

VMware NSX for vSphere 6.3.0 릴리스 정보

VMware NSX for vSphere 6.3.0 | 릴리스 날짜: 2017년 2월 2일 | 빌드 5007049

릴리스 정보에 포함된 내용

릴리스 정보에는 다음과 같은 항목이 포함됩니다.

- 새로운 기능
- 버전, 시스템 요구 사항 및 설치
- 제거 및 지원 중단된 기능
- 업그레이드 정보
- 알려진 문제
- 해결된 문제
- 문서 개정 이력

새로운 기능

NSX 6.3.0의 새로운 기능은 다음 범주로 분류될 수 있습니다.

- 플랫폼 및 규정 준수 기능
- 작업 개선
- 서비스 및 라우팅 개선
- 보안 개선
- CMP 및 파트너 통합
- 설치 및 업그레이드
- 백업 및 복원

플랫폼 및 규정 준수 기능

- 플랫폼 측면:
 - 크로스 vCenter NSX 활성화-대기 DFW 개선: NSX 6.3.0에서는 다음 사항이 개선되었습니다.
 - 여러 범용 DFW 섹션이 현재 지원됩니다. 범용 및 로컬 규칙은 **Source, Destination** 및 **AppliedTo** 필드에서 범용 Security Group을 사용할 수 있습니다.
 - 범용 Security Group: 범용 보안 그룹 멤버 자격은 정적 또는 동적 방식으로 정의할 수 있습니다. 정적 멤버 자격은 범용 보안 태그를 각 VM에 수동으로 추가하여 얻을 수 있습니다. 동적 멤버 자격은 동적 조건(VM이름)에 따라 멤버로 VM을 추가하여 얻습니다.
 - 범용 보안 태그: 이제 기본 NSX Manager에서 범용 보안 태그를 정의하고 보조 NSX Manager를 이용하여 범용 동기화로 표시할 수 있습니다. 범용 보안 태그는 고유한 ID 선택 항목에 따라 정적으로 VM에 할당하거나, 바이러스 백신 또는 취약점 스캔 등의 기준에 대해 동적으로 VM에 할당할 수 있습니다.

- 고유한 ID 선택 조건: 이전 NSX 릴리스에서 보안 태그는 NSX Manager에 대해 로컬이며 VM의 관리 개체 ID를 사용하여 VM에 매핑됩니다. 활성-대기 환경에서 주어진 VM의 관리 개체 ID는 활성 및 대기 데이터 센터에서 동일하지 않을 수 있습니다. NSX 6.3.x를 통해 기본 NSX Manager에서 고유한 ID 선택 조건을 구성하여 범용 보안 태그에 연결 시 VM을 식별하도록 사용할 수 있습니다. VM 인스턴스 UUID, VM BIOS UUID, VM 이름 또는 이러한 옵션의 조합. 자세한 내용은 NSX 관리 가이드에서 [고유한 ID 선택](#)을 참조하십시오.

- **제어부 에이전트(netcpa) 자동 복구:** netcpa 프로세스의 개선된 자동 복구 메커니즘은 연속적인 데이터 경로 통신을 보장합니다. 자동 netcpa 모니터링 프로세스는 또한 모든 문제 발생 시 자동 재시작되며 syslog 서버를 통해 경고를 제공합니다. 이점 요약:

- 자동 netcpa 프로세스 모니터링
- 문제 발생 시 프로세스 자동 재시작(예: 시스템이 중단된 경우)
- 디버깅을 위한 자동 핵심 파일 생성
- syslog를 통해 자동 재시작 이벤트 경고

- **vSphere 6.5 호환성:** NSX 6.3.0에는 vSphere 6.5a 이상에 대한 지원이 새로 추가됩니다. NSX 6.3.0은 vSphere 5.5 및 6.0과의 호환성을 유지합니다.

- **기술 미리보기:CDO(Controller Disconnected Operation) 모드:** CDO(Controller Disconnected Operation) 모드가 기술 미리보기 기능으로 도입되었습니다. 이 모드는 호스트에서 컨트롤러와의 연결이 끊어졌을 때 데이터부 연결에 영향을 주지 않도록 합니다. NSX 관리 가이드에서 [CDO\(Controller Disconnected Operation\) 모드](#) 섹션을 참조하십시오. 문제 1803220도 참조하십시오.

- **규정 준수 기능:**

- **FIPS:** NSX 6.3.0에는 FIPS를 준수하는 암호 모음만 사용하는 FIPS 모드가 있습니다. NSX Manager 및 NSX Edge에는 vSphere Web Client 또는 NSX REST API를 통해 사용하도록 설정할 수 있는 FIPS 모드가 있습니다. FIPS 모드의 영향을 받는 기능 목록은 *NSX 관리 가이드*에서 [FIPS 모드 및 비 FIPS 모드 간 기능 차이](#)를 참조하십시오.

참고: VMware 개발 파트너는 NSX에서의 사용을 위해 새로운 FIPS 규정 준수 파트너 솔루션의 인증을 수행하고 있습니다. NSX 6.3.0 아웃바운드 연결은 TLS 1.1 이상이며 FIPS 승인 암호 모음만 사용합니다. 이는 콜백을 수신하는 파트너 장치가 더욱 안전한 암호 모음에 보안 웹 수신기를 구성해야 함을 의미합니다. 다음 목록은 기본 모드 및 FIPS 모드 암호입니다.

- 기본 모드 암호: (FIPS 모드 해제) [TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDH_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
- FIPS 모드 암호: [TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA]

기본 및 FIPS 모드 둘 다 TLS 1.1 및 1.2 프로토콜을 지원합니다. 파트너 솔루션이 FIPS 모드 인증을 받았는지 여부를 확인하려면 [VMware 호환성 가이드](#)를 참조하십시오.

- **공통 조건:** 공통 조건 규정을 준수하기 위해 NSX는 EAL2+ 수준의 보장을 갖춘 규정 준수에 대한 테스트를 받았습니다. 공통 조건 규정 준수 NSX 설치를 실행하려면 NSX 관리 가이드에 포함되는 [공통 조건에 대해 NSX 구성](#) 문서에 설명된 대로 NSX를 구성해야 합니다.
- **ICSA:** 바이러스 백신, 방화벽, IPSec VPN, 암호화, SSL VPN, 네트워크 IPS, 스파이웨어 방지 및 PC 방화벽 제품 등을 테스트하고 인증하는 업계 전반에서 수용된 표준 인증입니다. 분산 방화벽 및 Edge 방화벽 모두 ICSA 회사 방화벽 조건에 대해 인증되었습니다.
- **ICSA 인증 요구로 인한 DFW 패킷 로그 형식 변경:** NSX 6.3.0에는 DFW 패킷 로그 변경이 새로 추가됩니다. 6.3.0 이상에는 ICSA 인증 요구를 충족하기 위해 ICMP 유형 및 코드가 포함됩니다.

ICMP 코드 및 유형이 없는 6.3.0 이전 로그 형태는 다음과 같습니다.

```
2016-09-29T20:52:21.983Z 6673 INET6 match PASS domain-c27/1001 IN 96 ICMP
fe80:0:0:0:21d:b502:f984:c601->ff02:0:0:0:0:0:1
```

6.3.0 이상에서는 ICMP 코드 및 유형이 포함되므로 다음과 같이 표시됩니다. 이 예에서 8은 코드이고 0은 유형입니다.

```
2016-09-29T20:54:16.051Z 42991 INET match PASS domain-c27/1001 IN 84 ICMP 8 0 10.113.226.5->10.28.79.55
```

작업 개선

- **문제 해결 대시보드:** NSX 대시보드가 NSX 6.3.0에서 업데이트되어 서비스 배포 상태, NSX Manager 백업 상태 및 Edge 장치 알림 등의 다양한 기능이 포함되었습니다.
- **보안 태깅:** 이 기능을 사용하여 API 호출을 통해 제공된 VM에 대한 여러 태그를 할당하고 삭제할 수 있습니다.
- **Syslog 개선:** 특히 로드 밸런서에서 새 syslog 업데이트를 사용할 수 있습니다.
- **Log Insight 콘텐츠 팩:** 로드 밸런서에 대해 업데이트되어 중앙 집중식 대시보드, 전체 모니터링 및 UI(사용자 인터페이스)에서 더 나은 용량 계획을 제공합니다.
- **역할 기반 액세스 제어:** 이 기능은 사용자 관리를 엔터프라이즈 관리자로서만 제한하여 NSX 관리자에게 더 이상 신규 사용자를 만들거나 신규 사용자에게 역할을 할당할 수 있는 권한이 없습니다. 보안 관점에서 이 기능은 두 관리자 역할의 명확한 구분을 생성하는 데 도움이 됩니다.
- **로드 밸런서 풀 멤버에 대한 추출 상태:** 이제 풀 멤버를 추출 상태로 배치하여 서버가 유지 보수를 위해 정상적으로 종료를 수행할 수 있습니다. 풀 멤버를 추출 상태로 설정하면 로드 밸런싱에서 백엔드 서버가 제거되지만 서버에서 계속 새 영구적인 연결을 수락할 수 있습니다.

서비스 및 라우팅 개선

- **BGP의 4바이트 ASN 지원:** 4바이트 ASN 지원이 되는 BGP 구성을 기존 2바이트 ASN BGP 피어에 대한 이전 호환성에 따라 사용할 수 있습니다.
- **5-튜플 일치에 대한 NAT 개선:** NAT 규칙에 더욱 세분화된 구성 및 유연성을 제공하기 위해 5-튜플 일치 지원을 NSX 6.3.0에서 사용할 수 있습니다.
 - 일치 조건은 5개의 매개 변수, 즉 프로토콜, 소스 IP, 소스 포트, 대상 IP, 대상 포트를 기준으로 합니다.
 - 더욱 쉽게 SNAT/DNAT 구성을 지정할 수 있도록 UI(사용자 인터페이스) 변경이 제공되었습니다. 이전 Edge 버전에서 DNAT/SNAT 구성을 변경하는 경우 UI는 계속 이전 스타일의 창을 표시합니다.
 - NSX REST API는 새 매개 변수에 대한 필드를 추가합니다.

```
<natRules>
  <natRule>
    {...}
  <!-- new fields applicable for DNAT -->
    <dnatMatchSourceAddress>any</dnatMatchSourceAddress>
    <dnatMatchSourcePort>any</dnatMatchSourcePort>
  </natRule>

  <natRule>
    {...}
  <!-- new fields applicable for SNAT -->
    <snatMatchDestinationAddress>any</snatMatchDestinationAddress>
    <snatMatchDestinationPort>any</snatMatchDestinationPort>
  </natRule>
</natRules>
```

- **향상된 계층 2 VPN 성능:** 계층 2 VPN의 성능이 향상되었습니다. 이를 통해 단일 Edge 장치가 최대 1.5Gb/s 처리량을 지원할 수 있으며 이는 이전 750Mb/s에서 개선된 사항입니다.
- **OSPF의 향상된 구성 가능성** ESG(Edge Services Gateway)에서 OSPF를 구성하는 동안 NSSA는 모든 Type-7 LSA를 Type-5 LSA로 변환할 수 있습니다.

보안 개선

분산 방화벽에 여러 가지 개선 사항이 있습니다.

- **DFW 타이머:** NSX 6.3.0은 비활성 상태가 된 후에 방화벽에서 세션이 유지되는 기간을 정의하는 세션 타이머를 도입합니다. 프로토콜에 대한 세션 제한 시간이 만료되면 세션이 닫힙니다. 방화벽에서 TCP, UDP 및 ICMP 세션에 대한 시간 초과를 정의하고 VM 또는 vNIC의 사용자 정의 집합에 적용할 수 있습니다. NSX 관리 가이드에서 [세션 타이머](#)를 참조하십시오.
- **마이크로 세분화를 지원하는 새로운 기능:** 가시성 및 계획 도구에서 마이크로 세분화를 지원하도록 두 가지 새로운 기능이 도입되었습니다.
 - 애플리케이션 규칙 관리자는 기존 애플리케이션에 대해 보안 그룹을 생성하고 방화벽 규칙을 허용하는 프로세스를 간소화합니다.
 - 끝점 모니터링을 통해 애플리케이션 소유자는 애플리케이션을 프로파일링하고 네트워크 연결을 만드는 프로세스를 식별할 수 있습니다.
- **Guest Introspection에 대한 Linux 지원:** NSX 6.3.0은 Linux VM에서 Guest Introspection을 사용하도록 설정합니다. Linux 기반의 게스트 VM에서 NSX Guest Introspection 기능은 Linux 커널에서 제공한 fanotify 및 inotify 기능을 활용합니다. 자세한 내용은 NSX 관리 가이드에서 [Linux용 Guest Introspection 설치](#)를 참조하십시오. NSX에서 지원하는 Linux 버전 목록은 [버전](#)을 참조하십시오.
- **Service Composer 게시 상태:** 이제 정책이 동기화되었는지 여부를 확인하도록 Service Composer 게시 상태를 이용할 수 있습니다. 이 기능은 호스트에서 증가된 보안 정책 변환의 가시성을 DFW 규칙에 제공합니다.

CMP(Cloud Management Platform) 및 파트너 통합

- vCloud Director 8.20 및 NSX 6.3.0 간의 보다 나은 상호 운용성은 서비스 제공업체가 고급 네트워킹과 보안 서비스를 테넌트에 제공하도록 도와줍니다. NSX 6.3.0을 사용하는 vCloud Director 8.20은 여러 테넌트와 테넌트 셀프 서비스를 지원하는 네이티브 NSX 기능을 표시합니다.
- NSX 6.3.0은 vRA를 지원하고 vRA 애플리케이션이 아닌 다른 항목을 지원하는 기능을 도입한 새 vRO 플러그인 버전 1.1을 지원합니다.
- NSX NetX 6.3.0은 Service Insertion과 관련된 규모 및 성능 개선을 제공합니다.

설치 및 업그레이드

- **현재 ESXi 버전과 독립된 NSX 커널 모듈:** NSX 6.3.0부터 NSX 커널 모듈은 인터페이스가 릴리스에서 보장되도록 공개적으로 사용 가능한 VMKAPI만 사용합니다. 이 개선 사항은 잘못된 커널 모듈 버전으로 인한 호스트 업그레이드 실패를 줄여줍니다. 이전 릴리스에서 NSX 환경의 모든 ESXi 업그레이드는 NSX 기능이 계속 적용되도록 2개 이상의 재부팅이 필요했습니다(새로운 모든 ESXi 버전에 새 커널 모듈을 푸시해야 했기 때문).
- 또한 NSX 6.3.0은 호스트를 유지 보수 모드에서 제외하기 전에 NSX 준비를 확인합니다. 이를 통해 DRS는 NSX가 준비된 호스트에만 워크로드를 이동합니다. 또한 일부 워크로드 VM에 대한 네트워킹 손실을 예방합니다.
- **쉽표로 구분된 OVF 매개 변수:** 다음의 OVF 매개 변수는 공백으로 구분된 것에서 쉽표로 구분된 것으로 변경되었습니다.
 - DNS 서버 목록(vsm_dns1_0)
 - 도메인 검색 목록(vsm_domain_0)
 - NTP 서버 목록(vsm_ntp_0)

백업 및 복원

NSX 6.3.0부터 다음 암호가 SFTP 백업에 지원됩니다.

- **암호화:** aes128-cbc, aes128-ctr, aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr
- **메시지 인증(mac):** hmac-sha2-256
- **키 교환:** diffie-hellman-group-exchange-sha256

참고: Hmac-sha1에 대한 지원은 없으며 hmac-sha2-256만 지원됩니다. 백업에 SFTP를 사용하는 경우 6.3.0으로 업그레이드한 다음 hmac-sha2-256으로 변경합니다. 자세한 내용은 [VMware 기술 자료 문서 2149282](#)를 참조하십시오.

버전, 시스템 요구 사항 및 설치

- 참고:**
- 다음 표에서는 권장 VMware 소프트웨어 버전을 나열합니다. 이러한 권장 릴리스는 일반적인 것이며, 환경별 권장 사항을 대신하거나 재정의하지 않습니다.
 - 이 정보는 이 문서 발행 당시를 기준으로 최신 정보입니다.
 - NSX 및 기타 VMware 제품의 **최소 지원** 버전에 대해서는 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오. VMware는 내부 테스트를 기준으로 최소 지원 버전을 선언합니다.

| 제품 또는 구성 요소 | 권장 버전 |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NSX for vSphere | <p>새로 배포할 경우 및 6.1.x에서 업그레이드할 때는 최신 NSX 6.3 릴리스가 권장됩니다.</p> <p>기존 배포를 업그레이드할 경우 업그레이드를 계획하기 전에 특정 문제에 관한 자세한 내용은 NSX 릴리스 정보를 검토하거나 VMware 기술 지원 담당자에게 문의하십시오.</p> |
| vSphere | <ul style="list-style-type: none">• vSphere 5.5U3 이상• vSphere 6.0U3 이상. vSphere 6.0U3는 vCenter Server를 재부팅한 후 ESXi 호스트에서의 중복 VTEP 문제를 해결합니다. 자세한 내용은 VMware 기술 자료 문서 2144605를 참조하십시오.• vSphere 6.5U1 이상. vSphere 6.5U1은 OutOfMemory로 인한 EAM 실패 문제를 해결합니다. 자세한 내용은 VMware 기술 자료 문서 2135378를 참조하십시오. |
| Windows용 Guest Introspection | <p>모든 VMware Tools 버전이 지원됩니다. 일부 Guest Introspection 기반의 기능에는 최신 VMware Tools 버전이 필요합니다.</p> <ul style="list-style-type: none">• VMware Tools와 함께 패키지로 제공되는 선택적 Thin Agent Network Introspection Driver 구성 요소를 사용하도록 설정하려면 VMware Tools 10.0.9 및 10.0.12를 사용합니다.• NSX/vCloud Networking and Security에서 VMware Tools를 업그레이드한 후에 VM이 느려지는 문제를 해결하려면 VMware Tools 10.0.8 이상으로 업그레이드합니다(VMware 기술 자료 문서 2144236 참조).• Windows 10 지원을 위해 VMware Tools 10.1.0 이상을 사용합니다. |

이 NSX 버전은 다음 Linux 버전을 지원합니다.

Linux용 Guest
Introspection

- RHEL 7 GA(64비트)
- SLES 12 GA(64비트)
- Ubuntu 14.04 LTS(64비트)

vRealize
Orchestrator

NSX-vRO 플러그인 1.1.0 이상

참고: VMware는 현재 vRealize Networking Insight 3.2를 사용하는 NSX for vSphere 6.3.x를 지원하지 않습니다.

시스템 요구 사항 및 설치

NSX 설치 사전 요구 사항의 전체 목록을 보려면 "NSX 설치 가이드"에서 [NSX 시스템 요구 사항](#) 섹션을 참조하십시오.

설치 지침을 보려면 [NSX 설치 가이드](#) 또는 [크로스 vCenter NSX 설치 가이드](#)를 참조하십시오.

제거 및 지원 중단된 기능

수명 종료 또는 지원 종료 경고

곧 업그레이드해야 하는 NSX 및 기타 VMware 제품에 대한 자세한 내용은 [VMware 수명 주기 제품 매트릭스](#)를 참조하십시오.

