Alibaba Cloud
Virtual Private Cloud

VPC プロダクト紹介

Document Version20190329

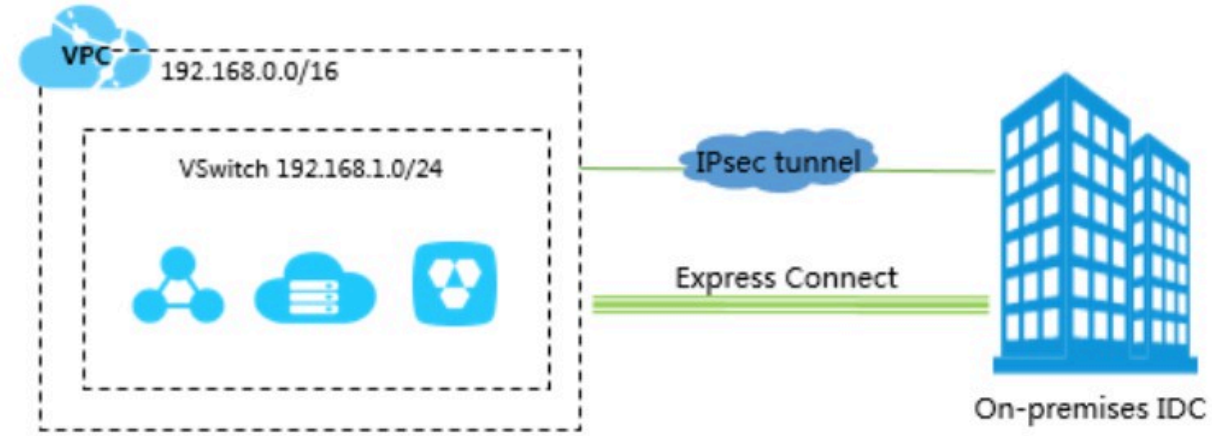
目次

1 VPCとは

VPCは、Alibaba Cloudに設置されたプライベートネットワークです。 VPCはAlibaba Cloudの他の仮想ネットワークと論理的に分離されています。

VPCはAlibaba Cloud でお客様専用のプライベートネットワークです。 IPアドレス範囲の指定、ルートテーブルとネットワークゲートウェイの設定など、VPCを完全に制御できます。 お客様ご自身のVPCで、ECS、RDS、SLBなどのAlibaba Cloudリソースを使用することができます。

さらに、VPCを他のVPCやローカルネットワークに接続してオンデマンドネットワーク環境を構築することで、 アプリケーションをAlibaba Cloudにスムーズに移行できるようになります。



コンポーネント

各VPCは、プライベートCIDRブロック、VRouter、及びVSwitchで構成されます。

- CIDRブロック

  VPCやVSwitchを作成する場合は、プライベートIPアドレス範囲をCIDR（Classless Inter-Domain Routing）ブロックの形式で指定する必要があります。 詳細は*Classless Inter-Domain Routing*を参考してください。

  次に表示されるいずれかのスタンダードCIDRブロックやそのサブネットを参考してVPCのIPアドレス範囲を設定してください。 詳細は次を参照してくださいネットワーク環境の設計。

  注：

スタンダードCIDRブロックのサブネットを使用するには、*CreateVPC* APIを使用してVPCを作成してください。

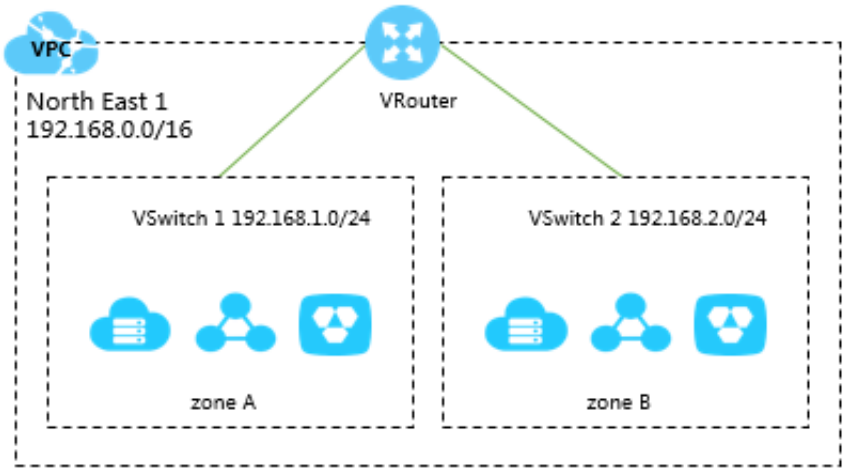
CIDRブロック	利用可能なプライベートIPの数（システム予約済みIPは含まれていません）
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

