Alibaba Cloud
Virtual Private Cloud

ベストプラクティス

Document Version20190329

目次

1 VPC環境の設計

VPCとVSwitchを作成する前に、業務の規模に合わせてVPC及びVSwitchの数量及びCIDRブロックを決める必要があります。

VPC（仮想プライベートクラウド）は お客様専用のAlibaba Cloudプライベートネットワークである。 VPC はAlibaba Cloud内で他のVPCと論理的に分離されています。 VPCネットワークを使用するユーザーが増えつつある原因としては：

- 分離されたネットワーク環境

  VPC では、トンネリング技術に基づいてデータリンク層を分離することにより、分離され独立した安全なネットワークを各ユーザーに提供します。 VPC内のリソースは、イントラネット経由で相互通信できますが、VPCリソースにパブリック IP を設定するか EIP をバインドしていなければ、他の VPC 内のリソースと 直接通信することはできません。
- 制御可能なネットワーク設定

  IP アドレス範囲の選択、ルートテーブルやネットワークゲートウェイの構成など、VPC ネットワークは全面的に制御することにより、さらなる簡単的なリソースアクセスを実行できます。 また、VPCを他のVPC,またはローカルIDC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にスムーズにいこうでし、ローカルIDSネットワークを拡張することあできます。

  詳細については、*VPCとは*を参照してください。

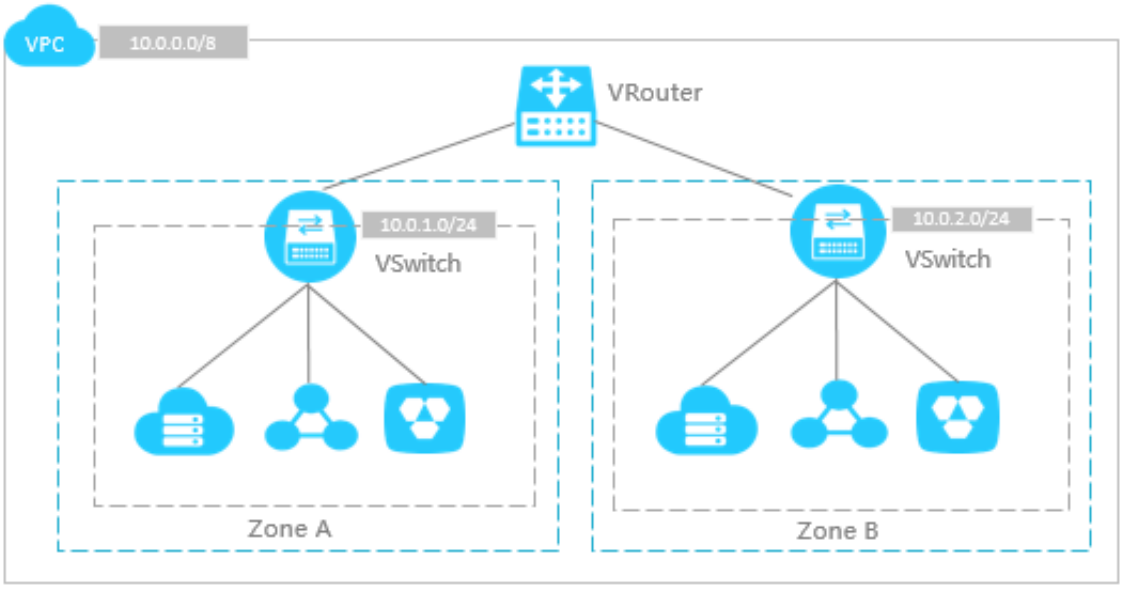
VPCを使用するする際には、最初に解決すべき問題は、VPCネットワーク環境の設定です¥。 次のいくつかの問題からVPCのデザインを開始します：

- 質問*1*：必要な*vpc*の数は？
- 質問*2*：*VSwitch*の必要な数は？
- 質問*3*：*CIDR*ブロックの選び方は？
- 質問*4*：*VPC* をローカルデータセンターまたは他の *VPC* に接続する計画がある場合に*CIDR* ブロックの選び方は?

質問1：必要なvpcの数は？

- **1つのVPC**

  複数のリージョンにシステムをデプロイするという要件がなく、システムを分離する必要がない場合は、1 つのVPCの作成をお勧めします。 現在、VPCでは15,000のクラウドプロダクトインスタンスを実行できます。



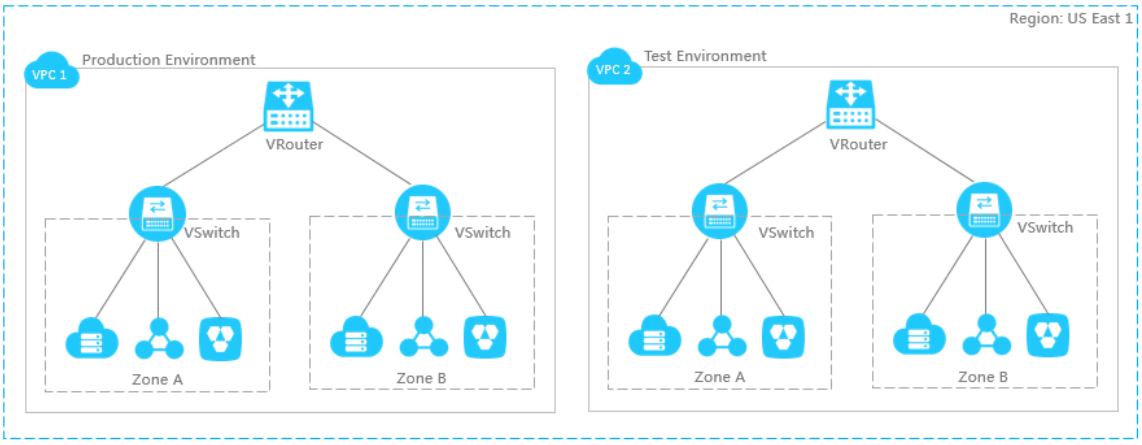
- **複数のVPC**

  次に示すような要件がある場合は、複数 VPC の作成をお勧めします。

  - **異なる複数のリージョンにクラウドプロダクトリソースをデプロイします**

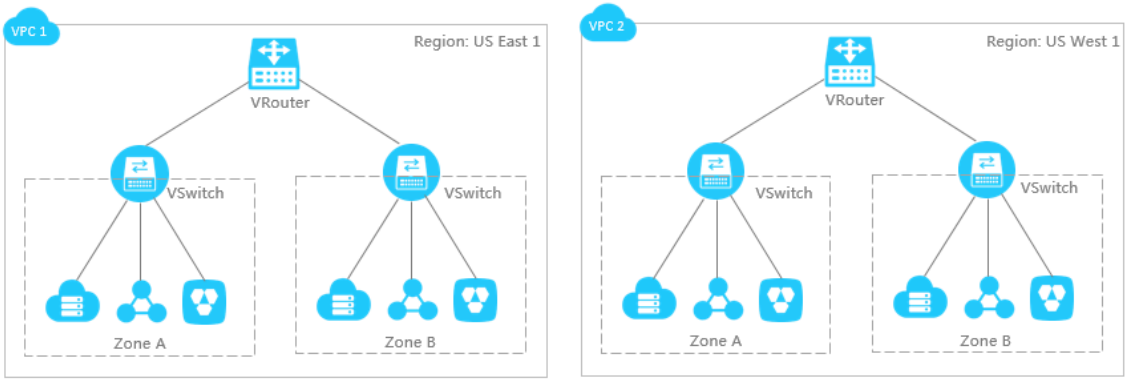
    VPC は、リージョン固有のリソースであり、複数のリージョンにわたってデプロイすることはできません。 異なるリージョン内に異なるシステムをデプロイする場合は、複数の

VPC を作成する必要があります。 Express Connect/VPNゲートウェイ/CENを使用してVPCに接続できます。



- 異なったシステムの分離

  試作環境から本番環境の分離など、システムを分離する必要がある場合は、VPCを複数作成します。 異なったVPCの間は完全に分離されています。



質問2：VSwitchの必要な数は？

一般的に、VPCごとに2つ以上のVSwitchを作成し、こｎ2つのVSwitchを2つの異なったゾーンにデプロイすることをお勧めします。（ゾーンとは、リージョン内の独立電源及びネットワークが備えられた物理的な空間です。 同一リージョン内のゾーンの間でイントラネットを通じて相互接続されています）。 これにより、単一障害点からアプリケーションが保護されます。

同一リージョン内の異なったゾーンの間でのネットワーク応答時間が非常に短いです。 実際のビジネスシステムでのネットワーク応答時間を確認する必要があります。 ネットワーク応答時間は、複雑なシステム呼び出しやクロスゾーン呼び出しによって、予測より長くなることがあります。 システムの最適化と調整を行い、高い可用性と短い応答時間の間で最適なバランスを見つけます。

さらに、VSwitch の数はシステムの規模やデザインにも関連しています。 フロントエンドシステムでインターネットへの相互アクセスが必要な場合は、耐障害性向上のために各フロントエンドシステムを別々のVSwitchにデプロイし、 バックエンドシステムを他のVSwitchにデプロイすることができます。

質問3：CIDRブロックの選び方は？

VPCとVSwitchを作成時、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とVSwitchの IP アドレス範囲を指定する必要があります。

・ VPCのCIDRブロック

VPCのプライベートCIDRブロックとして192.168.0.0/16、172.16.0.0/12及び10.0.0.0/8を使用できます。 VPCのCIDRブロックを指定する際には、次の注意事項を参照してください：

- VPCが1つだけであり、このVPCでローカルデータセンターとの通信が必要ない場合は、上の表に示されているIPアドレス範囲をどれでも使用できます。
- 複数のVPCがある場合や、1つ以上のVPCとローカルデータセンターで構成されるハイブリッドクラウドを構築する場合は、VPCのIPアドレス範囲としてこれらの標準CIDRブロックのサブネットを使用し、ネットマスクが/16 を超えないようにすることをお勧めします。
- また、VPCのCIDRブロックの選択時にクラシックネットワークを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。

・ VSwitchのCIDRブロック

VSwitchのCIDRブロックはVSwitchの所属しているVPC、またはVPCのサブセットと同じように設定できます。 たとえば、VPCのCIDRブロックは192.168.0.0/16である場合、VSwitchのCIDRブロックをVPCのものそのままにするか、192.168.0.0/17から192.168.0.0/29までに設定できます。

VSwitchのCIDRブロックを選択時、次の注意事項を参照してください：

- 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。 この制限

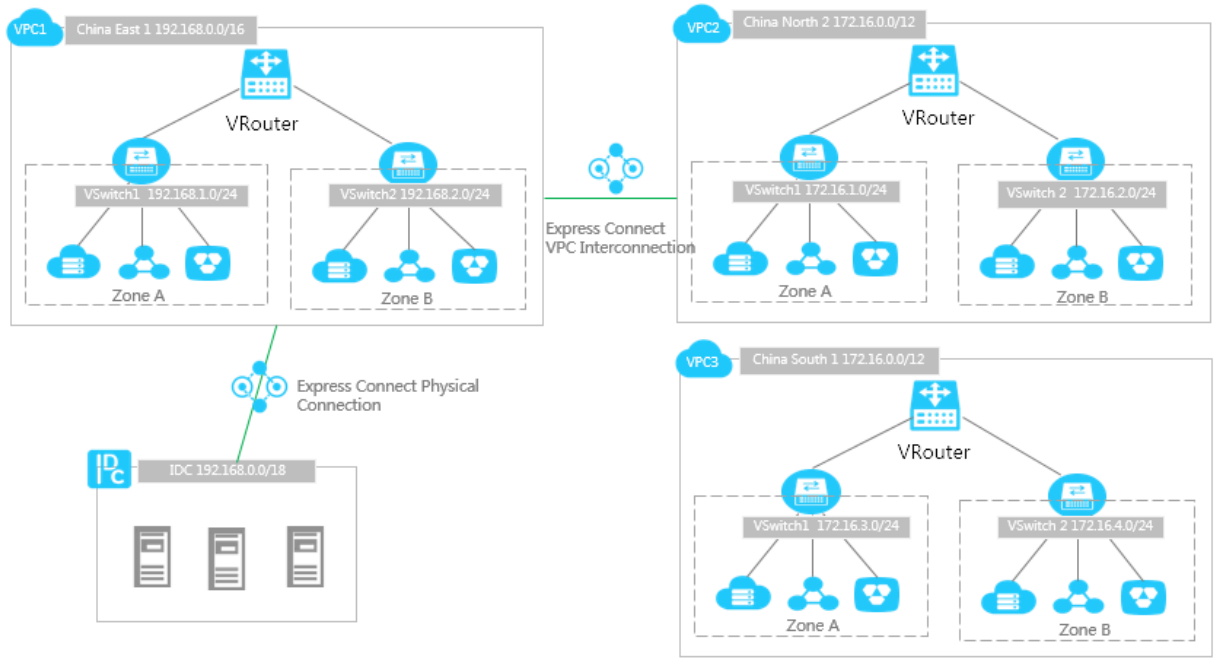
の理由は、/16は65,532のIPアドレスを使用できるので大きさは十分であり、/29 ネットマスクは小さすぎて現実的ではないためです。

- 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ています。 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ています。
- ClassicLink機能を使用すると、クラシックネットワーク内のECSインスタンスが192.168.0.0/16、10.0.0.0/8及び172.16.0.0/12 IP範囲内のVPCにあるECSインスタンスに通信できます。 ClassicLink機能を使用して、クラシックネットワーク内のECSインスタンスをVSwitchに接続しようとする場合、またVPCのCIDRブロックは10.0.0.0/8とすれば、VSwitchのCIDRブロックは10.111.0.0/16でなければなりません。 詳細は次を参照してください*ClassicLink*概要。
- VSwitchのCIDRブロックを決めるには、そのVSwitchに実行されているクラウドプロダクトインスタンスの数を考慮する必要があります。

質問4：VPC をローカルデータセンターまたは他の VPC に接続する計画がある場合にCIDR ブロックの選び方は?

VPCを他のVPC、またはローカルデータセンターに接続する場合、接続されたネットワークのCIDRブロックが重複していないことを確かめてください。

下の図のように 3 つの VPC があり、VPC1は中国（杭州）、VPC2は中国（上海）、VPC3は中国（北京） に配置されているものとします。 VPC1とVPC2 はExpress Connectを使用してイントラネット経由で相互通信できます。 VPC3には現在、他のVPCと通信する要件はなく、将来的にはVPC2との通信が必要になる可能性があります。 そして自身で構築したローカルデータセンターがあり、Express Connectの物理的なコネクションを通してVPC1に接続しています。



VPCを他のVPC またはローカルデータセンターに接続する必要がある場合は、各VPCのCIDRブロックが同じにならないように注意してください。 この例では、VPC1のCIDRブロックはVPC2のものとは異なりますが、VPC3のCIDRブロックはVPC2と変わりません。 ただし、将来相互通信が必要となったことに対応できるように、2つのVPC内のVSwitchは、まったく異なったCIDRブロックを使用しています。 VPC間の通信では、相互通信するVSwitchのCIDRブロックを同じようにすることはできませんが、VPCのCIDRブロックを同じようにすることはできます。

他のVPCまたはローカルデータセンターとの通信を必要とするVPCのCIDRブロックを指定する場合、次のルールを参照してください：

- 異なったVPCに異なったCIDRブロックを使用します。 スタンダードCIDRブロックのサブセットを使用して、VPCの数を増やすことができます。
- 第一原則には該当しない場合、異なったVPCのVSwitchに異なったCIDRブロックを使用するべきです。
- 上記のいずれの条件も満たされない場合は、通信を必要とするVSwitchのCIDRブロックが異なっていることを確かめてください。

2 プライベートネットワークプロダクトの選び方

仮想プライベートクラウド（VPC）は Alibaba Cloudでのお客様専用のプライベートネットワークです。 Alibaba Cloudは、Express Connect、VPN Gateway、CEN、Smart Access Gatewayなど、様々なシナリオでVPCにアクセスするプロダクトとサービスを提供しています。

本ドキュメントでは、VPCに接続するためのプライベートネットワークソリューションを紹介します。

VPCへの接続			
プロダクト	説明	メリット	制限
VPNゲートウェイ	インターネットベースの暗号化されたIPsec-VPNトンネルを使用して2つのVPCネットワークを接続します。	低コスト セキュリティ インストールは不要です。	ただし、ネットワークの応答時間と可用性はインターネットの違いによって変わります。
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一つや複数のVPCを接続し、相互接続ネットワークを構築します。	簡易な構成、ルーターの自動ラーニング及び配布。 低遅延及び高速度。 CENインスタンスにアタッチされたネットワーク（VPC/VBR）が相互に接続しています。 同一リージョン内のネットワークの間の相互接続は無料です。	—
ローカルIDCへの接続			
プロダクト	説明	メリット	制限
VPNゲートウェイ	インターネットベースの暗号化されたIPsec-VPNトンネルを使用してローカルIDCとVPCを接続します。	低コスト セキュリティ 構成はすぐに有効になります。	ただし、ネットワークの応答時間と可用性はインターネットの違いによって変わります。

