

# VMware NSX for vSphere 6.3.7 릴리스 정보

VMware NSX for vSphere 6.3.7 | 릴리스 날짜: 2018년 11월 15일 | 빌드 10667122

이 문서의 [개정 이력](#)을 참조하십시오.

## 릴리스 정보에 포함된 내용

릴리스 정보에는 다음과 같은 항목이 포함됩니다.

- [NSX 6.3.7 새로운 기능](#)
- [버전, 시스템 요구 사항 및 설치](#)
- [제거 및 지원 중단된 기능](#)
- [업그레이드 정보](#)
- [FIPS 준수](#)
- [개정 이력](#)
- [해결된 문제](#)
- [알려진 문제](#)

## NSX 6.3.7 새로운 기능

NSX for vSphere 6.3.7은 다양한 특정 고객 버그를 해결합니다. 자세한 내용은 [해결된 문제](#)를 참조하십시오.

이전 버전에 대한 릴리스 정보를 확인하십시오.

- [NSX 6.3.6](#)
- [NSX 6.3.5](#)
- [NSX 6.3.4](#)
- [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 최신 NSX 릴리스를 사용하는 것이 좋습니다.</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"> <li>• vSphere 5.5U3 이상</li> <li>• vSphere 6.0U3 이상. vSphere 6.0U3는 vCenter Server를 재부팅한 후 ESXi 호스트에서의 중복 VTEP 문제를 해결합니다. 자세한 내용은 <a href="#">VMware 기술 자료 문서 2144605</a>를 참조하십시오.</li> <li>• vSphere 6.5U1 이상. vSphere 6.5U1은 OutOfMemory로 인한 EAM 실패 문제를 해결합니다. 자세한 내용은 <a href="#">VMware 기술 자료 문서 2135378</a>을 참조하십시오.</li> </ul>
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"> <li>• 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.</li> <li>• NSX/vCloud Networking and Security에서 VMware Tools를 업그레이드한 후에 VM이 느려지는 문제를 해결하려면 VMware Tools 10.0.8 이상으로 업그레이드합니다(<a href="#">VMware 기술 자료 문서 2144236</a> 참조).</li> <li>• Windows 10 지원을 위해 VMware Tools 10.1.0 이상을 사용합니다.</li> <li>• Windows Server 2016 지원을 위해 VMware Tools 10.1.10 이상을 사용합니다.</li> </ul>
Linux용 Guest Introspection	<p>이 NSX 버전은 다음 Linux 버전을 지원합니다.</p> <ul style="list-style-type: none"> <li>• RHEL 7 GA(64비트)</li> <li>• SLES 12 GA(64비트)</li> <li>• Ubuntu 14.04 LTS(64비트)</li> </ul>

## 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 for vSphere 6.2.x**는 2018년 8월 20일에 EOGS(일반 지원 종료) 상태가 됩니다.
- **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.

## 일반적인 동작 변경

둘 이상의 vSphere Distributed Switch가 있고 이러한 스위치 중 하나에 VXLAN이 구성된 경우, 모든 논리적 분산 라우터 인터페이스를 해당 vSphere Distributed Switch의 포트 그룹에 연결해야 합니다. NSX 6.3.6부터 이 구성이 UI 및 API에 적용됩니다. 이전 릴리스에서는 사용자가 잘못된 구성을 생성하는 것을 막을 수 없었습니다.

## API 제거 및 동작 변경

### API 오류 처리 변경

NSX 6.3.5에서는 오류 처리가 다음과 같이 변경되었습니다.

- API 요청이 NSX Manager에서 데이터베이스 예외를 발생할 경우 응답은 500 내부 서버 오류입니다. 이전 릴리스에서는 요청이 실패하더라도 NSX Manager가 200 정상으로 응답했습니다.
- 요청 본문이 필요한 상황에서 본문이 비어 있는 API 요청을 전송하면 응답은 400 잘못된 요청입니다. 이전 릴리스에서는 NSX Manager가 500 내부 서버 오류로 응답했습니다.
- 이 API, GET /api/2.0/services/policy/securitygroup/{ID}/securitypolicies에 잘못된 보안 그룹을 지정하는 경우 응답은 404 찾을 수 없음입니다. 이전 릴리스에서는 NSX Manager가 200 정상으로 응답했습니다.

