Virtual Private Cloud

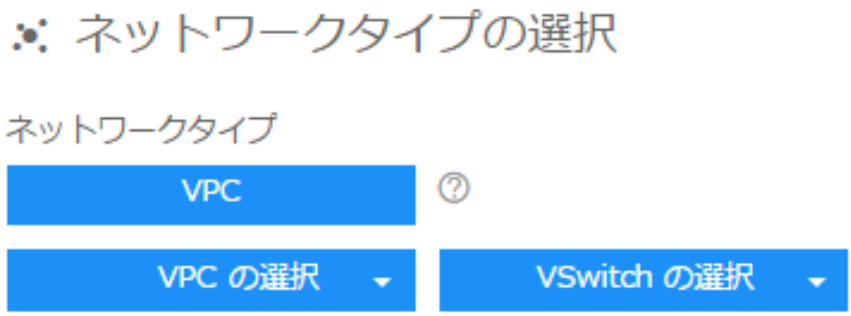
ユーザーガイド

ユーザーガイド

デフォルトの VPC と VSwitch

デフォルトの VPC と VSwitch

Alibaba Cloud は、デフォルトの VPC を VSwitch を備えています。VPC がない場合は、最初にクラウドサービスインスタンスを作成できます。クラウドサービスインスタンスの作成時に、デフォルトの VPC と VSwitch も作成されます。



デフォルトの VPC と VSwitch の設定は、次のとおりです。

デフォルト VPC	デフォルト VSwitch
各リージョンのデフォルト VPC は 1 つのみです。	各アベイラビリティゾーンのデフォルト VSwitch は 1 つのみです。
デフォルト VPC の CIDR ブロックは、常に /16 ネットマスク (172.31.0.0/16) であり、最大 65,536 個のプライベート IP アドレスが利用できます。	デフォルト VSwitch の CIDR ブロックは、常に /20 ネットマスク (172.31.0.0/20) であり、 最大 4,096 個のプライベート IP アドレスが利用できます。
デフォルト VPC は、Alibaba Cloud から割り当てられる VPC クォータを占有しません。	デフォルト VSwitch は、Alibaba Cloud から割り当てられる VSwitch クォータを占有しません。
デフォルト VPC はシステムによって作成され、ユーザーが作成する VPC はいずれもデフォルト以外の VPC です。	デフォルト VSwitch はシステムによって作成され、ユーザーが作成する VSwitch はいずれもデフォルト以外の VSwitch です。
デフォルト VPC もデフォルト以外の VPC も、動作は変わらず、制限も同じです。	デフォルト VPC もデフォルト以外の VSwitch も、動作は変わらず、制限も同じです。

VPC の構築

VPC の作成

前提条件

VPCを作成する前に、VPCネットワークの計画と設計を参照して、プライベートネットワークを設計してください。

手順

[VPC コンソール] にログインします。

左側のナビゲーションバーで **[VPC]** をクリックします。

VPC があるリージョンを選択します。

右上隅にある **[VPCの作成]** をクリックします。

表示されたダイアログボックスで、次の情報を指定します。

設定	説明
VPC Name	VPC の名前を入力します。
Description (オプション)	VPC の説明を追加します。
CIDR block	CIDR (クラスレスドメイン間ルーティング) ブロックの形式で、VPC の IP アドレス範囲を指定します。CIDR ブロックを選択する際には、次の点に注意してください。 - IP アドレス範囲としては、標準のプライベート CIDR ブロック (10.0.0.0/8、172.16.0.0/12、192.168.0.0/1) またはこれらのサブセットを使用できます。 **注意:**

	指定された CIDR ブロックのサブネットを IP アドレス範囲として使用する場合は、Open API を使用して VPC を作成してください。詳細については、「VPC の作成」を参照してください。 - 複数の VPC がある場合や、複数の VPC とオンプレミスの IDC で構成されるハイブリッドクラウドを構築する場合は、ここに示されている CIDR ブロックのサブネットを使用し、ネットワークマスクが /16 を超えないようにすることをお勧めします。 - VPC が 1 つだけであり、この VPC でオンプレミスのデータセンターとの通信が必要ない場合は、ここに示されている CIDR ブロックをどれでも使用できます。 - クラシックネットワークの使用も考慮する必要があります。VPC でクラシックネットワーク内のクラウドプロダクトインスタンスへの接続を計画している場合は、クラシックネットワークの CIDR ブロックとしても使用される CIDR ブロック 10.0.0.0/8 を使用しないことをお勧めします。 - **注意**: IP アドレス範囲に関して特別な要件がある場合は、チケットを起票してお問い合わせください。

[VPCの作成] をクリックします。

関連する操作

VSwitch の作成

VSwitch は、VPC ネットワーク内の基本的なネットワークデバイスです。VPC 内のクラウドプロダクトイン

スタンスの接続に使用されます。VSwitch を追加することにより、仮想ネットワークをサブネットにセグメント化することができます。詳細については、「VSwitch の作成」を参照してください。

ルートテーブルの管理

VRouterとルートテーブルはVPCが作成された後に作成されます。カスタムルートエントリをルートテーブルに追加することができます。ルートテーブルの管理を参照してください。

VPC の削除

VPC リストページでターゲットの VPC を指定して、**[削除]** をクリックします。

> **注意**: VPC を削除する前に、VPC の VSwitch ですべてのインスタンスがリリースまたは移行され、VSwitch が削除されていることを確認してください。

