

VMware NSX-T Data Center 2.4 릴리스 정보

VMware NSX-T Data Center 2.4 | 2019년 2월 28일 | 빌드 12456646

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
- API 및 CLI 리소스
- 개정 이력
- 해결된 문제
- 알려진 문제

새로운 기능

NSX-T Data Center 2.4는 사설 클라우드, 공용 클라우드 및 하이브리드 클라우드의 가상화된 네트워킹 및 보안에 대한 새로운 기능을 제공하기 위해 여러 가지 새 기능을 제공합니다. 여기에는 새로운 의도 기반 네트워킹 사용자 인터페이스, 컨텍스트 인식 방화벽, 게스트/네트워크 검사 기능, IPv6, 클러스터링된 고가용성 관리, vSphere 계산 클러스터를 위한 프로파일 기반 NSX 설치, NSX for vSphere 계산의 재부팅이 필요 없는 유지 보수 업그레이드 모드, vSphere 계산을 위한 새로운 인플레이스 업그레이드 모드 및 NSX Data Center for vSphere에서 NSX-T Data Center로 마이그레이션하기 위한 마이그레이션 조정기가 포함됩니다.

NSX-T Data Center 2.4 릴리스에는 다음과 같은 새로운 기능과 향상된 기능이 제공됩니다.

관리 클러스터

NSX-T Data Center 2.4는 이제 사용자 인터페이스 및 API의 고가용성을 위해 관리자 클러스터를 생성하는 기능을 지원합니다. 이 클러스터링은 이중화를 위해 NSX에서 제공하는 가상 IP나 이중화 및 로드 분산을 위한 외부 밸런서를 지원합니다. 또한 NSX 관리에서 배포 및 관리해야 하는 가상 장치 수를 줄이기 위해 관리부 기능과 제어부 기능이 새로운 관리 클러스터로 결합되었습니다. NSX Manager 장치는 다양한 배포 시나리오에 맞게 세 가지 크기로 사용할 수 있습니다. 소형 장치는 랩 및 개념 증명 배포에 적합합니다. 중형 장치는 64개의 호스트에 배포하는 데 적합하고 대형 장치는 대규모 환경에 배포하는 고객이 사용하는 데 적합합니다. 구성 최대값에 대한 자세한 내용은 다음 페이지에서 VMware Configuration Maximums 도구를 참조하십시오. <https://configmax.vmware.com>

단일 클러스터 설계 지원

단일 물리적 호스트의 단일 N-VDS로 구동되는 축소된 Edge, 관리, 계산 VM이 있는 단일 클러스터 설계를 지원합니다. VCF SP 고객을 위한 일반적인 참조 설계는 Edge 및 관리용과 계산용 VM의 두 호스트 스위치를 사용하여 10G pNIC 4개를 규정합니다. 이렇게 하면 트래픽이 호스트를 나갔다가 다시 돌아오도록 Edge VM과 계산 VM 간의 통신이 효율적으로 분리됩니다. 그렇지만 25G NIC의 경제적 추세 덕분에 VCF SP 고객은 2개의 25G NIC 호스트에서 표준화를 시행하고, 이 설계를 통해 단일 N-VDS로 이동하여 2pNIC로 호스트를 구동할 수 있게 됩니다. 이 설계에서 동일한 서브넷에 속하는 Edge VM 및 계산 VM은 트래픽이 호스트 업링크를 나갔다가 다시 돌아오지 않고도 통신할 수 있습니다.

정책 및 UI

NSX 관리 및 자동화

- **선언적 정책 관리** - 결과 중심의 정책 문을 통해 네트워크 및 보안 구성을 간소화하고 자동화합니다. 이 새로운 선언적 정책 API는 사용자가 원하는 최종 목표를 설명할 수 있도록 하는 동시에 시스템에서 최적의 목표 달성 방법을 파악할 수 있게 하여 구성 단계 수를 줄입니다. 순서에 관계 없이 지정된 방식으로 전체 네트워크 토폴로지 정의 및 배포를 한 번에 수행할 수 있습니다.

사용자 인터페이스 기능 향상

- **향상된 탐색 및 페이지 레이아웃**: 중요한 정보에 액세스하기 위한 클릭 수를 줄이기 위해 탐색 모음 및 페이지 레이아웃이 향상되었습니다.
- **국제화**: 로케일별 항목(예: 날짜/시간 형식, 숫자 형식, 표준 시간대)에 대한 처리 기능이 향상되었습니다.

참고: 버전 2.3에서 도입된 NSX Policy Manager의 네트워크 토폴로지 시각화 기능은 이 릴리스에서 더 이상 사용되지 않습니다.

방화벽

NSX-T Data Center 2.4부터는 분산 방화벽 및 게이트웨이 방화벽이 IPv6 트래픽 필터링을 지원합니다. 또한 제품에 다음과 같이 다양한 작동 기능이 추가되었습니다.

게시/되돌리기 버튼

전체 방화벽 테이블에 대해 하나의 게시 버튼을 사용할 수 있습니다. 이 버튼은 분산 방화벽 및 게이트웨이 방화벽 모두에 사용할 수 있습니다. NSX-T Data Center 2.4 이전까지는 게시 버튼이 각 세션에 대해 별도로 있었습니다. 이 버튼은 API를 통해 사용할 수 있습니다. 또한 변경 내용을 되돌리는 옵션도 있습니다. 뿐만 아니라 변경 내용이 업데이트될 때 섹션을 잠그는 옵션도 있습니다.

규칙 통계

각 규칙에는 적중 수, 패킷 수, 세션 수, 바이트 수 및 인기도 인덱스가 포함됩니다. 또한 적중 수 대비 최대값도 표시됩니다. 버튼 하나로 이 통계를 재설정할 수 있습니다.

그룹화 기능 향상

VM 및 Active Directory 그룹에 대해 운영 체제를 기반으로 하는 추가적인 그룹화 기준을 사용할 수 있습니다.

VM별 규칙 가시성

모든 가상 시스템에 대한 논리적 스위치 포트 연결을 확인하여 특정 VM에 대한 방화벽 규칙을 나열할 수 있습니다.

가상 시스템에 대한 IP 검색

ARP 스누핑 및 DHCP 스누핑 외에 VMTools 기반 IP 검색도 포함하도록 기본 IP 검색 프로파일이 업데이트되고 있습니다. 이전 릴리스에서 업그레이드하는 고객은 VMTools 기반 감지 기능을 사용하도록 IP 검색 프로파일을 업데이트해야 합니다. NSX-T 2.4에서는 글로벌 IP 검색 프로파일을 생성하는 기능도 지원됩니다. 또한 다음과 같은 변경 사항도 있습니다.

1. DHCPv6 및 Neighbor Discovery 메커니즘에 기반한 IPv6 IP 검색을 사용할 수 있습니다.
2. IPv6 검색은 기본적으로 사용하지 않도록 설정됩니다.
3. 자동 검색된 IP 바인딩을 수동으로 허용 목록에 포함하거나 무시 목록에 포함할 수 있습니다.
4. 로컬 링크 IPv4 주소는 기본적으로 무시됩니다.

ID 기반 방화벽

NSX-T Data Center 2.4에서는 분산 방화벽에 대해 ID(사용자 ID) 기반 규칙을 사용합니다. 방화벽 관리자는 이제 Active Directory 기반 그룹에 기반하여 가상 시스템에 분산 규칙을 구성할 수 있습니다. 방화벽 관리자는 이 기능을 사용하여 가상 시스템에 로그인한 사용자를 기반으로 방화벽 규칙을 제공할 수 있습니다. NSX는 로그인/로그오프한 사용자를 자동으로 감지하며, 이를 기반으로 사용자에게 특정 규칙이 사용되도록 설정됩니다. ID 기반 방화벽은 VM당 단일 사용자를 감지하여 규칙을 적용하거나, 동일한 VM에서 특정 세션을 가진 여러 사용자를 추적할 수도 있습니다. 방화벽 관리자는 Active Directory 그룹을 기준으로 NSX-T 그룹을 생성합니다. NSX-T Manager는 제공된 도메인 컨트롤러에서 Active Directory 그룹 목록을 자동으로 검색합니다. 방화벽 관리자는 특히 가상 데스크톱 환경 또는 터미널 서비스를 사용하는 원격 데스크톱 세션에서 사용자의 East-West 액세스를 제어할 수 있습니다.

컨텍스트 인식 분산 방화벽에 대한 L7 애플리케이션 서명

NSX-T Data Center 2.4는 분산 방화벽 규칙에 L7 기반 애플리케이션 서명을 사용할 수 있는 기능을 제공합니다. 사용자는 L3/L4 규칙과 L7 애플리케이션 서명을 함께 사용하거나 L7 애플리케이션 서명 기반 규칙만 생성할 수 있습니다. 현재 애플리케이션 서명과 여러 하위 특성은 서버-서버 또는 클라이언트-서버 통신에 대해서만 지원됩니다. NSX-T Data Center 2.4에서는 ESXi 기반 전송 노드에 대해서만 이 기능을 사용할 수 있습니다.

컨텍스트 인식 분산 방화벽에 대한 FQDN/URL 허용 목록

NSX-T Data Center 2.4에서는 분산 방화벽에 대해 URL/FQDN 허용 목록 기반 규칙을 사용합니다. NSX-T Data Center는 분산 DNS 스누핑을 사용하는 혁신 기술을 도입하여 각 VM의 각 연결이 고유한 URL/FQDN으로 확인됩니다. 방화벽 관리자는 미리 제공된 URL 도메인을 사용하여 분산 방화벽의 규칙에 적용할 수 있습니다. SaaS 서비스나 클라우드 기반 서비스에 액세스하는 하이브리드 애플리케이션은 액세스한 URL을 기반으로 마이크로 세분화할 수 있습니다. SaaS 애플리케이션에 액세스하는 클라이언트 애플리케이션 또는 브라우저에 대해 더 세부적으로 액세스 권한을 부여할 수 있습니다. NSX-T Data Center 2.4에서는 ESXi 기반 전송 노드에 대해서만 이 기능을 사용할 수 있습니다.

서비스 삽입

NSX-T Data Center 2.4에서는 계층 7 애플리케이션 ID, FQDN 허용 목록 및 ID 기반 방화벽 같이 세부적인 마이크로 세분화를 가능하게 하는 다양한 기본 보안 기능을 사용합니다. 분산 및 게이트웨이 방화벽에 제공되는 기본 보안 제어 기능 외에 NSX 서비스 삽입 프레임워크를 사용하면 토폴로지를 변경하지 않고 IDS/IPS, NGFW 및 네트워크 모니터링 솔루션 같은 다양한 유형의 파트너 서비스를 데이터 경로에 투명하게 삽입하고 NSX 내에서 사용할 수 있습니다.

NSX-T Data Center 2.4에서는 서비스 삽입 기능이 이제 East-West 트래픽(예: 데이터 센터에 있는 VM 간의 트래픽)을 지원합니다. 데이터 센터에 있는 VM 간의 모든 트래픽을 파트너 서비스의 동적 체인으로 리디렉션할 수 있습니다.

E-W 서비스부는 서비스 체인에서 정책에 기반하여 트래픽을 리디렉션 할 수 있는 고유한 전달 메커니즘을 제공합니다. 플랫폼에서는 장애 감지, 기존 또는 새 흐름 리디렉션, 상태 저장 서비스 지원을 위한 흐름 고정, 처리량/지연 시간 또는 밀도 최적화를 위한 여러 경로 선택 정책 제공 등 서비스부에서의 전달을 완전히 자동화합니다.