クラウドエンタープライズネットワーク（CEN）	ルーターの自動ラーニング及び配布を通じて、CENはすべてのネットワーク名のリソースに接続できます。 ローカル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するだけで済みます。	簡易な構成、ルーターの自動ラーニング及び配布。 低遅延及び高速度。 CENインスタンスにアタッチされたネットワーク（VPC/VBR）が相互に接続しています。 同一リージョン内のネットワークの間の相互接続は無料です。	—
スマートアクセスゲートウェイ	Alibaba Cloudにローカルデータセンターを接続します。	高度に自動化された構成、またインストールは不要です。 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に暗号化認証されるような機能が実装されます。 最寄りシティーからのインターネット接続に対応しています。 さらに、複数のローカルブランチは、アクティブ/スタンバイリンクを備えたSmart Access Gatewayデバイスを使用してAlibaba Cloudにアクセスできます。	—
Express Connect	Express Connectの物理コネクションを通して、ローカルIDCとVPCを接続します。	高品質ネットワーク 高帯域	高コスト アクティブするのにかかる時間が長い

Alibaba Cloud Marketplace内のVPCソフトウェア	Alibaba Cloud MarketplaceでVPNゲートウェイを購入してVPCにデプロイし、インターネットベースの暗号化されたIPsec-VPNトンネルを通してVPCにローカルデータセンターを接続することができます。	セキュリティ 様々なVPNソフトウェアが利用可能です。 構成はすぐに有効になります。	お客様ご自身でVPNゲートウェイを構築/メンテナンスする必要があります。 ネットワークの応答時間と可用性はインターネットの違いによって変わります。
複数のサイトの接続			
プロダクト	説明	メリット	制限
VPNゲートウェイ（VPN-ハブ）	VPNゲートウェイを通して複数のサイト間で安全な通信を確立します。 VPNハブ機能は、各サイトがクラウド上のVPCと通信できるようにするだけでなく、各サイトが相互に通信できるようにしています。	低コスト インストールは不要です	—
スマートアクセスゲートウェイ	ローカルブランチが接続されるようにスマートアクセスゲートウェイを購入し、スマートアクセスゲートウェイをクラウドコネクトネットワーク（CCN）に追加します。 これらのローカルブランチの間のイントラネット接続を有効にするには、CENインスタンスにCCNをアタッチする必要があります。	インストールは不要です 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に暗号化認証されるような機能が実装されます。 最寄りシティーからのインターネット接続に対応しています。 さらに、複数のローカルブランチは、アクティブ/スタンバイリンクを備えたSmart Access Gatewayデバイスを使用してAlibaba Cloudにアクセスできます。	—

VPNゲートウェイ(VPN-Hub) + Express Connect	VPN GatewayとExpress Connectを使用して、世界中のアプリケーションシステムとオフィスサイトに接続できます。	高品質ネットワークインストールは不要です	ネットワークの応答時間と可用性はインターネットの違いによって変わります。
VPCへのリモートアクセス			
プロダクト	説明	メリット	制限
VPNゲートウェイ（SSL-VPN）	SSL-VPN機能を使用して、リモートクライアントからVPCに安全かつ迅速にアクセスします。	低コスト 高信頼性 簡単に構成及びデプロイできます	—
Alibaba Cloud Marketplace内のSSL-VPNソフトウェア	Alibaba Cloud MarketplaceでSSL-VPNソフトウェアを購入してVPCにデプロイし、リモートクライアントからVPNサーバーにアクセスします。	様々なSSL-VPNソフトウェアが利用可能です。	高コスト 低信頼性 お客様ご自身でSSL-VPNソフトウェアをデプロイ/メンテナンスする必要があります。

VPCへの接続

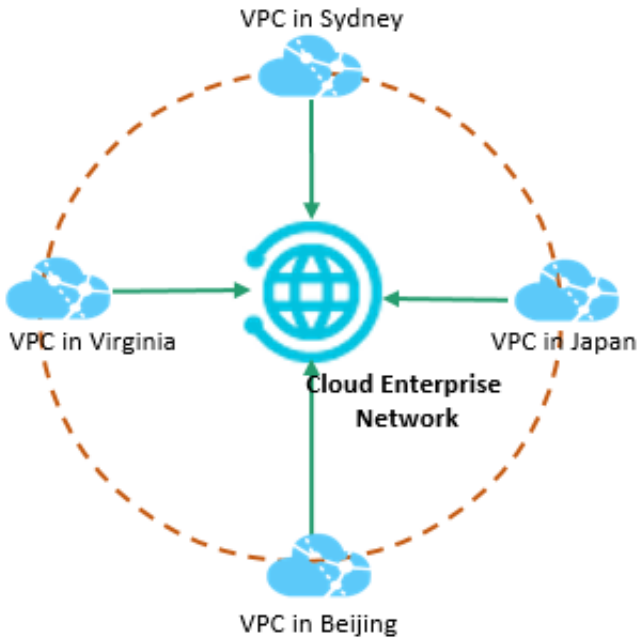
異なったVPCネットワークにアプリケーションをデプロイし、多地域サービスネットワークを構築することで、最寄りの場所からサービスの提供、ネットワークの応答時間の短縮、相互バックアップの実現など、システム全体の信頼性を向上させることができます。

Express ConnectとVPNゲートウェイ両方も、異なった地域または同一地域内のVPCに接続できます。

・ クラウドエンタープライズネットワーク（CEN）

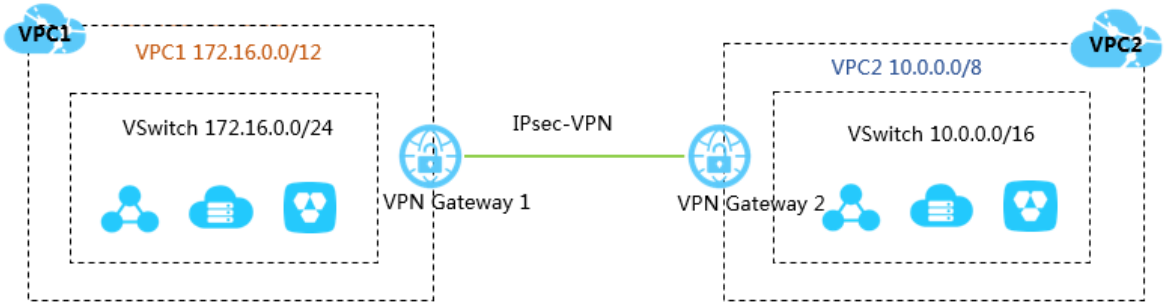
CEN（クラウドエンタープライズネットワーク）は、VPCの間でイントラネット通信チャネルを構築することができます。 ルーターの自動ラーニングと配布により、ネットワークの収束を加速し、ネットワーク間の通信品質及びセキュリティを向上させます、ネットワーク全体

のリソースを接続することで、エンタープライズレベルの規模と通信能力を備えた相互接続ネットワークを構築できます。



- VPNゲートウェイ

  VPNゲートウェイは、インターネットベースの暗号化されたチャネルを通じて、ローカルデータセンター、ローカルサイト、インターネットターミナルをVPCに安全かつ確実に接続できます。 VPNゲートウェイを通して、異なったリージョン、異なったアカウントからVPCに接続することができます。 VPCごとに1つのVPNゲートウェイと1つのカスタマーゲートウェイを作成し、イントラネット通信を実現するためにVPCゲートウェイと対応するカスタマーゲートウェイの間にIPsec暗号化トンネルを確立する必要があります。



ローカルIDCへの接続

VPCをローカルIDCに接続して、ハイブリッドクラウドを構築することができます。 Alibaba Cloud上のVPCとIDC、大規模なコンピューティング、ストレージ、ネットワーク、CND、GBPリソースの間の安全で信頼性の高い接続により、必要に応じてローカルITインフラストラクチャ

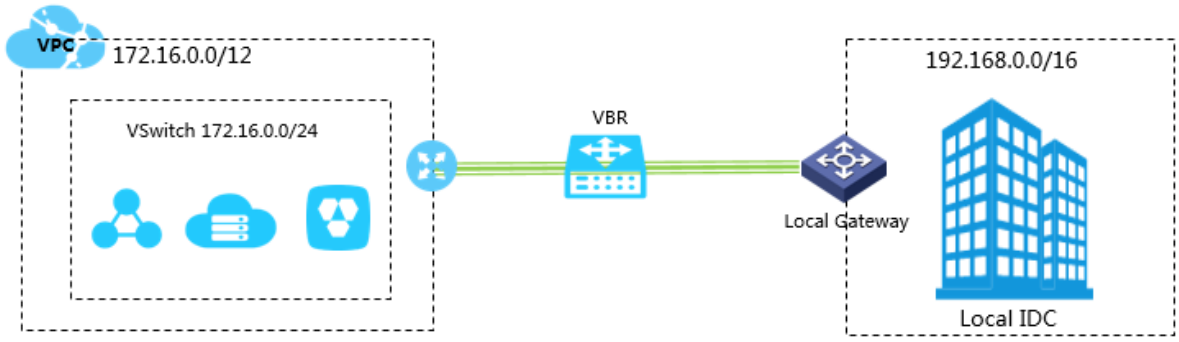
をAlibaba Cloudにシームレスに拡張し、リアルタイムでサービスの変動に対処することができます。

Express Connect、VPNゲートウェイまたはCENを通してローカルIDCをVPCに接続できます。

- Express Connect

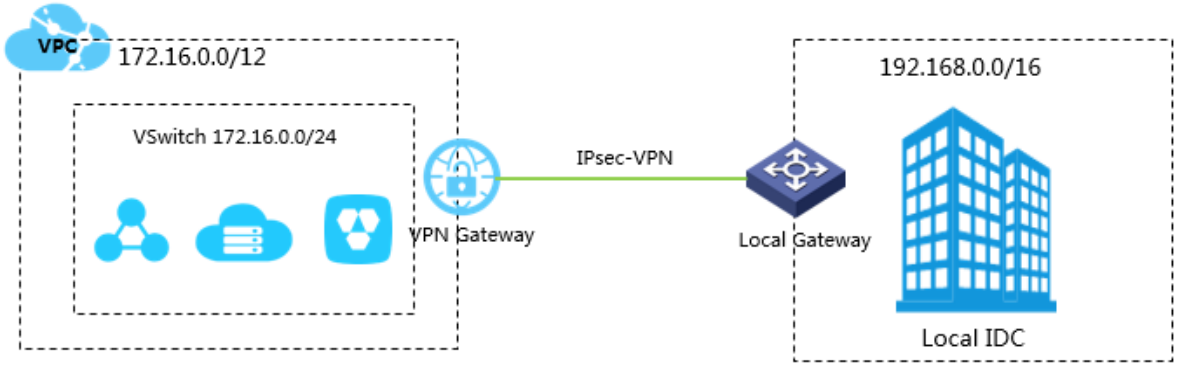
  Express Connectは物理コネクション機能を提供しています。 専用回線をAlibaba Cloudアクセスポイントにアクセス後、VBRとVPC間のピア接続を作成してハイブリッドクラウドを構築することができます。

  専用回線のイントラネットコネクションはインターネットを経由しません。 それにより、従来のインターネット接続と比較すると、物理コネクションは更なる高安全性、高信頼性、高速度及び低遅延を提供しています。



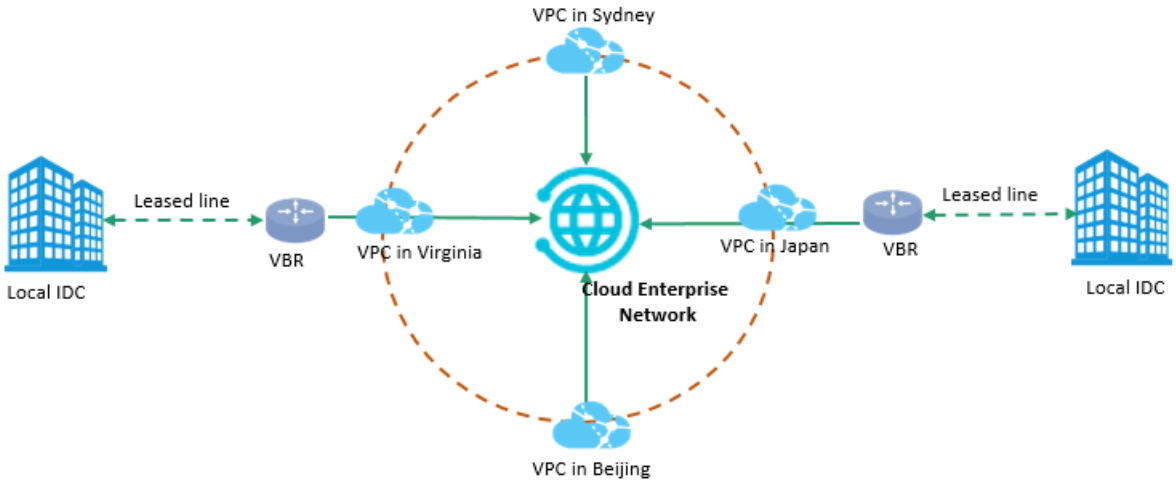
- VPNゲートウェイ

  VPNゲートウェイは、インターネットベースの暗号化されたチャネルを通じて、ローカルデータセンター、ローカルサイト、インターネットターミナルをVPCに安全かつ確実に接続できます。 VPNゲートウェイには、アクティブ/スタンバイホットバックアップを提供する2つの異なるゲートウェイインスタンスが含まれています。 アクティブノードに障害が発生すると、トラフィックは自動的にスタンバイノードに分散されます。 IPsec-VPNを使用してローカルデータセンターをVPCに接続できます。



- クラウドエンタープライズネットワーク（CEN）

  CENを使用することで、ルーターの自動ラーニング及び配布機能により、異なった地域のVPCとローカルデータセンターの間で、安全でプライベートなエンタープライズレベルの相互接続ネットワークを構築できます。 CENインスタンスにローカルIDCに関連付けられたVBRを接続するだけで、ローカルIDCはCENインスタンスに接続されたすべてのネットワーク（VPCまたはVBR）と通信できます。

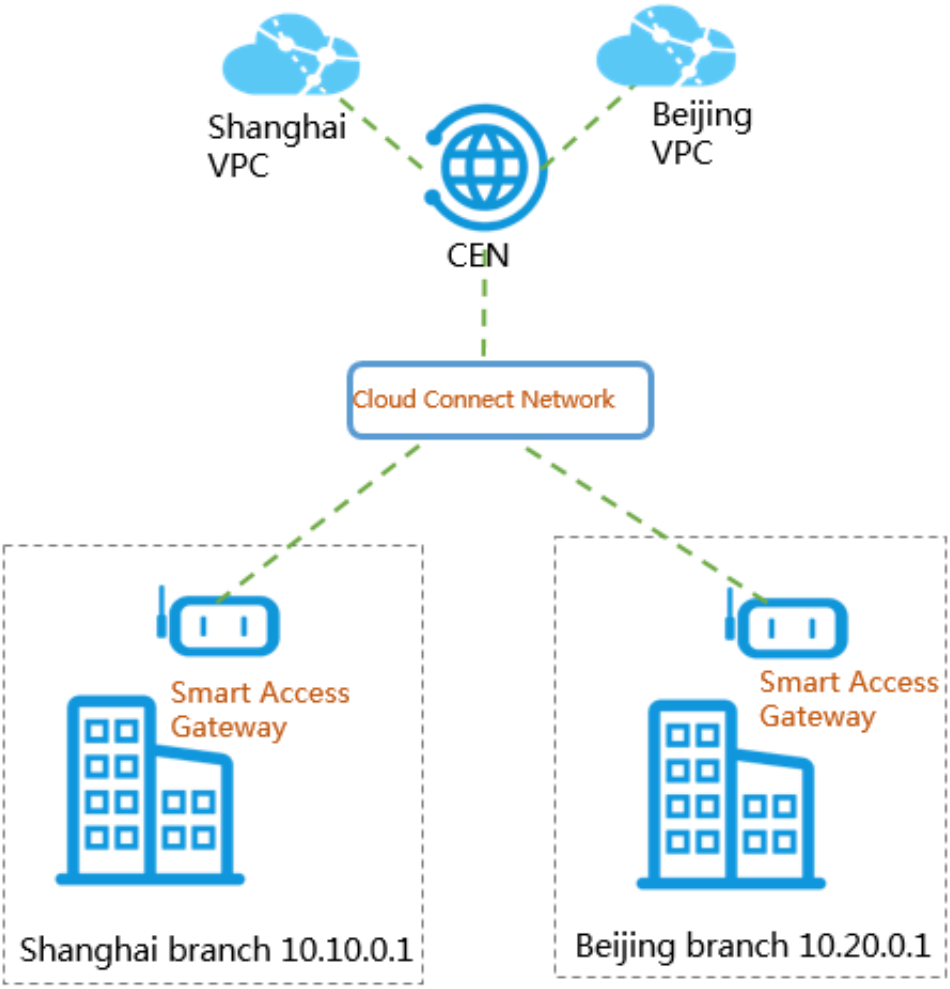


- スマートアクセスゲートウェイ

  スマートアクセスゲートウェイは、ローカル組織をAlibaba Cloudに接続するためのワンストップソリューションです。 スマートアクセスゲートウェイを使用することで、企業はインターネットを通して暗号化された方法でAlibabaクラウドにアクセスすることができ、よりイ

