Windows® NLB を使ったHP IceWall SSOのロードバランス

はじめに

IceWallサーバーの負荷分散を実現するには、Webサーバーの負荷分散装置として一般的に広く使われている「ロードバランサー」と呼ばれるネットワーク製品を使用することが一般的です。しかし、HP IceWall SSO 10.0 Windows版が販売されたことで、HP IceWall SSOをWindows Server ™上に構築することが可能となり、Windows Server に標準で搭載されているネットワーク負荷分散機能（以下、Windows® NLB）を使った構成も可能となりました。
Windows NLBを使った構成はいくつか制約事項はありますが、ネットワーク製品（ロードバランサー）を必要としない構成となるため、構築コストも抑えることが可能です。本技術レポートでは、Windows NLBの仕組み、HP IceWall SSOと連携した場合の構成例、機能検証とその結果について記述します。

1.Windows NLB とは

Windows NLBとはWindows Serverに標準で搭載されているネットワーク負荷分散機能です。
※ NLB(Network Load Balancing)。旧名称はWLBS(Windows Load Balancing Service)。

NLBはWindowsネットワークドライバーとして実行され、複数台のホストを仮想的な1つのクラスターとして統合します。1つのクラスターには最大32のホストを含めることが可能で、複数の仮想IPアドレスを割り当てることが可能です。

NLBクラスター構成

ご参考:≫ ネットワーク負荷分散の概要

2. Windows NLBの仕組み

2.1 振り分け

クライアントから送られたリクエストのサーバーへの振り分けは、クラスター構成時に設定されたアフィニティによって制御されます。
設定されたアフィニティから算出基礎が決められ、得られたハッシュ値によってリクエストの振り分けが行われます。

アフィニティには3種類あり、それぞれの算出基礎は下表の通りです。

アフィニティ	ハッシュ値算出基礎
なし	クライアントのIPアドレスとポート
単一	クライアントのIPアドレス
クラスC	クライアントのIPアドレスの上位24ビット

※1. 通信プロトコルに「UDP」が使用される場合は「単一」or「クラスC」にする必要があります。
※2. SSLリクエストを受け付ける場合は「単一」にする必要があります。

2.2 クラスター操作モード

Windows NLBのクラスター操作モードは下記の2つがあります。

モード	概要	懸念事項
ユニキャスト	全てのクラスターホストに同じMACアドレスが割り当てられる。	クラスター構成に含まれるホスト間での通信ができない。
マルチキャスト	クラスターホストのMACアドレスはそのままで、NLB用のMACアドレスを割り当てる。	NW機器側で静的なARPエントリを追加する必要がある。 ※1

※1. クラスターホストからのARP応答によって、ホストのMACアドレスとクラスターの仮想IPがマッピングされる場合があるため。

※VMWareではマルチキャストを推奨しています。
ユニキャストを使用する場合はvSwitchにRARPを送信しないようにする設定が必要です。
ご参考:≫ Microsoft NLB not working property in Unicast Mode

2.3 障害検知/拡張性/管理

障害検知は各ホストが別のホストに発行するハートビートによって行います。
ハートビートは毎秒発行され、必要な帯域は1,500バイトのみです。
ハートビートはデータが送受信されるネットワークに送受信されます。

