Alibaba Cloud Server Load Balancer

アーカイブ

Document Version20190906

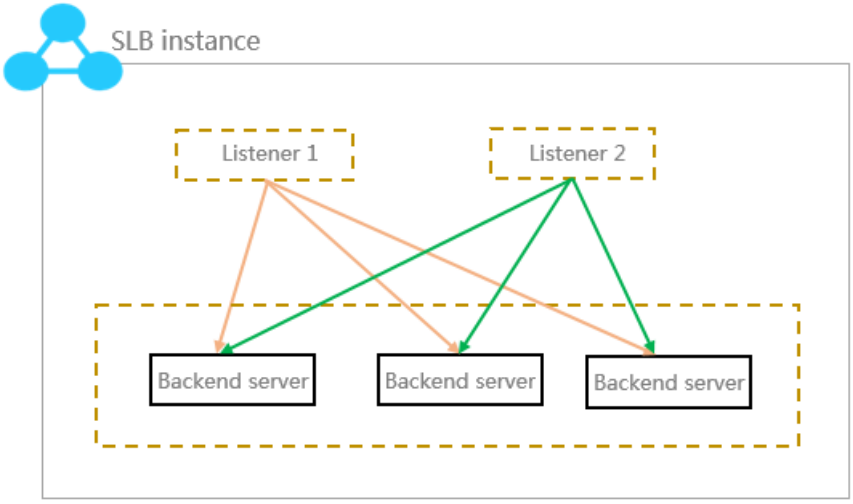
目次

1 ユーザーガイド (旧コンソール)

1.1 SLB インスタンス

1.1.1 SLB インスタンスの概要

SLB インスタンスは Server Load Balancer サービスの実行エンティティです。 負荷分散サービスを使用するには、SLB インスタンスを作成後、リスナーとバックエンドサーバーを追加する必要があります。

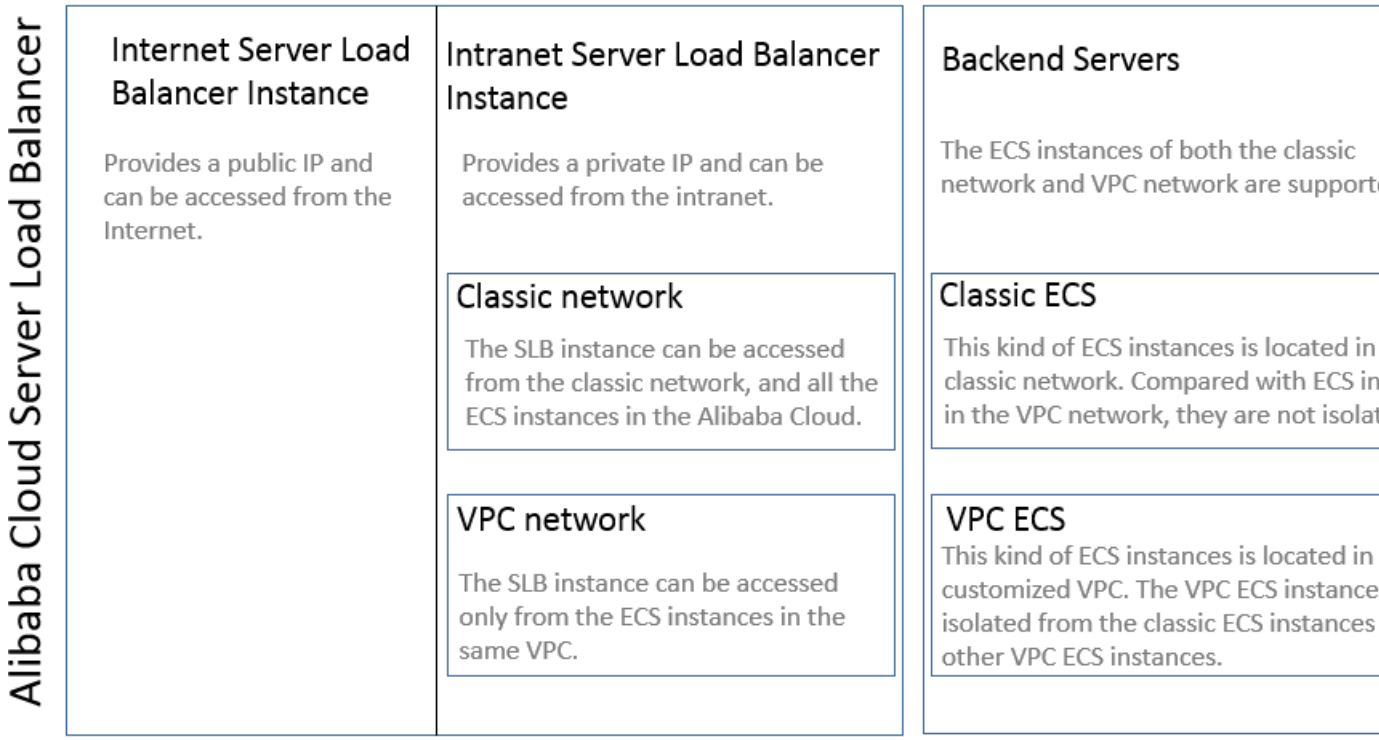


Alibaba Cloudは、インターネット負荷分散サービスとイントラネット負荷分散の 2 種類の負荷分散サービスを提供します。 選択したインスタンスタイプに応じて、パブリック IP アドレスまたはプライベート IP アドレスが SLB インスタンスに割り当てられます。

インターネット SLB インスタンス

インターネット SLB インスタンスは、設定された転送ルールに従ってバックエンドの ECS サーバーにインターネット経由でクライアントからのリクエストを配信します。

インターネット Server Load Balancer インスタンスを作成後、そのインスタンスにはパブリック IP アドレスが割り当てられます。 パブリックサービスを提供するために、ドメイン名をパブリック IP に解決できます。



イントラネット SLB インスタンス

イントラネット SLB インスタンスは、Alibaba Cloud 内でのみ使用でき、SLB のイントラネットにアクセス可能なクライアントからのリクエストのみ転送できます。

イントラネット SLB インスタンスでは、さらにネットワークタイプを選択できます。

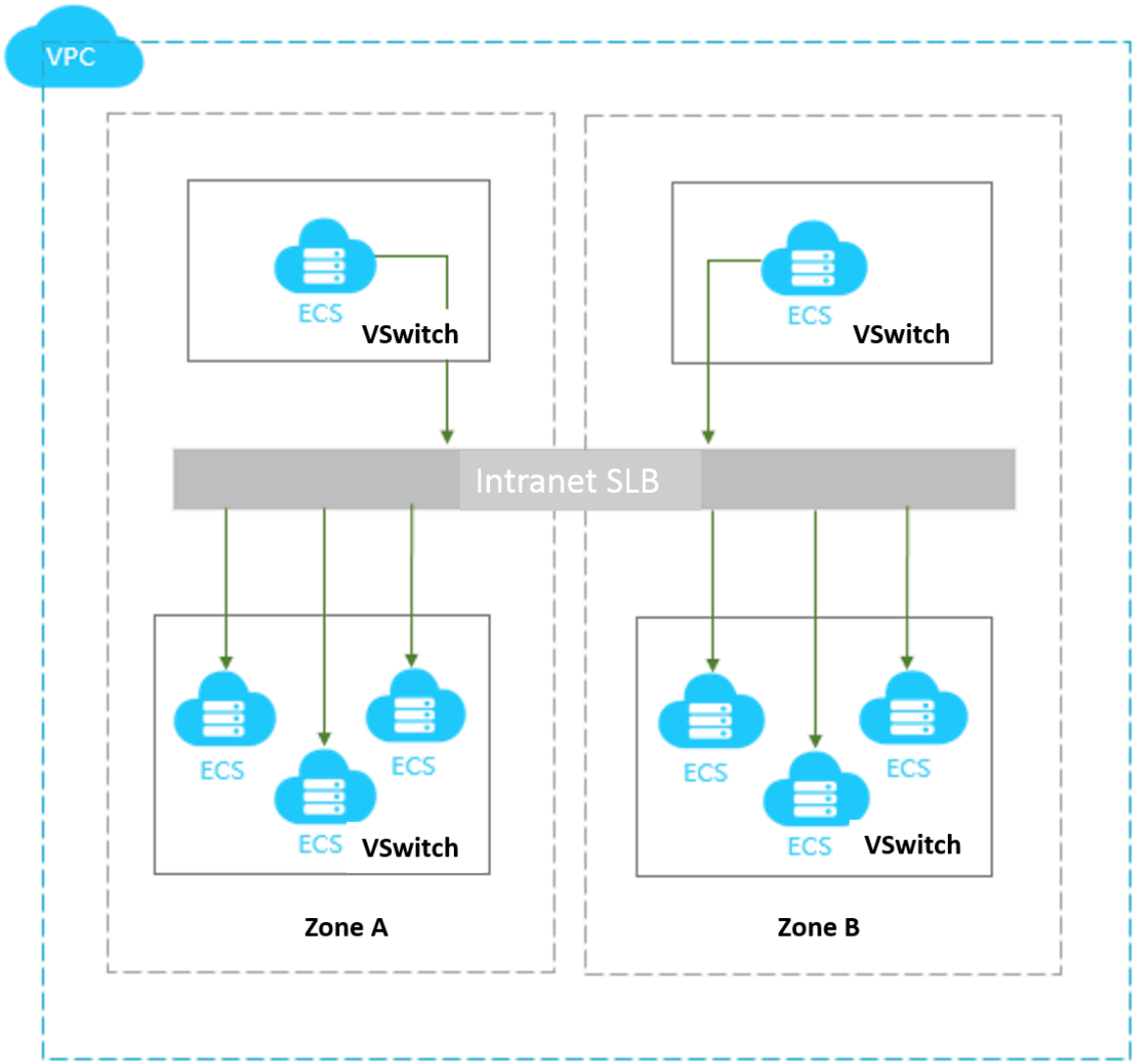
- クラシックネットワーク

  イントラネット SLB インスタンスにクラシックネットワークを選択した場合、Alibaba Cloud が SLB インスタンスの IP アドレスを割り当て、管理します。 クラシック SLB インスタンスには、クラシック ECS インスタンスのみがアクセスできます。

