

# Versionshinweise zu VMware Cloud Director 10.1

VMware Cloud Director 10.1 | 9. April 2020 | Build 15967253 (installierter Build 15967236)

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

## Inhalt dieses Dokuments

- [Neuheiten in dieser Version](#)
- [Sicherheit](#)
- [Hinweise zu Produktunterstützung](#)
- [Upgrade von früheren Versionen](#)
- [Systemanforderungen und Installation](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

## Neuheiten in dieser Version

- Informationen zu den neuen und aktualisierten Funktionen dieser Version finden Sie im technischen Whitepaper von VMware, [What's New with VMware vCloud Director 10.1](#).
- Geändertes Verhalten der HTML5-UI:  
In früheren Versionen von VMware Cloud Director können Sie das Aktionsmenü „vApp“ in der HTML-UI verwenden, um eine vApp zu beenden oder auszuschalten. Beide Vorgänge heben die Bereitstellung der vApp auf, wirken sich jedoch unterschiedlich auf die vApp aus. Der Ausschaltvorgang befolgt nicht die Einstellungen der Start- und Beendigungsreihenfolge für die virtuellen Maschinen in der vApp. Der Ausschaltvorgang hebt auch die Bereitstellung aller vApp-Netzwerke auf, indem alle VM-Netzwerkkarten von den VDC-Organisationsnetzwerken getrennt und alle für die vApp bereitgestellten Edge-Gateways entfernt werden.

In VMware Cloud Director 10.1 führt der Ausschaltvorgang bei einer laufenden vApp dazu, dass alle virtuellen Maschinen in der vApp ausgeschaltet werden, ohne jedoch die Bereitstellung der vApp und der darin befindlichen virtuellen Maschinen aufzuheben. Die Netzwerkkarten der virtuellen Maschinen bleiben mit den entsprechenden Netzwerken verbunden und alle vApp-Edge-Gateways bleiben bereitgestellt. Die vApp und die virtuellen Maschinen in der vApp bleiben bereitgestellt. Der Ausschaltvorgang für die einzelnen virtuellen Maschinen in der vApp bleibt aktiv, und Sie können ihn zum Ausschalten einer virtuellen Maschine verwenden. Dieser Vorgang führt zur Aufhebung der Bereitstellung dieser virtuellen Maschine.

Wenn Sie eine vApp ausschalten, folgt der Ausschaltvorgang der Startreihenfolge, die Sie in den Einstellungen der Start- und Beendigungsreihenfolge definiert haben. Dies führt dazu, dass die virtuellen Maschinen in umgekehrter Reihenfolge ausgeschaltet werden, wie Sie für den Start festgelegt haben. Die Einstellung „Wartezeit beim Beenden“ hat während des Ausschaltvorgangs keine Wirkung. Wenn Sie eine vApp ausschalten, wird der Betriebszustand der vApp, der aus dem Betriebsstatus der virtuellen Maschinen in der vApp abgeleitet wird, als ausgeschaltet angezeigt.

- Das VMware Cloud Director API 34.0-Schema enthält Definitionen für die Attribute numberOfCpus und MemoryAllocationMB.

## Sicherheit

- **WARNUNG:** Nach dem Upgrade auf Version 10.1 überprüft VMware Cloud Director immer die Zertifikate für alle mit ihm verbundenen Infrastruktur-Endpoints. Der Grund hierfür besteht darin, dass die Verwaltung von SSL-Zertifikaten durch VMware Cloud Director geändert wurde. Wenn Sie die Zertifikate vor dem Upgrade nicht in VMware Cloud Director importieren, kommt es in vCenter Server und NSX-Verbindungen aufgrund von Problemen bei der SSL-Überprüfung möglicherweise zu fehlgeschlagenen Verbindungen. In diesem Fall haben Sie nach dem Upgrade zwei Möglichkeiten:
  1. Führen Sie den Befehl `trust-infra-certs` des Zellenverwaltungstools aus, um Zertifikate aller Infrastruktur-Endpoints für vCenter Server- und NSX Manager-Instanzen automatisch zu verbinden und im zentralen Zertifikatspeicher abzurufen. Weitere Informationen finden Sie unter [Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen](#).
  2. Wählen Sie auf der Benutzeroberfläche des Administrator-Portals des Dienstanbieters alle vCenter Server- und NSX-Instanzen aus geben Sie die Anmeldedaten erneut ein und akzeptieren Sie das Zertifikat.
- Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshakes zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware Cloud Director API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste nach der Installation oder dem Upgrade von VMware Cloud Director und bevor Sie den Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie unter [Konfigurieren einer Verweigerungsliste für Testverbindungen](#).
- Ab VMware Cloud Director 10.1 werden nicht mehr alle SSL-Zertifikate als vertrauenswürdig eingestuft. In dieser Version bieten vCenter Server- und NSX-Verbindungen keine Unterstützung für diese Option. Für alle anderen Verbindungen gilt die Einstufung aller Zertifikate als vertrauenswürdig ebenfalls als veraltet und wird nach VMware Cloud Director 10.1 nicht mehr unterstützt. Systemadministratoren müssen sich auf diesen Übergang vorbereiten.
  - Wenn Sie die VMware Cloud Director-Systemorganisation mithilfe von LDAP verwalten, können Sie das Dialogfeld „Vertrauen bei erster Nutzung“ auf der Benutzeroberfläche verwenden oder Zertifikate über die API hochladen.
  - Überwachen Sie alle Verwendungen dieser Option und stellen Sie entsprechende Zertifikate mithilfe der Benutzeroberfläche oder API bereit.
  - Informieren Sie die Mandanten über diese Änderungen. Alle Mandanten, die benutzerdefiniertes LDAP bei aktivierter Option **Alle Zertifikate akzeptieren** verwenden, sollten von dieser Konfiguration absehen. Mandanten können entweder das Dialogfeld „Vertrauen bei erster Nutzung“ auf der Benutzeroberfläche verwenden oder Zertifikate über die API hochladen.

