Alibaba Cloud
##均衡

アクセス制御

Document Version20200203

目次

1 アクセス制御の設定.....1
2 アクセス制御リスト.....3
2.1 アクセス制御リストの作成.....3
2.2 IP エントリの追加.....3
2.3 IP エントリの削除.....5
3 アクセス制御の有効化.....7
4 アクセス制御の無効化.....9
5 新しいアクセス制御リストへの移行.....10

1 アクセス制御の設定

Server Load Balancer では、リスナーのアクセス制御を設定できます。 リスナーごとに異なるホワイトリストまたはブラックリストを設定できます。

リスナーの作成時にアクセス制御を設定できます。また、リスナー作成後にアクセス制御の設定を変更することもできます。

ここでは、リスナー作成後にアクセス制御を設定する方法について説明します。

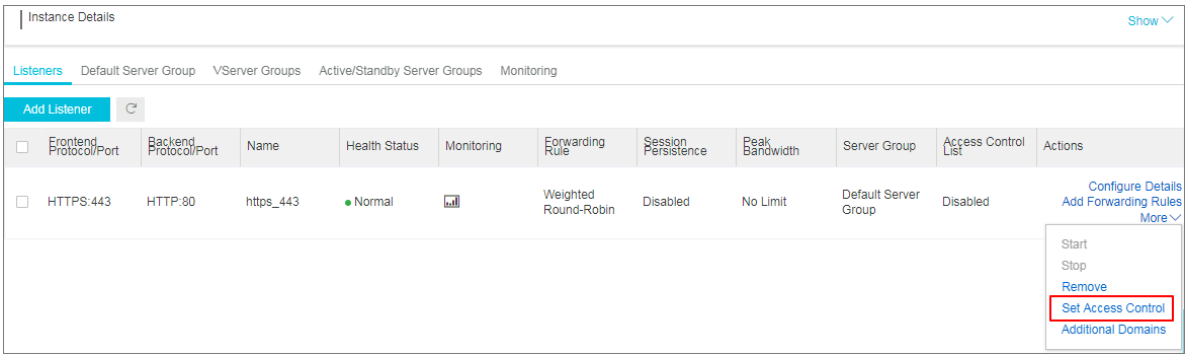
アクセス制御の有効化

アクセス制御を有効化する前に、以下の点を確認してください。

- アクセス制御リストを作成済みであること。 詳細については、「アクセス制御リストの作成」をご参照ください。
- リスナーを作成済みであること。

アクセス制御を有効化するには、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. リージョンを選択します。
3. 対象 SLB インスタンスの ID をクリックします。
4. [インスタンスの詳細] ページで、 [リスナー] タブをクリックします。
5. 対象リスナーを見つけ、**[詳細] > [アクセス制御の設定]** をクリックします。



6. [アクセス制御の設定] ページで、アクセス制御を有効にし、アクセス制御方式とアクセス制御リストを選択して、[**OK**] をクリックします。

   - [ホワイトリスト]: 選択したアクセス制御リストに記載されている IP アドレスや CIDR ブロックからのリクエストのみが転送されます。 特定の IP アドレスからのアクセスのみをアプリケーションで許容するシナリオに利用します。

     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 アドレスのみがリスナーにアクセスできます。 対応する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化すると、すべてのリクエストが転送されます。
   - [ブラックリスト]: 選択したアクセス制御リストに記載されている IP アドレスや CIDR ブロックからのリクエストは転送されません。 特定の IP アドレスからのアクセスのみをアプリケーションで拒否するシナリオに利用します。

     対応するアクセス制御リストに IP エントリを 1 つも追加せずにブラックリストを有効化すると、すべてのリクエストが転送されます。

アクセス制御の無効化

アクセス制御を無効化するには、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. リージョンを選択します。
3. 対象 SLB インスタンスの ID をクリックします。
4. [インスタンスの詳細] ページで、 [リスナー] タブをクリックします。
5. 対象リスナーを見つけ、**[詳細] > [アクセス制御の設定]**をクリックします。
6. [アクセス制御の設定] ページで、アクセス制御を無効にし、 [**OK**] をクリックします。

2 アクセス制御リスト

2.1 アクセス制御リストの作成

リスナーのアクセス制御機能を設定する前に、まずアクセス制御リストを設定する必要があります。

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ペインで、**[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、アクセス制御リスト名を入力し、IP バージョンを選択して、リソースグループを選択します。
5. **[OK]** をクリックします。

関連情報
#unique_4

2.2 IP エントリの追加

ここでは、1 つ以上の IP エントリをアクセス制御リストに追加する方法について説明します。 1 つの IP エントリは、IP アドレスまたは CIDR ブロックのいずれかを 1 つ持ちます。

