Cisco ASAv(Adaptive Security Virtual Appliance) 빠른 시작 설명서

버전 9.5

게시 날짜: 2015년 8월 12일
수정: 2016년 1월 28일

Cisco ASAv 소개

Cisco Adaptive Security Virtual Appliance(ASAv)는 전체 방화벽 기능을 가상화된 환경으로 가져와 데이터 센터 트래픽과 다중 테넌트 환경을 보호합니다.

ASDM 또는 CLI를 사용하여 ASAv를 관리하고 모니터링할 수 있습니다. 다른 관리 옵션을 사용할 수도 있습니다.

- ASAv에 대한 사전 요구 사항, 3페이지
- ASAv에 대한 지침, 3페이지
- ASAv Rate Limiter, 4페이지
- ASAv에 대한 라이센싱, 5페이지
- ASAv 인터페이스 및 가상 NIC, 6페이지

ASAv에 대한 사전 요구 사항

하이퍼바이저 지원은 Cisco ASA 호환성을 참조하십시오.

ASAv에 대한 지침

상황 모드 지침

단일 상황 모드에서만 지원됩니다. 다중 상황 모드는 지원되지 않습니다.

장애 조치 지침

장애 조치 구축의 경우, 대기 유닛에 동일한 라이센스 모델이 있는지 확인합니다. 예를 들어, 두 유닛 모두 ASAv30s여야 합니다.

지원되지 않는 ASA 기능

ASAv는 다음 ASA 기능을 지원하지 않습니다.

- 클러스터링
- 다중 컨텍스트 모드
- 활성/활성 장애 조치
- EtherChannel
- AnyConnect Premium 라이센스 공유

ASAv5에 대한 지침, 기능, 제한

- 점보 프레임은 지원되지 않습니다.
- VMware, KVM, Hyper-V에 1GB 메모리로 구축됩니다.

  1GB 메모리로 실행하려면 ASAv5 VM을 9.5.1.200 이미지로 다시 프로비저닝 해야 합니다. 9.5.1.200을 실행하는 ASAv만 1GB 메모리에서 작동할 수 있습니다. 이전 버전으로 다운그레이드할 경우 메모리를 2GB로 늘려야 합니다.

- 100Mbps의 성능.

  ASAv5는 임계값인 100Mbps에 도달하자마자 패킷을 삭제하기 시작합니다(100Mbps의 성능을 완전히 실행할 수 있는 약간의 여유가 있습니다). ASAv5는 적은 양의 메모리 공간 및 성능을 필요로 하는 사용자를 위한 제품이므로 더 많은 수의 ASAv5를 불필요한 메모리 소모 없이 구축할 수 있습니다.

- 초당 8,000건의 연결, 최대 35개의 VLAN, 50,000건의 동시 세션, 50개의 VPN 세션을 지원합니다.

ASAv Rate Limiter

참고: ASAv Rate Limiter는 약간의 여유를 두고 ASAv5에 대한 처리량 성능 제한을 적용하여 엔타이틀먼트 및 기본 Lab Edition 모드 ASAv 플랫폼을 매칭합니다.

4페이지의 표 1에서는 ASAv에 대한 라이센스 엔타이틀먼트를 매칭하는 적법한 리소스 시나리오를 보여줍니다.

표 1 라이센스 엔타이틀먼트

라이센스 엔타이틀먼트	vCPU/RAM	성능	Rate Limiter 적용
Lab Edition Mode(라이센스 없음)	모든 플랫폼	100Kbps	예
ASAv5(100M)	1vCPU/1GB	100Mbps	예
ASAv10(1G)	1vCPU/2GB	vCPU/RAM constrained	아니요
ASAv30(2G)	4vCPU/8 GB	vCPU/RAM constrained	아니요

4페이지의 표 2에서는 ASAv에 대한 리소스 및 엔타이틀먼트와 연결된 ASAv 상태 및 메시지를 보여줍니다.

표 2 ASAv 상태 및 메시지

상태	리소스와 엔타이틀먼트 비교	작업 및 메시지
규정 준수	리소스 = 엔타이틀먼트 한도 (vCPU, GB, RAM)	어플라이언스 리소스 최적 상태 ASAv5(1vCPU,1G), ASAv10(1vCPU,2G), ASAv30(4vCPU,8G) 작업 없음, 메시지 없음
	리소스 < 엔타이틀먼트 한도 프로비저닝 부족	작업 없음, ASAv가 라이센스 처리량으로 실행될 수 없다는 경고 메시지 로깅
규정 위반	리소스 > 엔타이틀먼트 한도 프로비저닝 초과	ASAv5 Rate Limiter가 작동하여 성능을 제한하고 콘솔에 경고를 로깅
		ASAv10 및 ASAv30은 콘솔에 오류 메시지를 로깅한 다음 재부팅

ASAv에 대한 라이센싱

ASAv에서는 Cisco Smart Software Licensing을 사용합니다. 자세한 내용은 ASAv를 위한 스마트 소프트웨어 라이센싱을 참조하십시오.

모델	라이센스 요건
ASAv5	Standard 라이센스 다음 사양을 참조하십시오. ■ 처리량 100Mbps ■ vCPU 1개 ■ 1GB RAM ■ 50,000개의 동시 방화벽 연결 ■ AWS 지원 안 함 ■ Standard D3 인스턴스에서 Azure 지원
ASAv10	Standard 라이센스 다음 사양을 참조하십시오. ■ 처리량 1Gbps ■ 1 vCPU ■ 2GB RAM ■ 100,000개의 동시 방화벽 연결 ■ c3.large 인스턴스에서 AWS 지원 ■ Standard D3 인스턴스에서 Azure 지원
ASAv30	Standard 라이센스 다음 사양을 참조하십시오. ■ 처리량 2Gbps ■ vCPU 4개 ■ 8GB RAM ■ 500,000개의 동시 방화벽 연결 ■ c3.xlarge 인스턴스에서 AWS 지원 ■ 베타 테스트에 Azure 지원 안 함

참고: ASAv에 스마트 라이센스를 설치해야 합니다. 라이센스를 설치할 때까지 예비 연결 테스트를 수행할 수 있도록 처리량이 100Kbps로 제한됩니다. 스마트 라이센스는 일반적인 운영에 필요합니다.

ASAv 인터페이스 및 가상 NIC

가상화 플랫폼의 게스트인 ASAv에서는 기본 물리적 플랫폼의 네트워크 인터페이스를 활용합니다. 각 ASAv 인터페이스는 가상 NIC(vNIC)에 매핑됩니다.

- ASAv 인터페이스, 6페이지
- 지원되는 vNIC, 6페이지

ASAv 인터페이스

ASAv에는 다음과 같은 기가비트 이더넷 인터페이스가 포함되어 있습니다.

- 관리 0/0

  Azure의 경우 Management 0/0이 트래픽을 전달하는 "외부" 인터페이스일 수 있습니다.

- GigabitEthernet 0/0에서 0/8까지 포함. GigabitEthernet 0/8은 ASAv를 장애 조치 쌍의 일부분으로 구축할 경우 장애 조치 링크에 사용됩니다.
- Hyper-V는 최대 8개의 인터페이스를 지원합니다. Management 0/0 및 GigabitEthernet 0/0 ~ 0/6입니다. GigabitEthernet을 페일오버 링크로 사용할 수 있습니다.

지원되는 vNIC

ASAv에서는 다음 vNIC를 지원합니다.

vNIC 유형	Hypervisor 지원		ASAv 버전	참고
	VMWare	KVM		
e1000	**예**	**예**	9.2(1) 이상	VMware 기본값
Virtio	아니요	**예**	9.3(2.200) 이상	KVM 기본값

VMware를 사용하여 ASAv 구축

VMware를 사용하여 ASAv를 구축할 수 있습니다.

- ASAv에 지원되는 VMware 기능, 7페이지
- ASAv 및 VMware에 대한 사전 요구 사항, 8페이지
- ASAv 및 VMware에 대한 지침, 8페이지
- ASAv 소프트웨어 압축 풀기 및 VMware용 Day 0 컨피그레이션 파일 생성, 9페이지
- VMware vSphere Web Client를 사용하여 ASAv 구축, 11페이지
- VMware vSphere 독립형 클라이언트 및 Day 0 컨피그레이션을 사용하여 ASAv 구축, 15페이지
- OVF 툴과 Day 0 컨피그레이션을 사용하여 ASAv 구축, 16페이지
- ASAv 콘솔 액세스, 17페이지
- vCPU 또는 처리량 라이센스 업그레이드, 19페이지

ASAv에 지원되는 VMware 기능

7페이지의 표 1에서는 ASAv에 대한 VMware 기능 지원을 나열합니다.

표 1 ASAv에 대한 VMware 기능 지원

기능	설명	지원(예/아니요)	코멘트
Cold clone	복제하는 동안 VM의 전원이 꺼집니다.	예	—
DRS	동적 리소스 예약 및 DPM(Distributed Power Management)에 사용됩니다.	예	—
Hot add	추가하는 동안 VM이 실행됩니다.	예	—
Hot clone	복제하는 동안 VM이 실행됩니다.	아니요	—
Hot removal	제거하는 동안 VM이 실행됩니다.	예	—
Snapshot	VM이 몇 초간 중지됩니다.	예	주의해서 사용해야 합니다. 트래픽이 손실될 수 있습니다. 장애 조치가 발생할 수 있습니다.
일시 중지 및 재개	VM이 일시 중지되었다가 재개됩니다.	예	—
vCloud Director	VM의 자동 구축을 허용합니다.	아니요	—
VM 마이그레이션	마이그레이션하는 동안 VM의 전원이 꺼집니다.	예	—
vMotion	VM의 라이브 마이그레이션에 사용됩니다.	예	—
VMware FT	VM의 HA에 사용됩니다.	아니요	ASAv VM 장애에는 ASAv 장애 조치를 사용합니다.
VMware HA	ESX 및 서버 장애에 사용됩니다.	예	ASAv VM 장애에는 ASAv 장애 조치를 사용합니다.

표 1 ASAv에 대한 VMware 기능 지원(계속)

기능	설명	지원(예/아니요)	코멘트
VM 하트비트를 지원하는 VMware HA	VM 장애에 사용됩니다.	아니오	ASAv VM 장애에는 ASAv 장애 조치를 사용합니다.
VMware vSphere 독립 실행형 Windows 클라이언트	VM을 구축하는 데 사용됩니다.	예	—
VMware vSphere Web Client	VM을 구축하는 데 사용됩니다.	예	—

ASAv 및 VMware에 대한 사전 요구 사항

VMware vSphere Web Client, vSphere 독립형 클라이언트 또는 OVF 툴을 사용하여 ASAv를 구축할 수 있습니다. 시스템 요구 사항은 Cisco ASA 호환성을 참조하십시오.

vSphere 표준 스위치에 대한 보안 정책

vSphere 스위치의 경우 계층 2 보안 정책을 수정하고 ASAv 인터페이스에서 사용하는 포트 그룹에 대한 보안 정책 예외를 적용할 수 있습니다. 다음 기본 설정을 확인하십시오.

- Promiscuous Mode(무차별 모드): **Reject(거부)**
- MAC Address Changes(MAC 주소 변경): **Accept(허용)**
- Forged Transmits(위조된 전송): **Accept(허용)**

다음 ASAv 컨피그레이션에 대해 이러한 설정을 수정해야 할 수도 있습니다. 자세한 내용은 vSphere 설명서를 참조하십시오.

표 2 포트 그룹 보안 정책 예외

보안 예외	라우팅 방화벽 모드		투명 방화벽 모드	
	장애 조치 없음	장애 조치	장애 조치 없음	장애 조치
Promiscuous Mode(무차별 모드)	<모두>	<모두>	수락	수락
MAC Address Changes(MAC 주소 변경)	<모두>	수락	<모두>	수락
Forged Transmits(위조된 전송)	<모두>	수락	수락	수락

ASAv 및 VMware에 대한 지침

OVF 파일 지침

asav-vi.ovf 또는 asav-esxi.ovf 파일은 구축 대상에 따라 선택합니다.

- asav-vi—vCenter에서 구축할 경우.
- asav-esxi—ESXi에서 구축할 경우(vCenter 없음)

장애 조치 지침

장애 조치 구축의 경우, 대기 유닛에 동일한 라이센스 모델이 있는지 확인합니다. 예를 들어, 두 유닛 모두 ASAv30s여야 합니다.

IPv6 지침

VMware vSphere Web Client를 사용하여 ASAv OVF 파일을 처음 구축할 때는 관리 인터페이스의 IPv6 주소를 지정할 수 없습니다. 나중에 ASDM 또는 CLI를 사용하여 IPv6 주소를 추가할 수 있습니다.

추가 지침 및 제한

- ASAv OVF 구축은 현지화(영어 이외의 언어 모드로 구성 요소 설치)를 지원하지 않습니다. 사용자 환경의 VMware vCenter와 LDAP 서버가 ASCII 호환 모드로 설치되어 있는지 확인해 주십시오.
- ASAv를 설치하고 VM 콘솔을 사용하려면 먼저 키보드를 영어(미국)로 설정해야 합니다.
- ASAv에 할당된 메모리의 크기는 처리량 레벨에 따라 지정됩니다. 다른 처리량 레벨에 대한 라이센스를 요청할 때를 제외하고 **Edit Settings(설정 수정)** 대화 상자에서 메모리 설정이나 vCPU 하드웨어 설정을 변경하지 마십시오. 부족한 프로비저닝은 성능에 영향을 줄 수 있으며, 과도한 프로비저닝은 ASAv가 다시 로드된다는 경고를 발생시킵니다. 과도한 프로비저닝 시 일정한 대기 시간(100~125%의 경우 24시간, 125% 이상의 경우 1시간) 후 ASAv가 다시 로드됩니다.

  참고: 메모리 또는 vCPU 하드웨어 설정을 변경해야 하는 경우 ASAv에 대한 라이센싱, 5페이지에 나와 있는 값만 사용해야 합니다. VMware 권장 메모리 컨피그레이션 최소값, 기본값, 최대값을 사용하지 마십시오.

  ASAv **show vm** 및 **show cpu** 명령이나 ASDM **Home(홈) > Device Dashboard(디바이스 대시보드) > Device Information(디바이스 정보) > Virtual Resources(가상 리소스)** 탭 또는 **Monitoring(모니터링) > Properties(속성) > System Resources Graphs(시스템 리소스 그래프) > CPU** 창을 사용하여 리소스 할당 및 과도하거나 부족하게 프로비저닝된 모든 리소스를 확인할 수 있습니다.
- 호스트 클러스터가 있는 경우 ASAv를 구축하는 동안 특정 호스트에 로컬로 스토리지를 프로비저닝하거나 공유 호스트에 스토리지를 프로비저닝할 수 있습니다. 그러나 ASAv를 다른 호스트로 vMotion하려는 경우 어떤 종류든 스토리지(SAN 또는 로컬)를 사용하면 연결이 중단됩니다.
- ESXi 5.0을 실행하는 경우 ASAv OVF 구축에 vSphere Web Client가 지원되지 않습니다. vSphere 클라이언트를 사용하십시오.

ASAv 소프트웨어 압축 풀기 및 VMware용 Day 0 컨피그레이션 파일 생성

ASAv를 시작하기 전에 Day 0 컨피그레이션 파일을 준비할 수 있습니다. 이 파일은 ASAv를 시작할 때 적용할 ASAv 컨피그레이션이 포함된 텍스트 파일입니다. 이 초기 컨피그레이션은 사용자가 선택하는 작업 디렉토리의 "day0-config"라는 이름의 텍스트 파일에 위치하며, 이 파일은 최초 부팅 시 마운트되고 읽히는 day0.iso 파일로 조작됩니다. Day 0 컨피그레이션 파일에는 최소한 관리 인터페이스를 활성화하고 공용 키 인증용 SSH 서버를 설정하는 명령이 포함되어야 할 뿐만 아니라, 완전한 ASA 컨피그레이션도 포함되어야 합니다. 빈 day0-config를 포함하는 기본 day0.iso이 이번 릴리스에 제공됩니다. 최초 부팅 동안 day0.iso 파일(사용자 정의 day0.iso 또는 기본 day0.iso)을 사용할 수 있어야 합니다.

참고: 초기 구축 동안 ASAv 라이센스를 자동으로 적용하려면, Cisco Smart Software Manager에서 다운로드한 Smart Licensing ID(Identity) Token을 Day 0 컨피그레이션 파일과 같은 디렉토리에 있는 'idtoken'이라는 이름의 텍스트 파일로 가져옵니다.

참고: 투명 모드에서 ASAv를 구축하려는 경우, 투명 모드에서 실행 중인 알려진 ASA 컨피그레이션 파일을 Day 0 컨피그레이션 파일로 사용해야 합니다. 이 사항은 라우팅 방화벽용 Day 0 컨피그레이션 파일에는 적용되지 않습니다.

참고: 이 예에서는 Linux를 사용하지만 Windows의 경우에도 유사한 유틸리티가 있습니다.

절차

1. Cisco.com에서 ZIP 파일을 다운로드하고 로컬 디스크에 저장합니다.

   http://www.cisco.com/go/asa-software

   참고: Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

2. 작업 디렉터리에 파일의 압축을 풉니다. 이 디렉터리의 어떤 파일도 삭제하지 마십시오. 다음 파일이 포함됩니다.
   - asav-vi.ovf—vCenter 구축용
   - asav-esxi.ovf—비 vCenter 구축용
   - boot.vmdk—부팅 디스크 이미지
   - disk0.vmdk—ASAv 디스크 이미지
   - day0.iso—day0-config 파일과 선택적으로 idtoken 파일을 포함하는 ISO
   - asav-vi.mf—vCenter 구축용 매니페스트 파일
   - asav-esxi.mf—비 vCenter 구축용 매니페스트 파일
3. "day0 config"라는 텍스트 파일에 ASAv에 대한 CLI 컨피그레이션을 입력합니다. 3개의 인터페이스에 대한 인터페이스 컨피그레이션 및 원하는 기타 모든 컨피그레이션을 추가합니다.

   첫 줄은 ASAv 버전으로 시작해야 합니다. day0-config는 유효한 ASA 컨피그레이션이어야 합니다. day0-config를 생성하는 가장 좋은 방법은 기존 ASA 또는 ASAv에서 실행 중인 컨피그레이션 중 원하는 부분을 복사하는 것입니다. day0-config에서 줄의 순서가 중요하며 기존 **show run** 명령 출력의 순서와 일치해야 합니다.

