

VMware NSX for vSphere 6.3.4 릴리스 정보

VMware NSX for vSphere 6.3.4 | 릴리스 날짜: 2017년 10월 12일 | 빌드 7087695

이 문서의 [개정 이력](#)을 참조하십시오.

릴리스 정보에 포함된 내용

릴리스 정보에는 다음과 같은 항목이 포함됩니다.

- [NSX 6.3.4의 새로운 기능](#)
- [버전, 시스템 요구 사항 및 설치](#)
- [제거 및 지원 중단된 기능](#)
- [업그레이드 정보](#)
- [FIPS 준수](#)
- [개정 이력](#)
- [해결된 문제](#)
- [알려진 문제](#)

NSX 6.3.4의 새로운 기능

NSX 6.3.4에 대한 중요 정보: NSX for vSphere 6.3.4는 VMware 기술 자료 문서 [2151719](#) 및 [000051144](#)에서 언급된 문제를 해결하기 위해 다시 패키징되었습니다. 원래 릴리스된 빌드 6845891은 빌드 7087695로 대체됩니다. 자세한 내용은 기술 자료 문서를 참조하십시오. 업그레이드 정보를 보려면 [업그레이드 정보](#)를 참조하십시오.

NSX for vSphere 6.3.4는 다양한 특정 고객 버그를 해결합니다. 자세한 내용은 [해결된 문제](#)를 참조하십시오.

이전 버전에 대한 릴리스 정보를 확인하십시오.

- [NSX 6.3.3](#)
- [NSX 6.3.2](#)
- [NSX 6.3.1](#)
- [NSX 6.3.0](#)

버전, 시스템 요구 사항 및 설치

참고:

- 다음 표에서는 권장 VMware 소프트웨어 버전을 나열합니다. 이러한 권장 릴리스는 일반적인 것이며, 환경별 권장 사항을 대신하거나 재정의하지 않습니다.
- 이 정보는 이 문서 발행 당시를 기준으로 최신 정보입니다.
- NSX 및 기타 VMware 제품의 **최소 지원** 버전에 대해서는 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오. VMware는 내부 테스트를 기준으로 최소 지원 버전을 선언합니다.
 - **NSX 상호 운용성에 필요한 vSphere 최소 지원 버전이 NSX 6.3.2와 NSX 6.3.3 간에 변경되었습니다.** 자세한 내용은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

제품 또는 구성 요소	권장 버전
NSX for vSphere	<p>새로 배포할 경우 및 6.1.x에서 업그레이드할 때는 최신 NSX 6.3 릴리스가 권장됩니다.</p> <p>기존 배포를 업그레이드할 경우 업그레이드를 계획하기 전에 특정 문제에 관한 자세한 내용은 NSX 릴리스 정보를 검토하거나 VMware 기술 지원 담당자에게 문의하십시오.</p>
vSphere	<ul style="list-style-type: none"> • vSphere 5.5U3 이상 • vSphere 6.0U3 이상. vSphere 6.0U3는 vCenter Server를 재부팅한 후 ESXi 호스트에서의 중복 VTEP 문제를 해결합니다. 자세한 내용은 VMware 기술 자료 문서 2144605를 참조하십시오. • vSphere 6.5U1 이상. vSphere 6.5U1은 OutOfMemory로 인한 EAM 실패 문제를 해결합니다. 자세한 내용은 VMware 기술 자료 문서 2135378을 참조하십시오.
Windows용 Guest Introspection	<p>모든 VMware Tools 버전이 지원됩니다. 일부 Guest Introspection 기반의 기능에는 최신 VMware Tools 버전이 필요합니다.</p> <ul style="list-style-type: none"> • VMware Tools와 함께 패키지로 제공되는 선택적 Thin Agent Network Introspection Driver 구성 요소를 사용하도록 설정하려면 VMware Tools 10.0.9 및 10.0.12를 사용합니다. • NSX/vCloud Networking and Security에서 VMware Tools를 업그레이드한 후에 VM이 느려지는 문제를 해결하려면 VMware Tools 10.0.8 이상으로 업그레이드합니다(VMware 기술 자료 문서 2144236 참조). • Windows 10 지원을 위해 VMware Tools 10.1.0 이상을 사용합니다. • Windows Server 2016 지원을 위해 VMware Tools 10.1.10 이상을 사용합니다.
Linux용 Guest Introspection	<p>이 NSX 버전은 다음 Linux 버전을 지원합니다.</p> <ul style="list-style-type: none"> • RHEL 7 GA(64비트) • SLES 12 GA(64비트) • Ubuntu 14.04 LTS(64비트)

참고: VMware는 현재 vRealize Networking Insight 3.2를 사용하는 NSX for vSphere 6.3.x를 지원하지 않습니다.

시스템 요구 사항 및 설치

NSX 설치 사전 요구 사항의 전체 목록을 보려면 "NSX 설치 가이드"에서 [NSX 시스템 요구 사항](#) 섹션을 참조하십시오.

설치 지침을 보려면 [NSX 설치 가이드](#) 또는 [크로스 vCenter NSX 설치 가이드](#)를 참조하십시오.

제거 및 지원 중단된 기능

수명 종료 또는 지원 종료 경고

곧 업그레이드해야 하는 NSX 및 기타 VMware 제품에 대한 자세한 내용은 [VMware 수명 주기 제품 매트릭스](#)를 참조하십시오.

- **NSX for vSphere 6.1.x**는 2017년 1월 15일에 EOA(End of Availability) 및 EOGS(End of General Support)에 도달했습니다. ([VMware 기술 자료 문서 2144769](#)도 참조하십시오.)
- **NSX Data Security가 제거됨:** NSX 6.3.0에서 NSX Data Security 기능이 제품에서 제거되었습니다.
- **NSX Activity Monitoring(SAM)이 더 이상 지원되지 않음:** NSX 6.3.0을 기준으로 Activity Monitoring은 더 이상 NSX의 기능으로 지원되지 않습니다. 교체 기능으로 Endpoint Monitoring을 사용하십시오. 자세한 내용은 NSX 관리 가이드의 [Endpoint Monitoring](#)을 참조하십시오.
- **Web Access Terminal이 제거됨:** WAT(Web Access Terminal)가 NSX 6.3.0에서 제거되었습니다. Web Access SSL VPN-Plus를 구성할 수 없으며 NSX Edge를 통해 공개 URL 액세스를 사용하도록 설정할 수 없습니다. VMware에서는 보안 향상을 위해 SSL VPN 배포에서 전체 액세스 클라이언트를 사용할 것을 권장합니다. 이전 릴리스에서 WAT 기능을 사용하고 있는 경우 6.3.0으로 업그레이드하려면 이 기능을 사용하지 않도록 설정해야 합니다.
- **IS-IS가 NSX Edge에서 제거됨:** NSX 6.3.0에서는 라우팅 탭에서 IS-IS 프로토콜을 구성할 수 없습니다.
- **vCNS Edge가 더 이상 지원되지 않음.** NSX 6.3.x로 업그레이드하기 전에 먼저 NSX Edge로 업그레이드해야 합니다.

API 제거 및 동작 변경

방화벽 구성 또는 기본 섹션 삭제:

- 기본 섹션이 지정된 경우 방화벽 섹션 삭제 요청은 이제 거부됩니다. DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId
- 기본 구성을 설정하기 위해 새 메서드가 도입되었습니다. 이 메서드의 결과를 사용하여 전체 구성 또는 기본 섹션을 대체합니다.
 - GET /api/4.0/firewall/globalroot-0/defaultconfig를 사용하여 기본 구성 설정
 - PUT /api/4.0/firewall/globalroot-0/config를 사용하여 전체 구성 업데이트
 - PUT /4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}를 사용하여 단일 섹션 업데이트

논리적(분산) 라우터 NSX Edge 장치에 대해서만 **defaultOriginate** 매개 변수가 다음 메서드로부터 제거됨:

- GET/PUT /api/4.0/edges/{edge-id}/routing/config/ospf
- GET/PUT /api/4.0/edges/{edge-id}/routing/config/bgp
- GET/PUT /api/4.0/edges/{edge-id}/routing/config

NSX 6.3.0 이상 논리적 (분산) 라우터 Edge 장치에서 defaultOriginate를 true로 설정하면 실패합니다.

모든 IS-IS 메서드가 NSX Edge 라우팅에서 제거됨

- GET/PUT/DELETE /4.0/edges/{edge-id}/routing/config/isis
- GET/PUT /4.0/edges/{edge-id}/routing/config

CLI 제거 및 동작 변경

NSX Controller 노드에서 지원되지 않는 명령을 사용하지 않도록 할 것

NSX Controller 노드에서 NTP 및 DNS를 구성하기 위한 문서화되지 않은 명령이 있습니다. 이러한 명령은 지원되지 않으므로 NSX Controller 노드에서 사용하지 않아야 합니다. NSX CLI 가이드에 나오는 명령만 사용해야 합니다.

업그레이드 정보

- [일반 업그레이드 정보](#)
- [NSX 구성 요소에 대한 업그레이드 정보](#)
- [FIPS에 대한 업그레이드 정보](#)

참고: 설치 및 업그레이드에 영향을 주는 알려진 문제 목록은 [설치 및 업그레이드에 대한 알려진 문제](#) 섹션을 참조하십시오.

일반 업그레이드 정보

- **NSX 6.3.4 빌드 6845891에서 NSX 6.3.4 빌드 7087695로 업그레이드:** 이 업그레이드에는 NSX Manager 및 NSX Controller 클러스터 업그레이드만 필요합니다. 호스트, NSX Edge 및 Guest Introspection은 업그레이드할 필요가 없습니다.
- **전체 NSX 업그레이드:** NSX를 업그레이드하려면 호스트 클러스터 업그레이드(호스트 VIB를 업그레이드)를 포함하여 전체 NSX 업그레이드를 수행해야 합니다. 지침을 보려면 [호스트 클러스터 업그레이드](#) 섹션을 포함한 [NSX 업그레이드 가이드](#)를 참조하십시오.
- **시스템 요구 사항:** NSX를 설치하고 업그레이드할 때의 시스템 요구 사항에 관해서는 NSX 설명서의 [NSX의 시스템 요구 사항](#) 섹션을 참조하십시오.
- **NSX 6.x에서의 업그레이드 경로:** [VMware 제품 상호 운용성 매트릭스](#)에는 VMware NSX에서의 업그레이드 경로에 대한 자세한 내용이 나와 있습니다. 크로스 vCenter NSX 업그레이드는 [NSX 업그레이드 가이드](#)에서 다룹니다.
- **다운그레이드는 지원되지 않습니다.**
 - 항상 업그레이드를 진행하기 전에 NSX Manager의 백업을 캡처하십시오.
 - NSX가 업그레이드되면 NSX를 다운그레이드할 수 없습니다.
- NSX 6.3.x로의 업그레이드에 성공했는지 **검증**하려면 [기술 자료 문서 2134525](#)를 참조하십시오.
- vCloud Networking and Security에서 NSX 6.3.x로의 업그레이드는 지원되지 않습니다. 먼저 지원되는 6.2.x 릴리스로 업그레이드해야 합니다.
- **상호 운용성:** 업그레이드하기 전에 모든 관련 VMware 제품에 대한 [VMware 제품 상호 운용성 매트릭스](#)를 확인하십시오.
 - **vSphere 6.5a 이상으로 업그레이드:** vSphere 5.5 또는 6.0에서 vSphere 6.5a 이상으로 업그레이드하는 경우 먼저 NSX 6.3.x로 업그레이드해야 합니다. NSX 업그레이드 가이드에서 [NSX 환경에서 vSphere 업그레이드](#)를 참조하십시오.
참고: NSX 6.2.x는 vSphere 6.5와 호환되지 않습니다.
 - **NSX 6.3.3 이상으로 업그레이드:** 최소 지원 버전의 vSphere for NSX 상호 운용성이 NSX 6.3.2와 NSX 6.3.3 간에 변경되었습니다. 자세한 내용은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.
- **파트너 서비스 호환성:** 사이트에서 Guest Introspection 또는 네트워크 검사에 대해 VMware 파트너 서비스를 사용하는 경우 업그레이드하기 전에 [VMware 호환성 가이드](#)를 검토하여 벤더의 서비스가 이 NSX 릴리스와 호환되는지 확인해야 합니다.
- **Networking and Security 플러그인:** NSX Manager를 업그레이드한 후에 로그아웃했다가 vSphere Web Client에 다시 로그인해야 합니다. NSX 플러그인이 제대로 표시되지 않으면 브라우저 캐시 및 기록을 지우십시오. Networking and Security 플러그인이 vSphere Web Client에 나타나지 않으면 [NSX 업그레이드 가이드](#)에 설명된 대로 vSphere Web Client 서버를 재설정하십시오.
- **상태 비저장 환경:** 상태 비저장 호스트 환경에서 NSX를 업그레이드할 경우, NSX 업그레이드 프로세스 중에 새로운 VIB가 호스트 이미지 프로파일에 미리 추가됩니다. 그 결과 상태 비저장 호스트의 NSX에 대한 업그레이드 프로세스는 다음과 같은 순서로 진행됩니다.
NSX 6.2.0 전에는 특정 버전의 ESX 호스트에 대한 VIB를 찾을 수 있는 URL이 NSX Manager에 하나밖에 없었습니다. 즉, 관리자는 NSX 버전에 관계없이 하나의 URL만 알고 있으면 되었습니다. NSX 6.2.0 이상에서는 새로운 NSX VIB가 서로 다른 URL을 통해 제공됩니다. 올바른 VIB를 찾으려면 다음과 같은 단계를 수행해야 합니다.

1. <https://<NSXManager>/bin/vdn/nwfabric.properties>에서 새 VIB URL을 찾습니다.
2. 해당하는 URL에서 필요한 ESX 호스트 버전의 VIB를 가져옵니다.
3. 그런 다음 VIB를 호스트 이미지 프로파일에 추가합니다.

NSX 구성 요소에 대한 업그레이드 정보

NSX Manager 업그레이드

- SFTP for NSX 백업을 사용하는 경우 hmac-sha1에 대한 지원이 없으므로 6.3.x로 업그레이드한 후 hmac-sha2-256으로 변경합니다. 6.3.x에서 지원되는 보안 알고리즘 목록은 [VMware 기술 자료 문서 2149282](#)를 참조하십시오.
- NSX 6.3.3에서 NSX 6.3.4로 업그레이드하려는 경우 [VMware 기술 자료 문서 2151719](#)의 해결 방법 지침을 먼저 수행해야 합니다.