### 백업 및 복원 API 기본값 변경

6.3.3부터, 두 백업 및 복원 매개 변수의 기본값이 UI의 기본값과 일치하도록 변경되었습니다. 이전에 **passiveMode** 및 **useEPSV** 기본값은 *false*였으나 지금은 *true*입니다. 이러한 점은 다음 API에 영향을 줍니다.

- PUT /api/1.0/appliance-management/backuprestore/backupsettings
- PUT /api/1.0/appliance-management/backuprestore/backupsettings/ftpsettings

### 방화벽 구성 또는 기본 섹션 삭제

- 6.3.0부터 기본 섹션이 지정된 경우 이 요청이 거부됩니다. DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId
- 기본 구성을 가져오기 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

### defaultOriginate 매개 변수:

NSX 6.3.0부터 defaultOriginate 매개 변수는 논리적(분산) 라우터 NSX Edge 장치의 경우에만 다음 메시드에서 제거됩니다.

- 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 메시드가 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

- 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 가이드에서 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

- **중요:** NSX 6.2.0, 6.2.1 또는 6.2.2를 NSX 6.3.5 이상으로 업그레이드하는 경우 업그레이드를 시작하기 전에 해결 방법을 완료해야 합니다. 자세한 내용은 [VMware 기술 자료 문서 000051624](#)를 참조하십시오.
- 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 6.3.4 이상으로 업그레이드하려는 경우 [VMware 기술 자료 문서 2151719](#)의 해결 방법 지침을 먼저 수행해야 합니다.
- NSX Manager를 NSX 6.3.6 이상으로 업그레이드하면 업그레이드 프로세스의 일부로 백업이 자동으로 생성되어 로컬에 저장됩니다. 자세한 내용은 [NSX Manager 업그레이드](#)를 참조하십시오.

### 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.

컨트롤러가 삭제되면 연결된 모든 DRS 반선택도 규칙도 삭제됩니다. 새 컨트롤러 VM이 동일한 호스트에 상주하지 않도록 하려면 vCenter에서 새로운 반선택도 규칙을 생성해야 합니다.