- VPC ネットワーク

  イントラネット SLB インスタンスに VPC ネットワークを選択した場合、SLB インスタンスの IP アドレスは、インスタンスが属する VSwitch の CIDR から割り当てられます。 VPC

ネットワークの SLB インスタンスは、同一 VPC 内の ECS インスタンスのみがアクセスできます。



1.1.2 ネットワークトラフィックフロー

受信ネットワークトラフィック

SLB は、コンソールまたは API で設定された転送ルールに従って受信トラフィックを配信します。 次の図は、ネットワークトラフィックフローを示しています。

1. TCP/UDP プロトコル、HTTP/HTTPS プロトコルにかかわらず、受信トラフィックは最初に LVS クラスターを介して転送される必要があります。
2. 無数の受信トラフィックが LVS クラスター内のすべてのノードサーバーに均等に分散され、ノードサーバーはセッションを同期させて高可用性を保証します。

3. レイヤー 4 リスナー (フロントエンドプロトコルは UDP または TCP) の場合、LVS クラスターのノードサーバーは、設定された転送ルールに従ってバックエンド ECS インスタンスにリクエストを直接配信します。
4. レイヤー 7 リスナー (フロントエンドプロトコルは HTTP) の場合、LVS クラスター内のノードサーバーは、最初に Tengine クラスターにリクエストを配信します。 続いて、Tengine クラスター内のノードサーバーは、設定された転送ルールに従ってバックエンド ECS インスタンスにリクエストを配信します。
5. レイヤー 7 リスナー (フロントエンドプロトコルは HTTPS) の場合、リクエストの配信は HTTP プロトコルに似ています。 ただし、バックエンド ECS インスタンスにリクエストを配信する前に、 システムは鍵サーバーを呼び出して証明書を検証し、データパケットを復号化します。

送信ネットワークトラフィック

SLB は、イントラネットを通してバックエンド ECS インスタンスと通信します。 バックエンド ECS インスタンスが SLB から配信されたトラフィックを処理するだけであれば、パブリック帯域幅 (EIP、NAT Gateway およびパブリック IP) は必要ありません。 ただし、バックエンド ECS インスタンスから外部サービスを提供したい場合、またはバックエンド 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、 EIP や NAT Gateway の設定など、パブリック IP を設定する必要があります。 次の図は、送信ネットワークのトラフィックフローを示しています。

一般的に、トラフィックは受信した場所から送信されます。

1. SLB からのトラフィックについては、課金と速度制限が SLB で行われます。 受信トラフィックではなく、送信トラフィックに基づいて課金されます (ルールは将来変更される可能性があります)。 SLB はイントラネットを通してバックエンドの ECS インスタンスと通信しますが、内部通信にはトラフィック料金が発生しません。
2. EIP または NAT Gateway からのトラフィックは、課金と速度制限は EIP または NAT Gateway で行われます。 ECS インスタンスが作成された時点でパブリック IP が既に設定されている場合、課金と速度制限は ECS インスタンスで行われます。
3. SLB はインターネットからアクセスされる機能のみを提供しています。 つまり、バックエンド ECS インスタンスは、SLB により転送されたリクエストにレスポンスする場合にのみインターネットにアクセスできます。 バックエンド ECS インスタンスからインターネットにアクセスする場合は、ECS インスタンスのパブリック IP (EIP または NAT Gateway の設定) を設定する必要があります。

4. パブリック IP (ECS インスタンスの作成時に設定される)、EIP、および NAT Gateway はすべてインターネットの相互アクセス (アクセスする、またはアクセスされる) を実現できますが、トラフィックの転送やトラフィック負荷の分散をすることはできません。

1.1.3 インスタンスの作成

Server Load Balancer を使用するには、まず Server Load Balancer インスタンスを作成する必要があります。

SLB インスタンスを作成する前に、環境が正しく準備されていることを確認してください。 詳細は、「計画と準備」をご参照ください。

1. SLB 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、[Server Load Balancer] をクリックします。 左上端にある [SLB インスタンスの作成] をクリックします。
3. 次の情報に従って SLB インスタンスを設定します。

設定項目	説明
リージョン	SLB インスタンスのリージョンを選択します。 注: SLB インスタンスがバックエンド ECS インスタンスと同じリージョンにあることを確認してください。
ゾーンタイプ	選択したリージョンのゾーンタイプを表示します。 クラウド製品のゾーンは、一連の独立したインフラストラクチャを指し、通常はインターネットデータセンター (IDC) により表されます。 異なったゾーンには独立したインフラストラクチャ (ネットワーク、電源、エアコンなど) があります。 それにより、1 つのゾーンのインフラストラクチャ障害が他のゾーンに影響することはありません。 ゾーンは特定のリージョンに属しますが、1 つのリージョンには 1 つ以上のゾーンがあります。 SLB はほとんどのリージョンで複数のゾーンにデプロイされています。 ・ シングルゾーン: SLB インスタンスを 1 つのゾーンにのみでデプロイします。 ・ マルチゾーン: SLB インスタンスを 2 つのゾーンでデプロイします。 デフォルトでは、プライマリゾーンのインスタンスがトラフィックの配信に使用されます。 プライマリゾーンに障害が発生している場合、バックアップゾーンのインスタンスが自動的に負荷分散サービスを引き継ぎます。
プライマリゾーン	SLB インスタンスのプライマリゾーンを選択します。 通常、プライマリゾーンがトラフィックを配信します。

設定項目	説明
バックアップゾーン	SLB インスタンスのバックアップゾーンを選択します。 バックアップゾーンは、プライマリゾーンが使用できない場合にのみトラフィックを引き継ぎます。
インスタンスのスペック	インスタンスのパフォーマンススペックを選択します。 パフォーマンスメトリクスは仕様によって異なります。 詳細については、「パフォーマンス専有型インスタンス」をご参照ください。
インスタンスタイプ	ビジネス需要に応じてインスタンスタイプを選択します。 システムはインスタンスタイプに応じてパブリック IP またはプライベート IP を割り当てます。 詳細については、「SLB インスタンスの概要」をご参照ください。 ・ インターネット: インターネット SLB インスタンスはインターネット IP のみを提供します、インターネットを介して SLB サービスにアクセスできます。 ・ イントラネット: イントラネット SLB インスタンスはプライベート IP のみを提供します、イントラネットを介して SLB サービスにアクセスできます。
IP バージョン	IPv4 を選択します。
ネットワークタイプ	選択したインスタンスタイプがイントラネットの場合、インスタンスのネットワークタイプを指定する必要があります。 ・ クラシックネットワーク: インスタンスの IP は Alibaba Cloud により一元的に割り当てられ、管理されます。 ・ VPC: インスタンスの IP は、ユーザーが指定した VSwitch CIDR ブロックから割り当てられます。
課金	課金方法を選択します。
数量	作成するインスタンスの数量を選択します。

4. [今すぐ購入] をクリックして、支払いを行います。

1.1.4 SLB インスタンスの管理

[インスタンス] ページで、リージョンを選択すると、選択したリージョン内で作成したすべてのインスタンスを表示することができます。 他にも、次の操作が可能です。

・ SLB インスタンスの名前の変更

インスタンス ID にマウスカーソルを合わせ、表示された鉛筆のアイコンをクリックしてインスタンス名を入力します。

- SLB インスタンスの停止

  実行中の SLB インスタンスを選択し、ページ下部の [停止] をクリックするか、[詳細] > [停止] をクリックします。
- SLB インスタンスの起動

  停止中の SLB インスタンスを選択し、ページ下部の [開始] をクリックするか、[詳細] > [開始] をクリックします。
- SLB インスタンスの削除

  SLB インスタンスを選択し、ページ下部の [リリース] をクリックするか、 [詳細] > [リリース] をクリックします。 [リリース] ダイアログボックス内で、インスタンスを直ちにリリースするか、任意の時間にリリースするかを選択することができます。
- タグの設定

  タグを使用してインスタンスを一元的に分類および管理できます。 詳細については、「タグの管理」をご参照ください。
- インスタンス設定の変更

  [詳細] > [設定の変更] をクリックし、インスタンスタイプを変更することができます。
- インスタンスの詳細の表示

  インスタンス ID または [管理] をクリックすることにより、SLB インスタンスの詳細情報を表示することができます。

  - 詳細ページで、[課金の詳細] をクリックし、選択した SLB インスタンスのより詳細な課金状況を表示することができます。

  - [リスナー] をクリックし、リスナーの作成や表示をすることができます。 詳細については、「リスナーの概要」をご参照ください。
  - [サーバー] をクリックし、バックエンドサーバーの追加や表示をすることができます。 詳細は、「#unique_11」をご参照ください。
  - [モニタリング] をクリックし、モニタリング情報の表示やアラームの設定をすることができます。 詳細は、「モニタリングデータの表示」をご参照ください。

1.1.5 タグの管理

SLB が提供するタグ機能では、タグを使用して SLB インスタンスの分類や管理を行うことができます。

各タグはキーと値で構成されています。 タグを使用する場合は、次の制限にご注意ください。

- タグは単独では存在できません。 タグは 1 つ以上の SLB インスタンスに追加する必要があります。
- 最大 10 個のタグを SLB インスタンスにバインドできます。
- インスタンスに追加するタグのキーは一意である必要があります。 一意でない場合、同じキーのタグが上書きされます。
- タグはリージョンを越えて使用することはできません。 リージョン固有のリソースです。 たとえば、中国 (杭州) で作成されたタグは、中国 (上海) では使用できません。

