

# Versionshinweise für VMware NSX-T Data Center 2.4.1

VMware NSX-T Data Center 2.4.1 | 21. Mai 2019 | Build 13716575

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

## Neuigkeiten

VMware HCX unterstützt jetzt NSX-T für die Migration virtueller Maschinen in lokale NSX-T-basierte Bereitstellungen. Damit können Kunden eine Massenmigration virtueller Maschinen aus NSX Data Center for vSphere zu NSX-T, von NSX-T in Site-übergreifende NSX-T-Migrationen und Nicht-NSX-vSphere-Umgebungen in NSX-T-basierte SDDC-Umgebungen durchführen.

Verbesserungen der Kennwortrichtlinie wurden zu Version 2.4.0 hinzugefügt, die eine minimale Kennwortlänge von 12 Zeichen für Standardkennwörter erzwingen und die Möglichkeit zur Festlegung von Kennwortablaufzeiten eingeführt haben. Standardmäßig laufen Kennwörter nach 90 Tagen ab. Anweisungen zum Zurücksetzen von Kennwörtern und zum Anpassen des Kennwortablaufs finden Sie im Knowledgebase-Artikel [70691](#).

## 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

21. Mai 2019. Erste Auflage.

3. Juni 2019. Zweite Auflage. Behobenes Problem 2339832 wurde hinzugefügt.

20. Juni 2019. Dritte Auflage. Die bekannten Probleme 2261818 und 2334442 wurden hinzugefügt.

21. Juni 2019. Vierte Auflage. Problem 2304571 wurde in den Status „Behoben“ verschoben.

23. August 2019. Fünfte Auflage. Die bekannten Probleme 2362688, 2395334 und 2392093 wurden hinzugefügt.

12. November 2019. Sechste Auflage. Problem 2295470 wurde in den Status „Behoben“ verschoben.

## Behobene Probleme

- **Behobenes Problem 2248345:** Nach der Installation des NSX-T Edge wird die Maschine mit einem leeren schwarzen Bildschirm gestartet.  
NSX-T Edge kann nicht auf einer Maschine des Typs HPE ProLiant DL380 Gen9 installiert werden.
- **Behobenes Problem 2264386:** Die Löschung des Transportknotens findet statt, obwohl der Transportknoten Teil einer NS-Gruppe ist  
Die Löschung des Transportknotens ist zulässig, selbst wenn der Knoten Teil einer NS-Gruppe ist. Die Löschung sollte vermieden werden. Wenn dieses Problem auftritt, müssen Sie die NS-Gruppen neu erstellen und die Beziehungen mit ihren Transportknoten erneut herstellen.
- **Behobenes Problem 2275869:** Rollover des cfgAgent-Protokolls in weniger als 1 Minute auf dem ESXi-Host, wenn Regeln auf dem Host Tags mit einer Länge von mehr als 31 Zeichen aufweisen  
Häufige Protokoll-Rollover können zum Verlust nützlicher Informationen im Protokoll „cfgAgent.log“ für Debugging und Fehlerbehebung auf dem Host führen. Protokollspeicherort auf dem ESXi-Host: `/var/log/cfgAgent.log`
- **Behobenes Problem 2288872:** Installationsstatus wird als „Knoten nicht bereit“ angezeigt  
Der Edge-Knoten wird nicht integriert. Der Konfigurationszustand des Transportknotens lautet „Ausstehend“, und der Knoten kann daher nicht einem Edge-Cluster hinzugefügt werden.  
Speicherort des Protokolls: `/var/log/proton/nsxapi.log`
- **Behobenes Problem 2291267:** Einem vom PCM erstellten Standard-Gateway-Richtlinienabschnitt ist keine Sequenznummer zugewiesen, sodass die Richtlinie diese standardmäßig auf 0 festlegt  
Wenn ein Benutzer Gateway-Richtlinien ohne Sequenznummern oder insert\_top-Optionen erstellt, führt dies zu einem Richtlinienkonflikt. Speicherort des Protokolls: `/var/log/policy/policy.log`
- **Behobenes Problem 2292995:** Der Realisierungsstatus ist auf „Fehler“ festgelegt, obwohl alle konfigurierten Regeln in OVS programmiert sind  
Die API vermittelt fälschlicherweise einen negativen Eindruck, selbst wenn die DFW-Regeln in der Data Plane programmiert sind.
- **Behobenes Problem 2292997:** Bestimmte logische Routerschnittstellen können möglicherweise für Linux-Netzwerk-Stack nicht erstellt werden  
Bestimmte logische Routerschnittstellen können für Linux-Netzwerk-Stack möglicherweise nicht erstellt werden und geben den folgenden Fehler zurück: `errorCode="EDG0100002", Operation failed creating sub-interface: max sub-interface exceeded`. Dies kann dazu führen, dass von einem Tier0-Dienstrouter (TO SR) weitergeleiteter Datenverkehr aufgrund fehlender Routen verworfen wird.
- **Behobenes Problem 2295470 – Firewallfilter sind nach der Migration zu NSX-T von NSX for vSphere nicht vorhanden.**  
Wenn Dienste in vielen Firewallregeln verwendet werden, kann dies zu häufigen Updates der Dienste während des Migrationsvorgangs führen. Daher werden Firewallfilter nicht auf dem ESXi-Host installiert. Dies kann zu einer Unterbrechung des Datenverkehrs führen.
- **Behobenes Problem 2285117:** Kernel-Upgrade auf NSX-verwalteten VMs wird nicht unterstützt

