Alibaba Cloud Virtual Private Cloud

User Guide

Document Version20190221

目次

| 1 VPC とサブネット 1.1 デフォルトVPCとVSwitchの作成 | 1 |
|---|----|
| 1.2 Linuxカーネルのためのマルチキャスト構成 | 2 |
| 2 ルート | 7 |
| 3 ネットワーク接続 | 8 |
| 3.1 Classic Link | 8 |
| 3.1.1 Classic Link 接続の作成 | |
| 3.1.2 ClassicLink概要 | |
| 3.1.3 ClassicLink接続のキャンセル | |
| 3.1.4 ClassicLinkの無効化 | |
| 4 アクセス制御 | 15 |
| 4.1 ECSセキュリティグループの構成 | 15 |

1 VPC とサブネット

1.1 デフォルトVPCとVSwitchの作成

クラウドリソースを作成時に使用可能なVPCとVSwitchがない場合は、デフォル トVPCとVSwitchを使用できます。デフォルトVPCとVSwitchはインスタンスを作成するとと もに作成されます。本ドキュメントではECSを例として、デフォルトVPCとVSwitchの作成方法 を説明します。

一つのリージョンには、一つだけのVPCと複数のVSwitchを作成できます。 その理由は、VPCが リージョンに基づいたリソースで、VSwitchはゾーンに基づいたリソースなのである。 デフォル トVSwitchは各ゾーンに存在可能です。 デフォルトVPCとVSwitchのプロパティは次の通りで す:

| デフォルトVPC | デフォルトVSwitch |
|---|---|
| 各リージョン内のデフォルトVPCがユニークで | 各ゾーン内のデフォルトVSwitchがユニークで |
| ある。 | ある。 |
| デフォルトVPCのネットマスクは/16であり、 | デフォルトVSwitchのネットマスクは/20であ |
| (例:172.31.0.0/16)最大65536のプライ | り、(例:172.31.0.0/20)最大4096のプライ |
| ベートIPアドレスを提供できます。 | ベートIPアドレスを提供できます。 |
| デフォルトVPCはAlibaba Cloudに割り当て られたVPCのクォータを占めません。 | デフォルトVSwitchはAlibaba Cloudに割 り当てられたVSwitchのクォータを占めませ ん。 |
| デフォルトVPCはシステムにより作成されま | デフォルトVSwitchはシステムにより作成さ |
| す、ご自身で作成されたVPCはノンデフォルト | れます、ご自身で作成されたVSwitchはノンデ |
| VPCです。 | フォルトVSwitchです。 |
| デフォルトVPCとノンデフォルトVPCの操作 方法及び仕様が一致しています。 | デフォルトVSwitchとノンデフォルト VSwitchの操作方法及び仕様が一致していま す。 |

1. ECSコンソールにログインします。

2. 左側のメニューで、インスタンスをクリックして、インスタンスを作成をクリックします。

- 3. エキスパート向けを選択します。
- 基本構成ページで、ECSインスタンスを設定して、次のステップ:ネットワークをクリックします

5. ネットワークページで、デフォルトVPCとデフォルトVSwitchを選択します。 次のステッ プ:システム構成をクリックします。

| Elastic Compute Service (ECS) | Basic Custom | | | 🐺 Purchased history 🗎 Buy Disk 🖃 Console |
|---|---|------------------------------------|---|--|
| Basic Configurations (R | equired) 2 Networking (Required) | ③ System Configurations | ④ Grouping | 5 Preview (Required) |
| Wetwork * | VPC ① | | | |
| How to Select a Network | [Default]vpc-m5en3xz5v6d V 📀 Default VSwitch | You can Go to Console and Create > | | |
| | If you need to create a new VPC, you can Go to Console and Create > | | | |
| | VPC: [Default]vpc- VSwitch Zone: Random | | VSwitch: Default VSwitch VSwitch CIDR Block: - | |

