

Versionshinweise für VMware NSX-T Data Center 2.3

VMware NSX-T Data Center 2.3 | 18. September 2018 | Build 10085361

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](#)
- [API-Referenzinformationen](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

Neuigkeiten

NSX-T Data Center 2.3 ist die inkrementelle Upgradeversion, in der die neue für Cloud und Container bereitgestellte Multi-Hypervisor-Plattform erweitert wird.

Die folgenden neuen Funktionen und Verbesserungen sind in der Version NSX-T Data Center 2.3 verfügbar.

Einführung der NSX-T Data Center-Unterstützung für Bare Metal Hosts

Die Bare Metal-Unterstützung schließt auf Bare Metal-Servern ausgeführte Linux-basierte Arbeitslasten und Container, die auf Bare Metal-Servern ohne einen Hypervisor ausgeführt werden, ein. NSX-T Data Center nutzt den Open vSwitch, um zu ermöglichen, dass jeder Linux Host ein NSX-T Data Center-Transportknoten werden kann.

- **Bare-Metal-Server-Unterstützung:** beinhaltet systemeigene Computing-Arbeitslasten unter den Betriebssystemen RHEL 7.4, CentOS 7.4 und Ubuntu 16.0.4, um so den Benutzern zu ermöglichen, Bare Metal-Computing-Arbeitslasten über VLAN zu vernetzen, gesicherte Verbindungen zu überlagern und Mikro-Segmentierungsrichtlinien (statusbehaftete Schicht-4-Durchsetzung) für virtuelle/physische und physische/physische Kommunikationen zu erzwingen.
- **Bare-Metal-Linux-Container-Unterstützung:** führt Docker-Container mithilfe der RedHat OpenShift Container-Plattform auf Bare Metal-Linux-Hosts mit RHEL 7.4 oder RHEL 7.5 aus.

Verbesserungen der NSX-Cloud

- **Unterstützung von AWS-Bereitstellungen:** NSX-Cloud-Unterstützung von AWS-Arbeitslasten.
- **Automatische Bereitstellung von NSX-Agents in Azure VNets**
- **VPN-Unterstützung zwischen lokalen Maschinen und Public Cloud:** enthält integrierte VPN-Funktionen innerhalb des NSX Cloud Public Cloud-Gateways mithilfe von APIs. Sie können die VPN-Funktionen verwenden, um IPSEC Links zwischen den folgenden Optionen anzulegen:

- Managed Computing Amazon VPCs/Azure VNETs und Drittanbieter-Dienst-VMs beim Übergang Amazon VPCs/Azure VNETs
- Managed Amazon VPC/Azure VNET und ein dezentrales VPN-Gerät
- **Erweiterte Betriebssystemunterstützung für den NSX Cloud-Agent:** NSX Cloud unterstützt RHEL 7.5-Betriebssysteme in der Public Cloud.

Unterstützung von Sicherheitsdiensten

Einführung in Service Insertion auf den Routing-Ebenen

- **Service Insertion-Unterstützung auf Ebene-0- und Ebene-1-Routern:** umfasst die Fähigkeit zum Onboarding von Drittanbieter-Sicherheitslösungen, zum Bereitstellen einer Drittanbieter-Hochverfügbarkeits-Sicherheitslösung auf Ebene-0 oder Ebene-1 oder beiden, und das Integrieren der Drittanbieter-Sicherheitslösung durch eine Umleitungsrichtlinie.
Im VMware-Kompatibilitätshandbuch – Netzwerk und Sicherheit finden Sie Informationen zu den neuesten Zertifizierungsstatus von Drittanbieterlösungen in NSX-T Data Center.

Verbesserungen der verteilten Firewall

- **Unterstützung mehrerer Abschnitte in der NSX Edge-Firewall:** fügt der NSX Edge-Firewall für mehrere Abschnitte hinzu, um die Verwaltung zu vereinfachen
- **Die Firewall-Regel Hit Count- und -Regelbeliebtheitsindex:** überwacht die Regelnutzung und die schnelle Identifizierung von nicht verwendeten Regeln für die Bereinigung
- **Sperren von Firewall-Abschnitten:** ermöglicht es mehreren Sicherheitsadministratoren, gleichzeitig an der Firewall zu arbeiten.
- **Gruppieren von Objekten:** unterstützt das Hinzufügen eines Objekts zu einer Gruppe, wenn es alle fünf angegebenen Kennzeichen erfüllt – zuvor waren dies nur zwei Kennzeichen
- **Tag-Länge:** erhöht den Tag-Längenwert von 65 auf 256 und den Tag-Geltungsbereich von 20 auf 128
- **Anwendungserkennung:** ermittelt und kategorisiert (und lässt dabei auch benutzerdefinierte Kategorisierungen durch Benutzer zu) in den Gast-VMs installierte Anwendungen. Die Anwendungen enthalten Details zu ausführbaren Dateien, Hash, Herausgeber und Installationsdatum.

Unterstützung des Netzwerks und der NSX Edge-Dienste

- **Overlay-Unterstützung für den Modus „Erweiterter Datenpfad“ in N-VDS:** In Verbindung mit vSphere 6.7 unterstützt der Modus „Erweiterter Datenpfad“ in N-VDS für NSX-T Data Center 2.3 Arbeitslasten im NFV-Stil, wofür ein leistungsstarker Datenpfad erforderlich ist.
- **Unterstützung für statusbehaftete NAT- und Firewalldienste am zentralen Dienstport**
- **API-Unterstützung zum Löschen aller DNS-Einträge in DNS-Weiterleitung:** bietet die Möglichkeit, alle DNS-Cache-Einträge in einem einzelnen API-Aufruf in einer bestimmten DNS-Weiterleitung zu löschen. Dieser Befehl ist nützlich, wenn ein DNS-Server falsche Antworten zurückgibt, sowie zur Vermeidung des Wartens auf die DNS-Eintrag-Zeitüberschreitung nach der Instandsetzung des DNS-Servers.
- **Load Balancer-Erweiterungen**
 - **Unterstützung für die vordefinierte Verschlüsselungsliste:** Vordefinierte SSL-Profile für HTTPS VIP für höhere Sicherheit oder Leistung.
 - **Verbesserung der Load Balancer-Regel:** neue Load Balancer-Regeln, *Header löschen-Aktion SSL Übereinstimmungsbedingung* und *Variable bei Übereinstimmungsbedingung zuweisen*.
 - **Load Balancer-Unterstützung auf eigenständigen Dienstroutern:** bietet die Möglichkeit zur Bereitstellung eines Load Balancing-Dienstes auf einem Dienstrouter, der nicht über einen Router-Port verfügt.

Verbesserungen der Benutzeroberfläche

- **Unterstützung neuer Sprache:** die Benutzeroberfläche ist jetzt auf Englisch, Deutsch, Französisch,

- Japanisch, Chinesisch (vereinfacht), Koreanisch, Chinesisch (traditionell) und Spanisch verfügbar.
- **Verbesserte Navigation und Startseite:** Suche mit Hervorhebung auf der Startseite und kompakte Systemübersicht.
- **Verbesserte Suche:** Die Suche umfasst Type-ahead-Vorschläge, auf die von der Startseite aus zugegriffen werden kann.
- **Visualisierung der Netzwerktopologie:** NSX Policy Manager bietet die Möglichkeit, die Kommunikation von Gruppe zu Gruppe, VM zu VM und Prozess zu Prozess zu überwachen. Sie können Beziehungen zwischen Netzwerkobjekten wie z. B. logischen Switches, Ports, Routern und NSX Edges visualisieren.

Unterstützung von Betrieb und Fehlerbehebung

- **Verbesserungen bei Installation und Upgrade**
 - **NSX-T Data Center in einer statusfreien vSphere-Umgebung:** aktiviert zusätzliche Bereitstellungsoptionen, indem Unterstützung für statusfreie ESXi-Hosts bereitgestellt wird, die vSphere Auto Deploy- und Host-Profile verwenden. Für die Unterstützung der Funktionen ist vSphere 6.7 U1 oder höher erforderlich.
 - **Unterstützung für gleichzeitiges Vorhandensein von NSX Edge VM und Bare Metal in demselben NSX Edge-Cluster:** Die NSX Edge Knoten-VM und Bare Metal können nun in demselben NSX Edge-Cluster existieren, um die Skalierung der auf dem NSX Edge-Knoten gehosteten Dienste, wie dem Load Balancer, zu vereinfachen.
 - **Modulares NSX-T Data Center-Upgrade:** bietet Unterstützung für modulare Upgrades im Upgrade-Koordinator. Sie können nur die NSX-T Data Center-Komponenten aktualisieren, die in der neuen Release-Version geändert wurden. Diese zusätzliche Funktionalität verringert den operativen Overhead beim Patchen einer NSX-T Data Center-Version.
- **Überwachung und Fehlerbehebung**
 - **ERSPAN für KVM-Hypervisor:** umfasst die Unterstützung für Port-Mirroring auf KVM – ERSPAN Typ II und III.
 - **Traceflow zu und von logischen Tier-0 Router-Uplinks:** bietet die Möglichkeit zum Generieren des Traceflow-Datenverkehrs von logischen Tier-0 Router-Uplinks und zum Melden des Empfangs von Traceflow-Paketen auf logischen Tier-0 Router-Uplinks zur Vereinfachung der Fehlerbehebungsoperationen unter Einbindung der nördlichen Schnittstellen der NSX Edge-Knoten beim Traceflow-Reporting.
 - **CLI-Unterstützung zum Herunterfahren von DPDK-Ports auf einem Bare Metal-Edge-Knoten:** bietet die Möglichkeit, einen von DPDK beanspruchten Port auf dem Bare Metal-NSX Edge-Knoten herunterzufahren, um die Portisolierung während Installations- und Fehlerbehebungsvorgängen zu vereinfachen.

Unterstützung für OpenStack Neutron-Plug-In

Diese Funktionen werden ab der OpenStack-Upstream-Version Queens unterstützt.

- **Möglichkeit zum Bereitstellen eines durch „Erweiterter Datenpfad“ unterstützen logischen Overlay-Switches durch das Neutron-Plug-In:** Das NSX Neutron-Plug-In bietet die Möglichkeit zur Nutzung des Modus „Erweiterter Datenpfad“ für Overlay. Dieser war früher nur VLAN vorbehalten. Mit der Unterstützung für diese Funktionen können Sie beispielsweise die Leistung von „Erweiterter Datenpfad“ zusätzlich zur OpenStack-Umgebung für NFV-bezogene Arbeitslasten nutzen.
- **Unterstützung für die Koexistenz von NSX-Produkten und OpenStack:** Das NSX Neutron-Plug-In unterstützt jetzt die simultane Verwaltung von NSX Data Center for vSphere und NSX-T Data Center für eine OpenStack-Implementierung.
- **Möglichkeit zur Nutzung der VPN-as-a-Service-Funktion in OpenStack:** Unterstützung für OpenStack VPNaaS in der Neutron-Erweiterung in OpenStack, die den VPN-Funktionssatz einführt.

Unterstützung des NSX Container Plug-Ins (NCP)

- **Concourse Pipeline zur Installation von NSX-T Data Center**
- **Annotation für die Load Balancer SNAT IP:** Die SNAT-IP für einen Load Balancer wird in einem Kubernetes-Dienst vom Typ LoadBalancer annotiert, `ncp/internal_ip_for_policy: <SNAT IP>`, und dem Status des Dienstes hinzugefügt: `status.loadbalancer.ingress.ip: [<SNAT IP>, <Virtual IP>]`. Diese IP-Adresse kann verwendet werden, um eine Netzwerkrichtlinie zu

- erstellen, die diesen IP CIDR ermöglicht.
- **Verbesserung der Kubernetes-Netzwerkrichtlinie:** bietet die Möglichkeit, Pods aus verschiedenen Namespaces mit Kubernetes-Netzwerkrichtlinienregeln auszuwählen.
- **Verbesserungen bei Kubernetes-Load Balancer/SNAT-Annotationen**
 - Wenn NCP keinen Load Balancer für einen Dienst konfigurieren kann, wird der Dienst mit `ncp/error.loadbalancer` annotiert.
 - Wenn NCP keine SNAT-IP für einen Dienst konfigurieren kann, wird dem Dienst `ncp/error.snat` annotiert.
- **Sitzungspersistenz des NSX-T Data Center Load Balancers** für Kubernetes Ingress- und OpenShift-Routen
- **Verbesserung des Bereinigungsskripts**

Kompatibilität und Systemvoraussetzungen

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

NSX-T Data Center in einer statusfreien vSphere-Umgebung – für statusfreie ESXi-Hosts, die vSphere Auto Deploy und Host-Profile verwenden, ist vSphere 6.7 U1 oder höher erforderlich.

NCP-Kompatibilitätsanforderungen:

Produkt	Version
NCP/NSX-T Data Center-Kachel für PAS	2.3.0
NSX-T Data Center	2.2, 2.3
Kubernetes	1.10, 1.11
OpenShift	3.9, 3.10
Kubernetes-Host-VM-Betriebssystem	Ubuntu 16.04, RHEL 7.4, 7.5
OpenShift-Host-VM-Betriebssystem	RHEL 7.4, RHEL 7.5
PAS (PCF)	OpsManager 2.1.x + PAS 2.1.x (außer PAS 2.1.0) OpsManager 2.2.0 + PAS 2.2.0

Allgemeine Änderungen des Verhaltens

Änderung des Standard-HA-Modus für logische Tier-1 Router von Vorbeugend zu Nicht vorbeugend

Beim Erstellen eines logischen Tier-1 Routers war der Standard-HA-Modus Präventiv, was zu einer Verlangsamung des Datenverkehrs führte, wenn der bevorzugte NSX Edge-Knoten wieder online ging. Mit dem neuen Standard HA-Modus, der auf Nicht vorbeugend festgelegt ist, kommt es nicht zu einer Verlangsamung des Datenverkehrs an den neu erstellten logischen Tier-1 Routern. Die vorhandenen logischen Tier-1 Router sind von dieser Änderung nicht betroffen.

Änderung der Kommunikation vom Transportknoten zum NSX Controller

Aufgrund von Änderungen in der Kommunikation vom Transportknoten zum NSX Controller müssen Sie jetzt den TCP-Port 1235 für NSX-T 2.2 und höher öffnen. Weitere Informationen finden Sie im [Installationshandbuch für NSX-T](#).

Beim Upgrade von NSX-T 2.1 auf höhere Versionen müssen sowohl der TCP-Port 1234 als auch der TCP-Port 1235 geöffnet sein. Nachdem das Upgrade abgeschlossen ist, wird der TCP-Port 1235 verwendet.

API-Referenzinformationen

Weitere Informationen finden Sie unter [Veraltete API-Aufrufe und Eigenschaften der NSX-T Data Center- und NSX-Richtlinie](#).

Die aktuelle API-Referenz finden Sie unter [NSX-T Data Center-Produktinformationen](#).

Behobene Probleme

Die behobenen Probleme werden in die im Folgenden aufgeführten Kategorien unterteilt.

- [Allgemeine behobene Probleme](#)
- [Behobene Installationsprobleme](#)
- [Behobene Probleme beim NSX Manager](#)
- [Behobene Probleme bei NSX Edge](#)
- [Behobene Probleme bei logischen Netzwerken](#)
- [Behobene Probleme bei Sicherheitsdiensten](#)
- [Behobene Probleme beim Load Balancer](#)
- [Behobene Probleme bei der Lösungsinteroperabilität](#)
- [Behobene Probleme bei Betriebs- und Überwachungsdiensten](#)
- [Behobene Upgradeprobleme](#)
- [Behobene API-Probleme](#)
- [Behobene Probleme beim NSX-Container-Plug-In \(NCP\)](#)

Allgemeine behobene Probleme

- **Problem 1775315:** Ein CSRF-Angriff tritt auf, wenn der Postman-Client über den Webbrowser geöffnet wird
Für API-Aufrufe, die über Postman-, CURL- oder andere REST-Clients durchgeführt werden, müssen Sie den XAAS-TOKEN-Header und dessen Wert explizit angeben. Der erste API-Aufruf mithilfe von Remothe-authN oder ein Aufruf von /api/session/create(local authN) enthält das XSRF-Token im Antwortobjekt. Darauf folgende API-Aufrufe beinhalten den Tokenwert im XSRF-TOKEN-Header als Teil der Anforderung.
- **Problem 1989412:** Eine Domänenlöschung bei nicht erreichbarbarem NSX Manager wird nicht widergespiegelt, wenn die Verbindung wiederhergestellt wird
Wenn eine Domäne aus einer Richtlinie gelöscht wird, während der NSX Manager nicht erreichbar ist, sind die Firewall und die entsprechenden Regeln, die auf die gelöschte Domäne verweisen, immer noch vorhanden, wenn die Verbindung zum NSX Manager wiederhergestellt wird.
- **Problem 2018478:** Der Versuch, ein Widget aus dem Dashboard zu entfernen, führt zu einem Absturz mit Stack-Trace-Fehler
Benutzerdefinierte Änderungen der Dashboard-Benutzeroberfläche, wie etwa das Entfernen eines Widgets von mehreren Widgets, führen dazu, dass die Benutzeroberfläche mit einem Stack-Trace-Fehler abstürzt.
- **Problem 1959647:** Verwendung eines Aliasnamens für einen Datenbankserver zur Erstellung eines DSN kann dazu führen, dass sich die Installation von vCenter Server nicht durchführen lässt
Wenn Sie einen Datenbankserver-Aliasnamen zum Erstellen eines DSN verwenden, schlägt die Installation von vCenter Server mit einer externen Microsoft SQL-Datenbank fehl. Die folgende Fehlermeldung wird während der Installation des Inventory Service angezeigt: Fehler beim Starten des Dienstes „invsvc“.

