

AWSサイト間VPNの構築（2.AWSのEC2構築）

AWS



AWSサイト間VPNの構築 （2.AWSのEC2構築）

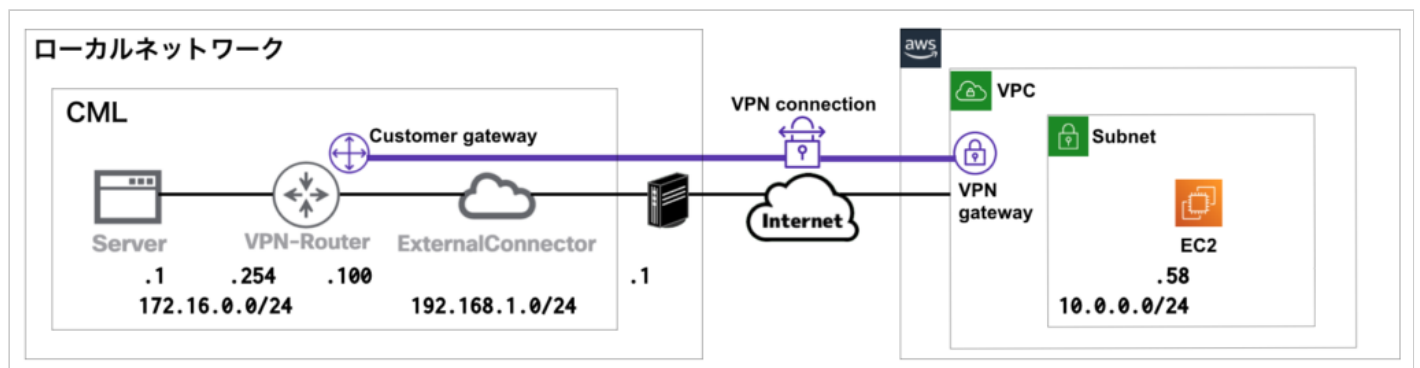
2021.08.31 2021.08.11

[【前回】AWSサイト間VPNの構築（1.AWSの基本設定）](#)[【次回】AWSサイト間VPNの構築（3.AWSのVPN構築）](#)

