# Alibaba Cloud ##**均衡**

設定

**Document Version20191206** 

## 目次

1 リージョン別のピーク帯域幅制限	1
2 API Inspector	2
3マルチゾーンのデプロイメント	9
4 Global Traffic Manager を使用したリージョン間の負荷分散の実	
現現	14
5 Anti-DDoS Basic	21

### 1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によって、購入できる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は異なります。

**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

### 2 API Inspector

API Inspector は実験的な機能です。 API Inspector では、各ステップの背後にある API 呼び 出しをコンソールに表示すること、および異なる言語の API コードを自動生成することができま す。 Cloud Shell または API Explorer からオンラインでデバッグすることができます。

#### 機能

**API Inspector、API Explorer、**および **Cloud Shell** は、**API** を学習しデバッグするための統 合的なソリューションを形成します。 以下の機能が備わっています。

- ・ 自動記録: 関連する API 呼び出しを取得するには、通常どおりコンソールで操作を実行しま す。詳細は、「API 呼び出しの自動記録」をご参照ください。
- ワンクリックでのコード生成:事前に入力されたパラメーターを使用し、さまざまな言語の API コードスクリプトが生成され、これらを直接実行することができます。詳細は、「ワン クリックで API コードを生成する」をご参照ください。
- オンラインデバッグ: API Inspector を API Explorer および Cloud Shell と一緒に使用すると、ワンクリックのオンラインデバッグ環境を実装することができ、開発環境を構築する必要はありません。取得したものがそのまま表示されます。詳細は、「API Explorer によるオンラインデバッグ」および「Cloud Shell によるオンラインデバッグ」をご参照ください。

#### API Inspector の有効化

API Inspector を有効化するには、以下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、[SLB Lab] > [API Inspector] をクリックします。

3. [API Inspector] ページで、API Inspector を有効化します。 API 中断ペンダントがページ

の右側に表示されます。



#### API 呼び出しの自動記録

API Inspector の自動記録機能を説明するため、SLB インスタンスの名前の変更を例として取り上げます。

- 1. [インスタンス] > [Server Load Balancer] をクリックします。
- 2. SLB インスタンスの名前を SLB1 に変更します。
- 3. [OK] をクリックします。

4. ページ右側の API をクリックします。 前の操作に関連した API 呼び出しをすべて見ること

ができます。



5. コア API を表示するには、[クラス OpenAPI Explorer の説明を非表示にする] をクリック

Api Inspecto	r			
SetLoadBala	ncerName			
17:01:39	Status ア	Monitoring	Port/Health	Check/
)	<ul> <li>Active</li> </ul>	a	UDP: 80	• Abn
nh1qc5cm Jygk9bmlj	<ul> <li>Active</li> </ul>	a	TCP: 80	• Abn
) beb2wxl8 }1lahgdcz	<ul> <li>Inactive</li> </ul>	a	Configure	
lic IPv4	• Inactive		TCP: 80 HTTP <b>\$</b> 43	Turcharan
🛛 🗹 Hide Descr	ibe Class		OpenAPI	Explorer

します。 この例でのコア API は SetLoadBalancerName です。

#### ワンクリックで API コードを生成する

API の記録の完了後、 API 名をクリックすると、事前に入力されたパラメーターを使用し、 Python、Java、Go、Node.js、および PHP の API コードスクリプトが生成されます。



SetLoadBalancerName	0 🖾		Api Inspector	Select an item
product:slb action: SetLoadBalancerName Monitoring			SetLoadBalancerName	
params: LoadBalancerld: "lb-bp1bl2mrpsgej3t20om82				
LoadBalancerName: "test-slb2"			normalefault Server Group 2	$\sim$
Python Java Go Node.js PHP		æ		
<pre>#!/usr/bin/env python #coding=utf-8</pre>		Â		
<pre>from aliyunsdkcore.client import AcsClient from aliyunsdkcore.request import</pre>		١d	norm <b>a</b> lefault Server Group 1	~
<pre>client = AcsClient('<accesskeyid>', '</accesskeyid></pre>		L		
<pre>request = CommonRequest() request.set_accept_format('json') request.set_domain('slb.aliyuncs.com')</pre>		U		
<pre>request.set_method('POST') request.set_version('2014-05-15')</pre>			Not Configured	
<pre>2 request.set_action_name     ('SetLoadBalancerName')</pre>			Not Configured	
<pre>request.add_query_param('LoadBalancerId',</pre>		Ц		
<pre>request.add_query_param('LoadBalancerName'    , 'test-slb2')</pre>			Not Configured	-
		Ψ.	Vide Describe Class	OpenAPI Explorer

