



VMware NSX-T Data Center 2.3.1 및 NSX Container Plug-in 2.3.1 릴리스 정보

VMware NSX-T Data Center 2.3.1 | 2018년 12월 20일

VMware NSX 컨테이너 플러그인 2.3.1 | 2018년 11월 8일

이 릴리스 정보의 추가 사항 및 업데이트 사항을 정기적으로 확인하십시오.

릴리스 정보에 포함된 내용

릴리스 정보에는 다음과 같은 항목이 포함됩니다.

- 새로운 기능
- 호환성 요구 사항
- 해결된 문제
- 알려진 문제

새로운 기능

NSX-T Data Center 2.3.1의 새로운 기능

NSX-T Data Center 2.3.1은 새로운 기능을 도입했습니다. NSX-T Data Center 2.3.1은 NSX-T Data Center 2.3.1과 호환됩니다. [NSX-T Data Center 2.3 릴리스 정보](#).

NSX Container Plug-in 2.3.1의 새로운 기능

NCP(NSX Container Plug-in) 2.3.1은 새로운 기능을 도입했습니다.

- Kubernetes LoadBalancer는 NSX-T의 새로운 기능을 도입했습니다. Kubernetes LoadBalancer는 NSX-T의 새로운 기능을 도입했습니다.

NSX-T Data Center 2.3.1에 권장되는 ESXi 버전

- ESXi 6.5 P03 빌드 10884925
- ESXi 6.7 U1 빌드 10302608

NCP 2.3.1의 호환성 요구 사항

제품	버전
PAS에 대한 NCP/NSX-T 타일	2.3.1
NSX-T	2.2, 2.3, 2.3.1
Kubernetes	1.11, 1.12

OpenShift	3.10, 3.11
Kubernetes 호스트 VM OS	Ubuntu 16.04, RHEL 7.4, 7.5
OpenShift 호스트 VM OS	RHEL 7.4, 7.5
PAS(PCF)	OpsManager 2.2.0 + PAS 2.2.0 OpsManager 2.3.x + PAS 2.3.x

해결된 문제

해결된 문제는 다음과 같이 분류됩니다.

- [NSX-T Data Center 2.3.1에서 해결된 문제](#)
- [NCP 2.3.1에서 해결된 문제](#)

NSX-T Data Center 2.3.1에서 해결된 문제

- **문제 2238957: ESXi 호스트 재부팅 후 오래된 Hyperbus 포트가 정리되지 않음**
호스트에서 실행 중인 컨테이너 VM의 전원을 끄지 않고 ESXi 호스트를 재부팅하는 경우 Hyperbus 포트가 예상대로 정리되지 않습니다.
- **문제 2226523: CLI 명령 "get debug bgp"가 작동하지 않음**
"get debug bgp" CLI 명령을 실행했을 때 출력이 생성되지 않습니다.
- **문제 2241365: NSX-T Data Center 2.2에서 2.3으로 업그레이드하는 동안 ALG(애플리케이션 수준 게이트웨이) 트래픽이 있는 방화벽으로 보호된 VM의 네트워크 연결이 끊김**
NSX-T Data Center 2.2에서 2.3으로 업그레이드하는 동안 VM이 NSX-T Data Center 2.2를 실행 중인 호스트에서 NSX-T Data Center 2.3을 실행 중인 호스트로 마이그레이션됩니다. 방화벽으로 보호되고 ALG 트래픽이 있는 VM은 마이그레이션 후 네트워크 연결이 끊깁니다.
- **문제 2241378: VPN 터널이 변동 동작을 표시하고 트래픽이 손실됨**
방화벽 중지 규칙이 구성되어 있고 조각화된 트래픽이 있는 VPN 터널이 변동 동작을 표시하고 트래픽이 손실됩니다.
- **문제 2232034: ESXi 호스트에 1024개가 넘는 MAC 주소가 있는 DLR 브리지가 있는 경우 지원 번들을 생성하는 동안 호스트가 충돌함**
다수의 브리지 전달 항목이 있을 때 vm-support 또는 "net-bridge --mac-address-table \$bridgeName" 명령을 실행하면 버퍼 오버플로가 발생합니다.
- **문제 2216746: VM에 대해 vMotion을 수행하거나 전원을 켜 때 VM의 NIC 연결이 끊기고 VM에 네트워크 연결이 없음**
다수의 VM에 대해 전원을 동시에 켜거나 vMotion을 수행하면 일부 VM의 NIC 연결이 끊기고 VM이 네트워크에 연결되지 않습니다.
- **문제 2216747: VM에 대해 vMotion을 수행하면 해당 포트의 연결이 끊김**
VM이 NFS에 스토리지가 있고 VM에 대해 vMotion이 수행되면(HA에 의해 트리거될 수 있음) VM의 네트워크 연결이 끊깁니다.
- **문제 2229210: 논리적 스위치 포트 생성 및 삭제 작업을 반복하면 NSX Controller에서 메모리 누수가 발생함**
이 문제는 논리적 스위치 포트가 삭제될 때 삭제되지 않은 Spoof Guard 도메인 개체로 인해 발생합니다.
- **문제 2220560: metricRegistry의 과도한 이벤트 로그로 인해 NSX Controller에서 메모리 누수가 발생할 수 있음**
NSX Controller에서 다수의 트랜잭션을 처리한 후 대량의 로깅으로 인해 메모리 누수가 발생할 수 있습니다.
- **문제 2221286: VM 연결이 중지되면 바로 ARP 항목이 만료됨**

이 문제로 인해 특정 시간 동안 VM에 연결하지 못할 수 있습니다.