- VRouter

  VRouterはVPCのハブです。 VPCの重要な構成要素として、ハブとしてVPC内の各VSwitchを接続でき、ゲートウェイとしてもVPCを他のネットワークに接続することもできます。 VPCを作成すると、VRouterはAlibaba Cloudにより自動的に作成されます。 VRouterはルートテーブルとデフォルトで関連付けられます。 詳細は次を参照してくださいルーティング。

- VSwitch

  VSwitchは、VPCの基本的なネットワークデバイスであり、様々なクラウド製品インスタンスに接続するために使用されます。 VPCを作成後、VSwitchを作成してさらに仮想プライベートネットワークを一つ、或いは複数のサブネットにセグメントすることができます。 VPC内の各VSwitchは、互いにデフォルトで接続しています。 サービス向上のために、異なるゾーンの異なる VSwitchに異なるアプリケーションを導入することができます。 詳細は次を参照してくださいVSwitchの管理。



2 VPCコネクション

Alibaba Cloudは、VPCをインターネット、その他VPC及びローカルデータセンターなどに接続する接続オプションを数多く提供しています。

インターネットに接続

VPCをインターネットに接続するには、次のテーブルに表示されるプロダクトや機能を使用します。

プロダクト	機能と特徴	利点
VPC ネットワークの ECS インスタンスパブリック IP	VPC ネットワーク内で ECS インスタンスを作成時に自動的に割り当てられるパブリック IPです。 このパブリック IP を使用することで、ECS インスタンスがインターネット（SNAT）にアクセスできるようになり、インターネット（DNAT）からアクセスされることも可能になります。	データ転送プランを使用することができます。 パブリック IP を EIP に変更すると、 インターネット共有帯域幅も使用できるようになります。
Elastic IP アドレス(EIP)	EIP を使用することで、ECS インスタンスがインターネット（SNAT）にアクセスできるようになり、インターネット（DNAT）からアクセスされることも可能になります。	ECS インスタンスからいつでも EIP をバインド/バインド解除することができます。 インターネットコストを削減するためにインターネット共有帯域幅とデータ転送プランを使うことができます。
NAT Gateway	NAT Gateway はエンタープライズ級のインターネットゲートウェイであり、複数の ECS インスタンスが一つの EIP（SNAT）を通してのインターネットへのアクセスや、インターネット（DNAT）からのアクセスを対応しています。 注： SLB に比べ、NAT Gateway 自体はトラフィックの負荷分散機能を提供していません。	複数の ECS インスタンスへのインターネットアクセスがサポートされています。 （EIP はこのサポートを提供していないことにご注意ください。）

プロダクト	機能と特徴	利点
Server Load Balancer	ポートに基づいたロードバランシング。SLB にはレイヤ 4（TCP と UDP プロトコル）とレイヤ 7（HTTP と HTTPS プロトコル）のロードバランシングを対応しています。 SLB はクライアントのリクエストをインターネットからバックエンド ECS インスタンスに転送できます。 注： ECS インスタンスはパブリック IP なしでは SLB を通してのインターネット（SNAT）へのアクセスを対応していません。	DNAT では、SLB はインターネットリクエストを複数の ECS インスタンスに転送できます。 Server Load Balancer は、サービス機能を向上させ、全体的な可用性を向上させることができます。 EIP でバインドすると、 インターネット共有帯域幅と データ転送プランを使用してインターネットコストを削減することができます。

