追加の EBS ボリュームをアタッチすることもできますが、インスタンスストアボリュームはアタッチできません。Amazon EC2 のストレージオプションに関する [詳細](#) はこちらをご覧ください。

ボリュームタイプ ⓘ	デバイス ⓘ	スナップショット ⓘ	サイズ (GiB) ⓘ	ボリュームタイプ ⓘ	IOPS ⓘ	スループット (MB/秒) ⓘ	終了時に削除 ⓘ	暗号化 ⓘ
ルート	/dev/xvda	snap-0f7fd88c24fa4e2f6	8	汎用 SSD (gp2)	100 / 3000	該当なし	<input checked="" type="checkbox"/>	暗号化なし

新しいボリュームの追加

無料利用枠の対象であるお客様は 30 GB までの EBS 汎用 (SSD) ストレージまたはマグネティックストレージを取得できます。無料利用枠の対象と使用制限に関する [詳細はこちら](#)。

キャンセル

戻る

確認と作成

次のステップ: タグの追加

2.6 インスタンスのタグ付け

- インスタンスに対して、各種メタデータを設定できる
- デフォルトの「Name」という項目に、サーバー名「mywebserver」をセットする

1. AMI の選択 2. インスタンスタイプの選択 3. インスタンスの設定 4. ストレージの追加 5. タグの追加 6. セキュリティグループの設定 7. 確認

ステップ 5: タグの追加

タグは、大文字と小文字が区別されるキーと値のペアから構成されます。たとえば、キーに「Name」、値に「Webserver」を使用してタグを定義することができます。

タグのコピーは、ボリューム、インスタンス、またはその両方に適用できます。

タグは、すべてのインスタンスとボリュームに適用されます。Amazon EC2 リソースのタグ付けに関する [詳細はこちら](#)。

キー (最大 128 文字)	値 (最大 256 文字)	インスタンス i	ボリューム i
Name	mywebserver	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

別のタグを追加 (最大 50 個のタグ)

キャンセル

戻る

確認と作成

次のステップ: セキュリティグループの設定

2.7 セキュリティグループの設定

- セキュリティグループを設定する
- デフォルトの名称から「webserverSG」に変更

1. AMI の選択 2. インスタンスタイプの選択 3. インスタンスの設定 4. ストレージの追加 5. タグの追加 **6. セキュリティグループの設定** 7. 確認

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は、インスタンスのトラフィックを制御するファイアウォールのルールセットです。このページで、特定のトラフィックに対してインスタンスへの到達を許可するルールを追加できます。たとえば、ウェブサーバーをセットアップして、インターネットトラフィックにインスタンスへの到達を許可する場合、HTTP および HTTPS ポートに無制限のアクセス権限を与えます。新しいセキュリティグループを作成するか、次の既存のセキュリティグループから選択することができます。Amazon EC2 セキュリティグループに関する [詳細はこちら](#)。

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

☐ 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:

webserverSG

説明:

launch-wizard-1 created 2020-04-11T01:01:23.994+09:00

タイプ ⓘ	プロトコル ⓘ	ポート範囲 ⓘ	ソース ⓘ	説明 ⓘ
SSH ▾	TCP	22	カスタム ▾ 0.0.0.0/0	例: SSH for Admin Desktop ✕

ルールの追加



警告

送信元が 0.0.0.0/0 のルールを指定すると、すべての IP アドレスからインスタンスにアクセスすることが許可されます。セキュリティグループのルールを設定して、既知の IP アドレスからのみアクセスできるようにすることをお勧めします。

キャンセル

戻る

確認と作成

2.8 確認とキーペア作成

- インスタンス作成の確認画面を通り、起動を押す
- するとキーペアの作成に関し聞かれるのでキーペア名を入力し、ダウンロードして保管する
ここでしかダウンロード出来ず、無くすとEC2インスタンスにログインできなくなるので注意
- キーペアはSSH(22番ポート)の暗号化通信時に用いる