VPC 名の変更

VPC リストページで、ターゲット VPC の ID にマウスポインターを合わせます。鉛筆のアイコンが表示されます。鉛筆のアイコンをクリックして VPC の名前を変更します。

VSwitch の作成

前提条件

ネットワーク環境の設計

VPC の作成

手順

[VPC コンソール]にログオンします。

メニューから [**VPC**] をクリックします。

作成する VSwitch のある VPC のリージョンをクリックします。

ターゲット VPC の ID をクリックします。

[**VPC の詳細**] ページにリダイレクトされます。

[**VSwitch**] をクリックし、[**VSwitchの作成**] をクリックします。

[**VSwitchの作成**] ダイアログで、次の情報を指定します。

設定	説明
VPC	VSwitch がある VPC の ID。
VPC CIDR block	VPC の CIDR ブロック。 CIDR ブロックをバイナリ形式で表示するには、[**Display Binary**] をクリックします。
名前	VSwitch の名前を入力します。
ゾーン	VSwitch のゾーンを選択します。 ゾーンは、1 つのリージョン内で互いに独立した送電網とネットワークを備えている物理的な領域です。同じリージョン内のゾーンは、イントラネットで接続されています。ディザスタリカバリに対応するために、異なる VSwitch を別々のゾーンに作成することをお勧めします。
CIDR block	CIDR (クラスレスドメイン間ルーティング) ブロックの形式で、VSwitch の IP アドレスを指定します。 VSwtich CIDR ブロックを指定する際には、次の点に注意してください。 - VSwitch の使用可能なブロックサイズは、/16 ネットマスクから /29 ネットマスクまでの間の数値です。これにより、8 から 65,536 までの IP アドレスを提供できます。 - VSwitch の CIDR ブロックは、その VSwitch が属する VPC の CIDR ブロックや、VPC CIDR ブロックのサブセットと同じでもかまいません。 **注意**: VSwitch の CIDR ブロックが VPC の CIDR ブロックと同じである場合、作成できる VSwitch は 1 つだけです。 - 先頭と末尾 3 つの IP アドレスは、

	システムによって予約されます。たとえば、CIDR ブロック 192.168.1.0/24 の場合、IP アドレス 192.168.1.0、192.168.1.253、192.168.1.254、192.168.1.255 はシステムによって予約されます。 - VSwitch 内で実行するクラウドプロダクトインスタンスの数も考慮する必要があります。
使用可能なプライベート IP	VSwitch 内で使用可能な IP アドレスの数。
説明(オプション)	VSwitch の説明を追加します。

7. [**OK**] をクリックします。

関連操作

VPC でのクラウドプロダクトインスタンスの作成

[**VSwitch 一覧**] ページで [**インスタンスの作成**] をクリックして、ECS、SLB、または RDS インスタンスを作成します。詳細については、「VPCにインスタンスの作成」を参照してください。

VSwtich の変更

[**VSwitch 一覧**] ページでターゲットの VSwitch を指定して、[**編集**] をクリックします。または、マウスポインターを VSwitch 名に合わせて、VSwitch の名前を変更します。

VSwitch の削除

[**VSwitch 一覧**] ページでターゲットの VSwitch を指定して、[**削除**] をクリックして、**確認**をクリックしてVSwitchを削除します。

注意: VSwitch を削除する前に、その VSwitch に含まれるクラウドプロダクトインスタンスがすべてリリースまたは移行されているか確認してください。

ルートテーブルの管理

ルートテーブルの管理

概要

VPC の中枢的な存在である VRouter は、VPC 内のすべての VSwitch を接続します。VPC と他のネットワークを接続するためのゲートウェイデバイスでもあります。各 VRouter は、特定のルートエントリ設定に基づいてネットワークトラフィックを転送するルートテーブルを保持します。

> **注意**: VRouter またはそのルートテーブルを作成または削除することはできません。VRouter とルートテーブルは、VPC を作成すると自動的に作成され、VPC を削除すると自動的に削除されます。

ルートエントリには、システムルートエントリおよびカスタマイズルートエントリが含まれます。

システムルートエントリ

システムルートエントリを変更または削除することはできません。また、システムルートエントリは、次の 2 種類に分類されます。

- 1つ目は VPC の作成時に作成されるルートエントリで、相互通信のため、VPC 内でクラウドプロダクトインスタンスを有効にします。ルートエントリの宛先 CIDR ブロックは、100.64.0.0/10 です。
- もう 1 つのルートエントリは VSwitch の作成時に作成され、システムルートエントリの宛先 CIDR ブロックは VSwich です。

カスタマイズルートエントリ

カスタマイズルートエントリは、作成または削除できます。各ルートテーブルで作成できるカスタマイズルートエントリは最大 48 個です。

> **注意**: 通常、システムルートエントリは、一般的なニーズを満たします。ただし、特定のケースでは、カスタマイズルートエントリが必要になる場合があります。カスタマイズルートエントリを追加する前に、適切なネットワークデプロイメントを構築することをお勧めします。

VRouter のルートテーブルでは、最長プレフィックスマッチアルゴリズムが適用されます。ルートテーブルの複数のルートエントリが送信先 IP アドレスに一致した場合、VRouter によって、マスクが最長のルートエントリがルーターインターフェイスとして選択されます。

このしくみの例を以下に示します。次のテーブルは、特定の VPC のルートテーブルです。

ターゲットの CIDR	次のホップタイプ	次のホップ ECS インスタンス	タイプ
100.64.0.0/10	-	-	システム
192.168.0.0/24	-	-	システム

