Cisco Content Security Virtual Appliance 설치 가이드

최종 업데이트: 2016년, 6월 17일

목차

Cisco Content Security Virtual Appliance 정보

Cisco Content Security Virtual Appliance는 물리적 이메일 보안, 웹 보안 또는 콘텐츠 보안 관리 하드웨어 어플라이언스와 기능이 동일하며, Cisco Content Security Virtual Appliance 관리, 17페이지에 문서화된 몇 가지 사소한 차이점만 있습니다.

Cisco Systems, Inc.
www.cisco.com

KVM 구축 시 지원되는 가상 어플라이언스 모델 및 AsyncOS 릴리스

제품	AsyncOS 릴리스	모델	디스크 공간	RAM	프로세서 코어
Cisco Web Security Virtual Appliance	AsyncOS 8.6 이상	**S000V**	250GB	4096MB	1
		S100V	250GB	6144MB	2
		S300V	1024GB	8192MB	4

VMware ESXi 구축을 위한 가상 어플라이언스 모델

참고 **AsyncOS 자료에 명시적으로 언급된 경우를 제외하고 OVF에 정의된 ESXi 컨피그레이션의 수정은 지원되지 않습니다.**

Cisco Content Security Virtual Appliance OVF 이미지는 다음 표의 값으로 사전 구성되었습니다.

제품	모델	디스크 공간	메모리	프로세서 코어
Cisco Email Security Virtual Appliance	**C000V** (평가 및 데모에만 해당)	200GB	4GB	1
	C100V	200GB	6GB	2
	C300V	500GB	8GB	4
	C600V	500GB	8GB	8
Cisco Web Security Virtual Appliance	**S000V**	250GB	4GB	1
	S100V	250GB	6GB	2
	S300V	1024GB	8GB	4
Cisco Content Security Management Virtual Appliance	**M000V**	250GB	4GB	1
	M100V	250GB	6GB	2
	M300V	1024GB	8GB	4
	M600V	2032GB	8GB	8

AsyncOS 버전 요건은 지원되는 VMWare ESXi 하이퍼바이저, 4페이지에 설명되어 있습니다.

시스템 요건

KVM 구축

다음은 KVM 구축에 적합한 환경입니다. 모든 구축에 디스크 스도리지로 씬 프로비저닝을 사용합니다.

Red Hat Enterprise Linux Server

Host OS:

- Red Hat Enterprise Linux Server 7.0

  (Red Hat Enterprise Virtualization 및 Red Hat OpenStack 플랫폼은 지원되지 않습니다.)

버전 정보:

- Linux: 3.10.0-123.13.2.el7.x86_64
- libvirt/QEMU:

  라이브러리에 대해 컴파일: libvirt 1.1.1

  라이브러리 사용: libvirt 1.1.1

  API 사용: QEMU 1.1.1

  하이퍼바이저 실행: QEMU 1.5.3

하드웨어:

- 적합성: UCS B200 M3
- Redhat 7.0 인증 UCS 플랫폼: https://access.redhat.com/search/browse/certified-hardware/#?&col=portal_certified_hardware&language=All&portal_certification_version=Red+Hat+Enterprise+Linux+7&portal_vendor=Cisco

Ubuntu Server

호스트 OS:

- Ubuntu Server 14.04.1 LTS(최신 업데이트)

버전 정보:

- Linux: 3.13.0-43-generic
- Virsh/QEMU

  라이브러리에 대해 컴파일: libvirt 1.2.2

  라이브러리 사용: libvirt 1.2.2

  API 사용: QEMU 1.2.2

  하이퍼바이저 실행: QEMU 2.0.0

하드웨어:

- 적합성: UCS B200 M3
- Ubuntu 14.04 인증 UCS 플랫폼: http://www.ubuntu.com/certification/server/make/Cisco%20UCS/?query=&level=Certified&release=14.04+LTS

KVM 드라이버

지원되는 KVM 드라이버:

- CDROM: IDE CDROM
- 네트워크: E1000, Virtio
- 디스크: VirtIO

KVM 패키지

호스트에 설치할 필수/관련 KVM 패키지:

- qemu-kvm
- qemu-img
- libvirt
- libvirt-python
- libvirt-client
- virt-manager(X-windows 필요)
- virt-install

VMware ESXi 구축

지원되는 VMWare ESXi 하이퍼바이저

AsyncOS 버전	VMware ESXi 버전
AsyncOS 9.x(이메일) AsyncOS 9.x (관리) AsyncOS 8.7 이상(웹)	5.0, 5.1 및 5.5
AsyncOS 8.5(웹) AsyncOS 8.4(관리)	5.0 및 5.1
AsyncOS 8.5.x(이메일) AsyncOS 8.0.x(웹)	4.x, 5.0 및 5.1
AsyncOS 8.0(이메일) AsyncOS 7.7.5(웹)	4.x 및 5.0

기타 VMware 하이퍼바이저는 "최선의 노력"으로 지원됩니다. 즉, Cisco에서 최선을 다해 지원하지만 모든 문제를 재현하지 못할 수도 있으며 Cisco에서 해결을 보장할 수 없습니다.

VMware ESXi 구축을 위한 하드웨어 요구 사항

Cisco UCS Server(블레이드 또는 랙 마운트)는 지원되는 유일한 하드웨어 플랫폼입니다.

가상 어플라이언스를 호스트하는 서버의 최소 요구 사항:

- 각각 최소 1.5GHz의 64비트 x86 프로세서 2개
- 물리적 RAM 8GB
- 10k RPM SAS 하드 드라이브 디스크

기타 하드웨어 플랫폼은 "최선의 노력"으로 지원됩니다. 즉, 최선을 다해 지원하지만 모든 문제를 재현하지 못할 수도 있으며 해결을 보장할 수 없습니다.