Behobene Installationsprobleme

- **Problem 1739120:** Nach dem Neustart der Management Plane oder des Proton-Dienstes in der Management Plane reagiert der Bereitstellungsstatus des Fabric-Knotens nicht mehr

Wenn Sie auf der Fabric-Seite einen neuen unterstützten Host mit Hostanmeldedaten hinzufügen, ändert sich der Status in **Installation läuft**. Nach dem Neustart der Management Plane oder des Proton-Diensts auf der Management Plane wird der Bereitstellungsstatus des Hosts auf unbestimmte Zeit als **Installation läuft** oder **Deinstallation läuft** angezeigt.

- **Problem 1944669:** Bei der Bereitstellung von NSX-T Data Center-Appliances auf KVM muss die genaue Arbeitsspeichergröße angegeben werden
Die Bereitstellung von NSX-TData Center -Appliances auf ESX ist in kleinen, mittleren und großen Größen mit unterschiedlichen RAM-Konfigurationen möglich. Allerdings muss bei der Bereitstellung von NSX-TData Center -Appliances auf KVM die RAM-Zuweisung explizit konfiguriert werden.
- **Problem 1944678:** Die Bereitstellung einer einheitlichen NSX-T-Appliance erfordert einen gültigen Rollentyp
Wenn eine einheitliche NSX-T-Appliance in KVM ohne eine angegebene Rolle oder mit einem ungültigen Rollentyp bereitgestellt wird, wird sie in einer nicht unterstützten Konfiguration bereitgestellt, bei der alle Rollen aktiviert sind.
- **Problem 1958308:** Die Hostvorbereitung oder das Erstellen eines Transportknotens kann nicht durchgeführt werden, wenn der Host gesperrt ist
Die Hostvorbereitung oder das Erstellen eines Transportknotens kann nicht durchgeführt werden, wenn der Host gesperrt ist. Dabei wird die folgende Fehlermeldung angezeigt: `Die Berechtigung zur Durchführung dieses Vorgangs wurde verweigert.`

Behobene Probleme beim NSX Manager

- **Problem 1954923:** vMotion-Vorgänge für VMs, die mit logischen Switches verbunden sind, schlagen während des Upgrades der Management Plane fehl
Wenn Sie während eines Upgrades der Management Plane versuchen, einen vMotion-Vorgang für eine virtuelle Maschine durchzuführen, die mit einem logischen Switch verbunden ist, schlägt dieser vMotion-Vorgang fehl.
- **Problem 1954927:** Nachdem die Wiederherstellung von NSX Manager abgeschlossen und ein neuer nicht-VC-verwalteter ESX-Host bei NSX Manager registriert ist und seine virtuellen Maschinen mit vorhandenen logischen Switches verbunden sind, ist die MAC-Adresse für die VM auf dem MOB des ESX-Hosts leer.
Nachdem die Wiederherstellung von NSX Manager abgeschlossen und ein neuer nicht-VC-verwalteter ESX-Host bei NSX Manager registriert ist und seine virtuellen Maschinen mit vorhandenen logischen Switches verbunden sind, ist die MAC-Adresse für die VM auf ESX-Hosts-MOB leer.
- **Problem 1978104:** Auf manche Seiten in der NSX Manager-Benutzeroberfläche kann in Internet Explorer 11 nicht zugegriffen werden
Das Dashboard, die Erste-Schritte-Workflows und die Load Balancer-Seiten auf der NSX Manager-Benutzeroberfläche sind bei Nutzung von Internet Explorer auf einem Windows-Computer nicht zugänglich.
- **Problem 1954986:** Der Lizenzschlüssel wird in den Protokollen angezeigt, wenn der Schlüssel über die Benutzeroberfläche gelöscht wird
Der NSX-Lizenzschlüssel wird in `/var/log/syslog` wie folgt angezeigt:

```
<182>1 2017-03-24T05:03:47.008Z bb-mgr-221 NSX - SYSTEM [nsx@6876 audit="true" comp="nsx-manager" reqId="3d146f2b-fa34-460f-8ac3-56e3c7326015" subcomp="manager"] UserName:'admin', ModuleName:'License', Operation:'DeleteLicense, Operation status:'success', New value: ["<license_key>"] <182>1 2017-03-24T05:03:47.009Z bb-mgr-221 NSX - - [nsx@6876 audit="true" comp="nsx-manager" subcomp="manager"] UserName:'admin', ModuleName:'Batch', Operation:'RegisterBatchRequest, Operation status:'success', New value: [{"atomic":false} {"request": [{"method":"DELETE","uri":"/v1/licenses/<license_key>"}]}]
```

Wenn die Appliance zum Senden von Protokollen an einen externen Log-Collector konfiguriert ist, ist der Schlüsselwert für autorisierte Benutzer des externen Log-Collector ebenfalls sichtbar.

- **Problem 1956055:** Lokale Admin-Benutzer haben von der Benutzeroberfläche aus keinen Zugriff auf das Tech-Support-Paket, wenn der Datenspeicher der Management Plane inaktiv ist
Lokale Admin-Benutzer haben von der Benutzeroberfläche aus keinen Zugriff auf das Tech-Support-Paket, wenn der Datenspeicher der Management Plane inaktiv ist
- **Problem 1957165:** Das Laden der letzten Seite in einem Suchergebnissatz mit 10.040 Datensätzen oder mehr führt zu einem Fehler
In einer großen Umgebung, in der eine Suchabfrage 10.040 oder mehr Objekte ergeben kann, kann es zu einem Fehler kommen, wenn die letzten Datensätze des Suchergebnisses geladen werden.

Behobene Probleme bei NSX Edge

- **Problem 1762064:** Die Konfiguration des VTEP-IP-Pools und des Uplink-Profiles von NSX Edge direkt nach einem Neustart von NSX Edge führt dazu, dass die VTEP-BFD-Sitzung nicht erreichbar ist.
Nach dem Neustart von NSX Edge benötigt der Broker etwas Zeit, um die NSX Edge-Verbindungen zurückzusetzen.

Behobene Probleme bei logischen Netzwerken

- **Problem 1966641:** Wenn Sie einen Host hinzufügen und ihn als Transportknoten konfigurieren, wird der Knotenstatus als „Inaktiv“ angezeigt, wenn der Knoten nicht Teil eines logischen Switches ist
Nach dem Hinzufügen eines neuen Hosts und Konfigurieren des Hosts als Transportknoten oder beim Konfigurieren eines Plans für ein Upgrade auf NSX-T 2.1 wird der Transportknotenstatus auf der Benutzeroberfläche als „Inaktiv“ angezeigt, wenn der Knoten nicht Teil eines logischen Switches ist.
- **Problem 2015445:** Der Firewallstatus auf dem aktiven Dienstrouter wird möglicherweise auf dem neu aktiven Dienstrouter nicht dupliziert
Beim logischen Router des Mandanten (Tenant Logical Router, TLR) treten möglicherweise mehrere Failover von NSX Edge1 auf NSX Edge2 und von NSX Edge2 auf NSX Edge1 auf. Firewall- oder NAT-Flow-Zustände werden zwischen aktiven/Standby-TLR-Dienstroutern synchronisiert. Wenn der TLR in einem nicht präemptiven Failover-Modus konfiguriert ist, findet die Synchronisierung vor dem ersten Failover statt, aber nicht zwischen dem ersten und dem nachfolgenden Failover. Dies kann dazu führen, dass beim zweiten Failover eine Zeitüberschreitung beim TCP-Datenverkehr eintritt. Dieses Problem tritt bei einem im präemptiven Modus konfigurierten TLR nicht auf.
- **Problem 2016629:** RSPAN_SRC-Spiegelungssitzung schlägt nach der Migration fehl
Wenn eine mit einem Port, der für eine RSPAN_SRC-Spiegelungssitzung zugewiesen ist, verbundene VM zu einem anderen Hypervisor migriert wird und im Zielnetzwerk des Ziel-Hypervisor keine erforderliche pNic vorhanden ist, kann die RSPAN_SRC-Spiegelungssitzung auf dem Port nicht konfiguriert werden. Dieser Fehler führt zu dem Port-Verbindungsfehler, aber der vMotion-Migrationsvorgang ist erfolgreich.
- **Problem 1620144:** In der NSX-T Data Center-Befehlszeile (CLI) werden beim Befehl `get logical-switches` logische Switches mit dem Status „AKTIV“ angezeigt, selbst wenn der Transportknoten gelöscht wurde.
Die CLI kann fälschlicherweise anzeigen, dass ein funktionierender logischer Switch vorhanden ist. Selbst wenn logische Switches erkennbar sind, funktionieren sie nicht. Der opake Switch wird deaktiviert, wenn der Transportknoten gelöscht wird, weshalb kein Datenverkehr mehr durchfließt.

- **Problem 1590888:** Der Warnhinweis fehlt, dass logische Ports, die im Ethernetbereich ausgewählt werden, nur im selben L2-Netzwerk gelten.
Wenn bei der verteilten Firewall im Ethernetbereich ein logischer Port oder eine MAC-Adresse als Quelle bzw. Ziel eingegeben wird, sollte ein Warnhinweis angezeigt werden, dass MAC-Adressen oder logische Ports zu VM-Ports im selben L2-Netzwerk gehören (mit demselben logischen Switch verbunden sein) müssen. Derzeit gibt es keinen Warnhinweis.
- **Problem 1763576:** Hypervisoren lassen sich selbst dann als Transportknoten entfernen, wenn sie VMs im NSX-T Data Center-Netzwerk aufweisen.
NSX-T Data Center hält Sie nicht davon ab, einen Transportknoten zu löschen, selbst wenn sich auf dem Knoten VMs befinden, die zum NSX-T-Netzwerk gehören. Die Anbindung der VMs geht verloren, nachdem der Transportknoten gelöscht wurde.
- **Problem 1780798:** In großen Umgebungen kann es zum Ausfall bestimmter Hosts kommen
In großen Umgebungen mit 200 oder mehr Hostknoten geht nach längerem Betrieb die Verbindung bestimmter Hosts mit NSX Manager unter Umständen verloren. Das Protokoll enthält dann folgende Fehlermeldungen:
`2016-12-09T00:57:58Z mpa: [nsx@6876 comp="nsx-esx" subcomp="mpa" level="WARN"]
Unknown routing key: com.vmware.nsx.tz.*`
- **Problem 1954997:** Löschen von Transportknoten schlägt fehl, wenn VMs auf dem Transportknoten zum Zeitpunkt der Löschung mit logischem Switch verbunden sind
 1. Fabric-Knoten und Transportknoten werden erstellt.
 2. VIFs werden dem logischen Switch zugeordnet.
 3. Das Löschen des Transportknotens ohne Entfernen der VIF-Zuordnung zum logischen Switch schlägt fehl.
- **Problem 1958041:** BUM-Datenverkehr funktioniert möglicherweise nicht für einen Layer-3-Datenfluss über physische Layer 2-Segmente, wenn der ESX-Hypervisor über mehrere Uplinks verfügt
Wenn alle nachfolgenden Bedingungen zutreffen, kann es vorkommen, dass der BUM-Datenverkehr von Quell-Hypervisoren über logische Router den Ziel-Hypervisor nicht erreicht.
 - ESX verfügt über mehrere Uplinks
 - Quell- und Ziel-VMs sind über logische Router verbunden
 - Quell- und Ziel-Hypervisor befinden sich in unterschiedlichen physischen Segmenten
 - Das logische Zielnetzwerk verwendet die MTEP-Replikation
 Dies tritt auf, wenn das BFD-Modul die Sitzung nicht erstellt hat, d. h., es wurde keine MTEP-Auswahl für das logische Zielnetzwerk vorgenommen.

Behobene Probleme bei Sicherheitsdiensten

- **Problem 1520694:** Unter RHEL 7.1 Kernel 3.10.0-229 und früher kann das FTP-ALG den ausgehandelten Port auf dem Datenkanal nicht öffnen.
Bei einer FTP-Sitzung, bei der sich Client und Server auf VMs auf demselben Hypervisor befinden, öffnet das FTP-ALG (Application Layer Gateway) den ausgehandelten Port für den Datenkanal nicht. Dieses Problem tritt nur unter Red Hat bei RHEL 7.1 Kernel 3.10.0-229 auf. Neuere RHEL-Kernel sind nicht betroffen.
- **Problem 2008882:** Damit Application Discovery korrekt funktioniert, erstellen Sie keine Sicherheitsgruppe, die sich über mehrere Hosts erstreckt.
Wenn eine Sicherheitsgruppe VMs aufweist, die sich über mehrere Hosts erstrecken, schlägt die Application Discovery-Sitzung möglicherweise fehl.

Behobene Probleme beim Load Balancer

- **Problem 1995228:** Gewichtete Round-Robin- und gewichtete Least-Connection-Algorithmen verteilen den Datenverkehr möglicherweise nicht ordnungsgemäß, nachdem eine Konfiguration geändert und neu geladen wurde.

Die Verbindung von Servern geht verloren, wenn eine gewichtete Round-Robin- oder eine gewichtete Least-Connection-Konfiguration geändert und neu geladen wird. Nach dem Verbindungsverlust werden die historischen Verteilungsinformationen des Datenverkehrs nicht beibehalten. Dies führt dazu, dass der Datenverkehr nicht ordnungsgemäß verteilt wird.

- **Problem 2018629: Integritätsprüfungstabelle zeigt für den NS-Gruppenpool nicht den aktualisierten Überwachungstyp an**
Wenn Sie statische und dynamische NS-Gruppenpools mit denselben Mitgliedern mit einem Überwachungstyp erstellen und diesen Überwachungstyp für den dynamischen Pool ändern, wird die Integritätsprüfung des dynamischen Pools nicht in der Integritätsprüfungstabelle angezeigt.
- **Problem 2020372: Die passive Integritätsprüfung berücksichtigt nicht das inaktive Poolmitglied, nachdem die maximale Fehleranzahl erreicht wurde**
Die passive Integritätsprüfung erfordert einen über die Konfiguration hinausgehenden Wert für die Fehleranzahl, um das inaktive Poolmitglied zu berücksichtigen.

Behobene Probleme bei der Lösungsinteroperabilität

- **Problem: 2025624: Splunk-Dashboards bleiben beim Laden hängen, oder die Diagramme auf den Dashboards sind leer**
Splunk ruft die alte Version von *nsx_splunk_app* ab, da die HTML-Vorlage fälschlicherweise auf den vorherigen Pfad des Abfrageskripts verweist. Daher führen die Dashboards alte Abfragen mit Feldern wie *vmw_nsxt_comp*, *vmw_nsxt_subcomp* und *vmw_nsxt_errorcode* aus, die in der neueren Version des Abfrageskripts anders benannt sind. Als Folge geben die Abfragen keine Ergebnisse zurück, und die Dashboards sind leer.

Behobene Probleme bei Betriebs- und Überwachungsdiensten

- **Problem 1957092: NSX Controller-Cluster kann durch einen Fehler beim Laden des Docker-Images nicht initialisiert werden**
Der Befehl `initialize control-cluster` schlägt fehl mit der Fehlermeldung `Control-Cluster-Aktivierung ist abgelaufen`. Versuchen Sie es erneut. Das Syslog enthält darüber hinaus die folgenden Protokollinformationen:

```
<30>1 2017-08-03T22:52:41.258925+00:00 localhost load-zookeeper-image 1183 - -  
grpc: the connection is unavailable. (grpc: Die Verbindung ist nicht verfügbar.)
```

Behobene Upgradeprobleme

- **Problem 1847884: Nehmen Sie keine NSX-T Data Center-bezogenen Änderungen vor, bis der Upgradevorgang für die Management Plane abgeschlossen ist**
Wenn während des Upgrades der Management Plane Änderungen durchgeführt werden, wie etwa das Erstellen, Aktualisieren oder Löschen einer Transportzone, eines Transportknotens oder eines logischen Switches, kann dies zu einer Beschädigung der Management Plane und damit zu Verbindungsfehlern bei NSX Edge, beim Host und beim Datenpfad führen.
- **Problem 2005709: Die Upgrade-Koordinatorseite ist nicht mehr verfügbar, wenn Sie den NSX Manager-FQDN verwenden**
Wenn Sie den NSX Manager-FQDN verwenden, um die NSX Manager-Benutzeroberfläche zu öffnen, wird auf der Upgrade-Koordinatorseite eine Fehlermeldung ähnlich der folgenden angezeigt: Diese Seite ist nur auf dem NSX Manager verfügbar, auf dem der Upgrade-Koordinator ausgeführt wird. Um den Dienst zu aktivieren, führen Sie den Befehl „`set service install-upgrade enabled`“ auf dem NSX Manager aus. Wenn der Dienst `install-upgrade` bereits aktiviert ist, versuchen Sie, ihn mit „`clear service install-upgrade enabled`“ zu deaktivieren, und aktivieren Sie ihn dann erneut.
- **Problem 2022609: Verwaltete Hosts werden im Upgrade-Koordinator als nicht verwaltete Hosts behandelt**
Wenn in einer Umgebung mehr als 128 verwaltete Hosts vorhanden sind, werden die Hosts, die Teil eines Clusters waren, während des Upgrades in der nicht verwalteten ESXi-Gruppe angezeigt.

- Problem 1944731: DHCP-Leases weisen möglicherweise widersprüchliche Datensätze auf, wenn eine große Anzahl an Anforderungen vom ersten NSX Edge, für das ein Upgrade durchgeführt wurde, bedient werden, während für das zweite NSX Edge ein Upgrade durchgeführt wird. Wenn eine große Anzahl an Anforderungen vom ersten NSX Edge, für das ein Upgrade durchgeführt wurde, bedient werden, während für das zweite NSX Edge ein Upgrade durchgeführt wird, weisen die DHCP-Leases möglicherweise widersprüchliche Datensätze auf.