Auf einigen Linux Ubuntu-Marketplace-Images führt der Kernel beim Neustart der VM automatisch für sich selbst ein Upgrade durch. Dies führt dazu, dass NSX-Agent nicht erwartungsgemäß funktioniert. Auch wenn es so aussehen kann, als ob der NSX-Agent funktionierte, sind einige nicht realisierte Netzwerkrichtlinien vorhanden, die sich auf den NSX-Agent auswirken. Der Agent versucht die Realisierung dieser Richtlinien immer wieder erneut, was zu einer hohen CPU-Auslastung führt.

- **Behobenes Problem 2252776: Ein Transportknotenprofil kann auf einem der Mitgliederhosts des Clusters nicht angewendet werden, obwohl der zuvor aufgetretene Validierungsfehler jetzt behoben ist**  
Das Transportknotenprofil wird auf dem Cluster angewendet. Aber es kann auf einem der Mitgliederhosts des Clusters nicht angewendet werden, weil eine der Validierungen nicht bestanden wurde (z. B. sind VMs auf dem Host eingeschaltet). Der Benutzer behebt dieses Problem, aber die Validierung wird weiterhin auf der Benutzeroberfläche angezeigt, und das Transportknotenprofil wird nicht automatisch auf diesem Host angewendet.
- **Behobenes Problem 228688: Der BGP-Nachbar muss beim Löschen einer IPsec-Routen-Basisierung zuerst gelöscht werden, wenn BGP über VTI konfiguriert ist**  
Wenn BGP über VTI konfiguriert ist und Sie die IPsec-Sitzung löschen, sind beide SR inaktiv, und dies blockiert wiederum den Datenverkehr. Um den Datenverkehr wiederaufzunehmen, muss der für VTI konfigurierte BGP-Nachbar gelöscht werden. In diesem Szenario ist nur BGP über VTI konfiguriert.
- **Behobenes Problem 2288509: Eigenschaft MTU wird für Tier0-/Tier1-Dienstschnittstelle (zentraler Dienstport) nicht unterstützt**  
Die Eigenschaft MTU wird für die Tier0-/Tier1-Dienstschnittstelle (zentraler Dienstport) nicht unterstützt.
- **Behobenes Problem 2266553: In der NSX-Appliance schlägt die Initialisierung eines Diensts möglicherweise beim ersten Starten fehl**  
Der bereitgestellte Knoten kann keine Anforderungen bedienen oder keinen Cluster bilden.
- **Behobenes Problem 2267632: Verlust von GI-Schutzkonfiguration**  
Eine auf der Richtlinien-Benutzeroberfläche veröffentlichte Gastschutzregel zeigt ERFOLGREICH an. Die entsprechende Änderung im Verhalten wird auf der Gast-VM nicht widerspiegelt. Gleichzeitige OpsAgent-Protokolle zeigen Neustart an. Verlust des Gast-VM-Schutzes.
- **Behobenes Problem 2288773: Die noch verfügbare alte TLS-Protokoll-API wird überschrieben**  
NSX-T verfügt über eine neue API zum Einstellen der NSX-TLS-Protokollversionen und -Verschlüsselungs-Suites, was zu einem Update aller Knoten in einem NSX-T-Cluster führt. Die alte API ist jedoch immer noch verfügbar. Diese kann verwendet werden, aber die neuen Einstellungen werden von den globalen Einstellungen überschrieben.
- **Behobenes Problem 2269901: Die vmk-Schnittstelle ist nicht in der Paketerfassungs-CLI enthalten.**  
Dieser Befehl kann nicht ausgegeben werden.
- **Behobenes Problem 2304571: Ein kritischer Fehler (PSOD) kann auftreten, wenn L3-Datenverkehr mit VDR ausgeführt wird.**  
Ein ausstehender arp(ND)-Eintrag ist in einigen Fällen nicht ordnungsgemäß geschützt, was zu einem kritischen Fehler (PSOD) führen kann.
- **Behobenes Problem 2275985: Nicht mit einem logischen Switch verbundene VNICs werden als Optionen für direkte NSGroup-Mitglieder aufgeführt**  
Eine nicht mit einem logischen Switch verbundene VNIC wird als direktes Mitglied der NSGroup hinzugefügt. Der Vorgang ist erfolgreich, aber die für diese Gruppe angewendeten Richtlinien werden auf der VNIC nicht durchgesetzt.
- **Behobenes Problem 2279973: Wenn eine leere Gruppe erstellt und das Upgrade fortgesetzt**

