



# VMware NSX-T Data Center 2.3 릴리스 정보

VMware NSX-T Data Center 2.3 | 2018년 9월 18일 | 빌드 10085361

이 릴리스 정보의 추가 사항 및 업데이트 사항을 정기적으로 확인하십시오.

## 릴리스 정보에 포함된 내용

릴리스 정보에는 다음과 같은 항목이 포함됩니다.

- 새로운 기능
- 호환성 및 시스템 요구 사항
- 일반적인 동작 변경
- API 참조 정보
- 해결된 문제
- 알려진 문제

## 새로운 기능

NSX-T Data Center 2.3은 새로운 기능을 도입하여 성능을 향상시키고 사용자 경험을 개선합니다.

NSX-T Data Center 2.3은 새로운 기능을 도입하여 성능을 향상시키고 사용자 경험을 개선합니다.

### 베어메탈 호스트에 대한 NSX-T Data Center 지원 도입

베어메탈 지원에는 베어메탈 서버에서 실행되는 Linux 기반 워크로드와 하이퍼바이저 없이 베어메탈 서버에서 실행되는 컨테이너가 포함됩니다. NSX-T Data Center는 Open vSwitch를 활용하여 모든 Linux 호스트를 NSX-T Data Center 전송 노드로 사용하도록 설정합니다.

- **베어메탈 서버 지원:** RHEL 7.4, CentOS 7.4 및 Ubuntu 16.0.4 운영 체제를 실행하는 네이티브 계산 워크로드가 포함되어 있어서 사용자가 VLAN, 오버레이 지원 연결을 통해 베어메탈 계산 워크로드를 네트워크에 연결할 수 있고 V2P(가상에서 물리) 및 P2P(물리에서 물리) 통신 흐름에 마이크로 세분화 정책(상태 저장 계층 4 적용)을 적용할 수 있습니다.
- **베어메탈 Linux 컨테이너 지원:** RHEL 7.4 또는 RHEL 7.5가 적용된 베어메탈 Linux 호스트에서 RedHat OpenShift 컨테이너 플랫폼을 사용하여 Docker 컨테이너를 실행합니다.

### NSX Cloud 기능 향상

- **AWS 배포에 대한 지원:** NSX Cloud는 AWS 워크로드를 지원합니다.
- **Azure VNet의 자동 NSX 에이전트 프로비저닝**
- **온-프레미스에서 공용 클라우드로의 VPN 지원:** API를 사용하여 NSX Cloud 공용 클라우드 게이트웨이 내에 기본 제공 VPN 기능을 제공합니다. VPN 기능을 사용하여 다음 간의 IPSEC 링크를 생성할 수 있습니다.
  - 전송 중인 Amazon VPC/Azure VNet의 타사 서비스 VM 및 관리되는 컴퓨팅 Amazon VPC/Azure VNet
  - 관리되는 Amazon VPC/Azure VNet 및 온-프레미스 VPN 디바이스
- **NSX Cloud 에이전트에 대한 운영 체제 지원 확대:** NSX Cloud는 공용 클라우드에서 RHEL 7.5 운영 체제를 지원합니다.

### 보안 서비스 지원

## 라우팅 계층에 서비스 삽입 도입

- **Tier-0 및 Tier-1 라우터에 서비스 삽입 지원:** 타사 보안 솔루션을 등록하고, Tier-0이나 Tier-1 또는 둘 다에 고가용성 타사 보안 솔루션을 배포하고 리디렉션 정책을 통해 타사 보안 솔루션을 삽입하는 기능을 포함합니다.  
NSX-T Data Center에서 타사 솔루션의 최신 인증 상태에 대해서는 VMware 호환성 가이드 - 네트워크 및 보안을 참조하십시오.

## 분산 방화벽 기능 향상

- **NSX Edge 방화벽의 여러 섹션 지원:** 관리 용이성을 위해 NSX Edge 방화벽에 여러 섹션 추가
- **방화벽 규칙 적중 수 및 규칙 인기도 인덱스:** 규칙 사용량 모니터링 및 정리를 위해 사용되지 않은 규칙 신속하게 식별
- **방화벽 섹션 잠금:** 여러 보안 관리자가 방화벽에서 동시에 작업 가능
- **그룹 개체:** 다섯 개의 지정된 태그(이전에 두 개였음)가 모두 일치하는 경우 개체가 그룹에 추가되도록 지원
- **태그 길이:** 태그 길이 값은 65에서 256으로, 태그 범위는 20에서 128로 증가
- **Application Discovery:** 게스트 VM 내부에 설치된 애플리케이션 검색 및 분류(사용자별로 사용자 지정 분류도 가능함). 애플리케이션에는 실행 파일, 해시, 게시자 정보 및 설치 날짜에 대한 세부 정보가 포함됩니다.

## 네트워크 및 NSX Edge 서비스 지원

- **N-VDS의 향상된 데이터 경로 모드에 대한 오버레이 지원:** vSphere 6.7과 함께 NSX-T Data Center 2.3용 N-VDS의 향상된 데이터 경로 모드는 고성능 데이터 경로가 필요한 NFV 스타일 워크로드를 지원합니다.
- **중앙 집중식 서비스 포트에서 방화벽 서비스 및 상태 저장 NAT 지원**
- **DNS 전달자에서 모든 DNS 항목을 지우는 API 지원:** 주어진 DNS 전달자에서 단일 API 호출로 모든 DNS 캐시 항목을 지우는 기능을 제공합니다. 이 명령은 DNS 서버가 잘못된 응답을 제공하는 경우 및 DNS 서버가 수정된 후 DNS 항목 시간 초과를 기다리지 않도록 하는 데 유용합니다.
- **로드 밸런서 기능 향상**
  - **미리 정의된 암호 목록 지원:** 높은 보안 또는 성능을 위해 HTTPS VIP용으로 미리 정의된 SSL 프로파일입니다.
  - **로드 밸런서 규칙 향상:** 새 로드 밸런서 규칙, 헤더 삭제 작업, SSL 일치 조건 및 일치 조건의 변수 할당.
  - **독립형 서비스 라우터에서 로드 밸런서 지원:** 라우터 포트가 없는 서비스 라우터에 로드 밸런싱 서비스를 배포할 수 있는 기능을 제공합니다.

## 사용자 인터페이스 기능 향상

- **새로운 언어 지원:** 이제 영어, 독일어, 프랑스어, 일본어, 중국어 간체, 한국어, 중국어 번체 및 스페인어로 사용자 인터페이스가 제공됩니다.
- **향상된 탐색 및 홈 페이지:** 새로운 홈 페이지의 핵심 기능은 검색 및 시스템에 대한 개요 요약입니다.
- **향상된 검색:** 검색에는 홈 페이지에서 액세스할 수 있는 자동 완성 제안이 포함됩니다.
- **네트워크 토폴로지 시각화:** NSX Policy Manager는 그룹 간, VM 간, 프로세스 간 통신을 모니터링하는 기능을 제공합니다. 논리적 스위치, 포트, 라우터 및 NSX Edge와 같은 네트워크 개체 간의 관계를 시각화할 수 있습니다.

## 작업 및 문제 해결 지원

- **설치 및 업그레이드 기능 향상**
  - **상태 비저장 vSphere 환경에서 NSX-T Data Center:** 는 vSphere Auto Deploy 및 호스트 프로파일을 사용하는 상태 비저장 ESXi 호스트에 대한 지원을 제공하여 추가 배포 옵션을 사용하도록 설정합니다. 이 기능을 지원하려면 vSphere 6.7 U1 이상이 필요합니다.
  - **NSX Edge VM 및 베어메탈이 동일한 NSX Edge 클러스터에서 공존하도록 지원:** 이제 NSX Edge 노드 VM 및 베어메탈이 동일한 NSX Edge 클러스터에 존재할 수 있어 NSX Edge 노드에서 호스팅되는 서비스(예: 로드 밸런서)의 크기 조정이 간소화되었습니다.
  - **모듈식 NSX-T Data Center 업그레이드:** 업그레이드 조정기에서 모듈식 업그레이드가 지원됩니다. 새 릴리스 버전에서 변경된 NSX-T Data Center 구성 요소만 업그레이드할 수 있습니다. 이렇게 추가된 기능은 NSX-T Data Center 버전의 패치를 적용하는 작업의 오버헤드를 줄여줍니다.
- **모니터링 및 문제 해결**
  - **KVM 하이퍼바이저의 ERSPAN:** KVM - ERSPAN 유형 II 및 III에서 포트 미러링에 대한 지원을 포함

합니다.

- **Tier-0 논리적 라우터 업링크에서 송수신되는 Traceflow 사용:** Tier-0 논리적 라우터 업링크에서 traceflow 트래픽을 생성하고 Tier-0 논리적 라우터 업링크에서 traceflow 패킷 수신을 보고하는 기능을 제공하여 문제 해결 작업을 간소화하고 NSX Edge 노드의 노스바운드 인터페이스를 traceflow 보고에 포함시킵니다.
- **베어메탈 Edge 노드에서 DPDK 포트를 종료하기 위한 CLI 지원:** 설치 및 문제 해결 작업 중에 포트 분리를 간소화하기 위해 베어메탈 NSX Edge 노드에서 DPDK가 할당한 포트를 종료하는 기능을 제공합니다.

## OpenStack Neutron 플러그인 지원

이러한 기능은 OpenStack Upstream Queens 릴리스 이후부터 지원됩니다.

- **Neutron 플러그인이 고급 데이터 경로에서 지원하는 오버레이 논리적 스위치를 프로비저닝하는 기능:** NSX Neutron 플러그인은 이전에는 VLAN에 불과했던 오버레이에 고급 데이터 경로 모드를 활용할 수 있는 기능을 제공합니다. 이 지원을 통해 일례로 NFV 관련 워크로드에 대한 OpenStack 환경 외에도 고급 데이터 경로 성능을 활용할 수 있습니다.
- **NSX 제품과 OpenStack의 공존 지원:** NSX Neutron 플러그인은 OpenStack 구현을 위해 NSX Data Center for vSphere와 NSX-T Data Center를 동시에 관리하도록 지원합니다.
- **OpenStack에서 VPN을 서비스로 사용하는 기능:** VPN 기능 집합을 도입하는 OpenStack의 Neutron 확장에서 OpenStack VPNaaS에 대한 지원.

## NCP(NSX Container Plug-in) 지원

- **NSX-T Data Center를 설치하기 위한 중앙 홀 파이프라인**
- **로드 밸런서 SNAT IP에 대한 주석:** 로드 밸런서의 SNAT IP는 LoadBalancer 유형의 Kubernetes 서비스인 ncp/internal\_ip\_for\_policy: <SNAT IP>에 주석 처리되고 서비스의 상태인 status.loadbalancer.ingress.ip: [<SNAT IP>, <Virtual IP>]에 추가됩니다. 이 IP는 이 IP CIDR을 허용하는 네트워크 정책을 만드는 데 사용할 수 있습니다.
- **Kubernetes 네트워크 정책 향상:** Kubernetes 네트워크 정책 규칙으로 다른 네임스페이스에서 포드를 선택할 수 있는 기능을 제공합니다.
- **Kubernetes 로드 밸런서/SNAT 주석 개선**
  - NCP가 서비스에 대한 로드 밸런서를 구성하지 못하면 서비스에 ncp/error.loadbalancer가 주석으로 추가됩니다.
  - NCP가 서비스에 대한 SNAT IP를 구성하지 못하면 서비스에 ncp/error.snat가 주석으로 추가됩니다.
- **Kubernetes 수신 및 OpenShift 라우팅용 NSX-T Data Center 로드 밸런서의 세션 지속성**
- **정리 스크립트 향상**

## 호환성 및 시스템 요구 사항

호환성 및 시스템 요구 사항 정보에 대해서는 [NSX-T Data Center 설치 가이드](#)를 참조하십시오.

**상태 정보를 저장하지 않는 vSphere 환경의 NSX-T Data Center** - vSphere Auto Deploy 및 호스트 프로파일을 사용하는 상태 정보를 저장하지 않는 ESXi 호스트의 경우 vSphere 6.7 U1 이상이 필요합니다.

### NCP 호환성 요구 사항:

??	??
PAS?? NCP/NSX-T Data Center ??	2.3.0
NSX-T Data Center	2.2, 2.3
Kubernetes	1.10, 1.11
OpenShift	3.9, 3.10
Kubernetes ??? VM OS	Ubuntu 16.04, RHEL 7.4, 7.5
OpenShift ??? VM OS	RHEL 7.4, RHEL 7.5

PAS(PCF)	OpsManager 2.1.x + PAS 2.1.x(PAS 2.1.0 <a href="#">[?]?</a> ) OpsManager 2.2.0 + PAS 2.2.0
----------	---

## 일반적인 동작 변경

### Tier-1 논리적 라우터의 기본 HA 모드가 선점 모드에서 비선점 모드로 변경됨

Tier-1 논리적 라우터를 생성할 때 기본 HA가 선점 모드여서 기본 설정 NSX Edge 노드가 다시 온라인 상태가 되면 트래픽 속도가 저하되었습니다. 새로운 기본 HA는 비선점 모드여서, 새로 생성된 Tier 1 논리적 라우터에 트래픽 속도 저하가 발생하지 않습니다. 기존 Tier-1 논리적 라우터는 이 변경의 영향을 받지 않습니다.

### 전송 노드에서 NSX Controller로의 통신 변경

전송 노드에서 NSX Controller로의 통신 변경으로 인해, 이제는 NSX-T 2.2 이상에 대해 TCP 포트 1235가 열려 있어야 합니다. [NSX-T 설치 가이드](#)를 참조하십시오.

NSX-T 2.1에서 최신 버전으로 업그레이드하는 경우 모두 TCP 포트 1234 및 1235 둘 다 열려 있어야 합니다. 업그레이드가 완료되면 TCP 포트 1235가 사용됩니다.

## API 참조 정보

[NSX-T Data Center](#) 및 [NSX 정책](#)에서 더 이상 지원되지 않는 API 호출 및 속성을 참조하십시오.

최신 API 참조는 [NSX-T Data Center 제품 정보](#)에 제공됩니다.

## 해결된 문제

해결된 문제는 다음과 같이 분류됩니다.

- [일반적인 해결된 문제](#)
- [설치에 대해 해결된 문제](#)
- [NSX Manager에 대해 해결된 문제](#)
- [NSX Edge에 대해 해결된 문제](#)
- [논리적 네트워킹에 대해 해결된 문제](#)
- [보안 서비스에 대해 해결된 문제](#)
- [로드 밸런서에 대해 해결된 문제](#)
- [솔루션 상호 운용성에 대해 해결된 문제](#)
- [작동 및 모니터링 서비스에 대해 해결된 문제](#)
- [업그레이드에 대해 해결된 문제](#)
- [API에 대해 해결된 문제](#)
- [NCP\(NSX Container Plug-in\)에 대해 해결된 문제](#)

### 일반적인 해결된 문제

- **문제 1775315: 웹 브라우저에서 Postman 클라이언트가 열리면 CSRF 공격이 발생함**  
Postman, CURL 또는 다른 REST 클라이언트를 사용하여 만든 API 호출에 대해서는 XSRF-TOKEN 헤더와 값을 명시적으로 제공해야 합니다. /api/session/create(로컬 authN)에 대한 호출 또는 원격 authN을 사용하는 첫 번째 API 호출은 응답 개체에 XSRF-Token을 전달합니다. 후속 API 호출은 요청의 일부로 XSRF-TOKEN 헤더에 토큰 값을 전달합니다.
- **문제 1989412: NSX Manager에 연결할 수 없을 때 도메인을 삭제한 것이 연결이 복원된 후 반영되지 않음**  
NSX Manager에 연결할 수 없을 때 도메인을 정책에서 삭제하면, NSX Manager에 대한 연결이 복원된 후에도 삭제된 도메인에 대한 방화벽 및 규칙이 계속 존재합니다.
- **문제 2018478: 대시보드에서 위젯을 제거하려고 하면 스택 추적 오류로 인해 충돌이 발생함**

사용자 지정 대시보드 사용자 인터페이스가 변경되면(예: 여러 위젯에서 위젯 제거) 스택 추적 오류로 인해 사용자 인터페이스가 중단됩니다.

