目次

1. はじめに

日本から海外のWebサイトにアクセスすると、インターネット回線を通ってアクセスすることになり、パフォーマンスが落ちる場合があります。Alibabaクラウドでは専用線サービス(ExpressConnect)を用意していますが、相手国までの通信経路を変更する必要がでてきた場合(特定の経路を経由して通信する)、Proxyの機能を使って簡単に通信経路を変更することができます。本ナレッジでは、apache proxy機能を使って目的のWebサイトまでの経路を変更する方法をご紹介します。

また、日本／海外で同じWebサービスを展開している場合に、片側のリージョンにWebサーバーを設置して、両方のリージョンからアクセスさせる際にも応用ができます。

※シングル構成については、こちら。

2. リバースプロキシとは

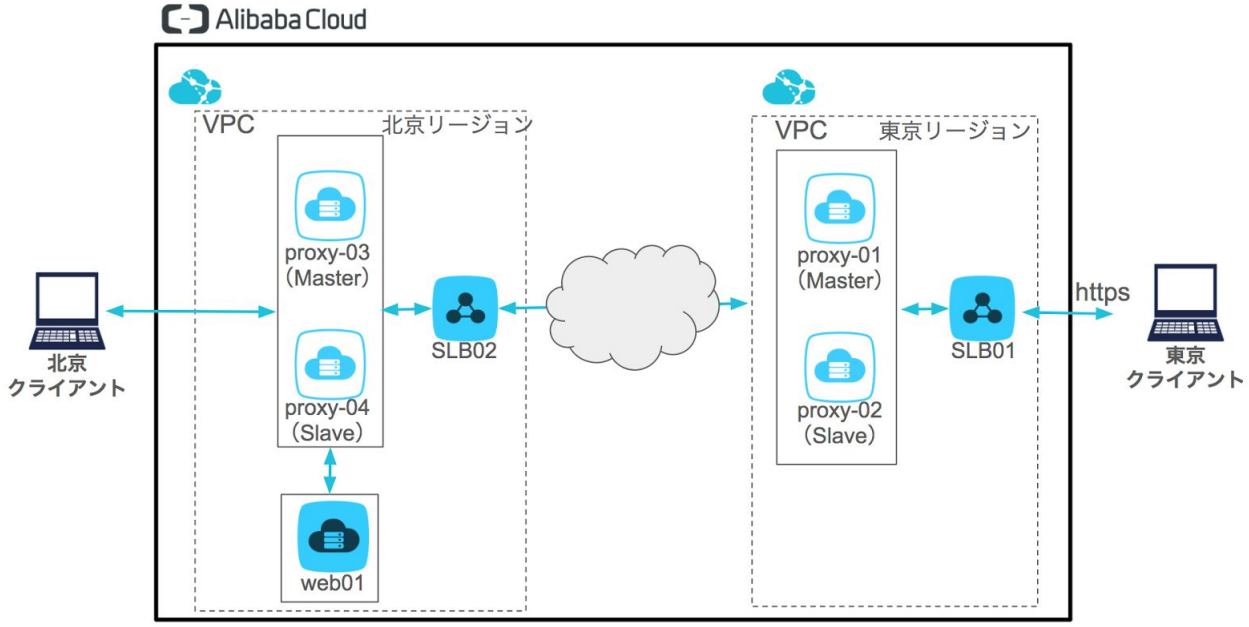
アクセス先のサーバ側に設置して、バックエンドの宛の特定サーバ宛のリクエストを中継します。クライアントからのアクセス先窓口は、リバースプロキシ宛になりますので、実際にコンテンツを返すサーバにはクライアントからは直接アクセスしません。

このため、セキュリティ性やバックエンドサーバの負荷軽減等のためによく利用されています。

3.SLB（サーバーロードバランサー）とは

Alibaba Cloud Server Load Balancerは、複数のバックエンドサーバーに転送ルールとスケジューリングアルゴリズムに基づいてトラフィックを配信するトラフィック分散制御サービスです。本ナレッジではマスタースレーブ機能を使って、冗長化します。

4. イメージ図



本ドキュメントではリバースプロキシは転送機能のみを利用します。また、SLB（サーバー・ロード・バランサー）のマスター・スレーブ機能を使い、冗長構成をとります。通常はマスター機を通して通信をし、マスター機に障害があった場合はスレーブ機に自動的に切り替わります。