ネットワーク構成

下記のネットワーク構成で、CML上のLAN(172.16.0.0/24)とAWSのサブネット(10.0.0.0/24)が直接通信できるようにします。

※Server(172.16.0.1)からEC2(10.0.0.58)にPingによる疎通確認ができるようにしていきます。



EC2構築

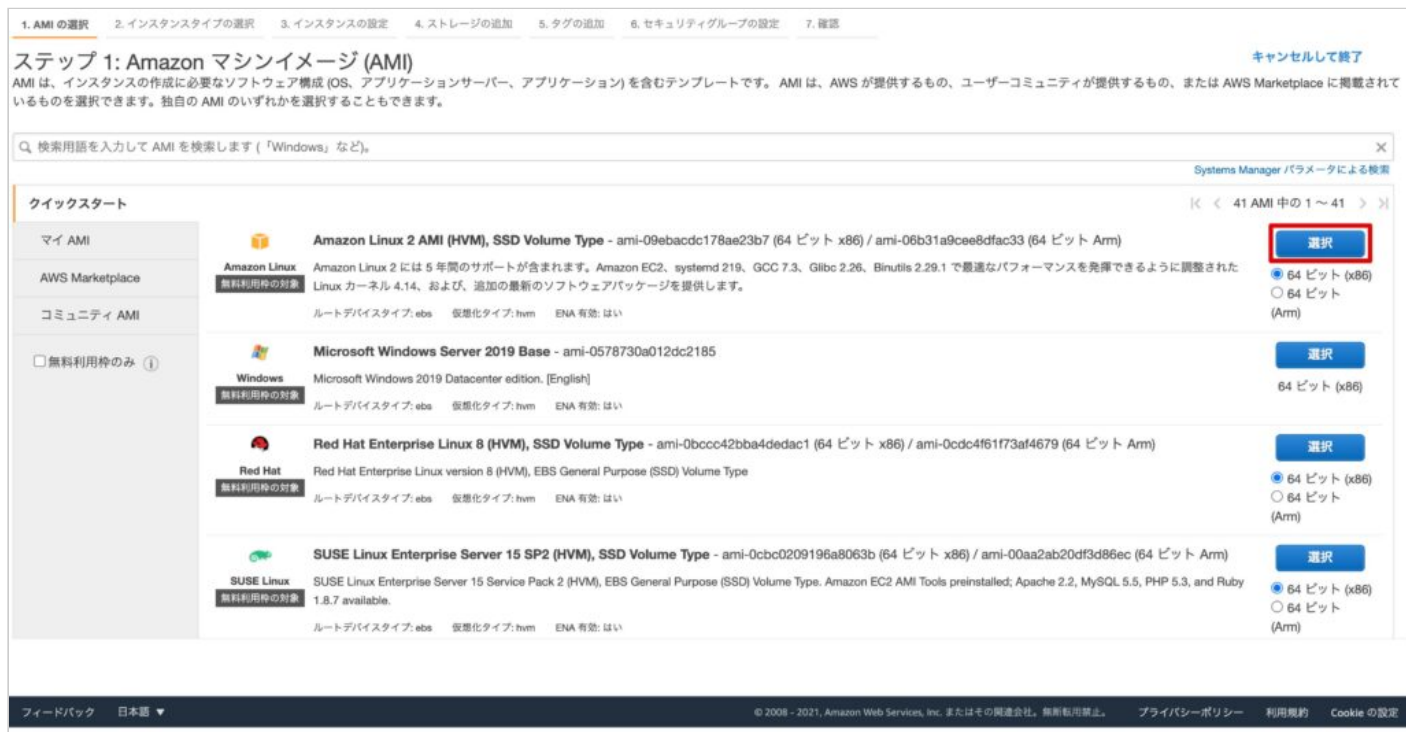
疎通先となるAWSのEC2を構築します。

インスタンスの起動

EC2のトップ画面から「インスタンスの起動」をクリックします。



マシンイメージを選択します。ここでは、無料利用枠の対象となる「Amazon Linux」を選択しています。



インスタンスタイプを選択します。ここでは無料利用枠の対象となる「t2.micro」を選択しています。

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ファミリー 現行世代 列の表示/非表示

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	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
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS のみ	-	中	はい
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS のみ	-	中	はい
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS のみ	はい	最大 5 ギガビット	はい
<input type="checkbox"/>	t3	t3.micro	2	1	EBS のみ	はい	最大 5 ギガビット	はい
<input type="checkbox"/>	t3	t3.small	2	2	EBS のみ	はい	最大 5 ギガビット	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

フィードバック

日本語

© 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。 [プライバシーポリシー](#) [利用規約](#) [Cookie の設定](#)

インスタンスの詳細を設定します。

ネットワークとサブネットは、前回作成したものを選択します。

自動割り当てパブリックIPは「有効」を選択します。

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 Auto Scaling グループに作成する

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 新しい VPC の作成

サブネット 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 ☒ 有効

配置グループ ☐ インスタンスをプレース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 新しいディレクトリの作成

IAM ロール 新しい IAM ロールの作成

シャットダウン動作

停止 - 休止動作 ☐ 停止動作に休止動作を追加する

終了保護の有効化 ☐ 誤った終了を防止します

モニタリング ☐ CloudWatch 詳細モニタリングを有効化
追加料金が適用されます。

テナンシー

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

フィードバック

日本語

© 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。 [プライバシーポリシー](#) [利用規約](#) [Cookie の設定](#)

ストレージの設定は変更不要です。

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-03680f2b2c0474345	<input type="text" value="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 GiB 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

フィードバック日本語 © 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。プライバシーポリシー利用規約Cookie の設定

タグの追加も変更不要です。

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 ⓘ
このリソースには現在、タグがありません				
[タグの追加] ボタンをクリックするか クリックして Name タグを追加します。タグを作成するためのアクセス許可が IAM ポリシー に含まれていることを確認します。				