## Aktualisierte Open Source-Pakete

- jackson-databind wurde auf Version 2.9.10.1 aktualisiert.
- jre wurde auf Version 1.8.0u231 aktualisiert.
- openssl wurde auf Version 1.0.2u aktualisiert.
- xstream wurde auf Version 1.4.11.1 aktualisiert.

# Hinweise zu Produktunterstützung

VMware Cloud Director 10.1 bietet keine Unterstützung für vSphere 7.0 und NSX-T Data Center 3.0. Die Interoperabilitätszertifizierung wird durchgeführt, und vSphere 7.0 und NSX-T Data Center 3.0 werden in einer gepatchten Nebenversion von VMware Cloud Director 10.1 unterstützt.

Externe Netzwerke, die von VRF-lite-Tier-0-Gateways in NSX-T Data Center gestützt werden, werden nicht unterstützt.

## Warnungen zum Ende der Lebensdauer und zum Ende der Unterstützung

- SQL Server-Datenbank wird nicht mehr unterstützt. Nur die PostgreSQL-Datenbank wird unterstützt.
- Oracle Linux wird nicht mehr als Hostbetriebssystem zur Installation der VMware Cloud Director-Anwendung unterstützt.
- VMware Cloud Director API Version 20 und niedriger wird nicht unterstützt.
- Die VMware Cloud Director API-Versionen 27.0 bis 29.0 sind veraltet und werden nach VMware Cloud Director 10.1 nicht mehr unterstützt.
- VMware Cloud Director API Version 30.0 ist veraltet.
- Die auf Flex basierende Benutzeroberfläche wurde aus dem Produkt entfernt und wird nicht mehr unterstützt.
- Der API-Anmelde-Endpoint `/api/sessions` wurde in VMware Cloud Director API Version 33.0/VMware Cloud Director 10.0 als veraltet deklariert und wird in zukünftigen Versionen von VMware Cloud Director nicht mehr unterstützt. Sie können die gesonderten VMware Cloud Director OpenAPI-Anmelde-Endpoints für den Dienstanbieter- und den Mandantenzugriff auf VMware Cloud Director verwenden.
- Die API `/cloud/server_status` ist sowohl für HTTP- als auch für HTTPS-Protokolle veraltet und wird in zukünftigen Versionen entfernt. Sie müssen `/api/server_status` für HTTP- und HTTPS-Protokolle verwenden.
- Die Zurücksetzaktionen `/ldap/action/resetLdapCertificate` und `/ldap/action/resetLdapKeyStore` werden aufgrund der Art und Weise, wie VMware Cloud Director 10.1 SSL-Zertifikate speichert und verarbeitet, aus VMware Cloud Director API Version 34.0 entfernt. Sie müssen den Endpoint `/cloudapi/1.0.0/ssl/trustedCertificates` verwenden, um Zertifikate als nicht vertrauenswürdig einzustufen.
- Die Aktualisierungsaktionen `/ldap/action/updateLdapCertificate` und `/ldap/action/updateLdapKeyStore` sind veraltet und werden in zukünftigen Versionen nicht mehr unterstützt. VMware Cloud Director führt einen neuen Endpoint ein, mit dem LDAP-Zertifikate als vertrauenswürdig eingestuft werden: `/cloudapi/1.0.0/ssl/trustedCertificates`.
- vSphere-SSO als SAML-IDP gilt in vSphere als veraltet. Alle VMware Cloud Director-Bereitstellungen, die für die Verwendung von vSphere-SSO als SAML-IDP konfiguriert sind, müssen zu einem anderen externen SAML-IDP migriert werden. Die Verwendung dieses IDP wird in zukünftigen vSphere- und VMware Cloud Director-Versionen nicht unterstützt.
- DSA- und DSS-Zertifikate werden nicht mehr unterstützt, da keine empfohlenen Verschlüsselungs-Suites für sie verfügbar sind.

## Hinweis zum bevorstehenden Support-Ende (EOS)

- VMware Cloud Director API 34.0 (VMware Cloud Director 10.1) enthält APIs, die besonders schnell veralten und in zukünftigen Versionen entfernt werden. Weitere Informationen finden Sie im [VMware Cloud Director API-Programmierhandbuch](#).

## Upgrade von früheren Versionen

Weitere Informationen zum Upgrade auf VMware Cloud Director 10.1, zu Upgrade- und Migrationspfaden und -Workflows finden Sie unter [Upgrade und Migration der VMware Cloud Director Appliance](#) oder [Upgrade von vCloud Director unter Linux](#).

## Systemanforderungen und Installation

### Ports und Protokolle

Informationen zu den von VMware Cloud Director 10.1 verwendeten Netzwerkports und -protokollen finden Sie unter [VMware Ports and Protocols](#).