タグの追加

タグを追加するには、次の手順を実行します。

1. SLB コンソールにログインします。
2. [インスタンス] ページでリージョンを選択し、タグを追加するインスタンスを探します。
3. [タグの編集] をクリックします。

4. [タグの編集] ダイアログボックスで、[作成] をクリックし、キーと値を入力します。 [確認] をクリックします。

タグを使用したインスタンスの検索

タグを使用してインスタンスを検索する場合、次の手順を実行します。

1. SLB コンソールにログインします。
2. [インスタンス] ページで、リージョンを選択します。
3. [タグ] をクリックし、タグを選択します。

   指定したタグを持つインスタンスが表示されます。

4. 選択したタグの横にある削除アイコンをクリックすると、フィルタをクリアできます。

タグの削除

タグは、関連付けられているすべてのインスタンスから削除されると削除されます。 一度に複数のタグを削除することはできません。

タグを削除するには、次の手順を実行します。

1. SLB コンソールにログインします。
2. [インスタンス] ページで、リージョンを選択します。
3. タグを削除するインスタンスを探し、[詳細] > [タグの編集] をクリックします。

4. [タグの編集] ダイアログで、削除するタグの [削除] アイコンをクリックしてから [確認] をクリックします。

> 注：
> タグが複数のインスタンスに追加されている場合は、各インスタンスからタグを削除する必要があります。 タグは、どのインスタンスとも関連付けられなくなった時点で、システムから削除されます。

1.1.6 仕様の変更

パフォーマンス共有型インスタンスからパフォーマンス専有型インスタンスに変更したり、パフォーマンス専有型インスタンスの仕様を変更したりすることができます。

インスタンスの仕様を変更する前に、次の点にご注意ください。

- パフォーマンス共有型インスタンスをパフォーマンス専有型インスタンスに変更すると、サービスは10～30 秒間中断することがあります。 サービスのビジー状態を避けて、仕様を変更することを推奨します。
- パフォーマンス共有型インスタンスをパフォーマンス専有型インスタンスに変更した後、元に戻すことはできません。

  代わりに、 パフォーマンス専有型インスタンスに変更した後、(slb.s1.small) 仕様を使用することができます。

1. SLB コンソールにログインします。
2. リージョンを選択します。
3. 目的のインスタンスを検索し、[詳細] > [設定の変更] をクリックします。

4. [アップグレード] ページで、新しい仕様を選択し、支払いを行います。

1.2 リスナー

1.2.1 共有インスタンス帯域幅

SLB は、帯域幅課金の SLB インスタンス内のすべてのインスタンスのリスナーで合計帯域幅を共有することができます。 モニターの作成時、ピーク帯域幅を設定できますが、必須ではありません。

- 設定：リスナーの帯域幅を制限できますが、すべてのリスナーのピーク帯域幅の合計が、インスタンスのピーク帯域幅を超えることはできません。
- 制限なし：帯域幅を制限しない場合、インスタンス内のリスナーでインスタンスの帯域幅を共有します。

帯域幅の共有方法

ピーク帯域幅が 10 MBの SLB インスタンスを購入し、このインスタンスに 3 つのリスナー (リスナー A、リスナー B、リスナー C) を作成したとします。 リスナー A のピーク帯域幅に 4 MB が設定され、他 2 つのリスナーのピーク帯域幅は設定されていません。 3 つのリスナーの帯域幅使用量は、以下のようになります。

- リスナー A とリスナー C でトラフィック不足が起きていない場合、リスナー B の帯域幅は残りの 6 MB (10 MB - 4 MB) になります。
- リスナー C でトラフィック不足が起きておらず、リスナー B で非常に大きいトラフィックが発生した場合、帯域幅は残りの 6 MB を超えます。 この時点で、リスナー B でドロップが発生しますが、 4 MB だけをリッスンすると、設定された帯域幅のピークを超えないため、ドロップは発生しません。
- リスナー A が常にフルスピード (リスナーのピークの 4 MB) で実行されていて、リスナー B とリスナー C も大量のトラフィックをリッスンする場合、リスナー B とリスナー C は残りの 6 MB を共有します。 帯域幅 この時点では、リスナー A のトラフィックはリスナー B とリスナー C の影響を受けません。常に最大 4 MB のピークが確保されています。 リスナー B とリスナー C のトラフィックサイズが同じ場合、2 つのリスナーが使用する帯域幅はほぼ同じです。

したがって、リスナーの帯域幅の制限はリソース予約です。これは、コアビジネスが常に十分な帯域幅を確保できるようにするためです。 コアビジネスでない場合、リスナーの帯域幅の値を設定しなくてもかまいません。インスタンスの残りの帯域幅リソースを競合します。

1.3 バックエンドサーバー

1.3.1 バックエンドサーバーの概要

SLB サービスを使用する前に、配信されたクライアントリクエストを処理するために、1 つ以上の ECS インスタンスをバックエンドサーバーとして SLB インスタンスに追加する必要があります。

バックエンド ECS インスタンスの数はいつでも増減することができます。 ただし、ヘルスチェック機能を有効にすることを推奨します。サービスの安定性を維持するには、正常な ECS が少なくとも 1 つ必要です。

SLB サービスは、同じリージョンに追加された ECS インスタンスを、高性能かつ高可用性を備えたアプリケーションプールに仮想化します。 デフォルトでは、バックエンドサーバーはインスタンス内で管理されます。つまり、SLB インスタンス内のすべてのリスナーは、同じサーバーの同じポートにしかトラフィックを転送できません。

サーバーグループの方法で ECS インスタンスを追加することもできます。 リスナーごとに異なるサーバーグループに関連付けることができるため、SLB インスタンス内のリスナーは、ポートの異なるバックエンドサーバーにリクエストを転送できます。

 注:
リスナーにサーバーグループを設定した後、リスナーは、バックエンドサーバープール内の ECS インスタンスではなく、選択したサーバーグループの ECS インスタンスにリクエストを転送します。

デフォルトサーバーグループ

デフォルトサーバーグループは、フロントエンドリクエストの受信に使用される ECS インスタンスで構成されています。 リスナーが VServer グループにもアクティブ/スタンバイサーバーグループにも関連付けられていない場合、デフォルトサーバーグループ内の ECS インスタンスにリクエストが転送されます。

デフォルトサーバーグループを作成するには、「#unique_19」をご参照ください。

アクティブ/スタンバイサーバーグループ

1 つのバックエンドサーバーをアクティブサーバーとして使用し、もう 1 つをスタンバイサーバーとして使用するという従来のアクティブ/スタンバイ要件がある場合、アクティブ/スタンバイサーバーグループを作成できます。 アクティブサーバーが正常に動作している場合、リクエストはアクティブサーバーへ配信されますが、アクティブサーバーに障害が発生した場合、サービスの中断を避けるため、リクエストはスタンバイサーバーに転送されます。 サービスの中断を避けるには、アクティブ/スタンバイサーバーグループを作成します。

スタンバイサーバーでは、ヘルスチェックは実行されません。 アクティブサーバーに障害が発生した場合、トラフィックはスタンバイサーバーに直接配信されます。 アクティブサーバーのヘルスチェックが成功すると、トラフィックは自動的にそのサーバーに配信されます。

アクティブ/スタンバイサーバーグループは、レイヤー 4 リスナーにのみ使用できます。 詳細については、「アクティブ /スタンバイサーバーグループの作成」をご参照ください。

VServer グループ

異なるバックエンドサーバーに異なるリクエストを配信する必要がある場合、あるいはドメイン名または URL に基づいた転送ルールを設定する場合は、VServer グループを使用できます。 詳細については、「VServer グループの作成」をご参照ください。

注

SLB インスタンスに ECS インスタンスを追加する際は、次の点に注意してください。

- SLB は、クロスリージョンのデプロイに対応していません。 ECS インスタンスのリージョンと、SLB インスタンスのリージョンが同じであることを確認してください。
- SLB は、複数の ECS インスタンスにデプロイされているアプリケーションが同じで、かつデータが一致している限り、ECS インスタンスに使用されるオペレーティングシステムを制限しません。 ただし、管理とメンテナンスを容易にするために、同じオペレーティングシステムを使用することを推奨します。
- SLB インスタンスには最大 50 のリスナーを追加できます。 各リスナーは、ECS インスタンスにデプロイされたアプリケーションに対応しています。 リスナーのフロントエンドポートは、ECS インスタンスで開かれたアプリケーションポートに対応しています。
- ECS インスタンスごとに重みを指定できます。 重み：重み付けの大きい ECS インスタンスは、より多くの接続リクエストを受信します。 サービスの仕様とバックエンド ECS インスタンスのステータスに基づいて重みを設定します。

  > 注：
  > セッション維持機能を有効にしている場合、バックエンド ECS インスタンスに配信されるリクエストは不均衡になる可能性があります。 その場合は、セッション維持機能を無効にして、引き続きこの問題が発生するかどうか確認することを推奨します。

  設定したとおりにバックエンドサーバー間でトラフィックが均等に分散されない場合は、次のトラブルシューティングを行います。

  1. 一定期間の Web サービスのアクセスログを収集します。
  2. 複数の ECS インスタンス間でログの数が異なっているか確認します。 (セッション維持機能が有効になっている場合は、同一 IP アドレスからのアクセスログを取り除く必要があります。 SLB に重みが設定されている場合、ログに記録されたアクセストラフィックの割合が、重みの比率と一致するかどうかを計算する必要があります。)
- ECS インスタンスがライブマイグレーションを実行中の場合、SLB の持続接続は切断されることがありますが、再接続することによって復旧できます。 再接続の準備をしておいてください。

1.3.2 デフォルトサーバーの追加

SLB サービスを使用する前に、少なくとも 1 つのデフォルトサーバーを追加する必要があります。

- SLB インスタンスの作成が済んでいます。
- ECS インスタンスを作成し、転送されたリクエストを処理するアプリケーションをデプロイしています。

1. SLB コンソールにログインします。
2. Server Load Balancer ページで、リージョンを選択します。
3. 対象 の SLB インスタンスの ID をクリックします。
4. デフォルトのサーバーグループ タブをクリックします。
5. 追加 をクリックします。
6. 未追加サーバー ページで、 追加 をクリックします。

   使用可能サーバー ページが表示されます。
7. 対象の ECS インスタンスの横にある 追加 をクリックするか、複数の ECS インスタンスを選択し、選択されたサーバーリストに追加 をクリックします。
8. 表示された 使用可能サーバー ダイアログボックスで、追加した ECS インスタンスの重みを指定して OK をクリックします。

