



Versionshinweise für VMware NSX-T Data Center 2.5

VMware NSX-T Data Center 2.5 | 19. September 2019 | Build 14663974

Überprüfen Sie regelmäßig, ob Erweiterungen und Updates für diese Versionshinweise zur Verfügung stehen.

Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

- [Neuigkeiten](#)
- [Kompatibilität und Systemvoraussetzungen](#)
- [Allgemeine Änderungen des Verhaltens](#)
- [Veraltete APIs und Änderungen des Verhaltens](#)
- [Verfügbare Sprachen](#)
- [API und CLI-Ressourcen](#)
- [Revisionsverlauf](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

Neuigkeiten

NSX-T Data Center 2.5 bietet verschiedene neue Funktionen für virtualisierte Netzwerke und Sicherheit für Private Cloud, Public Cloud und Hybrid Cloud. Zu den wichtigsten Neuerungen gehören Verbesserungen bei der Intent-basierten Netzwerkbenutzeroberfläche, der kontextbezogenen Firewall, den Gast- und Netzwerk-Introspektionsfunktionen, der IPv6-Unterstützung, der hochverfügbaren Cluster-Verwaltung, profilbasierte NSX-Installation für vSphere-Computing-Cluster und Verbesserungen beim Migrations-Koordinator für das Migrieren von NSX Data Center for vSphere zu NSX-T Data Center.

NSX Intelligence

Mit NSX-T Data Center 2.5 wird NSX Intelligence v1.0, eine neue NSX Analysekomponente, eingeführt. NSX Intelligence bietet eine Benutzeroberfläche über einen einzelnen Verwaltungsbereich innerhalb von NSX Manager und bietet die folgenden Funktionen:

- Nahezu Echtzeit-Flow-Informationen für Arbeitslasten in Ihrer Umgebung.
- NSX Intelligence korreliert Live-Flows oder historische Flows, Benutzerkonfigurationen und Arbeitslast-Bestandslisten.
- Verlaufsinformationen zu Flows, Benutzerkonfigurationen und Arbeitslast-Bestandslisten können angezeigt werden.
- Automatisierte Planung der Mikrosegmentierung durch Empfehlung von Firewallregeln, Gruppen und Diensten.

Unterstützung der Container-API

Für die Container-Bestandsliste ist eine neue API-Unterstützung verfügbar. Informationen finden Sie in der API-Dokumentation.

L2-Netzwerk

- **Verbesserungen der Edge-Bridge** – Bei der Edge-Bridge können Sie nun dasselbe Segment an mehrere Bridge-Profile anhängen und damit ein Segment mehrmals über eine Bridge mit VLANs in der physischen Infrastruktur verbinden. Diese neue Funktionalität ersetzt und verdrängt die ursprüngliche ESXi-Bridge in früheren Versionen von NSX-T Data Center. **Vorsicht:** Die Verwendung dieser Funktion erfolgt auf eigene Gefahr. Dadurch entsteht das Risiko, eine Bridging-Schleife zu erstellen, indem dasselbe Segment zweimal mit derselben L2-Domäne im physischen Netzwerk überbrückt wird. Es gibt keinen Mechanismus zur Vermeidung von Schleifen.
- **MTU/VLAN-Integritätsprüfung** – Aus Betriebssicht sind Probleme bei der Netzwerkkonnektivität, die durch Konfigurationsfehler verursacht werden, oft schwer zu identifizieren. Bei häufig auftretenden Szenarien verwenden Administratoren virtueller Netzwerke NSX Manager, während Administratoren physischer Netzwerke die Managementzuständigkeit für physische Netzwerk-Switches übernehmen.
 - **VLAN-Integritätsprüfung** – überprüft, ob die N-VDS-VLAN-Einstellungen der Trunk-Port-Konfiguration auf den benachbarten physischen Switch-Ports entsprechen.
 - **MTU-Integritätsprüfung** – überprüft, ob die MTU-Einstellung für den auf VLAN basierenden physischen Zugriffs-Switch-Port der MTU-Einstellung für N-VDS entspricht.
- **Gast-Inter-VLAN-Tagging** – Der erweiterte Datenpfad N-VDS ermöglicht es Benutzern, einem Segment ein Gast-VLAN-Tag zuzuordnen. Diese Funktion überwindet die Beschränkung von 10 vNICs pro VM und ermöglicht einen durch die NSX-Infrastruktur gerouteten Gast-Datenverkehr mit VLAN-Tags (der verschiedenen Segmenten zugeordnet ist).

L3-Netzwerk

- **Tier-1-Platzierung innerhalb des Edge-Clusters basierend auf der Fehlerdomäne** – damit werden von NSX-T automatisch Tier-1-Gateways basierend auf den benutzerdefinierten Fehlerdomänen platziert. Dies erhöht die Zuverlässigkeit von Tier-1-Gateways bei Verfügbarkeitsbereichen, Racks oder Hosts, auch wenn die automatische Platzierung von Tier-1-Gateways verwendet wird.
- **Asymmetrische Lastfreigabe nach einem Router-Ausfall in der ECMP-Topologie** – bei aktiv/aktiv Tier-0-Gateways Übernahme, wenn ein fehlerhafter Dienstrouter ausgefallen ist, ein anderer Router den Datenverkehr des fehlerhaften Routers und verdoppelte den Datenverkehr, der über den Dienstrouter verlief. 30 Minuten nach einem Router-Ausfall wird die IP-Adresse des fehlerhaften Routers aus der Liste der nächsten Hops entfernt, wodurch der zusätzliche Datenverkehr zu einem bestimmten Router vermieden wird.
- **Abrufen von BGP-angekündigten und -empfangenen Routen pro Peer über API** – vereinfacht BGP-Vorgänge, indem die CLI-Nutzung zur Überprüfung der empfangenen und an BGP-Peers gesendeten Routen vermieden wird.
- **BGP Large Community-Unterstützung** – bietet die Option, Communities in Verbindung mit 4-Byte-ASN gemäß der Definition in RFC8092 zu verwenden.
- **BGP Graceful Restart Hilfsmodusoption pro Peer** – Mit dieser Option können für Tier-0-Gateways Router für physische Northbound-Router mit redundanter Control Plane beibehalten werden, ohne die Failover-Zeit bei Tier-0-Routern zu gefährden.
- **Massen-API zur Erstellung mehrerer NAT-Regeln** – verbessert die vorhandene NAT-API, um die Erstellung einer großen Anzahl von NAT-Regeln in einem einzigen API-Aufruf zu bündeln.

Edge-Plattform

- **Unterstützung von Mellanox ConnectX-4 und ConnectX-4 LX auf dem Bare Metal Edge-Knoten** – Bare Metal Edge-Knoten unterstützen jetzt die physischen Netzwerkkarten Mellanox ConnectX-4 und ConnectX-4 LX in 10/25/40/50/100 GBit/s.
- **Bare Metal Edge PNIC Management** – bietet die Option, die physischen Netzwerkkarten auszuwählen, die als Netzwerkkarten auf Dateiebene (FastPath) verwendet werden sollen.

Außerdem wird die Anzahl der physischen Netzwerkkarten, die auf dem Bare Metal Edge-Knoten unterstützt werden, von 8 auf 16 PNICs erhöht.

Verbesserte IPv6-Unterstützung

Bei NSX-T 2.5 wurde der Funktionssatz für IPv6-Routing/-Weiterleitung weiter verbessert. Dies schließt die Unterstützung für Folgendes ein:

- IPv6-SLAAC (statusfreie Adressenautokonfiguration), die automatisch IPv6-Adressen für virtuelle Maschinen bereitstellt.
- IPv6-Router-Ankündigung: NSX-T-Gateways stellen IPv6-Parameter über die Router-Ankündigung bereit.
- IPv6-DAD: NSX-T Gateways erkennen eine duplizierte IPv6-Adresszuteilung.

Firewall-Verbesserungen

Unterstützung der Schicht-7-App-ID

Bei NSX-T 2.5 sind weitere Schicht-7-Funktionen für verteilte Firewalls und Gateway-Firewalls enthalten. Dies schließt die Unterstützung für Folgendes ein:

- Unterstützung der Schicht-7-App-ID für verteilte Firewalls auf KVM.
- Unterstützung der Schicht-7-App-ID für Gateway-Firewalls.
- Mehrere Konfigurationen für die Schicht-7-App-ID in einer einzigen Firewallregel.

Verbesserungen bei FQDN-/URL-Filterung

NSX-T 2.5 verfügt über folgende geringfügige Verbesserungen bei der Unterstützung der FQDN-Filterung:

- Konfigurieren von TTL-Timern für DNS-Einträge.
- Unterstützung für auf dem KVM-Hypervisor durchgeführte Arbeitslasten.

Firewall-Vorgänge wurden durch die folgenden Funktionen erweitert:

- **Autosave-Konfiguration und Wiederherstellungsfunktion** – das System erstellt bei der Veröffentlichung eine Kopie der Konfiguration. Diese Konfiguration kann für die Wiederherstellung eines vorhandenen Status erneut bereitgestellt werden.
- **Manuelle Entwürfe** – Benutzer können jetzt Entwürfe ihrer Regeln speichern, bevor Sie diese Regelsätze für die Durchsetzung veröffentlichen. Benutzer können die Regeln in manuellen Entwürfen bereitstellen. Mit dem System können mehrere Benutzer am selben Entwurf arbeiten. Außerdem gibt es einen Sperrmechanismus, um die Überschreibung von Regeln durch andere Benutzer zu deaktivieren.
- **Sitzungs-Timer** – Benutzer können Sitzungs-Timer für TCP-, UDP-und ICMP-Sitzungen konfigurieren.
- **Flood Protection** – sowohl verteilte Firewalls als auch Gateway-Firewalls können mit SYN-Flood-Schutz geschützt werden. Benutzer können Schwellenwerte für Alarme, Protokolle und verringerten Datenverkehr einstellen, um benutzerdefinierte Workflows zu erstellen.
- **Das System generiert automatisch zwei Gruppen**, wenn der NSX-LoadBalancer erstellt wird und virtuelle Server bereitgestellt werden. Eine Gruppe enthält den Serverpool, während die andere Gruppe die IP des virtuellen Servers enthält. Diese Gruppen können auf verteilten Firewalls oder Gateway-Firewalls verwendet werden, damit Firewall-Administratoren den Datenverkehr zulassen oder verweigern können. Diese Gruppen folgen den Änderungen in der NSX-Load-Balancer-Konfiguration.
- **Die Anzahl der IP-Adressen**, die pro VM-vNIC erkannt wird, wurde von 128 auf 256 IP-Adressen erhöht.

Identitätsbasierte Firewall

- Mit NSX-T 2.5 werden auf Windows 2016 bereitgestellte Active Directory-Server unterstützt.

- Es wird die identitätsbasierte Firewall für Arbeitslasten auf dem Windows Server ohne aktivierte Terminaldienste unterstützt. Auf diese Weise können Kunden die Lateral Movements von Administratoren von einem Server auf einen anderen streng steuern.

Service Insertion

- **Unterstützung für Paketkopien** – zusätzlich zur Umleitung von Datenverkehr über einen Dienst unterstützt NSX-T jetzt den Anwendungsfall für die Netzwerküberwachung, bei dem eine Kopie der Pakete an eine Partnerdienst-VM (SVM) weitergeleitet wird. Damit ist eine Überprüfung, Überwachung oder Erhebung von Statistiken möglich, wobei das ursprüngliche Paket nicht über den Netzwerküberwachungsdienst geleitet wird.
- **Bereitstellung automatisierter host-basierter Partner-SVMs** – Ab NSX-T 2.5 werden zwei Modi für die Bereitstellung von Partner-SVMs unterstützt: Geclusterte Bereitstellung, bei der Dienst-VMs auf einem dedizierten vSphere (Dienst)-Cluster bereitgestellt werden, und host-basierte Bereitstellung, bei der eine Dienst-VM pro Dienst auf jedem Computing-Host in einem bestimmten Cluster bereitgestellt wird. Bei diesem Modus werden die entsprechenden SVMs, wenn ein neuer Computing-Host zu einem Cluster hinzugefügt wird, automatisch bereitgestellt.
- **Benachrichtigungsunterstützung für Nord-Süd-Diensteinfügungen** – NSX-T 2.4 führte das Benachrichtigungs-Framework für die Ost-West-Diensteinfügung ein. Damit konnten Partnerdienste automatisch Benachrichtigungen über wichtige Änderungen, wie Aktualisierungen in der dynamischen Gruppe, erhalten. Mit NSX-T 2.5 wurde dieses Benachrichtigungs-Framework auch auf die N-S-Diensteinfügung ausgeweitet. Partner können diesen Mechanismus nutzen, um Kunden die Verwendung dynamischer NSX-Gruppen (z. B. basierend auf Tags, Betriebssystem, VM-Name) in der Partnerrichtlinie zu erlauben.
- **Weitere Fehlerbehebungen und Visualisierungsfunktionen** – Bei NSX-T 2.5 wurden verschiedene Verbesserungen bei der Wartungsfreundlichkeit vorgenommen, um eine bessere Fehlerbehebung bei Problemen in Verbindung mit Diensteinfügungen zu ermöglichen. Jetzt können der Laufzeitstatus einer Dienstinstanz überprüft, verfügbare Dienstpfade über die API abgerufen und die mit der Diensteinfügung verknüpften Protokolle in das Support-Paket einbezogen werden.

Endpoint-Schutz (Guest Introspection)

- **Linux-Unterstützung** – Unterstützung für Linux-basierte Betriebssysteme mit Endpoint-Schutz. Weitere Informationen zu unterstützten Linux-Betriebssystemen und zur Guest Introspection finden Sie im Administratorhandbuch für NSX-T.
- **Endpoint-Schutz-Dashboard** – Über das Endpoint-Schutz-Dashboard können der Konfigurationsstatus von geschützten und ungeschützten VMs, Probleme mit dem Hostagent und Dienst-VMs sowie VMs, die mit dem in der VMware Tools-Installation enthaltenen Datei-Introspektionstreiber konfiguriert wurden, eingesehen und überwacht werden.
- **Dashboardüberwachung** – Damit können Sie den Bereitstellungsstatus des Partnerdienstes in den Clustern des Systems überwachen.