### Kompatibilitätstabelle

In den [VMware-Produkt-Interoperabilitätstabellen](#) finden Sie aktuelle Informationen für Folgendes:

- VMware Cloud Director-Interoperabilität mit anderen VMware-Plattformen
- Unterstützte VMware Cloud Director-Datenbanken

### Unterstützte VMware Cloud Director-Serverbetriebssysteme

- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7

### Unterstützte AMQP-Server

VMware Cloud Director verwendet AMQP zur Bereitstellung des von Erweiterungsdiensten, Objekterweiterungen und Benachrichtigungen genutzten Nachrichtenbusses. Diese Version von VMware Cloud Director erfordert RabbitMQ Version 3.7.9 oder 3.8.2

Weitere Informationen erhalten Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

### Unterstützte Datenbanken für das Speichern von historischen Metrikdaten

Sie können Ihre VMware Cloud Director-Installation zum Speichern von Metriken konfigurieren, die VMware Cloud Director über die Leistung der virtuellen Maschine und den Ressourcenverbrauch erfasst. Daten für historische Metriken werden in einer Cassandra-Datenbank gespeichert. VMware Cloud Director unterstützt Cassandra Version 3.x.

Weitere Informationen erhalten Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

### Speicherplatzanforderungen

Jeder VMware Cloud Director-Server erfordert ca. 2.100 MB freien Speicherplatz für die Installations- und Protokolldateien.

## Arbeitsspeicheranforderungen

Informationen zu Speicheranforderungen finden Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*

## CPU-Anforderungen

VMware Cloud Director ist eine CPU-gebundene Anwendung. Richtlinien zur CPU-Überbelegung für die entsprechende Version von vSphere sollten befolgt werden. In virtualisierten Umgebungen muss es unabhängig von der Anzahl der für VMware Cloud Director verfügbaren Kerne ein sinnvolles Verhältnis zwischen vCPUs und physischen CPUs geben, das nicht zu extremer Überbelegung führt.

## Erforderliche Linux-Softwarepakete

Jeder VMware Cloud Director-Server muss Installationen mehrerer häufig verwendeter Linux-Softwarepakete enthalten. Diese Pakete werden meist standardmäßig mit der Betriebssystemsoftware installiert. Wenn Pakete fehlen, schlägt das Installationsprogramm mit einer Diagnosemeldung fehl.

alsa-lib	libICE	module-init-tools
bash	libSM	net-tools
chkconfig	libstdc++	pciutils
coreutils	libX11	procps
findutils	libXau	redhat-lsb
glibc	libXdmcp	sed
grep	libXext	tar
initscripts	libXi	wget
krb5-libs	libXt	which
libgcc	libXtst	

Zusätzlich zu den für das Installationspaket erforderlichen Paketen erfordern mehrere Vorgänge für die Konfiguration von Netzwerkverbindungen und die Erstellung von SSL-Zertifikaten die Verwendung des Linux-Befehls `nslookup`. Dieser Befehl ist im `bind-utils`-Paket von Linux verfügbar.

## Unterstützte LDAP-Server

Sie können Benutzer und Gruppen aus den folgenden LDAP-Diensten in VMware Cloud Director importieren.

Plattform	LDAP-Dienst	Authentifizierungsmethoden
Windows Server 2012	Active Directory	Simple, Simple SSL
Windows Server 2016	Active Directory	Simple, Simple SSL
Linux	OpenLDAP	Simple, Simple SSL

## Unterstützte Sicherheitsprotokolle und Verschlüsselungssammlungen

VMware Cloud Director erfordert sichere Clientverbindungen. In SSL-Version 3 und TLS-Version 1.0 und 1.1 wurden erhebliche Sicherheitsprobleme erkannt. Diese Versionen sind nicht mehr in den Standardprotokollen enthalten, die vom Server zum Herstellen einer Clientverbindung angeboten werden. Systemadministratoren können weitere Protokolle und Verschlüsselungs-Suites aktivieren. Weitere Informationen finden Sie im Abschnitt zum Zellenverwaltungstool im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*. Die folgenden Sicherheitsprotokolle werden unterstützt:

- TLS Version 1.2

- TLS-Version 1.1 (standardmäßig deaktiviert)
- TLS-Version 1.0 (standardmäßig deaktiviert)

Standardmäßig aktivierte Verschlüsselungs-Suites:

- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Systemadministratoren können das Zellenverwaltungstool verwenden, um andere unterstützte Verschlüsselungs-Suites, die standardmäßig deaktiviert sind, explizit zu aktivieren.

**Hinweis:** Interoperabilität mit vCenter Server-Versionen vor 5.5-update-3e und ovftool-Versionen vor 4.2 erfordern zur Unterstützung von TLS Version 1.0 VMware Cloud Director. Sie können mit dem Zellenverwaltungstool die Gruppe der unterstützten SSL-Protokolle oder -Verschlüsselungen neu konfigurieren. Weitere Informationen finden Sie im Abschnitt zum Zellenverwaltungstool im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

## Unterstützte Browser

VMware Cloud Director ist kompatibel mit der aktuellen und der vorhergehenden Hauptversion der folgenden Browser:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11

## Unterstützte Gastbetriebssysteme und Versionen virtueller Hardware

VMware Cloud Director unterstützt alle Gastbetriebssysteme und Versionen virtueller Hardware, die von den ESXi-Hosts unterstützt werden, die jedem Ressourcenpool zugrunde liegen.