- **문제 1959647: 데이터베이스 서버 별칭을 사용하여 DSN을 생성하면 vCenter Server 설치가 실패할 수 있음**  
데이터베이스 서버 별칭 이름을 사용하여 DSN을 생성하면 외부 Microsoft SQL 데이터베이스와 함께 vCenter Server를 설치하는 데 실패합니다. 인벤토리 서비스를 설치하는 동안 다음과 같은 오류가 나타납니다. invsvc를 시작하는 중에 오류가 발생했습니다.

#### 설치에 대해 해결된 문제

- **문제 1739120: 관리부에서 Proton 서비스 또는 관리부를 다시 시작한 후 패브릭 노드 배포 상태가 멈춤**  
[패브릭] 페이지에서 호스트 자격 증명으로 새로 지원되는 호스트를 추가하면 상태가 **설치 진행 중**으로 변경됩니다. 관리부에서 Proton 서비스 또는 관리부를 다시 시작한 후에는 호스트의 배포 상태가 **설치 진행 중** 또는 **제거 진행 중**으로 무기한 표시됩니다.
- **문제 1944669: KVM에서 NSX-T Data Center 장치를 배포하려면 정확한 메모리 크기를 지정해야 함**  
ESX에 NSX-T Data Center 장치를 배포할 때 RAM 구성이 서로 다른 소형, 중형 및 대형 크기를 배포할 수 있습니다. 단, KVM에 NSX-T Data Center 장치를 배포할 때는 RAM 할당을 명시적으로 구성해야 합니다.
- **문제 1944678: NSX-T 통합 장치를 배포하려면 유효한 역할 유형이 필요함**  
NSX-T 통합 장치가 지정된 역할 없이 또는 잘못된 역할 유형으로 KVM에 배포되면 모든 역할이 사용하도록 설정되어 지원되지 않는 구성으로 배포됩니다.
- **문제 1958308: 호스트가 잠금 모드인 경우 호스트 준비 또는 전송 노드 생성이 실패함**  
호스트가 잠금 모드인 경우 호스트 준비 또는 전송 노드 생성이 실패합니다. 이 경우 다음과 같은 오류 메시지가 표시됩니다. 이 작업을 수행할 수 있는 사용 권한이 거부되었습니다.

#### NSX Manager에 대해 해결된 문제

- **문제 1954923: 관리부 업그레이드 동안 논리적 스위치에 연결된 VM의 vMotion이 실패함**  
관리부를 업그레이드하는 동안 논리적 스위치에 연결된 VM을 vMotion하려고 할 경우 vMotion이 실패합니다.
- **문제 1954927: NSX Manager 복원이 완료된 후 VC가 아닌 새로운 관리 ESX 호스트가 NSX Manager에 등록되고 해당 VM이 기존의 논리적 스위치에 연결되면 ESX 호스트의 MOB에서 VM의 MAC 주소가 비어 있음**  
NSX Manager 복원이 완료된 후 VC가 아닌 새로운 관리 ESX 호스트가 NSX Manager에 등록되고 해당 VM이 기존의 논리적 스위치에 연결되면 ESX 호스트의 MOB에서 VM의 MAC 주소가 비어 있습니다.
- **문제 1978104: NSX Manager 사용자 인터페이스의 일부 페이지를 Internet Explorer 11에서 액세스할 수 없음**  
NSX Manager 사용자 인터페이스의 대시보드, 시작 워크플로 및 로드 밸런서 페이지는 Windows 시스템에서 Internet Explorer를 사용하는 경우 액세스할 수 없습니다.
- **문제 1954986: 키가 UI에서 삭제되면 라이선스 키가 로그에 표시됨**  
NSX 라이선스 키는 /var/log/syslog에 다음과 같이 표시됩니다.  
<182>1 2017-03-24T05:03:47.008Z bb-mgr-221 NSX - SYSTEM [nsx@6876 audit="true" comp="nsx-manager" reqId="3d146f2b-fa34-460f-8ac3-56e3c7326015" subcomp="manager"] UserName:'admin', ModuleName:'License', Operation:'DeleteLicense, Operation status:'success', New value: ["<license\_key>"] <182>1 2017-03-24T05:03:47.009Z bb-mgr-221 NSX - - [nsx@6876 audit="true" comp="nsx-manager" subcomp="manager"] UserName:'admin', ModuleName:'Batch', Operation:'RegisterBatchRequest, Operation status:'success', New value: [{"atomic":false} {"request": [{"method": "DELETE", "uri": "/v1/licenses/<license\_key>"}]}]

장치가 외부 로그 수집기로 로그를 보내도록 구성되면 키 값은 외부 로그 수집기의 승인된 사용자에게도 표시됩니다.

- **문제 1956055: 관리부 데이터스토어가 다운되었을 때 로컬 관리자가 UI에서 기술 지원 번들에 액세스할 수 없음**  
관리부 데이터스토어가 다운되었을 때 로컬 관리자가 UI에서 기술 지원 번들에 액세스할 수 없음

- 문제 1957165: 10,040개 이상의 레코드가 있는 검색 결과 집합의 마지막 페이지를 로드하면 오류가 발생함  
검색 쿼리에 대해 10,040개 이상의 개체를 반환할 수 있는 대규모 환경에서, 결과 집합의 마지막 레코드 몇 개를 로드하려고 하면 오류가 표시될 수 있습니다.

## NSX Edge에 대해 해결된 문제

- 문제 1762064: NSX Edge를 재부팅한 직후에 NSX Edge VTEP IP 풀 및 업링크 프로파일을 구성하면 VTEP BFD 세션에 연결할 수 없게 됨  
NSX Edge를 재부팅한 후에 브로커에는 NSX Edge 연결을 재설정할 시간이 필요합니다.

## 논리적 네트워킹에 대해 해결된 문제

- 문제 1966641: 호스트를 추가하여 전송 노드로 구성하는 경우, 해당 노드가 논리적 스위치의 일부가 아니면 노드 상태가 [종료]로 표시됨  
새 호스트를 추가하여 전송 노드로 구성한 후 또는 NSX-T 2.1에 대한 업그레이드 계획을 구성하는 경우, 해당 노드가 논리적 스위치에 속하지 않으면 전송 노드 상태가 사용자 인터페이스에 [종료]로 표시됩니다.
- 문제 2015445: 활성 서비스 라우터의 방화벽 상태가 새로운 활성 서비스 라우터에서 복제되지 않을 수 있음  
TLR(테넌트 논리적 라우터)에 NSX Edge1에서 NSX Edge2로의 페일오버 및 NSX Edge2에서 NSX Edge1로의 페일오버가 여러 번 발생할 수 있습니다. 활성/대기 TLR 서비스 라우터 사이에 방화벽 또는 NAT 흐름 상태가 동기화됩니다. TLR이 비선점형 페일오버 모드에서 구성된 경우에는 동기화가 첫 번째 페일오버 전에 발생하지만 첫 번째 페일오버와 그 다음 페일오버 사이에는 발생하지 않습니다. 그 결과 두 번째 페일오버가 발생할 때 TCP 트래픽이 시간 초과될 수 있습니다. 선점형 모드에서 구성된 TLR에서는 이 문제가 발생하지 않습니다.
- 문제 2016629: 마이그레이션 후 RSPAN\_SRC 미러 세션이 실패함  
RSPAN\_SRC 미러 세션에 할당된 포트에 연결된 VM이 다른 하이퍼바이저로 마이그레이션되었으며 대상 하이퍼바이저의 대상 네트워크에 필수 pNic가 없는 경우 RSPAN\_SRC 미러 세션이 포트에서 구성되지 못합니다. 이 실패로 인해 포트 연결이 실패하지만 vMotion 마이그레이션 프로세스는 성공합니다.
- 문제 1620144: NSX-T Data Center CLI, get logical-switches를 실행하면 전송 노드가 삭제된 이후에도 논리적 스위치가 작동 상태로 표시됨  
CLI는 작동하는 논리적 스위치가 있다고 사용자에게 잘못 알릴 수 있습니다. 논리적 스위치가 표시되더라도 작동하지 않습니다. 전송 노드가 삭제될 때 불투명한 스위치가 사용되지 않도록 설정되므로 트래픽이 통과하지 않습니다.
- 문제 1590888: [이더넷] 섹션에서 선택한 논리적 포트가 동일한 L2 네트워크 내에서만 적용되어야 한다는 경고가 표시됨  
분산 방화벽의 경우 [이더넷] 섹션에서 [소스/대상] 섹션에 논리적 포트 또는 MAC 주소를 입력하면 MAC 주소 또는 논리적 포트가 동일한 L2 네트워크의 VM 포트(동일한 논리적 스위치에 연결)에 속해야 한다는 경고가 표시됩니다. 현재 경고 메시지는 표시되지 않습니다.
- 문제 1763576: NSX-T Data Center 네트워크에 VM이 있더라도 하이퍼바이저를 전송 노드로 제거할 수 있음  
네트워크에 속하는 VM이 노드에 있더라도 NSX-T Data Center는 전송 노드 삭제를 막지 않습니다. 전송 노드가 삭제된 후에 VM의 연결이 끊어집니다.
- 문제 1780798: 대규모 환경에서 일부 호스트가 실패 상태가 될 수 있음  
호스트 노드가 200개 이상인 대규모 환경에서 얼마 동안 실행된 후에 일부 호스트와 NSX Manager 간의 연결이 끊어지고 다음과 같은 오류 메시지가 로그에 표시됩니다.  
2016-12-09T00:57:58Z mpa: [nsx@6876 comp="nsx-esx" subcomp="mpa" level="WARN"] Unknown routing key: com.vmware.nsx.tz.\*
- 문제 1954997: 전송 노드 삭제 시 해당 전송 노드의 VM이 논리적 스위치에 연결되어 있으면 전송 노드 삭제가 실패함
  1. 패브릭 노드와 전송 노드가 생성됩니다.
  2. 논리적 스위치에 VIF를 연결합니다.
  3. 논리적 스위치에 연결된 VIF를 제거하지 않고 전송 노드를 삭제하면 실패합니다.
- 문제 1958041: ESX 하이퍼바이저에 여러 개의 업링크가 있을 때 물리적 계층 2 세그먼트에 있는 계층 3 흐름

## 에 대해 BUM 트래픽이 작동하지 않음

다음 조건이 모두 충족될 경우 논리적 라우터를 통한 소스 하이퍼바이저의 BUM 트래픽이 대상 하이퍼바이저에 도달하지 않습니다.

- ESX에 여러 개의 업링크가 있음
- 소스 및 대상 VM이 논리적 라우터를 통해 연결되어 있음
- 소스 및 대상 하이퍼바이저가 서로 다른 물리적 세그먼트에 있음
- 대상 논리적 네트워크가 MTEP 복제를 사용하고 있음

이러한 상황은 BFD 모듈이 세션을 생성하지 않아서, 즉 대상 논리적 네트워크에 대한 MTEP 선택이 발생하지 않았을 수 있기 때문에 발생합니다.

## 보안 서비스에 대해 해결된 문제

- 문제 1520694: RHEL 7.1 커널 3.10.0-229 및 이전 버전에서 FTP ALG가 데이터 채널에서 협상된 포트를 열지 못함  
FTP 세션의 경우 클라이언트 및 서버가 동일한 하이퍼바이저의 VM에 상주하는 경우 FTP ALG(애플리케이션 수준 게이트웨이)가 데이터 채널에 대해 협상된 포트를 열지 못합니다. 이 문제는 Red Hat에 국한되며 RHEL 7.1 커널 3.10.0-229에서 나타납니다. 이후 RHEL 커널은 영향을 받지 않습니다.
- 문제 2008882: Application Discovery가 제대로 작동하려면 여러 호스트에 걸쳐 보안 그룹을 생성하지 마십시오.  
하나의 보안 그룹에 여러 호스트에 걸쳐 있는 VM이 있으면 Application Discovery 세션이 실패할 수 있습니다.

## 로드 밸런서에 대해 해결된 문제

- 문제 1995228: 구성이 변경되고 다시 로드된 후 가중 라운드 로빈 및 가중 최소 연결 알고리즘이 트래픽을 제대로 분산하지 못할 수 있음  
가중 라운드 로빈 또는 가중 최소 연결 구성이 변경되고 다시 로드되면 서버 연결이 끊어질 수 있습니다. 연결이 끊어진 후에 트래픽 분산 정보가 보존되지 않아서 트래픽이 부적절하게 분산될 수 있습니다.
- 문제 2018629: 상태 점검 테이블에 NS 그룹 풀의 업데이트된 모니터 유형이 표시되지 않음  
멤버가 동일한 정적 및 동적 NS 그룹 풀을 한 가지 모니터 유형으로 생성하고 동적 풀에서 해당 모니터 유형을 변경하면 상태 점검 테이블에 동적 풀 상태 점검이 나타나지 않습니다.
- 문제 2020372: 최대 장애 횟수에 도달한 이후에도 수동 상태 점검이 풀 멤버가 다운된 것으로 간주하지 않음  
수동 상태 점검이 풀 멤버가 다운된 것으로 간주하려면 장애 횟수 값이 구성되어 있는 값보다 커야 합니다.

## 솔루션 상호 운용성에 대해 해결된 문제

- 문제: 2025624: Splunk 대시보드가 로드 중 멈추거나 대시보드의 그래프가 비어 있음  
HTML 템플릿이 쿼리 스크립트의 이전 경로를 잘못 가리키기 때문에 Splunk가 *nsx\_splunk\_app*의 이전 버전을 가져옵니다. 따라서 대시보드에서는 *vmw\_nsxt\_comp*, *vmw\_nsxt\_subcomp* 및 *vmw\_nsxt\_errorcode* 같은 필드가 포함된 이전 쿼리를 실행하지만, 새 버전의 쿼리 스크립트에서는 이러한 필드의 이름이 달라졌습니다. 그 결과, 쿼리가 빈 결과를 반환하고 대시보드에 아무것도 표시되지 않습니다.

## 작동 및 모니터링 서비스에 대해 해결된 문제

- 문제 1957092: Docker 이미지 로드 중 오류가 발생하여 NSX Controller 클러스터를 초기화하지 못함  
initialize control-cluster 명령이 오류 메시지 Control cluster activation timed out. Please try again.을 표시하며 실패합니다. 을 표시하며 실패합니다. 또한 syslog에 다음과 같은 로그 정보가 있습니다.  
<30>1 2017-08-03T22:52:41.258925+00:00 localhost load-zookeeper-image 1183 - - grpc: the connection is unavailable.

## 업그레이드에 대해 해결된 문제

- 문제 1847884: 관리부에 대한 업그레이드 프로세스가 완료될 때까지 NSX-T Data Center 관련 사항을 변경하지 마십시오.  
관리부를 업그레이드하는 동안 전송 영역, 전송 노드 또는 논리적 스위치를 생성, 업데이트 또는 삭제하는 등의 변경 작업을 수행하면 관리부가 손상되어 NSX Edge, 호스트 및 데이터 경로 연결 오류가 발생할 수 있습니다.



- **문제 2005709: NSX Manager FQDN을 사용하면 업그레이드 코디네이터 페이지에 액세스할 수 없음**  
NSX Manager FQDN을 사용하여 NSX Manager 사용자 인터페이스를 열면 업그레이드 코디네이터 페이지에 다음 오류 메시지가 표시됩니다. 이 페이지는 업그레이드 코디네이터가 실행되고 있는 NSX Manager에서만 사용할 수 있습니다. 서비스를 사용하려면 NSX Manager에서 "set service install-upgrade enabled" 명령을 실행하십시오. install-upgrade 서비스가 사용되도록 이미 설정되어 있으면 "clear service install-upgrade enabled" 명령을 사용하여 이 서비스를 사용하지 않도록 설정한 후 다시 사용하도록 설정합니다.
- **문제 2022609: 업그레이드 코디네이터에서 관리 호스트가 관리되지 않는 호스트로 처리됨**  
환경에 관리 호스트가 128개보다 많은 경우, 클러스터에 포함되어 있던 호스트는 업그레이드 프로세스 동안 관리되지 않는 ESXi 그룹에 표시됩니다.
- **문제 1944731: 두 번째 NSX Edge를 업그레이드하는 동안 첫 번째로 업그레이드된 NSX Edge에서 많은 요청을 처리할 경우 DHCP 리스에 충돌 레코드가 있을 수 있음**  
두 번째 NSX Edge를 업그레이드하는 동안 첫 번째로 업그레이드된 NSX Edge에서 많은 요청을 처리하면 DHCP 리스에 충돌 레코드가 있을 수 있습니다.

