

Alibaba Cloud Express Connect

クイックスタート (新コンソール)

Document Version20190605

目次

1 VPC の接続.....	1
2 同じアカウントによる 2 つの VPC の相互接続.....	3
3 異なるアカウントでの 2 つの VPC の相互接続.....	7
4 物理接続を介したオンプレミス IDC からの VPC への接続.....	14

1 VPC の接続

CEN と Express Connect を使用して異なる VPC を接続できます。

概要

さまざまなアプリケーションシナリオの多様な需要を満たすために、Alibaba Cloud は VPC を接続するためのいくつかの製品を提供しています。VPC を接続するには、CEN または Express Connect を使用できます。構成が簡単で、ルートを自動的に配布して学習できるため、CEN を使用することをお勧めします。

- ・ [CEN](#)

クラウドエンタープライズネットワーク (CEN) を使用して、複数の VPC 間または VPC とローカルデータセンター間のイントラネット接続を構築できます。CEN は自動ルート配布および自動学習を提供します。これにより、迅速なネットワークコンバージェンスが保証され、ネットワーク間通信の品質とセキュリティが向上します。

- ・ [Express Connect](#)

Express Connect を使用して、2 つの VPC の間でイントラネット通信を確立できます。

シナリオ

シナリオ	プロダクト	方法
同じリージョンの同じアカウントで VPC を接続する	CEN	同じリージョンの同じアカウントで VPC を接続する
	Express Connect	同じアカウントによる 2 つの VPC の相互接続
同じリージョンの異なるアカウントで VPC を接続する	CEN	同じリージョンの異なるアカウントで VPC を接続する
	Express Connect	異なるアカウントに属する VPC 間のイントラネット接続
同じアカウントで異なるリージョンの VPC を接続する	CEN	同じアカウントで異なるリージョンの VPC を接続する
	Express Connect	同じアカウントによる 2 つの VPC の相互接続
異なるリージョン、異なるアカウントで VPC を接続する	CEN	異なるリージョン、異なるアカウントで VPC を接続する

シナリオ	プロダクト	方法
	Express Connect	異なるアカウントに属する VPC 間のイントラネット接続

2 同じアカウントによる 2 つの VPC の相互接続

このチュートリアルでは、Express Connect を使用して、同じアカウントに属する 2 つの VPC を接続する方法について説明します。

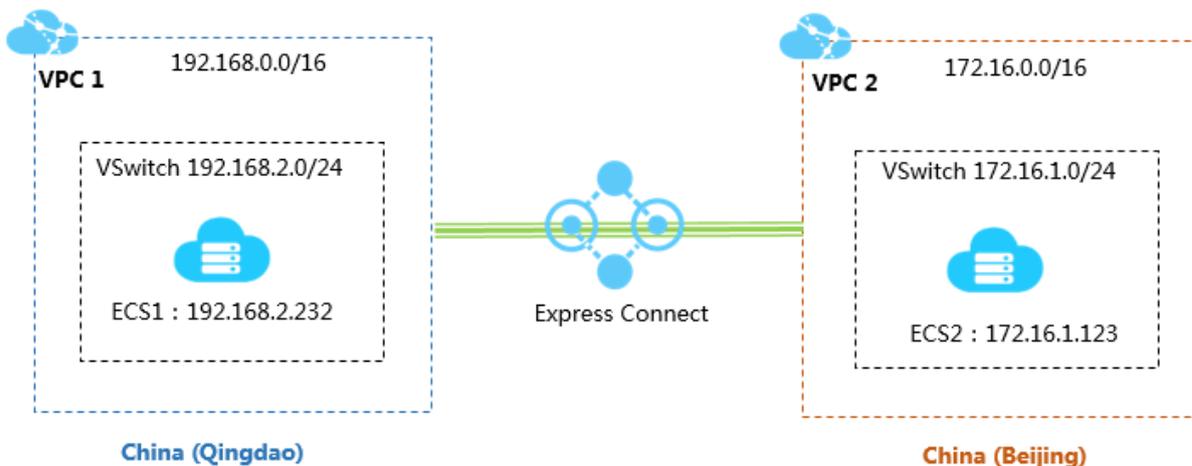


注：

Express Connect を使用して、2 つの VPC を初めて相互接続する場合は、CEN (Cloud Enterprise Network) を使用することを推奨します。詳細は、「[チュートリアルの概要](#)」をご参照ください。

例

このチュートリアルでは、次の 2 つの VPC を例として、Express Connect を使用して VPC 相互接続を実現する方法を示します。



前提条件

相互接続する VPC または VSwitch の Classless Inter-Domain Routing (CIDR) ブロックが競合していないことを確認します。