## VMware Cloud Director WebMKS 2.1.1

Die VMware Cloud Director WebMKS 2.1.1-Konsole bietet Unterstützung für Folgendes:

- Drucktaste in Google Chrome und in Mozilla Firefox für Windows.
- Windows-Taste in Windows und macOS. Um das Drücken der Windows-Taste zu simulieren, drücken Sie STRG+Windows-Taste unter Windows OS oder STRG+Befehlstaste unter macOS.
- Automatische Erkennung von Tastaturlayouts in Google Chrome und Mozilla Firefox.

## Behobene Probleme

- **Wenn Sie zwei VMware Cloud Director-Appliance-Sites verknüpfen, sind Objekte über die Sites hinweg nicht sichtbar**  
Wenn Sie eine Site-Verknüpfung durchführen und Ihre Sites über Objekte wie Organisationen, Organisations-VDCs, vApps und VMs verfügen, können Sie die Objekte auf der aktuellen Site nicht anzeigen. Die HTML 5-Benutzeroberfläche zeigt nur die Objekte von der anderen zugeordneten Site an. Dieses Problem tritt während der Fanout-Kommunikation mehrerer Standorte auf, da die Datei `/etc/hosts` der VMware Cloud Director-Appliance nicht die korrekten Inhalte aufweist.
- **Das Aktualisieren einer VM-Größenrichtlinie schlägt mit einem Arbeitsspeicherzuteilungsfehler fehl**  
Wenn Sie ein Zuteilungspool-VDC in ein Flex-Organisations-VDC konvertieren, behält vCloud Director die Informationen der Richtlinie für das Maximum aus dem Zuweisungspool-VDC vor der Konvertierung bei. Werte für die garantierten CPU- oder Arbeitsspeicherreservierungen, die höher als die im Zuteilungspool-VDC definierten Reservierungen sind, schlagen mit einem Fehler des Typs Einstellungen für Reservierung, Grenzwerte und Anteile der virtuellen Maschine sind ungültig fehl.
- **Durch Stilllegen oder Anhalten der primären Zelle in einer Umgebung mit mehreren Zellen werden die periodischen Aufgaben in der sekundären Zelle nicht neu gestartet**  
Wenn Sie in einer Umgebung mit mehreren Zellen die primäre Zelle stilllegen oder anhalten, werden die periodischen Aufgaben, die im Hintergrund der primären Zelle ausgeführt werden, nicht aus der sekundären Zelle gestartet.
- **Das Klonen einer VM in einer hostbasierten Speicherrichtlinie mit aktivierten Datendiensten in eine VM mit einer anderen hostbasierten Speicherrichtlinie schlägt mit einem Fehler fehl**  
Wenn Sie eine VM in einer Speicherrichtlinie mit aktivierten hostbasierten Regeln wie IOPS- oder VM-Verschlüsselung erstellen, schlägt das Klonen der VM und Ändern der Speicherrichtlinie der Ziel-VM mit folgendem Fehler fehl: Das Ändern oder Anwenden von VM-Speicherrichtlinien mit Datendienst-Funktionen ist während des Klonvorgangs nicht zulässig. VM-Speicherrichtlinien mit Datendienst-Funktionen können der bereitgestellten VM nach Abschluss des Klonvorgangs und vor dem Einschalten der VM zugewiesen werden.
- **Der Benutzer mit der globalen Mandantenrolle „vApp-Autor“ kann Vorlagen und Medien hochladen und erstellen, ohne über das erforderliche Recht für solche Vorgänge zu verfügen**  
Die globale Mandantenrolle „vApp-Autor“ verfügt standardmäßig über das Recht vApp von „Meine Cloud“ hinzufügen. Da dieses Recht und das Recht Vorlage/Medien: Erstellen/Hochladen einen einzelnen Vorgang gemeinsam nutzen, gewährt VMware Cloud Director der Rolle „vApp-Autor“ fälschlicherweise auch das Recht Vorlage/Medien: Erstellen/Hochladen.  
  
Das Problem wurde behoben. Wenn Sie möchten, dass die Rolle „vApp Autor“ weiterhin über das Recht Vorlage/Medien: Erstellen/Hochladen verfügt, kann ein Dienstanbieter der globalen Rolle „vApp-Autor“ dieses Recht hinzufügen und es in einer Organisation veröffentlichen.
- **Neu erstellte virtuelle Maschinen werden gemäß der Standardspeicherrichtlinie des Organisations-VDC bereitgestellt**  
Wenn Sie im vCloud Director-Mandantenportal eine neue eigenständige virtuelle Maschine erstellen, fehlt die Option zum Angeben der Speicherrichtlinie. Dies führt dazu, dass die erstellte virtuelle Maschine mit der Standardspeicherrichtlinie des Organisations-VDC bereitgestellt wird.

## Bekannte Probleme

- **Neu Sie können keine VM-Webkonsole öffnen, wenn Sie Microsoft Internet Explorer 11 verwenden**  
Wenn Sie Microsoft Internet Explorer 11 zum Herstellen einer Verbindung mit der Konsole einer VM verwenden, wird ein leeres Fenster geöffnet, und Sie können nicht auf die VM-Konsole zugreifen.



Umgehung: Nein

- **Neu VMs werden nichtkonform, nachdem ein Reservierungspool-VDC in ein Flex-Organisations-VDC konvertiert wurde**

Wenn in einem Organisations-VDC mit einem Reservierungspool-Zuweisungsmodell bestimmte VMs eine Reservierung ungleich Null für CPU und Arbeitsspeicher, eine nicht unbegrenzte Konfiguration für CPU und Arbeitsspeicher oder beides aufweisen, werden diese VMs nach der Konvertierung in ein Flex-Organisations-VDC nichtkonform. Wenn Sie versuchen, die Konformität der VMs wiederherzustellen, wendet das System eine falsche Richtlinie für die Reservierung und den Grenzwert an und legt die CPU- und Arbeitsspeicherreservierungen auf Null und die Grenzwerte auf **Unbegrenzt** fest.