- **NSX for vSphere 6.1.x:** EOA(End of Availability) 및 EOGS(End of General Support)가 2017년 1월 15일 NSX for vSphere 6.1.x에 대해 도달했습니다. ([VMware 기술 자료 문서 2144769](#)도 참조하십시오.)
- **새로 만들기 NSX Data Security가 제거됨:** NSX 6.3.0에서 NSX Data Security 기능이 제품에서 제거되었습니다.
- **새로 만들기 NSX Activity Monitoring(SAM)이 더 이상 지원되지 않음:** NSX 6.3.0을 기준으로 Activity Monitoring은 더 이상 NSX의 기능으로 지원되지 않습니다. 교체 기능으로 Endpoint Monitoring을 사용하십시오. 자세한 내용은 NSX 관리 가이드의 [Endpoint Monitoring](#)을 참조하십시오.
- **새로 만들기 Web Access Terminal이 제거됨:** WAT(Web Access Terminal)가 NSX 6.3.0에서 제거되었습니다. Web Access SSL VPN-Plus를 구성할 수 없으며 NSX Edge를 통해 공개 URL 액세스를 사용하도록 설정할 수 없습니다. VMware에서는 보안 향상을 위해 SSL VPN 배포에서 전체 액세스 클라이언트를 사용할 것을 권장합니다. 이전 릴리스에서 WAT 기능을 사용하고 있는 경우 6.3.0으로 업그레이드하려면 이 기능을 사용하지 않도록 설정해야 합니다.
- **새로 만들기 IS-IS가 NSX Edge에서 제거됨:** NSX 6.3.0에서는 라우팅 탭에서 IS-IS 프로토콜을 구성할 수 없습니다.
- **새로 만들기 vCNS Edge가 더 이상 지원되지 않습니다.** NSX 6.3.x로 업그레이드하기 전에 먼저 NSX Edge로 업그레이드해야 합니다.

API 제거 및 동작 변경

방화벽 구성 또는 기본 섹션 삭제:

- 기본 섹션이 지정된 경우 방화벽 섹션 삭제 요청은 이제 거부됩니다. DELETE /api/4.0/firewall/globalroot-

0/config/layer2sections|layer3sections/sectionId

- 기본 구성을 설정하기 위해 새 메서드가 도입되었습니다. 이 메서드의 결과를 사용하여 전체 구성 또는 기본 섹션을 대체합니다.
 - GET api/4.0/firewall/globalroot-0/defaultconfig를 사용하여 기본 구성 설정
 - PUT /api/4.0/firewall/globalroot-0/config를 사용하여 전체 구성 업데이트
 - PUT /4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}를 사용하여 단일 섹션 업데이트

논리적(분산) 라우터 NSX Edge 장치에 대해서만 **defaultOriginate** 매개 변수가 다음 메서드로부터 제거됨:

- GET/PUT /api/4.0/edges/{edge-id}/routing/config/ospf
- GET/PUT /api/4.0/edges/{edge-id}/routing/config/bgp
- GET/PUT /api/4.0/edges/{edge-id}/routing/config

NSX 6.3.0 이상 논리적 (분산) 라우터 Edge 장치에서 defaultOriginate를 true로 설정하면 실패합니다.

모든 IS-IS 메서드가 NSX Edge 라우팅에서 제거되었습니다.

- GET/PUT/DELETE /4.0/edges/{edge-id}/routing/config/isis
- GET/PUT /4.0/edges/{edge-id}/routing/config

업그레이드 정보

- [NSX 및 vSphere 관련 업그레이드 정보](#)
- [NSX 구성 요소 관련 업그레이드 정보](#)
- [FIPS 관련 업그레이드 정보](#)

참고: NSX 백업에 SFTP를 사용하는 경우 6.3.x부터 지원되는 보안 알고리즘 목록은 [백업 및 복원](#)을 참조하십시오.

참고: 설치 및 업그레이드에 영향을 주는 알려진 문제 목록은 [설치 및 업그레이드에 대한 알려진 문제](#) 섹션을 참조하십시오.

NSX 및 vSphere 관련 업그레이드 정보

- NSX를 업그레이드하려면 호스트 클러스터 업그레이드(호스트 VIB를 업그레이드)를 포함하여 전체 NSX 업그레이드를 수행해야 합니다. 지침을 보려면 [호스트 클러스터 업그레이드](#) 섹션을 포함한 [NSX 업그레이드 가이드](#)를 참조하십시오.
- **시스템 요구 사항:** NSX를 설치하고 업그레이드할 때의 시스템 요구 사항에 관해서는 NSX 설명서의 [NSX의 시스템 요구 사항](#) 섹션을 참조하십시오.

NSX 6.3.0에서 NSX Edge 장치 디스크 크기가 변경되었습니다.

- 소형, 대형, 4배 대형: 584MB 디스크 1개 + 512MB 디스크 1개
- 2배 대형: 584MB 디스크 1개 + 2GB 디스크 1개 + 256MB 디스크 1개

- **NSX 6.x에서의 업그레이드 경로:** [VMware 제품 상호 운용성 매트릭스](#)에는 VMware NSX에서의 업그레이드 경로에 대한 자세한 내용이 나와 있습니다. 크로스 vCenter NSX 업그레이드는 [NSX 업그레이드 가이드](#)에서 다룹니다.

- **다운그레이드는 지원되지 않습니다.**

- 항상 업그레이드를 진행하기 전에 NSX Manager의 백업을 캡처하십시오.
- NSX가 업그레이드되면 NSX를 다운그레이드할 수 없습니다.

- NSX 6.3.x로의 업그레이드에 성공했는지 **검증**하려면 [기술 자료 문서 2134525](#)를 참조하십시오.

- vCloud Networking and Security에서 NSX 6.3.0으로의 업그레이드는 지원되지 않습니다. 먼저 지원되는 6.2.x 릴리스로 업그레이드해야 합니다.
- **vSphere 6.5a로 업그레이드:** vSphere 5.5 또는 6.0에서 vSphere 6.5a로 업그레이드하는 경우 먼저 NSX 6.3.0으로 업그레이드해야 합니다. NSX 업그레이드 가이드에서 [NSX 환경에서 vSphere 업그레이드](#)를 참조하십시오.

참고: NSX 6.2.x는 vSphere 6.5와 호환되지 않습니다.

- **파트너 서비스 호환성:** 사이트에서 Guest Introspection 또는 네트워크 검사에 대해 VMware 파트너 서비스를 사용하는 경우 업그레이드하기 전에 [VMware 호환성 가이드](#)를 검토하여 벤더의 서비스가 이 NSX 릴리스와 호환되는지 확인해야 합니다.
- 환경에 하드웨어 게이트웨이(하드웨어 VTEP)가 설치된 경우 NSX 6.3.0으로의 업그레이드가 차단됩니다. 업그레이드를 진행하려면 VMware 지원 팀에 문의해야 합니다. 자세한 내용은 [VMware 기술 자료 문서 2148511](#)을 참조하십시오.
- **vSphere Web Client 재설정:** NSX Manager를 업그레이드한 후에는 [NSX 업그레이드 설명서](#)에 설명되어 있는 대로 vSphere Web Client 서버를 재설정해야 합니다. 이렇게 하기 전까지는 vSphere Web Client에 **Networking & Security** 탭이 표시되지 않을 수 있습니다. 또한 브라우저 캐시 또는 기록을 지워야 할 수 있습니다.
- **상태 비저장 환경:** 상태 비저장 호스트 환경에서의 NSX 업그레이드에는 새로운 VIB URL이 사용됩니다. 상태 비저장 호스트 환경에서 NSX를 업그레이드할 경우, NSX 업그레이드 프로세스 중에 새로운 VIB가 호스트 이미지 프로파일에 미리 추가됩니다. 그 결과 상태 비저장 호스트의 NSX에 대한 업그레이드 프로세스는 다음과 같은 순서로 진행됩니다.

1. 고정 URL을 통해 NSX Manager에서 최신 NSX VIB를 수동으로 다운로드합니다.

2. VIB를 호스트 이미지 프로파일에 추가합니다.

NSX 6.2.0 전에는 특정 버전의 ESX 호스트에 대한 VIB를 찾을 수 있는 URL이 NSX Manager에 하나밖에 없었습니다. 즉, 관리자는 NSX 버전에 관계없이 하나의 URL만 알고 있으면 되었습니다. NSX 6.2.0 이상에서는 새로운 NSX VIB가 서로 다른 URL을 통해 제공됩니다. 올바른 VIB를 찾으려면 다음과 같은 단계를 수행해야 합니다.

- <https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties>에서 새 VIB URL을 찾습니다.
- 해당하는 URL에서 필요한 ESX 호스트 버전의 VIB를 가져옵니다.
- 그런 다음 VIB를 호스트 이미지 프로파일에 추가합니다.

NSX 구성 요소 관련 업그레이드 정보

- **ESG(Edge Services Gateway) 업그레이드:**
NSX 6.2.5부터 NSX Edge 업그레이드 시에 리소스 예약이 수행됩니다. 리소스가 부족한 클러스터에서 vSphere HA가 사용되도록 설정되면 vSphere HA 제약 조건 위반으로 인해 업그레이드 작업이 실패할 수 있습니다.

이러한 업그레이드 실패를 방지하려면 ESG를 업그레이드하기 전에 다음 단계를 수행하십시오.

1. 항상 vSphere HA에 대한 모범 사례에 따라 설치를 수행합니다. [기술 자료 문서 1002080](#) 문서를 참조하십시오.
2. NSX 튜닝 구성 API를 사용합니다.
PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>
edgeVCpuReservationPercentage 및 edgeMemoryReservationPercentage 값이 폼 팩터에 대해 사용 가능한 리소스 범위 내에 있는지 확인합니다(기본값은 아래 표 참조).

설치 또는 업그레이드 시에 값을 명시적으로 설정하지 않은 경우 다음 리소스 예약이 NSX Manager에서 사용됩니다.

| NSX Edge 폼 팩터 | CPU 예약 | 메모리 예약 |
|------------------|---------|--------|
| 소형 | 1000MHz | 512MB |
| 대형 | 2000MHz | 1024MB |
| 4배 대형 | 4000MHz | 2048MB |
| 초대형 | 6000MHz | 8192MB |

- NSX Edge 장치로 업그레이드하기 전에 NSX에 사용할 수 있게 호스트 클러스터를 준비해야 합니다. VIX 채널을 통한 NSX Manager 및 Edge 간 관리부 통신이 6.3.0부터 더 이상 지원되지 않습니다. 메시지 버스 채널만 지원됩니다. NSX 6.2.x 이하 버전에서 NSX 6.3.0 이상으로 업그레이드할 때는 NSX Edge 장치가 배포된 호스트 클러스터가 NSX에 사용할 수 있게 준비되어 있는지와 메시징 인프라 상태가 녹색인지 확인해야 합니다. 호스트 클러스터가 NSX에 사용할 수 있게 준비되지 않은 경우 NSX Edge 장치 업그레이드가 실패합니다. 자세한 내용은 *NSX 업그레이드 가이드*의 [NSX Edge 업그레이드](#)를 참조하십시오.

다음은 수행하여 NSX Edge가 배포될 호스트의 메시징 인프라 상태가 녹색인지 확인하십시오.

- API 메서드 GET /api/2.0/nwfabric/status?resource={resourceId}를 사용합니다. 여기서 **resourceId**는 클러스터 또는 호스트의 vCenter 관리 개체 ID(예: domain-c33 또는 host-21)입니다. 클러스터 및 호스트의 리소스 ID를 찾는 방법은 NSX API 가이드의 "vCenter 개체 ID 찾기"를 참조하십시오.
- 응답 본문에서 com.vmware.vshield.vsm.messagingInfra의 **featureId**에 해당하는 status를 확인하십시오.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- vSphere HA가 사용되도록 설정되고 Edge가 배포되는 경우 vSphere의 [가상 시스템 시작] 옵션을 사용하지 않도록 설정합니다. 6.2.4 또는 이전 NSX Edge를 6.2.5 이상으로 업그레이드한 후 vSphere HA가 사용되도록 설정되고 Edge가 배포된 클러스터에서 각 ESX Edge에 대해 vSphere [가상 시스템 시작] 옵션을 해제해야 합니다. 이를 수행하려면 vSphere Web Client를 열고, NSX Edge 가상 시스템이 있는 ESXi 호스트를 찾은 다음 [관리] > [설정]을 클릭하고 가상 시스템 아래에서 [VM 시작/종료]를 선택하고 [편집]을 클릭한 다음 가상 시스템이 수동 모드인지 확인합니다(즉, [자동 시작/종료] 목록에 추가되어 있지 않아야 합니다).
- 컨트롤러 디스크 레이아웃: 6.2.2 이전에서의 업그레이드는 컨트롤러 안정성을 개선하기 위해 데이터 및 로그에 별도의 디스크 파티션을 제공하는 6.2.3에서 도입된 새 디스크 레이아웃을 수락하지 않습니다.
- NSX 6.2.5 이상으로 업그레이드하기 전에 모든 로드 밸런서 암호 목록이 콜론으로 구분되어야 합니다. 암호 목록이 쉼표 등의 다른 구분 기호를 사용하는 경우 https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles에 PUT 호출을 수행하고 <clientSsl> 및 <serverSsl>에 있는 각 <ciphers> 목록을 콜론으로 구분된 목록으로 교체합니다. 예를 들어 요청 본문의 관련 세그먼트는 다음과 같이 표시될 수 있습니다. 모든 애플리케이션 프로파일에 대해 다음 절차를 반복하십시오.

```
<applicationProfile>
  <name>https-profile</name>
  <insertXForwardedFor>false</insertXForwardedFor>
```

```

<sslPassthrough>false</sslPassthrough>
<template>HTTPS</template>
<serverSslEnabled>true</serverSslEnabled>
<clientSsl>
  <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
  <clientAuth>ignore</clientAuth>
  <serviceCertificate>certificate-4</serviceCertificate>
</clientSsl>
<serverSsl>
  <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
  <serviceCertificate>certificate-4</serviceCertificate>
</serverSsl>
...
</applicationProfile>

```

- **6.2.0 이전의 vROP 버전에서 로드 밸런싱된 클라이언트에 대한 올바른 암호 버전 설정:** 6.2.0 이전 vROP 버전의 vROP 풀 멤버는 TLS 버전 1.0을 사용하므로 NSX 로드 밸런서 구성에서 "ssl-version=10"을 설정하여 모니터 확장 값을 명시적으로 설정해야 합니다. 지침에 대해서는 NSX 관리 가이드의 [서비스 모니터 생성](#)을 참조하십시오.

```

{
  "expected" : null,
  "extension" : "ssl-version=10",
  "send" : null,
  "maxRetries" : 2,
  "name" : "sm_vrops",
  "url" : "/suite-api/api/deployment/node/status",
  "timeout" : 5,
  "type" : "https",
  "receive" : null,
  "interval" : 60,
  "method" : "GET"
}

```

- **호스트가 설치 중 상태로 중단될 수 있음:** 대규모 NSX 업그레이드 동안 호스트가 장시간 설치 중 상태로 중단될 수 있습니다. 이 문제는 이전 NSX VIB의 제거와 관련된 문제 때문에 발생할 수 있습니다. 이 경우 이 호스트와 연결된 EAM 스레드가 VI Client 작업 목록에서 중단된 상태로 보고됩니다.

해결 방법: 다음을 수행합니다.

- VI Client를 사용하여 vCenter에 로그인합니다.
- 중단된 EAM 작업을 마우스 오른쪽 버튼으로 클릭하고 취소합니다.
- vSphere Web Client에서 클러스터에 대해 [해결]을 실행합니다. 중단된 호스트가 이제 [진행 중]으로 표시될 것입니다.
- 호스트에 로그인하고 재부팅을 실행하여 해당 호스트에 대한 업그레이드를 강제로 완료합니다.

FIPS 관련 업그레이드 정보

- NSX 6.3.0 이전의 NSX 버전에서 NSX 6.3.0 이상으로 업그레이드하는 경우 업그레이드를 완료하기 전에 FIPS 모드를 사용하도록 설정해서는 안 됩니다. 업그레이드를 완료하기 전에 FIPS 모드를 사용하도록 설정하면 업그레이드된 구성 요소와 업그레이되지 않은 구성 요소 간 통신이 중단됩니다. 자세한 내용은 NSX 업그레이드 가이드에서 [FIPS 모드 및 NSX 업그레이드 이해](#)를 참조하십시오.

- OS X Yosemite 및 OS X El Capitan에서 지원되는 암호: OS X 10.11(EL Capitan)에서 SSL VPN 클라이언트를 사용 중인 경우 AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA38, AES256-SHA 및 AES128-SHA 암호를 사용하여 연결할 수 있으며 OS X 10.10(Yosemite)을 사용 중인 경우 AES256-SHA 및 AES128-SHA 암호만 사용하여 연결할 수 있습니다.
- NSX 6.3.0으로의 업그레이드가 완료되기 전에는 FIPS를 사용하도록 설정하지 마십시오. 자세한 내용은 NSX 업그레이드 가이드에서 [FIPS 모드 및 NSX 업그레이드 이해](#)를 참조하십시오.
- FIPS를 사용하도록 설정하기 전에 파트너 솔루션이 FIPS 모드 인증을 받았는지 확인하십시오. [VMware 호환성 가이드](#) 및 관련 파트너 설명서를 참조하십시오.

알려진 문제

알려진 문제는 다음과 같이 분류됩니다.

- [일반적인 알려진 문제](#)
- [설치 및 업그레이드에 대한 알려진 문제](#)
- [NSX Manager에 대한 알려진 문제](#)
- [논리적 네트워킹에 대한 알려진 문제 및 NSX Edge에 대한 알려진 문제](#)
- [보안 서비스에 대한 알려진 문제](#)
- [모니터링 서비스에 대한 알려진 문제](#)
- [솔루션 상호 운용성에 대한 알려진 문제](#)
- [NSX Controller에 대한 알려진 문제](#)

일반적인 알려진 문제

새로 만들기 문제 1740625, 1749975: Firefox 및 Safari에서의 Mac OS UI 문제

Mac OS에서 Firefox 또는 Safari를 사용하는 경우 vSphere 6.5 Web Client의 [Networking & Security] 페이지에 있는 NSX Edge에서 [뒤로 탐색] 버튼이 작동하지 않으며 Firefox에서 UI가 응답하지 않는 경우가 있습니다.

해결 방법: Mac OS에서 Google Chrome을 사용하거나 [홈] 버튼을 클릭한 다음 필요에 따라 계속 진행합니다.

문제 1700980: 보안 패치 CVE-2016-2775의 경우 쿼리 이름이 너무 길면 lwresd에서 세분화 오류가 발생할 수 있음

NSX 6.2.4는 BIND 9.10.4를 함께 설치하지만 *named.conf*에서 lwres 옵션을 사용하지 않으므로 제품이 취약해지지 않습니다.

해결 방법: 제품이 취약해지지 않으므로 해결 방법도 필요하지 않습니다.

문제 1558285: vCenter에서 Guest Introspection이 있는 클러스터를 삭제하면 null 포인터 예외가 발생함 vCenter에서 클러스터를 제거하기 전에 먼저 Guest Introspection과 같은 서비스를 제거해야 합니다.

해결 방법: 연결된 클러스터가 없는 서비스 배포에 대한 EAM 에이전시를 삭제합니다.

문제 1629030: 패킷 캡처 중앙 CLI(패킷 캡처 디버그 및 패킷 캡처 표시)를 사용하려면 vSphere 5.5U3 이상이 필요함

이러한 명령은 이전 vSphere 5.5 릴리스에서는 지원되지 않습니다.

해결 방법: 모든 NSX 고객은 vSphere 5.5U3 이상을 실행하도록 권장됩니다.

문제 1568180: vCSA(vCenter Server Appliance) 5.5 사용 시 잘못된 NSX 기능 목록

라이센스를 선택하고 **작업 > 기능 보기**를 클릭하면 vSphere Web Client에서 라이선스의 기능을 볼 수 있습니다.

NSX 6.2.3으로 업그레이드하면 라이선스가 Enterprise 라이선스로 업그레이드되어 모든 기능을 사용할 수 있게 됩니다. 그러나 vCSA(vCenter Server Appliance) 5.5에 NSX Manager가 등록되어 있는 경우에 **기능 보기**를 선택하면 새 Enterprise 라이선스가 아닌 업그레이드 전에 사용하던 라이선스의 기능 목록이 표시됩니다.