ンテリジェントで、高信頼性で、安全なAlibaba Cloudへのアクセス体験を得ることができます。

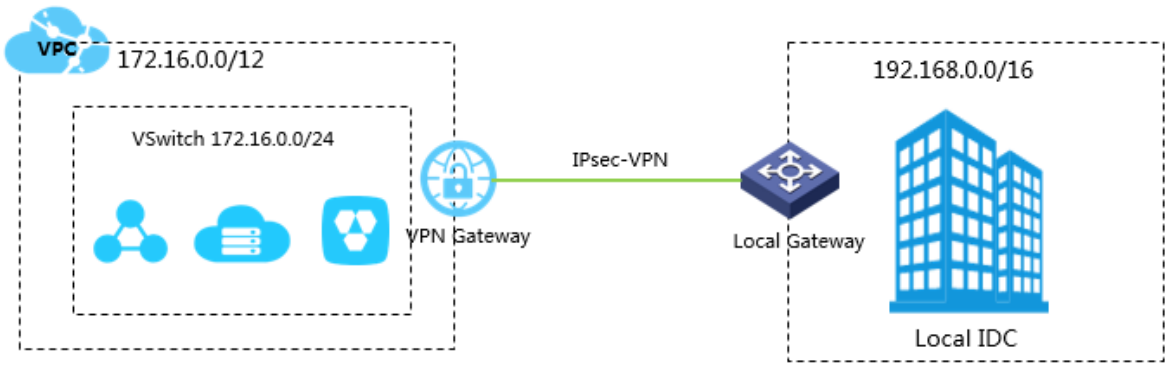
ローカルデータセンター用のスマートアクセスゲートウェイデバイスを購入し、スマートアクセスゲートウェイに関連付けられたCCNインスタンスをCENインスタンスにアタッチすることで、ローカルIDCをAlibaba Cloudに接続できるようになります。



- Alibaba Cloud Marketplace内のVPNソフトウェア

  Alibaba Cloud Marketplaceは、さまざまなVPNソフトウェアまたはイメージデータを提供しています。 Alibaba Cloud MarketplaceからVPNソフトウェアを購入して、ECSインス

タンスにデプロイできます。 そうすればEIPを使用してVPCをインターネット経由でローカルIDCのカスタマーゲートウェイに接続することができます。



複数のサイトの接続

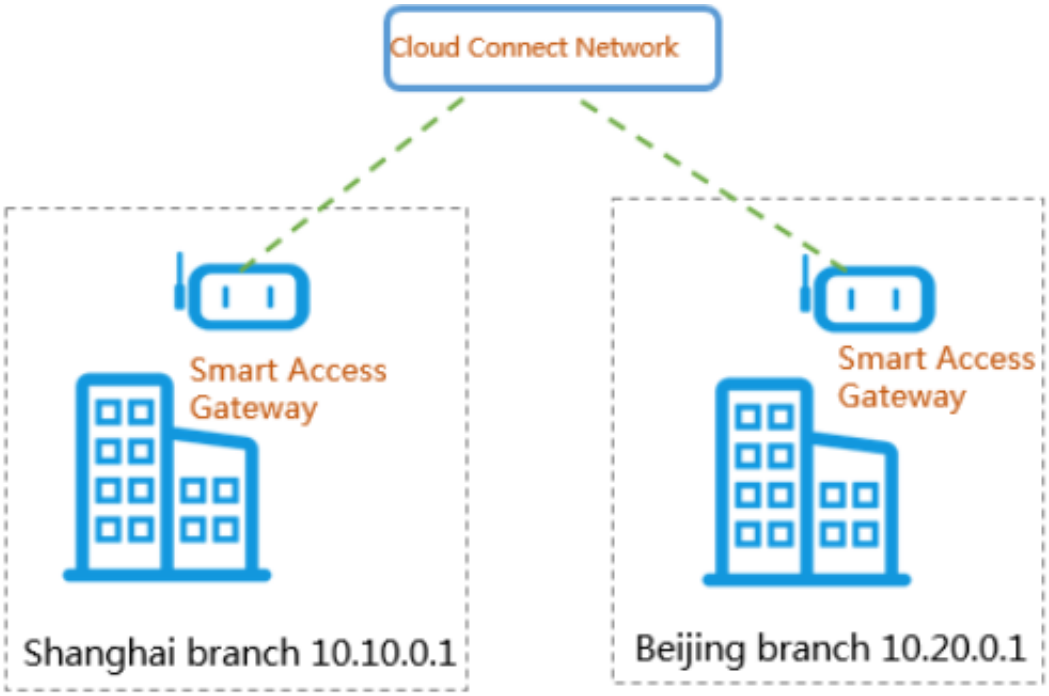
Smart Access GatewayまたはVPNゲートウェイのVPNハブ機能を使用して複数のサイトを接続できます。

- スマートアクセスゲートウェイ

  スマートアクセスゲートウェイは、ローカル組織をAlibaba Cloudに接続するためのワンストップソリューションです。 スマートアクセスゲートウェイを使用することで、企業はインターネットを通して暗号化された方法でAlibabaクラウドにアクセスすることができ、よりイ

ンテリジェントで、高信頼性で、安全なAlibaba Cloudへのアクセス体験を得ることができます。

ローカルブランチ用のスマートアクセスゲートウェイデバイスを購入し、CENを通じてデバイスを接続することができます。それによりローカルブランチが相互に通信できるようになります。



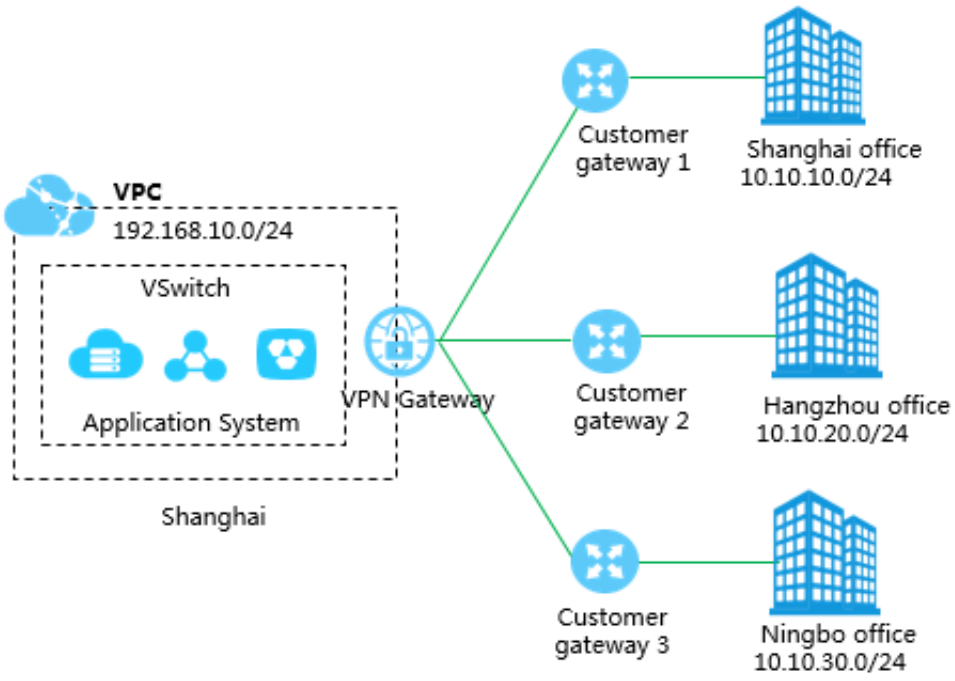
- 複数のローカルサイトを接続

  VPNゲートウェイのIPsec-VPN機能は、サイト間のVPN通信を提供しています。 各VPNゲートウェイには10のIPsec-VPNコネクションに対応しています。 それにより、VPN Gatewayを購入して、10のIDCまたは異なった地域のローカルサイトを接続することができます。

  VPNハブ機能を使用すると、複数のサイト間で安全な通信を確立できます。 サイトは、接続されたVPCとの通信のみならず、お互いにでも通信することができます。 VPNハブは、大規模企業のニーズを満たし、さまざまなサイト間でイントラネット通信を確立します。

  VPNハブ機能はデフォルトで有効にしています。 各オフィスサイトとAlibaba Cloudの間のIPsec-VPN接続を構成するだけで済みます、また追加料金は請求されません。 1つのVPNゲートウェイは最大10のIPsecコネクションに対応しています。 よって、1つのVPNゲートウェイでは最大10のオフィスサイトを接続することができます。 次の図に示すように、3つの

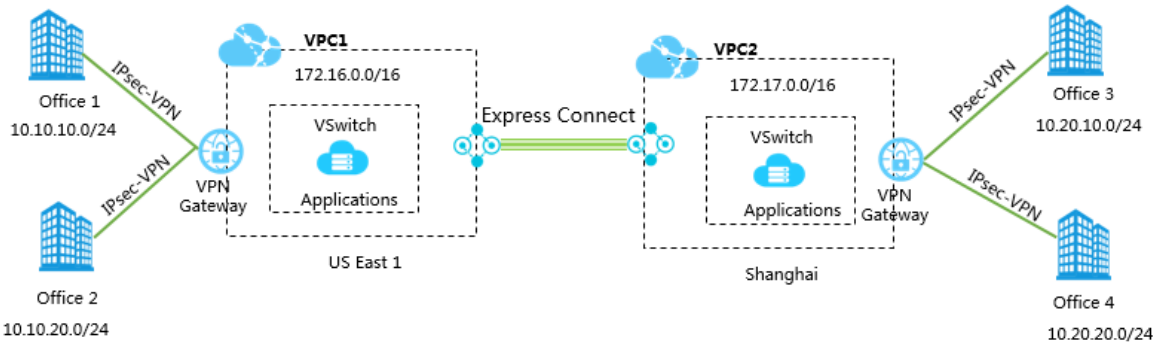
オフィスサイト（上海、杭州、寧波）を接続するには、VPNゲートウェイと3つのカスタマーゲートウェイを作成し、3つのIPsec接続を確立する必要があります。



- 高速度グローバルネットワークの構築

  VPNゲートウェイとExpress Connectを通して世界中のアプリケーションシステムとオフィスサイトを接続できます。 この方法には高安全性、高品質ネットワーク、低コストなどの特徴があります。

  次の図に示すように、米国（バージニア州）のオフィスサイトと上海のオフィスサイトを接続するには、米国東部のVPCと上海のVPCにそれぞれアプリケーションシステムをデプロイし、VPCの間でExpress Connectを通して接続し、 2つのリージョンのオフィスサイトはIPsec-VPNを通して2つのVPCに接続します。



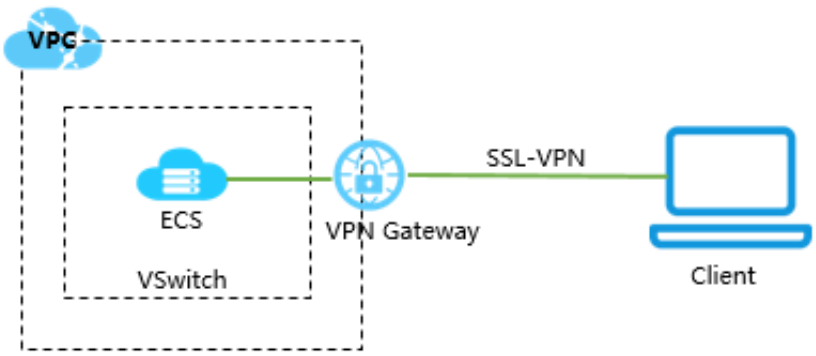
VPCへのリモートアクセス

VPNゲートウェイのSSL-VPN機能は、サイト間のVPNコネクションを提供しています。 端末は、カスタマーゲートウェイを構成することなしに、VPCに直接アクセスできます。 ローカル内部アプリケーションをVPCにデプロイし、内部スタッフがSSL-VPNを通して内部システムにアクセスすることができます。 たとえば、ローカルITスタッフは、イントラネットを通してVPCにアクセスし操作とメンテナンスを行い。、出張中のスタッフはリモートサイトを通してVPCのローカルアプリケーションにアクセスできます。

VPNゲートウェイまたはAlibaba Cloud MarketplaceのVPNソフトウェア/イメージデータを使用することで、VPCへのリモートアクセスを実現できます。

- VPNゲートウェイ (SSL-VPN)

  SSL-VPNコネクションを作成して、リモートクライアントをVPCにデプロイされたアプリケーションに接続することができます。 デプロイメントの完了時、クライアントで証明書をロードして接続を開始するだけで済みます。 VPNゲートウェイには、アクティブスタンバイホットバックアップ機能を提供する2つの異なるゲートウェイインスタンスが含まれています。 アクティブノードに障害が発生すると、トラフィックは自動的にスタンバイノードに分散されます。



- Alibaba Cloud MarketplaceでSSL-VPNソフトウェアの購入

  Alibaba Cloud MarketplaceでSSL-VPNソフトウェアまたはイメージデータを購入し、VPC内のEIPにバインドされたECSインスタンスにSSL-VPNをデプロイすることで、リモートクライアントからインターネットにアクセスできます。

3 インターネット向けプロダクトの選び方

VPCネットワークでは、Elastic IPアドレス（EIP）、NATゲートウェイ、インターネットサーバーロードバランサー（SLB）、及びECSインスタンスのパブリックIPを使用してインターネットへアクセスできます。

パブリックIPアドレス

Alibaba Cloudには、ECSインスタンスのパブリックIP、NAT帯域幅パッケージのパブリックIP、インターネットSLBインスタンスのパブリックIP、VPNゲートウェイのパブリックIPなど、さまざまなパブリックIPアドレスがあります。 パブリックIPアドレスの一元的な管理を簡単に実行するため、ECS、NAT Gateway、およびSLBは、EIPにバインドできるようになりました。

インターネット向けプロダクト

次の表に、利用可能なインターネット向けプロダクトと対応する機能を示します。

プロダクト	機能	メリット
ECS 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。しかし、ECSインスタンスからパブリックIPをバインド/バインド解除することはできません。	None
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。

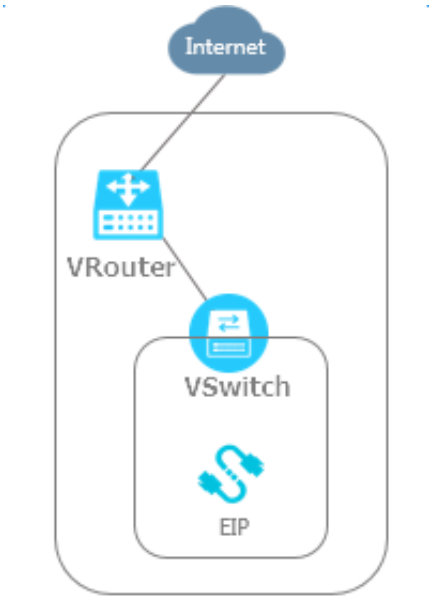
プロダクト	機能	メリット
NATゲートウェイ	NATゲートウェイはエンタープライズ級のインターネットゲートウェイであり、複数のECSインスタンスが一つのEIP（SNAT）を通してのインターネットへのアクセスや、インターネット（DNAT）からのアクセスを対応しています。 注： SLBに比べ、NATゲートウェイ自体はトラフィックの負荷分散機能を提供していません。	NATゲートウェイとEIPの根本的な違いは、NATゲートウェイは複数のECSインスタンスのインターネット接続を対応しているが、EIPは一つのECSインスタンスのみのインターネット接続を対応している。
Server Load Balancer	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。 SLBは、構成された転送ルールに従って、複数のECSインスタンスの間の着信トラフィック負荷を分散するトラフィック分散制御サービスです。 アプリケーションサービスの能力を拡張し、アプリケーションの可用性を高めます。

シナリオ1：外部サービスの提供

- 単一ECSインスタンスで外部サービスを提供します

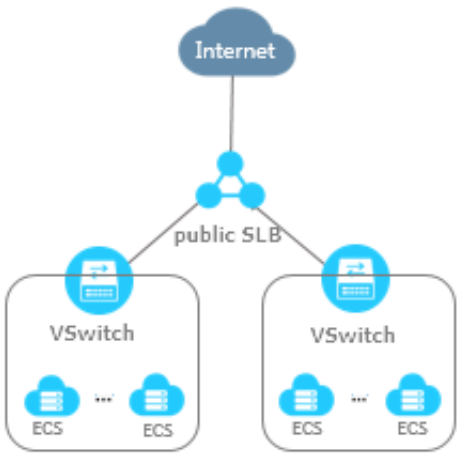
  アプリケーションが1つしかなく、事業の規模が大きくなければ、単一ECSだけでもご希望の要件を満たせます。 このECSには、アプリケーション、データベース、ファイルをデプロイす

ることができます。 そしてECSインスタンスにEIPをバインドすれば、 ユーザーがインターネットを通してデプロイされたアプリケーションにアクセスできるようになります。



- レイヤ4ロードバランシング付きの外部サービスを提供

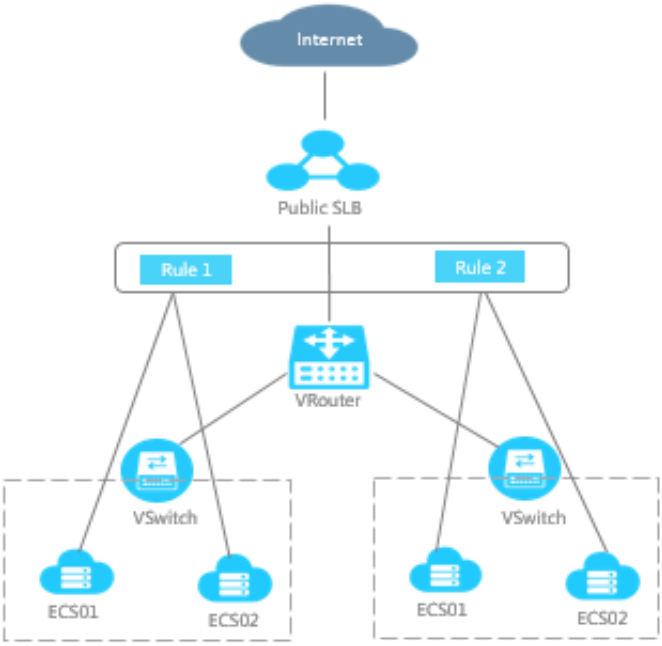
  トラフィックが大量発生する場合は、ECSがすべてのアクセストラフィックに対応することはできません。 複数のECSインスタンスを配置する必要があります。 このような状況では、レイヤー4リスナー付きのインターネットSLBインスタンスを配置し、これらのECSインスタンスをバックエンドサーバーとして追加するだけで良いです。