Controller 업그레이드

- NSX 6.3.3에서 NSX Controller 장치 디스크 크기가 20GB에서 28GB로 변경되었습니다.
- NSX Controller 클러스터는 3개의 컨트롤러 노드를 포함하여 NSX 6.3.3으로 업그레이드해야 합니다. 컨트롤러가 3개보다 적으면 업그레이드를 시작하기 전에 컨트롤러를 추가해야 합니다. 자세한 내용은 [NSX Controller 클러스터 배포](#)를 참조하십시오.
- NSX 6.3.3에서는 NSX Controller의 기본 운영 체제가 변경됩니다. 즉, NSX 6.3.2 또는 이전 버전에서 NSX 6.3.3 이상으로 업그레이드할 경우 인플레이스 소프트웨어 업그레이드 대신, 기존 컨트롤러가 한 번에 하나씩 삭제되고 새 Photon OS 기반 컨트롤러가 동일한 IP 주소를 사용해서 배포됩니다. [NSX Controller 클러스터 업그레이드](#)를 참조하십시오.

호스트 클러스터 업그레이드

- NSX 6.3.3에서는 NSX VIB 이름이 변경됩니다. NSX 6.3.3 이상이 설치된 경우 esx-vxlan 및 esx-vsip VIB가 esx-nsxv로 교체됩니다.
- **호스트에서 재부팅이 필요 없는 업그레이드 및 제거:** vSphere 6.0 이상에서는 NSX 6.3.x로 업그레이드하고 나면 다음 NSX VIB 변경 시 재부팅이 필요 없습니다. 대신 호스트는 VIB 변경을 완료하도록 유지 보수 모드를 입력해야 합니다.

호스트 재부팅은 다음 작업 동안 필요하지 않습니다.

- ESXi 6.0 이상에서 NSX 6.3.0에서 NSX 6.3.x로의 업그레이드.
 - 6.0에서 6.5.0a 이상으로 ESXi를 업그레이드한 후 필요한 NSX 6.3.x VIB 설치.
- 참고: ESXi 업그레이드에는 계속 호스트 재부팅이 필요합니다.

- ESXi 6.0 이상에서의 NSX 6.3.x VIB 제거.

호스트 재부팅은 다음 작업 동안 필요합니다.

- NSX 6.2.x 이하에서 NSX 6.3.x로의 업그레이드(모든 ESXi 버전).
- ESXi 5.5에서 NSX 6.3.0에서 NSX 6.3.x로의 업그레이드.
- 5.5에서 6.0 이상으로 ESXi를 업그레이드한 후 필요한 NSX 6.3.x VIB 설치.
- ESXi 5.5에서 NSX 6.3.x VIB 제거.
- **호스트가 설치 중 상태로 중단될 수 있음:** 대규모 NSX 업그레이드 동안 호스트가 장시간 설치 중 상태로 중단될 수 있습니다. 이 문제는 이전 NSX VIB의 제거와 관련된 문제 때문에 발생할 수 있습니다. 이 경우 이 호스트와 연결된 EAM 스레드가 VI Client 작업 목록에서 중단된 상태로 보고됩니다.
해결 방법: 다음을 수행합니다.
 - VI Client를 사용하여 vCenter에 로그인합니다.
 - 중단된 EAM 작업을 마우스 오른쪽 버튼으로 클릭하고 취소합니다.
 - vSphere Web Client에서 클러스터에 대해 [해결]을 실행합니다. 중단된 호스트가 이제 [진행 중]으로 표시될 것입니다.
 - 호스트에 로그인하고 재부팅을 실행하여 해당 호스트에 대한 업그레이드를 강제로 완료합니다.

NSX Edge 업그레이드

- NSX 6.3.0에서 NSX Edge 장치 디스크 크기가 변경되었습니다.
 - 소형, 대형, 4배 대형: 584MB 디스크 1개 + 512MB 디스크 1개
 - 2배 대형: 584MB 디스크 1개 + 2GB 디스크 1개 + 256MB 디스크 1개
- NSX Edge 장치로 업그레이드하기 전에 NSX에 사용할 수 있게 호스트 클러스터를 준비해야 합니다. VIX 채널을 통한 NSX Manager 및 Edge 간 관리부 통신이 6.3.0부터 더 이상 지원되지 않습니다. 메시지 버스 채널만 지원됩니다. NSX 6.2.x 이하 버전에서 NSX 6.3.0 이상으로 업그레이드할 때는 NSX Edge 장치가 배포된 호스트 클러스터가 NSX에 사용할 수 있게 준비되어 있는지와 메시징 인프라 상태가 녹색인지 확인해야 합니다. 호스트 클러스터가 NSX에 사용할 수 있게 준비되지 않은 경우 NSX Edge 장치 업그레이드가 실패합니다. 자세한 내용은 *NSX 업그레이드 가이드*의 [NSX Edge 업그레이드](#)를 참조하십시오.
- ESG(Edge Services Gateway) 업그레이드:
NSX 6.2.5부터 NSX Edge 업그레이드 시에 리소스 예약이 수행됩니다. 리소스가 부족한 클러스터에서 vSphere HA가 사용되도록 설정되면 vSphere HA 제약 조건 위반으로 인해 업그레이드 작업이 실패할 수 있습니다.
이러한 업그레이드 실패를 방지하려면 ESG를 업그레이드하기 전에 다음 단계를 수행하십시오.

설치 또는 업그레이드 시에 값을 명시적으로 설정하지 않은 경우 다음 리소스 예약이 NSX Manager에서 사용됩니다.

NSX Edge 폼 팩터	CPU 예약	메모리 예약
소형	1000MHz	512MB
대형	2000MHz	1024MB
4배 대형	4000MHz	2048MB
초대형	6000MHz	8192MB

1. 항상 vSphere HA에 대한 모범 사례에 따라 설치를 수행합니다. [기술 자료 문서 1002080](#) 문서를 참조하십시오.
 2. NSX 튜닝 구성 API를 사용합니다.
PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>
edgeVCpuReservationPercentage 및 edgeMemoryReservationPercentage 값이 폼 팩터에 대해 사용 가능한 리소스 범위 내에 있는지 확인합니다(기본값은 위의 표 참조).
- vSphere HA가 사용되도록 설정되고 Edge가 배포되는 경우 vSphere의 [가상 시스템 시작] 옵션을 사용하지 않도록 설정합니다. 6.2.4 또는 이전 NSX Edge를 6.2.5 이상으로 업그레이드한 후 vSphere HA가 사용되도록 설정되고 Edge가 배포된 클러스터에서 각 ESX Edge에 대해 vSphere [가상 시스템 시작] 옵션을 해제해야 합니다. 이를 수행하려면 vSphere Web Client를 열고, NSX Edge 가상 시스템이 있는 ESXi 호스트를 찾은 다음 [관리] > [설정]을 클릭하고 가상 시스템 아래에서 [VM 시작/종료]를 선택하고 [편집]을 클릭한 다음 가상 시스템이 수동 모드인지 확인합니다(즉, [자동 시작/종료] 목록에 추가되어 있지 않아야 합니다).
 - NSX 6.2.5 이상으로 업그레이드하기 전에 모든 로드 밸런서 암호 목록이 콜론으로 구분되어야 합니다. 암호 목록이 쉽표 등의 다른 구분 기호를 사용하는 경우 https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles에 PUT 호출을 수행하고 <clientSsl> 및 <serverSsl>에 있는 각 <ciphers> 목록을 콜론으로 구분된 목록으로 교체합니다. 예를 들어 요청 본문의 관련 세그먼트는 다음과 같이 표시될 수 있습니다. 모든 애플리케이션 프로파일에 대해 다음 절차를 반복하십시오.

```
<applicationProfile>  
<name>https-profile</name>
```

```

<insertXForwardedFor>false</insertXForwardedFor>
<sslPassthrough>false</sslPassthrough>
<template>HTTPS</template>
<serverSslEnabled>true</serverSslEnabled>
<clientSsl>
  <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
  <clientAuth>ignore</clientAuth>
  <serviceCertificate>certificate-4</serviceCertificate>
</clientSsl>
<serverSsl>
  <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
  <serviceCertificate>certificate-4</serviceCertificate>
</serverSsl>
...
</applicationProfile>

```

- **6.2.0 이전의 vROP 버전에서 로드 밸런싱된 클라이언트에 대한 올바른 암호 버전 설정:** 6.2.0 이전 vROP 버전의 vROP 풀 멤버는 TLS 버전 1.0을 사용하므로 NSX 로드 밸런서 구성에서 "ssl-version=10"을 설정하여 모니터 확장 값을 명시적으로 설정해야 합니다. 지침에 대해서는 NSX 관리 가이드의 [서비스 모니터 생성](#)을 참조하십시오.

```

{
  "expected" : null,
  "extension" : "ssl-version=10",
  "send" : null,
  "maxRetries" : 2,
  "name" : "sm_vrops",
  "url" : "/suite-api/api/deployment/node/status",
  "timeout" : 5,
  "type" : "https",
  "receive" : null,
  "interval" : 60,
  "method" : "GET"
}

```

FIPS에 대한 업그레이드 정보

NSX 6.3.0 이전의 NSX 버전에서 NSX 6.3.0 이상으로 업그레이드하는 경우 업그레이드를 완료하기 전에 FIPS 모드를 사용하도록 설정해서는 안 됩니다. 업그레이드를 완료하기 전에 FIPS 모드를 사용하도록 설정하면 업그레이드된 구성 요소와 업그레이드되지 않은 구성 요소 간 통신이 중단됩니다. 자세한 내용은 NSX 업그레이드 가이드에서 [FIPS 모드 및 NSX 업그레이드 이해](#)를 참조하십시오.

- OS X Yosemite 및 OS X El Capitan에서 지원되는 암호: OS X 10.11(El Capitan)에서 SSL VPN 클라이언트를 사용 중인 경우 AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA38, AES256-SHA 및 AES128-SHA 암호를 사용하여 연결할 수 있으며 OS X 10.10(Yosemite)을 사용 중인 경우 AES256-SHA 및 AES128-SHA 암호만 사용하여 연결할 수 있습니다.
- NSX 6.3.x로의 업그레이드가 완료되기 전에는 FIPS를 사용하도록 설정하지 마십시오. 자세한 내용은 NSX 업그레이드 가이드에서 [FIPS 모드 및 NSX 업그레이드 이해](#)를 참조하십시오.
- FIPS를 사용하도록 설정하기 전에 파트너 솔루션이 FIPS 모드 인증을 받았는지 확인하십시오. [VMware 호환성 가이드](#) 및 관련 파트너 설명서를 참조하십시오.

FIPS 준수

- **NSS 및 OpenSwan:** NSX Edge IPsec VPN은 Mozilla NSS 암호화 모듈을 사용합니다. 중요한 보안 문제로 인해 이 버전의 NSX는 FIPS 140-2 유효성이 검사되지 않은 최신 버전의 NSS를 사용합니다. VMware에서는 해당 모듈이 제대로 작동한다고 확인하지만 이 모듈은 더 이상 공식적으로 유효성이 검사되지 않습니다.
- **NSS 및 암호 입력:** NSX Edge 암호 해시는 Mozilla NSS 암호화 모듈을 사용합니다. 중요한 보안 문제로 인해 이 버전의 NSX는 FIPS 140-2 유효성이 검사되지 않은 최신 버전의 NSS를 사용합니다. VMware에서는 해당 모듈이 제대로 작동한다고 확인하지만 이 모듈은 더 이상 공식적으로 유효성이 검사되지 않습니다.
- **Controller 및 클러스터링 VPN:** NSX Controller는 IPsec VPN을 사용하여 Controller 클러스터를 연결합니다. IPsec VPN은 CMVP 유효성 검사 중인 VMware Linux 커널 암호화 모듈(Photon 1 환경)을 사용합니다.

문서 개정 이력

2017년 10월 12일: 1차 개정판.

2017년 10월 27일: 2차 개정판. 알려진 문제 1965859를 추가함.

2017년 11월 9일: 3차 개정판. 6.3.4에 대한 새 빌드 정보를 추가함. 해결된 문제 1989763을 추가함. 알려진 문제를 추가함: 1783528, 1843197.

2019년 5월 13일: 4차 개정판. 호스트 클러스터 업그레이드 섹션이 업데이트되었습니다.

해결된 문제

해결된 문제는 다음과 같이 분류됩니다.

- [NSX 6.3.4에서 해결된 논리적 네트워킹 및 Edge 서비스 관련 문제](#)
- [NSX 6.3.4에서 해결된 NSX Controller 관련 문제](#)

NSX 6.3.4에서 해결된 논리적 네트워킹 및 Edge 서비스 관련 문제

- **해결된 문제 1970527:** 논리적 분산 라우터 ARP 테이블이 5K 제한을 초과할 경우 ARP가 VM을 확인하지 못함
6.3.4에서 해결되었습니다.
- **해결된 문제 1961105:** 컨트롤러 재부팅 시 하드웨어 VTEP 연결이 끊어짐
특정 하드웨어 VTEP 구성이 NSX Manager에서 NSX Controller로 푸시될 때 BufferOverflow 예외가 표시됩니다. 이 오버플로우 문제로 인해 NSX Controller에서 완전한 하드웨어 게이트웨이 구성을 얻지 못합니다.
6.3.4에서 해결되었습니다.

NSX 6.3.4에서 해결된 NSX Controller 관련 문제

- **해결된 문제 1955855:** API 서버 참조 파일의 정리로 인해 컨트롤러 API가 실패함
필요한 파일 정리 시, traceflow 및 중앙 CLI와 같은 워크플로우가 실패합니다. 외부 이벤트로 인해 NSX Manager와 컨트롤러 간의 영구 TCP 연결이 중단되면 NSX Manager는 컨트롤러에 대해 API 연결을 설정하는 능력을 상실하며 UI에 컨트롤러의 연결이 끊어진 것으로 표시됩니다. 데이터 경로에는 영향을 미치지 않습니다.
6.3.4에서 해결되었습니다.
- **문제 1989763:** 사용자 계정의 암호 만료로 인해 NSX Controller를 배포하지 못함
NSX Controller의 사용자 계정 만료 기간은 90일입니다. 이로 인해 NSX Controller가 빌드된 지 90일 이후에 배포된 경우 암호가 즉시 만료되게 됩니다. 데이터 경로에 미치는 영향은 없습니다.

해결 방법: [VMware 기술 자료 문서 000051144](#)를 참조하십시오.

NSX 6.3.3 빌드 7087283 및 NSX 6.3.4 빌드 7087695에서 해결되었습니다.

알려진 문제

알려진 문제는 다음과 같이 분류됩니다.

- 일반적인 알려진 문제
- 설치 및 업그레이드에 대한 알려진 문제
- NSX Controller에 대한 알려진 문제
- 논리적 네트워킹 및 NSX Edge에 대한 알려진 문제
- 보안 서비스에 대한 알려진 문제
- 모니터링 서비스에 대한 알려진 문제
- 솔루션 상호 운용성에 대한 알려진 문제

일반적인 알려진 문제

- **문제 1874863: 논리 인증 서버에서 sslvpn 서비스 사용 안 함/사용 설정 후 변경된 암호로 인증을 받을 수 없음**
SSL VPN 서비스가 사용되지 않도록 설정되었다가 다시 사용되도록 설정되고 로컬 인증을 사용할 경우 사용자는 변경된 암호로 로그인할 수 없습니다.

