

Versionshinweise zu VMware Cloud Director 10.2

VMware Cloud Director 10.2 | 15. Oktober 2020 | Build 17029810 (installierter Build 17008054)

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

VMware Cloud Director Version 10.2 umfasst Folgendes:

- **Erweiterte funktionale Parität für NSX-T:** NSX Advanced Load Balancer (Avi), verteilte Firewall, VRF-lite, VDC-übergreifende Netzwerke, IPv6, Dual Stack (IPv4/IPv6) im selben Netzwerk, SLAAC, DHCPv6, CVDS (vSphere 7.0/NSX-T 3.0), L2VPN – nur API
- **Unterstützung moderner Anwendungen in VMware Cloud Director mit Tanzu-Laufzeit vSphere with Kubernetes:** Anbieter- und Mandantenbenutzeroberfläche für die Verwaltung und den Verbrauch von Kubernetes-Clustern
- **Verbesserungen bei der virtuellen VMware Cloud Director-Appliance:** Validierung der Benutzereingabe während der ersten Bereitstellung; vereinfachte Wiederherstellung von Zellen mit optimierter Standby-Zellerstellung
- **Verbesserungen beim Speicher:** IOPS-Steuerung auf Festplattenebene für Anbieter und Mandanten; freigegebene Festplatten
- **Verbesserungen bei der Sicherheit:** Informationen hierzu finden Sie im Abschnitt [Sicherheit](#).
- **Verbesserungen bei der Benutzeroberfläche:** Schnellsuche; Empfehlungen; Zertifikatsverwaltung
- **Verbesserungen bei der Plattformerweiterbarkeit**
- **Verbesserungen bei der Skalierung:** Weitere Informationen finden Sie unter [Maximalwerte für VMware-Konfiguration](#)

Informationen zu den neuen und aktualisierten Funktionen dieser Version finden Sie unter [Neuheiten in VMware Cloud Director 10.2](#).

Die neuesten Versionshinweise für die VMware Cloud Director-Add-on-Lösungen finden Sie unter den folgenden Links:

- [Container Service Extension 3.0](#)
- [Object Storage Extension 2.0](#)
- [App Launchpad 2.0](#)
- [Terraform](#)
- [Tenant App 2.5](#)

Sicherheit

Im Lieferumfang der virtuellen Appliance für VMware Cloud Director 10.2 ist Photon OS mit erfolgreichem Update entsprechend dieser [Photon-Sicherheitsempfehlung](#) enthalten.

VMware Cloud Director 10.2 unterstützt PKCS12-Keystores. Sie können einen mit PKCS12 formatierten Keystore verwenden, wenn Sie die Netzwerk- und Datenbankverbindungen von VMware Cloud Director konfigurieren oder das Zellenverwaltungstool zum Generieren oder Ersetzen von Zertifikaten verwenden. Weitere Informationen finden Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

Hinweise zu Produktunterstützung

TKG-Clusterknoten werden isoliert. Die in einem TKG-Cluster verfügbaren Dienste sind jedoch für jeden mit Netzwerkzugriff auf die virtuelle IP oder den Endpoint des Diensts zugänglich und werden durch die eigenen Authentifizierungs- und Autorisierungsmechanismen der Dienste geschützt. Da die Authentifizierung der einzige Schutz für den sicheren Zugriff auf die Arbeitslasten ist, wird dringend empfohlen, nur verschlüsselten Datenverkehr, wie z. B. TLS, für die Dienste mit eingehendem Datenverkehr zuzulassen.

Warnungen zum Ende der Lebensdauer und zum Ende der Unterstützung

- VMware Cloud Director API Version 29 und niedriger wird nicht unterstützt.
- VMware Cloud Director API Version 30 und 31 sind veraltet.
- VMware Cloud Director API Version 30 wird in der nächsten Version nicht mehr verfügbar sein.
- Der API-Anmelde-Endpoint `/api/sessions` wird seit VMware Cloud Director API Version 33.0/VMware Cloud Director 10.0 als veraltet betrachtet 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 für die Protokolle HTTP und HTTPS veraltet. Das Entfernen von `/cloud/server_status` erfolgt in einer zukünftigen VMware Cloud Director-Version. Sie müssen `/api/server_status` für HTTP- und HTTPS-Protokolle verwenden.
- Die Zurücksetzaktionen `/amqp/action/resetAmqpCertificate` und `/amqp/action/resetAmqpKeyStore` werden aufgrund der Art und Weise, wie VMware Cloud Director SSL-Zertifikate speichert und verarbeitet, aus VMware Cloud Director API Version 35.0 entfernt. Sie müssen den Endpoint `/cloudapi/1.0.0/ssl/trustedCertificates` verwenden, um Zertifikate als nicht vertrauenswürdig einzustufen.
- Die Aktualisierungsaktionen `/amqp/action/updateAmqpCertificate` und `/amqp/action/updateLdapKeyStore` sind veraltet. Das Entfernen der Aktionen erfolgt in einer zukünftigen VMware Cloud Director-Version. Sie können den neuen Endpoint verwenden, um AMQP-Zertifikate als vertrauenswürdig einzustufen: `/cloudapi/1.0.0/ssl/trustedCertificates`.
- 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, ab 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 der nächsten vSphere- und VMware Cloud Director-Version nicht mehr unterstützt.
- DSA- und DSS-Zertifikate werden nicht mehr unterstützt, da keine empfohlenen Verschlüsselungs-Suites für sie verfügbar sind.