Behobene API-Probleme

- Problem 1619450: Bei der API zur Konfiguration der Abfragefrequenz `GET /api/v1/hpm/features` werden Testinformationen zurückgegeben.
`GET /api/v1/hpm/features` gibt eine Liste aller Funktionen zurück, für die sich die Abfragefrequenz konfigurieren lässt. Diese API gibt einige interne Funktionen, die nur für Tests gelten, zurück. Bis auf zusätzliches Rauschen beeinträchtigt dieser Fehler die Funktionsweise nicht.
- Problem 1781225: Die API `GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/module` funktioniert unter Ubuntu nicht.
Die API `GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules` funktioniert unter ESXi und RHEL, nicht aber unter Ubuntu.
- Problem 1954990: Falscher Status von Umsetzungs-API zurückgegeben.
Wenn Sie eine Umsetzungs-API verwenden, um den Umsetzungsstatus für alle APIs zu überprüfen, die vor einer Grenze ausgeführt werden, kann der Rückgabestatus von der Umsetzungs-API in Bezug auf den tatsächlichen Status irreführend sein. Aufgrund der Komplexität bei der Ausführung der verteilten Firewall innerhalb der Management Plane kann die API der verteilten Firewall hinter die für sie gültige Grenze fallen. Dies führt zu dieser Ungenauigkeit.

Behobene Probleme beim NSX-Container-Plug-In (NCP)

- Problem 2167491: NCP kann nicht gestartet werden, wenn die maximale Anzahl virtueller Server für den NSX-T Load Balancer erreicht ist
In der ConfigMap für NCP können Sie die Größe des NSX-T Load Balancers auf Klein, Mittel oder Groß festlegen. Die maximale Anzahl an virtuellen Servern ist 10 für einen kleinen Load Balancer, 100 für einen mittleren und 1000 für einen großen Load Balancer. Wenn die maximale Anzahl an virtuellen Servern für den Load Balancer erreicht ist, startet NCP nicht. Um festzustellen, ob die maximale Anzahl an virtuellen Servern für den Load Balancer erreicht ist, suchen Sie in der NSX-T Manager-Benutzeroberfläche den Load Balancer (er hat ein Tag mit dem Clusternamen) und zählen Sie die Anzahl der virtuellen Server.
- Problem 2160806: Aktualisieren der TLS-Spezifikation eines aktiven Ingress, wenn NCP nicht läuft, wird nicht unterstützt.
Wenn NCP einer Ingress-Ressource eine externe IP-Adresse zugewiesen hat und Sie die TLS-Spezifikation des Ingress aktualisieren, wenn NCP nicht ausgeführt wird (z. B. durch Entfernen oder Ändern des Parameters `secretName`), erkennt NCP die Änderungen nicht. Wenn NCP wieder ausgeführt wird, ist das Zertifikat, das dem alten Geheimnis entspricht, noch vorhanden und wird nicht gelöscht.

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 bei KVM-Netzwerken](#)

- Bekannte Probleme beim Load Balancer
- Bekannte Probleme bei der Lösungsinteroperabilität
- Bekannte Probleme bei Betriebs- und Überwachungsdiensten
- Bekannte Upgradeprobleme
- Bekannte Probleme mit APIs
- Bekannte Probleme beim NSX Policy Manager
- Bekannte Probleme bei NSX Cloud
- Bekannte Probleme beim NSX-Container-Plug-In (NCP)
- Dokumentationsfehler und -ergänzungen

Allgemeine bekannte Probleme

- **Problem 1842511: Multihop-BFD wird für statische Routen nicht unterstützt**

In NSX-T 2.0 kann BFD (Bidirectional Forwarding Detection, bidirektionale Weiterleitungserkennung) für einen Multihop-BGP-Nachbarn (MH-BGP) aktiviert werden. Eine statische Multihop-Route kann in NSX-T 2.0 nicht mit BFD konfiguriert werden. Nur BGP ist konfigurierbar. Beachten Sie: Wenn Sie einen Multihop-BGP-Nachbarn mit BFD konfiguriert haben und eine entsprechende statische Multihop-Route mit demselben Nexthop als BGP-Nachbarn konfigurieren, hat der BFD-Sitzungsstatus Auswirkungen sowohl auf die BGP-Sitzung wie auf die statische Route.

Problemumgehung: Keine.

- **Problem 1931707: Für die automatische Transportknoten-Funktion müssen alle Hosts im Cluster über dieselbe pNIC-Einrichtung verfügen.**

Wenn die automatische TN-Funktion für ein Cluster aktiviert ist, wird eine Vorlage für einen Transportknoten erstellt, die für alle Hosts in diesem Cluster angewendet wird. Alle pNICs in der Vorlage müssen auf allen Hosts für die Transportknotenkonfiguration frei sein, da andernfalls die Transportknotenkonfiguration auf Hosts fehlschlagen kann, deren pNICS fehlen oder besetzt sind.

Problemumgehung: Wenn die TN-Konfiguration fehlgeschlagen ist, konfigurieren Sie zum Korrigieren den einzelnen Transportknoten neu.

- **Problem 1909703: NSX-Administrator kann neue statische Routen, NAT-Regeln und Ports in einem Router erstellen, der direkt vom Back-End von OpenStack erstellt wurde**
Im Rahmen der RBAC-Funktion in NSX-T 2.0 können Ressourcen, wie z. B. Switches, Router oder Sicherheitsgruppen, die vom OpenStack-Plug-In erstellt wurden, nicht direkt vom NSX-Administrator über die NSX-Benutzeroberfläche/API gelöscht oder geändert werden. Diese Ressourcen können nur durch die APIs, die durch das OpenStack-Plug-In gesendet wurden, geändert/gelöscht werden. Es besteht eine Einschränkung in dieser Funktion. Der NSX-Administrator kann keine von OpenStack erstellten Ressourcen löschen/ändern. Der Admin ist jedoch berechtigt, neue Ressourcen wie statische Routen und NAT-Regeln innerhalb der von OpenStack erstellten vorhandenen Ressourcen zu erstellen.

Problemumgehung: Keine.

- **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 1989407: vIDM-Benutzer mit der Rolle „Enterprise-Administrator“ können den Objektschutz nicht außer Kraft setzen**

Ein vIDM-Benutzer mit der Rolle „Enterprise-Administrator“ kann den Objektschutz nicht außer Kraft setzen und keine Prinzipalidentitäten erstellen oder löschen.

Problemumgehung: Melden Sie sich mit den Administratorrechten an.

- **Problem 2030784: Die Anmeldung beim NSX Manager mit einem Remotebenutzernamen, der ASCII-fremde Zeichen enthält, ist nicht möglich.**

Sie können sich nicht bei der NSX Manager-Appliance als Remotebenutzer mit einem Benutzernamen anmelden, der ASCII-fremde Zeichen enthält.

Problemumgehung: Der Remotebenutzername sollte ASCII-Zeichen enthalten, wenn Sie sich bei der NSX Manager-Appliance anmelden.

ASCII-fremde Zeichen können verwendet werden, wenn der Remotebenutzername mit ASCII-fremden Zeichen auf dem Active Directory-Server eingerichtet ist.

- **Problem 2111047: Anwendungserkennung wird auf VMware vSphere 6.7-Hosts in der Version NSX-T 2.2 nicht unterstützt.**

Die Ausführung von Anwendungserkennung in einer Sicherheitsgruppe mit VMs, die auf einem vSphere 6.7-Host ausgeführt werden, hat zur Folge, dass die Erkennungssitzung fehlschlägt.

Problemumgehung: Keine

- **Problem 2157370: Bei der Konfiguration von L3 Switched Port Analyzer (SPAN) mit Trunkierung verwirft ein spezifischer physischer Switch gespiegelte Pakete**

Bei der Konfiguration von L3 SPAN, einschließlich GRE/ERSPAN mit Trunkierung, werden trunkierte gespiegelte Pakete aufgrund der Richtlinie zu physischen Switches verworfen. Eine mögliche Ursache ist unter Umständen, dass der Port Pakete empfängt, bei denen die Anzahl der Bytes in der Nutzlast nicht gleich dem Typplängenfeld ist.

Problemumgehung: Entfernen Sie die L3 SPAN-Trunkierungskonfiguration.

- **Problem 216992: Gespiegelte Pakete mit der MAC-Zieladresse 02:50:56:56:44:52 von anderen Hosts werden vom vSphere ESXi-Uplink verworfen**

Wenn der Host gespiegelte Pakete mit der MAC-Zieladresse 02:50:56:56:44:52 von anderen Hosts empfängt, verwirft der vSphere ESXi-Uplink diese gespiegelten Pakete.

Problemumgehung: Keine

- **Problem 2174583: Im Assistenten „Erste Schritte“ funktioniert die Schaltfläche „Transportknoten einrichten“ im Microsoft Edge-Browser nicht ordnungsgemäß**
Nachdem Sie im Assistenten „Erste Schritte“ auf die Schaltfläche Transportknoten einrichten geklickt haben, stürzt der Microsoft Edge-Webbrowser ab und ein JavaScript-Fehler wird ausgegeben.

Problemumgehung: Verwenden Sie stattdessen die Browser Firefox oder Google Chrome.

Bekannte Installationsprobleme

- **Problem 1617459: Das Abrufen von Konfigurationsdateien für Schnittstellen wird von der Hostkonfiguration für Ubuntu nicht unterstützt.**
Wenn sich die pNIC-Schnittstelle nicht in der Datei `/etc/network/interfaces` befindet, wird die MTU in der Netzwerk-Konfigurationsdatei nicht korrekt konfiguriert. Aus diesem Grund geht die MTU-Konfiguration auf der Transport-Bridge nach jedem Neustart verloren.

Problemumgehung: Verschieben Sie die pNIC-Schnittstellenkonfiguration in das Verzeichnis `/etc/network/interfaces`.

- **Problem 1906410: Der Versuch, den Host aus der Benutzeroberfläche zu löschen, ohne zuvor den Transportknoten zu löschen, führt dazu, dass der Host in einen inkonsistenten Zustand wechselt**
Der Versuch, den Host aus der Benutzeroberfläche zu löschen, ohne zuvor den Transportknoten zu löschen, führt dazu, dass der Host in einen inkonsistenten Zustand wechselt. Wenn Sie versuchen, den Transportknoten zu löschen, während sich der Host in einem inkonsistenten Zustand befindet, lässt die Benutzeroberfläche das Löschen dieses Hosts nicht zu.

Problemumgehung:

1. Schalten Sie vor dem Löschen des Transportknotens alle auf diesem Transportknoten bereitgestellten Mandanten-VMs aus.
2. Entfernen Sie die Transportzone aus dem Transportknoten.
3. Löschen Sie den Transportknoten.
4. Wenn der Transportknoten erfolgreich gelöscht wurde, löschen Sie den entsprechenden Host.

Wenn die Löschung des Transportknotens fehlschlägt, führen Sie die Schritte im KB-Artikel <https://kb.vmware.com/s/article/52068> aus.

- **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.

- **Problem 2106956: Die Verknüpfung von zwei NSX-Controllern desselben Clusters mit zwei verschiedenen NSX Managern führt zu Problemen wegen nicht definierter Datenpfade.**
Die Verknüpfung von zwei NSX Controllern desselben NSX Controller-Clusters mit zwei verschiedenen NSX Managern führt zu Problemen wegen nicht definierter Datenpfade.

Problemumgehung: Verwenden Sie den CLI-Befehl „detach“ auf dem NSX Manager, um den NSX Controller aus dem NSX Controller-Cluster zu entfernen. Konfigurieren Sie den NSX Controller-Cluster so, dass alle NSX Controller in einem Cluster bei demselben NSX Manager registriert sind.

Weitere Informationen finden Sie im Abschnitt „NSX Controller-Installation und -Cluster“ des NSX-TData CenterInstallationshandbuchs.

- **Problem 2106973: Durch Initialisierung des NSX Controller-Clusters auf allen NSX Controllern wird jeder NSX Controller zu einem NSX Controller-Cluster mit einem Knoten. Dies hat Konnektivitätsprobleme wegen nicht definierter Datenpfade zur Folge.**
Vermeiden Sie die Initialisierung des NSX Controller-Clusters auf allen NSX Controllern, wodurch jeder NSX Controller zu einem NSX Controller-Cluster mit einem Knoten wird, da dies Konnektivitätsprobleme wegen nicht definierter Datenpfade zur Folge hat. Initialisieren Sie den NSX Controller-Cluster lediglich auf dem ersten NSX Controller und verknüpfen Sie die anderen NSX Controller mit dem Cluster, indem Sie den CLI-Befehl `join control-cluster` auf dem ersten NSX Controller ausführen.

Problemumgehung: Konfigurieren Sie den NSX Controller-Cluster neu und folgen Sie dabei den Anweisungen im Abschnitt „NSX Controller-Installation und -Cluster“ des NSX-T Data Center Installationshandbuchs.

- **Problem 2114756:** In bestimmten Fällen werden VIBs nicht entfernt, wenn ein Host aus dem vorbereiteten NSX-T Data Center Cluster entfernt wird

Wenn ein Host vom vorbereiteten NSX-T Data Center Cluster entfernt wird, verbleiben möglicherweise einige VIBs auf dem Host.

Problemumgehung: Deinstallieren Sie VIBs manuell vom Host.

- **Problem 2059414:** Die RHEL LCP-Paket-Installation schlägt aufgrund einer älteren Version von python-gevent RPM fehl

Wenn ein RHEL-Host eine neuere Version von python-gevent RPM enthält, schlägt die RHEL LCP-Paket-Installation fehl, da der NSX-T Data Center RPM eine ältere Version von python-gevent RPM enthält.

Problemumgehung: Installieren Sie das LCP-Paket manuell auf dem RHEL-Host, wenn sich auf dem Host die neueste Version von python-gevent RPM befindet.

Führen Sie die folgenden Schritte aus:

1. Extrahieren Sie das RHEL LCP-Paket.
 2. Navigieren Sie zum LCP-Paket-Ordner.
 3. Löschen Sie die libev-, python-greenlet- und python-gevent-RPMs aus dem LCP-Ordner.
 4. Installieren Sie die verbleibenden RPMs. Siehe das NSX-T Data Center-Installationshandbuch.
- **Problem 2142755:** Die Installation der OVS-Kernel-Module schlägt fehl, je nachdem, welche Unterversion von RHEL 7.4 Kernel-Version ausgeführt wird.

OVS-Kernel-Module lassen sich möglicherweise nicht auf einem RHEL 7.4-Host mit einer Kernel-Unterversion 17.1 oder höher installieren. Der Installationsfehler führt dazu, dass die Datenpfade des Kernels nicht mehr länger funktionieren, wodurch die Appliance-Verwaltungskonsole nicht länger verfügbar ist.

Problemumgehung: Aktualisieren Sie die RHEL 7.4-Kernel-Version. Führen Sie mit Admin-Rechten das Skript `/usr/share/openvswitch/scripts/ovs-kmod-manage.sh` auf dem Host aus und laden Sie die OVS-Kernel-Module neu.

Bekannte Probleme bei NSX Manager

- **Problem 1950583:** Die geplante Sicherung von NSX Manager kann nach einem System-Upgrade auf NSX-T 2.0.0 fehlschlagen.

Die Ausführung der geplanten Sicherung schlägt in manchen NSX-T-Umgebungen nach dem Upgrade von früheren Version von NSX-T auf 2.0.0 fehl. Dieses Problem tritt aufgrund einer Änderung im SSH-Fingerabdruck-Format aus früheren Versionen auf.

Problemumgehung: Konfigurieren Sie die geplante Sicherung neu.

- **Problem 1576112:** Bei KVM-Hypervisoren muss das Gateway manuell konfiguriert werden, wenn sie sich in unterschiedlichen Layer-2-Segmenten befinden.

Wenn Sie bei NSX Manager einen IP-Pool konfigurieren und mit diesem IP-Pool Transportknoten erstellen, zeigen Ubuntu KVM-Boxen keine Route für das Gateway an, das in der IP-Pool-Konfiguration eingerichtet wurde. Dies hat zur Folge, dass der Overlay-Datenverkehr zwischen VMs, die sich auf Hypervisoren in unterschiedlichen L2-Segmenten befinden, fehlschlägt, da der zugrunde liegende Fabric-Host nicht weiß, wie er die Fabric-Knoten in entfernten Remotesegmenten erreichen kann.

Problemumgehung: Fügen Sie eine Route für das Gateway hinzu, damit es den Datenverkehr zu anderen Hypervisoren weiterleiten kann, die sich in anderen Segmenten befinden. Wenn diese Konfiguration nicht manuell erfolgt, schlägt der Overlay-Datenverkehr fehl, da der Fabric-Knoten nicht weiß, wie er die entfernten Remote-Fabric-Knoten erreichen kann.

- **Problem 1710152:** Die Benutzeroberfläche von NSX Manager funktioniert im Kompatibilitätsmodus nicht in Internet Explorer 11.

Problemumgehung: Vergewissern Sie sich unter Extras > Einstellungen der Kompatibilitätsansicht, dass Internet Explorer die Benutzeroberfläche von NSX Manager nicht im Kompatibilitätsmodus anzeigt.

- **Problem 2128476:** Bei einem Skalierungs-Setup mit einer Bestandsliste von mehr als 500 Hosts, 1.000 VMs und 10.000 VIFs kann eine vollständige Synchronisierung nach einem harten Neustart etwa 30 Minuten dauern.

Nach dem Neustart des NSX Managers wird jeder Host mit dem NSX Manager synchronisiert, damit der NSX Manager die aktuellen Daten auf dem Host empfängt. Dies umfasst Informationen zu den auf dem Host vorhandenen VMs und den auf den VMs vorhandenen VIFs. Bei einem Skalierungs-Setup mit einer Bestandsliste von mehr als 500 Hosts, 1.000 VMs und 10.000 VIFs werden für eine vollständige Synchronisierung etwa 30 Minuten benötigt.