VPC への接続

次のテーブルに表示されるプロダクトや機能を使用して、VPC を他の VPC に接続します。

プロダクト	機能と特徴	利点
VPN Gateway	VPN Gateway では、IPsec-VPN を作成して 2 つの VPC ネットワークの間で暗号化された通信を構築することができます。 詳細は、*VPC間接続の設定*をご参照ください。	・ 低コスト、安全、簡易な構成。（ネットワークの品質はご使用するインターネット接続によるものです。） ・ IPsec-VPN は IKEv1 と IKEv2 プロトコルに対応しています。この 2 つのプロトコルをサポートするデバイスは、Alibaba VPN Gateway に接続できます。対応デバイス：Huawei、H3C、SANGFOR、Cisco ASA、Juniper、SonicWall、Nokia、IBM、Ixia。

プロダクト	機能と特徴	利点
クラウド エンタープライズ ネットワーク (CEN)	CEN は、異なったリージョン、異なったアカウント内の VPC を接続し、相互接続ネットワークを構築できます。 詳細は、チュートリアルの概要をご参照ください。	・ 簡易な構成、ルートの自動ラーニング及び配布。 ・ 低遅延、高速度。 ・ CEN インスタンスにアタッチされるネットワーク（VPC / VBR）の間は相互に接続されています。 ・ 同一リージョン内のネットワーク接続は無料です。

オンプレミスのデータセンターへの VPC の接続

次のテーブルに、VPC をオンプレミスに接続するためのプロダクトや機能が表示されています。

プロダクト	機能と特徴	利点
Express Connect	Express Connect を使用すると、VPC をオンプレミスのデータセンターに接続できます。 詳細、物理接続を介したオンプレミス IDC からの VPC への接続をご参照ください。	・ 基幹ネットワークに基づくため、低遅延。 ・ 専用回線接続で安全性、信頼性を確保の上、高速度と低遅延な接続を提供します。

プロダクト	機能と特徴	利点
VPN Gateway	・ VPN Gateway を使用することで、VPC とオンプレミスデータセンターの間に IPsec-VPN 接続を作成できます。 ・ 複数のオンプレミスデータセンターの接続 VPN Gateway の VPN ハブ機能を使用することで、複数のオンプレミスデータセンターを VPC に接続できます。 接続されたデータセンターは VPC との通信のみならず、各データセンターの間でも互いに通信可能です。 ・ リモートアクセス VPN Gateway を使用することで、SSL-VPN 接続を作成して、クライアントがリモートコンピュータを通して VPC への接続ができます。	・ 低コスト、安全、簡易な構成。 もちろん、ネットワークのクオリティはインターネットによって異なります。 ・ IPsec-VPN は IKEv1 と IKEv2 プロトコルに対応しています。 この 2 つのプロトコルをサポートするデバイスは、Alibaba VPN Gateway に接続できます。 対応デバイス：Huawei、H3C、SANGFOR、Cisco ASA、Juniper、SonicWall、Nokia、IBM、Ixia。 ・ SSL-VPN 接続が以下のリモートコンピュータを使用して VPC へ接続できます：Linux、Windows、MacOS。

プロダクト	機能と特徴	利点
CEN	・ オンプレミスデータセンターへの接続 CEN を使用することで、オンプレミスデータセンターに関連付けられた VBR を CEN インスタンスに接続し、相互接続されたネットワークを構築できます。 ・ 複数の VPC をオンプレミスデータセンターに接続する CEN を使用することで、複数のネットワーク（VPC / VBR）を CEN インスタンスにアタッチすることができます。 アタッチされたすべてのネットワークは相互に接続しています。	・ 簡易な構成、ルートの自動ラーニング及び配布。 ・ 低遅延、高速度。 ・ CEN インスタンスにアタッチされるネットワーク（VPC / VBR）の間は相互に接続されています。 ・ 同一リージョン内のネットワーク接続は無料です。
Smart Access Gateway(SAG)	・ Smart Access Gateway では、オンプレミスブランチを Alibaba Cloud に接続して、大規模な組織向けのハイブリッククラウドを構築できます。 ・ ローカルブランチへの接続。	・ SAG は、高度に自動化された構成を特徴とし、自動的かつ迅速にネットワークトポロジの変更に適応します。 ・ インターネットを介して都市の最寄りポイントからアクセスが提供されます。 さらに、複数のローカルブランチは、マスター/スレーブリンクを備えた Smart Access Gateway デバイスを使用して Alibaba Cloud にアクセスできます。 ・ ローカルブランチと Alibaba Cloud は、暗号化されたプライベートネットワークを通して接続され、インターネットの送信中の暗号化認証が実装されます。