0.0.0.0/0	インスタンス	i-12345678	カスタマイズ
10.0.0.0/24	インスタンス	i-87654321	カスタマイズ

上のテーブルでは、宛先が 100.64.0.0/10 および 192.168.0.0/24 のルートエントリは、システムルートエントリです。100.64.0.0/10 はシステムに予約された CIDR ブロックで、192.168.0.0/24 は VPC で VSwitch をターゲットとする CIDR ブロックです。

宛先が 0.0.0.0/0 および 10.0.0.0/24 のルートエントリは、カスタマイズルートエントリです。宛先が 0.0.0.0/0 のトラフィックは、ID が i-12345678 の ECS インスタンスに転送されます。宛先が 10.0.0.0/24 のトラフィックは、ID が i-87654321 の ECS インスタンスに転送されます。

最長プレフィックスマッチアルゴリズムに従って、この VPC では、宛先が 10.0.0.1/0 のトラフィックは ID が i-87654321 の ECS インスタンスに転送され、宛先が 10.0.1.1/24 のトラフィックは ID が i-12345678 の ECS インスタンスに転送されます。

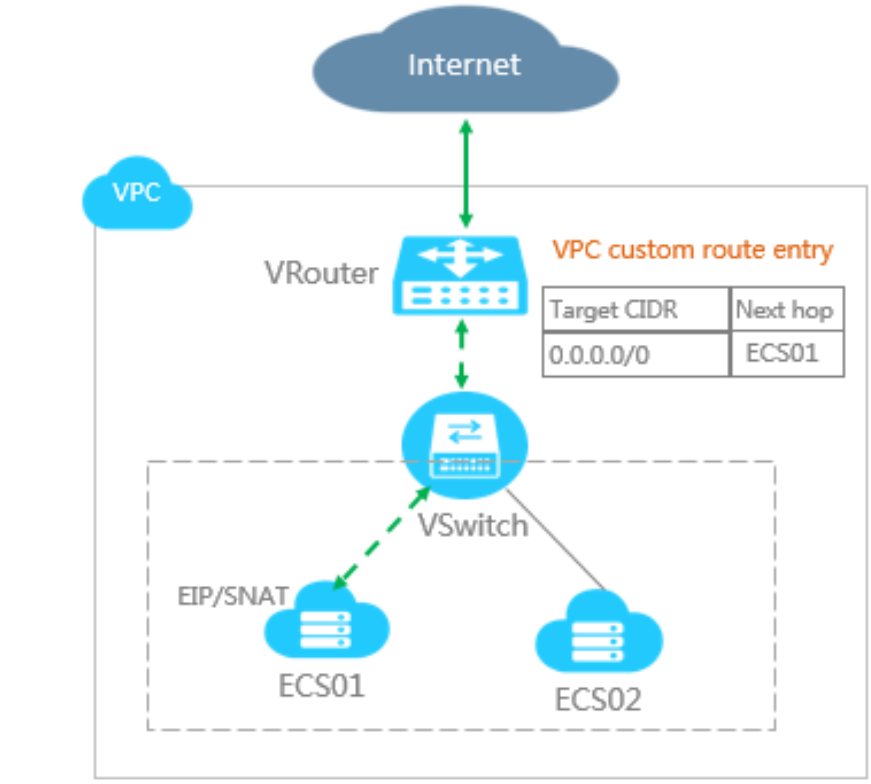
カスタマイズルートエントリの計画

カスタマイズルートエントリが必要なシナリオは、次のとおりです。

VPC 国内ルーティング

VPC に 2 つの ECS インスタンス (ECS01、ECS02) があることを想定しています。

ECS01 は EIP (Elastic IP) にバインドされ、これにより、ECS01 はインターネットにアクセスできるようになります。ECS02 も、リクエストを ECS01 に転送することにより、インターネットにアクセスすることができます。カスタマイズルートエントリを追加して、ECS02 がインターネットにアクセスしたときのルーターインターフェイスとして ECS01 を定義します。

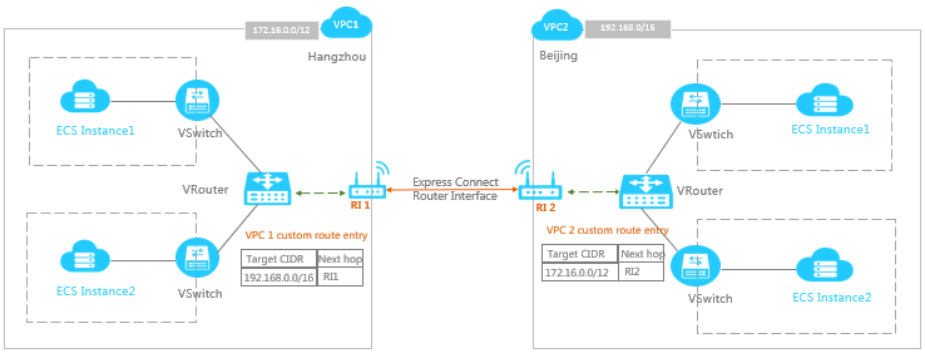


ターゲットの CIDR	次のホップタイプ	次のホップ ECS インスタンス
0.0.0.0/0	ECS インスタンス	ECS01

VPC 相互接続

次の 2 つの VPC があると仮定します: CIDR が 172.16.0.0/12 の VPC1、CIDR が 192.168.0.0/12 の VPC2。

ExpressConnect を使用して VPC1 と VPC2 を接続する必要があり、各 VPC にルーターインターフェイスを作成しているものとします。VPC に接続するには、VPC1 と VPC2 用に次のルートエントリを追加する必要があります。