Load Balancing

- **API zum Abrufen des Edge-Kapazitätsstatus für Load Balancer** – Es wurden neue API-Aufrufe hinzugefügt, damit der Administrator die Edge-Kapazität in Bezug auf Load Balancing-Instanzen überwachen kann.
- **Intelligente Auswahl der IP-Adresse für die Integritätsprüfung** – Wenn die SNAT-IP-Liste konfiguriert ist, wird die erste IP-Adresse in der Liste für die Zustandsüberwachung anstelle der Uplink-IP-Adresse eines Tier-1-Gateways verwendet. Die IP-Adresse kann mit der IP-Adresse des virtuellen Servers identisch sein. Durch diese Verbesserung kann der Load Balancer eine einzelne IP-Adresse für die Überwachung der Quell-NAT und des Zustands verwenden.
- **Verbesserungen bei der Protokollierung des Load Balancer** – Mit dieser Verbesserung kann der Load Balancer für jeden virtuellen Server eine umfangreiche Protokollmeldung zur Überwachung generieren. Das Zugriffsprotokoll für den virtuellen Server enthält beispielsweise nicht nur die Client-IP-Adresse, sondern auch die IP-Adresse des Poolmitglieds.
- **Dauerhafte Verbesserung bei LB-Regeln** – eine neue Aktion mit dem Namen „Beibehalten“ ist bei

den LB-Regeln verfügbar. Mit der Aktion „Beibehalten“ kann der Load Balancer basierend auf den von Poolmitgliedern gesetzten Cookies Anwendungspersistenzen bieten.

- **Passendes LB** – Eine kleine LB-Instanz passt in eine kleine Edge-VM. Eine mittlere LB-Instanz passt in eine mittlere Edge-VM. Zuvor unterstützte die kleine Edge-VM keine Load Balancing-Dienste, da die Größe einer Edge-VM größer als die einer LB-Instanz sein musste.
- **VS-/Pool-/Mitgliederstatistik** – Alle LB-bezogenen Statistiken sind über die vereinfachte Schnittstelle verfügbar. Bisher waren die Informationen nur über die Schnittstelle „Netzwerk und Sicherheit – Erweitert“ verfügbar.
- **ECC (Elliptisches Kurvenzertifikat)-Unterstützung für SSL-Beendigung** – EC-Zertifikate können für eine verbesserte SSL-Leistung verwendet werden.
- **FIPS-Knopf** – Es gibt eine über API verfügbare globale Einstellung für die FIPS-Übereinstimmung der Load Balancer. Standardmäßig ist die Einstellung deaktiviert, um die Leistung zu verbessern.

VPN

- **IPSec-VPN-Unterstützung auf Tier-1-Gateway** – IPSec-VPN kann für eine bessere Mandantenisolierung und Skalierbarkeit auf einem Tier-1-Gateway bereitgestellt und beendet werden. Bisher wurde es nur auf dem Tier-0-Gateway unterstützt.
- **VLAN-Unterstützung für Schicht-2-VPN auf NSX-verwaltetem Edge** – Mit dieser Verbesserung können VLAN-gestützte Segmente erweitert werden. Bisher wurden nur logische Segmente für die Schicht-2-Erweiterung unterstützt. Dies beinhaltet die Unterstützung von VLAN-Trunking, sodass mehrere VLANs auf einer Edge-Schnittstelle und einer Schicht-2-VPN-Sitzung erweitert werden können.
- **TCP-MSS-Klemmung für IPSec-VPN** – Die TCP-MSS-Klemmung ermöglicht es dem Administrator, den MSS-Wert aller TCP-Verbindungen zu erzwingen, um eine Paketfragmentierung zu vermeiden.
- **ECC (Elliptisches Kurvenzertifikat)-Unterstützung für IPSec-VPN** – Das EC-Zertifikat ist erforderlich, um verschiedene IPSec-Übereinstimmungs-Suites wie CNSA, UK Prime usw. zu aktivieren.
- **Easy Button für die Konfiguration der Übereinstimmungs-Suite** – CNSA, Suite-B-GCM, Suite-B-GMAC, Prime, Foundation und FIPS können mit einem einzigen Klick in der Benutzeroberfläche oder einem einzelnen API-Aufruf konfiguriert werden.

Automatisierung, OpenStack und anderer CMP

- **Erweiterte OpenStack-Versionsunterstützung** – Enthält jetzt die Stein- und Rocky-Versionen.
- **OpenStack Neutron-Plug-In zur Unterstützung der Richtlinien-API** – Zusätzlich zur Plug-In unterstützenden Verwaltungs-API bieten wir nun ein OpenStack Neutron-Plug-In, das die neue NSX-T-Richtlinien-API nutzt. Dieses Plug-In unterstützt IPv6 für Schicht-2, L3, Firewall und SLAAC.
- **OpenStack Neutron Router-Optimierung** – Der OpenStack Neutron Router wird jetzt durch das Plug-In optimiert, indem das Erstellen/Löschen des Dienst-Routers dynamisch verwaltet wird. Damit haben Kunden nur einen verteilten Router, wenn keine Dienste konfiguriert sind, und einen, sobald die Dienste hinzugefügt werden. Dabei wird alles vom Plug-In verwaltet.
- **OpenStack Neutron-Plug-In-Schicht-2-Bridge** – Die von OpenStack konfigurierte Schicht-2-Bridge ist jetzt auf dem Edge-Cluster und nicht auf dem ESXi-Cluster konfiguriert.
- **Openstack Octavia-Unterstützung** – Neben LBaaSv2 unterstützt das OpenStack Neutron-Plug-In auch Octavia als eine Möglichkeit, das Load Balancing zu unterstützen.
Weitere Informationen finden Sie in den Versionshinweisen zum VMware NSX-T Data Center 2.5-Plug-In für OpenStack Neutron.

NSX Cloud

- **Neuer Betriebsmodus hinzugefügt** – NSX Cloud verfügt nun über zwei Betriebsmodi. Dadurch ist NSX Cloud offiziell die einzige Hybrid Cloud-Lösung auf dem Markt, die Betriebsmodi mit und ohne Agent unterstützt.
 - **NSX-erzwungener Modus (mit Agent)** – bietet ein „konsistentes“ Richtlinien-Framework zwischen lokalen Systemen und einer Public Cloud. NSX-Richtliniendurchsetzung erfolgt mit NSX-Tools, die in jeder Arbeitslast installiert sind. Dies bietet Granularität auf VM-Ebene und

alle gekennzeichneten VMs werden von NSX verwaltet. Mit diesem Modus werden die Unterschiede/Einschränkungen einzelner Public Cloud-Anbieter überwunden und ein konsistentes Richtlinien-Framework zwischen lokalen und Public Cloud-Arbeitslasten bereitgestellt.

- **Native Cloud-erzwungener Modus (ohne Agent)** – stellt ein „allgemeines“ Richtlinien-Framework zwischen lokalen Systemen und einer Public Cloud bereit. Für diesem Modus ist die Installation von NSX Tools bei den Arbeitslasten nicht erforderlich. NSX-Sicherheitsrichtlinien werden in die Sicherheitskonstrukte der nativen Cloud-Anbieter konvertiert. Daher sind alle Skalierungs-und Funktionseinschränkungen der ausgewählten Public Cloud anwendbar. Die Granularität der Steuerung liegt auf der VPC/VPNET-Ebene und jede Arbeitslast innerhalb einer verwalteten VPC/VNET wird von NSX verwaltet, sofern Sie nicht in der Whitelist enthalten ist.

Beide Modi bieten eine dynamische Gruppenmitgliedschaft und eine umfassende Reihe an Abstraktionen für die Mitgliedschaftskriterien der NSX-Gruppe.

- **Unterstützung der Sichtbarkeit und Sicherheit von nativen Public Cloud-Diensten von NSX Cloud** – Ab dieser Version ist es möglich, die Sicherheitsgruppen von nativen SaaS-Diensten in Azure und AWS zu programmieren, die einen lokalen VPC/VNET-Endpoint und eine zugeordnete Sicherheitsgruppe aufweisen. Das Hauptziel ist die Ermittlung und Sicherung von Native Cloud-Dienst-Endpoints mit benutzerdefinierten Regeln für die NSX-Richtlinie. Die folgenden Dienste werden bei dieser Version in AWS (ELB, RDS und DynamoDB) und Azure (Azure Storage, Azure LB, Azure SQL Server und CosmosDB) unterstützt. Bei zukünftigen NSX-T-Versionen werden zusätzliche Unterstützungen für weitere Dienste hinzugefügt.
- **Unterstützung folgender neuer Betriebssysteme:**
 - Unterstützung für Windows Server 2019
 - Windows 10 v1809
 - Unterstützung für Ubuntu 18.04
- **Erweiterte Quarantäne-Richtlinie und VM-White-Listing** – ab NSX 2.5 können Nutzer in NSX Cloud über die CSM-Schnittstelle VMs auf die Whitelist setzen. Nachdem die VMs auf die Whitelist gesetzt wurden, werden ihre Cloud-Sicherheitsgruppen nicht von NSX verwaltet und Benutzer können die VMs in alle Cloud-Sicherheitsgruppen platzieren.
- **Verbesserte Fehlerberichte auf der CSM-Schnittstelle** – ermöglicht eine schnellere Fehlerbehebung.

Betrieb

- **Unterstützung von vSphere HA für den/die NSX Manager** – Der NSX-Management-Cluster kann jetzt durch vSphere HA geschützt werden. Auf diese Weise kann ein Knoten des NSX-Management-Clusters wiederhergestellt werden, wenn der ausführende Host ausfällt. Darüber hinaus kann der gesamte NSX-Management-Cluster auf einer anderen Site wiederhergestellt werden, wenn ein Fehler auf Site-Ebene vorliegt. Weitere Informationen zu unterstützten Szenarien finden Sie im Installationshandbuch für NSX-T.
- **Verbesserungen beim Kapazitäts-Dashboard** – Neue und verbesserte Metriken für das Kapazitäts-Dashboard zeigen die Anzahl der Objekte an, die ein Kunde in Bezug auf den im Produkt unterstützten Maximalwert konfiguriert hat. Eine vollständige Auflistung der Maximalwerte für die Konfiguration von NSX-T Data Center finden Sie im Tool VMware Configuration Maximums.
- **Unterstützung für den vSphere-Sperrmodus** – Geben Sie Kunden mehr Bereitstellungsoptionen, indem Sie die Möglichkeit bieten, NSX-T in einer Umgebung mit vSphere-Sperrmodus zu installieren, zu aktualisieren und zu betreiben.
- **Verbesserte Protokollierung** – Reduzieren Sie die Dienstauswirkung bei der Fehlerbehebung, indem Sie die dynamische Änderung der Protokollebenen über die NSX-Befehlszeilenschnittstelle für NSX-Benutzerspeicher-Agenten aktivieren.
- **SNMPv3-Unterstützung** – verbesserte Sicherheitsübereinstimmung durch Hinzufügen der Konfigurationsunterstützung für SNMPv3 für NSX Edge und Manager Appliance.
- **Neue Traceflow-Funktion zur Fehlerbehebung von Problemen bei der VM-Adressauflösung** – Zusätzliche Unterstützung für das Einfügen von ARP-/NDP-Paketen über Traceflow, um Verbindungsprobleme bei der Adressauflösung für ein IP-Ziel zu erkennen.
- **Änderung der Upgrade-Reihenfolge** – beim Upgrade auf NSX-T 2.5 ist die neue Upgrade-

Reihenfolge wie folgt: erst das Upgrade der Edge-Komponente und dann das Upgrade der Host Komponente. Diese Verbesserung bietet große Vorteile beim Upgrade der Cloud-Infrastruktur, da durch Optimierungen das allgemeine Wartungsfenster reduziert werden kann.

- **Verbesserung des Log Insight-Inhaltspakets** – Zusätzliche Unterstützung für vorgefertigte Protokollwarnungen durch das neue mit NSX-T 2.5 kompatible NSX-T-Inhaltspaket.

Plattformsicherheit

- **FIPS** – Benutzer können jetzt FIPS-Übereinstimmungsberichte generieren. Außerdem können sie ihre NSX-Bereitstellungen im FIPS-kompatiblen Modus konfigurieren und verwalten. Kryptografische Module werden gemäß den FIPS-Standards validiert und bieten Kunden, die Bundesvorschriften entsprechen oder NSX sicher entsprechend der FIPS-Standards betreiben möchten, Sicherheit. Bis auf die bekannten Ausnahmen sind alle kryptografischen Module in NSX-T 2.5 FIPS-zertifiziert. Die gewährten Zertifikate für FIPS-validierte Module finden Sie unter <https://www.vmware.com/security/certifications/fips.html>.
- **Verbesserungen beim Kennwort-Management** – Benutzer können jetzt den Kennwortablaufzeitraum (Anzahl Tage) seit der letzten Kennwortänderung auch nach dem Upgrade verlängern. Warnungen zum Ablauf von dreißig Tagen und Benachrichtigungen über Kennwortablauf werden jetzt in der-Schnittstelle, in der CLI und in den Syslogs angezeigt.

Unterstützung für ein Design mit einem einzelnen Cluster

Unterstützung für Designs mit einem einzelnen Cluster, in dem Edge- Management- + Computing-VMs, die alle von einem einzelnen N-VDS in einem Cluster mit mindestens vier Hosts betrieben werden, zusammengefasst sind. Für typische Referenzdesigns für VxRail und andere Host-Lösungen von Cloud-Anbietern sind 4x10G pNICs mit zwei Host-Switches vorgegeben. Ein Switch ist für Edge- + Management-VMs (VDS) dediziert und der andere für Computing-VMS (N-VDS). Zwei Host-Switches trennen effektiv den Management-Datenverkehr vom Computing-Datenverkehr. Durch die mit 10G und 25G möglichen Einsparungen, werden Hosts mit zwei pNICs jedoch zunehmend zum Standard für kleine Datacenter und Kunden von Cloud-Anbietern. Mit diesem Formfaktor können kleine Datacenter und Cloud-Anbieter-Kunden eine NSX-T-basierte Lösung mit einem einzigen N-VDS erstellen und alle Komponenten mit zwei pNICs versorgen.

Migration von NSX Data Center for vSphere zu NSX-T Data Center

- **Verbesserungen beim Migrations-Koordinator** – Beim Migrations-Koordinator wurden mehrere Verbesserungen der Benutzerfreundlichkeit eingeführt, die den Workflow des Prozesses zur Migration von NSX Data Center for vSphere zu NSX-T Data Center verbessern. Außerdem gibt es Verbesserungen bei der Bereitstellung von Benutzerfeedback während der Migration.

Kompatibilität und Systemvoraussetzungen

Informationen zur Kompatibilität und zu den Systemvoraussetzungen finden Sie im [Installationshandbuch für NSX-T Data Center](#).

