クラウド基盤構築演習
第二部: Eucalyptusによるクラウド基盤構築

第12回: Eucalyptusの仕組み（後編）

ver1.0 2012/02/28

目次

- セキュリティグループ管理機能の仕組み
- ElasticIP機能の仕組み
- EBS機能の仕組み

本講で学ぶこと、実施すること -1-

- セキュリティグループ管理機能の仕組みを理解しましょう
  - iptablesによって実現されているポートベースのファイアウォールがCCにて実装されていることを理解します
  - タグVLANによるネットワークセグメントの分離について理解します
- ElasticIP機能の仕組みを理解しましょう
  - ElasticIPがiptablesで実現されていることを理解します

本講で学ぶこと、実施すること -2-

- EBS機能を理解しましょう
  - どのようなアーキテクチャを利用してEBSが提供されているかを理解します
  - AoEとiSCSIによってどう実装が違うかを理解します
- マルチクラスタ機能を理解しましょう
  - 複数クラスタにまたぐ同一セキュリティグループ同士がどうやって疎通できるようにしているかを理解します

セキュリティグループ管理機能の仕組み

セキュリティグループ -1-

インスタンスに対するアクセス制御はセキュリティグループで設定します。セキュリティグループは「タグVLANによるプライベートネットワークセグメントの分離」と「iptablesによるパケットフィルタリング」によって実装されています。