Problemumgehung: Warten Sie nach einem harten Neustart darauf, dass die aktuellen Informationen im NSX Manager angezeigt werden.

Verwenden Sie die API `api/v1/fabric/nodes/<nodeid>/status` zur Überprüfung der Eigenschaft „last_sync_time“, die die Uhrzeit der letzten Synchronisierung für einen bestimmten Knoten angibt.

- **Problem 1928376:** Controller-Cluster-Mitglieds-knoten hat fehlerhaften Status nach Wiederherstellung von NSX Manager

Der Controller-Cluster-Mitglieds-knoten kann möglicherweise instabil werden und einen herabgestuften Systemzustand melden, wenn NSX Manager mit einem Sicherungs-Image wiederhergestellt wird, das vor der Trennung dieses Mitglieds-knotens vom Cluster erstellt wurde.

Problemumgehung: Wenn die Cluster-Mitgliedschaft geändert wird, stellen Sie sicher, dass eine neue NSX Manager-Sicherung erstellt wird.

- **Problem 1956088:** Die Änderung der Ansicht der Firewallbenutzeroberfläche bei auf einen Regelsatz angewendetem Filter geht eventuell vor dem Speichern im Manager verloren, wenn die Filter aufgehoben werden

Die Änderung der Ansicht der Firewallbenutzeroberfläche bei auf einen Regelsatz angewendetem Filter geht eventuell vor dem Speichern im Manager verloren, wenn die Filter aufgehoben werden

Problemumgehung: Keine.

- **Problem 1928447:** Hypervisoren mit doppelten virtuellen Tunnel-Endpoint-IP-Adressen werden nicht im Syslog des Management Plane-Knotens protokolliert

Hypervisoren mit doppelten virtuellen Tunnel-Endpoint-IP-Adressen werden nicht im Syslog des Management Plane-Knotens protokolliert. Stellen Sie sicher, dass den virtuellen Tunnel-Endpoints von Hypervisoren und den Uplink-Schnittstellen von NSX Edge-Knoten eindeutige IP-Adressen zugewiesen sind.

Problemumgehung: Keine.

- **Problem 2125725:** Nach der Wiederherstellung umfangreicher Topologiebereitstellungen sind die Suchdaten nicht mehr synchron und mehrere NSX Manager-Seiten reagieren nicht mehr. Nach dem Wiederherstellen von NSX Manager mit umfangreichen Topologiebereitstellungen sind die Suchdaten nicht mehr synchron und auf mehreren NSX Manager-Seiten wird folgende Fehlermeldung angezeigt: `Ein nicht behebbarer Fehler ist aufgetreten.`

Problemumgehung: Führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der NSX Manager-CLI als Administrator an.
2. Starten Sie den Suchdienst neu.

`Dienstsuche neu starten`

Warten Sie mindestens 15 Minuten, während der Suchdienst Datenabweichungen im Hintergrund behebt.

- **Problem 2128361:** CLI-Befehl zum Setzen der Protokollebene des NSX Manager auf den Debug-Modus wird nicht ordnungsgemäß ausgeführt

Bei Verwendung des CLI-Befehls `set service manager logging-level debug` zum Setzen der Protokollebene des NSX Managers auf den Debug-Modus werden keine Debugging-Protokollinformationen gesammelt.

Problemumgehung: Führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der NSX Manager-CLI als Administrator an.
2. Führen Sie den Befehl `st e` aus, um zum Root-Benutzer zu wechseln.
3. Kopieren Sie die Dateien „log4j2.xml.default“ und „log4j2.xml“.

`cp /opt/vmware/proton-tomcat/conf/log4j2.xml.default /opt/vmware/proton-tomcat/conf/log4j2.xml`

4. Ändern Sie den Besitzer der Datei „log4j2.xml“.

`chown uproton:uproton /opt/vmware/proton-tomcat/conf/log4j2.xml`

- **Problem 1964681:** Die Registerkarte Hosts der Manager-Benutzeroberfläche zeigt den Status eines Transportknoten-Host als „Löschvorgang läuft“ an, selbst wenn der Host bereits gelöscht wurde

Auf der Registerkarte Hosts der Registerkarte Fabric > Knoten > Transportknoten wird der Status des Hosts nach dem erfolgreichen Löschen eines Transportknoten-Hosts weiterhin als „Löschvorgang wird ausgeführt“ angezeigt.

Problemumgehung: Aktualisieren Sie den Browser.

- **Problem 2169998:** Das Löschen der Browserdaten, wenn Sie beim NSX Manager angemeldet sind, führt im Chrome-Browser dazu, dass die Manager-Benutzeroberfläche nicht mehr funktioniert

Wenn Sie nach der Anmeldung beim NSX Manager mit dem Chrome-Browser zu den Browsereinstellungen wechseln und alle Browserdaten, einschließlich aller Basisdaten und erweiterten Daten, löschen, verliert der Browser seine Verbindung zum NSX Manager.

Problemumgehung: Löschen Sie die Browserdaten nicht, während Sie bei NSX Manager angemeldet sind.

Bekannte Probleme bei NSX Edge

- **Problem 1765087:** Die Kernel-Schnittstellen, die NSX Edge für die Übertragung von Paketen vom Datenpfad zum Linux-Kernel erstellt, unterstützen nur eine MTU bis 1600. Jumbo Frames werden von Kernel-Schnittstellen zwischen Datenpfad und Kernel nicht unterstützt. BGP-Paketgrößen über 1600 werden abgeschnitten und vom BGP-Dämon verworfen. SPAN-Paketgrößen über 1600 werden abgeschnitten, und das Paketerfassungstool zeigt eine Warnung an. Die Nutzlast wird nicht abgeschnitten und bleibt gültig.

Problemumgehung: Keine.

- **Problem 1738960:** Wenn der NSX Edge-Knoten eines DHCP-Serverprofils durch einen NSX Edge-Knoten von einem anderen Cluster ersetzt wird, ändern sich die IP-Adressen, die der DHCP-Server den VMs zuweist. Dieses Problem wird durch die mangelnde Koordination zwischen dem alten und dem neuen Knoten verursacht.

Problemumgehung: Keine.

- **Problem 1629542:** Wenn für einen einzelnen NSX Edge-Knoten eine Weiterleitungsverzögerung festgelegt wird, wird ein falscher Routingstatus angezeigt. Wenn ein NSX Edge als einzelner NSX Edge-Knoten (nicht in einem HA-Paar) ausgeführt wird, kann die Festlegung einer Weiterleitungsverzögerung zu einem falsch angezeigten Routingstatus führen. Nach der Konfiguration der Weiterleitungsverzögerung wird der Routingstatus fälschlicherweise als **INAKTIV** angezeigt, bis der Weiterleitungstimer abläuft. Wenn die Routerkonvergenz abgeschlossen ist, der Weiterleitungstimer jedoch noch nicht abgelaufen ist, läuft der Süd-Nord-Datenpfad problemlos weiter, selbst wenn der Routingstatus als **INAKTIV** angezeigt wird. Sie können diese Warnung bedenkenlos ignorieren.
- **Problem 1601425:** Das Klonen einer NSX Edge-VM, die bereits beim NSX Manager angemeldet ist, ist nicht möglich. Das Klonen einer NSX Edge-VM wird nicht unterstützt, nachdem sie beim NSX Manager angemeldet wurde. Stattdessen sollten Sie ein neues Image bereitstellen.

Problemumgehung: Keine.

- **Problem 1585575:** Die NSX Edge-Clusterinformationen auf einem Tier-1-Router, der mit einem Tier-0-Router verbunden ist, können nicht bearbeitet werden. Wenn Sie auf einem logischen Tier-1-Router NAT aktiviert haben, müssen Sie einen NSX Edge-Knoten oder ein NSX Edge-Cluster festlegen, bevor Sie den Tier-1-Router mit einem Tier-0-Router verbinden. Die Bearbeitung der NSX Edge-Clusterinformationen auf einem Tier-1-Router, der bereits mit einem Tier-0-Router verbunden ist, wird von NSX nicht unterstützt.

Problemumgehung: Wenn Sie die NSX Edge-Clusterinformationen auf einem Tier-1-Router bearbeiten möchten, der bereits mit einem Tier-0-Router verbunden ist, trennen Sie den Tier-1-Router vom Tier-0-Router, nehmen Sie die Änderungen vor und verbinden Sie die beiden Router erneut.

- **Problem 1955830:** Upgrade von NSX-T 1.1 auf NSX-T 2.0 schlägt fehl, wenn der NSX Edge-Cluster-Name erweiterte ASCII-Zeichen oder Nicht-ASCII-Zeichen enthält. Wenn beim NSX-T 1.1-Setup für den Namen eines NSX Edge-Clusters erweiterte ASCII-Zeichen oder Nicht-ASCII-Zeichen verwendet wurden, schlägt das Upgrade von NSX-T 1.1 auf NSX-T 2.0 mit einer Fehlerendlosschleife fehl.

Problemumgehung: Benennen Sie vor dem Upgrade die NSX Edge-Cluster um und entfernen Sie erweiterte ASCII-Zeichen oder Nicht-ASCII-Zeichen in der NSX-T 1.1-Setup-Instanz.

- **Problem 2122332:** In einigen Fällen funktioniert die SSH-Anmeldung bei einem Bare Metal Edge nicht. Gelegentlich funktioniert die SSH-Anmeldung bei einem Bare Metal Edge nicht.

Problemumgehung: Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum iLO-Treiber. Starten Sie den Edge-SSH-Dienst neu.

- **Problem 2187888:** Das über die NSX Manager-Benutzeroberfläche bereitgestellte NSX Edge verbleibt auf unbestimmte Zeit im Status „Registrierung ausstehend“
Das über die NSX Manager-Benutzeroberfläche bereitgestellte NSX Edge verbleibt auf unbestimmte Zeit im Status „Registrierung ausstehend“. Dieser Zustand führt dazu, dass NSX Edge zur weiteren Konfiguration nicht mehr verfügbar ist.

Problemumgehung: Verwenden Sie CLI zur manuellen Registrierung von NSX Edge mit NSX Manager.

Bekannte Probleme bei logischen Netzwerken

- **Problem 1769922:** Die NSX Controller-Clusterebene zeigt möglicherweise beim vSphere Client die interne IP-Adresse 172.17.0.1 statt der tatsächlichen IP-Adresse an
Bei vSphere-Client wird für NSX Controller statt der tatsächlichen IP-Adresse fälschlicherweise die IP-Adresse 172.17.0.1 angezeigt. Die IP-Adresse für NSX Manager wird korrekt angezeigt.

Problemumgehung: Nicht erforderlich. Dieser kleine Fehler hat keine Auswirkungen auf die Funktionen.

- **Problem 1771626:** Das Ändern der IP-Adresse des NSX Controller-Knotens wird nicht unterstützt

Problemumgehung: Stellen Sie den NSX Controller-Cluster erneut bereit.

- **Problem 1940046:** Wenn dieselbe statische Route in mehreren logischen Tier-1-Routern hinzugefügt und angekündigt wird, schlägt der Ost-West-Datenverkehr fehl
Wenn dieselbe statische Route in mehreren logischen Tier-1-Routern hinzugefügt und angekündigt wird, schlägt der Ost-West-Datenverkehr fehl.

Problemumgehung: Statische Routen sollten nur vom ursprünglichen logischen Tier-1-Router angekündigt werden, wenn sich das Präfix hinter einem verbundenen Netzwerk des verteilten Tier-1-Routers befindet.

- **Problem 1753468:** Nach dem Aktivieren des Spanning Tree Protocols (STP) in einem überbrückten VLAN wird der Bridge-Clusterstatus als „Inaktiv“ angezeigt.
Wenn bei VLANs, die für das Bridging mit LACP-Teaming genutzt werden, STP aktiviert wird, wird der Portkanal des physischen Switches blockiert. Daraufhin wird der Bridge-Cluster auf dem ESX-Host als „Inaktiv“ angezeigt.

Problemumgehung: Deaktivieren Sie STP oder aktivieren Sie BPDU Filter und BPDU Guard.

- **Problem 1753468:** Der logische Tier-O-Router aggregiert die Routen nicht. Stattdessen verteilt er sie individuell neu.
Der logische Tier-O-Router führt keine Routenaggregation für ein Präfix durch, das nicht alle mit ihm verbundenen Sub-Präfixe abdeckt. Stattdessen verteilt der logische Router die Routen separat.

Problemumgehung: Keine.

- **Problem 1536251:** Das Kopieren von VMs von einem ESX-Host auf einen anderen ESX-Host, der mit demselben logischen Switch verbunden ist, wird nicht unterstützt.

Das Layer-2-Netzwerk fällt aus, wenn eine VM von einem ESX kopiert wird und dieselbe VM auf einem anderen ESX-Host angemeldet ist.

Problemumgehung: Nutzen Sie das VM-Klonen, wenn der ESX-Host zum Virtual Center gehört. Wenn Sie eine VM von einem ESX-Host auf einen anderen kopieren, muss die externe ID in der VMX-Datei der VM eindeutig sein, damit das Layer-2-Netzwerk funktioniert.

- **Problem 1747485:** Das Entfernen eines Uplinks von der LAG-Schnittstelle sorgt für einen Ausfall des gesamten BFD-Protokolls und unterbricht die BGP-Routen.

Wenn aus der konfigurierten LAG-Schnittstelle eine Schnittstelle gelöscht wird, kommt es zu einem Ausfall des gesamten BFD-Protokolls und einer Unterbrechung der BGP-Routen mit entsprechender Beeinträchtigung des Datenverkehrs.

Problemumgehung: Keine.

- **Problem 1741929:** Wenn in einer KVM-Umgebung Portspiegelung konfiguriert und Abschneiden aktiviert ist, werden Jumbo-Pakete von der Quelle in Fragmenten gesendet, am Spiegelungsziel jedoch wieder zusammengesetzt.

Problemumgehung: Keine erforderlich, da die erneute Zusammensetzung vom vNIC-Treiber der Ziel-VM durchgeführt wird.

- **Problem 1619838:** Das Ändern einer Transportzonenverbindung eines logischen Routers in ein anderes Set an logischen Switches schlägt mit einem Nichtübereinstimmungsfehler fehl.

Der logische Router unterstützt nur eine einzige Overlay-Transportzone für Downlink-Ports. Daher können Sie eine Transportzonenverbindung zu einem anderen Set an logischen Switches nicht ändern, ohne die vorhandenen Downlink- oder Routerlink-Ports zu löschen.

Problemumgehung: Führen Sie die folgenden Schritte aus.

1. Löschen Sie alle vorhandenen Downlink- oder Routerlink-Ports.
2. Warten Sie, bis das System aktualisiert wurde.
3. Versuchen Sie erneut, die Transportzonenverbindung zu einem anderen Set an logischen Switches zu ändern.

- **Problem 1625360:** Nach dem Einrichten eines logischen Switches zeigt der NSX Controller keine Informationen zu diesem Switch an.

Problemumgehung: Warten Sie nach dem Einrichten des logischen Switches 60 Sekunden, bevor Sie die Informationen beim NSX Controller überprüfen.

- **Problem 1581649:** Nach dem Erstellen und Löschen eines logischen Switches lässt sich der VNI-Pool-Bereich nicht verkleinern.

Das Verkleinern des Bereichs schlägt fehl, da VNIs nicht sofort wieder freigegeben werden, nachdem ein logischer Switch gelöscht wurde. VNIs werden nach sechs Stunden freigegeben. Auf diese Weise soll verhindert werden, dass die VNIs bei der Erstellung eines anderen logischen Switches erneut verwendet werden. Aus diesem Grund können Sie Bereiche erst sechs Stunden nach dem Löschen des logischen Switches verkleinern oder bearbeiten.

Problemumgehung: Warten Sie nach dem Löschen der logischen Switches sechs Stunden, bevor Sie den Bereich bearbeiten, aus dem den logischen Switches VNIs zugeteilt wurden. Alternativ können Sie auch andere Bereiche aus dem VNI-Pool verwenden oder denselben Bereich erneut nutzen, ohne ihn zu verkleinern oder zu löschen.

- **Problem 1516253:** Die Intel 82599-Netzwerkkarten weisen eine Hardwarebegrenzung für den QBRC-Zähler (Queue Bytes Received Counter) auf. Dies führt zu einem Überlauf, wenn insgesamt mehr als 0xFFFFFFFF Bytes empfangen wurden.

Aufgrund dieser Hardwareeinschränkung stimmt im Fall eines Überlaufs die Ausgabe in der Befehlszeile nach der Ausführung des Befehls `get dataplane physical-port stats` nicht mit der tatsächlichen Anzahl überein.

Problemumgehung: Führen Sie den Befehl einmal so aus, dass die Zähler zurückgesetzt werden, und führen Sie ihn dann in kürzeren Abständen erneut aus.

- **Problem 2075246:** Das Verschieben eines logischen Tier-1 Routers von einem logischen Tier-0 Router zu einem anderen Router wird nicht unterstützt.
Das Verschieben eines logischen Ebene-1-Routers von einem logischen Ebene-0-Router zu einem anderen logischen Router führt dazu, dass die Routenverbindung des Downlink-Ports des logischen Ebene-1-Routers getrennt wird.

Problemumgehung: Führen Sie die folgenden Schritte aus:

1. Trennen Sie den logischen Tier-1 Router vom logischen Tier-0 Router.
2. Warten Sie etwa 20 Minuten, bis der logische Tier-1 Router vollständig vom logischen Tier-0 Router getrennt ist.
3. Verbinden Sie den logischen Tier-1 Router mit einem anderen logischen Tier-0 Router.
Die Routenverbindung des Downlink-Ports wird wiederhergestellt.