Allgemeine Änderungen des Verhaltens

Änderungen des NSX-T Data Center-Systemkommunikations-Ports

Ab NSX-T Data Center 2.5 wurde der TCP-Port des NSX-Messaging-Kanals von allen Transport- und Edge-Knoten zu NSX Managern von TCP-Port 5671 zu Port 1234 geändert. Stellen Sie aufgrund dieser Änderung sicher, dass alle NSX-T-Transport- und -Edge-Knoten sowohl auf den TCP-Ports 1234 zu den NSX Managern als auch auf dem TCP-Port 1235 zu den NSX-Controllern kommunizieren können, bevor Sie ein Upgrade auf NSX-T Data Center 2.5 durchführen. Stellen Sie außerdem sicher, dass Port 5671 während des Upgrade-Vorgangs geöffnet bleibt.

L2-Netzwerk

Aufgrund der Verbesserungen bei Schicht-2-Bridges ist die ESXi-Bridge veraltet. NSX-T wurde anfänglich mit der Funktion eingeführt, einen ESXi-Host als Bridge zu dedizieren, um ein Overlay-Segment auf ein VLAN zu erweitern. Dieses Modell wird ab dieser Version nicht mehr unterstützt, da die neue Edge-Bridge es mit ihren Funktionen ersetzt, keinen dedizierten ESXi-Host benötigt und den optimierten Datenpfad des Edge-Knotens nutzt. Weitere Informationen finden Sie im Abschnitt „Neuigkeiten“

Veraltete APIs und Änderungen des Verhaltens

Vorlagen-APIs für Transportknoten sind in dieser Version veraltet. Sie sollten stattdessen Profil-APIs für Transportknoten verwenden. Eine Liste der veralteten Typen und Methoden finden Sie im [API-Handbuch](#).

API und CLI-Ressourcen

Informationen zur Verwendung der NSX-T Data Center-APIs oder -CLIs für die Automation finden Sie unter code.vmware.com.

Die API-Dokumentation ist über die Registerkarte **API-Referenz** verfügbar. Die CLI-Dokumentation ist über die Registerkarte **Dokumentation** verfügbar.

Verfügbare Sprachen

NSX-T Data Center wurde in mehrere Sprachen lokalisiert: Englisch, Deutsch, Französisch, Japanisch, vereinfachtes Chinesisch, Koreanisch, traditionelles Chinesisch und Spanisch. Da die NSX-T Data Center-Lokalisierung die Browser-Spracheinstellungen verwendet, müssen Sie sicherstellen, dass Ihre Einstellungen mit der gewünschten Sprache übereinstimmen.

Revisionsverlauf der Dokumente

- 19. September 2019. Erste Auflage.
- 23. September 2019. Die bekannten Probleme 2424818 und 2419246 wurden hinzugefügt. Die bekannten Probleme 2364756, 2406018 und 2383328 wurden hinzugefügt.
- 24. September 2019. Elemente unter „Neuerungen“ wurden aktualisiert.
- 3. Oktober 2019. Behobenes Problem 2313673 wurde hinzugefügt.
- 12. November 2019. Die bekannten Probleme 2362688 und 2436302 wurden hinzugefügt. Das Problem 2282798 wurde behoben und unter „Behobene Probleme“ verschoben.
- 17. Dezember 2019. Das bekannte Problem 2444170 wurde hinzugefügt.
- 14. Januar 2020. Das behobene Problem 2399994 wurde hinzugefügt.
- 18. Februar 2020. Das bekannte Problem 2436302 wurde mit dem Link zum KB-Artikel aktualisiert.
- 14. Mai 2020. Das bekannte Problem 2467479 wurde hinzugefügt.
- 25. September 2020. Das bekannte Problem 2586606 wurde hinzugefügt.
- 15. März 2021. Bekanntes Problem 2730634 wurde hinzugefügt.

Behobene Probleme

- **Behobenes Problem 2288774 – Segment-Port gibt einen Realisierungsfehler aus, weil die Anzahl der Tags (fälschlicherweise) 30 überschreitet.**
Bei der Benutzereingabe wird fälschlicherweise versucht, mehr als 30 Tags anzuwenden. Der Richtlinien-Workflow validiert/verweigert jedoch die Benutzereingabe nicht ordnungsgemäß und lässt die Konfiguration zu. Die Richtlinie zeigt dann einen Alarm mit der korrekten Fehlermeldung an, dass der Benutzer nicht mehr als 30 Tags verwenden darf. An diesem Punkt kann der Benutzer das Problem beheben.

- **Behobenes Problem 2334442** – Benutzer verfügt nicht über die Berechtigung zum Bearbeiten oder Löschen von erstellten Objekten, nachdem der Admin-Benutzer umbenannt wurde.
Der Benutzer verfügt nicht über die Berechtigung zum Bearbeiten oder Löschen von erstellten Objekten, nachdem der Admin-Benutzer umbenannt wird. Admin-/Auditor-Benutzer können nicht umbenannt werden.
- **Behobenes Problem 2256709** – Eine Instant Clone-VM oder eine aus einem Snapshot wiederhergestellte VM verliert während vMotion kurzzeitig den AV-Schutz.
Der Snapshot einer VM wird wiederhergestellt, und die VM wird auf einen anderen Host migriert. Die Partnerkonsole zeigt keinen AV-Schutz für die migrierte Instant Clone-VM an. Es tritt ein kurzzeitiger Verlust des AV-Schutzes auf.
- **Behobenes Problem 2261431** – Abhängig von den anderen Bereitstellungsparametern ist eine gefilterte Liste von Datenspeichern erforderlich.
Entsprechender Fehler wird auf der Benutzeroberfläche angezeigt, wenn die falsche Option ausgewählt wurde. Der Kunde kann zur Behebung dieses Fehlers diese Bereitstellung löschen und eine neue erstellen.
- **Behobenes Problem 2274988** – Dienstketten unterstützen aufeinander folgende Dienstprofile vom selben Dienst nicht.
Der Datenverkehr durchläuft keine Dienstkette und wird immer dann verworfen, wenn die Kette zwei aufeinander folgende und zum selben Dienst gehörende Dienstprofile aufweist.
- **Behobenes Problem 2277742** – Der Aufruf von „PUT https://<nsx-manager>/api/v1/configs/management“ mit einem Anforderungstext, in dem „publish_fqdns“ auf „true“ festgelegt ist, kann fehlschlagen, wenn die NSX-T Manager-Appliance mit einem vollqualifizierten Domänennamen (FQDN) statt nur mit einem Hostnamen konfiguriert ist.
„PUT https://<nsx-manager>/api/v1/configs/management“ kann nicht aufgerufen werden, wenn ein FQDN konfiguriert ist.
- **Behobenes Problem 2279249** – Eine Instant Clone-VM verliert während vMotion kurzzeitig den AV-Schutz.
Von einem Host zu einem anderen migrierte Instant Clone-VM. Unmittelbar nach der Migration bleibt eine eicar-Datei auf der VM zurück. Kurzzeitiger Verlust des AV-Schutzes.
- **Behobenes Problem 2292116** – IPFIX L2-Funktion „Angewendet auf“ mit CIDR-basierter Gruppe von IP-Adressen, die nicht auf der Benutzeroberfläche aufgeführt werden, wenn die Gruppe über die Seite „IPFIX L2“ erstellt wird.
Wenn Sie versuchen, über das Dialogfeld „Angewendet auf“ eine Gruppe von IP-Adressen zu erstellen, und im Dialogfeld „Mitglieder festlegen“ eine falsche IP-Adresse oder CIDR eingeben, werden diese Mitglieder nicht unter den Gruppen aufgeführt. Sie müssen diese Gruppe erneut bearbeiten, um gültige IP-Adressen einzugeben.
- **Behobenes Problem 2268406** – Im Dialogfeld „Tag-Anker“ werden nicht alle Tags angezeigt, wenn die maximale Anzahl der Tags hinzugefügt wird.
Im Dialogfeld „Tag-Anker“ werden nicht alle Tags angezeigt, wenn die maximale Anzahl der Tags hinzugefügt wird, und es ist weder eine Größenanpassung noch ein Bildlauf möglich. Der Benutzer kann auf der Seite „Übersicht“ jedoch weiterhin alle Tags anzeigen. Es gehen keine Daten verloren.
- **Behobenes Problem 2282798** – Die Hostregistrierung schlägt möglicherweise fehl, wenn zu viele Anforderungen/Hosts gleichzeitig versuchen, sich bei NSX Manager zu registrieren.
Dieses Problem versetzt den Fabric-Knoten in den Fehlerzustand. Der API-Aufruf des Fabric-Knotenstatus zeigt an, dass der Client noch nicht auf Taktsignale geantwortet hat. Außerdem ist die Datei /etc/vmware/nsx-mpa/mpaconfig.json auf dem Host leer.
- **Behobenes Problem 2383867** – Die Protokollpaketerfassung schlägt für einen der Management Plane-Knoten fehl.
Beim Protokollfassungprozess tritt ein Fehler auf, wenn das Support-Paket auf den Remoteserver kopiert wird.

- **Behobenes Problem 2332397 – Die API erlaubt das Erstellen von DFW-Richtlinien in einer nicht vorhandenen Domäne.**
Nach dem Erstellen einer solchen Richtlinie in einer nicht vorhandenen Domäne reagiert die Schnittstelle nicht mehr, wenn der Benutzer eine DFW-Sicherheitsregisterkarte öffnet. Das entsprechende Protokoll ist /var/log/policy/policy.log.
- **Behobenes Problem 2410818 – Nach dem Upgrade auf 2.4.2 funktionieren virtuelle Server, die in NSX-T 2.3.x erstellt wurden, nach dem Erstellen weiterer virtueller Server möglicherweise nicht mehr.**
Bei einigen Bereitstellungen funktionieren virtuelle Server, die in Version 2.3.x erstellt wurden, nach dem Upgrade auf Version 2.4.2 und nach dem Erstellen weiterer virtueller Server nicht mehr.
- **Behobenes Problem 2310650 – Für die Schnittstelle wird die Fehlermeldung „Zeitüberschreitung bei Anforderung“ angezeigt.**
Mehrere Seiten auf der Schnittstelle zeigen die folgende Meldung an: „Zeitüberschreitung bei Anforderung. Dies kann der Fall sein, wenn das System ausgelastet ist oder nur wenige Ressourcen frei sind.“
- **Behobenes Problem 2314537 – Der Verbindungsstatus ist nach der Aktualisierung von vCenter-Zertifikat und Fingerabdruck nicht verfügbar.**
Neue Updates von vCenter werden nicht mit NSX synchronisiert und alle bedarfsgesteuerten Abfragen zum Abrufen von Daten aus vCenter schlagen fehl. Benutzer können keine neuen Edge/Service-VMs bereitstellen. Benutzer können keine neuen Cluster oder Hosts vorbereiten, die in vCenter hinzugefügt wurden. Speicherorte des Protokolls: /var/log/cm-inventory/cm-inventory.log und /var/log/proton/nsxapi.log auf dem NSX Manager-Knoten.
- **Behobenes Problem 2316943 – Arbeitslast ist während vMotion kurzzeitig ungeschützt.**
VMware Tools benötigt einige Sekunden, um nach vMotion den korrekten Computernamen für die VM zu melden. Infolgedessen sind VMs, die unter Verwendung des Computernamens zu NSGroups hinzugefügt wurden, nach vMotion einige Sekunden lang ungeschützt.
- **Behobenes Problem 2318525 – Problem mit dem nächsten IPv6-Hop, weil die IP-Adresse des eBGP-Peers in die eigene IP geändert wird.**
Bei eBGP-IP4-Sitzungen wird für angekündigte IPv4-Routen, die ihren eBGP-Peer als nächsten Hop besitzen, der nächste Hop der Route auf der Absenderseite NICHT in die eigene IP-Adresse geändert. Dies funktioniert für IPv4, für IPv6-Sitzungen wird aber der nächste Hop der Route auf der Absenderseite in die eigene IP-Adresse geändert. Dieses Verhalten kann zu Routenschleifen führen.
- **Behobenes Problem 2320147: VTEP fehlt auf dem betroffenen Host.**
Wenn ein LogSwitchStateMsg in derselben Transaktion entfernt und hinzugefügt wird und dieser Vorgang von der zentralen Control Plane verarbeitet wird, bevor die Management Plane den logischen Switch gesendet hat, wird der Status des logischen Switches nicht aktualisiert. Dies führt dazu, dass der Datenverkehr nicht in den oder aus dem fehlenden VTEP fließen kann.
- **Behobenes Problem 2320855 – Neues VM-Sicherheits-Tag wird nicht erstellt, wenn der Benutzer nicht auf die Schaltfläche „Hinzufügen/Prüfen“ klickt.**
Schnittstellenproblem. Wenn ein Benutzer ein neues Sicherheits-Tag zu einem Richtlinienobjekt oder einer Bestandsliste hinzufügt und auf Speichern klickt, ohne zuerst neben dem Feld mit dem Tag-Geltungsbereich-Paar auf die Schaltfläche Hinzufügen/Prüfen zu klicken, wird das neue Tag-Paar nicht erstellt.
- **Behobenes Problem 2331683 – Das Add-Load-Balancer-Formular in der erweiterten Benutzeroberfläche zeigt keine aktualisierte Kapazität der Version 2.4 an.**
Wenn das Add-Load-Balancer-Formular geöffnet wird, wird die in der erweiterten Benutzeroberfläche angezeigte Formfaktorkapazität nicht für Version 2.4 aktualisiert. Die angezeigte Kapazität entspricht der vorherigen Version.
- **Behobenes Problem 2295819: L2-Bridge verbleibt im Status „gestoppt“, obwohl die Edge-VM**

und PNIC aktiv sind.

L2-Bridge verbleibt im Status „Gestoppt“, obwohl die Edge-VM und die PNIC für den L2-Bridge-Port aktiv sind. Dies liegt daran, dass das Edge-LCP den PNIC-Status in seinem lokalen Cache nicht aktualisieren kann und daher annimmt, dass die PNIC ausgefallen ist.