Guest Introspection

NSX-T Data Center 2.4에서는 VMware 파트너를 위한 Guest Introspection 서비스 플랫폼을 도입하여 vSphere ESXi 하이퍼바이저에서 Windows 기반 게스트 VM 워크로드에 대해 정책 기반의 에이전트 없는 바이러스 백신 및 멀웨어 방지 오프로드 기능을 제공합니다.

NSX-T Data Center 2.4에서 Guest Introspection 플랫폼은 다음과 같은 이점을 제공합니다.

- Guest Introspection 배포를 NSX 에이전트 호스트 준비 설치에 통합하고, 더 이상 Guest Introspection 범용 서비스 VM을 각 ESXi 하이퍼바이저에 배포할 필요가 없게 하여 배포 및 수명주기 관리를 간소화합니다.
- 여러 vCenter에 일관된 정책 기반 서비스를 제공합니다.
- 파트너 SVM 크기 조정(예: "소형", "중형", "대형" 파트너 장치)을 통해 VMware 파트너 규모 지정 기능을 개선합니다.

L2 네트워킹

호스트당 여러 N-VDS 지원

호스트당 여러 N-VDS를 지원할 수 있는 이 새로운 기능은 VM 트래픽을 구성할 때 유연성을 제공하는 것 이외에도 VM 트래픽의 엄격한 격리가 요구되는 PCI 규정의 준수를 용이하게 합니다.

이 기능이 추가되어 이제 ENS 업링크를 비 ENS 업링크와 구분할 수 있습니다. 현재 N-VDS에서는 ENS에 대해 이와 같은 기능이 없어 ENS를 사용하는 워크로드가 빠른 속도에 비해 기능이 많지 않기 때문에 이는 매우 유용한 기능입니다.

N-VDS 시각화

이 기능을 사용하면 드릴다운하여 연결된 호스트를 보는 등 N-VDS를 독립형 개체로 관리할 수 있습니다. 특정 호스트를 볼 때 해당 호스트가 N-VDS에 어떻게 연결되었는지 나와 있는 UI 그리드를 볼 수 있습니다. VM 커널 인터페이스 같은 논리적 인터페이스도 N-VDS의 일부로 표시됩니다. 이는 호스트 보기에 비해 크게 향상된 것으로, 모든 물리적 NIC, VM 커널 인터페이스 및 모든 OVS 포트가 포함된 인터페이스 목록을 보기 하나에 보여 줍니다.

물리적 NIC에 대해 LLDP 지원

이 기능은 NSX에 대해 LLDP 구현의 격차를 줄이는 데 도움이 됩니다. 이 기능은 물리적 스위치 연결에 대한 디버깅 기능을 제공합니다. 호스트의 인터페이스에 연결된 물리적 포트를 파악하여 케이블 연결 문제를 쉽게 해결할 수 있습니다. 이 기능의 범위는 NSX 데이터부에 참여하는 모든 물리적 호스트(ESXi, KVM, 베어메탈 Linux 호스트 및 베어메탈 Edge)에 적용됩니다.

Edge 노드에서 프록시 ARP 지원

외부 클라이언트가 동일한 서브넷 주소를 가진 LB, IKE 등의 서비스에 액세스할 경우 장치 라우팅이 실행됩니다. 이러한 클라이언트는 루프백 포트에 바인딩된 해당 주소에 대해 ARP 쿼리를 보내지만 LR 루프백 포트는 MAC 주소가 없기 때문에 이러한 ARP 쿼리에 응답하지 않습니다. 이 경우 액세스 문제가 발생합니다.

현재 해결 방법은 루프백 IP/32 → 업링크/CSP 같이 클라이언트에서 /32 라우팅을 구성하여 트래픽을 업링크/CSP 포트에 전달하는 것입니다. 그러면 트래픽이 올바른 루프백 포트에 이동합니다. ARP 프록시는 이 단점을 해결하는 데 적합한 솔루션입니다.

L3 네트워킹

MTU 구성 기능 향상

NSX-T 2.4는 다음의 두 가지 새로운 MTU 글로벌 매개 변수를 제공합니다.

- NSX 도메인에 있는 모든 N-VDS 인스턴스의 MTU를 구성하는 글로벌 물리적 업링크 MTU. 이 매개 변수는 GENEVE 캡슐화 프레임의 최대 프레임 크기 또는 TEP MTU로 변환될 수 있습니다.
 - 업링크 프로파일 MTU는 특정 호스트의 글로벌 물리적 업링크 매개 변수를 재정의할 수 있습니다.
- 모든 논리적 라우터 인터페이스의 MTU를 구성하는 글로벌 논리적 인터페이스 MTU
 - 필요한 경우, 논리적 라우터 업링크 MTU 및 CSP 포트 MTU가 특정 포트에서 글로벌 논리적 인터페이스 MTU를 재정의할 수 있습니다.

이러한 글로벌 매개 변수를 사용하면 East-West 및 North-South 트래픽에 대해 MTU가 1500바이트보다 크게 구성된 VM의 종단 간 통신이 가능합니다.

서비스 라우터 간 라우팅

이제 활성/활성 모드의 Tier0 논리적 라우터가 지정된 Tier0 논리적 라우터의 모든 SR(서비스 라우터) 부분 간에 폴메시 iBGP 피어링을 자동으로 설정할 수 있습니다. 따라서 여러 개의 업링크로 구성된 SR 중 하나에서 장애가 발생한 경우에 트래픽이 삭제되는 것을 방지할 수 있습니다. 이 시나리오에서 장애가 발생한 SR은 자체 업링크를 사용하여 대상에 연결할 수 없으면 다른 SR에 트래픽을 전달합니다.

DNS 전달자 기능 향상

- 이제 현재 구성의 손실 없이 DNS 전달자 기능을 사용하거나 사용하지 않도록 설정할 수 있습니다.
- DNS 전달자 기능은 API 및 UI를 통해 통계, 이벤트 및 경보도 표시합니다.

업링크 간에 SNAT 지원

NSX-T 2.4에서는 업링크를 통해 Tier0 논리적 라우터에 진입한 후 다른 업링크를 통해 동일한 논리적 라우터에서 나가는 트래픽에 대해 SNAT(Source Network Address Translation)를 지원합니다. 이 기능은 Tier0 논리적 라우터 여러 개가 상호 연결되어 있는 경우에 유용합니다.

Tier0 논리적 라우터에서 프록시 ARP 지원

NSX-T 2.4에서는 Tier0 논리적 라우터 업링크에 대해 프록시 ARP를 지원합니다. 이를 통해 Tier0 논리적 라우터의 노스바운드 라우터에 라우팅을 구성할 수 없는 환경에 NSX-T를 배포할 수 있습니다. 이 기능을 사용하면 NAT, LB 또는 모든 상태 저장 서비스를 Tier0 업링크의 네트워크에 속해 있는 IP 주소로 구성할 수 있습니다.

Edge 노드 기능 향상

- NSX-T 2.4에서는 베어메탈 Edge 노드에서 빠른 경로 NIC 관리 옵션을 사용할 수 있기 때문에 전용 관리 NIC가 더 이상 필요하지 않습니다.
- 베어메탈 Edge 노드는 25Gbps Intel NIC XXV710도 지원합니다.
- Edge 노드는 여러 개의 GENEVE TEP(터널 끝점)을 지원합니다. 따라서 Edge 노드에서 오버레이 트래픽의 고가용성을 위해 LAG를 강제로 사용하지 않아도 됩니다.

BGP 기능 향상

- NSX-T 2.4부터는 Tier0 논리적 라우터가 노스바운드 물리적 라우터와의 iBGP 피어링을 지원합니다.
- NSX-T 2.4에서는 서로 다른 ASN에 있는 eBGP 피어 사이에 ECMP를 사용하도록 설정하는 옵션(as-path multipath relax)을 사용할 수 있으며, Tier0 논리적 라우터가 자체 ASN을 AS-path에 사용하는 기능(allow-as in)도 지원됩니다.

IPv6

NSX-T 2.4에서는 IPv6 라우팅/전달 및 보안을 사용할 수 있습니다. 다음과 같은 기능이 포함됩니다.

- IPv6 정적 라우팅
- IPv6 Neighbor Discovery
- DHCPv6 릴레이
- IPv6 DFW(분산 방화벽)
- IPv6 Edge 방화벽
- MP-BGP 및 관련 prefix-list/route-map에 대한 IPv6 address-family
- IPv6 스위치 보안
- IPv6 주소 검색
- IPv6 ops 도구

작업

Traceflow 기능 향상

Traceflow는 훨씬 더 많은 문제 해결 및 시각화 기능을 지원합니다. NSX-T 2.4에서 Traceflow는 Edge 방화벽, 로드 밸런서, NAT 및 경로 기반 VPN 같은 중앙 집중식 서비스에 대한 관찰 기능을 제공합니다.

설치 기능 향상

- NSX를 사용하면 vSphere 계산 클러스터에 대해 새로운 프로파일 기반 NSX 구성 요소 설치를 통해 배포를 간소화할 수 있습니다. 이 기능은 배포 시간을 단축하고, 구성 일관성을 높이고, 수동 작업 시 발생하는 오류를 방지하며, "한 번 정의하여 여러 번 다시 사용"할 수 있는 방법을 제공합니다.
- UI에서 NSX Manager 노드의 자동 설치 및 클러스터링 기능을 지원합니다.
- 프로파일을 통해 VMKernel 포트 및 물리적 어댑터를 마이그레이션하고 여러 N-VDS 스위치를 생성할 수 있는 추가적인 배포 구성을 지원합니다.

업그레이드 기능 향상

- 기본 유지 보수 모드 NSX 업그레이드를 사용하여 호스트를 재부팅하는 비용 없이 ESXi 호스트에 대해 완전하게 조정된 업그레이드를 제공하도록 기능이 향상되었습니다.

- "인플레이스" 업그레이드라고 하는 새로운 NSX 업그레이드 모드를 사용할 수 있습니다. 이 기능은 운영을 간소화하고 더 빠르게 업그레이드할 수 있도록 지원합니다. 이 모드를 사용하면 워크로드의 전원을 끄거나 워크로드를 다른 하이퍼바이저로 마이그레이션할 필요 없이 ESXi 호스트의 NSX 구성 요소가 업그레이드됩니다.
- 새로운 프레임워크를 사용할 수 있으며 NSX 업그레이드 중에 사전 검사 및 사후 검사를 수행할 수 있는 즉시 사용 가능한 테스트가 제공됩니다. 이 테스트는 실제 업그레이드를 시작하기 전 또는 업그레이드를 수행한 직후에 유틸리티 기본 문제를 강조 표시하는 데 도움이 됩니다.

변경 감지 시 NSX 백업

NSX는 구성 변경 사항을 감지하고 이를 사전 예방적으로 보안 스토리지에 백업하는 기능을 제공하여 재해 복구 솔루션을 개선합니다. 이 기능을 통해 고객은 스토리지 서버에 불필요한 파일을 백업하는 비용을 들이지 않으면서 더 효율적인 구성 백업 SLA를 적용할 수 있습니다.

NFV

이제 N-VDS 스위치가 EDP 모드에서 다음과 같이 향상된 기능을 지원합니다.

- 분산 방화벽
- IP 검색
- Spoof guard
- IPFIX
- IPv6
- EDP 모드보다 최대 5배 더 높은 처리량을 제공하여 Edge VM의 성능 향상
- 멀티홈 애플리케이션에 대한 경로 이중화. VM을 특정 업링크에 고정할 수 있는 기능을 통해 VTEP를 사용하는 NSX에 멀티홈 이중화 경로를 구축할 수 있습니다.