6. ログイン認証情報とインスタンス名を設定し、注文を確定をクリックします。

インスタンスを作成後、デフォルトVPCとデフォルトVSwitchはリージョン内で自動的に作成 されます。

図 1-1: デフォルトVPC

| 🏴 China (Qingdao) 🕶 | | | a | k 🔺 | 306 Billi | ng Management | English |
|---------------------------|---------------------------|-------------------------------|-------------|---------|--------------|---------------------|---------------|
| VPCs | | | | | | | |
| Create VPC Refresh Custom | | | | | Instance Nar | ne 🗸 🛛 Enter a name | or ID |
| Instance ID/Name | Destination CIDR Block | Status | Default VPC | Route 1 | Table | VSwitch | Actions |
| vpc-f TEST.A | 172.16.0.0/12 | Available | No | 1 | | 0 | Manage Delete |
| vpc- | 172.31.0.0/16 | Available | Yes | 1 | | 2 | Manage Delete |

図 1-2: デフォルトVSwitch

| | 📕 China (Qingdao) 🕶 | | | | ۹ 🔺 | Billing Ma | anagement . | English |
|---|------------------------|--------|-----------|---------------------------|-----------------|--------------------------|---------------------------------------|-----------------------------|
| | VSwitches | | | | | | | |
| | Create VSwitch Refresh | Custom | | | | Instance Name \vee | Enter a name o | or ID |
| l | Instance ID/Name | VPC | Status | Destination CIDR Block | Default VSwitch | Zone | Number of Available Private IPs | Actions |
| | VSW- | vpc- | Available | 172.31.128.0/2 0 | Yes | China North 1 Z one C | 4091 | Manage Delete Purchase V |

1.2 Linuxカーネルのためのマルチキャスト構成

Linuxマルチキャストツールは主にAlibaba Cloud VPCネットワーク、及びクラシックネット ワークに使用されます。マルチキャストツールのクライアント及びサーバーにはLinuxカーネル モジュールとコマンドラインが含まれています。現在のネットワーク環境に適応するために、 カーネルモジュールを使用してマルチキャストパケットとユニキャストパケットを相互に変換す る必要があります。 コマンドラインはマルチキャストグループの設定に使用されます。

環境の配置

マルチキャストツールはkernel-devel及びrpm-buildパッケージに依存しています。 次のコ マンドを実行して、kernel-develとrpm-buildがインストールされてるかどうかを確認しま す。

#rpm -qa | grep kernel-devel-`uname -r
#rpm -qa | grep rpm-build

インストールされていない場合は、次のコマンドでインストールを実行します。

#yum install kernel-devel-`uname -r` -y
#yum install rpm-build -y

マルチキャストエージェントツールのインストール

マルチキャストエージェントツールをインストールするには、次の手順に従ってください:

1. マルチキャストエージェントツールをダウンロードします。

ダウンロードURL: https://github.com/aliyun/multicast_proxy

multicast_kernelフォルダーを選択します。

2. 次のコマンドを実行して、カーネルバージョンを確認します。

uname -r

注意:カーネルバージョンは4.0、または4.0以上の場合は、コードディレクトリに次のコマン ドを実行してパッチをインストールする必要があります。

patch -p1 < multicast_kernel/patch/kernel_v4.0.patch

3. 次のコマンドを実行して、インストールパッケージを生成します。

sh tmcc_client_auto_rpm.sh; sh tmcc_server_auto_rpm.sh

4. 次のコマンドを実行して、エージェントツールをインストールします。

rpm -Uvh multi_server-1.1-1.x86_64.rpm rpm -Uvh multi_client-1.1-1.x86_64.rpm

5. 次のコマンドを実行して、multisと multicサービスの自動起動を設定します。

🗎 注:

エージェントが停止されると、サービスは自動的に停止します。

chkconfig multis on --level 2345 chkconfig multis off --level 016

chkconfig multic on --level 2345 chkconfig multic off --level 016

エージェントサービスの起動及び停止

・エージェントサービスの起動

マルチキャストツールはserviceを通してクライアントとサーバーを起動します。 起動プロセ スにはカーネルモジュールのローディング、構成ファイルからの構成情報のローディングが含 まれています。 本ドキュメントでは、JSON形式で構成ファイルを保存します。

首注:

初回起動時は、構成ファイルは不要です。実行時構成ファイルは自動的に保存されます。

- サーバー (ルート権限)

service multis startを実行します

- クライアント (ルート権限)

service multic startを実行します

・エージェントサーバーの停止

停止プロセスとしては、構成情報の保存、及び対応するカーネルモジュールのアンインストー ルが実行されます。構成情報は、デフォルトで次回起動の構成ファイルとして保存されます。 つまり、エージェントが再起動されると、構成情報はデフォルトで自動的に復元されます。構 成情報を保存しない場合、サーバーを停止する前にコマンドラインで構成情報をクリアしてく ださい。