API Explorer によるオンラインデバッグ

API の記録の完了後、[OpenAPI Explorer] または **w** をクリックして、*OpenAPI Explorer* 

コンソールに移動し、対応する機能をデバッグします。 API のパラメーター値は、コンソールの 操作に従って自動的に生成されます。

SetLoad	Balanc	erName		
Regior	nld		Required Parameter	rs
LoadB	alanceri	Name		
LoadB	alancerl	d		
access	s_key_id	1		
Tags				]
Download	SDK	Documentation	Submit Request	
📋 注:				

② をクリックすると、呼び出された API のパラメーターを詳細に説明するドキュメントが

表示されます。

#### Cloud Shell によるオンラインデバッグ

API の記録の完了後、API 呼び出しの詳細を展開し、 下下 をクリックすることによ

り、Cloud Shell のオンラインワンクリックデバッグを利用することができます。



Cloud Shell のワンクリックデバッグを利用する場合、頻繁に利用するスクリプトとファイル を保存するための OSS バケットを作成し、関連付けることを推奨します。 ただし、少額の OSS 利用コストが発生します。 OSS バケットを作成しなくてもかまいません。

SLB の Cloud Shell デバッグ用クラウドコマンドラインの形式は以下のとおりです。

aliyun slb actionName --parameter1 value1 --paramter2 value2...

この例では、呼び出された SetLoadBalancerName API が、SLB インスタンスの名前を SLB1

に変更しています。同様に次のクラウドコマンドラインを実行します。

aliyun slb SetLoadBalancerName --RegionId cn-hangzhou --LoadBalanc erName SLB1 --LoadBalancerId lb-bp1b6c719dfa08exfuca5

このコマンドを実行した場合の戻り値は以下のようになります。

{"RequestId":"14466282-B00F-49C1-B11E-FB8D3772E3DA"}



### 3マルチゾーンのデプロイメント

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。

#### マルチゾーンのデプロイメントとは

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。 プライマリゾーンの データセンターが障害で利用できなくなった場合、SLB はバックアップ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 のプライマリゾーンとバックアップゾーンについては、次の点に注意してください。

- 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 スヘトラフィックを配信できます。
- ・通常、バックアップゾーンにある SLB インスタンスはスタンバイ状態です。 SLB インスタン スのプライマリ状態とバックアップ状態を手動で切り替えることはできません。 SLB は、プ ライマリ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)、バックアップゾー ンに切り替えます。 プライマリゾーン内の1つのインスタンスで障害が発生しただけでは、 SLB がバックアップゾーンに切り替わることはありません。
- SLB インスタンスと ECS インスタンスは、異なるクラスターにデプロイされています。ゾーン A の SLB インスタンスが利用できない場合、ゾーン A の ECS インスタンスは必ずしも利用できないわけではありません。したがって、SLB がバックアップゾーンに切り替わったとしても、バックアップゾーンの SLB インスタンスは依然として、追加された ECS インスタンスにトラフィックを配信することができます。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、または光ケーブルに障害が発生した場合は、ゾーン内のすべてのサービス(SLB インスタンスおよび ECS インスタンス以外のサービスも含む)は機能しなくなります。

詳細は、「SLB の高可用性」をご参照ください。



#### プライマリゾーンとバックアップゾーンの一覧

以下の表は、各リージョンのプライマリゾーンとバックアップゾーンの一覧です。 DescribeZones APIを呼び出して、リージョン内の使用可能なプライマリゾーンとバックアッ プゾーンを取得できます。