タグの追加 (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

フィードバック日本語 © 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。プライバシーポリシー利用規約Cookie の設定

セキュリティグループの設定に関しては、デフォルトで「0.0.0.0/0(全てのIPアドレス)」からのSSHアクセスが許可されているため、自身のネットワークからのみアクセス可能となるように設定を変更します。

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:
説明:

タイプ ①	プロトコル ①	ポート範囲 ①	ソース ①	説明 ①
SSH	TCP	22	カスタム <input type="text" value="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

フィードバック 日本語 ▼ © 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。 プライバシーポリシー 利用規約

まず、自身が利用しているグローバルIPアドレスを確認します。

ここでは[CMAN](#)のIPアドレス確認ページで確認しています。

CMAN サーバー監視/ネットワーク監視サービス <http://www.cman.jp/network/>

cman.jp > サーバ監視TOP > サーバメンテ支援 > IPアドレス確認

あなたが現在インターネットに接続しているグローバルIPアドレス確認

あなたの利用しているIPアドレス

(192.168.1.100)

このIP確認 ▶ 登録情報 ▶ PING応答 ▶ Port開放 ▶ DNS情報 ▶ HTTP確認

cman.jp 関連ページ

- ④ IPアドレス(グローバルIP)とは？
- ④ IPアドレスの確認方法は？
- ④ 固定IPと動的IPの違いは？
- ④ ホームページにアクセスすると情報が取られる？
- ④ IPアドレス一覧
- ④ サブネットマスクとは？
- ④ WHOISとは？

長期の機械的な利用は遮断や空ページとすることがあります。

ソースに「確認したグローバルIPアドレス」を入力します。サブネットマスクは"/32"で大丈夫です。

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:
説明:

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 <input type="text" value=":::/32"/>	例: SSH for Admin Desktop

ルールの追加

キャンセル 戻る **確認と作成**

フィードバック 日本語 ▼ © 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。 プライバシーポリシー 利用規約 Cookie の設定

グローバルアドレス

入力内容を確認し、「起動」をクリックします。

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。

AMI の詳細 [AMI の編集](#)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-
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
t2.micro	-	1	1	EBS のみ	-	Low to Moderate

セキュリティグループ [セキュリティグループの編集](#)

セキュリティグループ名: launch-wizard-2
説明: launch-wizard-2

タイプ	プロトコル	ポート範囲	ソース	説明
SSH	TCP	22	<input type="text" value=":::/32"/>	

インスタンスの詳細 [インスタンスの詳細の編集](#)

ストレージ [ストレージの編集](#)

