vShield Endpoint용 NSX 업그레이드 가이드

업데이트 5
2017년 11월 20일에 수정됨
VMware NSX for vSphere 6.2

vmware®

VMware 웹 사이트 (https://docs.vmware.com/kr/) 에서 최신 기술 문서를 확인할 수 있습니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

목차

vShield Endpoint에 대한 NSX 업그레이드 가이드

1

이 vShield Endpoint에 대한 NSX 업그레이드 가이드 설명서에서는 vSphere Web Client를 사용하여 VMware® NSX™ 시스템을 업그레이드하는 방법을 설명합니다. 또한 단계별 업그레이드 지침 및 권장 모범 사례에 대한 정보도 수록되어 있습니다.

대상 사용자

이 설명서는 Endpoint 기능을 위해서만 vCloud Networking and Security를 사용하며 바이러스 백신 오프로드 기능을 위해서만 vShield Endpoint를 배포 및 관리하기 위해 NSX로 업그레이드하는 사용자를 위해 작성되었습니다. 이 설명서의 정보는 가상 시스템 기술 및 가상 데이터 센터 작업에 익숙한 숙련된 시스템 관리자를 대상으로 작성되었으며, VMware ESXi, vCenter Server 및 vSphere Web Client를 비롯한 VMware vSphere 5.5 또는 6.0에 이미 익숙하다는 것을 전제로 합니다.

논리적 스위치, 논리적 라우터, 분산 방화벽 또는 NSX Edge를 비롯한 NSX의 다른 기능을 사용해야 하는 경우에는 NSX 업그레이드 가이드를 참조하십시오.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에 사용된 용어에 대한 정의를 보려면 http://www.vmware.com/support/pubs를 참조하십시오.

이 장에서는 다음 주제에 대해 설명합니다.

- 지원 문서 읽어 보기
- vShield Endpoint용 NSX의 시스템 요구 사항
- NSX에 필요한 포트 및 프로토콜

지원 문서 읽어 보기

이 업그레이드 가이드 외에도 VMware에서는 업그레이드 프로세스를 지원하는 다른 문서를 다양하게 제공하고 있습니다.

릴리스 정보	업그레이드를 시작하기 전에 릴리스 정보를 확인하십시오. 알려진 업그레이드 문제와 해결 방법이 NSX 릴리스 정보에 설명되어 있습니다. 업그레이드 프로세스를 시작하기 전에 업그레이드 문제를 읽어 보면 시간과 노력을 줄일 수 있습니다. https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html를 참조하십시오.
제품 상호 운용성 매트릭스	기타 VMware 제품(예: vCenter)과의 상호 운용성을 확인합니다. **상호 운용성(Interoperability)** 탭의 VMware 제품 상호 운용성 매트릭스(http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)를 참조하십시오. 현재 버전의 NSX에서 업그레이드하려는 버전으로 연결되는 업그레이드 경로가 지원되는지 확인합니다. **업그레이드 경로(Upgrade Path)** 탭의 제품 메뉴에서 **VMware NSX**를 선택합니다.
호환성 가이드	http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security의 "VMware 호환성 가이드"에서 NSX와의 파트너 솔루션 호환성을 확인합니다.

vShield Endpoint용 NSX의 시스템 요구 사항

NSX를 설치하거나 업그레이드하기 전에 네트워크 구성 및 리소스를 고려합니다. vCenter Server별로 NSX Manager 하나, ESXi™ 호스트별로 Guest Introspection 인스턴스를 하나 설치하고 데이터센터별로 NSX Edge 인스턴스를 여러 개 설치할 수 있습니다.

하드웨어

표 1-1. 하드웨어 요구 사항

장치	메모리	vCPU	디스크 용량
NSX Manager	16GB(특정 NSX 배포 크기에서는 24GB*)	4(특정 NSX 배포 크기에서는 8*)	60GB
Guest Introspection	1GB	2	4GB

일반적인 지침으로, NSX 관리 환경에 256개가 넘는 하이퍼바이저 또는 2000개가 넘는 VM이 있을 경우 NSX Manager 리소스를 8대의 vCPU 및 24GB RAM으로 늘리는 것이 좋습니다.

특정 크기 조정 세부 정보는 VMware 지원팀에 문의하십시오.

가상 장치에 대한 메모리 및 vCPU 할당을 늘리는 방법에 대한 자세한 내용은 vSphere 가상 시스템 관리에서 메모리 리소스 할당 및 가상 CPU의 수 변경을 참조하십시오.

소프트웨어

VMware 제품의 권장 버전은 다음과 같습니다.

- VMware vCenter Server 5.5U3
- VMware vCenter Server 6.0U2

클라이언트 및 사용자 액세스

- ESXi 호스트를 이름으로 vSphere 인벤토리에 추가한 경우 정방향 및 역방향 이름 확인이 작동하는지 확인하십시오. 그렇지 않으면 NSX Manager가 IP 주소를 확인할 수 없습니다.
- 가상 시스템을 추가하고 가상 시스템의 전원을 켤 수 있는 권한이 필요합니다.
- 가상 시스템 파일을 저장하는 데이터스토어에 대한 액세스 권한과 해당 데이터스토어에 파일을 복사할 계정 사용 권한이 있어야 합니다.
- NSX Manager 사용자 인터페이스에 액세스할 수 있도록 웹 브라우저에서 쿠키를 사용하도록 설정해야 합니다.
- 배포할 NSX 장치, vCenter Server 및 ESXi 호스트가 포트 443에 액세스할 수 있도록 NSX Manager에서 설정합니다. 이 포트는 배포할 OVF 파일을 ESXi 호스트에 다운로드하는 데 필요합니다.
- 사용 중인 vSphere Web Client 버전에서 지원되는 웹 브라우저. 자세한 내용은 vCenter Server 및 호스트 관리 설명서에서 vSphere Web Client 사용을 참조하십시오.

NSX에 필요한 포트 및 프로토콜

NSX가 올바르게 작동하려면 다음 포트가 열려 있어야 합니다.