해결 방법: vSphere Web Client에 올바르게 표시되지 않는 경우라도 모든 Enterprise 라이선스는 기능이 동일합니다. 자세한 내용은 [NSX 라이선싱 페이지](#)를 참조하십시오.

설치 및 업그레이드에 대한 알려진 문제

업그레이드하기 전에 이 문서의 앞부분에 나와 있는 [업그레이드 정보](#) 섹션을 읽으십시오.

새로 만들기 문제 1734245: 데이터 보안으로 인해 6.3.0으로의 업그레이드가 실패함

데이터 보안이 서비스 정책의 일부로 구성되어 있는 경우 6.3.0으로의 업그레이드가 실패합니다. 업그레이드하기 전 모든 서비스 정책에서 데이터 보안을 제거했는지 확인합니다.

새로 만들기 문제 1801685: 호스트 연결 오류로 인해 6.2.x에서 6.3.0으로의 업그레이드 후 ESXi에서 필터를 표시할 수 없음

설치 상태가 성공적이며 방화벽이 사용되도록 설정된 것으로 표시되더라도 NSX 6.2.x에서 6.3.0으로 업그레이드하고 클러스터 VIB에서 6.3.0 비트로 업그레이드한 후 “통신 채널 상태”가 방화벽 에이전트 연결과의 NSX Manager, ControlPlane 에이전트 연결과의 NSX Manager가 다운된 것으로 표시됩니다. 이는 호스트로 전송되지 않은 방화벽 규칙 게시, 보안 정책 게시 오류, VXLAN 구성으로 이어집니다.

해결 방법: API POST:<https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize>를 사용하여 클러스터에 대한 메시지 버스 동기화 API 호출을 실행합니다.

API Body:

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{Cluster-MOID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

새로 만들기 문제 1808478: NSX 6.2.x에서 NSX 6.3.0으로 업그레이드한 후에 vmvisor 메모리를 할당할 수 없는 경우 vsfwd 서비스가 시작되지 않음

NSX 6.2.x에서 NSX 6.3.0으로 업그레이드한 후에 vmvisor 메모리를 할당할 수 없는 경우 vsfwd 서비스가 시작되지 않습니다. 자세한 내용은 [VMware 기술 자료 문서 2148974](#)를 참조하십시오.

해결 방법: VMware 고객 지원에 문의하십시오.

새로 만들기 문제 1818257: NSX 6.2.x에서 NSX 6.3.0(ESXi 6.0 포함)으로의 VXLAN 호스트 업그레이드 후에 향상된 LACP가 사용될 경우 VTEP 정보가 컨트롤러에 보고되지 않음

NSX 6.2.x에서 6.3.0(ESXi 6.0)으로 업그레이드하는 동안 호스트 업그레이드 후에 향상된 LACP가 사용될 때 VTEP 정보가 컨트롤러에 보고되지 않습니다. 자세한 내용은 [VMware 기술 자료 문서 2149210](#)을 참조하십시오.

해결 방법: VMware 고객 지원에 문의하십시오.

새로 만들기 문제 1791371: ESXi 호스트를 vSphere 6.5a로 업그레이드할 때 Guest Introspection 및 VXLAN VIB를 동시에 업그레이드하면 경보가 발생함

Guest Introspection 및 VXLAN VIB는 vSphere 6.5a에 대해 다르므로, 이러한 프로그램을 동시에 업그레이드하면 VXLAN VIB 업그레이드 중에 호스트를 재부팅하라는 경보가 표시됩니다.

해결 방법: vSphere 6.5a로 업그레이드할 때 먼저 VXLAN VIB를 설치한 다음에 Guest Introspection VIB를 설치합니다.

새로 만들기 문제 1805983: NSX 6.2.5, 6.2.6 또는 6.3.0으로 업그레이드할 때 서버 풀이 포함되지 않은 가상 서버가 작동하지 않음

서버 풀이 없는 가상 서버는 HTTP/HTTPS 리더렉션만 제공할 수 있습니다. 다른 기능은 작동하지 않습니다.

해결 방법: 멤버가 없는 더미 풀을 생성한 후 가상 서버에 할당하십시오.

새로 만들기 문제 1797307: 업그레이드 또는 다시 배포 후에 NSX Edge가 분할 브레인으로 실행될 수 있음

대기 NSX Edge에서 show service highavailability CLI 명령을 실행하면 고가용성 상태가 "대기"로 표시되지만 구성 엔진 상태는 "활성"입니다.

해결 방법: 대기 NSX Edge를 재부팅합니다.

새로 만들기 문제 1789989: 호스트 클러스터 업그레이드 동안 데이터부에서 패킷이 손실될 수 있음

VIB 업그레이드 동안 VIB에 유지되는 VSFWD(vShield 방화벽 데몬)의 암호 파일이 제거되므로 VSFWD에서 이전 암호를 사용하여 NSX Manager에 연결할 수 없으며 새 암호가 업데이트될 때까지 기다려야 합니다. 호스트 재부팅 후에 이 프로세스를 완료하는 데 다소 시간이 걸리지만 완전 자동화 DRS 클러스터에서는 준비된 호스트가 나타나는 즉시 VM이 이동되며, VSFWD 프로세스가 해당 시점에 준비 완료 상태가 아니므로 짧은 시간 동안 데이터부에서 패킷이 손실될 수 있습니다.

해결 방법: 호스트가 다시 나타나는 즉시 장애가 복구되지 않고 이러한 VM의 새로 준비된 호스트에 대한 장애 복구가 지연됩니다.

새로 만들기 문제 1797929: 호스트 클러스터 업그레이드 후 메시지 버스 채널 다운

호스트 클러스터 업그레이드 후에 vCenter 6.0(및 이전 버전)은 이벤트 "다시 연결"을 생성하지 않으므로 NSX Manager는 호스트에서 메시징 인프라를 설정하지 않습니다. 이 문제는 vCenter 6.5에서 해결되었습니다.

해결 방법: 아래와 같이 메시징 인프라를 다시 동기화하십시오.

POST <https://<ip>/api/2.0/nwfabric/configure?action=synchronize>

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>host-15</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

새로 만들기 문제 1802688: NSX 6.2.x에서 6.3.0으로 업그레이드해도 업데이트된 DFW 사용 상태가 반영되지 않음

NSX를 6.2.x에서 6.3.0으로 업그레이드하고 클러스터 VIB를 6.3.0 비트로 업그레이드한 후에 업그레이드된 클러스터에 새 호스트를 추가하면, 새 VIB가 새 호스트에 설치되었더라도 관련 호스트 및 클러스터의 방화벽 상태는 계속 사용 중으로 표시되며 상태가 업데이트되지 않습니다.

해결 방법: 다음을 수행합니다.

1. API POST:<https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize>를 사용하여 호스트에 대한 메시지 버스 동기화 API 호출을 실행합니다. 이렇게 하면 호스트 및 클러스터 방화벽 상태가 "사용 안 함"이 됩니다.

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{HOST-ID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

2. 이제 [UI 설치] > [호스트 준비] 페이지에서 해당 클러스터에 대한 방화벽을 사용하도록 설정하십시오. 이렇게 하면 해당 클러스터의 모든 호스트가 DFW 사용 모드로 바뀝니다.

문제 1768144: 새로운 제한을 초과하는 이전 NSX Edge 장치 리소스 예약으로 인해 업그레이드 또는 다시 배포 중에 실패할 수 있음

NSX 6.2.4 및 이전 버전에서 NSX Edge 장치에 대해 임의의 대용량 리소스 예약을 지정할 수 있었습니다. NSX는 최댓값을 적용하지 않았습니다. ☒ NSX Manager를 6.2.5 이상으로 업그레이드한 후에 선택된 폼 팩터에 대해 새로 적용된 최댓값을 초과하는 리소스(특히 메모리)가 기존 Edge에 대해 예약되면 Edge 업그레이드 또는 다시 배포(업그레이드를 트리거하는) 중에 실패할 수 있습니다. 예를 들어 사용자가 6.2.5 이전의 LARGE Edge에 대해 1000MB의 메모리를 예약하고, 6.2.5로 업그레이드한 후에 장치 크기를 COMPACT로 변경하면 사용자 지정 메모리 예약이 새로 적용된 최댓값(이 경우 COMPACT Edge에 대한 512)을 초과하게 되어 작업이 실패합니다.

NSX 6.2.5부터 권장되는 리소스 할당에 대한 자세한 내용은 [ESG\(Edge Services Gateway\) 업그레이드](#)를 참조하십시오.

해결 방법: 다음 장치 REST API PUT <https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/> 를 사용하여 다른 장치 변경 없이, 폼 팩터에 대해 지정된 값 범위 내에서 메모리 예약을 다시 구성합니다. 이 작업이 완료되면 장치 크기를 변경할 수 있습니다.

문제 1600281: [서비스 배포] 탭에서 Guest Introspection에 대한 USVM 설치 상태가 [실패]로 표시됨

Guest Introspection 범용 SVM에 대한 지원 데이터스토어가 오프라인 상태가 되거나 액세스할 수 없게 되면 USVM을 재부팅하거나 재배포하여 복구해야 할 수 있습니다.

해결 방법: USVM을 재부팅하거나 재배포하여 복구합니다.

문제 1660373: vCenter가 만료된 NSX 라이선스를 적용

vSphere 5.5 업데이트 3 또는 vSphere 6.0.x 기준으로 vSphere Distributed Switch가 NSX 라이선스에 포함됩니다. 하지만 vCenter에서는 NSX 라이선스가 만료된 경우 ESX 호스트를 vSphere Distributed Switch에 추가할 수 없습니다.

해결 방법: 호스트를 vSphere Distributed Switch에 추가하려면 NSX 라이선스가 활성화 상태여야 합니다.

문제 1569010/1645525: vCenter 5.5에 연결된 시스템에서 6.1.x를 NSX for vSphere 6.2.3으로 업그레이드할 경우 [라이선스 키 할당] 창의 제품 필드에 NSX 라이선스가 "NSX for vSphere - Enterprise"와 같은 구체적인 버전이 아닌 일반적인 "NSX for vSphere"로 표시됩니다.

해결 방법: 없음.

문제 1636916: vCloud Air 환경에서 NSX Edge 버전이 vCNS 5.5.x에서 NSX 6.x로 업그레이드될 때 소스 프로토콜 값이 "any"인 Edge 방화벽 규칙이 "tcp:any, udp:any"로 변경됨
결과적으로 ICMP 트래픽이 차단되고 패킷 손실이 발생할 수 있습니다.

해결 방법: NSX Edge 버전을 업그레이드하기 전에 보다 구체적인 Edge 방화벽 규칙을 만들고 "any"를 구체적인 소스 포트 값으로 바꾸십시오.

문제 1660355: 6.1.5에서 6.2.3 이상으로 마이그레이션된 VM이 TFTP ALG를 지원하지 않음

호스트가 사용되도록 설정되어 있어도 6.1.5에서 6.2.3 이상으로 마이그레이션된 VM이 TFTP ALG를 지원하지 않습니다.

해결 방법: 제외 목록에서 VM을 추가한 후 제거하거나 VM을 다시 시작하여 TFTP ALG를 지원하는 새로운 6.2.3 이상 필터가 생성되도록 합니다.

문제 1474238: vCenter 업그레이드 후 vCenter와 NSX의 연결이 끊길 수 있음

vCenter에 내장된 SSO를 사용하고 vCenter 5.5를 vCenter 6.0으로 업그레이드하는 경우 vCenter와 NSX의 연결이 끊길 수 있습니다. 이는 vCenter 5.5가 루트 사용자 이름을 사용하여 NSX에 등록된 경우 발생합니다. NSX 6.2에서는 루트를 사용한 vCenter 등록이 더 이상 지원되지 않습니다.

참고: 외부 SSO를 사용하는 경우에는 아무것도 변경할 필요가 없습니다. 동일한 사용자 이름(예: admin@mybusiness.mydomain)을 사용할 수 있으며 vCenter 연결이 끊어지지 않습니다.

해결 방법: 루트 대신 administrator@vsphere.local 사용자 이름을 사용하여 NSX에 vCenter를 다시 등록합니다.

문제 1332563: 전원을 끄기 전에 에이전트 VM(SVA)에 대한 게스트 OS 종료

호스트가 유지 보수 모드로 전환되면 모든 서비스 장치가 정상적으로 종료되는 대신 전원이 꺼집니다. 이로 인해 타사 장치 내에서 오류가 발생할 수 있습니다.

해결 방법: 없음.

문제 1473537: 서비스 배포 보기를 사용하여 배포된 서비스 장치의 전원을 끌 수 없음

해결 방법: 계속하기 전에 다음을 확인하십시오.

- 가상 시스템의 배포가 완료되었습니다.
- vCenter 작업 창에 표시된 가상 시스템에 대한 복제, 재구성 등의 작업이 진행되지 않습니다.

- 배포가 시작된 후 가상 시스템의 vCenter 이벤트 창에 다음 이벤트가 표시됩니다.

에이전트 VM <vm name>이(가) 프로비저닝되었습니다.
에이전트 워크플로우를 진행하려면 에이전트를 사용 가능으로 표시하십시오.

이 경우 서비스 가상 시스템을 삭제하십시오. 서비스 배포 UI에 배포가 실패로 표시됩니다. 빨간색 아이콘을 클릭하면 호스트에 대해 에이전트 VM을 사용할 수 없다는 경보가 표시됩니다. 이 경보를 해결하면 가상 시스템이 다시 배포되고 전원이 켜집니다.

사용 환경 내 모든 클러스터가 준비되지 않은 경우, 분산 방화벽에 대한 업그레이드 메시지가 [설치] 페이지의 [호스트 준비] 탭에 표시되지 않음

네트워크 가상화를 위해 클러스터를 준비하면 해당 클러스터에 분산 방화벽이 사용되도록 설정됩니다. 사용 환경 내 모든 클러스터가 준비되지 않은 경우 분산 방화벽에 대한 업그레이드 메시지가 [호스트 준비] 탭에 표시되지 않습니다.

해결 방법: 다음 REST 호출을 사용하여 분산 방화벽을 업그레이드합니다.

PUT <https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state>

문제 1215460: 서비스 추가/제거 업그레이드 후에 서비스 그룹이 수정된 경우 이 변경 내용이 방화벽 테이블에 반영되지 않음

사용자 생성 서비스 그룹이 업그레이드 도중 Edge Firewall 테이블에서 확장됩니다. 즉, 방화벽 테이블에서 서비스 열이 서비스 그룹 내 모든 서비스를 표시합니다. 서비스 추가/제거 업그레이드 후에 서비스 그룹이 수정된 경우 이 변경 내용이 방화벽 테이블에 반영되지 않습니다.

해결 방법: 이름이 다른 서비스 그룹을 새로 만든 후 이 서비스 그룹을 방화벽 규칙에 사용합니다.

문제 1413125: 업그레이드 후 SSO를 재구성할 수 없음

NSX Manager에 구성된 SSO 서버가 vCenter Server의 유일한 기본 서버인 경우, vCenter Server를 버전 6.0으로 업그레이드하고 NSX Manager를 버전 6.x로 업그레이드한 이후에 NSX Manager에 SSO 설정을 재구성할 수 없습니다.

해결 방법: 없음.

문제 1266433: SSL VPN이 업그레이드 알림을 원격 클라이언트에 보내지 않음

SSL VPN 게이트웨이가 사용자에게 업그레이드 알림을 보내지 않습니다. 관리자가 SSL VPN 게이트웨이(서버)가 업데이트되고 해당 클라이언트를 업데이트해야 함을 원격 사용자에게 직접 알려야 합니다.

해결 방법: 사용자가 이전 버전의 클라이언트를 제거하고 최신 버전을 수동으로 설치해야 합니다.

문제 1474066: IP 검색을 사용하거나 사용하지 않도록 설정하는 NSX REST API 호출이 영향을 미치지 않는 것 같음

호스트 클러스터 준비가 아직 완료되지 않은 경우, IP 검색을 사용하거나 사용하지 않도록 설정하는 NSX REST API 호출(<https://<nsxmgr-ip>/api/2.0/xvs/networks/universalwire-5/features>)이 아무런 효과가 없습니다.

해결 방법: 이 API 호출을 실행하기 전에 호스트 클러스터 준비가 완료되었는지 확인합니다.

문제 1459032: VXLAN 게이트웨이 구성 중 오류

정적 IP 풀을 사용하는 VXLAN을 구성하는 경우(**Networking & Security>설치>호스트 준비>VXLAN 구성**), 게이트웨이가 제대로 구성되지 않았거나 연결이 불가능하여 VTEP에 IP 풀 게이트웨이 IP를 설정할 수 없으면, 호스트 클러스터에 대해 VXLAN 구성이 오류 상태(RED)로 전환됩니다.

오류 메시지는 호스트에서 VXLAN 게이트웨이를 설정할 수 없음이며 오류 상태는

VXLAN_GATEWAY_SETUP_FAILURE입니다. REST API 호출 GET <https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>>에서 VXLAN 상태가 다음과 같습니다.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
```

```
<message>VXLAN Gateway cannot be set on host</message>
<installed>true</installed>
<enabled>true</enabled>
<errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

해결 방법: 오류를 수정하는 옵션에는 두 가지가 있습니다.

- 옵션 1: 호스트 클러스터에 대한 VXLAN 구성을 제거하고, 게이트웨이가 제대로 구성되고 연결 가능한지 확인하여 IP 풀에서 기본 게이트웨이 설정을 수정한 다음 호스트 클러스터에 대한 VXLAN을 재구성합니다.
- 옵션 2: 다음 단계를 수행하십시오.
 1. 게이트웨이가 제대로 구성되고 연결 가능한지 확인하여 IP 풀에서 기본 게이트웨이 설정을 수정합니다.
 2. 호스트에 활성화된 VM 트래픽이 없도록 호스트를 유지 보수 모드로 전환합니다.
 3. 호스트에서 VXLAN VTEP를 삭제합니다.
 4. 호스트의 유지 보수 모드 설정을 해제합니다. 호스트의 유지 보수 모드 설정을 해제하면 NSX Manager에서 VXLAN VTEP 생성 프로세스가 트리거됩니다. NSX Manager는 호스트에서 필요한 VTEP의 재생성을 시도합니다.

문제 1462319: esx-dvfilter-switch-security VIB가 더 이상 "esxcli software vib list | grep esx" 명령의 출력에 존재하지 않습니다.

NSX 6.2부터 esx-dvfilter-switch-security 모듈은 esx-vxlan VIB 내에 포함됩니다. 6.2에서 설치되는 유일한 NSX VIB는 esx-vsip 및 esx-vxlan입니다. NSX를 6.2로 업그레이드하는 동안 이전 esx-dvfilter-switch-security VIB는 ESXi 호스트에서 제거됩니다.

NSX 6.2.3부터 esx-vsip 및 esx-vxlan NSX VIB와 함께 세 번째 VIB인 esx-vgpi가 제공됩니다. 설치가 성공하면 세 VIB가 모두 표시됩니다.

해결 방법: 없음.

문제 1481083: 명시적 페일오버 팀 구성이 구성된 논리적 라우터가 업그레이드 후 패킷을 제대로 전달하지 못함
호스트가 ESXi 5.5를 실행 중인 경우 명시적 페일오버 NSX 6.2 팀 구성 정책은 논리적 분산 라우터에서 여러 활성 업링크를 지원하지 않습니다.

해결 방법: 하나의 활성 업링크만 존재하며 다른 업링크는 대기 모드가 되도록 명시적 페일오버 팀 구성 정책을 수정합니다.

문제 1485862: 호스트 클러스터에서 NSX를 제거하면 경우에 따라 오류 조건이 발생함

설치: 호스트 준비 탭에서 제거 작업을 사용하면 오류가 발생하고 호스트에 대해 EAM 로그에 eam.issue.OrphanedAgency 메시지가 나타날 수 있습니다. 해결 작업을 사용하고 호스트를 재부팅하면 NSX VIB가 성공적으로 제거되었어도 오류 상태가 계속됩니다.