자세한 내용은 [VMware 기술 자료 문서 2151236](#)을 참조하십시오.

- **문제 1702339: 취약성 스캐너가 Quagga bgp_dump_routes 취약성 CVE-2016-4049를 보고할 수 있음**
취약성 스캐너가 NSX for vSphere에서 Quagga bgp_dump_routes 취약성 CVE-2016-4049를 보고할 수 있습니다. NSX for vSphere는 Quagga를 사용하지만 BGP 기능(취약성 포함)이 사용되지 않도록 설정됩니다. 이 취약성 경고는 무시해도 안전합니다.

해결 방법: 제품이 취약해지지 않으므로 해결 방법도 필요하지 않습니다.

- **문제 1740625, 1749975: Firefox 및 Safari에서의 Mac OS UI 문제**
Mac OS에서 Firefox 또는 Safari를 사용하는 경우 vSphere 6.5 Web Client의 [Networking & Security] 페이지에 있는 NSX Edge에서 [뒤로 탐색] 버튼이 작동하지 않으며 Firefox에서 UI가 응답하지 않는 경우가 있습니다.

해결 방법: Mac OS에서 Google Chrome을 사용하거나 [홈] 버튼을 클릭한 다음 필요에 따라 계속 진행합니다.

- **문제 1700980: 보안 패치 CVE-2016-2775의 경우 쿼리 이름이 너무 길면 lwresd에서 세분화 오류가 발생할 수 있음**
NSX 6.2.4는 BIND 9.10.4를 함께 설치하지만 *named.conf*에서 lwres 옵션을 사용하지 않으므로 제품이 취약해지지 않습니다.

해결 방법: 제품이 취약해지지 않으므로 해결 방법도 필요하지 않습니다.

- **문제 1568180: vCSA(vCenter Server Appliance) 5.5 사용 시 잘못된 NSX 기능 목록**
라이센스를 선택하고 **작업 > 기능 보기**를 클릭하면 vSphere Web Client에서 라이선스의 기능을 볼 수 있습니다. NSX 6.2.3으로 업그레이드하면 라이선스가 Enterprise 라이선스로 업그레이드되어 모든 기능을 사용할 수 있게 됩니다. 그러나 vCSA(vCenter Server Appliance) 5.5에 NSX Manager가 등록되어 있는 경우에 **기능 보기**를 선택하면 새 Enterprise 라이선스가 아닌 업그레이드 전에 사용하던 라이선스의 기능 목록이 표시됩니다.

해결 방법: vSphere Web Client에 올바르게 표시되지 않는 경우라도 모든 Enterprise 라이선스는 기능이 동일합니다. 자세한 내용은 [NSX 라이선싱 페이지](#)를 참조하십시오.

설치 및 업그레이드에 대한 알려진 문제

업그레이드하기 전에 이 문서의 앞부분에 나와 있는 [업그레이드 정보](#) 섹션을 읽으십시오.

- **문제 1932907: Guest Introspection SVM 업그레이드가 실패함**
Guest Introspection SVM을 업그레이드하려고 할 때 GI SVM의 설치 상태가 '실패'로 표시됩니다. 이러한 현상은 클러스터에 있는 하나 또는 여러 개의 호스트에 대한 GI-SVM에도 해당될 수 있습니다.

해결 방법:

1. VC에서 GI-SVM을 삭제합니다.
2. GI-SVM 서비스 배포 창에서 **[해결]**을 클릭합니다. 그러면 GI-SVM이 다시 배포됩니다.

● **문제 1848058: ESXi 호스트 VIB의 NSX 6.3.2 업그레이드가 실패할 수 있음**

경우에 따라 ESXi 호스트 VIB를 NSX 6.3.2로 업그레이드하는 동안 이전 VIB 디렉토리가 NSX Manager에서 삭제되어 업그레이드가 실패합니다. [해결] 버튼을 클릭해도 문제가 해결되지 않습니다.

해결 방법: 이러한 문제로부터 복구하려면 업그레이드 API를 사용하십시오.

PUT <https://<nsx-mgr-ip>/api/2.0/nwfabric/configure>

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.vxlan</featureId>
  <resourceConfig>
    <resourceId>domain-cXX</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

여기에서 <nsx-mgr-ip>는 NSX Manager의 IP 주소이며 domain-cXX는 클러스터의 도메인 ID입니다.

● **문제 1747217: ESXi 호스트를 준비하면 muxconfig.xml.bad 파일이 만들어지고 Guest Introspection이 제대로 작동하지 않음**

"vmx path"가 VM 중 하나의 muxconfig.xml에 없는 경우 MUX에서 구성 파일을 구문 분석하려고 할 때 "xml path" 속성을 찾지 못하면 구성 파일 이름을 "muxconfig.xml.bad"로 바꾸고 USVM에 "오류 - MUX 구성 구문 분석"을 전송한 후 구성 채널을 닫습니다.

해결 방법: vCenter 인벤토리에서 분리된 VM을 제거합니다.

● **문제 1859572: vCenter 버전 6.0.0에 의해 관리되는 ESXi 호스트에서 NSX VIB 버전 6.3.x를 제거하는 동안 호스트가 계속 유지 보수 모드를 유지함**

클러스터에서 NSX VIB 버전 6.3.x를 제거하는 경우 워크플로에서 EAM 서비스에 의해 호스트가 유지 보수 모드로 전환되고, VIB가 제거된 다음 호스트가 유지 보수 모드에서 제거됩니다. 그렇지만 이러한 호스트가 vCenter Server 버전 6.0.0에서 관리되는 경우 VIB 제거 후에 호스트가 유지 보수 모드 상태를 계속 유지하게 됩니다. VIB를 제거하는 일을 담당하는 EAM 서비스는 호스트를 유지 보수 모드로 전환하지만 유지 보수 모드를 종료하지 못합니다.

해결 방법: 수동으로 호스트의 유지 보수 모드를 종료합니다. 이 문제는 호스트가 vCenter Server 버전 6.5a 이상에서 관리되는 경우에는 나타나지 않습니다.

● **문제 1435504: 6.0.x 또는 6.1.x에서 6.3.x로 업그레이드한 후에 HTTP/HTTPS 상태 검사가 다운된 것으로 표시되고 실패 이유로 "반환 코드 127이 범위를 벗어났습니다. 플러그인이 없을 수 있습니다."가 표시됨**
NSX 6.0.x 및 6.1.x 릴리스에서 큰따옴표(“) 없이 URL을 구성하면 상태 검사가 다음 오류를 나타내며 실패합니다. "반환 코드 127이 범위를 벗어났습니다. 플러그인이 없을 수 있습니다." 이 문제의 해결 방법은 입력 URL에 큰따옴표(“)를 추가하는 것입니다(전송/수신/예상 필드에는 필요하지 않음). 그렇지만 이 문제는 6.2.0에서 해결되었으므로 6.0.x 또는 6.1.x에서 6.3.x로 업그레이드하는 경우 큰따옴표를 추가하면 상태 검사에서 폴 멤버가 다운된 것으로 표시됩니다.

해결 방법: 업그레이드 후에는 모든 관련 상태 검사 구성의 URL 필드에서 큰따옴표(“)를 제거합니다.

● **문제 1734245: 데이터 보안으로 인해 6.3.0으로의 업그레이드가 실패함**

데이터 보안이 서비스 정책의 일부로 구성되어 있는 경우 6.3.0으로의 업그레이드가 실패합니다. 업그레이드하기 전 모든 서비스 정책에서 데이터 보안을 제거했는지 확인합니다.

● **문제 1801685: 호스트 연결 오류로 인해 6.2.x에서 6.3.0으로의 업그레이드 후 ESXi에서 필터를 표시할 수 없음**

설치 상태가 성공적이며 방화벽이 사용되도록 설정된 것으로 표시되더라도 NSX 6.2.x에서 6.3.0으로 업그레이드하고 클러스터 VIB에서 6.3.0 비트로 업그레이드한 후 “통신 채널 상태”가 방화벽 에이전트 연결과의 NSX Manager, ControlPlane 에이전트 연결과의 NSX Manager가 다운된 것으로 표시됩니다. 이는 호스트로 전송되지 않은 방화벽 규칙 게시, 보안 정책 게시 오류, VXLan 구성으로 이어집니다.

해결 방법: API POST:<https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize>를 사용하여 클러스터에 대한 메시지 버스 동기화 API 호출을 실행합니다.

API Body:

```
<nwFabricFeatureConfig>
```

```
<featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
<resourceConfig>
  <resourceId>{Cluster-MOID}</resourceId>
</resourceConfig>
</nwFabricFeatureConfig>
```

- **문제 1797307: 업그레이드 또는 다시 배포 후에 NSX Edge가 분할 브레인으로 실행될 수 있음**

대기 NSX Edge에서 show service highavailability CLI 명령을 실행하면 고가용성 상태가 "대기"로 표시되지만 구성 엔진 상태는 "활성"입니다.

해결 방법: 대기 NSX Edge를 재부팅합니다.

- **문제 1789989: 호스트 클러스터 업그레이드 동안 데이터부에서 패킷이 손실될 수 있음**

VIB 업그레이드 동안 VIB에 유지되는 VSFWD(vShield 방화벽 데몬)의 암호 파일이 제거되므로 VSFWD에서 이전 암호를 사용하여 NSX Manager에 연결할 수 없으며 새 암호가 업데이트될 때까지 기다려야 합니다. 호스트 재부팅 후에 이 프로세스를 완료하는 데 다소 시간이 걸리지만 완전 자동화 DRS 클러스터에서는 준비된 호스트가 나타나는 즉시 VM이 이동되며, VSFWD 프로세스가 해당 시점에 준비 완료 상태가 아니므로 짧은 시간 동안 데이터부에서 패킷이 손실될 수 있습니다.

해결 방법: 호스트가 다시 나타나는 즉시 장애가 복구되지 않고 이러한 VM의 새로 준비된 호스트에 대한 장애 복구가 지연됩니다.

- **문제 1797929: 호스트 클러스터 업그레이드 후 메시지 버스 채널 다운**

호스트 클러스터 업그레이드 후에 vCenter 6.0(및 이전 버전)은 이벤트 "다시 연결"을 생성하지 않으므로 NSX Manager는 호스트에서 메시징 인프라를 설정하지 않습니다. 이 문제는 vCenter 6.5에서 해결되었습니다.

해결 방법: 아래와 같이 메시징 인프라를 다시 동기화하십시오.

POST https://<ip>:/api/2.0/nwfabric/configure?action=synchronize

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>host-15</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

- **문제 1768144: 새로운 제한을 초과하는 이전 NSX Edge 장치 리소스 예약으로 인해 업그레이드 또는 다시 배포 중에 실패할 수 있음**

NSX 6.2.4 및 이전 버전에서 NSX Edge 장치에 대해 임의의 대용량 리소스 예약을 지정할 수 있었습니다. NSX는 최댓값을 적용하지 않았습니다. NSX Manager를 6.2.5 이상으로 업그레이드한 후에 선택된 폼 팩터에 대해 새로 적용된 최댓값을 초과하는 리소스(특히 메모리)가 기존 Edge에 대해 예약되면 Edge 업그레이드 또는 다시 배포(업그레이드를 트리거하는) 중에 실패할 수 있습니다. 예를 들어 사용자가 6.2.5 이전의 LARGE Edge에 대해 1000MB의 메모리를 예약하고, 6.2.5로 업그레이드한 후에 장치 크기를 COMPACT로 변경하면 사용자 지정 메모리 예약이 새로 적용된 최댓값(이 경우 COMPACT Edge에 대한 512)을 초과하게 되어 작업이 실패합니다.

NSX 6.2.5부터 권장되는 리소스 할당에 대한 자세한 내용은 [ESG\(Edge Services Gateway\) 업그레이드](#)를 참조하십시오.

해결 방법: 다음 장치 REST API PUT https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/를 사용하여 다른 장치 변경 없이, 폼 팩터에 대해 지정된 값 범위 내에서 메모리 예약을 다시 구성합니다. 이 작업이 완료되면 장치 크기를 변경할 수 있습니다.

- **문제 1600281: [서비스 배포] 탭에서 Guest Introspection에 대한 USVM 설치 상태가 [실패]로 표시됨**

Guest Introspection 범용 SVM에 대한 지원 데이터스토어가 오프라인 상태가 되거나 액세스할 수 없게 되면 USVM을 재부팅하거나 재배포하여 복구해야 할 수 있습니다.

해결 방법: USVM을 재부팅하거나 재배포하여 복구합니다.

- **문제 1660373: vCenter가 만료된 NSX 라이선스를 적용**

vSphere 5.5 업데이트 3 또는 vSphere 6.0.x 기준으로 vSphere Distributed Switch가 NSX 라이선스에 포함됩니다. 하지만 vCenter에서는 NSX 라이선스가 만료된 경우 ESX 호스트를 vSphere Distributed Switch에 추가할 수 없습니다.

해결 방법: 호스트를 vSphere Distributed Switch에 추가하려면 NSX 라이선스가 활성화 상태여야 합니다.

- 문제 1569010/1645525: vCenter 5.5에 연결된 시스템에서 6.1.x를 NSX for vSphere 6.2.3으로 업그레이드할 경우 [라이선스 키 할당] 창의 제품 필드에 NSX 라이선스가 "NSX for vSphere - Enterprise"와 같은 구체적인 버전이 아닌 일반적인 "NSX for vSphere"로 표시됩니다.

해결 방법: 없음.

- 문제 1636916: vCloud Air 환경에서 NSX Edge 버전이 vCNS 5.5.x에서 NSX 6.x로 업그레이드될 때 소스 프로토콜 값이 "any"인 Edge 방화벽 규칙이 "tcp:any, udp:any"로 변경됨
결과적으로 ICMP 트래픽이 차단되고 패킷 손실이 발생할 수 있습니다.

해결 방법: NSX Edge 버전을 업그레이드하기 전에 보다 구체적인 Edge 방화벽 규칙을 만들고 "any"를 구체적인 소스 포트 값으로 바꾸십시오.

- 문제 1474238: vCenter 업그레이드 후 vCenter와 NSX의 연결이 끊길 수 있음
vCenter에 내장된 SSO를 사용하고 vCenter 5.5를 vCenter 6.0으로 업그레이드하는 경우 vCenter와 NSX의 연결이 끊길 수 있습니다. 이는 vCenter 5.5가 루트 사용자 이름을 사용하여 NSX에 등록된 경우 발생합니다. NSX 6.2에서는 루트를 사용한 vCenter 등록이 더 이상 지원되지 않습니다.
참고: 외부 SSO를 사용하는 경우에는 아무것도 변경할 필요가 없습니다. 동일한 사용자 이름(예: admin@mybusiness.mydomain)을 사용할 수 있으며 vCenter 연결이 끊어지지 않습니다.