- VPC1 のルートエントリ

ターゲットの CIDR	次のホップタイプ	ルーターインターフェイス
172.16.0.0/12	ルートインターフェイス (一般的なルーティング)	RI2

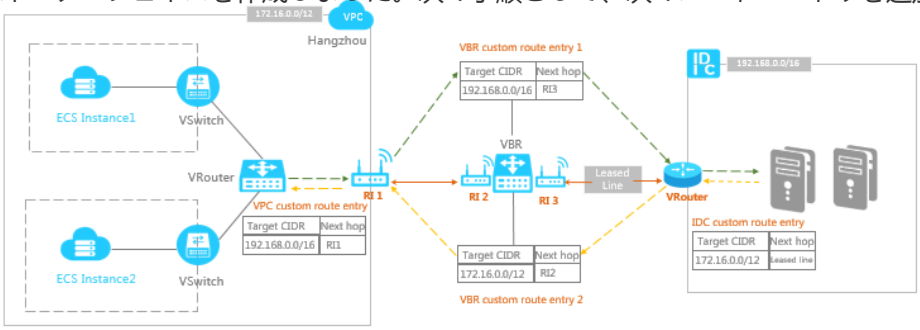
- VPC2 のルートエントリ

ターゲットの CIDR	次のホップタイプ	ルーターインターフェイス
172.16.0.0/12	ルートインターフェイス (一般的なルーティング)	RI4

ハイブリッドクラウドの実現

CIDR ブロックが 172.16.0.0/12 の VPC があり、ネットワークセグメントが 192.168.0.0/12 の IDC があると仮定します。

ExpressConnect を使用して、VPC および IDC に接続する必要があるとします。アクセスラインと仮想ボーダールーター (VBR) の準備はできています。VPC および VBR に接続するためのルーターインターフェイスを作成しました。次の手順として、次のルートエントリを追加します。



- VPC のルートエントリ

ターゲットの CIDR	次のホップタイプ	ルーターインターフェイス
192.168.0.0/12	ルートインターフェイス (一般的なルーティング)	RI1

- VBR のルートエントリ

ターゲットの CIDR	次のホップタイプ	ルーターインターフェイス
192.168.0.0/12	アクセスライン方向	RI3

172.16.0.0/12	VPC 方向	RI2

- IDC のルートエントリ

ターゲットの CIDR	次のホップタイプ	ルーターインターフェイス
172.16.0.0/12	—	RI4

カスタマイズルートエントリの追加

1. **VPC コンソール**にログオンします。
2. 左側のナビゲーションバーで [**VPC**] を選択します。
3. VPC を作成するリージョンを選択します。
4. VPC リストページで、VPC の ID をクリックします。VPC の詳細ページが表示されます。
5. 左側のナビゲーションバーで、**[VRouter] の [ルートエントリの追加]** を選択します。

ポップアップボックスで、次の情報を指定します。

設定	説明
ターゲット CIDR ブロック	IP アドレスまたは CIDR ブロックを入力します。 IP アドレスを入力した場合、システムはデフォルトで 32 ビットのサブネットマスクを使用します。
次のホップタイプ	次のホップタイプを選択します。 - ECS インスタンス: リクエストをターゲット CIDR ブロックから ECS インスタンスに転送します。 - ルーターインターフェイス: リクエストをターゲット CIDR ブロックから指定されたルーターインターフェイスに転送します。ルーターインターフェイスにより、リクエストがその接続先のルーターインターフェイスに転送されます。
ルーターインターフェイス	ルーターインターフェイスが、選択した次のホップタイプに基づいて、システムによってフィルター処理されます。 **注意:** ECMP を選択した場合、ルーターインターフェイスとして 2 ~ 4 個のインスタンスを選択する必要があり、ルーターインターフェイスの接続先ルートのタイプは仮想

	ボーダールーターである必要があります。
VPNゲートウェイ	宛先CIDR宛てのトラフィックを指定されたVPNゲートウェイにルーティングします。

7. [OK] をクリックします。

セキュリティグループを使用してECSインスタンスを制御し、VPCのパブリッククラウドにアクセスする

セキュリティグループは、ECS発信および着信トラフィックを制御するために使用される仮想ファイアウォールです。同じVPC内では、同じセキュリティグループ内のECSインスタンスがイントラネット上で互いに通信できます。詳細については、セキュリティを参照してください。

システムによって自動的に作成されたセキュリティグループ

VPCタイプのECSインスタンスを作成する場合は、システムが提供するデフォルトのセキュリティグループルールを使用するか、VPCですでに使用可能な他のセキュリティグループを選択できます。

セキュリティグループ	プロトコル	ポート範囲	説明
デフォルトのセキュリティグループ	ICMP	22および3389	ポート22は、Linux SSHログオン用です。ポート3389は、Windowsリモートデスクトップ用です。 HTTPポート80とHTTPSポート443からのインバウンドアクセスを許可することもできます。

ユースケース

ケース1：インターネットでサービスを提供する

VPCのECSインスタンスにWebサイトを設定する場合は、EIPまたはNATゲートウェイを使用してパブリックネットワークにアクセスして、HTTPまたはHTTPSサービスを提供できます。展開されたサービスに基づいて