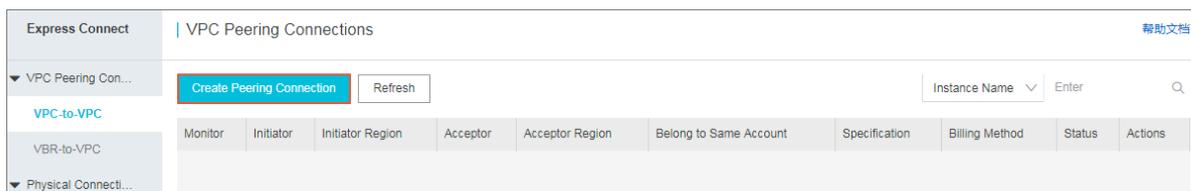
手順 1: ピアリング接続の作成

ピアリング接続を作成するには、次の手順を実行します。

1. [Express Connect コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、[VPC ピアリング接続] > [VPC-VPC] をクリックします。
3. リージョンを選択します。

この例では、[中国 (青島)] を選択します。

4. [ピアリング接続の作成] をクリックします。



5. ピアリング接続を設定します。

この例では、以下の設定を使用します。

- ・ 接続タイプ: [VPC-VPC] をクリックします。
- ・ 作成するルーター: [開始側と受信側] をクリックします。

システムは、ローカル VPC を開始側、ピア VPC を受信側として設定し、開始側を受信側に自動的に接続します。

- ・ ローカルリージョン: ローカル VPC のリージョンを選択します。このチュートリアルでは、[中国 (青島)] を選択します。
- ・ ローカル VPC ID: 接続の開始側となるローカル VPC を選択します。この例では、[VPC1] を選択します。
- ・ ピアリージョン: ピア VPC のリージョンを選択します。このチュートリアルでは、[中国 (北京)] を選択します。
- ・ ピア VPC ID: 接続するピア VPC を選択します。この例では、[VPC2] を選択します。
- ・ 仕様: 相互接続の帯域幅を選択します。この例では、[2 Mb] をクリックします。

6. [今すぐ購入] をクリックして、支払い手続きを完了します。

7. VPC ピアリング接続ページに戻り、作成されたピアリング接続を確認します。

開始側と受信側の両方が有効化状態になっていれば、接続は正常に確立されています。



手順 2: ルートの設定

ピアリング接続を確立したら、相互接続された各 VPC のルートを追加します。

ルートを設定するには、次の手順を実行します。

1. VPC ピアリング接続ページで、作成したピアリング接続を見つけます。

2. 開始側インスタンスの下にある [ルート設定] をクリックします。



3. [ルートエントリの追加] をクリックし、接続する VPC または VSwitch の宛先 CIDR ブロックを入力して、[確認] をクリックします。

この例では、ピア VPC の CIDR ブロック 172.16.0.0/16 を入力します。

4. 受信側インスタンスの下にある [ルート設定] をクリックします。



5. [ルートエントリの追加] をクリックし、接続する VPC または VSwitch の宛先 CIDR ブロックを入力して、[確認] をクリックします。

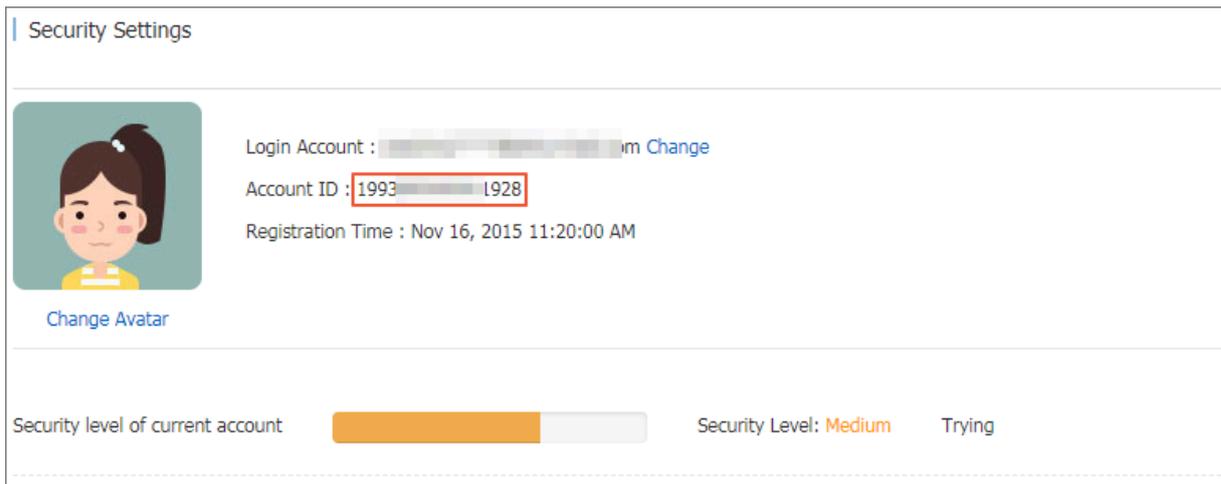
手順 3: セキュリティグループの設定

2 つの VPC 間でピアリング接続を確立したら、これら 2 つの VPC で ECS インスタンスの相互通信を有効にするようにセキュリティグループを設定する必要があります。