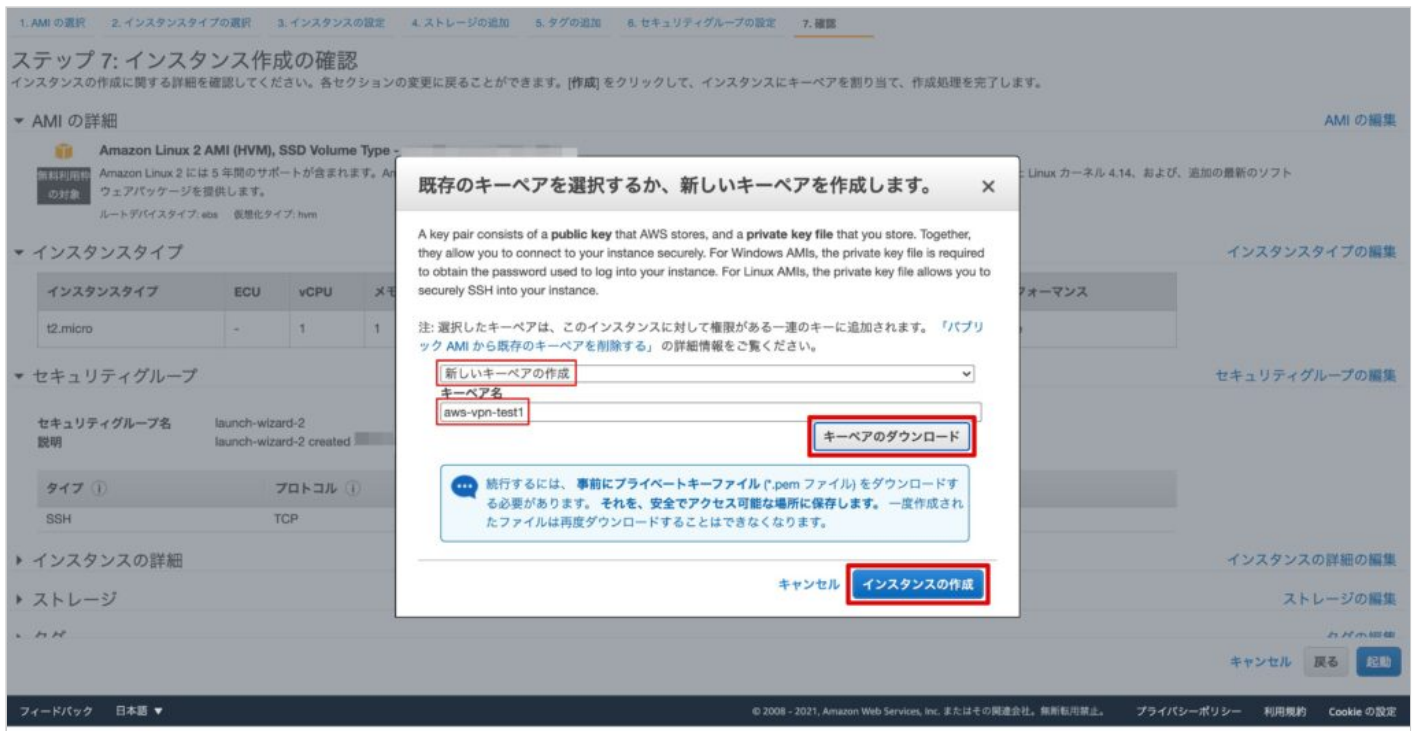
タグ [タグの編集](#)

キャンセル 戻る **起動**

フィードバック 日本語 ▼ © 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。 プライバシーポリシー 利用規約