、次の表に示すセキュリティグループルールを追加できます。

セキュリティグループのルール	ルールの方向	承認ポリシー	プロトコルタイプ	ポート範囲	承認タイプ	権限オブジェクト	優先
HTTPポート8080からの着信アクセスを許可する	インバウンド	許可する	TCP	8080/8080	アドレスセグメントアクセス	0.0.0.0/0	1
HTTPポート80からの受信アクセスを許可する	インバウンド	許可する	HTTP	80/80	アドレスセグメントアクセス	0.0.0.0/0	1
HTTPSポート433からの受信アクセスを許可する	インバウンド	許可する	TCP	443/443	アドレスセグメントアクセス	0.0.0.0/0	1

ケース2：VPCのECSインスタンスへのリモートアクセスを許可する

VPC内のNATゲートウェイやEIP for ECSインスタンスなどのパブリックIPを構成する場合は、Windowsリモートログオンまたは Linux SSHログオン用の次の表に示すセキュリティグループルールを適宜追加できます。

セキュリティグループのルール	ルールの方向	承認ポリシー	プロトコルタイプ	ポート範囲	承認タイプ	権限オブジェクト	優先
Windowsリモートログオンを許可する	インバウンド	許可する	RDP	3389/3389	アドレスセグメントアクセス	任意のパブリックIPからのログオンが許可されている場合は、0.0.0.0/0を入力します	1

						。 特定のIPからのリモートログオンのみが許可されている場合は、特定のIPアドレスを入力します。	
Linux SSHログオンを許可する	インバウンド	許可する	RDP	22/22	アドレスセグメントアクセス	任意のパブリックIPからのログオンが許可されている場合は、0.0.0.0/0を入力します。 特定のIPからのリモートログオンのみが許可されている場合は、特定のIPアドレスを入力します。	1

関連情報

- セキュリティグループルールの追加

VPC にインスタンスの作成

概要

VPC の VSwitch 下に ECS、RDS、SLB のインスタンスを作成できます。

前提条件

VPC と VSwitch を作成しておきます。

操作手順

[VPC コンソール] にログインします。

左側のナビゲーションバーで、**[VPC]** をクリックします。

リージョンを選択し、該当 VPC の ID をクリックし、**[VPC基本情報]** ページに移動します。

左側のメニューで、**[VSwitch]** をクリックし、**[VSwitchリスト]** ページに移動します。

該当 VSwitch の **[インスタンスの作成]** をクリックし、インスタンスタイプを選択します。

購入ページでスペックを選定し、支払い完了後、該当 VSwitch 下にインスタンスが作成されます。VPC作成後、ECS インスタンスのプライベート IP や VSwitch が変更可能になります。

アクセス制御

現在、Alibaba CloudのVirtual Private Cloud（VPC）には、専用のリソースアクセス管理ポリシーはありません。VPCのリソースアクセス管理は、各クラウド製品のアクセス制御機能に依存しています。たとえば、ECSのリソースアクセス管理はセキュリティグループを使用して実装され、SLBおよびRDSのリソースアクセ

ス管理はホワイトリストを使用して実装されます。

ECSセキュリティグループ

セキュリティグループは、ステートフルなパケット検査機能を提供する仮想ファイアウォールです。セキュリティグループは、1つ以上のECSのネットワークアクセス制御を設定するために使用されます。セキュリティ分離の重要な手段であるセキュリティグループは、クラウド上のセキュリティドメインを分割するために使用されます。

VPCタイプのECSインスタンスに対して、システムが提供するデフォルトのセキュリティグループルールを使用できます。既定のセキュリティグループのルールは変更できますが、既定のセキュリティグループは削除できません。

デフォルトのセキュリティグループ1：すべての発信アクセスが許可されます。インバウンドアクセスは、すべてのICMPポートとTCPポート22,3389,80、および443から許可されます。

デフォルト以外のVPCとVSwitchを使用してECSインスタンスを作成する場合は、このデフォルトのセキュリティグループルールを選択できます。

デフォルトセキュリティグループ2：すべての送信アクセスが許可されます。インバウンドアクセスは、すべてのICMPポートとTCPポート22および3389から許可されます。

デフォルトのVPCとVSwitchを使用してECSインスタンスを作成する場合は、このデフォルトのセキュリティグループルールを選択できます。セキュリティグループの詳細設定については、セキュリティグループ参照してください。

RDSホワイトリスト

ApsaraDB for RDSのホワイトリスト機能を使用すると、RDSにアクセスできるIPアドレスをカスタマイズできます。不特定のIPアドレスからのアクセスはすべて拒否されます。VPCでRDS製品を使用する場合は、必須のRDSのホワイトリストにECSのIPアドレスを追加して、ECSがRDSインスタンスにアクセスできるようにします。

ApsaraDB for RDSホワイトリストの詳細設定については、ホワイトリストを設定を参照してください。

SLBホワイトリスト

サーバーロードバランサ（SLB）リスナーは、特定のIPアドレスでのみアクセスできるように構成できます。この構成は、アプリケーションが特定のIPアドレスからのアクセスのみを許可するシナリオに適用されます。

SLBは、転送ポリシーに基づいて複数のバックエンドECSにアクセストラフィックを配信するトラフィック分

散制御サービスです。アクセスは通常インターネットまたはイントラネットユーザーが利用できます。指定したユーザーのみがサービスを利用できる場合、またはイントラネットアクセスのみが利用可能な場合、ホワイトリスト機能はサービス上で効果的なリソースアクセス管理を実行できます。ホワイトリストを設定するには、SLB経由でアクセスするVPC内のユーザのIPアドレスまたはクラウドサービスのIPアドレスを、SLBのアクセス管理ホワイトリストに追加します。