참고 설명서에 명시적으로 언급된 경우를 제외하면 Cisco에서는 어플라이언스의 CPU 코어 또는 RAM 크기 변경이나 IP 인터페이스 제거와 같은 Cisco Content Security Virtual Appliance의 하드웨어 컨피그레이션 변경을 지원하지 않습니다. 이러한 변경 사항이 있는 경우 어플라이언스에서경고를 전송할 수 있습니다.

(호스팅되는 Email Security에만 해당) FlexPod 솔루션으로 구축

AsyncOS for Email 릴리스 8.5 이상:

가상 Email Security 어플라이언스를 FlexPod 솔루션의 일부로 구축하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/white-paper-c11-731731.pdf를 참조하십시오. CCO 로그인에 따라 이 문서에 액세스할 수 있는지 여부가 결정됩니다.

FlexPod에 대한 일반 정보는 http://www.cisco.com/en/US/netsol/ns1137/index.html을 참조하십시오.

FlexPod는 가상 Web Security 어플라이언스 또는 가상 Content Security Management 어플라이언스 구축에 적용되지 않습니다.

(VMware ESXi 4.x에서 구축하는 경우에만 해당) 새 데이터스토어 만들기

VMWare ESXi 버전 4.x는 최대 1TB의 가상 디스크 이미지를 지원하는 4MB의 기본 블록 크기를 가지는 파일 시스템으로 제공됩니다. 하지만 더 큰 Cisco 가상 보안 어플라이언스(예: S300V, C600V)에는 1TB 이상의 디스크 공간이 필요합니다. 이러한 모델을 실행하려면 새 데이터 저장소를 만들고 8MB 이상의 블록 크기로 포맷해야 합니다.

블록 크기에 대한 정보와 새 데이터 저장소를 만드는 방법에 대해서는 http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003565에서 VMware의 기술 문서를 참조하십시오.

콘텐츠 보안 이미지 및 파일 준비

구축에 가장 적합한 크기의 가상 어플라이언스 이미지 확인

요구 사항에 맞는 가장 적합한 크기의 가상 어플라이언스를 확인합니다. 다음 위치에서 제공되는 자료에서 제품의 데이터 시트를 참조하십시오.

어플라이언스	데이터 시트 링크
ESA	다음 페이지에서 "Cisco Email Security Appliance Data Sheet" 링크를 참조하십시오. http://www.cisco.com/c/en/us/products/security/email-security-appliance/datasheet-listing.html 데이터 시트에서 "Email Security Virtual Appliance Specifications"라는 제목의 표를 참조하십시오.
WSA	다음 페이지에서 "Cisco Web Security Appliance Data Sheet" 링크를 참조하십시오. http://www.cisco.com/c/en/us/products/security/web-security-appliance/datasheet-listing.html 데이터 시트에서 "Cisco WSAV"라는 제목의 표를 참조하십시오.
SMA	다음 페이지에서"Cisco Content Security Management Appliance Data Sheet" 링크를 참조하십시오. http://www.cisco.com/c/en/us/products/security/content-security-management-appliance/datasheet-listing.html 데이터 시트에서 "Cisco SMAV"라는 제목의 표를 참조하십시오.

Cisco Content Security Virtual Appliance 이미지 다운로드

시작하기 전에

- Cisco에서 가상 어플라이언스용 라이센스를 구입합니다.
- 구축에 가장 적합한 크기의 가상 어플라이언스 이미지 확인, 6페이지를 참조하십시오.

단계 1 가상 어플라이언스에 해당하는 Cisco 소프트웨어 다운로드 페이지로 이동합니다.

- 이메일 보안:
  https://software.cisco.com/download/release.html?mdfid=284900944&flowid=41782&softwareid=282975113&release=9.1.0&relind=AVAILABLE&rellifecycle=ED&reltype=latest
- 웹 보안:
  https://software.cisco.com/download/release.html?mdfid=284806698&flowid=41610&softwareid=282975114&release=8.6.0&relind=AVAILABLE&rellifecycle=&reltype=latest
- 콘텐츠 보안 관리:
  https://software.cisco.com/download/release.html?mdfid=286283259&flowid=72402&softwareid=286283388&release=9.0&relind=AVAILABLE&rellifecycle=GD&reltype=latest

단계 2 왼쪽 탐색 창에서 AsyncOS 버전을 선택합니다.

단계 3 다운로드할 가상 어플라이언스 모델 이미지의 **Download(다운로드)**를 클릭합니다.

단계 4 로컬 시스템에 이미지를 저장합니다.

관련 항목

- KVM에서 구축, 7페이지
- VMware ESXi에서 구축, 11페이지

시작 시 로드할 라이센스 및 컨피그레이션 파일 준비(KVM 구축)

이 기능은 AsyncOS 8.6 for Cisco Web Security Appliances에 도입되었습니다. 다른 콘텐츠 보안 어플라이언스 또는 다른 AsyncOS 릴리스에는 이 기능이 제공되지 않습니다.

Cisco 어플라이언스를 처음 시작할 때 Cisco Content Security Virtual Appliance 라이센스 및 컨피그레이션 파일을 자동으로 로드할 수 있습니다. (이러한 파일은 최초 시작 후에는 로드되지 않습니다.)

단계 1 라이센스 및/또는 컨피그레이션 파일을 가져오고 이름을 설정합니다.

- 컨피그레이션 파일: `config.xml`
- 라이센스 파일: `license.xml`

단계 2 이러한 파일 중 하나 또는 두 가지를 모두 포함하는 ISO 이미지를 만듭니다.