   예:

```
ASA Version 9.5.1
!
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

4. (선택 사항) Cisco Smart Software Manager에서 발급한 Smart License ID 토큰 파일을 PC에 다운로드합니다.
5. (선택 사항) 다운로드 파일에서 ID 토큰을 복사하고 ID 토큰만 포함된 'idtoken'이라는 텍스트 파일에 붙여넣습니다.

   ID 토큰은 ASAv를 Smart Licensing 서버에 자동으로 등록합니다.
6. 텍스트 파일을 ISO 파일로 전환하여 가상 CD-ROM을 생성합니다.

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
```

```
Path table size (bytes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

7. day0.iso를 위해 Linux의 새 SHA1 값을 계산합니다.

   ```
   openssl dgst -sha1 day0.iso
   SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66 day0.iso
   ```

8. 작업 디렉터리의 asav-vi.mf 파일에 새 체크섬을 넣고 day0.iso SHA1 값을 새로 생성된 값으로 대체합니다.

   Example.mf 파일

   ```
   SHA1(asav-vi.ovf)= de0f1878b8f1260e379ef853db4e790c8e92f2b2
   SHA1(disk0.vmdk)= 898b26891cc68fa0c94ebd91532fc450da418b02
   SHA1(boot.vmdk)= 6b0000ddebfc38ccc99ac2d4d5dbfb8abfb3d9c4
   SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
   ```

9. ZIP 파일의 압축을 푼 디렉터리에 day0.iso 파일을 복사합니다. 기본 (비어 있는) day0.iso 파일을 덮어쓸 것입니다.

   이 디렉터리에서 구축되는 VM이 있을 경우 새로 생성된 day0.iso내부의 컨피그레이션이 적용됩니다.

VMware vSphere Web Client를 사용하여 ASAv 구축

이 섹션에서는 VMware vSphere Web Client를 사용하여 ASAv를 구축하는 방법에 대해 설명합니다. Web Client에는 vCenter가 필요합니다. vCenter가 없을 경우 VMware vSphere 독립형 클라이언트 및 Day 0 컨피그레이션을 사용하여 ASAv 구축, 15페이지 또는 OVF 툴과 Day 0 컨피그레이션을 사용하여 ASAv 구축, 16페이지를 참조하십시오.

- vSphere Web Client에 액세스하여 클라이언트 통합 플러그인 설치, 11페이지
- VMware vSphere Web Client를 사용하여 ASAv 구축, 12페이지

vSphere Web Client에 액세스하여 클라이언트 통합 플러그인 설치

이 섹션에서는 vSphere Web Client에 액세스하는 방법에 대해 설명합니다. 또한 ASAv 콘솔에 액세스하는 데 필요한 클라이언트 통합 플러그인을 설치하는 방법에 대해서도 설명합니다. 일부 Web Client 기능(플러그인 포함)은 Macintosh에서 지원되지 않습니다. 전체 클라이언트 지원 정보는 VMware 웹사이트를 참조하십시오.

절차

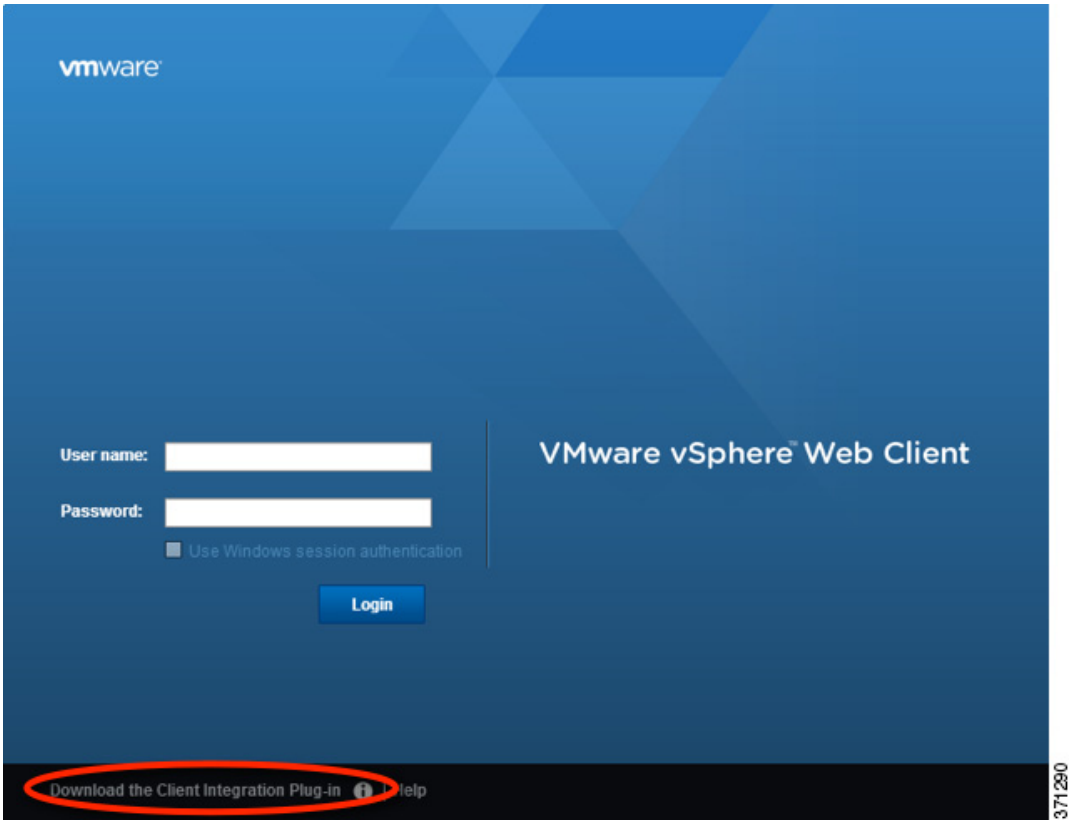
1. 브라우저에서 VMware vSphere Web Client를 실행합니다.

   https://*vCenter_server*:*port*/**vsphere-client/**

   기본적으로 포트는 9443입니다.

2. (한 번만 실행) ASAv 콘솔에 액세스할 수 있도록 클라이언트 통합 플러그인을 설치합니다.

   a. 로그인 화면에서 **Download the Client Integration Plug-in(클라이언트 통합 플러그인 다운로드)**을 클릭하여 플러그인을 다운로드합니다.



b. 브라우저를 닫고 설치 프로그램을 사용하여 플러그인을 설치합니다.

c. 플러그인이 설치되고 나면 vSphere Web Client에 다시 연결합니다.

3. 사용자 이름과 비밀번호를 입력하고 **Login(로그인)**을 클릭하거나, **Use Windows session authentication(Windows 세션 인증 사용)** 확인란(Windows에만 해당)을 선택합니다.

VMware vSphere Web Client를 사용하여 ASAv 구축

ASAv를 구축하려면 VMware vSphere Web Client(또는 vSphere Client)와 OVF(open virtualization format) 형식의 템플릿 파일을 사용합니다. vSphere Web Client에서 Deploy OVF Template(OVF 템플릿 구축) 마법사를 사용하여 ASAv용 Cisco 패키지를 구축할 수 있습니다. 이 마법사에서는 ASAv OVF 파일의 구문을 분석하고 ASAv를 실행할 가상 머신을 만들며 패키지를 설치합니다.

마법사의 단계는 대부분 VMware 표준 단계입니다. Deploy OVF Template(OVF 템플릿 구축)에 대한 자세한 내용은 VMware vSphere Web Client 온라인 도움말을 참조하십시오.

시작하기 전에

ASAv를 구축하기 전에 vSphere에서 하나 이상의 네트워크(관리용)를 구성해야 합니다.

절차

1. Cisco.com에서 ASAv ZIP 파일을 다운로드하여 PC에 저장합니다.

   http://www.cisco.com/go/asa-software

   참고: Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

2. vSphere Web Client **Navigator(탐색기)** 창에서 **vCenter**를 클릭합니다.

3. **Hosts and Clusters(호스트 및 클러스터)**를 클릭합니다.

4. ASAv를 구축할 데이터 센터, 클러스터 또는 호스트를 마우스 오른쪽 버튼으로 클릭하고 **Deploy OVF Template(OVF 템플릿 구축)**을 선택합니다.

   Deploy OVF Template(OVF 템플릿 구축) 마법사가 나타납니다.

5. 마법사 화면의 지시를 따릅니다.

6. **Setup networks(네트워크 설정)** 화면에서 사용하려는 각 ASAv 인터페이스에 네트워크를 매핑합니다.

   네트워크는 사전 순이 아닐 수도 있습니다. 네트워크를 찾기 어려운 경우 나중에 Edit Settings(설정 수정) 대화 상자에서 네트워크를 변경할 수 있습니다. 구축 후 ASAv 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings(설정 수정)**를 선택하면 **Edit Settings(설정 수정)** 대화 상자에 액세스할 수 있습니다. 그러나 ASAv 인터페이스 ID는 이 화면에 표시되지 않습니다(네트워크 어댑터 ID만 표시됨). 네트워크 어댑터 ID에 해당하는 ASAv 인터페이스 ID는 다음 표를 참조하십시오.

네트워크 어댑터 ID	ASAv 인터페이스 ID
네트워크 어댑터 1	Management 0/0
네트워크 어댑터 2	GigabitEthernet0/0
네트워크 어댑터 3	GigabitEthernet0/1
네트워크 어댑터 4	GigabitEthernet0/2
네트워크 어댑터 5	GigabitEthernet0/3
네트워크 어댑터 6	GigabitEthernet0/4
네트워크 어댑터 7	GigabitEthernet0/5
네트워크 어댑터 8	GigabitEthernet0/6
네트워크 어댑터 9	GigabitEthernet0/7
네트워크 어댑터 10	GigabitEthernet0/8

   모든 ASAv 인터페이스를 사용할 필요는 없지만 vSphere Web Client에서는 모든 인터페이스에 네트워크를 할당해야 합니다. 인터페이스를 비활성화된 상태로 두려면 ASAv 컨피그레이션 내에서 해당 인터페이스를 비활성화된 상태로 그대로 두면 됩니다. ASAv를 구축한 후 선택적으로 vSphere Web Client로 돌아가 Edit Settings(설정 수정) 대화 상자에서 추가 인터페이스를 삭제할 수 있습니다. 자세한 내용은 vSphere Web Client 온라인 도움말을 참조하십시오.

   참고: 장애 조치/HA 구축의 경우 GigabitEthernet 0/8이 장애 조치 인터페이스로 사전 구성됩니다.

7. 네트워크에서 인터넷 액세스에 HTTP 프록시를 사용하는 경우 **Smart Call Home Settings(Smart Call Home 설정)** 영역에서 스마트 라이센스를 위한 프록시 주소를 구성해야 합니다. 이 프록시는 Smart Call Home에도 일반적으로 사용됩니다.

8. 장애 조치/HA 구축의 경우 **Customize template(템플릿 사용자 정의)** 화면에서 다음을 수행합니다.

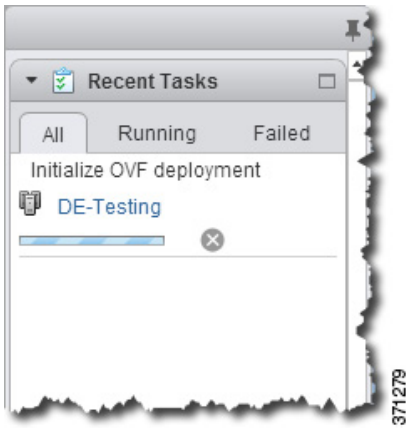
   – 대기 관리 IP 주소를 지정합니다.

     인터페이스를 구성할 때 활성 IP 주소와 대기 IP 주소를 같은 네트워크에 있는 주소로 지정해야 합니다. 기본 유닛 또는 장애 조치 그룹에서 장애 조치를 시작할 경우, 보조 유닛에서는 기본 유닛의 IP 주소와 MAC 주소를 가정하고 트래픽 전달을 시작합니다. 이제 대기 상태가 된 유닛에서는 대기 IP 주소와 MAC 주소를 인수합니다. 네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로 네트워크 어디에서도 ARP 항목의 변경 또는 시간 초과가 발생하지 않습니다.

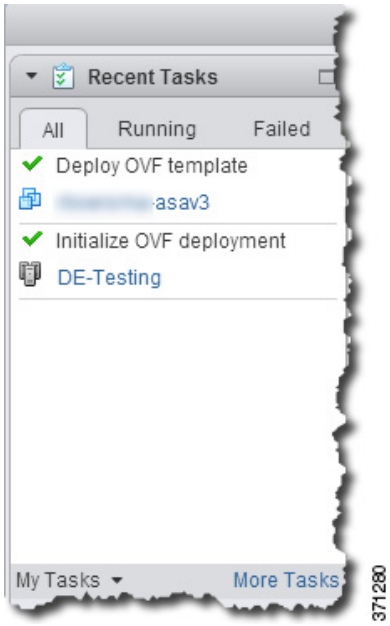
   – **HA Connection Settings(HA 연결 설정)** 영역에서 장애 조치 링크 설정을 구성합니다.

     장애 조치 쌍의 두 유닛은 장애 조치 링크를 통해 지속적으로 통신하여 각 유닛의 작동 상태를 확인합니다. GigabitEthernet 0/8이 장애 조치 링크로 사전 구성됩니다. 링크의 활성 및 대기 IP 주소를 같은 네트워크에 있는 주소로 입력합니다.

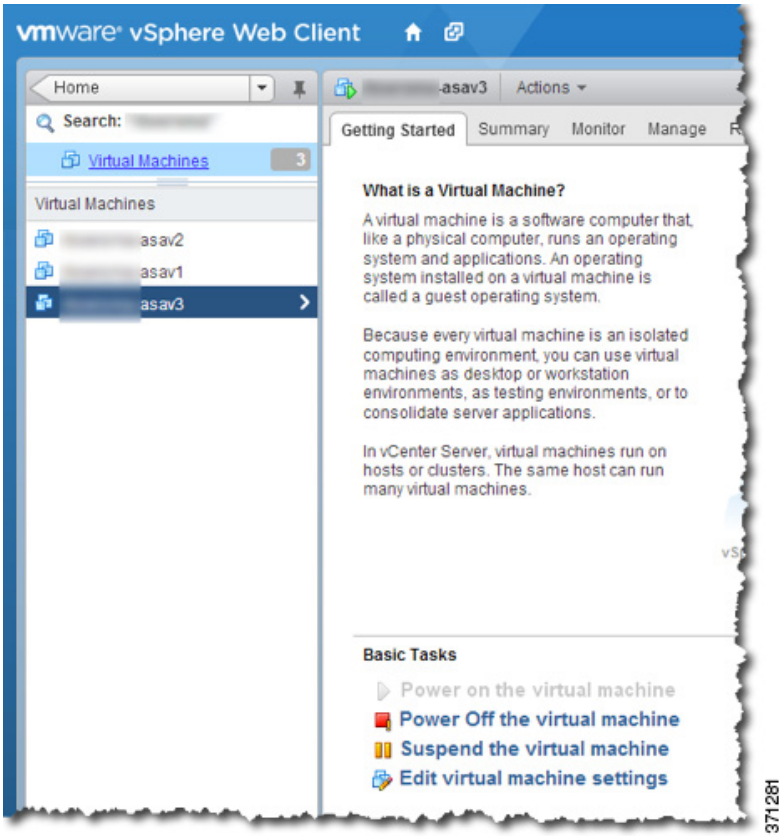
9. 마법사를 완료하면 vSphere Web Client에서 VM을 처리합니다. **Recent Tasks(최근 작업)** 창의 **Global Information(전체 정보)** 영역에서 "Initialize OVF deployment(OVF 구축 초기화)" 상태를 볼 수 있습니다.



작업이 완료되면 Deploy OVF Template(OVF 템플릿 구축) 완료 상태가 표시됩니다.



그런 다음 인벤토리의 지정된 데이터 센터 아래에 ASAv VM 인스턴스가 표시됩니다.



10. ASAv VM을 아직 실행하지 않은 경우 **Power on the virtual machine(가상 머신 전원 켜기)**을 클릭합니다.

    ASAv가 부팅될 때까지 기다렸다가 ASDM 또는 콘솔에 연결합니다. ASAv는 처음 시작될 때 OVF 파일을 통해 제공된 매개변수를 읽어 ASAv 시스템 컨피그레이션에 추가합니다. 그런 다음 가동 및 실행될 때까지 자동으로 부팅을 다시 시작합니다. 이러한 이중 부팅은 ASAv를 처음 구축한 경우에만 발생합니다. 부팅 메시지를 보려면 **Console(콘솔)** 탭을 클릭하여 ASAv 콘솔에 액세스합니다.

11. 장애 조치/HA 구축의 경우 이 절차를 반복하여 보조 유닛을 추가합니다. 다음 지침을 참조하십시오.

    - 기본 유닛과 동일한 처리량 레벨을 설정합니다.
    - 기본 유닛에 *정확히 동일한 IP 주소 설정*을 입력합니다. 두 유닛의 부트스트랩 컨피그레이션은 유닛을 기본 유닛 또는 보조 유닛으로 식별하는 매개변수를 제외하고 동일합니다.

참고: ASAv를 Cisco Licensing Authority에 성공적으로 등록하려면 ASAv에 인터넷 액세스가 필요합니다. 인터넷 액세스 및 성공적인 라이센스 등록을 위해 구축 이후에 추가 컨피그레이션을 수행해야 할 수도 있습니다.

VMware vSphere 독립형 클라이언트 및 Day 0 컨피그레이션을 사용하여 ASAv 구축

ASAv를 구축하려면 Mware vSphere Client 및 OVF(open virtualization format) 템플릿 파일(vCenter 구축은 asav-vi.ovf, 비 vCenter 구축에서는 asav-esxi.ovf)을 사용합니다. vSphere Client에서 Deploy OVF Template(OVF 템플릿 구축) 마법사를 사용하여 ASAv용 Cisco 패키지를 구축할 수 있습니다. 이 마법사에서는 ASAv OVF 파일의 구문을 분석하고 ASAv를 실행할 가상 머신을 만들며 패키지를 설치합니다.

마법사의 단계는 대부분 VMware 표준 단계입니다. Deploy OVF Template(OVF 템플릿 구축) 마법사에 대한 자세한 내용은 VMware vSphere Web Client 온라인 도움말을 참조하십시오.

시작하기 전에

- ASAv를 구축하기 전에 vSphere에서 하나 이상의 네트워크(관리용)를 구성해야 합니다.
- ASAv 소프트웨어 압축 풀기 및 VMware용 Day 0 컨피그레이션 파일 생성, 9페이지의 단계에 따라 Day 0 컨피그레이션을 생성합니다.

절차

1. VMware vSphere Client를 실행하고 **File(파일) > Deploy OVF Template(OVF 템플릿 구축)**을 선택합니다.

   Deploy OVF Template(OVF 템플릿 구축) 마법사가 나타납니다.

2. asav-vi.ovf 파일의 압축을 푼 작업 디렉터리로 이동하여 이 파일을 선택합니다.

3. OVF 템플릿 세부 정보가 표시됩니다. 다음 화면을 진행합니다. Day 0 컨피그레이션 파일을 사용하려는 경우 어떤 컨피그레이션도 변경할 필요 없습니다.

4. 구축 설정의 요약이 마지막 화면에 표시됩니다. **Finish(마침)**를 클릭하여 VM을 구축합니다.

5. ASAv를 켜고 VMware 콘솔을 열고 2번째 부팅을 기다립니다.

6. ASA에 SSH를 적용하고 원하는 컨피그레이션을 완료합니다. 원하는 컨피그레이션 중 일부가 Day 0 컨피그레이션 파일에 빠졌을 경우 VMware 콘솔을 열고 필요한 컨피그레이션을 완료합니다.

   이제 ASAv는 정상적으로 작동합니다.

OVF 툴과 Day 0 컨피그레이션을 사용하여 ASAv 구축

시작하기 전에

- OVF 툴을 사용하여 ASAv를 구축할 경우 day0.iso 파일이 필요합니다. ZIP 파일에 제공된 비어 있는 기본 day0.iso 파일을 사용하거나 맞춤형 Day 0 컨피그레이션 파일을 생성하여 사용할 수 있습니다. Day 0 컨피그레이션 생성에 대해서는 ASAv 소프트웨어 압축 풀기 및 VMware용 Day 0 컨피그레이션 파일 생성, 9페이지를 참조하십시오.
- OVF 툴이 Linux 또는 Windows PC에 설치되어 있고 대상 ESXi 또는 vCenter 서버와 연결되어 있어야 합니다.

절차

1. OVF 툴이 설치되어 있음을 확인합니다.

   ```
   linuxprompt# which ovftool
   ```

2. 원하는 구축 옵션으로 .cmd 파일을 생성합니다.

   예:

   ```
   linuxprompt# cat launch.cmd
   ovftool \
   --name="asav-941-demo" \
   --powerOn \
   --deploymentOption=ASAv30 \
   --diskMode=thin \
   --datastore=datastore1 \
   --acceptAllEulas \
   --net:Management0-0="Portgroup_Mgmt" \
   --net:GigabitEthernet0-1="Portgroup_Inside" \
   --net:GigabitEthernet0-0="Portgroup_Outside" \
   --prop:HARole=Standalone \
   asav-esxi.ovf \
   vi://root@10.1.2.3/
   ```

3. cmd 파일을 실행합니다.

   ```
   linuxprompt# ./launch.cmd
   ```

   ASAv가 켜집니다. 2번째 부팅을 기다립니다.

4. ASA에 SSH를 적용하여 원하는 컨피그레이션을 완료합니다. 추가 컨피그레이션이 필요할 경우 ASAv에 대한 VMware 콘솔을 열고 필요한 컨피그레이션을 적용합니다.

   이제 ASAv는 정상적으로 작동합니다.

ASAv 콘솔 액세스

ASDM을 사용할 때 경우에 따라 문제 해결에 CLI를 사용해야 할 수 있습니다. 기본적으로 내장형 VMware vSphere 콘솔에 액세스할 수 있습니다. 또는 복사 및 붙여넣기를 포함하여 더 나은 기능을 갖춘 네트워크 직렬 콘솔을 구성할 수 있습니다.

- VMware vSphere 콘솔 사용, 17페이지
- 네트워크 직렬 콘솔 포트 구성, 18페이지

VMware vSphere 콘솔 사용

초기 컨피그레이션 또는 문제 해결의 경우 VMware vSphere Web Client를 통해 제공된 가상 콘솔에서 CLI에 액세스합니다. 나중에 텔넷(Telnet) 또는 SSH에 대해 CLI 원격 액세스를 구성할 수 있습니다.

시작하기 전에

vSphere Web Client의 경우 ASAv 콘솔에 액세스하는 데 필요한 클라이언트 통합 플러그인을 설치합니다.

절차

1. VMware vSphere Web Client의 인벤토리에서 ASAv 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Open Console(콘솔 열기)**을 선택합니다. 또는 **Summary(요약)** 탭에서 **Launch Console(콘솔 실행)**을 클릭합니다.

2. 콘솔을 클릭하고 **Enter** 키를 누릅니다. 참고: 커서를 놓으려면 **Ctrl+Alt**를 누릅니다.

   ASAv가 여전히 시작 중인 경우 부팅 메시지가 나타납니다.

   ASAv는 처음 시작될 때 OVF 파일을 통해 제공된 매개변수를 읽어 ASAv 시스템 컨피그레이션에 추가합니다. 그런 다음 가동 및 실행될 때까지 자동으로 부팅을 다시 시작합니다. 이러한 이중 부팅은 ASAv를 처음 구축한 경우에만 발생합니다.

   참고: 라이센스를 설치할 때까지 예비 연결 테스트를 수행할 수 있도록 처리량이 100Kbps로 제한됩니다. 라이센스는 일반적인 운영에 필요합니다. 또한 라이센스를 설치할 때까지 콘솔에 다음 메시지가 반복적으로 표시됩니다.

   ```
   Warning: ASAv platform license state is Unlicensed.
   Install ASAv platform license for full functionality.