- **문제 2227882: 정책 기반 VPN의 작동이 오류 "활성 IPsec SA 없음, 하위가 없는 IKE SA 삭제 중" 오류와 함께 중지됨**
이 오류로 인해 재협상이 발생하고 및 트래픽이 중지됩니다.
- **문제 2227885 및 2227879: 특정 트래픽 패턴이 있는 Edge 노드의 IPsec VPN에서 메모리 누수가 관찰됨**
다음 기간 동안 Edge에서 소유한 대상 IP를 가진 UDP 캡슐화된 ESP 트래픽(대상 포트 4500이 있는 패킷)이 도착하면 다음과 같이 됩니다.
 - 리디렉션된 IP를 루프백 포트에 FIB 프로그래밍 후 PBR 리디렉션 규칙(HCX에서 사용)이 프로그래밍 됨
 - VPN 터널의 소스 주소 누락(예: iked 오동작 또는 코어 덤프 시)
- **문제 2227890: 논리적 포트 구성에서 터널 ID를 수정한 후 VLAN ID가 수정되지 않음**
논리적 포트의 터널 ID 변경을 위해 API를 호출할 때 VLAN ID가 수정되지 않습니다.
- **문제 2230277: vMotion 중 포트의 런타임 데이터를 플러시하면 안 됨**
ESXi 6.5의 경우 스토리지 vMotion 중의 문제로 인해 vMotion 프레임워크가 데이터를 저장하기 전에 포트의 런타임 데이터가 플러시됩니다.
- **문제 2236206: 메모리 누수로 인해 ESXi 전송 노드의 네트워크 액세스가 손실될 수 있음**
이 문제로 인해 PKS 환경에서 ESXi 전송 노드의 네트워크 연결이 끊길 수 있습니다.

NCP 2.3.1에서 해결된 문제

- **문제 2216781: 태그 값의 최대 길이가 NCP 2.2.x에서 65자, NCP 2.3.0에서 256자로 제한됨**
NCP 2.3.1에서는 다음 로드 밸런서 관련 Kubernetes 리소스에 대해 태그 값 제한을 초과하는 이름을 지원합니다.
 - LoadBalancer 서비스
 - 수신
 - 수신 규칙에 지정된 암호
 - 수신 규칙에 지정된 서비스
- **문제: 2217051: LoadBalancer 서비스의 loadBalancerIP가 변경된 후 가상 서버 IP가 업데이트되지 않음**
LoadBalancer 서비스를 생성한 후 서비스의 loadBalancerIP 값을 변경하면 변경 내용이 NSX-T 로드 밸런서의 가상 서버 IP에 반영되지 않습니다.
- **문제 2216085: 네임스페이스를 삭제한 후 NSX-T 로드 밸런서 규칙 및 풀이 삭제되지 않음**
수신 리소스와 NSX-T 로드 밸런싱을 구성하면 NSX-T 가상 서버, 풀 및 규칙이 생성됩니다. 수신 리소스가 포함되어 있는 네임스페이스를 삭제하는 경우 일부 규칙과 풀이 NSX-T에서 삭제되지 않습니다.

알려진 문제

알려진 문제는 다음과 같이 분류됩니다.

- [NSX-T Data Center 2.3.1의 알려진 문제](#)
- [NCP 2.3.1의 알려진 문제](#)

NSX-T Data Center 2.3.1의 알려진 문제

- **문제 2235834: Flow 캐시 사용 시 RDP 및 HTTPS 트래픽 문제가 발생함**
Flow 캐시를 사용하도록 설정하면 RDP 및 HTTPS 트래픽 문제가 발생할 수 있습니다.

해결 방법: Edge 노드에서 다음 명령을 실행하여 Flow 캐시가 사용되지 않도록 설정합니다.

- set dataplane flow-cache disabled
- restart service dataplane
- **문제 2227975: Edge 노드를 통과하는 TCP 트래픽이 간헐적으로 손실됨**
Edge 노드를 통과하는 TCP 트래픽이 간헐적으로 손실됩니다. ICMP 트래픽은 영향을 받지 않습니다.

해결 방법: Edge 노드에서 다음 명령을 실행하여 Flow 캐시가 사용되지 않도록 설정합니다.

- set dataplane flow-cache disabled
- restart service dataplane

NCP 2.3.1의 알려진 문제

- **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.

- **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

- **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: 현재 NSX-T 타일이 자체 라우터를 배포하는 PAS 격리 세그먼트를 지원하지 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.

- **문제 2224218: 서비스 또는 애플리케이션을 삭제했을 때 SNAT IP가 다시 IP 풀로 릴리스되는 데 2분이 걸림**
서비스 또는 애플리케이션을 삭제하고 2분 내에 다시 생성하면 IP 풀에서 새로운 SNAT IP를 받게 됩니다.

해결 방법: 동일한 IP를 다시 사용하려면 서비스 또는 애플리케이션을 삭제하고 다시 생성하기 전에 2분을 기다립니다.

- **문제 2218008: 동일한 IP 블록을 사용하도록 다른 Kubernetes 클러스터를 구성하면 연결 문제가 발생함**
동일한 IP 블록을 사용하도록 다른 Kubernetes 클러스터를 구성하는 경우 일부 포트가 다른 포트 또는 외부 네트워크와 통신할 수 없습니다.

해결 방법: 동일한 IP 블록을 사용하도록 다른 Kubernetes 클러스터를 구성하지 마십시오.