アクセス制御リストに追加された IP エントリには、次のいずれかのルールを適用できます。

- ホワイトリスト：選択されたアクセス制御リストに属する IP アドレスまたは CIDR ブロックからのリクエストのみが転送されます。 ホワイトリストは、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。
- ブラックリスト：選択されたアクセス制御リストに属する IP アドレスまたは CIDR ブロックからのリクエストは転送されません。 ブラックリストは、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拒否するシナリオに適用されます。

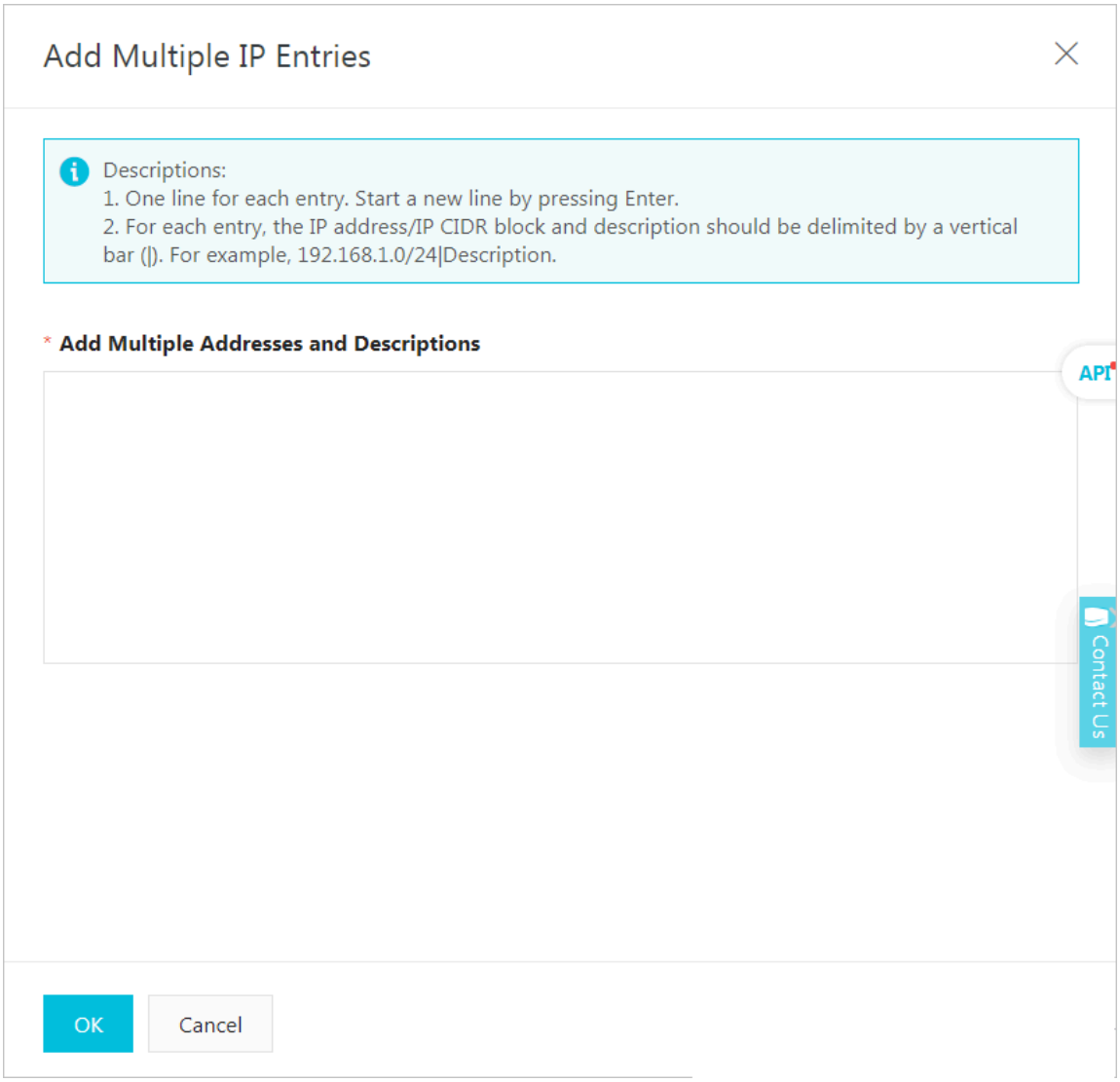
1. SLB コンソールにログインします。
2. 対象となるリージョンを選択します。
3. 左側のナビゲーションペインで、**[アクセス制御]** をクリックします。
4. 対象となるアクセス制御リストを見つけ、その行の **[操作]** 列にある **[管理]**をクリックします。