詳しいSLBホワイトリスト設定については、ホワイトリストアクセスコントロールを設定するを参照してください。

VPC のサブネットの分離

VPC内のサブネットを分離する

セキュリティグループを設定することにより、各VSwitchが同じVPC内の他の2つのVSwitchにアクセスするのを防ぐことができます。

前提条件

- 3つのVSwitchは同じVPC内になければなりません。
- 3つのVSwitchesには、CIDRブロック172.16.1.0/16、172.16.2.0/16、および172.16.3.0/16がそれぞれ必要です。
- 3つのVSwitchesは、相互アクセスを可能にするためにデフォルト設定で同じVRouterのもとで作成する必要があります。

手順

Alibaba Cloud ECSコンソールにログオンします。

左側のナビゲーションペインで「**セキュリティグループ**」をクリックします。

つのセキュリティグループをそれぞれ作成します。それぞれを作成する手順は次のとおりです。

リージョンを選択して、**セキュリティグループの作成**をクリックします。

次の情報を入力して、 **[OK]** をクリックします。

セキュリティグループ名：（識別しやすくするためにCIDRブロックを持つグループに名前を付ける）

ネットワークタイプ：VPC

VPC :(セキュリティグループのVPCを選択)

セキュリティグループリストページで、目的のインスタンスに対応する **Action** 列の **Configuration rules** をクリックします。

「セキュリティグループルールの追加」 をクリックして、CIDRブロック0.0.0.0からのアクセスを許可するルールを追加します。

情報を入力して、 **[OK]** をクリックします。

注：優先順位を100に設定してください。値が小さいほど優先度が高くなります。

「セキュリティグループルールの追加」をクリックして、CIDRブロック172.16.2.0/16からのアクセスを禁止するルールを追加します。

前述のセキュリティグループを完了し、**「OK」**をクリックします。

注：このルールの優先度が以前に作成された優先度より高くなるように、優先度を100より小さい値に設定します。

同じ方法を使用して、CIDRブロック172.16.3.0/16からのアクセスを拒否するルールを追加します。

注：このVPCに3つのCIDRブロックしかない場合、上記の設定により、CIDRブロック172.16.2.0/16および172.16.3.0/16は172.16.1.0/16にアクセスできなくなります。

3つのセキュリティグループ間の双方向アクセスを拒否するには、他の2つのVSスイッチに対して同様のルールを設定する必要があります。

VPC からインターネットへの接続

パブリック IP の割り当て

VPC の ECS インスタンスがインターネットにアクセスする必要がある場合は、ECS インスタンスを作成する際にパブリック IP を割り当てることができます。

下の図のように、ECS インスタンスを作成する VPC と VSwitch を選択した後、ネットワーク帯域幅のピークを設定する必要があります。ECS インスタンスの作成後にパブリック IP が割り当てられるように、この値は 0 より大きくする必要があります。

注意:

パブリック IP が割り当てられるのは、指定されたネットワーク帯域幅のピークが 0 より大きい場合のみです。それ以外の場合、パブリック IP は割り当てられません。この場合は、別の方法として、Elastic IP を ECS インスタンスにバインドすることもできます。

システム割り当ての IP を ECS インスタンスからバインド解除することはできません。

ECS インスタンスの作成後、[**インスタンス**] ページでパブリック IP を確認できます。このパブリック IP を使用すると、パブリックネットワーク内で ECS インスタンスにアクセスできます。

EIP のバインド

ECS インスタンスにシステム割り当てのパブリック IP がない場合は、EIP を ECS インスタンスにバインドしてインターネットにアクセスできます。

EIP (Elastic IP) は、個別に購入して所有できるパブリック IP アドレスリソースです。EIP は、ECS インスタンスを再起動することなく、VPC ECS インスタンスに動的にバインドできます。詳細については、「EIP の概要」を参照してください。

手順

[EIP コンソール]にログインします。

[Elastic IPのリクエスト] をクリックします。

購入ページで、EIP を設定してから **[今すぐ購入]** をクリックします。

購入を完了してから EIP コンソールに戻り、ターゲット EIP の横にある **[バインド]**をクリックします。

[バインド] ダイアログで、バインドする ECS インスタンスを選択して **[OK]** をクリックします。

> **注意**: ECS インスタンスのステータスが Running または Stopped であることを確認してください。さらに、ECS インスタンスにパブリック IP がシステムで割り当てられていないか、または ECS インスタンスが他の EIP にバインドされていないか確認してください。

EIP をバインドした後、ECS インスタンスは、この EIP を通じてインターネットにアクセスできます。インターネットにアクセスする必要がない場合はいつでも、EIP をバインド解除してリリースできます。詳細な設定については、「EIP の管理」を参照してください。

インターネットから VPC への接続

パブリック IP の割り当て

VPC 内の ECS インスタンスで外部サービスを提供する必要がある場合は、その ECS インスタンスを作成する際にパブリック IP を割り当てることもできます。

下の図のように、ECS インスタンスを作成する VPC と VSwitch を選択した後、ネットワーク帯域幅のピークを設定する必要があります。ECS インスタンスの作成後にパブリック IP が割り当てられるように、この値は 0 より大きくする必要があります。

注意:

パブリック IP が割り当てられるのは、指定されたネットワーク帯域幅のピークが 0 より大きい場合のみです。それ以外の場合、パブリック IP は割り当てられません。この場合は、別の方法として、Elastic IP を ECS インスタンスにバインドすることもできます。