해결 방법: 루트 대신 administrator@vsphere.local 사용자 이름을 사용하여 NSX에 vCenter를 다시 등록합니다.

- 문제 1375794: 전원을 끄기 전에 에이전트 VM(SVA)에 대한 게스트 OS 종료
호스트가 유지 보수 모드로 전환되면 모든 서비스 장치가 정상적으로 종료되는 대신 전원이 꺼집니다. 이로 인해 타사 장치 내에서 오류가 발생할 수 있습니다.

해결 방법: 없음.

- 문제 1112628: 서비스 배포 보기를 사용하여 배포된 서비스 장치의 전원을 끌 수 없음
해결 방법: 계속하기 전에 다음을 확인하십시오.

- 가상 시스템의 배포가 완료되었습니다.
- vCenter 작업 창에 표시된 가상 시스템에 대한 복제, 재구성 등의 작업이 진행되지 않습니다.
- 배포가 시작된 후 가상 시스템의 vCenter 이벤트 창에 다음 이벤트가 표시됩니다.

에이전트 VM <vm name>이(가) 프로비저닝되었습니다.

에이전트 워크플로우를 진행하려면 에이전트를 사용 가능으로 표시하십시오.

이 경우 서비스 가상 시스템을 삭제하십시오. 서비스 배포 UI에 배포가 실패로 표시됩니다. 빨간색 아이콘을 클릭하면 호스트에 대해 에이전트 VM을 사용할 수 없다는 경보가 표시됩니다. 이 경보를 해결하면 가상 시스템이 다시 배포되고 전원이 켜집니다.

- 사용 환경 내 모든 클러스터가 준비되지 않은 경우, 분산 방화벽에 대한 업그레이드 메시지가 [설치] 페이지의 [호스트 준비] 탭에 표시되지 않음
네트워크 가상화를 위해 클러스터를 준비하면 해당 클러스터에 분산 방화벽이 사용되도록 설정됩니다. 사용 환경 내 모든 클러스터가 준비되지 않은 경우 분산 방화벽에 대한 업그레이드 메시지가 [호스트 준비] 탭에 표시되지 않습니다.

해결 방법: 다음 REST 호출을 사용하여 분산 방화벽을 업그레이드합니다.

PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state

- **문제 1215460: 서비스 추가/제거 업그레이드 후에 서비스 그룹이 수정된 경우 이 변경 내용이 방화벽 테이블에 반영되지 않음**
사용자 생성 서비스 그룹이 업그레이드 도중 Edge Firewall 테이블에서 확장됩니다. 즉, 방화벽 테이블에서 서비스 열이 서비스 그룹 내 모든 서비스를 표시합니다. 서비스 추가/제거 업그레이드 후에 서비스 그룹이 수정된 경우 이 변경 내용이 방화벽 테이블에 반영되지 않습니다.

해결 방법: 이름이 다른 서비스 그룹을 새로 만든 후 이 서비스 그룹을 방화벽 규칙에 사용합니다.

- **문제 1413125: 업그레이드 후 SSO를 재구성할 수 없음**
NSX Manager에 구성된 SSO 서버가 vCenter Server의 유일한 기본 서버인 경우, vCenter Server를 버전 6.0으로 업그레이드하고 NSX Manager를 버전 6.x로 업그레이드한 이후에 NSX Manager에 SSO 설정을 재구성할 수 없습니다.

해결 방법: 없음.

- **문제 1263858: SSL VPN이 업그레이드 알림을 원격 클라이언트에 보내지 않음**
SSL VPN 게이트웨이가 사용자에게 업그레이드 알림을 보내지 않습니다. 관리자가 SSL VPN 게이트웨이(서버)가 업데이트되고 해당 클라이언트를 업데이트해야 함을 원격 사용자에게 직접 알려야 합니다.

해결 방법: 사용자가 이전 버전의 클라이언트를 제거하고 최신 버전을 수동으로 설치해야 합니다.

- **문제 1462319: esx-dvfilter-switch-security VIB가 더 이상 "esxcli software vib list | grep esx" 명령의 출력에 존재하지 않습니다.**

NSX 6.2부터 esx-dvfilter-switch-security 모듈은 esx-vxlan VIB 내에 포함됩니다. 6.2에서 설치되는 유일한 NSX VIB는 esx-vsip 및 esx-vxlan입니다. NSX를 6.2로 업그레이드하는 동안 이전 esx-dvfilter-switch-security VIB는 ESXi 호스트에서 제거됩니다.

NSX 6.2.3부터 esx-vsip 및 esx-vxlan NSX VIB와 함께 세 번째 VIB인 esx-vdpi가 제공됩니다. 설치가 성공하면 세 VIB가 모두 표시됩니다.

해결 방법: 없음.

- **문제 1481083: 명시적 페일오버 팀 구성이 구성된 논리적 라우터가 업그레이드 후 패킷을 제대로 전달하지 못함**

호스트가 ESXi 5.5를 실행 중인 경우 명시적 페일오버 NSX 6.2 팀 구성 정책은 논리적 분산 라우터에서 여러 활성 업링크를 지원하지 않습니다.

해결 방법: 하나의 활성 업링크만 존재하며 다른 업링크는 대기 모드가 되도록 명시적 페일오버 팀 구성 정책을 수정합니다.

- **문제 1411275: NSX for vSphere 6.2에서 백업 및 복구를 수행한 후 vSphere Web Client에 [Networking & Security] 탭이 표시되지 않음**
NSX for vSphere 6.2로 업그레이드한 후 백업 및 복원 작업을 수행하면 vSphere Web Client에 Networking & Security 탭이 표시되지 않습니다.

해결 방법: NSX Manager 백업을 복구하면 장치 관리자에서 로그아웃됩니다. 몇 분 정도 기다린 후 vSphere Web Client에 로그인합니다.

- **설치 페이지의 서비스 배포 탭을 사용해 배포한 서비스 가상 시스템의 전원이 켜지지 않음**

해결 방법:

1. 클러스터 내 ESX Agent 리소스 풀에서 서비스 가상 시스템을 수동으로 제거합니다.
2. **Networking & Security**를 클릭하고 **설치**를 클릭합니다.
3. **서비스 배포** 탭을 클릭합니다.
4. 적절한 서비스를 선택하고 **해결** 아이콘을 클릭합니다.
그러면 서비스 가상 시스템이 다시 배포됩니다.

- **문제 1764460: 호스트 준비를 완료한 후에 모든 클러스터 멤버가 준비 상태로 표시되지만 클러스터 수준이 [잘못됨]으로 잘못 표시됨**

호스트 준비를 완료한 후에 모든 클러스터 멤버가 [준비] 상태로 제대로 표시되지만 클러스터 수준이 [잘못됨]으로 표시되며 호스트가 이미 재부팅되었어도 호스트를 재부팅해야 한다는 이유가 표시됩니다.

해결 방법: 빨간색 주의 아이콘을 클릭하고 [해결]을 선택합니다.

NSX Manager에 대한 알려진 문제

- **문제 1892999: 범용 보안 태그에 연결된 VM이 없더라도 고유한 선택 기준을 수정할 수 없음**
범용 보안 태그에 연결된 VM이 삭제되어도 VM을 나타내는 내부 개체는 여전히 범용 보안 태그에 연결된 상태를 유지합니다. 이로 인해 범용 보안 태그가 여전히 VM에 연결되어 있다는 오류와 함께 범용 선택 기준 변경이 실패합니다.

해결 방법: 모든 범용 보안 태그를 삭제한 후 범용 선택 기준을 변경하십시오.

- **문제 1926309: NSX Manager 플러그인이 로드할 수 없고 "인증 예외"를 표시함**
경우에 따라 NSX Manager 플러그인이 페이지를 로드할 수 없으며 시간 초과 오류를 표시합니다.

해결 방법: NSX 관리 서비스를 다시 시작하거나 NSX Manager 장치를 재부팅하십시오.

- **문제 1904842: NSX Manager가 vCenter 또는 Platform Service Controller에 등록되지 않음**
NSX Manager가 UI에 표시되지 않으며, NSX Manager에 대한 REST 호출이 실패합니다.

해결 방법: NSX 관리 서비스를 다시 시작하거나 NSX Manager 장치를 재부팅하십시오.

- **문제 1801325: 높은 CPU 및/또는 디스크 사용량으로 NSX Manager에서 생성된 '심각한' 시스템 이벤트 및 로깅**

높은 디스크 공간 사용량, 작업 데이터의 높은 변동 또는 NSX Manager에서 높은 작업 대기열 크기가 있는 경우 다음 중 하나 이상의 문제가 발생할 수 있습니다.

- vSphere Web Client에서 '심각한' 시스템 이벤트
- /common 파티션에 대한 NSX Manager에서의 높은 디스크 사용량
- 연기된 기간 또는 정기적 간격에 대한 높은 CPU 사용량
- NSX Manager 성능에 대한 부정적인 영향

해결 방법: VMware 고객 지원에 문의하십시오. 자세한 내용은 [VMware 기술 자료 문서 2147907](#)을 참조하십시오.

- **문제 1781080: 심표 구분 기호를 사용해서 둘 이상의 도메인을 추가할 경우 DNS 검색 구성이 실패함**
NSX Manager에 둘 이상의 도메인 검색 접미사를 추가할 경우 정규화된 이름을 사용하지 않는 모든 DNS 조회가 실패합니다. 이 문제는 /etc/resolv.conf의 내부 형식 문제 때문입니다.

해결 방법: 단일 DNS 검색 접미사를 사용하십시오.

- **문제 1806368: 페일오버 후 다시 기본이 된 이전에 실패한 기본 NSX Manager 컨트롤러를 다시 사용하면 DLR 구성이 모든 호스트에 푸시되지 않음**
크로스 vCenter NSX 설정에서 기본 NSX Manager가 실패하는 경우 보조 NSX Manager가 기본으로 승격되며 새 컨트롤러 클러스터가 새로 승격된 보조(현재 기본) NSX Manager와 함께 사용되도록 배포됩니다. 기본 NSX Manager가 다시 사용되면 보조 NSX Manager의 등급이 낮아지며 기본 NSX Manager가 복원됩니다. 이 경우 페일오버 전에 이 기본 NSX Manager에 배포된 기존 컨트롤러를 다시 사용하면 DLR 구성이 모든 호스트에 푸시되지 않습니다. 이 문제는 새 컨트롤러 클러스터를 대신 생성하는 경우 발생하지 않습니다.

해결 방법: 복원된 기본 NSX Manager에 대한 새 컨트롤러 클러스터 하나를 배포하십시오.

- **문제 1831131: LocalOS 사용자를 사용하여 인증된 경우 NSX Manager의 SSO 연결이 실패함**
LocalOS 사용자를 사용하여 인증된 경우 오류와 함께 NSX Manager의 SSO 연결이 다음 오류와 함께 실패합니다. "NSX Manager와의 통신을 설정할 수 없습니다. 관리자에게 문의하십시오."

해결 방법: nsxmanager@domain 이외에 nsxmanager@localos에 대한 엔터프라이즈 관리자 역할을 추가합니다.

- **문제 1800820: 이전 UDLR 인터페이스가 시스템에서 이미 삭제된 경우 보조 NSX Manager에서 UDLR 인터페이스 업데이트가 실패함**

기본 NSX Manager에서 범용 동기화 서비스(Replicator)의 작동이 중지되는 시나리오에서는 기본 NSX Manager에서 UDLR(범용 분산 논리적 라우터) 및 ULS(범용 논리적 스위치) 인터페이스를 삭제하고 새로 생성한 후 보조 NSX Manager에서 복제해야 합니다. 이 경우 복제 중에 보조 NSX Manager에서 새 ULS가 생성되고 UDLR이 새 ULS에 연결되지 않으므로 UDLR 인터페이스는 보조 NSX Manager에서 업데이트되지 않습니다.

해결 방법: Replicator가 실행되고 있는지 확인하고 기본 NSX Manager에서 새로 만든 ULS를 백업으로 포함하는 UDLR 인터페이스(LIF)를 삭제하고 같은 백업 ULS를 사용해서 UDLR 인터페이스(LIF)를 다시 생성합니다.

● **문제 1772911: NSX Manager가 디스크 공간을 소비하면서 매우 느리게 작동하고 작업 및 작업 테이블 크기가 100% CPU 사용량에 가깝게 증가함**

다음 문제가 발생합니다.

- NSX Manager CPU 사용량이 100%에 다다르거나 정기적으로 100% 사용량으로 증가하며 NSX Manager 장치에 리소스를 더 추가해도 차이가 없습니다.
- NSX Manager CLI(명령줄 인터페이스)에서 `show process monitor` 명령을 실행할 경우 최고 CPU 주기를 소비하는 Java 프로세스가 표시됩니다.
- NSX Manager CLI에서 `show filesystems` 명령을 실행하면 `/common` 디렉토리가 아주 높은 사용량 상태(예: 90% 초과)를 나타냅니다.
- 일부 구성 변경이 시간 초과되고(경우에 따라 50분 이상 소요됨) 적용되지 않습니다.

자세한 내용은 [VMware 기술 자료 문서 2147907](#)을 참조하십시오.

해결 방법: 이 문제의 해결 방법을 보려면 VMware 고객 지원에 문의하십시오.

● **문제 1785142: 기본 및 보조 NSX Manager 간 통신이 차단될 경우 기본 NSX Manager에서 '동기화 문제'를 표시하는 데 시간이 지연됨**

기본 및 보조 NSX Manager 간 통신이 차단될 경우 기본 NSX Manager에서 '동기화 문제'가 바로 표시되지 않습니다.

해결 방법: 통신이 다시 설정될 때까지 20분 정도 기다리십시오.

● **문제 1786066: 크로스 vCenter NSX 설치에서 보조 NSX Manager의 연결을 끊으면 NSX Manager가 보조 NSX Manager로 다시 연결할 수 없게 될 수 있음**

크로스 vCenter NSX 설치에서 보조 NSX Manager의 연결을 끊을 경우 나중에 해당 NSX Manager를 보조 NSX Manager로 다시 추가하지 못할 수 있습니다. NSX Manager를 보조 NSX Manager로 다시 연결하려고 하면 NSX Manager가 vSphere Web Client의 [관리] 탭에서 "보조"로 표시되지만 기본 NSX Manager로의 연결이 설정되지 않습니다.

해결 방법:

1. 기본 NSX Manager에서 보조 NSX Manager의 연결을 끊습니다.
2. 보조 NSX Manager를 기본 NSX Manager에 다시 추가합니다.