- サーバー (ルート権限)

service multis stopを実行します

- クライアント (ルート権限)

service multic stopを実行します

エージェントサービスを再起動

- サーバー (ルート権限)

service multis restartを実行します

- クライアント (ルート権限)

service multic restartを実行します

スクリプトを使用しての、マルチキャストエージェントの設定

提供されるスクリプトを使用してマルチキャストを設定できます。 ここをクリックしてスクリプ トを取得します。

注:

自動化スクリプトを使用してマルチキャストを設定することをお勧めします。 スクリプトを実 行する前にreadmeをお読みください。

サーバー構成

サーバーでマルチキャストを配置し、グループにマルチキャストメンバーを追加する必要があり ます。各サーバーは最大10のマルチキャストグループを対応しています。各マルチキャストグ ループは最大128人のサーバーマルチキャストメンバーを対応しています。コマンドラインは/ usr/local/sbinディレクトリにインストールされます。

multis_adminコマンドを実行してサーバーを設定し、multis_admin -helpを実行して説明の詳細を確認できます。

```
multis_admin -- This command can be used to configure multicast server
Usage:
multis_admin -A -m {multi_ip} -j {ip1,ip2,ip3...}
multis_admin -A -m {multi_ip} -q {ip1,ip2,ip3...}
multis_admin -D -m {multi_ip}
multis_admin -C
multis_admin -P -m {multi_ip}
multis_admin -L -m {multi_ip}
multis_admin -S
multis_admin -H
Options:
-A/-- Add add multicast group
-D/--delete del multicast group
-C/--clear clear multicast group
-P/--stats packets statistic
-S/--show show multicast group
-L/--list list multicast group member
-H/--help help info
-j/--join vm join multicast group
-q/--quit vm quit multicast group
```

-m/--multiip multicast ip

クライアント構成

クライアントを追加したマルチキャストグループの情報を設定する必要があります。一つのクラ イアントサーバーは最大10の異なったマルチキャストグループに所属できます。

multic_adminコマンドをJっこうしてクライアントを設定し、 multic_admin -helpを実行 して説明の詳細を確認できます。

```
multic_admin -- This command can be used to configure multicast client
Usage:
multic_admin -A -i {ip} -p {port} -m {multi_ip}
multic_admin -D -i {ip} -p {port}
multic_admin -C
multic_admin -P -i {ip} -p {port}
multic_admin -L
multic_admin -H
Options:
-A/--add add multicast server ip and port
-D/--delete del multicast server ip and port
-C/--clear clear multicast server information
-P/--stats recv packets statistic
-L/--list list all multicast server ip and port
-H/--help help info
-i/--ip multicast server ip, the ip of multicast provider
-P/-- Port UDP port, the multicast Port
-m/--multi_ip multicast ip
```

2ルート

3ネットワーク接続

3.1 Classic Link

3.1.1 Classic Link 接続の作成

ClassicLink 接続を構築すると、クラシックネットワーク内の ECS インスタンスを VPC ネット ワークにデプロイされているリソースにアクセスすることができます。

Classic Link の制限事項をよく理解してください。 詳細はこちらをご参照ください*ClassicLink*概 要.

- 1. VPCコンソールにログインします。
- 2. 対象VPCのリージョンを選択し、IDをクリックします。
- 3. VPC の詳細ページで、Classic Link の有効化をクリックします。 表示されるダイアログボッ クスで、OKをクリックします。
- 4. ECS コンソールにログインします。
- 5. 左側のメニュで、 インスタンスをクリックします。
- 6. リージョンを選択し、対象クラシック ECS インスタンスを検索します。
- 7. 詳細 > ネットワークとセキュリティグループ > VPC へ接続をクリックします。
- 8. 表示されるダイアログボックスで、対象VPCを選択してOKをクリックします。 セキュリティ グループ構成のリンクをクリックします。

| Conn | ect to VPC | \times |
|------|--|----------|
| | Connected VPC: : VPC1 / vnc- ClassicLink | |
| | When you connect to a VPC, you must configure the security group rules to ensure connectivity. | |
| | Go to the instance security group list and add ClassicLink rules | |
| | | |
| | | OK |