このチュートリアルでは、次の表の ECS インスタンスとセキュリティグループを例として使用します。

設定項目	アカウント A	アカウント A
アカウント ID	AccountID_A	AccountID_A
ECS インスタンス ID	InstanceID_A	InstanceID_B
セキュリティグループ ID	SecurityGroupID_A	SecurityGroupID_B

アカウントセンターでアカウント ID を表示できます。



セキュリティグループルールを設定するには、次の手順を実行します。

1. [ECS コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、[ネットワークとセキュリティ] > [セキュリティグループ] 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ます。
4. 対象のセキュリティグループを見つけて、[ルール設定] をクリックします。
5. [セキュリティグループルール] ページで、[セキュリティグループルールの追加] をクリックします。
6. セキュリティグループルールを設定し、プロトコルタイプを選択して、ポート範囲を入力します。



リージョン間 VPC 相互接続の場合は、CIDR ブロック認証タイプを選択し、ピア VPC の CIDR ブロックを入力します。

セキュリティグループ認証タイプを選択する場合は、VPC が同じリージョンにあることを確認してください。

このチュートリアルでは、認証タイプとして CIDR ブロックを選択します。

手順 4: 接続のテスト

ピアリング接続を確立してルートを追加した後、どちらかの VPC 内の ECS インスタンスにログインし、もう一方の ECS インスタンスの IP アドレスに ping を実行します。ping が成功すれば、2 つの VPC 間の接続は成功しています。

3 異なるアカウントでの 2 つの VPC の相互接続

このチュートリアルでは、Express Connect を使用して、異なるアカウントに属する 2 つの VPC を接続する方法について説明します。

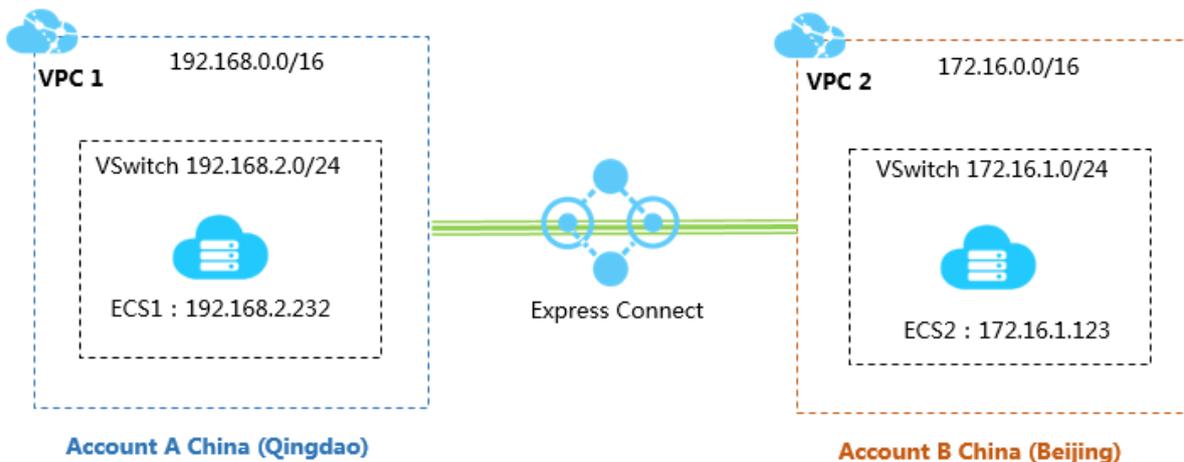


注：

2 つの VPC を相互接続するために Express Connect を初めて使用する場合は、CEN を使用することを推奨します。詳細は、[チュートリアルの概要](#)をご参照ください。

例

アカウント間 VPC 相互接続では、開始側と受信側を別々に作成し、ピアリング接続を確立してからルートを設定する必要があります。このチュートリアルでは、例として次の 2 つの VPC を使用します。アカウント A の VPC1 が開始側として機能し、アカウント B の VPC2 が受信側として機能します。



前提条件

- ・ ピア VPC の Alibaba Cloud アカウント ID と、VPC の VRouter ID を取得済み。
- ・ 相互接続する VPC または VSwitch の Classless Inter-Domain Routing (CIDR) ブロックは競合しません。