   ```

   다음 프롬프트가 표시됩니다.

   ```
   ciscoasa>
   ```

   이 프롬프트는 현재 사용자 EXEC 모드에 있음을 의미합니다. 사용자 EXEC 모드에서는 기본 명령만 사용 가능합니다.

3. 특권 실행 모드에 액세스합니다.

   ```
   ciscoasa> enable
   ```

   다음 프롬프트가 나타납니다.

   ```
   Password:
   ```

4. **Enter** 키를 눌러 계속합니다. 기본적으로 비밀번호는 비어 있습니다. 이전에 enable 비밀번호를 설정한 경우 Enter 키를 누르는 대신 enable을 입력합니다.

   프롬프트가 다음으로 변경됩니다.

   ```
   ciscoasa#
   ```

   모든 비 구성 명령은 특권 EXEC 모드에서 사용할 수 있습니다. 또한 특권 EXEC 모드에서 구성 모드를 입력할 수도 있습니다.

   특권 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

5. 전역 컨피그레이션 모드에 액세스합니다.

   ```
   ciscoasa# configure terminal
   ```

   프롬프트가 다음으로 변경됩니다.

   ```
   ciscoasa(config)#
   ```

   전역 구성 모드에서 ASAv 구성을 시작할 수 있습니다. 전역 구성 모드를 종료하려면 **exit**, **quit** 또는 **end** 명령을 입력합니다.

네트워크 직렬 콘솔 포트 구성

더 나은 콘솔 경험을 위해 콘솔에 액세스할 수 있는 네트워크 직렬 포트를 단독으로 구성하거나 vSPC(Virtual Serial Port Concentrator)에 연결하여 구성할 수 있습니다. 각 방법에 대한 자세한 내용은 VMware vSphere 설명서를 참조하십시오. ASAv에서 가상 콘솔 대신 직렬 포트로 콘솔 출력을 보내야 합니다. 이 섹션에서는 직렬 포트 콘솔을 사용하는 방법에 대해 설명합니다.

절차

1. VMware vSphere에서 네트워크 직렬 포트를 구성합니다. VMware vSphere 설명서를 참조하십시오.
2. ASAv에서 disk0의 루트 디렉토리에 "use_ttyS0"이라는 파일을 만듭니다. 파일 내용은 없어도 됩니다. 이 위치에 파일이 있기만 하면 됩니다.

   disk0:/use_ttyS0

   - ASDM에서 **Tools(툴) > File Management(파일 관리)** 대화 상자를 사용하여 이 이름으로 빈 텍스트 파일을 업로드할 수 있습니다.
   - vSphere 콘솔에서 파일 시스템에 있는 기존 파일(임의의 파일)을 새 이름으로 복사할 수 있습니다. 예를 들면 다음과 같습니다.

     ```
     ciscoasa(config)# cd coredumpinfo
     ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
     ```

3. ASAv를 다시 로드합니다.

   - ASDM에서 **Tools(툴) > System Reload(시스템 다시 로드)**를 선택합니다.
   - vSphere 콘솔에서 **reload(다시 로드)**를 입력합니다.

   ASAv에서 vSphere 콘솔로 보내는 것을 중지하고 대신 직렬 콘솔로 보냅니다.

4. 직렬 포트를 추가할 때 지정한 vSphere 호스트 IP 주소와 포트 번호로 텔넷 전송하거나, vSPC IP 주소 및 포트로 텔넷 전송합니다.

vCPU 또는 처리량 라이센스 업그레이드

ASAv에서는 처리량 라이센스를 사용합니다. 이는 사용 가능한 vCPU 수에 영향을 미칩니다.

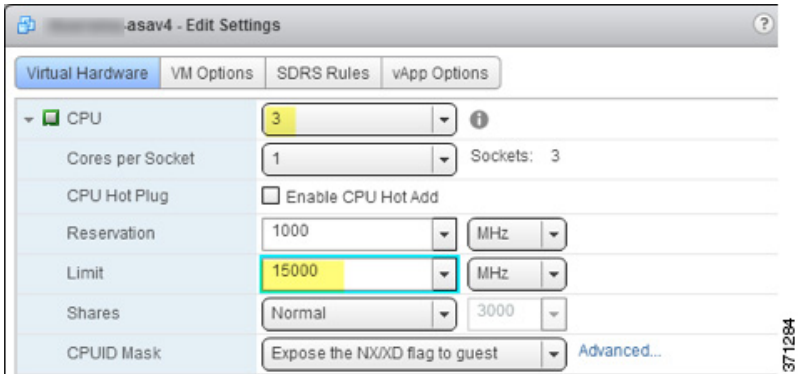
ASAv에 대한 vCPU 수를 늘리거나 줄이려면 새 라이센스를 요청하고 이를 적용한 후 VMware에서 VM 속성을 새 값과 일치하도록 변경하면 됩니다.

참고: 지정된 vCPU가 ASAv 가상 CPU 라이센스 또는 처리량 라이센스와 일치해야 합니다. RAM도 vCPU에 맞게 크기가 지정되어야 합니다. 업그레이드하거나 다운그레이드할 때 다음 절차에 따라 라이센스 및 vCPU를 즉시 조정하십시오. 일치하지 않은 항목이 있으면 ASAv가 제대로 작동하지 않습니다.

절차

1. 새 라이센스를 요청합니다.
2. 새 라이센스를 적용합니다. 장애 조치 쌍의 경우 두 유닛 모두에 새 라이센스를 적용합니다.
3. 장애 조치를 사용하는지 여부에 따라 다음 중 하나를 수행합니다.
   - 장애 조치를 사용하는 경우 - vSphere Web Client에서 *standby(대기)* ASAv의 전원을 끕니다. 예를 들어 ASAv를 클릭한 다음 **Power Off the virtual machine(가상 머신 전원 끄기)**를 클릭하거나, ASAv를 마우스 오른쪽 버튼으로 클릭하고 **Shut Down Guest OS(게스트 OS 종료)**를 선택합니다.
   - 장애 조치를 사용하지 않는 경우 - vSphere Web Client에서 ASAv의 전원을 끕니다. 예를 들어 ASAv를 클릭한 다음 **Power Off the virtual machine(가상 머신 전원 끄기)**를 클릭하거나, ASAv를 마우스 오른쪽 버튼으로 클릭하고 **Shut Down Guest OS(게스트 OS 종료)**를 선택합니다.
4. ASAv를 클릭한 다음 **Edit Virtual machine settings(가상 머신 설정 수정)**를 클릭하거나, ASAv를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings(설정 수정)**를 선택합니다.

   Edit Settings(설정 수정) 대화 상자가 나타납니다.
5. ASAv에 대한 라이센싱, 5페이지에서 CPU 메모리 요구 사항을 참조하여 새 vCPU 라이센스에 대한 올바른 값을 확인합니다.
6. **Virtual Hardware(가상 하드웨어)** 탭의 **CPU** 드롭다운 목록에서 새 값을 선택합니다.



7. **Memory(메모리)**에 RAM에 대한 새 값을 입력합니다.
8. **OK(확인)**를 클릭합니다.
9. ASAv의 전원을 켭니다. 예를 들어 **Power On the Virtual Machine(가상 머신 전원 켜기)**을 클릭합니다.

10. 장애 조치 쌍의 경우 다음을 수행합니다.

    a. 활성 유닛에 대한 콘솔을 열거나, 활성 유닛에서 ASDM을 실행합니다.

    b. 대기 유닛의 시작이 완료되면 대기 유닛에 장애 조치를 수행합니다.

    - ASDM: **Monitoring(모니터링) > Properties(속성) > Failover(장애 조치) > Status(상태)**를 선택하고 **Make Standby(대기로 전환)**를 클릭합니다.

    - CLI: ciscoasa**# failover active**

    c. 활성 유닛에 대해 3~9단계를 반복합니다.

관련 주제

- ASAv에 대한 라이센싱, 5페이지

KVM을 사용하여 ASAv 구축

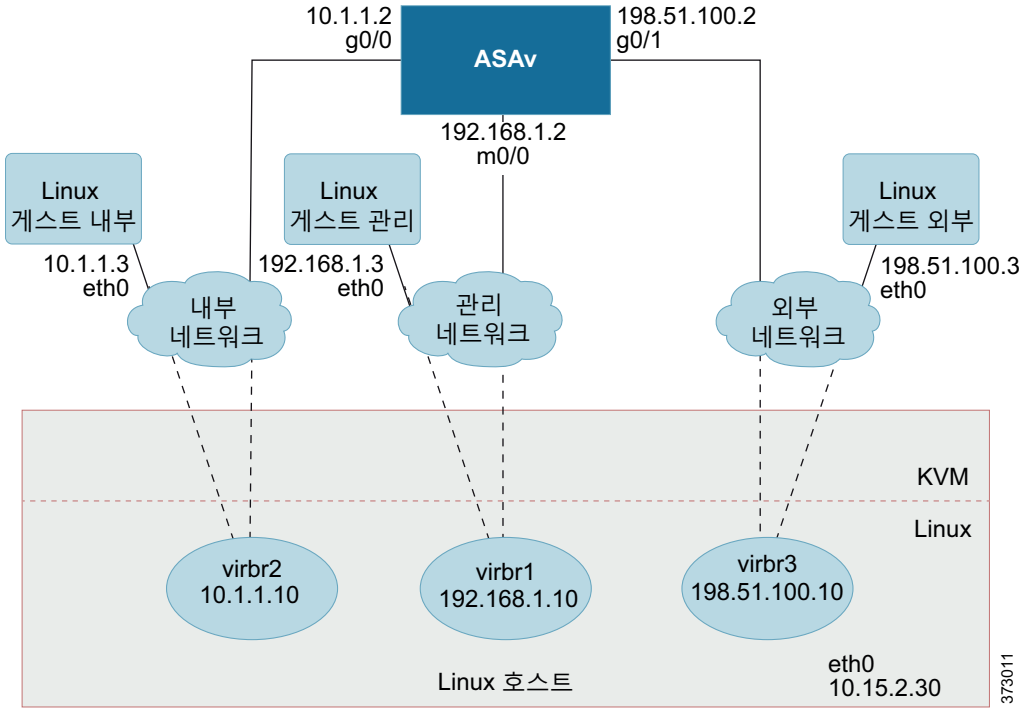
KVM(Kernel-based Virtual Machine)을 사용하여 ASAv를 구축할 수 있습니다.

- KVM을 사용한 ASAv 구축 정보, 21페이지
- ASAv 및 KVM에 대한 사전 요구 사항, 22페이지
- Day 0 컨피그레이션 파일 준비, 22페이지
- 가상 브리지 XML 파일 준비, 24페이지
- ASAv 시작, 25페이지

KVM을 사용한 ASAv 구축 정보

21페이지의 그림 1에는 ASAv 및 KVM이 있는 샘플 네트워크 토폴로지가 나와 있습니다. 이 장에 설명된 절차는 샘플 토폴로지를 기반으로 합니다. 사용자 요건은 사용자가 필요로 하는 정확한 절차에 영향을 미칩니다. ASAv는 내부 및 외부 네트워크 사이의 방화벽으로 작동합니다. 별도의 관리 네트워크도 구성됩니다.

그림 1 KVM을 사용하여 샘플 ASAv 구축



ASAv 및 KVM에 대한 사전 요구 사항

- Cisco.com에서 ASAv qcow2 파일을 다운로드하고 이를 Linux 호스트에 넣습니다.

  http://www.cisco.com/go/asa-software

  참고: Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

- 이 문서에 나와 있는 샘플 구축의 경우, 사용자가 Ubuntu 14.04 LTS를 사용 중인 것으로 가정합니다. Ubuntu 14.04 LTS 호스트의 상위에 다음 패키지를 설치합니다.
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- 성능은 호스트 및 해당 컨피그레이션에 영향을 받습니다. 호스트를 조정하여 KVM에서 ASAv의 처리량을 극대화할 수 있습니다. 일반적인 호스트 조정 개념에 대한 내용은 Linux 및 Intel 아키텍처를 활용한 가상화 플랫폼의 네트워크 기능 가상화 패킷 처리 성능을 참조해 주십시오.
- Ubuntu 14.04에 유용한 최적화는 다음과 같습니다.
  - macvtap - 고성능 Linux 브리지로, Linux 브리지 대신 macvtap을 사용할 수 있습니다. Linux 브리지 대신 macvtap을 사용하려면 특정 설정을 구성해야 합니다.
  - Transparent Huge Pages - 메모리 페이지 크기를 늘리며 Ubuntu 14.04에서 기본적으로 설정됩니다.
  - Hyperthread 비활성화 - 두 개의 vCPU를 단일 코어로 줄입니다.
  - txqueuelength - 기본 txqueuelength를 4000 패킷으로 늘이고 삭제율을 줄입니다.
  - 고정 - qemu 및 vhost 프로세스를 특정 CPU 코어에 고정합니다. 특정 조건에서 고정 기능을 사용하면 성능이 대폭 향상됩니다.
- RHEL 기반 배포에 대한 자세한 내용은 Red Hat Enterprise Linux6 가상화 조정 및 최적화 가이드를 참조해 주십시오.
- KVM 시스템 요구 사항은 Cisco ASA 호환성을 참조하십시오.

Day 0 컨피그레이션 파일 준비

ASAv를 시작하기 전에 Day 0 컨피그레이션 파일을 준비할 수 있습니다. 이 파일은 ASAv를 시작할 때 적용할 ASAv 컨피그레이션이 포함된 텍스트 파일입니다. 이 초기 컨피그레이션은 사용자가 선택하는 작업 디렉토리의 "day0-config"라는 이름의 텍스트 파일에 위치하며, 이 파일은 최초 부팅 시 마운트되고 읽히는 day0.iso 파일로 조작됩니다. Day 0 컨피그레이션 파일에는 최소한 관리 인터페이스를 활성화하고 공용 키 인증용 SSH 서버를 설정하는 명령이 포함되어야 할 뿐만 아니라, 완전한 ASA 컨피그레이션도 포함되어야 합니다. 최초 부팅 동안 day0.iso 파일(사용자 정의 day0.iso 또는 기본 day0.iso)을 사용할 수 있어야 합니다.

참고: 초기 구축 동안 ASAv 라이센스를 자동으로 적용하려면, Cisco Smart Software Manager에서 다운로드한 Smart Licensing ID(Identity) Token을 Day 0 컨피그레이션 파일과 같은 디렉토리에 있는 'idtoken'이라는 이름의 텍스트 파일로 가져옵니다.

참고: 투명 모드에서 ASAv를 구축하려는 경우, 투명 모드에서 실행 중인 알려진 ASA 컨피그레이션 파일을 Day 0 컨피그레이션 파일로 사용해야 합니다. 이 사항은 라우팅 방화벽용 Day 0 컨피그레이션 파일에는 적용되지 않습니다.

참고: 이 예에서는 Linux를 사용하지만 Windows의 경우에도 유사한 유틸리티가 있습니다.

절차

1. "day0 config"라는 텍스트 파일에 ASAv에 대한 CLI 컨피그레이션을 입력합니다. 3개의 인터페이스에 대한 인터페이스 컨피그레이션 및 원하는 기타 모든 컨피그레이션을 추가합니다.

   첫 줄은 ASAv 버전으로 시작해야 합니다. day0-config는 유효한 ASA 컨피그레이션이어야 합니다. day0-config를 생성하는 가장 좋은 방법은 기존 ASA 또는 ASAv에서 실행 중인 컨피그레이션 중 원하는 부분을 복사하는 것입니다. day0-config에서 줄의 순서가 중요하며 기존 **show run** 명령 출력의 순서와 일치해야 합니다.

   예:

   ```
   ASA Version 9.5.1
   !
   interface management0/0
      nameif management
      security-level 100
      ip address 192.168.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/0
      nameif inside
      security-level 100
      ip address 10.1.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/1
      nameif outside
      security-level 0
      ip address 198.51.100.2 255.255.255.0
      no shutdown
   http server enable
   http 192.168.1.0 255.255.255.0 management
   crypto key generate rsa modulus 1024
   username AdminUser password paSSw0rd
   ssh 192.168.1.0 255.255.255.0 management
   aaa authentication ssh console LOCAL
   ```

2. (선택 사항) Cisco Smart Software Manager에서 발급한 스마트 라이센스 ID 토큰 파일을 컴퓨터에 다운로드합니다.

3. (선택 사항) 다운로드 파일에서 ID 토큰을 복사하고 ID 토큰만 포함된 'idtoken'이라는 텍스트 파일에 붙여넣습니다.

4. (선택 사항) 초기 ASAv 구축 동안 라이센싱이 자동으로 이루어진 경우, day0-config 파일에 다음 정보가 포함되어 있는지 확인합니다.

   - 관리 인터페이스 IP 주소
   - (선택 사항) Smart Licensing에 사용할 HTTP 프록시
   - HTTP 프록시(지정된 경우) 또는 tools.cisco.com에 대한 연결을 지원하는 **route** 명령
   - tools.cisco.com을 IP 주소에 확인하는 DNS 서버
   - 사용자가 요청하는 ASAv 라이센스를 지정하는 Smart Licensing 컨피그레이션
   - (선택 사항) ASAv가 CSSM에서 검색을 더욱 쉽게 수행할 수 있도록 하는 고유한 호스트 이름

5. 텍스트 파일을 ISO 파일로 전환하여 가상 CD-ROM을 생성합니다.

   ```
   stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
   I: input-charset not specified, using utf-8 (detected in locale settings)
   Total translation table size: 0
   Total rockridge attributes bytes: 252
   Total directory bytes: 0
   Path table size (byptes): 10
   Max brk space used 0
   176 extents written (0 MB)
   stack@user-ubuntu:-/KvmAsa$
   ```

ID 토큰은 ASAv를 Smart Licensing 서버에 자동으로 등록합니다.

6. 1단계~5단계를 반복하여 구축하려는 각 ASAv에 대해 적절한 IP 주소가 포함된 별도의 기본 컨피그레이션 파일을 만듭니다.

가상 브리지 XML 파일 준비

ASAv 게스트를 KVM 호스트에 연결하고 게스트를 서로 연결하는 가상 네트워크를 설정해야 합니다.

참고: 이 절차는 KVM 호스트 밖의 외부 환경에 대한 연결을 설정하지 않습니다.

KVM 호스트에서 가상 브리지 XML 파일을 준비합니다. Day 0 컨피그레이션 파일 준비, 22페이지에 설명된 샘플 가상 네트워크 토폴로지 경우, virbr1.xml, virbr2.xml, virbr3.xml이라는 3개의 가상 브리지 파일이 필요합니다(이러한 3개의 파일 이름을 사용해야 함. 예를 들어, virbr0은 이미 존재하므로 사용할 수 없음). 각 파일에는 가상 브리지를 설정하는 데 필요한 정보가 포함되어 있습니다. 가상 브리지에 이름과 고유한 MAC 주소를 제공해야 합니다. IP 주소를 제공하는 것은 선택 사항입니다.

절차

1. 3개의 가상 네트워크 브리지 XML 파일을 만듭니다.

   virbr1.xml:

   ```
   <network>
     <name>virbr1</name>
     <bridge name='virbr1' stp='on' delay='0' />
     <mac address='52:54:00:05:6e:00' />
     <ip address='192.168.1.10' netmask='255.255.255.0' />
   </network>
   ```

   virbr2.xml:

   ```
   <network>
     <name>virbr2</name>
     <bridge name='virbr2' stp='on' delay='0' />
     <mac address='52:54:00:05:6e:01' />
     <ip address='10.1.1.10' netmask='255.255.255.0' />
   </network>
   ```

   virbr3.xml:

   ```
   <network>
     <name>virbr3</name>
     <bridge name='virbr3' stp='on' delay='0' />
     <mac address='52:54:00:05:6e:02' />
     <ip address='198.51.100.10' netmask='255.255.255.0' />
   </network>
   ```

2. 다음 정보가 포함된 스크립트를 만듭니다(이 예에서는 스크립트 이름을 virt_network_setup.sh로 지정함).

   ```
   virsh net-create virbr1.xml
   virsh net-create virbr2.xml
   virsh net-create virbr3.xml
   ```

3. 이 스크립트를 실행하여 가상 네트워크를 설정합니다. 스크립트는 가상 네트워크를 불러옵니다. 네트워크는 KVM 호스트가 실행되는 동안 계속 가동됩니다.

   ```
   stack@user-ubuntu:-/KvmAsa$ virt_network_setup.sh
   ```

   참고: Linux 호스트를 다시 로드할 경우, virt_network_setup.sh 스크립트를 다시 실행해야 합니다. 재부팅되면 스크립트가 지속되지 않습니다.

4. 가상 네트워크가 만들어졌는지 확인합니다.