작업 - AAA/RBAC 및 플랫폼 보안

작업

- **주체 ID 기능 향상:** 주체 ID 사용자가 NSX 구성 요소를 등록 및 설치할 수 있습니다. 주체 ID 사용자 생성 및 역할 할당을 위한 UI 지원이 추가되었습니다.
- **암호 정책 기능 향상:** 기본 암호에 최소 암호 길이(12자)를 적용합니다. 암호 만료 시간을 설정하고, 암호가 만료일에 임박할 때 경보를 생성하는 기능이 도입되었습니다. 기본적으로 암호는 90일 후에 만료됩니다. 암호 재설정 및 암호 만료 조정에 대한 지침은 기술 자료 문서 [70691](#)을 참조하십시오.
- **인증서 관리:** 인증서 해지 상태를 확인할 수 있는 기능이 추가되었습니다.

VPN

NSX-T 2.4에는 VPN 서비스에 대해 다음과 같은 기능이 추가되었습니다.

- 정책 API 및 GUI를 L3 VPN 서비스와 L2 VPN 서비스 모두에 사용할 수 있습니다.
- L3 VPN 서비스는 더 나은 보안 관리를 위해 인증서 기반 인증을 지원합니다.
- L2 VPN 클라이언트 모드를 사용하여 NSX-T SDDC에서 NSX-T SDDC로의 L2 확장을 지원할 수 있습니다.
- DH 그룹 19, 20 및 21을 사용하여 높은 수준의 보안 요구 사항을 충족할 수 있습니다.

로드 밸런싱

NSX-T 2.4에는 로드 밸런싱 서비스에 대해 다음과 같은 기능이 추가되었습니다.

- 정책 API 및 새로운 GUI를 사용할 수 있습니다. 이전 로드 밸런서 GUI는 [고급 네트워킹 및 보안] 탭에서 계속 사용할 수 있습니다.
- 독립 실행형 SR의 VIP가 CSP(중앙 집중식 서비스 포트)와 같은 서브넷에 속할 수 있습니다. 이전 릴리스에서는 CSP 네트워크와 동일한 서브넷에 VIP를 생성하려면 VIP에 CSP IP 주소를 사용해야 했습니다. 그렇지 않으면 다른 네트워크에 VIP를 생성해야 했습니다.
- 동일한 Tier 1 게이트웨이의 로드 밸런서 트래픽 흐름에 대해 DNAT 및 Edge 방화벽이 지원됩니다. 이전 릴리스에서는 로드 밸런서 트래픽 흐름이 Edge 방화벽을 우회했습니다.
- LB 규칙에 "_"로 시작하는 HTTP 헤더가 지원됩니다. 향상된 이 기능을 통해 vIDM 및 AirWatch에 대해 NSX

- 로드 밸런서를 배포할 수 있습니다.
- VIP를 LB SNAT의 소스 IP 주소로 사용할 수 있습니다.
- HTTP 응답 헤더의 최대 크기를 64KB까지 구성할 수 있습니다. 기본 크기는 이전 릴리스와 마찬가지로 4KB입니다.
- 대규모 Edge VM이 대규모 LB 인스턴스를 지원합니다. 이전 릴리스에서는 대규모 Edge VM이 중간 규모 LB 인스턴스까지 지원했습니다.

NSX Data Center for vSphere에서 NSX-T Data Center로의 마이그레이션

NSX-T 2.4에서는 이제 NSX Data Center for vSphere에서 NSX-T Data Center로 마이그레이션하는 데 마이그레이션 조정기를 사용할 수 있습니다. 이 기능은 vMotion을 사용하지 않고 기존 호스트를 마이그레이션하도록 설계되었습니다. 마이그레이션 조정기는 계층 2 네트워킹, 계층 3 네트워킹, 방화벽, 로드 밸런싱 및 VPN을 지원합니다. *NSX-T Data Center Migration Coordinator Guide*에서는 이 도구에 대한 자세한 정보를 제공합니다.

NSX-T Manager 및 Edge 노드의 배포 이외에는 추가적인 계산 리소스가 필요하지 않습니다. 마이그레이션이 완료되면 고객이 NSX for vSphere 및 연결된 Manager, Controller 및 Edge를 제거할 수 있습니다. 이 마이그레이션은 데이터부 트래픽에 영향을 주지 않으며 하나의 변경 창에서 완료할 수 있도록 설계되었습니다.

자동화, OpenStack 및 기타 CMP

NSX-T 2.4에서는 Neutron 플러그인을 통해 OpenStack에 대해 다음과 같은 기능을 사용할 수 있습니다.

- Rocky 및 Queen 지원
- 관리부 클러스터링 지원
OpenStack Neutron 플러그인은 이 새로운 기능을 활용하여 관리자 클러스터를 구축할 수 있습니다. 이 플러그인은 추가적인 성능 또는 고가용성을 위한 외부 VIP 없이 세 가지 관리자 REST API 끝점을 사용할 수 있습니다.
- Barbican 지원
OpenStack Neutron 플러그인은 이제 Barbican을 지원합니다. Barbican은 암호, 암호화 키 및 X.509 인증서 같은 비밀을 안전하게 저장, 프로비저닝 및 관리하기 위해 설계된 REST API입니다. 이를 통해 HTTPS 종료를 위해 Load Balancer as a Service에 대한 인증서를 관리할 수 있습니다. 이 기능은 현재 VIO 환경에서만 지원됩니다.

NSX-T Terraform 제공자는 기존 기능(논리적 스위치, 라우터, 방화벽 규칙 등의 생성) 이외에 다음과 같은 기능을 NSX-T 2.4에 제공합니다.

- 로드 밸런서 및 로드 밸런서 구성(모니터, 풀 등)에 대한 CRUD 지원 기능
- DHCP 서버에 대한 CRUD 지원 기능
- NSX-T IPAM(IP 블록, IP 풀)에 대한 CRUD 지원 기능

NSX Cloud

NSX Cloud용 NSX-T 2.4는 고객의 제품 채택/배포를 용이하게 하고, 고객이 서비스 삽입, VPN 종료, VDI 환경 관리를 통해 진정한 다중 영역/다중 클라우드 하이브리드 배포 환경을 관리할 수 있도록 더 많은 옵션을 제공하기 위한 여러 가지 새로운 기능을 갖추고 있습니다.

NSX Cloud용 NSX-T 2.4의 주요 기능은 다음과 같습니다.

- 간단하고 빠른 등록 및 통합을 위한 전송 VPC/VNET의 공유 게이트웨이
- 온-프레미스 DC로의 백홀 트래픽을 위한 VPN
- 선택적 North-South 서비스 삽입 및 파트너 통합
- Horizon Cloud for Azure의 마이크로 세분화
- 하이브리드 워크로드를 위한 의도 기반 정책

간소화된 전송 VPC/VNET 아키텍처: 버전 2.4부터 고객은 전송 VPC/VNET에 단일 NSX Cloud 게이트웨이를 설치하고 최대 10개의 계산 VPC/VNET을 관리할 수 있습니다. 이를 통해 허브 및 스포크 전송/계산 아키텍처가 간소화되고, 피어링 연결이 없는 경우에도 계산 VPC 간에 전이적 라우팅이 사용하도록 설정됩니다. NSX 오버레이 터널링을 사용하면 이제 VPC 간 트래픽을 오버레이 터널로 전송할 수 있습니다. 전달 정책은 VM 수준 바로 아래에서 설정하여 트래픽이 Geneve에서 캡슐화된 후 오버레이로 전송되어야 하는지 또는 공용 클라우드 제공자의 언더레이 네트워크에서 전송되어야 하는지를 결정할 수 있습니다. 이러한 모든 기능은 사용자가 공용 클라우드 네트워크에서 또는 외부에서 트래픽을 라우팅할 때 보다 유연하게 작업할 수 있도록 합니다.

백홀 트래픽을 위한 VPN: NSX Cloud는 이제 공용 클라우드에서 온-프레미스 Data Center로의 백홀 트래픽에 사용할 수 있는 VPN 터널이 기본적으로 지원됩니다. 이제 공용 클라우드의 NSX Cloud 게이트웨이에서 온-프레미스 Data Center의 VPN을 직접 종료할 수 있습니다. 공용 클라우드 벤더가 제공하는 VGW가 더 이상 필요하지 않기 때문에 비용을 절감할 수 있습니다. 뿐만 아니라 NSX Cloud 게이트웨이가 BGP를 통해 경로를 자동으로 전파하기 때문에 관리 오버헤드도 줄어듭니다. BW 관점에서 NSX Cloud는 용량에도 큰 영향을 미칩니다. 즉, VGW를 통해 제공되는 1Gbps에 비해 피어링된 VPC를 통해 5Gbps의 VPC 간 트래픽 흐름이 지원됩니다.

선택적 North-South 서비스 삽입 및 파트너 통합: 고객이 파트너 서비스를 공용 클라우드 마켓플레이스에서 직접 공유 서비스/전송 아키텍처에 직접 배포할 수 있습니다. 전송 VPC/VNET에 있는 NSX Cloud 게이트웨이를 프로그래밍하여 NSX 정책에 따라 파트너 서비스 장치에 트래픽을 선택적으로 라우팅할 수 있습니다. 이를 통해 고객은 공용 클라우드용으로 구입한 가상 L7 방화벽 장치(통과하는 트래픽에 따라 비용이 청구됨)로 모든 트래픽을 리디렉션하지 않아도 되기 때문에 막대한 비용 절감 효과를 얻을 수 있습니다. 뿐만 아니라 NSX Cloud를 사용하여 서비스를 삽입할 경우 계산 VPC/VNET에 VPN이 필요하지 않습니다. 결과적으로 비용 절감 효과는 높이고 운영 부담은 줄일 수 있습니다.

Horizon Cloud for Azure의 마이크로 세분화: NSX Cloud는 이제 Horizon Cloud for Azure와 결합된 솔루션을 제공합니다. Azure에 Horizon VDI 환경을 구축하려는 고객을 위해 NSX Cloud는 필요한 마이크로 세분화 기능을 제공하여 VDI 환경을 보호합니다.

하이브리드 워크로드를 위한 의도 기반 정책: CSM(Cloud Service Manager)이 이제 NSX Manager에 통합되었습니다. 이제 고객은 워크로드가 배포된 위치나 향후에 이동할 위치에 대해 걱정할 필요 없이 Policy Manager에서 의도 기반 정책을 하나만 정의하면 됩니다. 그러면 NSX Cloud가 온-프레미스 DC, Azure 및 AWS에서 이 정책을 일관된 방식으로 적용합니다.

호환성 및 시스템 요구 사항

호환성 및 시스템 요구 사항에 대한 자세한 내용은 [NSX-T Data Center 설치 가이드](#)를 참조하십시오.

API 및 CLI 리소스

자동화를 위해 NSX-T Data Center API 또는 CLI를 사용하려면 code.vmware.com을 참조하십시오.

API 설명서는 **API 참조** 탭에서 사용할 수 있습니다. CLI 설명서는 **설명서** 탭에서 사용할 수 있습니다.

문서 개정 이력

2019년 2월 28일. 초판.

2019년 4월 2일. 2차 버전입니다. 알려진 문제를 추가함: 2273651, 2279326, 2281095, 2296888. 해결된 문제를 추가함: 2199785.

2019년 4월 10일. 3차 버전입니다. 알려진 문제를 추가함: 2203863, 2248186, 2252738, 2277543, 2276398, 2279326, 2281537, 2287124, 2290688, 2294178, 2295592, 2296430, 2297157, 2297918 및 2298499. 단일 클러스터 설계에 대한 지원을 포함하도록 새로운 기능 섹션을 업데이트했습니다.