   重み付けの大きい ECS インスタンスは、より多くの接続リクエストを受信します。 ECS インスタンスのサービス仕様に基づいて重みを設定できます。

   > ：
   > 重みが 0 に設定されている場合、その ECS インスタンスにリクエストは送信されません。

   追加された ECS インスタンスの一覧は、 デフォルトのサーバーグループ ページに表示されます。 追加した ECS インスタンスの重みを削除または変更することができます。

1.3.3 VServer グループの作成

仮想サーバーグループ (VServer グループ) は、ECS インスタンスのグループです。 VServer グループを使用すると、リスナーディメンションでバックエンドサーバーを管理およびカスタマイズできます。 Server Load Balancer インスタンス内のリスナーは異なるバックエンドサーバーを使用できます。 つまり、さまざまなリクエストをさまざまなバックエンドサーバーに配信することができます。

- SLB インスタンスの作成を完了している。
- 転送されたリクエストを受信する ECS インスタンスの作成を完了している。

リスナーを設定する際に VServer グループを使用した場合、リスナーは関連付けられた VServer グループにリクエストを配信します。 リスナーは、バックエンドサーバープール内の ECS インスタンスにリクエストを配信しなくなります。

レイヤー 7 リスナーの場合、サーバープールにバックエンドサーバーを追加し、VServer グループを設定し、同時に転送ルールを追加した場合、リクエストは次の順序で配信されます。

- リクエストが転送ルールと一致する場合、このルールに関連付けられた VServer グループにリクエストが配信されます。
- そうでない場合、リクエストはリスナーに関連付けられた VServer グループに配信されます。
- リスナーに VServer グループが設定されていない場合、リクエストはデフォルトサーバーグループの ECS インスタンスに配信されます。

VServer グループを使用するときは、次の制限事項に注意してください。

- リスナーと同じリージョンにあるバックエンドサーバーだけを VServer グループに追加することができます。
- 1 つの ECS インスタンスを複数の VServer グループに追加できます。
- 1 つの VServer グループを複数のリスナーに関連付けることができます。
- VServer グループは、異なるポート番号を持つ複数の ECS インスタンスで構成されています。

1. SLB コンソールにログインします。
2. [インスタンス] ページで、リージョンを選択します。
3. SLB インスタンスの ID をクリックします。
4. 左側のナビゲーションウィンドウで、[サーバー] > [VServer グループ] をクリックします。
5. [VServer グループ] ページで、[VServer グループの作成] をクリックします。
6. [VServer グループの作成] ページで、次の手順に従ってください。

   a. [グループ名] にグループの名前を入力します。

   b. 追加する ECS インスタンスのネットワークタイプを選択します。
7. [使用可能サーバー] 一覧で、追加する ECS インスタンスを選択します。

   選択したインスタンスが、[選択したサーバー] リストに表示されます。
8. [選択したサーバー] リスト内で、ポート番号と重みを入力し、[確認] をクリックします。

   作成された VServer グループは、[VServer グループ] ページに表示されます。 VServer グループの ECS インスタンスを削除、または VServer グループに ECS インスタンスを追加で

きます ([編集] をクリックします)。 この VServer グループをインスタンスのリスナーまたは転送ルールに関連付けることもできます。

1.3.4 マスタースレーブサーバーグループの作成

1 つのバックエンドサーバーをアクティブサーバーとして使用し、もう 1 つをスタンバイサーバーとして使用するという従来のマスタースレーブ要件がある場合、マスタースレーブサーバーグループを作成できます。 アクティブサーバーが正常に動作している場合、リクエストは通常通り転送されますが、 アクティブサーバーに障害が発生した場合、サービスの中断を避けるため、リクエストはスタンバイサーバーに転送されます。

- SLB インスタンスの作成を完了している。
- ECS インスタンスを作成し、転送されたリクエストを処理するアプリケーションをデプロイしている。

リスナーにマスタースレーブサーバーグループが設定された後、リスナーは、バックエンドサーバープール内の ECS インスタンスの代わりに、サーバーグループの ECS インスタンスにリクエストを転送します。

 :

レイヤー 4 リスナー (TCP プロトコルと UDP プロトコル) に対してのみ、マスタースレーブサーバーグループを設定できます。

1. SLB コンソールにログインします。
2. [インスタンス] ページで、リージョンを選択します。
3. SLB インスタンスの ID をクリックします。
4. 左側のナビゲーションウィンドウで、[サーバー] > [マスタースレーブサーバーグループ] をクリックします。
5. [マスタースレーブ サーバーグループ] ページで、[マスタースレーブ サーバーグループ] をクリックします。

6. [マスタースレーブ サーバーグループ] ダイアログボックスで、以下の手順を実行します。
   a) [グループ名] に、グループ名を入力します。
   b) 追加する ECS インスタンスのネットワークタイプを選択します。
   c) [使用可能サーバー] リストから、追加する ECS インスタンスを選択します。
   d) [選択したサーバー] リストに、追加する ECS インスタンスのポート番号と重みを入力し、1 つの ECS インスタンスをスタンバイサーバーとして選択します。 [確認] をクリックします。

1.4 アクセス制御

1.4.1 アクセス制御リストの設定

Server Load Balancer (SLB) には、アクセス制御機能が用意されています。 ユーザーは、リスナーごとに異なるアクセス制御ルール (アクセスホワイトリストまたはブラックリスト) を設定することができます。 リスナーのアクセス制御を設定する前に、アクセス制御リストを設定する必要があります。

現在、アクセス制御機能は以下のリージョンで利用可能です。

- シンガポール
- オーストラリア (シドニー)
- マレーシア (クアラルンプール)
- 日本 (東京)
- 米国 (シリコンバレー)
- 米国 (バージニア)
- ドイツ (フランクフルト)
- UAE (ドバイ)
- インド (ムンバイ)

  他のリージョンでも順次サポートされる予定です。

複数のアクセス制御リストを作成することができます。 リストには複数の IP アドレスや CIDR ブロックが含まれています。 アクセス制御リストの制限事項は次のとおりです。

リソース	制限事項
1 つのリージョン内で作成可能なアクセス制御リストの最大数。	50
一度に追加できる IP アドレスの最大数。	50

リソース	制限事項
アクセス制御リストの最大エントリ数。	300
アクセス制御リストを追加可能なリスナーの最大数	50

アクセス制御リストの作成

1. Server Load Balancer コンソールにログインします。
2. リージョンを選択します。
3. 左側のナビゲーションウィンドウで、[アクセス制御] をクリックします。
4. [アクセス制御リストの作成] をクリックした後、リストの名前を入力し、[確認] をクリックします。

IP エントリの追加

1. Server Load Balancer コンソールにログインします。
2. リージョンを選択します。
3. 左側のナビゲーションウィンドウで、[アクセス制御] をクリックします。
4. 目的のアクセス制御リストを検索して、[管理] をクリックします。
5. IP エントリを追加します。

   - [複数のエントリの追加] をクリックした後、表示されたダイアログボックスに 1 つ以上の IP アドレスまたは CIDR ブロックを追加します。

     エントリを追加する際、次の点に注意してください。

     - 1 行につき 1 エントリです。 Enter キーで改行します。
     - IP アドレスまたは CIDR ブロックと、コメントを区切るには、“|” を使用します。
       例：192.168.1.0/24|メモ

   - [エントリの追加] をクリックしてから、IP アドレスまたは CIDR ブロックを追加します。[確認] をクリックし、アクセス制御リストにエントリを追加します。

IP エントリの削除

1. Server Load Balancer コンソールにログインします。
2. リージョンを選択します。
3. 左側のナビゲーションウィンドウで、[アクセス制御] をクリックします。

4. 目的のアクセス制御リストを見つけ、[管理] をクリックします。
5. 対象の IP アドレスの [操作] で [削除] をクリックするか、複数の IP エントリを選択して、エントリ一覧の下にある [削除] をクリックします。
6. 表示されたダイアログボックスで、[確認] をクリックします。

1.4.2 新しいアクセス制御リストへの移行

既にリスナーにホワイトリストが設定されている場合、Server Load Balancer は、ホワイトリスト内の IP アドレスまたは CIDR ブロックをアクセス制御リストに自動的に追加し、そのリストをリスナーに適用します。

ホワイトリストからアクセス制御リストへの移行

以前に設定したホワイトリストをアクセス制御リストに移行するには、以下の手順に従います。

1. SLB コンソールにログインします。
2. SLB インスタンスのリージョンを選択し、目的の SLB インスタンスの ID をクリックします。
3. 左側のナビゲーションウィンドウで、[リスナー] をクリックします。
4. 目的のリスナーを見つけ、[詳細] > [アクセス制御の設定] をクリックします。
5. [新しいアクセス制御機能の使用] をクリックします。
6. アクセス制御リストの名前を入力し、[アクセス制御リストの作成] をクリックします。
7. [適用] をクリックして、ホワイトリストとしてリストをリスナーに適用します。

> 注：
> リストをリスナーに適用しないと、ホワイトリストは有効になりません。

移行したアクセス制御リストの表示

移行したアクセス制御リストを表示するには、以下の手順に従います。

1. SLB コンソールにログインします。
2. リージョンを選択します。
3. 左側のナビゲーションウィンドウで、[アクセス制御] をクリックします。
4. 作成済みのアクセス制御リストを検索し、関連付けられたリスナーを表示します。 [管理] をクリックして、IP エントリを管理することもできます。

1.4.3 ホワイトリストの設定

ホワイトリストはアクセス制御方式の 1 つです。 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。

> 注 :
> SLB は、新しいバージョンのアクセス制御機能を公開しており、ホワイトリストとブラックリストの両方を設定できます。 以前に設定したホワイトリストを新しいバージョンに移行できます。 詳細については、「#unique_30」をご参照ください。

