

ICT BUSINESS ONLINE

クラウド 業務の効率化



Enterprise Cloud 2.0 上で、オープンソース「pfSense」、 「pound」を利用してファイアウォール、ロードバランサーを構築してみた

NTTコミュニケーションズのICTビジネスオンライン編集部です。

機能拡張されたEnterprise Cloud (以下、ECL2.0) では、ネットワーク系のメニューとして高機能なファイアウォール (Brocade 5600 vRouter)、 Managed Firewall/UTMおよびロードバランサー (NetScaler VPX)を提供しており、ご利用いただくことが可能です。しかし、もっと簡易にお手軽に ファイアウォールやロードバランサーを利用したいという方向けに、今回オープンソースの仮想アプライアンスやソフトウェアを利用してEnterprise Cloud 上でファイアウォール、ロードバランサーを構築してみました。

1.ファイアウォール

仮想ネットワークアプライアンス用のISOイメージとして提供されている「pfSense」を利用します。 公式サイトはこちら (https://pfsense.org/)

では、さっそくはじめていきます。

1.1 pfSenseのインストール方法

はじめに、 pfSenseサイト (https://www.pfsense.org/)より ISO イメージをダウンロードします。

「pfSense-CE-2.3.2-RELEASE-amd64.iso.gz 」 をダウンロードしました。



ECL2.0のカスタマーポータルにログインして、「ク ラウドコンピューティング」をクリックします。以降、 文中出てくるポータル操作の詳細は Knowledge Centerのチュートリアル (https://ecl.ntt.com/documents/tutorials/) を参照ください。

- イメージ保存領域のご利用方法
- ●仮想サーバーのご利用方法

など

「サーバー」>「仮想サーバー」>「イメージ保存領域」 をクリックします。





プライベートテンプレート/ISOアップロード機能より、最初にダウンロードしたpfSenseのISOイメージをアップロードします。



イメージを作成します。

イメージの作成	
名前・ タグ 0	説明: ファイルのアップロードによりイメージを作成することが可能です。
 イメージファイル ● 参照 ファイルが選択されていません。 形式 * ISO - 光学ディスクイメージ 	
最小ディスク (GB) D	
最小メモリー (MB) の (MB) (MB) (MB) (MB) (MB) (MB) (MB) (MB)	
ライセンススイッチ取YOL ライセンススイッチ種別を確認してください の 単 単 単 単	

③ ②でアップロードしたテンプレートよりインスタンスを作成します。

■詳細* データボリューム アクセ メタデータ	えとセキュリティー	- Post-Install sc	ript ネットワー	²
ゾーン/グループ		インスタンスを起動す	「るために『詳細を指算	記ます。
いずれかのゾーン/グループ	-	下のグラフは、このコ	加ジェクトで使用し	ているリソースを、
インスタンス名		フレーバーの詳	92月801ま示し ⁷ 細	(1)ます。
		名前	1CPU-4GE	9
フレーバー *0		仮想 CPU	1	
1CPU-468	-	メモリー	4.0 GB	
インスタンスのブートソース・0		ブロジェクトのリ	リース上限	
17-50-58580		インスタンス数		6 of 256 Used
1メージ名 '				
ptsense2.3 (604.4 MB)	-			

・ の ▼ C 😵 Login

Login to pfSense

User

I.

Enter your password

×

- 0

1.2 pfSenseの設定方法

 pfSenseには設定用の端末が別途必要です。設 定用端末のブラウザよりWebGUIにpfSenseに 割当したIPアドレスで接続し、pfSenseにログイ ンします。今回は、よく利用される以下機能につ いての設定画面を紹介します。 \mathbb{R}