EC2にアクセスするためのキーペアを作成し、ダウンロードします。

「新しいキーペアの作成」を選択し、キーペア名は「aws-vpn-test1」としています。
キーペアをダウンロードし、「インスタンスの作成」をクリックします。



作成されたインスタンスを確認します。

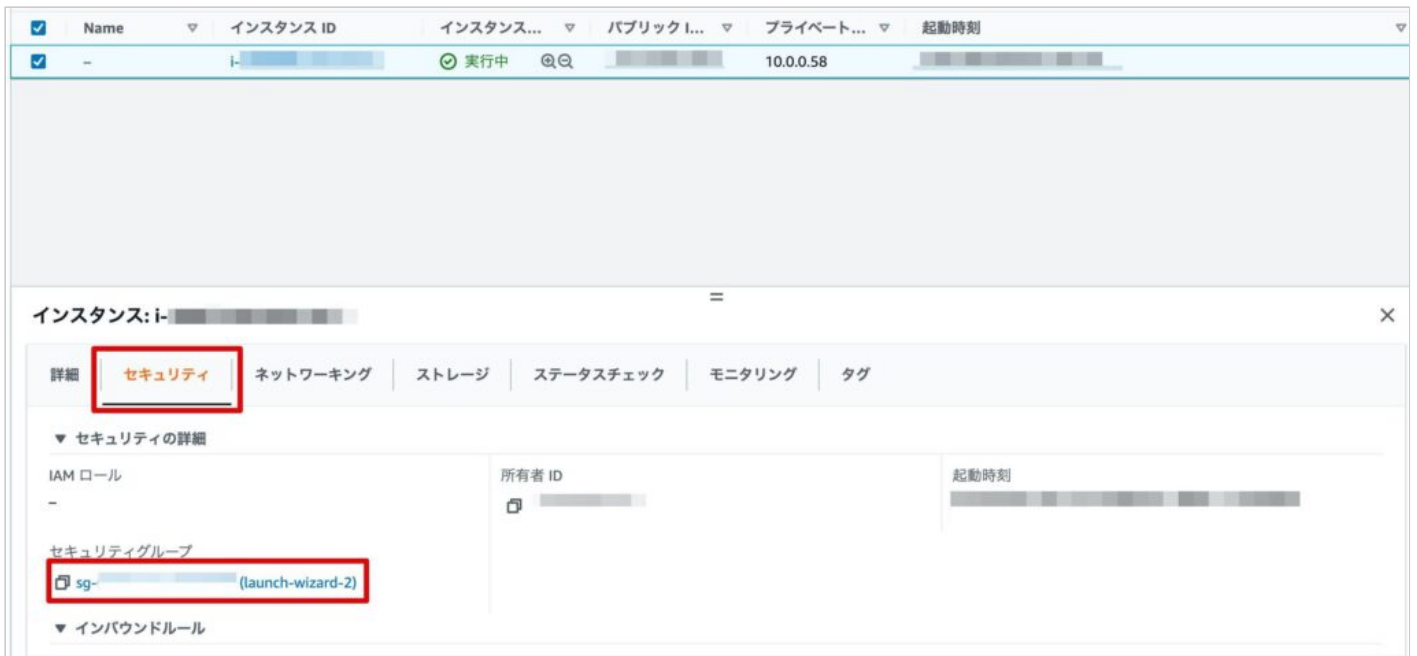
※パブリックIPv4アドレスとプライベートIPv4アドレスが付与されていることを確認します。