＜通信フロー＞

1) SLB01：東京にあるクライアントからリクエストを受け、proxy-01へ送信する
2) proxy-01:クライアントからのリクエストを受け、SLB02に送信する
3) SLB02：proxy−01から受けたリクエストをproxy-03へ送信する
4) proxy-03：proxy−01から受けたリクエストをweb-01へ送信する
5) web-01：レスポンスをproxy-03へ送信する
6) proxy-03：web-01から受けたレスポンスをSLB02に送信する
7) SLB02：proxy-03から受けたレスポンスをSLB01に送信する
8) SLB01：SLB02から受けたレスポンスをproxy-01に送信する
9) proxy-01：SLB01から受けたレスポンスをクライアントへ送信する

5.導入手順

5-1. ECS購入

本ドキュメントでは、下記のスペックでECSサーバを購入しています。ECSサーバの購入方法の詳細についてはこちらをご参照ください。SLBの購入についてはこちらをご参照ください。

＜東京サーバー＞

リージョン: 東京（日本）
CPU： 2-core
メモリ：4GB
OS: CentOS 7.3 64bit
システムディスク: 40GB Ultra クラウドディスク
インスタンス名: proxy-01（Master）
インスタンス名: proxy-02（Slave）

＜東京サーバーロードバランサー（SLB01）＞

ゾーンタイプ: シングルゾーン
プライマリ: 日本ゾーン A
リージョン: 東京（日本）
インスタンス: インターネット
課金サイクル: 1時間
Anti-DDos: 有効

＜北京サーバー＞

リージョン: 中国北部 2
CPU： 2-core
メモリ：4GB
OS: CentOS 7.3 64bit
システムディスク: 40GB Ultra クラウドディスク
インスタンス名: proxy-03（Master）
インスタンス名: proxy-04（Slave）
インスタンス名: web-01

＜北京サーバーロードバランサー（SLB02）＞

ゾーンタイプ: マルチゾーン
スペック: パフォーマンス共有型
リージョン: 北京（中国北部）
インスタンス: インターネット
課金サイクル: 1時間
Anti-DDos: 有効

5-2. OS設定（作業対象：proxy-01、proxy-02、proxy-03、proxy-04、web-01）

5-1-1. ミドルウェア（Apache）をインストールします。

```
# yum -y install httpd
```

※　インストールされた Apache httpd の主なファイルは以下に配置されます。
　　起動スクリプト : /etc/init.d/httpd
　　設定ファイル : /etc/httpd/conf/httpd.conf
　　ドキュメントルート : /var/www/html

5-1-2. 起動時に自動実行されるように設定します。

```
# systemctl enable httpd
```

5-1-3. 正常にインストールされたかバージョン確認をします。

```
# httpd -v
```

5-2. ミドルウェア設定（作業対象：proxy-01、proxy-02）

5-2-1. https通信用にSSLモジュールをインストールします。

```
#  yum -y install mod_ssl
```

5-2-2. ssl.confの編集をします。

```
vi /etc/httpd/conf.d/ssl.conf
```

5-2-3. 「<VirtualHost _default_:443>」をコメントアウトし、次行に追記します。

```
#<VirtualHost _default_:443> ←コメントアウトしておく
<VirtualHost *:443>
```

5-2-4.「SSLEngine on」の後に追記します。転送先、返答元アドレスを指定しています。

```
SSLProxyEngine on
ProxyPass / https://SLB01のIPアドレス/
ProxyPassReverse / https://SLB01のIPアドレス/
```

5-2-5. 最終行に追記します。今回はIPアドレスで証明書を作成するので、CommonName、サブジェクトの別名をチェックしないようにします。

```
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
```

5-2-6. サービスを再起動します

```
# systemctl restart httpd
```

5-3. ミドルウェア設定（作業対象：proxy-03、proxy-04）

5-3-1. https通信用にSSLモジュールをインストールします。

```
#  yum -y install mod_ssl
```

5-3-2. ssl.confを編集します。

```
# vi /etc/httpd/conf.d/ssl.conf
```

5-3-3. 「<VirtualHost _default_:443> 」をコメントアウトし、次行に追記します。

```
#<VirtualHost _default_:443> ←コメントアウトしておく
<VirtualHost *:443>
```