표 1-2. NSX에 필요한 포트 및 프로토콜

소스	대상	포트	프로토콜	용도	민감도	TLS	인증
클라이언트 PC	NSX Manager	443	TCP	NSX Manager 관리 인터페이스	아니요	예	PAM 인증
클라이언트 PC	NSX Manager	80	TCP	NSX Manager VIB 액세스	아니요	아니요	PAM 인증
ESXi 호스트	vCenter Server	443	TCP	ESXi 호스트 준비	아니요	아니요	
vCenter Server	ESXi 호스트	443	TCP	ESXi 호스트 준비	아니요	아니요	
ESXi 호스트	NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
ESXi 호스트	NSX Controller	1234	TCP	사용자 월드 에이전트 연결	아니요	예	

표 1-2. NSX에 필요한 포트 및 프로토콜 (계속)

소스	대상	포트	프로토콜	용도	민감도	TLS	인증
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	컨트롤러 클러스터 – 상태 동기화	아니요	예	IPsec
NSX Controller	NSX Controller	7777	TCP	컨트롤러 간 RPC 포트	아니요	예	IPsec
NSX Controller	NSX Controller	30865	TCP	컨트롤러 클러스터 – 상태 동기화	아니요	예	IPsec
NSX Manager	NSX Controller	443	TCP	컨트롤러와 Manager 간 통신	아니요	예	사용자/암호
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	아니요	예	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	아니요	예	
NSX Manager	ESXi 호스트	443	TCP	관리 및 프로비저닝 연결	아니요	예	
NSX Manager	ESXi 호스트	902	TCP	관리 및 프로비저닝 연결	아니요	예	
NSX Manager	DNS 서버	53	TCP	DNS 클라이언트 연결	아니요	아니요	
NSX Manager	DNS 서버	53	UDP	DNS 클라이언트 연결	아니요	아니요	
NSX Manager	Syslog 서버	514	TCP	Syslog 연결	아니요	아니요	
NSX Manager	Syslog 서버	514	UDP	Syslog 연결	아니요	아니요	
NSX Manager	NTP 시간 서버	123	TCP	NTP 클라이언트 연결	아니요	예	
NSX Manager	NTP 시간 서버	123	UDP	NTP 클라이언트 연결	아니요	예	
vCenter Server	NSX Manager	80	TCP	호스트 준비	아니요	예	
REST 클라이언트	NSX Manager	443	TCP	NSX Manager REST API	아니요	예	사용자/암호

표 1-2. NSX에 필요한 포트 및 프로토콜 (계속)

소스	대상	포트	프로토콜	용도	민감도	TLS	인증
VTEP(VXLAN Tunnel End Point)	VTEP(VXLAN Tunnel End Point)	8472(NSX 6.2.3 이전의 기본 값) 또는 4789(NSX 6.2.3 이상 새 설치의 기본 값)	UDP	VTEP 간 전송 네트워크 캡슐화	아니요	예	
ESXi 호스트	ESXi 호스트	6999	UDP	VLAN LIF의 ARP	아니요	예	
ESXi 호스트	NSX Manager	8301, 8302	UDP	DVS 동기화	아니요	예	
NSX Manager	ESXi 호스트	8301, 8302	UDP	DVS 동기화	아니요	예	
Guest Introspection VM	NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
기본 NSX Manager	보조 NSX Manager	443	TCP	크로스 vCenter NSX 범용 동기화 서비스	아니요	예	
기본 NSX Manager	vCenter Server	443	TCP	vSphere API	아니요	예	
보조 NSX Manager	vCenter Server	443	TCP	vSphere API	아니요	예	
기본 NSX Manager	NSX 범용 컨트롤러 클러스터	443	TCP	NSX Controller REST API	아니요	예	사용자/암호
보조 NSX Manager	NSX 범용 컨트롤러 클러스터	443	TCP	NSX Controller REST API	아니요	예	사용자/암호
ESXi 호스트	NSX 범용 컨트롤러 클러스터	1234	TCP	NSX 제어부 프로토콜	아니요	예	
ESXi 호스트	기본 NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
ESXi 호스트	보조 NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호

크로스 vCenter NSX 및 고급 연결 모드용 포트

크로스 vCenter NSX 환경을 사용하며 vCenter Server 시스템이 고급 연결 모드인 경우 vCenter Server 시스템에서 NSX Manager를 관리하려면 각 NSX Manager 장치가 환경의 각 vCenter Server 시스템에 반드시 연결되어 있어야 합니다.

vCloud Networking and Security에서 NSX로의 업그레이드

2

이 장에서는 다음 주제에 대해 설명합니다.

- vCloud Networking and Security에서 vShield Endpoint용 NSX로의 업그레이드 준비
- vCloud Networking and Security 5.5.x에서 vShield Endpoint용 NSX 6.2.x로 업그레이드

vCloud Networking and Security에서 vShield Endpoint용 NSX로의 업그레이드 준비

NSX로 성공적으로 업그레이드하기 위해 릴리스 정보를 읽고 업그레이드 문제를 확인하십시오. 올바른 업그레이드 순서를 따르고 있는지 및 인프라가 업그레이드를 위해 제대로 준비되었는지 확인해야 합니다. 다음 지침을 업그레이드 전 검사 목록으로 사용할 수 있습니다.

주의 다운그레이드는 지원되지 않습니다.

- 항상 업그레이드를 진행하기 전에 NSX Manager의 백업을 캡처하십시오.
- NSX Manager가 업그레이드되면 NSX를 다운그레이드할 수 없습니다.

회사에서 지정한 유지 보수 기간에 업그레이드 작업을 수행하는 것이 좋습니다.

다음 지침을 업그레이드 전 검사 목록으로 사용할 수 있습니다.

1 vCloud Networking and Security가 버전 5.5인지 확인합니다. 그렇지 않으면 vShield 설치 및 업그레이드 가이드 버전 5.5에서 업그레이드 지침을 참조하십시오.

2 모든 필수 포트가 열려 있는지 확인합니다. NSX에 필요한 포트 및 프로토콜를 참조하십시오.

3 vCenter가 NSX 6.2.x에 대한 시스템 요구 사항을 충족하는지 확인합니다. vShield Endpoint용 NSX의 시스템 요구 사항을 참조하십시오.

4 vSphere Distributed Switch에 대한 업링크 포트 이름 정보를 검색할 수 있는지 확인합니다. https://kb.vmware.com/kb/2129200를 참조하십시오.

5 vShield Endpoint 파트너 서비스가 배포된 경우 업그레이드 전에 호환성을 확인합니다.
   - 대부분의 환경에서 파트너 솔루션에 영향을 주지 않으면서 vCloud Networking and Security를 NSX로 업그레이드할 수 있습니다. 그렇지만 파트너 솔루션이 업그레이드하는 NSX 버전과 호환되지 않으면 NSX로 업그레이드하기 전에 파트너 솔루션을 호환되는 버전으로 업그레이드해야 합니다.

- Networking & Security에 대한 VMware 호환성 가이드를 참조하십시오. http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security를 참조하십시오.
- 호환성 및 업그레이드 세부 정보에 대해서는 파트너 설명서를 참조하십시오.

6 운영 환경에 Data Security가 설치되어 있으면 vShield Manager를 업그레이드하기 전에 제거합니다. vShield Data Security 제거를 참조하십시오.

7 Cisco Nexus 1000V를 외부 스위치 제공자로 사용하는 경우 NSX로 업그레이드하기 전에 해당 네트워크를 vSphere Distributed Switch로 마이그레이션해야 합니다. NSX가 설치되면 vSphere Distributed Switch를 논리적 스위치로 마이그레이션할 수 있습니다.

8 vShield Manager, vCenter 및 기타 vCloud Networking and Security 구성 요소의 최신 백업이 있는지 확인합니다. vCloud Networking and Security 백업 및 복원를 참조하십시오.

9 기술 지원 번들을 생성합니다.

10 nslookup 명령을 사용하여 정방향 및 역방향 도메인 이름 확인이 작동하는지 확인합니다.

