

# Versionshinweise für VMware NSX-T Data Center 2.4.2

VMware NSX-T Data Center 2.4.2 | 8. August 2019 | Build 14269501

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

## Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

- [Kompatibilität und Systemvoraussetzungen](#)
- [API und CLI-Ressourcen](#)
- [Revisionsverlauf](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

## Kompatibilität und Systemvoraussetzungen

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

## API und CLI-Ressourcen

Informationen zur Verwendung der NSX-T Data Center-APIs oder -CLIs für die Automation finden Sie unter [code.vmware.com](https://code.vmware.com).

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

## Revisionsverlauf der Dokumente

8. August 2019. Erste Auflage.

23. August 2019. Zweite Auflage. Die bekannten Probleme 2362688 und 2395334 wurden hinzugefügt.

12. November 2019. Dritte Auflage. Problem 2295470 (behoben in 2.4.1) wurde entfernt.

## Behobene Probleme

- **Behobenes Problem 2387470** – Ein Core-Speicherabbild (PSOD) kann auf dem Host während dem Abruf von ALG-Informationen ausgelöst werden.  
Bei einem für NSX-T vorbereiteten ESXi-Host kann bei der Übertragung von ALG-Datenverkehr bei der Ausführung des CLI-Befehls „vsipioctl getalginfo -f“ ein Core-Speicherabbild (PSOD) auftreten.
- **Behobenes Problem 2391093** – NSX-T-Host kann die Verwaltungsnetzwerkonnktivität verlieren, wenn alle pNICs auf N-VDS migriert werden.

Das Problem entsteht bei der wiederholten Hostmigration, bei der alle pNICs im N-VDS entfernt werden, für den vmk0 konfiguriert ist. Bei der ersten Hostmigration wurden alle pNICs und vmk0 in den N-VDS migriert, danach schlug dies aber fehl. Wenn Sie die Migration erneut durchführen, werden alle pNICs aus dem N-VDS entfernt. Dadurch können Benutzer nicht über das Netzwerk auf den Host zugreifen. Außerdem verlieren alle VMs im Host die Netzwerkkonnektivität, wodurch ihre Dienste nicht erreichbar sind.