3 アーキテクチャ

VPCでは、主流のトンネリング技術に基づいて 仮想ネットワークを分離しています。 VPC には一意のトンネル ID があり、トンネル ID は 1 つの VPC にのみ対応しています。

背景情報

クラウドコンピューティング技術の発展に伴い、スケーラビリティ、セキュリティ、弾力性、プライバシーなど、仮想ネットワークに対する要求が高まっています。相互接続のパフォーマンスに対する要求もきわめて高くなっています。 そのため、幅広いネットワーク仮想化技術が生み出されてきました。

大規模レイヤー2ネットワークなど、初期のソリューションでは、仮想マシンネットワークを物理ネットワークと結合して、フラットなネットワークアーキテクチャを形成していました。 これらのソリューションでは ARP スプーフィング、ブロードキャストストーム、 ホストスキャニングなどによる問題が深刻になってきました。 物理ネットワークを仮想ネットワークから完全に分離することでこのような問題を解決するための、さまざまなネットワーク分離技術が生まれました。 そのうちの 1 つの技術では、VLAN を使用してユーザーを分離しました。しかし、VLAN でサポート出来るノード数の上限は 4096 であり、 巨大なユーザーを持つクラウドには向いていません。

VPC原理

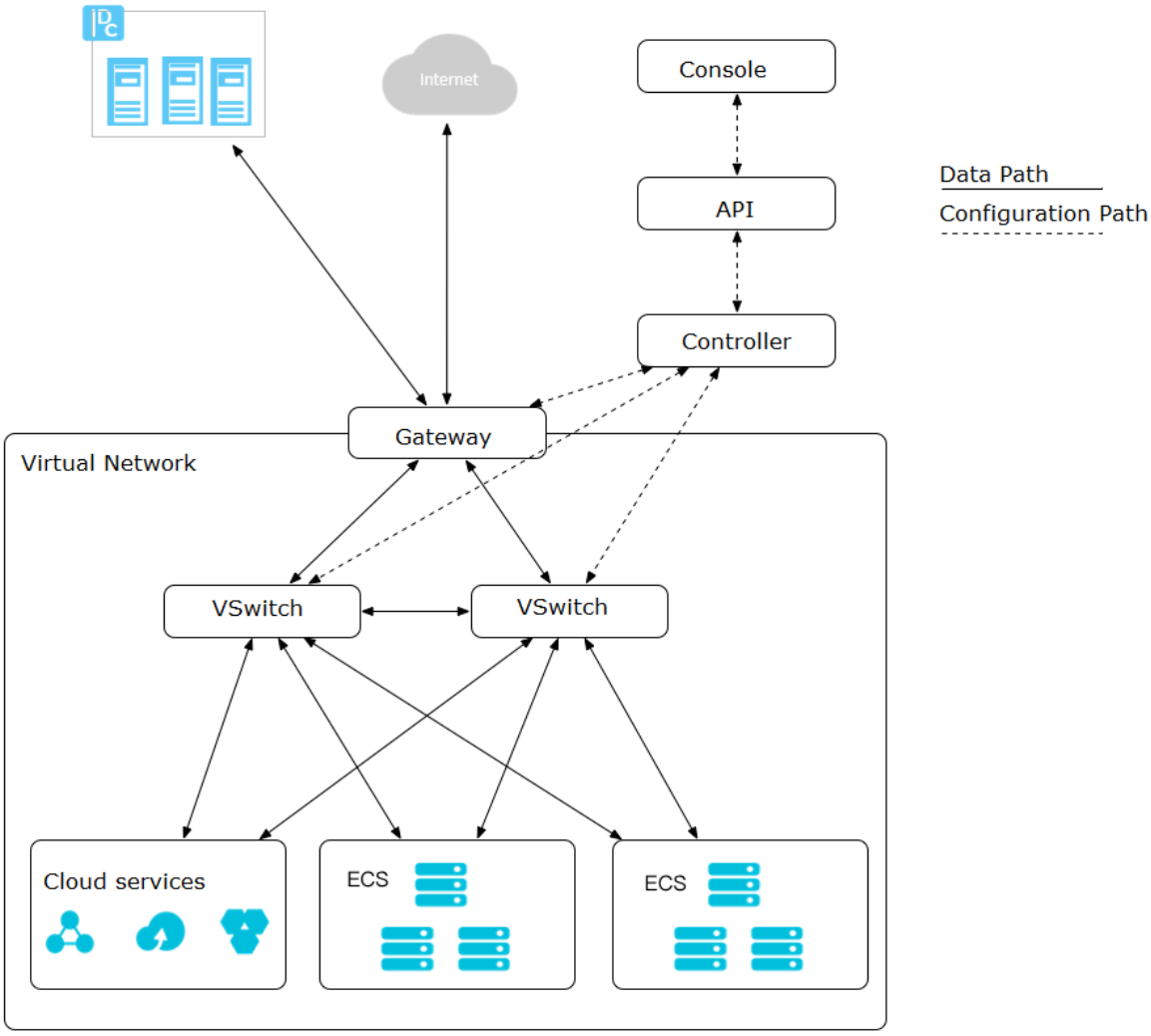
VPCでは、主流のトンネリング技術に基づいて 仮想ネットワークを分離できます。 VPC には一意のトンネル ID があり、トンネル ID は 1 つの VPC にのみ対応しています。 VPC内のECSインスタンス間で送信されるデータパケットはトンネルIDを与え、 カプセル化して物理ネットワーク上に送信されます。 異なるVPC内のECSインスタンスはトンネルIDが異なり、異なるルーティングプレーン上に存在するため、2つのトンネル間の通信は不可能であり、自ずと分離されます。