2019년 6월 20일. 4차 버전입니다. 알려진 문제 2261818을 추가함. 해결된 문제 2182745를 추가함.

2019년 8월 23일. 5차 버전입니다. 알려진 문제 2362688, 2395334, 및 2392093을 추가함.

해결된 문제

- **해결된 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.
- **해결된 문제 2279326: 5개 이상의 IP 포트 조합이 있는 IPFIX L2 수집기를 생성할 때 오류가 표시되지 않음**
허용되는 IP 포트 조합의 최대 수에 대해 오류 메시지가 표시되지 않습니다. 최대 제한을 초과할 경우 UI가 태그 생성을 제한하므로 큰 문제는 없습니다.
- **해결된 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.
- **해결된 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.
- **해결된 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.
- **해결된 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.
- **해결된 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.
- **해결된 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.
- **해결된 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.
- **해결된 문제 2114756: NSX-T 준비 클러스터에서 호스트를 제거할 때 VIB가 제거되지 않는 경우가 있음**
NSX-T 준비 클러스터에서 호스트를 제거할 때 일부 VIB가 호스트에 남아 있을 수 있습니다.
- **해결된 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.
- **해결된 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.

- **해결된 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.
- **해결된 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.
- **해결된 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.
- **해결된 문제 2099530: 브리지 노드 VTEP IP 주소를 변경하면 트래픽이 중단됨**
브리지 노드 VTEP IP 주소가 변경되면 VLAN에서 오버레이로의 MAC 테이블이 원격 하이퍼바이저에서 업데이트되지 않아서 트래픽 중단이 최대 10분까지 발생합니다.
- **해결된 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.
- **해결된 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.
- **해결된 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.
- **해결된 문제 2186040: 전송 노드가 시스템의 상위 250개 업링크 프로파일에 없는 경우 물리적 NIC의 업링크 드롭다운이 사용자 인터페이스에서 사용되지 않도록 설정됨**
전송 노드가 시스템의 상위 250개 업링크 프로파일에 없는 경우 물리적 NIC의 업링크 드롭다운이 사용자 인터페이스에서 사용되지 않도록 설정됩니다. 전송 노드 결과를 저장하면 전송 노드에서 업링크 이름이 제거됩니다.
- **해결된 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.
- **해결된 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.
- **해결된 문제 2128361: NSX Manager의 로그 수준을 디버그 모드로 설정하는 CLI 명령이 제대로 작동하지 않음**
CLI 명령 set service manager logging-level debug를 사용하여 NSX Manager의 로그 수준을 디버그 모드로 설정해도 디버깅 로그 정보가 수집되지 않습니다.
- **해결된 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.
- **해결된 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.

- **해결된 문제 2199785: 상태 모니터(포트 번호 없음)를 동적 풀(포트 번호 있음)에 추가할 때 NGINX 코어가 나타남**
동적 멤버(포트 번호 있음)가 있는 서버 풀로 로드 밸런싱을 구성한 다음, 모니터링 포트가 구성되지 않은 상태 모니터를 연결하려고 하면 nginx가 충돌할 수 있습니다.
- **해결된 문제 2182745: 재배포 규칙의 이전 le/ge가 Manager에서 검증되지 않아 제대로 작동하지 않음**
재배포 규칙은 prefixlist에서 le/ge를 지원합니다.

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

일반적인 알려진 문제

- **문제 2239365: "권한 없음" 오류가 발생함**
이 오류는 사용자가 동일한 유형의 브라우저에서 인증 세션을 여러 개 열려고 시도하는 경우에 발생할 수 있습니다. 그 결과, 위의 오류와 함께 로그인에 실패하고 인증을 진행할 수 없습니다. 로그 위치:
`/var/log/proxy/reverse-proxy.log /var/log/syslog`

해결 방법: 열려 있는 모든 인증 창/탭을 닫고 인증을 다시 시도합니다.
- **문제 2287482: 자동 검색된 바인딩 테이블에 현재 검색되지 않은 바인딩이 포함될 수 있음**
자동 검색된 바인딩 테이블에 "중복됨"으로 표시된 바인딩이 더 이상 검색되지 않을 수 있습니다.

해결 방법: 없음.
- **문제 2278142: 스위치 IPFIX 글로벌 프로파일을 편집할 수 없음**
시스템에서 글로벌 프로파일을 사용할 수 있는 경우 글로벌 프로파일에 대한 워크플로가 없으므로 인터페이스를 통해 글로벌 프로파일을 수정하거나 삭제할 수 없습니다.

해결 방법: API를 사용하여 이러한 글로벌 프로파일을 삭제합니다.
- **문제 2292222: [오류 해결] 화면에서 지문이 올바르지 않으면 사용자에게 알림이 전송되지 않음**
호스트 준비가 실패한 경우, 사용자는 [NSX 설치 실패]를 클릭한 후 사용자 이름, 암호 및 호스트 지문을 제공하여 문제를 해결할 수 있습니다. 사용자가 잘못된 지문을 제공하면 시스템에서 사용자에게 알림을 전송하지 않고, 문제가 해결되지 않은 상태로 남아 있습니다.

지문이 잘못되었음을 알 수 있는 확실한 방법은 없습니다. 이 ThumbPrintValidationFailedException이 기록된 로그를 확인해야 합니다.

해결 방법: 올바른 지문을 제공합니다.
- **문제 2252487: 여러 TN를 병렬로 추가할 경우 BM Edge 전송 노드에 대해 전송 노드 상태가 저장되지 않음**
전송 노드 상태가 MP UI에 올바르게 표시되지 않습니다.

해결 방법:

1. 모든 전송 노드 상태가 올바르게 업데이트되도록 Proton을 재부팅합니다.
2. 또는 API <https://<nsx-manager>/api/v1/transport-nodes/<node-id>/status?source=realtime>을 사용하여 전송 노드 상태를 쿼리합니다.

● 문제 2285117: NSX 관리 VM에서 커널 업그레이드가 지원되지 않음

일부 Linux Ubuntu 마켓플레이스 이미지에서 VM이 재부팅된 후 커널이 자체적으로 자동 업그레이드됩니다. 그 결과 nsx-agent가 예상대로 작동하지 않습니다. NSX 에이전트가 작동하는 것처럼 보일 수 있지만 인식되지 않은 일부 네트워킹 정책이 nsx-agent에 영향을 줄 수 있습니다. 에이전트가 이러한 정책을 반복적으로 인식하려고 시도하여 CPU 사용량이 증가합니다.

해결 방법: 커널 업그레이드가 필요한 경우, 해당 최신 커널에 대한 Linux-header를 먼저 다운로드하고 openvswitch 데이터 경로 dkms 패키지를 다시 컴파일해야 합니다.

● 문제 2285544: ssh_fingerprint 값을 지정해야 하는 NSX API를 호출할 때 MD5 해시가 더 이상 지원되지 않음

NSX-T 2.4에서는 백업/복원, file-store 및 지원 번들 NSX API를 호출하고 ssh_fingerprint 값으로 MD5 해시를 지정해야 하는 비 FIPS 암호화 알고리즘, 해시 등을 더 이상 지원하지 않습니다. 그 결과 MD5 해시도 더 이상 지원되지 않습니다.

해결 방법: 다른 해시 알고리즘을 사용하여 계산된 다른 해시를 지정하십시오(예: SHA256).

● 문제 2256709: 인스턴트 클론 VM 또는 스냅샷에서 되돌린 VM에 대한 AV 보호 기능이 vMotion 중에 잠시 중지됨

VM의 스냅샷이 되돌려지고 VM이 다른 호스트에 마이그레이션됩니다. 마이그레이션된 인스턴트 클론 VM에 대한 AV 보호가 파트너 콘솔에 표시되지 않습니다. AV 보호가 잠시 중지됩니다.

해결 방법: 없음.

● 문제 2261431: 다른 배포 매개 변수에 따라서 필터링된 데이터스토어 목록이 필요할 수 있음

잘못된 옵션을 선택한 경우 UI에 적절한 오류가 표시됩니다. 이 배포를 삭제한 후 새 배포를 생성하여 이 오류를 해결할 수 있습니다.

해결 방법: 클러스터링된 배포를 생성하는 경우, 공유 데이터스토어를 선택합니다.

● 문제 2266553: NSX 장치에서 서비스를 처음 부팅할 때 서비스가 초기화되지 않을 수 있음

배포된 노드가 요청을 처리할 수 없거나, 클러스터를 구성하지 못합니다.

해결 방법: 실패한 서비스를 다시 시작합니다.

● 문제 2267632: GI 보호 구성 손실

정책 UI에 게시된 게스트 보호 규칙이 [성공]으로 표시됩니다. 해당 동작의 변경 사항이 게스트 VM에 반영되지 않습니다. OpsAgent 로그에 동시에 다시 시작이 표시됩니다. 게스트 VM 보호가 손실됩니다.

해결 방법: 구성 변경 사항을 수동으로 재생합니다.

● 문제 2269901: vmk 인터페이스가 패킷 캡처 CLI에 포함되지 않음

이 명령을 실행할 수 없습니다.

해결 방법: 패킷 캡처 uw를 사용하여 같은 작업을 수행합니다.

● 문제 2274988: 서비스 체인이 동일한 서비스의 연속 서비스 프로파일을 지원하지 않음

체인에 동일한 서비스에 속해 있는 서비스 프로파일이 연속으로 2개 있으면 서비스 체인에서 트래픽이 이동하지 않고 삭제됩니다.

해결 방법: 동일한 서비스에 속한 서비스 프로파일 2개가 연속으로 나오지 않도록 다른 서비스에 속해 있는 서비스 프로파일을 추가합니다. 또는 원래 서비스 프로파일 2개를 연결한 것과 동일한 작업을 수행하는 또 다른 서비스 프로파일을 정의한 후 이 프로파일만 서비스 체인에서 사용합니다.

● 문제 2275285: 첫 번째 요청이 완료되고 클러스터가 안정화되기 전에 노드가 동일한 클러스터에 대한 두 번째 가입 요청을 생성함

클러스터가 제대로 작동하지 않고, get cluster status 및 get cluster config CLI 명령이 오류를 반환할 수 있습니다.

해결 방법: 첫 번째 가입 요청 이후 동일한 클러스터에 대해 새로운 join 명령을 10분 동안 실행하지 마십시오.

- **문제 2275388: 경로를 거부하는 필터가 추가되기 전에 루프백 인터페이스/연결된 인터페이스 경로가 재배포될 수 있음**
불필요한 경로 업데이트 때문에 트래픽이 몇 초부터 몇 분까지 분산될 수 있습니다.

해결 방법: 없음.

- **문제 2275708: 개인 키에 암호가 있으면 개인 키를 사용하여 인증서를 가져올 수 없음**
"인증서에 대해 잘못된 PEM 데이터를 받았습니다 (오류 코드: 2002)."라는 메시지가 반환됩니다. 개인 키를 사용하여 새 인증서를 가져올 수 없습니다.

해결 방법:

1. 개인 키를 사용하여 인증서를 생성합니다. 메시지가 표시될 때 새 암호를 입력하지 말고 대신 Enter 키를 누릅니다.
2. "인증서 가져오기"를 선택하고, 인증서 파일과 개인 키 파일을 선택합니다.
key-file 파일을 열어 확인합니다. 키를 생성할 때 암호를 입력한 경우, 파일의 둘째 줄에 "Proc-Type: 4,ENCRYPTED" 같은 내용이 표시됩니다.

암호 없이 key-file 파일을 생성한 경우에는 이 줄이 없습니다.