```
stack@user-ubuntu:-/KvmAsa$ brctl show
bridge name     bridge id               STP enabled     Interfaces
virbr0          8000.0000000000000      yes
virbr1          8000.5254000056eed      yes             virb1-nic
virbr2          8000.5254000056eee      yes             virb2-nic
virbr3          8000.5254000056eec      yes             virb3-nic
stack@user-ubuntu:-/KvmAsa$
```

5. virbr1 브리지에 할당된 IP 주소가 표시됩니다. 이는 XML 파일에 할당한 IP 주소입니다.

```
stack@user-ubuntu:-/KvmAsa$ ip address show virbr1
S: virbr1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 52:54:00:05:6e:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global virbr1
      valid_lft forever preferred_lft forever
```

ASAv 시작

virt-install 기반 구축 스크립트를 사용하여 ASAv를 시작합니다.

절차

1. "virt_install_asav.sh"라는 virt-install 스크립트를 만듭니다.

   ASAv VM의 이름은 이 KVM 호스트의 모든 기타 VM(Virtual Machines)을 통틀어 고유해야 합니다. ASAv는 최대 10개의 네트워크를 지원할 수 있습니다. 이 예에서는 3개의 네트워크를 사용합니다. 네트워크 브리지 절의 순서가 중요합니다. 첫 번째 줄의 항목은 항상 ASAv의 관리 인터페이스(Management 0/0)이고, 두 번째 줄의 항목은 ASAv의 GigabitEthernet 0/0이며, 세 번째 줄의 항목은 ASAv의 GigabitEthernet 0/1이고 이런 식으로 GigabitEthernet0/8까지 이어집니다. 가상 NIC는 Virtio여야 합니다.

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=asav \
   --cpu host \
   --arch=x86_64 \
   --machine=pc-1.0 \
   --vcpus=1 \
   --ram=2048 \
   --os-type=linux \
   --os-variant=generic26 \
   --noacpi \
   --virt-type=kvm \
   --import \
   --disk path=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=ide,cache=none \
   --disk path=/home/kvmperf/asav_day0.iso,format=iso,device=cdrom \
   --console pty,target_type=virtio \
   --serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

2. virt_install 스크립트를 실행합니다.