11 작업 환경에서 VUM이 사용 중인 경우 vCenter에서 bypassVumEnabled 플래그가 true로 설정되어 있는지 확인합니다. 이 설정을 수행하면 VUM이 설치되어 있으나 사용 가능하지 않을 경우에도 VIB를 ESXi 호스트에 직접 설치하도록 EAM이 구성됩니다. http://kb.vmware.com/kb/2053782를 참조하십시오.

12 업그레이드 번들을 다운로드한 후 스테이징하고 md5sum을 사용하여 유효성을 확인합니다. vShield Manager에서 NSX로의 업그레이드 번들 다운로드 및 MD5 확인를 참조하십시오.

13 가장 좋은 방법은 업그레이드의 모든 섹션이 완료될 때까지 작업 환경의 모든 작업을 거부하십시오.

14 지침이 있지 않는 한 vCloud Networking and Security 구성 요소나 장치를 끄거나 삭제하지 마십시오.

vShield Endpoint 업그레이드가 작동에 주는 영향

vCloud Networking and Security 업그레이드 프로세스는 다소 시간이 걸릴 수 있습니다. 업그레이드 동안 vCloud Networking and Security 구성 요소의 작동 상태를 이해하는 것이 중요합니다.

vCloud Networking and Security를 NSX 6.2로 업그레이드하려면 NSX 구성 요소를 다음 순서로 업그레이드해야 합니다.

- vShield Manager
- vShield Endpoint

단일 중단 기간에 업그레이드를 실행하여 다운타임을 최소화하고 업그레이드 중에 특정 vCloud Networking and Security 관리 기능에 액세스할 수 없는 vCloud Networking and Security 사용자가 겪는 불편함을 줄이는 것이 좋습니다. 하지만 사이트 요구 사항 때문에 단일 중단 기간에 업그레이드를 완료할 수 없는 경우에는 아래 정보를 vCloud Networking and Security 사용자에게 제공하여 업그레이드 중에 사용할 수 있는 기능에 대해 알릴 수 있습니다.

vCenter 업그레이드

vCenter에 내장된 SSO를 사용하고 vCenter 5.5를 vCenter 6.0으로 업그레이드하는 경우 vCenter와 vShield Manager의 연결이 끊길 수 있습니다. 이는 vCenter 5.5가 루트 사용자 이름을 사용하여 vShield에 등록된 경우 발생합니다. NSX 6.2부터는 루트를 사용한 vCenter 등록이 더 이상 지원되지 않습니다. 이에 대한 해결 방법으로 루트 대신 administrator@vsphere.local 사용자 이름을 사용하여 vCenter를 vShield에 다시 등록하십시오.

외부 SSO를 사용하는 경우에는 아무것도 변경할 필요가 없습니다. 동일한 사용자 이름(예: admin@mybusiness.mydomain)을 사용할 수 있으며 vCenter 연결이 끊어지지 않습니다.

vShield Manager 업그레이드

업그레이드 중:

- vShield Manager 구성이 차단됩니다. vShield API 서비스를 사용할 수 없습니다. vShield 구성을 변경할 수 없습니다. 기존 VM 통신이 계속 작동합니다.

업그레이드 후:

- 모든 vShield 및 NSX 구성을 변경할 수 있습니다.

vShield Endpoint가 Guest Introspection으로 마이그레이션됨

NSX 6.x에서 vShield Endpoint의 이름이 Guest Introspection으로 변경되었습니다. NSX Manager를 업그레이드한 후에 **Networking & Security > 설치 > 서비스 배포**로 이동하면 Guest Introspection 서비스에 **업그레이드** 링크가 표시됩니다.
vCloud Networking and Security에서 NSX로 업그레이드할 경우, Guest Introspection 가상 장치와 Guest Introspection의 호스트 에이전트는 Guest Introspection을 사용하도록 설정된 클러스터의 각 호스트에 배포됩니다.

업그레이드 중:

- VM 추가, vMotion 또는 삭제와 같은 VM에 대해 변경이 생긴 경우에는 이 NSX 클러스터의 VM을 보호하지 않게 됩니다.

업그레이드 후:

- VM 추가, vMotion 및 삭제 동안 VM이 보호됩니다.

vShield Endpoint의 작동 상태 확인

업그레이드를 시작하기 전에 vCloud Networking and Security 작동 상태를 테스트해야 합니다. 그렇지 않으면 업그레이드 후 발생한 문제가 업그레이드 프로세스로 인한 것인지 또는 업그레이드 이전부터 있었는지 파악할 수 없습니다.

vCloud Networking and Security 인프라 업그레이드를 시작하기 전에 모든 요소가 제대로 작동하고 있다고 가정해서는 안 되며, 반드시 사전 확인이 필요합니다.

다음 절차를 업그레이드 전 체크리스트로 사용할 수 있습니다.

프로시저

1 관리자 ID 및 암호를 식별합니다.

2 모든 구성 요소에서 정방향 및 역방향 이름 확인이 작동하는지 확인합니다.

3 모든 vSphere 및 vShield 구성 요소에 로그인할 수 있는지 확인합니다.

4 vShield Manager, vCenter Server 및 ESXi의 현재 버전을 적어둡니다.

5 vShield 환경을 육안으로 검사하여 모든 상태 표시기가 녹색, 보통 또는 배포됨인지 확인합니다.

6 syslog가 구성되어 있는지 확인합니다.

7 파트너 솔루션이 작동하고 있는지 확인합니다.

   예를 들어 바이러스 백신 기능 테스트를 위해 EICAR 표준 바이러스 백신 테스트 파일 http://www.eicar.org/86-0-Intended-use.html을 사용할 수 있습니다.

8 (선택 사항) 테스트 환경이 있는 경우 운영 환경을 업그레이드하기 전에 업그레이드 및 업그레이드 후 기능을 테스트합니다.

로컬 관리자를 CLI 관리자로 마이그레이션

NSX 6.x 시리즈 이전에는 관리자가 로컬 데이터베이스 사용자였습니다. NSX 6.0부터는 관리자가 CLI 사용자입니다. 이전 버전과의 호환성을 위해 관리자를 마이그레이션할 수 있는 단계가 마련되어 있습니다.

vCloud Networking and Security 5.x 시리즈에서는 CLI의 관리자와 UI(VSM)의 관리자가 서로 달랐습니다. CLI 관리자의 암호는 OS에서 관리했고 VSM 사용자의 암호는 사용자의 로컬 데이터베이스에서 관리했습니다. 따라서 CLI 관리자의 암호를 변경해도 VSM 관리자의 암호에는 영향을 주지 않았습니다. 마찬가지로 VSM 관리자의 암호를 변경해도 CLI 관리자 암호에는 영향을 주지 않았습니다.

NSX 6.x 시리즈에서는 VSM 사용자 데이터베이스가 더 이상 지원되지 않습니다. CLI 사용자가 NSX Manager에 직접 로그인할 수 있습니다.