향후 작업

AsyncOS .QCOW 이미지를 구축할 경우, ISO를 가상 머신 인스턴스에 가상 CD-ROM 드라이브로 연결해야 합니다.

시작 후에는 Cisco Virtual Appliance의 상태 로그를 확인할 수 있습니다. 이러한 기능과 관련된 오류 메시지에는 "ZERO" 키워드가 포함됩니다.

관련 항목

- KVM에서 구축, 7페이지

KVM에서 구축

	작업	추가 정보
단계 1	장비 및 소프트웨어가 모든 시스템 요건에 부합하는지 확인합니다.	시스템 요건, 2페이지 및 사용하려는 제품과 툴 설명서를 참조하십시오.
단계 2	AsyncOS 릴리스의 릴리스 정보를 검토하십시오.	릴리스 정보는 추가 정보, 22페이지의 위치에서 제공됩니다.
단계 3	UCS 서버, 호스트 OS, KVM을 설정합니다.	사용할 제품 및 툴의 설명서를 참조하십시오.

	작업	추가 정보
단계 4	가상 콘텐츠 보안 어플라이언스 이미지를 다운로드합니다.	Cisco Content Security Virtual Appliance 이미지 다운로드, 6페이지를 참조하십시오.
단계 5	Cisco 이미지가 구축과 호환되는지 확인합니다.	가상 어플라이언스 이미지가 KVM 구축과 호환되는지 확인, 8페이지를 참고하십시오.
단계 6	(선택 사항) 시작 시 자동으로 로드되는 라이센스 및 컨피그레이션 파일이 포함된 ISO 파일을 준비합니다.	시작 시 로드할 라이센스 및 컨피그레이션 파일 준비(KVM 구축), 7페이지를 참조하십시오.
단계 7	가상 어플라이언스 모델에 할당할 RAM 용량 및 CPU 코어 수를 확인합니다.	KVM 구축 시 지원되는 가상 어플라이언스 모델 및 AsyncOS 릴리스, 2페이지를 참조하십시오.
단계 8	가상 콘텐츠 보안 어플라이언스 이미지를 구축합니다.	다음 방법 중 하나를 사용합니다. • Virtual Machine Manager를 사용하여 가상 어플라이언스 구축, 8페이지 • virt-install을 사용하여 가상 어플라이언스 구축: 예, 10페이지
단계 9	AsyncOS 8.5 for Cisco Web Security Appliances에 도입된 고가용성 기능을 구축할 경우, 호스트에서 이 기능을 지원하도록 구성합니다.	(선택 사항) 고가용성을 지원하도록 가상 어플라이언스 구성, 11페이지를 참조하십시오.
단계 10	처음 시작 시 라이센스 및 컨피그레이션 파일을 로드하도록 시스템을 구성하지 않은 경우 • 가상 어플라이언스 라이센스 파일 설치 • 기능 라이센스 설치 • Cisco Content Security Virtual Appliance 구성	• 가상 어플라이언스 라이센스 파일을 설치하려면 가상 어플라이언스 라이센스 파일 설치, 14페이지를 참조하십시오. • 기능 라이센스를 설치하고 어플라이언스를 구성하려면 AsyncOS 릴리스의 사용 설명서 또는 온라인 도움말을 참조하십시오.
단계 11	라이센스 만료가 가까워지면 경고를 보내도록 어플라이언스를 구성합니다.	AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오.

가상 어플라이언스 이미지가 KVM 구축과 호환되는지 확인

Cisco 이미지의 qcow 버전은 1.1 이하의 QEMU 버전과 호환되지 않습니다. QEMU 버전이 1.1 이하인 경우 이미지를 변환하여 구축과 호환될 수 있도록 해야 합니다.

Virtual Machine Manager를 사용하여 가상 어플라이언스 구축

단계 1 virt-manager 애플리케이션을 실행합니다.

단계 2 **New(새로 만들기)**를 선택합니다.

단계 3 가상 어플라이언스의 고유한 이름을 입력합니다.

단계 4 **Import existing image(기존 이미지 가져오기)**를 선택합니다.

단계 5 **Forward(전달)**를 선택합니다.

단계 6 옵션을 입력합니다.

- OS 유형: **UNIX**
- 버전: **FreeBSD 8.X**

단계 7 다운로드한 가상 어플라이언스 이미지를 찾아 선택합니다.

단계 8 **Forward(전달)**를 선택합니다.

단계 9 구축하려는 가상 어플라이언스 모델의 RAM 및 CPU 값을 입력합니다.

KVM 구축 시 지원되는 가상 어플라이언스 모델 및 AsyncOS 릴리스, 2페이지를 참조하십시오.

단계 10 **Forward(전달)**를 선택합니다.

단계 11 **Customize(사용자 정의)** 체크 박스를 선택합니다.

단계 12 **Finish(마침)**를 선택합니다.

단계 13 디스크 드라이브를 구성합니다.

a. 왼쪽 창에서 드라이브를 선택합니다.

b. Advanced(고급) 옵션 아래에서 다음 옵션을 선택합니다.

- 디스크 버스: **Virtio**.
- 스토리지 형식: qcow2

c. **Apply(적용)**를 선택합니다.

단계 14 관리 인터페이스에 대해 네트워크 디바이스를 구성합니다.

a. 왼쪽 창에서 NIC를 선택합니다.

b. 옵션을 선택합니다.

- 소스 디바이스: 관리 VLAN
- 디바이스 모델: virtIO
- 소스 모드: VEPA

c. **Apply(적용)**를 선택합니다.

단계 15 4개의 추가 인터페이스에 대한 네트워크 디바이스를 구성합니다(WSA에만 해당).

사용할 각 인터페이스에 대해 이전 하위 단계 집합을 반복합니다.