해결 방법: 연결이 끊어진 에이전시를 vSphere ESX Agent Manager에서 삭제합니다(**관리: vCenter Server 확장: vSphere ESX Agent Manager**).

문제 1411275: NSX for vSphere 6.2에서 백업 및 복구를 수행한 후 vSphere Web Client에 [Networking & Security] 탭이 표시되지 않음

NSX for vSphere 6.2로 업그레이드한 후 백업 및 복원 작업을 수행하면 vSphere Web Client에 **Networking & Security** 탭이 표시되지 않습니다.

해결 방법: NSX Manager 백업을 복구하면 장치 관리자에서 로그아웃됩니다. 몇 분 정도 기다린 후 vSphere Web Client에 로그인합니다.

설치 페이지의 서비스 배포 탭을 사용해 배포한 서비스 가상 시스템의 전원이 켜지지 않음

해결 방법: 다음 단계를 따릅니다.

1. 클러스터 내 ESX Agent 리소스 풀에서 서비스 가상 시스템을 수동으로 제거합니다.

2. **Networking & Security**를 클릭하고 **설치**를 클릭합니다.
3. **서비스 배포** 탭을 클릭합니다.
4. 적절한 서비스를 선택하고 **해결** 아이콘을 클릭합니다.
그러면 서비스 가상 시스템이 다시 배포됩니다.

문제 1764460: 호스트 준비를 완료한 후에 모든 클러스터 멤버가 준비 상태로 표시되지만 클러스터 수준이 [잘못됨]으로 잘못 표시됨

호스트 준비를 완료한 후에 모든 클러스터 멤버가 [준비] 상태로 제대로 표시되지만 클러스터 수준이 [잘못됨]으로 표시되며 호스트가 이미 재부팅되었어도 호스트를 재부팅해야 한다는 이유가 표시됩니다.

해결 방법: 빨간색 주의 아이콘을 클릭하고 [해결]을 선택합니다.

NSX Manager에 대한 알려진 문제

새로 만들기 문제 1800820: 이전 UDLR 인터페이스가 시스템에서 이미 삭제된 경우 보조 NSX Manager에서 UDLR 인터페이스 업데이트가 실패함

기본 NSX Manager에서 Replicator의 작동이 중지되는 시나리오에서는 기본 NSX Manager에서 UDLR(범용 분산 논리적 라우터) 및 ULS(범용 논리적 스위치) 인터페이스를 삭제하고 새로 생성한 후 보조 NSX Manager에서 복제해야 합니다. 이 경우 복제 중에 보조 NSX Manager에서 새 ULS가 생성되고 UDLR이 새 ULS에 연결되지 않으므로 UDLR 인터페이스는 보조 NSX Manager에서 업데이트되지 않습니다.

해결 방법: Replicator가 실행되고 있는지 확인하고 기본 NSX Manager에서 새로 만든 ULS를 백업으로 포함하는 UDLR 인터페이스(LIF)를 삭제하고 같은 백업 ULS를 사용해서 UDLR 인터페이스(LIF)를 다시 생성합니다.

새로 만들기 문제 1770436: 중복된 Ip가 없는 경우에도 경고가 생성됨

arping 명령은 해당하는 경우가 아닌 경우에도 네트워크에서 NSX Manager IP 주소가 중복되었다고 보고하는 경우가 있습니다. 이는 오탐지 이벤트를 생성합니다.

해결 방법: VMware 고객 지원에 문의하십시오.

새로 만들기 문제 1772911: NSX Manager가 디스크 공간을 소비하면서 매우 느리게 작동하고 작업 및 작업 테이블 크기가 100% CPU 사용량에 가깝게 증가함

다음 문제가 발생합니다.

- NSX Manager CPU 사용량이 100%에 다다르거나 정기적으로 100% 사용량으로 증가하며 NSX Manager 장치에 리소스를 더 추가해도 차이가 없습니다.
- NSX Manager CLI(명령줄 인터페이스)에서 show process monitor 명령을 실행할 경우 최고 CPU 주기를 소비하는 Java 프로세스가 표시됩니다.
- NSX Manager CLI에서 show filesystems 명령을 실행하면 /common 디렉토리가 아주 높은 사용량 상태(예: 90% 초과)를 나타냅니다.
- 일부 구성 변경이 시간 초과되고(경우에 따라 50분 이상 소요됨) 적용되지 않습니다.

자세한 내용은 [VMware 기술 자료 문서 2147907](#)을 참조하십시오.

해결 방법: 이 문제의 해결 방법을 보려면 VMware 고객 지원에 문의하십시오.

새로 만들기 문제 1785142: 기본 및 보조 NSX Manager 간 통신이 차단될 경우 기본 NSX Manager에서 '동기화 문제'를 표시하는 데 시간이 지연됨

기본 및 보조 NSX Manager 간 통신이 차단될 경우 기본 NSX Manager에서 '동기화 문제'가 바로 표시되지 않습니다.

해결 방법: 통신이 다시 설정될 때까지 20분 정도 기다리십시오.

새로 만들기 문제 1786066: 크로스 vCenter NSX 설치에서 보조 NSX Manager의 연결을 끊으면 NSX Manager가 보조 NSX Manager로 다시 연결할 수 없게 될 수 있음

크로스 vCenter NSX 설치에서 보조 NSX Manager의 연결을 끊을 경우 나중에 해당 NSX Manager를 보조 NSX Manager로 다시 추가하지 못할 수 있습니다. NSX Manager를 보조 NSX Manager로 다시 연결하려고 하면 NSX Manager가 vSphere Web Client의 [관리] 탭에서 "보조"로 표시되지만 기본 NSX Manager로의 연결이 설정되지 않습니다.

해결 방법: 다음을 수행합니다.

1. 기본 NSX Manager에서 보조 NSX Manager의 연결을 끊습니다.
2. 보조 NSX Manager를 기본 NSX Manager에 다시 추가합니다.

새로 만들기 문제 1713669: 데이터베이스 테이블 ai_useripmap이 너무 커질 경우 디스크가 꽉 차서 NSX Manager가 실패함

이 문제는 NSX Manager 장치 디스크가 꽉 차게 되어 NSX Manager가 실패하도록 합니다. 재부팅 후에 postgres 프로세스를 시작할 수 없습니다. "/common" 파티션이 꽉 찼습니다. 이 문제는 ELS(이벤트 로그 서버)에 과도한 로드가 발생하는 사이트와 대량의 GI(Guest Introspection) 트래픽이 있는 사이트에서 일반적으로 발생합니다. IDFW(ID 방화벽)를 사용하는 사이트는 자주 영향을 받습니다. 자세한 내용은 [VMware 기술 자료 문서 2148341](#)을 참조하십시오.

해결 방법: 이 문제를 복구하기 위한 도움이 필요한 경우 VMware 고객 지원에 문의하십시오.

문제 1787542: 기본 NSX Manager에 DB를 복원한 후 보조 NSX Manager 로그에서 예외 발생
기본 Manager에 DB를 복원한 후 복구된 범용 DFW 섹션이 보조 NSX Manager에서 보이지 않습니다.

해결 방법: 없음. 보조 NSX Manager를 재부팅하여 복구합니다.

새로 만들기 문제 1715354: REST API의 가용성 지연

FIPS 모드가 토글될 때 NSX Manager가 다시 시작된 후 NSX Manager API가 가동되어 실행되는 데 다소 시간이 걸립니다. API가 정지된 경우 이러한 문제가 나타날 수 있지만 컨트롤러에서 NSX Manager로 연결을 다시 설정하는 데 시간이 걸리기 때문에 이 문제가 발생합니다. NSX API 서버가 가동되어 실행될 때까지 기다리고 작업을 수행하기 전에 모든 컨트롤러가 연결된 상태인지 확인하는 것이 좋습니다.

문제 1441874: vCenter Linked Mode 환경에서 단일 NSX Manager를 업그레이드하면 오류 메시지가 표시됨
여러 VMware vCenter Server에 여러 NSX Manager가 있는 환경의 [vSphere Web Client] > [Networking & Security] > [설치] > [호스트 준비]에서 하나 이상의 NSX Manager를 선택하면 다음 오류가 표시됩니다.
“NSX Manager와의 통신을 설정할 수 없습니다. 관리자에게 문의하십시오.”

해결 방법: 자세한 내용은 [VMware 기술 자료 문서 2127061](#)을 참조하십시오.

문제 1696750: PUT API를 통해 NSX Manager에 IPv6 주소를 할당한 경우 변경 내용이 반영되려면 재부팅해야 함

[https://{NSX Manager IP 주소}/api/1.0/appliance-management/system/network](#)를 통해 NSX Manager에 대해 구성된 네트워크 설정을 변경할 경우 시스템을 재부팅해야 변경 내용이 반영됩니다. 재부팅할 때까지 기존 설정이 그대로 표시됩니다.

해결 방법: 없음.

문제 1529178: 공통 이름이 포함되지 않은 서버 인증서를 업로드하면 "내부 서버 오류" 메시지가 반환됨

공통 이름이 없는 서버 인증서를 업로드하면 "내부 서버 오류" 메시지가 표시됩니다.

해결 방법: SubAltName과 공통 이름이 모두 있거나 공통 이름만이라도 있는 서버 인증서를 사용합니다.

문제 1655388: Windows 10 OS(JA, CN 및 DE 언어용)에서 IE11/Edge 브라우저 사용 시 NSX Manager 6.2.3 UI가 로컬 언어가 아닌 영어로 표시됨

Windows 10 OS(JA, CN 및 DE 언어용)에서 IE11/Edge 브라우저를 사용하여 NSX Manager 6.2.3을 실행하면 영어가 표시됩니다.

해결 방법:

다음 단계를 수행합니다.

1. Microsoft 레지스트리 편집기(regedit.exe)를 실행하고 컴퓨터 > HKEY_CURRENT_USER > SOFTWARE > Microsoft > Internet Explorer > International로 이동합니다.
2. AcceptLanguage 파일 값을 모국어로 바꿉니다. 예를 들어 언어를 DE로 바꾸고 싶다면 값을 변경하고 DE가 첫 번째 위치에 있도록 합니다.

3. 브라우저를 다시 시작하고 NSX Manager에 다시 로그인합니다. 올바른 언어가 표시됩니다.

문제 1435996: NSX Manager에서 CSV 형식으로 내보낸 로그 파일에 날짜/시간이 아니라 epoch가 타임스탬프로 표시됨

vSphere Web Client를 사용하여 NSX Manager에서 CSV로 내보낸 로그 파일이 표준 시간대 기반의 적합한 시간 대신 epoch 시간(밀리초)이 타임스탬프로 표시됩니다.

해결 방법: 없음.

문제 1644297: 기본 NSX에서 DFW 섹션에 대해 추가/삭제 작업을 수행하면 보조 NSX에서 2개의 DFW 저장된 구성이 생성됨

크로스 vCenter 설정에서 추가 범용 또는 로컬 DFW 섹션이 기본 NSX Manager에 추가되면 두 DFW 구성이 보조 NSX Manager에 추가됩니다. 이 문제는 기능에는 전혀 영향을 주지 않지만 저장된 구성 제한에 더 빠르게 도달하여 중요한 구성을 덮어쓸 수 있습니다.

해결 방법: 없음.

문제 1534877: 호스트 이름의 길이가 64자를 넘으면 NSX 관리 서비스가 실행되지 않음
OpenSSL 라이브러리를 통해 인증서를 만들려면 호스트 이름이 64자 이하여야 합니다.

문제 1537258: NSX Manager 목록이 웹 클라이언트에 표시되는 속도가 느림

여러 개의 NSX Manager가 있는 vSphere 6.0 환경에서 큰 AD 그룹 집합으로 로그인하는 사용자를 확인하는 동안 vSphere Web Client에서 NSX Manager 목록이 표시될 때까지 최대 2분이 걸릴 수 있습니다. NSX Manager 목록을 표시하려고 할 때 데이터 서비스 시간 초과 오류가 표시될 수 있습니다. 해결 방법이 없습니다. NSX Manager 목록을 보려면 목록이 로드될 때까지 기다리거나 다시 로그인해야 합니다.

문제 1534606: 호스트 준비 페이지 로드가 실패함

vCenter를 연결 모드로 실행할 경우 각 vCenter는 같은 NSX 버전의 NSX Manager에 연결되어 있어야 합니다. NSX 버전이 서로 다른 경우 vSphere Web Client는 더 높은 버전의 NSX를 실행하는 NSX Manager와만 통신할 수 있습니다. [호스트 준비] 탭에 "NSX Manager와의 통신을 설정할 수 없습니다. 관리자에게 문의하십시오"와 비슷한 오류가 표시됩니다.

해결 방법: 모든 NSX Manager를 동일한 NSX 소프트웨어 버전으로 업그레이드해야 합니다.

문제 1386874: vSphere Web Client에 [Networking & Security] 탭이 표시되지 않음

vSphere를 6.0으로 업그레이드한 후 루트 사용자 이름으로 vSphere Web Client에 로그인하면 [Networking & Security] 탭이 표시되지 않습니다.

해결 방법: administrator@vsphere.local 또는 업그레이드하기 전의 vCenter Server에서 NSX Manager에 정의되어 있던 역할을 가진 다른 vCenter 사용자로 로그인합니다.

문제 1027066: NSX Manager의 vMotion이 다음 오류 메시지를 표시할 수 있음: "가상 이더넷 카드 네트워크 어댑터 1이 지원되지 않습니다."

이러한 오류는 무시해도 됩니다. 네트워킹은 vMotion 후 올바르게 작동합니다.

문제 1477041: NSX Manager 가상 장치 요약 페이지에 DNS 이름이 표시되지 않음

NSX Manager 가상 장치에 로그인하면 요약 페이지에 DNS 이름에 대한 필드가 있습니다. NSX Manager 장치에 대해 DNS 이름이 정의된 경우에도 이 필드가 계속 비어 있습니다.

해결 방법: NSX Manager의 호스트 이름과 검색 도메인을 관리: 네트워크 페이지에서 볼 수 있습니다.

문제 1492880: NSX 명령줄 인터페이스를 사용하여 암호를 변경한 후 NSX Manager UI에서 자동으로 로그아웃되지 않음

NSX Manager에 로그인되어 있고 최근에 CLI를 사용하여 암호를 변경한 경우, 이전 암호로 NSX Manager UI에 로그인된 상태로 남아 있을 수 있습니다. 일반적으로 비활성 상태로 인해 세션이 시간 초과된 경우 NSX Manager 클라이언트에서 사용자가 자동으로 로그아웃되어야 합니다.

해결 방법: NSX Manager UI에서 로그아웃한 후 새 암호를 사용하여 다시 로그인합니다.

문제 1468613: 네트워크 호스트 이름을 편집할 수 없음

NSX Manager 가상 장치에 로그인하고 장치 관리로 이동한 후 장치 설정 관리를 클릭하고 설정 아래에서 네트워크를 클릭하여 네트워크 호스트 이름을 편집하면 잘못된 도메인 이름 목록 오류가 나타날 수 있습니다. 이 문제는 도메인 검색 필드에 지정된 도메인 이름이 쉼표 대신 공백 문자로 구분되어 있을 때 발생합니다. NSX Manager는 쉼표로 구분된 도메인 이름만 수용합니다.

해결 방법: 다음 단계를 수행합니다.

1. NSX Manager 가상 장치에 로그인합니다.
2. 장치 관리에서 장치 설정 관리를 클릭합니다.
3. 설정 패널에서 네트워크를 클릭합니다.
4. DNS 서버 옆의 편집을 클릭합니다.
5. 도메인 검색 필드에서 모든 공백 문자를 쉼표로 바꿉니다.
6. 확인을 클릭하여 변경 내용을 저장합니다.

문제 1436953: 백업에서 NSX Manager를 성공적으로 복원한 후에도 잘못된 시스템 이벤트가 생성됨

백업에서 NSX Manager를 성공적으로 복원한 후 **Networking & Security: NSX Manager: 모니터: 시스템 이벤트**로 이동하면 vSphere Web Client에 다음과 같은 시스템 이벤트가 나타납니다.

- 백업에서 NSX Manager를 복원하지 못했습니다(심각도=위험).
- NSX Manager 복원이 완료되었습니다(심각도=정보).

해결 방법: 마지막 시스템 이벤트 메시지가 성공으로 표시될 경우 시스템 생성 이벤트 메시지를 무시해도 됩니다.

문제 1489768: 데이터 센터에 네임스페이스를 추가하기 위한 NSX REST API 호출의 동작 변경

NSX 6.2의 경우 POST <https://<nsxmgr-ip>/api/2.0/namespace/datacenter/REST> API 호출은 절대 경로를 포함하는 URL을 반환합니다(예:

<http://198.51.100.3/api/2.0/namespace/api/2.0/namespace/datacenter/datacenter-1628/2>). NSX의 이전 릴리스에서는 이 API를 호출하면 상대 경로(예: [/api/2.0/namespace/datacenter/datacenter-1628/2](#))가 포함된 URL이 반환되었습니다.

해결 방법: 없음.

논리적 네트워킹에 대한 알려진 문제 및 NSX Edge에 대한 알려진 문제

새로 만들기 문제 1825416: NSX for vSphere 6.3.x로 업그레이드한 후에 vCloud Director 8.20에서 차단된 vApps가 실패함

vCloud Director 8.20에서 NSX 6.3.x로 업그레이드하고 NSX Edge Gateway를 6.3.x로 업그레이드한 후에 차단된 vApps가 실패하고 차단된 네트워크의 가상 시스템이 해당 게이트웨이와 통신하지 못합니다. 자세한 내용은 [VMware 기술 자료 문서 2150010](#)을 참조하십시오.

해결 방법: VMware 고객 지원에 문의하십시오.

새로 만들기 문제 1781438: ESG 또는 DLR NSX Edge Appliance에서 두 번 이상 BGP 경로 특성 MULTI_EXIT_DISC를 받는 경우 라우팅 서비스가 오류 메시지를 전송하지 않습니다.

Edge 라우터 또는 논리적 분산 라우터에서 두 번 이상 BGP 경로 특성 MULTI_EXIT_DISC를 받는 경우 오류 메시지를 전송하지 않습니다. RFC 4271[5초]에 따라 동일한 특성(동일한 유형이 있는 특성)이 특정 업데이트 메시지의 경로 특성 필드 내에서 두 번 이상 나타날 수 없습니다.

해결 방법: 없음.

새로 만들기 문제 1860583: DNS에 연결할 수 없는 경우 원격 sysloger를 FQDN으로 사용하지 마십시오.

NSX Edge에서 원격 sysloger가 FQDN을 사용하여 구성되고 DNS에 연결할 수 없으면 라우팅 기능에 영향을 미칠 수 있습니다. 이 문제는 일관되게 나타나지 않을 수 있습니다.

해결 방법: FQDN 대신 IP 주소를 사용하는 것이 좋습니다.

새로 만들기문제 1791264: [전송 영역]을 두 번 클릭하면 CDO 모드 사용/사용 안 함에 오류가 발생합니다.
vSphere Web Client에서 [전송 영역]을 두 번 클릭한 다음 도달하는 [요약] 페이지에서 CDO 모드를 사용하거나 사용하지 않도록 설정하려는 경우 내용이 반영되지 않습니다.

해결 방법: 다음을 수행합니다.

1. [전송 영역] 목록 페이지로 다시 이동합니다. 설치 > 논리 네트워크 준비 > 전송 영역으로 이동한 다음 원하는 [전송 영역]을 선택합니다.
2. 작업 드롭다운 메뉴에서 CDO 모드 사용/CDO 모드 사용 안 함을 선택합니다.
3. 선택한 작업이 적용됩니다.

새로 만들기문제 1773500: 잘못된 경로(0.0.0.0/32)가 NSX 충돌 유발

NSX DLR에서 0.0.0.0/32 경로를 푸시하는 경우 이 경로를 지원하지 않으며 이를 거부합니다. 그러나 연관 LIF가 삭제되고 동일한 서브넷에서 IP 주소로 다시 추가되는 경우 계속 충돌(PSOD)을 유발합니다.