업그레이드 시나리오의 경우 이전 버전과의 호환성을 위해 CLI와 웹 UI 데이터베이스 모두에 관리자가 제공됩니다. 이 경우 CLI 사용자의 암호가 변경되어도 UI나 REST API 호출에 반영되지 않습니다. NSX 6.x 시리즈 이전에는 CLI 사용자가 UI나 REST API에 로그인할 수 없었습니다.

NSX 6.x 시리즈를 새로 배포하는 경우(신규 배포) CLI 사용자와 NSX Manager(UI 또는 REST)가 동일하고 자격 증명도 같습니다.

업그레이드한 NSX 배포가 새로 배포한 NSX 6.x처럼 작동하도록 설정하려는 경우 두 가지 옵션을 사용할 수 있습니다.

- 옵션 1 – 데이터베이스 관리자의 암호를 변경합니다.

다음 REST API를 사용하여 암호를 변경할 수 있습니다. 이 옵션을 사용하려면 이전 암호를 알고 있어야 합니다.

PUT URI /api/2.0/services/usermgmt/user/local/<userId>

```
<userInfo>
      <userId></userId>
      <password></password>
      <fullname></fullname>
      <email></email>
      <accessControlEntry>
         <role></role>
         <resource>
             <resourceId></resourceId>
             ...
         </resource>
      </accessControlEntry>
</userInfo>
```

예를 들어 curl을 사용할 경우 다음과 같습니다.

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d '<userInfo><userId>admin</userId><password>123</password><fullname>admin</fullname><email>admin@company.com</email><accessControlEntry><role>security_admin</role><resource><resourceId>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
```

API를 사용하여 암호를 포함한 로컬 사용자 계정을 업데이트할 수 있습니다. 암호를 제공하지 않으면 기존 암호가 유지됩니다. URI의 userId 변수는 XML에 지정된 것과 동일해야 합니다.

- 옵션 2 – 웹 UI 관리자를 유지 보수하는 대신 웹 UI 관리자를 제거하고 CLI 관리자에게 역할을 추가할 수 있습니다. 이렇게 변경하고 나면 CLI 사용자 자격 증명을 사용하여 NSX Manager에 로그인할 수 있으며 CLI 관리자의 암호 변경 내용이 NSX Manager 관리자에게 반영됩니다.

  웹 UI 관리자는 super_user이므로 웹 UI 관리자를 삭제하려면 먼저 super_user 권한이 있는 다른 사용자를 추가해야 합니다.

  - super_user 역할이 있는 tempadmin이라는 새 사용자를 추가합니다.

    예를 들어 curl을 사용할 경우 다음과 같습니다.

    ```
    curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d '<userInfo><userId>tempadmin</userId><password>123</password><fullname>tempadmin</fullname><email>tempadmin@company.com</email><accessControlEntry><role>super_user</role><resource><resourceId>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
    ```

- tempadmin을 사용하여 웹 UI 관리자를 삭제합니다.

  예를 들어 curl을 사용할 경우 다음과 같습니다.

  ```
  curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X DELETE
  https://<vsm-ip>/api/2.0/services/usermgmt/user/admin
  ```

- super_user 역할을 CLI 관리자에게 추가합니다.

  예를 들어 curl을 사용할 경우 다음과 같습니다.