9. Classic Link ルールの追加をクリックし、次の情報に従ってセキュリティルールを構成して ください。 OKをクリックします。

| 構成 | 説明 |
|-----------------------|--|
| クラシックセキュリ ティグループ | クラシックネットワークセキュリティグループを表示します。 |
| VPC セキュリティグ ループの選択 | 使用したいセキュリティグループを選択します。 選択可能なセキュ リティグループは最大5までです。 |
| モード | 次のモードから1つ選んでください: |
| | クラシック<=>VPC:接続されたリソースの間には相互にアクセスできます(推奨) クラシック=>VPC:クラシック ECS インスタンスに権限付与して、接続された VPC 内のクラウドリソースにアクセスします。 クラシック<=VPC:接続された VPC 内のクラウドリソースに権限付与して、クラシック ECS インスタンスにアクセスします。 |
| プロトコルタイプ及 びポート範囲 | 通信に使用されるプロトコル及びポートを選択します。 ポートの形 式はxx/xxでなければなりません。 たとえば、ポート80が使用され る場合、80/80を入力してください。 |
| 優先度 | ルールの優先度を設定します。 数字が小さいほど、優先度が高くな ります。 |
| 説明 | セキュリティルールの説明を入力します。 |

10ECSインスタンスページで、右上にある表示項目のアイコンをクリックし、コネクションス テータスにチェックを入れます。 OKをクリックします。

図 3-1:表示項目

| Elastic Compute Serv | Instance List | | | | | | | Bulk Action |
|-----------------------------|--|--|------------------------|--|--|----------------|----------------------------|----------------------------------|
| Overview | * Select the instance attribute, or directly enter the keyword | Q Tag | | | | | Advanced Search | ≛ o ? |
| Launch Template | Instance ID/Name Tags Monitor Zone | IP Address Status - | Instance Type Family | VPC Details | Billing Method + In | top nstance | | Actions |
| Auto Scaling Block Storage | ECS01 | 47.97.160.112(Internet IP Address) 192.168.169.252(Private IP Running Address) | ecs.g5.large ecs.g5 | vpc- bp13cwaie5zzbuy740yqu vsw-bp1oisthjafqqsrqq7ppm | Subscription July 26, 2018, 00:00 Expiring soon | Mana | age Connect Change | e Configuration Renew More≁ |

図 3-2: コネクションステータス

| Se | et Display Items | | | | | | \times |
|----|------------------|---|-------------------|------|----------------|---|-------------------|
| | Operating System | | Tags | | Monitor | ¥ | Zone |
| • | IP Address | • | Status | | Network Type | | Configuration |
| • | VPC Details | • | Instance Type Fan | nily | Billing Method | | Automatic Renewal |
| | Key Pairs | | Link Status | | RAM Role | • | Stop Instance |
| | | | | | | | |
| | | | | | | | ОК |

図 3-3: VPC へ接続済み

| 1 | ins | stance Li | st | | | | | | | | | Create Instance |
|---|-----|-------------------------|-----------------------|---------------|------------------------|---|----------|-------------------|--------------------------------------|------------------|-------------------|--|
| | Ŧ | Select th | e instance attribute, | , or directly | y enter the key | word | Q | Tag | Adv | anced Search | Show All Resource | es 🔿 🗷 🔅 ? |
| 7 | T | Filters : | Billing Method: Su | Ibscription | × Netwo | rk Type: Classic × Clear All | | | | | | |
| 0 | | Instance | ID/Name | Monitor | Zone | IP Address | Status 👻 | Network Type 👻 | Configuration | Billing Method 👻 | Link Status | Actions |
| C | | i- bp12 Test04.10 | 6 | R | China East 1 Zone B | 112 (Internet IP Address) 10 (Intranet IP Address) | | Classic | 1 vCPU 1 GB ecs.t1.small 2Mbps | Subscription | Linked | Manage Change Configuration Renew More + |

3.1.2 ClassicLink概要

VPC は ClassicLink 機能を提供しています。ClassicLink を使用して、クラシックネットワー ク内の ECS インスタンスをイントラネットを通して VPC 内のクラウドリソースに接続できま す。

使用制限

ClassicLink 機能を使用する前に、次の各事項を確認してください:

- ・同一 VPC に接続可能なクラシックネットワークECSインスタンスの数は最大1000です。
- 1つのクラシックネットワークのECSインスタンスは1つのみのVPCに接続可能です。(同一ア カウント/同一リージョンに属する)