Alibaba Cloudの研究開発チームはトンネリング技術とSDN技術に基づき、ハードウェアゲートウェイ及びを自己開発したSwitch装置を基にしてVPCを開発しました。

論理アーキテクチャ

下図に示しているように、VPCのアーキテクチャには VSwitch、ゲートウェイ、コントローラの 3 つの主要なコンポーネントが含まれています。 VSwitch とゲートウェイがデータパスの中核です。 コントローラはAlibabaプロトコルを使用して転送テーブルをゲートウェイとVSwitchへ発送し、キーの構成パスを完了します。 全体アーキテクチャの中で、構成パスとデータパスは互いに分離しています。 VSwitchは分散ノードであり、ゲートウェイとコントローラはクラスタにデ

プロイされ、すべてのリンクには冗長化障害耐性を備えています。 これでVPCプロダクト全体の可用性が向上します。



4 メリット

VPCには高水準のセキュリティと柔軟な設定が備えられ、複数の接続方式に対応しています。

セキュリティ

各VPNには一意のトンネルIDがあり、トンネル ID は 1 つの VPC にのみ対応しています。
各VPCはトンネルIDにより分離されます。

- VPCにはVSwitchとVRouterがあるため、従来のネットワークのようにサブネットをセグメントすることができます。 同一サブネット内のCloudリソースはVSwitchを通じて相互に通信します、一方、異なったサブネットの間ではVRouterを通じて相互に通信します。
- 異なったVPCの間でのイントラネット通信は完全に分離され、外部IP（ElasticIPとNAT IP）のマッピングによってのみ相互接続が可能です。
- ECSのIPパケットはトンネリングIDでカプセル化されているため、サーバーのデータリンク層（レイヤ２のMACアドレス）は物理ネットワークに転送されません。 それにより、異なるECSの間のレイヤ２ネットワークが分離されます。 ようするに、異なるVPCの間のレイヤ２ネットワークが分離されています。
- VPCのECSインスタンスは、セキュリティグループをファイアウォールとして使用し、ECSインスタンスに対するトラフィックの転送を制御します。 これは第3層の分離です。

アクセス制御

セキュリティグループやホワイトリストを利用して、VPC内のクラウドリソースを通過する着信及び発信トラフィックを制御できます。

使い勝手

VPCコンソールを通じて、プライベートネットワークを簡単に作成/管理できます。 VPCを作成後、VRouterとルートテーブルがシステムにより自動的に作成されます。