5-3-4. 「SSLEngine on」の後に追記します。転送先、返答元アドレスを指定しています。

```
SSLProxyEngine on
ProxyPass / https://web-01のIPアドレス/
ProxyPassReverse / https://web-01のIPアドレス/
```

5-3-5. 最終行に追記します。今回はIPアドレスで証明書を作成するので、CommonName、サブジェクトの別名をチェックしないようにします。

```
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
```

5-3-6. サービスを再起動します。

```
# systemctl restart httpd
```

5-4. ミドルウェア設定（作業対象：web−01）

5-4-1. 動作確認のため、index.htmlを作成します。

```
vi /var/www/html/index.html
```

5-4-2. アクセスすると「Hello！proxy！」と表示されます

```
<html>
<head>
<title>HelloProxy</title>
</head>
<body>
Hello！proxy！
</body>
</html>
```

5-4-3. 検証のため、自己証明書（鍵ファイル）を発行します。パスワードを求められるので、パスワードを入力します。（後に削除します。）
本ドキュメントでは自己証明書を作成していますが、必要に応じて適切な証明書をご利用ください。

```
# cd /etc/pki/tls/certs/
# make server.key
```

5-4-4. 今回はパスワードは削除します。「5-4-3.」で入力したパスワードを再度入力します。

```
# openssl rsa -in server.key -out server.key
```

5-4-5. 自己証明書の発行（証明書）をします。

```
# make server.csr
# openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 3650
```

5-4-6. https通信用にSSLモジュールをインストールします。

```
#  yum -y install mod_ssl
```

5-4-7. 設定ファイルを編集します。

```
# vi /etc/httpd/conf.d/ssl.conf
```

5-4-8. 「SSLCertificateFile」に証明書の配置ディレクトリを指定します。

```
SSLCertificateFile /etc/pki/tls/certs/server.crt
```

5-4-9. 「SSLCertificateKeyFile」に鍵ファイルの配置ディレクトリを指定します。

```
SSLCertificateKeyFile /etc/pki/tls/certs/server.key
```

5-4-10. サービスを再起動します。

```
# systemctl restart httpd
```

5-5. SLB設定　設定対象：SLB01（東京リージョン）

5-5-1. 東京リージョンでSLBを購入します。購入方法については[こちら]を参照ください。

5-5-2. 左メニューより、「マスタースレーブサーバーグループ」を選択し、「マスターサーバーグループを作成する」をクリックします。

5-5-3. 443番ポート用のマスタースレーブサーバーグループを作成します。

1) 「グループ名」を入力します。
2) 「仮想ネットワーク」のチェックボックスをクリックします。
3) 表示されたインスタンス一覧より、冗長化したいインスタンスを選択します。
4) 選択したインスタンスの「ポート」に利用するポート番号（443）を入力し、スレーブサーバーのチェックボックスをクリックします。
5) 最後に右下の「確認」ボタンをクリックします。

5-5-4. 左のメニューより、インスタンスリスナーを選択し、「リスナーの作成」ボタンをクリックします。

5-5-5. モニターを配置します。

1) 「フロントエンドプロトコル」にポート番号を入力します。
2) 「バックエンドプロトコル」にポート番号を入力します。
3) 「マスタースレーブサーバーグループ」をクリックします。
4) 「グループID」より、1)で入力したポート番号と同じグループを選択します。
5) 「次のステップ」をクリックします。

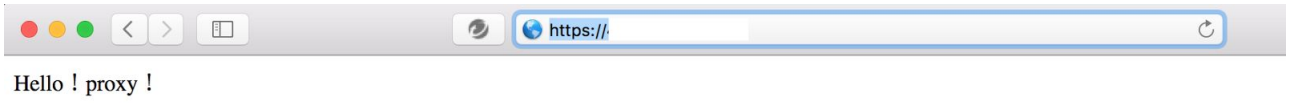
5-5-6. ヘルスチェックは特に変更がなければ「確認」ボタンをクリックします。