## API에 대해 해결된 문제

- **문제 1619450: 빈도 구성 API GET /api/v1/hpm/features를 폴링하여 수직 테스트가 반환됨**  
GET /api/v1/hpm/features는 폴링 빈도가 구성될 수 있는 모든 기능 목록을 반환합니다. 이 API는 일부 내부 테스트 전용 기능을 반환합니다. 추가적인 노이즈 외에 사용자에게 미치는 기능적 영향은 없습니다.
- **문제 1781225: API GET https://<NSX Manager>/api/v1/fabric/nodes/<노드 ID>/modules가 Ubuntu에서 작동하지 않음**  
API GET https://<NSX Manager>/api/v1/fabric/nodes/<노드 ID>/modules는 ESXi 및 RHEL에서는 작동하지만 Ubuntu에서는 작동하지 않습니다.
- **문제 1954990: 인식 API의 부정확한 상태 반환**  
인식 API를 사용하여 장애 요인 이전에 실행된 모든 API의 인식 상태를 확인하면 인식 API별 반환 상태가 실제 상태와 다르게 나타날 수 있습니다. 관리부 내부의 DFW 실행이 복잡하기 때문에 예정된 장벽 후에 따라올 DFW API가 우회되어 부정확성을 초래할 수 있습니다.

## NCP(NSX Container Plug-in)에 대해 해결된 문제

- **문제 2167491: NSX-T 로드 밸런서에 최대 개수의 가상 서버가 있는 경우 NCP가 시작되지 않음**  
NCP의 ConfigMap에서 NSX-T 로드 밸런서의 크기를 소형, 중형 또는 대형으로 설정할 수 있습니다. 소형 로드 밸런서의 경우 가상 서버의 최대 수는 10이고, 중형의 경우 100, 대형의 경우 1000입니다. 로드 밸런서에 최대 개수의 가상 서버가 있으면 NCP가 시작되지 않습니다. 로드 밸런서에 최대 개수의 가상 서버가 있는지 확인하려면, NSX-T Manager GUI에서 로드 밸런서(클러스터 이름으로 태그가 있음)를 찾고 가상 서버의 수를 계산합니다.
- **문제 2160806: NCP가 실행 중이 아닐 때 활성 수신의 TLS 규격 업데이트가 지원되지 않음**  
NCP에서 수신 리소스에 외부 IP를 할당한 경우 NCP가 실행되고 있지 않을 때 수신의 TLS 규격을 업데이트(예: 매개 변수 secretName 제거 또는 변경)하면 NCP에서 해당 변경을 인식하지 못합니다. NCP가 다시 실행되면 이전 암호에 해당하는 인증서가 계속 존재하고 삭제되지 않습니다.

## 알려진 문제

알려진 문제는 다음과 같이 분류됩니다.

- 일반적인 알려진 문제
- 설치에 대한 알려진 문제
- NSX Manager에 대한 알려진 문제
- NSX Edge에 대한 알려진 문제
- 논리적 네트워킹에 대한 알려진 문제
- 보안 서비스에 대한 알려진 문제
- KVM 네트워킹에 대한 알려진 문제
- 로드 밸런서에 대한 알려진 문제



- 솔루션 상호 운용성에 대한 알려진 문제
- 작동 및 모니터링 서비스에 대한 알려진 문제
- 업그레이드에 대한 알려진 문제
- API에 대한 알려진 문제
- NSX Policy Manager에 대한 알려진 문제
- NSX Cloud에 대한 알려진 문제
- NCP(NSX Container Plug-in)에 대한 알려진 문제
- 설명서 오류 및 추가 내용

## 일반적인 알려진 문제

- 문제 1842511: 다중 홉-BFD가 정적 경로에 대해 지원되지 않음

NSX-T 2.0에서는 MH-BGP(multihop BGP) 인접 네트워크에 대해 BFD(Bi-Directional Forwarding Detection)를 사용하도록 설정할 수 있습니다. BFD를 사용하여 다중 홉 정적 경로를 지원하는 기능은 NSX-T 2.0에서 구성할 수 없으며 BGP에서만 구성할 수 있습니다. BFD 지원 다중 홉 BGP 인접 네트워크를 구성한 후 BGP 인접 네트워크와 동일한 다중 홉을 사용하여 해당 다중 홉 정적 경로를 구성한 경우 BFD 세션 상태는 BGP 세션과 정적 경로 둘 다에 영향을 줍니다.

해결 방법: 없음.

- 문제 1931707: 자동 TN 기능을 사용하려면 클러스터의 모든 호스트에 동일한 pnics 설정이 필요함

클러스터에 대해 자동 TN 기능을 사용하도록 설정하면 이 클러스터의 모든 호스트에 적용되는 전송 노드 템플릿이 생성됩니다. 템플릿의 모든 pnics는 TN 구성을 위해 모든 호스트에서 사용 가능해야 하며 그렇지 않으면 pnics가 없거나 사용된 호스트에서 TN 구성이 실패할 수 있습니다.

해결 방법: TN 구성이 실패한 경우 개별 전송 노드를 다시 구성하여 수정하십시오.

- 문제 1909703: NSX 관리자는 OpenStack에 의해 백엔드에서 직접 생성된 라우터에 새로운 정적 경로, NAT 규칙 및 포트를 생성할 수 있음

NSX-T 2.0의 RBAC 기능의 일부로, OpenStack 플러그인에서 생성된 스위치, 라우터, Security Group과 같은 리소스는 NSX UI/API에서 NSX 관리자가 직접 삭제하거나 수정할 수 없습니다. 이러한 리소스는 OpenStack 플러그인을 통해 전송된 API를 통해서만 수정/삭제할 수 있습니다. 이 기능에는 한 가지 제한이 있습니다. 현재 NSX 관리자는 OpenStack에서 생성된 기존 리소스 내에 정적 경로, NAT 규칙과 같은 새로운 리소스를 생성할 수 있지만 OpenStack에서 생성된 리소스를 삭제/수정할 수는 없습니다.

해결 방법: 없음.

- 문제 1957072: 브리지 노드에 대한 업링크 프로파일이 둘 이상의 업링크에 대해 항상 LAG를 사용해야 함  
LAG로 구성되지 않은 여러 개의 업링크를 사용하는 경우 트래픽이 로드 밸런싱되지 않으며 잘 작동하지 않습니다.

해결 방법: 브리지 노드의 여러 업링크에 대해 LAG를 사용하십시오.

- 문제 1970750: 빠른 타이머로 LACP를 사용하는 전송 노드 N-VDS 프로필이 vSphere ESXi 호스트에 적용되지 않음

빠른 속도의 LACP 업링크 프로파일이 구성되어 NSX Manager의 vSphere ESXi 전송 노드에 적용되면, NSX Manager에 프로필이 성공적으로 적용된 것으로 표시되지만 vSphere ESXi 호스트는 기본 LACP 느린 타이머를 사용합니다.

vSphere Hypervisor에서 LACP NSX 관리 분산 스위치(N-VDS) 프로파일이 NSX Manager의 전송 노드에 사용되는 경우 lacp-timeout 값(SLOW/FAST)의 효과가 나타나지 않습니다.

해결 방법: 없음.

- 문제 1989407: 엔터프라이즈 관리자 역할이 있는 vIDM 사용자가 개체 보호를 재정의할 수 없음

엔터프라이즈 관리자 역할이 있는 vIDM 사용자가 개체 보호를 재정의할 수 없고 주체 ID를 생성하거나 삭제할 수 없습니다.

해결 방법: 관리자 권한으로 로그인합니다.

- **문제 2030784: 비 ASCII 문자가 포함된 원격 사용자 이름으로 NSX Manager에 로그인할 수 없음**  
비 ASCII 문자가 포함된 사용자 이름을 사용하여 원격 사용자로 NSX Manager 장치에 로그인할 수 없습니다.  
해결 방법: NSX Manager 장치에 로그인할 때 원격 사용자 이름에 ASCII 문자가 있어야 합니다.  
Active Directory 서버에서 원격 사용자 이름이 비 ASCII 문자로 설정된 경우에는 비 ASCII 문자를 사용할 수 있습니다.
- **문제 2111047: NSX-T 2.2 릴리스의 VMware vSphere 6.7 호스트에서 Application Discovery가 지원되지 않음**  
vSphere 6.7 호스트에서 실행 중인 VM이 있는 보안 그룹에서 Application Discovery를 실행하면 검색 세션이 실패합니다.  
해결 방법: 없음
- **문제 2157370: 잘림으로 L3 SPAN(Switched Port Analyzer)을 구성할 때 특정한 물리적 스위치가 미러링된 패킷을 삭제함**  
잘림으로 GRE/ERSPAN을 포함하는 L3 SPAN을 구성할 때 물리적 스위치 정책으로 인해 미러링된 잘린 패킷이 삭제됩니다. 가능한 원인은 포트가 수신한 패킷에서 페이로드의 바이트 수가 유형 길이 필드와 같지 않기 때문일 수 있습니다.  
해결 방법: L3 SPAN 잘림 구성을 제거합니다.
- **문제 216992: 다른 호스트의 대상 MAC 주소가 02:50:56:56:44:52인 미러링된 패킷이 vSphere ESXi 업링크에 의해 삭제됨**  
다른 호스트의 대상 MAC 주소가 02:50:56:56:44:52인 미러링된 패킷을 호스트가 수신하면 미러링된 패킷이 vSphere ESXi 업링크에 의해 삭제됩니다.  
해결 방법: 없음
- **문제 2174583: 시작 마법사의 [전송 노드 설정] 버튼이 Microsoft Edge 브라우저에서 제대로 작동하지 않음**  
시작 마법사에서 전송 노드 설정 버튼을 클릭한 후 Microsoft Edge 웹 브라우저가 JavaScript 오류를 나타내며 실패합니다.  
해결 방법: 대신 Firefox나 Google Chrome 브라우저를 사용하십시오.

## 설치에 대한 알려진 문제

- **문제 1617459: Ubuntu에 대한 호스트 구성이 인터페이스 구성 파일의 소싱을 지원하지 않음**  
pnk 인터페이스가 /etc/network/interfaces 파일에 있지 않으면 MTU가 네트워크 구성 파일에서 제대로 구성되지 않습니다. 이로 인해 전송 브리지의 MTU 구성이 재부팅할 때마다 손실됩니다.  
해결 방법: PNIC 인터페이스 구성을 /etc/network/interfaces로 이동하십시오.
- **문제 1906410: 먼저 전송 노드를 삭제하지 않고 UI에서 호스트를 삭제하려고 하면 호스트가 일관성 없는 상태가 됨**  
먼저 전송 노드를 삭제하지 않고 UI에서 호스트를 삭제하려고 하면 호스트가 일관성 없는 상태가 됩니다. 호스트가 일관성 없는 상태일 때 전송 노드를 삭제하려고 하면 UI로 호스트를 삭제할 수 없습니다.  
해결 방법:
  1. 전송 노드를 삭제하기 전에 이 전송 노드에 배포된 모든 테넌트 VM의 전원을 끄십시오.
  2. 전송 노드에서 전송 영역을 제거하십시오.
  3. 전송 노드를 삭제하십시오.
  4. 전송 노드가 삭제되면 해당 호스트를 삭제하십시오.
 전송 노드 삭제가 실패하는 경우 KB <https://kb.vmware.com/s/article/52068>의 단계를 완료하십시오.
- **문제 1957059: 준비를 취소하려고 할 때 기존 vib가 있는 호스트를 클러스터에 추가할 경우 호스트 준비 취소가 실패함**  
호스트를 클러스터에 추가하기 전에 vib를 완전히 제거하지 않으면 호스트 준비 취소 작업이 실패합니다.  
해결 방법: 호스트의 vib를 완전히 제거한 후에 호스트를 다시 시작해야 합니다.

- **문제 2106956: 동일한 클러스터의 두 NSX Controller를 두 개의 서로 다른 NSX Manager에 연결하면 정의되지 않은 데이터 경로 문제가 발생함**

동일한 NSX Controller 클러스터의 NSX Controller 두 개를 두 개의 서로 다른 NSX Manager에 연결하면 정의되지 않은 데이터 경로 문제가 발생합니다.

해결 방법: NSX Manager에서 detach CLI 명령을 사용하여 NSX Controller 클러스터에서 NSX Controller를 제거합니다. 클러스터의 모든 NSX Controller가 동일한 NSX Manager에 등록되도록 NSX Controller 클러스터를 재구성합니다.

NSX-TData Center설치 가이드.

- **문제 2106973: 모든 NSX Controller에서 NSX Controller 클러스터를 초기화하면 각 NSX Controller가 단일 노드 NSX Controller 클러스터가 되어 정의되지 않은 데이터 경로 연결 문제가 발생함**  
모든 NSX Controller에서 NSX Controller 클러스터를 초기화하지 마십시오. 그러면 각 NSX Controller가 단일 노드 NSX Controller 클러스터가 되어 정의되지 않은 데이터 경로 연결 문제가 발생합니다. 첫 번째 NSX Controller에서만 NSX Controller 클러스터를 초기화하고 첫 번째 NSX Controller에서 join control-cluster CLI 명령을 실행하여 다른 NSX Controller를 클러스터에 연결합니다.

해결 방법: NSX-TData Center설치 가이드.

- **문제 2114756: NSX-T Data Center 준비된 클러스터에서 호스트를 제거할 때 VIB가 제거되지 않는 경우가 있음**

NSX-TData Center준비된 클러스터에서 호스트가 제거되는 경우 일부 VIB가 호스트에 남아있을 수 있습니다.

해결 방법: VIB를 호스트에서 수동으로 제거합니다.

- **문제 2059414: python-gevent RPM의 버전이 오래되어 RHEL LCP 번들 설치가 실패함**  
RHEL 호스트에 python-gevent RPM의 새 버전이 포함되어 있으면 NSX-T Data Center RPM에 이전 버전의 python-gevent RPM이 포함되어 있으므로 RHEL LCP 번들 설치가 실패합니다.

해결 방법: 호스트에 최신 버전의 python-gevent RPM이 포함되어 있는 경우 RHEL 호스트에 LCP 번들을 수동으로 설치합니다.

다음 단계를 완료하십시오.

1. RHEL LCP 번들을 추출합니다.
  2. LCP 번들 폴더로 이동합니다.
  3. LCP 폴더에서 libev, python-greenlet 및 python-gevent RPM을 삭제합니다.
  4. 나머지 RPM을 설치합니다. NSX-T Data Center 설치 가이드를 참조하십시오.
- **문제 2142755: 어떤 RHEL 7.4 부 커널 버전을 실행하느냐에 따라 OVS 커널 모듈 설치가 실패함**  
17.1 이상의 부 커널 버전을 실행하는 RHEL 7.4 호스트에 OVS 커널 모듈을 설치하지 못합니다. 설치 실패로 인해 커널 데이터 경로가 작동을 중단하고 이로 인해 장치 관리 콘솔을 사용할 수 없게 됩니다.

해결 방법: RHEL 7.4 커널 버전을 업그레이드합니다. 관리자 권한으로 호스트에서 /usr/share/openvswitch/scripts/ovs-kmod-manage.sh 스크립트를 실행하고 OVS 커널 모듈을 다시 로드합니다.

## NSX Manager에 대한 알려진 문제

- **문제 1950583: NSX-T 2.0.0으로의 시스템 업그레이드 후 NSX Manager 예약 백업이 실패할 수 있음**  
일부 NSX-T 환경에서는 이전 버전의 NSX-T를 2.0.0으로 업그레이드한 후 예약된 백업을 실행하지 못합니다. 이 문제는 이전 릴리스의 SSH 지문 형식이 변경되기 때문에 발생합니다.

해결 방법: 예약된 백업을 다시 구성하십시오.

- **문제 1576112: KVM 하이퍼바이저가 다른 계층 2 세그먼트에 상주할 경우 게이트웨이를 수동으로 구성해야 함**

NSX Manager에서 IP 풀을 구성하고 전송 노드 생성에 해당 IP 풀을 사용할 경우 Ubuntu KVM 상자에 IP 풀 구성에 구성된 게이트웨이에 대한 경로가 표시되지 않습니다. 기본 패브릭 호스트는 원격 세그먼트의 패브릭 노드에 연결하는 방법을 알지 못하므로 다른 L2 세그먼트에 있는 하이퍼바이저에 상주하는 VM 간의 오버레이 트래픽이 실패합니다.