リージョ	ゾーンタ	ゾーン	
ン	イプ		
中国 (杭	マルチ	プライマリゾーン	利用可能なバックアップゾーン
州)	ゾーン	ゾーン B	ゾーン D
			ゾーン G
		ゾーン D	ゾーン E
		ゾーン E	ゾーン D
			ゾーン F
		ゾーン F	ゾーン E

リージョ ン	ゾーンタ イプ	ゾーン	
		ゾーン G	ゾーン B
			ゾーン H
		ゾーン H	ゾーン G
中国 (上	マルチ	プライマリゾーン	利用可能なバックアップゾーン
海)	ゾーン	ゾーン A	ゾーン B
		ゾーン B	ゾーン A
			ゾーンC
			ゾーン D
		ゾーン C	ゾーン B
		ゾーン D	ゾーン B
			ゾーン E
		ゾーン E	ゾーン D
			ゾーン F
		ゾーン F	ゾーン E
中国 (深セ	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ン)	ゾーン	ゾーン A	ゾーン <b>B</b>
		ゾーン B	ゾーン A
			ゾーンC
		ゾーン C	ゾーン B
			ゾーン D
		ゾーン D	ゾーン C
			ゾーン E
		ゾーン E	ゾーン D
中国 (青	マルチ	プライマリゾーン	利用可能なバックアップゾーン
島) 	ゾーン	ゾーン B	ゾーンC
		ゾーンC	ゾーン B

リージョ ン	ゾーンタ イプ	ゾーン	
中国 (北	マルチ	プライマリゾーン	利用可能なバックアップゾーン
京)	ゾーン	ゾーン A	ゾーン B
			ゾーン D
			ゾーン E
		ゾーン B	ゾーンC
		ゾーンC	ゾーン E
		ゾーン D	ゾーン A
		ゾーン E	ゾーン C
			ゾーン F
		ゾーン F	ゾーン E
			ゾーンG
		ゾーンG	ゾーン F
中国 (張家	マルチ ゾーン	プライマリゾーン	利用可能なバックアップゾーン
口)		ゾーン A	ゾーン B
		ゾーン B	ゾーン A
中国 (フフ	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ホト) 	ゾーン	ゾーン A	ゾーン B
		ゾーン B	ゾーン A
ドイツ (フ	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ランクフ ルト)	ゾーン	ゾーン A	ゾーン B
		ゾーン B	ゾーン A
イギリス	マルチ	プライマリゾーン	利用可能なバックアップゾーン
(ロンド	ゾーン	ゾーン A	ゾーン A
• )		ゾーン B	ゾーン B
UAE(ド バイ)	シングル ゾーン	ゾーン A	
シンガ	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ポール	ゾーン	ゾーン A	ゾーン B

リージョ	ゾーンタ	ゾーン	
ン	イプ		
		ゾーン B	ゾーン A
		ゾーンC	ゾーン B
オースト	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ラリア (シ	ゾーン	ゾーン A	ゾーン B
, _ ,		ゾーン B	ゾーン A
マレーシ	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ア (クアラ	ゾーン	ゾーン A	ゾーン B
ル)		ゾーン B	ゾーン A
インドネ シア (ジャ カルタ)	シングル ゾーン	ゾーン A	
インド (ム	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ンバイ)	ゾーン	ゾーン A	ゾーン B
		ゾーン B	ゾーン A
日本 (東 京)	シングル ゾーン	ゾーン A	
中国 (香	マルチ	プライマリゾーン	利用可能なバックアップゾーン
港)	ゾーン	ゾーン B	ゾーン C
		ゾーン C	ゾーン B
米国 (バー	マルチ	プライマリゾーン	利用可能なバックアップゾーン
ジニア) 	ゾーン	ゾーン A	ゾーン B
		ゾーン B	ゾーン A
米国 (シ	マルチ	プライマリゾーン	利用可能なバックアップゾーン
リコンバ	ゾーン	ゾーン A	$\overline{\gamma} - \gamma B$
		ゾーン B	ゾーン A