단계 16 시작 시 로드할 라이센스 및 컨피그레이션 파일이 포함된 ISO 이미지가 준비된 경우 ISO를 가상 머신 인스턴스에 가상 CD-ROM 드라이브로 연결합니다.

단계 17 **Begin Installation(설치 시작)**을 선택합니다.

관련 항목

- KVM에서 구축, 7페이지

virt-install을 사용하여 가상 어플라이언스 구축: 예

시작하기 전에

어플라이언스에 필요한 RAM 용량 및 CPU 코어의 수를 확인합니다. KVM 구축 시 지원되는 가상 어플라이언스 모델 및 AsyncOS 릴리스, 2페이지를 참조하십시오.

절차

단계 1 가상 어플라이언스가 상주할 스토리지 풀을 만듭니다.

```
virsh pool-define-as --name vm-pool --type dir --target /home/username/vm-pool
virsh pool-start vm-pool
```

단계 2 스토리지 풀에 가상 어플라이언스 이미지를 복사합니다.

```
cd /home/yusername/vm-pool
tar xvf ~/asyncos-8-6-0-007-S100V.qcow2.tar.gz
```

단계 3 가상 어플라이언스를 설치합니다.

```
virt-install \
--virt-type kvm \
--os-type=unix \
--os-variant=freebsd8 \
--name wsa-example \ (이 이름은 고유해야 함)
--ram 6144 \ (가상 어플라이언스 모델에 적합한 값 사용)
--vcpus 2 \ (가상 어플라이언스 모델에 적합한 값 사용)
--noreboot \
--import \
--disk
path=/home/username/vm-pool/asyncos-8-6-0-007-S100V.qcow2,format=qcow2,bus=virtio \
--disk path=/home/username/vm-pool/wsa.iso,bus=ide,device=cdrom \ (시작 시 로드할 라이센스 및 컨피그레이션 파일이 포함된 ISO를 만든 경우)
--network type=direct,source=enp6s0.483,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.484,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.485,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.486,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.487,source_mode=vepa,model=virtio
```

단계 4 가상 어플라이언스를 시작합니다.

```
virsh start wsa-example
```

관련 항목

- KVM에서 구축, 7페이지

(선택 사항) 고가용성을 지원하도록 가상 어플라이언스 구성

고가용성 기능은 AsyncOS 8.5 for Cisco Web Security Appliance에 도입되었으며 사용 설명서 및 온라인 도움말에 자세히 설명되어 있습니다.

Web Security 어플라이언스가 고가용성을 위해 페일오버 그룹에 추가된 경우, 페일오버 그룹의 어플라이언스가 멀티캐스팅을 사용하여 서로 통신할 수 있게 하기 위해 가상 어플라이언스가 무차별 모드를 사용하도록 구성합니다.

언제든 이 변경 사항을 적용할 수 있습니다.

단계 1 호스트 OS에서 멀티캐스트 트래픽을 연결할 인터페이스와 연결된 `macvtap` 인터페이스를 찾습니다.

단계 2 무차별 모드를 사용하도록 `macvtap` 인터페이스를 설정합니다.

호스트에 다음과 같이 입력합니다. `ifconfig macvtapX promisc`

관련 항목

- KVM에서 구축, 7페이지

VMware ESXi에서 구축

	작업	추가 정보
1.	AsyncOS 릴리스의 릴리스 정보를 검토하십시오.	릴리스 정보는 추가 정보, 22페이지의 위치에서 제공됩니다.
2.	Cisco에서 가상 어플라이언스 이미지 및 MD5 해시를 다운로드합니다.	어플라이언스 이미지의 데이터 무결성을 검사하려면 MD5 해시가 필요합니다. 콘텐츠 보안 이미지 및 파일 준비, 6페이지
3.	ESXi 호스트 또는 클러스터에 가상 어플라이언스를 구축합니다.	가상 어플라이언스 구축, 12페이지
4.	(선택 사항) 네트워크에서 여러 개의 가상 어플라이언스를 실행하려는 경우에는 이미지를 복제합니다.	(선택 사항) 가상 어플라이언스 복제, 12페이지
5.	연결이 간헐적으로 끊기는 문제를 방지합니다.	가상 머신에서 사용되지 않는 NIC(네트워크 인터페이스 카드)를 사용하지 않도록 설정합니다.
6.	Cisco Content Security Virtual Appliance에서 임의의 실패를 방지하기 위해 가상 머신에서 동기화를 구성합니다.	중요! 임의 실패 방지, 13페이지
7.	DHCP를 사용할 수 없으면 네트워크에서 어플라이언스를 설정합니다.	DHCP를 사용할 수 없는 경우 네트워크에서 어플라이언스 설정, 14페이지
8.	라이센스 파일을 설치합니다.	가상 어플라이언스 라이센스 파일 설치, 14페이지

	작업	추가 정보
9.	어플라이언스의 웹 UI에 로그인하고 물리적 어플라이언스를 구성할 때처럼 어플라이언스 소프트웨어를 구성합니다. 예를 들어, 다음이 가능합니다. • 시스템 설정 마법사를 실행 • 컨피그레이션 파일 업로드 • 수동으로 기능 구성	• 필요한 정보 수집을 포함하여 어플라이언스를 액세스하고 구성하는 방법은 추가 정보, 22페이지의 관련 위치에서 제공되는 AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오. • 물리적 어플라이언스에서 설정을 마이그레이션하려면 AsyncOS 릴리스에 대한 릴리스 정보를 참조하십시오. 해당 기능을 사용하도록 설정하기 전까지는 기능 키가 활성화되지 않습니다.
10.	라이센스 만료가 가까워지면 경고를 보내도록 어플라이언스를 구성합니다.	추가 정보, 22페이지의 관련 위치에서 제공되는 AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오.