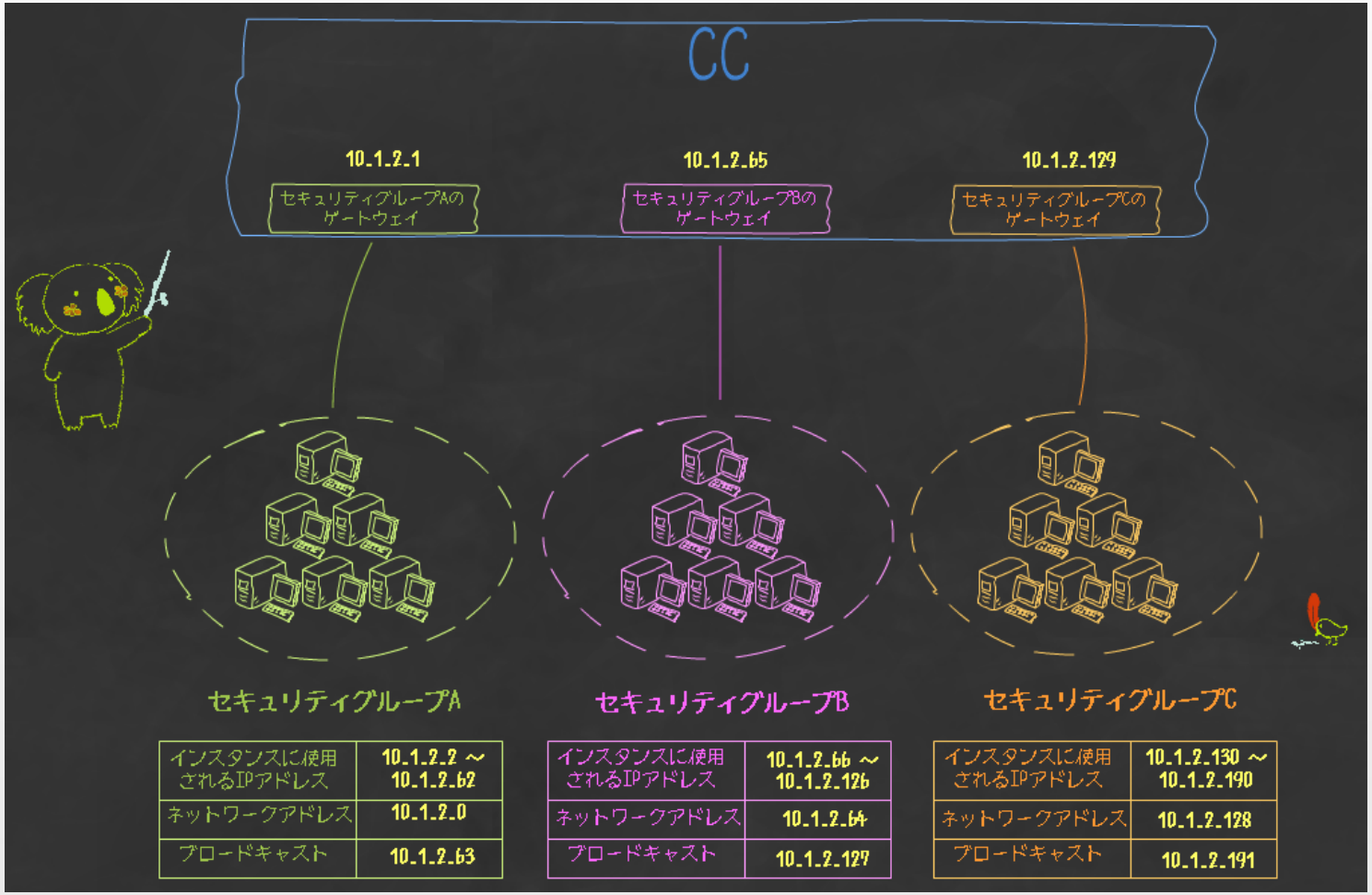
- タグVLANによるネットワーク分離

  タグVLANによるプライベートネットワークセグメントの設定はeucalyptus.conflに記述された値に従って、Eucalyptusが計算に基いて設定を自動的に行なうため一般利用者が勝手自由に設定を変更したりできないようになっています。

  よって、セキュリティグループ1つあたりのIPアドレス数などはEucalyptusの環境を構築する際にあらかじめ決めておくことが重要です。もちろんあとでも変更は可能ですが、これらの設定を変更した場合はインスタンスを停止しCCを再起動する必要があるため、稼働中のEucalyptusでおいそれと変更すべきではありません。

  なお、タグVLANによるプライベートネットワークの分離の詳細な仕組みについては前回の中井さんの資料を参考にしてください。

セキュリティグループ -2-



セキュリティグループA	
インスタンスに使用されるIPアドレス	10.1.2.2 ～ 10.1.2.62
ネットワークアドレス	10.1.2.0
ブロードキャスト	10.1.2.63

セキュリティグループB	
インスタンスに使用されるIPアドレス	10.1.2.66 ～ 10.1.2.126
ネットワークアドレス	10.1.2.64
ブロードキャスト	10.1.2.127

セキュリティグループC	
インスタンスに使用されるIPアドレス	10.1.2.130 ～ 10.1.2.190
ネットワークアドレス	10.1.2.128
ブロードキャスト	10.1.2.191

セキュリティグループ -3-

- iptablesによるフィルタリングとNAT

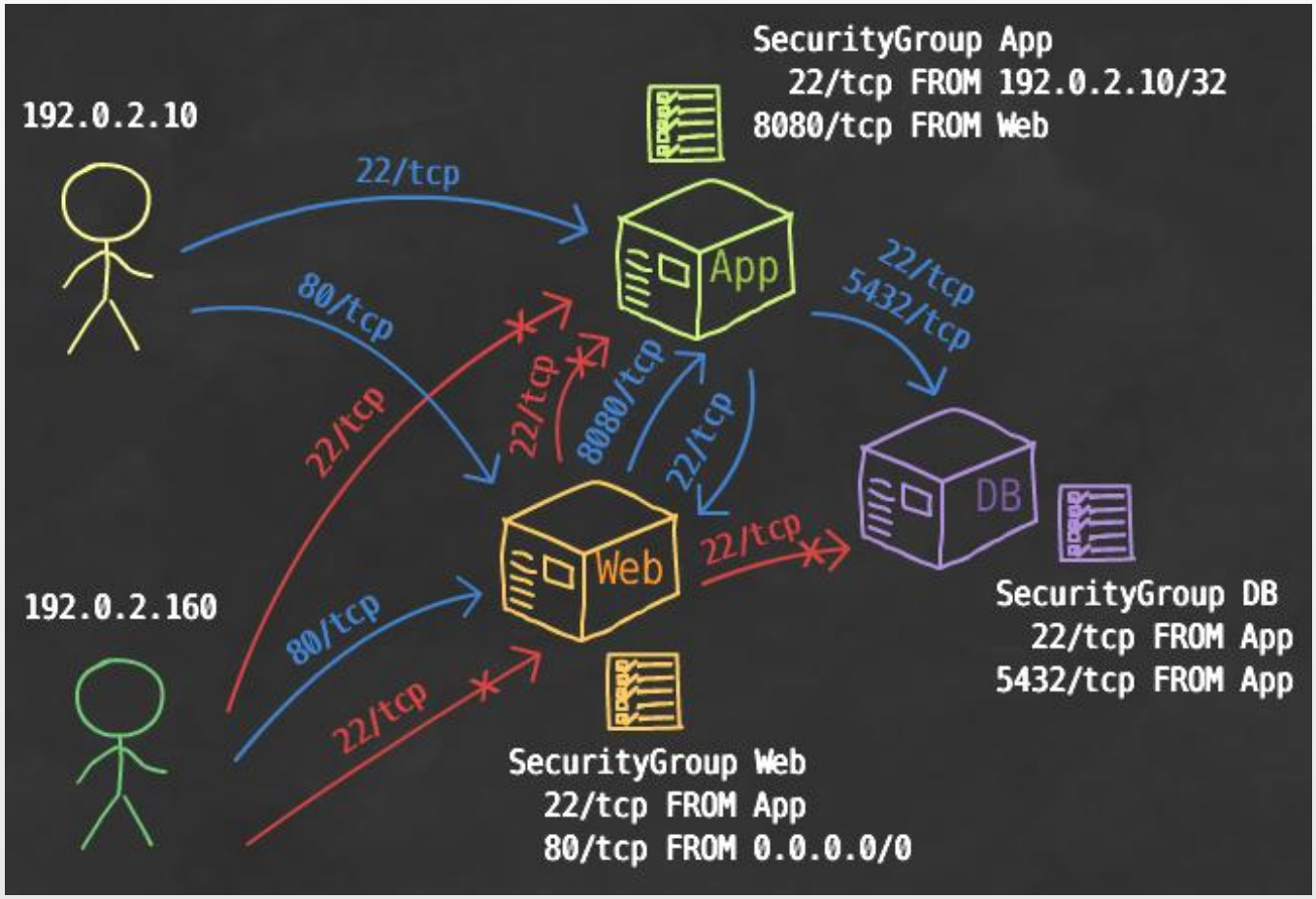
  iptablesによるパケットフィルタリングは、利用者がEuca2oolsのeuca-authorizeやeuca-revokeを使用して柔軟に設定することが可能です。前述のタグVLANがインスタンスのプライベートネットワークを分離する機能であるのに対し、パケットフィルタリングは外部からインスタンスにアクセスするためのPublicIPに対するアクセス制御の機能になります。