- **문제 2275985: 논리적 스위치에 연결되어 있지 않은 VNIC가 NSGroup 직접 멤버 옵션으로 나열됨**
논리적 스위치에 연결되어 있지 않은 VNIC가 NSGroup의 직접 멤버로 추가됩니다. 작업이 성공하지만 해당 그룹에 적용된 정책이 VNIC에 적용되지 않습니다.

해결 방법: 없음.

VNIC를 NSGroup의 직접 멤버로 추가하기 전에 해당 VNIC가 논리적 스위치에 연결되어 있는지 확인합니다.

- **문제 2277742: PUT https://<MGR_IP>/api/v1/configs/management를 호출할 때 publish_fqdns를 true로 설정하는 요청 본문을 포함할 경우, NSX-T Manager 장치가 호스트 이름 대신 FQDN(정규화된 도메인 이름)을 사용하여 구성되어 있으면 작업이 실패할 수 있음**
FQDN이 구성되어 있으면 PUT https://<MGR_IP>/api/v1/configs/management를 호출할 수 없습니다.

해결 방법: FQDN 대신 호스트 이름을 사용하여 NSX Manager를 배포합니다.

- **문제 2279249: vMotion 중에 인스턴트 클론 VM의 AV 보호가 잠시 중지됨**
인스턴트 클론 VM을 호스트 하나에서 다른 호스트로 마이그레이션합니다. 마이그레이션 직후 eicar 파일이 VM에 그대로 남아 있습니다. AV 보호가 잠시 중지됩니다.

해결 방법: 없음.

- **문제 2290669: 가상 서버의 수가 증가하면 각 가상 서버의 구성 시간이 증가함**
가상 서버 수가 증가하면 검증 횟수가 많아져서 각 가상 서버의 구성 시간이 증가합니다. 처음 100개의 가상 서버에 대해서는 평균 응답 시간이 1초 정도입니다. 가상 서버가 250개를 초과하면 평균 응답 시간이 5-10초로 증가합니다. 가상 서버가 450개를 초과하면 평균 응답 시간이 30초 정도로 증가합니다.

해결 방법: 없음. 토폴로지에 따라 가상 서버를 여러 LbService로 구성할 수도 있습니다. 그렇지 않은 경우, 가상 서버로 대규모 설정을 구성하면 응답 시간이 길어질 수 있습니다.

- **문제 2292116: IPFIX L2 페이지를 통해 그룹을 생성한 경우, CIDR 기반 IP 주소 그룹을 사용하여 적용된 IPFIX L2가 UI에 나열되지 않음**
[적용 대상] 대화상자에서 IP 주소 그룹을 생성할 때 [멤버 설정] 대화상자에 잘못된 IP 주소나 CIDR을 입력하면 해당 멤버가 그룹에 나열되지 않을 수 있습니다. 그룹을 다시 편집하여 올바른 IP 주소를 입력해야 합니다.

해결 방법: 그룹 목록 페이지로 이동하여 해당 그룹에 IP 주소를 추가합니다. 그러면 이 그룹이 [적용 대상] 대화상자에 채워질 수 있습니다.

- 문제 2294821: 클러스터 모니터링 대시보드에 NSX 장치 정보가 "노드 삭제 실패" 오류와 함께 표시되고, 사용자가 이 상황을 처리할 수 있는 지침은 표시되지 않음

이 문제는 사용자가 자동 배포된 노드를 인터페이스를 통해 삭제하려고 시도한 이후 노드의 전원 끄기가 실패했을 때 나타납니다. 클러스터의 노드가 손실되면 새 노드를 수동으로 추가하고 아래의 해결 방법을 사용하여 구성 상태를 정리해야 합니다.

해결 방법: API/UI를 통한 장치 삭제가 실패하면 다음과 같이 force-delete API를 사용하여 해당 장치를 수동으로 삭제합니다.

POST api/v1/cluster/nodes/deployments/467a102d-472f-4f43-a93c-08b992b9f471?

action=delete&force_delete=true

그런 다음 vCenter에서 해당 VM을 삭제합니다.

- 문제 2281095: SVM이 배포된 호스트를 동일한 클러스터에 다시 추가하면 EAM에서 콜백이 트리거되지 않음
모든 게스트 VM이 보호되지 않을 수 있습니다. NSX UI가 진행 중 상태로 계속 유지됩니다.

해결 방법: 호스트에서 SVM을 제거한 후 클러스터에 추가합니다.

- 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 2261818: eBGP 인접 네트워크에서 확인된 경로가 동일한 인접 네트워크로 다시 보급됨

bgp 디버그 로그를 사용하도록 설정하면 오류 메시지를 나타내며 패킷이 다시 수신된 후 삭제됩니다. BGP 프로세스는 피어에 전송된 업데이트 메시지를 삭제할 때 추가 cpu 리소스를 사용합니다. 많은 수의 경로 및 피어가 있는 경우 경로 컨버전스에 영향을 줄 수 있습니다.

해결 방법: 없음.

설치에 대한 알려진 문제

- 문제 2238093: NSX 패키지를 강제로 제거한 경우 해결 프로그램이 지원되지 않음

호스트에서 NSX를 제거하면 NSX 패키지가 강제로 제거됩니다. 이 경우 NSX 패키지가 손상된 상태가 될 수 있습니다. 해결 프로그램을 사용하기 전에 NSX 패키지를 강제로 제거한 경우에는 NSX 패키지 설치에 대한 해결 프로그램이 제대로 작동하지 않을 수 있습니다. 로그 위치: /var/log/proton/nsxapi.log

해결 방법: 없음.

NSX 패키지를 강제로 제거하지 마십시오. NSX 설명서에 나와 있는 표준 절차에 따라 NSX 구성 요소를 제거해야 합니다.

- 문제 2288872: 설치 상태가 "노드 준비 안 됨"으로 표시됨

Edge 노드가 등록되지 않습니다. 전송 노드 구성 상태가 보류 중으로 표시되어 노드를 Edge 클러스터에 추가할 수 없습니다. 로그 위치: /var/log/proton/nsxapi.log

해결 방법: Edge 노드 등록을 다시 시도합니다. 또는 Edge 노드의 전원을 끕니다. 노드가 시작되면 MP-MPA 채널이 설정됩니다.

- 문제 2252776: 클러스터 멤버 호스트 중 하나에서 이전에 검증 오류가 발생하여 문제를 해결한 이후에도 해당 호스트에 전송 노드 프로파일을 적용할 수 없음

TNP를 클러스터에 적용합니다. 하지만 검증 중 하나를 통과하지 못해서(예: 호스트에 VM 전원이 켜져 있음) 클러스터 멤버 호스트 중 하나에 TNP를 적용할 수 없습니다. 사용자가 문제를 해결한 이후에도 UI에 검증 오류가 계속 표시되고 해당 호스트에 TNP가 자동으로 적용되지 않습니다.

해결 방법: 호스트를 클러스터 외부로 이동했다가 다시 추가합니다. 이렇게 하면 호스트에 전송 노드 프로파일을 적용하는 작업이 트리거됩니다.

- **문제 2284683: 등록된 계산 관리자를 삭제했다가 다시 추가하면 자동 배포된 장치를 삭제할 수 없음**
"전원을 끄지 못함" 오류와 함께 장치 삭제가 실패하고 계산 관리자를 찾을 수 없다고 표시됩니다.

해결 방법: API/UI를 통한 장치 삭제가 실패하면 다음과 같이 force-delete API를 사용하여 해당 장치를 수동으로 삭제합니다. `POST api/v1/cluster/nodes/deployments/<node-id>?action=delete&force_delete=true` . VC에서 VM을 삭제합니다.

- **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 2296888: TN(전송 노드)/TNP(전송 노드 프로파일) 구성의 경우 호스트 스위치에서 PNIC 전용 마이그레이션 플래그를 true로 설정하지 않으며 설치를 위한 VMK 매핑을 채워진 상태로 유지할 수 없음**

생성 중에 구성 불일치를 지정하면(호스트 스위치에서 PNIC 전용 마이그레이션 플래그를 true로 설정하고 설치를 위한 VMK 매핑을 채워진 상태로 유지) 다음과 같은 예외가 표시됩니다.

호스트 b17afc36-bbdc-491a-b944-21f73cf91585에 대한 VMK 마이그레이션이 다음 오류를 나타내며 실패했습니다. [ESX VMK 인터페이스 null을 [null]로 마이그레이션하는 동안 com.vmware.nsx.management.switching.common.exceptions.SwitchingException: TransportNode[TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585]를 업데이트하거나 삭제할 수 없습니다.] (오류 코드: 9418)

업데이트 중에 구성 불일치를 지정하면 다음과 같은 예외가 표시됩니다.
일반 오류(오류 코드: 400)

true로 설정된 PNIC 전용 마이그레이션 플래그 및 VMK 마이그레이션 매핑을 둘 다 포함하는 TN/TNP 구성을 적용하는 경우 예외가 표시됩니다.

해결 방법: 호스트로 전송되는 각 구성에서는 PNIC 전용 마이그레이션 플래그가 true로 설정되거나 설치를 위한 VMK 매핑이 채워진 경우 중 하나만 허용될 수 있습니다.

1. PNIC 전용 마이그레이션을 true로 설정하도록 요구하는 호스트 스위치를 포함하는 TN 구성을 전송합니다.
2. 모든 PNIC 전용 마이그레이션 플래그를 false로 설정하여 TN 구성을 업데이트하고 설치를 위한 VMK 매핑을 원하는 대로 채웁니다. 즉, TN으로 전송되는 구성에 모든 호스트 스위치에서 PNIC 전용 마이그레이션 플래그가 true로 설정되거나 설치를 위한 VMK 매핑이 채워져 있는지 확인합니다. 둘 다 필요한 구성의 경우에는 두 가지 별도 구성을 호출해야 합니다.

- **문제 2273651 - 전송 노드를 삭제한 후에는 사용자가 호스트에서 SSH를 실행할 수 없습니다.**

KVM 구현에서 나타납니다. 사용자는 전송 노드를 삭제하고 성공적으로 삭제했다는 메시지를 받습니다. 하지만 그 이후에 SSH를 통해 동일한 호스트에 액세스할 수 없습니다. 이 문제는 NSX-T에서 관리되지 않고 KVM 템플릿의 일부로 미리 설치되었을 가능성이 있는 OVS(개방형 가상 스위치)가 있는 경우에 발생할 수 있습니다.

해결 방법: 전송 노드를 삭제하기 전에 문제가 있는 OVS를 식별합니다.

1. `ovs-vsctl` 표시를 실행하여 OVS를 식별합니다.
2. OVS의 워크로드 VM 인터페이스를 Linux 브리지로 마이그레이션합니다.
3. 다음과 같이 전송 노드를 삭제합니다.

`DELETE api/v1/transport-nodes/<uuid>`

- **문제 2281537 - 마이그레이션 후, 다중 VTEP가 있는 ESXi 전송 노드에서 BFD 세션을 시작하지 못합니다.**

NSX-V 노드를 NSX-T로 마이그레이션한 후 다중 VTEP가 있는 ESXi 전송 노드에서 모든 VTEP에서 Edge 노드로의 BFD 세션을 시작하지 못합니다.

해결 방법: netcpa 서비스를 다시 시작합니다.

NSX Manager에 대한 알려진 문제

- **문제 2285306: 서비스 VM의 전원을 켜기 전까지 Guest Introspection 서비스의 서비스 배포 상태가 "알 수 없음"으로 표시될 수 있음**

서비스 배포를 생성한 후 서비스 배포가 서비스 배포 그리드에 나열되지만 상태가 곧바로 "진행 중"으로 표시되지 않고, 그리드를 새로 고치기 전까지 "알 수 없음"으로 표시될 수 있습니다.