(선택 사항) 가상 어플라이언스 복제

환경에서 여러 가상 보안 어플라이언스를 실행하는 경우:

- 가상 보안 어플라이언스를 처음 실행하기 전에 복제하는 것이 좋습니다.
- 가상 어플라이언스의 라이센스를 설치한 후 가상 보안 어플라이언스를 복제하면 라이센스가 강제로 만료됩니다. 이 경우 라이센스를 다시 설치해야 합니다.
- 복제하기 전에 가상 어플라이언스를 종료해야 합니다.
- 이미 사용 중인 가상 어플라이언스를 복제하려면 이미 사용 중인 가상 어플라이언스 복제, 16페이지에서 자세한 내용을 확인하십시오.

가상 머신 복제에 대한 자세한 내용은 http://www.vmware.com/support/ws55/doc/ws_clone.html에서 VMWare의 기술 문서를 참조하십시오.

관련 항목

- KVM에서 구축, 7페이지
- VMware ESXi에서 구축, 11페이지

가상 어플라이언스 구축

시작하기 전에

- 가상 어플라이언스를 구축할 ESXi 호스트 또는 클러스터를 설정합니다. 자세한 내용은 시스템 요건, 2페이지를 참조하십시오.
- 로컬 시스템에 VMware vSphere Client를 설치합니다.
- 콘텐츠 보안 이미지 및 파일 준비, 6페이지의 설명대로 이미지를 다운로드합니다.

단계 1 가상 어플라이언스의 .zip 파일을 `C:\vESA\C100V` 또는 `:\vWSA\S300V`와 같은 자체 디렉토리에 압축을 해제합니다.

단계 2 로컬 시스템에서 VMware vSphere Client를 엽니다.

단계 3 가상 어플라이언스를 구축할 ESXi 호스트 또는 클러스터를 선택합니다.

단계 4 **File(파일) > Deploy OVF template(OVF 템플릿 구축)**을 선택합니다.

단계 5 앞서 만든 디렉토리의 OVF 파일 경로를 입력합니다.

단계 6 **Next(다음)**를 클릭합니다.

단계 7 마법사를 완료합니다.

- 디스크 스토리지의 씬 프로비저닝은 하이퍼바이저 레이어에서 지원됩니다. 이 옵션을 선택한 경우 디스크 공간 및 성능이 저하될 수 있습니다.

참고 **AsyncOS 설명서에 명시적으로 언급된 경우를 제외하면 OVF에 정의된 ESXi 컨피그레이션의 수정은 지원되지 않습니다.**

관련 항목

- KVM에서 구축, 7페이지
- VMware ESXi에서 구축, 11페이지

중요! 임의 실패 방지

가상 머신에는 Cisco Content Security Virtual Appliance에서 임의 실패를 방지하기 위해 해결해야 하는 타이밍 문제가 내재되어 있습니다. 이 문제를 방지하려면 가상 머신에서 정확한 타임 스탬프 카운터 동기화를 사용하도록 설정합니다.

시작하기 전에

- 시간 유지 기본 사항, 가상 타임 스탬프 카운터 및 정확한 동기화에 대한 자세한 내용은 http://www.vmware.com/files/pdf/techpaper/Timekeeping-In-VirtualMachines.pdf에 있는 가상 머신에서 VMWare의 시간 유지 PDF를 참조하십시오.
- 사용 중인 vSphere 클라이언트 버전에 대한 지침은 아래 절차와 다를 수 있습니다. 아래 내용을 일반 지침으로 사용하고 필요에 따라 클라이언트용 설명서를 참조하십시오.

단계 1 vSphere Client의 시스템 목록에서 가상 어플라이언스를 선택합니다.

단계 2 가상 어플라이언스의 전원을 끕니다.

단계 3 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings(설정 편집)**를 선택합니다.

단계 4 **Options(옵션)** 탭을 클릭하고 **Advanced(고급) > General(일반)**을 선택합니다.

단계 5 **Configuration Parameters(컨피그레이션 매개변수)**를 클릭합니다.

단계 6 다음 매개변수를 편집하거나 추가합니다.

```
monitor_control.disable_tsc_offsetting=TRUE
monitor_control.disable_rdtscopt_bt=TRUE
timeTracker.forceMonotonicTTAT=TRUE
```

단계 7 설정 창을 닫고 어플라이언스를 실행합니다.

관련 항목

- KVM에서 구축, 7페이지
- VMware ESXi에서 구축, 11페이지

DHCP를 사용할 수 없는 경우 네트워크에서 어플라이언스 설정

참고 가상 보안 어플라이언스 이미지를 복제한 경우에는 각 이미지에 대해 다음 단계를 수행합니다.

단계 1 vSphere 클라이언트 콘솔에서 `interfaceconfig`를 실행합니다.

단계 2 가상 어플라이언스 관리 포트의 IP 주소를 기록합니다.

참고 관리 포트가 DHCP 서버에서 IP 주소를 가져옵니다. 어플라이언스가 DHCP 서버에 연결할 수 없는 경우에는 기본적으로 `192.168.42.42`를 사용합니다.

단계 3 `setgateway` 명령을 사용하여 기본 게이트웨이를 구성합니다.

단계 4 변경 사항을 커밋합니다.

참고 호스트 이름은 설치 마법사를 완료할 때까지 업데이트되지 않습니다.

관련 항목

- KVM에서 구축, 7페이지
- VMware ESXi에서 구축, 11페이지

가상 어플라이언스 라이센스 파일 설치

참고 가상 보안 어플라이언스 이미지를 복제한 경우에는 각 이미지에 대해 다음 단계를 수행합니다.