- ●ACLによるセキュリティ設定
- ●外部からのアクセスをNAT変換する設定
- ●他ネットワークへのルーティング設定

[Firewall]の[Rules]よりACLを 設定します



Sense System • Interfaces • Firewall • Services • VPN • Status • Diagnostics • Gold • Help • • Aliases Firewall / NAT / 1:1 0 NAT Rules Schedules Port Forward 1:1 Outbound NPt Traffic Shaper Virtual IPs NAT 1:1 Mappings Interface External IP Internal IP Destination IP Description Actions / 🗋 û • • WAN 153.153.153.150 10.0.20.5 . 🕇 Add 🕽 Add 🎁 Delete 🖺 Sam

③[Firewall]の[NAT]よりNATを 設定します

 ④[System]の[Routing]よりルーティングを 設定します

	System -	Interfaces	- Firewall -	Services -	VPN -	Status 🕶	Diagnostics -	Gold 🗸	Help 👻		•
System /	Advanced Cert. Man	ager	ays						C	o 💷 📼	0
Gateways Stat	General S High Avai Logout	etup I. Sync	ups								
Gateways	Package	Manager									
Name	Routing		rerface	Gateway		Monitor I	P Dese	ription	Actic	ons	
Ø WANGW	Setup Wiz Update User Man	ager	WAN	10.0.10.3	0	10.0.10.3	30		~ (101 +	Add

これで、pfSenseを利用したファイアウォールの設 定は完了です。

2. Pound

2.1 Poundのインストール及び設定方法

 ECL2.0のカスタマーポータルよりオフィシャルイ メージテンプレート (CentOS7.1)を利用してイン スタンスを作成します。

耳細・ データポリューム アクセスとセキュリテ メタデータ	 Post-Install s 	cript ネットワーク・	
ゾーングループ しいずれかかブーングループ ▼ インスタンス名・	インスタンスを起動 下のグラフは、この ブロジェクトのクォー フレーバーの言	するために詳細を指定します。 プロジェクトで使用しているリソース - タン対比して表示しています。 羊細	.老、
	名前	1CPU-408	
フレーバー *0	仮想 CPU	1	
1CPU-408	メモリー	4.0 GB	
インスタンスのブートソース 🛛 😡			
イメージから記動	ブロジェクトの	ハノース上限	
イメージタ・	インスタンス数	6 of 256	Use
CentOS-7.1-1503_64_virtual-server_12 (440.1]		

 ② ①で作成したCentOS7.1のインスタンスにSSH 接続し、Yumインタフェースより下記コマンドに てpoundをインストールします。
 ※当該インスタンスがインターネットに接続できる

環境となっている必要があります。

 ボランシグルールの設定ファイル (/etc/pound.cfg)を編集し、保存します。以下、 HTTPアクセスを2台のサーバーに同じプライオリ ティでロードバランシングする場合の設定例です。

Poundのインストールおよび設定は以上で終了で す。

今回は2つのオープンソースのネットワークアプライ アンスおよびソフトウェアの活用についてご紹介い たしました。安価にシステムを構築したいというユー ザーの方は、ぜひともお試しください。 # yum install epel-release

yum --enablerepo=epel -y install Pound

User "pound" Group "pound" Control "/var/lib/pound/pound.cfg" LogLevel 3 LogFacility local1 Alive 30

#HTTPのListen設定 ListenHTTP Address 10.0.20.5 Port 80 End

#分散サーバーの設定 Service #HTTPサーバー1 BackEnd Address 10.0.20.3 Port 80 Priority 1 End #HTTPサーバー2 BackEnd Address 10.0.20.4 Port 80 Priority 1 End End

サービス紹介

≫ Enterprise Cloud

NTT Comの[Enterprise Cloud]は、サービスの開発に集中できるPaaS基盤の提供など、デジタル トランスフォーメーションの実現まで視野に入れたクラウドサービスです。高機能、かつオープンソース のソフトウェアと連携可能な柔軟性があります。

クラウド業務で課題をお持ちのお客さま

フリーダイヤル/ナビダイヤル回線から便利な機能まで、お客さまニーズに合わせた最適なソリューションをご提案いたします。

 $\begin{array}{c|c} & 0 \\ \hline 0$