- レイヤー7ロードバランシング付きの外部サービスを提供

  基本的なトラフィック分散機能に加え、異なった業務トラフィックを異なったバックエンドサーバーに配布する場合、レイヤー7リスナーにURL転送ルールを追加することができます。

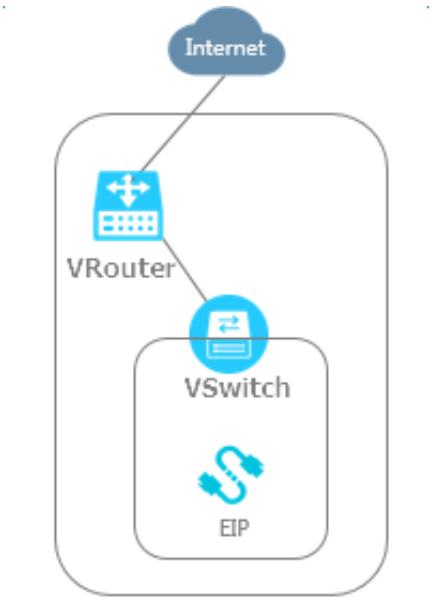
このような状況では、レイヤー7リスナー付きのインターネットSLBインスタンスを配置し、これらのECSインスタンスをバックエンドサーバーとして追加するだけで良いです。



シナリオ2：パブリックIPなしでECSインスタンスのインタネットへのアクセス

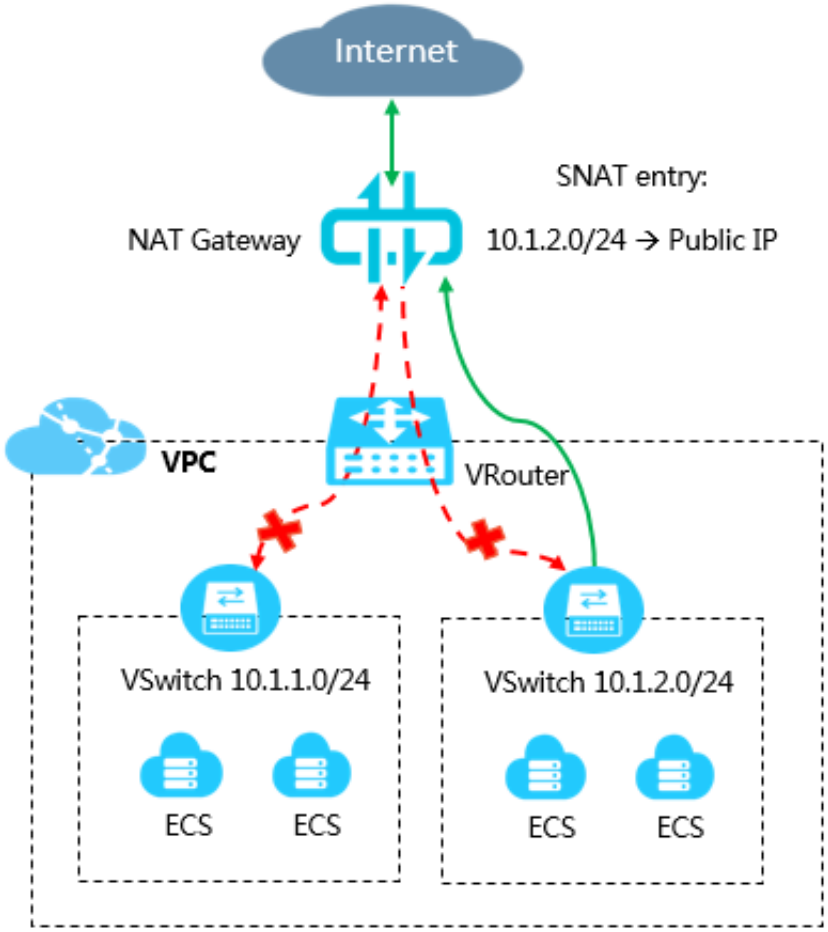
- EIPのバインド

  ECSインスタンスの所有量が少ない場合、各ECSインスタンスに1つのEIPをバインドすることができます。 そうすれば、ECSインスタンスはEIPを使用してインターネットにアクセスできます。 インターネットアクセスが不要になった場合は、いつでもECSインスタンスからEIPをバインド解除できます。



- NATゲートウェイを使用してのSNATエントリーの構成

  ECSインスタンスを多数所有し、各ECSインスタンスにそれぞれEIPをバインドする場合は、管理コストが高くなります。 さらに、ユーザーもEIPでインターネットを通してECSインスタンスにアクセス可能になってしまいます。 このような状況では、VSwitch内のECSインスタンスのためにSNATエントリーを構成してインターネットにアクセスすることをお勧めします。DNATエントリーの構成をしないでください。 そうすれば、ECSインスタンスはインターネットにアクセスできるようになりますが、ユーザーがインターネットを通してECSインスタンスにアクセスすることはできません。詳細は次を参照してください。



4 インターネットコストの削減方法

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。

データ転送プラン

データ転送プランは、サブスクリプション方式のインターネットトラフィックパッケージです。それは従量課金制よりも低い価格を提供し、またアイドル時間データ転送プランを提供し、インターネットトラフィックコストを大幅に削減します。 データ転送プランは、トラフィックにより請求される ECS インスタンス、EIP、および SLB インスタンスに適用されます。

データ転送プランを購入すると、トラフィック料金がプランから自動的に差し引かれ、追加の操作は必要ありません。 請求管理 - リソースパッケージで、さまざまな商品のデータ転送プランの使用状況を確認できます。

このセクションでは、次の観点からデータ転送プランを分析します：

・ データ転送プランはコストをどれくらい削減できますか？

データトラフィックパッケージは、低価格でアイドル時間データ転送プランをサポートします。 香港リージョンで例えると、 従量課金制トラフィック、フルタイムデータ転送プラン、およびアイドルタイムデータ転送プランの価格は次のとおりです。

例として、香港リージョンの 5 TB データ転送プランをとります。 コスト比較は次の通りです。 データ転送プランでトラフィックコストを多く削減していることがわかります。

香港 5 TB のトラフィック	単価（元/ GB）	合計金額（元）	削減したコスト（元）	削減したコストの割合
従量課金トラフィック	1	5120	0	0

香港 5 TB のトラフィック	単価（元/ GB）	合計金額（元）	削減したコスト（元）	削減したコストの割合
フルタイムデータ転送プラン	0.75	3727	1393	27.2%
アイドルタイムデータ転送プラン	0.51	2609	2511	49%

- データ転送プランの使用シナリオは？

  トラフィックによって請求されるすべての ECS インスタンス、EIP、および SLB インスタンスは、データ転送プランを使用できます。 コスト削減の観点からすると、データ転送プランはトラフィックの多いリソースに対してより多くのコストを削減します。

- データ転送プランの説明

  - データ転送プランには有効期間があります。 プランが期限切れになると、プラン内のトラフィック残量は使用できなくなります。 サービスシステムの使用状況履歴に応じてデータ転送プランの仕様を選択することをお勧めします。 浪費を避けるために最初は小仕様のプランを購入し、必要に応じて購入量を増やすことができます。
  - データ転送プランを使い切ると、さらに使用されたトラフィックは従量課金制として請求され、サービスは中断されません。
  - 複数のデータ転送プランを購入した場合、最初に期限切れになるデータ転送プラン内のトラフィックが優先に差し引かれます。

インターネット共有帯域幅への追加

インターネット共有帯域幅は、高品質のマルチライン BGP 帯域幅とさまざまな請求方法を提供する独立した帯域幅製品です。 EIP が帯域幅を共有できるように、EIP をインターネット共有帯域幅に追加できます。 EIP を VPC ネットワークの ECS インスタンス、NAT ゲートウェイ、および VPC ネットワークの SLB インスタンスにバインドして、これらの製品がインターネット共有帯域幅を使用できるようにすることができます。

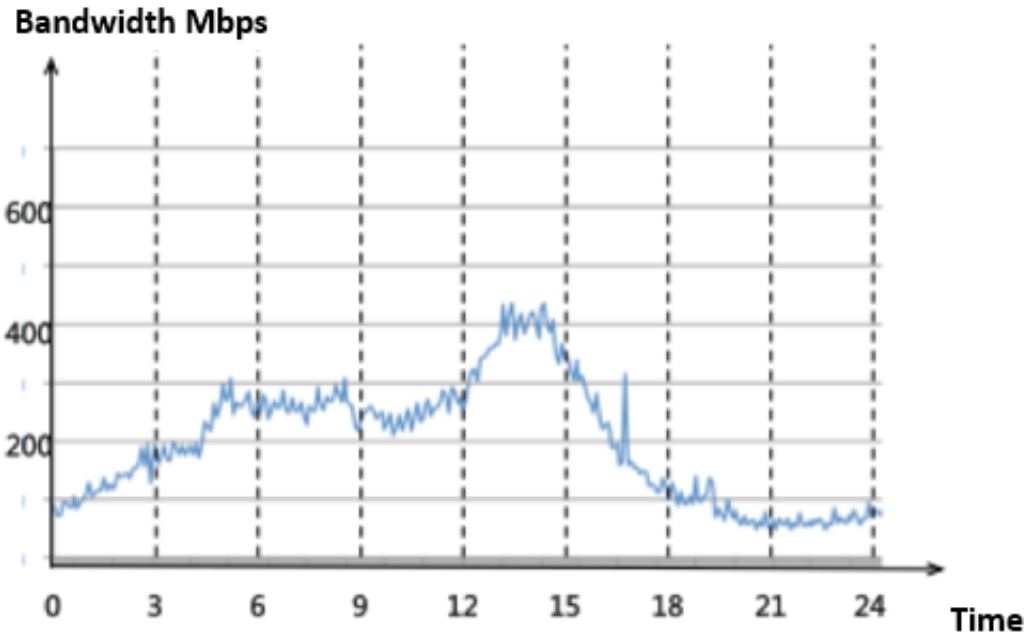
その上、インターネット共有帯域幅は 95 請求、固定帯域幅による請求などを含む豊富な請求方法を提供します。 インターネット共有帯域幅と豊富な請求方法を使用すると、帯域幅コストを効果的に削減し、強力で柔軟なサービス機能を提供できます。 インターネット共有帯域幅について、画像一枚でわかるインターネット共有帯域幅をご参照ください。

 注：

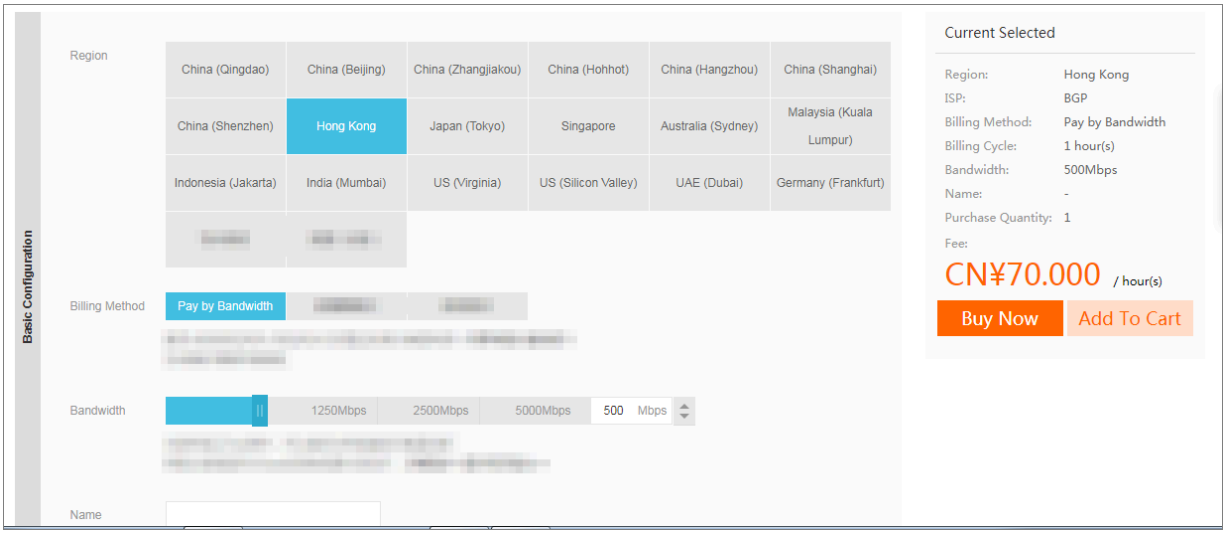
インターネット共有帯域幅は、デフォルトでパブリック IP が含まれない独立した帯域幅製品です。 インターネット共有帯域幅に EIP を追加できます。

インターネット共有帯域幅の帯域幅共有機能は、特に帯域幅の変動が大きい場合に、インターネットの帯域幅コストを削減するのに役立ちます。 香港に ECS インスタンスが 10個 あり、すべてのインスタンスが EIP にバインドされているとします。 帯域幅による課金が採用されている場合、ピーク帯域幅は 100 Mbps です。 次の図に示すように、3253 元/日を支払う必要があります。これは、100 Mbps のピーク帯域幅で 10個の EIPのコストです。

10 個のパブリック IP のトラフィック分析は、サービスが帯域幅変動によって異なることを示しています。 次の図に示すように、10 台のサーバーの最大送信帯域幅は約 500 Mbps です。



そのため、インターネット共有帯域幅を使用する場合は、500 Mbps のインターネット共有帯域幅を購入するだけで、10 個のECSインスタンスで使用できます。 このように、1 日あたり 1680 元の 500 Mbps の帯域幅のコストを支払うだけで、各 ECS インスタンスは元より 5 倍のピーク帯域幅を使用できます。 よって、50% の帯域幅コストの 1573 元が削減されます。



インターネット共有帯域幅は、95 請求と「無制限」のピーク帯域幅も提供します。 料金は、急激ピーク帯域幅を引いた実際の帯域幅使用量によって計算されます。 このようにして、帯域幅コストが削減され、限られた帯域幅がサービスに与える影響が回避されます。 帯域幅の変動が大きいユーザーにとって、適切なピーク帯域幅を予測することは特に困難です。 高いピーク帯域幅は無駄になる原因となります。また、ピーク帯域幅が低くなるとパケット損失が発生し、さらにサービス開発やユーザーエクスペリエンスに影響を与えます。 この場合、95 請求を選択できます。

そうすれば、複数の EIP があり、明らかな帯域幅の変動がある場合は、インターネット共有帯域幅を使用するとコストを大幅に削減できます。 頻繁に急激な帯域幅のピークに遭遇するサービスに対して 95 請求を選択することができます、そうすればサービスに対する限られたピーク帯域幅の影響と高いピーク帯域幅によって引き起こされるコストの浪費は避けられます。

注：

適切な請求モードを選択するには、システムのトラフィックモデルを分析する必要があります。

- トラフィックが安定しているシステムでは、帯域幅別にサブスクリプション 課金モードを選択できます。帯域幅別に従量課金制と比べれば、20%~30% のコストを削減できます。
- ご提供するサービスは頻繁に急激な帯域幅のピークを経験しているのであれば、95 請求を選ぶことをお勧めします。

5 VPC内のクラウドプロダクトの使用方法

ほとんどのクラウドプロダクトはVPCネットワークに対応しています。 クラウドリソースの作成する段階でVPCネットワークを選択することと、VPCを作成してから、VPCでクラウドリソースを作成することの、いずれにしましてもかまいません。

VPCの使用方法

VPC は分離されたプライベートネットワークです。 デフォルトでは、異なったVPCの間でイントラネットを通して相互に通信することはできません。 VPC内のECSインスタンスはインターネットにアクセス、またはインターネットからアクセスされることはできませんし、イントラネット経由でクラシックネットワークにアクセスすることもできません。 Alibaba Cloudは、インターネットとイントラネットへのアクセスを可能にする多くの接続オプションを提供しています。

> 注 :
> イントラネット通信を必要とするクラウドプロダクトは、同一ネットワークタイプを使用する必要があります。 たとえば、VPCネットワーク内のECSインスタンスがイントラネットを通してSLBインスタンスまたはRDSインスタンスにアクセスする必要がある場合、SLBインスタンスとRDSインスタンスもVPCネットワークを使用しなければなりません。

異なるクラウドプロダクトの場合、VPCの使用方法は異なります。

- 購入ページでVPCの使用を選択します

  この方法は、主にECS、RDS、SLBなどのクラウドプロダクトに適用されます。 これらのクラウドプロダクトは、さまざまなネットワークオプションを提供しています。 インスタンスの購入時に使用するVPCを選択できます。 インスタンスの作成後、プライベートIPアドレスまたはプライベートエンドポイントがインスタンスに割り当てられます。
- コンソールでVPCの使用を選択します