  ```
  curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X POST
  https://<nsx-ip>/api/2.0/services/usermgmt/role/admin?isCli=true -d
  '<accessControlEntry><role>super_user</role></accessControlEntry>'
  ```

vShield Data Security 제거

운영 환경에 Data Security가 설치되어 있으면 NSX로 업그레이드하기 전에 제거합니다.

NSX 6.2.3부터 NSX Data Security 기능이 더 이상 지원되지 않습니다. NSX 6.2.3에서도 사용자의 재량에 따라 이 기능을 계속 사용할 수 있지만 향후 릴리스에서는 NSX에서 이 기능이 제거될 것임을 유의하십시오.

프로시저

1 vShield Manager 5.5 인벤토리 패널에서 **데이터센터(Datacenters)** 폴더를 확장하고 vShield Data Security가 설치된 호스트로 이동합니다.

2 vShield Data Security가 설치된 각 호스트에서 다음 단계를 완료하여 제거합니다.

  a 호스트를 클릭하고 **요약(Summary)** 탭의 [vShield 호스트 준비] 창에서 vShield Data Security에 대한 **제거(Uninstall)** 링크를 클릭합니다.

  b [제거할 서비스를 선택하십시오.] 창에서 vShield Data Security가 선택되어 있는지 확인하고 **제거(Uninstall)** 버튼을 클릭합니다.

  vShield Data Security가 제거되고 [vShield 호스트 준비] 창에 해당 상태가 설치 안 됨으로 표시됩니다.

vCloud Networking and Security 백업 및 복원

모든 vCloud Networking and Security 구성 요소를 올바르게 백업해야 장애 발생 시 시스템을 작동 상태로 복원할 수 있습니다.

vShield Manager 백업에는 가상 와이어 및 라우팅 엔티티, 보안, vApp 규칙 및 vShield Manager UI나 API 내에서 구성하는 모든 항목을 포함하는 모든 vShield 구성이 포함되어 있습니다. vCenter 데이터베이스 및 관련 요소(예: 가상 스위치)는 별도로 백업해야 합니다.

vShield Manager와 vCenter는 정기적으로 백업하는 것이 좋습니다. 백업 빈도와 예약은 비즈니스 요구 사항 및 작동 절차에 따라 달라질 수 있습니다. 구성 변경을 자주 수행하는 시기에는 vCloud Networking and Security를 자주 백업하는 것이 좋습니다.

vShield Manager 백업은 필요시 수행할 수도 있고 매시간, 매일 또는 매주 수행할 수도 있습니다.

다음과 같은 경우 백업을 수행하는 것이 좋습니다.

- vCloud Networking and Security 또는 vCenter 업그레이드 전
- vCloud Networking and Security 또는 vCenter 업그레이드 후
- vCloud Networking and Security 구성 요소의 제로 데이(Day Zero) 배포 및 초기 구성이 완료된 후(예: 가상 스위치, Edge, 보안 및 방화벽 정책 생성 후)
- 인프라 또는 토폴로지 변경 후
- 주요 데이 2(Day 2) 변경 후

롤백하려는 특정 시점의 전체 시스템 상태를 제공할 수 있도록 vCloud Networking and Security 구성 요소 백업을 상호 작용 중인 다른 구성 요소(예: vCenter, 클라우드 관리 시스템, 운영 도구 등)의 백업 예약과 동기화하는 것이 좋습니다.

요청 시 vShield Manager 데이터 백업

언제든지 요청 시 백업을 수행하여 vShield Manager 데이터를 백업할 수 있습니다.

프로시저

1. vShield Manager 인벤토리 패널에서 **설정 및 보고서(Settings & Reports)**를 클릭합니다.
2. **구성(Configuration)** 탭을 클릭합니다.
3. **백업(Backups)**을 클릭합니다.
4. (선택 사항) 시스템 이벤트 테이블을 백업하지 않으려면 **시스템 이벤트 제외(Exclude System Events)** 확인란을 선택합니다.
5. (선택 사항) 감사 로그 테이블을 백업하지 않으려면 **감사 로그 제외(Exclude Audit Logs)** 확인란을 선택합니다.
6. 백업이 저장될 시스템의 **호스트 IP 주소(Host IP Address)**를 입력합니다.
7. 백업 시스템의 **호스트 이름(Host Name)**을 입력합니다.
8. 백업 시스템에 로그인하는 데 필요한 **사용자 이름(User Name)**을 입력합니다.
9. 백업 시스템의 사용자 이름과 연결된 **암호(Password)**를 입력합니다.
10. **백업 디렉토리(Backup Directory)** 필드에서 백업이 저장되는 절대 경로를 입력합니다.
11. **파일 이름 접두사(Filename Prefix)**에 텍스트 문자열을 입력합니다.

    이 텍스트는 백업 시스템에서 손쉽게 인식할 수 있도록 백업 파일 이름 앞에 붙습니다. 예를 들어 ppdb를 입력하면 백업 파일 이름은 ppdbHH_MM_SS_DayDDMonYYYY로 지정됩니다.
12. 백업 파일을 보호하려면 **암호(Pass Phrase)**를 입력합니다.

    vCloud Networking and Security에서 암호는 선택 사항입니다. NSX에서는 필수입니다.
13. **전송 프로토콜(Transfer Protocol)** 드롭다운 메뉴에서 **SFTP** 또는 **FTP**를 선택합니다.

14 **백업(Backup)**을 클릭합니다.

완료되면 이 양식 아래에 있는 테이블에 백업이 나타납니다.

15 **설정 저장(Save Settings)**을 클릭하여 구성을 저장합니다.

모든 백업이 단일 디렉토리에 저장되면 백업을 볼 때 문제가 발생할 수 있습니다. 경우에 따라 백업 파일을 아카이브 폴더에 이동하는 것이 가장 좋습니다.

vSphere Distributed Switch 백업

vSphere Distributed Switch 및 분산 포트 그룹 구성을 파일로 내보낼 수 있습니다.

파일에는 유효한 네트워크 구성이 유지되므로 이러한 구성을 다른 배포로 분배할 수 있습니다.

이 기능은 vSphere Web Client 5.1 이상에서만 사용할 수 있습니다. VDS 설정 및 포트 그룹 설정은 가져오기 작업의 일부로 가져오게 됩니다.

VXLAN에 사용할 수 있도록 클러스터를 준비하기 전에 VDS 구성을 내보내는 것이 좋습니다. 자세한 내용은 http://kb.vmware.com/kb/2034602 항목을 참조하십시오.

vCenter 백업

NSX 배포를 보호하려면 vCenter 데이터베이스를 백업하고 VM의 스냅샷을 생성해야 합니다.

vCenter 백업 및 복원 절차와 모범 사례는 사용 중인 vCenter 버전의 vCenter 설명서를 참조하십시오.

VM 스냅샷에 대한 자세한 내용은 http://kb.vmware.com/kb/1015180 항목을 참조하십시오.

vCenter 5.5에 유용한 링크:

- http://kb.vmware.com/kb/2057353
- http://kb.vmware.com/kb/2034505
- http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf

vCenter 6.0에 유용한 링크:

- https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html
- http://kb.vmware.com/kb/2110294

vShield Manager에서 NSX로의 업그레이드 번들 다운로드 및 MD5 확인

vShield Manager에서 NSX로의 업그레이드 번들에는 NSX 인프라를 업그레이드하는 데 필요한 모든 파일이 포함되어 있습니다. vShield Manager를 업그레이드하려면 먼저 업그레이드하려는 대상 버전에 맞는 업그레이드 번들을 다운로드해야 합니다.

필수 조건

MD5 체크섬 도구

프로시저

1 vShield Manager가 찾을 수 있는 위치에 vShield Manager에서 NSX로의 업그레이드 번들을 다운로드합니다. 업그레이드 번들 파일의 이름은 VMware-vShield-Manager-upgrade-bundle-to-NSX-릴리스 번호-*NSX* 빌드 번호.tar.gz와 비슷한 형식을 갖습니다.

2 업그레이드 파일 이름이 tar.gz로 끝나는지 확인합니다.

일부 브라우저에서는 파일 확장명이 바뀔 수 있습니다. 예를 들어 다운로드 파일 이름이 다음과 같을 수 있습니다.

VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz

이 이름을 다음과 같이 변경합니다.

VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.tar.gz

이렇게 하지 않으면 업그레이드 번들을 업로드한 후 "업그레이드 번들 파일 VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz가 잘못되었습니다. 업그레이드 파일의 확장명은 tar.gz입니다."라는 오류 메시지가 나타납니다.

3 MD5 체크섬 도구를 사용하여 VMware 웹 사이트에 게시된 업그레이드 번들의 공식 MD5 합계와 체크섬 도구로 계산한 MD5 합계를 비교합니다.

a MD5 체크섬 도구에서 업그레이드 번들을 찾습니다.

b 도구를 사용하여 번들의 체크섬을 계산합니다.

c VMware 웹 사이트에 게시된 체크섬을 붙여 넣습니다.

d 도구를 사용하여 두 체크섬을 비교합니다.

두 체크섬이 일치하지 않을 경우 업그레이드 번들 다운로드를 반복해서 수행합니다.

vCloud Networking and Security 5.5.x에서 vShield Endpoint용 NSX 6.2.x로 업그레이드

NSX 6.2.x로 업그레이드하려면 이 가이드에 설명된 순서에 따라 vCloud Networking and Security 구성 요소를 업그레이드해야 합니다.

vCloud Networking and Security 구성 요소는 다음 순서로 업그레이드해야 합니다.

1 vShield Manager를 NSX Manager로 업그레이드

2 vShield Endpoint를 NSX Guest Introspection으로 업그레이드

vShield Manager를 vShield Endpoint용 NSX Manager로 업그레이드

NSX 인프라 업그레이드 프로세스의 첫 번째 단계는 NSX Manager 장치 업그레이드입니다.

주의 배포된 vShield Manager 장치 인스턴스는 제거하지 마십시오.

필수 조건

- vCloud Networking and Security에서 vShield Endpoint용 NSX로의 업그레이드 준비에 설명된 모든 업그레이드 준비 작업을 완료했는지 확인합니다.
- vShield Manager에 NSX Manager로 업그레이드하기 위한 충분한 디스크 공간이 있는지 확인합니다. vShield Endpoint용 NSX의 시스템 요구 사항를 참조하십시오.
- NSX 6.2.x로 업그레이드하기 전에 vShield Manager 가상 장치의 예약 메모리를 16GB 이상으로 늘리고 vCPU 4개를 할당합니다.

  vShield Endpoint용 NSX의 시스템 요구 사항를 참조하십시오.

프로시저

1. NSX 업그레이드 번들을 vShield Manager에서 검색할 수 있는 위치에 다운로드합니다. 업그레이드 번들 파일의 이름은 VMware-vShield-Manager-upgrade-bundle-to-NSX-release-빌드 번호.tar.gz와 비슷합니다.
2. vShield Manager 5.5 인벤토리 패널에서 **설정 및 보고서**를 클릭합니다.
3. **업데이트** 탭을 클릭하고 **업그레이드 번들 업로드**를 클릭합니다.
4. **파일 선택**을 클릭하고 VMware-vShield-Manager-upgrade-bundle-to-NSX-release-빌드 번호.tar.gz 파일을 선택한 후 **열기**를 클릭합니다.
5. **파일 업로드**를 클릭합니다.

   파일을 업로드하는 데 몇 분 정도 걸립니다.
6. **설치**를 클릭하여 업그레이드 프로세스를 시작합니다.
7. **설치 확인**을 클릭합니다. 업그레이드 프로세스가 진행되는 동안 vShield Manager가 재부팅되므로 vShield Manager 사용자 인터페이스와의 연결이 끊길 수 있습니다. 다른 vShield 구성 요소는 재부팅되지 않습니다.
8. 재부팅 후에 웹 브라우저 창을 열고 https://10.10.10.10과 같이 IP 주소를 입력하여 NSX Manager 가상 장치에 로그인합니다. 업그레이드된 NSX Manager는 vShield Manager와 IP 주소가 동일합니다.

   [요약] 탭에는 방금 설치한 NSX Manager의 버전이 표시됩니다.
9. **홈 > vCenter 등록 관리**로 이동하여 vCenter Server 상태가 연결됨인지 확인합니다.
10. vSphere Web Client에 액세스 중인 기존 브라우저 세션을 닫습니다. vSphere Web Client에 다시 로그인하기 전에 몇 분 정도 기다린 후 브라우저 캐시를 지웁니다.
11. vShield Manager에서 SSH를 사용하도록 설정한 경우 업그레이드 후에도 NSX Manager에서 SSH를 사용하도록 설정해야 합니다. NSX Manager 가상 장치에 로그인하고 **요약 보기**를 클릭합니다. 시스템 수준 구성 요소에서 SSH 서비스에 대해 **시작**을 클릭합니다.

중요 vCloud Networking and Security 5.x에서 NSX 6.x로 업그레이드한 후에는 CLI 관리 로그인 자격 증명을 사용하여 NSX Manager에 로그인해야 합니다. 이전에는 vCloud Networking and Security에 두 개의 암호가 필요했습니다. 하나는 CLI에, 하나는 UI에 사용했습니다. NSX 6.x부터는 암호가 하나만 필요합니다. 예:

vCloud Networking and Security의 암호

- CLI에 대한 mypassword#123
- UI에에 대한 mypassword#456

NSX로 업그레이드한 후의 암호

- CLI에 대한 mypassword#123
- UI에 대한 mypassword#123

NSX Manager를 업그레이드한 후에 로그아웃했다가 vSphere Web Client에 다시 로그인해야 합니다.

NSX 플러그인이 vSphere Web Client에 올바르게 표시되지 않으면 브라우저의 캐시 및 방문 기록을 지웁니다. 이 단계가 완료되지 않으면 vSphere Web Client에서 NSX 구성을 변경할 때 "내부 오류가 발생했습니다. 오류 #1009"와 비슷한 오류가 표시될 수 있습니다.

Networking and Security 탭이 vSphere Web Client에 나타나지 않으면 vSphere Web Client 서버를 다시 설정합니다.

- vCenter 5.5에서 https://<vcenter-ip>:5480을 열고 Web Client 서버를 다시 시작합니다.
- vCenter Server Appliance 6.0에서 vCenter Server 셸에 루트 사용자 자격으로 로그인한 후 다음 명령을 실행합니다.

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Windows의 vCenter Server 6.0에서는 다음 명령을 실행하여 이 작업을 수행할 수 있습니다.