- **Behobenes Problem 2392093 – Datenverkehr sinkt aufgrund von RPF-Check, wenn SNAT und DNAT auf TO konfiguriert sind.**  
Die RPF-Prüfung kann zu einem verworfenen Datenverkehr führen, wenn der Datenverkehr über einen TO-Downlink angeheftet wird und sich die Tier0- und Tier1-Router bei der Konfiguration der SNATs und DNATs auf demselben Edge-Knoten befinden.
- **Behobenes Problem 2392201 – CBM-Prozess stürzt wiederholt aufgrund der Überfrachtung des Arbeitsspeichers durch den CBM-Prozess ab.**  
Die Datenbankkomprimierung bei CSM- und CBM-Prozessen auf der Cloud Service Manager-Appliance schlägt fehl. Infolgedessen führt die Überfrachtung des Arbeitsspeichers zu einem wiederholten Absturz des CBM-Prozesses.
- **Behobenes Problem 2382619 – VMware Identity Manager-Benutzer können auf dem NSX Manager Dashboard nicht auf die Richtlinienseiten zugreifen.**  
Benutzer mit Rollen, denen Gruppenberechtigungen in VMware Identity Manager zugewiesen sind, können nicht auf Richtlinienseiten im NSX Manager Dashboard zugreifen. Berechtigungen aus Gruppenzuweisungen werden ignoriert.
- **Behobenes Problem 2382620 – bei der NSX Edge-Appliance tritt ein Arbeitsspeicherverlust auf, was zu einem Absturz/Neustart des Prozesses führt.**  
Während der Konfiguration mit großer Skalierung führt der Versuch, die Router-Konfiguration abzurufen, unter anderem zu folgender Fehlermeldung: „Es ist ein unerwarteter Fehler aufgetreten: Der Data Plane-Dienst ist fehlgeschlagen oder ist deaktiviert“. Über einen längeren Zeitraum erfolgt beim Edge-Data-Plane-Prozess ein Absturz und Neustart/Verarbeitungs-Dump. Jedes Mal, wenn eine Regelsuche ausgeführt wurde, wurde ein Arbeitsspeicherverlust erkannt. Beim Löschen des Flow-Caches wird die VIF-Schnittstelle nicht entfernt, was zu einem Stau im Arbeitsspeicher führt.
- **Behobenes Problem 2382628 – Bei einem ESXi-Host kann bei der Übermittlung des ALG-Datenverkehrs ein PSOD auftreten.**  
Nach Ausführung des Datenverkehrs über einige Tage stürzt der ESXi ab (PSOD). Vor dem Absturz wurden keine anderen Symptome beobachtet. Das Problem wurde schließlich im ALG-Datenverkehr (FTP, Sunrpc, Oracle, Dcerpc, TFTP) identifiziert. Der nicht aufgelöste Inkrementindikator führte zu Race-Bedingungen, wodurch die ALG-Struktur beschädigt wurde.
- **Behobenes Problem 2387486 – BGPD-Prozess auf NSX-T EDGE kann 100 % der CPU verbrauchen, wenn mehrere VTYSH-Sitzungen vorliegen.**  
Der BGPD-Prozess auf NSX-T EDGE kann 100 % der CPU verbrauchen, wenn mehrere offene Sitzungen mit VTYSH vorhanden sind. Wenn der BGP-Prozess nicht neu gestartet wird, verbraucht er weiterhin 100 % der CPU und kann zu umfangreichen Problemen führen.
- **Behobenes Problem 2392089 – NAT-Regeln wurden für den Datenverkehr über den VERKNÜPFTEN Port ignoriert.**  
NAT-Dienste sind nicht auf dem Porttyp des VERKNÜPFTEN Routers aktiviert, der die logischen Tier-0 und Tier-1 Router verbindet.
- **Behobenes Problem 2382625 – Arbeitsspeicherverlust beim Load Balancer nach der Neukonfiguration.**  
Der NSX Load Balancer kann bei aufeinanderfolgenden/sich wiederholenden Konfigurationsereignissen Arbeitsspeicher verlieren, was zu einem Core-Speicherabbild des nginx-Prozesses führt.

# Bekannte Probleme

Die bekannten Probleme gliedern sich in folgende Gruppen.

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

## Allgemeine bekannte Probleme

- **Problem 2389109 – BGP/Routing funktioniert nicht auf TO-SR, wenn der Edge-Hostname mit einer Zahl beginnt.**  
BGP/Routing funktioniert nicht auf TO-SR, wenn der Edge-Hostname mit einer Zahl beginnt und die Konfiguration nicht an den Routing-Stack weitergeleitet wird. Dies ist eine bekannte Einschränkung.

Problemumgehung: Verwenden Sie die CLI, um den Hostnamen zu ändern, damit er nicht mehr mit einer Zahl beginnt. Aktivieren und deaktivieren Sie den Wartungsmodus auf dem Edge-Knoten, um die Änderung anzuwenden.

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

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

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

Problemumgehung:

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

- **Problem 2256709: Eine Instant Clone-VM oder eine aus einem Snapshot wiederhergestellte VM verliert während vMotion kurzzeitig den AV-Schutz**  
Der Snapshot einer VM wird wiederhergestellt, und die VM wird auf einen anderen Host migriert. Die Partnerkonsole zeigt keinen AV-Schutz für die migrierte Instant Clone-VM an. Es tritt ein kurzzeitiger Verlust des AV-Schutzes auf.

Problemumgehung: Keine.

- **Problem 2261431: Abhängig von den anderen Bereitstellungsparametern ist eine gefilterte Liste von Datenspeichern erforderlich**  
Entsprechender Fehler wird auf der Benutzeroberfläche angezeigt, wenn die falsche Option ausgewählt wurde. Der Kunde kann zur Behebung dieses Fehlers diese Bereitstellung löschen und eine neue erstellen.