5. IP エントリを追加します。

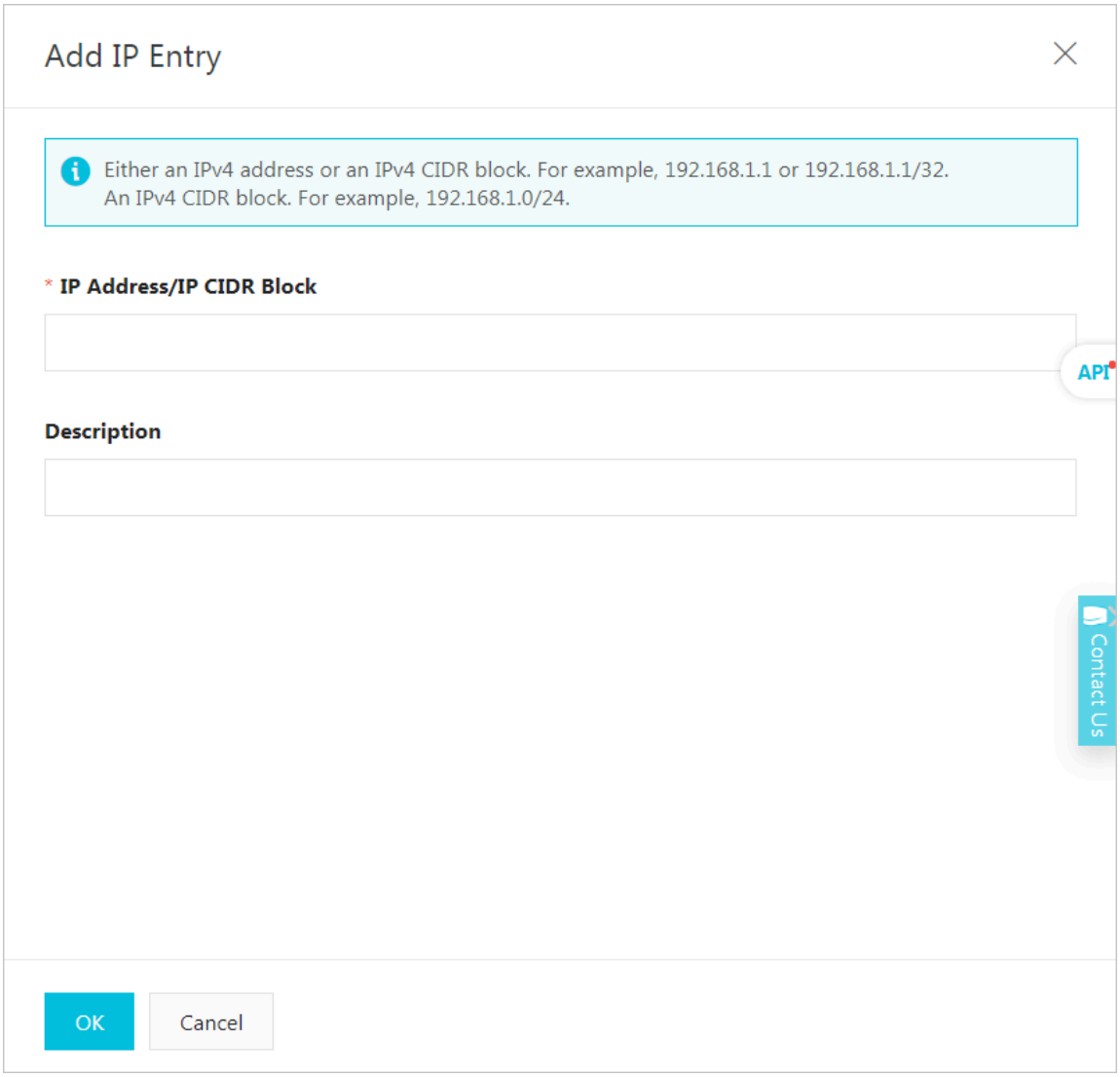
- **[複数のエントリの追加]** をクリックします。 表示されるダイアログボックスで、複数の IP アドレスまたは CIDR ブロックを追加し、**[追加]** をクリックします。

  IP エントリを追加する際には、次の点に注意してください。

  - IP エントリは 1 行に 1 つだけです。 Enter キーを使用して改行します。
  - 縦棒 (|) を使用して IP エントリとコメントを区切ります。例：**10.10.10.1 | 171.16.10.1** 。



- **[エントリの追加]** をクリックします。 表示されるダイアログボックスで、IP アドレスまたは CIDR ブロックとコメントを追加し、**[追加]** をクリックします。