ステップ 1. 開始側の作成

開始側を作成するには、次の手順を実行します。

1. アカウント A の資格情報を使用して、[Express Connect コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、VPC ピアリング接続 > VPC-VPC をクリックします。
3. [ピアリング接続の作成] をクリックします。

4. ピアリング接続を設定します。

次の設定を使用します。

- ・ アカウント: [ピアと異なる] をクリックします。
- ・ 接続タイプ: [VPC-VPC] をクリックします。
- ・ ルーターの作成: [開始側の作成] をクリックします。

開始側だけが受信側への接続を開始できます。

- ・ ローカルリージョン: VPC のリージョンをクリックします。このチュートリアルでは、[中国 (青島)] をクリックします。
- ・ ローカル VPC ID: 開始側インスタンスが作成される VPC をクリックします。この例では、[VPC1] をクリックします。
- ・ ピアリージョン: 接続する VPC が配置されているリージョンをクリックします。このチュートリアルでは、[中国 (北京)] をクリックします。
- ・ 仕様: 相互接続の帯域幅をクリックします。この例では、[2 Mb] をクリックします。

5. [今すぐ購入] をクリックして、支払いを済ませます。

6. [VPC ピアリング接続] ページに戻り、作成された開始側インスタンスを確認します。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vpc-m5e2htpw081sb44sznt rk-m5e4t8fyehjysvgecmku	China North 1 (Qingdao)	Add Acceptor	China North 2 (Beijing)	No	Small 1	Pay-As-You-Go Created at Oct 11, 2018, 20:18:26	● Initiator: Disconnected ● Acceptor: Disconnected	⋮

ステップ 2. 受信側の作成

受信側を作成するには、以下の手順を実行します。

1. アカウント B の資格情報を使用して、[Express Connect コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、VPC ピアリング接続 > VPC-VPC をクリックします。
3. [ピアリング接続の作成] をクリックします。

4. ピアリング接続を設定します。

次の設定を使用します。

- ・ アカウント: [ピアと異なる] をクリックします。
- ・ 接続タイプ: [VPC-VPC] をクリックします。
- ・ 作成するルーター: [受信側のみ] をクリックします。
- ・ ローカルリージョン: VPC のリージョンをクリックします。このチュートリアルでは、[中国 (北京)] をクリックします。
- ・ ローカル VPC ID: 受信側インスタンスが作成される VPC をクリックします。この例では、[VPC2] をクリックします。
- ・ ピアリージョン: 接続する VPC が配置されているリージョンをクリックします。このチュートリアルでは、[中国 (青島)] をクリックします。
- ・ 仕様: 受信側の帯域幅は開始側の帯域幅に依存します。この例では、[デフォルト] をクリックします。

5. [今すぐ購入] をクリックして、支払いを済ませます。

6. [VPC ピアリング接続] ページで、作成した受信側インスタンスを確認し、その ID をメモします。この例では、受信側インスタンス ID は ri-2zeix2q86uoyisagyz0pn です。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	Add Initiator	China North 1 (Qingdao)	vpc-2zesx2q ri-2zewk0o0mew7aroqj55thw Route Settings	China North 2 (Beijing)	No	Default	-	● Initiator: Disconnected ● Acceptor: Disconnected	

ステップ 3. 開始側の追加

開始側と受信側を作成した後、受信側に開始側を追加する必要があります。

受信側に開始側を追加するには、以下の手順を実行します。

1. アカウント B の資格情報を使用して、[Express Connect コンソール](#) にログインします。
2. 左側のナビゲーションウィンドウで、VPC ピアリング接続 > VPC-VPC をクリックします。
3. 受信側のリージョンをクリックします。

このチュートリアルでは、[中国 (北京)] をクリックします。

4. 作成した受信側インスタンスを見つけて、[開始側の追加] をクリックします。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	Add Initiator	China North 1 (Qingdao)	vpc-2zesx2q63b0mrf641yk3z ri-2zewk0o0mew7aroqj55thw Route Settings	China North 2 (Beijing)	No	Default	-	● Initiator: Disconnected ● Acceptor: Disconnected	

5. [インスタンスの追加] ページで [その他のアカウント] をクリックして、開始側のルーターインターフェイスを入力します。この例では、ri-m5e33r3n78zyi5573kf85 と入力します。[OK] をクリックします。

ステップ 4. 受信側の追加と、ピアリング接続の確立

開始側と受信側を追加した後、開始側は受信側に接続を開始して、2つのVPC間のピアリング接続を確立できます。

この例では、接続する開始側はアカウントAのVPC1です。ピアリング接続を確立するには、次の手順を実行します。

1. アカウント A の資格情報を使用して、[Express Connect コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、VPCピアリング接続 > VPC-VPC をクリックします。
3. 開始側インスタンスのリージョンをクリックします。