## 4 Global Traffic Manager を使用したリージョン間の 負荷分散の実現

#### グローバルトラフィックの管理

負荷分散は、アプリケーションの地理的な構造によって、ローカル負荷分散とグローバル負荷分 散に分けられます。 ローカル負荷分散は、同じリージョン内のサーバーグループの負荷を分散 します。 グローバル負荷分散は、異なるリージョンにあり、異なるネットワーク構造を持つサー バーグループのバランスを制御します。

Global Traffic Manager を使用することにより、グローバルトラフィック管理をローカル負荷 分散よりも高度に進化させ、リージョンを超えた耐障害性、異なるリージョンからのアクセスの 高速化の問題をインテリジェントに解決することができます。

・ マルチラインインテリジェント解決サービス

グローバルトラフィック管理は、DNS インテリジェント解決とアプリケーションの実行ス テータスに対するヘルスチェックを使用して、ユーザーが最も適切な IP アドレスにアクセス するように指示します。

リージョン間の耐障害性

グローバルトラフィック管理は、異なるアドレスプールへの異なるリージョンの IP アドレス の追加とヘルスチェックの設定をサポートします。 アクセスポリシー設定で、"アドレスプー ル A" をデフォルトの IP アドレスプールとして設定し、"アドレスプール B" をフェールオー バー IP アドレスプールとして設定します。 これにより、アプリケーションサービスのアク ティブ - スタンバイ IP 耐障害性を達成することができます。

・ 異なるリージョンからのアクセスを高速化

Global Traffic Manager を使用することにより、ユーザーのアクセスを異なるリージョン から異なる IP アドレスプールへ振り分けることができます。これにより、グループ化された ユーザー管理とグループ化されたアクセスを実現し、アプリケーションによるユーザーエクス ペリエンスの向上を支援します。

#### Global Traffic Manager の展開

このチュートリアルでは、例として "aliyuntest.club" を取り上げます (この Web サイトの主 なユーザーはシンガポールと中国にいます)。グローバルトラフィック管理と負荷分散を通じてグ ローバルな負荷分散を達成する方法を示します。

#### ステップ1: ECS インスタンスの購入と設定

アプリケーションサービスのユーザーが存在するリージョンで、それぞれ ECS インスタンスを 2 つ以上購入し、設定します。

このチュートリアルでは、北京、深セン、シンガポールでそれぞれ 2 つの ECS インスタンスを購入し、単純な静的 Web ページをそれぞれの ECS インスタンスで作成します。

#### ステップ2:SLB インスタンスの購入と設定

- 中国 (北京)、中国 (深セン)、シンガポールに、それぞれ SLB を作成します。詳しくは、 「#unique\_6」をご参照ください。
- **2.** リスナーを追加し、設定された ECS インスタンスをバックエンドサーバープールに追加しま す。詳しくは、「#unique\_7」をご参照ください。
- ・ 中国 (北京) リージョンの SLB インスタンスの例
- ・中国 (深セン) リージョンの SLB インスタンスの例
- ・ シンガポールリージョンの SLB インスタンスの例

#### ステップ3: Global Traffic Manager の設定

- 1. Global Traffic Manager インスタンスを購入します。
  - a. Alibaba Cloud DNS 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、 [Global Traffic Manager] をクリックします。
  - c. [Global Traffic Manager] ページで、[インスタンスの作成] をクリックします。
  - **d.** バージョン、数量、およびサービス期間を選択してください。
  - e. [今すぐ購入] をクリックします。

インスタンスが正常に購入されると、システムは自動的に CNAME アクセスドメイン名を 割り当てます。

Global Traffic Manager				
Search by keywords	Search Starter Guide			Create Instance
ID/Name	CNAME	Health Check Status	Request Status	Actions
gtm-cn-o400rchv50a	gtm-cn-	• Available	Available	Configure
gtm-cn-o400rchv509	gtm-cn-	• Available	Available	Configure Renew