- **Problem 2077145:** Erzwungenes Löschen des Transportknotens hat in bestimmten Fällen verwaiste Transportknoten zur Folge

Beim Versuch, den Transportknoten mit einem API-Aufruf zwangsweise zu löschen, wenn beispielsweise ein Hardwarefehler vorliegt oder die Hosts nicht mehr abgerufen werden können, wird der Status des Transportknotens in „Verwaist“ geändert.

Problemumgehung: Löschen Sie den Fabric-Knoten mit dem verwaisten Transportknoten.

- **Problem 2099530:** Eine Änderung der VTEP-IP-Adresse des Bridge-Knotens führt zu Ausfällen beim Datenverkehr

Bei einer Änderung der VTEP-IP-Adresse des Bridge-Knotens wird die MAC-Tabelle vom VLAN zum Overlay auf den Remote-Hypervisoren nicht aktualisiert, was zu Datenverkehrsausfällen von bis zu 10 Minuten führt.

Problemumgehung: Initiieren Sie Datenverkehrsänderungen über das VLAN, damit die MAC-Tabelle des Overlays auf den Hypervisoren aktualisiert wird.

- **Problem 2106176:** Die automatische Installation des NSX Controllers stagniert während des Installationsschritts zum Warten auf die Registrierung

Während der automatischen Installation von NSX Controllern mithilfe der NSX Manager-API oder -Benutzeroberfläche stagniert der Fortschritt eines der ausgeführten NSX Controller und wird dauerhaft als Warten auf Registrierung angezeigt.

Problemumgehung: Führen Sie die folgenden Schritte aus:

1. Senden Sie eine API-Anforderung, um nach der mit dem angehaltenen NSX Controller verknüpften VM-ID zu suchen.

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments
```

2. Senden Sie eine API-Anforderung, um den angehaltenen NSX Controller zu löschen.

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments/<Controller id>?action=delete
```

- **Problem 2112459:** Durch Ersetzen eines einzelnen Knotens im Bridge-Cluster kommt es zu

einem Rückgang des Datenverkehrs

Wenn Sie einen einzelnen Knoten im Bridge-Cluster ersetzen, wird der Bridge-Datenverkehr an den alten Knoten geleitet. Dies führt zu einem Rückgang des Datenverkehrs, bis die Weiterleitungseinträge in den Remote-Hypervisoren aktualisiert werden oder veraltet sind.

Problemumgehung: Führen Sie die folgenden Schritte aus:

1. Positionieren Sie den Ersatzknoten im Bridge-Cluster.
 2. Lassen Sie zu, dass HA eingerichtet wird.
 3. Entfernen Sie den alten Knoten.
- **Problem 216992: Die Verwendung der benutzerdefinierten MTU-Einstellung auf logischen Ports führt zu einem Rückgang bei Paketen**

Bei Verwendung einer benutzerdefinierten MTU-Einstellung auf logischen Ports, wie z. B. eines Werts, der dem Uplink-Port des logischen Routers nicht entspricht, oder einer bestimmten Konfiguration der logischen Ebene-0- und Ebene-1-Router, kann es zu einem Rückgang bei Paketen kommen. Die MTU-StandardEinstellung lautet 1500.

Problemumgehung: Verwenden Sie die MTU-StandardEinstellung.

Andernfalls muss die auf verschiedene logische Ports angewendete MTU der folgenden Beziehung entsprechen:

1. Legen Sie die Uplink-MTU des logischen Tier-0 Routers auf 8900 fest.
2. Legen Sie die VTEP-MTU von NSX Edge auf 9000 fest.
3. Legen Sie die VM-MTU auf 8900 fest.

Der logische Tier-0 Router und alle logischen Tier-1 Router, die mit dem Tier-0 Router verbunden sind, müssen auf denselben NSX Edge-Knoten angeordnet sein.

- **Problem 2125514: Nach dem Failover der Schicht-2-Bridge führt der logische Switch auf bestimmten NSX Edge-VMs so lange eine BUM-Replikation jedes einzelnen Pakets durch, bis die MAC-Adresse erneut bekannt ist.**
Nach dem Failover der Schicht-2-Bridge führt der logische Switch auf bestimmten NSX Edge-VMs so lange (etwa 10 Minuten) eine BUM-Replikation jedes einzelnen Pakets durch, bis die MAC-Adresse für den Endpunkt erneut bekannt ist. Das System stellt sich selbst wieder her, nachdem die Endpunkte das nächste ARP erzeugt haben.

Problemumgehung: Keine

- **Problem 2113769: DHCP-Relay wird auf der Schicht-2-Bridge des NSX Edge-VLANs nicht unterstützt**

Die Verbindung eines VLAN-Hosts mit dem VNI des logischen Switches über einen Port der Schicht-2-Bridge auf NSX Edge hat zur Folge, dass der DHCP-Relay-Agent auf dem Port des logischen Routers dem VLAN-Host keine IP-Adresse bereitstellt.

Problemumgehung: Führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie den VLAN-Host manuell.
 2. Verschieben Sie den Port der Schicht-2-Bridge auf den ESXi-Host.
- **Problem 2183549: Bei der Bearbeitung eines zentralen Dienstports kann ein neu erstellter logischer VLAN-Switch nicht angezeigt werden**
Nachdem Sie auf der Manager-Benutzeroberfläche einen zentralen Dienstport und einen logischen VLAN-Switch erstellt haben, können Sie, wenn Sie den zentralen Dienstport bearbeiten, den neu erstellten logischen VLAN-Switch nicht mehr sehen.

Problemumgehung: Verwenden Sie die API, um den Port zu bearbeiten.

- **Problem 2160634: Durch das Ändern der IP-Adresse auf einem Loopback kann die IP-Adresse der Router-ID auf einem Uplink geändert werden.**

Wenn die IP-Adresse auf dem Loopback geändert wird, wählt der NSX Edge die IP-Adresse auf dem Uplink als Router-ID. Die IP-Adresse des Uplinks, die als Router-ID zugewiesen ist, kann nicht geändert werden.

***Auswirkungen auf Kunden*:** 1. Eine erwartete Nebenwirkung der Router-ID ist, dass alle BGP-Sitzungen fluktuieren.
2. Eine reale Auswirkung ist die Änderung der Router-ID, welche das Debuggen des BGP erschweren und zu Verwirrung führen kann.

Problemumgehung: Deaktivieren Sie die BGP-Konfiguration und ändern Sie die IP-Adresse auf dem Loopback.

- **Problem 2186040:** Wenn ein Transportknoten im System nicht unter den Top 250 Uplink-Profilen im System ist, wird das Uplink-Dropdown-Menü der physischen Netzwerkkarten auf der Benutzeroberfläche deaktiviert
Wenn ein Transportknoten im System nicht unter den Top 250 Uplink-Profilen im System ist, wird das Uplink-Dropdown-Menü der physischen Netzwerkkarten auf der Benutzeroberfläche deaktiviert. Das Speichern des Transportknotens führt zum Entfernen des Uplink-Namens vom Transportknoten.

Problemumgehung: Wählen Sie das Uplink-Profil und den Uplink-Namen für diesen Transportknoten erneut aus.

- **Probleme 2106635:** Während der Erstellung statischer Routen führt das Ändern des Admin-Abstands der NULL-Routen dazu, dass die NULL-Einstellung für den nächsten Hop von der Benutzeroberfläche verschwindet
Wenn Sie den nächsten Hop beim Anlegen der statischen Routen auf NULL festlegen und dann den Admin-Abstand der NULL-Routen ändern, verschwindet die NULL-Einstellung des nächsten Hop von der Benutzeroberfläche.

Problemumgehung: Wählen Sie den nächsten Hop erneut aus.

Bekannte Probleme bei Sicherheitsdiensten

- **Problem 1680128:** Die DHCP-Kommunikation zwischen Client und Server ist nicht verschlüsselt.

Problemumgehung: Verwenden Sie IPsec, um die Kommunikation sicherer zu gestalten.

- **Problem 1711221:** IPFIX-Daten werden über das Netzwerk im Klartext übermittelt.
Standardmäßig ist die Option zur Erfassung des IPFIX-Datenflusses deaktiviert.

Problemumgehung: Keine.

- **Problem 1726081:** Geneve-Tunnel-Datenverkehr (UDP) wird in der KVM zurückgewiesen.

Problemumgehung: Führen Sie die folgenden Schritte aus:

Wenn die KVM firewallD nutzt, erstellen Sie mit folgendem Befehl ein Loch in der Firewall:

```
# firewall-cmd --zone=public --permanent --add-port=6081/udp
```

Wenn die KVM IPtables direkt nutzt, erstellen Sie mit folgendem Befehl ein Loch in der Firewall:

```
# iptables -A INPUT -p udp --dport 6081 -j ACCEPT
```

Wenn die KVM UFW nutzt, erstellen Sie mit folgendem Befehl ein Loch in der Firewall:

```
# ufw allow 6081/udp
```

- Die DHCP-Version und die Wiederholpakete erreichen den DHCP-Server nicht, wenn der Client sich in einem anderen Netzwerk befindet und der Routing-Dienst von einer Gast-VM bereitgestellt wird

NSX-T kann nicht feststellen, ob eine virtuelle Maschine als Router dient. Daher ist es möglich, dass Unicast-DHCP-Pakete, die mithilfe einer Router-VM weitergeleitet werden, verworfen werden, wenn der Inhalt des CHADDR-Feldes im Paket nicht der Quell-MAC entspricht. Das CHADDR-Feld enthält einen MAC der DHCP-Client-VM, während die Quell-MAC von der Routerschnittstelle stammt.

Problemumgehung: Wenn sich eine virtuelle Maschine wie ein Router verhält, deaktivieren Sie DHCP-Serverblockierung in den Switch-Sicherheitsprofilen, die für alle VIFs der Router-VM gelten.

- **Problem 2108290: Bare Metal-Server können als Transportknoten keine NSX-T Data Center-Sicherheitsfunktionen gewährleisten**

Bare Metal-Server als neuer Transportknotentyp bieten nicht dasselbe Sicherheitsmaß, z. B. die Mikro-Segmentierung, wie andere Hypervisor-Arbeitslasten. Dies liegt daran, dass keine zuverlässige Trust-Grenze zwischen den Arbeitslasten und dem NSX-Agent durchgesetzt wird.

Problemumgehung: Weisen Sie den Mandanten-VMs aus Sicherheitsgründen keine Root-Berechtigung für Bare Metal-Server zu bzw. führen Sie Anwendungen nicht als Root aus. Wenn Mandanten-VMs über einen solchen Zugriff verfügen, kann ein kompromittiertes Mandantenkonto oder eine kompromittierte Mandantenanwendung möglicherweise bösartige Aktivitäten auf dem Bare Metal-Server durchführen und Probleme in das NSX-T Data Center-Netzwerk einbringen.

- **Problem 2162722: Der Beliebtheitsindex gilt nicht für DROP- oder REJECT-Regeln sowie für statusfreie Regeln**

Wenn der Datenverkehr auf eine Regel mit DROP/REJECT-Aktion oder eine statusfreie Regel trifft, wird die Sitzungszahl für die Regel nicht hochgezählt, da „Sitzung“ nur auf eine zustandsbezogene ALLOW-Regel anwendbar ist. Der Beliebtheitsindex nutzt die Sitzungszahl als Schlüsselparameter. Daher ändert er sich für solche Regeln nicht.

Problemumgehung: Keine

- **Problem 2170512: Der CLI-Befehl zum Abrufen von Firewall-Regeln schlägt fehl, wenn eine Schnittstelle mehr als 1000 Regeln hat**

Wenn eine Schnittstelle mehr als 1000 Regeln hat, wird beim CLI-Befehl `get firewall <VIF_ID> ruleset rules` eine leere Zeichenfolge ausgegeben.

Problemumgehung: Es gibt 2 Problemumgehungen:

- Führen Sie stattdessen den Befehl „`nsxcli -c get firewall <VIF_ID> ruleset rules | json`“ aus.
- Führen Sie den folgenden RAW-CLI-Befehl aus. Es wird der Name einer Datei, die das Ergebnis enthält, angezeigt.

```
ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules
```

Bekannte Probleme bei KVM-Netzwerken

- **Problem 1775916: Die Resolver-API POST `/api/v1/error-resolver?action=resolve_error` behebt keine Fehler, nachdem das Hinzufügen eines RHEL-KVM-Hosts zum Fabric fehlgeschlagen ist.**

Nachdem das Hinzufügen eines RHEL-KVM-Hosts zum Fabric fehlgeschlagen ist und die Benutzeroberfläche von NSX Manager den Installationsstatus als „fehlgeschlagen“ anzeigt, wird die Resolver-API POST `/api/v1/error-resolver?action=resolve_error` zur Fehlerbehebung ausgeführt. Wird der Host jedoch erneut zum Fabric hinzugefügt, werden die folgenden Fehlermeldungen angezeigt:

```
Softwareinstallation auf Host fehlgeschlagen. Un-handled deployment plug-in perform-action.  
Install command failed.
```

Problemumgehung: Führen Sie die folgenden Schritte aus.

1. Entfernen Sie die folgenden Pakete manuell.

```
rpm -e glog-0.3.1-1nn5.x86_64
rpm -e json_spirit-v4.06-1.el6.x86_64
rpm -e kmod-openvswitch-2.6.0.4557686-1.el7.x86_64
rpm -e nicira-ovs-hypervisor-node-2.6.0.4557686-1.x86_64
rpm -e nsx-agent-1.1.0.0.0.4690847-1.el7.x86_64
rpm -e nsx-aggservice-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-cli-1.1.0.0.0.4690892-1.el6.x86_64
rpm -e nsx-da-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-host-1.1.0.0.0.4690932-1.x86_64 rpm -e nsx-
host_node_status_reporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-lldp-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-logical_exporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-mpa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-netcpa-1.1.0.0.0.4690924-1.el7.x86_64 rpm -e nsx-sfhc-
1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-support-bundle-client-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-transport_node_status-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsxa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e openvswitch-2.6.0.4557686-1.x86_64
rpm -e openvswitch-selinux-policy-2.6.0.4557686-1.noarch
rpm -e python-simplejson-3.3.3-1.el7.x86_64
```

Treten beim Ausführen des Befehls `rpm -e` Fehler auf, fügen Sie den Parameter `--noscripts` zum Befehl hinzu.

2. Führen Sie die Resolver-API POST `/api/v1/error-resolver?action=resolve_error` aus.

3. Fügen Sie den KVM-Host erneut zum Fabric hinzu.

- Problem 1602470: Das Lastausgleich-Teaming wird auf KVMs nicht unterstützt.
- Problem 1611154: VMs in einem KVM-Transportknoten können keine VMs in anderen Transportknoten erreichen.

Wenn für VTEPs, die zu unterschiedlichen Netzwerken gehören, mehrere IP-Pools verwendet werden, kann die VM auf dem KVM-Host möglicherweise die VM nicht erreichen, die auf anderen Hosts bereitgestellt ist, welche VTEP-IP-Adressen eines anderen IP-Pools nutzen.

Problemumgehung: Fügen Sie Routen hinzu, sodass der KVM-Transportknoten alle Netzwerke erreichen kann, die für VTEP auf anderen Transportknoten genutzt werden.

Beispiel: Sie verfügen über zwei Netzwerke, 25.10.10.0/24 und 35.10.10.0/24. Der lokale VTEP hat die IP-Adresse 25.10.10.20 mit dem Gateway 25.10.10.1. Mit folgendem Befehl können Sie die Route für ein anderes Netzwerk hinzufügen:

```
ip route add dev nsx-vtep0.0 35.10.10.0/24 via 25.10.10.1
```


- **Problem 1654999: Die Verbindungsnachverfolgung des Underlay-Datenverkehrs verringert den verfügbaren Speicher.**

Wenn Sie eine große Anzahl an Verbindungen zwischen virtuellen Maschinen herstellen, könnten die folgenden Symptome auftreten.