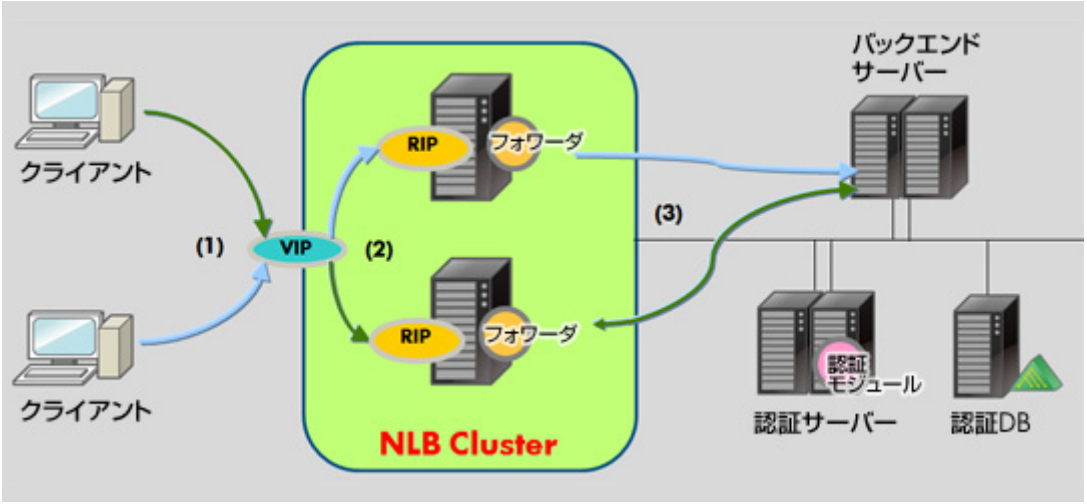
障害発生してハートビートを発行しないホストがある場合、該当のホストをクラスターから削除し、リクエストを残りのホストにマッピングします。
ハートビートを受け取らなくなってから5秒後に障害発生と判断します。

Windows NLBではNIC障害やサーバーダウンを検知することが可能ですが、サービスレベルでの障害検知(IISの障害検知)は行えません。
従ってサービスレベルでの障害については、IISの自動再起動機能で回避するものと考えて運用する必要があります。
ただし、マイクロソフトの製品「Operations Manager」のオプション「ネットワーク負荷分散管理パック」を使用すればサービス検知も可能です。(別途ライセンスの購入が必要です。)

Windows NLBではクラスターを停止することなくホストの追加/削除が可能です。
また、クラスターはGUIツール「NLB マネージャー」で管理可能です。
複数のクラスターを1つのNLBマネージャーから管理する事も可能です。

3. Windows NLBを用いたHP IceWall SSO構成例

以下はWindows NLBを用いた場合のHP IceWall SSOの構成例です。



処理フロー概要

1. クライアントはWindows NLBのVIP経由でIceWallサーバーへアクセスを行います。
2. Windows NLBはアフィニティ設定を元にリクエストをIceWallサーバーに振り分け処理を行います。

3. IceWallサーバーはバックエンドサーバーのへアクセスを行い、クライアントへコンテンツを返します。

※認証前であればログイン画面の返却、認証後であれば、認可の処理を行います。

4 Windows NLB 検証環境

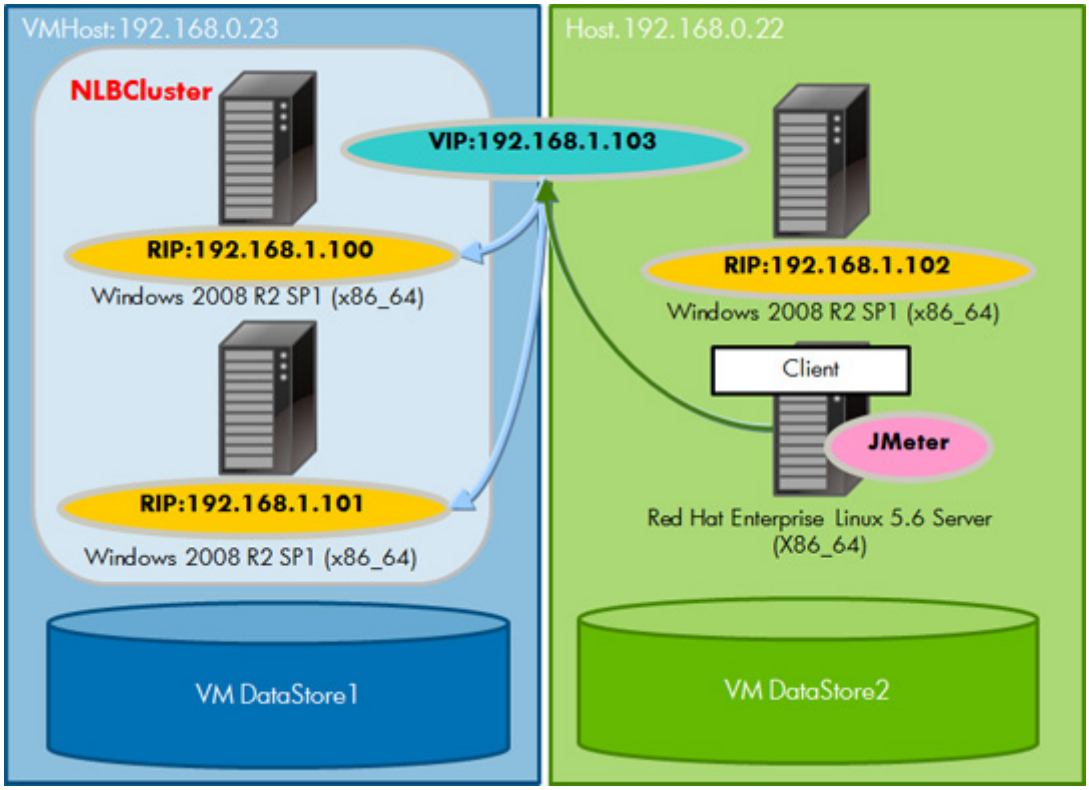
Windows NLBの振り分け機能、障害検知機能の検証を行いました。検証を行った環境は以下のとおりです。