Problemumgehung: Wählen Sie einen gemeinsam genutzten Datenspeicher aus, wenn Sie eine geclusterte Bereitstellung erstellen.

- **Problem 2274988: Dienstketten unterstützen aufeinander folgende Dienstprofile vom selben Dienst nicht**

Der Datenverkehr durchläuft keine Dienstkette und wird immer dann verworfen, wenn die Kette zwei aufeinander folgende und zum selben Dienst gehörende Dienstprofile aufweist.

Problemumgehung: Fügen Sie ein Dienstprofil von einem anderen Dienst hinzu, um sicherzustellen, dass keine zwei aufeinander folgenden Dienstprofile zum selben Dienst gehören. Definieren Sie alternativ dazu ein drittes Dienstprofil, das dieselben Vorgänge der ursprünglichen zwei Dienstprofile verkettet durchführt. Verwenden Sie dann dieses dritte Profil allein in der Dienstkette.

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

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

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

Problemumgehung: Keine.

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

Problemumgehung:

1. Erstellen Sie ein Zertifikat mit privatem Schlüssel. Geben Sie bei entsprechender Aufforderung keine neue Passphrase ein und drücken Sie stattdessen die Eingabetaste.
2. Wählen Sie „Zertifikat importieren“ und wählen Sie anschließend die Zertifikatsdatei und die Privatschlüsseldatei aus.

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

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

- **Problem 2277742: Der Aufruf von „PUT https://<MGR\_IP>/api/v1/configs/management“ mit einem Anforderungstext, in dem „publish\_fqdns“ auf „true“ festgelegt ist, kann fehlschlagen, wenn die NSX-T Manager-Appliance mit einem vollqualifizierten Domännennamen (FQDN) anstatt nur mit einem Hostnamen konfiguriert ist**  
„PUT https://<MGR\_IP>/api/v1/configs/management“ kann nicht aufgerufen werden, wenn ein FQDN konfiguriert ist.

Problemumgehung: Stellen Sie den NSX Manager mit einem Hostnamen anstatt mit einem FQDN bereit.

- **Problem 2279249: Eine Instant Clone-VM verliert während vMotion kurzzeitig den AV-Schutz**  
Von einem Host zu einem anderen migrierte Instant Clone-VM. Unmittelbar nach der Migration bleibt eine eicar-Datei auf der VM zurück. Kurzzeitiger Verlust des AV-Schutzes.

Problemumgehung: Keine.

- **Problem 2292116: IPFIX L2-Funktion „Angewendet auf“ mit CIDR-basierter Gruppe von IP-Adressen, die nicht auf der Benutzeroberfläche aufgeführt werden, wenn die Gruppe über die Seite „IPFIX L2“ erstellt wird**

Wenn Sie versuchen, über das Dialogfeld „Angewendet auf“ eine Gruppe von IP-Adressen zu erstellen, und im Dialogfeld „Mitglieder festlegen“ eine falsche IP-Adresse oder CIDR eingeben, werden diese Mitglieder nicht unter den Gruppen aufgeführt. Sie müssen diese Gruppe erneut bearbeiten, um gültige IP-Adressen einzugeben.

Problemumgehung: Wechseln Sie zur Seite mit der Auflistung der Gruppen und fügen Sie IP-Adressen in der betreffenden Gruppe hinzu. Danach kann das Auffüllen der Gruppe im Dialogfeld „Angewendet auf“ beginnen.

- **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 2268406: Im Dialogfeld „Tag-Anker“ werden nicht alle Tags angezeigt, wenn die maximale Anzahl der Tags hinzugefügt wird.**  
Im Dialogfeld „Tag-Anker“ werden nicht alle Tags angezeigt, wenn die maximale Anzahl der Tags hinzugefügt wird, und es ist weder eine Größenanpassung noch ein Bildlauf möglich. Der Benutzer kann auf der Seite „Übersicht“ jedoch weiterhin alle Tags anzeigen. Es gehen keine Daten verloren.