컨트롤러 업그레이드에 대한 자세한 내용은 [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 쉼표 등의 다른 구분 기호를 사용하는 경우 [https://nsxmgr\\_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles](https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles)에 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"
    }

```

## Guest Introspection 업그레이드

- 이제 Guest Introspection VM의 XML 파일에는 추가 호스트 식별 정보가 포함되어 있습니다. Guest Introspection VM에 로그인하면 파일 "/opt/vmware/etc/vami/ovfEnv.xml"에 호스트 ID 정보가 포함됩니다.

## 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

2018년 11월 15일 1차 개정판.

2019년 3월 3일: 2차 개정판. 해결된 문제 2249307을 추가했습니다.

2019년 5월 13일: 3차 개정판. 호스트 클러스터 업그레이드 섹션이 업데이트되었습니다.



# 해결된 문제

해결된 문제는 다음과 같이 분류됩니다.

- 논리적 네트워킹 및 NSX Edge에 대한 해결된 문제
- 일반적인 해결된 문제
- NSX Controller에 대해 해결된 문제
- NSX Manager에 대해 해결된 문제
- 설치 및 업그레이드에 대해 해결된 문제
- 보안 서비스에 대해 해결된 문제

## 논리적 네트워킹 및 NSX Edge에 대한 해결된 문제

- 해결된 문제 2207483: E-W 및 N-S 라우팅 트래픽에 대해 긴 지연 시간  
VM의 TxWorld가 생성하는 라우팅된 트래픽이 100%의 CPU를 사용하여 높은 지연 시간이 발생합니다.
- 해결된 문제 2188666: SSLVPN Linux 클라이언트 CLI를 사용하여 5자리 포트 번호를 갖는 게이트웨이에 연결할 수 없음  
Linux에서 5자리 포트 번호를 갖는 게이트웨이에 연결하려는 경우 SSLVPN 클라이언트 GUI를 사용해야 합니다. GUI에서는 가능하지만, SSLVPN Linux CLI는 최대 4자리 숫자에만 작동하기 때문입니다.
- 해결된 문제 2185457: 브리지 워크로드에 대한 네트워크 지연 시간 증가  
브리지 네트워크에서 높은 트래픽(pps)을 발생하는 워크로드로 인해 VLAN과 VXLAN 간에 지연 시간이 발생할 수 있습니다.
- 해결된 문제 2182874: 사이트 간에 겹치는 VDR ID가 있으면 VDR ID를 사용할 수 없음  
사이트를 다중 vc로 전환하려고 할 때 둘 이상의 사이트에 겹치는 세그먼트 범위가 있으면 한 사이트의 세그먼트 범위를 변경해야 했습니다.
- 해결된 문제 2181650: ARP 항목 새로 고침에 대한 ARP 요청을 전송할 때 GARP를 유효한 응답으로 수락함  
일부 오래된 디바이스에서는 ARP 요청에 대한 응답으로 GARP를 전송합니다.
- 해결된 문제 2181435: ESX 5.5에서 통계 폴링 동안 Hostd가 충돌함  
ESX 5.5에서 통계 폴링 동안 Hostd가 충돌합니다. Hostd를 다시 시작해야 합니다.
- 해결된 문제 2179054: NSX 설치 및 업그레이드 동안 IXGBE 드라이버를 다시 시작하지 않아야 함  
호스트의 서비스에 대해 5~10초 정도 네트워크 중단이 발생합니다.
- 해결된 문제 2178950: HA를 사용하도록 설정할 경우 트래픽 중단이 발생하거나 vCenter에서 같은 Edge에 대해 2개가 넘는 VM이 존재함  
HA를 사용하도록 설정할 경우 트래픽 중단이 확인되거나, vCenter에서 같은 Edge에 대해 2개가 넘는 VM이 존재합니다. 장치를 편집하거나 장치 배치를 변경하여 복원이 수행될 경우 VM이 꼬이게 되어 네트워크가 중단될 수 있습니다.