해결 방법: 0.0.0.0/32는 올바른 경로가 아닙니다. 이를 구성하지 않거나 경로맵을 사용하여 이를 거부합니다.

새로 만들기문제 1769941: 중복 ARP 응답이 있는 DLR PMAC의 L2VPN 브리지 테이블 “잘못됨”

호스트의 L2VPN 서버 vxlan 트렁크 포트가 대상 MAC가 pMAC인 클라이언트 가상 시스템의 ARP 응답을 삭제하지 않아 브리지의 MAC 테이블이 잘못되어 트래픽 삭제가 초래됩니다.

해결 방법: 이 문제를 해결하려면 VXLAN 트렁크 dvport의 트래픽 필터를 추가하여 pMAC에 지정된 ARP 응답을 삭제합니다.

트래픽 한정자를 추가하려면:

1. NSX Edge가 연결된 dvport로 이동합니다.
2. [설정 편집] > [트래픽 필터링 및 표시]로 이동합니다.
3. 대상이 pMAC로 설정된 MAC 한정자를 추가합니다.

새로 만들기문제 1782321: 고가용성 상태가 올바르게 표시되더라도 일부 NSX Edge는 분할 브레인 시나리오가 될 수 있음

HA 메커니즘의 레이스 상황 때문에 “고가용성 상태”가 올바르게 표시되더라도 NSX 6.2.5 이상으로 업그레이드된 일부 NSX Edge는 분할 브레인 시나리오가 될 수 있습니다. 이 문제는 Edge 재배포 후에 발생할 수도 있습니다.

해결 방법: 대기 NSX Edge를 재부팅합니다.

새로 만들기문제 1764258: HA 페일오버 또는 하위 인터페이스로 구성된 NSX Edge에서 강제 동기화한 후 최대 8분 간 트래픽이 블랙홀 처리됨

HA 페일오버가 트리거되거나 하위 인터페이스에서 강제 동기화를 시작하는 경우 트래픽이 최대 8분 동안 블랙홀 처리됩니다.

해결 방법: HA에 하위 인터페이스를 사용하지 마십시오.

새로 만들기문제 1771760: NAT가 사용되도록 설정된 경우 NSX Edge에서 OID 유형 Counter64를 포함하는 SNMP 응답 패킷을 삭제합니다.

NSX Edge의 SNMP ALG는 SNMP 응답 패킷에서 Counter64 유형을 처리할 수 없으며 패킷이 삭제됩니다. 그 결과 클라이언트에서 요청에 대한 응답을 받지 않습니다.

해결 방법: 이 문제가 발생하면 VMware 고객 지원 팀에 문의하시기 바랍니다.

새로 만들기문제 1767135: 로드 밸런서에서 인증서 및 애플리케이션 프로파일에 액세스하려고 할 때 오류 발생

보안 관리자 권한이 있고 Edge 범위에 있는 사용자는 로드 밸런서에서 인증서 및 애플리케이션 프로파일에 액세스할 수 없습니다. vSphere Web Client에 오류 메시지가 표시됩니다.

해결 방법: 없음.

새로 만들기 문제 1792548: NSX Controller가 다음 메시지를 표시하며 중단될 수 있음: '클러스터 가입 대기 중'
NSX Controller가 다음 메시지를 표시하며 중단될 수 있음: '클러스터 가입 대기 중'(CLI 명령: show control-cluster status). 이는 컨트롤러가 작동되는 동안 컨트롤러의 eth0 및 breth0 인터페이스에 대해 동일한 IP 주소가 구성되어 있기 때문에 발생합니다. 컨트롤러에서 다음 CLI 명령을 사용하여 이 사항을 확인할 수 있습니다. show network interface

해결 방법: VMware 고객 지원에 문의하십시오.

새로 만들기 문제 1747978: OSPF 인접성이 NSX Edge HA 패일오버 후 MD5 인증으로 삭제되었습니다.
NSX Edge가 정상적인 OSPF 재시작이 구성된 HA에 대해 구성되었으며 MD5가 인증에 사용된 NSX for vSphere 6.2.4에서 OSPF가 정상적으로 시작되지 않습니다. 정지된 타이머가 OSPF 인접 노드에서 만료된 후에만 인접성이 형성됩니다.

해결 방법: 없음

새로 만들기 문제 1803220: 컨트롤러-호스트 연결이 다운될 경우 VXLAN-CDO 사용 호스트 연결이 끊어짐
CDO(Controller Disconnected Operation) 기능은 전체 컨트롤러 클러스터가 다운/연결 불가능 상태일 때 VXLAN 연결을 보장합니다. 그렇지만 컨트롤러 클러스터가 작동 상태이지만 호스트와의 연결이 끊어진 경우 컨트롤러에 연결된 다른 호스트에서 해당 호스트로 지정된 데이터부 트래픽은 계속 삭제될 수 있습니다. 이 상태가 발생하면 호스트는 VNI 기준 VTEP 목록에서 제거되었으며 원격 호스트에서 전송된 ARP가 삭제됩니다. 컨트롤러와의 연결이 끊어진 호스트에서 시작된 트래픽의 경우 CDO 기능은 이 트래픽이 적절한 대상에 도달할 수 있는지 확인합니다.

새로 만들기 문제 1804116: NSX Manager와의 통신이 끊어진 호스트에서 논리적 라우터가 잘못된 상태로 전환됨
논리적 라우터가 켜지거나 NSX Manager와의 통신이 끊어진 호스트에 다시 배포될 경우(NSX VIB 업그레이드/설치 실패 또는 호스트 통신 문제로 인해) 논리적 라우터는 잘못된 상태가 되고 강제 동기화를 통한 연속 자동 복구 작업은 실패합니다.

해결 방법: 호스트 및 NSX Manager 통신 문제를 해결한 후에 NSX Edge를 수동으로 재부팅한 후 모든 인터페이스가 표시될 때까지 기다리십시오. 강제 동기화를 통한 자동 복구 프로세스는 NSX Edge를 재부팅하므로 이 해결 방법은 논리적 라우터에만 필요하며 NSX ESG(Edge Services Gateway)에는 필요하지 않습니다.

새로 만들기 문제 1783065: IPv4 및 IPv6 주소별로 TCP와 함께 UDP 포트에 대한 로드 밸런서를 구성할 수 없음
UDP는 ipv4-ipv4, ipv6-ipv6(프론트엔드-백엔드)만 지원합니다. IPv6 링크 로컬 주소까지도 그룹 개체의 IP 주소로 임하고 푸시되며 LB 구성에서 사용할 IP 프로토콜을 선택할 수 없는 NSX Manager의 버그가 있습니다.

다음은 이 문제를 보여 주는 LB 구성 예입니다.

로드 밸런서 구성에서 풀 "vCloud_Connector"가 그룹 개체(vm-2681)를 사용해서 풀 멤버로 구성되며 이 개체는 IPv4 및 IPv6 주소를 모두 포함합니다. 그렇지만 이러한 방식은 LB L4 엔진에서 지원될 수 없습니다.

```
{
  "algorithm": {
    ...
  },
  "members": [
    {
      ... ,
      ...
    }
  ],
  "applicationRules": [],
  "name": "vCloud_Connector",
  "transparent": {
    "enable": false
  }
}
```

```
"value" : [  
  "fe80::250:56ff:feb0:d6c9",  
  "10.204.252.220"  
],  
"id" : "vm-2681"  
}
```

해결 방법:

- 옵션 1: 풀 멤버에 그룹 개체 대신 풀 멤버의 IP 주소를 입력하십시오.
- 옵션 2: VM에 IPv6를 사용하지 마십시오.

새로 만들기 문제 1773127: 많은 수의 호스트 및 논리적 스위치가 있는 설정에서는 지정된 논리적 스위치와 관련된 호스트를 표시하는 화면이 제대로 로드되지 않습니다.

많은 수의 호스트가 있는 설정에서 [논리적 스위치] > [관련 개체] > [호스트]를 선택하면 몇 분 동안 기다린 후에 vSphere Web Client가 로드되지 않으며 다음 오류가 발생합니다. 백엔드 작업이 120초 이상 소요되었으므로 데이터 서비스가 시간 초과되었습니다. 이 문제는 NSX Manager로의 원격 API 호출이 응답을 반환하는 데 너무 오래 걸리기 때문에 발생합니다.

해결 방법: 이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

- 첫 번째 옵션: [VMware 기술 자료 문서 2040626](#)에 설명된 대로 API 시간 초과를 늘려 이 문제를 피할 수 있습니다. 이 시간 초과를 늘린 후에 vSphere Web Client를 다시 시작해야 할 수 있습니다. 시간 초과를 늘릴 때 가능한 결과는 오류가 발생하지 않는다는 것이지만 페이지가 다시 로드될 때까지 2-4분 동안 기다려야 합니다.
- 두 번째 옵션: 관련 호스트가 제대로 표시되는지만 확인하려면 [홈] > [네트워킹] > [포트 그룹] > [관련 개체] > [호스트]로 이동하여 논리적 스위치와 연결된 호스트 목록을 확인할 수 있습니다.

새로 만들기 문제 1777792: 피어 끝점이 'ANY'로 설정되면 IPsec 연결이 실패함

NSX Edge의 IPsec 구성이 원격 피어 끝점을 'ANY'로 설정하면 Edge는 IPsec "서버"로 작동하며 원격 피어가 연결을 시작하는 동안 기다립니다. 그렇지만 이니시에이터가 PSK+XAUTH를 사용하여 인증 요청을 보낼 경우 Edge는 다음 오류 메시지를 표시합니다. "XXX.XXX.XX.XX:500에서 초기 기본 모드 메시지가 수신되었으나 연결이 policy=PSK+XAUTH로 인증되지 않았습니다." 또한 IPsec을 설정할 수 없습니다.

해결 방법: IPsec VPN 구성에서 ANY 대신 특정 피어 끝점 IP 주소 또는 FQDN을 사용하십시오.

새로 만들기 문제 1770114: 호스트의 성공적인 준비 후에 클러스터 수준의 오류 메시지가 지워지지 않음

충분한 IP 주소가 없는 클러스터에 IP 풀을 할당하고 이 클러스터에 호스트를 추가하려고 하면 "IP 주소 부족" 오류가 표시됩니다. 이 풀을 변경하여 추가 IP 주소를 추가하고 이 클러스터에 호스트를 성공적으로 추가할 수 있는 경우에도 클러스터 수준에서 오류 메시지가 계속 표시됩니다.

해결 방법: VMware 고객 지원에 문의하십시오.

문제 1789088: NSX Edge가 grub 명령줄 프롬프트에서 멈춤

NSX Edge가 부팅되지 못하고 grub 명령줄 프롬프트에서 멈출 수 있습니다.

해결 방법:

- 먼저 다음 사항을 조사하십시오.
 1. set 명령을 사용하여 기존 환경을 확인합니다.
 2. ls 및 cat 명령을 사용하여 /boot/grub/grub.cfg 파일을 찾아 덤프합니다.

```
grub> ls /boot  
grub> ls /boot/grub  
grub> cat /boot/grub/grub.cfg
```

3. 이때 호스트 로그를 캡처합니다(발생하는 문제와 최대한 가깝게). NFS 스토리지 문제를 나타내는 몇몇 NFS 로그가 있을 수 있습니다.

- 다음에는 NSX Edge를 수동으로 부팅합니다. 다음을 제시된 순서대로 수행합니다(이전 옵션으로 Edge 부팅이

실패하는 경우에만 다음 옵션 시도).

1. vSphere Web Client에서 [전원 재설정] 옵션을 선택하여 Edge VM을 재부팅합니다.
2. 또는 grub 구성 파일을 다시 지정합니다. 이렇게 하면 메뉴가 로드되면서 Edge가 즉시 부팅됩니다. grub 프롬프트에서 다음 명령을 호출합니다.

```
grub> configfile /boot/grub/grub.cfg
```

3. 또는 grub 프롬프트에서 다음 명령을 사용합니다.

```
grub> insmod ext2
grub> set root=(hd0,1)
grub> linux /boot/vmlinuz loglevel=3 root=/dev/sda1
grub> boot
```

문제 1741158: 구성되지 않은 새 NSX Edge를 생성하고 구성을 적용하면 Edge 서비스 활성화가 너무 빨리 진행될 수 있음

NSX API를 사용하여 구성되지 않은 새 NSX Edge를 생성한 다음 해당 Edge에서 Edge 서비스 중 하나를 사용하지 않도록 설정하는 API 호출을 수행하고(예: dhcp-enabled를 "false"로 설정) 마지막으로 사용되지 않도록 설정된 Edge 서비스에 대해 구성 변경을 적용하면 해당 서비스가 즉시 활성화됩니다.

해결 방법: 사용 안 함 상태를 유지하려는 Edge 서비스의 구성을 변경한 후에 PUT 호출을 즉시 실행하여 해당 서비스에 대해 enabled 플래그를 "false"로 설정합니다.

문제 1758500: 구성된 다음 홉 중 하나 이상이 Edge의 vNIC IP 주소인 경우 다음 홉이 여러 개 있는 정적 경로가 NSX Edge 라우팅 및 전달 테이블에 설치되지 않음

ECMP 및 여러 개의 다음 홉 주소를 사용할 때 하나 이상의 다음 홉 IP 주소가 올바른 경우 NSX에서 Edge의 vNIC IP 주소가 다음 홉으로 구성될 수 있습니다. 이 작업은 오류 또는 주의 없이 수행되지만 네트워크에 대한 경로가 Edge의 라우팅/전달 테이블에서 제거됩니다.

해결 방법: ECMP를 사용할 때 정적 경로에서 Edge의 자체 vNIC IP 주소를 다음 홉으로 구성하지 마십시오.

문제 1716464: NSX 로드 밸런서가 보안 태그가 새로 지정된 VM으로 라우팅되지 않음

지정된 태그가 있는 2개의 VM을 배포한 다음 해당 태그로 라우팅되도록 LB를 구성하면 LB는 해당 두 VM으로 라우팅됩니다. 하지만 그런 다음 해당 태그가 있는 세 번째 VM을 배포할 경우 LB는 처음 두 VM으로만 라우팅됩니다.

해결 방법: LB 풀에서 [저장]을 클릭합니다. 그러면 VM이 재검색되고 새로 태그가 지정된 VM으로 라우팅되기 시작합니다.

문제 1753621: 개인 로컬 AS가 있는 Edge가 EBGP 피어로 경로를 전송하면 모든 개인 AS 경로가 전송된 BGP 라우팅 업데이트에서 제거됨

NSX에는 현재 AS 경로에 개인 AS 경로만 포함되어 있을 때 전체 AS 경로를 eBGP 인접과 공유하지 못하게 하는 제한이 있습니다. 이는 대부분의 경우에는 바람직한 동작이지만 관리자가 eBGP 인접과 개인 AS 경로를 공유하려고 하는 경우도 있을 수 있습니다.

해결 방법: Edge에서 BGP 업데이트의 모든 AS 경로를 알리도록 하는 해결 방법은 없습니다.

문제 1461421: NSX Edge에 대한 "show ip bgp neighbor" 명령 출력에 이전에 설정한 연결의 개수 내역이 유지됨

"show ip bgp neighbor" 명령을 실행하면 BGP 상태 시스템이 지정된 피어에 대해 [Established] 상태로 전환된 횟수가 표시됩니다. MD5 인증에 사용된 암호를 변경하면 피어 연결이 끊어졌다가 다시 생성되고, 카운터가 지워집니다. Edge DLR에서는 이 문제가 발생하지 않습니다.

해결 방법: 카운터를 지우려면 "clear ip bgp neighbor" 명령을 실행합니다.

문제 1676085: 리소스 예약이 실패하는 경우 Edge HA를 사용하도록 설정하지 못함

NSX for vSphere 6.2.3부터 두 번째 Edge VM 장치에 대해 충분한 리소스를 예약할 수 없는 경우 기존 Edge에서 고가용성을 사용하도록 설정할 수 없습니다. 구성은 마지막으로 알려져 있는 정상 구성으로 롤백됩니다. 이전 릴리스에서는 Edge 배포 및 리소스 예약이 실패한 후에 HA를 사용하도록 설정하면 Edge VM이 계속 생성됩니다.

해결 방법: 이는 예상된 동작 변경입니다.

문제 1656713: HA 페일오버 후 NSX Edge에 IPsec SP(보안 정책)가 없고 터널을 통해 트래픽이 흐를 수 없음

IPsec 터널에서 흐르는 트래픽에 대해 대기 > 활성화 전환이 작동하지 않습니다.

해결 방법: NSX Edge 전환 후에 IPsec를 사용/사용 안 함으로 설정합니다.

문제 1354824: Edge VM이 정전 등의 이유로 손상되거나 연결 불가능한 경우 NSX Manager의 상태 검사가 실패할 때 시스템 이벤트가 발생

시스템 이벤트 탭에서 "Edge 연결 불가" 이벤트를 보고합니다. NSX Edge 목록에서 계속 배포됨 상태로 보고될 수 있습니다.

해결 방법: *detailedStatus=true*를 지정하여 <https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status> API를 사용합니다.

문제 1556924: VXLAN과의 L3 연결 손실로 인한 차단 오류

호스트에 DLR LIF가 구성되어 있으나 기본 VXLAN 계층이 완전히 준비되지 않은 경우 일부 DLR LIF를 통한 연결이 영향을 받을 수 있습니다. DLR에 속하는 일부 VM이 연결되지 않을 수 있습니다. "VXLAN 트렁크 상태 생성 실패: 차단됨" 로그가 */var/log/vmkernel.log* 파일에 기록될 수 있습니다.

해결 방법: LIF를 삭제한 후 다시 만들 수 있습니다. 또는 영향을 받은 ESX 호스트를 재부팅할 수 있습니다.

문제 1647657: DLR(논리적 분산 라우터)이 있는 ESXi 호스트에서 show 명령을 실행할 경우 DLR 인스턴스당 경로가 2,000개까지만 표시됨

DLR이 사용되도록 설정된 ESXi 호스트에서 show 명령을 사용하면 실행 중인 DLR 인스턴스당 경로가 2,000개를 초과해도 2,000개 이하로 표시됩니다. 이 문제는 단순한 표시 문제이며 실제 데이터 경로는 모든 경로에 대해 정상 동작합니다.

해결 방법: 없음.

문제 1634215: OSPF CLI 명령 출력에 라우팅을 사용 안 함으로 설정했는지 표시되지 않음

OSPF를 사용하지 않도록 설정한 경우 라우팅 CLI 명령 출력에 "OSPF가 사용하지 않도록 설정되었습니다"와 같은 메시지가 전혀 표시되지 않습니다. 출력이 비어 있습니다.

해결 방법: *show ip ospf* 명령으로 올바른 상태를 표시할 수 있습니다.

문제 1647739: vMotion 작업 이후 Edge VM을 재배포하면 Edge 또는 DLR VM이 원래의 클러스터로 돌아갑니다.

해결 방법: Edge VM을 다른 리소스 풀 또는 클러스터에 배치하려면 NSX Manager UI를 사용하여 원하는 위치를 구성하십시오.

문제 1463856: NSX Edge 방화벽이 사용되도록 설정될 경우 기존 TCP 연결이 차단됨

초기 3방향 핸드셰이크를 확인할 수 없을 때 Edge 상태 저장 방화벽을 통해 TCP 연결이 차단됩니다.

해결 방법: 이러한 기존 흐름을 처리하려면 다음을 수행하십시오. NSX REST API를 사용하여 방화벽 전역 구성에서 "tcpPickOngoingConnections" 플래그를 사용하도록 설정합니다. 이렇게 하면 방화벽이 하드 모드에서 소프트 모드로 전환됩니다. 그다음 방화벽을 사용하도록 설정합니다. 기존 연결이 선택되면(방화벽을 사용하도록 설정하고 몇 분 정도 걸릴 수 있음) "tcpPickOngoingConnections" 플래그를 다시 false로 설정하여 방화벽을 하드 모드로 되돌립니다. (이 설정은 영구적입니다.)