- **Behobenes Problem 2243415 – Der Kunde kann den EPP-Dienst mithilfe des logischen Switches (als Verwaltungsnetzwerk) nicht bereitstellen.**
Auf dem EPP-Bereitstellungsbildschirm kann der Benutzer im Steuerelement für die Netzwerkauswahl keinen logischen Switch sehen. Wenn die API direkt mit dem als Verwaltungsnetzwerk erwähnten logischen Switch verwendet wird, wird dem Benutzer der folgende Fehler angezeigt: „Dienstbereitstellung kann nicht auf angegebenes Netzwerk zugreifen.“
- **Behobenes Problem 2364756 – Die Profilrealisierung schlägt aufgrund duplizierter Priorität fehl.**
Bei Skalierungseinrichtungen wird das Profil auf der Management Plane nicht realisiert, wenn Benutzer die vRNI mit NSX IPFIX verknüpft haben. Dies kann durch Umsetzungsfehler auftreten.
- **Behobenes Problem 2392093 – Datenverkehr sinkt aufgrund von RPF-Check.**
Die RPF-Prüfung kann zu einem verworfenen Datenverkehr führen, wenn der Datenverkehr über einen TO-Downlink angeheftet wird und sich die Tier0- und Tier1-Router auf demselben Edge-Knoten befinden.
- **Behobenes Problem 2307551 – NSX-T-Host kann die Verwaltungsnetzwerkonnktivität verlieren, wenn alle pNICs zu N-VDS migriert werden.**
Das Problem entsteht bei der wiederholten Hostmigration, bei der alle pNICs im N-VDS entfernt werden, für den vmk0 konfiguriert ist. Bei der ersten Hostmigration wurden alle pNICs und vmk0 in den N-VDS migriert, danach schlug dies aber fehl. Wenn Sie die Migration erneut durchführen, werden alle pNICs aus dem N-VDS entfernt. Dadurch können Benutzer nicht über das Netzwerk auf den Host zugreifen. Außerdem verlieren alle VMs im Host die Netzwerkkonnktivität, wodurch ihre Dienste nicht erreichbar sind.
- **Behobenes Problem 2369792 – CBM-Prozess stürzt wiederholt aufgrund der Überfrachtung des Arbeitsspeichers durch den CBM-Prozess ab.**
Die Datenbankkomprimierung bei CSM- und CBM-Prozessen auf der Cloud Service Manager-Appliance schlägt fehl. Infolgedessen führt die Überfrachtung des Arbeitsspeichers zu einem wiederholten Absturz des CBM-Prozesses.
- **Behobenes Problem 2361892 – Bei der NSX Edge-Appliance tritt ein Arbeitsspeicherverlust auf, was zu einem Absturz/Neustart des Prozesses führt.**
Über einen längeren Zeitraum kann es bei der NSX Edge-Appliance zu einem Arbeitsspeicherverlust aufgrund wiederholter Regelsuchen kommen, was zu einem Absturz/Neustart des Prozesses führt. Jedes Mal, wenn eine Regelsuche ausgeführt wurde, wurde ein Arbeitsspeicherverlust erkannt. Beim Löschen des Flow-Caches wird die VIF-Schnittstelle nicht entfernt, was zu einem Stau im Arbeitsspeicher führt.
- **Behobenes Problem 2364529 – Arbeitsspeicherverlust beim Load Balancer nach der Neukonfiguration.**
Der NSX Load Balancer kann bei aufeinander folgenden/sich wiederholenden Konfigurationsereignissen Arbeitsspeicher verlieren, was zu einem Core-Speicherabbild des nginx-Prozesses führt.
- **Behobenes Problem 2378876 – PSOD auf ESXi-Hosts mit Fehlern: „Nutzungsfehler in dlmalloc“ und „PF-Ausnahme 14 in World 3916803:VSIP PF Purg-IP“.**
Nach Ausführung des Datenverkehrs über einige Tage stürzt der ESXi ab (PSOD). Vor dem Absturz wurden keine anderen Symptome beobachtet. Das Problem wurde schließlich im ALG-Datenverkehr (FTP, Sunrpc, Oracle, Dcerpc, tftp) identifiziert. Der nicht aufgelöste Inkrementindikator führte zu Race-Bedingungen, wodurch die ALG-Struktur beschädigt wurde.
- **Behobenes Problem 2384922 – BGPD verbraucht 100 % der CPU-Auslastung auf dem Edge-**

Knoten.

Der BGPD-Prozess auf NSX-T EDGE kann 100 % der CPU verbrauchen, wenn mehrere offene Sitzungen mit VTYSH vorhanden sind.

- **Behobenes Problem 2386738 – NAT-Regeln wurden für den Datenverkehr über den VERKNÜPFTEN Port ignoriert.**
NAT-Dienste sind nicht auf dem Porttyp des VERKNÜPFTEN Routers aktiviert, der die logischen Tier-0 und Tier-1 Router verbindet.
- **Behobenes Problem 2363618 – VMware Identity Manager-Benutzer können auf dem NSX Manager Dashboard nicht auf die Richtlinienseiten zugreifen.**
Benutzer mit Rollen, denen Gruppenberechtigungen in VMware Identity Manager zugewiesen sind, können nicht auf Richtlinienseiten im NSX Manager Dashboard zugreifen. Berechtigungen aus Gruppenzuweisungen werden ignoriert.
- **Behobenes Problem 2298274 – Richtliniengruppe kann mit einem ungültigen oder einem teilweisen Domänennamen über die REST-API erstellt/aktualisiert werden.**
Über die Schnittstelle konnten Gruppen mit Identitätsausdrücken erstellt werden, die ungültige Active Directory-Gruppen oder einzelne Gruppenmitglieder für einen einzelnen gültigen Inhalt enthalten. Jedes Mitglied ist jedoch nur gültig, wenn es genau eine dem Domänennamen zugeordnete LDAP-Gruppe hat. Dadurch wurden diese in einer früheren Version von NSX-T erstellten Gruppen im Upgrade-Prozess nicht als Fehler markiert. Dadurch wurden die ungültigen Gruppen in nachfolgenden Versionen beibehalten. Behobene Probleme in 2.5:
- **Behobenes Problem 2317147 – Benutzer können keine effektiven VMs für eine Gruppe sehen, deren Mitgliedschaft auf IP- oder Mac-Adressen basiert.**
Wenn ein Benutzer eine Gruppe nur mit IP- oder Mac-Adressen in der Gruppe erstellt, werden keine VMs aufgelistet, wenn eine effektive Mitgliedschaft für diese Gruppe über die API aufgerufen wird. Es gibt keine funktionalen Auswirkungen. Die Richtlinie erstellt ordnungsgemäß eine NSGroup auf der Management Plane, und die Liste der IP- und Mac-Adressen wird direkt an die zentrale Control Plane gesendet.
- **Behobenes Problem 2327201 – Aktualisierungen von VMs auf KVM-Hypervisoren werden nicht direkt synchronisiert.**
VM-Aktualisierungen auf KVM-Hypervisoren können einige Stunden in Anspruch nehmen, um auf NSX-T synchronisiert zu werden. Dadurch können neue auf KVM-Hypervisoren erstellte VMs nicht zu NSGroups hinzugefügt werden. Außerdem können keine Firewallregeln auf diesen VMs angewendet werden und das Upgrade des KVM-Hypervisors ist nicht möglich, da der VM-Betriebsstatus nicht aktualisiert wird.
- **Behobenes Problem 2329443 – der Steuerungs-Cluster wird aufgrund einer forcesync-Zeitüberschreitung nicht initialisiert.**
Der Steuerungs-Cluster wird aufgrund einer forcesync-Zeitüberschreitung nicht initialisiert, wenn der IPv4-Bereich im Ipset mit 0.0.0.0 beginnt, z. B. 0.0.0.0-1.1.1.20. Dies wird durch ein Problem beim Befehl IPSetFullSyncMessageProvider verursacht, der in einer Endlosschleife blockiert wird. Da die zentrale Control Plane nicht initialisiert wird, können Benutzer keine neuen Arbeitslasten bereitstellen.
- **Behobenes Problem 2337839 – NSX-T-Sicherungs-Widgets zeigen falsche Feldnamen an.**
Speziell die NSX-T-Sicherungs-Widgets zeigen nicht die korrekte Anzahl von Sicherheitsfehlern an. Daher muss der Kunde in der Registerkarte „NSX Manager-Sicherung“ die genaue Anzahl der Sicherheitsfehler anzeigen.
- **Behobenes Problem 2341552 – Edge kann nicht gestartet werden, wenn das System über zu viele unterstützte Netzwerkkarten verfügt.**
Es wird kein Datenpfaddienst oder keine Konnektivität angezeigt, der Datenpfaddienst ist ausgefallen und der Edge-Knoten befindet sich in einem herabgestuften Status. Dies führt zu einem teilweisen oder vollständigen Konnektivitätsverlust, wenn Edge erforderlich ist.

- **Behobenes Problem 2390374 – NSX Manager wird sehr langsam oder reagiert nicht mehr und Protokolle zeigen viele Corfu-Ausnahmen.**
NSX kann ebenfalls nicht gestartet werden. Die Corfu-Ausnahmen deuten darauf hin, dass die Anzahl der Active Directory-Mitglieder zu groß und oberhalb der getesteten Grenzwerte liegt.
- **Behobenes Problem 2371150 – Schicht-7-Firewallregeln können nicht auf Bare Metal Edge-Knoten konfiguriert werden.**
Schicht-7-Firewallregeln auf Bare Metal Edge-Knoten werden in NSX-T 2.5 nicht unterstützt. Es gibt einen internen Befehl zur Aktivierung der Unterstützung. Dieser ist jedoch nur für Proof of Concepts verfügbar.
- **Behobenes Problem 2361238 – Downlink-Router wird nicht mit dem Dienst-Router gekoppelt.**
NAT-Regeln wirken sich nicht auf den Downlink-Router aus, nachdem ein mit dem Downlink-Router gekoppelter Dienst-Router gelöscht und neu erstellt wurde.
- **Behobenes Problem 2363248 – Der Zustand der Dienstinstanz wird im Status inaktiv angegeben, obwohl der API-Aufruf als verbunden angezeigt wird.**
Dieser inkonsistente Bericht kann zu einem Fehlalarm führen.

Ausführliche Informationen zu diesem Problem und der Lösung finden im [Knowledgebase-Artikel 67165 – Der Status der Dienstinstanz wird als „Inaktiv“ angezeigt, wenn in NSX-T keine zu schützenden VMs aktiv sind](#).

- **Behobenes Problem 2359936 – häufiges Rollover des cfgAgent-Protokolls auf dem ESX-Host.**
Durch häufige Protokoll-Rollover können nützlicher Informationen im Protokoll „cfgAgent.log“ für Debugging und Fehlerbehebung auf dem Host verloren gehen.
- **Behobenes Problem 2332938 – Wenn der SYN-Cache im Sicherheitsprofil der Flood Protection aktiviert ist, kann der tatsächliche Grenzwert für halb offene TCP-Verbindungen höher sein als der auf dem NSX Manager konfigurierte Grenzwert.**
NSX-T berechnet automatisch einen optimalen Grenzwert für halb offene TCP-Verbindungen, basierend auf dem konfigurierten Grenzwert. Dieser berechnete Grenzwert kann größer als der konfigurierte Grenzwert sein und basiert auf folgender Formel: Grenzwert = (PwrOf2 * Depth). Dabei steht „PwrOf2“ für eine Potenz von 2, nicht unter 64, und „Depth“ für eine Ganzzahl ≤ 32 .
- **Behobenes Problem 2376336 – Adressfamilie in der Route Redistribution wird von der Richtlinie und Edge nicht unterstützt.**
Die Adressfamilie in der Redistribution funktioniert nicht oder wird nicht in der Anwendung verwendet.
- **Behobenes Problem 2412842 – Grenzwertmetriken protokollieren 40 MB auf ESX zur Unterstützung von Hosts mit Ramdisk.**
Eine ausführliche Beschreibung des Problems finden Sie im [Knowledgebase-Artikel 74574](#).
- **Behobenes Problem 2385070 – IP Discovery und DFW verhalten sich gegensätzlich in Bezug auf das IPv6-Subnetz.**
Bei der IP Discovery wird 2001::1/64 als Host-IP betrachtet, während es bei DFW als IPv6-Subnetz betrachtet wird.
- **Behobenes Problem 2394896 – Host kann nicht von NSX-T Data Center 2.4.x auf 2.5 aktualisiert werden.**
Der Host kann nicht von NSX-T Data Center 2.4.0, 2.4.1 und 2.4.2 auf 2.5 aktualisiert werden. Dies kann auf einen Fehler beim Entladen des KCP-Moduls zurückzuführen sein.

Dieses Problem wird genauer im [Knowledgebase-Artikel 74674](#) beschrieben.
- **Behobenes Problem 2406018 – Ein Ereignis/Alarm wird ausgelöst, wenn der Kennwortablauf innerhalb von 30 Tagen liegt.**
Ein Ereignis/Alarm wird bezüglich des Kennwortablaufs ausgelöst, wenn der Kennwortablauf innerhalb von 30 Tagen liegt und der Kennwortablauf deaktiviert ist.

- **Behobenes Problem 2383328 – Funktionsanforderung zur Bereitstellung des Dienstprogramms, das Metrikdaten in lesbare Form rendert.**
NSX-T Data Center erfasst und speichert Metrikdaten in einem binären Format. Benutzer haben angefordert, dass diese Daten in einem lesbaren Format angezeigt werden können. Dieser Forderung wird mit dieser Anforderung nachgekommen.
- **Behobenes Problem 2248345: Nach der Installation des NSX-T Edge wird die Maschine mit einem leeren schwarzen Bildschirm gestartet.**
NSX-T Edge kann nicht auf einer Maschine des Typs HPE ProLiant DL380 Gen9 installiert werden.
- **Behobenes Problem 2313673 – VM-basierte Edge-Transportknoten: Benutzer können keine Uplinks mit den logischen NSX-T-Switches/-Segmenten verbinden.**
Für VM-basierte Edge-Transportknoten können Benutzer die Edge-Transportknoten-Uplinks nicht mit den logischen NSX-T-Switches/-Segmenten verbinden. Sie können sie nur mit den vCenter-DVPGs verbinden. Auf dem Bildschirm „NSX konfigurieren“ für die Abläufe zum Hinzufügen/Bearbeiten von VM-basierten Edge-Transportknoten wird Benutzern die Option angezeigt, die Uplinks nur vCenter-DVPGs zuzuordnen. Die Option zum Zuordnen der Uplinks zu den logischen NSX-T-Switches/-Segmenten fehlt.
- **Behobenes Problem 2424394: DHCP-Pakete, die von NSX-T DR weitergeleitet werden, können nicht mehr als 10 Hops erreichen.**
Wenn der DHCP-Server mehr als 10 Hops entfernt ist, können die weitergeleiteten DHCP-Pakete den Server nicht erreichen.
- **Behobenes Problem 2399994: Neu verteilte Routen fehlen zeitweise.**
Der Netzwerkdatenverkehr ist möglicherweise beeinträchtigt, da die Route zu T1 eine Zeit lang nicht verfügbar ist.

Bekannte Probleme

Die bekannten Probleme gliedern sich in folgende Gruppen.