- 2. Global Traffic Manager インスタンスを設定します。
  - a. [Global Traffic Manager] ページで、Global Traffic Manager インスタンスの ID をク リックするか、 [操作] の [設定] をクリックします。
  - **b.** 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。
  - **c.** [グローバル設定] タブで、[編集] をクリックし、 **Global Traffic Manager** インスタンス のパラメーターを設定します。

以下のパラメーターを設定し、残りのオプションにはデフォルト値を使用します。

- インスタンス名:アプリケーションに使用されるインスタンスを識別するために使用され、カスタマイズ可能です。
- ・ プライマリドメイン:プライマリドメイン名は、ユーザーがアプリケーションにアクセスするために使用します。このチュートリアルでは、"aliyuntest.club"と入力します。
- アラートグループ: CloudMonitor で設定した連絡先グループを選択します。エラー が発生すると、連絡先グループに通知されます。
- **d.** [確認] をクリックします。

3. IP アドレスプールを設定します。

- a. [アドレスプールの設定] で [アドレスプールの作成] をクリックします。
- **b.** [アドレスプールの作成] ページで、IP アドレスプールを設定します。

このチュートリアルでは、3 つの IP アドレスプールを追加し、各 IP アドレスプールは異なるリージョンにある 3 つの SLB アドレスのうちの 1 つに対応します。

- アドレスプール名:カスタム。例: China North\_Beijing、China East\_Hangzhou、Singapore など。
- ・アドレス:このリージョンに追加される、SLB パブリック IP アドレスです。

Create Address Pool		×
* Address Pool Name :		
You must enter an address pool name.		
* Address Pool Type 🕐		
IP	~	]
1		
Address	Mode	
	Smart Return 🗸	
+ New Row		

**c.** [確認] をクリックします。

4. ヘルスチェックを設定します。

この例では、3つのアドレスプールのヘルスチェックを別々に設定する必要があります。

- a. [アドレスプール] タブで [追加] をクリックします。このボタンはヘルスチェックの横にあ ります。
- **b.** ヘルスチェックのパラメーターを設定します。

[モニタリングノード] は、モニタリングノードの位置が表示されます。 アドレスプールの リージョンに応じて、モニタリングノードを選択します。

5. アクセスポリシーを設定します。

このチュートリアルでは、3つのリージョンにそれぞれに異なるアクセスポリシーを追加しま す。

- a. [アクセスポリシー] タブにある [アクセスポリシーの追加] をクリックします。
- **b.** [アクセスポリシーの追加] ページで、アクセスポリシーを設定します。
  - ・異なるアクセスリージョンに対応するデフォルトアドレスプールを設定し、別のリージョンのアドレスプールをフェールオーバーアドレスプールとして設定します。
  - アクセスリージョンを選択します。このリージョンのユーザーがアプリケーションにア クセスすると、アクセスポリシーで設定されているアドレスプールが照合されます。
     [グローバル]を選択したアクセスポリシーが必ず必要です。これを設定しなかった場 合、一部のエリアからアプリケーションにアクセスすることができません。

#### 6. CNAME アクセスを設定します。

- a. Alibaba Cloud DNS コンソールにログインします。
- **b.** 設定するドメイン名、 **"aliyuntest.club"** を見つけ、[操作] 列の [設定]をクリックしま す。
- c. [DNS 設定] ページで、[レコードの追加] をクリックします。
- d. [レコードの追加] ページで、エンドユーザーがアクセスするドメイン名

"aliyuntest.club" を CNAME 形式で Global Traffic Manager インスタンスのエイリア スレコードに設定します。

Add Record		×
Type:	A- IPV4 address $\lor$	
Host:	Enteraliyuntest.club (?)	
ISP Line :	Default - Return to the default value when the query is not $\vee$ ?	
* Value:	Enter	
* TTL:	10 minute(s) $\lor$	
	Synchronize the Default Line	
	Cancel	ОК

e. [確認] をクリックします。

#### ステップ4:テスト

SLB サービスが利用できないように、中国 (北京) リージョンの SLB インスタンスの ECS インス タンスを削除します。

Web サイトにアクセスし、正常にアクセスできるかを確認します。



IP がダウンしたことを Global Traffic Manager で検出してから判断するまでに1、2 分かか ります。 モニタリングの頻度を1 分に設定した場合、例外によるリンク切り替えが有効になる までに2、3 分がかかります。