既存のキーペアを選択するか、新しいキーペアを作成します。 ×

キーペアは、AWS が保存する**パブリックキー**とユーザーが保存する**プライベートキーファイル**で構成されます。組み合わせて使用することで、インスタンスに安全に接続できます。Windows AMI の場合、プライベートキーファイルは、インスタンスへのログインに使用されるパスワードを取得するために必要です。Linux AMI の場合、プライベートキーファイルを使用してインスタンスに SSH で安全に接続できます。

注: 選択したキーペアは、このインスタンスに対して権限がある一連のキーに追加されます。 [「パブリック AMI から既存のキーペアを削除する」](#) の詳細情報をご覧ください。

新しいキーペアの作成 ▼

キーペア名

mykey

キーペアのダウンロード



続行するには、事前に**プライベートキーファイル** (*.pem ファイル) をダウンロードする必要があります。それを、安全でアクセス可能な場所に保存します。一度作成されたファイルは再度ダウンロードすることはできません。

キャンセル

インスタンスの作成

3. インスタンスとENIの確認

3.1 EC2インスタンスのIPアドレスの確認

- メニューから「インスタンス」を選択し、「説明」部分を参照
- プライベートDNS・IPアドレス・パブリックIPアドレスなど確認可能

New EC2 Experience
Tell us what you think

インスタンスの作成 接続 アクション

EC2 ダッシュボード New

イベント New

タグ

レポート

制限

▼ インスタンス

インスタンス

インスタンスタイプ

テンプレートの起動

スポットリクエスト

Savings Plans

リザーブインスタンス

専有ホスト New

キャパシティの予約

▼ イメージ

AMI

バンドルタスク

▼ ELASTIC BLOCK STORE

ボリューム

スナップショット

タグや属性によるフィルター、またはキーワードによる検索

1 中の 1 ~ 1

Name	インスタンス ID	インスタンスタイプ	アベイラビリティゾーン	インスタンスの状態	ステータスチェック	アラームのステータス	パブリック DNS (IPv4)	IPv4 パブリック IP	IPv6 IP
mywebserver	i-0668aa5b0e7b2383a	t2.micro	ap-northeast-1a	running	2/2 のチェックが成功しています	なし	-	-	-

説明 ステータスチェック モニタリング タグ

インスタンス ID	i-0668aa5b0e7b2383a	パブリック DNS (IPv4)	-
インスタンスの状態	running	IPv4 パブリック IP	-
インスタンスタイプ	t2.micro	IPv6 IP	-
検索中	推奨事項については、AWS Compute Optimizer にオプトインしてください。 詳細はこちら	Elastic IP	-
プライベート DNS	ip-10-0-0-122.ap-northeast-1.compute.internal	アベイラビリティゾーン	ap-northeast-1a
プライベート IP	10.0.0.122	セキュリティグループ	webserverSG. インバウンドルールの表示. アウトバウンドルールの表示
セカンダリプライベート IP	-	予定されているイベント	予定されているイベントはありません
VPC ID	vpc-0b0a4cd74b79bd69b (mvvpc01)	AMI ID	amzn-ami-hvm-2018.03.0.20200318.2-x86_64-gp2 (ami-0318ecd6d05daa212)
サブネット ID	subnet-09fe5f845fe2e06e2 (mysubnet01)	Platform details	-
ネットワークインターフェイス	eth0	Usage operation	-
IAM ロール	-	送信元/送信先チェック	True
キーペア名	mykey	T2/T3 無制限	無効

3.2 EC2インスタンスに割り当てられたENIの確認

- ENIの情報確認は「説明」部分を下にスクロールし、「ネットワークインターフェイス」をクリック
- ENIの名称などが確認できる

The screenshot shows the AWS Management Console interface. On the left, there's a sidebar with 'リソースグループ' (Resource Groups) and a list of instances. One instance, 'mywebserver' with ID 'i-0668aa5b0e...', is selected. The main panel displays the details of the network interface 'eth0'. The details are as follows:

ネットワークインターフェイス eth0	
インターフェイス ID	eni-0784c6da324a28a77
VPC ID	vpc-0b0a4cd74b79bd69b
アタッチ所有者	281370848616
アタッチステータス	attached
アタッチ時刻	Sat Apr 11 01:07:10 GMT+900 2020
終了時に削除	true
プライベート IP アドレス	10.0.0.122
プライベート DNS 名	-
パブリック IP アドレス	-
送信元/送信先チェック	true
説明	Primary network interface
セキュリティグループ	webserverSG
Elastic Fabric Adapter	無効

3.3 ENIの構成確認

- メニューから「ネットワークインターフェイス」を選択
- ENIの構成などが確認できる
- 追加のENIの設定(≒ネットワークカード2枚差し)はこの画面から可能

New EC2 Experience
Tell us what you think

ネットワークインターフェイスの作成 アタッチ デタッチ 削除 アクション

タグや属性によるフィルター、またはキーワードによる検索

1 中の 1 ~ 1

Name	ネットワーク ID	サブネット ID	VPC ID	ゾーン	セキュリティグループ	説明	インスタンス ID	ステータス	IPv4 パブリック
eni-0784c6da3...	subnet-09fe5f8...	vpc-0b0a4cd7...	ap-northeast...	webserverSG	Primary netwo...	i-0668aa5b0e7b2383a	in-use	-	

ネットワークインターフェイス : eni-0784c6da324a28a77

詳細 フローログ タグ

項目	値	項目	値
ネットワークインターフェイス ID	eni-0784c6da324a28a77	サブネット ID	subnet-09fe5f845fe2e06e2
VPC ID	vpc-0b0a4cd74b79bd69b	アベイラビリティゾーン	ap-northeast-1a
MAC アドレス	06:ca:c6:53:bb:ec	説明	Primary network interface
セキュリティグループ	webserverSG. インバウンドルールの表示. アウトバウンドルールの表示	ネットワークインターフェイスの所有者	281370848616
ステータス	in-use	プライマリプライベート IPv4	10.0.0.122
プライベート DNS (IPv4)	-	IPv4 パブリック IP	-
セカンダリプライベート IPv4 IP	-	IPv6 IP	-
Elastic Fabric Adapter	無効	送信元/送信先チェック	true
アタッチメント ID	eni-attach-00ec7c14d041ed38d	インスタンス ID	i-0668aa5b0e7b2383a
アタッチメントの所有者	281370848616	デバイスインデックス	0
アタッチメントのステータス	attached	終了時に削除	true
Elastic IP 所有者	-	割り当て ID	-
関連付け ID	-	Outpost ID	-

ELASTIC BLOCK STORE

ボリューム

スナップショット

ライフサイクルマネージャー

ネットワーク & セキュリティ

セキュリティグループ

New

Elastic IP New

プレースメントグループ

New

キーペア New

ネットワークインターフェイス

ロードバランシング

ロードバランサー

ターゲットグループ

AUTO SCALING

起動設定

Auto Scaling グループ

4. リンク集

DNSサーバ

<https://wa3.i-3-i.info/word1288.html>

OSI参照モデル

<https://wa3.i-3-i.info/word1783.html>

DHCP

<https://wa3.i-3-i.info/word1959.html>

metadeta情報取得の簡単な方法

<https://dev.classmethod.jp/articles/ec2-metadata-command/>

AMIのlinux無印とlinux 2の違い

<https://qiita.com/akira345/items/2a09c4d06d2e3415bc8d>

秘密鍵と公開鍵やその利用例(SSH暗号化通信)

<https://milestone-of-se.nesuke.com/sv-advanced/digicert/public-private-key/>

共通鍵暗号と公開鍵暗号

<https://www.infraexpert.com/study/security4.html>

Visual Studio Codeで作るLT資料 ～ 脱パワーポイント

<https://qiita.com/gogogonkun/items/b90c5ef3ca4710211c76>