시작하기 전에

(선택 사항) 가상 어플라이언스에 FTP로 연결하여 라이센스 파일을 업로드합니다. 터미널에 라이센스를 붙여넣는 경우에는 이렇게 할 필요가 없습니다.

절차

단계 1 터미널 애플리케이션에서 SSH 또는 텔넷을 사용하여 어플라이언스의 CLI에 `admin/ironport` 사용자로 로그인합니다.

참고 vSphere 클라이언트 콘솔을 사용하여 라이센스 파일의 내용을 CLI에 붙여넣을 수 없습니다.

단계 2 `loadlicense` 명령을 실행합니다.

단계 3 다음 옵션 중 하나를 사용하여 라이센스 파일을 설치합니다.

- 옵션 1을 선택하고 라이센스 파일의 내용을 터미널에 붙여넣습니다.
- FTP를 사용하여 어플라이언스의 `configuration` 디렉토리에 라이센스 파일을 이미 업로드한 경우에는 옵션 2를 선택하고 `configuration` 디렉토리에서 로드 파일을 로드합니다.

단계 4 라이센스 계약서를 읽고 동의합니다.

단계 5 (선택 사항) `showlicense`를 실행하여 라이센스 세부 사항을 검토합니다.

다음 작업

KVM 구축의 경우

- KVM에서 구축, 7페이지 섹션으로 돌아갑니다.

ESXi 구축의 경우

- 관리 인터페이스의 IP 주소에 대한 자세한 내용은 VMware ESXi에서 구축, 11페이지를 참조하십시오.
- 가상 보안 어플라이언스 이미지를 복제한 경우에는 각 이미지에 이 주제의 절차를 반복합니다.
- VMware ESXi에서 구축, 11페이지에서 나머지 설정 단계를 참조하십시오.

가상 어플라이언스를 다른 물리적 호스트로 마이그레이션

VMware® VMotion™을 사용하여, 실행 중인 가상 어플라이언스를 다른 물리적 호스트로 마이그레이션할 수 있습니다.

요건:

- 두 물리적 호스트의 네트워크 컨피그레이션이 동일해야 합니다.
- 두 물리적 호스트 모두가 가상 어플라이언스의 인터페이스가 매핑된 동일한 정의 네트워크에 액세스할 수 있어야 합니다.
- 두 물리적 호스트 모두가 가상 어플라이언스가 사용하는 데이터 저장소에 액세스할 수 있어야 합니다. 이 데이터 저장소는 SAN(Storage Area Network)이거나 NAS(Network Attached Storage)일 수 있습니다.
- Email Security 가상 어플라이언스의 대기열에 메일이 없어야 합니다.

단계 1 VMotion 설명서를 활용하여 가상 머신을 마이그레이션합니다.

단계 2 마이그레이션 후 라이센스를 로드합니다.

이미 사용 중인 가상 어플라이언스 복제

시작하기 전에

- 가상 머신 복제에 대한 자세한 내용은 http://www.vmware.com/support/ws55/doc/ws_clone.html에서 VMWare의 기술 문서를 참조하십시오.
- 어플라이언스의 네트워크 설정 및 보안 기능을 관리하는 방법에 대해서는 Cisco Content Security 제품 및 릴리스의 사용 설명서를 참조하십시오.

단계 1 Email Security 가상 어플라이언스를 복제 중인 경우:
CLI에서 `suspend` 명령을 사용하여 어플라이언스를 일시 중지하고 어플라이언스가 대기열의 모든 메시지를 배달하기에 충분한 지연 시간을 입력합니다.

단계 2 Security Management 가상 어플라이언스를 복제 중인 경우
관리되는 Email 및 Web Security Appliance에서 중앙 집중식 서비스를 비활성화합니다.

단계 3 CLI에서 `shutdown` 명령을 사용하여 가상 어플라이언스를 종료합니다.

단계 4 가상 어플라이언스 이미지를 복제합니다.

단계 5 VMware vSphere Client를 사용하여 복제된 어플라이언스를 시작하고 다음을 수행합니다.

a. Cisco.com에서 다운로드한 수정되지 않은 .OVF 이미지 파일이 아닌 구성된 이미지를 복제한 경우

- 복제된 가상 어플라이언스에 라이센스 파일을 설치합니다.
- 복제된 가상 어플라이언스의 네트워크 설정을 수정합니다.

전원을 켤 때 네트워크 어댑터가 자동으로 연결되지 않습니다. IP 주소, 호스트 이름 및 IP 주소를 다시 구성합니다. 그런 다음 네트워크 어댑터의 전원을 켭니다.

기능 키를 설치할 때까지는 컨피그레이션이 완료되지 않습니다.

b. 복제된 Email Security 가상 어플라이언스의 경우:

- 격리에서 모든 메시지를 삭제합니다.
- 메시지 추적 및 보고 데이터를 삭제합니다.

c. 복제된 Web Security 가상 어플라이언스의 경우:

- 프록시 캐시를 지웁니다.
- CLI에서 `authcache > flushall` 명령을 사용하여 프록시 인증 캐시를 지웁니다.
- CLI에서 `diagnostic > reporting > deletedb` 명령을 사용하여 보고 및 추적 데이터를 제거합니다.
- Authentication Realms(인증 영역)의 경우 도메인에 다시 참가합니다.
- Authentication Settings(인증 설정)의 경우 리디렉션 호스트 이름을 수정합니다.
- 원래의 가상 어플라이언스가 Security Management 어플라이언스에 의해 관리되는 경우, 복제된 어플라이언스를 Security Management 어플라이언스에 추가합니다.

단계 6 VMware vSphere Client를 사용하여 원래 가상 어플라이언스를 시작하고 작업을 다시 시작합니다. 제대로 실행되고 있는지 확인합니다.