5-6. SLB設定　設定対象：SLB02（北京リージョン）

5-6-1. 北京リージョンでSLBを購入します。購入方法、設定方法については前章と同じです。

5-7. 動作確認

5-7-1. ブラウザからの確認（Master経由）
SLB01のIPアドレスで北京webサーバー（web-01）のindex.htmlが見られることを確認します。



5-7-2. ブラウザからの冗長確認
以下の状態でも途切れることなく北京webサーバーのindex.htmlが見られることを確認します。

1) proxy-01をシャットダウンします。
2) proxy-03をシャットダウンします。
3) proxy-01を起動します。
4) proxy-03を起動します。

5-7-3. SLBコンソールからの確認

「マスタースレーブグループ」の「詳細」よりどちらのポートが『実行中』か確認ができます。

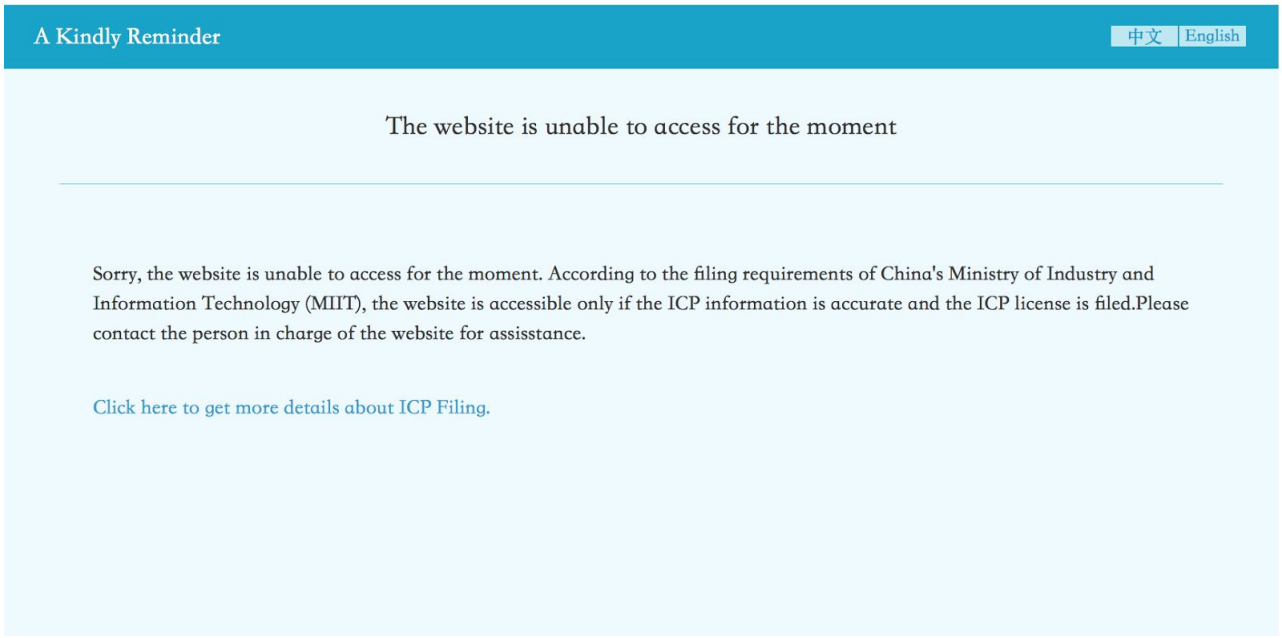
5-7-4. アクセスログの確認

各インスタンスのアクセスログ確認方法です。

```
# tail /var/log/httpd/ssl_access_log
```

6. ICPライセンスについて

　中国でwebサーバを構築するにはICPライセンスが必要となります。（ICPライセンスについてはこちらを参照ください）
検証で構築したとしても以下のような画像が出てくることがあるので、ご注意ください。



ご利用上の注意事項

この資料は、Alibaba Cloudの提供するクラウドサービスの機能について説明したもので、サービスのご利用を検討する際の参考となる技術的情報を提供するものです。
今後、本資料はクラウドサービスの機能追加・変更等に合わせて、予告なく変更される場合があります。閲覧された情報は最新のものではない場合がありますので、予めご了承下さい。

改版履歴

日付	版数	変更内容
2017/10/23	1.0	初版作成

SB Cloud