해결 방법: 없음. 10초 후에 페이지를 새로 고칩니다. 그러면 상태가 업데이트됩니다.

- **문제 2292526: 호스트를 추가하면 "호스트에 연결할 수 없습니다." 메시지가 표시됨**

ESXi 호스트를 추가할 때 "호스트에 연결할 수 없습니다." 메시지만 표시되고 이유는 표시되지 않습니다. 잘못된 자격 증명이 원인일 수 있습니다.

해결 방법: 호스트 구성을 검토하고, 자격 증명을 다시 입력한 후 호스트를 다시 추가합니다.

- **문제 2292701: 사용자가 바인딩 맵에서 시퀀스 번호를 업데이트할 수 없음**

사용자가 시퀀스 번호를 업데이트하는 방법으로 엔티티에 적용된 프로파일의 순서나 우선 순위를 변경할 수 없습니다.

해결 방법: 바인딩 맵을 삭제한 후 원하는 새 시퀀스 번호를 사용하여 다시 생성합니다.

- **문제 2294345: ESXi 호스팅 VM과 KVM 호스팅 VM 모두 있는 그룹에서 Application Discovery 분류를 실행하면 작업이 실패할 수 있음**

Application Discovery 기능은 ESXi 하이퍼바이저에서만 지원됩니다. 지원되지 않는 호스트를 포함하여, VM이 혼합된 호스트에 있는 그룹에 대해서는 Application Discovery 분류 결과가 보장되지 않습니다.

해결 방법: 없음.

NSX Edge에 대한 알려진 문제

- **문제 2248345: NSX-T Edge 설치 후 시스템이 부팅되면 검정색 빈 화면이 표시됨**

HPE ProLiant DL380 Gen9 시스템에는 NSX-T Edge를 설치할 수 없습니다.

해결 방법: 다른 시스템을 사용하거나 하이퍼바이저에 NSX-T Edge를 VM으로 배포합니다.

- **문제 2283559: Edge에 RIB에 대해 65k 이상의 경로와 FIB에 대해 100k 이상의 경로가 있으면 /routing-table 및 /forwarding-table MP API가 오류를 반환함**

Edge에 RIB에 대해 65k 이상의 경로와 FIB에 대해 100k 이상의 경로가 있으면 MP에서 Edge로 보내는 요청이 10초 이상 소요되어 결과적으로 시간이 초과됩니다. 이 API는 읽기 전용이며, API/UI를 사용하여 RIB에 대해 65k 이상의 경로와 FIB에 대해 100k 이상의 경로를 다운로드해야 하는 경우에만 영향을 줍니다.

해결 방법: 두 가지 방법으로 RIB/FIB를 가져올 수 있습니다.

- 이러한 API는 네트워크 접두사 또는 경로 유형에 기반하여 필터링 옵션을 지원합니다. 이러한 옵션을 사용하여 원하는 경로를 다운로드할 수 있습니다.
- 전체 RIB/FIB 테이블이 필요하고 시간 초과가 없는 경우 CLI가 지원됩니다.

논리적 네트워킹에 대한 알려진 문제

- **문제 2243415: 고객이 논리적 스위치를 사용하여(관리 네트워크로 사용) NXGI 서비스를 배포할 수 없음**

NXGI 배포 화면에서 네트워크 선택 컨트롤에 논리적 스위치가 사용자에게 표시되지 않습니다. 논리적 스위치를 관리 네트워크로 직접 지정하여 API를 사용할 경우, 다음과 같은 오류가 표시됩니다. "서비스 배포를 위해 지정된 네트워크에 액세스할 수 없습니다."

해결 방법: 로컬 스위치 또는 분산 스위치 같이 다른 유형의 스위치를 사용하여 배포합니다.

- 문제 2264386: 전송 노드가 NS 그룹의 일부인 경우에도 전송 노드가 삭제됨**
 전송 노드가 NS 그룹의 일부인 경우에도 해당 전송 노드의 삭제가 허용됩니다. 삭제가 방지되어야 합니다. 이 문제가 발생하면 NS 그룹을 다시 생성하고 전송 노드를 사용하여 관계를 다시 구축해야 합니다.

 해결 방법: 이 문제를 방지하려면 전송 노드가 NS 그룹에 연결되어 있는지 수동으로 확인합니다. 관리부 인터페이스에서 **고급 네트워킹 및 보안 > 인벤토리 > 그룹**으로 이동하거나 **시스템 > 노드 > 전송 노드 > 관련 > NSGroup**으로 이동합니다.
- 문제 2292997: Linux 네트워크 스택에 대해 특정 논리적 라우터 인터페이스를 생성하지 못할 수 있음**
 Linux 네트워크 스택에 대해 특정 논리적 라우터 인터페이스가 생성되지 못하고 다음 오류가 반환될 수 있습니다. `errorCode="EDG0100002"`, 작업 하위 인터페이스 생성 실패: 최대 하위 인터페이스 초과. 그 결과 tier0 서비스 라우터(T0 SR)가 전달한 트래픽이 경로 누락으로 인해 삭제될 수 있습니다.

 해결 방법: 영향을 받은 Edge 노드를 재부팅합니다.
- 문제 228688: VTI를 통해 BGP가 구성된 경우, IPsec 경로 기반 세션을 삭제할 때 BGP 인접 항목부터 삭제해야 함**
 VTI를 통해 BGP가 구성된 경우에 IPsec 세션을 삭제하면 양쪽 SR이 종료 상태로 표시되고 그 결과 트래픽이 차단됩니다. 트래픽을 재개하려면 VTI에 대해 구성된 BGP 인접 항목을 삭제해야 합니다. 이 시나리오에서는 BGP만 VTI를 통해 구성되었습니다.

 해결 방법: IPsec 세션을 삭제하기 전에 BGP 인접 항목부터 삭제합니다.
- 문제 2288509: Tier0/Tier1 서비스 인터페이스(중앙 서비스 포트)에 대해 MTU 속성이 지원되지 않음**
 Tier0/Tier1 서비스 인터페이스(중앙 서비스 포트)에 대해 MTU 속성이 지원되지 않습니다.

 해결 방법: 정책 워크플로를 통해 CSP 포트를 생성한 경우에도 관리부 API를 사용하여 MTU를 구성합니다.
- 문제 2288774: 잘못해서 태그가 30개를 초과한 경우 세그먼트 포트에서 인식 오류가 발생합니다.**
 사용자가 태그를 30개 넘게 적용하도록 잘못 입력합니다. 하지만 정책 워크플로가 사용자 입력을 제대로 검증/거부하지 않고 해당 구성을 허용합니다. 그런 후 정책은 태그를 30개 넘게 사용하면 안 된다는 적절한 오류 메시지와 함께 경보를 표시합니다. 이제 사용자가 이 문제를 해결할 수 있습니다.

 해결 방법: 오류가 표시된 후 구성을 수정합니다.
- 문제 2275412: 여러 TZ에서 포트 연결이 작동하지 않음**
 포트 연결은 단일 TZ에서만 사용할 수 있습니다.

 해결 방법: 없음.
- 문제 2290083: VLAN 기반 세그먼트를 생성할 때 검증이 누락됨**
 VLAN ID 속성을 사용하여 VLAN 전송 영역을 지정하면 시스템이 검증 및 오류 식별에 실패합니다. 그 결과 인식 중에 의도가 실패하고 오류가 발생합니다.

 해결 방법: 인식 정보 오류 세부 정보에 나와 있는 지침을 참조하여 입력을 수정합니다.
- 문제 2292096: "get service router config route-maps" CLI 명령이 빈 출력을 반환함**
 경로 맵이 구성되어 있는 경우에도 "get service router config route-maps" CLI 명령이 빈 출력을 반환합니다. 이는 표시 문제일 뿐입니다.

 해결 방법: get service router config CLI 명령을 사용합니다. 이 명령은 경로 맵 구성을 전체 출력의 일부로 반환합니다.
- 문제 2994002: DNS 전달자 생성 시 선택할 수 있는 Tier0/ Tier1 게이트웨이 드롭다운 목록에 Tier1이 나열되지 않음**
 레코드 수가 수천 개에 이르는 대규모 배포에서 DNS 전달자 생성 워크플로에서 선택할 수 있는 Tier0/ Tier1 게이트웨이 드롭다운 목록에 Tier1이 나열되지 않습니다. 그 결과 API를 사용하여 DNS 전달자 생성을 구성해야 합니다.

 해결 방법: API를 사용하여 구성 작업을 수행합니다.

- 문제 2298499 - 게이트웨이가 공용 IP를 사용하여 배포되지 않은 경우 공용 클라우드 게이트웨이와 피어 호스트 간의 VPN이 실패합니다.

PCG(공용 클라우드 게이트웨이)가 업링크에 공용 IP 주소 없이 배포된 경우 PCG와 피어 호스트 간에 VPN 터널을 설정할 수 없습니다. PCG가 기본적으로 VPN 트래픽에서 SNAT를 수행하므로 이런 문제가 발생합니다.

해결 방법: 공용 클라우드 게이트웨이를 배포할 때 업링크 인터페이스에 공용 IP를 사용하도록 설정합니다.

- 문제 2392093: RPF-확인으로 인한 트래픽 감소

T0 다운링크를 통해 트래픽이 헤어핀되고 Tier0 및 Tier1 라우터가 동일한 Edge 노드에 있는 경우 RPF 검사 시 트래픽이 삭제될 수 있습니다.

해결 방법: 없음.

보안 서비스에 대한 알려진 문제

- 문제 2288523: NSX Guest Introspection 드라이버를 언로드하면 보안 문제가 발생할 수 있음

IDFW는 NSX Guest Introspection 드라이버의 사용자 ID 정보를 사용합니다. 드라이버를 언로드하면 해당 Guest에서 로그인한 사용자에게 보안 문제가 발생할 수 있습니다. 다음과 같은 증상이 나타납니다.

- Guest Introspection 드라이버가 언로드된 특정 Guest VM에서 로그인한 사용자에게 방화벽 규칙이 적용되지 않습니다.
- Guest Introspection 드라이버가 언로드된 특정 Guest VM에서 로그인하는 사용자에게 사용자 세부 정보에 IDFW 구성 요소가 기록되지 않습니다.
- 호스트에서 IDFW를 사용하도록 설정한 경우에도 MUX 로그에 이러한 게스트 VM의 연결이 표시되지 않습니다.
- 호스트에서 IDFW를 사용하도록 설정한 경우에도 MUX 로그에 이러한 게스트 VM의 네트워크 이벤트가 표시되지 않습니다.

그 결과 [기본적으로 모두 거부] 규칙이 Guest Introspection 드라이버가 언로드된 게스트 VM에서 로그인한 사용자의 액세스를 차단할 수 있습니다.

해결 방법: 없음. 게스트 VM 내에서 Guest Introspection 드라이버를 언로드할 수 있는 권한을 가진 사용자가 없도록 IT 관리자가 보안 모범 사례를 따라야 합니다.

- 문제 2288773: 이전 TLS 프로토콜 API를 계속 사용할 수 있지만 해당 설정이 덮어쓰임

NSX TLS 프로토콜 버전 및 암호 그룹을 설정하는 새 API가 NSX-T에 추가되었으며, 이 API는 NSX-T 클러스터의 모든 노드를 업데이트합니다. 하지만 이전 API도 계속 사용할 수 있습니다. 이전 API를 사용할 수 있지만 글로벌 설정이 새 설정을 덮어씁니다.

해결 방법: 새 API를 사용합니다.