Die Datei `var/log/syslog` oder `/var/log/messages` enthält Einträge, die folgendem Eintrag ähneln:

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950872] net_ratelimit: 239 callbacks suppressed
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950875] nf_conntrack: table full, dropping packet
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.958436] nf_conntrack: table full, dropping packet
```

Dieser Fehler tritt offenbar auf, wenn standardmäßige Firewallregeln festgelegt wurden. Sind keine Firewallregeln konfiguriert, kommt es nicht zu diesem Fehler. (Beispiel: Logische Switches werden zur Firewall-Ausnahmeliste hinzugefügt.)

Hinweis: Die vorgenannten Protokollauszüge sind lediglich Beispiele. Datums- und Zeitangaben sowie Umgebungsvariablen können je nach Umgebung unterschiedlich ausfallen.

Problemumgehung: Fügen Sie eine Firewallregel zur Deaktivierung der Verbindungsnachverfolgung für UDP auf Port 6081 auf Underlay-Geräten hinzu.

Hier ist ein entsprechender Befehl als Beispiel:

```
# iptables -A PREROUTING -t raw -p udp --dport 6081 -j CT --notrack
```

Die Konfiguration sollte die Ausführung beim Startvorgang festlegen. Wenn auf der Plattform auch ein Firewall-Verwaltungstool (Ubuntu: UFW, RHEL: firewallD) aktiviert ist, sollten Sie die entsprechende Regel über dieses Tool konfigurieren. Siehe den zugehörigen Artikel [KB 2145463](#).

- **Problem 2002353: Das Verwenden von Linux Network Manager zum Verwalten der Uplinks eines KVM-Hosts wird nicht unterstützt**

NSX-TData Centerverwaltet alle Netzwerkkarten (NICs) auf KVM-Hosts, die für N-VDS verwendet werden. Ein Konfigurationsfehler tritt auf, wenn der Network Manager ebenfalls für diese Uplinks aktiviert ist.

Problemumgehung: Schließen Sie für Ubuntu-Hosts die für NSX-TData CenterVerwendeten NICs vom Netzwerk Manager aus.

Ändern Sie vor der Aktivierung von NSX-TData Center auf einem Red Hat-Host das NIC-Konfigurationsskript in `/etc/sysconfig/network-scripts` in `NM_CONTROLLED="no"`. Wenn NSX-TData Center bereits für den Host aktiviert wurde, nehmen Sie dieselbe Skriptänderung vor und starten Sie das Netzwerk für den Host neu.

- **Problem 2186045: Bei KVM wird logrotate standardmäßig täglich und nicht minütlich ausgeführt**

Wenn bei KVM die Größe einer Protokolldatei die maximale Dateigröße, die in der größenbasierten Rotationsrichtlinie definiert ist, innerhalb eines Tages überschreitet, wird sie erst zum Tagesende rotiert, wenn logrotate ausgeführt wird. Aus diesem Grund können die Protokolldateien größer als das festgelegte Größenlimit sein.

Problemumgehung: Führen Sie die folgenden Schritte aus:

1. Erstellen Sie ein neues Verzeichnis `/etc/cron.minutes`.
2. Erstellen Sie das Skript `/etc/cron.minutes/logrotate` mit folgendem Inhalt:

```
#!/bin/sh
/usr/sbin/logrotate /etc/logrotate.conf
```

3. Ändern Sie die Berechtigung von `/etc/cron.minutes/logrotate`:

```
chmod 755 /etc/cron.minutes/logrotate
```

4. Fügen Sie `cron.minutes` als ein Eintrag in `/etc/crontab` hinzu:

```
echo "* * * * * root cd / && run-parts --report /etc/cron.minutes"
>>/etc/crontab
```

Bekannte Probleme beim Load Balancer

- **Problem 2010428: Erstellung von Load Balancer-Regeln und Anwendungseinschränkungen**
In der Benutzeroberfläche können Sie eine Load Balancer-Regel nur über einen virtuellen Server erstellen. Mithilfe der REST-API erstellte Load Balancer-Regeln können nicht an den virtuellen Server in der Benutzeroberfläche angehängt werden.

Problemumgehung: Wenn Sie eine Load Balancer-Regel mithilfe der REST-API erstellt haben, hängen Sie diese Load Balancer-Regel mithilfe der REST-API an den virtuellen Server an. Die mithilfe der REST-API erstellten Regeln werden nun im virtuellen Server in der Benutzeroberfläche angezeigt.

- **Problem 2016489: LCP kann das Standardzertifikat nicht konfigurieren, wenn die Angabe des Servernamens ausgewählt wird**

Wenn in der Angabe des Servernamens (Server Name Indication, SNI) mehrere Zertifikat-IDs verwendet werden, sollte die Standardzertifikat-ID zuerst festgelegt werden. Hierdurch wird vermieden, dass LCP das Standardzertifikat ignoriert.

Problemumgehung: Das Standardzertifikat sollte in der SNI-Zertifikatsliste an erster Stelle stehen.

- **Problem 2115545: Wenn eine Load Balancer-Integritätsprüfung aktiviert ist, schlägt eine direkte Verbindung zu den Mitgliedern des Backend-Serverpools unter Umständen fehl**

Wenn ein Load Balancer mit einem logischen Router verbunden ist, kann ein mit dem Downlink des logischen Routers verknüpfter Client nicht mit demselben Protokoll wie die Integritätsprüfung auf die Poolmitglieder zugreifen, wenn die Poolmitglieder über den Uplink des logischen Routers erreichbar sind.

Wenn ein Load Balancer beispielsweise mit einem logischen Router (LR1) verbunden und ICMP-Integritätsprüfung für Poolmitglieder aktiviert ist, die über den LR1-Uplink erreichbar sind, kann ein Client auf dem LR1-Downlink diese Poolmitglieder nicht direkt anpingen. Derselbe Client kann jedoch andere Protokolle, wie z. B. SSH oder HTTP, verwenden, um mit dem Server zu kommunizieren.

Problemumgehung: Verwenden Sie einen anderen Integritätsprüfungstyp auf dem Load Balancer. Verwenden Sie zum Anpingen des Backend-Servers beispielsweise die TCP- oder UDP-Integritätsprüfung anstelle der ICMP-Integritätsprüfung.

- **Problem 2128560: Die Konfiguration von automatischer SNAT-Zuordnung und Integritätsprüfung für den Load Balancer kann zu gelegentlichen Fehlern bei der Integritätsprüfung oder Verbindung führen**

Wenn für denselben Serverpool automatische SNAT-Zuordnung für Load Balancer und Integritätsprüfung (z. B. TCP, HTTP, HTTPS oder UDP) konfiguriert werden, kann es in diesem Serverpool zu gelegentlichen Fehlern bei der Integritätsprüfung oder Verbindung kommen.

Problemumgehung: Verwenden Sie anstelle von automatischer SNAT-Zuordnung die SNAT-IP-Liste.

Hinweis: Im SNAT-IP-Listenmodus angegebene SNAT-IP-Adressen sollten die Uplink-IP-Adresse des logischen Routers nicht enthalten.

Wenn ein Load Balancer beispielsweise mit einem logischen Tier-1 Router (LR1) verbunden ist, sollte der konfigurierte SNAT-IP-Bereich nicht die IP-Adresse des LR1-Uplinks enthalten.

Bekannte Probleme bei der Lösungsinteroperabilität

- **Problem 1588682:** Werden ESXi-Hosts in den Sperrmodus versetzt, wird der Benutzer nsx-user deaktiviert.

Wenn ein ESXi-Host in den Sperrmodus versetzt wird, ist der Benutzer vpxuser der einzige Benutzer, der sich beim Host authentifizieren oder Befehle ausführen kann. NSX-TData Centerstützt sich für die Durchführung aller NSX-TData Center-bezogenen Aufgaben auf dem Host auf einem anderen Benutzer:nsx-user.

Problemumgehung: Verwenden Sie den Sperrmodus nicht. Siehe [Sperrmodus](#) in der vSphere-Dokumentation.

Bekannte Probleme bei Betriebs- und Überwachungsdiensten

- **Problem 1749078:** Nach dem Löschen einer Mandanten-VM auf einem ESXi-Host und des entsprechenden Hosttransportknotens schlägt das Löschen des ESXi-Hosts fehl.

Beim Löschen eines Hostknotens müssen mehrere Objekte neu konfiguriert werden. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.

Problemumgehung: Warten Sie ein paar Minuten und versuchen Sie erneut, den Löschvorgang zu starten. Wiederholen Sie diesen Schritt, wenn nötig.

- **Problem 1761955:** Nach der Registrierung der VM lässt sich die vNIC der VM nicht mit einem logischen NSX-T Data Center Switch verbinden.

Wenn für die Registrierung einer VM auf einem ESXi-Host eine vorhandene VMX-Datei genutzt wird, ignoriert der Registrierungsvorgang folgende vNIC-spezifischen Fehler:

- vNICs, die mit ungültiger Netzwerksicherung konfiguriert wurden
- VIF-Verbindungsfehler für vNICs, die mit einem logischen NSX-T-Switch verbunden sind

Problemumgehung: Führen Sie die folgenden Schritte aus.

1. Erstellen Sie auf einem Standard-vSwitch eine temporäre Portgruppe.
2. Hängen Sie die vNICs mit dem Status „Getrennt“ an die neue Portgruppe an und markieren Sie sie als „Verbunden“.
3. Verbinden Sie die vNICs mit einem gültigen logischen NSX-TData Centerlogischer Switch.

- **Problem 1774858:** In seltenen Fällen wird der NSX Controller-Cluster inaktiv, nachdem er mehrere Tage lang ausgeführt wurde.

Wenn der NSX Controller-Cluster inaktiv wird, gehen die Verbindungen aller Transportknoten und NSX Edge-Knoten mit den NSX Controllern verloren. Änderungen an der Konfiguration sind dann nicht mehr möglich. Der Datenverkehr ist davon jedoch nicht betroffen.

Problemumgehung: Führen Sie die folgenden Schritte aus.

- Beheben Sie Festplatten-Latenzprobleme, sofern welche vorliegen.
- Starten Sie den cluster-mgmt-Dienst auf allen NSX Controllern neu.

- **Problem 1576304:** Der Zähler der verworfenen Bytes ist nicht im Portstatus und im Statistikbericht enthalten.

Wenn Sie über /api/v1/logical-ports/<lport-id>/statistics oder NSX Manager den Portstatus und die Statistiken einsehen, weist der Zähler für verworfene Pakete den Wert 0 auf. Dieser Wert ist nicht korrekt. Unabhängig von der tatsächlichen Anzahl an verworfenen Paketen ist der hier angezeigte Wert immer leer.

Problemumgehung: Keine.

- **Problem 1955822:** Die CSV-Datei mit den Daten zur Lizenznutzung muss neben der tatsächlichen Nutzung auch die CPU- und VM-Berechtigungen enthalten

Bei einer Abfrage des Lizenznutzungsberichts (über API/Benutzeroberfläche) geben die Daten nur die aktuelle Nutzung wieder.

Problemumgehung: Führen Sie über die Benutzeroberfläche oder über die REST-API eine Abfrage der Nutzungsbeschränkungen durch die aktuelle(n) Lizenz(en) durch:

Methode: GET; URL: /api/v1/licenses

- **Problem 2081979: Keine Verbindung des Transport-Knoten-Hosts mit einem beliebigen Controller möglich**

Das NSX-Proxy-Protokoll zeigt Folgendes an. Eine Meldung „Zertifikatvalidierung“ wird erwartet, ist jedoch nicht vorhanden.

```
Die TCP-Verbindung wurde gestartet: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757:1234
```

```
SSL-Handshake wird ausgeführt
```

```
TCP-Verbindung ist hergestellt: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757, local addr: 10.171.0.59:36048, remote addr: 10.171.0.73
```

Problemumgehung: Melden Sie sich bei einem Controller als Administrator an und führen Sie die folgenden Befehle aus:

```
set debug
get mediator forcesync
```

Bekannte Upgradeprobleme

- **Problem 1930705: vMotion-Vorgänge für virtuelle Maschinen, die mit logischen Switches verbunden sind, können während des Upgrades der Management Plane nicht durchgeführt werden**

Während des Upgrades der Management Plane kann für virtuelle Maschinen, die mit einem logischen Switch verbunden sind, kein vMotion-Vorgang durchgeführt werden.

Problemumgehung: Führen Sie den vMotion-Vorgang erst nach dem Abschluss des Upgrades der Management Plane durch.

- **Problem 2005423: In einer vorherigen NSX-T-Version aktualisierte KVM-Knoten werden nicht automatisch zur Verwendung von „balance-tcp“ geändert.**

NSX-T ändert den Bindungsmodus eines aktualisierten KVM-Host-Uplinks nicht automatisch von „active-backup“ in „balance-tcp“.

Problemumgehung: Bearbeiten Sie den Transportknoten, selbst wenn keine Konfigurationsänderungen vorliegen, um die Moduseinstellung zu korrigieren.

- **Problem 2101728: Gelegentlich wird der NSX Edge-Upgrade-Vorgang nach einem erfolgreichen Upgrade einer NSX Edge-Gruppe angehalten**
Das Upgrade einer NSX Edge-Gruppe verlief erfolgreich, das Upgrade der zweiten NSX Edge-Gruppe wurde jedoch angehalten.

Problemumgehung: Klicken Sie auf **Weiter**, um mit dem Upgrade der NSX Edge-Gruppe fortzufahren.

- **Problem 2106257: Änderungen des Workflows zur Annahme in der EULA-API für das Upgrade von NSX-T 2.1 auf NSX-T 2.2**

Die Annahme in der EULA-API sollte nach der Aktualisierung des Upgrade-Koordinators und vor dem Upgrade der vorhandenen Hosts aufgerufen werden.

Problemumgehung: Keine

- **Problem 2108649: Das Upgrade schlägt fehl, wenn in der Partition, für die das Upgrade durchgeführt wird, Dateien oder Verzeichnisse geöffnet sind**

Vermeiden Sie geöffnete Dateien oder Verzeichnisse in der Partition, wie z. B. den zu aktualisierenden NSX Manager oder NSX Controller, da dies das Fehlschlagen des Upgrade-Vorgangs zur Folge hätte.

Problemumgehung: Starten Sie zuerst die Appliance, auf der der Fehler aufgetreten ist, und dann den Upgrade-Vorgang neu.

- **Problem 2116020: Nach dem Upgrade von NSX-T 2.1 auf NSX-T 2.2 werden bestimmte veraltete Ubuntu KVM-Pakete nicht entfernt**

Nach dem Upgrade von NSX-T 2.1 auf NSX-T 2.2 werden die folgenden veralteten Ubuntu KVM-Pakete nicht entfernt.

- nsx-host-node-status-reporter
- nsx-lldp
- nsx-logical-exporter
- nsx-netcpa
- nsx-support-bundle-client
- nsx-transport-node-status-reporter
- nsxa

Problemumgehung: Führen Sie die folgenden Schritte aus.

1. Erstellen Sie eine temporäre Datei im Verzeichnis `/etc/vmware/nsxa/`.

```
cd /etc/vmware/nsxa
touch temp.txt
```

2. Listen Sie alle Verzeichnisse und Dateien des nsxa-Pakets auf.

```
dpkg -L nsxa
/etc/vmware/nsxa# ls
```

3. Entfernen Sie die folgenden Pakete.

- a) `dpkg --purge nsx-lldp`
- b) `dpkg --purge nsx-support-bundle-client`
- c) `dpkg --purge nsx-transport-node-status-reporter`
- d) `dpkg --purge nsx-logical-exporter`
- e) `dpkg --purge nsx-netcpa`
- f) `dpkg --purge nsxa`
- g) `dpkg --purge nsx-host-node-status-reporter`

4. Stellen Sie sicher, dass folgendes Verzeichnis verfügbar ist.

```
/etc/vmware/nsxa/
```

5. Entfernen Sie die Datei „temp.txt“ aus dem Verzeichnis `/etc/vmware/nsxa/`.

```
rm -f temp.txt
```

- **Problem 2164930: Das Upgrade auf der Management Plane ist abgeschlossen, und der Status „Angehalten“ wird angezeigt, wenn eine leere Host-Upgrade-Einheitsgruppe vorhanden ist**
Der allgemeine Status des Upgrades der Management Plane wird als „Angehalten“ angezeigt und der Host-Upgrade-Status ist nicht als 100 % gekennzeichnet, wenn eine leere Host-Upgrade-Einheitsgruppe vorhanden ist.

***Auswirkungen auf Kunden*:** Wenn der Kunde während des Upgrades über leere Hostgruppen verfügt, wird der Upgrade-Status nach dem Abschluss des MP-Upgrades als ANGEHALTEN angezeigt.

Problemumgehung: Löschen Sie vor dem Upgrade der Management Plane die leere Host-Upgrade-Einheitsgruppe.

Wenn die Management Plane aktualisiert wird, löschen Sie die leere Host-Upgrade-Einheitsgruppe. Starten Sie den `Installations-/Upgradedienst` mithilfe der Befehlszeilenschnittstelle (CLI) neu.

- **Problem 2097094: Das Abbrechen eines Upgrade-Paket-Uploads während des Hochladens wird nicht unterstützt**

Sie können das Hochladen nicht abbrechen, während die .mub-Datei des Upgrade-Pakets hochgeladen wird.

Problemumgehung: Warten Sie, bis die .mub-Datei des Upgrade-Pakets hochgeladen ist.

- **Problem 2122242: Beim Upgrade eines Ubuntu-KVM-Hosts von NSX-T 2.1 auf 2.2 oder NSX-T Data Center 2.3 wird das Client-Paket des NSX-Support-Pakets nicht entfernt**
Beim Upgrade eines Ubuntu-KVM-Hosts von Version NSX-T 2.1 auf eine neuere Version (NSX-T 2.2 oder NSX-T Data Center 2.3) ist das Client-Paket des NSX-Support-Pakets weiterhin installiert, obgleich es nicht mehr verwendet wird. Benutzer können sehen, dass das Paket noch immer installiert ist, indem sie Befehle, wie z. B. `/usr/bin/dpkg -l` ausführen.

Problemumgehung: Melden Sie sich als Root an und führen Sie den folgenden Befehl aus, um das Paket manuell zu entfernen:

```
# /usr/bin/dpkg --purge nsx-support-bundle-client
```

- **Problem 2186957: Der ESXi-Host verlässt den Wartungsmodus nach dem Upgrade nicht mehr**
Ein ESXi-Host verlässt den Wartungsmodus nach dem Upgrade nicht mehr, wenn der Cluster nur einen Host hat und wenn der vorherige Versuch des Upgrade-Koordinators, mit dem Host in den Wartungsmodus zu wechseln, fehlgeschlagen ist.

Problemumgehung: Bringen Sie den Host manuell aus dem Wartungsmodus oder stellen Sie sicher, dass der Host in den Wartungsmodus wechseln kann (Sie müssen mindestens 2 Hosts pro Cluster haben).

- **Problem 2166207: Während des Upgrades von NSX-T Data Center 2.2 auf NSX-T Data Center 2.3 mit 500 Hypervisoren bleibt der allgemeine Upgradevorgang unter Umständen auf unbestimmte Zeit im Status IN_PROGRESS (Wird ausgeführt)**
Während des Upgrades von NSX-T Data Center 2.2 auf NSX-T Data Center 2.3 mit 500 Hypervisoren bleibt der allgemeine Upgradevorgang unter Umständen auf unbestimmte Zeit im Status IN_PROGRESS (Wird ausgeführt), nachdem Sie auf Pause geklickt haben, gefolgt von mehreren Aktualisierungen des Webbrowsers.

Problemumgehung: Melden Sie sich bei der NSX-T Data Center CLI im NSX Manager an. Geben Sie den Befehl `install-upgrade`, um den Dienst neu zu starten.

- **Problem 2113681: Wenn ein KVM-Host nicht erreicht werden kann und nach dem NSX Edge-Upgrade ausfällt, versucht der Upgrade Coordinator, ein Update des ausgefallenen Hosts durchzuführen, anstatt mit dem Upgrade der NSX Controller-Knoten fortzufahren**
Nach dem Upgrade des KVM-Hosts und von NSX Edge und nach dem Deinstallieren des neuen RPM und dem Installieren eines alten RPM auf dem Host ist der Host im Upgrade-Koordinator nicht mehr verfügbar. Aus diesem Grund versucht der Upgrade-Koordinator, ein Upgrade des KVM-Hosts vorzunehmen, statt mit dem Upgrade der NSX Controller-Knoten fortzufahren.

Problemumgehung: Aktualisieren Sie die Benutzeroberfläche des Upgrade-Koordinators. Klicken Sie auf die Registerkarte Hosts und versuchen Sie, ein Upgrade des KVM-Hosts durchzuführen.

Sie können das Upgrade des KVM-Hosts auch überspringen, eine Eingabeaufforderung öffnen und den Befehl `curl -i -k -u admin -X POST https://<nsx-manager-ip-address>/api/v1/upgrade/plan?action=continue\&skip=true` eingeben.

Bekannte Probleme mit APIs

- **Problem 1605461: NSX-T-API-Protokolle in Syslog zeigen systeminterne API-Aufrufe an NSX-T protokolliert sowohl von Benutzern ausgelöste API-Aufrufe als auch vom System ausgelöste API-Aufrufe in Syslog**

Die Protokollierung eines API-Aufrufereignisses im Syslog ist kein Nachweis, dass ein Benutzer direkt die NSX-T-API aufgerufen hat. Die Protokolle enthalten API-Aufrufe von NSX Controller und NSX Edge, obwohl diese NSX-T-Appliances keinen öffentlichen API-Dienst aufweisen. Diese privaten API-Dienste werden von anderen NSX-T-Diensten genutzt, beispielsweise von der NSX-T-Befehlszeile.

Problemumgehung: Keine.

- **Problem 1641035: Der REST-Aufruf `POST/hpm/features/<feature-stack-name>action=reset_collection_frequency` zum Zurücksetzen der Erfassungshäufigkeit stellt die Erfassungshäufigkeit für Überschreibstatistiken nicht wieder her.**

Wenn Sie die Erfassungshäufigkeit mit diesem REST-Aufruf auf den Standardwert zurücksetzen möchten, schlägt dieser Versuch fehl.

Problemumgehung: Verwenden Sie `PUT /hpm/features/<feature-stack-name>` und setzen Sie den Wert für die Erfassungshäufigkeit (`collection_frequency`) auf den neuen Wert.

- **Problem 1648571: On-Demand-Anforderungen von Status und Statistiken schlagen unregelmäßig fehl. Der HTTP-Fehlercode ist inkonsistent.**

In bestimmten Situationen schlagen On-Demand-Anforderungen fehl. Manchmal schlagen diese Anforderungen mit einem HTTP 500-Fehler statt einem HTTP 503-Fehler fehl, obwohl die API beim erneuten Versuch erfolgreich ausgeführt wird.

Bei statistischen APIs kann die Zeitüberschreitungsbedingung zu falschen Fehlerprotokollen zur Nachrichtenweiterleitung führen. Dazu kommt es, weil die Antwort erst nach Ablauf des festgelegten Zeitraums erfolgt.

Beispielsweise kann folgender Fehler auftreten: `java.lang.IllegalArgumentException:`

`Unknown message handler for type`

`com.vmware.nsx.management.agg.messaging.AggService$OnDemandStatsResponseMsg.`

Wenn unter der Zeitüberschreitungsbedingung bei Status-APIs die Antwort nach dem festgelegten Zeitraum erfolgt, wird der Zwischenspeicher möglicherweise zu früh aktualisiert.

Problemumgehung: Versuchen Sie erneut, die API-Anforderung auszuführen.

- **Problem 1963850: Die GET-API zeigt Elemente an, die unter Beachtung von Groß- und Kleinschreibung sortiert sind**

Wenn die GET-API Elemente ausgibt, die nach dem Anzeigenamen sortiert sind, wird bei der Sortierung Groß-/Kleinschreibung beachtet.

Problemumgehung: Keine.

- **Problem 2070136: Die API einer verteilten Firewall, die eine große Datenmenge verarbeitet, fällt aus**

Die API einer verteilten Firewall, die mehr als 100 MB Daten erstellen oder aktualisieren muss, fällt aus und es werden der Fehlercode 500 sowie eine Meldung ausgegeben, die auf eine fehlgeschlagene Transaktion verweist. Die API umfasst in der Regel einen Abschnitt mit mehr als 1000 Regeln, wobei jede Regel viele Quellen, Ziele und Objekte umfasst, auf die die entsprechende Regel angewendet wurde.

Problemumgehung: Erstellen oder aktualisieren Sie die Regeln inkrementell.

- **Problem 1895497: Der Load Balancer-Algorithmus SRCDESTMACIPPORT in der API funktioniert nicht**

Das Aufrufen einer API zum Erstellen des Uplink-Profiles eines Transportknotens mit LAG, das über MAC-Quell- und Zieladresse, IP-Adresse und TCP/UDP-Port verfügt, schlägt fehl.

Problemumgehung: Keine

Bekannte Probleme beim NSX Policy Manager

- **Problem 2057616:** Während des Upgrades von NSX Policy Manager von NSX-T 2.1 auf NSX-T 2.2 werden nicht unterstützte NSServices und NSGroups nicht übertragen
Nicht unterstützter NSService vom Typ „Ether“ und nicht unterstützte NSGroups mit MAC Set und Mitgliedschaftskriterien des logischen Ports werden während des Upgrades von NSX Policy Manager von NSX-T 2.1 auf NSX-T 2.2 nicht übertragen.

Problemumgehung: Führen Sie die folgenden Schritte aus.

1. Entfernen und bearbeiten Sie in NSX-T 2.1 NSServices vom Typ „Ether“, falls sie in Kommunikationseinträgen verwendet werden.
 2. Entfernen und bearbeiten Sie NSGroups mit MAC Set und Mitgliedschaftskriterien des logischen Ports, falls sie in Kommunikationseinträgen verwendet werden.
 3. Aktualisieren Sie den NSX Manager von NSX-T 2.1 auf NSX-T 2.2.
 4. Aktualisieren Sie den NSX Policy Manager mithilfe der Befehlszeilenschnittstelle (CLI).
- **Problem 2116117:** Auf der Registerkarte „Topologie“ des NSX Policy Managers werden fehlgeschlagene Datenverbindungen angezeigt
Auf der Registerkarte „Topologie“ des NSX Policy Managers werden Datenverbindungen angezeigt, die fehlgeschlagen sind, weil Gruppen in der Richtliniendomäne VMs enthalten, die auf der nicht unterstützten ESXi 6.7-Version gehostet werden.

Problemumgehung: Keine

- **Problem 2126647:** Gleichzeitige Updates der verteilten Firewall des NSX Policy Managers haben Überschreibungen zur Folge
Wenn zwei Benutzer zur gleichen Zeit den Abschnitt des NSX Policy Managers zur verteilten Firewall bearbeiten, überschreiben die Änderungen des letzten Benutzers die Änderungen des vorherigen Benutzers.

Problemumgehung: Stellen Sie die vom ersten Benutzer durchgeführten Änderungen an der verteilten Firewall wieder her. Nach dem Speichern der Änderungen kann der zweite Benutzer Änderungen vornehmen.

Bekannte Probleme bei NSX Cloud

- **Problem 2112947:** Während des Upgrades der NSX Agents im Cloud Service Manager (CSM) werden bestimmte Instanzen unter Umständen als fehlgeschlagen angezeigt
Während der Aktualisierung der NSX Agents im CSM werden bestimmte Instanzen aufgrund einer inaktiven Benutzeroberfläche unter Umständen als fehlgeschlagen angezeigt.

Problemumgehung: Aktualisieren Sie die Benutzeroberfläche.

- **Problem 2111262:** Während der Bereitstellung von PCG wird unter Umständen folgender Fehler angezeigt: „Gateway-Bereitstellung fehlgeschlagen: [Fehlercode: 60609] Async-Vorgang ist mit folgendem Bereitstellungsstatus fehlgeschlagen: Fehlgeschlagen.“ Oder „Virtuelle Gateway-Maschine mit dem Namen nsx-gw konnte nicht erstellt werden, Gateway-Bereitstellung fehlgeschlagen.“
Hierbei handelt es sich um ein seltenes Ereignis, das aufgrund der Microsoft Azure-Infrastruktur auftritt.

Problemumgehung: Stellen Sie das fehlgeschlagene PCG (Public Cloud Gateway) erneut bereit.

- **Problem 2110728:** Wenn Sie HA verwenden, jedoch den NSX-Agent unter Verwendung nur eines PCG DNS-Namens mit der --gateway-Option auf VMs installiert haben, funktioniert das Failover zum sekundären PCG nicht.
Arbeitslast-VMs können nach einem Failover keine Verbindung zum PCG herstellen. Deshalb kann das PCG keinen logischen Status auf der VM erzwingen/realisieren.

Problemumgehung: Verwenden Sie auf keinen Fall die Option `--gateway`, wenn Sie Agents auf den Arbeitslast-VMs installieren. Verwenden Sie den Wert aus dem Gateway-Bildschirm von VPC oder VNet. Nähere Angaben finden Sie im NSX-T Data Center-Administratorhandbuch unter Installieren des NSX-Agents.

- **Problem 2071374:** Harmlose Fehlermeldungen in Bezug auf „nscd“ werden unter Umständen beim Installieren des NSX-Agents auf bestimmten Linux-VM-Instanzen eingeblendet
Beschreibung: Auf virtuellen Maschinen, auf denen „nscd“ ausgeführt wird, können Fehlermeldungen ähnlich der folgenden angezeigt werden: „Ungültige Kennwortanfrage gesendet, Abbruch.“ Dies geschieht auf VMs, auf denen z. B. Ubuntu 14.04 oder 16.04 ausgeführt wird.

Problemumgehung: Die Meldungen werden aufgrund eines bekannten Fehlers in der Linux-Distribution angezeigt. Diese Meldungen sind harmlos und wirken sich nicht auf die Installation des NSX Agents aus.

- **Problem 2010739:** Beide Public Cloud Gateways (PCGs) werden als „Standby“ angezeigt
Kann das primäre PCG während der Gateway-Einbindung keine Verbindung zum Controller herstellen, werden beide Gateways (primäres und sekundäres Gateway) im Standby-Modus ausgeführt, bis die Verbindung zwischen dem Controller und dem Gateway wiederhergestellt ist.
- **Problem 2121686:** CSM zeigt die Ausnahme „Server konnte die Anforderung nicht authentifizieren“ an.
Dieser Fehler wird möglicherweise in CSM angezeigt, und der Grund dafür ist, dass die Uhrzeit der CSM-Appliance nicht mit derjenigen des Microsoft Azure-Speicherservers oder NTP-Servers übereinstimmt. In diesem Fall gibt Microsoft Azure die Ausnahme „Server konnte die Anforderung nicht authentifizieren“ aus, was missverständlich ist, aber der gleiche Fehler wird in CSM angezeigt.

Problemumgehung: Synchronisieren Sie die Uhrzeit der CSM-Appliance mit derjenigen des NTP-Servers oder des Microsoft Azure-Speicherservers.

- **Problem 2092378:** Bei der PCG-Bereitstellung im HA-Modus werden beide PCGs im Standby-Modus angezeigt, und bei der Cloud-Synchronisierung wird das primäre PCG als aktiv angezeigt.
Nach der HA-Bereitstellung von PCGs über CSM in einem privaten Netzwerk wird auf den bereitgestellten PCGs für bis zu 1 Stunde der Status „Standby/Standby“ oder „Aktiv/Aktiv“ angezeigt. Während dieses Zeitraums sieht es für den Benutzer so aus, als ob ein Problem mit den bereitgestellten PCGs vorläge, und die PCGs weisen möglicherweise einen unklaren Zustand auf, wenn Sie fortfahren.

Problemumgehung: Gehen Sie wie folgt vor:

1. Synchronisieren Sie nach der PCG-Bereitstellung, über die CSM die neuesten Daten abrufen und in CSM anzeigen kann, das Konto über die Benutzeroberfläche neu.
 2. Wenn CSM nach der Neusynchronisierung immer noch PCGs im falschen Zustand anzeigt, überprüfen Sie den PCG-Konnektivitätsstatus in NSX Manager.
 3. Wenn die Verbindung als AKTIV angezeigt wird und die Zustände immer noch falsch sind, führen Sie ein PCG-Debugging durch.
- **Problem 2119726:** Während der PCG-Bereitstellung in einem Microsoft Azure VNet können öffentliche IPs, die zuvor VMs zugeordnet waren, fälschlicherweise als zur Verwendung verfügbar angezeigt werden.
Wenn die VMs, denen zuvor öffentliche IPs zugewiesen waren, nun ausgeschaltet sind, sind diese öffentlichen IPs diesen VMs nicht mehr zugeordnet. Dies liegt daran, dass Microsoft Azure die Zuordnung von öffentlichen IPs zu VMs aufhebt, nachdem diese über einen bestimmten Zeitraum hinweg ausgeschaltet waren. Dieser Zeitraum ist von Microsoft Azure nicht speziell festgelegt.

Problemumgehung: Schalten Sie die PCGs in Ihrem VNet nicht aus. Auf diese Weise wird verhindert, dass die Zuordnung der öffentlichen IP zur Uplink-Schnittstelle des primären PCG aufgehoben wird. Wenn Sie die PCGs ausschalten müssen, stellen Sie sicher, dass die den PCGs jeweils zugeordnete PIP nicht wiederverwendet wird und die PCGs dieselbe PIP erhalten, wenn sie wieder eingeschaltet werden.

- **Problem 2165915: NSX Cloud-Unterstützung für Red Hat Enterprise Linux 7.4 mit kmod.x86_64 0:20-15.el7_4.6**

NSX Cloud unterstützt keine VM-Instanzen, auf denen Red Hat Enterprise Linux 7.4 mit `kmod-20-15.el7_4.6` ausgeführt wird. Die Ursache hierfür ist ein von Red Hat gemeldeter Fehler: https://bugzilla.redhat.com/show_bug?id=1522994.

Problemumgehung: Führen Sie für eine erfolgreiche Installation von NSX Agent ein Update auf die kmod-Version durch, in der dieser Fehler behoben wurde.

- **Problem 2102828: In Microsoft Azure-Bereitstellungen kann es während und nach dem Upgrade von NSX-T 2.2 auf NSX-T Data Center 2.3 so wirken, als ob das Public Cloud Gateway (PCG) nicht funktionieren würde.**

In Microsoft Azure-Bereitstellungen, in denen das System von NSX-T 2.2 auf NSX-T Data Center 2.3 aktualisiert wurde, ist es dem Public Cloud Gateway (PCG) in seltenen Fällen nicht möglich, IP-Adressen für seine Schnittstellen abzurufen. Dies kann während eines Upgrade-Schritts für das PCG geschehen, bei dem der Upgrade-Prozess des PCG „eingefroren“ zu sein scheint. Dieses Problem äußert sich möglicherweise auch als nicht-operatives PCG, wenn der Administrator die PCG-Appliance über das Microsoft Azure-Portal neu startet. Dieses Problem gilt nicht für neue Systeme, auf denen NSX-T Data Center 2.3 zum ersten Mal installiert wird.

Problemumgehung: Starten Sie das PCG, das Sie gerade upgraden, vom Microsoft Azure-Portal aus neu. Verifizieren Sie dann im CSM (Cloud Service Manager), dass der Status der PCGs und der VM-Instanzen gültig ist.

- **Problem 2180531: NSX-Agent wird für Ubuntu 16.04-VM-Instanzen mit Kernel 4.14 und niedriger unterstützt**

NSX Agent wird für Ubuntu 16.04-VM-Instanzen mit Kernel 4.14 und niedriger unterstützt. NSX Agent funktioniert nicht mit der Ubuntu 16.04-VM-Instanz mit Kernel 4.15 und höher.

Es ist keine Umgehung für dieses Problem vorhanden

- **Problem 2170445: Nach dem Upgrade des PCG von NSX-T Data Center 2.2 auf NSX-T Data Center 2.3 wird der PCG HA-Status für Microsoft Azure-PCGs nicht richtig festgelegt**

Nach dem Upgrade von Microsoft Azure PCGs von NSX-T 2.2 auf NSX-T Data Center 2.3 ändert sich der HA-Status der PCGs nicht, wie erwartet, in Aktiv/Standby. Der bevorzugte PCG HA-Status wird als SYNC angezeigt und der nicht bevorzugte PCG HA-Status wird als Aktiv angezeigt. Aus diesem Grund hat beim HA-Failover nach dem Upgrade nur eines der PCGs einen gültigen Status.

Problemumgehung: Aktualisieren Sie in NSX-T 2.2 den MTU-Wert im Uplink-Host-Switch-Profil 1500 des Gateways, bevor Sie die Upgrades im NSX-T Data Center 2.3.

Dies kann entweder über die NSX Manager-Benutzeroberfläche oder über NSX Manager REST-APIs erfolgen.

Führen Sie folgende Schritte über die Benutzeroberfläche aus:

1. Wechseln Sie zu **Fabric > Profile**
2. Wählen Sie das Profil mit dem Namen „PCG-Uplink-HostSwitch-Profile“ und der Beschreibung „PublicCloudGateway Uplink HostSwitch Profile“ aus
3. Klicken Sie auf **EDIT** (Bearbeiten) und ändern Sie den MTU-Wert in 1500. Klicken Sie dann auf **SAVE** (Speichern)
4. Starten Sie das Upgrade von NSX-T 2.2 auf NSX-T Data Center 2.3.

Führen Sie über die REST-API folgende Schritte aus:

1. Rufen Sie unter Verwendung von GET alle Host-Switch-Profile ab:

```
curl -X GET \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles \
  -H 'authorization: Basic <AUTH ID>' \
  -H 'content-type: application/json'
```

2. Identifizieren Sie das Host-Switch-Profil mit dem Namen „PCG-Uplink-HostSwitch-Profile“ und der Beschreibung „PublicCloudGateway Uplink HostSwitch Profile“ und rufen Sie die ID dieses Profils ab:

```
curl -X PUT \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles/<host-switch-profile-id> \
  -H 'authorization: Basic <AUTH ID>' \
  -H 'content-type: application/json' \
  -d '{
    "resource_type": "UplinkHostSwitchProfile",
    "description": "PublicCloudGateway Uplink HostSwitch Profile",
    "id": "<host-switch-profile-id>",
    "display_name": "PCG-Uplink-HostSwitch-Profile",
    "tags": [
      {
        "scope": "CrossCloud",
        "tag": "public-cloud-manager"
      },
      {
        "scope": "PcmId",
        "tag": "<Existing PCM ID>"
      },
      {
        "scope": "EntityType",
        "tag": "default"
      },
      {
        "scope": "CloudScope",
        "tag": "<Existing VPC/VNET name>"
      },
      {
        "scope": "CloudType",
        "tag": "<Existing cloud type>"
      },
      {
        "scope": "CloudVpcId",
        "tag": "<Existing Vpc/Vnet id>"
      }
    ],
    "transport_vlan": 0,
    "teaming": {
      "active_list": [
        {
          "uplink_type": "PNIC",
```

```

        "uplink_name": "uplink-1"
    },
    ],
    "policy": "FAILOVER_ORDER"
},
"overlay_encap": "GENEVE",
"mtu": 1500,
"_revision": 1
}'

```

- **Problem 2174725: Managed VPC/VNet mit bereitgestellten PCGs wird in CSM als nicht verwaltet (unmanaged) angezeigt.**
Managed AWS VPC oder Microsoft Azure VNet mit bereitgestellten PCGs wird in CSM als nicht verwaltet (unmanaged) angezeigt.

Problemumgehung: Nach einem CSM-Neustart sollte das Problem behoben sein.

- **Problem 2162856: Azure PCGs haben einen ungültigen HA-Status (beide aktiv oder beide im Standby-Modus)**
Wenn Sie ein Paar von PCGs in AWS und dann ein weiteres Paar von PCGs für Azure bereitstellen, haben die Azure-APIs einen ungültigen HA-Status (beide aktiv oder beide im Standby-Modus).

Problemumgehung: Aktualisieren Sie den MTU-Wert im Uplink-Host-Switch-Profil, das vom PCM angelegt wurde, auf 1500, bevor Sie mit dem Cross Cloud-Upgrade auf NSX-T Data Center 2.3 beginnen. Führen Sie auf der Manager-Benutzeroberfläche die folgenden Schritte aus:

- Wechseln Sie zu Fabric> Profile.
- Wählen Sie das Profil mit dem Namen „CG-Uplink-HostSwitch-Profile“ und der Beschreibung „PublicCloudGateway Uplink HostSwitch Profile“.
- Klicken Sie auf „EDIT“ (Bearbeiten), ändern Sie den „MTU“-Wert in 1500, und klicken Sie auf „SAVE“ (Speichern).
- Starten Sie den Upgrade-Workflow.
- **Problem 2102321: Einige NSX Cloud-Vorgänge sind während der Traffic-Spitzenzeiten in Microsoft Azure unter Umständen langsam.**
NSX Cloud stützt sich für bestimmte Operationen, wie das Verwalten von VMs oder das Zurückziehen aus dem NSX-Management bzw. das Ergreifen von Quarantänemaßnahmen auf einer VM, auf die Microsoft Azure-ARM-API. Zu Spitzenzeiten erreicht Microsoft Azure bei bestimmten Subskriptionen unter Umständen die API-Grenzwerte. In diesem Fall werden alle API-Anfragen für diese Subskription durch Microsoft Azure gedrosselt. Während dieser Zeit werden die oben erwähnten NSX-Vorgänge unter Umständen nicht rechtzeitig abgeschlossen. Diese Vorgänge werden letztendlich abgeschlossen, wenn Microsoft Azure die Anfragen nicht länger drosselt. PCM-Protokolle im Public Cloud Gateway haben Protokolle wie die folgenden, die darauf verweisen, dass die Drosselung derzeit angewendet wird. *Das Lese-/Schreiblimit pro Stunde des Ressourcenmanagers ist erreicht. Wiederholung in: X Sekunden*

PROBLEMUMGEHUNG: Warten Sie, bis die Microsoft Azure-Drosselung beendet ist.

- **Problem 2189738: Die AWS-Arbeitslast-VMs können nicht erreicht werden, nachdem die Quarantäne-Richtlinie für einen integrierten VPC deaktiviert wurde, wenn sie zuvor aktiviert war.**
Wenn ein PCG mit aktivierter Quarantäne-Richtlinie bereitgestellt wird und Sie diesen Quarantäne-Modus später deaktivieren, kommunizieren einige von NSX verwaltete AWS-Arbeitslast-VMs in diesem VPC nicht mehr mit dem PCG.

Problemumgehung: Fügen Sie die folgenden eingehenden Regeln der NSX Cloud-Sicherheitsgruppe in AWS VPC hinzu: **gw-mgmt-sg**:
Hinweis: Entfernen Sie diese Regeln, wenn Sie die Quarantäne-Richtlinie aus Sicherheitsgründen erneut aktivieren.

TYP	Protokoll	Port	Quelle
CUSTOM-TCP	TCP	8080	VPC-CIDR
CUSTOM-TCP	TCP	5555	VPC-CIDR

- **Problem 2188950:** Der folgende Fehler wird angezeigt: „Keine VNet für die angegebene ID gefunden.“ – wenn die API zum Abrufen einer Liste der PCGs verwendet wird.
Dieser Fehler wird angezeigt, wenn ein Konto, das mit den bereitgestellten PCGs assoziiert ist, vom CSM gelöscht wird.

Problemumgehung: Fügen Sie das Microsoft Azure-Konto dem CSM, auf dem die PCGs bereitgestellt wurden, hinzu.

- **Problem 2191571:** Die PCG-Bereitstellung startet nicht, wenn der öffentliche SSH-Schlüssel für die PCG-Bereitstellung nicht mit einer E-Mail-ID endet.
Ein öffentlicher SSH-Schlüssel muss mit einer E-Mail-ID enden, ansonsten startet die PCG-Bereitstellung nicht und ein Fehler wird angezeigt.

Problemumgehung: Stellen Sie sicher, dass der SSH-Schlüssel mit einer E-Mail-ID endet

- **Problem 2092073:** IPFIX-Vorlagen werden auf Windows-Arbeitslast-VMs nicht ordnungsgemäß empfangen.
Auf Windows-Arbeitslast-VMs werden Vorlagen für logische Switches und Firewall-IPFIX nicht sofort gesendet, wenn der IPFIX-Collector im selben Subnetz wie die virtuelle Maschine konfiguriert ist. Dies liegt daran, dass Windows Socket einen ARP-Eintrag für die IPFIX-Collector-IP-Adresse erwartet, bevor das UDP-Paket gesendet wird. Wenn kein ARP-Eintrag vorhanden ist, werden automatisch alle UDP-Pakete mit Ausnahme des letzten verworfen. Folglich wird das Datenpaket auf dem IPFIX-Collector ohne Vorlageninformationen empfangen.

Problemumgehung: Führen Sie einen der folgenden Schritte aus:

- Fügen Sie mit dem folgenden Befehl einen statischen ARP-Eintrag für den IPFIX-Collector hinzu:

```
netsh interface ipv4 add neighbors "<Interface name>" <collector IP> <physical address of collector>
```

Beispiel:

```
netsh interface ipv4 add neighbors "Ethernet 3" 172.26.15.7 12-34-56-78-9a-bc
```

- Konfigurieren Sie den IPFIX-Collector in einem anderen Subnetz als dem, zu dem die Arbeitslast-VMs gehören.
- **Problem 2210490:** Wenn Sie in CSM ein Proxy-Profil hinzufügen, wird das Kennwort für alle CSM-API-Benutzer, denen eine der folgenden Rollen zugewiesen ist, sichtbar: Prüfer für Cloud-Dienste oder Cloud-Dienstadministrator
Wenn Sie in CSM ein Proxy-Profil erstellen und einen Benutzernamen und ein Kennwort bereitstellen, wird das Kennwort als Antwort auf die folgenden APIs sichtbar, auch wenn Sie selbst das Kennwort in der CSM-Benutzeroberfläche nicht anzeigen können:
 - /csm/proxy-server-profiles
 - /csm/proxy-server-profiles/<profile-id>
- **Problem 2039804:** Die PCG-Bereitstellung schlägt fehl, aber die PCG-Instanz wird in AWS nicht beendet

Wenn Sie ein PCG bereitstellen, die Bereitstellung jedoch fehlschlägt, werden trotzdem weiterhin in AWS VPC eine oder mehrere PCG-Instanzen und in NSX Manager automatisch erstellte Protokolleinträge angezeigt.

Problemumgehung: Löschen Sie die automatisch erstellten NSX Manager-Entitäten und beenden Sie die PCG-Instanz in AWS VPC.

Bekannte Probleme beim NSX-Container-Plug-In (NCP)

- **Änderung bei PAS 2.1.0 CNI**

Aufgrund des CNI-Plug-in-Wechsels in PAS 2.1.0 funktioniert keine NSX-T-Kachel, unabhängig von der Version, mit PAS 2.1.0. Dieses Problem wurde in PAS 2.1.1 behoben.

- **Problem 2118515: In einem umfangreichen Setup benötigt NCP viel Zeit für die Erstellung von Firewalls auf NSX-T**

In einem großen Setup (z. B. 250 Kubernetes-Knoten, 5.000 Pods, 2.500 Netzwerkrichtlinien) kann es einige Minuten dauern, bis NCP die Firewallabschnitte und -regeln in NSX-T erstellt hat.

Problemumgehung: Keine. Nachdem die Firewallabschnitte und -regeln erstellt wurden, sollte die Leistung wieder das normale Niveau erreichen.

- **Problem 2125755: Ein StatefullSet könnte die Netzwerkkonnektivität verlieren, wenn Canary-Updates und gestaffelte fortlaufende Updates durchgeführt werden**

Wenn ein StatefullSet erstellt wurde, bevor NCP auf die aktuelle Version aktualisiert wurde, könnte das StatefullSet die Netzwerkkonnektivität verlieren, wenn Canary-Updates und gestaffelte fortlaufende Updates durchgeführt werden.

Problemumgehung: Erstellen Sie ein StatefullSet, nachdem NCP auf die aktuelle Version aktualisiert wurde.

- **Problem 2131494: NGINX-Kubernetes-Ingress funktioniert weiterhin nach der Änderung der Ingress-Klasse von „nginx“ in „nsx“**

Bei der Erstellung eines NGINX-Kubernetes-Ingress erstellt NGINX Regeln für die Weiterleitung des Datenverkehrs. Wenn Sie die Ingress-Klasse in einen anderen Wert ändern, werden die Regeln von NGINX nicht gelöscht und weiterhin angewendet, selbst wenn Sie den Kubernetes Ingress nach der Änderung der Klasse löschen. Dies ist eine Einschränkung von NGINX.

Problemumgehung: Um die von NGINX erstellten Regeln zu löschen, löschen Sie den Kubernetes-Ingress, wenn der Klassenwert „nginx“ lautet. Erstellen Sie dann den Kubernetes-Ingress neu.

- **Problem 2194845: Die PAS Cloud Foundry-V3-API-Funktion „Mehrere Prozesse pro App“ wird nicht unterstützt**

Wenn Sie die PAS Cloud Foundry V3 API `v3-push` verwenden, um eine App mit mehreren Prozessen zu pushen, erstellt NCP keine logischen Switch-Ports für die Prozesse, mit Ausnahme des Standard-Ports. Das Problem tritt in NCP 2.3.0 und früheren Versionen auf.

Problemumgehung: Keine

- **Problem 2193901: Mehrere PodSelectors oder mehrere NsSelectors für eine einzelne Kubernetes-Netzwerkregel wird nicht unterstützt**

Beim Anwenden mehrerer Selektoren ist nur eingehender Datenverkehr von bestimmten Pods möglich.

Problemumgehung: Verwenden Sie stattdessen MatchLabels mit MatchExpressions in einem einzelnen PodSelector oder NsSelector.

- **Problem 2194646: Das Aktualisieren von Netzwerkrichtlinien, wenn NCP heruntergefahren ist, wird nicht unterstützt**

Wenn Sie eine Netzwerkrichtlinie aktualisieren, wenn NCP heruntergefahren ist, ist das Ziel-IPset für die Netzwerkrichtlinie falsch, wenn NCP wieder hochgefahren wird.

Problemumgehung: Erstellen Sie die Netzwerkrichtlinie neu, wenn NCP hochgefahren ist.

- **Problem 2192489: Nach dem Deaktivieren des „BOSH DNS-Servers“ in der PAS Director-Konfiguration wird der Bosh DNS-Server (169.254.0.2) auch weiterhin in der resolve.conf Datei angezeigt.**

In einer PAS-Umgebung, in der PAS 2.2 ausgeführt wird, wird der Bosh DNS-Server (169.254.0.2) nach dem Deaktivieren des „BOSH DNS-Servers“ in der PAS Director-Konfiguration weiterhin in der in der resolve.conf-Datei des Containers angezeigt. Dadurch nimmt ein Ping-Befehl mit einem vollqualifizierten Domännennamen viel Zeit in Anspruch. Dieses Problem liegt bei PAS 2.1 nicht vor.

Problemumgehung: Keine. Hierbei handelt es sich um ein PAS-Problem.

- **Problem 2194367: Die NSX-T Kachel funktioniert nicht mit PAS-Isolationssegmenten, die ihre eigenen Router bereitstellen**
Die NSX-T Kachel funktioniert nicht mit PAS (Pivotal Application Service)-Isolationssegmenten, die ihre eigenen GoRouter und TCPRouter bereitstellen. Der Grund dafür ist, dass NCP die IP-Adressen der Router-VMs nicht abrufen und keine NSX-Firewall-Regeln erstellen kann, welche einen Datenverkehr von den Routern zu den PAS-App-Containern ermöglichen.

Problemumgehung: Keine.

- **Problem 2199504: Der Anzeigename der vom NCP generierten NSX-T Ressourcen ist auf 80 Zeichen begrenzt**
Wenn das NCP eine NSX-T Ressource für eine Ressource in der Container-Umgebung erstellt, generiert es den Anzeigenamen der NSX-T Ressource durch eine Kombination aus Clusternamen, Namespace oder Projektnamen sowie dem Namen der Ressource in der Container-Umgebung. Wenn der Anzeigename länger als 80 Zeichen ist, wird er auf 80 Zeichen abgeschnitten (trunkiert).

Problemumgehung: Keine

- **Problem 2199778: Mit NSX-T 2.2 werden Ingress, Dienste und Secrets mit Namen, die länger sind als 65 Zeichen, nicht unterstützt**
Wenn `use_native_loadbalancer` bei NSX-T 2.2 auf `True` (Wahr) eingestellt ist, dürfen die Namen des eingehenden Datenverkehrs (Ingress), der Secrets und Dienste, auf die vom eingehenden Datenverkehr (Ingress) und Diensten vom Typ LoadBalancer verwiesen wird, max. 65 Zeichen lang sein. Andernfalls funktionieren der eingehende Datenverkehr (Ingress) oder der Dienst nicht ordnungsgemäß.

Problemumgehung: Geben Sie beim Konfigurieren eines eingehenden Datenverkehrs (Ingress), eines Secrets oder Dienstes einen Namen mit max. 65 Zeichen ein.

- **Problem 2065750: Das Installieren des NSX-T CNI-Pakets schlägt mit einem Dateikonflikt fehl**
Wenn in einer Umgebung mit RHEL, in der Kubernetes installiert ist, das NSX-T CNI-Paket mit den Befehlen `yum localinstall` oder `RPM-i` installiert wird, wird ein Fehler angezeigt, der auf einen Konflikt mit einer Datei aus dem Kubernetes-Cni-Paket verweist.

Problemumgehung: Installieren Sie das NSX-T CNI-Paket mit dem Befehl `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm`.

- **Für einen Kubernetes-Dienst des Typs „ClusterIP“ wird die Client-IP-basierte Sitzungsaffinität nicht unterstützt**
NCP unterstützt keine Client-IP-basierte Sitzungsaffinität für einen Kubernetes-Dienst des Typs „ClusterIP“.

Problemumgehung: Keine

- **Für einen Kubernetes-Dienst des Typs „ClusterIP“ wird das Hairpin-Modus-Flag nicht unterstützt**
NCP unterstützt das Hairpin-Modus-Flag für einen Kubernetes-Dienst des Typs „ClusterIP“ nicht.

Problemumgehung: Keine

Dokumentationsfehler und -ergänzungen

- **Problem 1372211: Zwei Schnittstellen im selben Subnetz**

Tunnel-Datenverkehr kann zur Verwaltungsschnittstelle gelangen, wenn sich der Tunnelendpunkt im selben Subnetz befindet wie die Verwaltungsschnittstelle. Das kann passieren, da getunnelte Pakete die Verwaltungsschnittstelle passieren können. Stellen Sie sicher, dass sich die Verwaltungsschnittstellen in einem anderen Subnetz befinden als die Tunnelendpunktschnittstellen.

Copyright © 2022 VMware, Inc. Alle Rechte vorbehalten.