해결 방법: 다른 세그먼트에 상주하는 다른 하이퍼바이저로 트래픽을 라우팅할 수 있도록 게이트웨이에 대한 경로를 추가하십시오. 이 구성을 수동으로 수행하지 않으면 패브릭 노드가 원격 패브릭 노드에 연결하는 방법을 알지 못하므로 오버레이 트래픽이 실패합니다.

- **문제 1710152: NSX Manager GUI가 호환성 모드의 Internet Explorer 11에서 작동하지 않음**

해결 방법: 도구 > 호환성 보기 설정으로 이동한 후 Internet Explorer에 호환성 모드의 NSX Manager GUI가 표시되지 않는지 확인하십시오.

- **문제 2128476: 호스트 500개, VM 1000개 및 VIF 10000개가 넘는 인벤토리를 포함하는 대규모 설정의 경우 하드 재부팅 후 전체 동기화에 약 30분이 걸릴 수 있음**

NSX Manager가 재부팅된 후에는 각 호스트가 NSX Manager와 동기화되어 호스트의 최신 데이터를 NSX Manager가 수신합니다. 여기에는 호스트에 있는 VM 및 VM에 있는 VIF에 대한 정보가 포함됩니다. 호스트 500개, VM 1000개 및 VIF 10000개가 넘는 인벤토리를 포함하는 대규모 설정의 경우 전체 동기화에 약 30분이 소요됩니다.

해결 방법: 하드 재부팅 후 NSX Manager에 최신 정보가 표시될 때까지 기다리십시오.

API `api/v1/fabric/nodes/<nodeid>/status`를 사용하여 특정 노드에 대한 최신 동기화 시간을 나타내는 `last_sync_time` 속성을 확인합니다.

- **문제 1928376: NSX Manager를 복원한 후 컨트롤러 클러스터 멤버 노드가 저하된 상태가 됨**

컨트롤러 클러스터 멤버 노드가 클러스터에서 분리되기 전에 생성한 백업 이미지로 NSX Manager가 복원될 경우 이 멤버 노드가 불안정해지고 저하된 상태를 보고할 수 있습니다.

해결 방법: 클러스터 멤버 자격이 변경되면 새 NSX Manager 백업이 생성되는지 확인하십시오.

- **문제 1956088: 보기의 규칙 집합에 필터링이 적용되는 동안 방화벽 UI에 대해 변경한 내용은 해당 필터가 취소되면 Manager에 저장하기 전에 손실될 수 있습니다.**

보기의 규칙 집합에 필터링이 적용되는 동안 방화벽 UI에 대해 변경한 내용은 해당 필터가 취소되면 Manager에 저장하기 전에 손실될 수 있습니다.

해결 방법: 없음.

- **문제 1928447: 중복 가상 터널 끝점 IP 주소가 있는 하이퍼바이저가 관리부 노드 syslog에 로깅되지 않음**  
중복 가상 터널 끝점 IP 주소가 있는 하이퍼바이저가 관리부 노드 syslog에 로깅되지 않습니다. 하이퍼바이저의 가상 터널 끝점 및 NSX Edge 노드의 업링크 인터페이스에 고유한 IP 주소가 할당되어 있는지 확인합니다.

해결 방법: 없음.

- **문제 2125725: 대규모 토폴로지 배포를 복원한 후 검색 데이터가 동기화되지 않고 다수의 NSX Manager 페이지가 응답하지 않음**

대규모 토폴로지 배포를 통해 NSX Manager를 복원한 후 검색 데이터가 동기화되지 않고 다수의 NSX Manager 페이지에 복구할 수 없는 오류가 발생했습니다.라는 오류 메시지가 표시됩니다.

해결 방법: 다음 단계를 완료하십시오.

1. NSX Manager CLI에 관리자로 로그인합니다.
2. 검색 서비스를 다시 시작합니다.

`restart service search`

검색 서비스가 백그라운드에서 데이터 불일치 수정을 마칠 때까지 15분 이상 기다립니다.

- **문제 2128361: NSX Manager의 로그 수준을 디버그 모드로 설정하는 CLI 명령이 제대로 작동하지 않음**

CLI 명령 `set service manager logging-level debug`를 사용하여 NSX Manager의 로그 수준을 디버그 모드로 설정해도 디버깅 로그 정보가 수집되지 않습니다.

해결 방법: 다음 단계를 완료하십시오.

1. NSX Manager CLI에 관리자로 로그인합니다.
  2. `st e` 명령을 실행하여 루트 사용자로 전환합니다.
  3. `log4j2.xml.default` 및 `log4j2.xml` 파일을 복사합니다.  
`cp /opt/vmware/proton-tomcat/conf/log4j2.xml.default /opt/vmware/proton-tomcat/conf/log4j2.xml`
  4. `log4j2.xml` 파일의 소유권을 변경합니다.  
`chown uproton:uproton /opt/vmware/proton-tomcat/conf/log4j2.xml`
- **문제 1964681: 호스트가 삭제된 후에도 Manager UI의 [호스트] 탭에 전송 노드 호스트의 상태가 [삭제 진행 중]으로 표시됨**  
Manager UI의 [패브릭] > [노드] > [전송 노드] 탭에서 전송 노드 호스트를 삭제한 후에도 [호스트] 탭에 호스트의 상태가 [삭제 진행 중]으로 표시됩니다.

해결 방법: 브라우저를 새로 고칩니다.

- **문제 2169998: Chrome 브라우저를 사용하면 NSX Manager에 로그인할 때 탐색 데이터를 지우면 Manager UI가 작동을 중단함**  
Chrome 브라우저를 사용하여 NSX Manager에 로그인한 후 브라우저 설정으로 이동하여 탐색 데이터(기본 및 고급 모두 포함)를 모두 지우면 브라우저의 NSX Manager에 대한 연결이 끊어집니다.

해결 방법: NSX Manager에 로그인할 때 탐색 데이터를 지우지 않습니다.

## NSX Edge에 대한 알려진 문제

- **문제 1765087: NSX Edge가 데이터 경로에서 Linux 커널로 패킷을 전송하기 위해 생성하는 커널 인터페이스가 최대 1600까지만 MTU 지원**  
데이터 경로와 커널 사이의 커널 인터페이스는 점보 프레임을 지원하지 않습니다. 1600을 초과하는 BGP 패킷 크기는 BGP 데몬에 의해 잘리고 삭제됩니다. 1600을 초과하는 SPAN 패킷 크기는 잘리고 패킷 캡처 유틸리티에 경고가 표시됩니다. 페이로드가 잘리고 유효한 상태를 유지합니다.
- 해결 방법: 없음.
- **문제 1738960: DHCP 서버 프로파일 NSX Edge 노드가 다른 클러스터의 NSX Edge 노드로 바뀌면 DHCP 서버에 의해 VM에 제공된 IP 주소가 변경됨**  
이 문제는 바뀐 노드와 새 노드 간에 조정 작업이 제대로 진행되지 않으면 발생합니다.
- 해결 방법: 없음.
- **문제 1629542: 단일 NSX Edge 노드에서 전달 지연을 설정하면 잘못된 라우팅 상태가 표시됨**  
NSX Edge를 단일 NSX Edge 노드(HA 쌍에 없음)로 실행할 경우 전달 지연을 구성하면 라우팅 상태가 잘못 보고될 수 있습니다. 전달 지연이 구성되면 전달 타이머가 만료될 때까지 라우팅 상태가 **다운**으로 잘못 표시됩니다. 라우터 수렴이 완료되지만 전달 지연 타이머가 아직 만료되지 않은 경우 라우팅 상태는 **다운**으로 보고되더라도 남-북으로의 데이터 경로는 계속 예상대로 진행됩니다. 이 경고는 무시해도 안전합니다.
  - **문제 1601425: NSX Manager 클러스터에 이미 등록된 NSX Edge VM을 복제할 수 없음**  
NSX Manager 클러스터에 이미 등록된 NSX Edge VM을 복제하는 것은 지원되지 않습니다. 대신 새로운 이미지를 배포해야 합니다.

해결 방법: 없음.

- **문제 1585575: Tier-0 라우터에 연결된 Tier-1 라우터에서 NSX Edge 클러스터 세부 정보를 편집할 수 없음**  
Tier-1 논리적 라우터에서 NAT를 사용하도록 설정한 경우 Tier-1 라우터를 Tier-0 라우터에 연결하기 전에 NSX Edge 노드 또는 NSX Edge 클러스터를 지정해야 합니다. NSX는 Tier-0 라우터에 이미 연결된 Tier-1 라우터에서 NSX Edge 클러스터 세부 정보를 편집하는 것을 지원하지 않습니다.

해결 방법: Tier-0 라우터에 이미 연결된 Tier-1 라우터에서 NSX Edge 클러스터 세부 정보를 편집하려면 Tier-0 라우터에서 Tier-1 라우터의 연결을 끊고 변경을 수행한 후 다시 연결하십시오.

- **문제 1955830: NSX Edge 클러스터 이름에 상위 ASCII 또는 ASCII가 아닌 문자가 포함된 경우 NSX-T 1.1에서 NSX-T 2.0으로의 업그레이드가 실패함**  
NSX-T 1.1 설치에서 상위 ASCII 또는 ASCII가 아닌 문자를 사용하여 NSX Edge 클러스터 이름을 지정할 경우 NSX-T 1.1에서 NSX-T 2.0으로의 업그레이드가 무한 루프 오류를 나타내며 실패합니다.

해결 방법: 업그레이드하기 전에 NSX-T 1.1 설치 인스턴스에서 상위 ASCII 또는 ASCII가 아닌 문자를 제거하여 NSX Edge 클러스터를 이름을 바꾸십시오.

- **문제 2122332: 경우에 따라 베어메탈 Edge에 SSH 로그인이 작동하지 않음**  
가끔, 베어메탈 Edge에 SSH 로그인이 작동하지 않습니다.

해결 방법: 명령 프롬프트를 열고 iLO 드라이버로 이동합니다. Edge SSH 서비스를 다시 시작합니다.

- **문제 2187888: NSX Manager 사용자 인터페이스에서 자동으로 배포된 NSX Edge가 무기한 [등록 보류 중] 상태로 표시됨**  
NSX Manager 사용자 인터페이스에서 자동으로 배포된 NSX Edge가 무기한 [등록 보류 중] 상태로 표시됩니다. 이 상태에서는 NSX Edge를 더 이상 구성할 수 없게 됩니다.

해결 방법: CLI를 사용하여 NSX Manager에 NSX Edge를 수동으로 등록합니다.

## 논리적 네트워킹에 대한 알려진 문제

- **문제 1769922: NSX Controller 클러스터부에 실제 IP 주소가 아니라 vSphere Client의 내부 IP 주소 172.17.0.1이 표시될 수 있음**  
vSphere Client에서 NSX Controller의 IP 주소가 실제 IP 주소가 아닌 172.17.0.1로 잘못 표시됩니다. NSX Manager의 경우에는 IP 주소가 올바르게 표시됩니다.

해결 방법: 별도의 조치는 필요 없습니다. 이 표면적인 문제는 기능에 영향을 주지 않습니다.

- **문제 1771626: NSX Controller 노드의 IP 주소를 변경할 수 없음**

해결 방법: NSX Controller 클러스터를 다시 배포하십시오.

- **문제 1940046: 여러 Tier-1 논리적 라우터에 동일한 정적 경로가 추가되고 보급되면 동-서 트래픽이 실패함**  
여러 Tier-1 논리적 라우터에 동일한 정적 경로가 추가되고 보급되면 동-서 트래픽이 실패합니다.

해결 방법: 접두사가 Tier-1 분산 라우터의 연결된 네트워크 뒤에 있는 경우 정적 경로는 원래 Tier-1 논리적 라우터에서만 보급되어야 합니다.

- **문제 1753468: 브리징된 VLAN에서 STP(Spanning Tree Protocol)를 사용하도록 설정하면 브리지 클러스터 상태가 다운으로 표시됨**  
STP가 LACP 팀 구성이 적용된 브리징에 사용되는 VLAN에서 사용되도록 설정되면 물리적 스위치 포트-채널이 차단되어 ESX 호스트의 브리지 클러스터가 다운 상태로 표시됩니다.

해결 방법: STP를 사용하지 않도록 설정하거나 BPDU 필터 및 BPDU 보호를 사용하도록 설정하십시오.



- 문제 1753468: Tier-0 논리적 라우터가 경로를 집계하지 않고, 논리적 라우터가 개별적으로 경로를 재배포함  
Tier-0 논리적 라우터가 연결된 모든 하위 접두사를 포함하지 않는 접두사에 대한 경로 집계를 수행하지 않고, 대신 논리적 라우터가 경로를 별도로 배포합니다.

해결 방법: 없음.

- 문제 1536251: ESX 호스트에서 동일한 논리적 스위치에 연결된 다른 ESX 호스트로 VM을 복사하는 것은 지원되지 않음  
VM이 한 ESX 호스트에서 복사되고 동일한 VM이 다른 ESX 호스트에 등록될 경우 계층 2 네트워크가 실패합니다.

해결 방법: ESX 호스트가 Virtual Center에 속할 경우 VM 복제를 사용하십시오.

ESX 호스트 간에 VM을 복사하는 경우 계층 2 네트워크가 작동하려면 외부 ID가 VM .vmx 파일에서 고유해야 합니다.

- 문제 1747485: LAG 인터페이스에서 업링크를 제거할 경우 모든 BFD 프로토콜이 다운되고 BGP 경로가 불안정해짐  
구성된 LAG 인터페이스에서 인터페이스가 삭제될 경우 모든 BFD 프로토콜이 다운되고 BGP 경로가 불안정해져서 트래픽 흐름에 영향을 미칩니다.

해결 방법: 없음.

- 문제 1741929: KVM 환경에서 포트 미러링을 구성하고 잘림을 사용하도록 설정할 경우 소스에서의 점포 패킷이 분할된 상태로 전송되었다가 미리 대상에서 다시 조합됨

해결 방법: 대상 VM vNIC 드라이버에 의해 재조합이 수행되므로 해결 방법은 필요하지 않습니다.

- 문제 1619838: 논리적 라우터의 전송 영역 연결을 다른 논리적 스위치 집합으로 변경하려고 하면 불일치 오류로 인해 실패함  
논리적 라우터는 다운링크 포트에 대해 단일 오버레이 전송 영역만 지원합니다. 따라서 기존 다운링크 또는 라우터링 포트는 삭제하지 않으면 전송 영역 연결을 다른 논리적 스위치 집합으로 변경할 수 없습니다.

해결 방법: 다음 단계를 완료하십시오.

1. 기존의 모든 다운링크 또는 라우터링 포트를 삭제합니다.
2. 시스템이 업데이트될 때까지 잠시 기다립니다.
3. 전송 영역 연결을 다른 논리적 스위치 집합으로 변경해 봅니다.

- 문제 1625360: 논리적 스위치를 생성한 후에 NSX Controller에 새로 생성된 논리적 스위치 정보가 표시되지 않을 수 있음

해결 방법: 논리적 스위치를 생성한 후에 NSX Controller에서 논리적 스위치 정보가 확인될 때까지 60초 동안 기다리십시오.

- 문제 1581649: 논리적 스위치 생성 및 삭제 후에 VNI 풀 범위를 축소할 수 없음  
논리적 스위치가 삭제된 직후에 VNI가 해제되지 않으므로 범위 축소가 실패합니다. 6시간 후에 VNI가 해제됩니다. 이로 인해 다른 논리적 스위치가 생성될 때 VNI가 재사용되지 않게 됩니다. 따라서 논리적 스위치 삭제 후 6시간이 경과할 때까지 범위를 축소하거나 수정할 수 없습니다.

해결 방법: 논리적 스위치에 대해 VNI가 할당된 범위를 수정하려면 논리적 스위치 삭제 후 6시간 동안 기다리십시오. 또는 VNI 풀의 다른 범위를 사용하거나 범위를 축소 또는 삭제하지 말고 같은 범위를 재사용하십시오.

- 문제 1516253: Intel 82599 NIC는 QBRC(Queue Bytes Received Counter)에 대한 하드웨어 제한이 있으므로 총 수신된 바이트 수가 0xFFFFFFFF를 초과한 후에 오버플로가 발생함  
하드웨어 제한 때문에 오버플로가 발생할 경우 get dataplane physical-port stats의 CLI 출력이 실제 숫자와 일치하지 않습니다.

해결 방법: 카운터가 재설정되고 짧은 기간 안에 다시 실행되도록 CLI를 한 번 실행합니다.