Problemumgehung:

1. Ein Systemadministrator muss eine VM-Größenrichtlinie mit der korrekten Konfiguration erstellen.
  2. Ein Systemadministrator muss die neue VM-Größenrichtlinie im konvertierten Flex-Organisations-VDC veröffentlichen.
  3. Die Mandanten können die VMware Cloud Director-API oder das VMware Cloud Director-Mandantenportal verwenden, um die VM-Größenrichtlinie den vorhandenen virtuellen Maschinen im Flex-Organisations-VDC zuzuweisen.
- **Neu Wenn Sie in der Benutzeroberfläche des Mandantenportals eine Affinitäts- oder Anti-Affinitätsregel erstellen, wirkt sich das Deaktivieren des Kontrollkästchens „Erforderlich“ nicht auf die Regelkonfiguration aus**

Wenn Sie in der Benutzeroberfläche des Mandantenportals eine Affinitäts- oder Anti-Affinitätsregel erstellen, wirkt sich das Deaktivieren des Kontrollkästchens „Erforderlich“ nicht auf die Regelkonfiguration aus. Affinitäts- und Anti-Affinitätsregeln sind immer „Erforderlich“. Das bedeutet, dass die der Regel hinzugefügten VMs nicht eingeschaltet werden können, wenn eine Regel nicht erfüllt werden kann.

Umgehung: Nein

- **NEU Bei Verwendung der VMware Cloud Director-API zum Abfragen einer vApp werden leere Felder für die Attribute „numberOfCpus“ und „MemoryAllocationMB“ zurückgegeben**

Wenn Sie die VMware Cloud Director-API 33.0 oder eine frühere Version zum Ausführen einer vApp-REST API-Abfrage verwenden, werden im Antworttext der REST API leere Felder für die Attribute numberOfCpus und MemoryAllocationMB zurückgegeben. Ursache: Das API-Schema enthält keine Definitionen für die Attribute numberOfCpus und MemoryAllocationMB .

Problemumgehung: Verwenden Sie die VMware Cloud Director-API 34.0 zum Abfragen einer vApp.

- **Neu Der Versuch, einem NSX-T Edge Gateway eine NAT-Regel hinzuzufügen, schlägt fehl**  
Der Versuch, einem NSX-T-Edge-Gateway eine NAT-Regel hinzuzufügen, schlägt mit dem Fehler „Neue und veraltete Werte wurden zusammen für die Neuverteilung aktualisiert, Fehlercode 503266“ fehl.

Problemumgehung: Verwenden Sie die NSX-T Data Center-Richtlinien-API, um die Neuverteilungskonfiguration des externen Netzwerks zu aktualisieren, mit dem das NSX-T-Edge-Gateway verbunden ist.

1. Notieren Sie sich die ID des Tier-0-Routers, der dem externen Netzwerk zugrunde liegt, mit dem Ihr NSX-T-Edge-Gateway verbunden ist.
  - Führen Sie eine GET-Anforderung aus, um eine Liste der Tier-0-Router in Ihrer Umgebung abzurufen.  
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s
  - Überprüfen Sie die Liste, um Tier-0 anhand des Anzeigenamens zu identifizieren. Dieser entspricht dem Namen des Tier-0-Routers auf der Registerkarte „Allgemeine Informationen“ für das externe Netzwerk auf der VMware Cloud Director-Benutzeroberfläche.



2. Aktualisieren Sie das externe Netzwerk (Tier-0-Gateway) manuell.

- Führen Sie eine GET-Anforderung aus, um die localeServices-Liste auf dem Router abzurufen.

GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services

Die Antwort gibt einen Gebietsschemadienst zurück.

- Kopieren Sie die localeService-ID und führen Sie eine GET-Anforderung aus, um sie zu prüfen.

GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services/<LocaleServiceId>.

Die Antwort gibt eine Liste der Eigenschaften für den Gebietsschema-Dienst zurück.

```
{
  "route_redistribution_config": {
    "bgp_enabled": true,
    "enabled": true,
    "redistribution_rules": [
      {
        "name": "some-name",
        "route_redistribution_types": [
          "TIER1_DNS_FORWARDER_IP",
          "TIER1_NAT",
          "TIER1_STATIC"
        ]
      }
    ]
  },
  ...
}
```

- Ändern Sie die Antwort wie folgt.

```
{
  "route_redistribution_config": null,
  "route_redistribution_types": [
    "TIER1_DNS_FORWARDER_IP",
    "TIER1_NAT",
    "TIER1_STATIC"
  ],
  ...
}
```

- Führen Sie eine PUT-Anforderung mit den geänderten Eigenschaften aus, um den localeService des Tier-0-Routers zu aktualisieren.

- **Neu Die Verschiebung einer virtuellen Maschine in einen anderen Cluster schlägt fehl, wenn es sich bei dem Zielspeichercontainer um einen Datenspeicher-Cluster handelt**

Wenn Sie einen Vorgang ausführen, in dessen Folge versucht wird, eine virtuelle Maschine in einen anderen Cluster zu verschieben, und es sich bei dem Zielspeichercontainer um einen Datenspeicher-Cluster handelt, schlägt die Migration mit dem Fehler NO\_FEASIBLE\_PLACEMENT\_SOLUTION fehl. In den VMware Cloud Director-Protokollen wird ein Storage DRS-Aufruffehler mit invalidProperty = spec.host angezeigt.