● **문제 1713669: 데이터베이스 테이블 ai_useripmap이 너무 커질 경우 디스크가 꽉 차서 NSX Manager가 실패함**

이 문제는 NSX Manager 장치 디스크가 꽉 차게 되어 NSX Manager가 실패하도록 합니다. 재부팅 후에 postgres 프로세스를 시작할 수 없습니다. `/common` 파티션이 꽉 찼습니다. 이 문제는 ELS(이벤트 로그 서버)에 과도한 로드가 발생하는 사이트와 대량의 GI(Guest Introspection) 트래픽이 있는 사이트에서 일반적으로 발생합니다. IDFW(ID 방화벽)를 사용하는 사이트는 자주 영향을 받습니다. 자세한 내용은 [VMware 기술 자료 문서 2148341](#)을 참조하십시오.

해결 방법: 이 문제를 복구하기 위한 도움이 필요한 경우 VMware 고객 지원에 문의하십시오.

● **문제 1783528: NSX Manager CPU 활용률이 금요일 밤/토요일 아침마다 최대로 높아짐**

NSX는 금요일 밤마다 전체 동기화를 위해 LDAP를 폴링합니다. 특정 Active Directory 조직 구성 단위 또는 컨테이너를 구성하는 옵션은 제공되지 않으므로 NSX는 제공된 도메인과 관련된 모든 개체를 가져옵니다.

해결 방법: NSX Manager vCPU를 4에서 6으로 늘리십시오.

● **문제 1715354: REST API의 가용성 지연**

FIPS 모드가 토글될 때 NSX Manager가 다시 시작된 후 NSX Manager API가 가동되어 실행되는 데 다소 시간이 걸립니다. API가 정지된 경우 이러한 문제가 나타날 수 있지만 컨트롤러에서 NSX Manager로 연결을 다시 설정하는 데 시간이 걸리기 때문에 이 문제가 발생합니다. NSX API 서버가 가동되어 실행될 때까지 기다리고 작업을 수행하기 전에 모든 컨트롤러가 연결된 상태인지 확인하는 것이 좋습니다.

- **문제 1441874: vCenter Linked Mode 환경에서 단일 NSX Manager를 업그레이드하면 오류 메시지가 표시됨**

여러 VMware vCenter Server에 여러 NSX Manager가 있는 환경의 [vSphere Web Client] > [Networking & Security] > [설치] > [호스트 준비]에서 하나 이상의 NSX Manager를 선택하면 다음 오류가 표시됩니다.

“NSX Manager와의 통신을 설정할 수 없습니다. 관리자에게 문의하십시오.”

해결 방법: 자세한 내용은 [VMware 기술 자료 문서 2127061](#)을 참조하십시오.

- **문제 1696750: PUT API를 통해 NSX Manager에 IPv6 주소를 할당한 경우 변경 내용이 반영되려면 재부팅해야 함**

<https://{NSX Manager IP 주소}/api/1.0/appliance-management/system/network>를 통해 NSX Manager에 대해 구성된 네트워크 설정을 변경할 경우 시스템을 재부팅해야 변경 내용이 반영됩니다. 재부팅할 때까지 기존 설정이 그대로 표시됩니다.

해결 방법: 없음.

- **문제 1529178: 공통 이름이 포함되지 않은 서버 인증서를 업로드하면 "내부 서버 오류" 메시지가 반환됨**
공통 이름이 없는 서버 인증서를 업로드하면 "내부 서버 오류" 메시지가 표시됩니다.

해결 방법: SubAltName과 공통 이름이 모두 있거나 공통 이름만이라도 있는 서버 인증서를 사용합니다.

- **문제 1655388: Windows 10 OS(JA, CN 및 DE 언어용)에서 IE11/Edge 브라우저 사용 시 NSX Manager 6.2.3 UI가 로컬 언어가 아닌 영어로 표시됨**

Windows 10 OS(JA, CN 및 DE 언어용)에서 IE11/Edge 브라우저를 사용하여 NSX Manager 6.2.3을 실행하면 영어가 표시됩니다.

해결 방법:

1. Microsoft 레지스트리 편집기(regedit.exe)를 실행하고 **컴퓨터 > HKEY_CURRENT_USER > SOFTWARE > Microsoft > Internet Explorer > International**로 이동합니다.
2. *AcceptLanguage* 파일 값을 모국어로 바꿉니다. 예를 들어 언어를 **DE**로 바꾸고 싶다면 값을 변경하고 **DE**가 첫 번째 위치에 있도록 합니다.
3. 브라우저를 다시 시작하고 NSX Manager에 다시 로그인합니다. 올바른 언어가 표시됩니다.

- **문제 1435996: NSX Manager에서 CSV 형식으로 내보낸 로그 파일에 날짜/시간이 아니라 epoch가 타임스탬프로 표시됨**

vSphere Web Client를 사용하여 NSX Manager에서 CSV로 내보낸 로그 파일이 표준 시간대 기반의 적합한 시간 대신 epoch 시간(밀리초)이 타임스탬프로 표시됩니다.

해결 방법: 없음.

- **문제 1644297: 기본 NSX에서 DFW 섹션에 대해 추가/삭제 작업을 수행하면 보조 NSX에서 2개의 DFW 저장된 구성이 생성됨**

크로스 vCenter 설정에서 추가 범용 또는 로컬 DFW 섹션이 기본 NSX Manager에 추가되면 두 DFW 구성이 보조 NSX Manager에 추가됩니다. 이 문제는 기능에는 전혀 영향을 주지 않지만 저장된 구성 제한에 더 빠르게 도달하여 중요한 구성을 덮어쓸 수 있습니다.

해결 방법: 없음.

- **문제 1477138: 호스트 이름의 길이가 64자를 넘으면 NSX 관리 서비스가 실행되지 않음**

OpenSSL 라이브러리를 통해 인증서를 만들려면 호스트 이름이 64자 이하여야 합니다.

- **문제 1437664: NSX Manager 목록이 웹 클라이언트에 표시되는 속도가 느림**

여러 개의 NSX Manager가 있는 vSphere 6.0 환경에서 큰 AD 그룹 집합으로 로그인하는 사용자를 확인하는 동안 vSphere Web Client에서 NSX Manager 목록이 표시될 때까지 최대 2분이 걸릴 수 있습니다. NSX Manager 목록을 표시하려고 할 때 데이터 서비스 시간 초과 오류가 표시될 수 있습니다. 해결 방법이 없습니

다. NSX Manager 목록을 보려면 목록이 로드될 때까지 기다리거나 다시 로그인해야 합니다.

- **문제 1534606: 호스트 준비 페이지 로드가 실패함**

vCenter를 연결 모드로 실행할 경우 각 vCenter는 같은 NSX 버전의 NSX Manager에 연결되어 있어야 합니다. NSX 버전이 서로 다른 경우 vSphere Web Client는 더 높은 버전의 NSX를 실행하는 NSX Manager와만 통신할 수 있습니다. [호스트 준비] 탭에 "NSX Manager와의 통신을 설정할 수 없습니다. 관리자에게 문의하십시오"와 비슷한 오류가 표시됩니다.

해결 방법: 모든 NSX Manager를 동일한 NSX 소프트웨어 버전으로 업그레이드해야 합니다.

- **문제 1386874: vSphere Web Client에 [Networking & Security] 탭이 표시되지 않음**

vSphere를 6.0으로 업그레이드한 후 루트 사용자 이름으로 vSphere Web Client에 로그인하면 [Networking & Security] 탭이 표시되지 않습니다.

해결 방법: administrator@vsphere.local 또는 업그레이드하기 전의 vCenter Server에서 NSX Manager에 정의되어 있던 역할을 가진 다른 vCenter 사용자로 로그인합니다.

- **문제 1027066: NSX Manager의 vMotion이 다음 오류 메시지를 표시할 수 있음: "가상 이더넷 카드 네트워크 어댑터 1이 지원되지 않습니다."**

이러한 오류는 무시해도 됩니다. 네트워킹은 vMotion 후 올바르게 작동합니다.

- **문제 1460766: NSX 명령줄 인터페이스를 사용하여 암호를 변경한 후 NSX Manager UI에서 자동으로 로그아웃되지 않음**

NSX Manager에 로그인되어 있고 최근에 CLI를 사용하여 암호를 변경한 경우, 이전 암호로 NSX Manager UI에 로그인된 상태로 남아 있을 수 있습니다. 일반적으로 비활성 상태로 인해 세션이 시간 초과된 경우 NSX Manager 클라이언트에서 사용자가 자동으로 로그아웃되어야 합니다.

해결 방법: NSX Manager UI에서 로그아웃한 후 새 암호를 사용하여 다시 로그인합니다.

- **문제 1467382: 네트워크 호스트 이름을 편집할 수 없음**

NSX Manager 가상 장치에 로그인하고 장치 관리로 이동한 후 장치 설정 관리를 클릭하고 설정 아래에서 네트워크를 클릭하여 네트워크 호스트 이름을 편집하면 잘못된 도메인 이름 목록 오류가 나타날 수 있습니다. 이 문제는 도메인 검색 필드에 지정된 도메인 이름이 쉼표 대신 공백 문자로 구분되어 있을 때 발생합니다. NSX Manager는 쉼표로 구분된 도메인 이름만 수용합니다.

해결 방법:

1. NSX Manager 가상 장치에 로그인합니다.
2. 장치 관리에서 장치 설정 관리를 클릭합니다.
3. 설정 패널에서 네트워크를 클릭합니다.
4. DNS 서버 옆의 편집을 클릭합니다.
5. 도메인 검색 필드에서 모든 공백 문자를 쉼표로 바꿉니다.
6. 확인을 클릭하여 변경 내용을 저장합니다.

- **문제 1436953: 백업에서 NSX Manager를 성공적으로 복원한 후에도 잘못된 시스템 이벤트가 생성됨**
백업에서 NSX Manager를 성공적으로 복원한 후 **Networking & Security: NSX Manager: 모니터: 시스템 이벤트**로 이동하면 vSphere Web Client에 다음과 같은 시스템 이벤트가 나타납니다.

- 백업에서 NSX Manager를 복원하지 못했습니다(심각도=위험).

- NSX Manager 복원이 완료되었습니다(심각도=정보).

해결 방법: 마지막 시스템 이벤트 메시지가 성공으로 표시될 경우 시스템 생성 이벤트 메시지를 무시해도 됩니다.

- **문제 1843197: NSX Manager 네트워크 어댑터에 "이 유형의 네트워크 어댑터는 {0}기타 Linux(64비트)에서 지원되지 않습니다." 경고가 표시됨**

NSX Manager를 설치 및 구성한 후 배포된 NSX Manager의 [vCenter] > [설정 편집]으로 이동합니다. 네트워크 어댑터에 "이 유형의 네트워크 어댑터는 {0}기타 Linux(64비트)에서 지원되지 않습니다." 경고가 표시됩니다.

NSX Controller에 대한 알려진 문제

- **문제 1856465: ESXi 호스트가 NSX Cross-vCenter 환경의 사이트 중 하나에서 다운되면 CDO 모드가 해당 사이트에서 사용되도록 설정되지 않음**
ESXi 호스트가 사이트에서 다운될 경우 해당 사이트에서 CDO 모드가 완전하게 사용하거나 사용하지 않도록 설정되지 않습니다.
보조 사이트 중 하나에서 호스트가 다운되면 기본 사이트에서 CDO 모드 작업이 성공적으로 수행됩니다. 그렇지만 CDO 모드 작업이 보조 사이트에서는 실패합니다. 이로 인해 일관되지 않은 동작이 발생할 수 있습니다.

해결 방법: 이 문제는 NSX 6.3.0 이상에 영향을 미칩니다.

- CDO 작업을 수행하기 전에 모든 ESXi 호스트가 작동되고 있는지 확인하십시오.
- 일관되지 않은 상태에서 복구하려면 vCenter 인벤토리에서 호스트를 제거했다가 다시 추가하십시오.

- **문제 1965859: 하드웨어 VTEP 구성을 사용할 경우 NSX Controller 메모리가 늘어나 CPU 사용량이 높아짐**
하드웨어 VTEP 구성을 며칠 동안 실행할 경우 컨트롤러 프로세스 메모리 증가가 확인됩니다. 메모리가 증가하면서 컨트롤러가 메모리를 복구하는 동안 일정 기간(분) CPU 사용량이 높아집니다. 이 기간 동안 데이터 경로도 영향을 받습니다.

해결 방법: VMware 고객 지원에 문의하십시오.

논리적 네트워킹 및 NSX Edge에 대한 알려진 문제

- **문제 1904612: 클라이언트 전원이 꺼져 있을 때 L2VPN 서버에서 계층 2 VPN 터널이 "실행"으로 표시됨**
두 NSX Edge 간에 L2 VPN을 생성한 후 클라이언트 NSX Edge 전원을 꺼도 서버 NSX Edge는 여전히 VPN 터널을 실행 상태로 표시합니다.

해결 방법: 없음.

- **문제 1242207: 런타임 동안 라우터 ID를 변경할 경우 OSPF 토폴로지에 반영되지 않음**
OSPF를 사용하도록 설정한 상태에서 라우터 ID를 변경하려고 하면 이 라우터 ID를 사용하여 새로운 외부 LSA(링크 상태 보급)가 재생성되지 않아 OSPF 외부 경로가 손실됩니다.

OSPF를 사용하지 않도록 설정하고, 라우터 ID를 변경한 후 OSPF를 다시 사용하도록 설정하십시오.

- **문제 1894277: 로컬 또는 피어 서브넷이 변경될 때 IPSec 사이트 구성 PSK가 유지되지 않음**
마스크된 PSK가 데이터베이스에 저장되므로 암호 불일치로 인해 피어 간 터널이 작동되지 않습니다.

해결 방법: 올바른 암호를 사용하여 IPSec 구성을 다시 구성하십시오.

- **문제 1492497: NSX Edge DHCP 트래픽을 필터링할 수 없음**
NSX Edge에서 DHCP 서버가 TCP/IP 스택을 우회하는 원시 소켓을 활용하므로 NSX Edge에서 DHCP 트래픽에 방화벽 필터링을 적용할 수 없습니다.

해결 방법: 없음.

- **문제 1781438: ESG 또는 DLR NSX Edge 장치에서 두 번 이상 BGP 경로 특성 MULTI_EXIT_DISC를 받는 경우 라우팅 서비스가 오류 메시지를 전송하지 않습니다.**
Edge 라우터 또는 논리적 분산 라우터에서 두 번 이상 BGP 경로 특성 MULTI_EXIT_DISC를 받는 경우 오류 메시지를 전송하지 않습니다. RFC 4271[5초]에 따라 동일한 특성(동일한 유형이 있는 특성)이 특정 업데이트 메시지의 경로 특성 필드 내에서 두 번 이상 나타날 수 없습니다.