```
cd C:¥Program Files¥VMware¥vCenter Server¥bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

여러 버전의 NSX 플러그인이 실행 중인 경우 여러 버전의 NSX Manager가 실행 중인 vCenter Server를 관리하고 예기치 않은 오류를 방지하기 위해 각기 다른 Web Client를 사용하는 것이 좋습니다.

후속 작업

NSX Manager의 백업을 생성합니다. 이전 NSX Manager 백업은 이전 릴리스에만 유효합니다. vShield Endpoint에 대한 NSX Manager 데이터 백업를 참조하십시오.

vShield Endpoint에 대한 NSX Manager 데이터 백업

요청 시 백업 또는 예약된 백업을 수행하여 NSX Manager 데이터를 백업할 수 있습니다.

NSX Manager 가상 장치 웹 인터페이스에서 또는 NSX Manager API를 통해 NSX Manager 백업 및 복원을 구성할 수 있습니다. 매시간, 매일, 매주 단위로 백업을 예약할 수 있습니다.

백업 파일은 NSX Manager가 액세스할 수 있는 원격 FTP 또는 SFTP 위치에 저장됩니다. NSX Manager 데이터에는 구성, 이벤트 및 감사 로그 테이블이 포함됩니다. 구성 테이블은 모든 백업에 포함됩니다.

복원은 백업 버전과 동일한 NSX Manager 버전에서만 지원됩니다. 이러한 이유로 NSX 업그레이드를 수행하기 전과 후에 새 백업 파일(이전 버전에 대한 백업 하나와 새 버전에 대한 백업 하나)을 생성해야 합니다.

프로시저

1 NSX Manager 가상 장치에 로그인합니다.

2 장치 관리에서 **백업 및 복원(Backups & Restore)**을 클릭합니다.

3 백업 위치를 지정하려면 FTP 서버 설정 옆의 **변경(Change)**을 클릭합니다.

   a 백업 시스템의 IP 주소 또는 호스트 이름을 입력합니다.

   b **전송 프로토콜(Transfer Protocol)** 드롭다운 메뉴에서 대상 시스템이 지원하는 프로토콜에 따라 **SFTP** 또는 **FTP**를 선택합니다.

   c 필요한 경우 기본 포트를 편집합니다.

   d 백업 시스템에 로그인하는 데 필요한 사용자 이름과 암호를 입력합니다.

   e **백업 디렉토리(Backup Directory)** 필드에서 백업이 저장될 절대 경로를 입력합니다.

