VMware 환경에서 적절한 가상 WSA HA 그룹 기능 확인

목차

소개

이 문서에서는 Cisco WSA(Web Security Appliance) HA(High Availability) 기능이 VMware 환경에서 실행되는 가상 WSA에서 제대로 작동하도록 완료해야 하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco WSA
- HTTP
- 멀티캐스트 트래픽
- CARP(Common Address Resolution Protocol)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AsyncOS for Web 버전 8.5 이상

- VMware ESXi 버전 4.0 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

하나 이상의 HA 그룹으로 구성된 가상 WSA는 우선 순위가 가장 높은 경우에도 항상 *백업* 상태에 HA가 있습니다.

시스템 로그에는 이 로그 조각에 표시된 것과 같이 일정한 플래핑이 표시됩니다.

```
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)
```

패킷 캡처(이 예에서 멀티캐스트 IP 주소 224.0.0.18의 경우)를 수행할 경우 다음과 유사한 출력을 확인할 수 있습니다.

```
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
13:49:04.601931 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
13:49:04.602798 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
13:49:13.621706 IP (tos 0x10, ttl 255, id 24801, 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=15790098039517178284
13:49:13.622007 IP (tos 0x10, ttl 255, id 24801, 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=15790098039517178284
13:49:13.622763 IP (tos 0x10, ttl 255, id 24801, 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=15790098039517178284
13:49:13.622770 IP (tos 0x10, ttl 255, id 24801, 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=15790098039517178284
13:49:22.651653 IP (tos 0x10, ttl 255, id 44741, 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=15790098039517178285
```

문제 분석

이전 섹션에서 제공하는 WSA 시스템 로그에는 HA 그룹이 CARP 협상에서 마스터가 되면 우선순위가 더 높은 알림이 수신됨을 나타냅니다.

패킷 캡처에서도 이를 확인할 수 있습니다.가상 WSA에서 전송되는 패킷입니다.

```
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
```

밀리초 단위의 시간 프레임에서는 동일한 소스 IP 주소(동일한 가상 WSA 어플라이언스)에서 다른 패킷 집합을 볼 수 있습니다.

```
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
```

이 예에서 소스 IP 주소 192.168.0.131은 문제가 있는 가상 WSA의 IP 주소입니다.멀티캐스트 패킷이 가상 WSA로 다시 루프되는 것 같습니다.

이 문제는 VMware 측의 결함으로 인해 발생합니다. 다음 섹션에서는 문제를 해결하기 위해 완료해야 하는 단계에 대해 설명합니다.

솔루션

이 문제를 해결하고 VMware 환경에서 전송되는 멀티캐스트 패킷의 루프를 중지하려면 다음 단계를 완료하십시오.

1. vSwitch(가상 스위치)에서 프로미스큐어스 모드를 활성화합니다.

2. **MAC 주소 변경 사항을 활성화합니다**.

3. 위조된 **전송을 활성화합니다**.

4. 동일한 vSwitch에 여러 개의 물리적 포트가 있는 경우 멀티캐스트 트래픽이 호스트로 다시 루프되는 vSwitch 버그를 해결하려면 Net.ReversePathFwdCheckPromisc 옵션을 활성화해야 합니다. 그러면 CARP는 *링크 상태*와 함께 *작동하지* 않습니다.자세한 내용은 다음 섹션을 참조하십시오.

Net.ReversePathFwdCheckPromisc *옵션* 수정

Net.ReversePathFwdCheckPromisc 옵션을 수정하려면 다음 단계*를* 완료합니다.

1. VMware vSphere 클라이언트에 로그인합니다.

2. 각 VMware 호스트에 대해 다음 단계를 완료합니다.

   host를 클릭하고 *Configuration* 탭으로 이동합니다.

   왼쪽 창에서 **Software Advanced Settings(소프트웨어 고급 설정)**를 클릭합니다.

   Net**을** 클릭하고 아래로 스크롤하여 Net.ReversePathFwdCheckPromisc 옵션**으로** 이동합니다.

   Net.ReversePathFwdCheckPromisc *옵션을* 1로 **설정합니다**.

   확인을 **클릭합니다**.

프로미스큐어스 모드에 있는 인터페이스*를* 설정하거나 해제한 다음 다시 켜야 합니다.이 작업은 호스트 단위로 완료됩니다.

인터페이스를 설정하려면 다음 단계를 완료합니다.

1. Hardware(*하드웨어*) 섹션으로 이동하고 Networking(네트워킹)을 **클릭합니다**.

2. 각 vSwitch 및/또는 VM(Virtual Machine) 포트 그룹에 대해 다음 단계를 완료합니다.

   vSwitch에서 Properties를 클릭합니다.

   기본적으로 프로미스큐어스 모드는 거부로 *설정됩니다*.이 설정을 변경하려면 **편집**을 클릭하고 *보안* 탭으로 이동합니다.

   드롭다운 메뉴에서 Accept(수락)를 선택합니다.

   확인을 **클릭합니다**.

   참고:이 설정은 일반적으로 vSwitch가 기본 설정(거부)에 남아 있는 VM 포트 그룹 단위로 적용됩니다.

무차별 모드를 비활성화한 다음 다시 활성화하려면 다음 단계를 완료하십시오.

1. Edit(편집) **> Security(보안) > Policy Exceptions(정책 예외)로 이동합니다**.
2. Promiscuous Mode(프로미스큐어스 **모드) 확인란의 선택을** 취소합니다.
3. **확인**을 **클릭합니다**.
4. Edit(편집) **> Security(보안) > Policy Exceptions(정책 예외)로 이동합니다**.
5. Promiscuous **Mode(프로미스큐어스 모드)** 확인란을 선택합니다.
6. 드롭다운 메뉴에서 Accept(수락)를 선택합니다.

관련 정보

- CARP 구성 문제 해결
- 기술 지원 및 문서 – Cisco Systems