해결 방법: 없음.

- **문제 1786515: ‘보안 관리자’ 권한이 있는 사용자가 vSphere Web Client UI를 통해 로드 밸런서 구성을 편집할 수 없습니다.**
특정 NSX Edge에 대해 “보안 관리자” 권한이 있는 사용자가 vSphere Web Client UI를 사용하여 해당 Edge에 대해 글로벌 로드 밸런서 구성을 편집할 수 없습니다. 다음 오류 메시지가 표시됩니다. “사용자에게 개체 글로벌 및 기능 si.service에 액세스할 수 있는 권한이 부여되지 않았습니다. 개체 액세스 범위와 이 사용자의 기능 사용 권한을 확인하십시오.”

해결 방법: 없음.

- **문제 1849042/1849043: 암호 수명이 NSX Edge 장치에 구성되는 경우 관리자 계정 잠금**
암호 수명이 NSX Edge 장치에서 관리자에 대해 구성되어 있는 경우 암호 수명이 다 되면 장치 로그인 시 사용자에게 암호를 변경하라는 메시지가 나타나는 7일의 기간이 있습니다. 암호 변경에 실패하면 계정이 잠깁니다. 또한 CLI 프롬프트에서 암호가 로그인 시 변경되는 경우 새로운 암호가 UI 및 REST에서 강제 집행하는 강력한 암호 정책을 충족하지 않을 수 있습니다.

해결 방법: 이 문제를 방지하려면 항상 UI 또는 REST API를 사용하여 기존 암호가 만료되기 전에 관리자 암호를 변경합니다. 계정이 잠겨도 UI 또는 REST API를 사용하여 새 암호를 구성하면 계정이 다시 잠금 해제됩니다.

- **문제 1711013: 대기 VM을 재부팅한 후에 활성/대기 NSX Edge 간에 FIB를 동기화하는 데 약 15분이 걸립니다.**

대기 NSX Edge의 전원이 꺼지면 활성 및 대기 모드 사이에서 TCP 세션이 닫히지 않습니다. 활성 Edge는 KA(keepalive)가 실패하고 15분 후에 대기 Edge가 다운되었다는 사실을 감지하게 됩니다. 15분 후에 대기 Edge와의 새 소켓 연결이 설정되고 FIB는 활성/대기 Edge 간에 동기화됩니다.

해결 방법: 없음.

- **문제 1733282: NSX Edge가 정적 디바이스 경로를 더 이상 지원하지 않음**
NSX Edge가 NULL 다음 홉 주소를 갖는 정적 경로의 구성을 지원하지 않습니다.

해결 방법: 없음.

- **문제 1860583: DNS에 연결할 수 없는 경우 원격 sysloger를 FQDN으로 사용하지 마십시오.**
NSX Edge에서 원격 sysloger가 FQDN을 사용하여 구성되고 DNS에 연결할 수 없으면 라우팅 기능에 영향을 미칠 수 있습니다. 이 문제는 일관되게 나타나지 않을 수 있습니다.

해결 방법: FQDN 대신 IP 주소를 사용하는 것이 좋습니다.

- **문제 1850773: 여러 포트가 로드 밸런서 구성에서 사용될 때 NSX Edge NAT가 잘못된 구성을 보고함**
이 문제는 둘 이상의 포트가 있는 로드 밸런서 가상 서버를 구성할 때마다 발생합니다. 이로 인해 영향받는 NSX Edge에 대해 이 구성 상태가 존재하는 동안 NAT를 관리할 수 없게 됩니다.

해결 방법: 자세한 내용 및 해결 방법은 [VMware 기술 자료 문서 2149942](#)를 참조하십시오.

- **문제 1764258: HA 페일오버 또는 하위 인터페이스로 구성된 NSX Edge에서 강제 동기화한 후 최대 8분간 트래픽이 블랙홀 처리됨**

HA 페일오버가 트리거되거나 하위 인터페이스에서 강제 동기화를 시작하는 경우 트래픽이 최대 8분 동안 블랙홀 처리됩니다.

해결 방법: HA에 하위 인터페이스를 사용하지 마십시오.

- **문제 1767135: 로드 밸런서에서 인증서 및 애플리케이션 프로파일에 액세스하려고 할 때 오류 발생**
보안 관리자 권한이 있고 Edge 범위에 있는 사용자는 로드 밸런서에서 인증서 및 애플리케이션 프로파일에 액세스할 수 없습니다. vSphere Web Client에 오류 메시지가 표시됩니다.

해결 방법: 없음.

- **문제 1792548: NSX Controller가 다음 메시지를 표시하며 중단될 수 있음: '클러스터 가입 대기 중'**
NSX Controller가 다음 메시지를 표시하며 중단될 수 있음: '클러스터 가입 대기 중'(CLI 명령: show control-cluster status). 이는 컨트롤러가 작동되는 동안 컨트롤러의 eth0 및 breth0 인터페이스에 대해 동일한 IP 주소가 구성되어 있기 때문에 발생합니다. 컨트롤러에서 다음 CLI 명령을 사용하여 이 사항을 확인할 수 있습니다. show network interface

해결 방법: VMware 고객 지원에 문의하십시오.

- **문제 1747978: OSPF 인접성이 NSX Edge HA 페일오버 후 MD5 인증으로 삭제되었습니다.**
NSX Edge가 정상적인 OSPF 재시작이 구성된 HA에 대해 구성되었으며 MD5가 인증에 사용된 NSX for vSphere 6.2.4에서 OSPF가 정상적으로 시작되지 않습니다. 정지된 타이머가 OSPF 인접 노드에서 만료된 후에만 인접성이 형성됩니다.

해결 방법: 없음

- 문제 1804116: NSX Manager와의 통신이 끊어진 호스트에서 논리적 라우터가 잘못된 상태로 전환됨
논리적 라우터가 켜지거나 NSX Manager와의 통신이 끊어진 호스트에 다시 배포될 경우(NSX VIB 업그레이드/설치 실패 또는 호스트 통신 문제로 인해) 논리적 라우터는 잘못된 상태가 되고 강제 동기화를 통한 연속 자동 복구 작업은 실패합니다.

해결 방법: 호스트 및 NSX Manager 통신 문제를 해결한 후에 NSX Edge를 수동으로 재부팅한 후 모든 인터페이스가 표시될 때까지 기다리십시오. 강제 동기화를 통한 자동 복구 프로세스는 NSX Edge를 재부팅하므로 이 해결 방법은 논리적 라우터에만 필요하며 NSX ESG(Edge Services Gateway)에는 필요하지 않습니다.

- 문제 1783065: IPv4 및 IPv6 주소별로 TCP와 함께 UDP 포트에 대한 로드 밸런서를 구성할 수 없음
UDP는 ipv4-ipv4, ipv6-ipv6(프론트엔드-백엔드)만 지원합니다. IPv6 링크 로컬 주소까지도 그룹 개체의 IP 주소로 읽고 푸시되며 LB 구성에서 사용할 IP 프로토콜을 선택할 수 없는 NSX Manager의 버그가 있습니다.

다음은 이 문제를 보여 주는 LB 구성 예입니다.

로드 밸런서 구성에서 풀 "vCloud_Connector"가 그룹 개체(vm-2681)를 사용해서 풀 멤버로 구성되며 이 개체는 IPv4 및 IPv6 주소를 모두 포함합니다. 그렇지만 이러한 방식은 LB L4 엔진에서 지원될 수 없습니다.

```
{
  "algorithm" : {
    ...
  },
  "members" : [
    {
      ... ,
      ...
    }
  ],
  "applicationRules" : [],
  "name" : "vCloud_Connector",
  "transparent" : {
    "enable" : false
  }
}

{
  "value" : [
    "fe80::250:56ff:feb0:d6c9",
    "10.204.252.220"
  ],
  "id" : "vm-2681"
}
```

해결 방법:

- 옵션 1: 풀 멤버에 그룹 개체 대신 풀 멤버의 IP 주소를 입력하십시오.
- 옵션 2: VM에 IPv6를 사용하지 마십시오.

- 문제 1777792: 피어 끝점이 'ANY'로 설정되면 IPSec 연결이 실패함
NSX Edge의 IPSec 구성이 원격 피어 끝점을 'ANY'로 설정하면 Edge는 IPSec "서버"로 작동하며 원격 피어가

연결을 시작하는 동안 기다립니다. 그렇지만 이니시에이터가 PSK+XAUTH를 사용하여 인증 요청을 보낼 경우 Edge는 다음 오류 메시지를 표시합니다. "XXX.XXX.XX.XX:500에서 초기 기본 모드 메시지가 수신되었으나 연결이 policy=PSK+XAUTH로 인증되지 않았습니다." 또한 IPsec을 설정할 수 없습니다.

해결 방법: IPsec VPN 구성에서 ANY 대신 특정 피어 끝점 IP 주소 또는 FQDN을 사용하십시오.

- **문제 1741158: 구성되지 않은 새 NSX Edge를 생성하고 구성을 적용하면 Edge 서비스 활성화가 너무 빨리 진행될 수 있음**

NSX API를 사용하여 구성되지 않은 새 NSX Edge를 생성한 다음 해당 Edge에서 Edge 서비스 중 하나를 사용하지 않도록 설정하는 API 호출을 수행하고(예: dhcp-enabled를 "false"로 설정) 마지막으로 사용되지 않도록 설정된 Edge 서비스에 대해 구성 변경을 적용하면 해당 서비스가 즉시 활성화됩니다.

해결 방법: 사용 안 함 상태를 유지하려는 Edge 서비스의 구성을 변경한 후에 PUT 호출을 즉시 실행하여 해당 서비스에 대해 enabled 플래그를 "false"로 설정합니다.

- **문제 1758500: 구성된 다음 홉 중 하나 이상이 Edge의 vNIC IP 주소인 경우 다음 홉이 여러 개 있는 정적 경로가 NSX Edge 라우팅 및 전달 테이블에 설치되지 않음**

ECMP 및 여러 개의 다음 홉 주소를 사용할 때 하나 이상의 다음 홉 IP 주소가 올바른 경우 NSX에서 Edge의 vNIC IP 주소가 다음 홉으로 구성될 수 있습니다. 이 작업은 오류 또는 주의 없이 수행되지만 네트워크에 대한 경로가 Edge의 라우팅/전달 테이블에서 제거됩니다.

해결 방법: ECMP를 사용할 때 정적 경로에서 Edge의 자체 vNIC IP 주소를 다음 홉으로 구성하지 마십시오.

- **문제 1716464: NSX 로드 밸런서가 보안 태그가 새로 지정된 VM으로 라우팅되지 않음**

지정된 태그가 있는 2개의 VM을 배포한 다음 해당 태그로 라우팅되도록 LB를 구성하면 LB는 해당 두 VM으로 라우팅됩니다. 하지만 그런 다음 해당 태그가 있는 세 번째 VM을 배포할 경우 LB는 처음 두 VM으로만 라우팅됩니다.

해결 방법: LB 풀에서 [저장]을 클릭합니다. 그러면 VM이 재검색되고 새로 태그가 지정된 VM으로 라우팅되기 시작합니다.

- **문제 1753621: 개인 로컬 AS가 있는 Edge가 EBGW 피어로 경로를 전송하면 모든 개인 AS 경로가 전송된 BGP 라우팅 업데이트에서 제거됨**

NSX에는 현재 AS 경로에 개인 AS 경로만 포함되어 있을 때 전체 AS 경로를 eBGP 인접과 공유하지 못하게 하는 제한이 있습니다. 이는 대부분의 경우에는 바람직한 동작이지만 관리자가 eBGP 인접과 개인 AS 경로를 공유하려고 하는 경우도 있을 수 있습니다.

해결 방법: Edge에서 BGP 업데이트의 모든 AS 경로를 알리도록 하는 해결 방법은 없습니다.

- **문제 1461421: NSX Edge에 대한 "show ip bgp neighbor" 명령 출력에 이전에 설정한 연결의 개수 내역이 유지됨**

"show ip bgp neighbor" 명령을 실행하면 BGP 상태 시스템이 지정된 피어에 대해 [Established] 상태로 전환된 횟수가 표시됩니다. MD5 인증에 사용된 암호를 변경하면 피어 연결이 끊어졌다가 다시 생성되고, 카운터가 지워집니다. Edge DLR에서는 이 문제가 발생하지 않습니다.

해결 방법: 카운터를 지우려면 "clear ip bgp neighbor" 명령을 실행합니다.

- **문제 1656713: HA 페일오버 후 NSX Edge에 IPsec SP(보안 정책)가 없고 터널을 통해 트래픽이 흐를 수 없음**

IPsec 터널에서 흐르는 트래픽에 대해 대기 > 활성화 전환이 작동하지 않습니다.

해결 방법: NSX Edge 전환 후에 IPsec를 사용/사용 안 함으로 설정합니다.

- **문제 1354824: Edge VM이 정전 등의 이유로 손상되거나 연결 불가능한 경우 NSX Manager의 상태 검사가 실패할 때 시스템 이벤트가 발생**

시스템 이벤트 탭에서 "Edge 연결 불가" 이벤트를 보고합니다. NSX Edge 목록에서 계속 배포됨 상태로 보고될 수 있습니다.

해결 방법: 다음 API를 사용하여 NSX Edge에 대한 상세한 상태 정보를 얻으십시오.

GET https://NSX-Manager-IP-Address/api/4.0/edges/edgeld/status?detailedStatus=true

- 문제 1647657: DLR(논리적 분산 라우터)이 있는 ESXi 호스트에서 show 명령을 실행할 경우 DLR 인스턴스당 경로가 2,000개까지만 표시됨

DLR이 사용되도록 설정된 ESXi 호스트에서 show 명령을 사용하면 실행 중인 DLR 인스턴스당 경로가 2,000개를 초과해도 2,000개 이하로 표시됩니다. 이 문제는 단순한 표시 문제이며 실제 데이터 경로는 모든 경로에 대해 정상 동작합니다.

해결 방법: 없음.

- 문제 1634215: OSPF CLI 명령 출력에 라우팅을 사용 안 함으로 설정했는지 표시되지 않음
OSPF를 사용하지 않도록 설정한 경우 라우팅 CLI 명령 출력에 "OSPF가 사용하지 않도록 설정되었습니다"와 같은 메시지가 전혀 표시되지 않습니다. 출력이 비어 있습니다.

해결 방법: show ip ospf 명령으로 올바른 상태를 표시할 수 있습니다.

- 문제 1647739: vMotion 작업 이후 Edge VM을 재배포하면 Edge 또는 DLR VM이 원래의 클러스터로 돌아갑니다.

해결 방법: Edge VM을 다른 리소스 풀 또는 클러스터에 배치하려면 NSX Manager UI를 사용하여 원하는 위치를 구성하십시오.