  この方法は、Table Store、Container Service、E-MapReduce及びNetwork Attached Storageなどのクラウドプロダクトに適用されます。

  Table StoreコンソールでTable Storeインスタンスの VPCエンドポイントを設定し、コンソールにContainer Serviceクラスタまたは E-MapReduceクラスタの作成時にVPCの使用を選択できます。

- VPCエンドポイントの提供

  これはLog ServiceやObject Storage Serviceなどのクラウドプロダクトに適用されます。

  次のプロダクトのヘルプドキュメントを確認できます：

  - *Log ServiceのVPCエンドポイント*
  - *Object Storage Serviceの VPCエンドポイント*

ネットワークタイプの変更方法

- ApsaraDB for RDSなどの一部のインスタンスクラウドプロダクトは、コンソールでネットワークタイプをクラシックネットワークからVPCに変更することができます。
- SLBはネットワークタイプの変更に対応していません。 VPCネットワークのSLBインスタンスを購入して、VPCタイプのECSインスタンスを追加することができます。

詳細は次を参照してください移行方法概要。

6 クラシックネットワークからVPCへの移行

6.1 移行方法概要

クラシックネットワークにデプロイされたリソースをVPCネットワークに移行することができます。 VPCは分離されたネットワーク環境で、安全性が高いです。

VPCへ移行する理由は？

仮想プライベートクラウド(VPC)はAlibaba Cloudでのお客様専用のプライベートネットワークです。 お客様はご自身のVPC内のAlibaba Cloudリソース、及びプロダクトを使用することができます。 VPCには次のような利点があります：

- 安全で分離されたネットワーク環境

  VPCはトンネリング技術に基づき、データリンク層を分離し、各ユーザーに独立で隔離されたネットワークを提供しています。 異なったVPCの間は完全に分離しています。

- 制御可能なネットワーク構成

  お客様にはご自身のVPCネットワークに完全な制御権を持っています。 IPアドレス範囲の指定、サブネットの作成、ルートテーブルやゲートウェイの設定などができます。 また、VPCを専用回線またはVPN経由でローカルIDCネットワークに接続して、Alibaba Cloudにアプリケーションのスムーズな移行、ローカルIDCのネットワークトポロジの拡張などに対応できるようにするための、オンデマンドネットワーク環境を構築することができます。

移行の方法は？

次の2つの方法でシステムをVPCネットワークに移行することができます。 この2つの方法のいずれも単独で使用するか、組み合わせで使用することができます、様々な移行シナリオに対応しています。

- ハイブリッド追加及びハイブリッドアクセスでの移行

  システムはRDS、SLB、または他のクラウドプロダクトにデプロイされている場合、この方法をお勧めします。 サービスを中断することなくシステムをVPCネットワークに移行できるシームレスな移行ソリューションです。

  ClassicLink機能を使用して、クラシックネットワーク内のECSインスタンスはVPCネットワーク内のリソースにアクセスできます。 詳細は次を参照してください*ClassicLink概要*。

・ 単一ECSの移行

アプリケーションはECSインスタンスにデプロイされ、ECSインスタンスの再起動はシステムに影響を与えない場合は、この方法をお勧めします。

ハイブリッドアクセス及びハイブリッド追加

ハイブリッドアクセスとハイブリッド追加はシームレスな移行方法です。 まず、移行先のVPCネットワーク内にECSなどのクラウドリソースを新規作成して、この方法を使用してシステムをスムーズにVPCに移行します。 すべてのリソースがVPCに移行後、クラシックネットワーク内のクラウドリソースをリリースして、すべての移行プロセスを完了させます 詳細は次を参照してくださいハイブリッド追加とハイブリッドアクセス方式での移行の例。

・ ハイブリッド追加

ハイブリッド追加とは、SLBがクラシック、及びVPCネットワーク両方のECSインスタンスをバックエンドサーバーとして追加し、転送された要求の処理に対応していることを意味します。 仮想サーバーグループもハイブリッド追加に対応しています。

インターネット及びイントラネットSLBの両方もハイブリッド追加に対応しています。

> 注：
> クラシックECSインスタンスとVPC ECSインスタンスを同時にイントラネットSLBインスタンスに追加し、レイヤー4（TCP及びUDPプロトコル）リスナーを構成することで、VPCネットワーク内のECSインスタンスクライアントの実IPアドレスを取得できるようになります。（クラシックECSインスタンスでは取得できません） レイヤー7リスナーには関係なく、 バックエンドサーバーのネットワークタイプを問わず、実IPアドレスを取得できます。

・ ハイブリッドアクセス

RDS、OSSなどのクラウドプロダクトがハイブリッドアクセスに対応しています。つまり、クラシックネットワーク及びVPCネットワーク内のECSインスタンスに同時にアクセスされることに対応しています。 一般的に、この類のプロダクトには2つのエンドポイントがあり、1つはクラシックネットワークへのアクセス用で、もう1つはVPCネットワークへのアクセス用です。

この方法を使用するには次の点に注意してください：

・ この方法は大概のシステムの移行要件を満たしています。 クラシックネットワーク内のECSインスタンスはVPCネットワーク内のクラウドリソースに通信する必要がある場合、ClassicLink機能を使用します。

・ この方法は、システムをクラシックネットワークからVPCネットワークへの移行にのみ使用されます。

6.2 データベースハイブリッドアクセス

6.2.1 ApsaraDBのハイブリッドアクセス

ハイブリッドアクセスとは、クラシックネットワーク内、及びVPCネットワーク内のECSインスタンスが両方データベースにアクセスできることを意味しています。 ハイブリッドアクセス/バイアス方法を使用してAsaraDBをクラシックネットワークからVPCネットワークに移行するには、ApsaraDBをハイブリッドアクセスモード（クラシックネットワークエンドポイントとVPCエンドポイントを同時に保留すること）に切り替える必要があります、そうすれば移行中のサービス中断を避けることができます。

ApsaraDBをVPCに移行する際には、クラシックネットワークエンドポイントの保留時間を指定できます。 クラシックネットワークエンドポイントは、時間に達すると自動的にリリースされます。

次のApsaraDBのハイブリッドアクセスの制限事項をご注意ください。

・ 現時点では、次のデータベースがハイブリッドアクセスに対応しています：

- 安全接続モードでのApsaraDBのRDS MySQL、SQL Server、PPAS、及びPostgreSQL
- ApsaraDB for Redis/Redisクラスタバージョン
- ApsaraDB for Memcache新バージョン（2017年5月12日後に購入）
- ApsaraDB for MongoDBレプリカセット

  MongoDBインスタンス、RDSインスタンス、Redisインスタンスの場合は、コンソールまたはAPIを使用してネットワークタイプを変更できます。 クラシックネットワークエンドポイントは変更されず、スイッチオーバー後にVPCエンドポイントが追加されます。 クラシックネットワークエンドポイントとVPCネットワークエンドポイントをコンソールで確認できます。

  Memcacheインスタンスの新バージョンに対しては、APIを使用して移行する必要があります。 現時点では、コンソールでネットワークタイプを変更後、クラシックネットワークエンドポイントを保留することはできません。 クラシックネットワークエンドポイントは変更されず、スイッチオーバー後にVPCエンドポイントが追加されます。 コンソールには、VPCネットワークエンドポイントのみが表示されます。 クラシックネットワークエンドポイントを確認するには、APIを使用する必要があります。

- 現時点では、次のデータベースはハイブリッドアクセスに対応していません：
  - 標準ネットワークモードにあるApsaraDB for RDS。 ネットワークタイプを変更するには、安全接続モードに切り替えてください。
  - ApsaraDB for MongoDBクラスタバージョン。
  - ApsaraDB for Memcache以前のバージョン（2017年5月12日前に購入）。 ネットワークタイプを変更するには、新しくインスタンスを購入し、ApsaraDB for Memcacheの新バージョンに移行します。

6.2.2 ApsaraDB for RDSのネットワークタイプの変更

本ドキュメントでは、 ApsaraDB for RDSのネットワークタイプをコンソールまたはAPI経由でVPCに変更し、クラシックネットワークエンドポイントを保持する方法を紹介します。

詳細は、クラシックネットワークからVPCへの移行を参照してください。

> 注：
>
> - クラシックネットワークエンドポイントには有効期限があります。 必要に応じて有効期限を指定することができます。 指定した期限に達すると、クラシックネットワークエンドポイントはシステムにより自動的に削除されます。 エンドポイントが削除される前に、通知メッセージが届きます。
> - RDSインスタンスがDRDSインスタンスのブランチデータベースである場合、DRDSとRDSインスタンスの間のネットワーク接続は中断され、再接続する必要があります。

前提

- インスタンスのアクセスモードは安全接続モードである必要があります。 詳細は、アクセスモードの設定を参照してください。 MySQL 5.7、SQL Server 2012及びSQL Server 2016はスタンダードモードにのみ対応しています。 このモードではネットワークタイプの変更に対応しています。
- ネットワークタイプはクラシックネットワークである必要があります。
- RDSインスタンスが配置されているゾーンには、使用可能なVPCとVSwitchがある必要があります。 詳細は次を参照してくださいVPCの管理。

コンソールでネットワークタイプを変更します。

1. RDSコンソールにログインします。
2. インスタンスが配置されたリージョンを選択します。
3. 対象インスタンスのIDをクリックします。
4. 左側のメニューで、データベース接続を選択します。

5. インスタンス接続タブで、VPCへ切り替えをクリックします。
6. VPCへ切り替えページで、RDSインスタンスが配置されているVPCとVSwitchを選択します。
7. オリジナルクラシックエンドポイントを保留チェックボックスにチェックを入れ、 有効期限を選択します。
   - クラシックネットワークエンドポイントが削除される前の7日間で、システムは毎日アカウントにバインドされた携帯電話に通知メッセージを送信します。
   - クラシックネットワークエンドポイントが期限切れになると、システムにより自動的削除され、クラシックネットワークエンドポイント経由でのデータベースアクセスはできなくなります。 サービスの中断を防ぐため、必要に応じて保持期間を設定します。 ハイブリッドアクセスを設定後、有効期限を変更できます。
8. OKをクリックすれば。 保持されたクラシックネットワークの接続アドレスがコンソールに追加されます。

有効期限の変更

クラシックネットワークエンドポイントの保持期間を設定後、有効期限が切れる前ならいつでもコンソールを使用して保持期間を延長できます。

ハイブリッドアクセス期間中は、必要に応じてクラシックネットワークエンドポイントの保持期間をいつでも変更できます。 有効期限は、変更した時点から計算されます。 たとえば、クラシックネットワークエンドポイントが2017年8月18日までに期限切れになるように設定されています、2017年8月15日にその有効期限を14日後に変更した場合、エンドポイントのリリース日は2017年8月29日になります。

1. RDSコンソールにログインします。
2. 対象インスタンスが配置されたリージョンを選択します。
3. 対象インスタンスのIDをクリックします。
4. 左側のメニューで、データベース接続を選択します。
5. インスタンス接続タブで、有効期限を変更をクリックします。
6. 有効期限を選択してOKをクリックします。

APIを通してのネットワークタイプの変更

1. SDKをダウンロードします。
   - *aliyun-java-sdk-rds-new.zip*
   - *aliyun-python-sdk-rds-new.zip*
   - *aliyun-php-sdk-rds-new.zip*

2. ModifyDBInstanceNetworkTypeAPIを呼び出してネットワークタイプを変更します。

リクエストパラメータ

名前	データ型	必須	説明
Action	String	はい	実行する操作。 有効値： ModifyDBIn stanceNetw orkType
DBInstance Id	String	はい	インスタンスのID。
InstanceNetworkType	String	はい	インスタンスのネットワークタイプ。 ・ VPC ：VPCネットワークのインスタンス。 ・ Classic ：クラシックネットワークのインスタンス。
VPCId	String	いいえ	VPCのID。
VSwitchId	String	いいえ	VSwitchのID。 VPCのIDが指定されている場合、このパラメータも指定する必要があります。
PrivateIpAddress	String	いいえ	VSwitchのCIDRブロックにIPアドレスを入力します。 IPアドレスが入力されていない場合は、システムにより VPC IDとVSwitch IDに従ったイントラネットIPアドレスが割り当てられます。
RetainClas sic	String	いいえ	クラシックネットワークエンドポイントを保持するかどうか。 デフォルト値は False です： ・ True ：保持する ・ False ：保持しない
ClassicExpiredDays	String	いいえ	クラシックネットワークエンドポイントの保持期間。 最短1日、最長120日。デフォルト値は7日。 RetainClassicがTrueに設定されている場合、このパラメータを指定する必要があります。

リターンパラメータ

名前	データ型	説明
RequestId	String	リクエストのID。

名前	データ型	説明
TaskId	String	タスクのID。

コード例

クラシックネットワークエンドポイントを保持しようとする場合は、次のようにしてください：

- **パラメータRetainClassicをTrueに設定します。**
- **パラメータClassicExpiredDaysに値を設定します。 有効期限が切れたクラシックネットワークエンドポイントは削除されます。**

```
import   com . aliyuncs . DefaultAcs  Client ;
 import   com . aliyuncs . IAcsClient ;
 import   com . aliyuncs . exceptions . ClientExce  ption ;
 import   com . aliyuncs . exceptions . ServerExce  ption ;
 import   com . aliyuncs . profile . DefaultPro  file ;
 import   com . aliyuncs . profile . IClientPro  file ;
 import   com . aliyuncs . rds . model . v20140815 .  ModifyDBIn
stanceNetw  orkTypeReq  uest ;
 import   com . aliyuncs . rds . model . v20140815 .  ModifyDBIn
stanceNetw  orkTypeRes  ponse ;
 import   org . junit . Test ;
 public   class   ModifyDBIn  stanceNetw  orkTypeTes  t  {
    @ Test
     public    void   switchNetw  ork_succes  s () {
     ModifyDBIn  stanceNetw  orkTypeReq  uest   request = new
ModifyDBIn  stanceNetw  orkTypeReq  uest  ();
         request . setInstanc  eId ("< Your   instance   ID >");
         request . setInstanc  eNetworkTy  pe  (" VPC ");
         request .  setVPCId ("< VpcId : This   parameter   is
required   when   the   TargetNetw  orkType   is   VPC >");
         request . setVSwitch  Id ("< VSwitchId :  This   parameter
  is   required   when   the   TargetNetw  orkType   is   VPC >");
         request . setRetainC  lassic ("< Whether   to   retain
the   classic   network   endpoint .>");
         request . setClassic  ExpiredDay  s (" The   retention
time   of   the   classic   network   endpoint ");
         IClientPro  file   profile  =  DefaultPro  file .
getProfile (" cn - hangzhou ", "< Your   AK >",
            < Your   Security >");
         IAcsClient   client  =  new   DefaultAcs  Client ( profile
);
     try  {
             ModifyDBIn  stanceNetw  orkTypeRes  ponse   response
                 response  =  client . getAcsResp  onse ( request
);
             System . out . println ( response . getRequest  Id
());
    }  catch  ( ServerExce  ption   e ) {
             e . printStack  Trace ();
    }
        }  catch  ( ClientExce  ption   e ) {
             e . printStack  Trace ();
         }
    }
```

```
}
```

3. DescribeDBInstanceNetInfoAPIを呼び出して、クラシックネットワークエンドポイントとVPCエンドポイントを確認します。

リクエストパラメータ

名前	データ型	必須	説明
Action	String	はい	実行する操作。 有効値： DescribeDB InstanceNe tInfo
DBInstance Id	String	はい	インスタンスのID。

リターンパラメータ

名前	データ型	説明
DBInstance NetInfos	List	インスタンスのネットワーク情報のリスト。
InstanceNe tworkType	String	インスタンスのネットワークタイプ。 ・ VPC ：VPCネットワークのインスタンス。 ・ Classic ：クラシックネットワークのインスタンス。

DBInstanceNetInfo

名前	データ型	説明
Connection String	String	DNSの接続文字列。
IPAddress	String	IPアドレス。
IPType	String	クラシックネットワークインスタンスのIPタイプ： Inner | Public 。 VPCネットワークインスタンスのIPタイプ： Private | Public 。
Port	String	ポート情報。
VPCId	String	VPCのID。
VSwitchId	String	VSwitchのID。

名前	データ型	説明
ExpiredTime	String	期限切れ日時。

コード例

```
import   com . aliyuncs . IAcsClient ;
 import   com . aliyuncs . exceptions . ClientExce  ption ;
 import   com . aliyuncs . exceptions . ServerExce  ption ;
 import   com . aliyuncs . profile . DefaultPro  file ;
 import   com . aliyuncs . profile . IClientPro  file ;
 import   com . aliyuncs . rds . model . v20140815 .  DescribeDB
InstanceNe  tInfoReque  st ;
 import   com . aliyuncs . rds . model . v20140815 .  DescribeDB
InstanceNe  tInfoRespo  nse ;
 import   org . junit . Test ;
 public   class   DescribeDB  InstanceNe  tInfoTest  {
    @ Test
     public    void   describeDB  InstanceNe  tInfo_succ  ess () {
         DescribeDB  InstanceNe  tInfoReque  st   request = new
DescribeDB  InstanceNe  tInfoReque  st ();
         request . setInstanc  eId ("< Your   instance   ID >");
         IClientPro  file   profile  =  DefaultPro  file .
getProfile (" cn - hangzhou ", "<お客様の AK >",
            "<お客様の Security >");
         IAcsClient   client  =  new   DefaultAcs  Client ( profile
);
         try  {
             DescribeDB  InstanceNe  tInfoRespo  nse   response
                 response  =  client . getAcsResp  onse ( request
);
             System . out . println ( response . getRequest  Id
());
    }  catch  ( ServerExce  ption   e ) {
             e . printStack  Trace ();
    }
         }  catch  ( ClientExce  ption   e ) {
             e . printStack  Trace ();
         }
    }
}
```