- **문제 2075246: Tier-1 논리적 라우터를 Tier-0 논리적 라우터에서 다른 논리적 라우터로 이동할 수 없음**  
Tier-1 논리적 라우터를 Tier-0 논리적 라우터에서 다른 논리적 라우터로 이동하면 Tier-1 논리적 라우터에서 다운링크 포트 라우팅 연결이 손실됩니다.

해결 방법: 다음 단계를 완료하십시오.

1. Tier-0 논리적 라우터에서 Tier-1 논리적 라우터를 분리합니다.
2. Tier-1 논리적 라우터가 Tier-0 논리적 라우터에서 완전히 분리될 때까지 약 20분 동안 기다립니다.
3. Tier-1 논리적 라우터를 다른 Tier-0 논리적 라우터에 연결합니다.  
다운링크 포트 라우팅 연결이 복원됩니다.

- **문제 2077145: 경우에 따라 전송 노드를 강제로 삭제하려고 하면 전송 노드 분리가 발생할 수 있음**  
API 호출을 사용하여 전송 노드를 강제로 삭제하려고 하면(예: 하드웨어 장애가 발생하여 호스트가 회복할 수 없게 되는 경우) 전송 노드가 분리된 상태로 변경됩니다.

해결 방법: 분리된 전송 노드가 있는 패브릭 노드를 삭제합니다.

- **문제 2099530: 브리지 노드 VTEP IP 주소를 변경하면 트래픽이 중단됨**  
브리지 노드 VTEP IP 주소가 변경되면 VLAN에서 오버레이의 MAC 테이블이 원격 하이퍼바이저에서 업데이트되지 않아서 트래픽 중단이 최대 10분까지 발생합니다.

해결 방법: 하이퍼바이저에서 오버레이 MAC 테이블이 새로 고쳐지도록 VLAN에서 트래픽 변경을 시작합니다.

- **문제 2106176: 설치의 [등록 대기 중] 단계에서 NSX Controller 자동 설치가 정지됨**  
NSX Manager API 또는 UI를 사용하여 NSX Controller를 자동 설치하는 동안 진행 중인 NSX Controller 중 하나의 상태가 정지되고 무기한 **등록 대기 중**으로 표시됩니다.

해결 방법: 다음 단계를 완료하십시오.

1. 정지된 NSX Controller와 연결된 VM ID를 찾으려면 API 요청을 보냅니다.

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments
```

2. 정지된 NSX Controller를 삭제하도록 API 요청을 보냅니다.

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments/<Controller id>?action=delete
```

- **문제 2112459: 브리지 클러스터에서 단일 노드를 교체하면 트래픽이 손실됨**  
브리지 클러스터에서 단일 노드를 교체하면 브리지된 트래픽이 이전 노드로 이동하여 원격 하이퍼바이저의 전달 항목이 업데이트되거나 오래된 상태가 될 때까지 트래픽이 손실됩니다.

해결 방법: 다음 단계를 완료하십시오.

1. 브리지 클러스터에 교체 노드를 넣습니다.
2. HA가 설정되도록 허용합니다.
3. 이전 노드를 제거합니다.

- **문제 216992: 사용자 지정 논리적 포트 MTU 설정을 사용하면 패킷 삭제가 발생할 수 있음**  
논리적 포트에서 사용자 지정 MTU 설정(예: 논리적 라우터 업링크 포트와 맞지 않는 값 또는 Tier-0 및 Tier-1 논리적 라우터의 특정 구성)을 사용하면 패킷 삭제가 발생할 수 있습니다. 기본 MTU 설정은 1500입니다.

해결 방법: 기본 MTU 설정을 사용하십시오.

그렇지 않으면 다른 논리적 포트에 적용된 MTU가 다음 관계를 준수해야 합니다.

1. Tier-0 논리적 라우터 업링크 MTU를 8900으로 설정합니다.
2. NSX Edge VTEP MTU를 9000으로 설정합니다.
3. VM MTU를 8900으로 설정합니다.

Tier-0 논리적 라우터와 Tier-0 논리적 라우터에 연결된 모든 Tier-1 논리적 라우터는 동일한 NSX Edge 노드에 공동 배치되어야 합니다.

- 문제 2125514: 계층 2 브리지 페일오버 후 MAC이 다시 학습될 때까지 일부 NSX Edge VM의 논리적 스위치가 모든 단일 패킷의 BUM 복제를 수행할 수 있음  
계층 2 브리지 페일오버 후 MAC이 끝점에 대해 다시 학습될 때까지 일부 NSX Edge VM의 논리적 스위치가 모든 단일 패킷의 BUM 복제를 거의 10분 동안 수행할 수 있습니다. 끝점이 다음 ARP를 생성하면 시스템이 자체적으로 복구됩니다.

해결 방법: 없음

- 문제 2113769: DHCP 릴레이가 NSX Edge VLAN 계층 2 브리징에서 지원되지 않음  
NSX Edge의 계층 2 브리징 포트를 통해 VLAN 호스트를 논리적 스위치 VNI에 연결하면 논리적 라우터 포트의 DHCP 릴레이 에이전트가 VLAN 호스트에 IP 주소를 제공하지 않게 됩니다.

해결 방법: 다음 단계를 완료하십시오.

1. VLAN 호스트를 수동으로 구성합니다.
2. 계층 2 브리징 포트를 ESXi 호스트로 이동합니다.

- 문제 2183549: 중앙 집중식 서비스 포트를 편집할 때 새로 생성된 VLAN 논리적 스위치를 볼 수 없음  
Manager UI에서 중앙 집중식 서비스 포트와 새 VLAN 논리적 스위치를 생성한 다음 중앙 집중식 서비스 포트를 편집하면 새로 생성된 VLAN 논리적 스위치를 볼 수 없습니다.

해결 방법: API를 사용하여 포트를 편집합니다.

- 문제 2160634: 루프백에서 IP 주소를 변경하면 업링크에서 라우터 ID의 IP 주소가 변경될 수 있음  
루프백의 IP 주소가 변경되면 NSX Edge는 업 링크의 IP 주소를 라우터 ID로 선택합니다. 라우터 ID로 할당된 업링크의 IP 주소는 변경할 수 없습니다.

\*고객에게 미치는 영향\*: 1. 라우터 ID의 예상되는 부작용은 모든 BGP 세션이 플래핑되는 것입니다.  
2. 실질적인 영향은 라우터 ID의 변경이며, 이로 인해 BGP 디버깅이 어려워져서 혼동을 야기할 수 있습니다.

해결 방법: BGP 구성을 사용하지 않도록 설정하고 루프백의 IP 주소를 변경합니다.

- 문제 2186040: 전송 노드가 시스템의 상위 250개 업링크 프로파일에 없는 경우 물리적 NIC의 업링크 드롭다운이 사용자 인터페이스에서 사용하지 않도록 설정됨  
전송 노드가 시스템의 상위 250개 업링크 프로파일에 없는 경우 물리적 NIC의 업링크 드롭다운이 사용자 인터페이스에서 사용하지 않도록 설정됩니다. 전송 노드 결과를 저장하면 전송 노드에서 업링크 이름이 제거됩니다.

해결 방법: 해당 전송 노드에 대한 업링크 프로파일 및 업링크 이름이 다시 선택합니다.

- 문제 2106635: 정적 경로를 생성하는 동안 NULL 경로의 관리 거리를 변경하면 다음 홉 NULL 설정이 사용자 인터페이스에서 사라짐  
정적 경로를 생성하는 동안 다음 홉 NULL을 설정하고 NULL 경로의 관리 거리를 변경하면 다음 홉 NULL 설정이 사용자 인터페이스에서 사라집니다.

해결 방법: 다음 홉을 다시 선택합니다.

## 보안 서비스에 대한 알려진 문제

- 문제 1680128: 클라이언트와 서버 간의 DHCP 통신이 암호화되지 않음

해결 방법: IPSEC를 사용하여 통신 안전을 강화하십시오.

- 문제 1711221: IPFIX 데이터가 일반 텍스트 형태로 네트워크를 통해 전송됨  
기본적으로 IPFIX 흐름을 수집하는 옵션이 해제되어 있습니다.

해결 방법: 없음.

- 문제 1726081: Geneve 터널 트래픽(UDP)이 KVM에서 거부됨

해결 방법: 다음 단계를 완료하십시오.

KVM이 firewalld를 사용하는 경우 다음 명령을 수행하여 방화벽에 홀을 생성하십시오.

```
# firewall-cmd --zone=public --permanent --add-port=6081/udp
```

KVM이 IPtable을 직접 사용하는 경우 다음 명령을 수행하여 홀을 생성하십시오.

```
# iptables -A INPUT -p udp --dport 6081 -j ACCEPT
```

KVM이 UFW를 사용하는 경우 다음 명령을 수행하여 홀을 생성하십시오.

```
# ufw allow 6081/udp
```

- 클라이언트가 다른 네트워크에 있고 게스트 VM에서 라우팅 서비스를 제공하는 경우 DHCP 릴리스 및 갱신 패킷이 DHCP 서버에 도달하지 않음

NSX-T는 VM이 라우터로 작동 중인지 여부를 구분할 수 없으므로 라우터 VM을 사용하여 라우팅되는 유니캐스트 DHCP 패킷에 있는 CHADDR 필드가 소스 MAC와 일치하지 않을 때 해당 패킷이 삭제됩니다.

CHADDR은 DHCP 클라이언트 VM의 MAC를 갖지만, 소스 MAC는 라우터 인터페이스의 MAC를 갖습니다.

해결 방법: VM이 라우터처럼 동작하는 경우 라우터 VM의 모든 VIF에 적용되는 스위치 보안 프로파일에서 DHCP 서버 차단을 사용하지 않도록 설정하십시오.

- 문제 2108290: 베어메탈 서버는 전송 노드로써 NSX-T Data Center 보안 기능을 보장할 수 없음

새로운 유형의 전송 노드인 베어메탈 서버는 다른 하이퍼바이저 워크로드와 동일한 수준의 보안 보증(예: 마이크로 세분화)을 제공하지 않습니다. 이것은 애플리케이션 워크로드와 NSX 에이전트 사이에 신뢰할 수 있는 신뢰 경계가 적용되지 않기 때문입니다.

해결 방법: 보안상의 이유로 테넌트 VM에 베어메탈 서버에 대한 루트 권한을 할당하거나 애플리케이션을 루트로 실행하지 마십시오. 테넌트 VM에 이러한 액세스 권한이 있으면 손상된 테넌트 계정 또는 애플리케이션이 베어메탈 서버에 악성 작업을 수행하고 NSX-T Data Center 네트워크에서 문제를 일으킬 수 있습니다.

- 문제 2162722: 인기도 인덱스를 삭제나 거절 규칙 및 상태 비저장 규칙에 적용할 수 없음

트래픽이 규칙 삭제/거절 작업이 있는 규칙이나 상태 비저장 규칙에 도달하는 경우, "세션"이 상태 저장 허용 규칙에만 적용되기 때문에 규칙의 세션 수가 증가하지 않습니다. 인기도 인덱스에서 세션 수를 키 매개 변수로 사용 중이기 때문에 이러한 규칙에 대해 세션 수가 변경되지 않습니다.

해결 방법: 없음

- 문제 2170512: 인터페이스에 1,000개 넘는 규칙이 있으면 방화벽 규칙을 가져오는 CLI 명령이 실패함

인터페이스에 1,000개 넘는 규칙이 있으면 CLI 명령 `get firewall <VIF_ID> ruleset rules`에서 빈 문자열이 반환됩니다.

해결 방법: 두 가지 해결 방법이 있습니다.

- "nsxcli -c get firewall <VIF\_ID> ruleset rules | json" 명령을 대신 실행합니다.
- 다음 원시 CLI 명령을 실행합니다. 결과가 포함된 파일의 이름이 표시됩니다.  
`ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules`

## KVM 네트워킹에 대한 알려진 문제

- 문제 1775916: RHEL KVM 호스트가 패브릭에 추가되지 못한 후에 문제 해결 API POST /api/v1/error-resolver?action=resolve\_error가 오류를 해결하지 못함

RHEL KVM 호스트가 패브릭에 추가되지 못하고 NSX Manager 사용자 인터페이스가 설치 상태를 실패함으로 표시한 후에 문제 해결 API POST /api/v1/error-resolver?action=resolve\_error가 오류 해결을 위해 실행됩니다. 하지만 패브릭에 호스트를 추가하면 다음과 같은 오류 메시지가 다시 표시됩니다.

Failed to install software on host. Un-handled deployment plug-in perform-action.

Install command failed.

해결 방법: 다음 단계를 완료하십시오.

1. 다음 패키지를 수동으로 제거하십시오.

- ```

rpm -e glog-0.3.1-1nn5.x86_64
rpm -e json_spirit-v4.06-1.el6.x86_64
rpm -e kmod-openvswitch-2.6.0.4557686-1.el7.x86_64
rpm -e nicira-ovs-hypervisor-node-2.6.0.4557686-1.x86_64
rpm -e nsx-agent-1.1.0.0.4690847-1.el7.x86_64
rpm -e nsx-aggservice-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-cli-1.1.0.0.4690892-1.el6.x86_64
rpm -e nsx-da-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-host-1.1.0.0.4690932-1.x86_64 rpm -e nsx-host_node_status_reporter-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-lldp-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-logical_exporter-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-mpa-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-netcpa-1.1.0.0.4690924-1.el7.x86_64 rpm -e nsx-sfhc-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-support-bundle-client-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsx-transport_node_status-1.1.0.0.4690845-1.el7.x86_64
rpm -e nsxa-1.1.0.0.4690845-1.el7.x86_64
rpm -e openvswitch-2.6.0.4557686-1.x86_64
rpm -e openvswitch-selinux-policy-2.6.0.4557686-1.noarch
rpm -e python-simplejson-3.3.3-1.el7.x86_64
rpm -e 명령을 실행하는 동안 오류가 발생하는 경우 해당 명령에 --noscripts 플래그를 포함하십시오.
2. 문제 해결 API POST /api/v1/error-resolver?action=resolve_error를 실행하십시오.
3. 패브릭에 KVM 호스트를 다시 추가하십시오.

```

- 문제 1602470: KVM에서 로드 밸런스 팀 구성이 지원되지 않음

- 문제 1611154: 한 KVM 전송 노드의 VM이 다른 전송 노드에 있는 VM에 연결할 수 없음

여러 IP 풀이 다른 네트워크에 속하는 VTEP에 사용될 경우 KVM 호스트의 VM이 다른 IP 풀의 VTEP IP 주소를 갖는 다른 호스트에 배포된 VM에 연결하지 못할 수 있습니다.

해결 방법: KVM 전송 노드가 다른 전송 노드의 VTEP에 사용되는 모든 네트워크에 연결할 수 있도록 경로를 추가하십시오.

예를 들어 2개의 네트워크 25.10.10.0/24 및 35.10.10.0/24가 있고 로컬 VTEP가 게이트웨이가 25.10.10.1인 IP 주소 25.10.10.20을 가질 경우 다음 명령을 사용하여 다른 네트워크에 대한 경로를 추가할 수 있습니다.

```
ip route add dev nsx-vtep0.0 35.10.10.0/24 via 25.10.10.1
```

- 문제 1654999: 언더레이 트래픽에 대한 연결 추적 수행 시 사용 가능한 메모리가 감소함

가상 시스템 간에 많은 수의 연결을 설정할 경우 다음과 같은 현상이 나타날 수 있습니다.

/var/log/syslog 또는 /var/log/messages 파일에 다음과 비슷한 항목이 표시됩니다.

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950872] net_ratelimit: 239 callbacks suppressed
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950875] nf_conntrack: table full, dropping packet
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.958436] nf_conntrack: table full, dropping packet
```

기본 방화벽 규칙이 구성되었을 경우 문제가 발생하는 것으로 보입니다. 방화벽 규칙이 구성되지 않은 경우에는 문제가 발생하지 않습니다(예: 논리적 스위치가 방화벽 예외 목록에 있음).

참고: 앞서 발췌한 로그는 예일 뿐입니다. 날짜, 시간 및 환경 변수는 사용 환경에 따라 다를 수 있습니다.

해결 방법: 언더레이 디바이스의 포트 6081에서 UDP에 대한 연결 추적을 사용하지 않도록 설정하는 방화벽 규칙을 추가하십시오.

명령 예는 다음과 같습니다.