  Eucalyptusの場合、PublicIPはCCのVNET_PUBINTERFACEに設定され、CC上のiptablesで制御されます。パケットフィルタリングは、設定対象としてプロトコルとポートの組み合わせを指定し、制御対象として接続元のネットワークか他のセキュリティグループを指定します。

  なお、iptablesのパケットフィルタリングの詳細な仕組みについては前回の中井さんの講義資料で復習してください。

セキュリティグループ -4-

- EucalyptusではPublicIPは全てCCに付与され、CCのiptablesのNAT機能により各NC上のインスタンスに付与されているPrivateIPに対して転送されます。



ELASTICIP機能の仕組み

ElasticIP機能について

- インスタンスに取り付けられているPublicIPはインスタンスを停止すると解放されてしまいます。そのため第三者に対してインスタンスでサービスを提供する場合などにPublicIPが都度変ってしまっては不便なため、ElasticIPの機能を利用してPublicIPを確保しインスタンスに取り付け、PublicIPがインスタンスの停止時に解放されてしまうことを防ぐことができます。

- なお、一般利用者がPublicIPの確保や解放を行なうにはコマンド「euca-allocate-address」「euca-release-address」やAPI「AllocateAddress」「ReleaseAddress」を使用し、確保したPublicIPをインスタンスへ取り付けたり取り外したりするにはコマンド「euca-associate-address」「euca-disassociate-address」やAPI「AssociateAddress」「DisassociateAddress」を使用します。

- インスタンスのPublicIPは前述したようにCCのVNET_PUBINTERFACEに対して設定されるため、PublicIPの取り付け/取り外しはCC上で処理されます。なお、PublicIPをインスタンスから取り外した場合、そのインスタンスに以前取り付けられていたPublicIPが取り付けられます。

EBS機能の仕組み

EBSボリューム -1-

- EBSボリュームの作成と取り付け

  インスタンスのディスクは揮発性のディスクであり、インスタンスが停止すると全てのデータが削除されます(S3インスタンスの場合のみ)。そのため、永続化したいデータを扱う場合はEBSボリュームを作成してインスタンスで利用します。