wird, wird nach dem MP-Upgrade diese leere Gruppe nicht als „Gestartet“ angezeigt  
Dies tritt auf, wenn eine leere Gruppe erstellt und das Upgrade fortgesetzt wird.

- **Behobenes Problem 2282389: Der UC-Upgrade-Plan ist nicht mit der VC-Cluster-Mitgliedschaft synchronisiert, wenn ESX über Cluster hinweg verschoben wird**  
Wenn ESX im VC von einem Cluster in einen anderen verschoben wird, spiegelt sich die Änderung nicht im UC-Upgrade-Plan wider. Dies kann dazu führen, dass mehr als ein HOST gleichzeitig in den Wartungsmodus wechselt, wenn der Benutzer über Gruppen hinweg „Paralleles Upgrade“ ausgewählt hat.
- **Behobenes Problem 2288921: Der Upgrade-Status ist nicht mehr synchronisiert, wenn Edge-Knoten mit einer alten Version hinzugefügt werden**  
Der Upgrade-Status ist nicht mehr synchronisiert, wenn der Benutzer nach einem Edge-Upgrade Edge-Knoten einer älteren Version hinzufügt. Dies führt zu Problemen beim Fortsetzen des Upgrade-Aufrufs.
- **Behobenes Problem 2289278: Die Richtlinien-API löst einen Fehler aus, lässt jedoch die Konfiguration von mehreren virtuellen Servern mit demselben Pool und mit unterschiedlichem Persistenzprofil zu**  
Das System unterstützt die Konfiguration von widersprüchlichen Persistenztypen für denselben Pool und für unterschiedliche LbVirtualServers nicht. Die Richtlinie validiert/verweigert jedoch die widersprüchliche Eingabe nicht ordnungsgemäß und lässt die Konfiguration zu. In der Folge zeigt die Richtlinie einen Alarm mit der entsprechenden Fehlermeldung an.
- **Behobenes Problem 2289984: „mux\_connectivity\_status“ wird selbst nach dem Beenden des Dienstes „nsx-context-mux“ auf dem Host als CONNECTED angezeigt.**  
Wenn „nsx-context-mux“ oder „nsx-opsagent“ nicht auf dem Host ausgeführt wird, zeigt das System (NSX-Schnittstellen- oder -Dienstinstanz-API) fälschlicherweise den Lösungsstatus und den GI-Agent-Status als „Wird ausgeführt“ mit einem unveränderten Zeitstempel an. Dies führt dazu, dass der AV-Schutz der Gast-VMs möglicherweise verloren geht.
- **Behobenes Problem 2290083: Beim Erstellen eines VLAN-basierten Segments fehlt die Validierung**  
Wenn Sie eine VLAN-Transportzone mit einer VLAN-ID-Eigenschaft angeben, kann der Fehler vom System nicht validiert und identifiziert werden. Dies führt dazu, dass der Intent während der Realisierung fehlschlägt und einen Fehler auslöst.
- **Behobenes Problem 2290669: Mit zunehmender Anzahl an virtuellen Servern steigt die Konfigurationszeit für jeden dieser Server an**  
Aufgrund einer großen Anzahl an Validierungen steigt mit zunehmender Anzahl an virtuellen Servern die Konfigurationszeit für jeden dieser Server an. Bei den ersten 100 virtuellen Servern beträgt die durchschnittliche Reaktionszeit ca. 1 Sekunde. Nach 250 virtuellen Servern steigt die durchschnittliche Reaktionszeit auf 5–10 Sekunden an. Nach 450 virtuellen Servern steigt die durchschnittliche Reaktionszeit auf ca. 30 Sekunden an.
- **Behobenes Problem 2291625: Nach der Synchronisierung des Upgrade-Plans wird der PCG-Upgrade-Status von SUCCESS in NOT\_STARTED geändert**  
Dieses Problem tritt nur dann auf, wenn der Benutzer ein Upgrade des PCG durchführt und dann versucht, nachträglich ein Upgrade weiterer Agents/PCGs durchzuführen.  
Im empfohlenen Workflow sind nach dem PCG-Upgrade keine weiteren Cross-Cloud-Komponenten mehr vorhanden, für die ein Upgrade über die UC-Schnittstelle durchgeführt werden soll.