```
# iptables -A PREROUTING -t raw -p udp --dport 6081 -j CT --notrack
```

이 명령은 부팅 동안 실행되도록 구성해야 합니다. 플랫폼에도 사용되도록 설정된 방화벽 관리자가 있는 경우 (Ubuntu: UFW; RHEL: firewalld), 방화벽 관리자를 통해 동급의 규칙을 구성해야 합니다. 관련 [KB 2145463](#)을 참조하십시오.

- **문제 2002353: Linux Network Manager를 사용한 KVM 호스트 업링크 관리가 지원되지 않음**  
NSX-TData Center는 N-VDS에 사용되는 KVM 호스트의 모든 NIC를 관리합니다. 이러한 업링크에 대해서도 Network Manager를 사용하도록 설정되어 있는 경우 구성 오류가 발생합니다.

해결 방법: Ubuntu 호스트의 경우 NSX-TData Center에 사용할 NIC를 Network Manager에서 제외시킵니다.

Red Hat 호스트에서 NSX-TData Center 를 사용하도록 설정하기 전에 /etc/sysconfig/network-scripts의 NIC 구성 스크립트를 NM\_CONTROLLED="no"로 수정합니다. 호스트에 대해 NSX-TData Center 를 사용하도록 이미 설정된 경우 스크립트를 동일하게 수정하고 호스트에 대한 네트워킹을 다시 시작합니다.

- **문제 2186045: KVM에서 기본적으로 로그 순환(logrotate)이 1분마다 실행되지 않고 매일 실행됨**  
KVM에서 로그 파일의 크기가 1일 이내에 크기 기반 순환 정책에 정의된 크기 제한을 초과하는 경우, 로그 순환 (logrotate)이 실행되는 날이 끝날 때까지 로그가 순환되지 않습니다. 따라서 로그 파일 크기가 정의된 크기 제한보다 클 수 있습니다.

해결 방법: 다음 단계를 수행합니다.

1. 새 디렉토리 /etc/cron.minutes를 생성합니다.
2. 다음 내용으로 /etc/cron.minutes/logrotate 스크립트를 생성합니다.  
#!/bin/sh  
/usr/sbin/logrotate /etc/logrotate.conf
3. /etc/cron.minutes/logrotate에 대한 사용 권한을 변경합니다.  
chmod 755 /etc/cron.minutes/logrotate
4. cron.minutes를 /etc/crontab에서 항목으로 추가합니다.  
echo " \* \* \* \* \* root cd / && run-parts --report /etc/cron.minutes" >>/etc/crontab

## 로드 밸런서에 대한 알려진 문제

- **문제 2010428: 로드 밸런서 규칙 생성 및 애플리케이션 제한 사항**  
사용자 인터페이스에서는 가상 서버에서만 로드 밸런서 규칙을 생성할 수 있습니다. REST API를 사용하여 생성된 로드 밸런서 규칙은 사용자 인터페이스에서 가상 서버에 연결할 수 없습니다.

해결 방법: REST API를 사용하여 로드 밸런서 규칙을 만든 경우 REST API를 사용하여 가상 서버에 해당 로드 밸런서 규칙을 연결하십시오. 이제 REST API를 사용하여 생성된 규칙이 사용자 인터페이스의 가상 서버에 나타납니다.

- **문제 2016489: 서버 이름 표시가 선택되면 LCP가 기본 인증서를 구성하지 못함**  
LCP가 기본 인증서를 무시하지 않도록 하려면 SNI(서버 이름 표시)에 여러 인증서 ID가 사용되는 경우 기본 인증서 ID를 인증서 목록에서 첫 번째로 설정해야 합니다.

해결 방법: 기본 인증서가 SNI 인증서 목록의 첫 번째 인증서여야 합니다.

- **문제 2115545: 로드 밸런서 상태 점검을 사용하도록 설정하면 백엔드 서버 풀 멤버에 대한 직접 연결이 실패할 수 있음**  
로드 밸런서가 논리적 라우터에 연결된 경우, 논리적 라우터의 업링크를 사용하여 풀 멤버에 연결할 수 있으면 논리적 라우터의 다운링크에 연결된 클라이언트는 상태 점검과 동일한 프로토콜을 사용하여 풀 멤버에 액세스할 수 없습니다.

예를 들어 로드 밸런서가 논리적 라우터 LR1에 연결되어 있고 LR1 업링크를 통해 연결할 수 있는 풀 멤버에 대해 ICMP 상태 점검을 사용하도록 설정된 경우에는 LR1 다운링크의 클라이언트가 해당 풀 멤버를 직접 ping할 수 없습니다. 하지만 동일한 클라이언트가 SSH나 HTTP와 같은 다른 프로토콜을 사용하여 서버와 통신할 수 있습니다.

해결 방법: 로드 밸런서에서 다른 상태 점검 유형을 사용합니다. 예를 들어 백엔드 서버에 ping을 수행하려면 ICMP 상태 점검 대신 TCP 또는 UDP 상태 점검을 사용합니다.

- **문제 2128560: 로드 밸런서 SNAT 자동 맵과 상태 점검을 모두 구성하면 상태 점검 또는 연결이 가끔 실패할 수 있음**



동일한 서버 풀에 대해 로드 밸런서 SNAT 자동 맵과 상태 점검(TCP, HTTP, HTTPS 또는 UDP)을 모두 구성하면 해당 서버 풀에 대한 상태 점검 또는 연결이 가끔 실패할 수 있습니다.

해결 방법: SNAT 자동 맵 대신 SNAT IP 목록을 사용합니다.

**참고:** SNAT IP 목록 모드에 지정된 SNAT IP 주소에는 논리적 라우터 업링크 IP 주소가 포함되지 않아야 합니다.

예를 들어 로드 밸런서가 Tier-1 논리적 라우터인 LR1에 연결된 경우에는 구성된 SNAT IP 범위에 LR1 업링크 IP 주소가 포함되지 않아야 합니다.

## 솔루션 상호 운용성에 대한 알려진 문제

- **문제 1588682: ESXi 호스트를 잠금 모드로 두면 사용자 nsx-user가 사용되지 않도록 설정됨**  
ESXi 호스트가 잠금 모드가 될 경우 사용자 vpxuser는 호스트에서 인증할 수 있거나 명령을 실행할 수 있는 유일한 사용자가 됩니다. NSX-TData Center는 호스트에서 모든 NSX-TData Center관련 작업을 수행하기 위해 다른 사용자인 nsx-user에 의존합니다.

해결 방법: 잠금 모드를 사용하지 마십시오. vSphere 설명서에서 [잠금 모드](#)를 참조하십시오.

## 작동 및 모니터링 서비스에 대한 알려진 문제

- **문제 1749078: ESXi 호스트 및 해당 호스트 전송 노드에서 테넌트 VM을 삭제한 후에 ESXi 호스트를 삭제하려고 하면 실패함**  
호스트 노드를 삭제하면 다양한 개체가 재구성되며 삭제를 완료하는 데 몇 분 이상이 소요될 수 있습니다.

해결 방법: 몇 분 동안 기다린 후 삭제 작업을 다시 시도하십시오. 필요한 경우 반복하십시오.

- **문제 1761955: VM을 등록한 후에 VM의 vNIC를 NSX-T Data Center 논리적 스위치로 연결할 수 없음**  
기존 vmx 파일이 ESXi 호스트에 VM을 등록하는 데 사용될 경우 등록 작업 중에 다음 vNIC 관련 오류가 무시됩니다.
  - 잘못된 네트워크 지원으로 구성된 vNIC
  - NSX-T 논리적 스위치에 연결된 vNIC에 대한 VIF 연결 실패

해결 방법: 다음 단계를 완료하십시오.

1. 표준 vSwitch에 임시 포트 그룹을 생성합니다.
2. 연결 해제된 상태의 vNIC를 새 포트 그룹에 연결하고 연결된 상태로 표시합니다.
3. vNIC를 유효한 NSX-TData Center논리적 스위치에 연결합니다.

- **문제 1774858: 드문 경우지만 NSX Controller 클러스터가 며칠 동안 실행된 후에 비활성 상태가 됨**  
NSX Controller 클러스터가 비활성화되면 모든 전송 및 NSX Edge 노드와 NSX Controller 간의 연결이 끊어지고 구성 변경을 수행할 수 없습니다. 하지만 데이터 트래픽은 영향을 받지 않습니다.

해결 방법: 다음 단계를 완료하십시오.

- 디스크 지연 시간 문제가 있으면 수정합니다.
- 모든 NSX Controller에서 cluster-mgmt 서비스를 다시 시작합니다.

- **문제 1576304: 삭제된 바이트 수가 포트 상태 및 통계 보고서의 일부로 포함되지 않음**  
/api/v1/logical-ports/<논리적 포트 ID>/statistics 또는 NSX Manager를 사용하여 논리적 포트 상태 및 통계를 확인하면 삭제된 패킷 수 값이 0으로 표시됩니다. 이 값은 정확하지 않습니다. 삭제된 패킷 수와 관계없이 여기에 표시되는 수는 항상 0입니다.

해결 방법: 없음.

- **문제 1955822: 라이선스 사용량 보고 csv 파일에 실제 사용량뿐만 아니라 CPU 및 VM 사용 권한도 포함되어야 함**  
라이선싱 사용량 보고서를 쿼리할 경우(API/UI를 통해) 데이터에 현재 사용량만 포함되어 있습니다.

해결 방법: UI 또는 REST API를 통해 현재 라이선스에서 허용하는 사용량 제한을 쿼리하십시오.

방법: GET; URI: /api/v1/licenses

- 문제 2081979: 전송 노드 호스트가 모든 컨트롤러에 연결할 수 없음

NSX 프록시 로그에 다음 내용이 표시됩니다. "인증서 검증" 메시지가 필요하지만 없습니다.

TCP connection started: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757:1234

Doing SSL handshake

TCP connection established: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757, local addr:

10.171.0.59:36048, remote addr: 10.171.0.73

해결 방법: 컨트롤러에 관리자로 로그인하여 다음 명령을 실행합니다.

set debug

get mediator forcesync

## 업그레이드에 대한 알려진 문제

- 문제 1930705: 관리부를 업그레이드하는 동안 논리적 스위치에 연결된 VM의 vMotion이 실패함

관리부 업그레이드 동안 논리적 스위치에 연결된 VM을 vMotion하려고 하면 실패합니다.

해결 방법: 관리부 업그레이드가 완료될 때까지 기다렸다가 vMotion 프로세스를 다시 시도하십시오.

- 문제 2005423: 이전 NSX-T 버전에서 업그레이드된 KVM 노드가 balance-tcp를 사용하도록 자동으로 변경되지 않음

NSX-T는 업그레이드된 KVM 호스트 업링크의 결합 모드를 active-backup에서 balance-tcp로 자동 수정하지 않습니다.

해결 방법: 구성이 변경되지 않은 경우에도 전송 노드를 편집하여 모드 설정을 수정합니다.

- 문제 2101728: NSX Edge 그룹 업그레이드에 성공한 후 NSX Edge 업그레이드 프로세스가 일시 중지되는 경우가 있음

NSX Edge 그룹 업그레이드가 성공했지만 두 번째 NSX Edge 그룹 업그레이드 중에 프로세스가 일시 중지됩니다.

해결 방법: 계속을 클릭하여 NSX Edge 그룹 업그레이드를 계속 진행합니다.

- 문제 2106257: NSX-T 2.1에서 NSX-T 2.2로 업그레이드하면 EULA API 동의 워크플로가 변경됨

EULA API 동의는 업그레이드 코디네이터를 업데이트한 후 기존 호스트를 업그레이드하기 전에 호출해야 합니다.

해결 방법: 없음

- 문제 2108649: 업그레이드를 수행할 파티션에 파일 또는 디렉토리가 열려 있으면 업그레이드가 실패함

업그레이드할 NSX Manager나 NSX Controller와 같은 파티션에 파일이나 디렉토리를 열어두지 말아야 합니다. 열려 있는 경우 업그레이드 프로세스가 실패합니다.

해결 방법: 장애가 발생한 장치를 재부팅하고 업그레이드 프로세스를 다시 시작합니다.

- 문제 2116020: NSX-T 2.1에서 NSX-T 2.2로 업그레이드한 후 일부 Ubuntu KVM의 더 이상 지원되지 않는 패키지가 제거되지 않음

NSX-T 2.1에서 NSX-T 2.2로 업그레이드한 후 다음과 같은 Ubuntu KVM의 더 이상 지원되지 않는 패키지가 제거되지 않습니다.

- nsx-host-node-status-reporter
- nsx-lldp
- nsx-logical-exporter
- nsx-netcpa
- nsx-support-bundle-client
- nsx-transport-node-status-reporter

○ nsxa

해결 방법: 다음 단계를 완료하십시오.

1. /etc/vmware/nsxa/ 디렉토리에 임시 파일을 생성합니다.  
cd /etc/vmware/nsxa  
touch temp.txt
2. 모든 nsxa 패키지 디렉토리 및 파일을 나열합니다.  
dpkg -L nsxa  
/etc/vmware/nsxa# ls
3. 다음 패키지를 제거합니다.
  - a) dpkg --purge nsx-lldp
  - b) dpkg --purge nsx-support-bundle-client
  - c) dpkg --purge nsx-transport-node-status-reporter
  - d) dpkg --purge nsx-logical-exporter
  - e) dpkg --purge nsx-netcpa
  - f) dpkg --purge nsxa
  - g) dpkg --purge nsx-host-node-status-reporter
4. 다음 디렉토리를 사용할 수 있는지 확인합니다.  
/etc/vmware/nsxa/
5. /etc/vmware/nsxa/ 디렉토리에서 temp.txt 파일을 제거합니다.  
rm -f temp.txt

- 문제 2164930: 빈 호스트 업그레이드 단위 그룹이 있는 경우 관리부 업그레이드가 완료되고 일시 중지됨 상태가 표시됨

빈 호스트 업그레이드 단위 그룹이 있으면 전체 관리부 업그레이드 상태가 일시 중지됨으로 나타나고 호스트 업그레이드 상태가 100%로 표시되지 않습니다.

\*고객에게 미치는 영향\*: 업그레이드하는 동안 고객에게 빈 호스트 그룹이 있으면 MP 업그레이드가 완료된 후 업그레이드 상태가 [일시 중지됨]으로 표시됩니다.

해결 방법: 관리부를 업그레이드하기 전에 빈 호스트 업그레이드 단위 그룹을 삭제합니다.

관리부가 업그레이드된 경우에는 빈 호스트 업그레이드 단위 그룹을 삭제하고 CLI를 사용하여 install-upgrade 서비스를 다시 시작합니다.

- 문제 2097094: 업로드 도중 업그레이드 번들 업로드를 취소할 수 없음  
업그레이드 번들 .mub 파일을 업로드하는 도중에는 업로드 작업을 취소할 수 없습니다.

해결 방법: 업그레이드 번들 .mub 파일 업로드가 완료될 때까지 기다립니다.

- 문제 2122242: Ubuntu KVM 호스트를 NSX-T 2.1에서 2.2 또는 NSX-T Data Center 2.3으로 업그레이드해도 nsx-support-bundle-client 패키지가 제거되지 않음

Ubuntu KVM 호스트를 NSX-T 2.1 릴리스에서 최신 릴리스(NSX-T 2.2 또는 NSX-T Data Center 2.3)로 업그레이드하는 경우 nsx-support-bundle-client 패키지가 더 이상 사용되지 않아도 계속 설치되어 있습니다. 사용자가 명령(예: /usr/bin/dpkg -l)을 호출하면 패키지가 아직 설치되어 있는 것을 확인할 수 있습니다.

해결 방법: 루트로 로그인하고 다음 명령을 실행하여 패키지를 수동으로 제거합니다.