- [Allgemeine bekannte Probleme](#)
- [Bekannte Installationsprobleme](#)
- [Bekannte Probleme bei NSX Manager](#)
- [Bekannte Probleme bei NSX Edge](#)
- [Bekannte Probleme bei logischen Netzwerken](#)
- [Bekannte Probleme bei Sicherheitsdiensten](#)
- [Bekannte Probleme beim Load Balancer](#)
- [Bekannte Probleme bei der Lösungsinteroperabilität](#)
- [Bekannte Probleme bei NSX Intelligence](#)
- [Bekannte Probleme bei Betriebs- und Überwachungsdiensten](#)
- [Bekannte Upgradeprobleme](#)
- [Bekannte Probleme mit APIs](#)
- [Bekannte Probleme bei NSX Cloud](#)

Allgemeine bekannte Probleme

- **Problem 2261818 – Von eBGP-Nachbarn erlernte Routen werden an denselben Nachbarn zurückgegeben.**
Durch das Aktivieren von BGP-Debug-Protokollen werden Pakete angezeigt, die erneut empfangen werden, und das Paket wird mit einer Fehlermeldung verworfen. Der BGP-Prozess verbraucht zusätzliche CPU-Ressourcen, um die an Peers gesendeten Aktualisierungsmeldungen zu verworfen. Wenn viele Routen und Peers vorhanden sind, kann dies Auswirkungen auf die Routenkonvergenz haben.

Problemumgehung: Keine.

- **Problem 2390624 – Die Antiaffinitätsregel verhindert die Service-VM von vMotion, wenn sich der Host im Wartungsmodus befindet.**
Wenn eine Service-VM in einem Cluster mit genau zwei Hosts bereitgestellt wird, verhindert das HA-Paar mit Antiaffinitätsregel, dass die VMs während Aufgaben im Wartungsmodus auf den anderen Host übertragen werden. Dadurch kann der Host nicht automatisch in den Wartungsmodus wechseln.

Problemumgehung: Schalten Sie die Service-VM auf dem Host aus, bevor die Aufgabe im Wartungsmodus auf vCenter gestartet wird.

- **Problem 2329273 – Es besteht keine Konnektivität zwischen VLANs, die mit denselben Edge-Knoten auf dasselbe Segment überbrückt werden.**
Das zweimalige Bridging eines Segments auf demselben Edge-Knoten wird nicht unterstützt. Es können jedoch zwei VLANs auf zwei unterschiedlichen Edge-Knoten auf dasselbe Segment überbrückt werden.

Problemumgehung: Keine

- **Problem 2239365 – „Nicht autorisiert“-Fehler wird ausgelöst**
Möglicherweise kommt es zu diesem Fehler, weil der Benutzer versucht, mehrere Authentifizierungssitzungen im selben Browsertyp zu öffnen. Dies führt dazu, dass die Anmeldung mit dem oben angegebenen Fehler fehlschlägt und die Authentifizierung nicht möglich ist.
Speicherort des Protokolls: `/var/log/proxy/reverse-proxy.log/var/log/syslog`

Problemumgehung: Schließen Sie alle offenen Authentifizierungsfenster/-registerkarten und versuchen Sie die Authentifizierung erneut.

- **Problem 2252487 – Der Transportknotenstatus wird für einen BM-Edge-Transportknoten nicht gespeichert, wenn mehrere Transportknoten gleichzeitig hinzugefügt werden.**
Der Transportknotenstatus wird auf der MP-Benutzeroberfläche nicht korrekt angezeigt.

Problemumgehung:

1. Starten Sie den Proton neu, dann werden alle Transportknotenstatus korrekt aktualisiert.
2. Verwenden Sie alternativ die API „`https://<nsx-manager>/api/v1/transport-nodes/<node-id>/status?source=realtime`“, um den Transportknotenstatus abzufragen.

- **Problem 2275285 – Ein Knoten stellt eine zweite Anforderung, um demselben Cluster beizutreten, bevor die erste Anforderung abgeschlossen und der Cluster stabilisiert wurde.**
Der Cluster funktioniert möglicherweise nicht ordnungsgemäß und die CLI-Befehle zum Abrufen des Clusterstatus und zum Abrufen der Clusterkonfiguration geben möglicherweise einen Fehler zurück.

Problemumgehung: Geben Sie nach der ersten Beitrittsanforderung für einen Zeitraum von 10 Minuten keinen weiteren Beitrittsbefehl für den Beitritt zum selben Cluster aus.

- **Problem 2275388 – Routen über eine Loopback-Schnittstelle/verbundene Schnittstelle werden möglicherweise neu verteilt, bevor Filter zum Verweigern der Routen hinzugefügt werden.**
Unnötige Updates von Routen können für einen Zeitraum zwischen wenigen Sekunden und einer Minute zur Umleitung von Datenverkehr führen.

Problemumgehung: Keine.

- **Problem 2275708 – Ein Zertifikat mit seinem privaten Schlüssel kann nicht importiert werden, wenn der private Schlüssel eine Passphrase aufweist.**
Die zurückgegebene Meldung lautet „Ungültige PEM-Daten für Zertifikat empfangen. (Fehlercode: 2002)“. Das Importieren eines neuen Zertifikats mit privatem Schlüssel ist nicht möglich.

Problemumgehung:

1. Erstellen Sie ein Zertifikat mit privatem Schlüssel. Geben Sie bei entsprechender

- Aufforderung keine neue Passphrase ein und drücken Sie stattdessen die Eingabetaste.
2. Wählen Sie „Zertifikat importieren“ und wählen Sie anschließend die Zertifikatsdatei und die Privatschlüsseldatei aus.

Überprüfen Sie den Vorgang, indem Sie die Schlüsseldatei öffnen. Wenn beim Generieren des Schlüssels eine Passphrase eingegeben wurde, steht in der zweiten Zeile der Datei etwas wie „Proc-Type: 4,ENCRYPTED“.

Diese Zeile fehlt, wenn die Schlüsseldatei ohne Passphrase generiert wurde.

- **Problem 1957072 – Das Uplink-Profil für den Bridge-Knoten muss für mehrere Uplinks immer eine LAG verwenden.**

Wenn Sie mehrere Uplinks verwenden, die keine Linkzusammenfassungsvergruppe (Link Aggregation Group, LAG) bilden, findet für den Datenverkehr kein Lastausgleich statt, sodass der Datenverkehr möglicherweise nicht richtig funktioniert.

Problemumgehung: Verwenden Sie für mehrere Uplinks auf Bridge-Knoten eine LAG.

- **Problem 1970750 – N-VDS-Profil des Transportknotens, das LACP mit schnellen Timern verwendet, wird nicht auf vSphere ESXi-Hosts angewendet.**

Wenn ein LACP-Uplink-Profil mit schnellen Raten auf einen vSphere ESXi-Transportknoten auf NSX Manager angewendet wird, zeigt der NSX Manager an, dass das Profil erfolgreich angewendet wird, aber der vSphere ESXi-Host verwendet den standardmäßigen langsamen LACP-Timer. Auf dem vSphere Hypervisor können Sie den Effekt des lacp-timeout-Werts (SLOW/FAST) nicht sehen, wenn das Profil des verwalteten LACP-NSX-Distributed Switch (N-VDS) über den NSX Manager auf dem Transportknoten verwendet wird.

Problemumgehung: Keine.

- **Problem 2320529: Nach dem Hinzufügen von Drittanbieter-VMs für neu hinzugefügte Datenspeicher wird die Fehlermeldung „Dienstbereitstellung kann nicht auf Speicher zugreifen“ angezeigt.**

Nach dem Hinzufügen von Drittanbieter-VMs für neu hinzugefügte Datenspeicher wird die Fehlermeldung „Dienstbereitstellung kann nicht auf Speicher zugreifen“ angezeigt, obwohl alle Hosts im Cluster auf den Speicher zugreifen können. Dieser Fehlerstatus bleibt bis zu dreißig Minuten lang bestehen.

Problemumgehung: Versuchen Sie es nach 30 Minuten erneut. Alternativ können Sie den folgenden API-Aufruf ausführen, um den Cache-Eintrag des Datenspeichers zu aktualisieren:

`https://<nsx-manager>/api/v1/fabric/compute-collections/<CC Ext ID>/storage-resources?uniform_cluster_access=true&source=realtime`

Dabei steht <nsx-manager> für die IP-Adresse des NSX Managers, bei dem die Dienstbereitstellungs-API fehlgeschlagen ist, und CC Ext ID für den Bezeichner in NSX für den Cluster, in dem die Bereitstellung versucht wird.

- **Problem 2328126: Bare Metal-Problem: Eine Bond-Schnittstelle im Linux-Betriebssystem führt bei Verwendung im NSX-Uplink-Profil zu einem Fehler.**

Wenn Sie im Linux-Betriebssystem eine Bond-Schnittstelle erstellen und diese Schnittstelle dann im NSX-Uplink-Profil verwenden, wird die folgende Fehlermeldung angezeigt: „Erstellung des Transportknotens schlägt möglicherweise fehl.“ Dieses Problem tritt auf, weil VMware kein Linux-Bonding unterstützt. VMware unterstützt jedoch mit Open vSwitch (OVS) erstellte Bond-Schnittstellen für Bare-Metal-Server-Transportknoten.

Problemumgehung: Falls dieses Problem auftritt, finden Sie weitere Informationen im Knowledgebase-Artikel 67835: [Bare Metal Server supports OVS bonding for Transport Node configuration in NSX-T](#).

- **Problem 2370555 – Benutzer können bestimmte Objekte in der Schnittstelle „Erweitert“ löschen, aber die Löschungen werden nicht in der Schnittstelle „Vereinfacht“ widerspiegelt.**

Speziell die Gruppen, die zu einer Ausschlussliste für verteilte Firewalls hinzugefügt wurden, können über die Schnittstelle „Erweitert“ in den Einstellungen der „Ausschlussliste für verteilte Firewalls“ gelöscht werden. Dies führt zu einem inkonsistenten Verhalten in der Schnittstelle.

Problemumgehung: Wenden Sie das folgende Verfahren an, um dieses Problem zu beheben:

- Fügen Sie ein Objekt zu einer Ausschlussliste in der Schnittstelle „Vereinfacht“ hinzu.
- Stellen Sie sicher, dass es in der Schnittstelle „Erweitert“ in der Ausschlussliste für „Verteilte Firewalls“ angezeigt wird.
- Löschen Sie das Objekt in der Schnittstelle „Erweitert“ aus der Ausschlussliste für „Verteilte Firewalls“.
- Kehren Sie zur Schnittstelle „Vereinfacht“ zurück, fügen Sie ein zweites Objekt zur Ausschlussliste hinzu und wenden Sie es an.
- Stellen Sie sicher, dass das neue Objekt in der Schnittstelle „Erweitert“ angezeigt wird.
- **Problem 2377217 – Nach einem Neustart des KVM-Hosts funktionieren die Datenverkehrsflüsse zwischen VMs möglicherweise nicht erwartungsgemäß.**

Der Neustart des KVM-Hosts kann zu Problemen bei der Erreichbarkeit zwischen VMs führen.

Problemumgehung: Starten Sie nach dem Neustart des Hosts den NSX-Agent-Dienst mit dem folgenden Befehl neu:

```
# systemctl restart nsx-agent.service
```

- **Problem 2371251 – die Dashboard-Schnittstelle blinkt, wenn Sie zur Seite „Sichern und Wiederherstellen“ navigieren.**

Dieses Problem trat nur im Firefox-Browser und nur bei einigen Bereitstellungen auf.

Problemumgehung: Aktualisieren Sie die Seite manuell oder verwenden Sie einen anderen unterstützten Browser.

- **Problem 2408453 – VMware Tools 10.3.5 stürzt ab, wenn der Treiber für die NSX Guest Introspection installiert ist.**

VMware Tools 10.3.5 stürzt unregelmäßig auf der Windows-VM ab. Am häufigsten fällt dies auf, wenn die Remote-Sitzung getrennt wird oder wenn die Gast-VM heruntergefahren wird.

Problemumgehung: Weitere Details finden Sie im [Knowledgebase-Artikel 70543](#).

- **Problem 2267964 – Wenn vCenter entfernt wird, wird der Benutzer nicht vor dem Verlust der Dienste gewarnt, die auf vCenter durchgeführt werden.**

Wenn ein Benutzer den Computer Manager (vCenter) entfernt, in dem Dienste wie Guest Introspection bereitgestellt werden, wird der Benutzer nicht über den potenziellen Verlust dieser Dienste benachrichtigt.

Problemumgehung: Um dieses Problem zu vermeiden, muss der Benutzer die richtige Vorgehensweise für das Hinzufügen eines neuen vCenter als Computer Manager befolgen.

- **Problem 2444170: NSX-CLI-Befehle können den Datenpfad nicht deinstallieren**
Mit dem Befehl *del nsx* werden die NSX-T-Konfiguration und die Module auf dem Host nicht deinstalliert. Dies führt dazu, dass die Installation oder das Upgrade von NSX-T fehlschlägt.

Problemumgehung: Keine.

- **Problem 2467479 – Sobald für die Firewall für eine SNAT-Regel „Umgehung“ eingestellt ist, kann sie nicht blockiert werden, wenn von „Umgehung“ zu „Ohne“ gewechselt wird.**
Sobald für die Firewall für eine SNAT-Regel „Umgehung“ eingestellt ist, kann sie nicht blockiert werden, wenn von „Umgehung“ zu „Ohne“ gewechselt wird.

Problemumgehung: Löschen und erstellen Sie die SNAT-Regel neu.

- **Problem 2586606: Der Load Balancer funktioniert nicht, wenn die Persistenz der Quell-IP auf einer großen Anzahl virtueller Server konfiguriert ist.**

Wenn die Persistenz der Quell-IP auf einer großen Anzahl virtueller Server auf einem Load Balancer konfiguriert ist, verbraucht sie eine erhebliche Menge an Arbeitsspeicher, was dazu führen kann, dass der Arbeitsspeicher von NSX Edge knapp wird. Dieses Problem kann jedoch mit dem Hinzufügen mehrerer virtueller Server erneut auftreten.

Problemumgehung: Deaktivieren Sie die Persistenz der Quell-IP oder verschieben Sie mehr VIPs mit der Persistenz der Quell-IP in verschiedene LB-Dienste.

- **Problem 2730634:** Nach dem Uniscale-Upgrade zeigt die Netzwerkkomponentenseite den Fehler „Index nicht synchronisiert“ an.

Nach dem Uniscale-Upgrade zeigt die Netzwerkkomponentenseite den Fehler „Index nicht synchronisiert“ an.