システム割り当ての IP を ECS インスタンスからバインド解除することはできません。

ECS インスタンスの作成後、[**インスタンス**] ページでパブリック IP を確認できます。このパブリック IP をドメイン名に解決して、外部サービスを提供することもできます。

EIP のバインド

ECS インスタンスにシステム割り当てのパブリック IP がない場合は、EIP を ECS インスタンスにバインドして外部サービスを提供できます。

EIP (Elastic IP) は、個別に購入して所有できるパブリック IP アドレスリソースです。EIP は、ECS インスタンスを再起動することなく、VPC ECS インスタンスに動的にバインドできます。詳細については、「EIP の概要」を参照してください。

手順

[EIP コンソール] にログインします。

[Elastic IPのリクエスト] をクリックします。

購入ページで、EIP を設定してから **[今すぐ購入]** をクリックします。

購入を完了してから EIP コンソールに戻り、ターゲット EIP の横にある **[バインド]** をクリックします。

[バインド] ダイアログで、バインドする ECS インスタンスを選択して **[OK]** をクリックします。

> **注意**: ECS インスタンスのステータスが Running または Stopped であることを確認してください。さらに、ECS インスタンスにパブリック IP がシステムで割り当てられていないか、または ECS インスタンスが他の EIP にバインドされていないか確認してください。

EIP をバインドした後、ECS インスタンスは、この EIP を通じてインターネットにアクセスできます。外部サービスを提供する必要がない場合はいつでも、EIP をバインド解除してリリースできます。詳細な設定については、「EIP の管理」を参照してください。

インターネット接続対応の SLB 作成

Server Load Balancer (SLB) とは、転送ルールとスケジューリングアルゴリズムに基づいてトラフィックを複数のバックエンドサーバーに分散するためのトラフィック分散制御サービスです。詳細は「プロダクトの

概要」を参照してください。

インターネット接続対応の SLB インスタンスを作成し、バックエンドサーバーとして VPC ECS インスタンスを追加して、インターネットからの分散要求を処理することもできます。このようにすると、VPC ECS インスタンスで外部サービスを提供できます。

> このチュートリアルでは、Apache の静的 Web ページがデプロイされている 2 つの ECS インスタンスを使用します。

手順

[Server Load Balancer コンソール]にログオンし、**[サーバーロードバランサの作成]** をクリックして、インターネット接続対応の SLB インスタンスを作成します。

SLB インスタンスには、作成後、パブリック IP アドレスが割り当てられます。この IP アドレスを使用すると、外部サービスを提供できます。

バックエンドサーバーを追加します。

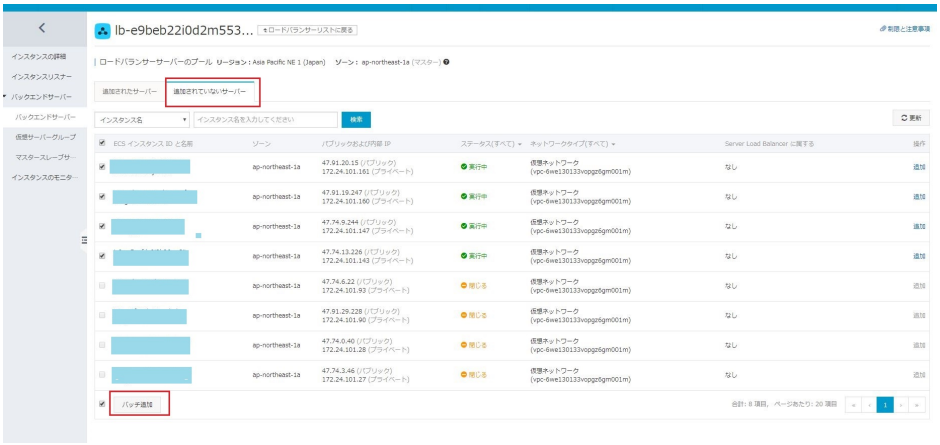
作成された SLB インスタンスの ID をクリックします。

左側の **[インスタンスの詳細]** ペインで、**[サーバー]**、**[バックエンドサーバー]** の順にクリックします。

[追加されていないサーバー] タブをクリックします。

VPC ECS インスタンスの横にあるチェックボックスをオンにし、**[バッチ追加]** をクリ

ックします。表示されたダイアログボックスで、重みを 100 に設定し、**[確認]** をクリックして追加します。



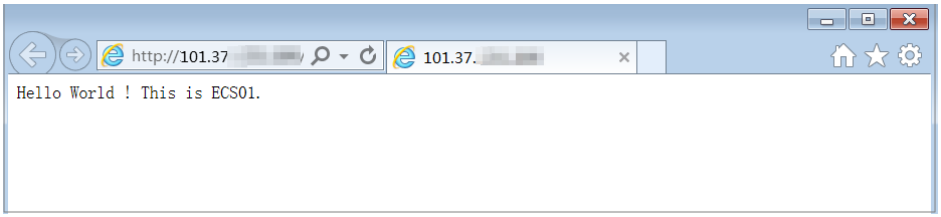
リスナーを追加します。

左側のナビゲーションペインで **[インスタンスリスナー]** をクリックし、**[リスナーの作成]** をクリックします。

リスナーの追加ダイアログで、次の図を参照してTCPリスナーを構成します。

[次のステップ] をクリックしてヘルスチェックを設定し、他の設定は変更せずに **[TCP]** を選択します。**[確認]** を 2 回クリックして設定を完了します。

Server Load Balancer リストのページに戻り、ページを更新してインスタンスのステータスを確認します。インスタンスが実行中でありヘルスチェックが正常であれば、SLB インスタンスのパブリック IP アドレスを使用して外部サービスを提供できます。