ホワイトリストを設定する際、次の点に注意してください。

- ホワイトリストを有効にした場合、ビジネス上のリスクをもたらす可能性があります。 ホワイトリストの設定後、リスト内の IP アドレスのみが SLB インスタンスのリスナーにアクセスできます。
- アクセス制御リストに IP エントリを追加せずにホワイトリストを有効にすると、リクエストは転送されません。
- ホワイトリストを設定すると、一時的に SLB リスナーへのアクセスが中断される場合があります。

1. SLB コンソールにログインします。
2. SLB インスタンスの存在するリージョンを選択します。
3. SLB インスタンスの ID をクリックします。
4. 左側のナビゲーションウィンドウで、[リスナー] をクリックします。
5. 目的のリスナーを見つけ、[詳細] > [アクセス制御の設定] をクリックします。
6. 表示されたダイアログボックスで、以下の手順を実行します。
   a) [アクセス制御の有効化] スイッチをクリックします。
   b) リスナーへのアクセスを許可する IP アドレスを入力します。
      複数の IP アドレスを指定する場合、カンマで区切ります。 最大 300 個の IP アドレスを指定できます。 CIDR ブロックを入力することもできます。
   c) [確認] をクリックします。

1.5 証明書管理

1.5.1 証明書の要件

Server Load Balancer では、PEM 形式の証明書のみに対応しています。 証明書、証明書チェーン、秘密鍵が、このセクションで説明されている規則に準拠していることを確認してください。

ルート CA 発行の証明書

ルート CA 発行の証明書の場合、Server Load Balancer にアップロードする必要があるのは、受け取った証明書だけです。 この証明書が設定されたWebサイトは、追加の証明書を設定しなくても Webブラウザーから信頼されます。

証明書の形式は、次の要件を満たす必要があります。

- 証明書の内容は、`----- BEGIN  CERTIFICAT  E -----`, `----- END  CERTIFICAT  E -----` の間に記載されています。 証明書をアップロードする際、このヘッダーとフッターも含めます。
- 各行 (最後の行を除く) は 64 文字にする必要があります。 最後の行は、64 文字以下にすることができます。
- 内容に空白文字を含めることはできません。

ルート CA 発行の証明書のサンプルを以下に示します。

中間 CA 発行の証明書

中間 CA 発行の証明書の場合、複数の中間証明書を受け取ります。 まずサーバー証明書と中間証明書を結合してから、Server Load Balancer にアップロードする必要があります。

証明書チェーンの形式は、以下の要件を満たす必要があります。

- サーバー証明書を先頭部分に記載し、その後ろに空白文字を入れずに中間証明書を記載します。
- 内容に空白文字を含めることはできません。
- 各行 (最後の行を除く) は 64 文字にする必要があります。 最後の行は、64文字以下にすることができます。 詳細については、『RFC1421』をご参照ください。
- 証明書の説明文書に記載されている証明書の要件に準拠しています。 一般的に、中間 CA は証明書の発行時に証明書の形式に関する説明文書を提供します。証明書チェーンは、その形式の要件に従う必要があります。

証明書チェーンのサンプルを以下に示します。

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

RSA 秘密鍵

サーバー証明書をアップロードする際、証明書の秘密鍵もアップロードする必要があります。

RSA 秘密鍵の形式は、以下の要件を満たす必要があります。

- 鍵は、`-----BEGIN RSA PRIVATE KEY-----`, `-----END RSA PRIVATE KEY-----` の間に記載されています。 鍵をアップロードする際、このヘッダーとフッターも含めます。
- 内容に空白文字を含めることはできません。 各行 (最後の行を除く) は 64 文字にする必要があります。 最後の行は、64文字以下にすることができます。 詳細は『RFC1421』をご参照ください。

秘密鍵が暗号化されている場合、 たとえばヘッダーとフッターが `-----BEGIN PRIVATE KEY-----`, `-----END PRIVATE KEY-----` か、`-----BEGIN ENCRYPTED PRIVATE KEY-----`, `-----END ENCRYPTED PRIVATE KEY-----` であるか、秘密鍵に `Proc-Type: 4,ENCRYPTED` が含まれている場合、以下のコマンドを実行して秘密鍵を変換してから、Server Load Balancer にアップロードしてください。

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

RSA 秘密鍵のサンプルを以下に示します。

1.5.2 CA 証明書の生成

HTTPS リスナーを設定する際、自己署名 CA 証明書を使用することができます。 このドキュメントの手順に従って、CA 証明書を生成し、作成された CA 証明書を使用してクライアント証明書に署名します。

Open SSL を使用した CA 証明書の生成

1. 次のコマンドを実行して、*/root* ディレクトリに *ca* フォルダーを作成し、 *ca* フォルダーに 4 つのサブフォルダーを作成します。

   ```
   $ sudo mkdir ca
   ```

```
$ cd ca
$ sudo mkdir newcerts private conf server
```

- *newcerts* フォルダーには、CA 証明書によって署名されたデジタル証明書が保存されます。
- *private* フォルダーには、CA 証明書の秘密鍵が保存されます。
- *conf* フォルダーには、設定ファイルが保存されます。
- *server* フォルダーには、サーバー証明書が保存されます。

2. conf ディレクトリに open-USssl.conf ファイルを作成し、次の情報を書き込みます。

```
[ ca ]
default_ca = foo
[ foo ]
dir = / root / ca
database = / root / ca / index . txt
new_certs_ dir = / root / ca / newcerts
certificat e = / root / ca / private / ca . crt
serial = / root / ca / serial
private_ke y = / root / ca / private / ca . key
RANDFILE = / root / ca / private /. rand
default_da ys = 365
default_cr l_days = 30
default_md = md5
Unique_sub ject = No
Policy = policy_any
[ policy_any ]
countryNam e = match
stateOrPro vinceName = match
organizati onName = match
organizati onalUnitNa me = match
localityNa me = optional
commonName = supplied
emailAddre ss = optional
```

3. 次のコマンドを実行して、秘密鍵を生成します。

```
$ cd / root / ca
$ sudo openssl genrsa - out private / ca . key
```

秘密鍵を生成する例を以下に示します。

4. 次のコマンドを実行して、プロンプトに従って必要な情報を入力します。 Enter キーを押して、 *csr* ファイルを生成します。

```
$ sudo openssl req - new - key private / ca . key - out
private / ca . csr
```

注：

コモンネームは、SLB インスタンスのドメイン名です。

5. 次のコマンドを実行して、 *crt* ファイルを生成します。

```
$ sudo openssl x509 -req -days 365 -in private/ca.csr -signkey private/ca.key -out private/ca.crt
```

6. 次のコマンドを実行して、秘密鍵の開始シーケンス番号を設定します。シーケンス番号には、任意の 4 文字を使用できます。

```
$ sudo echo FACE > serial
```

7. 次のコマンドを実行して、CA 鍵ライブラリを作成します。

```
$ sudo touch index.txt
```

8. 次のコマンドを実行して、クライアント証明書を削除するための証明書失効リストを作成します。

```
$ sudo openssl ca -gencrl -out /root/ca/private/ca.crl -crldays 7 -config "/root/ca/conf/openssl.conf"
```

次のレスポンスが返されます。

```
Using configuration from /root/ca/conf/openssl.conf
```

クライアント証明書の署名

1. 次のコマンドを実行して、クライアント鍵を保存する *users* ディレクトリを *ca* ディレクトリの下に生成します。

```
$ sudo mkdir users
```

2. 次のコマンドを実行して、クライアント証明書の鍵を作成します。

```
$ sudo openssl genrsa -des3 -out /root/ca/users/client.key 1024
```

注:

鍵を作成する際、パスフレーズを入力します。パスフレーズは、不正なアクセスから秘密鍵を保護するためのパスワードです。入力されたパスフレーズは、この鍵のパスワードになります。

3. 次のコマンドを実行して、証明書署名リクエストのための *csr* ファイルを作成します。

```
$ sudo openssl genrsa -des3 -out /root/ca/users/client.key 1024
```

```
            / root / ca / users / client . csr
```

プロンプトが表示されたら、前の手順で設定したパスフレーズを入力します。

注：

チャレンジパスワードは、クライアント証明書のパスワードです。 クライアント鍵のパスワードではありません。

4. 次のコマンドを実行して、クライアント鍵に署名します。

```
$ sudo openssl ca - in / root / ca / users / client . csr -
 cert / root / ca / private / ca . crt - keyfile
          / root / ca / private / ca . key - out / root / ca /
 users / client . crt - config
          "/ root / ca / conf / openssl . conf "
```

プロンプトが表示されたら、どちらのプロンプトにも y と入力します。

5. 次のコマンドを実行して、証明書を *PKCS12* ファイルに変換します。

```
$ sudo openssl pkcs12 - export - clcerts - in / root / ca /
 users / client . crt - inkey
          / root / ca / users / client . key - out / root / ca /
 users / client . p12
```

プロンプトが表示されたら、クライアント鍵のパスワードを入力します。 次に、クライアント証明書のエクスポートに使用するパスワードを入力します。 これはクライアント証明書を保護するためのパスワードです。クライアント証明書をインストールするときに必要です。

6. 生成されたクライアント証明書を表示するには、次のコマンドを実行します。

```
cd users
ls
```

1.5.3 証明書形式の変換

Server Load Balancer は、PEM 証明書のみに対応します。 他の形式の証明書は、PEM 形式に変換してから、Server Load Balancer にアップロードする必要があります。 形式の変換には、Open SSLを使用することを推奨します。

DER を PEM に変換

DER ：一般的に、この形式は Java プラットフォームで使用されます。

- 次のコマンドを実行して、証明書の形式を変換します。

```
openssl x509 -inform der -in certificat e.cer -out
certificat e.pem
```

- 次のコマンドを実行して、秘密鍵を変換します。

```
openssl rsa -inform DER -outform PEM -in privatekey.
der -out privatekey.pem
```

P7B を PEM に変換

P7B：一般的に、この形式は Windows Server および Tomcat で使用されます。

次のコマンドを実行して、証明書の形式を変換します。

```
openssl pkcs7 -print_cert s -in incertific ate.p7b -out
  outcertifi cate.cer
```