- VMWare環境で2台のサーバーを使用したクラスターを構成しました。
  OSは「Microsoft® Windows Server 2008 R2 SP1(x86 64bit)」を使用し、
  VMWare環境であるためクラスター操作モードを「マルチキャスト」としました。

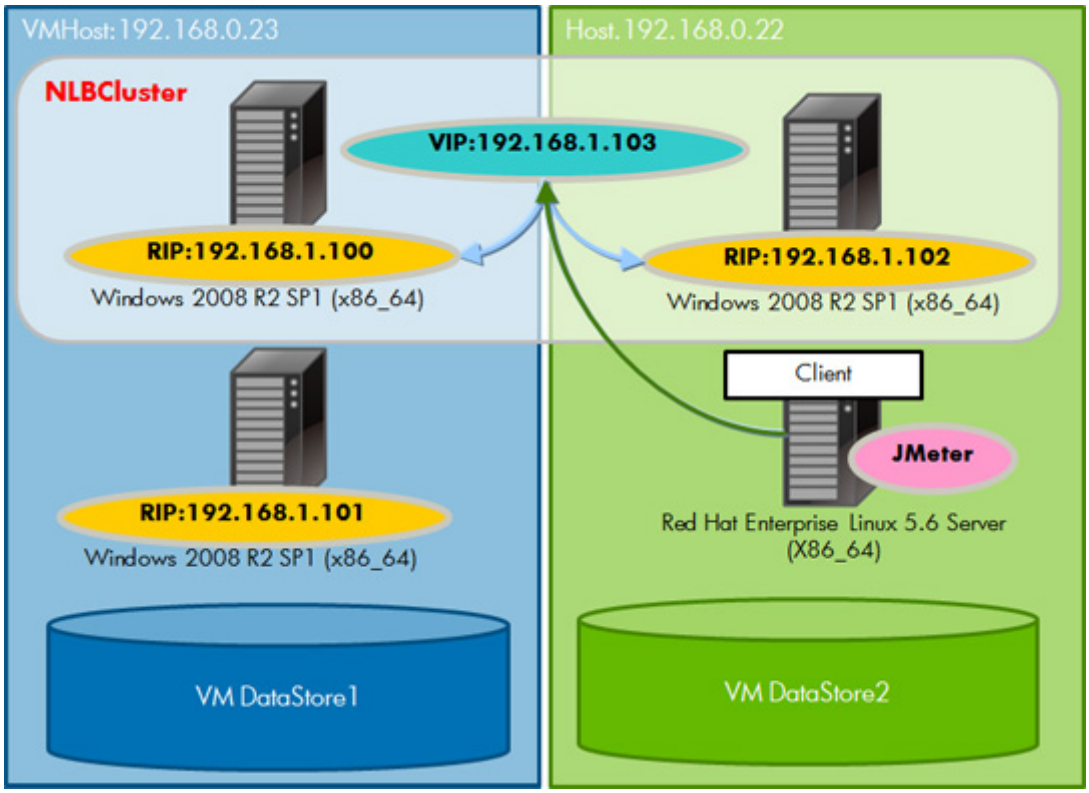
- クライアントには負荷ツール(JMeter2.6)を使用しました。
  クライアントのOSは「Red Hat Enterprise Linux 5.6 Server (x86_64) 」を使用し、
  NLBはネットワークレベルでの振り分けしか行えないため、
  クライアントのIPアドレスを40個割り当てました。