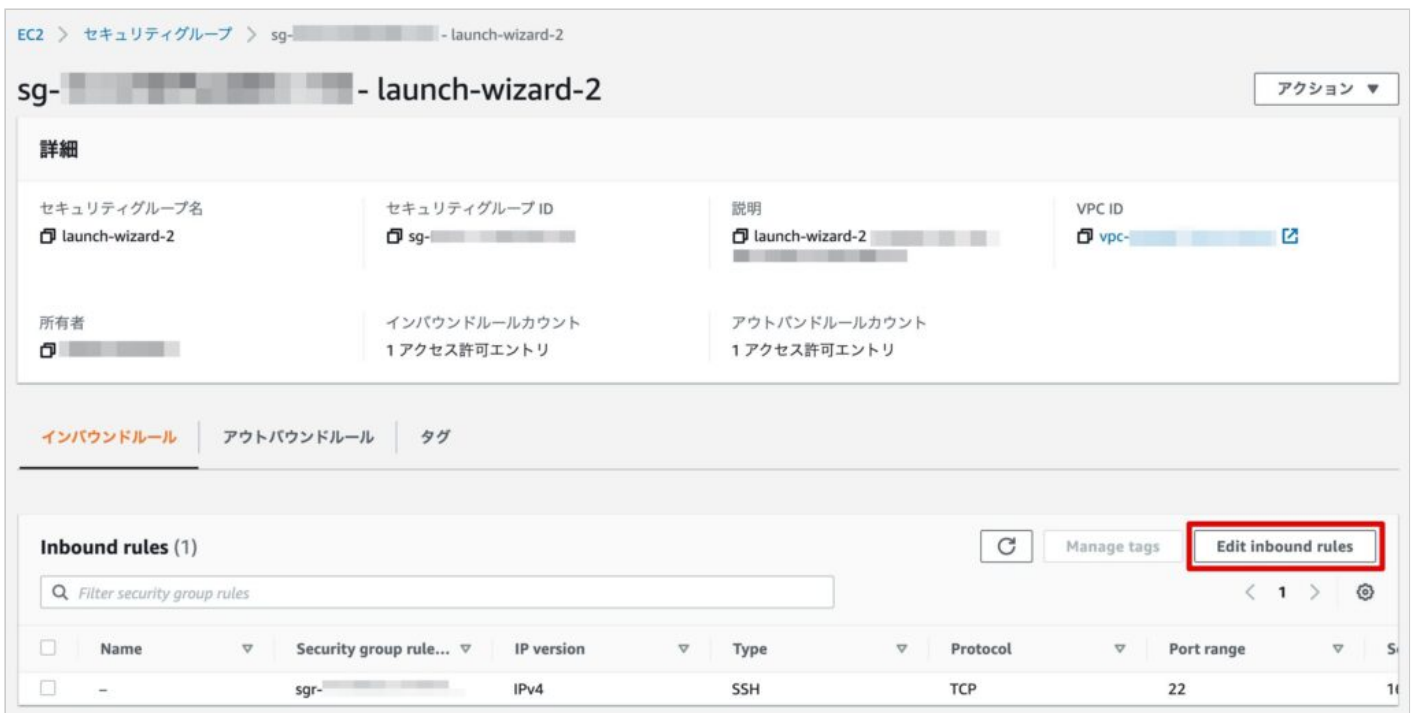
セキュリティグループの追加設定

CML環境からのアクセスを許可するために、セキュリティグループの追加設定を行います。

「セキュリティ」タブから「セキュリティグループ」をクリックします。



「Edit inbound rules」をクリックします。



「ルールを追加」をクリックします。

EC2 > セキュリティグループ > sg- - launch-wizard-2 > インバウンドルールを編集

インバウンドルールを編集 情報

インバウンドルールは、インスタンスに到達できる着信トラフィックをコントロールします。

Security group rule ID	タイプ <small>情報</small>	プロトコル <small>情報</small>	ポート範囲 <small>情報</small>	ソース <small>情報</small>	説明 - オプション <small>情報</small>
sgr-	SSH	TCP	22	カスタム	<input type="text" value="Q"/> <input type="text" value="/32 X"/>

グローバルアドレス、ローカルネットワーク(192.168.1.0/24)、CMLのLAN(172.16.0.0/24)からのICMP通信を許可します。

EC2 > セキュリティグループ > sg- - launch-wizard-2 > インバウンドルールを編集

インバウンドルールを編集 情報

インバウンドルールは、インスタンスに到達できる着信トラフィックをコントロールします。

Security group rule ID	タイプ <small>情報</small>	プロトコル <small>情報</small>	ポート範囲 <small>情報</small>	ソース <small>情報</small>	説明 - オプション <small>情報</small>
sgr-	SSH	TCP	22	カスタム	<input type="text" value="Q"/> <input type="text" value="/32 X"/>
-	すべての ICMP - IPv4	ICMP	すべて	カスタム	<input type="text" value="Q"/> <input type="text" value="/32 X"/>
-	すべての ICMP - IPv4	ICMP	すべて	カスタム	<input type="text" value="Q"/> <input type="text" value="192.168.1.0/24 X"/>
-	すべての ICMP - IPv4	ICMP	すべて	カスタム	<input type="text" value="Q"/> <input type="text" value="172.16.0.0/24 X"/>

グローバルアドレス
ローカルネットワーク
CMLのLAN

インバウンドルールに追加されていることを確認します。

EC2 > セキュリティグループ > sg- - launch-wizard-2

sg- - launch-wizard-2

アクション

詳細

セキュリティグループ名 launch-wizard-2	セキュリティグループ ID sg-	説明 launch-wizard-2	VPC ID vpc-
所有者 -	インバウンドルールカウント 4 アクセス許可エントリ	アウトバウンドルールカウント 1 アクセス許可エントリ	

インバウンドルール アウトバウンドルール タグ

Inbound rules (4)

Filter security group rules

	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sg-	IPv4	SSH	TCP	22	/32
<input type="checkbox"/>	-	sg-	IPv4	すべての ICMP - IPv4	ICMP	すべて	/32
<input type="checkbox"/>	-	sg-	IPv4	すべての ICMP - IPv4	ICMP	すべて	172.16.0.0/24
<input type="checkbox"/>	-	sg-	IPv4	すべての ICMP - IPv4	ICMP	すべて	192.168.1.0/24