- 문제 2291872: 방화벽 규칙에 TFTP 서비스를 사용하면 로그 메시지에 주의 메시지가 표시됨

ESXi 노드에서 방화벽 rule.Log 위치에 TFTP 서비스를 사용하면 적절하지 않은 주의 메시지가 로그 메시지에 표시됩니다. /var/log/cfgAgent.log.

해결 방법: TFTP에 대한 새 서비스를 L4PortSet 서비스로 생성하여 방화벽 규칙에 사용합니다.

- 문제 2203863 - UDP 및 ICMP 트래픽에 대해 ID 방화벽 규칙이 지원되지 않습니다.

ID 방화벽 규칙이 ping 테스트에서 작동하지 않습니다. 현재 기능은 TCP 트래픽에서만 지원됩니다.

해결 방법: ID 방화벽 규칙을 테스트하는 데 TCP를 사용합니다. ID 방화벽 규칙을 구성할 때 서비스 열에 ANY/UDP/ICMP를 설정하지 마십시오.

- 문제 2296430 - NSX-T Manager API는 인증서 생성 중에 주체 대체 이름을 제공하지 않습니다.

NSX-T Manager API는 특히 CSR 생성 중에 인증서를 발급하기 위해 주체 대체 이름을 제공하지 않습니다.

해결 방법: 확장을 지원하는 외부 도구를 사용하여 CSR을 생성합니다. 서명된 인증서를 CA(인증 기관)에서 수신한 후에 CSR의 키를 사용하여 NSX-T Manager로 가져옵니다.

- 문제 2252738 - FQDN(정규화된 도메인 이름) 규칙의 경우 규칙과 일치하지 않는 패킷이 대상에 도달하도록 허용됩니다.

특정 FQDN 규칙이 생성되면 IP 주소에 연결된 도메인 이름이 규칙과 일치하는 방화벽 데이터베이스에 추가되고 해당 도메인 이름으로 전송된 패킷이 서버에 도달하도록 허용됩니다. 그러나 사용자가 도메인 이름 서버에서 해당 IP 주소에 연결된 도메인 이름을 변경하는 경우, 새 도메인 이름과 일치하는 다른 FQDN 규칙이 없으면 해당 도메인 이름 항목이 방화벽 데이터베이스에서 업데이트되지 않습니다. 결과적으로 패킷이 FQDN 규칙에 의해 삭제되어야 하나 삭제되지 않고 새 도메인 이름으로 전송됩니다.

해결 방법: 없음.

- 문제 2395334 - (Windows) 패킷이 상태 비저장 방화벽 규칙 Conntrack 항목으로 인해 잘못 삭제되었습니다.

상태 비저장 방화벽 규칙은 Windows VM에서 잘 지원되지 않습니다.

해결 방법: 대신 상태 저장 방화벽 규칙을 추가하십시오.

- 문제 2458384 - 403 오류를 나타내며 NSX-T Manager 인터페이스 페이지가 로드되지 않습니다.
릴리스 버전 2.4.0 및 2.4.1에서 발견되었습니다. 이 문제는 관리자 로그인과 ID 관리자 로그인 둘 다에 영향을 미칩니다. NSX-T Manager의 FQDN은 *.SLD.TLD 형식을 사용합니다. 예: *.co.uk, *.co.il, *.com.au 등

해결 방법: FQDN 대신 짧은 이름 또는 IP를 사용하여 NSX-T Manager UI에 액세스합니다.

<https://kb.vmware.com/s/article/71217>을 참조하십시오.

KVM 네트워킹에 대한 알려진 문제

- 문제 2292995: 구성된 모든 규칙이 OVS에 프로그래밍되어 있더라도 인식 상태가 오류로 설정됨
DFW 규칙이 데이터부에 프로그래밍되어 있더라도 API가 부정 오류를 반환합니다.

해결 방법: DFW 규칙을 업데이트하면 이 오류가 해결됩니다. 예를 들어 규칙 로깅을 토글하기만 해도 KVM DFW 모듈의 오류 조건이 지워집니다.

로드 밸런서에 대한 알려진 문제

- 문제 2290899: IPsec VPN이 작동하지 않고 제어부의 IPsec 인식이 실패함
동일한 Edge 노드의 Tier 0에서 IPsec 서비스와 함께 62개가 넘는 LbServer가 사용하도록 설정된 경우 IPsec VPN(또는 L2VPN)이 나타나지 않습니다.

해결 방법: LbServer 수를 62개 미만으로 줄입니다.

- 문제 2297157 - 로드 밸런싱 HTTPS 성능은 FIPS 모드의 영향을 받습니다.
기본 FIPS 모드를 사용하도록 설정하면 로드 밸런싱 성능이 저하될 수 있습니다.

해결 방법: 해결 방법에 대해서는 기술 자료 문서 67400 [NSX-T 2.4.0 로드 밸런싱 서비스에서 HTTP의 성능 저하가 나타날 수 있음](#)을 참조하십시오.

- 문제 2362688: 로드 밸런서 서비스에서 일부 풀 멤버가 다운된 경우 UI에는 통합된 상태가 작동 중으로 표시됩니다.

하나의 풀 멤버가 다운된 경우에는 정책 UI에 풀 상태가 녹색이고 작동 중임을 나타내는 표시가 없습니다.

해결 방법: 없음.

솔루션 상호 운용성에 대한 알려진 문제

- 문제 2289150: AWS에 대한 PCM 호출이 실패하기 시작함
CSM에서 AWS 계정의 PCG 역할을 *old-pcg-role*에서 *new-pcg-role*로 업데이트하면 CSM이 AWS에서 PCG 인스턴스에 대한 역할을 *new-pcg-role*로 업데이트합니다. 하지만 PCM은 PCG 역할이 업데이트되었다는 사실을 모르기 때문에 *old-pcg-role*을 사용하여 생성된 이전 AWS 클라이언트를 계속해서 사용합니다. 그 결과 PCM AWS 클라우드 인벤토리 검색 및 기타 AWS 클라우드 호출이 실패합니다.

해결 방법: 이 문제가 발생한 경우, 적어도 6.5시간 동안 새 역할로 변경한 직후에 이전 PCG 역할을 수정/삭제하지 마십시오. PCG를 다시 시작하면 모든 AWS 클라이언트가 새 역할 자격 증명을 사용하여 다시 초기화됩니다.

작동 및 모니터링 서비스에 대한 알려진 문제

- **문제 2275869: ESXi 호스트에 31자를 초과하는 태그가 있으면 해당 호스트에서 cfgAgent 로그가 1분 이내에 롤오버됨**
로그가 자주 롤오버되면 호스트에서 디버깅 및 문제 해결을 위한 cfgAgent.log의 유용한 정보가 손실될 수 있습니다. ESXi 호스트에서의 로그 위치: /var/log/cfgAgent.log

해결 방법: 없음.

- **문제 2289984: 호스트에서 nsx-context-mux 서비스가 중지된 이후에도 mux_connectivity_status가 [연결됨] 상태로 표시됨**
nsx-context-mux 또는 nsx-opsagent가 호스트에서 실행 중이 아닌데 시스템(NSX 인터페이스 또는 서비스 인스턴스 API)이 솔루션 상태 및 GI 에이전트 상태를 실행 중인 것으로 잘못 표시하고, 타임 스탬프도 변경하지 않고 표시합니다. 그 결과 게스트 VM에 대한 AV 보호가 중지될 수 있습니다.

해결 방법: 아직 실행 중이 아닌 경우, 호스트에서 mux 및 opsagent를 수동으로 시작해 봅니다.

1. 호스트에 루트 권한으로 로그인하고 다음 명령을 실행합니다.
/etc/init.d/nsx-opsagent start
/etc/init.d/nsx-context-mux start
2. 에이전트를 시작한 후 몇 분 정도 기다렸다가 UI에 상태와 타임 스탬프가 업데이트되었는지 확인합니다.

업그레이드에 대한 알려진 문제

- **문제 2273737: NSX-T 2.3에서 2.4로 업그레이드한 후 vIDM 서버 세부 정보가 누락됨**
vIDM을 사용하는 경우 vIDM 서버가 NSX 정책 장치에만 구성되어 있으면 업그레이드 시 vIDM 서버가 마이그레이션되지만 통합된 장치에는 vIDM 서버가 누락됩니다.

해결 방법: 문제가 언제 발생했는지에 따라 두 가지 옵션이 있습니다.

- 버전 2.3에서 2.4로 업그레이드하기 전에 문제가 발생한 경우:
NSX 정책 장치와 NSX Manager VM 둘 모두에 동일한 vIDM 서버 세부 정보를 구성합니다.
- 버전 2.3에서 2.4로 업그레이드한 이후에 문제가 발생한 경우:
통합된 장치에서 동일한 vIDM 서버 세부 정보를 다시 구성합니다.

- **문제 2288549: 매니페스트 파일의 체크섬 실패로 인해 RepoSync가 실패함**
최근에 2.4로 업그레이드된 배포에서만 나타납니다. 업그레이드된 설정을 백업한 후 새로 배포된 관리자에 복원하면 데이터베이스에 있는 저장소 매니페스트 체크섬과 실제 매니페스트 파일의 체크섬이 일치하지 않습니다. 이로 인해 백업을 복원한 이후 RepoSync가 실패한 것으로 표시됩니다.

해결 방법: 이 실패를 복구하려면 다음 단계를 수행하십시오.

1. get service install-upgrade CLI 명령을 실행합니다.
결과에서 "Enabled on"의 IP를 적어 둡니다.
2. 위의 명령이 반환한 결과에서 "Enabled on"에 표시된 NSX Manager IP에 로그인합니다.
3. 시스템 > 개요로 이동한 후, 반환된 "Enabled on"에 표시된 것과 동일한 IP를 가진 노드를 찾습니다.
4. 해당 노드에서 해결을 클릭합니다.
5. 위의 해결 작업이 성공하면 동일한 인터페이스에서 모든 노드에 대해 해결을 클릭합니다.
그러면 3개 노드 모두의 RepoSync 상태가 완료됨으로 표시됩니다.

- **문제 2279973: 빈 그룹을 생성한 후 업그레이드를 진행하면 MP 업그레이드 이후에 빈 그룹이 시작되지 않은 것으로 표시됨**

이 문제는 빈 그룹을 생성한 후에 업그레이드를 진행하면 발생합니다.

해결 방법: 빈 그룹을 생성하지 마십시오.

다음 중 하나를 수행하여 계속합니다.

- 빈 그룹을 삭제합니다.
- 재개 버튼을 클릭하여 업그레이드를 완료합니다.

○ 계획 재설정

- **문제 2282389: 클러스터 간에 ESX를 이동하면 UC 계획이 VC 클러스터 멤버 자격과 동기화되지 않음**
ESX를 클러스터 하나에서 VC 내의 다른 클러스터로 이동하면 변경 내용이 UC 업그레이드 계획에 반영되지 않습니다. 사용자가 그룹 간에 "병렬 업그레이드"를 선택한 경우에는 둘 이상의 호스트가 동시에 유지 보수 모드에 전환될 수 있습니다.

해결 방법: UC 업그레이드 계획이 VC 클러스터와 동기화되도록 [호스트 업그레이드] 페이지에서 [재설정] 옵션을 클릭하여 계획을 다시 구축합니다.

- **문제 2288921: 이전 버전의 Edge 노드를 추가하면 업그레이드 상태가 동기화되지 않음**
사용자가 Edge 업그레이드 후 이전 버전의 Edge 노드를 추가하면 업그레이드 상태가 동기화되지 않습니다. 이 경우 업그레이드 호출을 계속하면 문제가 발생합니다.