スケーラブル

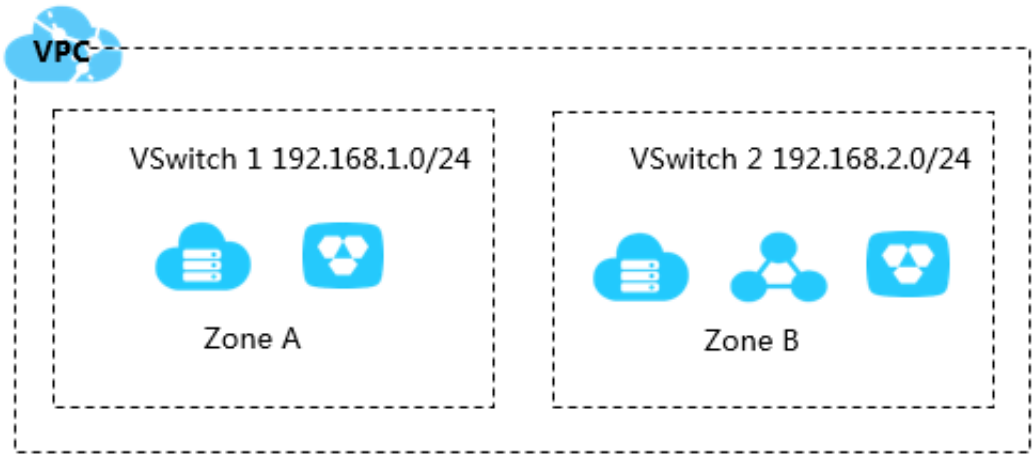
同一VPCで複数のサブネットを作成でき、様々なサービスをデプロイできます。 さらに、VPCをローカルデータセンターまたは他のVPCに接続して、ネットワークアーキテクチャを拡張することもできます。

5 シナリオ

VPC は、完全に分離されたネットワーク環境であり、異なる状況で使用することができます。

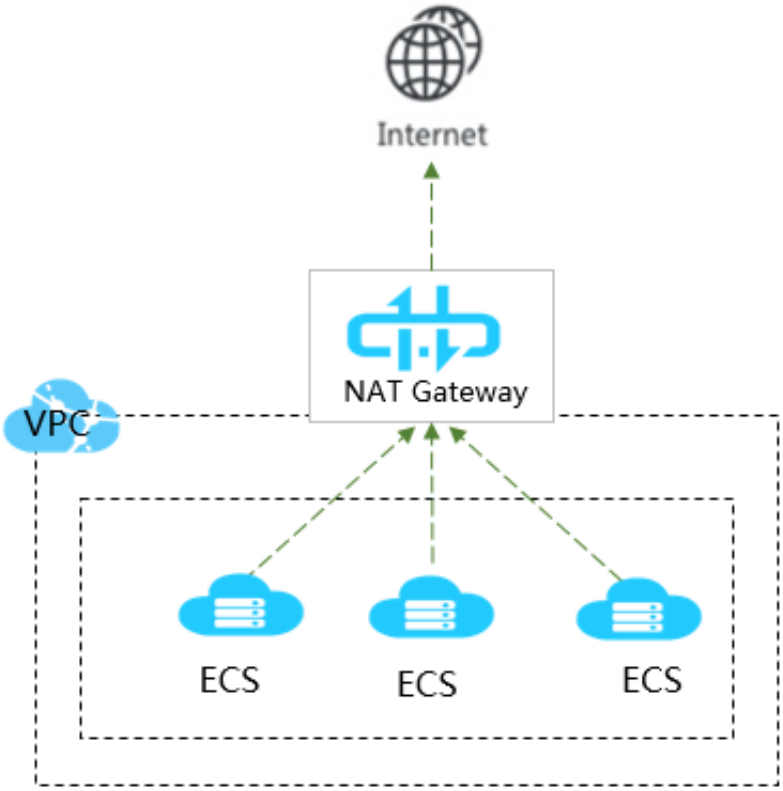
アプリケーションをホストする

VPCで外部サービスを提供するアプリケーションをホストし、セキュリティグループのルール及びホワイトリストを作成することでインターネットアクセスを制御することができます。 アプリケーションサーバーをデータベースから分離することでアクセスを制御することもできます。 たとえば、インターネットに通信可能なサブネットにWebサーバーをデプロイし、インターネットに通信できないサブネットにアプリケーションのデータベースをデプロイします。