PFX を PEM に変換

PFX: 一般的に、この形式は Windows Server で使用されます。

- 次のコマンドを実行して、証明書を取り出します。

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.
pem
```

- 次のコマンドを実行して、秘密鍵を取り出します。

```
openssl pkcs12 -in certname.pfx -nocerts -out key.
pem -nodes
```

1.5.4 証明書のアップロード

HTTPS リスナーを作成する前に、必要なサーバー証明書と CA 証明書を SLB にアップロードする必要があります。 証明書を SLB にアップロードすれば、バックエンドサーバーで証明書を設定する必要がなくなります。

- サーバー証明書を購入していること。
- CA 証明書とクライアント証明書を生成済みであること。 詳細については、「#unique_36」をご参照ください。

証明書をアップロードする前に、次の点に注意してください。

- SLB の証明書はリージョンごとのリソースです。 1 つの証明書を複数のリージョンで使用する場合は、すべてのリージョンに証明書をアップロードする必要があります。
- 1 アカウントにつき、最大 100 の証明書をアップロードできます。

1. SLB 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、[証明書] をクリックします。
3. [証明書のアップロード] をクリックします。
4. [証明書の作成] ページで、証明書の内容をアップロードし、[OK] をクリックします。

設定項目	説明
証明書名	証明書の名前を入力します。 名前は、1～80 文字です。文字、数字、および以下の特殊文字を使用できます。 _/. -
証明書のリージョン	証明書をアップロードするリージョンを 1 つ以上選択します。 このリージョンは、HTTPS リスナーが配置されている場所です。 複数のリージョン間で 1 つの証明書を使用することはできません。
証明書のタイプ	証明書のタイプを選択します。 ・ [サーバー証明書]：1 方向認証には、サーバー証明書のみが必要です。 クライアントはこれを使用して、サーバーから送信された証明書が信頼できる認証局で発行されているかどうかをチェックします。 ・ [CA 証明書]：双方向認証には、CA 証明書とサーバー証明書が必要です。 サーバーは、安全な接続を開始する前に、CA 証明書を使用してクライアント証明書の CA 署名を権限付与の一部として認証します。
証明書の内容	証明書の内容をエディターに貼り付けます。 有効な証明書の形式を表示するには、[サンプルのインポート] をクリックします。 PEM 形式の証明書のみに対応しています。 詳細については、「#unique_37」をご参照ください。
秘密鍵	サーバー証明書の秘密鍵をエディターに貼り付けます。 有効な証明書の形式を表示するには、[サンプルのインポート] をクリックします。 詳細については、「#unique_37」をご参照ください。 ： 秘密鍵は、サーバー証明書をアップロードする場合に必要です。

1.6 ログ管理

1.6.1 操作ログの表示

SLB インスタンス、HTTP リスナー、およびサーバー証明書に対して、過去 1 か月以内に実行された操作のログを確認できます。

操作ログは、ActionTrail に記録されます。 ActionTrail では、Alibaba Cloud のリソースに対する操作が記録されます。これらの記録を使用してアカウントのセキュリティの分析、リソースに対する変更の追跡、コンプライアンスの遵守を行うことができます。

1. SLB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、[ログ] > [操作ログ] をクリックします。
3. [操作ログの表示] をクリックします。
4. [履歴検索] ページで、以下の手順を実行して操作ログを表示します。
   a) フィルターとして [リソースタイプ] を選択します。
   b) どの SLB リソースの操作ログを表示するのかを選択します。
      この例では、[LoadBalancer] が選択されています。
   c) イベントタイプを選択します。
      この例では、[全タイプ] が選択されています。
   d) 検索の時間範囲を選択します。
   e) [検索] をクリックすると、選択したリソースに対する操作ログが表示されます。
      さらに詳しい情報を表示するには、リソースを展開します。

1.6.2 アクセスログの設定

Log Service を使用して、SLB インスタンスのアクセスログを分析することにより、クライアントユーザーの動作や地理的分布を理解したり、問題をトラブルシューティングしたりできます。

アクセスログの概要

SLB アクセスログは、SLB インスタンスに送信された全リクエストの詳細情報 (リクエスト時間、クライアント IP アドレス、レイテンシ、リクエスト URL、サーバーレスポンスなど) を収集します。 インターネットアクセスの入り口として、SLB は大量のクライアントリクエストを受信します。 クセスログを使用することで、ユーザーの動作や地理的な分布を分析し、問題のトラブルシューティングを行うことができます。

SLB アクセスログを有効にすると、アクセスログが Logstore に保存され、分析が可能になります。 アクセスログは、いつでも無効にすることができます。

SLB アクセスログに追加料金は発生しません。 ただし、Log Service を使用すると、通信費が徴収されます。 OSS にログを保存した場合、ストレージコストを節約できます。

注 :

レイヤー 7 SLB のみ、アクセスログの設定をサポートしています。この機能は現在、すべてのリージョンで使用可能です。

SLB アクセスログの利点

Server Load Balancer アクセスログには、次の利点があります。

- シンプルなログ処理

  開発者や保守スタッフは、煩雑で時間のかかるログ処理から解放され、ビジネス開発や技術調査に集中できるようになります。
- 費用対効果

  SLB アクセスログの分量は非常に多いため、アクセスログを処理する際、パフォーマンスとコストの問題を考慮する必要があります。 Log Service と統合されており、自己構築型のオープンソースソリューションよりもアクセスログの処理速度が早く、費用対効果に優れています。 Log Service は、1 秒間に 1 億件のログを分析可能です。
- リアルタイム

  DevOps、モニタリング、アラートなどのシナリオには、リアルタイムのログデータが必要です。 従来のデータストレージや分析ツールでは、この要件を満たすことができません。 たとえば、データ統合に多くの作業を費やす Hive でデータの ETL 処理を行うには長時間かかります。 Log Service は、強力なコンピューティング機能によって、アクセスログを数秒で処理、分析することができます。
- 柔軟性

  インスタンス仕様に合わせて、SLB アクセスログを有効または無効にすることができます。また、必要に応じて保存期間 (1～365 日) を設定できるほか、ビジネスサービスの要件の拡大に合わせて、Logstore の容量を拡張できます。

アクセスログの設定

アクセスログを設定する前に、次の点を確認してください。

1. レイヤー 7 リスナーが追加されていること。
2. Log Service が有効化されていること。

アクセスログを設定するには、次の手順に従います。

1. SLB 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、[ログ] > [アクセスログ] をクリックします。
3. [権限付与] をクリックし、[権限付与ポリシーに同意] をクリックして、Log Service へのログの書き込みを Server Load Balancer に許可します。

    注：
   RAM ユーザーの場合、SLB アクセスログの使用権限が付与されている必要があります。 詳細については、「RAM ユーザーにアクセスログの使用を許可」 をご参照ください。

4. [アクセスログ] ページで、対象の SLB インスタンスを探し、[設定] をクリックします。

5. Log Service プロジェクトと Logstore を選択し、[設定] をクリックします。

   使用可能な Logstore が存在しない場合、[作成] をクリックします。 プロジェクト名が一意であることを確認してください。

    注：
   Log Service プロジェクトと SLB インスタンスが同じリージョンにあることを確認してください。

6. データインポートの設定

   a. [データインポートウィザード] リンクをクリックし、データインポートの設定をします。または、[設定] をクリックし、Log Service コンソール上で後からデータインポートの設定をします。 このチュートリアルでは、[データインポートウィザード] リンクが選択されています。

   b. [次へ] をクリックします。

   c. Log Service には、事前に構成された SLB 用のインデックスフィールドがあります。 [次へ] をクリックします。

       注：

インデックス検索を有効にすると、トラフィックのインデックス作成に対し料金が発生します。

d. [設定] をクリックし、データインポートを完了します。

アクセスログの検索と分析

SLB アクセスログ設定後、次のフィールドを使用してログの検索と表示を行うことができます。

フィールド	説明
body_bytes_sent	クライアントに送信された HTTP 本文のサイズ (バイト)。
client_ip	クライアント IP。
host	リクエスト内のホストヘッダー。
http_user_agent	受信したリクエスト内の http_user_agent ヘッダー。
request_length	リクエストの長さ (startline、HTTP ヘッダー、HTTP 本文を含む)。
request_method	リクエスト方式。
request_time	SLB が最初のリクエストを受信してからレスポンスを返すまでの時間。
request_uri	受信したリクエストの URI。
slbid	SLB インスタンスの ID。
status	SLB が送信したレスポンスステータスコード。
upstream_addr	バックエンドサーバーの IP アドレスとポート番号。
upstream_response_time	SLB がバックエンドサーバーにリクエストを送信してから、クライアントにレスポンスを送信するまでの時間。
upstream_status	バックエンドサーバーから送信されたレスポンスステータスコード。

アクセスログの検索

アクセスログを検索するには、次の手順に従います。

1. ログの検索ページに移動します。 検索ページには、 SLB コンソールまたは Log Service コンソールから移動できます。

   ・ SLB コンソールからの場合

   [アクセスログ] ページで、[ログの表示] をクリックします。

   ・ Log Service コンソールからの場合

   [Logstores] ページで、目的の Logstore の [検索] をクリックします。

2. 対応するインデックスフィールドをクリックすると、詳細情報が表示されます。

3. SQL 文を入力し、クエリを実行します。

   たとえば、上位 20 位のクライアントを照会するには、次の SQL 文を入力します。