このチュートリアルでは、[中国 (青島)] をクリックします。

4. [受信側の追加] をクリックします。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vpc-m5e2htpw031sb84esznt ri-m5e4rttyehjyvgcemku	China North 1 (Qingdao)	Add Acceptor	China North 2 (Beijing)	No	Small.1	Pay-As-You-Go Created at Oct 11, 2018, 20:18:26	Initiator: Disconnected Acceptor: Disconnected	

5. [インスタンスの追加] ページで [その他のアカウント] をクリックして、受信側のルーターインターフェイスを入力します。この例では、ri-2zeix2q86uoyisagyz0pn と入力します。[OK] をクリックします。
6.  > 接続の開始をクリックします。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vpc-m5e2htpw031sb84esznt ri-m5e4rttyehjyvgcemku	China North 1 (Qingdao)	vpc-2zesx2q63b0mrf641yk3z ri-2zewk0o8mew7srq858tw Add Acceptor	China North 2 (Beijing)	Yes	Small.1	Pay-As-You-Go Created at Oct 11, 2018, 20:18:26	Initiator: Disconnected Acceptor: Disconnected	Initiate Connection Upgrade/Downgrade Switch to Subscription Delete
	vpc-m5e2htpw031sb84esznt ri-m5e33r3n78zyi5573kf85	China North 1 (Qingdao)	vpc-2zeimshn7190nmfwcuo5 ri-2zeix2q86uoyisagyz0pn	China North 2 (Beijing)	No	Mini.2	Subscription Expires at Oct 28, 2018, 00:00:00 Connected at Sep 28, 2018, 16:14:00	Initiator: Activated Acceptor: Activated	

接続が確立されると、開始側と受信側はアクティブ状態になります。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vpc-m5e2htpw031sb84esznt ri-m5e33r3n78zyi5573kf85	China North 1 (Qingdao)	vpc-2zeimshn7190nmfwcuo5 ri-2zeix2q86uoyisagyz0pn	China North 2 (Beijing)	No	Mini.2	Subscription Expires at Oct 28, 2018, 00:00:00 Connected at Sep 28, 2018, 16:14:00	Initiator: Activated Acceptor: Activated	

ステップ 5. ルートの設定

ピアリング接続を確立したら、2 つの VPC それぞれにルートを追加する必要があります。

ルートを設定するには、次の手順を実行します。

1. アカウント A の資格情報を使用して、[Express Connect コンソール](#)にログインします。
2. [VPC ピアリング接続] ページで、作成したピアリング接続を見つけます。
3. 開始側インスタンスを見つけ、[ルート設定] をクリックします。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vpc-m5e2hltwd81sb04esznf r-n5er4trtyehysvgecmku	China North 1 (Qingdao)	vpc-2zeexzq63b0mrf641yk3z r-2zew0do3mew7srq858fw Route Settings	China North 2 (Beijing)	Yes	Small.1	Pay-As-You-Go Created at Oct 11, 2018, 20:18:26 Connected at Oct 11, 2018, 20:26:46	<ul style="list-style-type: none"> Initiator: Activated Acceptor: Activated 	

4. [ルートエントリの追加] をクリックし、接続する VPC または VSwitch の CIDR ブロックを入力して、[確認] をクリックします。

この例では、ピア VPC の CIDR ブロック 172.16.0.0/16 を入力します。

5. アカウント B の資格情報を使用して、[Express Connect コンソール](#)にログインします。
6. 受信側インスタンスを見つけ、[ルート設定] をクリックします。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vpc-m5e2hltwd81sb04esznf r-n5er4trtyehysvgecmku	China North 1 (Qingdao)	vpc-2zeexzq63b0mrf641yk3z r-2zew0do3mew7srq858fw Route Settings	China North 2 (Beijing)	Yes	Small.1	Pay-As-You-Go Created at Oct 11, 2018, 20:18:26 Connected at Oct 11, 2018, 20:26:46	<ul style="list-style-type: none"> Initiator: Activated Acceptor: Activated 	

7. [ルートエントリの追加] をクリックし、接続する VPC または VSwitch の CIDR ブロックを入力して、[確認] をクリックします。

この例では、ピア VPC の CIDR ブロック 192.168.0.0/16 を入力します。

ステップ 6. セキュリティグループの設定

2 つの VPC 間でピアリング接続を確立したら、これら 2 つの VPC で ECS インスタンスの相互通信を有効にするように、セキュリティグループを設定する必要があります。

このチュートリアルでは、次の表の ECS インスタンスとセキュリティグループ設定を例として使用します。

設定項目	アカウント A	アカウント B
アカウント ID	AccountID_A	AccountID_B
ECS インスタンス ID	InstanceID_A	InstanceID_B
セキュリティグループ ID	SecurityGroupID_A	SecurityGroupID_B