EC2への接続確認

起動したEC2への接続を確認していきます。

※ここでは、MACのTerminalを利用し接続していきます。

インスタンスの画面から「接続」をクリックします。

EC2 > インスタンス > i-

i- のインスタンス概要 情報

接続 インスタンスの状態

インスタンス ID i-	パブリック IPv4 アドレス オープンアドレス	プライベート IPv4 アドレス 10.0.0.58
IPv6 アドレス -	インスタンスの状態 実行中	パブリック IPv4 DNS -
プライベート IPv4 DNS ip-10-0-0-58.ap-northeast-1.compute.internal	インスタンスタイプ t2.micro	Elastic IP アドレス -
VPC ID vpc- (aws-vpn-test)	AWS Compute Optimizer の検出結果 ①レコメンデーションについては、AWS Compute Optimizer に オプトインしてください。 詳細はこちら	IAM ロール -
サブネット ID subnet- (aws-vpn-test-subnet1)		

「SSHクライアント」タブを選択し、アクセス方法を確認します。

EC2 > インスタンス > i- [redacted] > インスタンスに接続

インスタンスに接続 情報

これらのオプションのいずれかを使用してインスタンス i- [redacted] に接続する

EC2 Instance Connect

セッションマネージャー

SSH クライアント

EC2 シリアルコンソール

インスタンス ID

i- [redacted]

1. SSH クライアントを開きます。
2. プライベートキーファイルを見つけます。このインスタンスの起動に使用されるキーは `aws-vpn-test1.pem` です。
3. 必要に応じて、このコマンドを実行して、キーが公開されていないことを確認します。

```
chmod 400 aws-vpn-test1.pem
```

4. ご使用のインスタンスの パブリック IP を使用してインスタンスに接続:

```
[redacted]
```

例:

```
ssh -i "aws-vpn-test1.pem" ec2-user@[redacted]
```

注意: ほとんどの場合、推測されたユーザー名に間違いはありませんが、AMI の使用手順を読んで AMI の所有者がデフォルトの AMI ユーザー名を変更していないか確認してください。

ダウンロードしてキーペアを確認します。

```
[Terminal[AWS]:  
[Terminal[AWS]: ls -l  
total 8  
-rw-r--r--@ 1 [redacted] 1700 [redacted] aws-vpn-test1.pem  
[Terminal[AWS]:
```

このままSSH接続を試みると、キーペアのアクセス権が不適切というメッセージが表示され接続できません。

```
[Terminal[AWS]:  
[Terminal[AWS]: ssh -i "aws-vpn-test1.pem" ec2-user@[redacted]  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@      WARNING: UNPROTECTED PRIVATE KEY FILE!      @  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
Permissions 0644 for 'aws-vpn-test1.pem' are too open.  
It is required that your private key files are NOT accessible by others.  
This private key will be ignored.  
Load key "aws-vpn-test1.pem": bad permissions  
ec2-user@[redacted]: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
[Terminal[AWS]:
```

AWSの接続説明にある通り、アクセス権を変更します。

```
[Terminal[AWS]:  
[Terminal[AWS]: chmod 400 aws-vpn-test1.pem  
[Terminal[AWS]:
```

アクセス権が変更されたことを確認します。

```
[Terminal[AWS]: ls -l  
total 8  
-r-----@ 1 1700 aws-vpn-test1.pem  
[Terminal[AWS]:
```

再度SSH接続を試みると、EC2へ接続できました。

```
[Terminal[AWS]:  
[Terminal[AWS]: ssh -i "aws-vpn-test1.pem" ec2-user@  
[ec2-user@ip-10-0-0-58 ~]$  
  
  __|  __|_ )  
 _| (  /  Amazon Linux 2 AMI  
___|\___|___|  
  
https://aws.amazon.com/amazon-linux-2/  
4 package(s) needed for security, out of 16 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-0-0-58 ~]$
```

これで、AWSサイト間VPN接続のためのEC2構築は完了です！