アカウントAのECSインスタンスをアカウントBのVPCに接続するなどのクロスアカウント接 続を行う場合、ECSインスタンスをアカウントAからアカウントBへ転送できます。

· VPCのClassicLink機能を有効にするには、次の条件を満たす必要があります:

| VPCのCIDRブロック | 制限事項 |
|----------------|--|
| 172.16.0.0/12 | 当該VPCには10.0.0.0/8というカスタマイズルートエントリ がありません。 |
| 10.0.0/8 | 当該VPCには10.0.0.0/8というカスタマイズルートエント リがありません。 クラシックネットワーク内のECSインスタンスと通信する VSwitchのCIDRブロックは10.111.0.0/16であることを 確かめてください。 |
| 192.168.0.0/16 | 当該VPCには10.0.0/8というカスタマイズルートエント リがありません。 クラシックネットワークのECSインスタンスに、CIDRブ ロックが192.168.0.0/16で、次ホップはプライベー トNICであるルートエントリを追加します。次に配信し ているスクリプトを使用してルートを追加できます。ここをクリックして、ルートスクリプトをダウンロードして ください。 注: スクリプトを実行する前に、スクリプトにあ るreadmeファイルを熟読してください。 |

接続シナリオ

次のテーブルでは、クラシックネットワーク内のECSインスタンスをVPCネットワークに接続す るシナリオを示しています。

| イニシェー | リージョ | 受信側ネットワークタイプ/イントラネット通信 | | | | | | |
|---------------------|--|--|---|--|--|--|--|--|
| タのネット ワークタイ プ | $\begin{array}{c c} (x,y,y,y) & (y,y,y,y,y) \\ (x,y,y,y,y,y,y,y,y,y,y,y,y,y,y,y,y,y,y,y$ | | VPC | | | | | |
| Classicネッ トワーク | 同一リー ジョン 同一アカウ ント | セキュリティグループに同一ア カウントの権限付与ルールを追 加します。 | ClassicLink接続を作成します。 | | | | | |
| | 同一リー セキュリティグループにアクロ ジョン スアカウント権限付与ルールを 異なるアカ 追加します。 ウント | | ・ ソリューションA: 1. クラシックネットワーク内のECSインスタンスをVPCネットワークへ移行します 2. VPC間の接続を行います ・ ソリューションB: 1. クラシックネットワーク内のECSインスタンスの所有権をVPCのアカウントに変更します。 2. ClassicLink接続を作成します。 | | | | | |
| | 異なるリー ジョン 同一アカウ ント 異なるリー ジョな ス アカ ウント | 両方のECSインスタンスとも VPCネットワークへ移行しま す。 2. 2つのVPCを相互に接続しま す。 | イニシェータECSインスタン スをVPCネットワークへ移行 します。 2つのVPCを相互に接続しま す。 | | | | | |
| VPC | 同一リー ジョン 同一アカウ ント | ClassicLink接続を作成します。 | VPC間の接続を行います | | | | | |

| 同一リー ジョン クロスアカ | ・ ソリューションA: 1. クラシックネットワーク内 | |
|------------------------------|---|--|
| ウント | のECSインスタンスをVPC へ移行します 2. VPC間の接続を行います ・ソリューションB: | |
| | クラシックネットワーク内 のECSインスタンスをVPC のアカウントへ移行しま す。 ClassicLink接続を作成し ます。 | |
| クロスリー ジョン 同一アカウ ント | クラシックネットワーク内の 受信側のECSインスタンスを VPCへ移行します VPC間の接続を行います | |
| クロスリー ジョン クロスアカ ウント | | |

ClassicLinkの説明

クラシックネットワークとVPCの間の相互通信の実現する方法と、異なった2つのクラシック ネットワークの間の相互通信を実現する方法が一致しています。 それにより、イントラネットの 遅延と帯域幅の制限が変わりません。 ダウンタイム移行、ホット移行、停止、起動、再起動、 システムディスクの交換などの操作は構築済みのClassicLinkの接続を変更することができませ ん。

クラシックネットワークとVPCは異なった種類のネットワークです。 ClassicLinkはルーターを 通して2つのネットワークの間でプライベート通信チャネルを構築します。 ClassicLink機能を 使用するには、ネットワークIPアドレスの重複をできるだけ避けてください。