- 해결된 문제 2177514: 일부 경우에 DaD ping이 다시 전달되어 DaD 프로세스가 중복된 IP 주소를 감지하게 됩니다.  
시스템 이벤트는 가짜 중복 IP를 감지했다고 보고합니다.
- 해결된 문제 2176316: Edge 이름이 방화벽 규칙에서 업데이트되지 않음  
Edge UI에서 Edge 이름을 변경해도 방화벽 UI에 계속 이전 Edge 이름이 표시됩니다.
- 해결된 문제 2172005: "show ip bgp" CLI 명령을 실행하는 경우 BGP 인접 네트워크가 불안정함  
BGP가 AS\_PATH가 126자보다 긴 학습 경로를 사용하며 "show ip bgp" 명령을 실행할 경우 라우팅 스택이 다시 시작됩니다. BGP가 다시 통합될 때까지 경로가 변동되며 트래픽 중단이 발생할 수 있습니다.
- 해결된 문제 2171616: ESG 호스트 이름을 확인할 수 없는 경우 SSL VPN Windows 클라이언트 프로세스가 충돌함  
HTTP 프록시가 구성되고 ESG 호스트 이름을 확인할 수 없는 경우 클라이언트 프로세스가 충돌합니다.

- **해결된 문제 2167176: HA 지원 tmpfs 파티션이 있는 DLR Edge가 꽉 채워짐**  
HA를 사용하도록 설정하면 /var/run 디렉토리(tmpfs)가 완전히 채워집니다. 꽉 차면 구성이 작동하지 않게 됩니다.
- **해결된 문제 2164068: HA를 사용하도록 설정하면 잠시 후에 전체 Edge tmpfs 파티션이 꽉 채워짐**  
Rsync를 사용하여 HA 쌍의 Edge VM 간에 파일이 동기화됩니다. Rsync가 컴파일된 방식 때문에 주기적인 rsync 호출이 수행될 때마다 오류 로그 메시지가 생성되어 tmpfs 파티션의 로그 파일에 저장되었습니다. 얼마 후에 파티션은 꽉 채워지며 Edge의 정상적인 작업에 심각한 영향을 미칩니다.
- **해결된 문제 2156094: SSL VPN Linux 클라이언트 CLI를 사용하여 5자리 포트 번호를 갖는 게이트웨이에 연결할 수 없음**  
Linux에서 5자리 포트 번호를 갖는 게이트웨이에 연결하려는 경우 SSL VPN 클라이언트 GUI를 사용해야 합니다. GUI에서는 가능하지만, SSL VPN Linux CLI는 최대 4자리 숫자에만 작동하기 때문입니다.
- **해결된 문제 2152060: Edge의 모니터 서비스 엔진(Nagios)에서 메모리 누수가 발생함**  
로드 밸런서는 해당 구성이 메모리가 없는 모니터 서비스를 사용할 때 잘 작동하지 않습니다.
- **해결된 문제 2140512: 6.3.x 이상으로 업그레이드한 후 MP 데이터베이스에서 TransportZone(vdnscope) 항목이 누락되면 VXLAN 및 논리적 네트워킹 오류가 발생함**  
NSX용으로 준비된 클러스터에서 VXLAN 및 논리적 네트워크 오류가 발생합니다.
- **해결된 문제 2134760: SSL VPN Mac 클라이언트 설치가 성공적으로 완료되었으나 이 애플리케이션을 실행할 수 없음**  
이 클라이언트는 설치는 성공적으로 완료되었으나 열리지 않습니다.
- **해결된 문제 2100704: 특정 시나리오에서 NSX Edge에서 NSX Manager와의 VMCI 연결이 끊어질 수 있음**  
Edge를 관리할 수 없게 되어 Edge로 구성을 푸시하지 못할 수 있습니다.
- **해결된 문제 2092516: 여러 모니터 작업자가 풀 멤버 상태를 동시에 업데이트함**  
로드 밸런싱이 잘 작동하지 않거나, 일부 트래픽이 느려져서 비정상 서버로 발송되거나, 정상 서버에서 처리할 트래픽이 없어집니다.
- **해결된 문제 2078866: 호스트 재부팅 시 refreshHostdNetstackCache()에서 nsxv-vib가 실패함**  
VXLAN Rx 처리량 성능이 저하될 수 있습니다.
- **해결된 문제 2028337: Edge CPU 사용량이 90%를 초과할 경우 상위 5개의 CPU 사용 프로세스가 표시되지 않음**  