Dies wirkt sich auf keine der Funktionen aus. Der Status des zuvor erfolgreich abgeschlossenen PCG-Upgrades wird auf der Upgrade-Benutzeroberfläche als „Keine“ angezeigt.

- **Behobenes Problem 2291872: Eine Protokollmeldung zeigt eine Warnmeldung an, wenn der TFTP-Dienst in einer Firewallregel verwendet wird**

Eine Protokollmeldung zeigt eine irrelevante Warnmeldung an, wenn der TFTP-Dienst in einer Firewallregel verwendet wird. Protokollspeicherort auf dem ESXi-Knoten:

`/var/log/cfgAgent.log.`

- **Behobenes Problem 2292096: Der CLI-Befehl „get service router config route-maps“ gibt eine leere Ausgabe zurück**  
Der CLI-Befehl „get service router config route-maps“ gibt selbst dann eine leere Ausgabe zurück, wenn „route-maps“ konfiguriert ist. Dieses Problem betrifft nur die Anzeige.
- **Behobenes Problem 2292526: Beim Hinzufügen eines Hosts wird die Meldung „Host nicht erreichbar“ angezeigt**  
Beim Hinzufügen eines ESXi-Hosts wird die Meldung „Host nicht erreichbar“ angezeigt, es wird jedoch kein Grund angezeigt. Der wahrscheinliche Grund dafür liegt in falschen Anmeldedaten.
- **Behobenes Problem 2292701: Der Benutzer kann die Sequenznummer in einer Bindungszuordnung nicht aktualisieren**  
Der Benutzer kann die Reihenfolge oder Rangfolge von Profilen, die auf eine Einheit angewendet werden, nicht durch Aktualisieren der Sequenznummer ändern.
- **Behobenes Problem 2293227: Nach dem Upgrade auf Version 2.4 werden für VMs, auf denen VMTools 10.3.5 ausgeführt wird, keine IDFW-Regeln angewendet**  
Nach dem Durchführen eines Live-NSX-T-Upgrades werden für VMs, auf denen VMTools 10.3.5 ausgeführt wird, keine IDFW-Regeln angewendet. Dies kann zu einem Verlust des AV-Schutzes für diese VMs führen.
- **Behobenes Problem 2994002: Bei der DNS-Weiterleitungserstellung wird Tier1 in der Dropdown-Liste der Tier0-/Tier1-Gateways nicht zur Auswahl angeboten**  
In einer großen Bereitstellung mit Tausenden von Datensätzen wird im Workflow zur DNS-Weiterleitungserstellung Tier1 in der Dropdown-Liste der Tier0-/Tier1-Gateways nicht zur Auswahl angeboten. Sie müssen deshalb zum Konfigurieren der DNS-Weiterleitungserstellung die API verwenden.
- **Behobenes Problem 2294345: Das Ausführen einer Anwendungserkennungs-Klassifizierung für eine Gruppe mit sowohl ESXi- als auch KVM-gehosteten VMs kann fehlschlagen**  
Die Funktion der Anwendungserkennung wird nur auf ESXi-Hypervisoren unterstützt. Für Gruppen von VMs, die sich auf verschiedenen Hosts befinden, die nicht unterstützte Hosts umfassen, wird für die Ergebnisse der Anwendungserkennungs-Klassifizierung keine Garantie übernommen.
- **Behobenes Problem 2294821: NSX-Appliance-Informationen werden im Cluster-Überwachungs-Dashboard mit dem Fehler „Fehler beim Löschen des Knotens“ und ohne Hinweise an den Benutzer zur Handhabung der Situation angezeigt**  
Dieses Problem wurde beobachtet, nachdem der Benutzer versuchte, den automatisch bereitgestellten Knoten über die Schnittstelle zu löschen, und das Ausschalten des Knotens fehlschlug. Wenn der Cluster einen Knoten verliert, müssen Sie manuell einen neuen Knoten hinzufügen und die Konfigurationszustände mithilfe der Problemumgehung unten bereinigen.
- **Behobenes Problem 2281095: Wenn der Host, auf dem die SVM bereitgestellt ist, dem selben Cluster erneut hinzugefügt wird, wird kein Callback von EAM ausgelöst**  
Alle Gast-VMs sind möglicherweise ungeschützt. Die NSX-Benutzeroberfläche bleibt im Status „In Bearbeitung“ hängen.
- **Behobenes Problem 2295564: Die Konnektivität des Edge-Knoten-Controllers geht möglicherweise nach dem Upgrade von 2.3 auf 2.4 verloren**  
Dies ist ein Problem, das zeitweilig auftritt und sich teilweise auf den Nord-Süd-Datenverkehr auswirkt.
- **Behobenes Problem 2296888: Für die Konfiguration von Transportknoten (TN)/Transportknotenprofil (TNP) können nicht sowohl das Flag für die Migration nur von PNIC auf „true“ gesetzt als auch VMK-Zuordnungen für die Installation für alle Host-Switches**

**festgelegt werden**

Wenn mit einer falschen Konfiguration (sowohl PNIC-Migrations-Flag auf „true“ festgelegt als auch VMK-Zuordnungen für die Installation, die für alle Host-Switches angegeben wurden) CREATE ausgeführt wird, kommt es zur folgenden Ausnahme:

VMK-Migration für Host b17afc36-bbdc-491a-b944-21f73cf91585 ist mit Fehler

[com.vmware.nsx.management.switching.common.exceptions.SwitchingException: TransportNode [TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585] kann während der Migration der ESX-vmk-Schnittstelle null auf [null] nicht aktualisiert oder gelöscht werden.] fehlgeschlagen.  
(Fehlercode: 9418)

Wenn mit einer falschen Konfiguration ein UPDATE-Befehl ausgeführt wird, kommt es zur folgenden Ausnahme:

Allgemeiner Fehler (Fehlercode: 400)

Eine Ausnahme tritt auf, wenn die TN/TNP-Konfiguration angewendet wird, in der sowohl das Flag für die Migration nur von PNIC auf „true“ als auch die VMK-Migrationszuordnung festgelegt ist.