단계 7 복제된 어플라이언스에서 작업을 다시 시작합니다.

Cisco Content Security Virtual Appliance 관리

IP 주소

가상 어플라이언스의 전원을 처음 켤 때, 관리 포트는 DHCP 호스트에서 IP 주소를 가져옵니다. 가상 어플라이언스가 DHCP 서버에서 IP 주소를 가져올 수 없는 경우에는 `192.168.42.42`를 관리 인터페이스의 IP 주소로 사용합니다. 가상 어플라이언스에서 시스템 설정 마법사를 실행할 때 CLI에 관리 인터페이스의 IP 주소가 표시됩니다.

가상 어플라이언스 라이센스

참고 가상 어플라이언스 라이센스를 설치하기 전에는 기술 지원 터널을 열 수 없습니다. 기술 지원 터널에 대한 자세한 내용은 AsyncOS 릴리스의 사용 설명서를 참조하십시오.

Cisco Content Security Virtual Appliance의 경우 호스트에서 가상 어플라이언스를 실행하기 위한 추가적인 라이센스가 필요합니다. 이 라이센스는 여러 개의 복제된 가상 어플라이언스에 사용할 수 있습니다. 라이센스는 하이퍼바이저와 별개입니다.

AsyncOS for Web Security 8.5 이상, AsyncOS for Email Security 8.5.x 이상, AsyncOS for Security Management 8.4 이상 버전의 경우

- 개별 기능의 기능 키는 만료일이 각자 다릅니다.
- 가상 어플라이언스가 만료된 후 어플라이언스는 웹 프록시로서의 역할을 계속 수행하고(Web Security 어플라이언스), 메일을 전송하고(Email Security 어플라이언스), 180일 동안 보안 서비스 없이 격리된 메시지를 자동으로 처리합니다(Security Management 어플라이언스). 이 기간 중에는 보안 서비스가 업데이트되지 않습니다. Content Security Management 어플라이언스에서 관리자 및 최종 사용자는 격리를 관리할 수 없으나, 관리 어플라이언스는 관리되는 Email Security 어플라이언스에서 격리된 메시지를 계속 승인하며 격리된 메시지의 예약 삭제가 이루어집니다.

AsyncOS for Email Security 8.0 및 AsyncOS for Web Security 7.7.5, 8.0

- 기능 키는 가상 어플라이언스 라이센스의 일부로 포함됩니다. 기능 키는 기능이 활성화되지 않았더라도 라이센스와 동일한 시점에 만료됩니다. 새 기능 키를 구입하려면 새 가상 어플라이언스 라이센스 파일을 다운로드하고 설치해야 합니다.
- 기능 키가 가상 어플라이언스 라이센스에 포함되어 있으므로 AsyncOS 기능에는 평가 라이센스가 없습니다.

참고 AsyncOS 버전 되돌리기의 영향에 대한 자세한 내용은 AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오.

관련 항목

- 가상 어플라이언스 라이센스 파일 설치, 14페이지

강제 재설정, 전원 끄기, 재설정 옵션이 완전히 지원되지 않음

다음 작업은 하드웨어 어플라이언스에서 플러그를 뽑는 것과 동일하며 지원되지 않습니다. 특히 AsyncOS를 시작하는 동안에도 지원되지 않습니다.

- KVM의 경우, Force Reset(강제 재설정) 옵션입니다.
- VMware의 경우, Power Off(전원 끄기) 및 Reset(재설정) 옵션입니다. (이러한 옵션은 어플라이언스가 완전히 나타난 후에 안전하게 사용할 수 있습니다.)

가상 어플라이언스의 CLI 명령

Cisco Content Security Virtual Appliance에는 기존 CLI 명령에 대한 업데이트가 포함되며 가상 어플라이언스 전용 명령인 `loadlicense`가 포함됩니다. 다음의 CLI 명령이 변경되었습니다.

명령	가상 SMA에서 지원 여부	정보
loadlicense	예	가상 어플라이언스에 대한 라이센스를 설치할 수 있는 명령입니다. 이 명령을 먼저 사용하여 라이센스를 설치하지 않으면 가상 어플라이언스에서 시스템 설정 마법사를 실행할 수 없습니다.
etherconfig	—	가상 어플라이언스에는 페어링 옵션이 포함되지 않습니다.
version	—	이 명령은 UDI, RAID 및 BMC 정보를 제외하고 가상 어플라이언스에 대한 모든 정보를 반환합니다.
resetconfig	—	이 명령을 실행하면 가상 어플라이언스 라이센스 및 기능 키가 어플라이언스에 남겨집니다.
revert	—	AsyncOS 8.5 for Email Security 이후부터: 어플라이언스의 온라인 도움말 및 사용 설명서의 시스템 관리 장에서 동작에 대해 설명합니다.
reload	—	이 명령을 실행하면 가상 어플라이언스 라이센스 및 모든 기능 키가 어플라이언스에서 제거됩니다. 이 명령은 Web Security Appliance에만 사용할 수 있습니다.

diagnostic	—	다음의 `diagnostic > raid` 하위 메뉴 옵션은 정보를 반환하지 않습니다.
		`1. Run disk verify`
		`2. Monitor tasks in progress`
		`3. Display disk verify verdict`
		이 명령은 Email Security Appliance에만 사용할 수 있습니다.

showlicense	예	라이센스 세부 정보를 봅니다. Email 및 Web Security Appliance의 경우, `featurekey` 명령을 통해 추가 정보가 제공됩니다.

가상 어플라이언스의 SNMP

가상 어플라이언스의 AsyncOS는 하드웨어 관련 정보를 보고하지 않으며 하드웨어 관련 트랩도 생성되지 않습니다. 다음 정보가 쿼리에서 생략됩니다.