Edge CPU 사용량이 90%를 초과하면 Edge가 시작된 후에 상위 5개 CPU 사용 프로세스 목록을 표시하는 알림이 Manager로 전송됩니다. 이 순간에 이 목록에 상위 5개 CPU 사용자가 표시되지 않아 CPU 사용량 문제를 진단하기 어려울 수 있습니다.
- **해결된 문제 1983497: 브리지 페일오버 및 브리지 구성 변경이 동시에 발생할 경우 보라색 화면이 표시됨**  
브리지 페일오버 및 브리지 구성 변경이 동시에 발생할 경우 교착 상태가 발생하고 보라색 화면이 표시될 수 있습니다. 교착 상태로 진행될 가능성은 낮습니다.
- **해결된 문제 2181633: 게스트 VM의 하위 인터페이스 IP 주소의 ARP 억제 실패**  
이러한 인터페이스의 ARP 확인이 처음에는 일반적인 경우(1초)보다 약간 더 오래 걸립니다.
- **해결된 문제 2170329: DNS 구성이 SSLVPN Windows 클라이언트 인터페이스에 적용되지 못함**  
DNS 쿼리가 실패하여 액세스에 영향을 미칩니다.

#### 일반적인 해결된 문제

- **해결된 문제 2183198: 포트가 없는 ToR 스위치에서 포트를 검색할 때 UI에 오류가 표시됨**  
하드웨어 게이트웨이의 물리적 스위치에 포트가 없는 경우 스위치에서 포트를 가져오려고 할 때 NSX UI에서 오류가 발생합니다. 포트 정보를 검색하는 동안 UI에 "인벤토리 정보를 가져올 수 없습니다." 오류가 표시됩니다.
- **해결된 문제 2176000: 관리부에서 전송한 메시지와 호스트에 필요한 메시지의 인코딩 차이 때문에 DVS의 업링크 포트 이름이 올바르게 표시되지 않아 MAC 확인이 실패할 수 있음**

DLR이 다른 ESXi 호스트에서 VM의 mac 주소를 확인하지 못합니다.

- **해결된 문제 2170413: API /api/3.0/ai/directorygroup이 작동하지 않음**  
백엔드에서 NullPointerException이 발생하고 API는 오류를 반환합니다. 워크플로를 자동화할 수 없습니다.
- **해결된 문제 2170395: domain\_object가 ai\_group 테이블과 동기화되지 않음**  
Service Composer 페이지가 로드될 경우 그룹 ID의 빈 목록을 포함하는 SQL로 인해 SQLGrammarException 예외가 발생합니다.
- **해결된 문제 2131680: 거부 방화벽 규칙을 충족하는 멀티캐스트 패킷으로 인해 vmkernel 로그에서 로깅이 과도하게 증가함**  
vmkernel 로그의 과도한 로깅으로 인해 호스트가 로깅을 중지하게 됩니다.
- **해결된 문제 2129177: 업그레이드 프로세스 동안 및 이전 버전과의 호환성 모드에서 GI-SVM을 삭제하거나 제거하면 GI 클러스터가 업그레이드되지 않는 한, GI(Guest Introspection)를 통한 ID 방화벽이 작동하지 않음**  
ID 방화벽이 작동하지 않으며 ID 방화벽과 관련된 로그가 표시되지 않습니다. 클러스터가 업그레이드되지 않으면 ID 방화벽 보호가 일시 중단됩니다.
- **해결된 문제 2105632: USVM이 Google(외부) NTP 서버와 시간을 동기화하려고 함**  
이 동작을 방지하기 위해 timesync 서비스가 수정되었습니다.
- **해결된 문제 2003396: 많은 수의 경로가 구성된 경우 재부팅 후 또는 새 호스트 가입 시 DLR LIF/경로가 누락됨**  
경로가 구성된 것으로 표시되지 않습니다.
- **문제 1960383: 많은 수의 인벤토리 개체가 짧은 기간 안에 삭제될 경우 시간 초과로 인해 네트워크 생성이 실패함**  
NSX의 dvpg 생성 지연으로 인해 네트워크 생성 시간 초과가 발생합니다.
- **해결된 문제 2058770: vCenter에서 과도한 로그인 이벤트가 발생하고 vCenter SSO 서버에서 로드가 많아짐**  
vCenter SSO 사용자가 짧은 기간 안에 많은 NSX API 요청을 수행하는 경우 vCenter SSO 서버에서 과도한 로그인 이벤트가 발생하고 로드가 많아집니다. 이로 인해 동작이 느려질 수 있습니다.