[アカウントセンター](#)でアカウント ID を確認できます。

Security Settings



Login Account : ██████████ @ ██████████.com [Change](#)

Account ID : 1993 ██████████ 1928

Registration Time : Nov 16, 2015 11:20:00 AM

[Change Avatar](#)

Security level of current account Security Level: Medium Trying

セキュリティグループルールを設定するには、次の手順を実行します。

1. [ECS コンソール](#)にログインします。
2. 左側のナビゲーションウィンドウで、ネットワークとセキュリティ > セキュリティグループをクリックします。
3. インスタンスのリージョンをクリックします。
4. 対象のセキュリティグループを見つけて、[ルール追加] をクリックします。
5. [セキュリティグループルール] ページで、[セキュリティグループルールを追加] をクリックします。
6. セキュリティグループルールを設定し、プロトコルタイプを選択して、ポート範囲を入力します。次に、以下の情報に従って権限付与タイプをクリックします。

シナリオ	権限付与タイプ	説明
リージョン間 VPC 相互接続	CIDR ブロック	ピア VPC の CIDR ブロック
同一リージョン間 VPC 相互接続	セキュリティグループ	ピア ECS インスタンスに関連付けられているセキュリティグループの ID <div style="background-color: #f2f2f2; padding: 5px; border: 1px solid #ccc;">  注： 相互接続する VPC が異なるアカウントに属している場合は、[その他のアカウントを許可する] をクリックし、[アカウント ID] フィールドにピアアカウント ID を入力します。 </div>



:

- ・ 相互接続する VPC が異なるリージョンにある場合は、CIDR ブロック権限付与タイプをクリックして、ピア VPC の CIDR ブロックを入力します。このチュートリアルでは、権限付与タイプとして CIDR ブロックをクリックします。
- ・ 相互接続する VPC が同じリージョンにある場合は、セキュリティグループの権限付与の種類を選びます。アカウント間相互接続で、[その他のアカウントを許可する] をクリックし、[アカウント ID] フィールドにピアアカウント ID を入力します。

ステップ 7. 接続のテスト

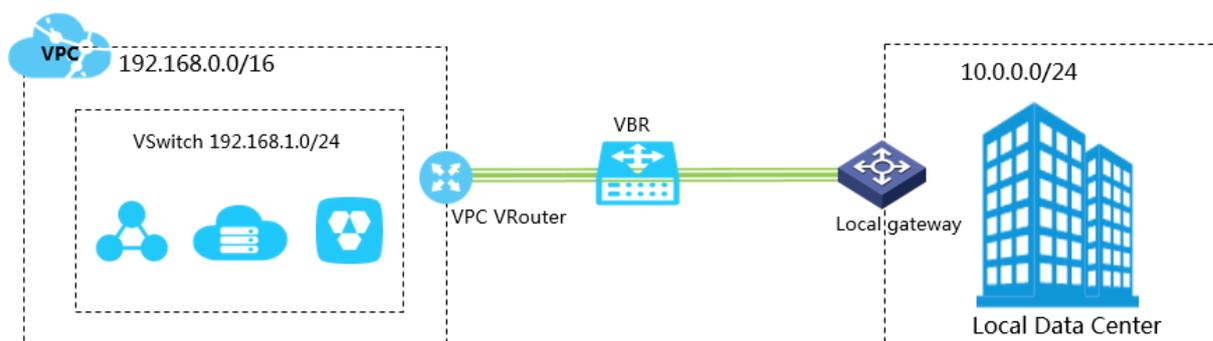
ピアリング接続を確立し、ルートを追加した後、どちらかの VPC 内の ECS インスタンスにログインし、もう一方の VPC 内の ECS インスタンスの IP アドレスに ping を実行します。ping が成功すると、2 つの VPC 間の接続は成功します。

4 物理接続を介したオンプレミス IDC からの VPC への接続

本ドキュメントでは、Express Connect を使用してオンプレミス IDC と Alibaba Cloud VPC の間の相互通信を実装する方法について説明します。

例

本ドキュメントでは、次の図に示す VPC とオンプレミス IDC の構成を使用します。



ステップ 1：物理接続インターフェイスを申請する

1. [Express Connect コンソール](#) にログインします。
2. 左側のナビゲーションペインで、物理接続 > 物理接続インターフェイス をクリックします。
3. 新しいインターフェイスの申請をクリックします。