Problemumgehung: Zeigen Sie die Tags stattdessen auf der Seite „Übersicht“ an.

- **Problem 2310650: Für die Schnittstelle wird die Fehlermeldung „Zeitüberschreitung bei Anforderung“ angezeigt.**  
Mehrere Seiten auf der Schnittstelle zeigen die folgende Meldung an: „Zeitüberschreitung bei Anforderung. Dies kann der Fall sein, wenn das System ausgelastet ist oder nur wenige Ressourcen frei sind.“

Problemumgehung: Melden Sie sich mithilfe von SSH bei der NSX Manager-VM an und führen Sie den CLI-Befehl „start search resync manager“ aus.

- **Problem 2320529: Nach dem Hinzufügen von Drittanbieter-VMs für neu hinzugefügte Datenspeicher wird die Fehlermeldung „Dienstbereitstellung kann nicht auf Speicher zugreifen“ angezeigt.**  
Nach dem Hinzufügen von Drittanbieter-VMs für neu hinzugefügte Datenspeicher wird die Fehlermeldung „Dienstbereitstellung kann nicht auf Speicher zugreifen“ angezeigt, obwohl alle Hosts im Cluster auf den Speicher zugreifen können. Dieser Fehlerstatus bleibt bis zu dreißig Minuten lang bestehen.

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

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

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

- **Problem 2320855: Neues VM-Sicherheits-Tag wird nicht erstellt, wenn der Benutzer nicht auf die Schaltfläche „Hinzufügen/Prüfen“ klickt.**

Schnittstellenproblem. Wenn ein Benutzer ein neues Sicherheits-Tag zu einem Richtlinienobjekt oder einer Bestandsliste hinzufügt und auf **Speichern** klickt, ohne zuerst neben dem Feld mit dem Tag-Geltungsbereich-Paar auf die Schaltfläche Hinzufügen/Prüfen zu klicken, wird das neue Tag-Paar nicht erstellt.

Problemumgehung: Klicken Sie auf die Schaltfläche Hinzufügen/Prüfen, bevor Sie auf **Speichern** klicken.

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

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

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

- **Problem 2334442: Benutzer verfügt nicht über die Berechtigung zum Bearbeiten oder Löschen von erstellten Objekten, nachdem der Admin-Benutzer umbenannt wurde.**

Der Benutzer verfügt nicht über die Berechtigung zum Bearbeiten oder Löschen von erstellten Objekten, nachdem der Admin-Benutzer umbenannt wird. Admin-/Auditor-Benutzer können nicht umbenannt werden.

Problemumgehung: Starten Sie die Richtlinie nach der Umbenennung neu, indem Sie den Befehl „Service service nsx-policy-manager restart“ ausgeben.

- **Problem 2261818: Von eBGP-Nachbarn erlernte Routen werden an denselben Nachbarn zurückgegeben.**

Durch das Aktivieren von BGP-Debug-Protokollen werden Pakete angezeigt, die erneut empfangen werden, und das Paket wird mit einer Fehlermeldung verworfen. Der BGP-Prozess nutzt zusätzliche CPU-Ressourcen, um die an Peers gesendeten Updatemeldungen zu verwerfen. Wenn viele Routen und Peers vorhanden sind, kann dies Auswirkungen auf die Routenkonvergenz haben.

Problemumgehung: Keine.

- **Problem 2390624 – Die Antiaffinitätsregel verhindert die Service-VM von vMotion, wenn sich der Host im Wartungsmodus befindet.**

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

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

- **Problem 1957059:** Das Aufheben der Hostvorbereitung schlägt fehl, wenn dabei dem Cluster ein Host mit vorhandenen VIBs hinzugefügt wird  
Wenn die VIBs vor dem Hinzufügen der Hosts zum Cluster nicht vollständig entfernt wurden, kann die Hostvorbereitung nicht aufgehoben werden.