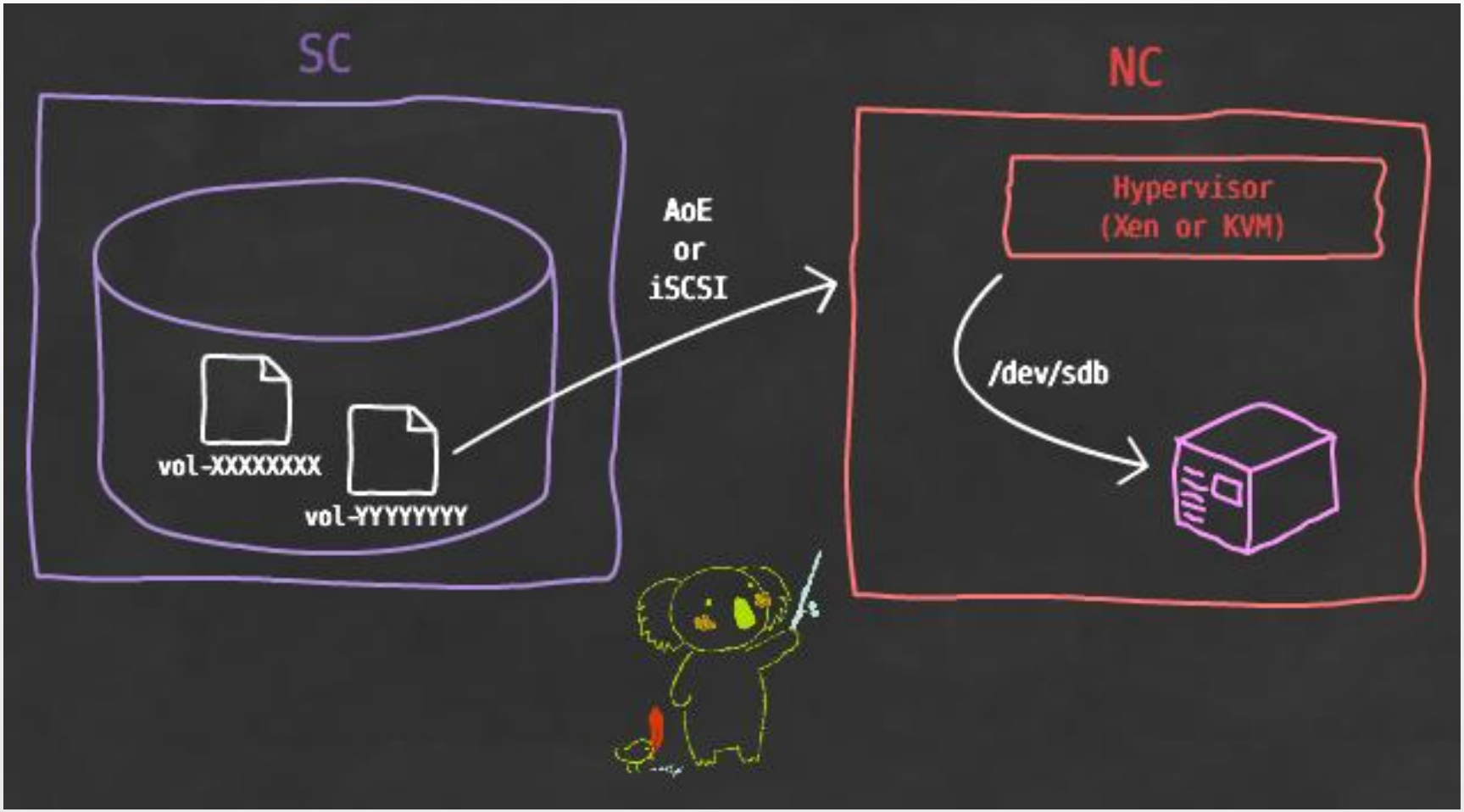
  Eucalyptusでは、EBSボリュームを実現するためにATA over Ethernet(AoE)かiSCSIのどちらかを使用します。

  どちらを使用する場合でも、SC上にEBSボリュームのデータを格納するためのファイルが作成され、そのファイルにLVMパーティションやLVMの管理構造体を作成し、AoEやiSCSIによってインスタンスが起動しているNCに提供されます。

  作成したEBSボリュームは、コマンド「euca-attach-volume」「euca-detach-volume」やAPI「AttachVolume」「DetachVolume」を使用してインスタンスに取り付け/取り外しを行ないます。AoEでもiSCSIでもEBSボリュームはインスタンスに直接取り付けられるわけではなく、インスタンスが起動しているNCに渡されてNCのハイパーバイザーの機能によってインスタンスに取り付けられます。

  なお、インスタンスにEBSボリュームを取り付ける際には/dev/sdbや/dev/xvdbのようなデバイス名を指定します。

EBSボリューム -2-



EBSボリュームのスナップショット -1-

- EBSボリュームからのスナップショット作成

  EBSボリュームをバックアップする場合、取り付けられているインスタンス上で――例えばバックアップツールを利用してバックアップを取得することも可能ですが、簡単な方法としてEBSボリュームからスナップショットを作成する方法があります。このEBSスナップショットは、当然のことですがEBSボリュームを利用している最中でもスナップショットを作成することが可能です。

  ただし、インスタンスやNCの管理下で行なわれるわけではなくSC上で実施されるため、EBSボリュームに高負荷なI/Oが発生している状況下ではデータ不整合が発生する可能性がゼロではありません。よってEBSスナップショットを作成する際はインスタンス上で発生している負荷に注意を払う必要があります。

  なお、EBSスナップショットはEBSボリュームのLVM管理構造体の中身だけを取り出して、SCには生のファイルとして格納し、Walrusにはgzip圧縮したファイルとして格納します。

EBSボリュームのスナップショット -2-