```
stack@user-ubuntu:-/KvmAsa$ ./virt_install_asav.sh

Starting install...
Creating domain...
```

   VM의 콘솔을 표시하는 창이 나타납니다. VM이 부팅 중인 것으로 표시됩니다. VM이 부팅될 때까지 몇 분 정도 소요됩니다. VM이 부팅을 멈추면 콘솔 화면에서 CLI 명령을 발급할 수 있습니다.

AWS 클라우드에 ASAv 구축

AWS(Amazon Web Sources) 클라우드에 ASAv를 구축할 수 있습니다.

- AWS 클라우드에 ASAv 구축 정보, 27페이지
- ASAv 및 AWS 사전 요구 사항, 27페이지
- ASAv 및 AWS에 대한 지침과 제한, 28페이지
- AWS 기반 ASAv의 샘플 네트워크 토폴로지, 29페이지
- AWS에 ASAv 구축, 29페이지

AWS 클라우드에 ASAv 구축 정보

참고: ASAv5는 AWS에서 지원되지 않습니다.

AWS는 프라이빗 Xen Hypervisor를 사용하는 퍼블릭 클라우드 환경입니다. ASAv는 Xen Hypervisor의 AWS 환경에서 게스트로 실행됩니다. AWS에서 ASAv는 다음 인스턴스 유형을 지원합니다.

- C3.large—2개의 vCPU, 3.75GB, 2개의 인터페이스, 1개의 관리 인터페이스

  참고: ASAv10 및 ASAv30 모두 c3.large에서 지원되지만 c3.large에서 ASAv30을 사용하는 것은 프로비저닝 부족 때문에 권장하지 않습니다.

- c3.xlarge—4개의 vCPU, 7.5GB, 3개의 인터페이스, 1개의 관리 인터페이스

  참고: ASAv30만 c3.xlarge에서 지원됩니다.

참고: 이 ASAv는 AWs 환경이 아닌 곳에서 Xen Hypervisor를 지원하지 않습니다.

AWS에서 계정을 생성하고, AWS 마법사를 사용하여 ASAv를 설정하고, AMI(Amazon Machine Image)를 선택합니다. AMI는 인스턴스 실행에 필요한 소프트웨어 컨피그레이션을 포함한 템플릿입니다.

참고: AMI 이미지는 AWS 환경이 아닌 곳에서 다운로드할 수 없습니다.

ASAv 및 AWS 사전 요구 사항

- aws.amazon.com에서 계정을 생성합니다.
- ASAv 라이센스를 적용합니다. ASAv 라이센스를 적용할 때까지 저성능 모드에서 실행됩니다. 이 모드에서는 100개의 연결 및 100Kbps의 성능만 허용됩니다. ASAv 스마트 소프트웨어 라이센싱을 참조하십시오.
- 인터페이스 요건:
  - 관리 인터페이스
  - 내부 및 외부 인터페이스
  - (선택 사항) 추가 서브넷(DNZ)

- 커뮤니케이션 경로:
  - 관리 인터페이스—ASAv를 ASDM에 연결할 때 사용합니다. 통과 트래픽에는 사용할 수 없습니다.
  - 내부 인터페이스(필수)—ASAv를 내부 호스트에 연결하는 데 사용합니다.
  - 외부 인터페이스(필수)—ASAv를 공용 네트워크에 연결하는 데 사용합니다.
  - DMZ 인터페이스(선택 사항)—c3.xlarge 인터페이스 사용 시 ASAv를 DMZ 네트워크에 연결하는 데 사용합니다.
- ASAv 시스템 요건은 Cisco ASA 호환성을 참조하십시오.

ASAv 및 AWS에 대한 지침과 제한

지원 기능

- VPC(Virtual Private Cloud)에 구축
- 확장 네트워킹(SR-IOV) - 사용 가능한 경우
- Amazon Marketplace에서 구축
- 인스턴스당 최대 4개의 vCPU
- L3 네트워크의 사용자 구축
- 라우팅 모드(기본값)

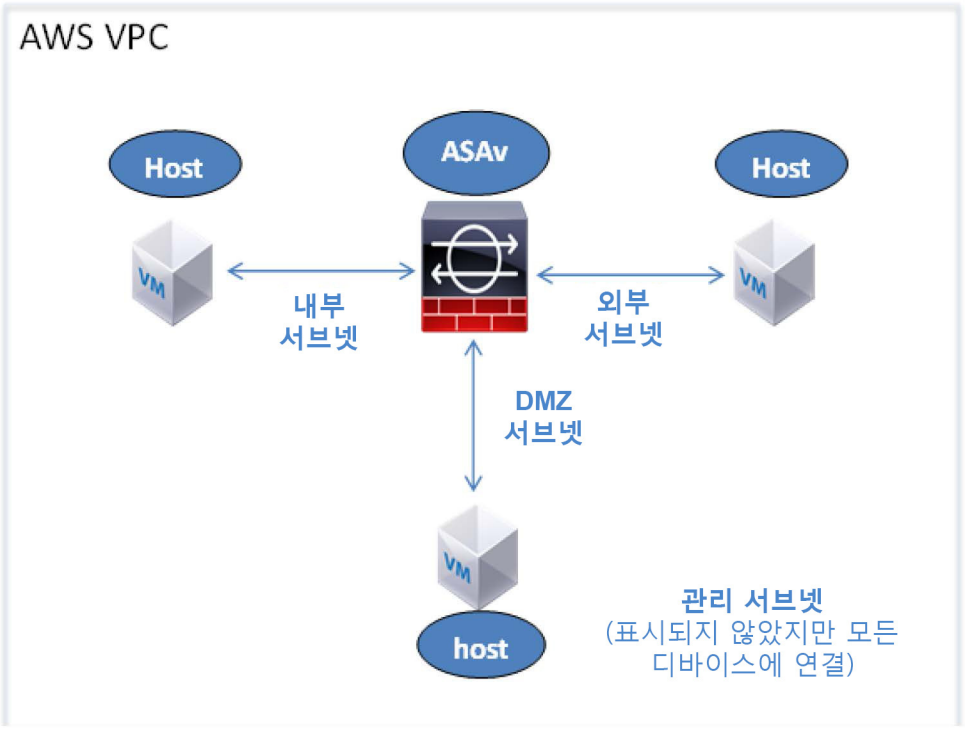
지원되지 않는 기능

- 콘솔 액세스(네트워크 인터페이스를 통해 SSH 또는 ASDM을 사용하여 관리)
- IPv6
- VLAN
- 100Mbps 성능의 ASAv5
- 무차별(Promiscuous) 모드(스니핑 또는 투명 모드 방화벽 지원 없음)
- 다중 상황 모드
- 클러스터링
- ASAv 기본 HA
- EtherChannel은 직접 물리적 인터페이스에서만 지원됩니다.
- VM 가져오기/내보내기
- Amazon Cloudwatch
- 하이퍼바이저 독립적 패키징
- VMware ESXi

AWS 기반 ASAv의 샘플 네트워크 토폴로지

29페이지의 그림 1에서는 Routed Firewall Mode의 ASAv에 대한 권장 토폴로지를 보여줍니다. AWS에 ASAv를 위한 4개의 서브넷(관리, 내부, 외부, DMZ)이 구성되어 있습니다.

그림 1 AWS 구축 기반 샘플 ASAv



AWS에 ASAv 구축

다음 절차는 ASAv에 AWS를 설정하는 단계를 간략하게 정리한 것입니다. 자세한 설정 단계는 AWS 시작하기를 참조하십시오.

절차

1. aws.amazon.com에 로그인하고 지역을 선택합니다.

   AWS는 여러 지역으로 나뉘며, 이 지역은 상호 격리되어 있습니다. 화면의 우측 상단에 지역이 표시됩니다. 한 지역의 리소스가 다른 지역에는 나타나지 않습니다. 원하는 지역에 있는지 정기적으로 확인합니다.

2. **My Account(내 계정) > AWS Management Console(AWS 관리 콘솔)**을 클릭하고 Networking(네트워킹)에서 **VPC > Start VPC Wizard(VPC 마법사 시작)**를 클릭한 다음 단일 공용 서브넷을 선택하여 VPC를 생성하고 다음과 같이 설정합니다. 달리 표시되지 않는 한 기본 설정을 사용할 수 있습니다.

   - 내부 및 외부 서브넷—VPC 및 서브넷의 이름을 입력합니다.
   - 인터넷 게이트웨이—인터넷을 통한 직접 연결을 활성화합니다. 인터넷 게이트웨이의 이름을 입력합니다.
   - 외부 테이블—인터넷에 대한 아웃바운드 트래픽을 활성화하려면 항목을 추가합니다. 인터넷 게이트웨이에 0.0.0.0/0을 추가합니다.

3. **My Account(내 계정) > AWS Management Console(AWS 관리 콘솔) > EC2**를 클릭한 후, **Create an Instance(인스턴스 생성)**를 클릭합니다.
   - AMI를 선택합니다(예: Ubuntu Server 14.04 LTS).

     이미지 전달 알림에 식별된 AMI를 사용합니다.
   - ASAv에서 지원하는 인스턴스 유형(예: c3.large)을 선택합니다.
   - 인스턴스를 구성합니다. CPU 및 메모리는 고정되어 있습니다.
   - 원한다면 Advanced Details(고급 세부 정보)에서 Day 0 Configuration을 추가합니다. Day 0 컨피그레이션에 추가 정보를 구성하는 방법과 절차(예: 스마트 라이센싱)는 Day 0 컨피그레이션 파일 준비, 22페이지를 참조하십시오.

     Day 0 컨피그레이션 샘플

     ```
     ! ASA 9.5.1.200
     interface management0/0
     management-only
     nameif management
     security-level 100
     ip address dhcp setroute
     no shut
     !
     same-security-traffic permit inter-interface
     same-security-traffic permit intra-interface
     !
     crypto key generate rsa modulus 2048
     ssh 0 0 management
     ssh timeout 30
     username admin nopassword privilege 15
     username admin attributes
     service-type admin
     ! required config end
     ! example dns configuration
     dns domain-lookup management
     DNS server-group DefaultDNS
     ! where this address is the .2 on your public subnet
     name-server 172.19.0.2
     ! example ntp configuration
     name 129.6.15.28 time-a.nist.gov
     name 129.6.15.29 time-b.nist.gov
     name 129.6.15.30 time-c.nist.gov
     ntp server time-c.nist.gov
     ntp server time-b.nist.gov
     ntp server time-a.nist.gov
     ```
   - 스토리지(기본값 적용).
   - 태그 인스턴스—다수의 태그를 생성하여 디바이스를 분류할 수 있습니다. 손쉽게 찾을 수 있도록 이름을 지정합니다.
   - 보안 그룹—보안 그룹을 생성하고 이름을 지정합니다. 보안 그룹은 인바운드 및 아웃바운드 트래픽을 제어하기 위한 인스턴스에 대한 가상 방화벽입니다.

     기본적으로 보안 그룹은 모든 주소에 개방되어 있습니다. ASAv 액세스에 사용할 주소의 SSH만 허용하도록 규칙을 변경합니다.
   - 컨피그레이션을 검토하고 **Launch(실행)**를 클릭합니다.
4. 키 쌍을 생성합니다.

   키 쌍을 인식할 수 있는 이름을 지정하고 안전한 곳에 키를 다운로드합니다. 키는 다시 다운로드할 수 없습니다. 키 쌍을 잃어버릴 경우 인스턴스를 삭제하고 다시 구축해야 합니다.
5. **Launch Instance(인스턴스 실행)**를 클릭하여 ASAv를 구축합니다.

6. **My Account(내 계정) > AWS Management Console(AWS 관리 콘솔) > EC2 > Launch an Instance(인스턴스 실행) > My AMIs(내 AMI)**를 클릭합니다.

7. ASAv에 대한 인스턴스 각각에서 Source/Destination Check(소스/목적지 확인)가 비활성화되었음을 확인합니다.

   AWS 기본 설정에서는 인스턴스가 자체 IP 주소에 대한 트래픽만 수신하고 자체 IP 주소에서만 트래픽을 보낼 수 있습니다. ASAv가 라우팅 홉의 역할을 할 수 있으려면 ASAv 트래픽 인스턴스(내부, 외부, DMZ) 각각에서 소스/목적지 확인을 비활성화해야 합니다.

AWS에 ASAv 구축

Microsoft Azure 클라우드 기반 ASAv 구축

Microsoft Azure 클라우드에 ASAv를 구축할 수 있습니다.

- Microsoft Azure 클라우드 기반 ASAv 구축 정보, 33페이지
- ASAv 및 Azure의 사전 요구 사항과 시스템 요구 사항, 33페이지
- ASAv 및 Azure에 대한 지침과 제한, 34페이지
- Azure 기반 ASAv의 샘플 네트워크 토폴로지, 35페이지
- 구축 중에 생성된 리소스, 35페이지
- Azure 라우팅, 36페이지
- 가상 네트워크의 VM을 위한 라우팅 컨피그레이션, 36페이지
- IP 주소, 37페이지
- DNS, 37페이지
- Microsoft Azure에서 ASAv 구축, 37페이지

Microsoft Azure 클라우드 기반 ASAv 구축 정보

Microsoft Azure는 전용 Microsoft Hyper V 하이퍼바이저를 사용하는 퍼블릭 클라우드 환경입니다. ASAv는 Hyper V 하이퍼바이저의 Microsoft Azure 환경에서 게스트로 실행됩니다. Microsoft Azure 기반 ASAv는 단일 인스턴스 유형, 즉 Standard D3를 지원합니다. 이 유형은 4개의 vCPU, 14GB, 4개의 인터페이스를 지원합니다.

ASAv 및 Azure의 사전 요구 사항과 시스템 요구 사항

- Azure.com에서 계정을 생성합니다.

  Microsoft Azure에서 계정을 생성한 다음 로그인하고 Microsoft Azure Marketplace에서 ASAv를 선택하여 구축합니다.

- ASAv 라이센스를 등록합니다.

  ASAv 라이센스를 등록할 때까지 저성능 모드에서 실행됩니다. 이 모드에서는 100개의 연결 및 100Kbps의 처리량만 허용됩니다. ASAv를 위한 스마트 소프트웨어 라이센싱을 참조하십시오.

- 인터페이스 요구 사항:

  4개의 네트워크에서 4개의 인터페이스로 ASAv를 구축해야 합니다.

  - 관리 인터페이스

    참고: 에지 방화벽 컨피그레이션의 경우 관리 인터페이스가 "외부 인터페이스"로도 사용됩니다.

    참고: Azure에서는 처음 정의되는 인터페이스(항상 관리 인터페이스)가 유일하게 Azure 공용 IP 주소를 가질 수 있는 인터페이스입니다. 이런 이유로 Azure의 ASAv는 관리 인터페이스에서 통과-데이터 트래픽을 허용합니다. 따라서 관리 인터페이스에 대한 초기 컨피그레이션은 **management-only** 설정을 포함하지 않습니다.

  - 내부 및 외부 인터페이스
  - 추가 서브넷(DMZ 또는 사용자가 선택하는 임의의 네트워크)

- 통신 경로:
  - 관리 인터페이스(통신)—SSH 액세스에 그리고 ASDM에 ASAv를 연결하는 데 사용합니다.
  - 내부 인터페이스(필수)—ASAv를 내부 호스트에 연결하는 데 사용합니다.
  - 외부 인터페이스(필수)—ASAv를 공용 네트워크에 연결하는 데 사용합니다.
  - DMZ 인터페이스(선택 사항)—Standard_D3 인터페이스 사용 시 ASAv를 DMZ 네트워크에 연결하는 데 사용합니다.
- ASAv 시스템 요구 사항은 Cisco ASA 호환성을 참조하십시오.

ASAv 및 Azure에 대한 지침과 제한

지원 기능

- Microsoft Azure 클라우드에서 구축
- 인스턴스당 최대 4개의 vCPU
- L3 네트워크의 사용자 구축

  참고: Azure는 구성 가능한 L2 vSwitch 기능을 제공하지 않습니다.

- 라우팅 방화벽 모드(기본)

  참고: 라우팅 방화벽 모드의 ASAv는 네트워크의 일반 레이어 3 경계입니다. 이 모드에서는 각 인터페이스에 IP 주소가 필요합니다. Azure에서는 VLAN 태깅 인터페이스를 지원하지 않으므로 태그가 지정되지 않은 비 트렁크 인터페이스에서 IP 주소를 구성해야 합니다.

지원되지 않는 기능

- 콘솔 액세스(네트워크 인터페이스를 통해 SSH 또는 ASDM을 사용하여 관리 수행)
- IPv6
- 사용자 인스턴스 인터페이스의 VLAN 태깅
- 점보 프레임
- Azure의 관점에서는 디바이스 소유가 아닌 IP 주소에 대한 프록시 ARP
- 임의의 인터페이스상의 공용 IP 주소

  관리 0/0 인터페이스만 공용 IP 주소를 가질 수 있습니다.

- 프로미스큐어스 모드(스니핑 또는 투명 모드 방화벽 지원 없음)

  참고: Azure 정책에서는 ASAv가 투명 방화벽 모드에서 작동할 수 없습니다. 이 모드에서는 인터페이스가 프로미스큐어스 모드에서 작동할 수 없기 때문입니다.

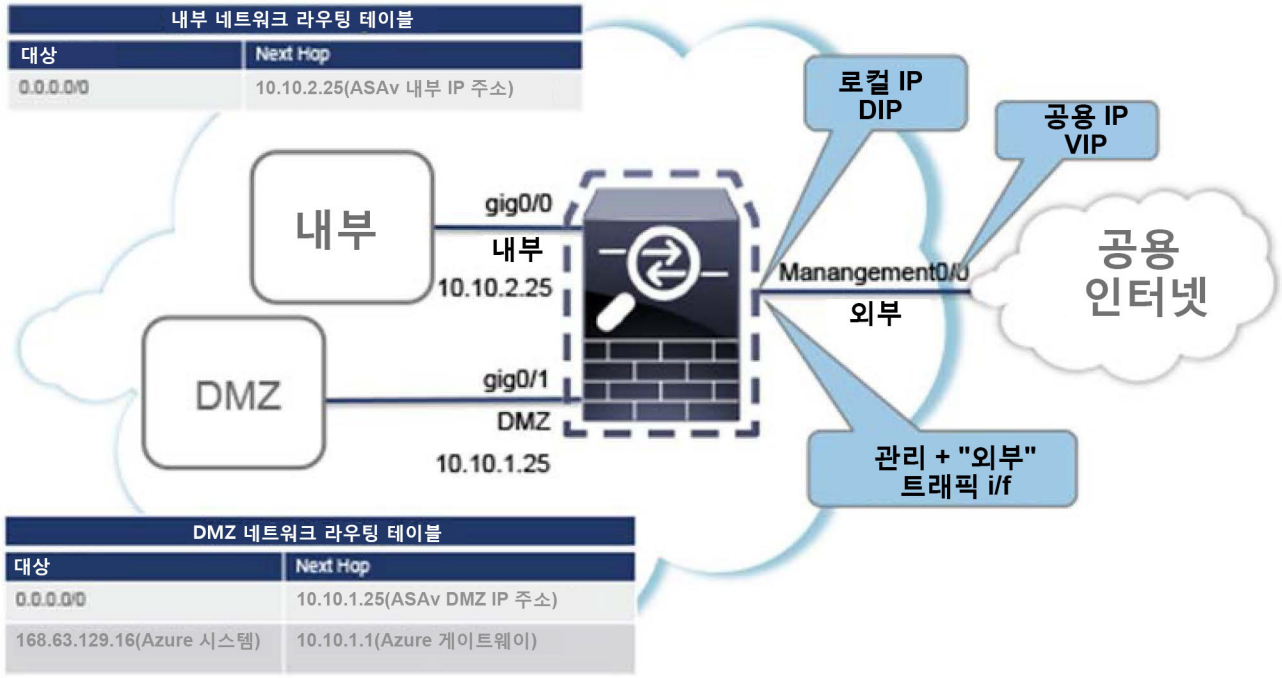
- 멀티컨텍스트 모드
- 클러스터링
- ASAv 기본 HA
- VM 가져오기/내보내기
- 기본적으로 FIPS 모드는 Azure 클라우드에서 실행 중인 ASAv에 대해 활성화되지 않습니다.

  주의: FIPS 모드를 활성화할 경우 **ssh key-exchange group dh-group14-sha1** 명령을 사용하여 Diffie-Helman 키 교환 그룹을 더 강력한 키로 변경해야 합니다. Diffie-Helman 그룹을 변경하지 않을 경우 더 이상 ASAv에 대한 SSH가 불가합니다. 이는 초기에 ASAv를 관리할 수 있는 유일한 방법입니다.

Azure 기반 ASAv의 샘플 네트워크 토폴로지

35페이지의 그림 1에서는 라우팅 방화벽 모드의 ASAv에 대한 권장 토폴로지를 보여줍니다. Azure에 3개의 서브넷(관리, 내부, DMZ)이 구성되어 있습니다. 4번째 필수 인터페이스(외부)는 표시되지 않습니다.

그림 1 Azure 구축 기반 샘플 ASAv



구축 중에 생성된 리소스

Azure에서 ASAv를 구축할 때 다음 리소스가 생성됩니다.

- ASAv VM(Virtual Machine)
- 리소스 그룹(기존 리소스 그룹을 선택하지 않는 한)

  ASAv 리소스 그룹은 가상 네트워크 및 스토리지 계정에서 사용하는 것과 동일한 리소스 그룹이어야 합니다.
- 4개의 NIC - *vm name*-Nic0, *vm name*-Nic1, *vm name*-Nic2, *vm name*-Nic3

  이 NIC는 ASAv의 인터페이스인 Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2에 각각 매핑됩니다.
- *vm name*-SSH-SecurityGroup이라는 보안 그룹

  보안 그룹이 VM의 Nic0에 매핑되며, 이는 ASAv Management 0/0에 매핑됩니다.

  보안 그룹은 VPN 목적으로 SSH 및 UDP 포트 500, UDP 4500을 허용하는 규칙을 포함합니다. 구축 후에 이 값을 수정할 수 있습니다.

- 공용 IP 주소. 구축 중에 선택한 값에 따라 이름이 지정됩니다.

  공용 IP 주소가 VM Nic0과 연결되며, 이는 Management 0/0에 매핑됩니다. Azure에서는 공용 IP 주소를 첫 NIC에 연결하는 것만 허용합니다.

  참고: 공용 IP 주소(신규 또는 기존)를 선택해야 합니다. NONE 옵션은 지원되지 않습니다.

- 4개의 서브넷이 있는 가상 네트워크(기존 네트워크를 선택하지 않은 경우)
- 각 서브넷에 대한 라우팅 테이블(이미 있을 경우 업데이트됨)

  이 테이블의 이름은 *subnet name*-ASAv-RouteTable입니다.

  각 라우팅 테이블에는 다른 3개 서브넷에 대한 경로가 포함되며 ASAv IP 주소가 다음 홉입니다. 트래픽이 다른 서브넷 또는 인터넷에 도달해야 하는 경우 기본 경로 추가를 선택할 수 있습니다.

- 선택된 스토리지 계정의 부팅 진단 파일

  부팅 진단 파일은 Blob(binary large object)에 포함됩니다.

- Blob과 컨테이너 VHD인 *vm name*-disk.vhd 및 *vm name*-<uuid>.status에 속한 선택된 스토리지 계정의 파일 2개
- 스토리지 계정(기존 스토리지 계정을 선택하지 않은 경우)

  참고: VM을 삭제할 경우 이 리소스에서 유지할 것을 제외하고 각각을 개별적으로 삭제해야 합니다.

Azure 라우팅

Azure 가상 네트워크의 라우팅은 가상 네트워크의 유효 라우팅 테이블에 따라 결정됩니다. 유효 라우팅 테이블은 기존 시스템 라우팅 테이블과 사용자 정의 라우팅 테이블의 조합입니다.

참고: 현재는 유효 라우팅 테이블 또는 시스템 라우팅 테이블 어느 쪽도 볼 수 없습니다.

사용자 정의 라우팅 테이블은 보고 수정할 수 있습니다. 시스템 테이블과 사용자 정의 테이블의 조합으로 유효 라우팅 테이블이 구성될 경우 가장 구체적인 경로가 선택되며 동등할 때는 사용자 정의 라우팅 테이블이 적용됩니다. 시스템 라우팅 테이블은 Azure의 가상 네트워크 인터넷 게이트웨이를 가리키는 기본 경로(0.0.0.0/0)를 포함합니다. 시스템 라우팅 테이블은 나머지 정의된 서브넷에 대한 경로도 포함하는데, 다음 홉은 Azure의 가상 네트워크 인프라 게이트웨이를 가리킵니다.

ASAv 구축 프로세스에서는 ASAv를 통과하도록 트래픽을 라우팅하기 위해 각 서브넷에 대한 경로를 다음 홉으로 ASAv를 사용 중인 나머지 세 서브넷에 추가합니다. 서브넷의 ASAv 인터페이스를 가리키는 기본 경로(0.0.0.0/0)를 추가하려는 경우도 있습니다. 그러면 서브넷의 모든 트래픽이 ASAv를 통과합니다. 따라서 이 트래픽 처리를 위해 (아마도 NAT/PAT를 사용하여) 미리 ASAv 정책이 구성되어야 할 수도 있습니다.

시스템 라우팅 테이블의 기존 경로 때문에 ASAv를 다음 홉으로 가리키는 경로를 사용자 정의 라우팅 테이블에 추가해야 합니다. 그렇지 않으면 사용자 정의 테이블의 기본 경로가 시스템 라우팅 테이블의 더 구체적인 경로에 밀려 트래픽이 ASAv를 우회하게 됩니다.

가상 네트워크의 VM을 위한 라우팅 컨피그레이션

Azure 가상 네트워크의 라우팅은 클라이언트의 특정 게이트웨이 설정이 아니라 유효 라우팅 테이블에 따라 달라집니다. 가상 네트워크에서 실행 중인 클라이언트는 DHCP에서 경로를 지정할 수도 있습니다. 이는 해당 서브넷의 1번 주소입니다. 이는 자리 표시자이며 가상 네트워크의 인프라 가상 게이트웨이에 패킷을 보내는 기능만 할 뿐입니다. 패킷이 VM을 떠나면 유효 라우팅 테이블에 따라 (사용자 정의 테이블에서 수정한 대로) 라우팅됩니다. 클라이언트의 게이트웨이가 1로 구성되었거나 ASAv 주소로 구성된 어떤 경우에도 유효 라우팅 테이블에 따라 다음 홉이 결정됩니다.

Azure VM ARP 테이블에서는 모든 확인된 호스트에 대해 동일한 MAC 주소(1234.5678.9abc)를 표시합니다. 그러면 Azure VM을 떠나는 모든 패킷이 Azure 게이트웨이에 도달하며, 여기서 유효 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.

IP 주소

다음 정보가 Azure의 IP 네트워크에 적용됩니다.

- ASAv의 첫 NIC(Management 0/0에 매핑됨)는 연결된 서브넷에서 전용 IP 주소를 받습니다.

  공용 IP 주소를 이 전용 IP 주소와 연결할 수 있으며 Azure Internet 게이트웨이에서 NAT 변환을 처리합니다.
- VM의 첫 NIC만 공용 IP 주소가 연결될 수 있습니다.
- 동적 공용 IP 주소는 Azure 중지/시작 사이클에 변경될 수 있습니다. 그러나 Azure가 재시작하고 ASAv가 다시 로드될 때는 유지됩니다.
- 고정 공용 IP 주소는 Azure에서 변경하지 않는 한 바뀌지 않습니다.
- ASAv 인터페이스에서 IP 주소 설정에 DHCP를 사용할 수 있습니다. Azure 인프라는 Azure에서 설정된 IP 주소가 ASAv 인터페이스에 지정되게 합니다.

DNS

모든 Azure 가상 네트워크는 내장된 DNS 서버인 168.63.129.16에 액세스할 수 있으며, 이는 다음과 같이 사용 가능합니다.

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

스마트 라이센싱을 구성할 때 자체 DNS 서버가 설정되지 않은 경우 이 컨피그레이션을 사용할 수 있습니다.

Microsoft Azure에서 ASAv 구축

다음 절차는 ASAv에 Microsoft Azure를 설정하는 단계를 간략하게 정리한 것입니다. 자세한 Azure 설정 단계는 Azure 시작하기를 참조하십시오.

Azure에서 ASAv를 구축할 경우 리소스, 공용 IP 주소, 경로 테이블과 같은 다양한 컨피그레이션이 자동으로 생성됩니다. 구축 후에 이 컨피그레이션을 추가로 관리할 수 있습니다. 이를테면 유휴 시간 초과 값을 낮게 설정된 기본값에서 변경할 수 있습니다.

절차

1. ARM(Azure Resource Manager) 포털에 로그인합니다.

   Azure 포털에서는 데이터 센터 위치와 상관없이 현재 계정 및 서브스크립션의 가상 요소를 보여줍니다.
2. 마켓플레이스에서 Cisco ASAv를 검색한 다음 구축하려는 ASAv를 클릭합니다.
3. 기본 설정을 구성합니다.
   a. 가상 시스템의 이름을 입력합니다. 이 이름은 Azure 서브스크립션 내에서 고유해야 합니다.

      참고: 기존 이름을 사용하면 구축이 실패하므로 주의합니다.

   b. 사용자 이름을 입력합니다.

   c. 권한 부여 유형을 비밀번호 또는 SSH 키 중 하나로 선택합니다.

      비밀번호를 선택할 경우 비밀번호를 입력하고 커밋합니다.

   d. 서브스크립션 유형을 선택합니다.

e. 리소스 그룹을 선택합니다.

   리소스 그룹은 가상 네트워크의 리소스 그룹과 동일해야 합니다.

f. 위치를 선택합니다.

   이 위치는 네트워크 및 리소스 그룹과 동일해야 합니다.

g. **OK(확인)**를 클릭합니다.

4. ASAv 설정을 구성합니다.

   a. 가상 시스템 크기를 선택합니다.

      참고: ASAv에서 사용 가능한 크기는 Standard D3뿐입니다.

   b. 스토리지 계정을 선택합니다.

      참고: 기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다. 스토리지 계정의 위치가 네트워크 및 가상 시스템에 대한 위치와 동일해야 합니다.

   c. Name(이름) 필드에 IP 주소에 대한 레이블을 입력하여 공용 IP 주소를 요청한 다음 **OK(확인)**를 클릭합니다.

      참고: Azure는 기본적으로 동적 공용 IP를 생성합니다. 이는 VM이 중지하고 재시작할 때 변경될 수 있습니다. 고정 IP 주소를 선호할 경우 포털에서 public-ip를 열고 동적 주소에서 고정 주소로 변경할 수 있습니다.

   d. 필요하다면 DNS 레이블을 추가합니다.

      참고: FQDN(fully qualified domain name)은 DNS 레이블 + Azure URL이 됩니다. 즉 <dnslabel>.<location>.cloupapp.azure.com입니다.

   e. 기존 가상 네트워크를 선택하거나 새로 만듭니다.

   f. ASAv 구축 대상이 될 4개의 서브넷을 구성하고 **OK(확인)**를 클릭합니다.

      참고: 각 인터페이스가 고유한 서브넷에 연결되어야 합니다.

   g. **OK(확인)**를 클릭합니다.

5. 컨피그레이션 요약을 본 다음 **OK(확인)**를 클릭합니다.

6. 이용 약관을 보고 **Create(생성)**를 클릭합니다.

7. SSH를 통해 입력 가능한 CLI 명령을 사용하여 컨피그레이션을 계속하거나 ASDM을 사용합니다. ASDM 액세스에 대한 지침은 ASDM 시작, 55페이지를 참조하십시오.

Hyper-V를 사용하여 ASAv 구축

Microsoft Hyper-V를 사용하여 ASAv를 구축할 수 있습니다.

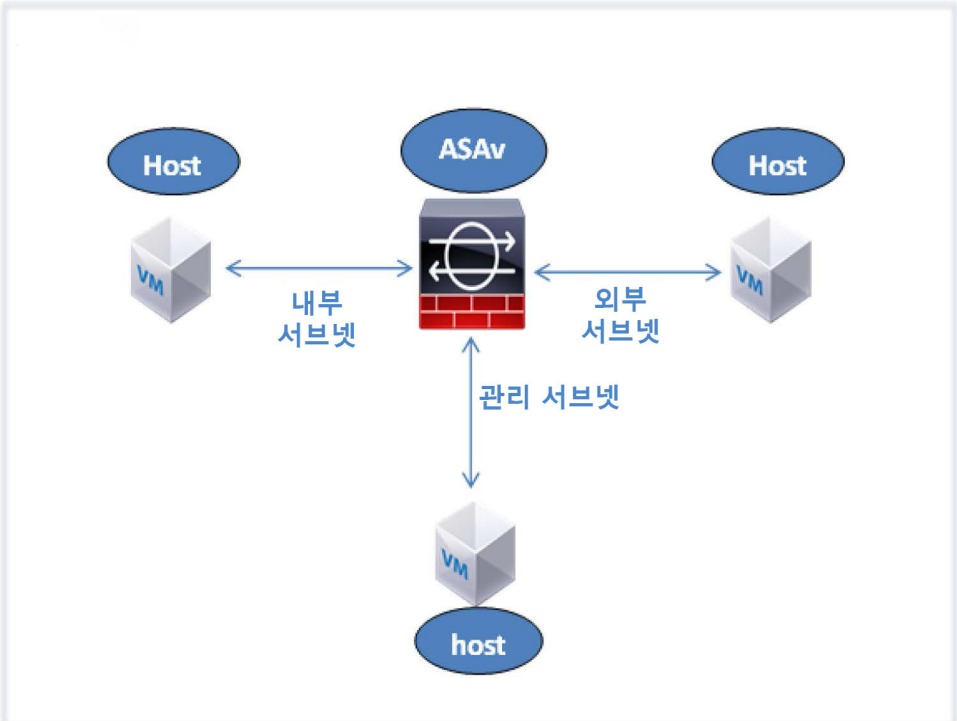
- Hyper-V를 사용한 ASAv 구축 정보, 39페이지
- ASAv 및 Hyper-V에 대한 지침과 제한, 40페이지
- ASAv 및 Hyper-V 사전 요구 사항, 41페이지
- Day 0 컨피그레이션 파일 준비, 41페이지
- 명령행을 사용하여 Hyper-V에 ASAv 설치, 44페이지
- Hyper-V Manager를 사용하여 Hyper-V에 ASAv 설치, 44페이지
- Hyper-V Manager에서 네트워크 어댑터 추가, 51페이지
- 네트워크 어댑터 이름 수정, 53페이지
- MAC 주소 스푸핑 구성, 54페이지
- SSH 구성, 54페이지

Hyper-V를 사용한 ASAv 구축 정보

독립형 Hyper-V 서버에 또는 Hyper-V Manager를 통해 Hyper-V를 구축할 수 있습니다. Powershell CLI 명령을 사용하는 설치 방법은 명령행을 사용하여 Hyper-V에 ASAv 설치, 44페이지를 참조하십시오. Hyper-V Manager를 사용하는 설치 방법은 Hyper-V Manager를 사용하여 Hyper-V에 ASAv 설치, 44페이지를 참조하십시오. Hyper-V는 시리얼 콘솔 옵션을 제공하지 않습니다. 관리 인터페이스에서 SSH 또는 ASDM을 통해 Hyper-V 를 관리할 수 있습니다. SSH 설정에 대한 내용은 SSH 구성, 54페이지를 참조하십시오.

40페이지의 그림 1에서는 라우팅 방화벽 모드의 ASAv에 대한 권장 토폴로지를 보여줍니다. Hyper-V에 ASAv를 위한 3가지 서브넷(관리, 내부, 외부)이 설정되어 있습니다.

그림 1 라우팅 방화벽 모드 ASAv를 위한 권장 토폴로지



ASAv 및 Hyper-V에 대한 지침과 제한

- 플랫폼 지원
  - Cisco UCS B-Series 서버
  - Cisco UCS C-Series 서버
  - Hewlett Packard Proliant DL160 Gen8
- OS 지원
  - Windows Server 2012
  - 기본 Hyper-V

  참고: ASAv는 현재 가상화에 사용되는 최신 64비트 고성능 플랫폼에서 실행해야 합니다.
- 파일 형식

  Hyper-V에서 ASAv 초기 구축에 VHDX 형식을 지원합니다.
- Day 0 컨피그레이션

  필요한 ASA CLI 컨피그레이션 명령을 포함한 텍스트 파일을 생성합니다. 절차는 Day 0 컨피그레이션 파일 준비, 41페이지를 참조하십시오.
- Day 0 컨피그레이션의 방화벽 투명 모드

  컨피그레이션 줄 'firewall transparent'가 Day 0 컨피그레이션 파일의 맨 위에 있어야 합니다. 파일에서 다른 곳에 위치할 경우 잘못된 동작이 나올 수 있습니다. 절차는 Day 0 컨피그레이션 파일 준비, 41페이지를 참조하십시오.

- 장애 조치

  Hyper-V 기반 ASAv는 액티브/스탠바이 페일오버를 지원합니다. 라우팅 모드와 투명 모드에서 액티브/스탠바이 페일오버를 구현하려면 모든 가상 네트워크 어댑터에서 MAC 주소 스푸핑을 활성화해야 합니다. MAC 주소 스푸핑 구성, 54페이지를 참조하십시오. 독립형 ASAv의 투명 모드에서는 관리 인터페이스에서 MAC 주소 스푸핑을 활성화지 않아야 합니다. 액티브/액티브 페일오버는 지원되지 않습니다.

- Hyper-V는 최대 8개의 인터페이스를 지원합니다. Management 0/0 및 GigabitEthernet 0/0 ~ 0/6입니다. GigabitEthernet을 페일오버 링크로 사용할 수 있습니다.
- VLAN

  Set-VMNetworkAdapterVLan Hyper-V Powershell 명령을 사용하여 트렁크 모드의 인터페이스에 VLAN을 설정합니다. 관리 인터페이스에 대한 기본 VLAN ID를 특정 VLAN으로 또는 VLAN 없음을 의미하는 '0'으로 설정할 수 있습니다. 트렁크 모드는 Hyper-V 호스트 재부팅 시 유지되지 않습니다. 재부팅한 후 매번 트렁크 모드를 재구성해야 합니다.

- 레거시 네트워크 어댑터는 지원되지 않습니다.
- 2세대 가상 시스템은 지원되지 않습니다.
- Microsoft Azure는 지원되지 않습니다.

ASAv 및 Hyper-V 사전 요구 사항

- MS Windows 2012에 Hyper-V를 설치합니다.
- Day 0 컨피그레이션 텍스트 파일을 생성합니다(사용 중인 경우).

  ASAv가 처음으로 구축되기 전에 Day 0 컨피그레이션을 추가해야 합니다. 그렇지 않으면 ASAv에서 **write erase**를 수행해야 Day 0 컨피그레이션을 사용할 수 있습니다. 절차는 Day 0 컨피그레이션 파일 준비, 41페이지를 참조하십시오.

- Cisco.com에서 ASAv VHDX 파일을 다운로드합니다.

  http://www.cisco.com/go/asa-software

  참고: Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

- 3개 이상의 서브넷/VLAN에 구성된 Hyper-V 스위치.
- Hyper-V 시스템 요구 사항은 Cisco ASA 호환성을 참조하십시오.

Day 0 컨피그레이션 파일 준비

ASAv를 시작하기 전에 Day 0 컨피그레이션 파일을 준비할 수 있습니다. 이 파일은 ASAv를 시작할 때 적용할 ASAv 컨피그레이션이 포함된 텍스트 파일입니다. 이 초기 컨피그레이션은 사용자가 선택하는 작업 디렉토리의 "day0-config"라는 이름의 텍스트 파일에 위치하며, 이 파일은 최초 부팅 시 마운트되고 읽히는 day0.iso 파일로 조작됩니다. Day 0 컨피그레이션 파일에는 최소한 관리 인터페이스를 활성화하고 공용 키 인증용 SSH 서버를 설정하는 명령이 포함되어야 할 뿐만 아니라, 완전한 ASA 컨피그레이션도 포함되어야 합니다. 최초 부팅 동안 day0.iso 파일(사용자 정의 day0.iso 또는 기본 day0.iso)을 사용할 수 있어야 합니다.

참고: 처음으로 ASAv를 부팅하기 전에 Day 0 컨피그레이션 파일을 추가해야 합니다. 처음으로 ASAv를 부팅한 후에 Day 0 컨피그레이션을 사용하기로 결정할 경우 **write erase** 명령을 실행하고 Day 0 컨피그레이션 파일을 적용한 다음 ASAv를 부팅해야 합니다.

참고: 초기 구축 동안 ASAv 라이센스를 자동으로 적용하려면, Cisco Smart Software Manager에서 다운로드한 Smart Licensing ID(Identity) Token을 Day 0 컨피그레이션 파일과 같은 디렉토리에 있는 'idtoken'이라는 이름의 텍스트 파일로 가져옵니다.

참고: 투명 모드에서 ASAv를 구축하려는 경우, 투명 모드에서 실행 중인 알려진 ASA 컨피그레이션 파일을 Day 0 컨피그레이션 파일로 사용해야 합니다. 이 사항은 라우팅 방화벽용 Day 0 컨피그레이션 파일에는 적용되지 않습니다.

참고: 이 예에서는 Linux를 사용하지만 Windows의 경우에도 유사한 유틸리티가 있습니다.

절차

1. "day0 config"라는 텍스트 파일에 ASAv에 대한 CLI 컨피그레이션을 입력합니다. 3개의 인터페이스에 대한 인터페이스 컨피그레이션 및 원하는 기타 모든 컨피그레이션을 추가합니다.

   첫 줄은 ASAv 버전으로 시작해야 합니다. day0-config는 유효한 ASA 컨피그레이션이어야 합니다. day0-config를 생성하는 가장 좋은 방법은 기존 ASA 또는 ASAv에서 실행 중인 컨피그레이션 중 원하는 부분을 복사하는 것입니다. day0-config에서 줄의 순서가 중요하며 기존 **show run** 명령 출력의 순서와 일치해야 합니다.

   예

   ```
   ASA Version 9.5.1
   !
   interface management0/0
      nameif management
      security-level 100
      ip address 192.168.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/0
      nameif inside
      security-level 100
      ip address 10.1.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/1
      nameif outside
      security-level 0
      ip address 198.51.100.2 255.255.255.0
      no shutdown
   http server enable
   http 192.168.1.0 255.255.255.0 management
   crypto key generate rsa modulus 1024
   username AdminUser password paSSw0rd
   ssh 192.168.1.0 255.255.255.0 management
   aaa authentication ssh console LOCAL
   ```

2. (선택 사항) Cisco Smart Software Manager에서 발급한 스마트 라이센스 ID 토큰 파일을 컴퓨터에 다운로드합니다.
3. (선택 사항) 다운로드 파일에서 ID 토큰을 복사하고 ID 토큰만 포함된 '텍스트 파일에 붙여넣습니다.
4. (선택 사항) 초기 ASAv 구축 동안 라이센싱이 자동으로 이루어진 경우, day0-config 파일에 다음 정보가 포함되어 있는지 확인합니다.
   - 관리 인터페이스 IP 주소
   - (선택 사항) Smart Licensing에 사용할 HTTP 프록시
   - HTTP 프록시(지정된 경우) 또는 tools.cisco.com에 대한 연결을 지원하는 **route** 명령
   - tools.cisco.com을 IP 주소에 확인하는 DNS 서버
   - 사용자가 요청하는 ASAv 라이센스를 지정하는 Smart Licensing 컨피그레이션
   - (선택 사항) ASAv가 CSSM에서 검색을 더욱 쉽게 수행할 수 있도록 하는 고유한 호스트 이름
5. 텍스트 파일을 ISO 파일로 전환하여 가상 CD-ROM을 생성합니다.

   ```
   stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
   I: input-charset not specified, using utf-8 (detected in locale settings)
   Total translation table size: 0
   Total rockridge attributes bytes: 252
   Total directory bytes: 0
   Path table size (byptes): 10
   Max brk space used 0
   ```