- **해결된 문제 2046427: Vmknics 또는 LS dvs 포트 그룹 팀 구성 정책을 변경하면 DP가 중단될 수 있음**  
사용자가 호스트 준비(VXLAN) 동안 vmknics 팀 구성 정책을 설정하는 경우 DVS의 업링크 팀 구성 정책이 그에 따라 설정됩니다. 생성된 모든 새로운 논리적 스위치 dvs pg도 이 팀 구성 정책을 가져옵니다.
- **해결된 문제 2178339: rsyslog 8.15.0-7.ph1이 systemd service 파일에서 ExecReload 줄을 제거하여 /var/log/syslog 및 /var/log/messages가 적절히 logrotate되지 않음**  
이로 인해 /var/log 파티션이 100%까지 디스크 공간을 채우므로 새 로그를 쓸 수 없습니다.
- **해결된 문제 2146879: 독립형 설정에서 강제 동기화로 ToR 및 ToR 바인딩이 동기화되지 않음**  
독립형 설정에서 관리부와 컨트롤러 사이에 HW 바인딩 또는 HW 전송 노드 구성이 동기화되지 않을 경우 강제 동기화로 구성을 동기화할 수 없습니다. ToR 바인딩이 동기화되지 않은 경우 ToR 구성을 컨트롤러와 동기화할 수 없습니다.
- **해결된 문제 2146749: ESXi 호스트가 재부팅 후 로케일 ID 구성을 손실함**  
호스트가 잘못된 로케일 ID를 수신하고 해당 경로는 플러시됩니다.
- **해결된 문제 2200396: 페일오버 후 보조 사이트의 ESXi 호스트에서 Vdr 인스턴스가 다시 생성됨**  
페일오버가 있고 약 40초 후에 트래픽이 중단되고 네트워크 가동이 멈춥니다.
- **해결된 문제 2100296: vCenter/PSC에서 SSL/TLS1.0을 사용하지 않도록 설정한 후에 NSX 6.3.5 Web Client 플러그인에 어떤 NSX Manager도 표시되지 않음**  
vCenter에서 SSL/TLS1.0을 사용하지 않도록 설정할 경우 NSX와 vCenter, NSX 또는 ESX와의 통신이 끊어집니다. vCenter 애플리케이션은 NSX Manager와 통신하지 않습니다.

- **해결된 문제 2077492: ipsec 사이트에 대한 NSX Manager auto creates ipsecsite Id가 이미 있음**
  - ipsec 사이트에 대한 NSX Manager auto creates ipsecsite Id가 이미 있습니다.
  - NSX for vSphere를 6.2.X에서 6.3.5 또는 6.4.0a로 업그레이드하면 Ipsec 사이트의 사이트 ID가 중복될 수 있습니다.
  - 중복된 사이트 ID가 도입되면 다음 ipsec 구성이 실패합니다.
  - 다음과 유사한 오류가 표시됩니다. [13646] [Ipsec] 중복된 Ipsec 사이트 ID ipsecsite-id를 찾았습니다.
- **해결된 문제 2177097: API 호출 /api/2.0/vdn/config/segments를 사용하여 세그먼트 ID가 1인 폴을 생성할 경우 "세그먼트 ID가 올바른 범위 5000-16777215를 벗어납니다."를 나타내며 실패함**  
API /api/2.0/vdn/config/segments를 사용할 경우 단일 값 세그먼트를 생성할 때 동일한 시작 및 종료 값을 제공하면 오류를 발생하며 실패합니다.
- **해결된 문제 2172267: 호스트가 응답하지 않을 때 NSX Edge를 삭제하면 vCenter에서 분리된 개체가 나타남**  
NSX Manager에서 Edge 인스턴스는 삭제되지만, NSX Manager가 이 Edge를 분리된 항목으로 표시하고 정리 프로세스에서 Edge를 삭제할 때까지 Edge 장치는 vCenter에 계속 존재하며 데이터 경로를 제공합니다. NSX Manager에서 Edge 장치를 삭제할 수 있는 방법은 없습니다.
- **해결된 문제 2097255: NSX Manager 장치에서 FIPS를 사용하도록 설정할 경우 SNMP 트랩이 전송되지 않음**  