- 문제 1463856: NSX Edge 방화벽이 사용되도록 설정될 경우 기존 TCP 연결이 차단됨

초기 3방향 핸드셰이크를 확인할 수 없을 때 Edge 상태 저장 방화벽을 통해 TCP 연결이 차단됩니다.

해결 방법: 이러한 기존 흐름을 처리하려면 다음을 수행하십시오. NSX REST API를 사용하여 방화벽 전역 구성에서 "tcpPickOngoingConnections" 플래그를 사용하도록 설정합니다. 이렇게 하면 방화벽이 하드 모드에서 소프트 모드로 전환됩니다. 그다음 방화벽을 사용하도록 설정합니다. 기존 연결이 선택되면(방화벽을 사용하도록 설정하고 몇 분 정도 걸릴 수 있음) "tcpPickOngoingConnections" 플래그를 다시 false로 설정하여 방화벽을 하드 모드로 되돌립니다. (이 설정은 영구적입니다.)

PUT /api/4.0/edges/{edgeld}/firewall/config/global

<globalConfig>

<tcpPickOngoingConnections>true</tcpPickOngoingConnections>

</globalConfig>

- 문제 1374523: esxcli를 사용하여 VXLAN 명령을 사용할 수 있게 하려면 VXLAN VIB를 설치한 후에 ESXi를 재부팅하거나 [services.sh restart]를 실행함

esxcli를 사용하여 VXLAN 명령을 사용할 수 있게 하려면 VXLAN VIB를 설치한 후에 ESXi를 재부팅하거나 [services.sh restart] 명령을 실행해야 합니다.

해결 방법: esxcli를 사용하는 대신 localcli를 사용합니다.

- 문제 1525003: 잘못된 암호로 NSX Manager 백업을 복원할 경우 중요한 루트 폴더에 액세스할 수 없어 실패함

해결 방법: 없음.

- 문제 1637639: Windows 8 SSL VPN PHAT 클라이언트를 사용할 경우 IP 풀에서 가상 IP가 할당되지 않음
Edge Services Gateway가 새 IP 주소를 할당하거나 IP 풀이 다른 IP 범위로 변경될 경우 Windows 8에서 가상 IP 주소가 IP 풀에서 예상대로 할당되지 않습니다.

해결 방법: 이 문제는 Windows 8에서만 발생합니다. 다른 Windows OS를 사용하여 이 문제를 방지하십시오.

- 문제 1628220: 수신기 측에서 DFW 또는 NetX 관찰을 볼 수 없음

대상 vNIC와 연결된 스위치 포트가 변경된 경우 Traceflow가 수신기 측에서 DFW 및 NetX 관찰을 표시하지 않을 수 있습니다. vSphere 5.5 릴리스의 경우에는 이 문제가 수정되지 않습니다. vSphere 6.0 이상의 경우 이 문제가 발생하지 않습니다.

해결 방법: vNIC를 사용하지 않도록 설정하지 마십시오. VM을 재부팅합니다.

- 문제 1483426: IPsec 및 L2 VPN 서비스를 사용하도록 설정하지 않은 경우에도 서비스 상태가 다운된 것으로 표시됨

UI의 설정 탭에서 L2 서비스 상태가 다운된 것으로 표시되지만 API에서는 L2 상태가 가동 중인 것으로 표시됩니다. UI 페이지를 새로 고치지 않는 한 L2 VPN 및 IPsec 서비스는 [설정] 탭에서 항상 다운된 것으로 표시됩니다.

해결 방법: 페이지를 새로 고칩니다.

- **문제 1446327: NSX Edge를 통해 연결할 때 일부 TCP 기반 애플리케이션이 시간 초과될 수 있음**
기본 TCP 설정된 연결 비활성 시간 초과 값은 3600초입니다. NSX Edge는 비활성 시간 초과 값보다 더 오래 유휴 상태인 연결을 모두 삭제하고 연결을 해제합니다.

해결 방법:

1. 애플리케이션의 비활성 시간이 비교적 긴 경우에 keep_alive_interval이 3600초 미만으로 설정된 호스트에서 TCP keepalive를 사용하도록 설정합니다.
2. 다음과 같은 NSX REST API를 사용하여 Edge TCP 비활성 시간 초과 값이 2시간을 넘도록 늘립니다. 예를 들어, 비활성 시간 초과 값을 9000초로 늘릴 수 있습니다. NSX API URL:
/api/4.0/edges/{edgclid}/systemcontrol/config PUT Method <systemControl>
<property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</property>
</systemControl>

- **문제 1089238: 두 개 이상의 DLR Edge 업링크에 OSPF를 구성할 수 없음**
현재 8개의 DLR Edge 업링크 중 두 개 이상에 OSPF를 구성할 수 없습니다. 이러한 제한은 DLR 인스턴스당 하나의 전달 주소 공유에 따른 결과입니다.

해결 방법: 이는 현재 시스템 제한이며 해결 방법은 없습니다.

- **문제 1499978: Edge syslog 메시지가 원격 syslog 서버에 도달하지 않음**
배포 직후에 Edge syslog 서버가 구성된 원격 syslog 서버에 대한 호스트 이름을 확인할 수 없습니다.
해결 방법: 해당 IP 주소를 사용하여 원격 syslog 서버를 구성하거나, UI를 사용하여 Edge를 강제로 동기화합니다.

- **문제 1489829: REST Edge API를 업데이트한 후 논리적 라우터 DNS 클라이언트 구성 설정이 완전하게 적용되지 않음**

해결 방법: REST API를 사용하여 DNS 전달자(확인 프로그램)를 구성할 때 다음 단계를 수행합니다.

1. DNS 클라이언트 XML 서버의 설정을 DNS 전달자 설정과 일치하도록 지정합니다.
2. DNS 전달자를 사용하도록 설정하고, 전달자 설정이 XML 구성에 지정된 DNS 클라이언트 서버 설정과 동일한지 확인합니다.

- **문제 1243112: ECMP가 사용되도록 설정된 상태에서 정적 경로의 잘못된 다음 홉에 대한 검증 및 오류 메시지가 없음**

ECMP가 사용되도록 설정된 상태에서 정적 경로를 추가하려고 시도할 때 라우팅 테이블에 기본 경로가 포함되어 있지 않고 정적 경로 구성에 도달할 수 없는 다음 홉이 있는 경우, 오류 메시지가 표시되지 않고 정적 경로가 설치되지 않습니다.

해결 방법: 없음.

- **문제 1281425: 논리적 스위치로 지원되는 하나의 하위 인터페이스를 포함한 NSX Edge 가상 시스템이 vCenter Web Client 사용자 인터페이스를 통해 삭제된 경우, 데이터 경로가 동일한 포트에 연결된 새 가상 시스템에 대해 작동하지 않음**

Edge 가상 시스템을 NSX Manager에서 삭제하지 않고 vCenter Web Client 사용자 인터페이스를 통해 삭제하면 opaque 채널에서 dvPort에 구성된 VXLAN 트렁크가 재설정되지 않습니다. 이는 트렁크 구성이 NSX Manager에 의해 관리되기 때문입니다.

해결 방법: 다음 단계를 따라 수동으로 VXLAN 트렁크 구성을 삭제하십시오.

1. 브라우저 창에 다음을 입력하여 vCenter Managed Object Browser로 이동합니다.
<https://<vc-ip>/mob?vmodl=1>
2. 콘텐츠를 클릭합니다.
3. 다음 단계를 따라 dvsUuid 값을 회수합니다.
 - a. rootFolder 링크를 클릭합니다(예: group-d1(Datacenters)).
 - b. 데이터 센터 이름 링크를 클릭합니다(예: datacenter-1).
 - c. networkFolder 링크를 클릭합니다(예: group-n6).

- d. DVS 이름 링크를 클릭합니다(예: dvs-1).
- e. uuid 값을 복사합니다.
4. **DVSManager**를 클릭하고 **updateOpaqueDataEx**를 클릭합니다.
5. *selectionSet*에 다음 XML을 추가합니다.

```
<selectionSet xsi:type="DVPortSelection">
<dvsUuid>value</dvsUuid>
<portKey>value</portKey> <!--트렁크 vnic가 연결된 DVPG의 포트 번호-->
</selectionSet>
```

6. *opaqueDataSpec*에서 다음 XML을 추가합니다.

```
<opaqueDataSpec>
<operation>remove</operation>
<opaqueData>
<key>com.vmware.net.vxlan.trunkcfg</key>
<opaqueData></opaqueData>
</opaqueData>
</opaqueDataSpec>
```

7. **isRuntime**을 거짓으로 설정합니다.
8. **메서드 호출**을 클릭합니다.
9. 삭제된 Edge 가상 시스템에 구성된 각 트렁크 포트에 대해 5-8단계를 반복합니다.

- **문제 1637939: 하드웨어 게이트웨이 배포 중에 MD5 인증서가 지원되지 않음**

논리적 L2 VLAN-VXLAN 브리징을 위해 하드웨어 게이트웨이 스위치를 VTEP로 배포할 때 물리적 스위치가 NSX Controller와 OVSDB 스위치 사이의 OVSDB 연결에 대한 최소 SHA1 SSL 인증서를 지원합니다.

해결 방법: 없음.

- **문제 1637943: 하드웨어 게이트웨이 바인딩이 있는 VNI에 대한 하이브리드 또는 멀티캐스트 복제 모드 미지원**

L2 VXLAN-VLAN 브리징을 위한 VTEP로 하드웨어 게이트웨이 스위치를 사용할 경우 유니캐스트 복제 모드만 지원합니다.

해결 방법: 유니캐스트 복제 모드만 사용하십시오.

보안 서비스에 대한 알려진 문제

- **문제 1918023: Guest Introspection USVM이 100%의 메모리를 소비함**

Guest Introspection USVM이 100%의 메모리를 소비하고 이로 인해 게스트 VM과 Guest Introspection USVM과의 연결이 끊어질 수 있습니다.

해결 방법: 자세한 내용 및 해결 방법은 [VMware 기술 자료 문서 2151235](#)를 참조하십시오.

- **문제 1897878: ESXi 작업 및 이벤트가 "ESX 모듈과 통신이 끊어짐" 오류를 표시함**

ESXi 호스트 Guest Introspection 모듈(EPsec Mux)과 ESX 모듈 간의 통신이 끊어지면 ESXi 호스트에 "ESX 모듈과 통신이 끊어짐" 오류가 나타납니다.

해결 방법: 자세한 내용 및 해결 방법은 [VMware 기술 자료 문서 2151235](#)를 참조하십시오.

- **문제 1944599: 변환된 IP가 vNIC 필터에 추가되지 않아 분산 방화벽이 트래픽을 삭제함**

새 VM이 배포될 때 vNIC 필터가 올바른 IP 집합으로 업데이트되지 않아 분산 방화벽이 트래픽을 차단하게 됩니다.

해결 방법:

1. 새 VM이 배포된 영향을 받는 클러스터에서 분산 방화벽 규칙을 강제로 동기화합니다. 방화벽 규칙 강제 동기화를 참조하십시오.
2. VM IP가 누락된 보안 그룹에 대해 [편집]을 클릭하고 변경 내용을 제출합니다.

● **문제 1854661: 크로스 VC 설정에서 NSX Manager 간 전환 시 필터링된 방화벽 규칙이 인덱스 값을 표시하지 않음**

규칙 필터 기준을 NSX Manager에 적용한 다음 다른 NSX Manager로 전환하면 규칙 인덱스에서 규칙의 실제 위치를 표시하는 대신 필터링된 모든 규칙에 대해 '0'으로 표시합니다.

해결 방법: 필터를 삭제하여 규칙 위치를 확인합니다.

● **문제 1846402: 동일한 vNIC의 다중 IP 주소로 인해 방화벽 게시 작업이 지연됨**

이 문제는 vNIC에 여러 IP 주소가 있고 ARP 스누핑이 사용되도록 설정되어 있을 때 발생합니다. vNIC 외부의 각 패킷으로 인해 새로 검색된 IP를 사용해서 호스트로부터 관리자로 ARP 메시지가 전송될 수 있습니다. 이는 호스트가 관리자에게 ARP 스누핑 IP 주소를 하나만 전송할 수 있기 때문입니다. vNIC가 IP 간에 전환되면 호스트는 IP를 새 IP로 감지하고 ARP 스누핑 메시지를 관리자로 전송합니다. 이로 인해 NSX Manager에서 컨테이너 메시지가 변동되고 호스트에서 방화벽 구성을 실현하는 데 시간이 오래 지연됩니다.

해결 방법: vNIC에 여러 IP 주소가 있을 때 ARP 스누핑을 사용하지 않도록 설정합니다. DHCP 스누핑 또는 VMTools를 대신 사용하십시오.

● **문제 1474650: NetX 사용자의 경우 ESXi 5.5.x 및 6.x 호스트에서 다음을 언급하는 자주색 진단 화면이 나타납니다. ALERT: NMI: 709: NMI IPI received**

서비스 VM에서 다량의 패킷이 전송되거나 수신된 경우 DVFilter가 계속 CPU에서 점유하여 하트비트 손실 및 자주색 진단 화면으로 이어집니다. 자세한 내용은 [VMware 기술 자료 문서 2149704](#)를 참조하십시오.

해결 방법: NetX 사용에 필요한 다음의 최소 ESXi 버전으로 ESXi 호스트를 업그레이드합니다.

- 5.5 패치 10
- ESXi 6.0U3
- ESXi 6.5

● **문제 1799543: NSX 6.2.x에서 NSX 6.3.0으로 업그레이드한 후에 첫 번째 활성-대기 범용 Security Group을 생성하려고 하면 vSphere Web Client가 잘못 표시되고 NSX 6.2.x 범용 Security Group 및 비활성-대기 범용 Security Group을 선택할 수 있도록 허용함**

첫 번째 활성-대기 범용 Security Group을 생성할 경우 vSphere Web Client UI가 표시되고 NSX 6.2.x에서 생성된 범용 Security Group을 추가할 수 있도록 허용합니다. "요청된 멤버가 유효한 멤버가 아닙니다." 오류를 표시하면서 작업이 실패합니다.

해결 방법: 하나 이상의 활성-대기 범용 Security Group을 생성한 후 다음 활성-대기 범용 Security Group을 생성하는 동안에는 이 문제가 발생하지 않습니다.

● **문제 1787680: NSX Manager가 전송 모드인 경우 범용 방화벽 섹션이 삭제되지 않음**

전송 모드인 NSX Manager의 UI에서 범용 방화벽 섹션 삭제를 시도하고 게시할 때 게시가 되지 않고 그 결과 NSX Manager를 독립형 모드로 설정할 수 없습니다.

해결 방법: 범용 방화벽 섹션을 삭제하려면 단일 삭제 섹션 REST API를 사용하십시오.

