Vmware 環境で適切な仮想 WSA HA グループ機能を確認する

目次

概要

このドキュメントでは、VMware 環境で稼動する仮想 WSA 上で Cisco Web セキュリティ アプライアンス（WSA）の高可用性（HA）機能を正しく動作させるために実行する必要のあるプロセスについて説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco WSA
- HTTP
- マルチキャスト トラフィック
- Common Address Resolution Protocol（CARP）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- AsyncOS for Web バージョン 8.5 以降

- VMware ESXi バージョン 4.0 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

問題

HA グループを 1 つ以上設定した仮想 WSA の HA が、優先度を最高にしても、常にバックアップ状態になります。

次の口グの抜粋が示すように、システム ログに、常に状態が変化していることが示されます。

```
Tue May 19 08:05:52 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:05:52 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:37 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:37 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
```

パケット キャプチャを実行（この例ではマルチキャスト IP アドレス 224.0.0.18 に対して実行）すると、次のような出力を確認できます。

```
Tue May 19 08:05:52 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:05:52 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 is down
```

```
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:37 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:37 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
```

問題の分析

前のセクションで示した WSA システム ログには、HA グループが CARP のネゴシエーションでマスターになった時点で、より優先度が高いアドバタイズメントを受信していることが示されています。

これは、パケット キャプチャからも確認できます。 仮想 WSA から送信されたパケットを次に示します。

```
13:49:04.601713 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
```

ミリ秒の時間内に、同じ送信元 IP アドレス (同じ仮想 WSA アプライアンス) から別のパケット セットが送信されていることを確認できます。

```
13:49:04.602798 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
13:49:04.602809 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
```

この例では、192.168.0.131 という送信元 IP アドレスが、問題のある仮想 WSA の IP アドレスです。 マルチキャスト パケットが仮想 WSA にループバックされていることが予想されます。

この問題は、VMware 側の問題に起因しています。次のセクションで、この問題を解決するために実行する必要のある手順について説明します。

解決策

この問題を解決し、VMware 環境に送信されるマルチキャスト パケットのループを停止するには、次の手順を実行します。

1. 仮想スイッチ (vSwitch) の**無差別モード**を有効にします。
2. **MAC アドレスの変更**を有効にします。
3. **偽装転送**を有効にします。
4. 同一の vSwitch 上に複数の物理ポートが存在する場合は、Net.ReversePathFwdCheckPromisc オプションを有効にする必要があります。これにより、

マルチキャスト トラフィックがホストにループバックされ、CARP が *link states coalesced* メッセージを出して機能しなくなる vSwitch のバグを回避できます（詳しくは、次のセクションを参照してください）。

Net.ReversePathFwdCheckPromisc オプションの変更

Net.ReversePathFwdCheckPromisc オプションを変更するには、次の手順を実行します。

1. VMware vSphere クライアントにログインします。
2. 各 VMware ホストに対して、次の手順を実行します。

   [host] をクリックし、[Configuration] タブに移動します。

   左ペインで、[Software Advanced Settings] をクリックします。

   [Net] をクリックし、[Net.ReversePathFwdCheckPromisc] オプションが表示されるまで下にスクロールします。

   [Net.ReversePathFwdCheckPromisc] オプションを [1] に設定します。

   [OK] をクリックします。

次は、*無差別モード*のインターフェイスを設定する、または、オフにしてから再度オンにする必要があります。 この手順はホストごとに実行します。

次の手順を実行して、インターフェイスを設定します。

1. [Hardware] セクションに移動し、[Networking] をクリックします。
2. vSwitch や仮想マシン（VM）のポート グループごとに、次の手順を実行します。

   vSwitch から [Properties] をクリックします。

   デフォルトでは、無差別モードは [Reject] に設定されています。 この設定を変更するには、[edit] をクリックし、[Security] タブに移動します。

   ドロップダウン メニューから [Accept] を選択します。

   [OK] をクリックします。

   注: この設定は、通常、VM ポート グループごとに適用され（より安全です）、vSwitch はデフォルト設定（[Reject]）のままです。

無差別モードを無効にしてから再度有効にするには、次の手順を実行します。

1. [Edit] > [Security] > [Policy Exceptions] の順に移動します。
2. [Promiscuous Mode] チェックボックスをオフにします。

3. [OK] をクリックします。

4. [Edit] > [Security] > [Policy Exceptions] の順に移動します。

5. [Promiscuous Mode] チェックボックスをオンにします。

6. ドロップダウン メニューから [Accept] を選択します。

関連情報

- CARP 構成のトラブルシューティング
- テクニカル サポートとドキュメント – Cisco Systems