SNMP 트랩이 수신되지 않습니다.

#### NSX Controller에 대해 해결된 문제

- **해결된 문제 2181306: 컨트롤러에서 메모리가 부족하여 서비스를 정상적으로 제공할 수 없음**  
이 컨트롤러는 클러스터 멤버 자격 및 상태를 쿼리하기 위한 ssh 인터페이스를 지원합니다. 클라이언트가 이 인터페이스에 액세스하여 세션을 닫지 않으면 컨트롤러는 세션을 무기한 활성 상태로 유지합니다. 충분한 세션을 열린 상태로 두면 컨트롤러의 메모리가 부족해집니다.

#### NSX Manager에 대해 해결된 문제

- **해결된 문제 2171653: NSX Manager의 보안 검사 기능이 "HTTP 보안 헤더가 감지되지 않음"을 보고함**  
보안 검사 기능이 이 문제를 보고합니다. 클릭재킹 공격이 발생할 수 있습니다.
- **해결된 문제 2161066: API 응답을 처리하는 동안 Usage Meter를 NSX Manager에 연결하지 못하고 잘못된 XML 문자 오류가 발생함**  
오류를 나타내며 Usage Meter를 NSX Manager에 연결하지 못합니다.
- **해결된 문제 2145195: NSX Manager에서 모든 USVM 및 높은 CPU 사용량에 대한 하트비트 경고 발생**  
NSX Manager는 모든 USVM이 하트비트에 응답하지는 않았음을 경고합니다. postgres 세션에 의해 해당 CPU 사용량이 높아집니다.
- **해결된 문제 2144825: 많은 nsx-tcserver-wrapper.log 파일 때문에 Manager 루트 파티션이 꽉 채워짐**  
공간 부족으로 인해 NSX UI에 액세스할 수 없고 많은 다른 서비스가 작동을 중지합니다.
- **해결된 문제 2141490: NSX Manager 및 Controller의 ToR 바인딩이 동기화되지 않음**  
논리적 스위치에서 HW 바인딩을 수정하거나 구성을 삭제할 수 없습니다. UI에 다음과 같은 오류가 표시됩니다. "컨트롤러에서 작업을 수행하지 못했습니다. {0}"
- **해결된 문제 2066631: 보안 관리자 사용자 역할을 사용하여 로그인하고 VM을 선택할 때 오류 메시지 팝업이 표시됨**  
"개체 global 및 함수 library.tagging에 액세스할 수 있는 권한이 없습니다. 함수 및 개체 액세스 범위에 대한 권한을 확인하십시오." 오류 메시지가 팝업으로 표시됩니다.
- **해결된 문제 2189810: 서비스 삽입의 일부로 구성된 모든 SecurityGroup/IPSet을 검색하기 위해 타사 서비스 삽입 솔루션에 의해 NSX Manager로 API 호출이 수행될 경우 PAN으로 보호된 게스트 VM이 트래픽을 제거함**

NSX Manager는 IPSet 또는 IPSet을 포함하는 SecurityGroup에 대해 빈 구성을 반환합니다. 결과적으로, IPSet 또는 IPSet을 포함하는 SecurityGroup이 타사 Manager에 비어 있는 것으로 보고됩니다. PAN 또는 기타 타사 방화벽 디바이스로 보호되는 게스트 VM은 일치하는 규칙이 없고 기본 거부 규칙에 해당하므로 트래픽을 제거합니다. API 호출 [https://NSXMGR\\_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset](https://NSXMGR_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset)을 실행할 경우 IPSet 또는 IPSet을 포함하는 SecurityGroup에 대한 Ip를 반환하지 않습니다.

PAN 또는 기타 타사 방화벽 디바이스로 보호되는 모든 게스트 VM은 일치하는 규칙이 없고 기본 거부 규칙에 해당하므로 트래픽을 제거합니다.

- **해결된 문제 2178700: VDR LIF 중 하나가 삭제된 virtualwire를 사용하는 경우 NSX Manager가 VDR LIF 정보를 컨트롤러와 동기화하지 못함**  
VDR LIF 작업이 실패하여 사용자가 LIF 구성을 수정할 수 없게 됩니다.