해결 방법: 우선 이전 버전의 Edge 노드는 추가하지 않아야 합니다. 이 문제가 발생하면 UC 서비스를 다시 시작합니다.

- **문제 2291625: 업그레이드 계획을 동기화한 후 PCG 업그레이드 상태가 SUCCESS에서 NOT_STARTED로 변경됨**
이 문제는 사용자가 PCG를 업그레이드한 이후에 더 많은 에이전트/PCG를 업그레이드하려고 하는 경우에만 발생합니다.
권장 워크플로에는 PCG 업그레이드 후 UC 인터페이스를 통해 업그레이드해야 하는 Cross-Cloud 구성 요소가 없습니다.

이 문제는 기능에는 영향을 주지 않습니다. 이전에 완료된 PCG 업그레이드의 상태가 업그레이드 UI에 "없음"으로 표시됩니다.

해결 방법: 없음. 기능에는 영향을 주지 않습니다.

- **문제 2293227: 2.4로 업그레이드한 후 VMTools 10.3.5를 실행하는 VM에 IDFW 규칙이 적용되지 않음**
라이브 NSX-T 업그레이드를 수행한 이후 VMTools 10.3.5를 실행하는 VM에 IDFW 규칙이 적용되지 않고 이로 인해 해당 VM에 대해 AV 보호가 중지될 수 있습니다.

해결 방법: 영향을 받은 VM을 다시 시작합니다.

- **문제 2295564: 2.3에서 2.4로 업그레이드한 후 Edge 노드 컨트롤러 연결이 끊어질 수 있음**
이는 일부 north-south 트래픽에 영향을 주는 일시적인 문제입니다.

해결 방법: 동일한 Edge 노드에서 유지 보수 모드를 사용하도록 설정했다가 사용하지 않도록 설정합니다.

- **문제 2294178 - 2.3.1에서 2.4로 업그레이드하는 동안 호스트 VIB를 업데이트하지 못합니다.**
버전 2.3.1에서 2.4로의 업그레이드 프로세스가 호스트의 오프라인 번들 설치 오류를 나타내며 실패할 수 있습니다. 좀 더 구체적으로 말하면, 스위치 보안 모듈이 로드되지 않기 때문에 호스트 VIB를 업데이트하지 못합니다. 이 문제는 IP 검색 기능이 스위칭 프로파일에서 사용하도록 설정되어 있고, ESXi-6.7EP06(빌드 11675023)을 실행하는 호스트를 사용하여 NSX-T 2.3.1에서 NSX-T 2.4로 인플레이스 업그레이드할 때 발생하는 것으로 알려져 있습니다.

해결 방법: 해결 방법에 대해서는 기술 자료 문서 67445 [IP 검색을 사용하도록 설정한 경우 NSX-T 2.3.1에서 NSX-T 2.4로 업그레이드할 때 호스트 VIB를 업데이트할 수 없음](#)을 참조하십시오.

- **문제 2277543 - 인플레이스 업그레이드 동안 '호스트에서 오프라인 번들 설치 실패' 오류를 나타내며 호스트 VIB를 업데이트하지 못합니다.**
NSX-T 2.3.x에서 2.4로 인플레이스 업그레이드하기 전 호스트와 ESXi-6.5P03(빌드 10884925)을 실행하는 호스트에서 Storage vMotion을 수행하면 이 오류가 발생할 수 있습니다. 호스트 업그레이드 직전에 Storage vMotion을 수행한 경우 2.3.x의 스위치 보안 모듈이 제거되지 않습니다. Storage vMotion은 메모리 누수를 트리거하여 스위치 보안 모듈을 로드하지 못하게 합니다.

해결 방법: 기술 자료 문서 67444 [호스트 업그레이드 전에 VM에서 Storage vMotion을 수행할 경우 NSX-T 2.3.x에서 NSX-T 2.4.0으로 업그레이드할 때 호스트 VIB를 업데이트할 수 없음](#)을 참조하십시오.

- **문제 2276398 - NSX를 사용하여 AV 파트너 서비스 VM을 업그레이드하면 최대 20분 동안 보호 기능이 중지**

될 수 있습니다.

파트너 SVM이 업그레이드되면 새 SVM이 배포되고 이전 SVM이 삭제됩니다. 호스트 Syslog에 SolutionHandler 연결 오류가 나타날 수 있습니다.

해결 방법: 업그레이드한 후 호스트에서 ARP 캐시 항목을 삭제한 다음, 호스트의 파트너 제어 IP를 Ping하여 이 문제를 해결합니다.

- 문제 2297918 - 2.3.1에서 2.4로 업그레이드한 후 클러스터에서 NSX를 제거할 수 없습니다.
클러스터를 2.3.1에서 2.4로 업그레이드한 후 NSX-T를 제거할 수 없으며 다음 메시지를 나타내며 실패합니다.
“클러스터에서 NSX를 제거하지 못했습니다. 이 패브릭 템플릿에 대한 관련 전송 노드 템플릿 또는 전송 노드 컬렉션이 있습니다. 이 패브릭 템플릿에서 삭제하거나 사용하지 않도록 설정하기 전에 전송 노드 템플릿 또는 전송 노드 컬렉션을 삭제해야 합니다.

해결 방법: 영향을 받는 클러스터에서 전송 노드 프로파일을 분리한 다음, "NSX 제거" 워크플로를 사용합니다.

- 문제 2286030 - NSX-T 2.3.x 및 이전 버전에서 2.4.x로 업그레이드할 때 전송 노드 구성이 실패 상태로 표시됩니다.
Null 포인터 예외로 인해 NSX-T 2.3.x 및 이전 버전에서 2.4.x로 업그레이드할 때 전송 노드 구성이 실패 상태로 전환됩니다. vmkernel 어댑터가 N-VDS VLAN 논리적 스위치로 마이그레이션된 ESXi 전송 노드가 있고 NSX-T 2.3.x에서 NSX-T 2.4.x로 업그레이드하는 경우 경합 조건으로 인해 ESXi 전송 노드 구성 상태가 실패로 표시될 수 있습니다. 그러나 노드가 실패 구성 상태로 표시된 후에도 업그레이드 중에 NSX Manager 및 컨트롤러와의 ESXi 전송 노드 연결이 그대로 유지됩니다.

해결 방법: 전송 노드를 업데이트하거나 다시 보내 구성 상태를 성공으로 재설정합니다.

1. NSX Manager에서 실패로 표시되는 ESXi 전송 노드를 편집합니다.
2. ESXi 전송 노드 구성 팝업에서 **저장**을 클릭합니다.
이 작업은 상태를 재설정합니다. 구성을 수정할 필요는 없습니다.

API에 대한 알려진 문제

NSX Policy Manager에 대한 알려진 문제

- 문제 2291267: PCM에서 생성한 기본 게이트웨이 정책 섹션에 시퀀스 번호가 할당되지 않아 0이 기본적으로 사용됨
사용자가 시퀀스 번호 또는 insert_top 옵션을 사용하지 않고 게이트웨이 정책을 생성하면 정책 충돌이 발생합니다. 로그 위치: /var/log/policy/policy.log

해결 방법: 항상 적절한 sequence_numbers를 사용하여 정책을 생성하거나 url 매개 변수 action=revise&operation=insert_top을 사용하여 정책을 생성하여 이 문제를 방지합니다.

- 문제 2289278: 정책 API가 오류를 발생시키지만 폴은 동일하고 지속성 프로파일이 서로 다른 여러 가상 서버의 구성이 허용됨
시스템에서는 동일한 폴의 여러 LbVirtualServer에 대해 충돌하는 지속성 유형을 구성하는 기능을 지원하지 않습니다. 하지만 정책이 충돌하는 입력을 제대로 검증/거부하지 않고 해당 구성을 허용합니다. 그 결과 정책이 오류 메시지와 함께 경보를 표시합니다.

해결 방법: 이 문제가 발생한 경우 LbVirtualServer의 그룹 설정을 변경하여 문제를 수정할 수 있습니다.

- 문제 2248186 - BGP 라우터가 자체 인터페이스를 사용하여 해당 인접 항목의 IPV6 경로를 다음번 홉으로 설치합니다.
그 결과 설치된 경로에 대한 IPV6을 전달하지 못하고 전달 루프가 발생할 수 있습니다.

해결 방법: 이 문제를 방지하려면 BGP 업데이트에서 IPv6 연결 주소를 다음번 홉으로 필터링하도록 경로 맵을 구성합니다.

NSX Cloud에 대한 알려진 문제

- 문제 2287884: NSX Cloud에서 특정 Centos 마켓플레이스 이미지가 지원되지 않음

NSX Cloud에서는 해당 배포 버전이 예상되는 부 커널 버전과 일치하는 Centos 마켓플레이스 이미지만 지원됩니다.

예를 들어 배포 버전과 해당하는 커널 버전은 다음과 같아야 합니다.

- RHEL 7.5 3.10.0-862
- RHEL 7.4 3.10.0-693
- RHEL 7.3 3.10.0-514

해결 방법: 설명서에서 권장하는 권장 Centos 배포만 사용합니다.

- **문제 2275232: DFW Connectivity_statregy를 BLACKLIST에서 WHITELIST로 변경하면 클라우드에서 VM에 대해 DHCP를 사용할 수 없음**
새 DHCP 리스를 요청하는 모든 VM의 IP가 손실됩니다. DFW에서 클라우드 VM에 대해 DHCP를 명시적으로 허용해야 합니다.

해결 방법: DFW에서 클라우드 VM에 대해 DHCP를 명시적으로 허용합니다.

- **문제 2277814: nsx.network 태그 값이 잘못된 경우 VM이 vm-overlay-sg로 이동됨**
잘못된 nsx.network 태그가 지정된 VM은 vm-overlay-sg로 이동됩니다.

해결 방법: 잘못된 태그를 제거합니다.

- **문제 2280663: 드문 경우지만 여러 VPC를 병렬 방식으로 오프보딩하면 작업이 실패할 수 있음**
계산 VPC 중 하나의 오프보딩이 실패합니다.

해결 방법: 정책에서 VPC 및 해당하는 그룹을 수동으로 정리합니다.

- **해결된 문제 2287124: Microsoft Azure VNet에 PCG를 배포한 후 CSM의 VNet 타일이 주의를 잘못 보고함**
Microsoft Azure VNet에 PCG를 배포한 후 CSM에서 VNet이 주의 기호(느낌표가 있는 노란색 삼각형)를 보고합니다. 주의 아이콘 위로 마우스를 가져가면 CSM에서 MP(관리부) 및 CCP(제어부)의 상태를 알 수 없음으로 보고합니다. 그러나 연결에는 문제가 없을 수 있으며 주의가 잘못 표시되는 것입니다.

- **문제 2290688 - AWS에서 Windows 2016 VM을 업그레이드하지 못합니다.**
AWS에서 여러 Windows 워크로드 VM을 업그레이드하지 못합니다. VM 업그레이드 상태는 AWS 포털에 "1/2 확인" 상태에서 중단된 것으로 표시됩니다. 다시 시도해도 실패합니다. 이 문제는 동일한 NSX-T 버전 업그레이드에서만 나타납니다.

해결 방법: 이 문제를 복구하려면 다음 단계를 수행합니다.

1. 최신 호스트 구성 요소를 VM에서 다운로드할 수 있도록 영향을 받는 호스트에서 PCG가 업그레이드되었는지 확인합니다.
2. VM을 재부팅하여 정상 상태로 전환합니다.
3. uninstall cmd를 수동으로 실행합니다.
4. install cmd를 수동으로 실행합니다.