- **Behobenes Problem 2287124: Nach der Bereitstellung des PCG in einem Microsoft Azure-VNET wird auf der VNET-Kachel in CSM fälschlicherweise eine Warnung angezeigt**  
Nach der Bereitstellung des PCG in einem Microsoft Azure-VNET zeigt VNET in CSM ein Warnsignal (gelbes Dreieck mit Ausrufezeichen). Wenn Sie den Mauszeiger über das Warnsymbol bewegen, meldet CSM, dass der Status von MP (Management Plane) und CCP (Control Plane) unbekannt ist. Es liegt jedoch möglicherweise kein Problem mit der Konnektivität vor und die Warnung wird fälschlicherweise angezeigt.
- **Behobenes Problem 2273651: Nach dem Löschen des Transportknotens kann der Benutzer kein SSH in den Host ausführen.**  
In KVM-Implementierungen beobachtet. Der Benutzer löscht einen Transportknoten und erhält eine Meldung, dass der Löschvorgang erfolgreich war. Danach kann der Benutzer jedoch nicht mehr über SSH auf denselben Host zugreifen. Das Problem wird wahrscheinlich durch das Vorhandensein eines Open Virtual Switchs (OVS) verursacht, der nicht von NSX-T verwaltet wird und wahrscheinlich als Teil der KVM-Vorlage vorab installiert wurde.
- **Behobenes Problem 2297157: Die HTTPS-Leistung von Load Balancing wird vom FIPS-Modus beeinträchtigt.**  
Die Leistung des Load Balancing kann beeinträchtigt werden, wenn der standardmäßige FIPS-Modus aktiviert ist.
- **Behobenes Problem 2290688: Das Upgrade von Windows 2016-VMs in AWS schlägt fehl.**  
Upgrade mehrerer Windows-Workload-VMs schlägt in AWS fehl. Der Status der VM-Aktualisierung bleibt im AWS-Portal bei der ersten von zwei Überprüfungen stehen. Ein erneuter Versuch schlägt ebenfalls fehl. Dieses Problem tritt nur bei Upgrades derselben NSX-T-Version auf.
- **Behobenes Problem 2203863: Identitäts-Firewallregeln werden für UDP- und ICMP-Datenverkehr nicht unterstützt.**  
Identitäts-Firewallregeln funktionieren nicht mit Ping-Tests. Die aktuelle Funktionalität wird nur für TCP-Datenverkehr unterstützt.
- **Behobenes Problem 2248186: Der BGP-Router installiert IPv6-Routen von seinem Nachbarn mit seiner eigenen Schnittstelle als nächster Hop.**  
Infolgedessen kann die IPv6-Weiterleitung für die installierte Route fehlschlagen und zu einer Weiterleitungsschleife führen.
- **Behobenes Problem 2281537: Nach der Migration kann der ESXi-Transportknoten mit Multi-VTEP die BFD-Sitzung nicht starten.**  
Nach der Migration eines NSX-V-Knotens zu NSX-T kann der ESXi-Transportknoten mit Multi-VTEP auf allen VTEPs zu Edge-Knoten keine BFD-Sitzung starten.