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

### Bekannte Probleme bei NSX Manager

- **Problem 2282798:** Die Hostregistrierung schlägt möglicherweise fehl, wenn zu viele Anforderungen/Hosts gleichzeitig versuchen, sich bei NSX Manager zu registrieren. Dieses Problem versetzt den Fabric-Knoten in den Fehlerzustand. Der API-Aufruf des Fabric-Knotenstatus zeigt an, dass der Client noch nicht auf Taktsignale geantwortet hat. Außerdem ist die Datei `/etc/vmware/nsx-mpa/mpaconfig.json` auf dem Host leer.

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

1. Nutzen Sie die Fehlerbehebung:
2. Löschen Sie den FN aus NSX.
3. Fügen Sie den FN mit dem CLI-Befehl „join management-plane“ manuell erneut hinzu.

### Bekannte Probleme bei NSX Edge

- **Problem 2283559:** Die MP-APIs „/routing-table“ und „/forwarding-table“ geben einen Fehler zurück, wenn der Edge mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB aufweist

Wenn der Edge mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB aufweist, nimmt die Anforderung von MP an den Edge mehr als 10 Sekunden in Anspruch, und dies führt zu einer Zeitüberschreitung. Dies ist eine schreibgeschützte API und wirkt sich nur dann aus, wenn die mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB mithilfe der API/UI heruntergeladen werden müssen.

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

- Diese APIs unterstützen Filteroptionen, die auf Netzwerkpräfixen oder Routentypen beruhen. Verwenden Sie diese Optionen zum Herunterladen der gewünschten Routen.
- Wenn die gesamte RIB-/FIB-Tabelle erforderlich ist, ist eine CLI-Unterstützung erforderlich, und in diesem Fall tritt keine Zeitüberschreitung auf.
- **Problem 2204932:** Das Konfigurieren von BGP-Peering kann die HA-Failover-Wiederherstellung verzögern.  
Wenn Dynamic-BGP-Peering auf Routern konfiguriert ist, die eine Peer-Beziehung mit den TO-Edges besitzen, und auf den Edges (Aktiv/Standby-Modus) ein Failover-Ereignis auftritt, kann die BGP-Nachbarschaft bis zu 120 Sekunden dauern.

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

- **Problem 2285650:** BGP-Routentabellen werden mit unerwünschten Routen gefüllt.  
Wenn in der BGP-Konfiguration die Option „allowas-in“ aktiviert ist, werden von Edge-Knoten angekündigte Routen zurückerhalten und in der BGP-Routentabelle installiert. Dies führt zu übermäßigem Arbeitsspeicherverbrauch und übermäßigem Routing-Berechnungen. Wenn für die überschüssigen Routen eine höhere lokale Einstellung konfiguriert ist, kann diese auf einigen Routern, die mit redundanten Routen gefüllt werden, zu einer Weiterleitungsschleife führen.

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

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

## Bekannte Probleme bei logischen Netzwerken

- **Problem 2243415:** Der Kunde kann den EPP-Dienst mithilfe des logischen Switches (als Verwaltungsnetzwerk) nicht bereitstellen

Auf dem EPP-Bereitstellungsbildschirm kann der Benutzer im Steuerelement für die Netzwerkauswahl keinen logischen Switch sehen. Wenn die API direkt mit dem als Verwaltungsnetzwerk erwähnten logischen Switch verwendet wird, wird dem Benutzer der folgende Fehler angezeigt: „Dienstbereitstellung kann nicht auf angegebenes Netzwerk zugreifen.“

**Problemumgehung:** Führen Sie die Bereitstellung mit einem anderen Switch-Typ wie etwa einem lokalen oder verteilten Switch durch.

- **Problem 2288774:** Segment-Port gibt einen Realisierungsfehler aus, weil die Anzahl der Tags (fälschlicherweise) 30 überschreitet

Bei der Benutzereingabe wird fälschlicherweise versucht, mehr als 30 Tags anzuwenden. Der Richtlinien-Workflow validiert/verweigert jedoch die Benutzereingabe nicht ordnungsgemäß und lässt die Konfiguration zu. Die Richtlinie zeigt dann einen Alarm mit der korrekten Fehlermeldung an, dass der Benutzer nicht mehr als 30 Tags verwenden darf. An diesem Punkt kann der Benutzer das Problem beheben.