PUT /api/4.0/edges/{edgeId}/firewall/config/global


```
<globalConfig>
<tcpPickOngoingConnections>true</tcpPickOngoingConnections>
</globalConfig>
```

문제 1374523: esxcli를 사용하여 VXLAN 명령을 사용할 수 있게 하려면 VXLAN VIB를 설치한 후에 ESXi를 재부팅하거나 `/services.sh restart`를 실행함

esxcli를 사용하여 VXLAN 명령을 사용할 수 있게 하려면 VXLAN VIB를 설치한 후에 ESXi를 재부팅하거나 `[services.sh restart]` 명령을 실행해야 합니다.

해결 방법: esxcli를 사용하는 대신 localcli를 사용합니다.

문제 1604514: [게시] 클릭 후 관리되지 않는 DLR의 기본 게이트웨이 편집/구성이 실패함

관리되지 않는 DLR에 기본 게이트웨이를 추가할 경우 "[Routing] Admin Distance는 NSX Edge VM이 배포된 NSX Edge 버전 6.2.0 이상에서만 지원됩니다." 오류와 함께 게시가 실패합니다. 이는 UI에 기본 admin distance "1"이 입력되어 있기 때문입니다.

해결 방법: 기본적으로 입력되어 있는 admin distance "1"을 제거합니다.

문제 1642087: IPsec VPN 확장에서 securelocaltrafficbyip 매개 변수 값을 수정한 후 대상 네트워크로의 전달이 실패함

NSX Edge Services Gateway를 사용할 때 다음 증상이 나타납니다.

- NSX UI(Edit IPsec VPN 편집 화면)에서 securelocaltrafficbyip 값을 0으로 변경한 후 IPsec VPN 터널의 원격 서브넷으로의 전달이 더 이상 작동하지 않음
- 이 매개 변수를 변경한 후 IP 라우팅 테이블의 원격 서브넷에 대해 더 이상 올바른 정보가 표시되지 않음

해결 방법: IPSec VPN 서비스를 사용 안 함으로 설정한 후 다시 사용함으로 설정합니다. 그런 다음 예상한 라우팅 정보가 CLI와 UI에 표시되는지 확인합니다.

문제 1525003: 잘못된 암호로 NSX Manager 백업을 복원할 경우 중요한 루트 폴더에 액세스할 수 없어 실패함

해결 방법: 없음.

문제 1637639: Windows 8 SSL VPN PHAT 클라이언트를 사용할 경우 IP 풀에서 가상 IP가 할당되지 않음
Edge Services Gateway가 새 IP 주소를 할당하거나 IP 풀이 다른 IP 범위로 변경될 경우 Windows 8에서 가상 IP 주소가 IP 풀에서 예상대로 할당되지 않습니다.

해결 방법: 이 문제는 Windows 8에서만 발생합니다. 다른 Windows OS를 사용하여 이 문제를 방지하십시오.

문제 1628220: 수신기 측에서 DFW 또는 NetX 관찰을 볼 수 없음

대상 vNIC와 연결된 스위치 포트가 변경된 경우 Traceflow가 수신기 측에서 DFW 및 NetX 관찰을 표시하지 않을 수 있습니다. vSphere 5.5 릴리스의 경우에는 이 문제가 수정되지 않습니다. vSphere 6.0 이상의 경우 이 문제가 발생하지 않습니다.

해결 방법: vNIC를 사용하지 않도록 설정하지 마십시오. VM을 재부팅합니다.

문제 1534603: IPsec 및 L2 VPN 서비스를 사용하도록 설정하지 않은 경우에도 서비스 상태가 다운된 것으로 표시됨

UI의 설정 탭에서 L2 서비스 상태가 다운된 것으로 표시되지만 API에서는 L2 상태가 가동 중인 것으로 표시됩니다. UI 페이지를 새로 고치지 않는 한 L2 VPN 및 IPsec 서비스는 [설정] 탭에서 항상 다운된 것으로 표시됩니다.

해결 방법: 페이지를 새로 고칩니다.

문제 1534799: IP 주소가 가장 높은 OSPF 영역 경계 라우터가 종료될 경우 수렴 속도가 느려짐

IP 주소가 가장 높은 NSX 기반의 OSPF 영역 경계 라우터(ABR)가 종료되거나 재부팅될 경우 수렴에 시간이 오래 걸립니다. 숫자가 가장 높지 않은 IP 주소의 ABR을 종료하거나 재부팅할 경우에는 트래픽이 다른 경로로 빠르게 수렴됩니다. 그러나 가장 높은 IP 주소의 ABR을 종료하거나 재부팅하면 다시 수렴하는 데 시간이 몇 분 이상 더 걸립니다. OSPF 프로세스를 수동으로 지우면 수렴 시간을 줄일 수 있습니다.

문제 1446327: NSX Edge를 통해 연결할 때 일부 TCP 기반 애플리케이션이 시간 초과될 수 있음
기본 TCP 설정된 연결 비활성 시간 초과 값은 3600초입니다. NSX Edge는 비활성 시간 초과 값보다 더 오래 유휴 상태인 연결을 모두 삭제하고 연결을 해제합니다.

해결 방법:

1. 애플리케이션의 비활성 시간이 비교적 긴 경우에 keep_alive_interval이 3600초 미만으로 설정된 호스트에서 TCP keepalive를 사용하도록 설정합니다.
2. 다음과 같은 NSX REST API를 사용하여 Edge TCP 비활성 시간 초과 값이 2시간을 넘도록 늘립니다. 예를 들어, 비활성 시간 초과 값을 9000초로 늘릴 수 있습니다. NSX API URL:
`/api/4.0/edges/{edgclid}/systemcontrol/config PUT Method <systemControl>
<property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</property>
</systemControl>`

문제 1089745: 두 개 이상의 DLR Edge 업링크에 OSPF를 구성할 수 없음
현재 8개의 DLR Edge 업링크 중 두 개 이상에 OSPF를 구성할 수 없습니다. 이러한 제한은 DLR 인스턴스당 하나의 전달 주소 공유에 따른 결과입니다.

해결 방법: 이는 현재 시스템 제한이며 해결 방법은 없습니다.

문제 1498965: Edge syslog 메시지가 원격 syslog 서버에 도달하지 않음
배포 직후에 Edge syslog 서버가 구성된 원격 syslog 서버에 대한 호스트 이름을 확인할 수 없습니다.

해결 방법: 해당 IP 주소를 사용하여 원격 syslog 서버를 구성하거나, UI를 사용하여 Edge를 강제로 동기화합니다.

문제 1494025: REST Edge API를 업데이트한 후 논리적 라우터 DNS 클라이언트 구성 설정이 완전하게 적용되지 않음

해결 방법: REST API를 사용하여 DNS 전달자(확인 프로그램)를 구성할 때 다음 단계를 수행합니다.

1. DNS 클라이언트 XML 서버의 설정을 DNS 전달자 설정과 일치하도록 지정합니다.
2. DNS 전달자를 사용하도록 설정하고, 전달자 설정이 XML 구성에 지정된 DNS 클라이언트 서버 설정과 동일한지 확인합니다.

문제 1243112: ECMP가 사용되도록 설정된 상태에서 정적 경로의 잘못된 다음 홉에 대한 검증 및 오류 메시지가 없음
ECMP가 사용되도록 설정된 상태에서 정적 경로를 추가하려고 시도할 때 라우팅 테이블에 기본 경로가 포함되어 있지 않고 정적 경로 구성에 도달할 수 없는 다음 홉이 있는 경우, 오류 메시지가 표시되지 않고 정적 경로가 설치되지 않습니다.

해결 방법: 없음.

문제 1288487: 논리적 스위치로 지원되는 하나의 하위 인터페이스를 포함한 NSX Edge 가상 시스템이 vCenter Web Client 사용자 인터페이스를 통해 삭제된 경우, 데이터 경로가 동일한 포트에 연결된 새 가상 시스템에 대해 작동하지 않음

Edge 가상 시스템을 NSX Manager에서 삭제하지 않고 vCenter Web Client 사용자 인터페이스를 통해 삭제하면 opaque 채널에서 dvPort에 구성된 VXLAN 트렁크가 재설정되지 않습니다. 이는 트렁크 구성이 NSX Manager에 의해 관리되기 때문입니다.

해결 방법: 다음 단계를 따라 수동으로 VXLAN 트렁크 구성을 삭제하십시오.

1. 브라우저 창에 다음을 입력하여 vCenter Managed Object Browser로 이동합니다.
`https://<vc-ip>/mob?vmodl=1`
2. 콘텐츠를 클릭합니다.
3. 다음 단계를 따라 dvsUuid 값을 회수합니다.
 - a. rootFolder 링크를 클릭합니다(예: group-d1(Datacenters)).
 - b. 데이터 센터 이름 링크를 클릭합니다(예: datacenter-1).
 - c. networkFolder 링크를 클릭합니다(예: group-n6).
 - d. DVS 이름 링크를 클릭합니다(예: dvs-1).

e. uuid 값을 복사합니다.

4. DVSManger를 클릭하고 updateOpaqueDataEx를 클릭합니다.

5. selectionSet에 다음 XML을 추가합니다.

```
<selectionSet xsi:type="DVPortSelection">
<dvsUuid>value</dvsUuid>
<portKey>value</portKey> <!--트렁크 vnic가 연결된 DVPG의 포트 번호-->
</selectionSet>
```

6. opaqueDataSpec에서 다음 XML을 추가합니다.

```
<opaqueDataSpec>
<operation>remove</operation>
<opaqueData>
<key>com.vmware.net.vxlan.trunkcfg</key>
<opaqueData></opaqueData>
</opaqueData>
</opaqueDataSpec>
```

7. isRuntime을 거짓으로 설정합니다.

8. 메서드 호출을 클릭합니다.

9. 삭제된 Edge 가상 시스템에 구성된 각 트렁크 포트에 대해 5-8단계를 반복합니다.

문제 1637939: 하드웨어 게이트웨이 배포 중에 MD5 인증서가 지원되지 않음

논리적 L2 VLAN-VXLAN 브리징을 위해 하드웨어 게이트웨이 스위치를 VTEP로 배포할 때 물리적 스위치가 NSX Controller와 OVSDB 스위치 사이의 OVSDB 연결에 대한 최소 SHA1 SSL 인증서를 지원합니다.

해결 방법: 없음.

문제 1637943: 하드웨어 게이트웨이 바인딩이 있는 VNI에 대한 하이브리드 또는 멀티캐스트 복제 모드 미지원
L2 VXLAN-VLAN 브리징을 위한 VTEP로 하드웨어 게이트웨이 스위치를 사용할 경우 유니캐스트 복제 모드만 지원
합니다.

해결 방법: 유니캐스트 복제 모드만 사용하십시오.

보안 서비스에 대한 알려진 문제

새로 만들기 문제 1847753: ALG 사용 프로토콜에 대한 흐름을 검색할 때 호스트가 자주색 진단 화면을 표시하면서
실패함

환경에서 흐름 모니터링을 사용하도록 설정한 상태로 NSX for vSphere 6.2.4에서 6.3.0 또는 6.3.1로 업그레이드하
면 ESXi 호스트에 자주색 진단 화면이 표시됩니다. 자세한 내용 및 해결 방법은 [VMware 기술 자료 문서 2149908](#)를
참조하십시오.

문제 1474650: NetX 사용자의 경우 ESXi 5.5.x 및 6.x 호스트에서 다음을 언급하는 자주색 진단 화면이 나타납니
다. **ALERT: NMI: 709: NMI IPI received**

서비스 VM에서 다량의 패킷이 전송되거나 수신된 경우 DVFilter가 계속 CPU에서 점유하여 하트비트 손실 및 자주
색 진단 화면으로 이어집니다. 자세한 내용은 [VMware 기술 자료 문서 2149704](#)를 참조하십시오.

해결 방법: NetX 사용에 필요한 다음의 최소 ESXi 버전으로 ESXi 호스트를 업그레이드합니다.

- 5.5 패치 10
- ESXi 6.0U3
- ESXi 6.5

새로 만들기 문제 1676043: 두 개의 동시 추가 후 제외 목록에서 VM이 제거됨

UI를 새로 고치지 않고 2명의 사용자가 동일한 VM 2개를 [제외 목록]에 동시에 추가하면 이미 추가된 VM이 제외된
목록에서 제거됩니다.

해결 방법: VM을 [제외 목록]에 추가하기 전에 vSphere Web Client UI를 새로 고치십시오.

새로 만들기 문제 1770259: DFW 규칙에 대한 appliedTo 필드를 여러 appliedTo 개체를 포함하도록 수정할 수 없음

DFW 규칙을 vNIC 또는 VM 집합, 클러스터 또는 데이터센터에 적용하고 게시한 다음 나중에 appliedTo 필드에 개체를 더 추가하여 수정하려고 하면 게시가 성공적으로 수행되더라도 새로운 변경 내용이 적용되지 않습니다.

해결 방법: 없음.

새로 만들기 문제 1798779: NSX를 6.2.x에서 6.3.0으로 업그레이드한 후에 vSphere Web Client의 GUI에서 범용 보안 태그를 추가하도록 잘못 허용함

6.3.0에는 범용 보안 태그가 도입됩니다. NSX 6.3.0으로 업그레이드하기 전에 6.2.x에서 생성한 범용 Security Group에 범용 보안 태그를 추가하려고 하면 "요청된 멤버가 올바른 멤버가 아닙니다." 오류를 나타내며 작업이 실패합니다. 이 오류는 범용 보안 태그를 NSX 6.2.x 범용 Security Group에 추가할 수 없기 때문에 정상적인 것입니다. 이 GUI에는 문제가 있습니다.

해결 방법: 업그레이드한 후에 NSX 6.3.0 범용 Security Group을 생성한 후 해당 그룹에 범용 보안 태그를 추가하십시오.

새로 만들기 문제 1799543: NSX 6.2.x에서 NSX 6.3.0으로 업그레이드한 후에 첫 번째 활성화-대기 범용 Security Group을 생성하려고 하면 vSphere Web Client가 잘못 표시되고 NSX 6.2.x 범용 Security Group 및 비활성-대기 범용 Security Group을 선택할 수 있도록 허용함

첫 번째 활성화-대기 범용 Security Group을 생성할 경우 vSphere Web Client UI가 표시되고 NSX 6.2.x에서 생성된 범용 Security Group을 추가할 수 있도록 허용합니다. "요청된 멤버가 유효한 멤버가 아닙니다." 오류를 표시하면서 작업이 실패합니다.

해결 방법: 하나 이상의 활성화-대기 범용 Security Group을 생성한 후 다음 활성화-대기 범용 Security Group을 생성하는 동안에는 이 문제가 발생하지 않습니다.

새로 만들기 문제 1786780: Service Composer UI에서 정책 순서를 바꾸거나 이동하면 CPU 활용률이 높아지고 시간이 오래 걸림

Service Composer UI에서 정책 순서를 바꾸거나 위치를 바꿀 경우 CPU 활용률이 높아지면서 시간이 오래 걸릴 수 있습니다.

해결 방법: 다음 단계가 도움이 됩니다.

- 정책을 생성하는 동안 정책에 적절한 우선 순위(가중치)를 부여하여 첫 번째 시도에서 올바른 위치에 배치되도록 하면 정책 순서를 다시 정렬할 필요가 없습니다.
- 정책을 다른 위치로 이동해야 할 경우 이동할 정책을 편집하고 우선 순위(가중치)를 적절한 값으로 변경하십시오. 이렇게 하면 단일 정책이 수정되고 빠르게 완료됩니다.

새로 만들기 문제 1787680: NSX Manager가 전송 모드인 경우 범용 방화벽 섹션이 삭제되지 않음

전송 모드인 NSX Manager의 UI에서 범용 방화벽 섹션 삭제를 시도하고 게시할 때 게시가 되지 않고 그 결과 NSX Manager를 독립형 모드로 설정할 수 없습니다.

해결 방법: 범용 방화벽 섹션을 삭제하려면 단일 삭제 섹션 REST API를 사용하십시오.

문제 1741844: 여러 IP 주소가 있는 vNIC의 주소를 감지하는 ARP 스누핑으로 인해 100% CPU 사용률이 발생함
이 문제는 가상 시스템의 vNIC가 여러 IP 주소로 구성되어 있으며 ARP 스누핑이 IP를 감지하는 데 사용되도록 설정되어 있을 때 발생합니다. IP 검색 모듈은 여러 IP 주소로 구성된 모든 VM에 대해 vNIC-IP 매핑을 변경하도록 지속적으로 NSX Manager에 vNIC-IP 업데이트를 보냅니다.

해결 방법: 해결 방법이 없습니다. 현재 ARP 스누핑 기능은 vNIC당 하나의 IP 주소만 지원합니다. 자세한 내용은 *NSX 관리 가이드*에서 [가상 시스템의 IP 검색](#) 섹션을 참조하십시오.

문제 1689159: Flow Monitoring의 [규칙 추가] 기능이 ICMP 흐름에 대해 제대로 작동되지 않음

Flow Monitoring에서 규칙을 추가할 때 [서비스] 필드를 명시적으로 [ICMP]로 설정하지 않으면 필드가 빈 상태로 표시되며, 이로 인해 서비스 유형이 [임의]인 규칙이 추가될 수 있습니다.

해결 방법: ICMP 트래픽을 반영하도록 [서비스] 필드를 업데이트합니다.

문제 1632235: Guest Introspection 설치 동안 네트워크 드롭다운 목록에 "호스트에 지정"만 표시됨
NSX 바이러스 백신 전용 라이선스 및 vSphere Essential 또는 Standard 라이선스를 사용하여 Guest Introspection을 설치할 경우 네트워크 드롭다운 목록에 DV 포트 그룹의 기존 목록만 표시됩니다. 이 라이선스는 DVS 생성을 지원하지 않습니다.

해결 방법: 이러한 라이선스 중 하나를 사용하여 vSphere 호스트에 Guest Introspection을 설치하기 전에 먼저 "에이전트 VM 설정" 창에서 네트워크를 지정합니다.

문제 1652155: 특정 상황에서 REST API를 사용하여 방화벽 규칙을 생성하거나 마이그레이션하지 못할 수 있으며 HTTP 404 오류가 보고됨

다음과 같은 상황에서는 REST API를 사용하여 방화벽 규칙을 추가하거나 마이그레이션할 수 없습니다.

- autosavedraft=true가 설정되었을 때 방화벽 규칙을 대량 작업으로 생성
- 여러 섹션에서 방화벽 규칙을 동시에 추가

해결 방법: 대량 방화벽 규칙 생성 또는 마이그레이션을 수행할 때 API 호출에서 autoSaveDraft 매개 변수를 false로 설정합니다.

문제 1509687: 하나의 API 호출로 한 번에 여러 VM에 단일 보안 태그를 할당할 경우 지원되는 최대 URL 길이는 16,000자임

URL 길이가 16,000자를 초과할 경우 하나의 API로 많은 수의 VM에 단일 보안 태그를 동시에 할당할 수 없습니다.

해결 방법: 성능을 최적화하려면 단일 호출에서 VM을 500개 이하로 태그합니다.

문제 1662020: 게시 작업이 실패하여 "일반 및 파트너 보안 서비스" 섹션의 DFW UI에 "호스트 번호 호스트에서 마지막 게시 실패" 오류 메시지가 표시됨

규칙을 변경하면 UI에 "호스트 번호 호스트에서 마지막 게시 실패"가 표시됩니다. UI에 등록된 호스트의 방화벽 규칙 버전이 올바르지 않아 보안이 되지 않거나 네트워크 중단이 발생할 수 있습니다.

이 문제는 일반적으로 다음 시나리오에서 볼 수 있습니다.