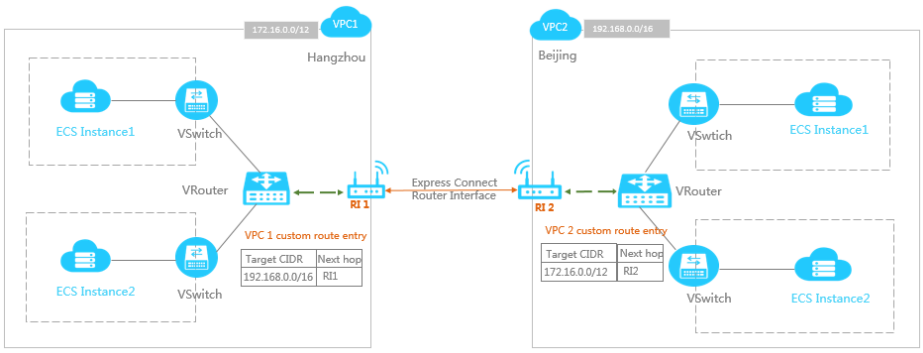
VPC間の接続

ExpressConnect

ExpressConnect では、どのリージョン内にも 2 つの VPC 間の専用プライベート接続を確立できます。接続はインターネット経由で行われません。このため、ExpressConnect は高速で安定した、セキュアな専用ネットワーク通信を提供できます。

次の図に示すように、CIDR ブロック 172.16.0.0/16 を持つ VPC1、CIDR ブロック 192.168.0.0/16 を持つ VPC2 の 2 つの VPC があるものとします。

VPC1 と VPC2 間の接続を確立するには、ExpressConnect のルーターインターフェイス機能を使用する必要があります。最初に、ルーターインターフェイスを作成し、VPC1 を接続元として、VPC2 を接続先として設定する必要があります。その後、2 つのカスタマイズルートエントリを追加する必要があります。



- VPC1 に追加されたカスタマイズルートエントリ

宛先 CIDR	ネクストホップのタイプ	ネクストホップ
192.168.0.0/16	ルートインターフェイス	RI1

- VPC2 に追加されたカスタマイズルートエントリ

宛先 CIDR	ネクストホップのタイプ	ネクストホップ
172.16.0.0/12	ルートインターフェイス	RI2

詳細については、以下を参照してください。

同じアカウントに属する VPC 間の接続

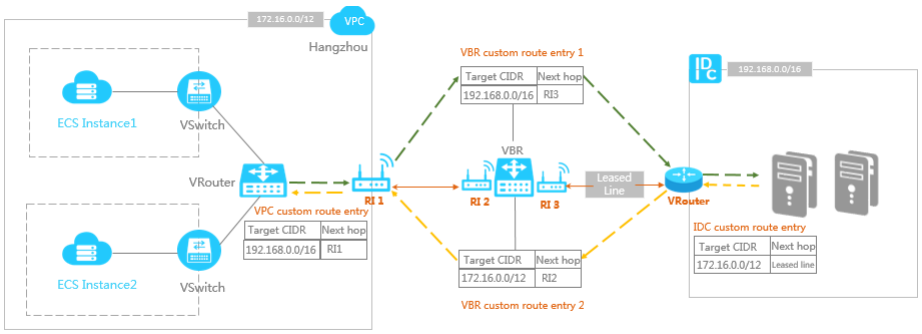
異なるアカウントに属する VPC 間の接続

VPCとIDCの接続

アクセスライン

ExpressConnect の物理接続機能を使用して、VPC とオンプレミスの IDC 間の接続を確立することができます。

たとえば、CIDR ブロックが 172.16.0.0/12 である VPC があり、CIDR ブロックが 192.168.0.0/16 であるオンプレミスのデータセンターがあるとします。クラウドサービスがオンプレミスのデータセンターにアクセスする必要がある場合、アクセスラインを申請してそれらの接続を行うことができます。



手順

アクセスラインの申請

アクセスラインは、IDC を Alibaba Cloud のアクセスポイントと接続する際に使用します。

仮想ボーダールーターの作成

仮想ボーダールーター (VBR) は、データを VPC から IDC に転送するブリッジの役割を果たします。

VBR を作成すると、システムによって自動的にアクセスラインを介してルーターインターフェイス (図では RI3) と IDC 間で接続が確立されます。

ルーターインターフェイスの作成

ルーターインターフェイスを作成し、VPC と VBR を接続します。ルーターインターフェイスを作成するときに、VBR のルーターインターフェイスをローカル側に設定し、VPC を接続先側に設定します。

ルーターインターフェイスを作成すると、システムによって自動的に 2 つのルーターインターフェイス (図では RI2 および RI3) を介して VPC と VBR 間で接続が確立されます。

ルートエントリの追加

最後に、ルートエントリを追加して、VPC と IDC 間のネットワークトラフィックをルーティングする必要があります。

VPC に追加されたカスタマイズルートエントリ

宛先 CIDR ブロック	ネクストホップのタイプ	ネクストホップ
192.168.0.0/16	ルーターインターフェイス	RI1

VBR に追加されたカスタマイズルートエントリ

宛先 CIDR ブロック	ネクストホップのタイプ	ネクストホップ
192.168.0.0/16	アクセスライン	RI3
172.16.0.0/12	VPC	RI2

IDC でのルート

IDC ルーターのアクセスラインまでのルートを追加します。

詳細については、「アクセスライン」を参照してください。