**Problemumgehung:** Korrigieren Sie die Konfiguration, nachdem der Fehler angezeigt wurde.

- **Problem 2275412:** Die Portverbindung funktioniert nicht über mehrere Transportzonen hinweg  
Die Portverbindung kann nicht nur in einer einzelnen Transportzone verwendet werden.

**Problemumgehung:** Keine.

- **Problem 2320147:** VTEP fehlt auf dem betroffenen Host.

Wenn ein LogSwitchStateMsg in derselben Transaktion entfernt und hinzugefügt wird und dieser Vorgang von der zentralen Control Plane verarbeitet wird, bevor die Management Plane den logischen Switch gesendet hat, wird der Status des logischen Switches nicht aktualisiert. Dies führt dazu, dass der Datenverkehr nicht in den oder aus dem fehlenden VTEP fließen kann.

**Problemumgehung:** Falls dieses Problem auftritt, starten Sie die zentrale Control Plane neu.

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

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

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

- **Problem 2295819:** L2-Bridge verbleibt im Status „gestoppt“, obwohl die Edge-VM und PNIC aktiv sind.

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

**\*Auswirkungen auf Kunden\*:**

Datenverkehrsausfall für VMs, die über den Edge-l2bridge-Port erreichbar sind

**Problemumgehung:** Starten Sie den Local-Control-Agent auf der betroffenen Edge-VM neu.

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



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

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

## **Bekannte Probleme bei Sicherheitsdiensten**

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

Problemumgehung: Fügen Sie stattdessen eine statusbehaftete Firewallregel hinzu.

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

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

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

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

- **Problem 2314537: Der Verbindungsstatus ist nach der Aktualisierung von vCenter-Zertifikat und Fingerabdruck nicht verfügbar.**  
Neue Updates von vCenter werden nicht mit NSX synchronisiert und alle bedarfsgesteuerten Abfragen zum Abrufen von Daten aus vCenter schlagen fehl. Benutzer können keine neuen Edge/Service-VMs bereitstellen. Benutzer können keine neuen Cluster oder Hosts vorbereiten, die in vCenter hinzugefügt wurden. Speicherorte des Protokolls: /var/log/cm-inventory/cm-inventory.log und /var/log/proton/nsxapi.log auf dem NSX Manager-Knoten.

Problemumgehung: Melden Sie sich bei jeder NSX Manager-VM an und wechseln Sie zum Root-Benutzer. Führen Sie auf jedem Manager-Knoten den Befehl „/etc/init.d/cm-inventory restart“ aus.

## **Bekannte Probleme beim Load Balancer**

- **Problem 2290899: IPSec-VPN funktioniert nicht, und die Realisierung der Control Plane für IPSec schlägt fehl**  
IPSec-VPN (oder L2VPN) wird nicht aktiviert, wenn zusammen mit dem IPSec-Dienst auf Tier-0 mehr als 62 LbServers auf demselben Edge-Knoten aktiviert sind.

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

- **Problem 2318525: Problem mit dem nächsten IPv6-Hop, weil die IP-Adresse des eBGP-Peers in die eigene IP geändert wird.**

Bei eBGP-IP4-Sitzungen wird für angekündigte IPv4-Routen, die ihren eBGP-Peer als nächsten Hop besitzen, der nächste Hop der Route auf der Absenderseite NICHT in die eigene IP-Adresse geändert. Dies funktioniert für IPv4, für IPv6-Sitzungen wird aber der nächste Hop der Route auf der Absenderseite in die eigene IP-Adresse geändert. Dieses Verhalten kann zu Routenschleifen führen.

Problemumgehung: Keine.

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

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

Problemumgehung: Problemumgehung: Keine.

