

■ EC2の起動

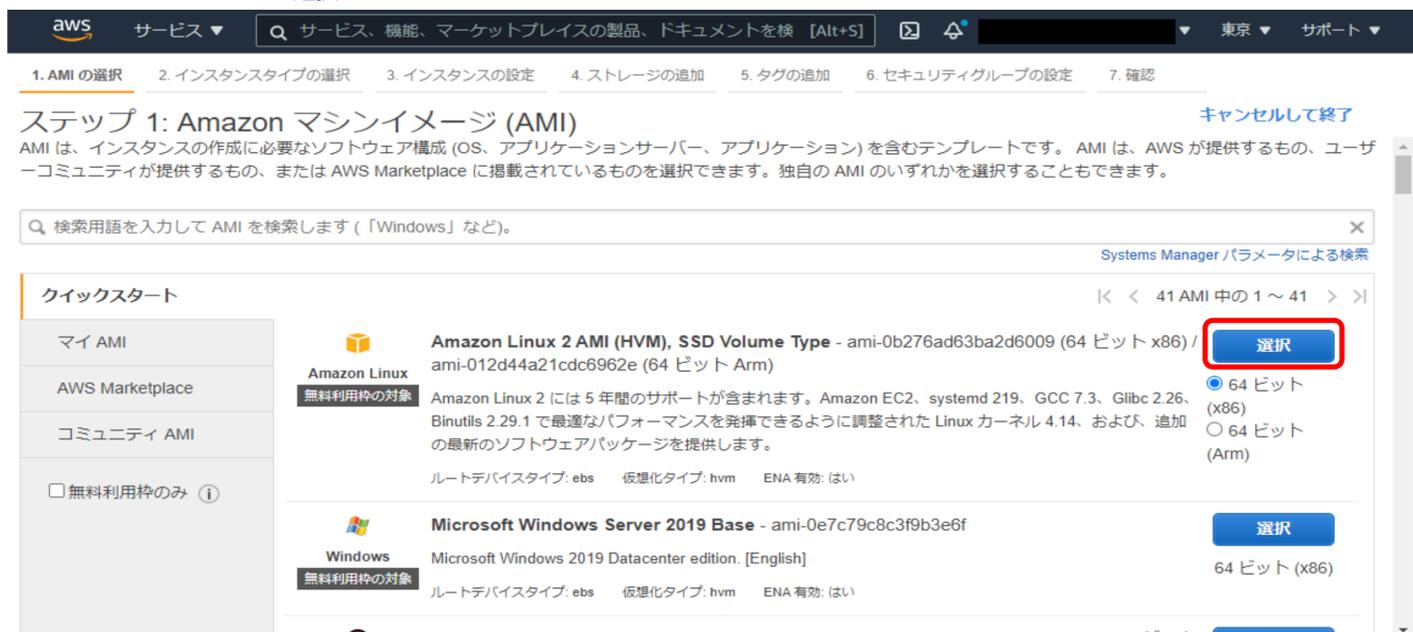
1. トップ画面でEC2を選択



2. 左メニューからインスタンスを選択 下記が表示されたら インスタンスを起動 をクリック



3. Amazon Linux 2 AMI を選択



4. デフォルトの「t2.micro」を選択して、「インスタンスの詳細設定」をクリック

aws サービス 東京 サポート

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:

現在選択中: t2.micro (- ECU, 1 vCPU, 2.5 GHz, -, 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"/>	t2	t2.nano	1	0.5	EBS のみ	-	低から中	はい
<input checked="" type="checkbox"/>	t2	t2.micro 無料利用枠の対象	1	1	EBS のみ	-	低から中	はい
<input type="checkbox"/>	t2	t2.small	1	2	EBS のみ	-	低から中	はい
<input type="checkbox"/>	t2	t2.medium	2	4	EBS のみ	-	低から中	はい
<input type="checkbox"/>	t2	t2.large	2	8	EBS のみ	-	低から中	はい