クラスター構成パターンは以下の2種類で行っています。

パターン1　同一のVMHOST上で動作するサーバー2台でのクラスター構成



パターン2　異なるVMHOST上で動作するサーバー2台でのクラスター構成



5. Windows NLBの検証結

5.1振り分け機能

Windows NLBの振り分け機能について、以下のテストケースで検証を行いました。

- httpリクエスト
  httpリクエストについて、アフィニティ単一/なしの振り分け動作を確認
  - アフィニティが「なし」の場合：JMeterから単一IPで40リクエストを発行
  - アフィニティが「単一」の場合：JMeterから40IPでリクエストを発行
- httpsリクエスト
  httpsリクエストについて、アフィニティ単一の振り分け動作を確認
  - JMeterから40IPでリクエストを発行

テスト実施結果(振り分け件数)は以下となりました。

- アフィニティが「なし」の場合： host1とhost2で振り分け数に差が生じました
- アフィニティが「単一」の場合：http、httpsともにhost1とhost2で均一にIPが振り分けられました

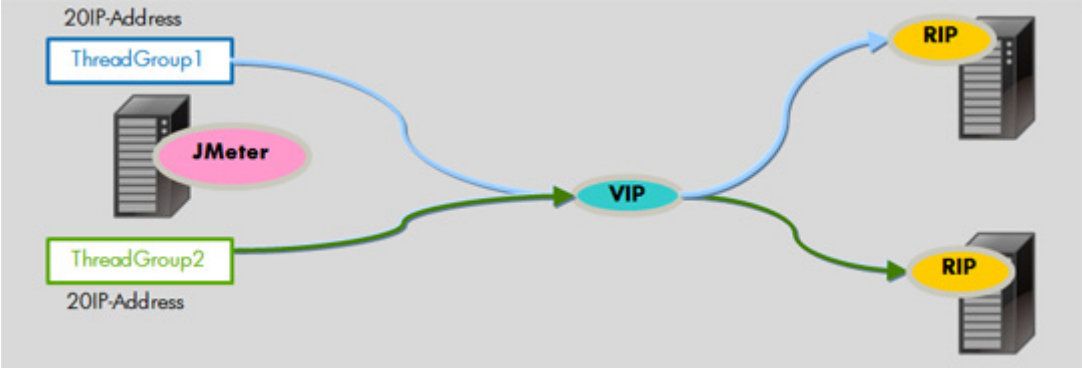
アフィニティの種類		単一		なし	
ホスト分類		host1	host2	host1	host2
同一VMHOST	http	20	20	23	17
	https	20	20	–	–
異なるVMHOST	http	20	20	18	22
	https	20	20	–	–

5.2 障害検知機能

Windows NLBの障害検知機能について、以下テストケースで検証を行いました。

テストケース

- JMeterで負荷を掛けている途中で片系をシャットダウンさせます。
- 予め各ホストに振り分けられるIPアドレスを確認し、2つのThreadGroupを同時に動かします。
  - 各20IPアドレスを割り当て、秒間20アクセスのリクエストを繰り返し発行します。



- アフィニティは単一を推奨とするため、単一で試験を行います。
- 通信プロトコルによる動作の違いは無いと考えられるため、「http」で試験を実施します。

上記を異なるVMHOST上で動作するサーバー2台でクラスター構成した場合と、同一のVMHOST上で動作するサーバー2台でクラスター構成した場合とで試験を実施しました。