Alibaba CloudクラシックネットワークのIPアドレス範囲は10.0.0.0/8 です(10.111.0.0/16 は含まれていません) VPCのIPアドレス範囲内のIPアドレスは10.0.0.0/8と重複しない限り、 ClassiLinkを通してプライベート通信を行うことが可能です。 ClassicLinkを通してクラシック ネットワークと通信できるVPCのIPアドレス範囲は172.16.0.0/12、10.111.0.0/16及び192.168 .0.0/16となります。

ClassicLinkの原理

クラシックネットワーク内のECSインスタンスがClassicLinkを通してVPCに接続した後:

 クラシックネットワーク内のECSインスタンスはVPC内のクラウドリソースへアクセス可能に なります。

たとえば、クラシックネットワーク内のECSインスタンスはIPアドレス範囲10.0.0.0/8のVPC に接続済みとします、その場合VPCにはIPアドレス範囲が10.111.1.0/24となるVSwitchがあ ります。 ECSインスタンスとRDSなどのクラウドリソースをVSwitchにデプロイしている場 合は、クラシックネットワーク内のECSインスタンスはClassicLinkを通してこれらのリソー スにアクセスすることができます。

ClassicLink接続が完全に確立された後、VPC内のECSインスタンスはVPCに接続済みのクラシックネットワーク内のECSインスタンスにのみアクセスできます。VPCに接続していないクラシックネットワーク内のECSインスタンスや、クラシックネットワーク内の他のクラウドリソースにアクセスすることはできません。

3.1.3 ClassicLink 接続のキャンセル

クラシックネットワークとVPCの間のイントラネット接続が不要になった場合は、いつで もClassicLink接続をキャンセルすることができます。

- 1. ECSコンソールにログインします。
- 2. 左側のメニュで、 インスタンスをクリックします。
- 3. インスタンスのリージョンを選択し、ターゲットのインスタンスを検索します。
- 4. 詳細 > ネットワークとセキュリティグループ > VPCから切断をクリックします。
- 5. 表示されるダイアログボックスで、OKをクリックします。

3.1.4 ClassicLinkの無効化

ClassicLinkの接続をキャンセル後、ClassicLink機能を無効にすることができます。

- 1. VPCコンソールにログインします。
- 2. ターゲットVPCのリージョンを選択し、IDをクリックします。
- 3. VPCの詳細ページで、クラシックリンクの無効化をクリックします 表示されるダイアログ ボックスでOKをクリックします。

4アクセス制御

4.1 ECSセキュリティグループの構成

- VPCネットワークのECSインスタンスを作成する際に、VPCのデフォルトセキュリティグループ や他のセキュリティグループを使用できます。 セキュリティグループは、ECSインスタンスを通 してインバウンド/アウトバウンドトラフィックを制御する仮想ファイアウォールです。
- VPCネットワークのECSインスタンスのための一般的なセキュリティグループシナリオを本ド キュメントにて一覧表示します。

ケース1:イントラネット通信

VPCのECSインスタンスの間の通信は次の2種類があります:

- ・同一VPC内の同一セキュリティグループに属するECSインスタンスはデフォルトの状況で相互 に通信できます。
- ・異なったVPCに存在する2つのECSインスタンスは相互に通信できません。異なったVPCに 存在する2つのECSインスタンスの間の通信を実現するには、Express ConnectまたはVPN Gatewayを使用してそれらのECSインスタンスを接続し、次の表の示すように、ECSインス タンスのセキュリティグループルールを相互にアクセスできるようにします。

| セキュリティグルー プルール | イ ン/ア ウト | 権限 付与 ポリ シー | プロトコルタ イプ及びポー ト範囲 | 権限付与 タイプ | 権限付与対象 |
|-------------------------------------|----------------|----------------------|--|---|--|
| VPC1内ECSインス タンスのセキュリ ティグループ構成 | イバン イバン イバン | म न म | Windows: RDP 3389/3389 Linux: SSH 22/22 カスタマイズ TCP カスタマイズ | アフドス アフドス アフドスアンドイアクロン ドイアクロシーク レーク レーク レーク スルセスルセス | VPC2内のアクセス元であ るECSインスタンスプライ ベートIP。 すべてのECSインスタンス からのアクセスを許可する 場合、0.0.0.0/0を入力しま す。 |