```
# /usr/bin/dpkg --purge nsx-support-bundle-client
```

- 문제 2186957: 업그레이드 후 ESXi 호스트의 유지 보수 모드가 종료되지 않음  
클러스터에 호스트가 하나만 있고 유지 보수 모드로 전환하려는 업그레이드 조정기의 이전 시도가 실패한 경우에는 업그레이드 후에도 ESXi 호스트의 유지 보수 모드가 종료되지 않습니다.

해결 방법: 수동으로 호스트의 유지 보수 모드를 종료하거나 호스트가 유지 보수 모드로 전환될 수 있는지 확인합니다(클러스터당 2개 이상의 호스트가 있어야 함).

- 문제 2166207: NSX-T Data Center 2.2를 하이퍼바이저가 500개 있는 NSX-T Data Center 2.3으로 업그레이드하는 동안, 전체 업그레이드 프로세스가 무기한 [진행 중] 상태로 남아 있을 수 있음

NSX-T Data Center 2.2를 하이퍼바이저가 500개 있는 NSX-T Data Center 2.3으로 업그레이드하는 동안, [일시 중지]를 클릭하고 웹 브라우저를 여러 번 새로 고침 후 전체 업그레이드 프로세스가 무기한 [진행 중] 상태로 남아 있을 수 있습니다.

해결 방법: NSX Manager에서 NSX-T Data Center CLI에 로그인합니다. install-upgrade 명령을 입력하여 서비스를 다시 시작합니다.

- **문제 2113681: NSX Edge 업그레이드 후에 KVM 호스트에 연결할 수 없게 되고 장애가 발생하면, 업그레이드 조정기가 NSX Controller 노드에 업그레이드를 진행하는 대신 실패한 호스트를 업그레이드하려고 시도함**  
KVM 호스트 및 NSX Edge를 업그레이드한 후 새 RPM을 제거하고 호스트에 이전 RPM을 설치하면 업그레이드 조정기에서 호스트를 사용할 수 없게 됩니다. 따라서 업그레이드 조정기가 NSX Controller 노드 업그레이드를 진행하는 대신 KVM 호스트를 업그레이드하려고 시도합니다.

해결 방법: 업그레이드 조정기 사용자 인터페이스를 새로 고치고, **호스트** 탭을 클릭하여 KVM 호스트 업그레이드를 시도합니다.

KVM 호스트 업그레이드를 건너뛰고 명령 프롬프트를 열어 `curl -i -k -u admin -X POST https://<NSX-Manager-IP-주소>/api/v1/upgrade/plan?action=continue&skip=true` 명령을 입력할 수도 있습니다.

## API에 대한 알려진 문제

- **문제 1605461: syslog의 NSX-T API 로그가 시스템 내부 API 호출을 표시함. NSX-T가 사용자 호출 API 호출과 시스템 호출 API 호출을 모두 syslog에 로깅함**  
syslog의 API 호출 이벤트 로깅은 사용자가 NSX-T API를 직접 호출한 증거가 되지 않습니다. 이러한 NSX-T 장치에 공개적으로 노출된 API 서비스가 없더라도 NSX Controller 및 NSX Edge API 호출이 로그에 표시됩니다. 이러한 개인 API 서비스는 NSX-T CLI 등의 다른 NSX-T 서비스에서 사용됩니다.

해결 방법: 없음.

- **문제 1641035: POST/hpm/features/<기능 스택 이름>?action=reset\_collection\_frequency에 대한 REST 호출이 덮어쓰기 통계에 대한 collection\_frequency를 복원하지 않음**  
이 REST 호출을 사용하여 수집 빈도를 기본값으로 재설정하려고 해도 재설정되지 않습니다.  
해결 방법: PUT /hpm/features/<기능 스택 이름>을 사용하고 collection\_frequency를 새 값으로 설정하십시오.

- **문제 1648571: 요청 시 상태 및 통계 요청이 간헐적으로 실패할 수 있음 HTTP 실패 코드가 일관되지 않음**  
특정 상황에서 요청 시 요청이 실패합니다. 경우에 따라 API 호출이 재시도에 성공하더라도 이러한 요청이 HTTP 503 오류가 아닌 HTTP 500 오류를 나타내며 실패합니다.  
통계 API의 경우 시간 초과 조건으로 인해 올바르게 않은 메시지 라우팅 오류 로그를 생성합니다. 이러한 문제는 시간 초과 기간이 만료된 후에 응답이 반환되기 때문에 발생합니다.  
예를 들어 다음과 같은 오류가 발생할 수 있습니다. `java.lang.IllegalArgumentException: Unknown message handler for type com.vmware.nsx.management.agg.messaging.AggService$OnDemandStatsResponseMsg.`  
상태 API의 경우 시간 초과 조건, 시간 초과 이후에 반환된 응답으로 인해 캐시가 미리 업데이트될 수 있습니다.

해결 방법: API 요청을 다시 시도하십시오.

- **문제 1963850: GET API가 대/소문자를 구분하는 방식으로 정렬된 항목을 표시함**  
GET API가 표시 이름을 기준으로 정렬된 항목을 반환하는 경우 정렬에서 대/소문자가 구분됩니다.

해결 방법: 없음.

- **문제 2070136: 많은 양의 데이터를 처리하는 분산 방화벽 API가 실패함**  
100MB를 초과하는 데이터를 생성하거나 업데이트해야 하는 분산 방화벽 API에 오류 코드 500 및 실패한 트랜잭션을 나타내는 메시지가 표시되면서 실패합니다. 일반적으로 API에는 규칙이 1000개가 넘게 있는 섹션이 포함되며 각 규칙에는 다수의 소스, 대상 및 적용 대상 개체가 포함됩니다.

해결 방법: 규칙을 점진적으로 생성하거나 업데이트합니다.

- 문제 1895497: API의 로드 밸런서 알고리즘 SRCDESTMACIPPORT가 작동하지 않음  
원본 및 대상 MAC 주소, IP 주소 및 TCP/UDP 포트가 있는 LAG를 사용하여 전송 노드의 업링크 프로파일을 만드는 API를 호출하면 실패합니다.

해결 방법: 없음

## NSX Policy Manager에 대한 알려진 문제

- 문제 2057616: NSX Policy Manager를 NSX-T 2.1에서 NSX-T 2.2로 업그레이드하는 동안 지원되지 않는 NSService 및 NSGroup이 전송되지 않음  
NSX Policy Manager를 NSX-T 2.1에서 NSX-T 2.2로 업그레이드하는 동안 이더넷 유형의 지원되지 않는 NSService와 MAC 집합 및 논리적 포트 멤버 자격 조건이 있는 NSGroup이 전송되지 않습니다.

해결 방법: 다음 단계를 완료하십시오.

1. NSX-T 2.1에서 모든 통신 항목에 사용되는 이더넷 유형의 NSService를 제거하고 수정합니다.
2. 모든 통신 항목에 사용되는 MAC 집합 및 논리적 포트 멤버 자격 조건이 있는 NSGroup을 제거하고 수정합니다.
3. NSX Manager를 NSX-T 2.1에서 NSX-T 2.2로 업그레이드합니다.
4. CLI를 사용하여 NSX Policy Manager를 업그레이드합니다.

- 문제 2116117: UI의 NSX Policy Manager 토폴로지 탭에 데이터 연결 실패가 표시됨  
정책 도메인의 그룹에 지원되지 않는 ESXi 6.7 버전에서 호스팅되는 VM이 포함되어 있기 때문에 UI의 NSX Policy Manager 토폴로지 탭에 데이터 연결 실패가 표시됩니다.

해결 방법: 없음

- 문제 2126647: NSX Policy Manager 분산 방화벽을 동시에 업데이트하면 재정의가 발생함  
두 사용자가 NSX Policy Manager 분산 방화벽 섹션을 동시에 편집하면, 마지막 사용자의 변경 사항이 이전에 다른 사용자가 편집한 내용을 재정의합니다.

해결 방법: 첫 번째 사용자가 수행한 분산 방화벽 변경 사항을 복구합니다. 변경 사항이 저장된 후 두 번째 사용자가 변경 작업을 수행할 수 있습니다.

## NSX Cloud에 대한 알려진 문제

- 문제 2112947: CSM(Cloud Service Manager)에서 NSX 에이전트를 업그레이드하는 동안 일부 인스턴스가 실패로 표시될 수 있음  
CSM에서 NSX 에이전트를 업그레이드하는 동안 사용자 인터페이스의 응답이 없어서 일부 인스턴스가 실패로 표시될 수 있음

해결 방법: 사용자 인터페이스를 새로 고칩니다.

- 문제 2111262: PCG를 배포하는 동안 다음 오류가 표시될 수 있음: "게이트웨이 배포 실패: [Errorcode: 60609] 프로비저닝 상태: 실패로 인해 비동기식 작업이 실패했습니다." 또는 "이름이 nsx-gw인 게이트웨이가 가상 시스템을 생성하지 못했습니다. 게이트웨이 배포에 실패했습니다."  
이런 이벤트는 드물며 Microsoft Azure 인프라로 인해 발생합니다.

해결 방법: 실패한 PCG(공용 클라우드 게이트웨이)를 다시 배포합니다.

- 문제 2110728: HA를 사용하고 있지만 --gateway 옵션을 사용하여 PCG의 DNS 이름을 하나만 지정하여 VM에 NSX 에이전트를 설치하면 보조 PCG로의 페일오버가 작동하지 않습니다.  
페일오버 후 워크로드 VM이 PCG에 연결할 수 없기 때문에 PCG가 VM에 논리적 상태를 적용/실행할 수 없습니다.

해결 방법: 워크로드 VM에 에이전트를 설치할 때는 ---gateway 옵션을 전혀 사용하지 마십시오. VPC 또는 VNet 게이트웨이 화면의 값을 사용합니다. 자세한 내용은 NSX-T Data Center 관리 가이드에서 NSX 에이전트 설치를 참조하십시오.

- 문제 2071374: 특정 Linux VM 인스턴스에 NSX 에이전트를 설치할 때 "nscd"와 관련된 무해한 오류 메시지

## 가 표시될 수 있음

설명: NSX 에이전트를 설치할 때 "nscd"를 실행 중인 VM에 "sent invalidate(passwd) request, exiting"과 같은 오류 메시지가 표시될 수 있습니다. 이런 상황은 실행 중인 VM(예: Ubuntu 14.04 또는 16.04)에서 발생합니다.

**해결 방법:** 이 메시지는 Linux 배포판의 알려진 버그로 인해 나타납니다. 이 메시지는 무해하며 NSX 에이전트 설치에 영향을 미치지 않습니다.

### • 문제 2010739: 두 PCG(공용 클라우드 게이트웨이)가 모두 대기로 표시됨

게이트웨이를 온보딩하는 동안 기본 PCG가 컨트롤러에 연결할 수 없으면 컨트롤러와 게이트웨이 사이의 연결이 복원될 때까지 기본 및 보조 게이트웨이 모두 대기 모드가 됩니다.

### • 문제 2121686: CSM에 "서버에서 요청을 인증하지 못했습니다." 예외가 표시됩니다.

CSM에 이 오류가 표시될 수 있으며, 그 이유는 CSM 장치 시간이 Microsoft Azure Storage 서버 또는 NTP와 동기화되지 않았기 때문입니다. 이 경우 Microsoft Azure에서 "서버에서 요청을 인증하지 못했습니다."라는 모호한 예외가 발생하며 동일한 오류가 CSM에 표시됩니다.

**해결 방법:** CSM 장치 시간을 NTP 또는 Microsoft Azure Storage 서버 시간과 동기화합니다.

### • 문제 2092378: HA 모드에서 PCG를 배포하면 두 PCG가 모두 대기 모드로 표시되고 클라우드 동기화에는 기본 PCG가 활성으로 표시됨

전용 네트워크에서 CSM을 통해 PCG의 HA 배포를 수행하면 배포된 PCG에 대기/대기 또는 활성/활성 상태가 최대 1시간 동안 표시됩니다. 이 간격 동안 배포된 PCG에 일부 문제가 있을 수 있으며 진행하기에 명확하지 않은 상태일 수 있습니다.

**해결 방법:** 다음을 수행합니다.

1. PCG 배포 후 UI에서 계정을 다시 동기화하면 CSM에서 최신 데이터를 가져와 CSM에서 표시할 수 있습니다.
2. 다시 동기화한 후 CSM에서 잘못된 상태의 PCG를 계속 표시할 경우 NSX Manager에서 PCG의 연결 상태를 확인합니다.
3. 연결이 [실행]으로 표시되는 경우에도 상태가 정확하지 않으면 PCG 디버깅을 진행합니다.

### • 문제 2119726: Microsoft Azure VNet에 PCG를 배포하는 동안 이전에 VM과 연결했던 공용 IP가 사용 가능한 것으로 잘못 나열될 수 있음

이전에 공용 IP가 할당되었던 VM의 전원이 꺼지면 공용 IP가 VM과 더 이상 연결되어 있지 않습니다. 일정 기간 VM의 전원이 꺼져 있으면 Microsoft Azure에서 VM에 연결된 공용 IP를 분리하기 때문입니다. 이 기간은 Microsoft Azure에서 구체적으로 정의되지 않았습니다.

**해결 방법:** VNet의 PCG 전원을 끄지 마십시오. 이렇게 하면 기본 PCG의 업링크 인터페이스와 공용 IP 연결이 해제되는 것을 방지할 수 있습니다. PCG의 전원을 꺼야 하는 경우에는 PCG와 연결된 PIP가 재사용되지 않도록 하고, PCG의 전원이 다시 켜지는 즉시 동일한 PIP를 얻도록 합니다.

### • 문제 2165915: kmod.x86\_64 0:20-15.el7\_4.6의 Red Hat Enterprise Linux 7.4에 대한 NSX Cloud 지원

NSX Cloud는 kmod-20-15.el7\_4.6의 Red Hat Enterprise Linux 7.4를 실행하는 VM 인스턴스를 지원하지 않습니다. 이 문제는 Red Hat에서 보고한 다음 버그로 인해 발생합니다.

[https://bugzilla.redhat.com/show\\_bug.cgi?id=1522994](https://bugzilla.redhat.com/show_bug.cgi?id=1522994).

**해결 방법:** NSX 에이전트 설치에 성공하려면 이 버그가 수정된 kmod 버전으로 업데이트하십시오.

### • 문제 2102828: Microsoft Azure 배포에서, NSX-T 2.2를 NSX-T Data Center 2.3으로 업그레이드하는 동안 및 업그레이드한 후에, PCG(공용 클라우드 게이트웨이)가 작동하지 않는 것으로 보일 수 있습니다.

시스템이 NSX-T 2.2에서 NSX-T Data Center 2.3으로 업그레이드된 Microsoft Azure 배포에서, 드물긴 하지만 PCG(공용 클라우드 게이트웨이)가 인터페이스에서 IP 주소를 가져오지 못할 수 있습니다. 이 문제는 PCG 단계를 업그레이드하는 동안 발생할 수 있으며 이 경우 PCG 업그레이드 프로세스가 중단된 것으로 나타납니다. 또한 관리자가 Microsoft Azure Portal에서 PCG 장치를 다시 시작하면 PCG가 작동하지 않는 것으로 나타날 수도 있습니다. 이 문제는 NSX-T Data Center 2.3을 처음 설치하는 새 시스템에는 적용되지 않습니다.



**해결 방법:** Microsoft Azure Portal에서 업그레이드 중인 PCG를 다시 시작한 다음 CSM(Cloud Service Manager)에서 PCG 및 VM 인스턴스의 상태가 유효한지 확인합니다.

- **문제 2180531: NSX 에이전트는 커널 4.14 이하가 포함된 Ubuntu 16.04 VM 인스턴스에서 지원됨**  
NSX 에이전트는 커널 4.14 이하가 포함된 Ubuntu 16.04 VM 인스턴스에서 지원됩니다. NSX 에이전트는 커널 4.15 이상의 Ubuntu 16.04 VM 인스턴스에서는 작동하지 **않습니다**.

이 문제에 대한 해결 방법은 없습니다.

- **문제 2170445: PCG를 NSX-T Data Center 2.2에서 NSX-T Data Center 2.3으로 업그레이드한 후 PCG HA 상태가 Microsoft Azure PCG에 대해 올바르게 설정되지 않음**  
Microsoft Azure PCG를 NSX-T 2.2에서 NSX-T Data Center 2.3으로 업그레이드한 후, PCG의 HA 상태가 예상대로 액티브-대기가 되지 않습니다. 기본 PCG HA 상태는 동기화로 표시되고 비기본 PCG HA 상태는 액티브로 표시됩니다. 이 때문에 업그레이드 후 HA 페일오버가 발생할 경우 PCG 중 하나만 유효한 상태입니다.

**해결 방법:** NSX-T 2.2에서 NSX-T Data Center 2.3.

이 작업은 NSX Manager UI 또는 NSX Manager REST API를 사용하여 수행할 수 있습니다.

UI를 사용할 경우 다음을 수행합니다.

1. **패브릭 > 프로파일**로 이동합니다.
2. 이름이 "PCG-Uplink-HostSwitch-Profile", 설명이 "PublicCloudGateway Uplink HostSwitch Profile"인 프로파일을 선택합니다.
3. **편집**을 클릭하고 **MTU** 값을 1500으로 수정하고 **저장**을 클릭합니다.
4. NSX-T 2.2에서 NSX-T Data Center 2.3.

REST API를 사용할 경우 다음을 수행합니다.

1. 다음을 사용하여 모든 호스트 스위치 프로파일을 가져옵니다.