- 이전 NSX 버전에서 최신 버전으로 업그레이드한 후
- 호스트를 클러스터 외부로 이동한 후 돌려 놓음
- 호스트를 한 클러스터에서 다른 클러스터로 이동함

해결 방법: 복구하려면 영향을 받은 클러스터를 강제로 동기화해야 합니다(방화벽만 해당).

문제 1481522: 6.1.x의 방화벽 규칙 초안을 6.2.3으로 마이그레이션하는 것은 두 릴리스 간에 초안이 호환되지 않기 때문에 가능하지 않음

해결 방법: 없음.

문제 1628679: ID 기반 방화벽을 사용하는 경우 제거된 사용자의 VM이 계속해서 보안 그룹에 포함됨

AD 서버의 그룹에서 사용자를 제거할 경우 사용자가 로그인된 VM은 계속해서 보안 그룹에 속합니다. 이를 통해 하이퍼바이저의 VM vNIC에서 방화벽 정책이 유지되므로 사용자에게 서비스에 대한 전체 액세스가 부여됩니다.

해결 방법: 없음. 이는 의도된 동작입니다.

문제 1462027: 크로스 vCenter NSX 배포에서 저장된 방화벽 구성의 여러 가지 버전이 보조 NSX Manager에 복제됨

범용 동기화를 수행하면 범용 구성 사본 여러 개가 보조 NSX Manager에 저장됩니다. NSX Manager 간에 동기화하여 생성된 여러 개의 초안이 저장된 구성 목록에 동일한 이름과 동일한 시간 또는 동일한 이름과 1초의 시간차로 포함됩니다.

해결 방법: API 호출을 실행하여 중복된 초안을 삭제합니다.

DELETE : <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts/>

모든 초안을 확인하여 삭제할 초안을 찾습니다.

GET: https://<nsxmgr-ip>/api/4.0/firewall/config/drafts

다음의 샘플 출력에서 초안 143과 144는 이름이 같고 같은 시간에 생성되었기 때문에 중복 항목입니다. 마찬가지로, 초안 127과 128도 이름이 같고 생성된 시간이 1초 차이만 나기 때문에 중복 항목입니다.

```
<firewallDrafts>
  <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
    timestamp="1438816120917">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
    timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT"
    timestamp="1438808882608">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT"
    timestamp="1438808881750">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
</firewallDrafts>
```

문제 1449611: 삭제된 Security Group 때문에 Service Composer에서 방화벽 정책이 동기화되지 않을 경우 UI에서 방화벽 규칙을 수정할 수 없음

해결 방법: UI에서 잘못된 방화벽 규칙을 삭제한 다음 다시 추가할 수 있습니다. 또는 API에서 잘못된 보안 그룹을 삭제하여 방화벽 규칙을 수정할 수 있습니다. 그런 다음 방화벽 구성을 동기화합니다. **Service Composer: 보안 정책**을 선택하고 연결된 방화벽 규칙이 있는 각 보안 정책에 대해 **작업**을 클릭하고 **방화벽 구성 동기화**를 선택합니다. 이 문제를 방지하려면 보안 그룹을 삭제하기 전에 보안 그룹을 참조하지 않도록 방화벽 규칙을 수정하십시오.

문제 1557880: 규칙에 사용된 VM의 MAC 주소가 수정된 경우 레이어 2(L2) 규칙이 누락될 수 있음

L2 규칙 최적화가 기본적으로 켜져 있기 때문에 소스 및 대상 필드가 모두 지정된('임의' 제외) L2 규칙은 vNIC MAC 주소가 소스 또는 대상 MAC 주소 목록과 일치하는 경우에만 vNIC(또는 필터)에 적용됩니다. 소스 또는 대상 MAC 주소와 VM이 일치하지 않는 호스트에는 해당 L2 규칙을 적용할 수 없습니다.

해결 방법: L2 규칙을 모든 vNIC(또는 필터)에 적용하려면 소스 또는 대상 필드 중 하나를 "임의"로 설정하십시오.

문제 1496273: UI에서 Edge에 적용할 수 없는 내부/외부 NSX 방화벽 규칙을 생성할 수 있음

PacketType이 IPV4 또는 IPV6이고, 규칙에 '내부' 또는 '외부' 방향으로 이동하는 트래픽이 포함된 경우에 웹 클라이언트가 하나 이상의 NSX Edge에 적용되는 NSX 방화벽 규칙을 생성할 수 있도록 잘못 허용합니다. NSX는 이러한 규칙을 NSX Edge에 적용할 수 없기 때문에 UI에서 해당 규칙을 생성할 수 없어야 합니다.

해결 방법: 없음.

문제 1557924: 로컬 DFW 규칙의 appliedTo 필드에서 범용 논리적 스위치를 사용하도록 허용됨

범용 논리적 스위치를 보안 그룹 멤버로 사용할 때 DFW 규칙에서 해당 보안 그룹을 AppliedTo 필드에서 사용할 수 있습니다. 이 경우 범용 논리적 스위치에 해당 규칙이 간접적으로 적용되는데, 그러면 이러한 규칙에 알 수 없는 동작이 발생할 수 있기 때문에 허용해서는 안 됩니다.

해결 방법: 없음.

문제 1559971: 한 클러스터에서 방화벽을 사용하지 않도록 설정된 경우 크로스 vCenter NSX 방화벽 제외 목록이 게시되지 않음

크로스 vCenter NSX에서, 클러스터 중 하나에서 방화벽을 사용하지 않도록 설정되어 있으면 방화벽 제외 목록이 어느 클러스터에도 게시되지 않습니다.

해결 방법: 문제가 발생한 NSX Edge를 강제 동기화합니다.

문제 1407920: DELETE API를 사용한 후 방화벽 규칙을 다시 게시할 수 없음

DELETE API 메서드를 통해 전체 방화벽 구성을 삭제한 다음 이전에 저장한 방화벽 초안에서 모든 규칙을 다시 게시하려고 하면, 규칙 게시에 실패합니다.

문제 1494718: 새로운 범용 규칙을 생성할 수 없고 흐름 모니터링 UI에서 기존 범용 규칙을 편집할 수 없음

해결 방법: 범용 규칙은 흐름 모니터링 UI에서 추가하거나 편집할 수 없습니다. EditRule은 자동으로 사용되지 않도록 설정됩니다.

문제 1442379: Service Composer 방화벽 구성이 동기화되지 않음

NSX Service Composer에서 잘못된 방화벽 정책이 있는 경우(예를 들어 방화벽 규칙에서 사용 중이던 Security Group을 삭제) 다른 방화벽 정책을 삭제하거나 수정하면 Service Composer는 오류 메시지 방화벽 구성이 동기화되지 않았습니.를 표시하고 동기화되지 않은 상태가 됩니다.

해결 방법: 잘못된 방화벽 규칙을 모두 삭제한 다음 방화벽 구성을 동기화합니다. **Service Composer: 보안 정책을** 선택하고 연결된 방화벽 규칙이 있는 각 보안 정책에 대해 **작업**을 클릭하고 **방화벽 구성 동기화**를 선택합니다. 이 문제를 방지하려면 방화벽 구성을 더 변경하기 전에 항상 잘못된 방화벽 구성을 수정하거나 삭제하십시오.

문제 1066277: 보안 정책 이름에 229자가 넘는 이름이 허용되지 않음

Service Composer의 [보안 정책] 탭에 있는 보안 정책 이름 필드는 최대 229자까지만 허용됩니다. 이는 내부적으로 정책 이름 앞에 접두사가 추가되기 때문입니다.

해결 방법: 없음.

문제 1443344: 타사 네트워크 VM 시리즈의 일부 버전이 NSX Manager 기본 설정에서 작동하지 않음

일부 NSX 6.1.4 이상의 구성 요소는 기본적으로 SSLv3를 사용하지 않도록 설정합니다. 업그레이드하기 전에 NSX 배포와 통합된 모든 타사 솔루션이 SSLv3 통신을 사용하지 않는지 확인하십시오. 예를 들어 Palo Alto Networks VM-시리즈 솔루션의 일부 버전에는 SSLv3의 지원이 필요하므로 벤더에 버전 요구 사항을 확인하십시오.

문제 1660718: Service Composer 정책 상태가 UI에서는 "진행 중"으로 나타나고 API 출력에서는 "보류 중"으로 나타남

해결 방법: 없음.

문제 1620491: Service Composer의 정책 수준 동기화 상태가 정책 내 규칙의 게시 상태를 나타내지 않음

정책이 생성되거나 수정될 때 Service Composer는 지속성 상태만 나타내는 성공 상태를 표시합니다. 이러한 상태는 규칙이 호스트에 성공적으로 게시되었는지에 대해서는 알려주지 않습니다.

해결 방법: 방화벽 UI를 사용하여 게시 상태를 확인합니다.

문제 1317814: Service Manager 중 하나가 중지된 상태에서 정책이 변경된 경우 Service Composer가 동기화되지 않음

여러 Service Manager 중 하나가 중지된 상태일 때 정책이 변경되면 변경은 실패하고 Service Composer는 동기화되지 않습니다.

해결 방법: Service Manager가 응답하는지 확인한 다음 Service Composer에서 강제 동기화를 수행합니다.

문제 1070905: Guest Introspection 및 타사 보안 솔루션에서 보호하는 클러스터에서 호스트를 제거했다 다시 추가할 수가 없음

Guest Introspection 및 타사 보안 솔루션에서 보호하는 클러스터의 호스트를 제거하기 위해 vCenter Server에서 연결을 끊어 호스트를 제거하는 경우 동일한 호스트를 동일한 클러스터에 다시 추가하려고 할 때 문제가 발생할 수 있습니다.

해결 방법: 보호되는 클러스터에서 호스트를 제거하려면 먼저 해당 호스트를 유지 보수 모드로 전환합니다. 그런 다음 호스트를 보호되지 않는 클러스터 또는 모든 클러스터의 외부로 이동한 다음 연결을 끊고 호스트를 제거합니다.

문제 1648578: 새 NetX 호스트 기반 서비스 인스턴스를 생성할 때 NSX가 클러스터/네트워크/스토리지를 강제로 추가하도록 함

방화벽, IDS 및 IPS와 같은 NetX 호스트 기반 서비스용 vSphere Web Client에서 새 서비스 인스턴스를 생성할 때 필수 요소가 아니더라도 클러스터/네트워크/스토리지를 강제로 추가하도록 요구됩니다.

해결 방법: 새 서비스 인스턴스를 생성할 때 클러스터/네트워크/스토리지에 대한 정보를 추가하여 필드를 채울 수 있습니다. 이를 통해 서비스 인스턴스를 생성할 수 있으며 필요에 따라 작업을 계속 진행할 수 있습니다.

문제 1772504: Service Composer가 MAC 집합이 있는 보안 그룹을 지원하지 않음

Service Composer는 [정책] 구성에서 Security Group을 사용하도록 허용합니다. MAC 집합이 포함된 보안 그룹이 있는 경우 Service Composer는 이상 없이 해당 보안 그룹을 허용하지만 해당 특정 MAC 집합에 대해 규칙을 적용하지 못합니다. 이는 Service Composer가 계층 3에서 작동하고 계층 2 구성을 지원하지 않기 때문입니다. 보안 그룹에 IP 집합 및 MAC 집합이 둘 다 있는 경우 IP 집합은 계속 유효하지만 MAC 집합은 무시됩니다. MAC 집합을 포함하는 보안 그룹을 참조해도 문제는 없습니다. 사용자는 MAC 집합이 무시된다는 사실을 알고 있어야 합니다.

해결 방법: 사용자의 의도가 MAC 집합을 사용하여 방화벽 규칙을 생성하는 것인 경우 Service Composer 대신 DFW 계층 2/이더넷 구성을 사용해야 합니다.

문제 1718726: 사용자가 DFW REST API를 사용하여 직접 Service Composer의 정책 섹션을 삭제한 후에 Service Composer를 강제 동기화할 수 없음

크로스 vCenter NSX 환경에서 정책 섹션이 하나만 있고 정책 섹션(Service Composer 관리 정책 섹션)이 REST API 호출을 통해 이전에 삭제된 경우 NSX Service Composer 구성을 강제 동기화하려는 사용자 시도가 실패합니다.

해결 방법: REST API 호출을 통해 Service Composer 관리 정책 섹션을 삭제하지 마십시오. (UI에서 이 섹션의 삭제를 방지합니다.)

모니터링 서비스에 대한 알려진 문제

문제 1466790: NSX traceflow 도구를 사용하여 브리지 네트워크에서 VM을 선택할 수 없음

NSX traceflow 도구를 사용하여 논리적 스위치에 연결되지 않은 VM을 선택할 수 없습니다. L2 브리지 네트워크의 VM을 VM 이름 기준으로 traceflow 검사의 소스 또는 대상 주소로 선택할 수 없습니다.

해결 방법: L2 브리지 네트워크에 연결된 VM의 경우 traceflow 검사에서 대상으로 지정하려는 인터페이스의 IP 주소 또는 MAC 주소를 사용합니다. L2 브리지 네트워크에 연결된 VM을 소스로 선택할 수 없습니다. 자세한 내용은 [기술 자료 문서 2129191](#)을 참조하십시오.

문제 1626233: NetX SVM(서비스 가상 시스템)이 패킷을 삭제하는 경우 traceflow가 삭제된 관찰을 생성하지 않음

traceflow 세션은 패킷이 NetX SVM(서비스 가상 시스템)으로 전송된 후 종료됩니다. SVM이 패킷을 삭제하는 경우 traceflow는 삭제된 관찰을 생성하지 않습니다.

해결 방법: 해결 방법이 없습니다. traceflow 패킷이 다시 주입되지 않는 경우 SVM이 패킷을 삭제했다고 가정할 수 있습니다.

솔루션 상호 운용성에 대한 알려진 문제

문제 1568861: vCenter 수신기가 없는 vCloud Director 셸에서 Edge를 배포할 때 NSX Edge 배포가 실패함

vCenter 수신기가 없는 vCloud Director 셸에서 Edge를 배포할 때 NSX Edge 배포가 실패합니다. 또한 재배포를 포함한 NSX Edge 작업이 vCloud Director에서 실패합니다.

해결 방법: vCenter 수신기가 있는 vCloud Director 셸에서 NSX Edge를 배포하십시오.

NSX Controller에 대한 알려진 문제

문제 1765354: <deployType>이 필수 속성이지만 사용되지 않음
<deployType>은 필수 속성이지만 사용되지 않으며 아무 의미도 없습니다.

문제 1516207: NSX Controller 클러스터에서 IPsec 통신을 다시 사용하도록 설정하면 컨트롤러가 격리될 수 있음
NSX Controller 클러스터가 암호화되지 않은 컨트롤러 간 통신을 허용하도록 설정하고(IPsec를 사용하지 않도록 설정) 나중에 IPsec 통신을 다시 사용하도록 설정할 경우 "PSK"(사전 공유 키)의 불일치로 인해 하나 이상의 컨트롤러가 대부분의 클러스터로부터 격리될 수 있습니다. 이 문제가 발생하면 NSX API에서 컨트롤러의 IPsec 설정을 변경하지 못할 수 있습니다.

해결 방법:

다음 단계를 수행하여 이 문제를 해결합니다.

1. NSX API를 사용하여 IPsec를 사용하지 않도록 설정합니다.

```
PUT /2.0/vdn/controller/node
```

```
<controllerNodeConfig>  
  <ipSecEnabled>false</ipSecEnabled>  
</controllerNodeConfig>
```

2. NSX API를 사용하여 IPsec를 다시 사용하도록 설정합니다.

```
PUT /2.0/vdn/controller/node
```

```
<controllerNodeConfig>  
  <ipSecEnabled>true</ipSecEnabled>  
</controllerNodeConfig>
```

다음 모범 사례에 따라 이 문제를 방지:

- 항상 NSX API를 사용하여 IPsec를 사용 안 함으로 설정하십시오. NSX Controller CLI를 사용하여 IPsec를 사용 안 함으로 설정하는 기능은 지원되지 않습니다.
- API를 사용하여 IPsec 설정을 변경하기 전에 모든 컨트롤러가 활성 상태인지 항상 확인하십시오.

문제 1306408: NSX Controller 로그를 반드시 순차적으로 다운로드해야 함

NSX Controller 로그는 동시에 다운로드할 수 없습니다. 여러 컨트롤러에서 다운로드하는 경우에도 현재 컨트롤러에서 다운로드가 완료될 때까지 기다렸다가 다음 컨트롤러에서 다운로드를 시작해야 합니다. 또한 로그 다운로드를 시작한 후에는 취소할 수 없습니다.

해결 방법: 현재 컨트롤러 로그 다운로드를 마칠 때까지 기다렸다가 다른 로그 다운로드를 시작합니다.

해결된 문제

새로 만들기 NSX 6.3.0에서 해결된 문제

NSX 6.3.0에서 해결된 문제는 다음과 같이 분류됩니다.

- [NSX 6.3.0에서 해결된 일반 문제](#)
- [NSX 6.3.0에서 해결된 설치 및 업그레이드 관련 문제](#)
- [NSX 6.3.0에서 해결된 NSX Manager 관련 문제](#)
- [NSX 6.3.0에서 해결된 네트워킹 및 Edge 서비스 관련 문제](#)

- [NSX 6.3.0에서 해결된 보안 서비스 관련 문제](#)
- [NSX 6.3.0에서 해결된 솔루션 상호 운용성 관련 문제](#)

NSX 6.3.0에서 해결된 일반 문제

해결된 문제 1497389: NSX 관리자 권한이 있는 사용자는 더 높은 사용자 역할인 엔터프라이즈 관리자로 권한을 변경할 수 있습니다. NSX 6.3.0부터 NSX 관리자 권한이 있는 사용자는 사용자를 관리할 수 없으며 엔터프라이즈 관리자 권한이 있는 사용자만 이를 수행할 수 있습니다. *6.3.0에서 해결되었습니다.*

해결된 문제 1575342, 1719402: NSX for vSphere 6.x 환경에서 SVM(서비스 VM)이 마이그레이션될 때 (vMotion/SvMotion) 서비스에서 중단이 발생하거나 ESXi 호스트가 충돌할 수 있음
6.3.0부터 vMotion/SvMotion을 사용하여 SVM(서비스 VM)을 마이그레이션할 수 없습니다. SVM이 올바르게 작동하려면 배포된 호스트에 유지되어야 합니다.
이전에는 다른 호스트로의 마이그레이션이 허용되었으나 지원되지 않았으며 그 결과 서비스가 중단되거나 호스트에 문제가 발생했습니다.
자세한 내용은 [VMware 기술 자료 문서 2141410](#)을 참조하십시오. *6.3.0에서 해결되었습니다.*

해결된 문제 1708769: NSX의 스냅샷 이후에 SVM(서비스 VM)의 지연 시간이 증가됨
이 문제는 SVM(서비스 VM)의 스냅샷을 실행할 경우 네트워크 지연 시간이 늘어날 수 있기 때문에 발생합니다. 스냅샷은 때때로 운영 환경에서 실행되는 백업 애플리케이션에 의해 호출됩니다. *6.3.0에서 해결되었습니다.*

해결된 문제 1760102: 스토리지 중단으로부터 복구하기 위해 NSX Controller를 삭제한 후 다시 배포한 다음 가상 시스템이 통신하지 못할 수 있음
vSphere 6.2.4/6.2.5 환경용 NSX Controller가 스토리지 중단 시 읽기 전용 모드로 전환될 수 있으며, 해당 상태에서부터 복구하기 위해 컨트롤러를 삭제한 후 다시 배포할 경우 일부 VM이 통신하지 못할 수 있습니다. 컨트롤러의 스토리지 중단 시 예상되는 동작은 컨트롤러를 재부팅한 후에 읽기 전용 모드에서 복구되는 것이지만 현재 NSX에서 해당 동작은 수행되지 않습니다. *6.3.0에서 해결되었습니다.*