| セキュリティグルー プルール | イ ン/ア ウト | 権限 付与 ポリ シー | プロトコルタ イプ及びポー ト範囲 | 権限付与 タイプ | 権限付与対象 |
|-------------------------------------|-----------------------|----------------------|---|--|--|
| VPC2内ECSインス タンスのセキュリ ティグループ構成 | インウンド インウド インウド | म म | Windows: RDP 3389/3389 Linux: SSH 22/22 | アドレス フィーク ドフィークセ ス アドレス アイーク マ ス ア | VPC1内のアクセス元であ るECSインスタンスプライ ベートIP。 すべてのECSインスタンス からのアクセスを許可する 場合、0.0.0.0/0を入力しま す。 |
| | イン バウ ンド | म् | カスタマイズ TCP カスタマイズ | アドレス フィール ドアクセ ス | |

ケース2:特定のIPまたはポートからのアクセスを拒否

セキュリティグループを構成することで特定のIPまたはポートをVPC内のECSインスタンスへの アクセスを拒否することができます。

| セキュリティグルー プルール | イ ン/ア ウト | 権 相 与 ポ シ ー | プロトコルタ イプ及びポー ト範囲 | 権限付与 タイプ | 権限付与対象 |
|--|----------------|----------------------------|-------------------------|---------------------------|-----------------------------------|
| ECSインスタンスの すべてのポートに対 する特定のIPアドレ ス範囲からのアクセ スを拒否します。 | イン バウ ンド | 不可 | すべて -1 | アドレス フィール ドアクセ ス | ブロックするIPアドレスの範 囲、例:10.0.0.1/32 |
| ECSインスタンスの ポート22に対する特 定のIPアドレス範囲 からのアクセスを拒 否します。 | イン バウ ンド | 不可 | SSH (22) 22/22 | アドレス フィール ドアクセ ス | ブロックするIPアドレスの範 囲、例:10.0.0.1/32 |

ケース3:特定IPからのアクセスを許可

VPC内のECSインスタンスのためのパブリックIPを構成した場合、次のセキュリティグループ ルールを追加してWindowsリモートログインやLinux SSHログインを許可することができま す。

| セキュリティグルー プルール | イ ン/ア ウト | 権限 付与 ポリ シー | プロトコルタ イプ及びポー ト範囲 | 権限付与 タイプ | 権限付与対象 |
|---------------------------|----------------|----------------------|-------------------------|---------------------------|---|
| Windowsリモートロ グインを許可します | インバウ | म् | RDP 3389/3389 | アドレス フィール ドアクセ ス | すべてのパブリックIPアドレ スからのログインを許可する 場合、0.0.0.0/0を入力して ください。 特定のIPアドレスからのリ モートログインのみを許可す る場合、IPアドレスを入力し てください。 |
| Linux SSHログイン を許可します | イン バウ ンド | र्म | SSH 22/22 | アドレス フィール ドアクセ ス | すべてのパブリックIPアドレ スからのログインを許可する 場合、0.0.0.0/0を入力して ください。 特定のIPアドレスからのリ モートログインのみを許可す る場合、IPアドレスを入力し てください。 |

ケース4:ECSインスタンスにデプロイされたHTTP/HTTPSサービスに対するインターネットからのア クセスを許可

VPC内のECSインスタンスにウェブサイトをデプロイし、EIPやNATゲートウェイを構築して サービスを提供している場合、次のセキュリティグループルールを構成し、インターネットから のアクセスを許可します。

| セキュリティグルー プルール | イ ン/ア ウト | 権限 付与 ポリ シー | プロトコルタ イプ及びポー ト範囲 | 権限付与 タイプ | 権限付与対象 |
|---------------------|----------------|----------------------|-------------------------|---------------------------|---------|
| ポート80へのアクセ スを許可 | イン バウ ンド | म् | HTTP 80/80 | アドレス フィール ドアクセ ス | 0.0.0/0 |
| ポート443へのアクセ スを許可 | イン バウ ンド | ग | HTTPS 443/443 | アドレス フィール ドアクセ ス | 0.0.0/0 |
| ポート80へのアクセ スを許可 | イン バウ ンド | ग | TCP 80/80 | アドレス フィール ドアクセ ス | 0.0.0.0 |