APIを通してのクラシックネットワークエンドポイントの有効期限の変更

1. SDKのURLをクリックしてSDKをダウンロードします。
   - *aliyun-java-sdk-rds-new.zip*
   - *aliyun-python-sdk-rds-new.zip*
   - *aliyun-php-sdk-rds-new.zip*

2. ModifyDBInstanceNetworkExpireTimeAPIを呼び出し、クラシックネットワークエンドポイントの有効期限を変更します。

リクエストパラメータの説明

名前	データ型	必須	説明
Action	String	はい	必須パラメータ。 値： ModifyDBInstanceNetworkExpireTime .
DBInstanceId	String	はい	対象RDSインスタンスのID。
ConnectionString	String	はい	延期するクラシックネットワーク接続文字列。 文字列型が2種類あります：現行インスタンスのクラシックネットワークエンドポイントと、読みと書きを分離しているクラシックネットワークエンドポイント
ClassicExpiredDays	Interger	はい	クラシックネットワークエンドポイントの保持期間は「1-120」日です。

リターンパラメータ

名前	データ型	説明
RequestId	String	リクエストのID。

コード例

```
public static void main ( String [] args ) {
    ModifyDBInstanceNetworkExpireTimeRequest request = new
ModifyDBInstanceNetworkExpireTimeRequest ();
    request . setClassicExpiredDays ( 3 );
    request . setConnectionString ("< URL の文字列>");
    request . setDBInstanceId ("<インスタンス ID >");
    IClientProfile profile
            = DefaultProfile . getProfile (" cn - qingdao ",
"<お客様の ak >",
            "<お客様の sk >");
    IAcsClient client = new DefaultAcsClient ( profile );
    try {
        ModifyDBInstanceNetworkExpireTimeResponse response
                = client . getAcsResponse ( request );
        System . out . println ( response . getRequestId ());
    } catch ( ServerException e ) {
        e . printStackTrace ();
    }
    } catch ( ClientException e ) {
        e . printStackTrace ();
    }
```

```
}
```

6.2.3 ApsaraDB for Redisに対するネットワークタイプの変更

本ドキュメントでは、クラシックネットワークエンドポイントを保持したまま、ApsaraDB for Redisインスタンスのネットワークタイプをコンソールとapiを通してVPCネットワークに切り替える方法について説明します。 クラシックネットワークエンドポイントには有効期限があります。 必要に応じて有効期限を指定することができます。 指定した期限に達すると、クラシックネットワークエンドポイントはシステムにより自動的に削除されます。 エンドポイントが削除される前に、通知メッセージが届きます。

前提

ネットワークタイプを変更する前に、次の条件が満たされていることが必要です。

- インスタンスのネットワークタイプがクラシックネットワークであることが必要です。
- Redisインスタンスが配置されているゾーンには、使用可能なVPCとVSスイッチがあります。詳細は次を参照してください*VPCとVSwitchの作成*。

コンソールでネットワークタイプを変更します。

1. Redisコンソールにログインします。
2. インスタンスが配置されたリージョンを選択します。
3. 対象インスタンスのIDをクリックします。
4. インスタンス情報ページで、VPCへ切り替えをクリックします。
5. 表示されるダイアログボックスで、次の手順に従って操作してください：
   a. 対象VPCとVSwitchを選択します。
   b. クラシックネットワークエンドポイントを保持するように選択し、期限を指定します。

      注：
      クラシックネットワークエンドポイントを保持すると、クラシックネットワークのECSインスタンスが引き続きデータベースにアクセスでき、サービスに影響はありません。 クラシックネットワークエンドポイントが期限切れになると、システムにより自動的削除され、クラシックネットワークエンドポイント経由でのデータベースアクセスはできなくなります。

   c. OKをクリックします。
6. インスタンス情報ページで、更新をクリックしてVPCエンドポイントとクラシックネットワークエンドポイントを確認できます。

有効期限の変更

クラシックネットワークエンドポイントの保持期間を設定後、有効期限が切れる前にコンソールを使用して保持期間を延長することができます。

ハイブリッドアクセス期間中は、必要に応じてクラシックネットワークエンドポイントの保持期間をいつでも変更できます。 たとえば、クラシックネットワークエンドポイントが2017年8月18日までに期限切れになるように設定されています、2017年8月15日にその有効期限を14日後に変更した場合、エンドポイントのリリース日は2017年8月29日になります。

1. Redisコンソールにログインします。
2. 対象インスタンスが配置されたリージョンを選択します。
3. 対象インスタンスのIDをクリックします。
4. 保持中のクラシックネットワーク接続アドレスセクションで、有効期限を変更をクリックします。
5. 表示されるダイアログボックスで、新しい有効期限を選択してOKをクリックします。

APIを通してのネットワークタイプの変更

1. SDKをダウンロードします。 （ ApsaraDB for MemcacheのSDKは、ApsaraDB for RedisのSDKと同じです）。
   - *aliyun-java-sdk- r-kvstore.zip*
   - *aliyun-python-sdk- r-kvstore.zip*
   - *aliyun-php-sdk-r-kvstore.zip*
2. SwitchNetworkAPIを呼び出してネットワークタイプを変更します。

   リクエストパラメータ

名前	データ型	必須	説明
Action	String	はい	実行する操作。 有効値： SwitchNetw ork
InstanceId	String	はい	インスタンスのID。
TargetNetw orkType	String	はい	インスタンスのネットワークタイプ。 ・ VPC ：VPC ・ Classic ：クラシックネットワーク
VPCId	String	いいえ	VPCのID。

名前	データ型	必須	説明
VSwitchId	String	いいえ	VSwitchのID。 VPCのIDが指定されている場合、このパラメータも指定する必要があります。
RetainClas sic	String	いいえ	クラシックネットワークエンドポイントを保持するかどうか。 デフォルト値は False です： ・ True ：保持する ・ False ：保持しない
ClassicExp iredDays	String	いいえ	クラシックネットワークエンドポイントの保持期間。 最短1日、最長120日。デフォルト値は7日。 RetainClassicがTrueに設定されている場合、このパラメータを指定する必要があります。

リターンパラメータ

名前	データ型	説明
RequestId	String	リクエストのID。
TaskId	String	タスクのID。

コード例

```
import   com . aliyuncs . DefaultAcs  Client ;
 import   com . aliyuncs . IAcsClient ;
 import   com . aliyuncs . exceptions . ClientExce  ption ;
 import   com . aliyuncs . exceptions . ServerExce  ption ;
 import   com . aliyuncs . profile . DefaultPro  file ;
 import   com . aliyuncs . profile . IClientPro  file ;
 import   com . aliyuncs . r_kvstore . model . v20150101 .
SwitchNetw  orkRequest ;
 import   com . aliyuncs . r_kvstore . model . v20150101 .
SwitchNetw  orkRespons  e ;
 Import   org .  JUnit .  test ;
/**
 *  Created   by   wb259286   on   2017 / 6 / 9 .
 */
 public   class   SwitchNetw  orkTest  {
    @ Test
     public    void   switchNetw  ork_succes  s () {
         SwitchNetw  orkRequest   request = new   SwitchNetw
orkRequest ();
         request . setInstanc  eId ("<インスタンス ID >");
         request . setTargetN  etworkType (" VPC ");
         request . setVpcId ("< VpcId : TargetNetw  orkType は VPC
である場合、このパラメータは必須>");
         request . setVSwitch  Id ("< VSwitchId : TargetNetw
orkType は VPC である場合、このパラメータは必須>");
```

```
            request . setRetainC  lassic ("<クラシックネットワークエンドポ
イントを保持するかどうか。>");
            request . setClassic  ExpiredDay  s ("クラシックネットワークエ
ンドポイントの保持期間");
            IClientPro  file   profile  =  DefaultPro  file .
 getProfile (" cn - hangzhou ", "<お客様の AK >",
                "<お客様の Security >");
            IAcsClient   client  =  new   DefaultAcs  Client ( profile
 );
            try  {
                SwitchNetw  orkRespons  e   response
                   =  client . getAcsResp  onse ( request );
                System . out . println ( response . getRequest  Id
 ());
        } catch  ( ServerExce  ption   e ) {
                e . printStack  Trace ();
        }
             catch  ( ClientExce  ption   e ) {
                e . printStack  Trace ();
            }
        }
 }
```

3. DescribeDBInstanceNetInfoAPIを呼び出し、クラシックネットワークエンドポイント及びVPCエンドポイントを確認します。

   リクエストパラメータ

名前	データ型	必須	説明
Action	String	はい	実行する操作。 有効値： DescribeDB InstanceNe tInfo
InstanceId	String	はい	インスタンスのID。

   リターンパラメータ

名前	データ型	説明
NetInfoIte ms	List	インスタンスの接続情報。

名前	データ型	説明
InstanceNetworkType	String	インスタンスのネットワークタイプ。 ・ VPC ：VPCネットワークのインスタンス。 ・ Classic ：クラシックネットワークのインスタンス。

InstanceNetInfo

名前	データ型	説明
ConnectionString	String	DNSの接続文字列。
IPAddress	String	IPアドレス。
IPType	String	クラシックネットワークインスタンスのIPタイプ。 Inner	Public 。 VPCネットワークインスタンスのIPタイプ。 Private	Public 。
Port	String	ポート情報
VPCId	String	VPCのID。
VSwitchId	String	VSwitchのID。
ExpiredTime	String	期限切れ日時。

コード例

```
import   com . aliyuncs . DefaultAcs  Client ;
 import   com . aliyuncs . IAcsClient ;
 import   com . aliyuncs . exceptions . ClientExce  ption ;
 import   com . aliyuncs . exceptions . ServerExce  ption ;
 import   com . aliyuncs . profile . DefaultPro  file ;
 import   com . aliyuncs . profile . IClientPro  file ;
 import   com . aliyuncs . r_kvstore . model . v20150101 .
DescribeDB  InstanceNe  tInfoReque  st ;
 import   com . aliyuncs . r_kvstore . model . v20150101 .
DescribeDB  InstanceNe  tInfoRespo  nse ;
 import   org . junit . Test ;
/**
 *
 */
 public   class   DescribeDB  InstanceNe  tInfoTest  {
@ Test
     public    void   describeDB  InstanceNe  tInfo_succ  ess () {
         DescribeDB  InstanceNe  tInfoReque  st   request = new
  DescribeDB  InstanceNe  tInfoReque  st ();
         request . setInstanc  eId ("<インスタンス ID >");
```

```
            IClientPro  file   profile  =  DefaultPro  file .
getProfile (" cn - hangzhou ", "<お客様の AK >",
               "<お客様の Security >");
            IAcsClient   client  =  new   DefaultAcs  Client ( profile
);
            try  {
                DescribeDB  InstanceNe  tInfoRespo  nse   response
                   =  client . getAcsResp  onse ( request );
                System . out . println ( response . getRequest  Id
());
        } catch  ( ServerExce  ption   e ) {
                e . printStack  Trace ();
            }
            catch  ( ClientExce  ption   e ) {
            e . printStack  Trace ();
            }
        }
}
```

APIを通してのクラシックネットワークエンドポイントの有効期限の変更

1. SDKのURLをクリックしてSDKをダウンロードします。（ApsaraDB for MemcacheのSDKはApsaraDB for RedisのSDKと同じです。）
   - *aliyun-java-sdk- r-kvstore.zip*
   - *aliyun-python-sdk- r-kvstore.zip*
   - *aliyun-php-sdk-r-kvstore.zip*
2. `ModifyInstanceNetExpireTime`APIを呼び出し、ネットワークタイプを変更します。

   リクエストパラメータ

名前	データ型	必須	説明
`Action`	String	はい	実行する操作。 有効値： `ModifyInst anceNetExp ireTime` .
`InstanceId`	String	はい	インスタンスのID。
`Connection String`	String	はい	クラシックネットワークのエンドポイント。

名前	データ型	必須	説明
ClassicExpiredDays	Interger	はい	有効期限を選択します。 有効値：14/30/60/120。

リターンパラメータ

名前	データ型	説明
RequestId	String	リクエストのID。

コード例

```
public   static   void   main ( String []  args ) {
     ModifyInst  anceNetExp  ireTimeReq  uest   request  =  new
ModifyInst  anceNetExp  ireTimeReq  uest ();
     request . setClassic  ExpiredDay  s ( 3 );
     request . setConnect  ionString ("< URL の文字列>");
     request . setInstanc  eId ("<インスタンス ID >");
     IClientPro  file   profile
             =  DefaultPro  file . getProfile (" cn - hangzhou ",
"<お客様の ak >",
             "<お客様の sk >");
     IAcsClient   client  =  new   DefaultAcs  Client ( profile );
     try  {
         ModifyInst  anceNetExp  ireTimeRes  ponse   response
                 =  client . getAcsResp  onse ( request );
         for  ( NetInfoIte  m   item : response . getNetInfo  Items
()) {
             System . out . println ( item . getConnect  ionString
());
             System . out . println ( item . getPort ());
             System . out . println ( item . getDBInsta  nceNetType
());
             System . out . println ( item . getIPAddre  ss ());
             System . out . println ( item . getExpired  Time ());
         }
    }  catch  ( ServerExce  ption   e ) {
         e . printStack  Trace ();
    }
    }  catch  ( ClientExce  ption   e ) {
         e . printStack  Trace ();
    }
}
```

6.2.4 ApsaraDB for MongoDBのネットワークタイプの変更

本ドキュメントでは、ApsaraDB for MongoDBのネットワークタイプをコンソールまたはAPI経由でVPCに変更し、クラシックネットワークエンドポイントを保持する方法を紹介します。 クラシックネットワークエンドポイントは、一定期間内に保持されます。 その期間を必要に応じて指定することができます。 指定した期限に達すと、クラシックネットワークエンドポイントはシステムにより自動的に削除されます。

前提

ネットワークタイプを変更する前に、次の条件が満たされていることが必要です。

- ネットワークタイプがクラシックネットワークであることが必要です。
- インスタンスタイプはMongoDBレプリカセットであることが必要です。
- データベースインスタンスのゾーンに使用可能なVPCとVSスイッチがあることが必要です。詳細は次を参照してください *VPCとVSwitchの作成*。

コンソールでネットワークタイプを変更します。

1. MongoDBコンソールにログインします。
2. 対象インスタンスを検索して、インスタンスIDまたは 操作列にある管理をクリックします。
3. 左側のメニュでデータベース接続タブをクリックし、VPCへ切り替えをクリックします。
4. 表示されるダイアログボックスで、次の手順に従って操作してください。
   a. 対象VPCとVSwitchを選択します。
   b. クラシックネットワークエンドポイントを保持するように選択し、期限を指定します。

      注：
      クラシックネットワークエンドポイントを保持すると、クラシックネットワークのECSインスタンスが引き続きデータベースにアクセスでき、サービスに影響はありません。 クラシックネットワークエンドポイントが期限切れになると、システムにより自動的削除され、クラシックネットワークエンドポイント経由でのデータベースアクセスはできなくなります。

   c. OKをクリックします。
5. データベース接続ページで、 更新をクリックしてVPCエンドポイント及びクラシックネットワークエンドポイントを確認できます。

APIを通してネットワークタイプを変更します。

1. SDKURLをクリックしてSDKをダウンロードします。
   - *aliyun-python-sdk-dds.zip*
   - *aliyun-java-sdk-dds.zip*
   - *aliyun-php-sdk-dds.zip*

2. ModifyDBInstanceNetworkTypeAPIを呼び出してネットワークタイプを変更します。

リクエストパラメータ

名前	データ型	必須	説明
Action	String	はい	実行する操作。 有効値： ModifyDBIn stanceNetw orkType
DBInstance Id	String	はい	インスタンスのID。
NetworkTyp e	String	はい	インスタンスのネットワークタイプ。 ・ VPC ：VPC ・ Classic ：クラシックネットワーク
VPCId	String	いいえ	VPCのID。
VSwitchId	String	いいえ	VSwitchのID。 VPCのIDが指定されている場合、このパラメータも指定する必要があります。
RetainClas sic	String	いいえ	クラシックネットワークエンドポイントを保持するかどうか。 デフォルト値は False です。 ・ True ：保持する ・ False ：保持しない
ClassicExp iredDays	String	いいえ	クラシックネットワークエンドポイントの保持期間。 最短1日、最長120日。デフォルト値は7日。 RetainClassicがTrueに設定されている場合、このパラメータを指定する必要があります。

リターンパラメータ

名前	データ型	説明
RequestId	String	リクエストのID。
TaskId	String	タスクのID。

3. DescribeReplicaSetRoleAPIを呼び出して、クラシックネットワークエンドポイント及びVPCエンドポイントを確認します。

リクエストパラメータ

名前	データ型	必須	説明
Action	String	はい	実行する操作。 有効値：DescribeReplicaSetRole
DBInstanceId	String	はい	インスタンスのID。