4. 以下の構成項目を設定して、インターフェースを構成します。

- ・ リージョン：専用回線をデプロイするリージョンを選択します。この例では、中国北部 3（張家口）を選択します。
- ・ SP：専用回線のサービスプロバイダーを選択します。この例では、China Unicom を選択します。
- ・ アクセスポイント：オンプレミス IDC に最寄りのアクセスポイントを選択します。この例では、Zhangjiakou-Xiaoertai-A-Ali を選択します。
- ・ ポート仕様：ポート仕様を選択します。この例では、10G を選択します。仕様が異なるとリソース料金も異なります。
- ・ ポートタイプ：物理接続のアクセスポートを選択します。この例では、1000Base-LX を選択します。
- ・ 冗長接続 ID: 2つの物理接続を介して等価コストマルチパス (ECMP) ルーティングを実装する場合は、この物理接続に冗長性を提供するために別の物理接続を選択できます。

この例では、冗長物理接続を選択しません。

5. 今すぐ購入をクリックして、初期インストール料金の支払いを完了します。

6. 物理接続インターフェイスページで、申請した物理接続インターフェイスを確認します。

物理接続インターフェイスは LOA 申請待ちという状態にあります。

7. アクション列の LOA を申請するをクリックします。

8. 会社名、データセンターケーブルの設置会社名、設置予定日時、およびデータセンターケーブルの設置技術者または担当者の連絡先情報を入力して、構造のタイプを選択します。

9. OK をクリックします。その後、アプリケーションは Alibaba Cloud の担当者へ送信されて確認され、物理接続インターフェイスの状態が LOA 申請中になります。

10. アプリケーションが承認されたら、LOA をダウンロードして、設置サイトの位置 (Alibaba Cloud IDC サイト)、キャビネットの位置、ポート情報などのインストール情報をコンソールに表示します。この段階では、設置会社に設置開始を指示することをお勧めします。

11. 設置が完了後、物理接続インターフェイスページでの配信レポートをクリックして、設置サイトでの専用回線コードとケーブルのラベル番号を入力し、OK をクリックします。

物理接続インターフェイスが待機中状態に入ります。

12. Alibaba Cloud は、提供された情報に従い、ケーブルを対応する CSW ポートに接続します。前のステップで OK をクリックすると、Alibaba Cloud は 2 営業日以内にこのステップを完了する必要があります。

物理接続インターフェイスが待機中状態に入ります。

13.物理接続インターフェイスがデプロイに成功したことを確認できたら、リソース料金を支払い、ポートを有効にします。

物理接続インターフェイスの状態が有効になると、物理接続が完了します。



注:

Alibaba Cloud からの LOA 申請、設置、および現場での支援の完了までの推定時間枠は、現地の法律および規制に従います。

ステップ 2: 仮想ボーダールーターの作成

物理接続が確立後、VPC とオンプレミス IDC 間の転送ブリッジとして、仮想ボーダールーター (VBR) を作成する必要があります。

VBR を作成するには、次の手順を実行します。

1. [Express Connect コンソール](#)にログインします。
2. 左側のナビゲーションペインで、物理接続 > 仮想ボーダールーター (VBR) をクリックします。
3. VBR の作成をクリックします。この例では、VBR を次のように設定します。
 - ・ アカウント: 現在のアカウントを選択します。
 - ・ 名前: VBR の名前を入力します。
 - ・ 物理接続インターフェイス: 手順 1 で作成した物理接続インターフェイスを選択します。
 - ・ VLAN ID: VLAN ID を入力します。この例では、1678 と入力します。
 - ・ Alibaba Cloud 側のゲートウェイ IP アドレス: VPC からオンプレミス IDC へのゲートウェイを入力します。この例では、10.0.0.1 と入力します。
 - ・ ユーザー側のゲートウェイ IP アドレス: オンプレミス IDC から VPC へのゲートウェイを入力します。この例では、10.0.0.2 と入力します。
 - ・ サブネットマスク: Alibaba Cloud 側とユーザー側の IP アドレスのサブネットマスクを入力します。この例では、255.255.255.0 と入力します。
4. OK をクリックします。

ステップ 3: ピアリング接続の作成

物理接続が確立された後、物理接続に関連付けられている VBR と接続される VPC の間にピアリング接続を確立する必要があります。

ピアリング接続を作成するには、次の手順を実行します。

1. [Express Connect コンソール](#)にログインします。

2. 左側のナビゲーションペインで、VPC ピアリング接続 > VBR-VPC 接続 をクリックします。
3. ピアリング接続の作成 をクリックします。
4. ピアリング接続を構成します。

次の構成を実行します。

- ・ 現在のアカウントに属している: はいを選択します。
- ・ 接続タイプ: VPC-VPC 接続 を選択します。
- ・ 作成するルーター: 開始側と受信側を選択します。