- **Behobenes Problem 2297918:** Nach dem Upgrade von 2.3.1 auf 2.4 kann NSX nicht von dem Cluster entfernt werden.  
Nach dem Upgrade eines Clusters von 2.3.1 auf 2.4 kann NSX-T nicht entfernt werden und schlägt mit der folgenden Meldung fehl: „Fehler beim Entfernen von NSX auf dem Cluster: Für diese Fabric-Vorlage existiert eine zugehörige Transportknotenvorlage oder Transportknotensammlung. Die Transportknotenvorlage oder Transportknotensammlung muss vor dem Löschen/Deaktivieren auf dieser Fabric-Vorlage gelöscht werden.“
- **Behobenes Problem 2298499:** VPN zwischen Public Cloud-Gateway und Peer-Host schlägt fehl, wenn das Gateway nicht mit öffentlicher IP bereitgestellt wurde.  
Der VPN-Tunnel zwischen dem Public Cloud-Gateway (PCG) und dem Peer-Host kann nicht hergestellt werden, wenn das PCG ohne öffentliche IP-Adresse auf dem Uplink bereitgestellt wurde. Dies passiert, weil das PCG für den VPN-Datenverkehr standardmäßig SNAT ausführt.
- **Behobenes Problem 2316831:** Für IPv6-Datenverkehr erfolgt immer eine Lastverteilung, selbst wenn ECMP deaktiviert ist.  
Das Deaktivieren von ECMP in der Richtlinie ist für die IPv6-Unicast-Adressfamilie unwirksam. (Obwohl es für die IPv4-Unicast-Adressfamilie wirksam ist.)
- **Behobenes Problem 2334515:** Die Verwendung des verbindungslokalen IPv4-Bereichs (169.254.0.0/16) für den T0-T1-Routerlink-Port funktioniert nicht.  
Die Verwendung des verbindungslokalen IPv4-Bereichs (169.254.0.0/16) für den T0-T1-Routerlink-Port funktioniert nicht. Die Verwendung eines IP-Bereichs, bei dem es sich nicht um einen verbindungslokalen IPv4-Adressbereich (169.254.0.0/16) für den T0-T1-Routerlink handelt, funktioniert jedoch.
- **Behobenes Problem 2339832:** „Knotenzertifikat kann nicht angewendet oder Cluster-Zertifikat kann nicht mit einem von einer Zertifizierungsstelle signierten Zertifikat festgelegt werden“ aufzunehmen.  
Dies führt zu Meldungen wie „Fehler beim Aktualisieren der Zertifikatsnutzung“ oder „Fehler beim Festlegen des Cluster Zertifikats“.  
Dies kann auf die wiederholte Anwendung von Zertifikaten zurückzuführen sein, wobei zwischen Knoten- und Cluster-Zertifikat gewechselt wurde. Das Zertifikat wird nicht ordnungsgemäß angewendet und REST API-Aufrufe über die VIP funktionieren möglicherweise nicht mehr.  
Speicherort des Protokolls: /var/log/proton/nsxapi.log.  
  