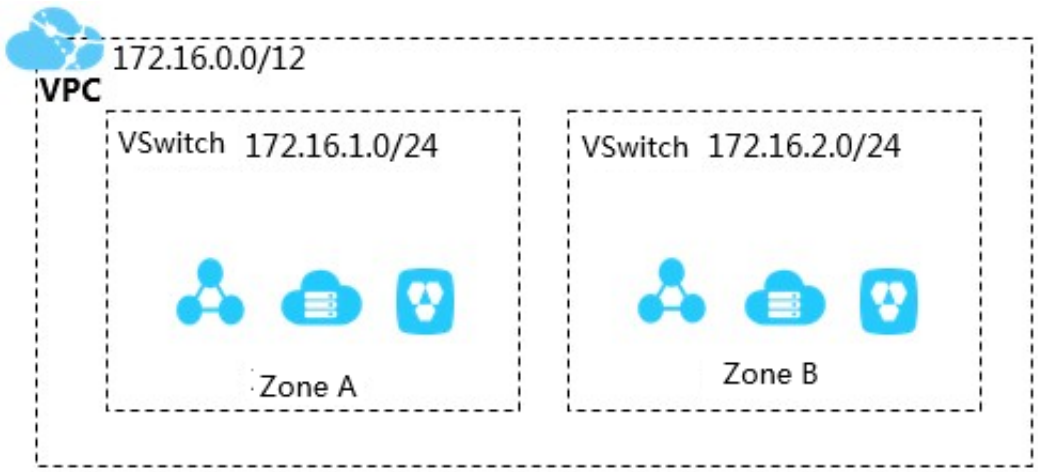
インターネットアクセスを要求するアプリケーションをホストする

VPC内のサブネットにインターネットアクセスを要求するアプリケーションをホストし、NATを通してトラフィックを送信することができます。 SNATルールを構築することで、サブネット内のインスタンスはプライベートIPアドレスを公開せずにインターネットにアクセスでき、外部IP攻撃を回避するためにプライベートIPアドレスをパブリックIPアドレスにいつでも変更できます。



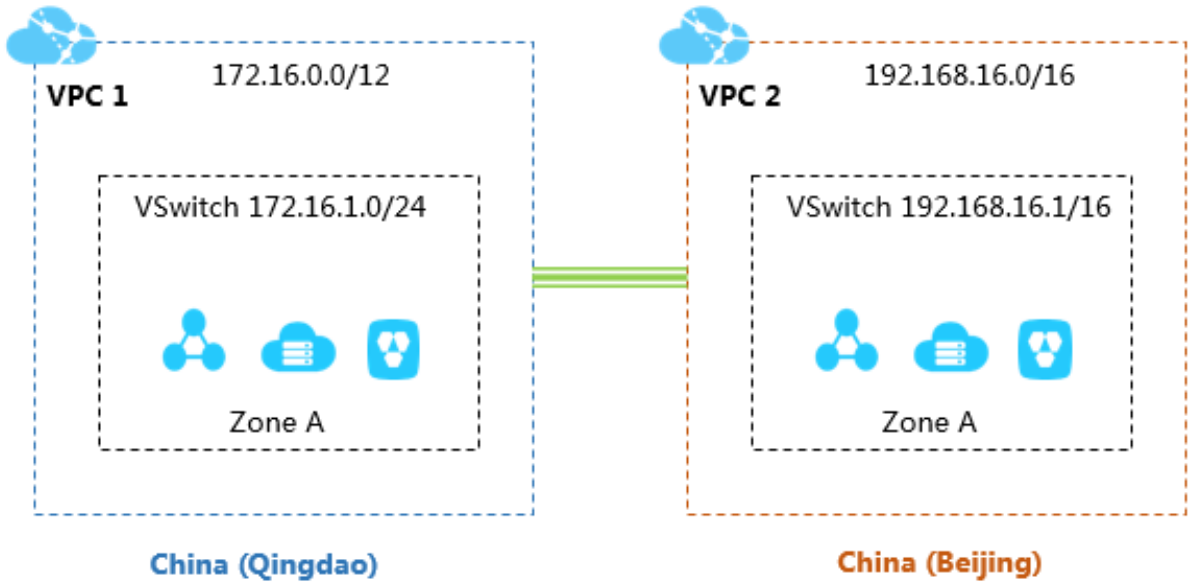
クロスゾーンの耐災害性

VSwitcheを作成することで、一つのVPC内で複数のサブネットを作成することができます。VPC内の各VSwitchは、イントラネットを通して互いに通信することができます。 各ゾーンのVSwitchにリソースをデプロイし、クロスゾーンの耐災害性を実現します。