Problemumgehung:

1. Verwenden Sie vSphere Client, um Storage DRS im Zieldatenspeicher-Cluster zu deaktivieren, oder verwenden Sie VMware Cloud Director API, um den Zielspeicher für die Verschiebung in einen Datenspeicher zu ändern.

2. Wiederholen Sie den fehlgeschlagenen Vorgang.

- **Neu Die Bereitstellung der VMware Cloud Director Appliance schlägt fehl, wenn Sie die Einstellung für den Ablauf des Root-Kennworts bei der ersten Anmeldung aktivieren.**

Wenn Sie versuchen, eine Appliance mit aktivierter Einstellung **Root-Kennwort läuft bei der ersten Anmeldung ab** bereitzustellen, schlägt die Bereitstellung fehl und die Protokolldatei `/opt/vmware/var/log/firstboot` zeigt einen Fehler an:

[FEHLER] Das Skript postgresauth konnte nicht ausgeführt werden.

Problemumgehung: Deaktivieren Sie die Einstellung **Root-Kennwort läuft bei der ersten Anmeldung ab** und geben Sie ein anfängliches Root-Kennwort aus mindestens acht Zeichen an, das mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthält.

- **Neu Wenn ein vApp-Benutzer versucht, eine vApp anhand einer Vorlage zu erstellen, kann dies dazu führen, dass die Meldung „Dieser Vorgang wird verweigert.“ angezeigt wird**  
Wenn Ihre zugewiesene Benutzerrolle „vApp-Benutzer“ lautet und Sie versuchen, eine vApp anhand einer Vorlage zu erstellen, sowie die VM-Größenrichtlinien für die virtuellen Maschinen in der vApp anpassen, führt dies dazu, dass die Meldung „Dieser Vorgang wird verweigert.“ angezeigt wird. Dies geschieht, weil die Rolle „vApp-Benutzer“ Ihnen die Instanziierung von vApps aus Vorlagen ermöglicht, aber keine Rechte umfasst, mit denen Sie den Arbeitsspeicher, die CPU oder die Festplatte einer virtuellen Maschine anpassen können. Beim Ändern der Größenrichtlinie könnten Sie den Arbeitsspeicher oder die CPU der virtuellen Maschine ändern.

Umgehung: Nein

- **Neu Ein NFS-Ausfall kann dazu führen, dass die Clusterfunktionen der VMware Cloud Director-Appliance nicht ordnungsgemäß funktionieren**  
Wenn das NFS nicht mehr verfügbar ist, da die NFS-Freigabe voll ist, unter Schreibschutz gestellt wird usw., kann dies dazu führen, dass die Clusterfunktionen der Appliance nicht ordnungsgemäß funktionieren. Die HTML5-Benutzeroberfläche reagiert nicht mehr, während das NFS ausgefallen ist oder nicht erreicht werden kann. Weitere Funktionen, die möglicherweise davon betroffen sind: Fencing einer fehlgeschlagenen primären Zelle, Switchover, Heraufstufen einer Standby-Zelle usw. Weitere Informationen zum korrekten Einrichten des freigegebenen NFS-Speichers finden Sie unter [Vorbereiten des Übertragungsserverspeichers für die VMware Cloud Director-Appliance](#).

Problemumgehung:

- Beheben Sie den NFS-Zustand so, dass er nicht read-only lautet.
- Bereinigen Sie die NFS-Freigabe, wenn sie voll ist.

- **Neu Obwohl Sie einen Endpoint als vertrauenswürdig eingestuft haben, wird dieser beim Hinzufügen von vCenter Server- und NSX-Ressourcen in einer Umgebung mit mehreren Sites nicht zum zentralen Zertifikatspeicherbereich hinzugefügt**

Wenn Sie in einer Umgebung mit mehreren Sites unter Verwendung der HTML5-UI bei einer vCloud Director 10.0-Site angemeldet sind oder versuchen, eine vCenter Server-Instanz bei einer vCloud Director 10.0-Site zu registrieren, fügt VMware Cloud Director den Endpoint nicht zum zentralen Zertifikatspeicherbereich hinzu.

Problemumgehung:

- Sie können das Zertifikat mithilfe der API in die VMware Cloud Director 10.1-Site importieren.
- Zum Auslösen der Zertifikatsverwaltungsfunktionalität navigieren Sie zum Administrator-Portal des Dienstansbieters auf der VMware Cloud Director 10.1-Site, wechseln zum Dialogfeld **Bearbeiten** des Diensts und klicken auf **Speichern**.

- **Neu Der Versuch, benannte Festplatten in vCenter Server Version 6.5 oder früher zu verschlüsseln, schlägt mit einer Fehlermeldung fehl**

Wenn Sie in vCenter Server-Instanzen der Version 6.5 oder früher versuchen, neue oder vorhandene benannte Festplatten einer verschlüsselungsfähigen Richtlinie zuzuordnen, schlägt der Vorgang mit dem Fehler Die benannte Datenträgerverschlüsselung wird in dieser Version von vCenter Server nicht unterstützt. fehl.