해결된 문제 1662842: Guest Introspection: 확인할 수 없는 Windows SID를 확인하려고 할 때 MUX와 USVM 간에 연결이 끊어짐
Guest Introspection 서비스가 주의 상태가 되고, 각 Guest Introspection은 주의 상태가 되었다가 해제됩니다. Guest Introspection VM이 다시 연결될 때까지 네트워크 이벤트가 NSX Manager로 전달되지 않습니다. 이러한 현상은 Guest Introspection 경로를 통해 로그인 이벤트가 감지될 경우 Activity Monitoring 및 ID 방화벽 둘 다에 영향을 미칩니다. *6.3.0에서 해결되었습니다.*

해결된 문제 1752051: NSX Manager에서 USVM으로의 통신 시간이 초과될 때 Guest Introspection의 서비스 상태가 "준비 안 됨"으로 보고됨

내부 메시지 버스(rabbit MQ)에서 NSX Manager의 예상된 암호 변경 프로세스가 실패할 경우 Guest Introspection 범용 SVM에 대해 "PLAIN 로그인이 거부됨: 사용자 'usvm-admin-host-14' - 잘못된 자격 증명"과 비슷한 오류 메시지가 보고될 수 있습니다. *6.3.0에서 해결되었습니다.*

해결된 문제 1716328: 유지 보수 모드인 호스트를 제거하면 나중에 클러스터 준비가 실패함

관리자가 NSX를 사용하는 유지 보수 모드의 ESXi 호스트를 배치했다가 NSX 준비 클러스터에서 제거하면 NSX가 제거된 호스트의 ID 번호 기록을 삭제하지 못합니다. 설치가 이 상태로 된 이후 다른 클러스터에 같은 ID를 가진 다른 호스트가 있거나 이 호스트가 다른 클러스터에 추가되는 경우에는 해당 클러스터에 대한 클러스터 준비 프로세스가 실패합니다. *6.3.0에서 해결되었습니다.*

해결된 문제 1710624: REST API 요청 본문에 serverType을 지정하지 않으면 Windows 2008 이벤트 로그 서버가 "WIN2K3" 유형으로 추가됨

EventLog 서버 API 요청을 생성하면 서버가 "WIN2K3" 유형으로 추가됩니다. IDFW에 대해서만 EventLog 서버를 사용할 경우 IDFW가 제대로 작동하지 않을 수 있습니다. *6.3.0에서 해결되었습니다.*

NSX 6.3.0에서 해결된 설치 및 업그레이드 관련 문제

해결된 문제 1463767: 크로스 vCenter 배포에서 범용 방화벽 구성 섹션이 로컬 구성 섹션보다 아래(종속됨)에 있을 수 있음

보조 NSX Manager를 독립형(전송) 상태로 이동했다가 다시 보조 상태로 변경하면, 일시적으로 독립형 상태에 있는 동안 적용한 모든 로컬 구성 변경 사항이 기본 NSX Manager에서 상속된 범용 구성 섹션보다 위쪽에 나열될 수 있습니다. 이로 인해 오류 조건 범용 섹션은 보조 NSX Manager에서 다른 모든 섹션의 위에 있어야 함이 생성됩니다.

6.3.0에서 해결되었습니다.

해결된 문제 1402307: NSX for vSphere 업그레이드 프로세스 도중 vCenter가 재부팅되는 경우 올바르게 표시되지 않은 클러스터 상태가 표시됨

업그레이드 도중 NSX 준비 클러스터가 여러 개 있는 환경에서 호스트 준비를 수행할 때 최소 하나의 클러스터가 준비된 후 vCenter Server가 재부팅되는 경우, 다른 클러스터의 [클러스터 상태]가 [업데이트] 링크 대신 [준비되지 않음]으로 표시될 수 있습니다. vCenter의 호스트도 재부팅이 필요한 것으로 표시될 수 있습니다.

6.3.0에서 해결되었습니다.

해결된 문제 1495307: 업그레이드 도중 L2 및 L3 방화벽 규칙이 호스트에 게시되지 않음

분산 방화벽 구성에 변경 내용을 게시한 후에도 UI와 API 모두에서 상태가 진행 중으로 계속 표시되고 vsfwd.log 파일에 L2 또는 L3 규칙에 대한 로그가 기록되지 않습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1491820: NSX 6.2로 업그레이드한 후 NSX Manager 로그가 WARN messagingTaskExecutor-7 메시지를 수집함

NSX 6.1.x에서 NSX 6.2로 업그레이드한 후 NSX Manager 로그가 다음과 같은 메시지로 가득 찹니다. WARN messagingTaskExecutor-7 ControllerInfoHandler:48 - host is unknown: host-15 return empty list. 작동에는 영향을 미치지 않습니다. 6.3.0에서 해결되었습니다.

NSX 6.3.0에서 해결된 NSX Manager 관련 문제

해결된 문제 1671067: ESXTOP 플러그인이 함께 설치된 경우 vCenter Web Client에 NSX 플러그인이 나타나지 않음

NSX를 배포하고 vCenter에 등록한 후에 vCenter Web Client에 NSX 플러그인이 나타나지 않습니다. 이 문제는 NSX 플러그인과 ESXTOP 플러그인 간 충돌로 인해 발생합니다. 6.3.0에서 해결되었습니다.

NSX 6.3.0에서 해결된 네트워킹 및 Edge 서비스 관련 문제

해결된 문제 1740231: HA 인터페이스에서 IP 주소를 추가할 수 없음

6.3.0부터 DLR HA 인터페이스에서 IP 주소를 추가할 수 있습니다. 이 기능은 일부 이전 NSX 버전에서는 사용할 수 없지만 DLR HA 관리 인터페이스의 API 동작 일치를 위해 재도입되었습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1716333: Edge HA를 사용하거나 사용하지 않도록 설정하면서 Edge VM 크기 또는 배치 매개 변수를 변경하면 불필요한 Edge VM이 생성될 수 있음

Edge VM 크기 또는 배치 매개 변수(예: 데이터스토어 또는 리소스 풀)를 변경하면서 동시에 Edge HA를 사용하거나 사용하지 않도록 설정하면 NSX 관리 개체 데이터베이스가 손상되어 사용할 수 없는 Edge VM이 뒤에 남아 있을 수 있습니다. 또한 크로스 vCenter 환경에서 뒤에 남겨진 Edge VM이 보조 사이트로 복제됩니다. 6.3.0에서 해결되었습니다.

해결된 문제 1717369: HA 모드에서 구성할 경우 활성 및 대기 Edge VM 둘 다 동일한 호스트에 배포됨

이 문제는 다시 배포 및 업그레이드 작업 중에 반선후도 규칙이 생성되지 않고 vSphere 호스트에 자동으로 적용되지 않기 때문에 발생합니다. 이 문제는 기존 Edge에서 HA가 사용되도록 설정되면 나타나지 않습니다.

6.3.0에서 해결되었습니다. 다음은 예상된 동작입니다.

- vSphere HA가 사용되도록 설정되면 HA 쌍의 Edge VM에 대한 반선후도 규칙이 다시 배포, 업그레이드 중에 생성됩니다.
- vSphere HA가 사용되지 않도록 설정되면 HA 쌍의 Edge VM에 대한 반선후도 규칙이 생성되지 않습니다.

해결된 문제 1675659: 플로팅 정적 경로가 OSPF 동적 경로보다 선호됨

OSPF 경로를 사용할 수 있더라도 [경로 재배포]가 사용되도록 설정되어 있을 때 백업 플로팅 정적 경로가 Edge의 라우팅 테이블에 잘못 입력됩니다. 6.3.0에서 해결되었습니다.

해결된 문제 1733165: IPsec를 사용할 경우 NSX Edge 전달 테이블에서 동적 경로가 제거될 수 있음

동적 경로를 통해 도달 가능한 서브넷이 IPsec 구성에 대한 원격 서브넷으로 사용될 경우 NSX Edge는 전달 테이블에서 이 서브넷을 제거하며, 이 서브넷이 IPsec 구성에서 삭제된 후에도 이를 다시 설치하지 않습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1663902: NSX Edge VM 이름을 바꾸면 Edge를 통한 트래픽 흐름이 중단됨

NSX Edge VM 이름을 바꾸면 Edge를 통한 트래픽 흐름이 중단됩니다. 6.3.0에서 해결되었습니다.

해결된 문제 1624663: [고급 디버깅 구성]을 클릭하면 vCenter UI가 새로 고쳐지고 변경 사항이 지속되지 않음

특정 [Edge ID] > [구성] > [작업] > [고급 디버깅 구성]을 클릭하면 vCenter UI가 새로 고쳐지고 변경 사항은 지속되지 않습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1706429: 초기 논리적(분산) 라우터 배포 이후에 HA(고가용성)를 사용하도록 설정하면 통신 문제로 인해 두 논리적 라우터 장치가 모두 활성 상태가 될 수 있습니다.

HA 없이 논리적 라우터를 배포한 후 나중에 HA를 사용하도록 설정하거나(새 논리적 라우터 장치 배포) HA를 사용하지 않도록 설정했다가 다시 사용하도록 설정하면 경우에 따라 논리적 라우터 장치 중 하나가 HA 인터페이스와 연결된 경로를 잃게 됩니다. 이로 인해 두 장치가 모두 활성 상태가 됩니다. 6.3.0에서 해결되었습니다.

해결된 문제 1542416: 하위 인터페이스를 사용한 Edge 다시 배포 및 HA 페일오버 후에 5분 동안 데이터 경로가 작동하지 않음

하위 인터페이스를 사용하여 다시 배포 또는 HA 페일오버 작업을 수행하면 5분 동안 작동이 중단됩니다. 인터페이스에서는 문제가 나타나지 않습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1492547: IP 주소가 가장 높은 NSX 기반의 OSPF 영역 경계 라우터가 종료되거나 재부팅될 경우 수렴 시간이 오래 걸림

가장 높은 IP 주소를 갖고 있지 않은 NSSA 영역 경계 라우터를 종료하거나 재부팅할 경우에는 트래픽이 다른 경로로 빠르게 수렴됩니다. 가장 높은 IP 주소의 NSSA 영역 경계 라우터를 종료하거나 재부팅하면 다시 수렴하는 데 시간이 몇 분 이상 더 걸립니다. OSPF 프로세스를 수동으로 지우면 수렴 시간을 줄일 수 있습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1510724: 새 UDLR(범용 논리적 분산 라우터)을 생성한 후에 호스트에 기본 라우터가 채워지지 않음

NSX for vSphere 6.2.x에서 크로스 vCenter를 구성하기 위해 NSX Manager를 독립 실행형 모드에서 기본 모드로 변경한 후에 다음과 같은 증상이 나타날 수 있습니다.

- 새 UDLR을 생성할 경우 기본 경로가 호스트 인스턴스에 채워지지 않습니다.
- 경로는 UDLR 제어 VM에는 채워지지만 호스트 인스턴스에는 채워지지 않습니다.
- `show logical-router host host-ID dlr Edge-ID route` 명령을 실행할 경우 기본 경로가 표시되지 않습니다.

6.3.0에서 해결되었습니다.

해결된 문제 1704540: NSX L2 브리지 및 LACP를 사용하여 고용량 MAC 학습 테이블을 업데이트하면 메모리가 부족해질 수 있음

NSX L2 브리지가 다른 업링크에서 MAC 주소를 확인할 경우 netcpa 프로세스를 통해 컨트롤러에 MAC 학습 테이블 변경 내용을 보고합니다. LACP가 있는 네트워킹 환경은 여러 인터페이스에서 동일한 MAC 주소를 학습하므로 매우 큰 용량의 테이블이 업데이트되고 netcpa 프로세스에서 보고를 수행하는 데 필요한 메모리가 고갈될 수 있습니다.

[VMware 기술 자료 문서 2147181](#)을 참조하십시오. 6.3.0에서 해결되었습니다.

해결된 문제 1716545: Edge의 장치 크기를 변경해도 대기 Edge의 CPU 및 메모리 예약에는 영향을 미치지 않음

HA 쌍의 일부로 생성된 첫 번째 Edge VM만 예약 설정에 할당됩니다.

해결된 문제 1772004: Edge HA를 노드 0에서 노드 1로 페일오버하는 데 예상보다 오래 걸림

노드 1에서 노드 0으로 트래픽을 페일오버하는 데 걸리는 시간은 정상 수준이지만 Edge HA 구성 환경의 경우 노드 0에서 노드 1로 페일오버하는 데 예상보다 시간이 오래 걸립니다. 6.3.0에서 해결되었습니다.

해결된 문제 1726379: IP 멀티캐스트 범위의 마지막 3개 8진수에서 상한값이 99를 초과한 경우 VXLAN 트렁크 포트 그룹 구성이 실패함

세그먼트 ID를 구성하는 동안 마지막 3개의 8진수에서 상한값이 99를 초과(예: 1.100.100.100)하는 멀티캐스트 IP를 생성하고 동일한 멀티캐스트 IP 범위를 갖는 멀티캐스트 또는 하이브리드 논리적 스위치를 생성하는 경우 VXLAN 트렁크 포트 그룹 구성이 실패합니다. 6.3.0에서 해결되었습니다.

NSX 6.3.0에서 해결된 보안 서비스 관련 문제

해결된 문제 1767402: "적용 대상"이 "보안 그룹"으로 설정된 DFW 규칙이 호스트에 게시되지 않음
"적용 대상" 필드가 보안 그룹으로 설정된 DFW 규칙이 새 클러스터에서 ESXi 호스트로 푸시되지 않습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1743366: 잠재적인 충돌을 방지하기 위해 NSX 임계값 모니터링이 기본적으로 사용되지 않도록 설정된 방화벽 모듈이 실행될 경우 NSX는 잠재적 충돌을 방지하기 위해 메모리에 대한 임계값 모니터링을 사용하지 않도록 설정합니다. 호스트에서 ESX 6.5P01 또는 ESX 6.0U3 이상이 실행 중일 경우 메모리 임계값 모니터링이 자동으로 사용되도록 설정됩니다. 6.3.0에서 해결되었습니다.

해결된 문제 1491046: Ipv4 IP 주소가 자동 승인되지 않음
VMware NSX for vSphere 6.2.x에서 SpoofGuard 정책이 TOFU(최초 사용 시 신뢰)로 설정되었을 때 IPv4 IP 주소가 자동 승인되지 않음 6.3.0에서 해결되었습니다.

해결된 문제 1686036: 기본 섹션이 삭제된 경우 방화벽 규칙을 추가, 수정 또는 삭제할 수 없음
기본 계층 2 또는 계층 3 섹션이 삭제된 경우 방화벽 규칙 게시가 실패할 수 있습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1717994: DFW(분산 방화벽) 상태 API 쿼리가 간헐적으로 500 내부 서버 오류를 보고함
새 호스트를 호스트 준비 클러스터에 추가할 때 DFW 상태 API 쿼리가 실행된 경우 500 내부 서버 오류와 함께 API 쿼리가 여러 번 실패하다가 호스트가 VIB 설치를 시작하면 올바른 응답을 반환합니다. 6.3.0에서 해결되었습니다.

해결된 문제 1717635: 둘 이상의 클러스터가 운영 환경에 존재하고 동시에 변경될 경우 방화벽 구성 작업이 실패함
여러 개의 클러스터가 있는 운영 환경에서 둘 이상의 사용자가 아주 짧은 간격으로 연속해서 방화벽 구성을 수정하려고 할 경우 (예: 섹션 또는 규칙 추가/삭제), 일부 작업이 실패하고 다음과 비슷한 API 응답이 표시됩니다.
org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update; nested exception is javax.persistence.PersistenceException: org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update
6.3.0에서 해결되었습니다.

해결된 문제 1707931: Service Composer에 정의된 서비스 정책이 있을 때 분산 방화벽 규칙 순서가 변경되고, 방화벽 UI에 적용된 필터를 사용해서 방화벽 규칙이 수정되거나 게시됨
[Networking & Security] > [방화벽 UI]에서 하나 이상의 게시 작업을 수행한 후에 순서를 변경하거나 Service Composer에서 생성한 서비스 정책을 추가 또는 삭제하면 방화벽 규칙 순서가 변경되고 의도치 않은 결과가 나타날 수 있습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1682552: CPU/메모리/CPS에 대한 DFW(분산 방화벽)의 임계값 이벤트가 보고되지 않음
CPU/메모리/CPS에 대한 DFW 임계값 보고가 설정되어 있음에도 임계값을 넘었을 때 임계값 이벤트가 보고되지 않습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1620460: NSX에서 사용자가 Service Composer 규칙 섹션에서 규칙을 만드는 것을 방지하지 못함
vSphere Web Client의 Networking and Security에서: 방화벽 인터페이스에서 사용자가 Service Composer 규칙 섹션에 규칙을 추가하는 것을 방지하지 못합니다. 사용자가 Service Composer 섹션 내부의 위/아래(섹션 내부 제외)에 규칙을 추가할 수 있도록 허용해야 합니다. 6.3.0에서 해결되었습니다.

해결된 문제 1445897: VMware NSX for vSphere 6.1.x 및 6.2.x에서 참조된 개체가 삭제된 후에 분산 방화벽 (DFW) 규칙 게시가 실패함 6.2.3에서 해결되었습니다.

해결된 문제 1704661, 1739613: VM에서 다음 오류가 발생하면서 네트워크 연결이 끊어짐: "PF 상태를 복원하지 못함: 제한을 초과했습니다"
VM에서 다음 오류가 발생하면서 네트워크 연결이 끊어짐: "PF 상태를 복원하지 못함: 제한을 초과했습니다." 6.3.0에서 해결되었습니다.

NSX 6.3.0에서 해결된 솔루션 상호 운용성 관련 문제

해결된 문제 1527402: NSX Network Introspection 드라이버가 있는 Windows VM이 TCP에 연결되지 않음
VMware NSX for vSphere 6.x에서 NSX Network Introspection 드라이버(vnetfit.sys)가 USVM(Guest Introspection SVM)에 연결된 Windows VM에서 임시 TCP 네트워크에 대한 연결이 끊어졌습니다. 6.3.0에서 해결되었습니다.

해결된 문제 1530360: NSX Manager VM이 페일오버된 후에 SRM(Site Recovery Manager)에서 시간 초과 오류를 잘못 보고함

NSX Manager VM이 페일오버된 경우, SRM에서 VMware Tools 대기 중에 시간 초과 오류를 잘못 보고합니다. 이 경우에는 시간 초과 제한 300초 이내에 VMware Tools가 실제로 가동되어 실행 중입니다. 6.3.0에서 해결되었습니다.

문서 개정 이력

2017년 2월 2일: NSX 6.3.0용 1차 개정판.

2017년 2월 3일: NSX 6.3.0용 2차 개정판. 알려진 문제 1799543을 추가함

2017년 2월 22일: NSX 6.3.0용 3차 개정판. 업데이트된 CDO 정보

2017년 2월 27일: NSX 6.3.0용 4차 개정판. 알려진 문제 1808478 및 1818257을 추가함

2017년 3월 30일: NSX 6.3.0용 5차 개정판. 알려진 문제 1474650 및 1782321을 추가함

2017년 4월 10일: NSX 6.3.0용 6차 개정판. 업그레이드 정보 섹션에 정보를 추가함.

2017년 5월 3일: NSX 6.3.0용 7차 개정판. vCNS Edge 및 VIX의 사용 중지에 대한 정보를 추가함.

2017년 6월 2일: NSX 6.3.0용 8차 개정판. 알려진 문제 1860583, 1781438 및 1825416을 추가함.

2017년 6월 22일: NSX 6.3.0용 9차 개정판. 알려진 문제 1847753을 추가함.

2017년 8월 21일: NSX 6.3.0용 10차 개정판. 해결된 문제 1463767을 추가함 및 일부 이전 문제를 삭제함.

2017년 10월 2일: NSX 6.3.0용 11차 개정판. 최소 권장 버전을 업데이트함.