#### Bekannte Probleme bei der Lösungsinteroperabilität

- **Problem 2289150:** PCM-Aufrufe an AWS beginnen fehlerauszuschlagen

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

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

#### Bekannte Probleme bei Betriebs- und Überwachungsdiensten

- **Problem 2316943:** Arbeitslast ist während vMotion kurzzeitig ungeschützt.

VMware Tools benötigt einige Sekunden, um nach vMotion den korrekten Computernamen für die VM zu melden. Infolgedessen sind VMs, die unter Verwendung des Computernamens zu NSGroups hinzugefügt wurden, nach vMotion einige Sekunden lang ungeschützt.

Problemumgehung: Verwenden Sie für Gruppen, die in DFW-Regeln verwendet werden, auf dem VM-Namen basierende anstelle von auf dem Computernamen basierenden Kriterien.

- **Problem 2331683:** Das Add-Load-Balancer-Formular in der erweiterten Benutzeroberfläche zeigt keine aktualisierte Kapazität der Version 2.4 an.

Wenn das Add-Load-Balancer-Formular geöffnet wird, wird die in der erweiterten Benutzeroberfläche angezeigte Formfaktorkapazität nicht für Version 2.4 aktualisiert. Die angezeigte Kapazität entspricht der vorherigen Version.

Problemumgehung: Keine.

#### Bekannte Upgradeprobleme

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

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

1. Führen Sie den CLI-Befehl `get service install-upgrade aus`.  
Beachten Sie die IP von „Aktiviert auf“ in den Ergebnissen.
2. Melden Sie sich bei der NSX Manager-IP an, die in der „Aktiviert auf“-Rückgabe des oben angegebenen Befehls ausgegeben wird.

3. Navigieren Sie zu **System > Übersicht** und suchen Sie den Knoten mit der in der „Aktiviert auf“-Rückgabe angegebenen IP.
4. Klicken Sie für diesen Knoten auf **Beheben**.
5. Klicken Sie, nachdem die oben angegebene Behebung erfolgreich war, für alle Knoten derselben Schnittstelle auf **Beheben**.

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

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

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

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

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

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

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

## Bekannte Probleme mit APIs

- **Problem 2260435: Statusfreie Umleitungsrichtlinien/-regeln werden standardmäßig durch die API erstellt, die nicht für Ost-West-Verbindungen unterstützt wird.**  
Statusfreie Umleitungsrichtlinien/-regeln werden standardmäßig durch die API erstellt, die nicht für Ost-West-Verbindungen unterstützt wird. Dies führt dazu, dass der Datenverkehr nicht an Partner umgeleitet wird.

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

- **Problem 2332397: Die API erlaubt das Erstellen von DFW-Richtlinien in einer nicht vorhandenen Domäne.**  
Nach dem Erstellen einer solchen Richtlinie in einer nicht vorhandenen Domäne reagiert die Schnittstelle nicht mehr, wenn der Benutzer eine DFW-Sicherheitsregisterkarte öffnet. Das entsprechende Protokoll ist `/var/log/policy/policy.log`.

Problemumgehung: Erstellen Sie die Domäne mit derselben ID, mit der die Richtlinie erstellt wurde. Dadurch verläuft die Validierung erfolgreich.

## Bekannte Probleme bei NSX Cloud

- **Problem 2275232: DHCP funktioniert nicht für VMs in der Cloud, wenn Connectivity\_statregy für DFWs von BLACKLIST in WHITELIST geändert wird**

Alle VMs, die neue DHCP-Leases anfordern, verlieren die IPs. DHCP muss in DFW explizit für Cloud-VMs zugelassen werden.

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

- **Problem 2277814: Eine VM wird aufgrund eines ungültigen Werts für das nsx.network-Tag zu „vm-overlay-sg“ verschoben**

Eine VM, die mit einem ungültigen nsx.network-Tag versehen ist, wird zu „vm-overlay-sg“ verschoben.

Problemumgehung: Entfernen Sie das ungültige Tag.