   절대 경로를 확인하려면 FTP 서버에 로그인하고 사용할 디렉토리로 이동한 다음 현재 작업 디렉토리 명령(pwd)을 실행합니다. 예:

```
PS C:WUsersWAdministrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

f **파일 이름 접두사(Filename Prefix)**에 텍스트 문자열을 입력합니다.

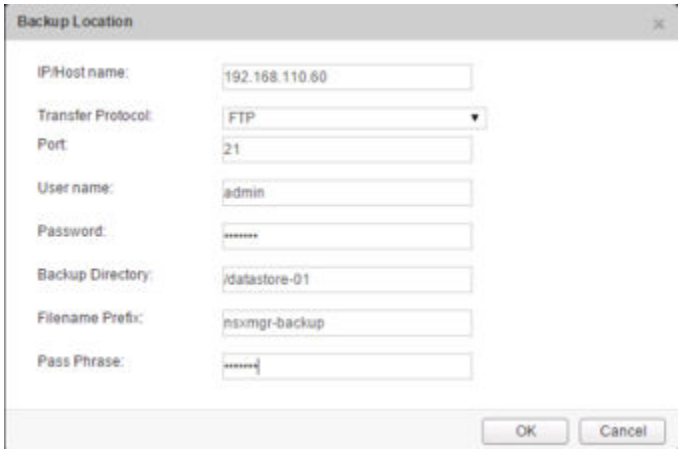
이 텍스트는 백업 시스템에서 손쉽게 인식할 수 있도록 각 백업 파일 이름 앞에 붙습니다. 예를 들어 ppdb를 입력하면 백업 파일 이름은 ppdbHH_MM_SS_DayDDMonYYYY로 지정됩니다.

g 백업 파일을 보호하려면 암호를 입력합니다.

이 암호는 백업을 복원할 때 필요합니다.

h **확인(OK)**을 클릭합니다.

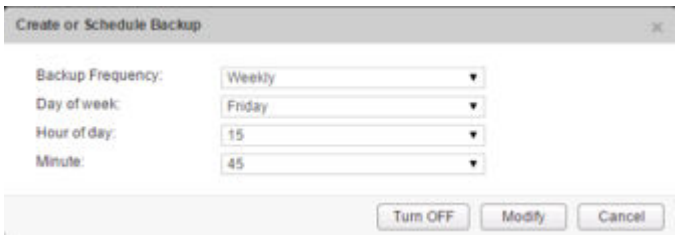
예:



4 요청 시 백업의 경우 **백업(Backup)**을 클릭합니다.

백업 기록(Backup History) 아래에 새 파일이 추가됩니다.

5 예약된 백업의 경우 [스케줄링] 옆의 **변경(Change)**을 클릭합니다.



a **백업 빈도(Backup Frequency)** 드롭다운 메뉴에서 **매시간(Hourly)**, **매일(Daily)** 또는 **매주(Weekly)**를 선택합니다. 요일, 시간 및 분 드롭다운 메뉴는 선택한 빈도에 따라 사용하지 않도록 설정됩니다. 예를 들어 매일을 선택하는 경우 매일 빈도에 적용되지 않는 요일 드롭다운 메뉴는 사용하지 않도록 설정됩니다.

b 매주 백업을 선택한 경우 데이터가 백업되는 요일을 선택합니다.

c 매주 또는 매일 백업을 선택한 경우 백업이 시작되는 시간을 선택합니다.

d 시작할 분을 선택하고 **스케줄(Schedule)**을 클릭합니다.

6 로그 데이터 및 흐름 데이터를 백업에서 제외하려면 제외 옆의 **변경(Change)**을 클릭합니다.

a 백업에서 제외할 항목을 선택합니다.

b **확인(OK)**을 클릭합니다.

7 FTP 서버 IP/호스트 이름, 자격 증명, 디렉토리 세부 정보 및 암호를 저장합니다. 이 정보는 백업을 복원할 때 필요합니다.

후속 작업

vShield Endpoint를 업그레이드합니다. vShield Endpoint용 NSX에서 Guest Introspection으로 업그레이드를 참조하십시오.

vShield Endpoint용 NSX에서 Guest Introspection으로 업그레이드

NSX Manager 버전에 맞춰 Guest Introspection을 업그레이드해야 합니다.

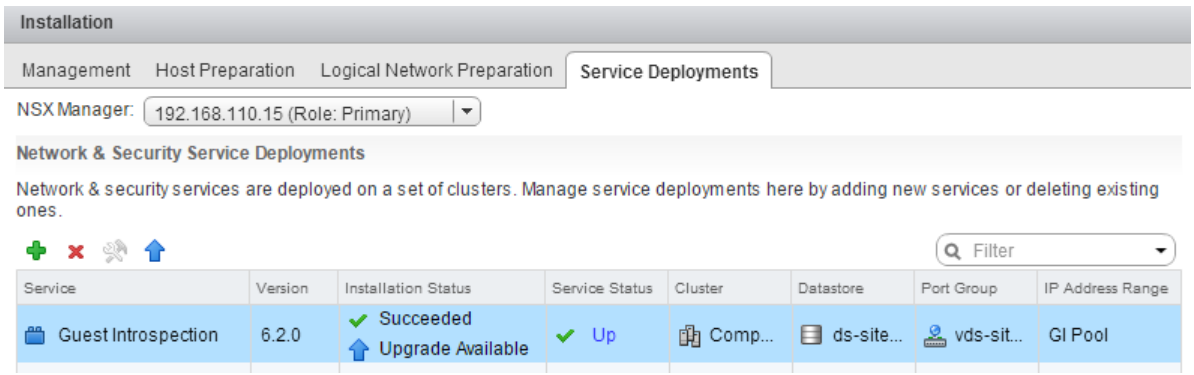
참고 Guest Introspection 서비스 VM은 vSphere Web Client에서 업그레이드할 수 있습니다. 이를 업그레이드하기 위해 NSX Manager를 업그레이드한 후에 서비스 VM을 삭제할 필요가 없습니다. 서비스 VM을 삭제하는 경우 에이전트 VM이 누락되므로 서비스 상태가 실패로 표시됩니다. **해결(Resolve)**을 클릭하여 새 서비스 VM을 배포한 다음 **업그레이드 사용 가능(Upgrade Available)**을 클릭하여 최신 Guest Introspection 서비스 VM을 배포합니다.

필수 조건

NSX Manager가 6.2.x로 업그레이드되었는지 확인합니다.

프로시저

1 **설치(Installation)** 탭에서 **서비스 배포(Service Deployments)**를 클릭합니다.

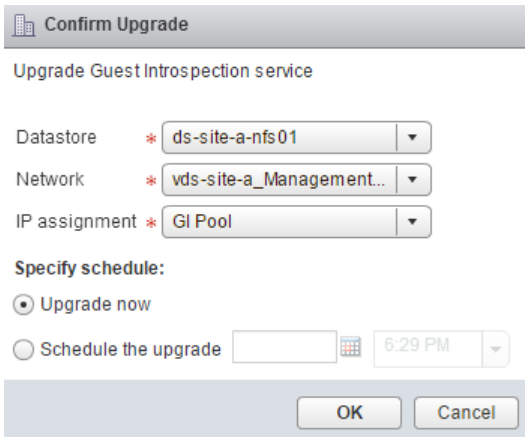


설치 상태(Installation Status) 열에 **업그레이드 사용 가능(Upgrade Available)**이 표시됩니다.

2 업그레이드할 Guest Introspection 배포를 선택합니다.

서비스 표 위의 도구 모음에서 **업그레이드(Upgrade)**(↑) 아이콘이 사용되도록 설정됩니다.

3 **업그레이드(Upgrade)**(⬆) 아이콘을 클릭하고 UI 메시지를 따릅니다.



Guest Introspection을 업그레이드한 후의 설치 상태는 성공이고 서비스 상태는 실행입니다. Guest Introspection 서비스 가상 시스템은 vCenter Server 인벤토리에 표시됩니다.

후속 작업

특정 클러스터에 대해 Guest Introspection이 업그레이드된 후에 파트너 솔루션을 업그레이드할 수 있습니다. 파트너 솔루션을 사용하도록 설정된 경우에는 파트너가 제공한 업그레이드 설명서를 참조하십시오. 파트너 솔루션이 업그레이드되지 않은 경우에도 보호는 유지됩니다.

파트너 솔루션을 NSX가 인증된 버전으로 업그레이드하는 경우 보호 기능을 유지하기 위해 Service Composer를 사용하여 파트너 솔루션을 기준으로 하는 정책을 생성해야 합니다. NSX 관리 가이드에서 "Service Composer 사용"을 참조하십시오.

사후 업그레이드 검사 목록

업그레이드가 완료된 후에 다음 단계를 따르십시오.

프로시저

1 업그레이드 후에 NSX Manager의 현재 백업을 생성합니다.

2 VIB가 호스트에 설치되었는지 확인합니다.

NSX에서 다음 VIB를 설치합니다.

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

Guest Introspection이 설치된 경우에는 호스트에 이 VIB가 있는지도 확인합니다.