リターンパラメータ

名前	データ型	説明
ReplicaSets	List	レプリカセットロールのリスト。
DBInstanceId	String	インスタンスのID。

ReplicaSetRole

名前	データ型	説明
ReplicaSetRole	String	レプリカセットロール： Primary | Secondary
ConnectionDomain	String	インスタンスの接続情報。
ConnectionPort	String	インスタンスの接続ポート。
ExpiredTime	String	クラシックネットワークは期限切れまでの残り時間（秒）。
NetworkType	String	インスタンスのネットワークタイプ。 ・ VPC ：VPC ・ Classic ：クラシックネットワーク

6.3 その他プロダクトのハイブリッドアクセス

ハイブリッドアクセスとは、クラシックネットワークと VPC ネットワークの両方で、ECS インスタンスから ApsaraDB へのアクセスを意味します。 ApsaraDB 以外に、次のプロダクトもハ

イブリッドアクセスに対応しています。 様々なクラウド製品のエンドポイントをドキュメントで確認できます。

ストレージ

- Object Storage Service：エンドポイントを取得。
- Table Store：エンドポイントを取得。

アプリケーションサービス

- Log Service：エンドポイントを取得。

ミドルウェア

- メッセージキュー
  - Management and control：エンドポイントを取得。

ビッグデータ

- MaxCompute：エンドポイントを取得。

6.4 ハイブリッド追加とハイブリッドアクセス方式での移行の例

本ドキュメントでは、ハイブリッドアクセスおよびハイブリッド追加ソリューションを使用して、リソースをクラシックネットワークからVPCネットワークへ移行する方法を説明します。

前提

移行する前に、次の各事項を確実にしてください：

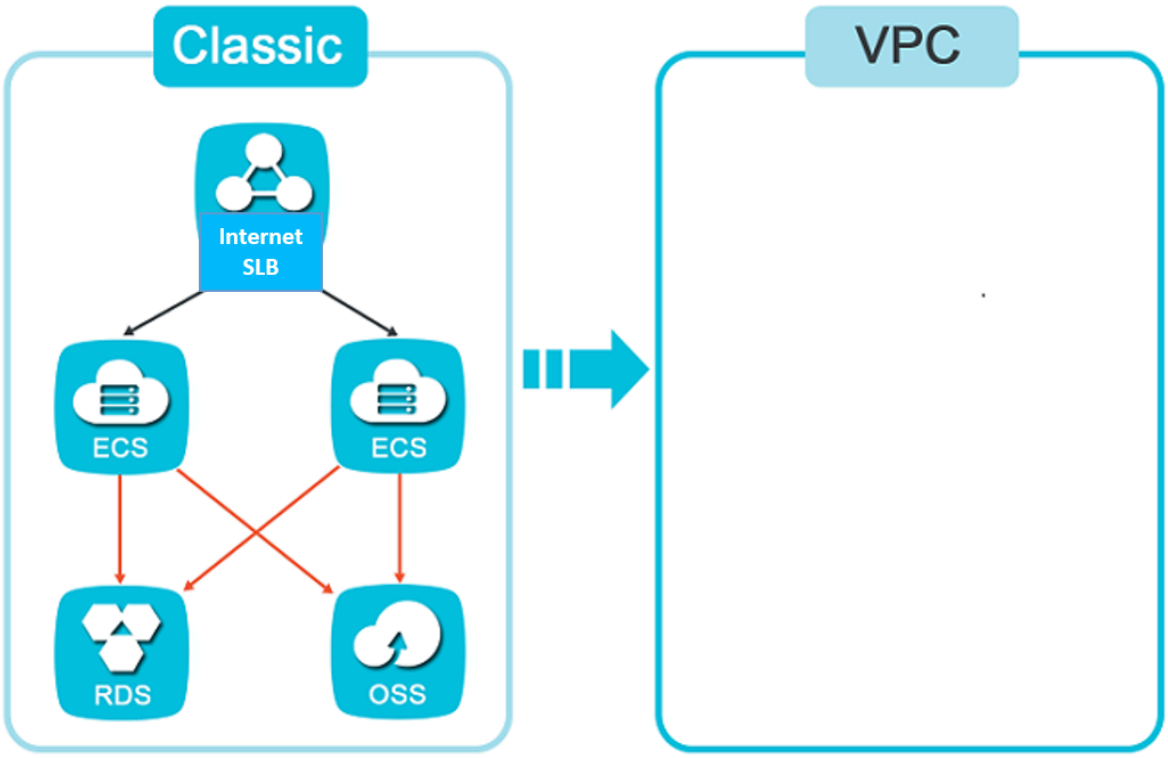
- 移行の詳細及び制限事項を理解していること。 詳細は移行の概要を参照してください。
- VPCと関連プロダクトに熟知していること。 VPCはクラシックネットワークと多くの点で異なっています。 VPCを使用すると、ネットワークの分離とは別に、他の関連プロダクトを通してプライベートネットワークを制御できます。
- 本ドキュメントで行った移行はあくまでも参考用です。 他の多くのシステムはこの例よりも複雑になります。 移行する前に、慎重に評価し、システムの依存関係を把握し、正確な移行計画を立てる必要があります。

移行対象のシステム

本ドキュメントでは、2つの移行の例を挙げています、 そのうちのシステムの一つは、もう一つよりも複雑です。

- システム1

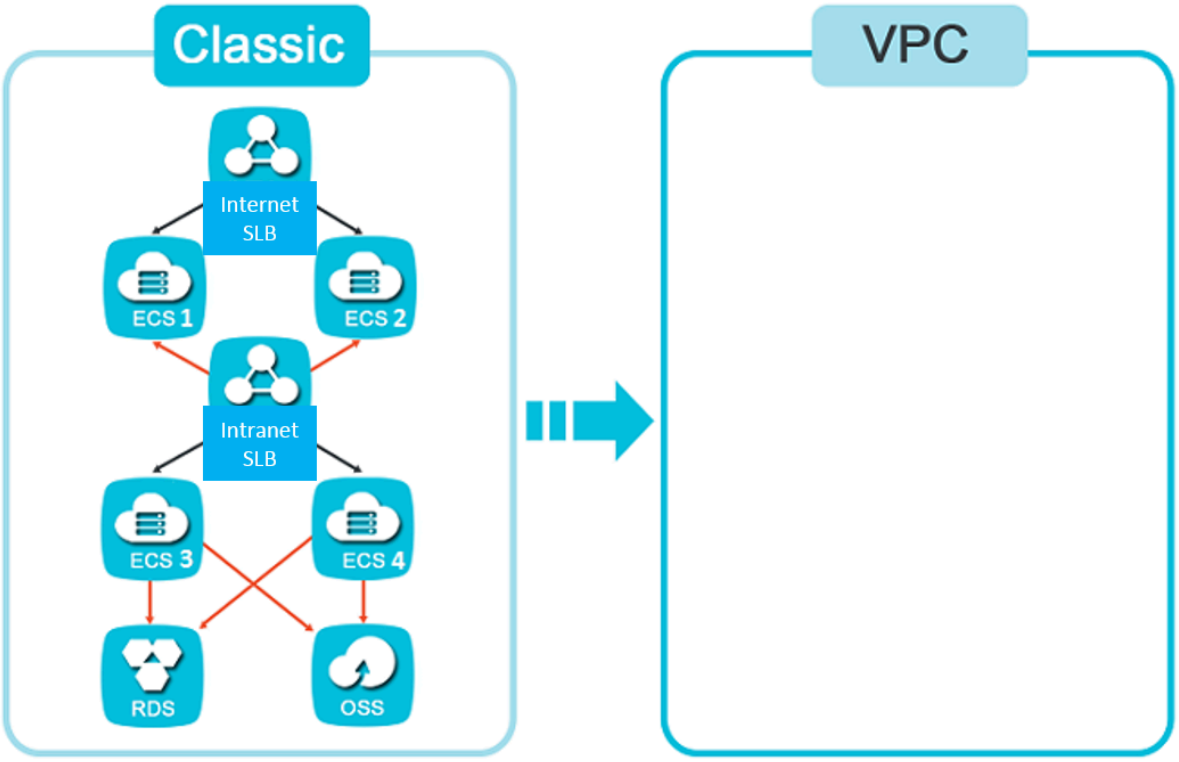
  下図のように、移行するシステムはSLB、ECS、RDSおよびOSSで構成されています。 インターネットSLBインスタンスはバックエンドサーバとして2つのECSインスタンスを使用しています、2つのECSインスタンスにデプロイされたアプリケーションはRDSおよびOSSにアクセスする必要があります。



- システム2

  下図のように、システム2のアーキテクチャはより複雑になっています。 インターネットSLBインスタンスは、バックエンドサーバーとして2つのECSインスタンス（ECS 1およびECS 2）を使用しています。 この2つのECSインスタンスはSLBインスタンスにアクセスする必要があ

ります。 それと同様に、イントラネットSLBインスタンスも、RDSおよびOSSにアクセスする必要がある2つのECSインスタンス（ECS 3およびECS 4）を使用しています。



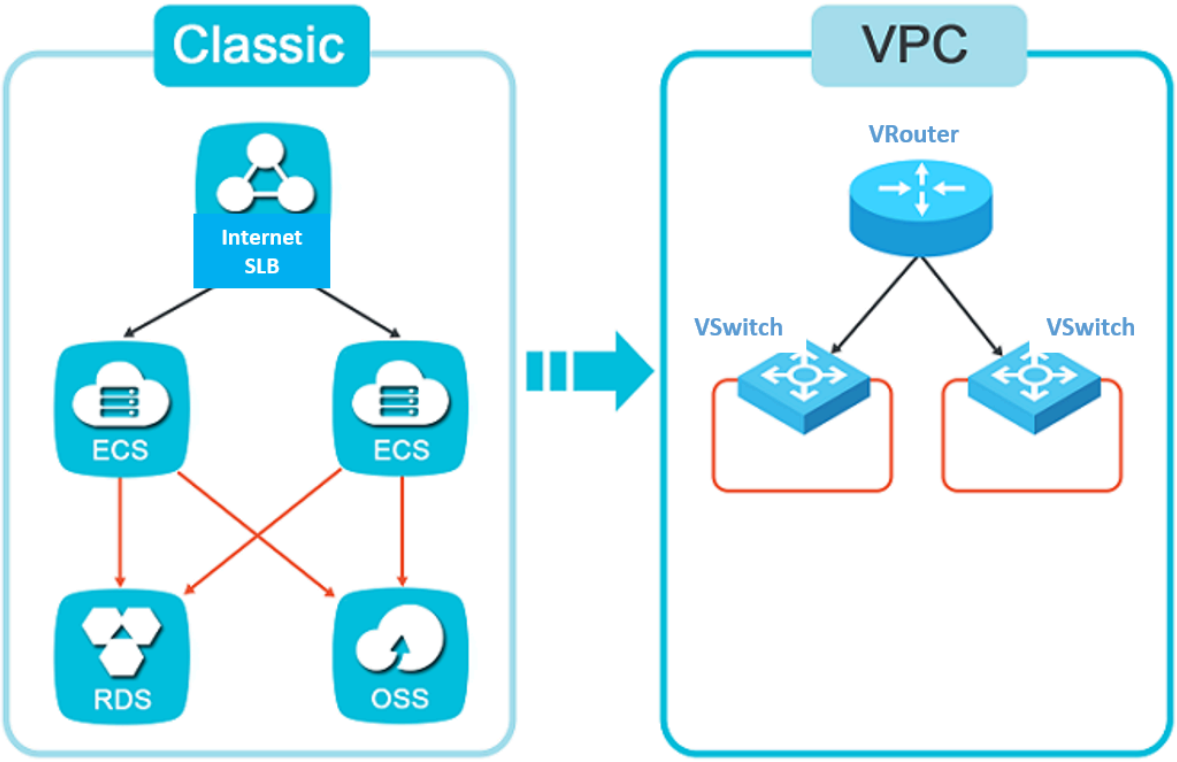
システム1をVPCへの移行

VPCに*system 1*を移行するには、次の手順に従ってください：

1. ネットワーク環境を準備します。

   まず、移行先となるVPCとVSwitchを作成し、関連情報を確認する必要があります。

   詳細は、*VPCの作成*を参照してください。



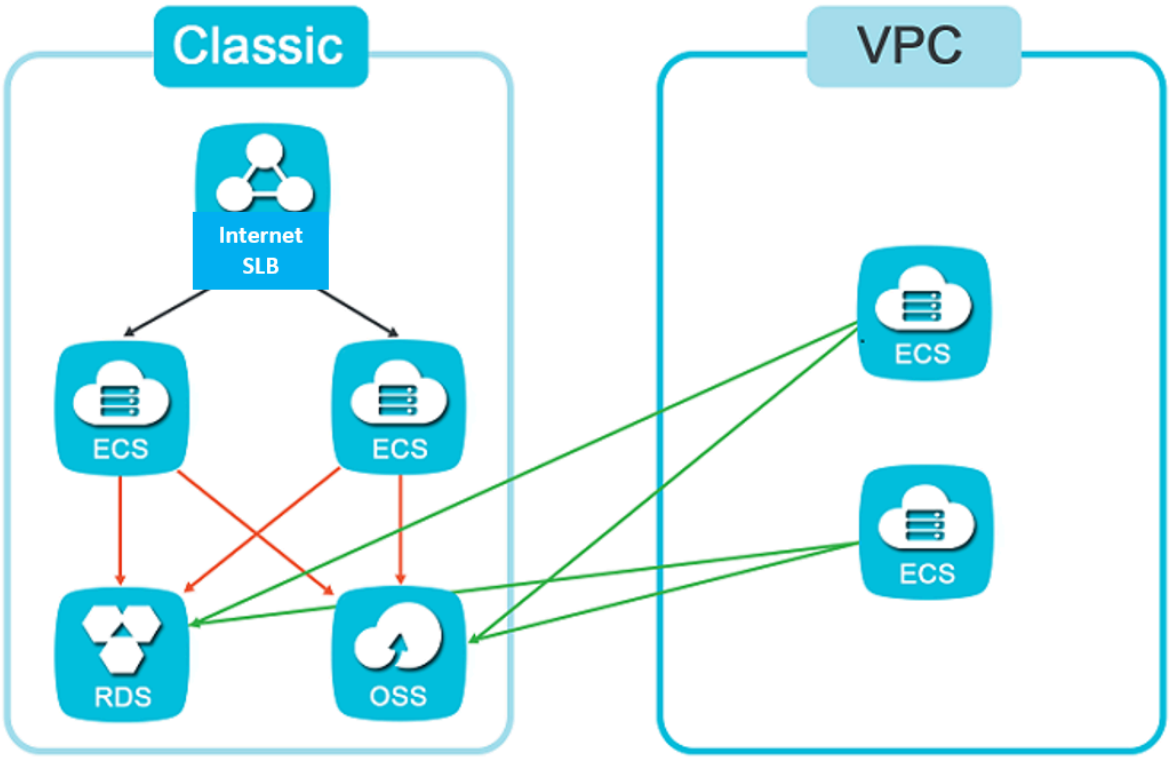
2. OSSとRDSのVPCエンドポイントの取得

   - APIまたはコンソールを使用してRDSインスタンスをVPCに移行すると同時に、クラシックネットワークエンドポイントを保持することができます。 詳細は、*ApsaraDB for RDSのネットワークタイプの変更*を参照してください。

     移行後、クラシックネットワークエンドポイントは変更されず、新しいVPCエンドポイントが追加されます。 そのおかげで、クラシックネットワークのECSインスタンスは引き続きデータにアクセスでき、サービスは中断されません。 クラシックネットワークエンドポイントが期限切れになると、システムにより自動的に削除され、クラシックネットワークエンドポイント経由でデータベースへのアクセスはできなくなります。
   - OSSには2つのエンドポイントがあり、切り替えは不要です。 OSSのVPCエンドポイントを取得するには、リージョンとエンドポイントを参照してください。

3. VPCでECSインスタンスを2つ作成し、構成します。

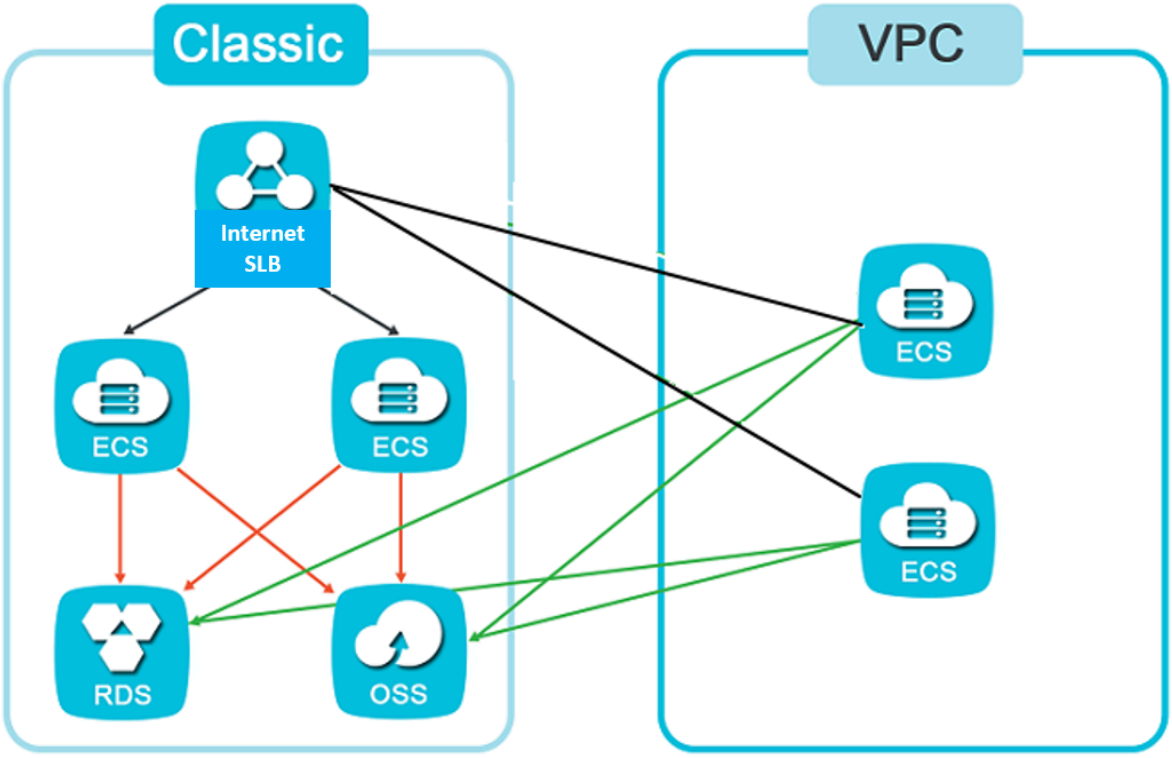
   下図のように、VPCでECSインスタンスを2つ作成して、これらにアプリケーションをデプロイし、RDSとOSSエンドポイントをVPCエンドポイントに変更します。 構成完了後、OSSとRDSがアクセス可能であるかどうかを確認するためにテストを行う必要があります。