Problemumgehung: Melden Sie sich mit Admin-Anmeldedaten bei NSX Manager an und führen Sie den Befehl „start search resync policy“ aus. Das Laden der Netzwerkkomponenten dauert einige Minuten.

Bekannte Installationsprobleme

- **Problem 1957059** – Das Aufheben der Hostvorbereitung schlägt fehl, wenn dabei dem Cluster ein Host mit vorhandenen VIBs hinzugefügt wird.

Wenn die VIBs vor dem Hinzufügen der Hosts zum Cluster nicht vollständig entfernt wurden, kann die Hostvorbereitung nicht aufgehoben werden.

Problemumgehung: Stellen Sie sicher, dass die VIBs auf den Hosts vollständig entfernt werden und starten Sie den Host neu.

Bekannte Probleme bei NSX Manager

- **Problem 2378970** – Die Einstellung „Aktivieren/Deaktivieren“ auf Cluster-Ebene für die verteilte Firewall wird fälschlicherweise als „Deaktiviert“ angezeigt.
Die Einstellung „Aktivieren/Deaktivieren“ auf Cluster-Ebene für IDFW auf der vereinfachten Benutzeroberfläche wird möglicherweise als „Deaktiviert“ angezeigt, obwohl Sie in der Management Plane als „Aktiviert“ angezeigt wird. Nach dem Upgrade von 2.4.x auf 2.5 besteht diese Ungenauigkeit, bis sie explizit geändert wurde.

Problemumgehung: Ändern Sie die Einstellung „Aktivieren/Deaktivieren“ für IDFW manuell auf der vereinfachten Benutzeroberfläche, damit sie mit der Angabe auf der Management Plane identisch ist.

Bekannte Probleme bei NSX Edge

- **Problem 2283559** – Die MP-APIs „https://<nsx-manager>/api/v1/routing-table“ und „https://<nsx-manager>/api/v1/forwarding-table“ geben einen Fehler zurück, wenn der Edge mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB aufweist.
Wenn der Edge mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB aufweist, nimmt die Anforderung von MP an den Edge mehr als 10 Sekunden in Anspruch, und dies führt zu einer Zeitüberschreitung. Dies ist eine schreibgeschützte API und wirkt sich nur dann aus, wenn die mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB mithilfe der API/UI heruntergeladen werden müssen.

Problemumgehung: Es gibt zwei Optionen zum Abrufen von RIB/FIB.

- Diese APIs unterstützen Filteroptionen, die auf Netzwerkpräfixen oder Routentypen beruhen. Verwenden Sie diese Optionen zum Herunterladen der gewünschten Routen.
- Wenn die gesamte RIB-/FIB-Tabelle erforderlich ist, ist eine CLI-Unterstützung erforderlich, und in diesem Fall tritt keine Zeitüberschreitung auf.
- **Problem 2204932:** Das Konfigurieren von BGP-Peering kann die HA-Failover-Wiederherstellung verzögern.

Wenn Dynamic-BGP-Peering auf Routern konfiguriert ist, die eine Peer-Beziehung mit den TO-Edges besitzen, und auf den Edges (Aktiv/Standby-Modus) ein Failover-Ereignis auftritt, kann die BGP-Nachbarschaft bis zu 120 Sekunden dauern.

Problemumgehung: Konfigurieren Sie spezifische BGP-Peers, um die Verzögerung zu vermeiden.

- **Problem 2285650: BGP-Routentabellen werden mit unerwünschten Routen gefüllt.**

Wenn in der BGP-Konfiguration die Option „allowas-in“ aktiviert ist, werden von Edge-Knoten angekündigte Routen zurückerhalten und in der BGP-Routentabelle installiert. Dies führt zu übermäßigem Arbeitsspeicherverbrauch und übermäßigen Routing-Berechnungen. Wenn für die überschüssigen Routen eine höhere lokale Einstellung konfiguriert ist, kann diese auf einigen Routern, die mit redundanten Routen gefüllt werden, zu einer Weiterleitungsschleife führen.

Beispiel: Route X stammt von Router D und wird den Routern A und B angekündigt. Router C, auf dem „allowas-in“ aktiviert ist, wird mit B verbunden, sodass er Route X erlernt und in seiner Routentabelle installiert. Infolgedessen gibt es jetzt für die Ankündigung von Route X an Router C zwei Pfade, was zu dem Problem führt.

Problemumgehung: Sie können Weiterleitungsschleifen verhindern, indem Sie den problematischen Router (oder seinen Peer) so konfigurieren, dass die Rückmeldung von Routen an ihn blockiert wird.

- **Problem 2343954 – In der Schnittstelle für den Edge-L2-Bridge-Endpunkt können nicht unterstützte VLAN-Bereiche konfiguriert werden.**

In der Schnittstelle für die Konfiguration der Edge-L2-Bridge und des Edge-L2-Points können Sie einen VLAN-Bereich und mehrere VLAN-Bereiche konfigurieren, obwohl diese nicht unterstützt werden.

Problemumgehung: Konfigurieren Sie diese VLAN-Bereiche nicht für die Konfiguration der Edge-L2-Bridge und des Edge-L2-Points.

Bekannte Probleme bei logischen Netzwerken

- **Problem 2389993: Die nach der Neuverteilungsregel entfernte Route Map wird über die Richtlinienseite oder die API geändert.**

Eine Route Map, die einer Neuverteilungsregel über die Schnittstelle oder API der Management Plane hinzugefügt wird, kann entfernt werden, wenn die gleiche Neuverteilungsregel anschließend über die Schnittstelle oder API der Richtlinienseite geändert wird. Dies ist darauf zurückzuführen, dass die Schnittstelle der Richtlinienseite oder die API das Hinzufügen von Routenzuordnungen nicht unterstützt. Dadurch können dem BGP-Peer ungewollte Präfixe angekündigt werden.

Problemumgehung: Sie können die Route Map wiederherstellen, indem Sie die Schnittstelle oder API der Management Plane zurückgeben, um sie erneut zur gleichen Regel hinzuzufügen. Wenn Sie eine Route Map in eine Neuverteilungsregel aufnehmen möchten, sollten Sie immer die Schnittstelle oder API der Management Plane zur Erstellung oder Änderung verwenden.

- **Problem 2275412 – Die Portverbindung funktioniert nicht über mehrere Transportzonen hinweg.**

Die Portverbindung kann nicht nur in einer einzelnen Transportzone verwendet werden.

Problemumgehung: Keine.

- **Problem 2327904: Nach Verwendung einer vordefinierten Linux-Bond-Schnittstelle als Uplink ist der Datenverkehr instabil oder schlägt fehl.**

NSX-T unterstützt keine vordefinierten Linux-Bond-Schnittstellen als Uplink.

Problemumgehung: Verwenden Sie für den Uplink die native OVS-Bond-Konfiguration aus dem Uplink-Profil.

- **Problem 2304571: Ein kritischer Fehler (PSOD) kann auftreten, wenn L3-Datenverkehr mit VDR**

ausgeführt wird.

Ein ausstehender arp(ND)-Eintrag ist in einigen Fällen nicht ordnungsgemäß geschützt, was zu einem kritischen Fehler (PSOD) führen kann.

Problemumgehung: Keine.

- **Problem 2388158 – Benutzer können die Einstellungen des Transitsubnetzes in der Konfiguration des logischen Tier-O-Routers nicht bearbeiten.**

Nach der Erstellung des logischen Tier-O-Routers kann die Konfiguration des Transitsubnetzes nicht in der NSX Manager-Schnittstelle geändert werden.

Problemumgehung: Keine. Am besten löschen Sie den logischen Router und erstellen ihn mit der gewünschten Transitsubnetzkonfiguration neu.

Bekannte Probleme bei Sicherheitsdiensten

- **Problem 2294410: Einige Anwendungs-IDs werden von der L7-Firewall erkannt.**
Folgende L7-Anwendungs-IDs werden basierend auf dem Port und nicht auf der Anwendung erkannt: SAP, SUNRPC und SVN. Die folgenden L7-Anwendungs-IDs werden nicht unterstützt: AD_BKUP, SKIP und AD_NSP.

Problemumgehung: Keine. Dies wirkt sich nicht auf Kunden aus.

- **Problem 2395334 – (Windows)-Pakete wurden fälschlicherweise aufgrund eines Conntrack-Eintrags für Stateless Firewall-Regeln verworfen.**
Stateless Firewall-Regeln werden auf Windows-VMs nicht gut unterstützt.

Problemumgehung: Fügen Sie stattdessen eine statusbehaftete Firewallregel hinzu.

- **Problem 2366599 – Regeln werden für VMs mit IPv6-Adressen nicht erzwungen.**
Wenn eine VM eine IPv6-Adresse verwendet, aber das IPv6-Snooping für diese VIF nicht über das IP Discovery-Profil aktiviert wurde, wird die IPv6-Adresse in der Regel für diese VM im Datenpfad nicht aufgefüllt. Dies führt dazu, dass diese Regel nie erzwungen wird.

Problemumgehung: Stellen Sie sicher, dass die IPv6-Option im Profil der IP Discovery entweder auf dem VIF oder dem logischen Switch aktiviert ist, wenn IPv6-Adressen verwendet werden.

- **Problem 2296430 – Die NSX-T Manager-API stellt bei der Zertifikatgenerierung keine alternativen Antragstellernamen (SANs) bereit.**
Die NSX-T Manager-API stellt keine alternativen Antragstellernamen für das Ausstellen von Zertifikaten bereit, insbesondere während der CSR-Generierung.

Problemumgehung: Erstellen Sie den CSR mit einem externen Tool, das die Erweiterungen unterstützt. Nachdem das signierte Zertifikat von der Zertifizierungsstelle empfangen wurde, importieren Sie es mit dem Schlüssel vom CSR in NSX-T Manager.

- **Problem 2379632 – Beim Treffen der Schicht-7-Regel in der klassifizierten Phase werden mehrere Pakete protokolliert.**
Mehrere (2-3) Pakete werden beim Treffen der Schicht-7-Regel in der klassifizierten Phase protokolliert (dfwpktlogs).

Problemumgehung: Keine.

- **Problem 2368948 – Verteilte Firewallregeln: Der realisierte Status für einzelne Abschnitte ist möglicherweise nicht aktuell.**
Durch das Aktualisieren der DFW-Regelansicht wird der realisierte Status einzelner Abschnitte in der Ansicht nicht aktualisiert. Dies führt dazu, dass die Informationen möglicherweise nicht aktuell sind.

Problemumgehung: Dies betrifft nur die manuelle Aktualisierung. Der Abruf des realisierten Status erfolgt periodisch und liefert genaue Aktualisierungen. Benutzer können für eine genaue Statusangabe auch einzelne Abschnitte aktualisieren.

- **Problem 2380833 – die Veröffentlichung des Richtlinienentwurfs mit 8.000 oder mehr Regeln erfordert viel Zeit.**

Die Veröffentlichung eines Richtlinienentwurfs mit 8.000 oder mehr Regeln kann sehr viel Zeit in Anspruch nehmen. Die Veröffentlichung eines Richtlinienentwurfs mit 8.000 Regeln kann beispielsweise 25 Minuten benötigen.

Problemumgehung: Keine.

- **Problem 2424818 – Schicht-2- und verteilte Firewall-Status nicht auf der NSX Manager-Schnittstelle aktualisiert.**

Die vom logischen Exporter auf Arbeitslast-VMs erzeugten Statusinformationen werden möglicherweise nicht an die Management Plane weitergeleitet. Infolgedessen werden die für diese Komponenten angezeigten Status nicht ordnungsgemäß aktualisiert.

Problemumgehung: Keine. Auf den entsprechenden VMs kann über CLI auf die korrekten Statusinformationen zugegriffen werden.

Bekannte Probleme beim Load Balancer

- **Problem 2290899 – IPSec-VPN funktioniert nicht, und die Realisierung der Control Plane für IPSec schlägt fehl.**

IPSec-VPN (oder L2VPN) wird nicht aktiviert, wenn zusammen mit dem IPSec-Dienst auf Tier-0 mehr als 62 LbServers auf demselben Edge-Knoten aktiviert sind.

Problemumgehung: Verringern Sie die Anzahl an LbServers auf weniger als 62.

- **Problem 2362688: Wenn einige Pool-Mitglieder in einem Load Balancer-Dienst INAKTIV sind, zeigt die Benutzeroberfläche den konsolidierten Status als AKTIV an.**

Wenn ein Pool-Mitglied ausgefallen ist, gibt es keine Hinweise auf der Benutzeroberfläche der Richtlinie, bei der der Pool-Status grün und aktiv ist.

Problemumgehung: Keine.

Bekannte Probleme bei der Lösungsinteroperabilität

- **Problem 2289150 – PCM-Aufrufe an AWS beginnen fehlschlagen.**

Wenn Sie die PCG-Rolle für ein AWS-Konto in CSM von *old-pcg-role* in *new-pcg-role* ändern, aktualisiert CSM die Rolle für die PCG-Instanz auf AWS auf *new-pcg-role*. Der PCM weiß jedoch nicht, dass die PCG-Rolle aktualisiert wurde, und verwendet daher weiterhin die alten AWS-Clients, die er unter Verwendung der Rolle *old-pcg-role* erstellt hat. Dies führt dazu, dass die Prüfung der AWS-Cloud-Bestandsliste des PCM und andere AWS-Cloud-Aufrufe fehlschlagen.

Problemumgehung: Wenn dieses Problem auftritt, ändern/löschen Sie nach dem Wechsel zu der neuen Rolle die alte PCG-Rolle für mindestens 6,5 Stunden nicht. Beim Neustarten des PCG werden alle AWS-Clients mit den Anmeldedaten der neuen Rolle neu gestartet.

- **Problem 2401715 – Beim Aktualisieren des Compute Manager wird der Fehler angezeigt, dass der Fingerabdruck ungültig ist, auch wenn ein korrekter Fingerabdruck angegeben ist.**

Das Problem tritt auf, wenn ein vCenter v 6.7 U3 als Compute Manager in NSX-T Manager hinzugefügt wird. vSphere 6.7 unterstützt Änderungen der PNID, wo der FQDN oder die IP-Adresse geändert werden können. NSX-T 2.5 unterstützt diese Funktion nicht, daher ergibt sich das Problem mit dem Fingerabdruck.

Problemumgehung: Löschen Sie das zuvor hinzugefügte vCenter und fügen Sie den VC mit dem neu geänderten FQDN hinzu. Das Hinzufügen der Registrierung schlägt möglicherweise fehl, da die vorherige Erweiterung bereits auf vCenter vorhanden ist. Beheben Sie die Registrierungsfehler, damit die Registrierung erfolgreich durchgeführt werden kann.