### 5 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 5 Gbps の Anti-DDoS Basic を SLB に対して提供します。 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 攻撃を防 御し、SYN フラッド、UDP フラッド、ACK フラッド、ICMP フラッド、DNS 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、スクラブしきい値 とブラックホールしきい値を設定します。 受信トラフィックがしきい値に達すると、スクラブま たはブラックホールがトリガーされます。

- スクラブ: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は、Alibaba Cloud Security は攻撃トラ フィックのスクラブを開始します。スクラブには、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、ブラックホールが発生し、すべての受信トラフィックがドロップされます。

しきい値は、次の原則に基づいて計算されます。

- ・しきい値は、SLB インスタンスの帯域幅、つまり SLB インスタンスの送信帯域幅によって決まります。しきい値は、インスタンスの帯域幅が高い場合は大きくなり、逆の場合は小さくなります。
- ブラックホールしきい値は、ユーザーのセキュリティクレジットスコアによって決定されます。



セキュリティクレジットスコアは、ブラックホールしきい値にのみ影響し、スクラブしきい 値には影響しません。

次の手順に従って、しきい値を計算します。

**1. SLB Backstage** は、購入した帯域幅に応じてインスタンスが正常に動作できる推奨しきい値 を提供します。

**注**:

従量課金インスタンスの送信帯域幅は、そのリージョンのピーク帯域幅です。 現時点では、 中国本土のピーク帯域幅の上限は 5G です。 詳細については、「リージョンごとのピーク帯 域幅」をご参照ください。

- ・ SLB 帯域幅とトラフィックスクラブしきい値 (ビット/秒)の関係
  - SLB 帯域幅が 100 Mbps 以下の場合、デフォルトトラフィックスクラブしきい値 (ビット/秒) は 120 Mbps となります。
  - SLB 帯域幅が 100 Mbps 以上の場合、デフォルトトラフィックスクラブしきい値 (ビット/秒) = 帯域幅 \* 1.2 となります。
- ・ SLB帯域幅とトラフィックスクラブしきい値 (パケット/秒)の関係

トラフィックスクラブしきい値 (パケット/秒) = (SLB 帯域幅/500) \* 150000

帯域幅の単位は Mbps です。

- ・ SLB 帯域幅とブラックホールしきい値 (ビット/秒)の関係
  - SLB 帯域幅が 1Gbps 以下の場合、デフォルトのブラックホールしきい値 (ビット/秒) は 2Gbps となります。
  - SLB 帯域幅が 1Gbps 以上の場合、デフォルトのブラックホールしきい値 (ビット/秒)
     は SLB 帯域幅 \* 1.5、または 2Gbps となります。

- 2. Alibaba Cloud Security は、推奨値、セキュリティクレジットスコア、および異なるリー ジョンのリソース条件に従ってしきい値を計算します。
  - ・トラフィックスクラブしきい値 (ビット/秒) およびトラフィックスクラブしきい値 (パケット/秒) を決めるルール

最小トラフィックスクラブしきい値 (ビット/秒) は 1,000 Mで、最小トラフィックスクラ ブしきい値 (パケット/秒) は 300,000 です。

- SLB の推奨しきい値が最小クリーニングしきい値より小さい場合、最小しきい値が使用 されます。
- SLB の推奨しきい値が最小クリーニングしきい値より大きい場合、推奨しきい値が使用 されます。
- Alibaba Cloud Security は、ユーザーのセキュリティクレジットスコアに基づいてブ ラックホールしきい値を決めます。