関連情報
#unique_6

2.3 IP エントリの削除

アクセス制御リストから IP エントリを削除できます。

1. SLB コンソールにログインします。
2. 対象となるリージョンを選択します。
3. 左側のナビゲーションペインで、**[アクセス制御]** をクリックします。
4. 対象となるアクセス制御リストを見つけ、その行の **[操作]** 列にある **[管理]** をクリックします。
5. 対象となる IP エントリを見つけ、**[操作]** 列にある、**[削除]** をクリックします。または、複数の IP エントリを選択して、リストの下部にある **[削除]** をクリックします。
6. 表示されるダイアログボックスで **[OK]** をクリックします。

関連情報
#unique_8

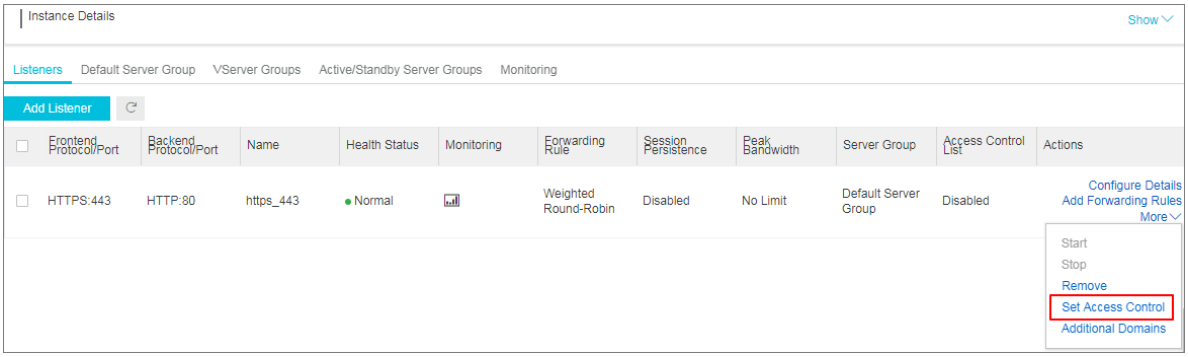
3 アクセス制御の有効化

Server Load Balancer (SLB) は、リスナーにアクセス制御機能を提供します。 リスナーごとに違うホワイトリストまたはブラックリストを設定できます。

アクセス制御を有効化する前に、次の点を確認してください。

- アクセス制御リストが作成されていること。 詳細については、アクセス制御の設定をご覧ください。
- リスナーが作成されていること。

1. SLB コンソールにログインします。
2. 対象となる SLB インスタンスのリージョンを選択します。
3. 対象となる SLB インスタンスを見つけ、インスタンス ID をクリックします。
4. **[**インスタンス詳細**]** ページで、**[**リスナー**]** タブをクリックします。
5. 対象となるリスナーを探し、**[**オプション**] > [**アクセス制御の設定**]** を選択します。



6. **[**アクセス制御設定**]** ページで、アクセス制御を有効にし、アクセス制御方法とアクセス制御リストを選択し、 **[OK]** をクリックします。

   - ホワイトリスト：選択されたアクセス制御リストに属する IP アドレスまたは CIDR ブロックからのリクエストのみが転送されます。 これは、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。

     ホワイトリストを有効化することによって、サービスにいくつかのリスクが生じます。 ホワイトリストが設定されると、リストに属する IP アドレスのみがリスナーにアクセスでき

ます。 選択されたアクセス制御リストに全く IP アドレスを追加せずにホワイトリストを有効化すると、すべてのリクエストが転送されます。

- ブラックリスト：選択したアクセス制御リストに属する IP アドレスまたは CIDR ブロックからのリクエストは転送されません。 これは、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拒否するシナリオに適用されます。

  選択されたアクセス制御リストに全く IP アドレスを追加せずにブラックリストを有効化すると、すべてのリクエストが転送されます。

 注：

アクセス制御機能は新しい接続リクエストに対してのみ機能し、既存の接続には影響しません。

4 アクセス制御の無効化

アクセス制限を設定する必要がない場合は、アクセス制御機能を無効にできます。

1. SLB コンソールにログインします。
2. 対象となる Server Load Balancer (SLB) インスタンスのリージョンを選択します。
3. 対象となる SLB インスタンスを見つけ、ID をクリックします。
4. **[**インスタンス詳細**]** ページで、**[**リスナー**]** をクリックします。
5. 対象となるリスナーを見つけ、**[**オプション**] > [**アクセス制御の設定**]** を選択します。
6. **[**アクセス制御設定**]** ページで、アクセス制御を無効化して **[OK]** をクリックします。

5 新しいアクセス制御リストへの移行

既にリスナーのホワイトリストが構成されている場合、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

以前に構成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、対象 SLB インスタンスの ID をクリックします。
3. リスナータブをクリックします。
4. 対象リスナーを検索し、オプション > 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メニューで、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。