Wenn dieser Fehler vor dem Upgrade auf 2.4.1 auftritt, verwenden Sie stattdessen selbstsignierte Zertifikate.

## 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 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](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.

### Bekannte Installationsprobleme

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

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

### Bekannte Probleme bei NSX Manager

- **Problem 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 übermäßigen Routing-Berechnungen. Wenn für die überschüssigen Routen eine höhere lokale Einstellung konfiguriert ist, kann diese auf einigen Routern, die mit redundanten Routen gefüllt werden, zu einer Weiterleitungsschleife führen.

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

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

## 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 2392093:** Datenverkehr sinkt aufgrund der RPF-Prüfung

Die RPF-Prüfung kann zu einem verworfenen Datenverkehr führen, wenn der Datenverkehr über einen TO-Downlink angeheftet wird und sich die Tier0- und Tier1-Router auf demselben Edge-Knoten befinden.

Problemumgehung: Keine.

## 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 2458384 – Seiten der NSX-T Manager-Schnittstelle** können nicht geladen werden (Fehler 403).

Trat in den Herausgabeverversionen 2.4.0 und 2.4.1 auf. Dieses Problem betrifft sowohl Admin- als auch Identity Manager-Anmeldungen. Der FQDN des NSX-T Manager verwendet das Format „\*.SLD.TLD“. Beispiel: \*.co.uk, \*.co.il, \*.com.au.

Problemumgehung: Greifen Sie auf die NSX-T Manager-Benutzeroberfläche zu, indem Sie anstelle des FQDN einen Kurznamen oder eine IP verwenden. Weitere Informationen hierzu finden Sie im [Knowledgebase-Artikel 71217](#).

- **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: Keine.

#### Bekannte Probleme bei der Lösungsinteroperabilität

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

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

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

#### 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 2286030** – Die Transportknotenkonfiguration wird als fehlgeschlagen angezeigt, wenn ein Upgrade von NSX-T 2.3.x und früher auf 2.4.x durchgeführt wird.

Die Transportknotenkonfiguration geht bei einem Upgrade von NSX-T 2.3.x und früher auf 2.4.x aufgrund einer Nullzeiger-Ausnahme in den Fehlerzustand über. Wenn Sie über einen ESXi-Transportknoten mit vmkernel-Adaptoren verfügen, die auf N-VDS VLAN logical-switch migriert wurden, und ein Upgrade von NSX-T 2.3.x auf NSX-T 2.4.x durchführen, kann eine Wettlaufsituation dazu führen, dass der Konfigurationsstatus des ESXi-Transportknotens als fehlgeschlagen angezeigt wird. Die Konnektivität des ESXi-Transportknotens mit NSX Manager und Controllern ist jedoch während des Upgrades intakt, auch wenn der Knoten für den Konfigurationsstatus fehlgeschlagen ist.

Problemumgehung: Aktualisieren oder senden Sie den Transportknoten erneut, um den Konfigurationsstatus auf „Erfolgreich“ zurückzusetzen.

1. Bearbeiten Sie im NSX Manager den ESXi-Transportknoten, der als fehlgeschlagen angezeigt wird.
2. Klicken Sie im Pop-up-Fenster für die Konfiguration des ESXi-Transportknotens auf **Speichern**.

Diese Aktion setzt den Status zurück. Sie müssen die Konfiguration nicht ändern.

- **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.