```
curl -X GET \
https://<NSX-Manager-URL>/api/v1/host-switch-profiles \
-H 'authorization: Basic <인증 ID>' \
-H 'content-type: application/json'
```

2. 이름이 "PCG-Uplink-HostSwitch-Profile", 설명이 "PublicCloudGateway Uplink HostSwitch Profile"인 호스트 스위치 프로파일을 식별하고 해당 프로파일의 ID를 구합니다.

```
curl -X PUT \
https://<NSX-Manager-URL>/api/v1/host-switch-profiles/<host-switch-profile-id> \
-H 'authorization: Basic <인증 ID>' \
-H 'content-type: application/json' \
-d '{
  "resource_type": "UplinkHostSwitchProfile",
  "description": "PublicCloudGateway Uplink HostSwitch Profile",
  "id": "<호스트-스위치-프로파일-ID>",
  "display_name": "PCG-Uplink-HostSwitch-Profile",
  "tags": [
    {
      "scope": "CrossCloud",
      "tag": "public-cloud-manager"
    }
  ],
}
```

```

    "scope": "PcmId",
    "tag": "<기존 PCM ID>"
  },
  {
    "scope": "EntityType",
    "tag": "default"
  },
  {
    "scope": "CloudScope",
    "tag": "<기존 VPC/VNET 이름>"
  },
  {
    "scope": "CloudType",
    "tag": "<기존 클라우드 유형>"
  },
  {
    "scope": "CloudVpId",
    "tag": "<기존 VPC/VNet ID>"
  }
],
"transport_vlan": 0,
"teaming": {
  "active_list": [
    {
      "uplink_type": "PNIC",
      "uplink_name": "uplink-1"
    }
  ],
  "policy": "FAILOVER_ORDER"
},
"overlay_encap": "GENEVE",
"mtu": 1500,
"_revision": 1
}'

```

- **문제 2174725:** PCG가 배포된 관리되는 VPC/VNet이 CSM에서 관리되지 않는 것으로 표시됩니다.  
관리되는 AWS VPC 또는 PCG가 배포된 Microsoft Azure VNet이 CSM에서 관리되지 않는 것으로 표시됩니다.

**해결 방법:** CSM을 다시 시작하면 문제가 해결됩니다.

- **문제 2162856:** Azure PCG의 HA 상태가 잘못됨(둘 다 활성화 또는 둘 다 대기)  
AWS에 PCG 한 쌍을 배포한 다음 Azure에 또 다른 PCG 쌍을 배포하면 Azure PCG의 HA가 잘못된 상태(둘 다 활성화 또는 둘 다 대기)가 됩니다.

**해결 방법:** Cross 클라우드를 NSX-T Data Center 2.3으로 업그레이드하기 전에, PCM에 의해 생성된 PCG의 업링크 호스트 스위치 프로파일에서 MTU를 1500으로 업데이트합니다. Manager UI에서 다음 단계를 수행합니다.

- [패브릭] > [프로파일]로 이동합니다.
- 이름이 "PCG-Uplink-HostSwitch-Profile", 설명이 "PublicCloudGateway Uplink HostSwitch

Profile"인 프로파일을 선택합니다.

- [편집]을 클릭하고 [MTU] 값을 1,500으로 수정하고 [저장]을 클릭합니다.
- 업그레이드 워크플로를 시작합니다.

● 문제 2102321: 트래픽이 많을 때 Microsoft Azure에서 일부 NSX Cloud 작업이 느려질 수 있음

NSX Cloud는 Microsoft Azure ARM API를 사용하여 VM을 관리하거나, NSX 관리에서 VM을 철회하거나, VM에 차단 조치를 수행하는 등의 작업을 수행합니다. 피크 시간 동안 Microsoft Azure는 특정 구독에 대해 API 제한을 넘어서지 못하도록 제안할 수 있습니다. 이렇게 되면 해당 구독에 대한 모든 API 요청의 임계치가 조절되기 시작합니다. 이 시간 동안은 위에서 언급한 NSX 작업이 시간 내에 완료되지 않을 수 있습니다. 이러한 작업은 Microsoft Azure가 요청에 대한 임계치 조절을 중지하면 완료됩니다. 공용 클라우드 게이트웨이의 PCM 로그에는 현재 임계치 조절이 진행 중임을 나타내는 다음과 같은 로그가 있습니다. "Azure Resource Manager 시간당 읽기/쓰기 한계에 도달했습니다. x 초 내에 다시 시도됩니다."

해결 방법: Microsoft Azure 임계치 조절이 중지될 때까지 기다립니다.

● 문제 2189738: 등록된 VPC에 대해 격리 정책을 사용하지 않도록 설정한 후(이전에 격리 정책을 사용하도록 설정한 경우) AWS 워크로드 VM에 연결할 수 없음

격리 정책을 사용하도록 설정한 상태에서 PCG를 배포한 후에 차단 모드를 사용하지 않도록 설정하면 이 VPC에 있는 일부 NSX 관리 AWS 워크로드가 PCG와 통신하지 못합니다.

해결 방법: AWS VPC의 NSX Cloud 보안 그룹에 인바운드 규칙인 gw-mgmt-sg를 추가합니다.

참고: 보안상의 이유로 격리 정책을 다시 사용하도록 설정하면 이 규칙을 제거하십시오.

| 유형         | 프로토콜 | 포트   | 소스       |
|------------|------|------|----------|
| CUSTOM-TCP | TCP  | 8080 | VPC-CIDR |
| CUSTOM-TCP | TCP  | 5555 | VPC-CIDR |

● 문제 2188950: API를 사용하여 PCG 목록을 검색할 때 "지정된 ID에 대해 VNet을 찾을 수 없습니다."라는 오류가 표시됩니다.

이 오류는 배포된 PCG와 연결된 계정이 CSM에서 삭제되면 표시됩니다.

해결 방법: PCG가 배포된 CSM에 Microsoft Azure 계정을 추가합니다.

● 문제 2191571: PCG 배포를 위한 SSH 공용 키가 이메일 ID로 끝나지 않는 경우 PCG 배포가 시작되지 않음

SSH 공용 키는 이메일 ID로 끝나야 합니다. 그렇지 않으면 PCG 배포가 시작되지 않고 오류가 표시됩니다.

해결 방법: SSH 키가 이메일 ID로 끝나도록 합니다.

● 문제 2092073: Windows 워크로드 VM에서 IPFIX 템플릿이 올바르게 수신되지 않음

Windows 워크로드 VM에서, IPFIX 수집기가 VM과 동일한 서브넷에 구성되어 있으면 논리적 스위치와 방화벽 IPFIX 템플릿이 즉시 발송되지 않습니다. 이것은 UDP 패킷을 보내기 전에 Windows 소켓에 IPFIX 수집기의 IP 주소에 대한 ARP 항목이 필요하기 때문입니다. ARP 항목이 누락되면 마지막 항목을 제외한 모든 UDP 패킷이 자동으로 삭제됩니다. 결과적으로, IPFIX 수집기에서 데이터 패킷이 템플릿 정보 없이 수신됩니다.

해결 방법: 다음 중 하나를 수행합니다.

- 다음 명령을 사용하여 IPFIX 수집기에 대한 정적 ARP 항목을 추가합니다.

```
netsh interface ipv4 add neighbors "<인터페이스 이름>" <수집기 IP> <수집기의 물리적 주소>
```

예:

```
netsh interface ipv4 add neighbors "Ethernet 3" 172.26.15.7 12-34-56-78-9a-bc
```

- 워크로드 VM과 다른 서브넷에 IPFIX 수집기를 구성합니다.

● 문제 2210490: CSM에서 프록시 프로파일을 추가하는 경우 클라우드 서비스 감사자 또는 클라우드 서비스 관리자 역할이 할당된 모든 CSM API 사용자에게 암호가 표시됨

CSM에서 프록시 프로파일을 생성하고 사용자 이름과 암호를 제공하면 CSM UI에서 암호를 볼 수 없더라도 다음 API에 대한 응답으로 암호를 볼 수 있습니다.

- /csm/proxy-server-profiles
- /csm/proxy-server-profiles/<profile-id>

- **문제 2039804: PCG 배포가 실패했을 때 AWS에서 PCG 인스턴스가 종료되지 않음**

PCG 배포 시 배포가 실패했는데 AWS VPC에 PCG 인스턴스가 표시되고 NSX Manager에 자동 생성된 논리적 엔티티가 표시됩니다.

**해결 방법:** 자동 생성된 NSX Manager 엔티티를 수동으로 삭제하고 AWS VPC에서 PCG 인스턴스를 종료합니다.

## NCP(NSX Container Plug-in)에 대한 알려진 문제

- **PAS 2.1.0 CNI 변경**

PAS 2.1.0의 CNI 플러그인 변경으로 인해, NSX-T 타일은 버전에 관계없이 PAS 2.1.0에서 작동하지 않습니다. 이 문제는 PAS 2.1.1에서 수정되었습니다.

- **문제 2118515: 대규모 설정에서 NCP가 NSX-T에 방화벽을 생성하는 시간이 오래 걸림**

대규모(예: Kubernetes 노드 250개, 포트 5000개, 네트워크 정책 2500개) 설정에서 NCP가 NSX-T에 방화벽 섹션과 규칙을 생성하는 데 몇 분 정도 걸릴 수 있습니다.

**해결 방법:** 없음. 방화벽 섹션과 규칙이 생성되면 성능이 정상으로 돌아옵니다.

- **문제 2125755: 카나리아 업데이트 및 단계적 롤링 업데이트를 수행할 때 StatefulSet의 네트워크 연결이 끊길 수 있음**

NCP가 현재 릴리스로 업그레이드되기 전에 StatefulSet이 생성된 경우 카나리아 업데이트 및 단계적 롤링 업데이트를 수행할 때 StatefulSet의 네트워크 연결이 끊길 수 있습니다.

**해결 방법:** NCP가 현재 릴리스로 업그레이드된 후에 StatefulSet을 생성합니다.

- **문제 2131494: 수신 클래스를 nginx에서 nsx로 변경한 후에도 NGINX Kubernetes 수신이 계속 작동함**

NGINX Kubernetes 수신을 생성할 때 NGINX에서 트래픽 전달 규칙이 생성됩니다. 수신 클래스를 다른 값으로 변경하면 클래스를 변경한 후에 Kubernetes 수신을 삭제하더라도 NGINX에서 규칙이 삭제되지 않고 계속 적용됩니다. 이 문제는 NGINX의 제한 사항입니다.

**해결 방법:** NGINX에서 생성된 규칙을 삭제하려면 클래스 값이 nginx일 때 Kubernetes 수신을 삭제합니다. 그런 다음 Kubernetes 수신을 다시 생성합니다.

- **문제 2194845: PAS Cloud Foundry V3 API 기능인 "앱당 여러 프로세스"가 지원되지 않음**

PAS Cloud Foundry V3 API v3-push를 사용하여 여러 프로세스로 앱을 푸시하는 경우, NCP에서 기본값 이외의 프로세스에 대한 논리적 스위치 포트가 생성되지 않습니다. 이 문제는 NCP 2.3.0 및 이전 릴리스에 존재합니다.

**해결 방법:** 없음

- **문제 2193901: 단일 Kubernetes 네트워크 정책 규칙에 대해 여러 PodSelector 또는 여러 NsSelector가 지원되지 않음**

여러 선택기를 적용하면 특정 포트에서 들어오는 트래픽만 허용됩니다.

**해결 방법:** 단일 PodSelector 또는 NsSelector에 matchExpressions와 matchLabels를 대신 사용합니다.

- **문제 2194646: NCP가 다운되면 네트워크 정책 업데이트가 지원되지 않음**

NCP가 종료된 상태에서 네트워크 정책을 업데이트하면 NCP가 다시 시작될 때 네트워크 정책의 대상 IPset가 유효하지 않게 됩니다.

**해결 방법:** NCP가 작동 중일 때 네트워크 정책을 다시 생성합니다.

- **문제 2192489: PAS director 구성에서 'BOSH DNS server'를 사용하지 않도록 설정한 후에도 컨테이너의 resolve.conf 파일에 Bosh DNS 서버(169.254.0.2)가 계속 나타남**

PAS 2.2를 실행하는 PAS 환경의 PAS director 구성에서 'BOSH DNS 서버'를 사용하지 않도록 설정한 후에도 컨테이너의 `resove.conf` 파일에 Bosh DNS 서버(169.254.0.2)가 여전히 나타납니다. 이로 인해 FQDN(정규화된 도메인 이름)을 사용한 `ping` 명령에 시간이 오래 걸립니다. PAS 2.1에는 이 문제가 존재하지 않습니다.

해결 방법: 없음. 이 문제는 PAS 문제입니다.

- **문제 2194367: NSX-T 타일이 자체 라우터를 배포하는 PAS 격리 세그먼트에서 작동하지 않음**

NSX-T 타일이 자체 GoRouters 및 TCP 라우터를 배포하는 PAS(Pivotal Application Service) 격리 세그먼트에서 작동하지 않습니다. NCP에서 라우터 VM의 IP 주소를 가져올 수 없고 라우터에서 PAS App 컨테이너로 이동하는 트래픽을 허용하는 NSX 방화벽 규칙을 만들 수 없기 때문입니다.

해결 방법: 없음.

- **문제 2199504: NCP에서 생성된 NSX-T 리소스의 표시 이름이 80자로 제한됨**

NCP에서 컨테이너 환경의 리소스에 대한 NSX-T 리소스가 생성되는 경우, 클러스터 이름, 네임스페이스 또는 프로젝트 이름, 컨테이너 환경에 있는 리소스의 이름을 결합하여 NSX-T 리소스의 표시 이름이 생성됩니다. 표시 이름이 80자 보다 길면 80자로 잘립니다.

해결 방법: 없음

- **문제 2199778: NSX-T 2.2에서는 이름이 65자보다 긴 수신, 서비스 및 암호가 지원되지 않음**

NSX-T 2.2에서 `use_native_loadbalancer`가 `True`로 설정되면 수신에서 참조하는 수신, 암호 및 서비스의 이름 및 LoadBalancer 유형의 서비스가 65자 이하여야 합니다. 그렇지 않으면 수신 또는 서비스가 제대로 작동하지 않습니다.

해결 방법: 수신, 암호 또는 서비스를 구성하는 경우 65자 이하의 이름을 지정합니다.

- **문제 2065750: 파일 충돌로 인해 NSX-T CNI 패키지 설치가 실패함**

Kubernetes가 설치된 RHEL 환경에서 `yum localinstall` 또는 `rpm -i`를 사용하여 NSX-T CNI 패키지를 설치하면, `kubernetes-cni` 패키지의 파일과 충돌을 나타내는 오류가 발생합니다.

해결 방법: `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm` 명령을 사용하여 NSX-T CNI 패키지를 설치합니다.

- **ClusterIP 유형의 Kubernetes 서비스에 대해 클라이언트 IP 기반 세션 선호도가 지원되지 않음**

NCP는 ClusterIP 유형의 Kubernetes 서비스에 대해 클라이언트 IP 기반 세션 선호도를 지원하지 않습니다.

해결 방법: 없음

- **ClusterIP 유형의 Kubernetes 서비스에 대해 hairpin-mode 플래그가 지원되지 않음**

NCP는 ClusterIP 유형의 Kubernetes 서비스에 대해 `hairpin-mode` 플래그를 지원하지 않습니다.

해결 방법: 없음

## 설명서 오류 및 추가 내용

- **문제 1372211: 동일한 서브넷의 두 인터페이스**

터널 끝점이 관리 인터페이스와 동일한 서브넷에 있는 경우 터널 트래픽이 관리 인터페이스로 누출될 수 있습니다. 이러한 문제는 터널링된 패킷이 관리 인터페이스를 통과할 수 있으므로 발생합니다. 관리 인터페이스가 터널 끝점 인터페이스와는 별개의 서브넷에 있는지 확인하십시오.