- `powerSupplyTable`
- `temperatureTable`
- `fanTable`
- `raidEvents`
- `raidTable`

트러블슈팅 및 지원

트러블슈팅: KVM 구축

재부팅 시 가상 어플라이언스 종료

문제 재부팅 시 가상 어플라이언스가 종료됩니다.

솔루션 이는 KVM 문제입니다. 호스트를 재부팅할 때마다 다음 해결책을 수행합니다.

단계 1 다음을 확인합니다.

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

단계 2 위의 값이 Y로 설정된 경우

a. 가상 어플라이언스를 중지하고 KVM 커널 모듈을 다시 설치합니다.

```
rmmod kvm_intel
modprobe kvm_intel enable_apicv=N
```

b. 가상 어플라이언스를 다시 시작합니다.

자세한 내용은 https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html 및 https://bugs.launchpad.net/qemu/+bug/1329956을 참조하십시오.

처음에는 네트워크 연결이 작동하다가 나중에 실패하는 경우

문제 이전에는 작동하던 네트워크 연결이 끊깁니다.

솔루션 이는 KVM 문제입니다. http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html의 OpenStack 설명서에서"KVM: Network connectivity works initially, then fails" 섹션을 참조하십시오.

성능 저하, 감시 문제, 높은 CPU 사용량

문제 어플라이언스 성능이 느리고, 감시 문제가 발생하며, Ubuntu 가상 머신에서 어플라이언스를 실행할 경우 CPU 사용량이 비정상적으로 높게 나타납니다.

솔루션 Ubuntu에서 최신 호스트 OS 업데이트를 설치합니다.

Linux 구축의 일반적인 트러블슈팅

문제 KVM 구축에서 실행 중인 가상 어플라이언스에 대한 모든 문제

솔루션 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf에서 제공되는 *Virtualization Deployment and Administration Guide*에서 트러블슈팅 섹션 및 기타 정보를 참조하십시오.

트러블슈팅: VMware ESXi 구축

연결이 간헐적으로 끊기는 문제

문제 연결이 간헐적으로 끊깁니다.

솔루션 사용되지 않는 모든 NIC를 ESXi에서 사용하지 않도록 설정하십시오.

임의 실패

문제 명확한 원인이 없는 임의 실패가 발생합니다.

솔루션 중요! 임의 실패 방지, 13페이지를 참고하십시오.

가상 어플라이언스에 대한 지원 받기

참고 가상 어플라이언스에 대한 지원을 받으려면 Cisco TAC에 문의하거나 VLN(Virtual License Number) 번호를 준비하십시오.

Cisco Content Security Virtual Appliance에 대한 케이스를 제출할 경우, 계약 번호 및 PID(Product Identifier code)를 제시해야 합니다.

가상 어플라이언스에서 실행되는 소프트웨어 라이센스를 기반으로 PID를 식별할 수 있습니다. 구매 발주서를 참조하거나 다음 목록에서 확인할 수 있습니다.

- Virtual Email Security Appliance의 PID(Product Identifier Code), 21페이지
- Virtual Web Security Appliance의 PID(Product Identifier Code), 21페이지
- Virtual Content Security Management Appliance의 PID(Product Identifier Code), 22페이지

Virtual Email Security Appliance의 PID(Product Identifier Code)

기능	PID	설명
Email Security 인바운드	ESA-ESI-LIC=	구성: • Anti-Spam • Anti-Virus • 보안 침해 필터
Email Security 아웃바운드	ESA-ESO-LIC=	구성: • DLP • 암호화
Email Security Premium	ESA-ESP-LIC=	구성: • Anti-Spam • Anti-Virus • 보안 침해 필터 • DLP • 암호화
Cloudmark Anti-Spam	ESA-CLM-LIC=	—
이미지 분석기	ESA-IA-LIC=	—
McAfee Anti-Virus	ESA-MFE-LIC=	—
Intelligent Multi-Scan	ESA-IMS-LIC=	—
AMP(Advanced Malware Protection)	ESA-AMP-LIC=	—
그레이메일 안전 수신 거부	ESA-GSU-LIC=	(개별 구매)

Virtual Web Security Appliance의 PID(Product Identifier Code)

기능	PID	설명
Web Security Essentials	WSA-WSE-LIC=	구성: • 웹 사용 제어 • 웹 평판
Web Security Premium	WSA-WSP-LIC=	구성: • 웹 사용 제어 • 웹 평판 • Sophos 및 Webroot Anti-Malware 서명
Web Security Anti-Malware	WSA-WSM-LIC=	Sophos 및 Webroot Anti-Malware 서명 포함

기능	PID	설명
McAfee Anti-Malware	WSA-AMM-LIC=	—
AMP(Advanced Malware Protection)	WSA-AMP-LIC=	—

Virtual Content Security Management Appliance의 PID(Product Identifier Code)

기능	PID	설명
모든 중앙 집중식 웹 보안 기능	SMA-WMGT-LIC=	—
모든 중앙 집중식 이메일 보안 기능	SMA-EMGT-LIC=	

Cisco TAC

다음에서 전화 번호를 비롯한 Cisco TAC 연락처 정보를 참조하십시오.
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

추가 정보

지원 옵션에 대한 정보를 포함한 자세한 내용은 사용 중인 AsyncOS 릴리스의 릴리스 정보와 사용 설명서 또는 온라인 도움말을 참조하십시오.

Cisco Content Security 제품용 설명서:	위치:
Content Content Security Management 어플라이언스	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web Security 어플라이언스	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Email Security 어플라이언스	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html

관련 항목

- KVM에서 구축, 7페이지
- VMware ESXi에서 구축, 11페이지