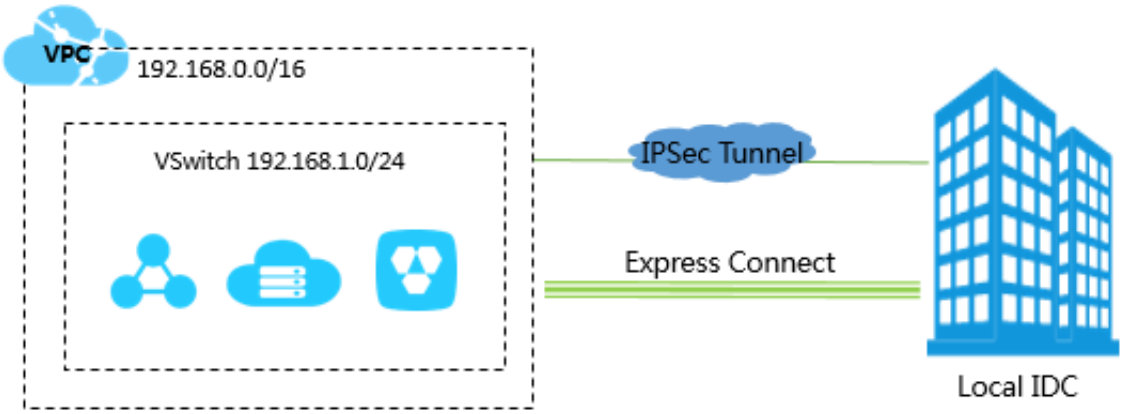
ビジネスシステムの分離

異なるVPCは論理的に分離されています プロダクション環境をテスト環境から分離するなど、複数のビジネスシステムを分離しなければならない場合、複数のVPCを作成することができます。VPC同士に通信する必要がある場合、それらの間にピア接続を作成することができます。



ハイブリッドクラウドを構築します

専用接続を作成して、VPCをローカルデータセンターに接続しローカルネットワークを拡張することができます。 専用接続を使用して、アプリケーションへのアクセス方法を変更することなく、ローカルアプリケーションをクラウドにシームレスに移行することができます。



6 VPC用語

用語	説明
仮想プライベートクラウド(VPC)	VPCはAlibaba Cloudに設置されたプライベートネットワークです。 Alibaba Cloudの他の仮想ネットワークから論理的に分離されています。 Alibaba Cloud VPCを使用すると、ECS、SLB及びRDSなどのAlibaba Cloudリソースを個人のVPCでアクセスすることができます。
VSwitch	VSwitch は、VPCの基本的なネットワークデバイスであり、様々なクラウド製品インスタンスに接続するために使用されます。 VPCでCloud製品インスタンスを作成する場合は、インスタンスを配置済みのVSwitchを指定しなければなりません。
VRouter	VRouterはVPCのハブとしてVPC内の各VSwitchに接続しています。またゲートウェイデバイスとしてもVPCを他のネットワークに接続しています。 VRouterはルートエントリの設定情報に基づいて、ネットワークトラフィックを発送しています。
ルートテーブル	ルートテーブルは、VRouterに保存されるルートエントリのリストです。
ルートエントリ	ルートエントリは、ルートテーブル内の各項目のことです。ルートエントリは、特定のCIDRブロックを経由するネットワークトラフィックのネクストホップアドレスを定義しています。 ルートエントリには、システムルートエントリとカスタマイズルートエントリの2種類があります。

7 使用制限

リソース	デフォルトの制限	クォータ量の増減
各リージョンでの最大VPC数	10	
使用可能なCIDRブロックの範囲	192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8,及びそのサブセット	サポートセンターまでお問い合わせください
VPC 内の VRouter の最大数	1	申請不可
VPC 内の VSwitch の最大数	24	サポートセンターまでお問い合わせください
VPC 内のルータテーブルの最大数	1	申請不可
ルータテーブル内のルートエントリの最大数	48	サポートセンターまでお問い合わせください
VPC で実行できるクラウド製品インスタンスの最大数	15,000	申請不可