同一のVMHOST上で動作するサーバー2台でのクラスター構成の場合の実施結果です。

実施結果(同一VMHOST)は以下となりました。

JMeterの実行結果

アクセス対象	総リクエスト数	エラー件数
シャットダウンしないホスト	1864	0
シャットダウンしたホスト	1142	129

エラー内容詳細

エラー分類	発生件数	発生時間(ms)
503,Service Unavailable	41	2003
Non HTTP response code: java.net.ConnectException	88	4352
合計	129	6335

異なるVMHOST上で動作するサーバー2台でのクラスター構成の場合の実施結果です。

テスト実施結果(異なるVMHOST)は以下となりました。

JMeterの実行結果

アクセス対象	総リクエスト数	エラー件数
シャットダウンしないホスト	2198	0
シャットダウンしたホスト	1776	136

エラー内容詳細

エラー分類	発生件数	発生時間(ms)
503,Service Unavailable	40	1950

Non HTTP response code: java.net.ConnectException	96	4752
合計	136	6702

6 Windows NLB の検証結果まとめ

Windows NLB 検証結果のまとめを記載します。

振り分け機能	「アフィニティ:単一」の方がアクセスを均等に振り分けることができました。 下記を考慮して、アフィニティは「単一」を推奨します。 • 「アフィニティ:単一」はHTTP,HTTPSの両方で適用可能です。 • リソース使用率(CPU,メモリ)は、アフィニティの違いによる差はありませんでした。 • VMHOSTが同一か、異なるかによる動作の違いはありませんでした。 「アフィニティ:なし」を適用するケースとしてはProxyを経由している等の影響で同一IPアドレスからの「http」リクエストが多く発生する場合に考えられます。 「アフィニティ:なし」は同一IPでもクライアントの送信元ポートが異なる場合には別々のホストにアクセス先が振り分けることが可能です。
障害検知機能	VMHOSTが同一、異なるいずれのケースも7秒弱で再振り分けが完了しました。 • Microsoft社が謳っている5秒で障害検知という内容とほぼ一致しました。 • 障害が発生しないホストに振り分けられているアクセスは停止しませんでした。 • VMHOSTが同一か、異なるかによる動作の違いはありませんでした。 NLBはNIC障害やサーバーダウンの障害検知が可能ですが、Webサービス(IIS)の障害検知ができません。ダウンしたIISへアクセスしているクライアントは、IISがダウンしている間はブラウザに接続エラーが表示されることになります。 実際の導入に際しては、要件に応じて下記のいずれかの検討が必要です。 • IISの自動再起動機能を使用する。 • IISダウン時にシャットダウンもしくはネットワークインターフェースをダウンさせる仕組みの実装を行う。

7 まとめ

本技術レポートでは、Windows NLBの仕組み、 HP IceWall SSOと連携した場合の構成例、機能検証とその結果について記述しました。

HP IceWall SSO 10.0 Windows版が販売されたことで、HP IceWall SSOをWindows Server上に構築することが可能となり、Windows Serverに標準で搭載されているWindows NLBを使った構成も可能となりました。

HP IceWall SSO 10.0 Windows版をご利用の際には本ソリューションを是非ご活用ください。

8 参考URL

» ネットワーク負荷分散
» ネットワーク負荷分散 - FAQ (よく寄せられる質問)
» ネットワーク負荷分散の機能強化
» Microsoft TechNet: IT Pro 道場 自主トレシリーズ – 負荷分散の設定
» Operations Manager
» Operations Manager:Windows Server 2008 ネットワーク負荷分散管理パック ガイド

2012.6.29 日本ヒューレット・パッカード テクノロジーコンサルティング統括本部 スペシャリスト 佐藤 義昭
日本ヒューレット・パッカード テクノロジーコンサルティング統括本部 日比 裕介

日本ヒューレット・パッカード テクノロジーコンサルティング統括本部　　佐藤　智行