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

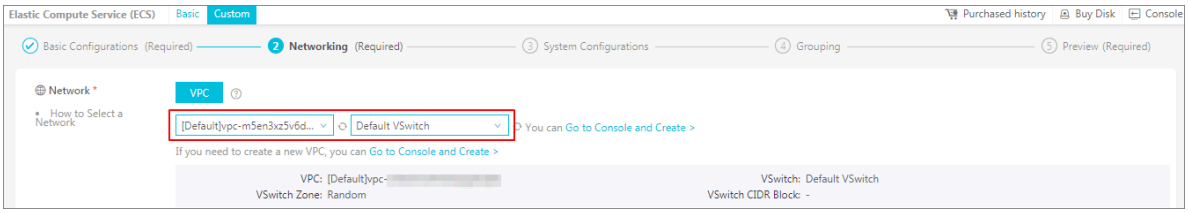
クラウドリソースを作成時に使用可能なVPCとVSwitchがない場合は、デフォルトVPCとVSwitchを使用できます。 デフォルトVPCとVSwitchはインスタンスを作成するとともに作成されます。 本ドキュメントではECSを例として、デフォルトVPCとVSwitchの作成方法を説明します。

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がユニークである。	各ゾーン内のデフォルトVSwitchがユニークである。
デフォルトVPCのネットマスクは/16であり、（例：172.31.0.0/16）最大65536のプライベートIPアドレスを提供できます。	デフォルトVSwitchのネットマスクは/20であり、（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。
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す、ご自身で作成されたVPCはノンデフォルトVPCです。	デフォルトVSwitchはシステムにより作成されます、ご自身で作成されたVSwitchはノンデフォルト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。
4. 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。



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

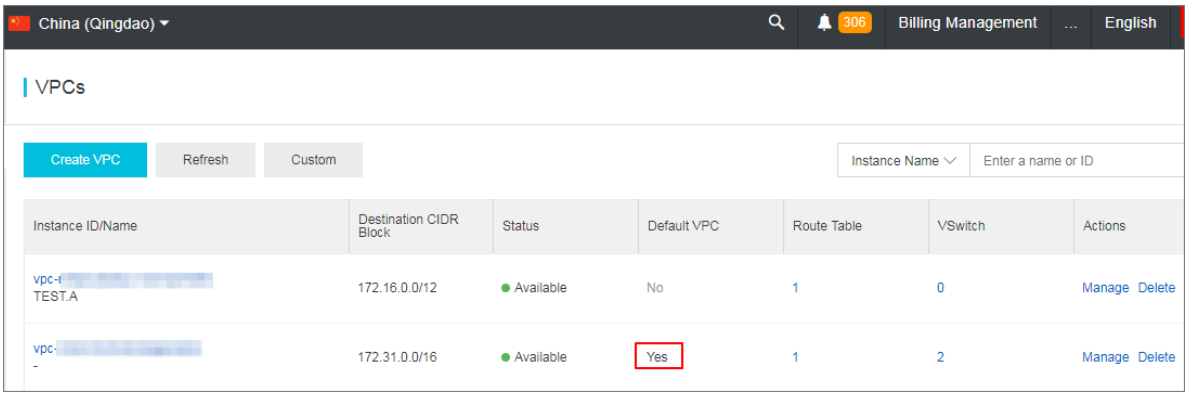
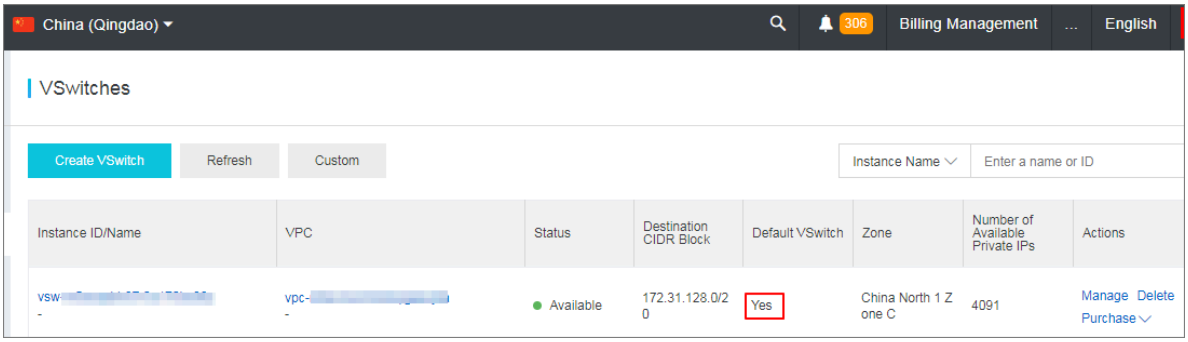