```
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

ID 토큰은 ASAv를 Smart Licensing 서버에 자동으로 등록합니다.

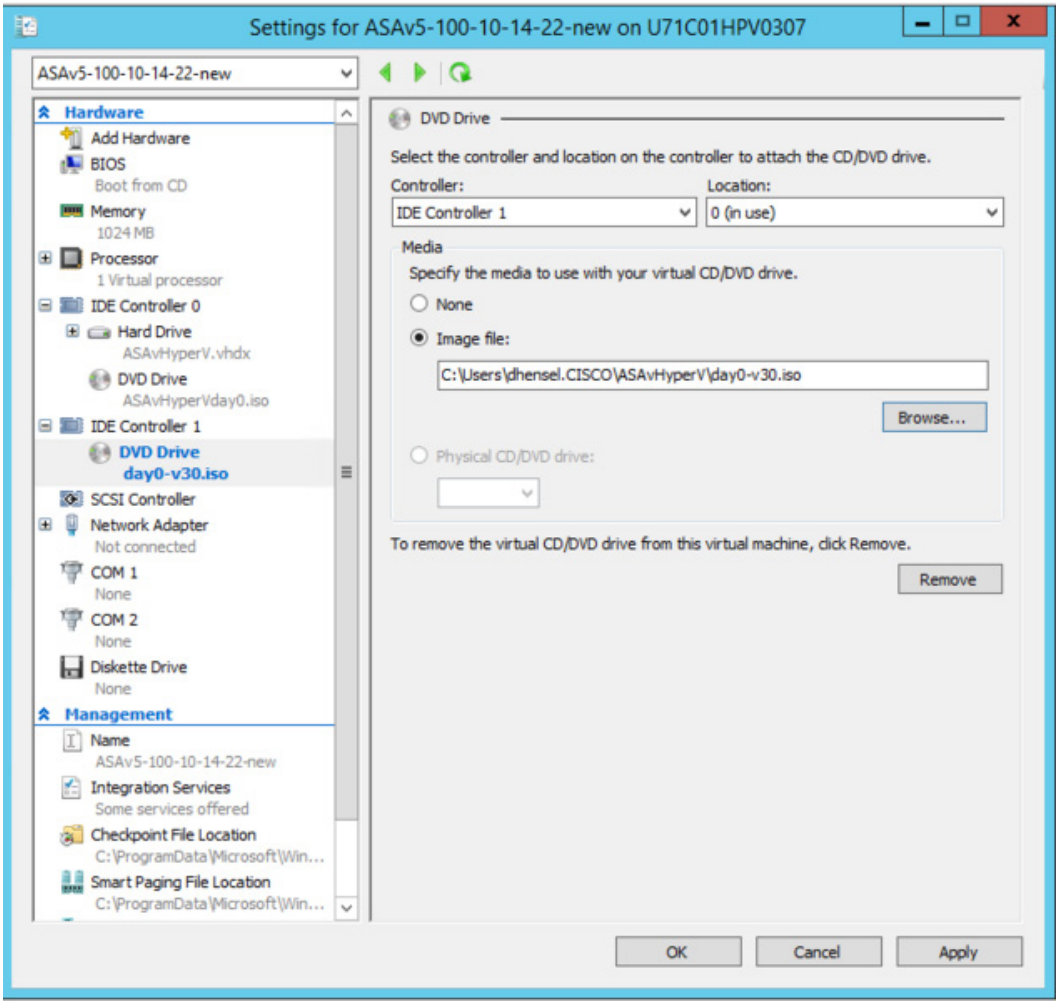
6. 1단계~5단계를 반복하여 구축하려는 각 ASAv에 대해 적절한 IP 주소가 포함된 별도의 기본 컨피그레이션 파일을 만듭니다.

Hyper-V Manager를 사용하여 Day 0 컨피그레이션으로 ASAv 구축

Day 0 컨피그레이션 파일(Day 0 컨피그레이션 파일 준비, 41페이지)을 설정한 다음 Hyper-V Manager를 사용하여 구축할 수 있습니다.

절차

1. Server Manager(서버 관리자) > Tools(툴) > Hyper-V Manager로 이동합니다.
2. Hyper-V Manager의 오른쪽에 있는 **Settings(설정)**를 클릭합니다. Settings(설정) 대화 상자가 열립니다. 왼쪽의 Hardware(하드웨어)에서 **IDE Controller 1(IDE 컨트롤러 1)**을 클릭합니다.



3. 오른쪽의 Media(미디어)에서 **Image file(이미지 파일)** 라디오 버튼을 선택한 다음 Day 0 ISO 컨피그레이션 파일을 저장한 디렉터리로 이동하고 **Apply(적용)**를 클릭합니다. ASAv를 처음으로 부팅하는 경우 Day 0 컨피그레이션 파일의 내용에 따라 구성됩니다.

명령행을 사용하여 Hyper-V에 ASAv 설치

Windows Powershell 명령행을 통해 Hyper_V에 ASAv를 설치할 수 있습니다. 독립형 Hyper-V 서버에 있다면 명령행을 사용하여 Hyper-V를 설치해야 합니다.

절차

1. Windows Powershell을 엽니다.
2. ASAv를 구축합니다.

```
new-vm -name $fullVMName -MemoryStartupBytes $memorysize -Generation 1 -vhdpath
C:\Users\jsmith.CISCO\ASAvHyperV\$ImageName.vhdx -Verbose
```

3. ASAv 모델에 따라 CPU 카운트를 기본값인 1에서 변경합니다.

```
set-vm -Name $fullVMName -ProcessorCount 4
```

4. (선택 사항) 인터페이스 이름을 의미 있는 이름으로 바꿉니다.

```
Get-VMNetworkAdapter -VMName $fullVMName -Name "Network Adapter" | Rename-vmNetworkAdapter -NewName
mgmt
```

5. (선택 사항) 네트워크에서 필요하다면 VLAN ID를 변경합니다.

```
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1151 -Access -VMNetworkAdapterName "mgmt"
```

6. Hyper-V에서 변경 사항을 적용하도록 인터페이스를 새로고침합니다.

```
Connect-VMNetworkAdapter -VMName $fullVMName -Name "mgmt" -SwitchName 1151mgmtswitch
```

7. 내부 인터페이스를 추가합니다.

```
Add-VMNetworkAdapter -VMName  $fullVMName -name "inside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1552 -Access -VMNetworkAdapterName "inside"
```

8. 외부 인터페이스를 추가합니다.

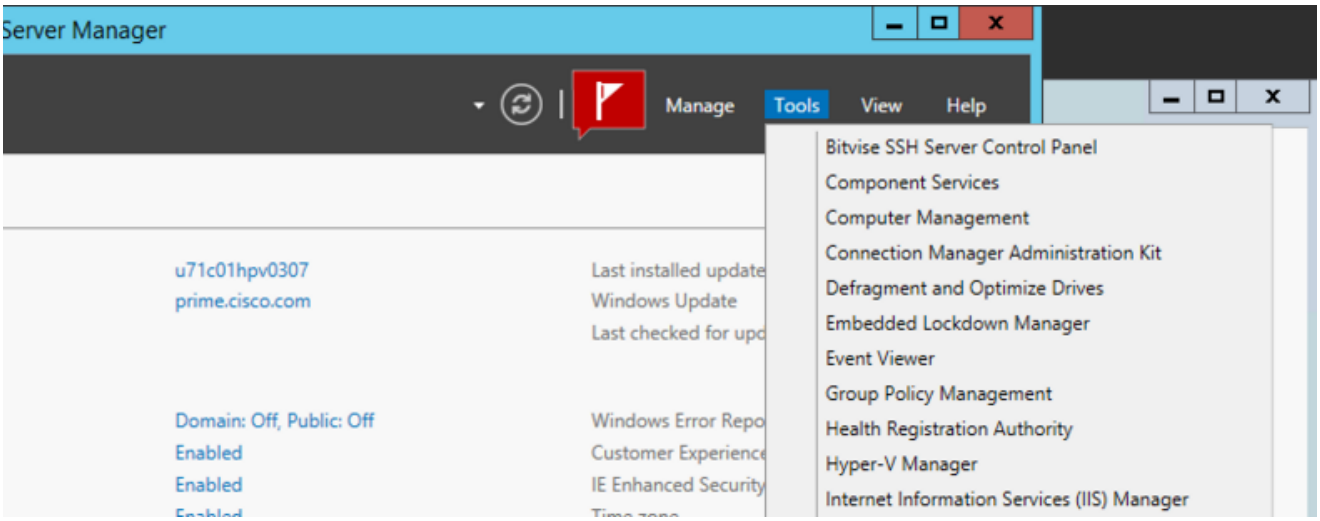
```
Add-VMNetworkAdapter -VMName  $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName "outside"
```

Hyper-V Manager를 사용하여 Hyper-V에 ASAv 설치

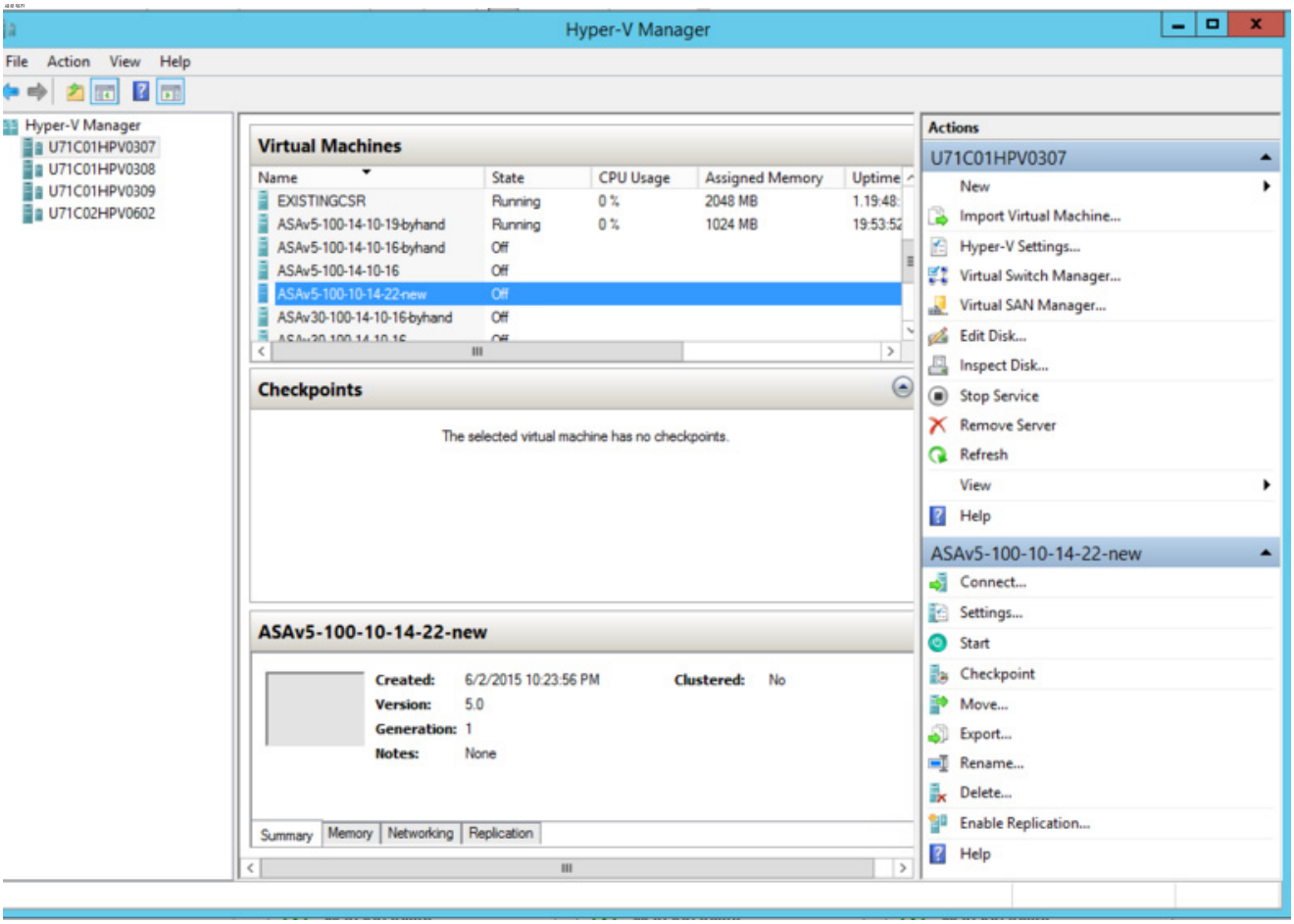
Hyper-V Manager를 사용하여 Hyper-V에 ASAv를 설치할 수 있습니다.