Bekannte Probleme bei NSX Intelligence

- **Problem 2410806 – Das Veröffentlichen der generierten Empfehlung schlägt fehl und die Ausnahme meldet eine Gesamtbeschränkung von 500.**

Wenn die Gesamtzahl der Mitglieder (IP-Adressen oder VMs) in einer empfohlenen Gruppe 500 überschreitet, schlägt die Veröffentlichung der generierten Empfehlung in eine Richtlinienkonfiguration fehl und die Ausnahmemeldung lautet z. B. „Die Summe der IPAdressExpressions, MACAddressExpressions, Pfade in einer PathExpression und externe IDs in ExternalIDExpression darf 500 nicht überschreiten.“

Problemumgehung: Wenn mehr als 500 Clients eine Verbindung mit der Anwendungs-VM oder dem Load Balancer herstellen, können Sie eine Regel für die Mikrosegmentierung des Zugangs zum Anwendungs-Load Balancer erstellen und dann die Anwendungs-VM auswählen, um mit der Empfehlungsermittlung zu beginnen. Alternativ können Sie eine Gruppe mit mehr als 500 Mitgliedern in mehrere, kleinere Gruppen unterteilen.

- **Problem 2362865 – Filtern nach „Regelname“ ist für Standardregel nicht verfügbar.**
Das Problem tritt auf der Seite **Planen und Fehler beheben > Ermitteln und Maßnahmen ergreifen** auf und betrifft nur Regeln, die über die Konnektivitätsstrategie erstellt wurden. Dieses Problem tritt aufgrund einer fehlenden auf der angegebenen Konnektivitätsstrategie basierenden Standardrichtlinie auf. Eine Standardregel kann auf der Management Plane erstellt werden, aber ohne eine entsprechende Standardrichtlinie kann der Benutzer nicht basierend auf dieser Standardregel filtern. (Der Filter für die Visualisierung der Flows verwendet den Regelnamen, um nach Flows zu filtern, die dieser Regel entsprechen.)

Problemumgehung: Wenden Sie nicht den Filter nach Regelnamen an. Überprüfen Sie stattdessen das Flag „Ungeschützt“. Diese Konfiguration umfasst Flows, die der Standardregel entsprechen, sowie jede Regel, bei der für Quelle und Ziel jeweils „Jede“ bzw. „Jedes“ angegeben ist.

- **Problem 2368926: Der Auftrag „Empfehlungen“ schlägt fehl, wenn der Benutzer die Appliance neu startet, während der Auftrag ausgeführt wird.**

Wenn der Benutzer die NSX Intelligence-Appliance neu startet, während der Auftrag „Empfehlungen“ ausgeführt wird, wechselt der Auftrag in den Zustand „Fehlgeschlagen“. Ein Benutzer kann einen Empfehlungsauftrag für eine Gruppe von Kontext-VMs starten. Der Neustart löscht den Kontext und der Auftrag schlägt daher fehl.

Problemumgehung: Wiederholen Sie nach dem Neustart den Auftrag „Empfehlungen“ für denselben Satz an VMs.

- **Problem 2385599 – Gruppen von statischen IPS werden in den NSX-T Intelligence-Empfehlungen nicht unterstützt.**

VMs und Arbeitslasten, die in der NSX-T-Bestandsliste nicht erkannt werden, wenn Sie über Intranet-IP-Adressen verfügen, sind möglicherweise weiterhin als Gruppe von statischen IPS Teil von Empfehlungen. Das gilt auch für Definitionsregeln für Empfehlungen, die diese Gruppen enthalten. Allerdings unterstützt NSX Intelligence solche Gruppen nicht und infolgedessen zeigt die Visualisierung, dass der an sie gesendete Datenverkehr an „Unbekannt“ anstelle der empfohlenen Gruppe gesendet wird.

Problemumgehung: Keine. Die Empfehlung funktioniert jedoch ordnungsgemäß. Hierbei handelt es sich um ein Anzeigeproblem.

- **Problem 2374231 – Für SCTP-, GRE- und ESP-Protokoll-Flows wird der Dienst als „UNBEKANNT“ und der Port als 0 angezeigt.**

NSX Intelligence unterstützt keine Analyse der Quell- oder Zielports für GRE-, ESP- und SCTP-Protokoll-Flows. NSX Intelligence bietet eine vollständige Kopfzeilenanalyse für TCP- und UDP-Flows sowie Flow-bezogene Statistiken. Für andere unterstützte Protokolle (z. B. GRE, ESP und SCTP) kann NSX Intelligence nur IP-Informationen ohne protokollspezifische Quell- oder Zielports bereitstellen. Für diese Protokolle ist der Quell- oder Zielport Null.

Problemumgehung: Keine.

- **Problem 2374229 – Die NSX Intelligence-Appliance verfügt über keinen Festplattenspeicher mehr.**

Die Datenaufbewahrungsfrist beträgt bei der NSX Intelligence-Appliance standardmäßig 30 Tage. Wenn die Menge der Flow-Daten innerhalb von 30 Tagen größer als der erwartete Wert ist, kann es vorkommen, dass die Appliance nicht mehr über genügend Festplattenspeicher verfügt und teilweise oder vollständig nicht-operativ ist.

Problemumgehung: Das Problem kann durch Überwachung der Festplattennutzung der NSX Intelligence-Appliance verhindert oder abgemildert werden. Wenn die Festplatte mit einer hohen Rate genutzt wird, wodurch der Speicherplatz knapp werden könnte, können Sie den Datenaufbewahrungszeitraum auf eine geringere Anzahl von Tagen einstellen.

1. Führen Sie SSH in die NSX Intelligence-Appliance aus und greifen Sie auf die Datei „/opt/vmware/pace/druid-config/druid_data_retention.properties“ zu.
2. Suchen und ändern Sie die Einstellung „correlated_flow“ auf einen Wert, der unter 30 Tagen liegt. Zum Beispiel: correlated_flow=P14D
3. Speichern Sie die Datei und wenden Sie die Änderungen an, indem Sie den folgenden Befehl ausführen:

```
/opt/vmware/pace/druid-config/druid-config-data-retention.sh
```

HINWEIS: Es kann bis zu zwei Stunden dauern, bis die Daten physisch gelöscht werden.

- **Problem 2389691 – Die Veröffentlichung des Empfehlungsauftrags schlägt mit der Fehlermeldung „Größe der Anforderungsnutzlast überschreitet den zulässigen Grenzwert, max. 2.000 Objekte sind pro Anforderung zulässig“ fehl.**

Wenn Sie versuchen, einen einzelnen Empfehlungsauftrag mit mehr als 2.000 Objekten zu veröffentlichen, schlägt die Veröffentlichung mit der Fehlermeldung „Größe der Anforderungsnutzlast überschreitet den zulässigen Grenzwert, max. 2.000 Objekte sind pro Anforderung zulässig“ fehl.

Problemumgehung: Reduzieren Sie die Anzahl der Objekte im Empfehlungsauftrag auf weniger als 2.000 und wiederholen Sie die Veröffentlichung.

- **Problem 2376389 – VMs werden in der Ansicht „In den letzten 24 Stunden“ im mittleren Setup fälschlicherweise als gelöscht markiert.**

Nachdem ein Transportknoten vom Compute Manager getrennt oder entfernt wurde, zeigt NSX Intelligence die vorherigen VMs als gelöscht an, wobei neue VMs an deren Stelle vorhanden sind. Dieses Problem ergibt sich daraus, dass NSX Intelligence die Aktualisierungsbestandslisten in der NSX-Datenbank nachverfolgt. Dieses Verhalten zeigt, wie die-Bestandsliste die Trennung des Transportknotens vom Compute Manager verarbeitet. Dies wirkt sich nicht auf die Gesamtanzahl der Live-VMs in NSX Intelligence aus, obwohl in NSX Intelligence möglicherweise duplizierte VMS angezeigt werden.

Problemumgehung: Keine Aktion erforderlich. Duplizierte VMs werden je nach ausgewähltem Zeitintervall aus der Schnittstelle entfernt.

- **Problem 2393240 – zusätzliche Flows von der VM zur IP-Adresse werden beobachtet.**

Der Kunde sieht zusätzliche Flows von der VM zu IP-xxxx. Dies ist darauf zurückzuführen, dass die Konfigurationsdaten (Gruppen, VMs und Dienste) des NSX Policy Manager die NSX Intelligence-Appliance nach der Erstellung des Flows erreichen. Daher kann der (frühere) Flow nicht mit der Konfiguration korreliert werden, da er aus Sicht der Flows nicht vorhanden ist. Da der Flow nicht normal korreliert werden kann, ist er standardmäßig auf IP-xxxx für seine VM während des Flow-Lookups gesetzt. Nach der Synchronisierung der Konfiguration wird der tatsächliche VM-Flow angezeigt.

Problemumgehung: Ändern Sie das Zeitfenster, um den Flow auszuschließen, den Sie sehen möchten.

- **Problem 2370660 – NSX Intelligence zeigt für bestimmte VMs inkonsistente Daten an.**
Dies wird wahrscheinlich durch VMs verursacht, die dieselbe IP-Adresse im Datacenter haben. Dies wird nicht von NSX Intelligence in NSX-T 2.5 unterstützt.

Problemumgehung: Keine. Vermeiden Sie es, zwei VMs im Datacenter dieselbe IP-Adresse zuzuweisen.

- **Problem 2372657 – Beziehung VM-GRUPPE und Flow-Korrelationen GRUPPE-GRUPPE werden vorübergehend nicht ordnungsgemäß angezeigt.**
Die Beziehung VM-GRUPPE und die Flow-Korrelation GRUPPE-GRUPPE werden vorübergehend falsch angezeigt, wenn während der Bereitstellung der NSX Intelligence-Appliance laufende Flows im Datacenter vorhanden sind. Besonders die folgenden Elemente können während dieses vorübergehenden Zeitraums nicht ordnungsgemäß angezeigt werden:

- VMs gehören fälschlicherweise zur Gruppe „Nicht kategorisiert“.
- VMs gehören fälschlicherweise zur Gruppe „Unbekannt“.
- Korrelierte Flows zwischen zwei Gruppen können falsch angezeigt werden.

Diese Fehler beheben sich von selbst, wenn die NSX Intelligence-Appliance länger als der vom Benutzer ausgewählte Visualisierungszeitraum bereitgestellt wurde.

Problemumgehung: Keine. Wenn der Benutzer den Visualisierungszeitraum, in dem die NSX Intelligence-Appliance bereitgestellt wurde, verlässt, tritt das Problem nicht auf.

- **Problem 2366630 – Der Vorgang zum Löschen des Transportknotens schlägt möglicherweise fehl, wenn die NSX Intelligence-Appliance bereitgestellt wird.**
Wenn ein Transportknoten gelöscht wird, während die NSX Intelligence-Appliance bereitgestellt wird, kann der Löschvorgang fehlschlagen, da sich die NSGroup „NSX-INTELLIGENCE-GROUP“ auf den Transportknoten bezieht. Wenn die NSX Intelligence-Appliance bereitgestellt wird, ist für das Löschen eines Transportknotens die Option „Löschen erzwingen“ erforderlich.

Problemumgehung: Verwenden Sie die Option „Löschen erzwingen“, um den Transportknoten zu löschen.

- **Problem 2357296 – Flows werden von einigen ESX-Hosts unter bestimmten Skalierungs- und Belastungsbedingungen möglicherweise nicht an NSX Intelligence gemeldet.**
Die NSX Intelligence-Schnittstelle zeigt möglicherweise keine Flows von bestimmten VMs auf bestimmten Hosts an und bietet keine Empfehlungen für die Firewallregeln für diese VMs. Dadurch kann die Firewall-Sicherheit auf einigen Hosts beeinträchtigt werden. Dieses Problem tritt bei Bereitstellungen mit älteren vSphere-Versionen als 6.7 U2 und 6.5 U3 auf. Das Problem wird als nicht funktionierende Erstellung und Löschung des Core-VM-Filters für den ESX-Hypervisor identifiziert.

Problemumgehung: Aktualisieren Sie den Host auf Version vSphere 6.7 U2 und höher oder auf vSphere 6.5 U3 und höher.

- **Problem 2393142 – Während der Anmeldung bei NSX Manager mit vIDM-Anmeldedaten wird möglicherweise die Fehlermeldung „403 unauthorized user“ zurückgegeben.**

Dies betrifft nur Benutzer, die sich nicht als lokale Nutzer, sondern als vIDM-Benutzer bei NSX Manager anmelden. Die vIDM-Anmeldung und -Integration werden in NSX-T 2.5 bei der Interaktion mit der NSX Intelligence-Appliance nicht unterstützt.

Problemumgehung: Melden Sie sich als lokaler Benutzer an, indem Sie der NSX Manager IP/FQDN die Zeichenfolge „login.jsp?local=true“ anhängen.

- **Problem 2369802 – Die Sicherung der NSX Intelligence-Appliance schließt die Sicherung des Ereignisdatenspeichers aus.**
Diese Funktionalität wird in NSX Manager 2.5 nicht unterstützt.

Problemumgehung: Keine.

- **Problem 2346545 – NSX Intelligence-Appliance: Die Zertifikatsersetzung wirkt sich auf neue Flow-Informationsberichte aus.**
Wenn der Benutzer das Zertifikat der Prinzipalidentität für die NSX Intelligence-Appliance durch ein selbstsigniertes Zertifikat ersetzt, wird die Verarbeitung neuer Flows beeinträchtigt und die Appliance zeigt keine aktualisierten Informationen an, die darauf hinweisen.

Problemumgehung: Keine.

- **Problem 2407198 – VMs werden in der Sicherheitsposition von NSX Intelligence fälschlicherweise in der Gruppe „Nicht kategorisierte VMs“ angezeigt.**
Wenn ESXi-Hosts von vCenter getrennt werden, können VMs in diesen Hosts in der Gruppe „Nicht kategorisierte VMs“ angezeigt werden, selbst wenn Sie zu anderen Gruppen gehören. Wenn die ESXi-Hosts erneut mit vCenter verbunden sind, werden die VMs in ihren korrekten Gruppen angezeigt.

Problemumgehung: Verbinden Sie die Hosts erneut mit vCenter.