- **해결된 문제 2249307: ESXi 호스트를 NSX Manager에 다시 연결할 경우 ESXi 호스트의 로케일 ID가 기본 값으로 재설정됨**  
DLR 경로가 누락되었습니다. DLR이 트래픽을 더 이상 라우팅하지 않습니다. 호스트에서 잘못된 로케일 ID를 수신하며 의도한 DLR 경로가 유지되지 않습니다.

#### 설치 및 업그레이드에 대해 해결된 문제

- **해결된 문제 2133143: NSX DB의 오래된 클러스터 항목**  
6.2.2를 6.2.9로 업그레이드한 후에 NSX DB에 일부 오래된 클러스터 항목이 남아 있습니다.
- **해결된 문제 2112773: 컨트롤러 업그레이드 실패**  
컨트롤러를 6.2.4에서 6.3.6으로 업그레이드하지 못함

#### 보안 서비스에 대해 해결된 문제

- **해결된 문제 2098645: 보안 그룹에 삭제된 AD 그룹에 대한 참조가 있을 경우 null 포인터 예외 발생**  
AD 그룹(ai\_group)이 삭제되며, 삭제된 AD 그룹에 대한 참조가 있는 보안 그룹이 있는 경우 SG->VM 변환을 수행하면 null 포인터 예외가 발생합니다. Service Composer 페이지가 올바르게 로드되지 않습니다.
- **해결된 문제 2032988, 2032990, 2032991: CVE-2017-5753, CVE-2017-5715(Specter) 및 CVE-2017-5754(Meltdown)로 인한 취약점**  
CVE-2017-5753, CVE-2017-5715(Specter) 및 CVE-2017-5754(Meltdown) 취약점으로 인한 잠재적 보안 문제가 있습니다.

## 알려진 문제

알려진 문제는 다음과 같이 분류됩니다.

- [설치 및 업그레이드에 대한 알려진 문제](#)
- [일반적인 알려진 문제](#)

#### 설치 및 업그레이드에 대한 알려진 문제

- **문제 2001988: NSX 호스트 클러스터 업그레이드 동안 클러스터의 각 호스트가 업그레이드될 때 [호스트 준비] 탭의 설치 상태가 전체 클러스터에 대해 "준비되지 않음" 및 "설치 중"으로 번갈아 표시됨**  
NSX 업그레이드 동안 NSX 준비 클러스터의 "업그레이드 사용 가능"을 클릭하면 호스트 업그레이드가 트리거됩니다. DRS FULL AUTOMATIC으로 구성된 클러스터의 경우 호스트가 백그라운드에서 문제없이 업그레이드되지만 설치 상태가 "설치 중" 및 "준비되지 않음"으로 번갈아 표시됩니다.

해결 방법: 이것은 사용자 인터페이스 문제이므로 무시해도 됩니다. 호스트 클러스터 업그레이드가 진행될 때까지 기다리십시오.

#### 일반적인 알려진 문제

- **문제 2158182: DHCP 서비스와 링크-로컬 IP 공유를 갖는 HA가 동일한 vNic를 공유하여 DHCP 갱신 패킷**



## 이 제거됨

HA 주소가 링크-로컬 주소(169.x.x.x)인 경우 DR이 이 링크-로컬 주소에 대한 DHCP 갱신 유니캐스트 패킷을 제거하여 DHCP 클라이언트가 갱신되지 못할 수 있습니다.

해결 방법: HA 인터페이스로 사용되는 DHCP 서비스가 없는 vNic를 선택하거나 라우팅 가능 IP 주소를 HA 인터페이스 IP로 사용합니다(예: 192.168.x.x).

- **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 관리]에서 [장치 설정 관리]를 클릭합니다.
3. [설정] 패널에서 [네트워크]를 클릭합니다.
4. DNS 서버 옆의 [편집]을 클릭합니다.
5. 도메인 검색 필드에서 모든 공백 문자를 쉼표로 바꿉니다.
6. [확인]을 클릭하여 변경 내용을 저장합니다.

- **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 2204383: SSLVPN Linux 클라이언트가 sql cert9.db를 사용하는 Linux 버전에 대해 서버 인증서를 검증하지 못함**

내부 오류로 인해 서버 유효성 검사가 실패합니다.

해결 방법: 없음.