5. ネットワーク「VPN-test」を選択して、「ストレージの追加」をクリック

aws サービス 東京 サポート

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 からの複数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

購入のオプション スポットインスタンスのリクエスト

ネットワーク

サブネット
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

配置グループ 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

ドメイン結合ディレクトリ

IAM ロール

6. 下へスクロールして、eth0のIPを「10.0.1.10」に設定して、「ストレージの追加」をクリック

aws サービス 東京 サポート

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

ファイルシステム

▼ ネットワークインターフェイス

デ	ネットワークインターフ	サブネット	プライマリ IP	セカンダリ IP アドレ	IPv6 IP
eth0	<input type="text" value="新しいネットワーク"/>	<input type="text" value="subnet-08e497a8"/>	<input type="text" value="10.0.1.10"/>	<input type="button" value="IP の追加"/>	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.

▼ 高度な詳細

Enclave 有効

アクセス可能なメタデータ

メタデータのバージョン

メタデータトークンレスポンスのホップ制限

7. 「タグの追加」をクリック

aws サービス サービス、機能、マーケットプレースの製品、ドキュメントを検 [Alt+S] 東京 サポート

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-05012eb1ff30321aa	8	汎用 SSD (gp2)	100 / 3000	該当なし	<input checked="" type="checkbox"/>	暗号化ス

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**

8. キー「Name」、値「VPN-test-EC2」を入力。「セキュリティグループの設定」をクリック

aws サービス サービス、機能、マーケットプレースの製品、ドキュメントを検 [Alt+S] 東京 サポート

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	ボリューム	ネットワークインターフェイス
Name	VPN-test-EC2	<input checked="" type="checkbox"/>	<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**

9. 許可したい通信がある場合には、ルールの追加をクリック

aws サービス サービス、機能、マーケットプレースの製品、ドキュメントを検 [Alt+S] 東京 サポート

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: launch-wizard-26
 説明: launch-wizard-26 created 2021-07-15T22:42:28.265+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

10. ルールを追加して、「確認と作成」をクリック

aws サービス サービス、機能、マーケットプレースの製品、ドキュメントを検索 [Alt+S] 東京 サポート

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: launch-wizard-26
 説明: launch-wizard-26 created 2021-07-15T22:42:28.265+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
すべてのICMI	ICMP	0 - 65535	任意の場所 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**

11. 「起動」をクリック

aws サービス サービス、機能、マーケットプレースの製品、ドキュメントを検索 [Alt+S] 東京 サポート

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 7: インスタンス作成の確認

インスタンスの作成に関する詳細を確認してください。各セクションの変更に戻ることができます。**[作成]** をクリックして、インスタンスにキーペアを割り当て、作成処理を完了します。

警告
 インスタンスのセキュリティを強化してください。セキュリティグループ launch-wizard-26 は世界に向けて開かれています。このインスタンスには、どの IP アドレスからもアクセスできる可能性があります。セキュリティグループのルールを更新して、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。
 また、セキュリティグループの追加ポートを開いて、実行中のアプリケーションやサービスへのアクセスを容易にすることもできます。たとえば、ウェブサーバー用に HTTP (80) を開きます。セキュリティグループの編集

AMIの詳細 AMIの編集

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0b276ad63ba2d6009
 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

インスタンスタイプ インスタンスタイプの編集

インスタンスタイプ	ECU	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

キャンセル 戻る **起動**

12 「新しいキーペアの作成」を選択し、キーペア名を入力して、「キーペアのダウンロード」をクリック（キーペアはSSH接続で使用する）。

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。 ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

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
 VPN-test-ssh-key

キーペアのダウンロード

続けるには、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**

13. インスタンスの作成 をクリック



14. 下へスクロールして、「インスタンスの表示」をクリック

15. 作成したインスタンス「VPN-test-EC2」が表示されることを確認。
ステータスが「初期化しています」から「2/2のチェック合格しました」に変わると起動完了。