절차

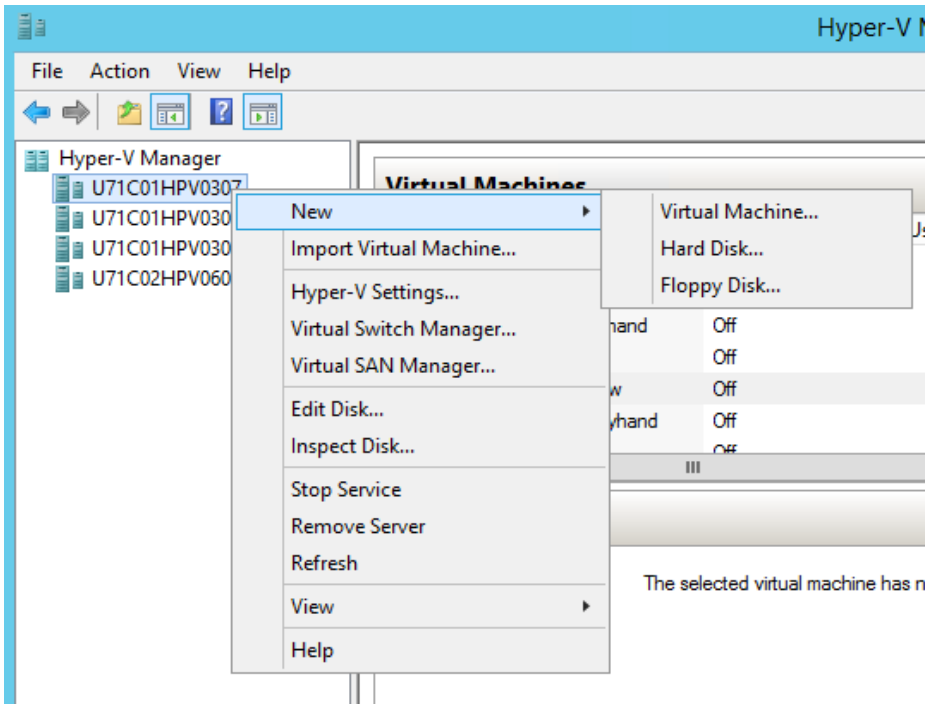
1. Server Manager(서버 관리자) > Tools(툴) > Hyper-V Manager로 이동합니다.



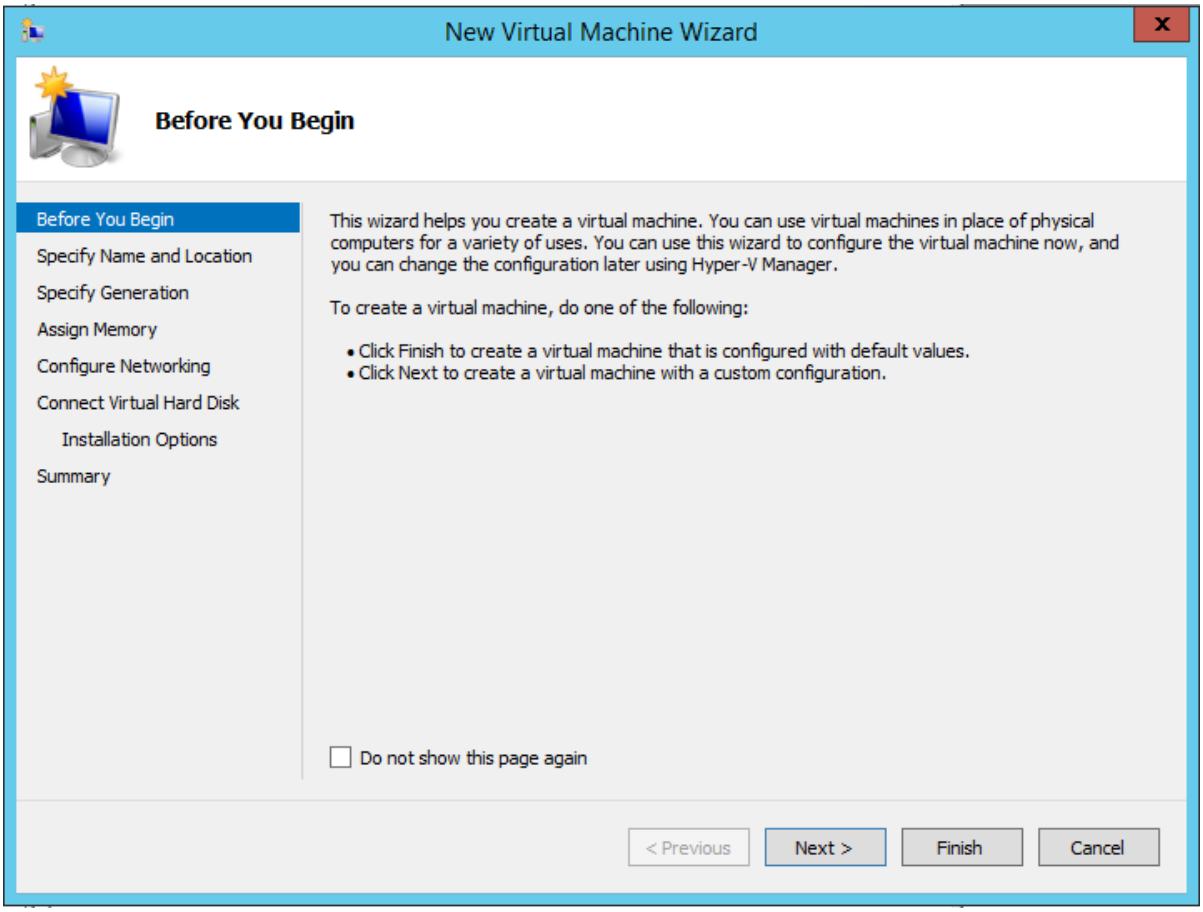
2. Hyper-V Manager가 나타납니다.



3. 오른쪽의 하이퍼바이저 목록에서 원하는 하이퍼바이저를 마우스 오른쪽 버튼으로 클릭하고 New(새로 만들기) > Virtual Machine(가상 시스템)을 선택합니다.



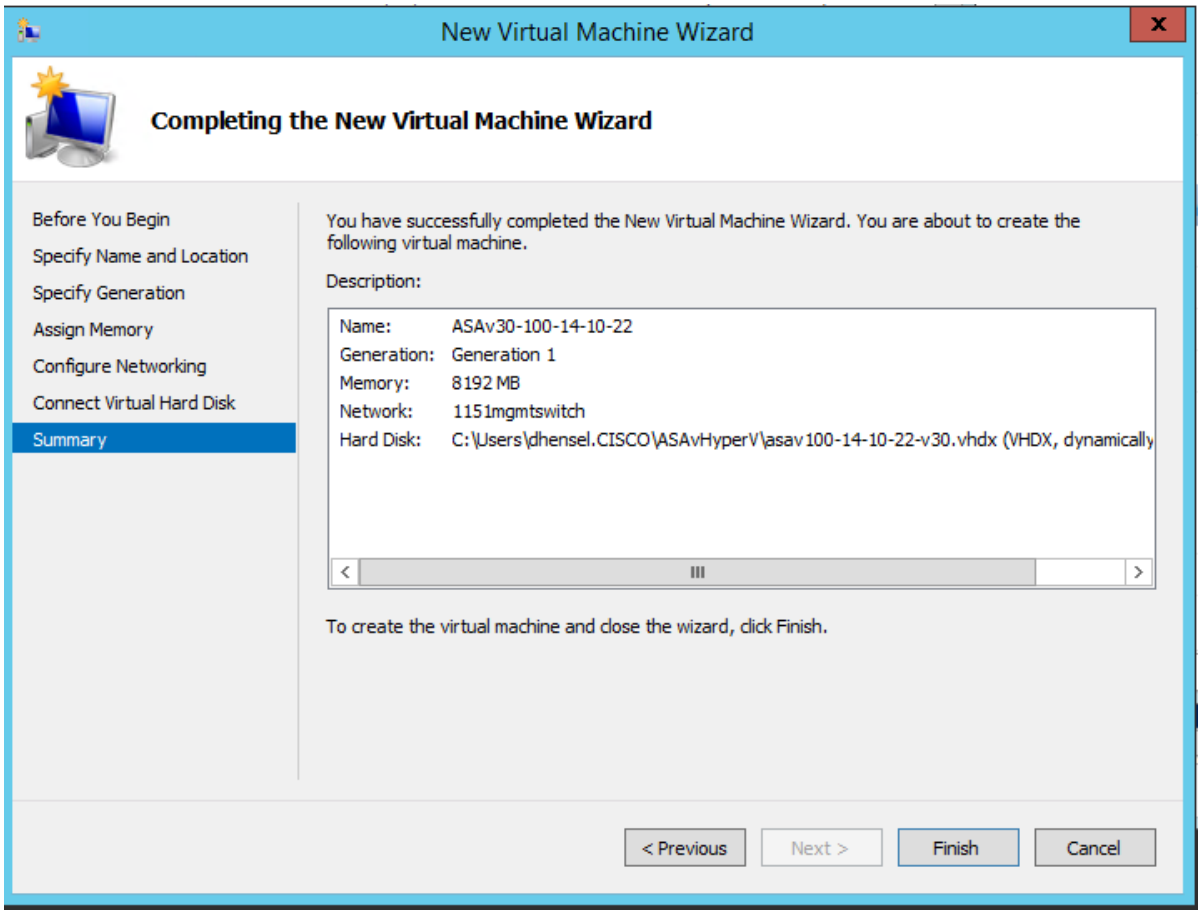
4. New Virtual Machine Wizard(새 가상 시스템 마법사)가 나타납니다.



5. 마법사에서 다음 정보를 지정합니다.
   - ASAv의 이름 및 위치
   - ASAv 세대

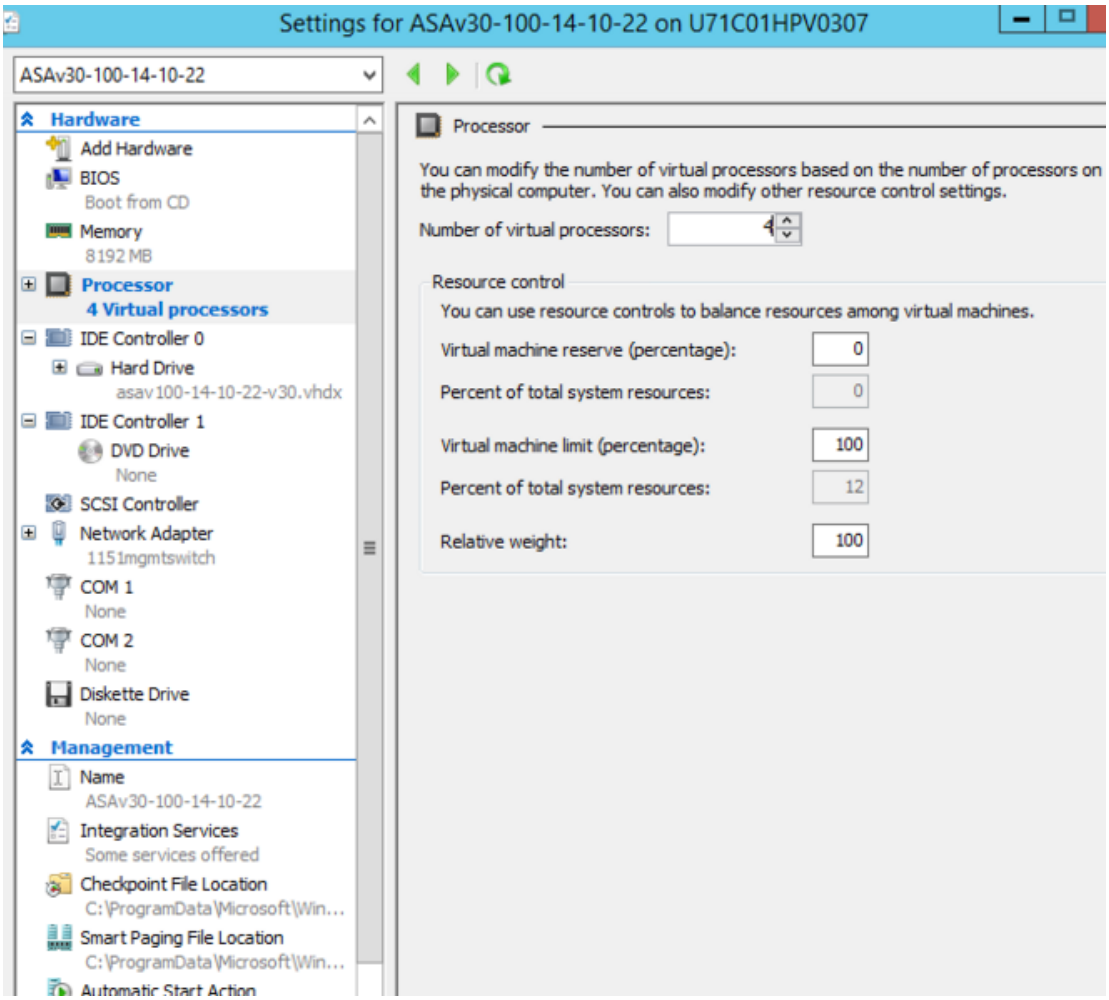
     ASAv에서 유일하게 지원되는 세대는 **Generation 1**입니다.
   - ASAv의 메모리 용량(ASAv5는 1024MB, ASAv 10은 2048MB, ASAv30은 8192MB)
   - 네트워크 어댑터(이미 설정한 가상 스위치에 연결)
   - 가상 하드 디스크 및 위치

     Use an existing virtual hard disk(기존 가상 하드 디스크 사용)를 선택하고 VHDX 파일의 위치로 이동합니다.
6. **Finish(마침)**를 클릭하면 ASAv 컨피그레이션을 보여주는 대화 상자가 나타납니다.

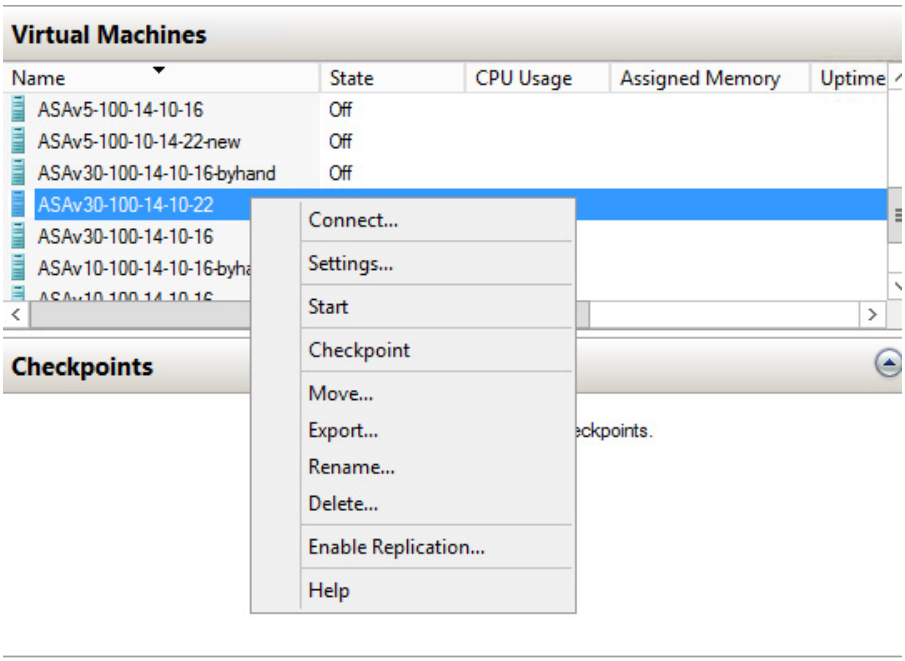


7. ASAv에 4개의 vCPU가 있을 경우 ASAv를 시작하기 전에 vCPU 값을 수정해야 합니다. Hyper-V Manager의 오른쪽에 있는 **Settings(설정)**를 클릭합니다. Settings(설정) 대화 상자가 열립니다. 왼쪽의 Hardware(하드웨어) 메뉴에서 **Processor(프로세서)**를 클릭하여 Processor(프로세서) 창으로 이동합니다. **Number of virtual processors(가상 프로세서 수)**를 4로 변경합니다.

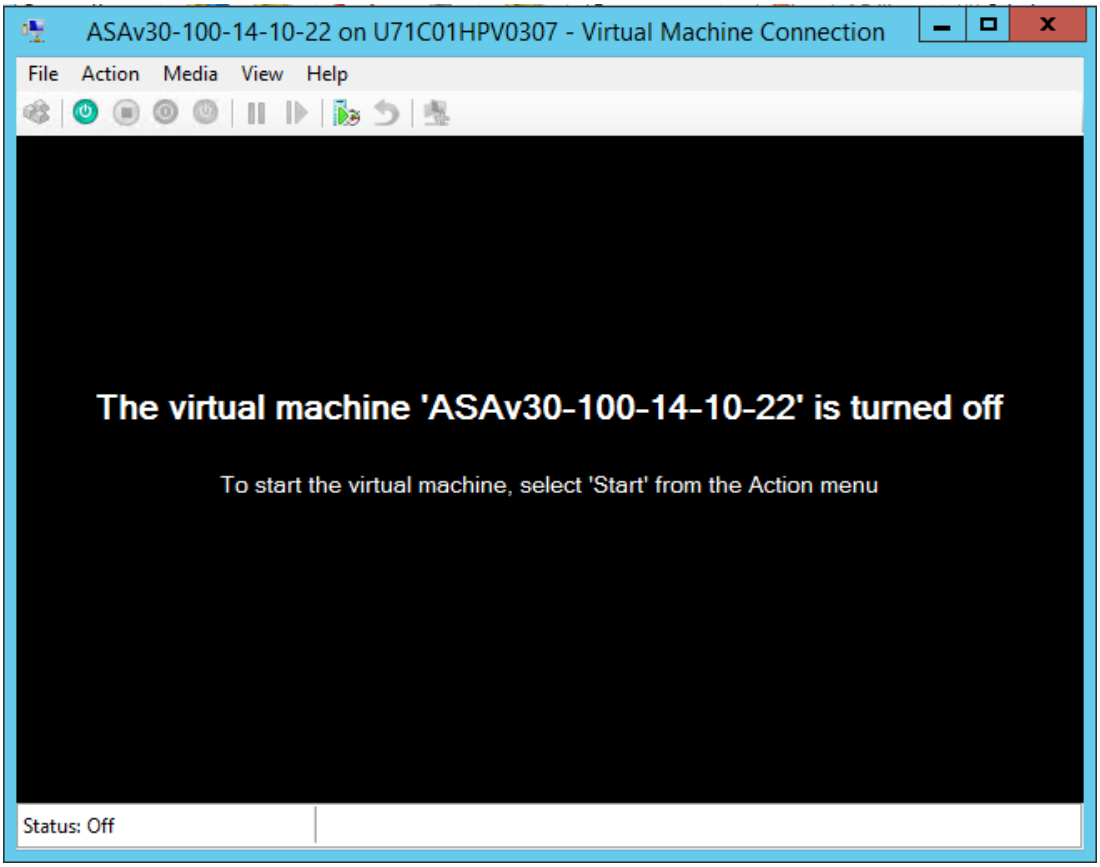
   ASAv5 및 ASAv10에는 1개의 vCPU가, ASAv 30에는 4개의 vCPU가 있습니다. 기본값은 1입니다.