```
esxcli software vib get --vibname epsec-mux
```

3 호스트 메시지 버스를 다시 동기화합니다. VMware에서는 모든 고객이 업그레이드 후에 다시 동기화를 수행하도록 권장합니다.

다음 API 호출을 사용하여 각 호스트에서 다시 동기화를 수행할 수 있습니다.

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST

Headers:

Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

vShield Endpoint용 NSX에서 파트너 서비스 사용

3

Guest Introspection을 사용하면 NSX 배포의 파트너 서비스를 사용할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- vShield Endpoint용 NSX에서 파트너 서비스 업그레이드
- 파트너 서비스 배포
- vShield Endpoint용 NSX에서 Service Composer 사용

vShield Endpoint용 NSX에서 파트너 서비스 업그레이드

vCloud Networking and Security에서 NSX로 업그레이드한 후에 파트너 서비스를 업그레이드해야 하거나 업그레이드하려고 할 수 있습니다.

필수 조건

호환성 및 업그레이드 세부 정보에 대해서는 파트너 서비스 설명서를 참조하십시오.

프로시저

1 파트너 관리 솔루션을 업그레이드합니다.

2 벤더의 콘솔에서 파트너 서비스를 NSX Manager에 등록합니다.

지침에 대해서는 파트너 서비스 설명서를 참조하십시오.

3 오래된 파트너 서비스 VM은 전원을 끄고 삭제합니다.

후속 작업

파트너 서비스 배포

파트너 서비스 배포

파트너 솔루션에 호스트 상주 가상 장치가 포함된 경우 솔루션을 NSX Manager에 등록한 후 서비스를 배포할 수 있습니다.

필수 조건

다음 사항을 충족하는지 확인하십시오.

- 파트너 솔루션이 NSX Manager에 등록되어 있는지 확인합니다.

- NSX Manager가 파트너 솔루션의 관리 콘솔에 액세스할 수 있는지 확인합니다.

프로시저

1. **네트워킹 및 보안(Networking & Security)**을 클릭하고 **설치(Installation)**를 클릭합니다.
2. **서비스 배포(Service Deployments)** 탭을 클릭하고 **새 서비스 배포(New Service Deployment)**( ) 아이콘을 클릭합니다.
3. 네트워크 및 보안 서비스 배포 대화상자에서 해당 솔루션을 선택합니다.
4. 대화상자 아래쪽의 **스케줄 지정(Specify schedule)**에서 **지금 배포(Deploy now)**를 선택하여 솔루션을 즉시 배포하거나 배포 날짜 및 시간을 선택합니다.
5. **다음(Next)**을 클릭합니다.
6. 솔루션을 배포할 데이터센터 및 클러스터를 선택하고 **다음(Next)**을 클릭합니다.
7. 솔루션 서비스 가상 시스템 스토리지를 추가할 데이터스토어를 선택하거나 **지정된 호스트(Specified on host)**를 선택합니다.

   선택한 데이터스토어는 선택한 클러스터의 모든 호스트에서 사용할 수 있어야 합니다.

   지정된 호스트(Specified on host)를 선택한 경우 ESX 호스트를 클러스터에 추가하기 전에 해당 ESX 호스트의 데이터스토어를 호스트의 **에이전트 VM 설정(AgentVM Settings)**에 지정해야 합니다. 자세한 내용은 vSphere API/SDK 설명서를 참조하십시오.
8. 관리 인터페이스를 호스팅할 분산 가상 포트 그룹을 선택합니다. 이 포트 그룹은 NSX Manager의 포트 그룹에 연결할 수 있어야 합니다.

   네트워크를 **지정된 호스트(Specified on host)**로 설정한 경우 클러스터에 있는 각 호스트의 **에이전트 VM 설정 > 네트워크(Agent VM Settings > Network)** 속성에 사용할 네트워크를 지정해야 합니다. 자세한 내용은 vSphere API/SDK 설명서를 참조하십시오.

   호스트를 클러스터에 추가하기 전에 호스트에 대해 에이전트 VM 네트워크 속성을 설정해야 합니다. **관리(Manage) > 설정(Settings) > 에이전트 VM 설정(Agent VM Settings) > 네트워크(Network)**로 이동하고 **편집(Edit)**을 클릭하여 에이전트 VM 네트워크를 설정합니다.

   선택한 포트 그룹은 선택한 클러스터의 모든 호스트에서 사용할 수 있어야 합니다.
9. IP 할당에서 다음 중 하나를 선택합니다.

선택	수행되는 작업
DHCP	DHCP(Dynamic Host Configuration Protocol)를 통해 IP 주소를 서비스 가상 시스템에 할당합니다.
IP 풀	선택한 IP 풀의 IP 주소를 서비스 가상 시스템에 할당합니다.

10. **다음(Next)**을 클릭한 후 [완료 준비] 페이지에서 **완료(Finish)**를 클릭합니다.
11. **설치 상태(Installation Status)**가 [성공]으로 표시될 때까지 배포를 모니터링합니다. 상태가 [실패]로 표시되면 [실패] 옆에 있는 아이콘을 클릭하고 오류를 해결할 조치를 취합니다.

후속 작업

이제 NSX UI 또는 NSX API를 통해 파트너 서비스를 사용할 수 있습니다.

vShield Endpoint용 NSX에서 Service Composer 사용

Service Composer는 네트워크 및 보안 서비스를 가상 인프라의 애플리케이션에 프로비저닝하고 할당하는 데 도움이 됩니다.

Service Composer를 사용하여 보안 그룹 및 보안 정책을 생성합니다. 보안 그룹에는 정적 및 동적 그룹 멤버 자격 정의가 포함될 수 있습니다. 보안 정책은 보안 그룹에 서비스를 적용합니다.

자세한 내용 및 지침에 대해서는 NSX 관리 가이드에서 Service Composer 설명서를 참조하십시오.