Umgehung: Nein

- **Neu In einer gemischten Multisite-Umgebung mit VMware Cloud Director 10.0 und 10.1 gelten die vertrauenswürdigen Zertifikate für vCenter Server- und NSX-Verbindungen nur für die Objekte aus der lokalen Site.**

Wenn in einer Multisite-Umgebung die VMware Cloud Director-Einrichtungen der Versionen 10.0 und 10.1 miteinander betrieben werden, können Sie bei der Anmeldung bei einer Site keine Instanz von vCenter Server oder NSX Manager bei der anderen Site registrieren.

Problemumgehung: Melden Sie sich bei der Site an, in der Sie die vCenter Server- oder NSX Manager-Instanz registrieren möchten, und starten Sie den Registrierungsprozess.

- **Neu Im VMware Cloud Director-Mandantenportal können Sie die virtuellen Maschinen auf der Registerkarte „Anwendungen“ in der erweiterten Filteroption für virtuelle Maschinen nicht nach Datencenter filtern.**

Wenn Sie im VMware Cloud Director-Mandantenportal auf der Registerkarte „Anwendungen“ in der oberen Navigationsleiste zu „Virtuelle Maschinen“ gehen, führt das Filtern der virtuellen Maschinen nach Datencenter über die Option „Erweiterte Filterung“ zu einem Fehler: Fehlerhafte Anforderung:

Unbekannter Eigenschaftsname vdcName.

Problemumgehung: Wählen Sie in der oberen Navigationsleiste in der Option **Datencenter** ein Datencenter aus, um die darin befindlichen virtuellen Maschinen anzuzeigen.

- **Neu Erweiterungsdienste können RabbitMQ-Meldungen von VMware Cloud Director nicht verarbeiten**

Erweiterungsdienste, die auf RabbitMQ beruhen, können den Header `notification.type` nicht aus der Meldung abrufen, da der Header einen neuen temporären Namen aufweist. Der Header-Name für VMware Cloud Director 10.1.0 lautet `notification.operationType`.

Problemumgehung: Wenn Ihre Erweiterungsdienste RabbitMQ-Meldungen von VMware Cloud Director verarbeiten und den Meldungs-Header `notification.type` verwenden, müssen Sie sie ändern. Wenn der Header „`notification.type`“ nicht verfügbar ist, müssen die Erweiterungsdienste den Wert aus dem Header `notification.operationType` abrufen. Diese Änderung ist nur für die Version 10.1.0 erforderlich.

- **Im VMware Cloud Director Service Provider Admin Portal schlägt das Löschen eines Organisations-VDC mit einer Fehlermeldung fehl**

Wenn Sie im VMware Cloud Director Service Provider Admin Portal ein Edge-Gateway zu Ihrem Organisations-VDC hinzufügen und es dem Gateway erlauben, VMware Cloud Director Distributed Routing bereitzustellen, schlägt der Versuch, das Organisations-VDC zu löschen, mit folgender Fehlermeldung fehl: VDC-Organisationsnetzwerk kann nicht gelöscht werden.

Problemumgehung:

1. Löschen Sie mithilfe der API die VDC-Organisationsnetzwerke und die Edge-Gateways, die damit verknüpft sind.
2. Löschen Sie mithilfe der API das Organisations-VDC.

- **Wenn Sie den Anbieterzugriff auf den Legacy-API-Anmelde-Endpoint deaktivieren, funktionieren alle API-Integrationen, für die die Systemadministratoranmeldung erforderlich ist, nicht mehr,**

### **einschließlich vCloud Usage Meter und vCloud Availability for VMware Cloud Director**

Ab vCloud Director 10.0 können Sie separate VMware Cloud Director-OpenAPI-Anmelde-Endpoints für Dienstanbieter- und Mandantenzugriff auf VMware Cloud Director verwenden. Wenn der Dienstanbieterzugriff auf den Legacy-Endpoint `/api/sessions` deaktiviert ist, führt dies dazu, dass Produkte, die in VMware Cloud Director integriert sind, wie vCloud Usage Meter und vCloud Availability for VMware Cloud Director, nicht mehr funktionieren. Für diese Produkte ist ein Patch erforderlich, damit der Betrieb fortgesetzt werden kann.

Das Problem betrifft nur Systemadministratoren. Die Mandantenanmeldung ist nicht betroffen.

Problemumgehung: Aktivieren Sie mithilfe des Zellenverwaltungstools den Zugriff des Dienstanbieters auf den Legacy-Endpoint `api/sessions` erneut.

- **Wenn Sie die Werte für die garantierten Reservierungen eines VDC ändern, werden die vorhandenen VMs auch nach einem Neustart nicht entsprechend aktualisiert**

Wenn Sie über ein Flex-Organisations-VDC mit der Standardrichtlinie für das System verfügen und eingeschaltete virtuelle Maschinen auf diesem VDC mit der standardmäßigen Größenrichtlinie konfiguriert sind, wird beim Erhöhen des Werts für die garantierten Ressourcen des VDC die Ressourcenreservierung für die vorhandenen VMs nicht aktualisiert, und diese VMs werden auch nicht als nicht konform gekennzeichnet. Dieses Problem tritt auch auf, wenn Sie ein Legacy-VDC-Zuteilungsmodell in ein Flex-Zuteilungsmodell konvertieren und die vorhandenen VMs nach der Konvertierung nicht mit der neuen Standardrichtlinie des Flex-Organisations-VDC übereinstimmen.