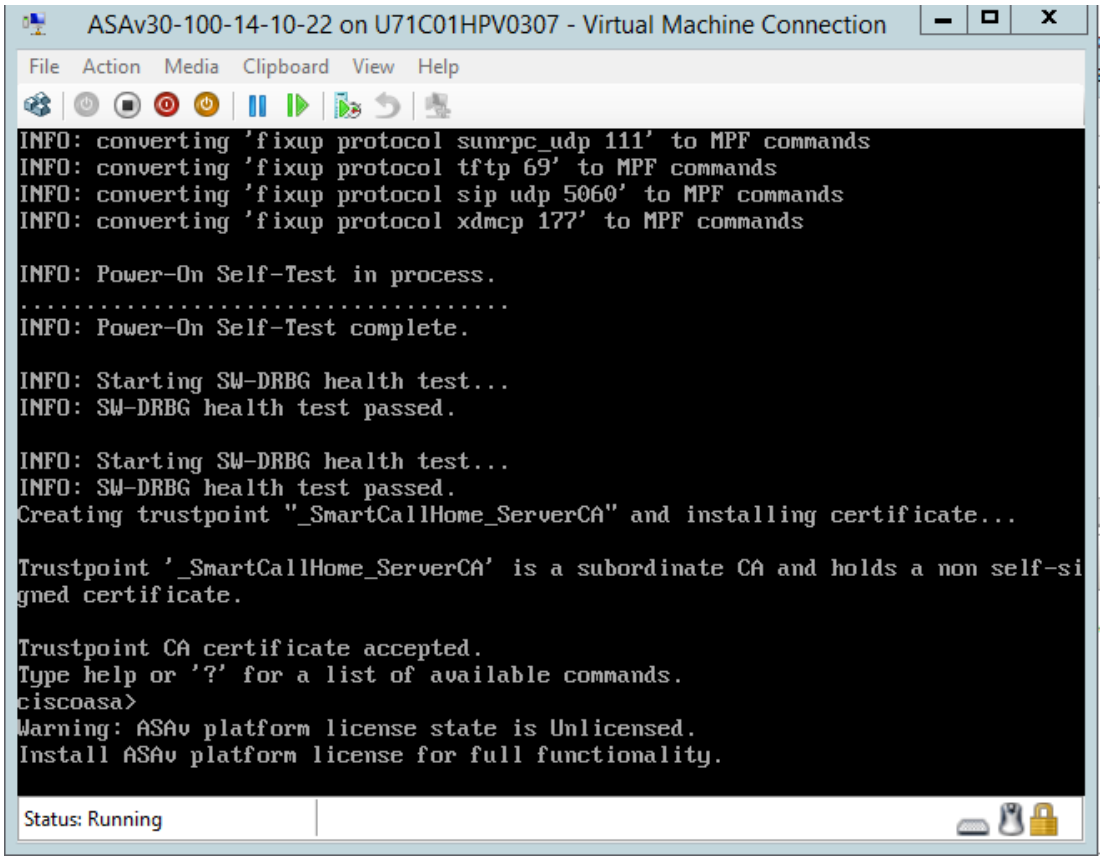
8. Virtual Machines(가상 시스템) 메뉴에서 목록의 ASAv 이름을 마우스 오른쪽 버튼으로 클릭하고 **Connect(연결)**를 클릭하여 ASAv에 연결합니다. 중지된 ASAv에 대한 콘솔이 열립니다.



9. Virtual Machine Connection(가상 시스템 연결) 콘솔 창에서 청록색 Start(시작) 버튼을 클릭하여 ASAv를 시작합니다.



10. ASAv의 부팅 진행 상황이 콘솔에 표시됩니다.



Hyper-V Manager에서 네트워크 어댑터 추가

새로 구축된 ASAv에는 네트워크 어댑터가 1개뿐입니다. 네트워크 어댑터를 2개 이상 추가해야 합니다. 여기서는 내부 네트워크 어댑터를 추가하고 있습니다.

시작하기 전에

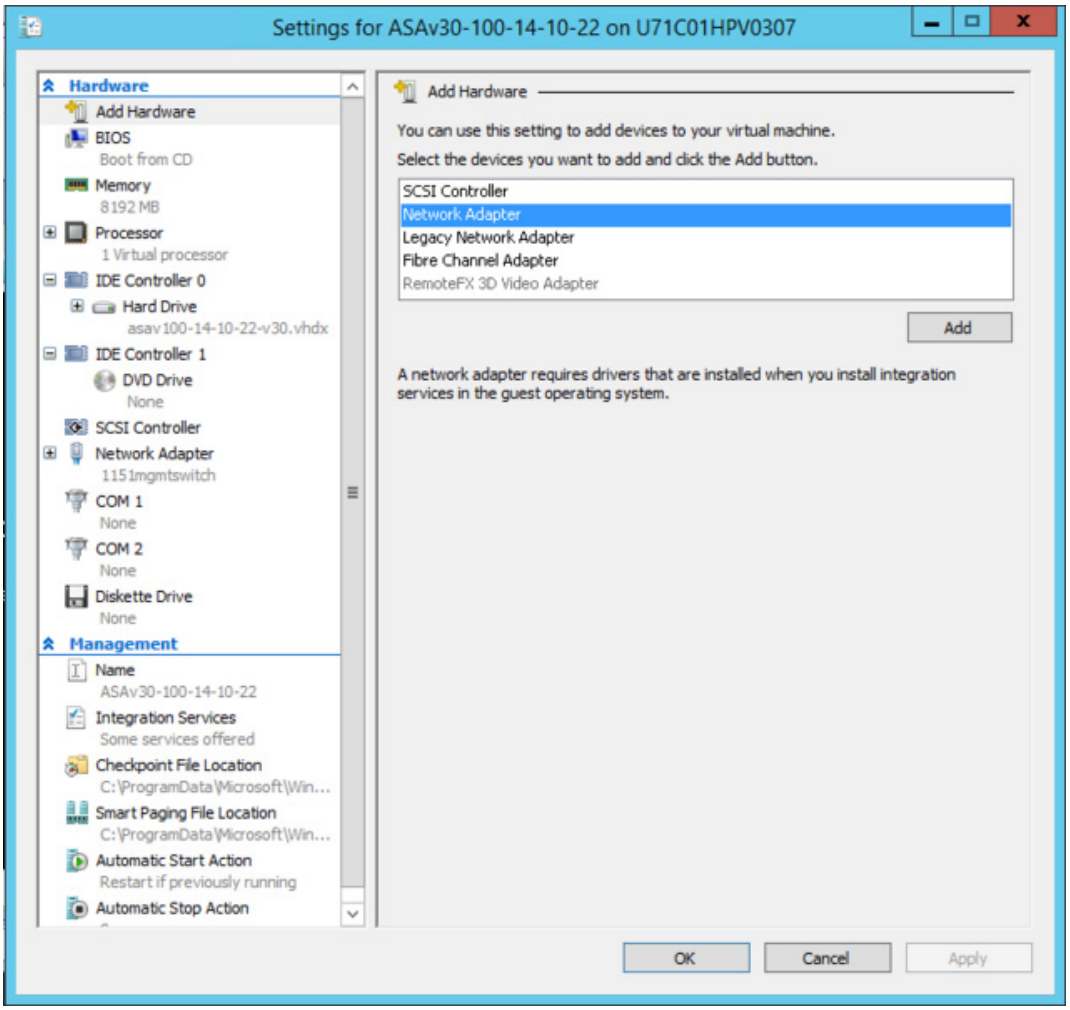
- ASAv는 off(꺼짐) 상태여야 합니다.

절차

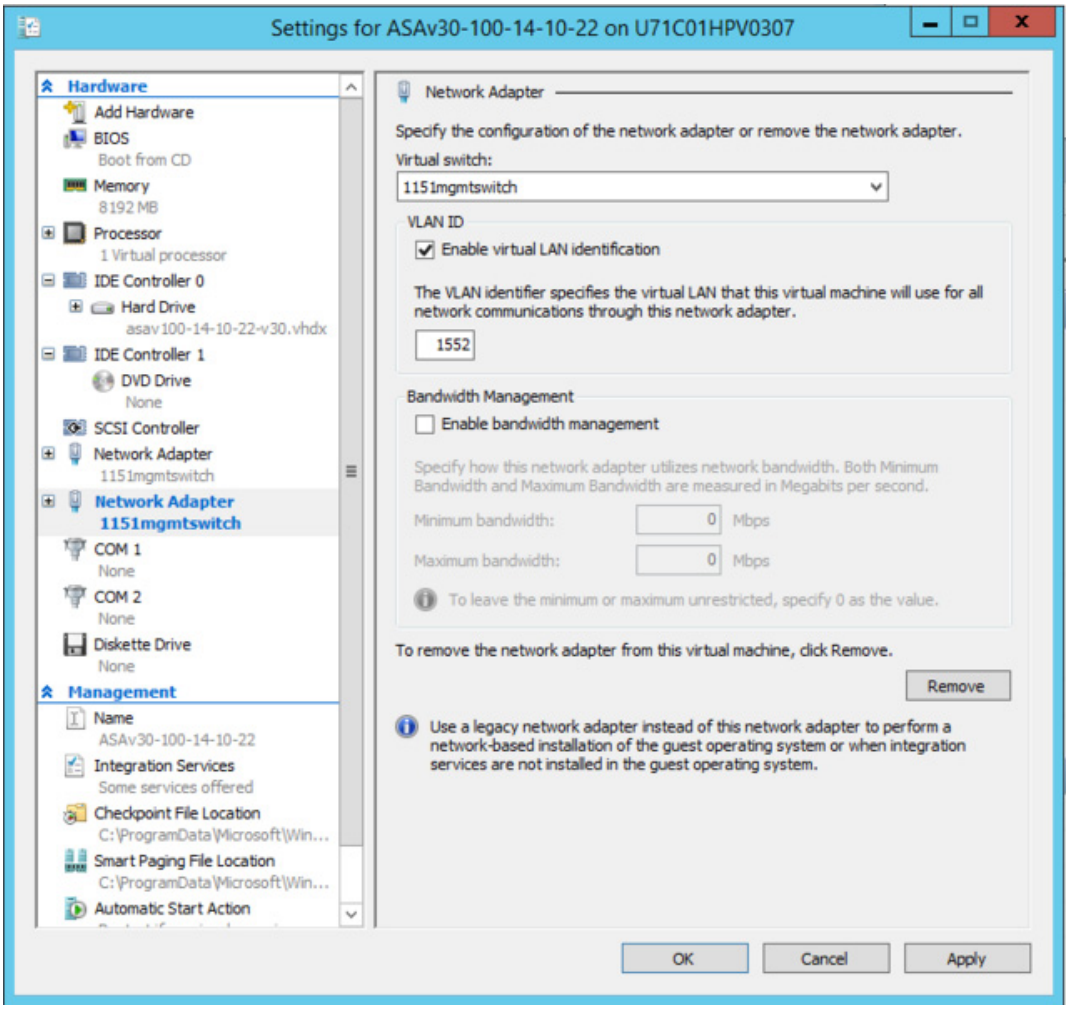
1. Hyper-V Manager의 오른쪽에 있는 **Settings(설정)**를 클릭합니다. Settings(설정) 대화 상자가 열립니다. 왼쪽의 Hardware(하드웨어) 메뉴에서 **Add Hardware(하드웨어 추가)**를 클릭하고 **Network Adapter(네트워크 어댑터)**를 클릭합니다.

   참고: 레거시 네트워크 어댑터는 사용하지 마십시오.

Hyper-V Manager에서 네트워크 어댑터 추가



2. 네트워크 어댑터가 추가된 다음 가상 스위치 및 기타 기능을 수정할 수 있습니다. 필요하다면 여기서 VLAN ID도 설정할 수 있습니다.



네트워크 어댑터 이름 수정

Hyper-V에서는 일반 네트워크 인터페이스 이름인 'Network Adapter'가 사용됩니다. 네트워크 인터페이스가 모두 동일한 이름일 경우 혼동될 수 있습니다. Hyper-V Manager를 사용하여 이름을 수정할 수 없습니다. Windows Powershell 명령을 사용하여 수정해야 합니다.

예

```
$NICRENAME= Get-VMNetworkAdapter -VMName 'ASAvVM' -Name "Network Adapter"
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[0] -newname inside
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[1] -newname outside
```

MAC 주소 스푸핑 구성

ASAv가 투명 모드에서 패킷을 전달하려면 그리고 HA 액티브/스탠바이 페일오버를 위해서는 모든 인터페이스에 대해 MAC 주소 스푸핑을 활성화해야 합니다. 이는 Hyper-V Manager에서 또는 Powershell 명령을 사용하여 수행할 수 있습니다.

Hyper-V Manager를 위한 절차

1. Hyper-V Manager의 오른쪽에 있는 **Settings(설정)**를 클릭합니다. Settings(설정) 대화 상자가 열립니다. 왼쪽의 Hardware(하드웨어) 메뉴에서 **Inside(내부)**를 클릭하고 메뉴를 확장한 다음 **Advanced Features(고급 기능)**를 클릭하여 MAC 주소 옵션으로 이동합니다. **Enable MAC address spoofing(MAC 주소 스푸핑 활성화)** 라디오 버튼을 클릭합니다.
2. 외부 인터페이스에 대해 1단계를 반복합니다.

Powershell 명령

```
Set-VMNetworkAdapter -VMName $vm_name\
-ComputerName $computer_name -MacAddressSpoofing On\
-VMNetworkAdapterName $network_adapter\r"
```

SSH 구성

Hyper-V Manager의 Virtual Machine Connection(가상 시스템 연결)에서 관리 인터페이스를 통한 SSH 액세스를 위해 ASAv를 구성할 수 있습니다. Day 0 컨피그레이션 파일을 사용하는 경우 여기에 SSH 액세스를 추가할 수 있습니다. 자세한 내용은 Day 0 컨피그레이션 파일 준비, 41페이지를 참조하십시오.

절차

1. RSA 키 쌍이 있음을 확인합니다.

   ```
   asav# show crypto key mypubkey rsa
   ```

2. RSA 키 쌍이 없을 경우 RSA 키 쌍을 생성합니다.

   ```
   asav(conf t)# crypto key generate rsa modulus 2048
   ```

   예

   ```
   asav((conf t)#
   username test password test123 privilege 15
   aaa authentication ssh console LOCAL
   ssh 10.7.24.0 255.255.255.0 management
   ssh version 2
   ```

3. 다른 PC에서 SSH를 사용하여 ASAv에 액세스할 수 있음을 확인합니다.

ASAv 구성

ASAv 구축에서는 ASDM 액세스를 사전에 구성합니다. 웹 브라우저를 사용하여 구축 중에 지정한 클라이언트 IP 주소에서 ASAv 관리 IP 주소에 연결할 수 있습니다. 이 장에서는 다른 클라이언트에서 ASDM에 액세스하도록 허용하는 방법 및 CLI 액세스(SSH 또는 텔넷)를 허용하는 방법에 대해서도 설명합니다. 이 장에서 다루는 그 밖의 필수 컨피그레이션 작업에는 ASDM에서 마법사를 통해 제공되는 라이센스 설치 및 일반 컨피그레이션 작업이 포함됩니다.

- ASDM 시작, 55페이지
- ASDM을 사용하여 초기 컨피그레이션 수행, 56페이지
- 지능형 컨피그레이션, 57페이지

ASDM 시작

절차

1. ASDM 클라이언트로 지정한 PC에서 다음 URL을 입력합니다.

   https://*asa_ip_address***/admin**

   다음 버튼과 함께 ASDM 시작 페이지가 나타납니다.

   - **Install ASDM Launcher and Run ASDM(ASDM 시작 관리자 설치 및 ASDM 실행)**
   - **Run ASDM(ASDM 실행)**
   - **Run Startup Wizard(시작 마법사 실행)**

2. Launcher를 다운로드하려면 다음을 수행합니다.

   a. **Install ASDM Launcher and Run ASDM(ASDM Launcher 설치 및 ASDM 실행)**을 클릭합니다.

   b. 사용자 이름 및 비밀번호 필드를 비워 두고(신규 설치) **OK(확인)**를 클릭합니다. 어떤 HTTPS 인증도 구성되지 않았으므로 사용자 이름 없이, **enable** 비밀번호(기본적으로 비어 있음)를 사용하여 ASDM에 액세스할 수 있습니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

   c. 설치 프로그램을 PC에 저장한 다음 시작합니다. 설치가 완료되면 ASDM-IDM Launcher가 자동으로 열립니다.

   d. 관리 IP 주소를 입력하고 사용자 이름과 비밀번호는 비워 둔 다음(새로운 설치의 경우) **OK(확인)**를 클릭합니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

3. Java Web Start를 사용하려면

   a. **Run ASDM(ASDM 실행)** 또는 **Run Startup Wizard(시작 마법사 실행)**를 클릭합니다.

   b. 메시지가 표시되면 PC에 바로 가기를 저장합니다. 저장하지 않고 열 수도 있습니다.

   c. 바로 가기에서 Java Web Start를 시작합니다.

   d. 표시되는 대화 상자에 따라 모든 인증서를 적용합니다. Cisco ASDM-IDM Launcher가 나타납니다.

   e. 사용자 이름과 비밀번호를 비어 있는 상태로 두고(새로 설치하는 경우) **OK(확인)**를 클릭합니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

ASDM을 사용하여 초기 컨피그레이션 수행

다음 ASDM 마법사 및 절차를 사용하여 초기 컨피그레이션을 수행할 수 있습니다. CLI 컨피그레이션은 CLI 컨피그레이션 가이드를 참조하십시오.

- Startup Wizard(시작 마법사) 실행, 56페이지
- (선택 사항) ASAv 뒤에 있는 공용 서버에 대한 액세스 허용, 56페이지
- (선택 사항) VPN 마법사 실행, 56페이지
- (선택 사항) ASDM에서 다른 마법사 실행, 57페이지

Startup Wizard(시작 마법사) 실행

구축에 맞게 보안 정책을 사용자 정의할 수 있도록 **Startup Wizard(시작 마법사)**를 실행합니다(**Wizards(마법사) > Startup Wizard(시작 마법사)** 선택). Startup Wizard(시작 마법사)를 사용하여 다음을 설정할 수 있습니다.

- 호스트 이름
- 도메인 이름
- 관리 비밀번호
- 인터페이스
- IP 주소
- 정적 경로
- DHCP 서버
- NAT(Network Address Translation) 규칙
- 그 외 기타

(선택 사항) ASAv 뒤에 있는 공용 서버에 대한 액세스 허용

Configuration(컨피그레이션) > Firewall(방화벽) > Public Servers(공용 서버) 창에서는 인터넷을 통해 내부 서버에 액세스할 수 있도록 하는 보안 정책을 자동으로 구성합니다. 비즈니스 소유자는 웹 및 FTP 서버 등 외부 사용자가 사용할 수 있도록 해야 하는 내부 네트워크 서비스를 운영할 수 있습니다. 이러한 서비스를 ASAv 뒤에 있는 DMZ(Demilitarized Zone)라는 별도의 네트워크에 둘 수 있습니다. 공용 서버를 DMZ에 두면 공용 서버에 대해 실행된 어떤 공격도 내부 네트워크에 영향을 주지 않습니다.

(선택 사항) VPN 마법사 실행

다음 마법사를 사용하여 VPN을 구성할 수 있습니다(**Wizards(마법사) > VPN Wizards(VPN 마법사)**).

- Site-to-Site VPN Wizard(사이트 대 사이트 VPN 마법사) - 두 ASAv 사이에 IPsec 사이트 대 사이트 터널을 만듭니다.
- AnyConnect VPN Wizard(AnyConnect VPN 마법사) - Cisco AnyConnect VPN 클라이언트에 대한 SSL VPN 원격 액세스를 구성합니다. AnyConnect는 회사 리소스에 대한 완전한 VPN 터널링을 통해 원격 사용자에게 ASA에 대한 보안 SSL 연결을 제공합니다. 원격 사용자가 브라우저를 통해 처음 연결할 때 AnyConnect 클라이언트를 다운로드하도록 ASA 정책을 구성할 수 있습니다. AnyConnect 3.0 이상을 사용하면 클라이언트에서 SSL 또는 IPsec IKEv2 VPN 프로토콜을 실행할 수 있습니다.
- Clientless SSL VPN Wizard(클라이언트리스 SSL VPN 마법사) - 브라우저에 대한 클라이언트리스 SSL VPN 원격 액세스를 구성합니다. 클라이언트리스 브라우저 기반 SSL VPN을 통해 사용자는 웹 브라우저를 사용하여 ASA에 보안 원격 액세스 VPN 터널을 설정할 수 있습니다. 사용자는 인증 후 포털 페이지에 액세스하여 지원되는 특정 내부 리소스에 액세스할 수 있습니다. 네트워크 관리자는 사용자 그룹별로 리소스에 대한 액세스를 제공합니다. ACL을 적용하여 특정 회사 리소스에 대한 액세스를 제한하거나 허용할 수 있습니다.
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard(IPsec(IKEv1 또는 IKEv2) 원격 액세스 VPN 마법사) - Cisco IPsec 클라이언트에 대한 IPsec VPN 원격 액세스를 구성합니다.

(선택 사항) ASDM에서 다른 마법사 실행

- High Availability and Scalability Wizard(고가용성 및 확장성 마법사) - 장애 조치 또는 VPN 로드 밸런싱을 구성합니다.
- Packet Capture Wizard(패킷 캡처 마법사) - 패킷 캡처를 구성하고 실행합니다. 이 마법사는 인그레스(ingress) 및 이그레스(egress) 인터페이스 각각에서 하나의 패킷 캡처를 실행합니다. 패킷 캡처가 완료되면 패킷 분석기에서 검사하고 재생하기 위해 패킷 캡처를 PC에 저장할 수 있습니다.

지능형 컨피그레이션

ASAv를 계속 구성하려면 Cisco ASA Series 설명서 탐색을 참조하십시오.

지능형 컨피그레이션