図 1-2 : デフォルトVSwitch



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 &lt; 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。

   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

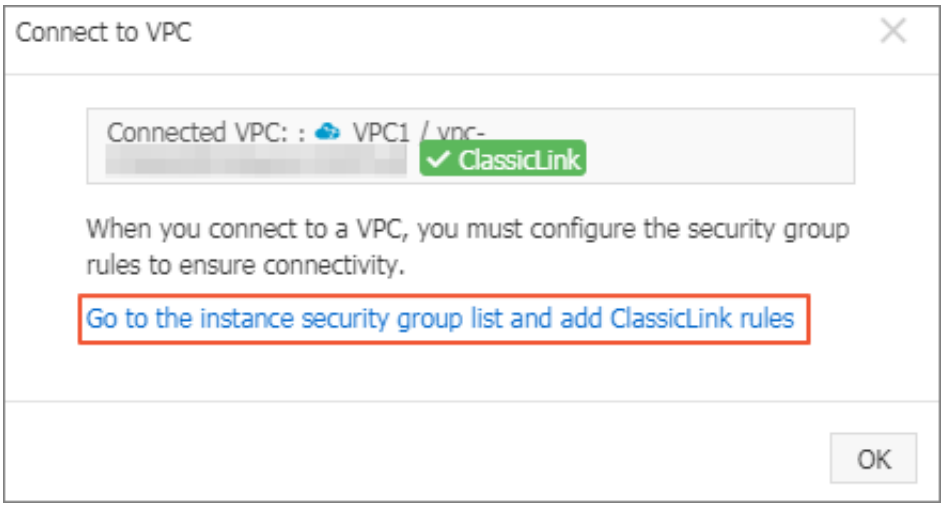
3.1 Classic Link

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。



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。

10.ECS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

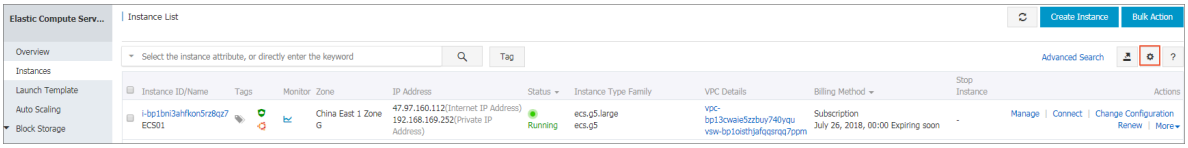


図 3-2 : コネクションステータス

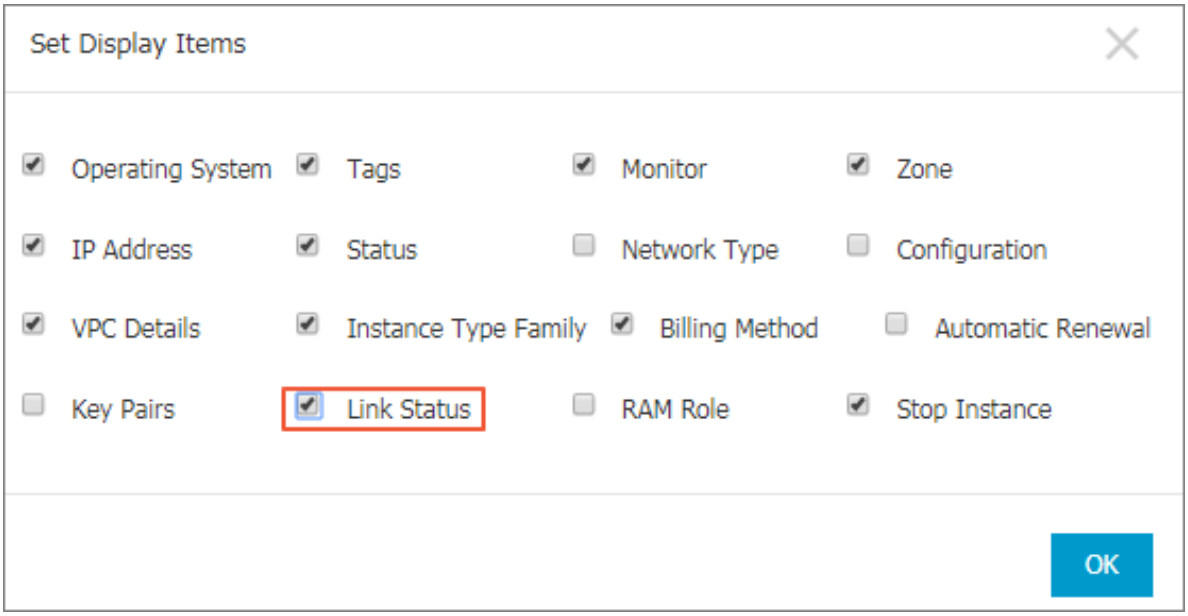
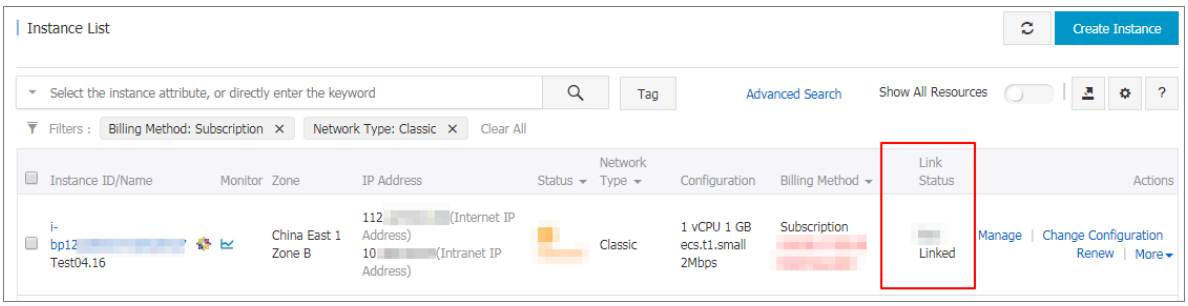


図 3-3 : VPC へ接続済み



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。
10.0.0.0/8	- 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10.0.0.0/8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。

イニシェータのネットワークタイプ	リージョン/アカウント	受信側ネットワークタイプ/イントラネット通信	
		クラシックネットワーク	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。
	同一リージョン 異なるアカウント	セキュリティグループにアクロスアカウント権限付与ルールを追加します。	・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	1. 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。	1. 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. 2つのVPCを相互に接続します。
	異なるリージョン 異なるアカウント		
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インスタンスをVPCのアカウントへ移行します。 2. ClassicLink接続を作成します。	
	クロスリージョン 同一アカウント	1. 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 2. 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	インバウンド	可	Windows: RDP 3389/3389	アドレスフィールドアクセス	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。
	インバウンド	可	Linux: SSH 22/22	アドレスフィールドアクセス	
	インバウンド	可	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	

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	インバウンド	可	Windows: RDP 3389/3389	アドレスフィールドアクセス	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	可	Linux: SSH 22/22	アドレスフィールドアクセス	
	インバウンド	可	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
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	インバウンド	可	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	可	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	可	HTTP 80/80	アドレスフィールドアクセス	0.0.0.0/0
ポート443へのアクセスを許可	インバウンド	可	HTTPS 443/443	アドレスフィールドアクセス	0.0.0.0/0
ポート80へのアクセスを許可	インバウンド	可	TCP 80/80	アドレスフィールドアクセス	0.0.0.0