物理接続のシナリオでは、ピアリング接続の開始側は VBR である必要があります。

- ・ ローカルリージョン: VBR が配置されているリージョンを選択します。この例では、中国 (張家口) を選択します。
 - ・ ローカルアクセスポイント: 物理接続のアクセスポイントを選択します。この例では、ap-cn-zhangjiakou-xrt-A を選択します。
 - ・ ローカル VBR ID: 作成した VBR を選択します。この例では、VBR1 を選択します。
 - ・ ピアリージョン: 接続先 VPC が配置されているリージョンを選択します。この例では、中国 (張家口) を選択します。
 - ・ ピア VPC ID: ピア VPC を選択します。この例では、VPC1 を選択します。
 - ・ 帯域幅: 相互接続の帯域幅をクリックします。この例では、1Gb を選択します。
5. 今すぐ購入 をクリックして、支払いを完了します。
 6. 作成したピアリング接続を確認します。開始側と受信側が有効状態になると、ピアリング接続は正常に確立されます。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vbr-2zccmmvg5gvu84telkhw ri-2ze7mi282a589luyeyb28 - [X] Route Settings	Beijing-Daxing-A	vpc-m5e2htpw081sb84esznt ri-mc8e9iq4qbh8jcc11j3 Route Settings	China North 1 (Qingdao)	Yes	Small.1	Pay-As-You-Go Created at Sep 29, 2018, 20:54:10 Connected at Sep 29, 2018, 20:55:24	<ul style="list-style-type: none"> ● Initiator: Activated ● Acceptor: Activated 	

ステップ 4: VPC ルーティングの構成

ピアリング接続を確立したら、ローカル IDC 宛のルートエントリを VPC に追加する必要があります。

オンプレミス IDC (11.11.11.0/24) 宛てのトラフィックを VBR に転送するには、次の手順を実行します。

1. VPC ページで、相互通信された VPC を特定し、その VPC の ID をクリックします。

Instance ID/Name	Destination CIDR Block	Status	Default VPC	Route Table	VSwitch	Actions
vpc-m5e2htpdw81sb84esznt	192.168.0.0/16	Available	No	1	1	Manage Delete

2. ネットワークリソースエリアで、ルートテーブルのリンクをクリックします。
3. ルートテーブルページで、VPC のルートテーブル ID、およびルートエントリの追加 をクリックします。
4. 次のようにルートエントリを設定し、OK をクリックします。
 - ・宛先 CIDR ブロック: オンプレミス IDC の CIDR ブロックを入力します。この例では、10.0.0.0/24 と入力します。
 - ・ネクストホップタイプ: ルーターインターフェイス (VBR へ) を選択します。
 - ・通常のルート: 物理接続に関連付けられている VBR を選択します。

ステップ 5: ルーティングの構成

オンプレミス IDC と VPC それぞれに宛てた VBR ルーティングを設定するには、次の手順を実行します。

1. [Express Connect コンソール](#) にログインします。
2. 左側のナビゲーションウィンドウで、VBR-VPC 接続 をクリックします。
3. 対象の VBR を見つけて、ルート設定 をクリックします。

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vbr-2zccmmvg5guu84telkhw i-2ze7n282a599luyey28	Beijing-Daxing-A	vpc-m5e2htpdw81sb84esznt i-m5e2htpdw81sb84esznt	China North 1 (Qingdao)	Yes	Small, 1	Pay-As-You-Go Created at Sep 29, 2018, 20:54:10 Connected at Sep 29, 2018, 20:55:24	Initiator: Activated Acceptor: Activated	

4. ルートエントリの追加をクリックします。
5. 表示されたダイアログボックスで、VPC の CIDR ブロック (この例では、192.168.0.0/16) を入力し、確認 をクリックします。
6. 再度、ルートエントリの追加 をクリックします。
7. オンプレミス IDC の CIDR ブロック (この例では、10.0.0.0/24) を入力し、確認 をクリックします。

ステップ 6: オンプレミス IDC 用のルーティングの構成

これで、Alibaba Cloud 側のルート構成は完了です。物理接続デバイスでは、VPC 宛のルートを構成する必要があります。次のように静的ルートまたは BGP ルートを構成して、オンプレミス IDC から VBR にデータを転送できます。

- ・ 静的ルート

例：

```
ip route 192 . 168 . 0 . 0 / 16 10 . 0 . 0 . 2
```

- ・ 動的ルート

BGP を構成して、オンプレミス IDC と VBR の間でデータを転送することもできます。詳細は、[#unique_12](#)をご参照ください。

ルート構成が完了すると、オンプレミス IDC と VPC 間のイントラネット通信リンク (オンプレミス IDC から物理接続、VBR、VPC まで) が確立されます。



注：

ECS セキュリティグループルールを調整するか、RDS ホワイトリストを追加することで、オンプレミス IDC デバイスと Alibaba Cloud プロダクト間のアクセスを管理できます。

ステップ 7: 接続のテスト

VPC をオンプレミス IDC に接続したら、専用回線の速度をテストして、サービスニーズが満たされていることを確認します。