Problemumgehung:

1. Navigieren Sie im VMware Cloud Director-Mandantenportal zum Auffinden des VM-Bezeichners zur Seite „Details“ der VM. Der Bezeichner wird in der URL `https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifizier/general` angezeigt
2. Um die nicht konformen VMs auf der VMware Cloud Director-Benutzeroberfläche anzuzeigen, führen Sie unter Verwendung der VMware Cloud Director-API eine explizite Konformitätsprüfung anhand der VMs durch.  
POST: `https://VCD_IP_Address/api/vApp/vm-Identifizier/action/checkComputePolicyCompliance`
3. Um die Richtlinie erneut anzuwenden und die Ressourcenreservierungen neu zu konfigurieren, klicken Sie im VMware Cloud Director-Mandantenportal für eine nicht konforme VM auf **VM konform machen**.

- **VMware Cloud Director zeigt falsche Informationen zu ausgeführten VMs, VMs insgesamt sowie CPU- und Arbeitsspeicherstatistiken in dedizierten vCenter Server-Instanzen an**

Wenn eine dedizierter vCenter Server-Instanz die Version 6.0 Update 3i oder früher, 6.5 Update 2 oder früher bzw. 6.7 Update 1 oder früher aufweist, zeigt VMware Cloud Director falsche Informationen zu ausgeführten VMs, VMs insgesamt sowie CPU- und Arbeitsspeicherstatistiken in der vCenter Server-Instanz an. Die dedizierte vCenter Server-Kachel im Mandantenportal und die dedizierten vCenter Server-Informationen im Service Provider Admin Portal zeigen für ausgeführte VMs und VMs insgesamt jeweils null an, selbst wenn sich virtuelle Maschinen in der vSphere-Umgebung befinden.

Problemumgehung: Führen Sie ein Upgrade der vCenter Server-Instanz auf Version 6.0 Update 3j, 6.5 Update 3 bzw. 6.7 Update 2 oder höher durch.

- **Das Ändern der Computing-Richtlinie einer eingeschalteten VM schlägt möglicherweise fehl**

Beim Versuch, die Computing-Richtlinie einer eingeschalteten VM zu ändern, tritt ein Fehler auf, wenn die neue Computing-Richtlinie einer Anbieter-VDC-Computing-Richtlinie zugeordnet ist, die VM-Gruppen oder logische VM-Gruppen aufweist. Die Fehlermeldung enthält: Zugrunde liegender Systemfehler: `com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation`.

Problemumgehung: Schalten Sie die VM aus und wiederholen Sie den Vorgang.

- **Wenn Sie das VMware Cloud Director Service Provider Admin Portal in Firefox öffnen, können die Mandanten-Netzwerkbildschirme nicht geladen werden**

Wenn Sie das VMware Cloud Director Service Provider Admin Portal in Firefox öffnen, können die Mandanten-Netzwerkbildschirme, z. B. der Bildschirm **Firewall verwalten** eines Organisations-VDC, möglicherweise nicht geladen werden. Dieses Problem tritt auf, wenn Ihr Firefox-Browser so konfiguriert ist, dass er Drittanbieter-Cookies blockiert.

Problemumgehung: Konfigurieren Sie Ihren Firefox-Browser so, dass er Drittanbieter-Cookies zulässt.

- **VMware Cloud Director 10.1 unterstützt nicht alle Eingabeparameter des vRealize Orchestrator-Workflows**

VMware Cloud Director 10.1 unterstützt die folgenden Eingabeparameter des vRealize Orchestrator-Workflows:

- boolesch
- sdkObject
- secureString
- Zahl
- mimeAttachment
- Eigenschaften
- Datum
- zusammengesetzt
- Regex
- encryptedString
- Array

Umgehung: Keine

- **Eine auf einem NFS-Array mit aktivierter VMware vSphere Storage APIs Array Integration (VAAI) oder auf vSphere Virtual Volumes (VVols) bereitgestellte virtuelle Maschine kann nicht konsolidiert werden**

In-Place-Konsolidierung einer schnell bereitgestellten virtuellen Maschine wird nicht unterstützt, wenn ein nativer Snapshot verwendet wird. Native Snapshots werden immer von VAAI-fähigen Datenspeichern sowie von VVols verwendet. Wenn eine schnell bereitgestellte virtuelle Maschine auf einem dieser Speichercontainer bereitgestellt wird, kann diese virtuelle Maschine nicht konsolidiert werden.

Problemumgehung: Aktivieren Sie die schnelle Bereitstellung nicht für ein Organisations-VDC, das VAAI-fähiges NFS oder VVols verwendet. Um eine virtuelle Maschine mit einem Snapshot auf einem VAAI- oder einem VVol-Datenspeicher zu konsolidieren, verschieben Sie die virtuelle Maschine in einen anderen Speichercontainer.

- **Bei Verwendung der VMware Cloud Director-API zum Erstellen einer VM anhand einer Vorlage und Nichtangabe einer Standardspeicherrichtlinie nutzt die neu erstellte VM die Speicherrichtlinie der Quellvorlage, wenn keine Standardspeicherrichtlinie für die Vorlage festgelegt wurde.**

Bei Verwendung der VMware Cloud Director-API zum Erstellen einer VM anhand einer Vorlage und Nichtangabe einer Standardspeicherrichtlinie verwendet die neu erstellte VM die Speicherrichtlinie der Quellvorlage, wenn keine Standardspeicherrichtlinie für die Vorlage festgelegt wurde, anstatt die Speicherrichtlinie des Organisations-VDC zu nutzen, in dem die Bereitstellung erfolgt.

Umgehung: Nein