しきい値の確認

SLB コンソールのインスタンスのしきい値は、RAM ユーザーとして確認できます。 確認できな い場合は、RAM アカウントに権限を付与する必要があります。 詳細は、「*Anti-DDoS Basic*への 読み取り専用アクセスの許可」をご参照ください。

- しきい値を確認するには、以下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.** 目的のインスタンスの横にある、DDoS アイコンにマウスポインタを合わせると、以下のしき い値が表示されます。 このリンクをクリックすると、DDoS コンソールにアクセスして詳細
  - トラフィックスクラブしきい値 (ビット/秒):受信トラフィックがこの値を超えた場合、ス クラブが実行されます。
  - トラフィックスクラブしきい値 (パケット/秒):受信トラフィックがこの値を超えた場合、
     スクラブが実行されます。
  - ブラックホールしきい値:受信トラフィックがこの値を超えた場合、ブラックホールが実行 されます。

Server	Server Load Balancer Back to Old Version>>											
Creat	e SLB Instance C ≔ ⊥	۲				Select a tag ∨	Zones: All $\smallsetminus$	Select an item $\vee$	Enter a	a value		
	Instance Name/ID	ID Address V	Otatua V7	Monitoring	Port/Hea	Health Check/Backend Server 🗠				Actions		
	The tag is not set.	Banowidth: 5120 M0ps Traffic Scrubbing Threshold (bits/s): 5 Traffic Scrubbing Threshold (packets/ Blackholing Threshold: Mbps Improve Anti-DDoS Threshold Ecomore information on to the Anti-L	500 Mbps s/s): 150000 DDoS Service • Active	Ð	Configure					Configure Listener Add Backend Servers More ~		
	auto samed alth II adrahj78u The tag is not set.	console.			HTTP\$43	Normal De	fault Server Grou	p 2 🗸		Configure Listener Add Backend Servers More >>		

Anti-DDoS Basic への読み取り専用アクセスの許可

情報を確認できます。

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

# 注:プライマリアカウントで権限を付与します。

- 1. プライマリアカウントで RAM コンソールヘログインします。
- 2. 左側のナビゲーションメニューで、 [ユーザー管理] をクリックし、対象 RAM ユーザーを検索して [管理] をクリックします。

User Management		Create User CRefre
Line Name T Courth hullon Name		
Search by User Marine Search by User Marine		
User Name/Display Name Description	Created At	Acti
acs_ram_account	2017-12-28 14:54:35	Manage   Authorize   Dele Join Gro
	User Namagement User Name   Search by User Name  Search User Name/Display Name Description  acs_ram_account	User Name  Search by User Name User Name/Display Name Description Created At acs_ram_account acs_ram_account

3. [ユーザー権限付与ポリシー]をクリックして、[権限付与ポリシーを編集] をクリックします。

#### 表示されるダイアログボックスで、"AliyunYundunDDosReadOnlyAccess" を検索して、 選択された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。

dit User-Level Authorization Members added to this group h	ave all the	permissions	of this group. A member cannot	> be
Available Authorization Policy N	ames	•		
	TypeQ			
aliyunyundunDDoS				
AliyunYundunDDosFullAccess Provides full acce	System	>		
			Selected Authorization Policy Name	
				Туре
			AliyunYundunDDosReadOnlyAd	tess
			Provides read-only	System
			OK	Close

#### セキュリティクレジットスコアの表示

セキュリティクレジットスコアは、攻撃を受けた履歴、購入履歴、アカウントアクティビティ、 セキュリティレベル、期待値などに基づき、 Alibaba Cloud によって提供されます。 セキュリ ティクレジットスコアが高いほど、無料のブラックホールしきい値が大きくなり、ブラックホー ルの期間 (ブラックホールの状態が続く期間)を短くすることができます。

以下の手順に従ってセキュリティクレジットスコアを表示します。

- 1. Anti-DDoS Basic コンソールヘログインします。
- 2. [Anti-DDoS Basic] > [インスタンス]を選択します。

3. セキュリティ信用性 の URLをクリックしてアカウントのセキュリティクレジットスコアを確認できます。