```
* | select ip_to_prov ince ( client_ip ) as client_ip_
 province , count (*) as pv group by
      client_ip_ province order by pv desc limit 50
```

アクセスログの分析

アクセスログは、ダッシュボードを使用して分析できます。このダッシュボードには、さまざまなグラフィック情報が提供されます。

アクセスログを分析するには、次の手順に従います。

1. Log Service コンソールで、目的のプロジェクトのプロジェクト名をクリックします。
2. 左側のナビゲーションウィンドウで、[LogSearch/Analytics - 照会] > [ダッシュボード] をクリックし、 [表示] をクリックします。

   上位クライアント、上位ホスト、ステータスコードなどの情報を確認できます。

アクセスログの無効化

アクセスログを無効化するには、次の手順を実行します。

1. SLB 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、[ログ] > [アクセスログ] をクリックします。
3. 対象のインスタンスを検索して、[削除] をクリックします。

1.6.3 RAM ユーザーにアクセスログの設定権限を付与

RAM ユーザーがアクセスログ機能の使用を開始する前に、プライマリアカウントによる権限付与が必要です。

1. 権限付与ポリシーを作成します。
   a) プライマリアカウントで RAM コンソールにログインします。
   b) 左側のナビゲーションウィンドウで、[ポリシー] をクリックし、[権限付与ポリシーの作成] をクリックします。

   c) [空白のテンプレート] をクリックします。

   d) ポリシー名 (例: SlbAccessLogPolicySet) を入力して、次のポリシーを入力します。 [権限付与ポリシーの作成] をクリックします。

```
{
" Statement ": [
 {
   " Action ": [
     " slb : Create *",
     " slb : List *"
   ],
   " Effect ": " Allow ",
   " Resource ": " acs : log :*:*: project /*"
 },
 {
   " Action ": [
     " log : Create *",
     " log : List *"
   ],
   " Effect ": " Allow ",
   " Resource ": " acs : log :*:*: project /*"
 },
 {
   " Action ": [
     " log : Create *",
     " log : List *",
     " log : Get *",
     " log : Update *"
   ],
   " Effect ": " Allow ",
   " Resource ": " acs : log :*:*: project /*/ logstore /*"
 },
 {
   " Action ": [
     " log : Create *",
     " log : List *",
     " log : Get *",
     " log : Update *"
   ],
   " Effect ": " Allow ",
   " Resource ": " acs : log :*:*: project /*/ dashboard /*"
 },
 {
```