4. VPC内のECSインスタンスをインターネットSLBインスタンスへの追加

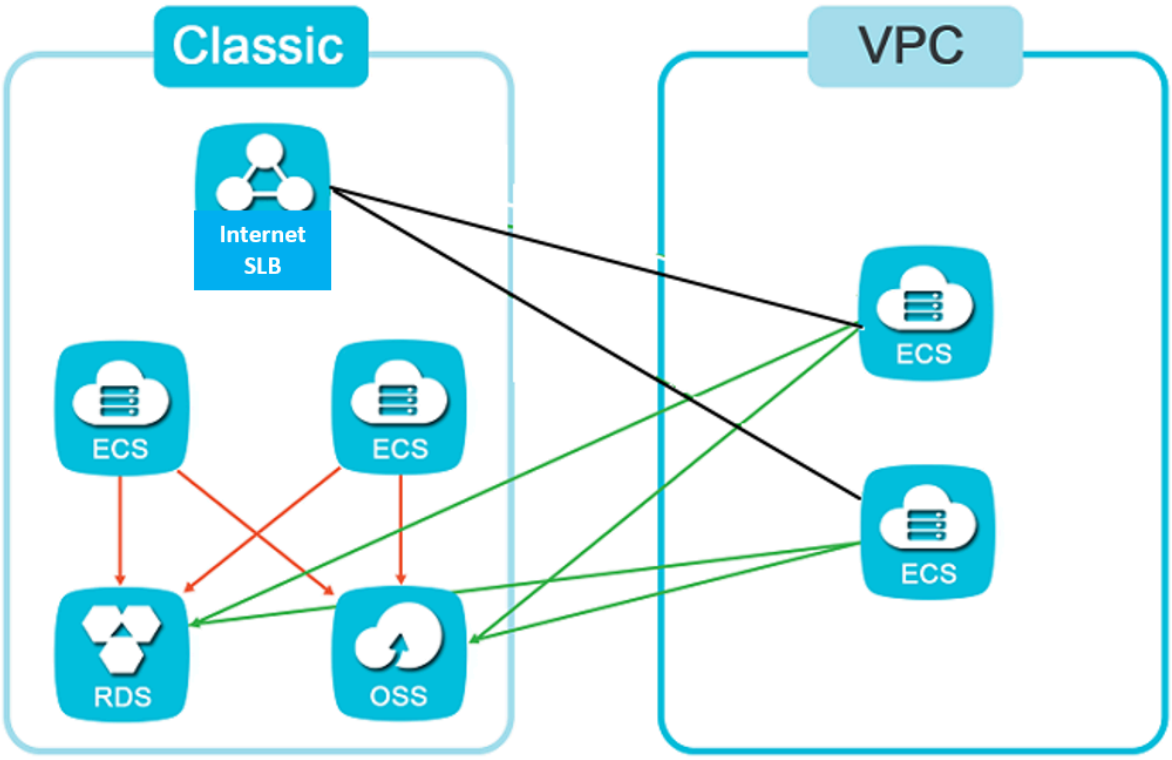
   下図のように、VPCで作成および構成されたECSインスタンスをインターネットSLBインスタンスに追加します。 そして新しく追加されたECSインスタンスのヘルス状態を確認します。 ECSインスタンスの重みを小さめに設定できます。 そうすればインスタンス状態が正常であっ

ても他に異常が発生した場合のシステムに与える影響を軽減できます。 また、システム状態、トラフィック監視、ヘルス状態ログなどの情報も確認してください。



5. インターネットSLBインスタンスからのクラシックネットワークECSインスタンスの削除

   下図のように、システムを正常に起動した後、クラシックネットワークのECSインスタンスをインターネットSLBインスタンスから削除します。 クラシックネットワークのECSインスタンスの重みを0に設定し、トラフィックの受信がなくなると削除することができます。

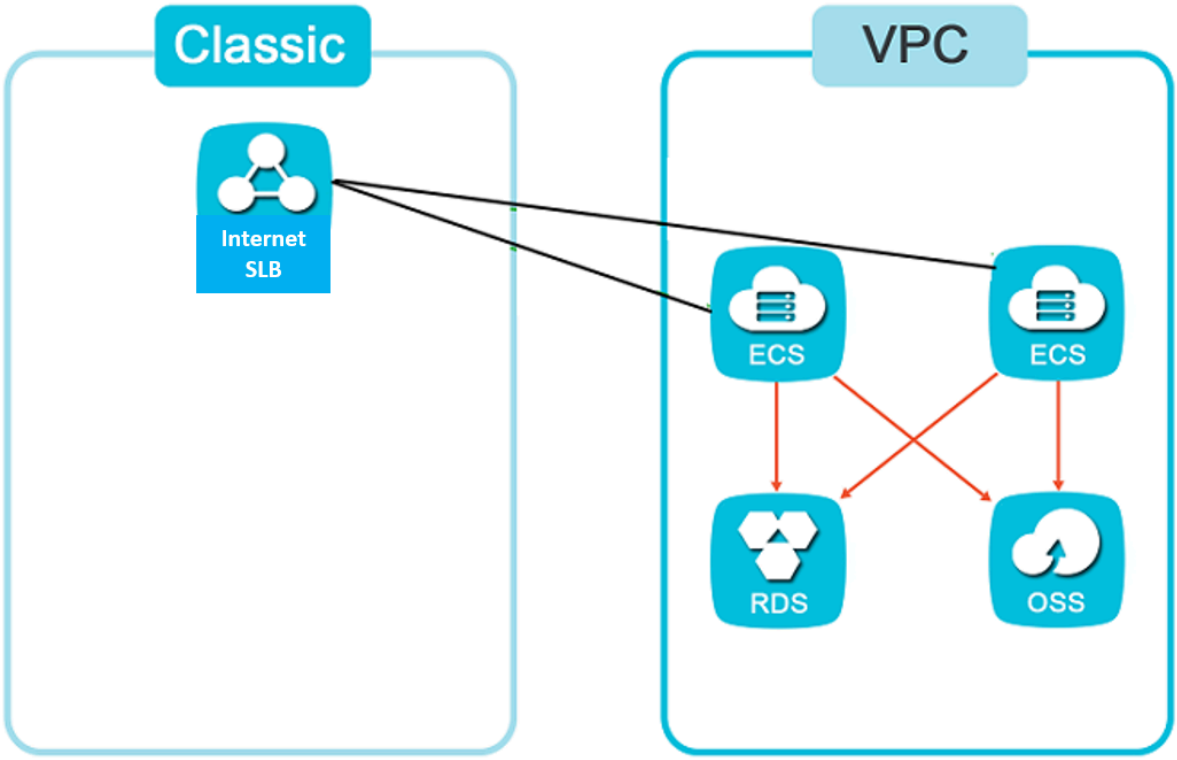


6. クラシックネットワークのインスタンスのリリース

   下図のように、システムが一定期間中に安定な動作が続くと、クラシックネットワークのECSインスタンスをリリースできます。 インターネットSLBインスタンス自体は、VPCネットワークのECSインスタンスを追加できるため、移行する必要はありません。 移行はこれで完成しました。

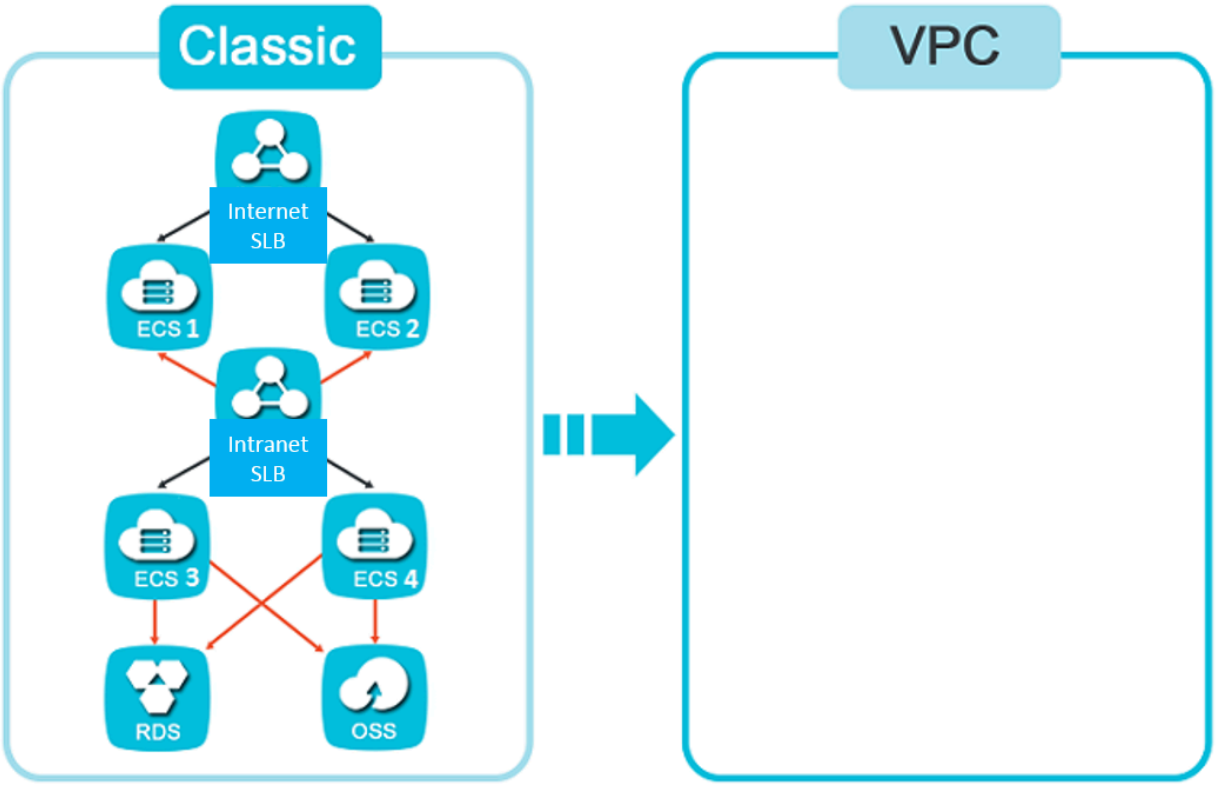
   注：

RDSのクラシックネットワークエンドポイントは、期限切れになると自動的に削除されます。



システム2をVPCへの移行

下図のような比較的複雑なシステムを移行する場合、システム1の移行手順に従う場合、 SLBインスタンスがハイブリッドアクセスを対応していないため、VPCネットワークのECSインスタンスはクラシックネットワークのECSインスタンスにアクセスできません。



システム2を移行する手順は次の通りです：

1. イントラネットSLBインスタンスに追加されたクラシックネットワークのECS 3とECS 4を移行するため、VPCでECSインスタンスを2つ作成します。
2. OSSおよびRDSのVPCエンドポイントを使用して、新規作成したECSインスタンスを構成します。
3. VPCでイントラネットSLBインスタンスを作成して、クラシックネットワーク内のイントラネットSLBインスタンスを置き換えます。
4. VPC内のイントラネットSLBを構成し、 手順1で作成した2つのECSインスタンスをバックエンドサーバーとして追加します。
5. VPCでさらに2つのECSインスタンスを作成して、インターネットSLBインスタンスに追加されたクラシックネットワークのECS 1とECS 2を移行します。
6. この2つのECSインスタンスを構成します。 イントラネットSLBインスタンスのクラシックネットワークエンドポイントをインスタンスのVPCエンドポイントに変更します。
7. これ以降の手順はシステム1の移行手順と類似しています。

6.5 ECS インスタンスのマイグレーション

1 台、あるいはそれ以上の ECS インスタンスをクラシックネットワークから VPC ネットワークにマイグレーションできます。

制限事項

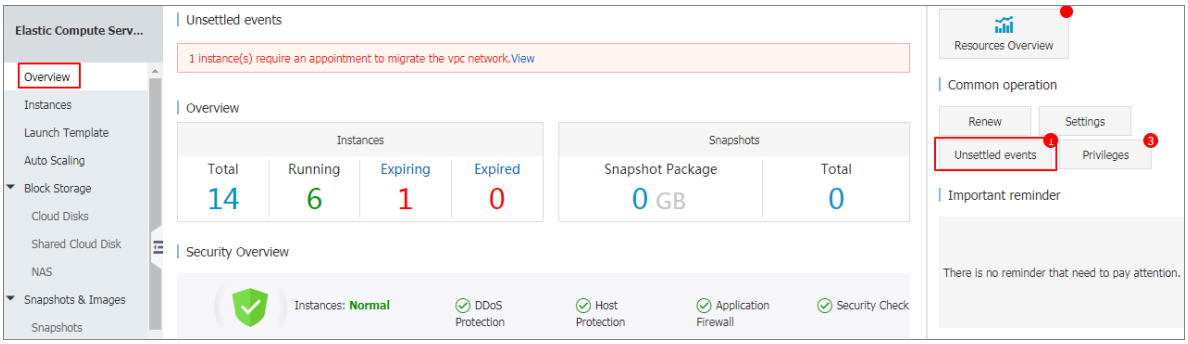
ECS インスタンスをマイグレーションする前に、次の点に注意します：

- マイグレーションプロセス中に、インスタンスが再起動され、システムやサービスに影響を与える可能性があります。
- マイグレーション後、特別な構成は不要で、ECS インスタンスのパブリック IP は変更されません。
  - マイグレーションされたすべての ECS インスタンスのパブリック IP は変更されませんが、このパブリック IP は ECS インスタンスのオペレーティングシステムには表示されません（VPC ネットワークの ECS インスタンスのパブリック IP と呼ばれます）。 従量課金制 ECS インスタンスのパブリック IP を EIP に変更できます。 詳細は、*ECS インスタンスのプライベート IP を EIP への変更*をご参照ください。
  - アプリケーションの 1 つが ECS インスタンスのオペレーティングシステム上の公開パブリック IP に依存している場合は、サービスに何らかの影響があるため、マイグレーションを慎重に行う必要があります。
- 対象の VPC の VSwitch とマイグレーションする ECS インスタンスは、同一ゾーンにある必要があります。
- インスタンス ID とログイン情報は、マイグレーションプロセスで変更されません。
- サブスクリプションインスタンスのマイグレーションに追加料金がかかりません。 新しい請求サイクルが開始されると、マイグレーションされた ECS インスタンスは、同じ仕様の VPC ネットワークのインスタンスと同じ料金で請求されます。 VPC へマイグレーション後、ECS の料金は安くなります。
- 仕様変更が有効になっていない、あるいは未支払い注文は、マイグレーション後にキャンセルされ、元に戻すことはできません。 その場合は再度注文する必要があります。

ステップ 1 マイグレーションをスケジュールする

1. ECS コンソールにログインします。
2. 対象のインスタンスを特定し、 詳細 > ネットワークとセキュリティグループ > VPC への移行スケジュールをクリックします。
3. 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. 概要ページの右上隅にある共通操作エリアにあるスケジュールされたタスクの表示または 保留中のタスクをクリックします。



5. 保留中のタスクページで、 VPC へのマイグレーションタブをクリックします。
6. マイグレーションするインスタンスを選択して、マイグレーションスケジュールの設定をクリックします。
7. 表示されるダイアログボックスで、対象の VPC、VSwitch、およびマイグレーション時間を選択し、 OK をクリックします。

ステップ 2 マイグレーションを開始する

予定作成後、Alibaba Cloud は予定された時間にマイグレーションを開始します。 マイグレーションには通常5分ほどかかります。

ステップ 3 マイグレーション結果を表示する

いくつかの方法でマイグレーション結果を表示できます。

- 対象のタスクの状態を表示できます。 タスクの状態が 実行完了に変わると、マイグレーションは成功です。
- マイグレーションが成功したことを示すメッセージを受け取れたかどうかを確認します。
- ECS コンソールにログインします。 インスタンス詳細 ページで、インスタンスのネットワークタイプが VPC になっていることを確認します。