- **Problem 2410224 – Nach Abschluss der Registrierung der NSX Intelligence-Appliance kann bei der Aktualisieren der Ansicht die Fehlermeldung „403 Forbidden“ zurückgegeben werden.**
Wenn Sie nach Abschluss der Registrierung der NSX Intelligence-Appliance auf Ansicht aktualisieren klicken, gibt das System möglicherweise die Fehlermeldung „403 Forbidden“ zurück. Dies ist ein vorübergehender Zustand, der durch die von der NSX Intelligence-Appliance für den Zugriff auf die Schnittstelle benötigte Zeit ausgelöst wird.

Problemumgehung: Wenn Ihnen diese Fehlermeldung angezeigt wird, warten Sie einen Moment und versuchen Sie es erneut.

- **Problem 2410096 – Nach dem Neustart der NSX Intelligence-Appliance werden die in den letzten 10 Minuten vor dem Neustart erfassten Flows möglicherweise nicht angezeigt.**
Dies wird durch ein Indizierungsproblem verursacht.

Problemumgehung: Keine.

- **Problem 2436302: Nach dem Ersetzen des Zertifikats für den NSX-T Unified Appliance-Cluster kann auf NSX Intelligence nicht über die API oder die Manager-Schnittstelle zugegriffen werden.**
Wechseln Sie in der NSX-T Manager-Schnittstelle zur Registerkarte Planen und Fehler beheben und klicken Sie auf Entdecken und Ergreifen von Aktionen oder Empfehlungen. Die Schnittstelle wird nicht geladen und gibt schließlich sinngemäß folgenden Fehler zurück: Fehler beim Laden der angeforderten Anwendung. Versuchen Sie es erneut oder wenden Sie sich an den Support, wenn das Problem weiterhin besteht.

Problemumgehung: Weitere Informationen und eine Problemumgehung finden Sie im [Knowledgebase-Artikel 76223](#).

Bekannte Probleme bei Betriebs- und Überwachungsdiensten

- **Problem 2401164 – Sicherungen werden fälschlicherweise als erfolgreich gemeldet, obwohl ein**

SFTP-Serverfehler aufgetreten ist.

Wenn das Kennwort des für die Sicherungen verwendeten SFTP-Server abläuft, meldet NSX-T den generischen Fehler „backup operation unknown error“.

Problemumgehung: Stellen Sie sicher, dass die Anmeldedaten für den Zugriff auf den SFTP-Server auf dem neuesten Stand sind.

Bekannte Upgradeprobleme

- **Problem 2288549 – RepoSync schlägt mit einem Prüfsummenfehler in der Manifestdatei fehl.**
Dies wurde bei Bereitstellungen beobachtet, für die kürzlich ein Upgrade auf Version 2.4 durchgeführt wurde. Wenn ein aktualisiertes Setup gesichert und auf einem neu bereitgestellten Manager wiederhergestellt wird, stimmen die Prüfsumme der Repository-Manifestdatei und die Prüfsumme der tatsächlichen Manifestdatei nicht überein. Dies führt dazu, dass RepoSync nach der Wiederherstellung der Sicherung als „Fehlgeschlagen“ markiert wird.

Problemumgehung: Um diesen Fehler zu beheben, führen Sie die folgenden Schritte aus:

1. Führen Sie den CLI-Befehl `get service install-upgrade` aus.
Beachten Sie die IP von „Aktiviert auf“ in den Ergebnissen.
2. Melden Sie sich bei der NSX Manager-IP an, die in der „Aktiviert auf“-Rückgabe des oben angegebenen Befehls ausgegeben wird.
3. Navigieren Sie zu **System > Übersicht** und suchen Sie den Knoten mit der in der „Aktiviert auf“-Rückgabe angegebenen IP.
4. Klicken Sie für diesen Knoten auf **Beheben**.
5. Klicken Sie, nachdem die oben angegebene Behebung erfolgreich war, für alle Knoten derselben Schnittstelle auf **Beheben**.

Für alle drei Knoten wird jetzt der RepoSync-Status als **Abgeschlossen** angezeigt.

- **Problem 2277543 – Das Host-VIB-Update schlägt während des direkten Upgrades mit der Fehlermeldung „Installieren von Offline-Paket auf dem Host fehlgeschlagen“ fehl.**
Dieser Fehler kann auftreten, wenn vor einem direkten Upgrade von NSX-T 2.3.x auf 2.4 Storage vMotion auf dem Host ausgeführt wurde und wenn auf dem Host ESXi-6.5P03 (Build 10884925) ausgeführt wird. Das Switch-Sicherheitsmodul von 2.3.x wird nicht entfernt, wenn kurz vor dem Host-Upgrade Storage vMotion ausgeführt wurde. Storage vMotion löst einen Arbeitsspeicherverlust aus, der dazu führt, dass das Entladen des Switch-Sicherheitsmoduls fehlschlägt.

Problemumgehung: Weitere Informationen finden Sie im Knowledgebase-Artikel 67444 [Host VIB update may fail when upgrading from NSX-T 2.3.x to NSX-T 2.4.0 if VMs are storage vMotioned before host upgrade](#).

- **Problem 2276398 – Wenn eine AV-Partnerdienst-VM mithilfe von NSX aktualisiert wird, kann es zu einem bis zu zwanzig Minuten dauernden Verlust des Schutzes kommen.**
Wenn eine Partner-SVM aktualisiert wird, wird die neue SVM bereitgestellt und die alte SVM wird gelöscht. Im Host-Syslog werden möglicherweise SolutionHandler-Verbindungsfehler angezeigt.

Problemumgehung: Löschen Sie nach dem Upgrade den ARP-Cache-Eintrag auf dem Host und pinggen Sie dann die Partnersteuerungs-IP auf dem Host, um dieses Problem zu beheben.

- **Problem 2330417: Upgrade für nicht aktualisierte Transportknoten kann nicht fortgesetzt werden.**
Beim Upgraden wird das Upgrade als erfolgreich markiert, obwohl einige Transportknoten nicht aktualisiert wurden. Speicherort des Protokolls: `/var/log/upgrade-coordinator/upgrade-coordinator.log`.

Problemumgehung: Starten Sie den Dienst „upgrade-coordinator“ neu.

- **Problem 2348994 – Zeitweiliger Fehler während des Upgrades von NSX VIBs auf ESXi 6.5 p03-Transportknoten.**

Tritt bei einigen Upgrades von 2.4.x auf 2.5 auf. Bei einem Upgrade der NSX-VIBs auf einem ESXi 6.5 p03-Transportknoten, schlägt der Upgrade-Vorgang manchmal mit dem folgenden Fehlermeldung fehl: „VI SDK-Aufrufausnahme: Keine Daten vom Prozess erhalten: LANG=en_US.UTF-8“.

Problemumgehung: Upgrade auf ESXi 5 p04 durchführen. Alternativ können Sie den Host in den Wartungsmodus versetzen und neu starten. Wiederholen Sie das Upgrade und beenden Sie den Wartungsmodus.

- **Problem 2372653 – Nach dem Upgrade auf 2.5, kann der Benutzer LogicalPort- und LogicalSwitch-basierte Gruppen in früheren NSX-T-Versionen nicht finden.**

Nach dem Upgrade auf 2.5 werden die über eine Richtlinie in früheren NSX-T-Versionen erstellten LogicalPort- und LogicalSwitch-basierten Gruppen nicht in der Dashboard-Schnittstelle angezeigt. Sie können sich jedoch weiterhin in der-API gefunden werden. Dies ist auf eine durch den Upgrade-Vorgang verursachte Namensänderung zurückzuführen. In 2.5 werden LogicalPort- und LogicalSwitch-basierte Gruppen als Segment- und SegmentPort-basierte Gruppen angezeigt.

Problemumgehung: Verwenden Sie nur die API, um nach dem Upgrade auf diese Richtliniengruppen zuzugreifen.

- **Problem 2408972 – Während des Upgrades ergibt sich ein Fehler bei vSphere Update Manager während der Standardisierung des letzten Hosts.**

Während des Upgrades schlägt bei vSphere Update Manager die Standardisierung für den letzten Host fehl, dessen Arbeitslasten von einem logischen NSX-T-Switch unterstützt werden.

Problemumgehung: Migrieren Sie alle NSX-T-gestützten Arbeitslast-VMs manuell auf einen bereits aktualisierten Host und versuchen Sie dann, das Upgrade für den fehlgeschlagenen Host erneut durchzuführen.

- **Problem 2400379 – Auf der Seite „Kontextprofil“ wird die Fehlermeldung „Nicht unterstützte APP_ID“ angezeigt.**

Auf der Seite „Kontextprofil“ wird die folgende Fehlermeldung angezeigt: „Dieses Kontextprofil verwendet eine nicht unterstützte APP_ID - [< APP_ID >]. Löschen Sie dieses Kontextprofil manuell, nachdem Sie sichergestellt haben, dass es in keiner Regel verwendet wird.“ Dies wird durch sechs veraltete APP_IDs (AD_BKUP, Skip, AD_NSP, SAP, sunrpc, SVN), die nach dem Upgrade vorhanden sind und nicht mehr auf dem Datenpfad funktionieren, verursacht.

Problemumgehung: Löschen Sie die sechs APP_ID-Kontextprofile manuell, nachdem Sie sichergestellt haben, dass sie nicht mehr verbraucht werden.

- **Problem 2419246 – Ubuntu KVM-Upgrade schlägt fehl.**

Das Upgrade von Ubuntu-KVM-Knoten schlägt möglicherweise fehl, da der nsx-vdpi-Dienst nicht ausgeführt wird. Der nsx-vdpi-Dienst ist jedoch vom nsx-agent abhängig, aber zu diesem Zeitpunkt des Upgrades ist der nsx-agent noch nicht konfiguriert. Der nsx-Agent schlägt fehl, da die vm-command-relay-Komponente nicht ordnungsgemäß gestartet wurde.

Problemumgehung: Konfigurieren Sie den nicht vollständig installierten nsx-agent. Mit dem folgenden Befehl werden alle ausgepackten oder teilweise konfigurierten Pakete neu konfiguriert:

```
dpkg --configure -a
```

Sie können auch die folgenden Befehle verwenden, um nur den nsx-agent und nsx-vdpi zu konfigurieren:

```
dpkg --configure nsx-agent
```

```
dpkg --configure nsx-vdpi
```

Bekannte Probleme mit APIs

- **Problem 2260435: Statusfreie Umleitungsrichtlinien/-regeln werden standardmäßig durch die API erstellt, die nicht für Ost-West-Verbindungen unterstützt wird.**

Statusfreie Umleitungsrichtlinien/-regeln werden standardmäßig durch die API erstellt, die nicht für Ost-West-Verbindungen unterstützt wird. Dies führt dazu, dass der Datenverkehr nicht an Partner umgeleitet wird.

Problemumgehung: Erstellen Sie einen Abschnitt „Statusbehaftet“, wenn Sie Umleitungsrichtlinien mithilfe der Richtlinien-API erstellen.

- **Problem 2200856 – Neustart des Cloud-Service-Manager-Diensts schlägt fehl.**
Der Neustart des Cloud-Service-Manager-Diensts kann fehlschlagen, wenn der Benutzer ihn durchführt, ohne auf den erstmaligen Start des API-Dienstes zu warten.

Problemumgehung: Warten Sie einige Minuten und versuchen Sie es erneut.

- **Problem 2378752 – Die API ermöglicht das Erstellen mehrerer Bindungszuordnungen unter Segmenten oder Ports.**

Das Problem tritt nur bei der API auf. Wenn ein Benutzer mehrere Bindungszuordnungen unter einem Segment oder Port erstellt, wird kein Fehler gemeldet. Das Problem tritt auf, wenn der Benutzer versucht, mehrere Profile gleichzeitig an einem Segment oder Port zu binden.

Problemumgehung: Verwenden Sie für diesen Vorgang stattdessen die NSX Manager-Schnittstelle.

Bekannte Probleme bei NSX Cloud

- **Problem 2275232 – DHCP funktioniert nicht für VMs in der Cloud, wenn die Konnektivitätsstrategie für DFWs von BLACKLIST in WHITELIST geändert wird.**
Alle VMs, die neue DHCP-Leases anfordern, verlieren die IPs. DHCP muss in DFW explizit für Cloud-VMs zugelassen werden.

Problemumgehung: Lassen Sie in DFW DHCP explizit für Cloud-VMs zu.

- **Problem 2277814 – Eine VM wird aufgrund eines ungültigen Werts für das nsx.network-Tag zu „vm-overlay-sg“ verschoben.**
Eine VM, die mit einem ungültigen nsx.network-Tag versehen ist, wird zu „vm-overlay-sg“ verschoben.

Problemumgehung: Entfernen Sie das ungültige Tag.

- **Problem 2355113 – NSX Tools können nicht auf RedHat- und CentOS-Workload-VMs mit aktiviertem beschleunigtem Netzwerk in Microsoft Azure installiert werden.**
Wenn in Microsoft Azure das beschleunigte Netzwerk auf RedHat- (7.4 oder höher) oder auf CentOS- (7.4 oder höher) basierenden Betriebssystemen mit installiertem NSX Agent aktiviert ist, erhält die Ethernet-Schnittstelle keine IP-Adresse.

Problemumgehung: Installieren Sie nach dem Starten einer RedHat- oder CentOS-basierten VM in Microsoft Azure die neuesten Linux Integration Services -Treiber, die sie unter <https://www.microsoft.com/en-us/download/details.aspx?id=55106> finden, vor der Installation von NSX Tools.

- **Problem 2391231 – Änderungen an Azure-VMs können verzögert erkannt werden.**
Änderungen an Azure-VMs werden zeitweise in der Cloud mit einer leichten Verzögerung erkannt. Eine entsprechende Verzögerung kann das Onboarding der VMs und das Erstellen logischer Entitäten für die VMs in NSX-T beeinträchtigen. Die beobachtete maximale Verzögerung beträgt etwa acht Minuten.

Problemumgehung: Keine. Nach Ablauf des Verzögerungszeitraums behebt sich das Problem von selbst.

- **Problem 2424818 – L2- und DFW-Statistiken werden auf NSX Manager-Benutzeroberfläche nicht aktualisiert.**

Alle vom logischen Exporteur auf Arbeitslast-VMs erzeugten Statistiken, werden nicht an MP weitergeleitet. Dies führt zu einem Fehler bei der Anzeige von Statistiken auf der NSX Manager-Benutzeroberfläche. DFW-Statistiken sind nicht über die NSX Manager-Benutzeroberfläche sichtbar. Der Betriebsstatus des logischen Switch-Ports wird als „Inaktiv“ angezeigt und die entsprechenden Statistiken werden nicht ausgeführt. Dies gilt nur für Cloud-VMs.

Problemumgehung: Keine. Die Statistiken können über die CLI auf den entsprechenden VMs angezeigt werden.