```
    " Action ": " cms : QueryMetri  c *",
    " Resource ": "*",
    " Effect ": " Allow "
  },
  {
    " Action ": [
      " slb : Describe *",
      " slb : DeleteAcce  ssLogsDown  loadAttrib  ute ",
      " slb : SetAccessL  ogsDownloa  dAttribute ",
      " slb : DescribeAc  cessLogsDo  wnloadAttr  ibute "
    ],
    " Resource ": "*",
    " Effect ": " Allow "
  },
  {
    " Action ": [
      " ram : Get *",
      " ram : ListRoles "
    ],
    " Effect ": " Allow ",
    " Resource ": "*"
  }
],
" Version ": " 1 "
}
```

a) [閉じる] をクリックします。

2. 作成したポリシーを RAM ユーザーに割り当てます。

a) 左側のナビゲーションウィンドウで、[ユーザー] をクリックします。

b) 対象のユーザー (SLB アクセスログ機能を使用するユーザー) を検索して、[許可] をクリックします。

c) 作成した権限付与ポリシーを検索して、RAM ユーザーに割り当てます。

d) [OK] をクリックします。

e) [ユーザー権限付与ポリシー] ページに移動し、作成したポリシーが、対象の RAM ユーザーに割り当てられているかどうかを確認します。

1.6.4 ヘルスチェックログの管理

[ヘルスチェックログ] ページには、3 日以内のヘルスチェックログが表示されます。3 日以上前のヘルスチェックログが必要な場合は、ヘルスチェックログを OSS に保存します。 こうすることで、完全なヘルスチェックログをダウンロードできます。

ヘルスチェックログの保存

ヘルスチェックログ機能を使用すると、バックエンドサーバーのヘルスチェックログを表示することができます。 現在、3 日分のログが提供されます。 さらに多くの日数分のログを表示する場合は、ヘルスチェックログを OSS に保存してください。

ストレージ機能は、いつでも有効または無効にすることができます。ストレージ機能を有効にすると、選択したバケットに、ヘルスチェックログの保存用フォルダー `AliyunSLBHealthCheck Logs` が作成されます。 ヘルスチェックログは 1 時間単位で生成されます。日付をフォルダー名とするサブフォルダーが作成され、その日に生成されたログファイルが保存されます (例: `20170707`)。

1 日のログファイルには、生成された時刻に基づいて名前が付けられます。 たとえば、00:00 から 01:00 の間に生成されたログファイルの名前は `01.txt` 、01:00 から 02:00 の間に生成されたログファイルの名前は `02.txt` となります。

> 注 :
> ヘルスチェックログは、バックエンドサーバーが正常に稼働していない場合にのみ生成されます。 1 時間の間にどのバックエンドサーバーでもエラーが発生しなかった場合、その時間帯のヘルスチェックログは生成されません。

ヘルスチェックログを保存するには、以下の手順に従います。

1. バケットを作成する
2. SLB に OSS へのアクセスを許可する
3. ログストレージを設定する

手順 1: バケットを作成する

1. OSS プロダクトページを開き、[今すぐ購入] をクリックして OSS サービスを有効化します。
2. OSS コンソールにログインします。
3. [バケットの作成] をクリックします。

4. [バケットの作成] ダイアログボックスで、バケットを設定し、[OK] をクリックします。

> 注 :
> バケットのリージョンと SLB インスタンスのリージョンが同じであることを確認します。

手順 2: SLB に OSS へのアクセスを許可する

バケットを作成したら、OSS リソースにアクセスするためのログロール (`SLBLogDefaultRole`) を許可する必要があります。

> :
> 許可の操作は、初回設定時にのみ必要です。

1. SLB コンソールで、[ログ] > [ヘルスチェックログ] をクリックします。
2. OSS がまだ有効化されていない場合は、[1. OSS の有効化] をクリックします。
3. [ヘルスチェックログ] ページで、[今すぐロールを追加] をクリックします ([2. RAM ロールをアカウントに追加] セクションにあります)。
4. 許可の説明を読み、[権限付与ポリシーに同意] をクリックします。

5. RAM コンソールにログインします。
6. 左側のナビゲーションウィンドウで、[ロール] をクリックし、SLBLogDefaultRole という名前のロールを見つけて [許可] をクリックします。
7. [ロールの権限付与ポリシーの編集] ダイアログボックスで、AliyunOSSFullAccess ポリシーを検索し、[OK] をクリックします。

   許可後、[SLBLogDefaultRole] をクリックし、[ロールの権限付与ポリシー] をクリックすると、割り当てられているポリシーが表示されます。

手順 3: ログストレージを設定する

1. SLB 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、[ログ] > [ヘルスチェックログ] をクリックします。
3. [ヘルスチェックログ] ページで、[ストレージ] をクリックします。
4. 対象のリージョンの [Logstore の設定] リンクをクリックします。

5. [Logstore の設定] ダイアログボックスで、ヘルスチェックログを保存するバケットを選択し、[確認] をクリックします。
6. ステータススイッチをクリックしてログの保存を有効にします。

ヘルスチェックログの表示

3 日間のヘルスチェックログを表示するには、次の手順を実行します。

1. SLB コンソールにログインします。
2. SLB コンソールにログインします。
3. 左側のナビゲーションウィンドウで、[ログ] > [ヘルスチェックログ] をクリックします。
4. [ヘルスチェックログ] ページで、[ログの表示] タブをクリックします。

注：
ヘルスチェックログは、バックエンドサーバーのヘルスステータスが異常の場合にのみ生成されます。 1 時間の間にどのバックエンドサーバーでもエラーが発生しなかった場合、その時間帯のヘルスチェックログは生成されません。

- `SLB_instan ce_IP : port to Added_ECS_ instance_I P : port abnormal ; cause : XXX` というログメッセージは、バックエンドサーバーが正常に稼働していないことを示しています。 エラーメッセージの詳細に従ってトラブルシューティングを行います。
- `SLB_instan ce_IP : port to Added_ECS_ instance_I P : port normal` というログメッセージは、バックエンドサーバーが正常な状態に戻ったことを示しています。

ヘルスチェックログのダウンロード

OSS に保存されているヘルスチェックログをダウンロードできます。

1. OSS コンソールにログインします。
2. [概要] ページで、対象のバケットをクリックし、[ファイル] をクリックします。
3. [ファイル] ページで、 *AliyunSLBH ealthCheck Logs /* をクリックします。

4. ダウンロードするヘルスチェックログのフォルダーをクリックします。

5. 対象フォルダーの [編集] をクリックします。 表示されたページで [ファイル URLのコピー] をクリックします。

6. コピーした URL を Web ブラウザーにを入力して、ログをダウンロードします。

1.7 モニタリング

1.7.1 モニタリングデータの表示

CloudMonitor サービスを使用して、SLB リスナーの接続数や QPS、その他のトラフィック情報を表示できます。

1. SLB コンソールにログインします。
2. 目的の SLB インスタンスが存在するリージョンをクリックします。
3. SLB インスタンスの ID をクリックします。
4. 左側のナビゲーションウィンドウで、[モニタリング] をクリックします。
5. 表示したいモニタリングメトリクスをクリックします。

SLB では、次のモニタリングメトリクスの表示がサポートされています。

モニタリングメトリクス	説明
トラフィック	・ インバウンドトラフィック: 外部アクセスによって消費されたトラフィック ・ アウトバウンドトラフィック: Server Load Balancer によって消費されたトラフィック
パケット	・ インバウンドパケット: 1 秒間に受信したリクエストパケット数 ・ アウトバウンドパケット: 1 秒間に送信されたレスポンスパケット数
同時接続数	・ アクティブ接続: 確立された TCP 接続数。 永続接続を使用している場合、一度の接続で複数のファイルリクエストを同時に送信できます。 ・ 非アクティブ接続: 接続が確立されていない状態の TCP 接続数。 `netstat -an` コマンドを使用して、アクティブな接続数を表示できます。 ・ 同時接続: TCP 接続の総数。

モニタリングメトリクス	説明
新規接続	統計期間中にクライアントと Server Load Balancer との間に確立された新規 TCP 接続の平均数
トラフィックロス	・ インバウンドトラフィックロス: 1 秒間にドロップされたインバウンドトラフィック量 ・ アウトバウンドトラフィックロス: 1 秒間にドロップされたアウトバウンドトラフィック量
パケットロス	・ インバウンドパケットロス: 1 秒間にドロップされたインバウンドパケット数 ・ アウトバウンドパケットロス: 1 秒間にドロップされたアウトバウンドパケット数
接続ロス	1 秒間にドロップされた TCP 接続数
以下のメトリクスは、レイヤー 7 リスナーに固有のメトリクスです。	
QPS	1 秒間に処理できる HTTP または HTTPS リクエスト数
RT	Server Load Balancer の平均レスポンス時間
ステータスコード(2XX)/(3xx)/(4xx)(5xx)(その他)	リスナーによって生成された HTTP レスポンスコードの平均数
UpstreamCode4XX/5XX	バックエンドサーバーによって生成された HTTP レスポンスコードの平均数
UpstreamRT	バックエンドサーバーの平均レスポンス時間

1.7.2 アラームルールの設定

CloudMonitor サービスを有効化した後、CloudMonitor コンソール上で SLB インスタンスのアラームルールを設定できます。

注:
リスナーまたは SLB インスタンスが削除されると、これに応じてアラーム設定も削除されます。

1. SLB コンソールにログインします。
2. リージョンを選択し、ターゲット SLB インスタンスの ID をクリックします。

:
インスタンスにリスナーが設定されていること、およびヘルスチェックが有効になっていること確認します。

3. 左側のナビゲーションウィンドウで、[モニタリング] をクリックします。

4. [しきい値アラーム設定] をクリックします。 CloudMonitor コンソールに移動します。

5. [アラームルールの作成] をクリックします。
6. アラームルールを設定します。

1.8 Anti-DDoS Basic

インターネット SLB インスタンスの Alibaba Cloud Security のしきい値は、SLB コンソールで確認できます。

Anti-DDoS Basic の概要

Alibaba Cloud は、最大 5Gbps の基本的な DDoS に対する防御機能を SLB に提供します。 次の図に示すように、インターネットからのすべてのトラフィックは、SLB に到着する前にまず Alibaba Cloud Security を通過する必要があります。 Anti-DDoS Basic は、一般的な DDoS 攻撃のクリーニングとフィルタリングを行い、SYN フラッド、UDP フラッド、ACK フラッド、ICMP フラッド、DNS クエリーフラッドなどの攻撃からサービスを保護します。

Anti-DDoS Basic は、インターネット SLB インスタンスの帯域幅に応じて、クリーニングしきい値とブラックホールしきい値を設定します。 インバウンドトラフィックがしきい値に達すると、クリーニングまたはブラックホールがトリガーされます。

- クリーニング: インターネットからの攻撃トラフィックがスクラブしきい値を超えた場合、あるいは特定の攻撃トラフィックモデルと一致した場合、Alibaba Cloud Security は攻撃トラフィックのクリーニングを開始します。 クリーニングには、パケットフィルタリング、トラフィック速度制限、パケット速度制限などが含まれます。
- ブラックホール: インターネットからの攻撃トラフィックがブラックホールしきい値を超えた場合、ブラックホールがトリガーされ、すべてのインバウンドトラフィックがドロップされます。

しきい値の確認

SLB コンソール上で、インスタンスのしきい値を確認できます。 RAM アカウントを使用してしきい値を確認できない場合、システム管理者に権限付与を依頼してください。 詳細は、「Anti-DDoS Basic への読み取り専用アクセスを許可」をご参照ください。

しきい値を確認するには、次の手順を実行します。

1. SLB コンソールにログインします。
2. リージョンを選択します。
3. マウスポインターをターゲットインスタンスの横にある DDoS アイコンに合わせます。 リンクをクリックすると、DDoS コンソールに移動し、詳細情報を確認できます。
   - BPS しきい値: インバウンドトラフィックが BPS クリーニングしきい値を超えると、クリーニングが実行されます。
   - PPS しきい値: インバウンドパケットが PPS クリーニングしきい値を超えると、クリーニングが実行されます。
   - ブラックホールしきい値：インバウンドトラフィックがブラックホールしきい値を超えると、ブラックホールがトリガーされます。

Anti-DDoS Basic への読み取り専用アクセスの許可

Anti-DDoS Basic への読み取り専用アクセスを許可するには、次の手順を実行します。

> 注：
> プライマリアカウントで権限付与を行います。

1. プライマリアカウントを使用して、RAM コンソールにログインします。
2. 左側のメニューで、[ユーザー] をクリックし、対象の RAM ユーザーを検索して [管理] をクリックします。
3. [ユーザー権限付与ポリシー] をクリックして、[権限付与ポリシーの編集] をクリックします。
4. 表示されたダイアログボックスで、AliyunYundunDDosReadOnlyAccess を検索して、選択済み権限付与ポリシー名リストに追加します。 [OK] をクリックします。

1.9 リージョン別のピーク帯域幅制限

次の表に示す通り、ロードバランシングエリアは、年間最大帯域幅およびトラフィック課金インスタンスのピーク帯域幅を販売します。

> 注：
> すべてのリージョンにおいて、プライベートネットワークのピーク帯域幅は 5Gbps です。

リージョン	ピーク帯域幅
中国 (青島)	5 Gbps
中国 (杭州)	5 Gbps
中国 (北京)	5 Gbps
中国 (上海)	5 Gbps
中国 (深セン)	5 Gbps
中国 (張家口)	5 Gbps
中国 (フフホト)	5 Gbps
中国 (香港)	2 Gbps
米国 (バージニア)	1 Gbps
米国 (シリコンバレー)	2 Gbps
日本 (東京)	1 Gbps
シンガポール	5 Gbps
オーストラリア (シドニー)	1 Gbps
マレーシア (クアラルンプール)	5 Gbps
UAE (ドバイ)	500 Mbps
ドイツ (フランクフルト)	1 Gbps
インド (ムンバイ)	5 Gbps

1.10 マルチゾーンのデプロイメント

SLB インスタンスを作成する際、複数のゾーンがあるリージョン内で SLB インスタンスを作成して、可用性を向上させることができます。

マルチゾーンとは

クラウドプロダクトのゾーンとは、独立したインフラストラクチャのセットを指します。 異なるゾーンには独立したインフラストラクチャ (ネットワーク、電源、エアコンなど) があり、あるゾーンのインフラストラクチャの障害は他のゾーンに影響しません。

より信頼性の高いサービスを提供するために、SLB はほとんどのリージョンで複数のゾーンをデプロイして、データセンター間のディザスタリカバリを実現しています。 マスターゾーンのデータセンターが障害で利用できなくなった場合、SLB はスレーブゾーンのデータセンターに切り替えて、30 秒以内にサービス機能を復元できます。

SLB のマスターゾーンとスレーブゾーンについては、次の点にご注意ください。

- SLB は、ECS インスタンスと SLB インスタンスが同一リージョンにある限り、異なるゾーンの ECS インスタンスへの接続をサポートします。 SLB は、異なるゾーンの ECS インスタンスへトラフィックを配信できます。
- 通常、スレーブゾーンにある SLB インスタンスはスタンバイ状態です。 SLB インスタンスのアクティブ状態とスタンバイ状態を手動で切り替えることはできません。 SLB は、マスターゾーンのデータセンターが利用不可能な場合にのみ (停電など)、スレーブゾーンに切り替えます。 SLB インスタンスで障害が発生した場合には、スレーブゾーンに切り替わりません。
- SLB と ECS は異なるクラスターにデプロイされています。 SLB インスタンスを利用できない場合でも、ECS インスタンスは引き続き使用可能です。 したがって、SLB がスレーブゾーンに切り替わったとしても、スレーブゾーンの SLB インスタンスは、追加された ECS インスタンスにトラフィックの配信を続行します。 ただし、ゾーン内のすべてのクラスターが使用できない場合、または光ケーブルが壊れている場合、SLB と ECS を含むゾーン内の全サービスは動作できません。

詳細は、「SLB の高可用性」をご参照ください。

マスターゾーンとスレーブゾーンの一覧

次の表は、ゾーン内のマスターゾーンとスレーブゾーンの一覧です。 `DescribeZones` API を呼び出して、リージョン内の使用可能なマスターゾーンとスレーブゾーンを取得できます。

リージョン	ゾーンタイプ	ゾーン	ゾーン
中国 (杭州)	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン B	ゾーン D
		ゾーン D	ゾーン E
		ゾーン E	ゾーン F
		ゾーン F	ゾーン E
中国 (上海)	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン A	ゾーン B
		ゾーン B	ゾーン A またはゾーン D
		ゾーン C	ゾーン B
		ゾーン D	ゾーン B
中国 (深セン)	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン A	ゾーン B

リージョン	ゾーンタイプ	ゾーン	ゾーン
		ゾーン B	ゾーン A
		ゾーン C	ゾーン B
中国 (青島)	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン B	ゾーン C
		ゾーン C	ゾーン B
中国 (北京)	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン A	ゾーン B またはゾーン D
		ゾーン B	ゾーン A またはゾーン C
		ゾーン C	ゾーン B
		ゾーン D	ゾーン A
中国 (張家口)	シングルゾーン	ゾーン A	ゾーン A
中国 (フフホト)	シングルゾーン	ゾーン A	ゾーン A
ドイツ (フランクフルト)	シングルゾーン	ゾーン A	ゾーン A
UAE (ドバイ)	シングルゾーン	ゾーン A	ゾーン A
シンガポール	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン A	ゾーン B
		ゾーン B	ゾーン A
オーストラリア (シドニー)	シングルゾーン	ゾーン A	ゾーン A
マレーシア (クアラルンプール)	シングルゾーン	ゾーン A	ゾーン A
日本 (東京)	シングルゾーン	ゾーン A	ゾーン A
中国 (香港)	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン B	ゾーン C
		ゾーン C	ゾーン B
米国 (バージニア)	シングルゾーン	ゾーン A	ゾーン A
米国 (バージニア)	マルチゾーン	マスターゾーン	スレーブゾーン
		ゾーン A	ゾーン B

リージョン	ゾーンタイプ	ゾーン	ゾーン
		ゾーン B	ゾーン A