

NSX Container Plug-in 2.4.1 릴리스 정보

VMware NSX Container Plug-in 2.4.1 | 2019년 5월 9일

이 설명서의 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

NCP(NSX Container Plug-in) 2.4.1에는 다음과 같은 새로운 기능이 포함되어 있습니다.

- 상태 점검을 위한 단일 분산 방화벽 섹션 사용
클러스터당 단일 분산 방화벽 섹션을 사용하여 포트에 필요한 모든 방화벽 규칙을 작동 여부 프로브 및 준비 프로브에 포함합니다. 하나의 분산 방화벽 섹션에 최대 1000개의 규칙만 있을 수 있으므로 하나의 클러스터에 작동 여부 프로브 또는 준비 프로브가 있는 경우 포트는 최대 1000개로 제한됩니다.
- NSX 노드 에이전트가 privsep 데몬의 예기치 못한 종료를 처리하도록 설정
NSX 노드 에이전트가 privsep 데몬의 예기치 못한 종료를 처리하고 복구하도록 개선되었습니다.
- Kubernetes 서비스 자동 크기 조정의 최대 제한 정의
새 NCP configMap 옵션 max_allowed_virtual_servers를 사용하면 사용자는 클러스터에서 생성하도록 허용된 최대 가상 서버 수를 정의할 수 있습니다.
- Kubernetes 수신용으로 특정 IP를 할당하는 기능
사용자는 NCP configMap의 http_and_https_ingress_ip 옵션을 사용하여 수신용으로 IP 주소를 할당할 수 있습니다.
- Kubernetes 수신용으로 X-Forwarded-For를 설정하는 기능
- Kubernetes 수신 지속성 시간 초과를 설정하는 기능
NCP configMap 옵션인 l7_persistence_timeout이 Kubernetes 수신을 지원하는 계층 7 가상 서버에 대한 지속성 프로파일의 시간 초과를 제어하기 위해 추가되었습니다.
- NodePort 유형의 Kubernetes 서비스 지원
NodePort를 사용하면 클러스터 외부에서 Kubernetes 서비스에 액세스할 수 있습니다. kube-proxy는 트래픽을 포트에 릴레이하도록 VM 호스트를 자동으로 구성합니다. 전달이 시작될 수 있도록 VM 호스트에서 적절한 iptables 규칙을 구성해야 합니다(예: iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT). 대상 포트가 Kubernetes 네트워크 정책에 따라 분리되면 관리자는 호스트 IP CIDR의 트래픽이 포트의 서비스에 액세스할 수 있도록 네트워크 정책을 구성해야 합니다. 그러면 NCP에서 트래픽이 통과하도록 허용하는 해당 방화벽 규칙을 자동으로 추가합니다.

호환성 요구 사항

제품	버전
PAS에 대한 NCP/NSX-T 타일	2.4.1

NSX-T	2.3.1, 2.4.0.1, 2.4.1
Kubernetes	1.13, 1.14
OpenShift	3.11
Kubernetes 호스트 VM OS	Ubuntu 16.04, CentOS 7.5, CentOS 7.6
OpenShift 호스트 VM OS	RHEL 7.6
OpenShift BMC	RHEL 7.6
PAS(PCF)	OpsManager 2.5 + PAS 2.5 OpsManager 2.4 + PAS 2.4

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 돌아갑니다.
- 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 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 resolve.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 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_loadbalancer가 True로 설정되면 수신, 수신에서 참조하는 암호 및 서비스, LoadBalancer 유형 서비스 등의 이름이 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 -i를 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 2330811: NCP가 종료된 상태에서 LoadBalancer 유형의 Kubernetes 서비스를 생성할 경우 NCP가 다시 시작되면 서비스가 생성되지 않을 수 있음**
NSX-T 리소스가 LoadBalancer 유형의 Kubernetes 서비스에 사용되는 경우 기존 서비스 중 일부를 삭제한 후 새 서비스를 생성할 수 있습니다. 하지만 NCP가 종료된 상태에서 서비스를 삭제했다가 생성하면 NCP가 새 서비스를 생성하지 못합니다.

해결 방법: NSX-T 리소스가 LoadBalancer 유형의 Kubernetes 서비스에 사용되는 경우 NCP가 종료된 상태에서 삭제 및 생성 작업을 둘 다 수행하지는 마십시오.

- **문제 2317608: 여러 CNI 플러그인이 지원되지 않음**
Kubernetes에는 .conflist 유형의 CNI 구성 파일이 있어야 합니다. 이 파일에는 플러그인 구성 목록이 포함되어 있습니다. Kubelet에서 이 conflist 파일에 정의된 플러그인을 정의된 순서대로 하나씩 호출합니다. 현재 nsx-cf-cni bosh 릴리스에서는 단일 CNI 플러그인 구성만 지원합니다. 추가 CNI 플러그인은 지정된 cni_config_dir에서 기존 CNI 구성 파일 10-nsx.conf를 덮어씁니다.

해결 방법: 없음. 이 문제는 NCP 2.5에서 수정되었습니다.