● **문제 1741844: 여러 IP 주소가 있는 vNIC의 주소를 감지하는 ARP 스누핑으로 인해 100% CPU 사용률이 발생함**

이 문제는 가상 시스템의 vNIC가 여러 IP 주소로 구성되어 있으며 ARP 스누핑이 IP를 감지하는 데 사용되도록 설정되어 있을 때 발생합니다. IP 검색 모듈은 여러 IP 주소로 구성된 모든 VM에 대해 vNIC-IP 매핑을 변경하도록 지속적으로 NSX Manager에 vNIC-IP 업데이트를 보냅니다.

해결 방법: 해결 방법이 없습니다. 현재 ARP 스누핑 기능은 vNIC당 하나의 IP 주소만 지원합니다. 자세한 내용은 NSX 관리 가이드에서 [가상 시스템의 IP 검색](#) 섹션을 참조하십시오.

● **문제 1689159: Flow Monitoring의 [규칙 추가] 기능이 ICMP 흐름에 대해 제대로 작동되지 않음**

Flow Monitoring에서 규칙을 추가할 때 [서비스] 필드를 명시적으로 [ICMP]로 설정하지 않으면 필드가 빈 상태로 표시되며, 이로 인해 서비스 유형이 [임의]인 규칙이 추가될 수 있습니다.

해결 방법: ICMP 트래픽을 반영하도록 [서비스] 필드를 업데이트합니다.

- **문제 1632235: Guest Introspection 설치 동안 네트워크 드롭다운 목록에 "호스트에 지정"만 표시됨**
NSX 바이러스 백신 전용 라이선스 및 vSphere Essential 또는 Standard 라이선스를 사용하여 Guest Introspection을 설치할 경우 네트워크 드롭다운 목록에 DV 포트 그룹의 기존 목록만 표시됩니다. 이 라이선스는 DVS 생성을 지원하지 않습니다.
해결 방법: 이러한 라이선스 중 하나를 사용하여 vSphere 호스트에 Guest Introspection을 설치하기 전에 먼저 "에이전트 VM 설정" 창에서 네트워크를 지정합니다.

- **문제 1652155: 특정 상황에서 REST API를 사용하여 방화벽 규칙을 생성하거나 마이그레이션하지 못할 수 있으며 HTTP 404 오류가 보고됨**
다음과 같은 상황에서는 REST API를 사용하여 방화벽 규칙을 추가하거나 마이그레이션할 수 없습니다.
 - autosavedraft=true가 설정되었을 때 방화벽 규칙을 대량 작업으로 생성
 - 여러 섹션에서 방화벽 규칙을 동시에 추가

해결 방법: 대량 방화벽 규칙 생성 또는 마이그레이션을 수행할 때 API 호출에서 autoSaveDraft 매개 변수를 false로 설정합니다.

- **문제 1509687: 하나의 API 호출로 한 번에 여러 VM에 단일 보안 태그를 할당할 경우 지원되는 최대 URL 길이는 16,000자임**
URL 길이가 16,000자를 초과할 경우 하나의 API로 많은 수의 VM에 단일 보안 태그를 동시에 할당할 수 없습니다.
해결 방법: 성능을 최적화하려면 단일 호출에서 VM을 500개 이하로 태그합니다.

- **문제 1662020: 게시 작업이 실패하여 "일반 및 파트너 보안 서비스" 섹션의 DFW UI에 "호스트 번호 호스트에서 마지막 게시 실패" 오류 메시지가 표시됨**
규칙을 변경하면 UI에 "호스트 번호 호스트에서 마지막 게시 실패"가 표시됩니다. UI에 등록된 호스트의 방화벽 규칙 버전이 올바르지 않아 보안이 되지 않거나 네트워크 중단이 발생할 수 있습니다.

이 문제는 일반적으로 다음 시나리오에서 볼 수 있습니다.

- 이전 NSX 버전에서 최신 버전으로 업그레이드한 후
- 호스트를 클러스터 외부로 이동한 후 돌려 놓음
- 호스트를 한 클러스터에서 다른 클러스터로 이동함

해결 방법: 복구하려면 영향을 받은 클러스터를 강제로 동기화해야 합니다(방화벽만 해당).

- **문제 1481522: 6.1.x의 방화벽 규칙 초안을 6.2.3으로 마이그레이션하는 것은 두 릴리스 간에 초안이 호환되지 않기 때문에 가능하지 않음**

해결 방법: 없음.

- **문제 1628679: ID 기반 방화벽을 사용하는 경우 제거된 사용자의 VM이 계속해서 보안 그룹에 포함됨**

AD 서버의 그룹에서 사용자를 제거할 경우 사용자가 로그인된 VM은 계속해서 보안 그룹에 속합니다. 이를 통해 하이퍼바이저의 VM vNIC에서 방화벽 정책이 유지되므로 사용자에게 서비스에 대한 전체 액세스가 부여됩니다.

해결 방법: 없음. 이는 의도된 동작입니다.

- **문제 1496273: UI에서 Edge에 적용할 수 없는 내부/외부 NSX 방화벽 규칙을 생성할 수 있음**
PacketType이 IPV4 또는 IPV6이고, 규칙에 '내부' 또는 '외부' 방향으로 이동하는 트래픽이 포함된 경우에 웹 클라이언트가 하나 이상의 NSX Edge에 적용되는 NSX 방화벽 규칙을 생성할 수 있도록 잘못 허용합니다. NSX는 이러한 규칙을 NSX Edge에 적용할 수 없기 때문에 UI에서 해당 규칙을 생성할 수 없어야 합니다.
해결 방법: 없음.

- **문제 1557924: 로컬 DFW 규칙의 appliedTo 필드에서 범용 논리적 스위치를 사용하도록 허용됨**
범용 논리적 스위치를 보안 그룹 멤버로 사용할 때 DFW 규칙에서 해당 보안 그룹을 AppliedTo 필드에서 사용할 수 있습니다. 이 경우 범용 논리적 스위치에 해당 규칙이 간접적으로 적용되는데, 그러면 이러한 규칙에 알 수 없는 동작이 발생할 수 있기 때문에 허용해서는 안 됩니다.

해결 방법: 없음.

- **문제 1559971: 한 클러스터에서 방화벽을 사용하지 않도록 설정된 경우 크로스 vCenter NSX 방화벽 제외 목록이 게시되지 않음**

크로스 vCenter NSX에서, 클러스터 중 하나에서 방화벽을 사용하지 않도록 설정되어 있으면 방화벽 제외 목록이 어느 클러스터에도 게시되지 않습니다.

해결 방법: 문제가 발생한 NSX Edge를 강제 동기화합니다.

- **문제 1407920: DELETE API를 사용한 후 방화벽 규칙을 다시 게시할 수 없음**

DELETE API 메서드를 통해 전체 방화벽 구성을 삭제한 다음 이전에 저장한 방화벽 초안에서 모든 규칙을 다시 게시하려고 하면, 규칙 게시에 실패합니다.

- **문제 1494718: 새로운 범용 규칙을 생성할 수 없고 흐름 모니터링 UI에서 기존 범용 규칙을 편집할 수 없음**

해결 방법: 범용 규칙은 흐름 모니터링 UI에서 추가하거나 편집할 수 없습니다. EditRule은 자동으로 사용되지 않도록 설정됩니다.

- **문제 1442379: Service Composer 방화벽 구성이 동기화되지 않음**

NSX Service Composer에서 잘못된 방화벽 정책이 있는 경우(예를 들어 방화벽 규칙에서 사용 중이던 Security Group을 삭제) 다른 방화벽 정책을 삭제하거나 수정하면 Service Composer는 오류 메시지 방화벽 구성이 동기화되지 않았습니.를 표시하고 동기화되지 않은 상태가 됩니다.

해결 방법: 잘못된 방화벽 규칙을 모두 삭제한 다음 방화벽 구성을 동기화합니다. **Service Composer: 보안 정책**을 선택하고 연결된 방화벽 규칙이 있는 각 보안 정책에 대해 **작업**을 클릭하고 **방화벽 구성 동기화**를 선택합니다. 이 문제를 방지하려면 방화벽 구성을 더 변경하기 전에 항상 잘못된 방화벽 구성을 수정하거나 삭제하십시오.

- **문제 1066277: 보안 정책 이름에 229자가 넘는 이름이 허용되지 않음**

Service Composer의 [보안 정책] 탭에 있는 보안 정책 이름 필드는 최대 229자까지만 허용됩니다. 이는 내부적으로 정책 이름 앞에 접두사가 추가되기 때문입니다.

해결 방법: 없음.

- **문제 1443344: 타사 네트워크 VM 시리즈의 일부 버전이 NSX Manager 기본 설정에서 작동하지 않음**

일부 NSX 6.1.4 이상의 구성 요소는 기본적으로 SSLv3를 사용하지 않도록 설정합니다. 업그레이드하기 전에 NSX 배포와 통합된 모든 타사 솔루션이 SSLv3 통신을 사용하지 않는지 확인하십시오. 예를 들어 Palo Alto Networks VM-시리즈 솔루션의 일부 버전에는 SSLv3의 지원이 필요하므로 벤더에 버전 요구 사항을 확인하십시오.

- **문제 1660718: Service Composer 정책 상태가 UI에서는 "진행 중"으로 나타나고 API 출력에서는 "보류 중"으로 나타남**

해결 방법: 없음.

- **문제 1620491: Service Composer의 정책 수준 동기화 상태가 정책 내 규칙의 게시 상태를 나타내지 않음**

정책이 생성되거나 수정될 때 Service Composer는 지속성 상태만 나타내는 성공 상태를 표시합니다. 이러한 상태는 규칙이 호스트에 성공적으로 게시되었는지에 대해서는 알려주지 않습니다.

해결 방법: 방화벽 UI를 사용하여 게시 상태를 확인합니다.

- **문제 1317814: Service Manager 중 하나가 중지된 상태에서 정책이 변경된 경우 Service Composer가 동기화되지 않음**

여러 Service Manager 중 하나가 중지된 상태일 때 정책이 변경되면 변경은 실패하고 Service Composer는 동기화되지 않습니다.

해결 방법: Service Manager가 응답하는지 확인한 다음 Service Composer에서 강제 동기화를 수행합니다.

- **문제 1070905: Guest Introspection 및 타사 보안 솔루션에서 보호하는 클러스터에서 호스트를 제거했다 다시 추가할 수가 없음**

Guest Introspection 및 타사 보안 솔루션에서 보호하는 클러스터의 호스트를 제거하기 위해 vCenter Server에서 연결을 끊어 호스트를 제거하는 경우 동일한 호스트를 동일한 클러스터에 다시 추가하려고 할 때 문제가 발생할 수 있습니다.

해결 방법: 보호되는 클러스터에서 호스트를 제거하려면 먼저 해당 호스트를 유지 보수 모드로 전환합니다. 그런 다음 호스트를 보호되지 않는 클러스터 또는 모든 클러스터의 외부로 이동한 다음 연결을 끊고 호스트를 제거합니다.

- **문제 1648578: 새 NetX 호스트 기반 서비스 인스턴스를 생성할 때 NSX가 클러스터/네트워크/스토리지를 강제로 추가하도록 함**

방화벽, IDS 및 IPS와 같은 NetX 호스트 기반 서비스용 vSphere Web Client에서 새 서비스 인스턴스를 생성할 때 필수 요소가 아니더라도 클러스터/네트워크/스토리지를 강제로 추가하도록 요구됩니다.

해결 방법: 새 서비스 인스턴스를 생성할 때 클러스터/네트워크/스토리지에 대한 정보를 추가하여 필드를 채울 수 있습니다. 이를 통해 서비스 인스턴스를 생성할 수 있으며 필요에 따라 작업을 계속 진행할 수 있습니다.

- **문제 1772504: Service Composer가 MAC 집합이 있는 보안 그룹을 지원하지 않음**

Service Composer는 [정책] 구성에서 Security Group을 사용하도록 허용합니다. MAC 집합이 포함된 보안 그룹이 있는 경우 Service Composer는 이상 없이 해당 보안 그룹을 허용하지만 해당 특정 MAC 집합에 대해 규칙을 적용하지 못합니다. 이는 Service Composer가 계층 3에서 작동하고 계층 2 구성을 지원하지 않기 때문입니다. 보안 그룹에 IP 집합 및 MAC 집합이 둘 다 있는 경우 IP 집합은 계속 유효하지만 MAC 집합은 무시됩니다. MAC 집합을 포함하는 보안 그룹을 참조해도 문제는 없습니다. 사용자는 MAC 집합이 무시된다는 사실을 알고 있어야 합니다.

해결 방법: 사용자의 의도가 MAC 집합을 사용하여 방화벽 규칙을 생성하는 것인 경우 Service Composer 대신 DFW 계층 2/이더넷 구성을 사용해야 합니다.

- **문제 1718726: 사용자가 DFW REST API를 사용하여 직접 Service Composer의 정책 섹션을 삭제한 후에 Service Composer를 강제 동기화할 수 없음**

크로스 vCenter NSX 환경에서 정책 섹션이 하나만 있고 정책 섹션(Service Composer 관리 정책 섹션)이 REST API 호출을 통해 이전에 삭제된 경우 NSX Service Composer 구성을 강제 동기화하려는 사용자 시도가 실패합니다.

해결 방법: REST API 호출을 통해 Service Composer 관리 정책 섹션을 삭제하지 마십시오. (UI에서 이 섹션의 삭제를 방지합니다.)

모니터링 서비스에 대한 알려진 문제

- **문제 1466790: NSX traceflow 도구를 사용하여 브리지 네트워크에서 VM을 선택할 수 없음**

NSX traceflow 도구를 사용하여 논리적 스위치에 연결되지 않은 VM을 선택할 수 없습니다. L2 브리지 네트워크의 VM을 VM 이름 기준으로 traceflow 검사의 소스 또는 대상 주소로 선택할 수 없습니다.

해결 방법: L2 브리지 네트워크에 연결된 VM의 경우 traceflow 검사에서 대상으로 지정하려는 인터페이스의 IP 주소 또는 MAC 주소를 사용합니다. L2 브리지 네트워크에 연결된 VM을 소스로 선택할 수 없습니다. 자세한 내용은 [기술 자료 문서 2129191](#)을 참조하십시오.

솔루션 상호 운용성에 대한 알려진 문제

- **문제 1568861: vCenter 수신기가 없는 vCloud Director 셀에서 Edge를 배포할 때 NSX Edge 배포가 실패함**

vCenter 수신기가 없는 vCloud Director 셀에서 Edge를 배포할 때 NSX Edge 배포가 실패합니다. 또한 재배포를 포함한 NSX Edge 작업이 vCloud Director에서 실패합니다.

해결 방법: vCenter 수신기가 있는 vCloud Director 셀에서 NSX Edge를 배포하십시오.