Upgrade von früheren Versionen

Weitere Informationen zum Upgrade auf VMware Cloud Director 10.2, 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 10.2 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
- NSX Advanced Load Balancer (Avi) – Diese Version von Cloud Director unterstützt derzeit lediglich NSX Advanced Load Balancer (Avi) 20.1.1

Unterstützte VMware Cloud Director-Serverbetriebssysteme

- CentOS 7
- CentOS 8
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8

Bereitstellen der VMware Cloud Director-Appliance

Wenn Sie die VMware Cloud Director-Appliance der Version 10.2 mithilfe des VMware OVF Tool als OVF-Vorlage bereitstellen, müssen Sie den folgenden, für Version 10.2 neuen Parameter einschließen: `--x:enableHiddenProperties`. Wenn Sie diesen Parameter nicht angeben, schlägt das VMware OVF Tool mit einem Fehler ähnlich dem folgenden fehl: Eigenschaft

`vcloudapp.nfs_mount.VMware_vCloud_Director` kann nicht vom Benutzer konfiguriert werden..

Weitere Informationen finden Sie unter [Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool](#).

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 3.8.x.

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

Unterstützte Datenbanken für das Speichern von historischen Metrikdaten

VMware Cloud Director unterstützt Apache Cassandra-Versionen 3.11.x.

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

Hinweis: Internet Explorer 11 wird in VMware Cloud Director 10.2 und höher nicht unterstützt. Sie können Microsoft Edge oder einen anderen unterstützten Browser verwenden. Wenn Sie Internet Explorer 11 verwenden müssen, ist es möglicherweise empfehlenswert, dass Sie bei VMware Cloud Director Version 10.0.x oder 10.1.x bleiben, bis Sie einen anderen Browser verwenden können.

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

- **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 folgendem Fehler fehl: Neue und veraltete Werte wurden zusammen für die Neuverteilung aktualisiert. Fehlercode 503266.
- **Das Verschieben einer VM über Cluster hinweg schlägt fehl, wenn es sich bei dem Zielspeichercontainer um einen Datenspeicher-Cluster handelt**
Das Verschieben einer VM über Cluster hinweg schlägt fehl, wenn es sich bei dem Zielspeichercontainer um einen Datenspeicher-Cluster handelt. In den Protokollen wird der folgende Fehler aufgeführt.

```
2020-05-18 15:51:12,083 | ERROR | task-service-activity-pool-23 | SdrsPlacementManagerImpl | SDRS invocation error  
| requestId=aaa593e5-e051-4423-ac02-97ad09a39f4c,request=POST https://bos1-vcd-sp-static-203-38.eng.vmware.com/ap  
i/vApp/vm-c2b0ee1f-02f1-4377-8852-a9711c2a571e/action/reconfigureVm,requestTime=1589817067877,remoteAddress=10.150.203.38:32049,userAgent=Mozilla/5.0  
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 ...,accept=application/*+xml;version 3 4.0 vcd=6e36bc7a-3850-4f2a-a057-d96758ef5f5be,task=1e8217b8-88f1-41f8-8292-1bb6178b0b3e activity=  
(com.vmware.vcloud.backendbase.management.system.TaskActivity,urn:uuid:1e8217b8-88f1-41f8-8292-1bb6178b0b3e)  
(vmodl.fault.InvalidArgument) { faultCause = null, faultMessage = null, invalidProperty = spec.host }
```

- **Appliance kann nicht bereitgestellt werden, wenn die Einstellung „Root-Kennwort läuft bei der ersten Anmeldung ab“ aktiviert ist**
Wenn Sie versuchen, eine Appliance bereitzustellen, schlägt die Bereitstellung fehl und ein Fehler ähnlich dem folgenden wird im Protokoll /opt/vmware/var/log/firstboot aufgeführt:
Invoking postgresauth script ... sudo: Account or password is expired, reset your password and try again Changing password for root. sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper sudo: unable to change expired password: Authentication token manipulation error cp: cannot stat '/var/vmware/vpostgres/current/.ssh/id_rsa': No such file or directory chown: cannot access '/opt/vmware/vcloud-director/id_rsa': No such file or directory [ERROR] postgresauth script failed to execute.
- **Im VMware Cloud Director-Mandantenportal funktioniert die erweiterte Filterung von VMs basierend auf dem VDC-Standort nicht**
Wenn Sie auf der Benutzeroberfläche des VMware Cloud Director-Mandantenportals versuchen, die auf dem VDC-Standort basierende erweiterte Filterung zum Filtern von VMs zu verwenden, schlägt die Suche mit einer Fehlermeldung fehl.

Bekannte Probleme

- **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.

Problemumgebung:

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 Der Status des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP) lautet **Enabled**, auch wenn die entsprechende Option während der Installation von VMware Cloud Director deaktiviert wurde**

Wenn Sie während der Installation von VMware Cloud Director die Option zum CEIP-Beitritt deaktivieren, ist der CEIP-Status nach Abschluss der Installation aktiv.

Problemumgehung: Deaktivieren Sie das CEIP, indem Sie die Schritte im Verfahren [Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit oder Verlassen des Programms](#) ausführen.

- **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 Nach dem Upgrade auf vCenter Server 7.0 Update 2a oder Update 2b können Sie keine Tanzu Kubernetes Grid-Cluster erstellen**

Wenn die zugrunde liegende vCenter Server-Version 7.0 Update 2a oder Update 2b lautet und Sie versuchen, einen Tanzu Kubernetes Grid-Cluster mithilfe des Kubernetes Container Clusters-Plug-Ins zu erstellen, schlägt die Aufgabe fehl.

Umgehung: Nein

- **Neu Die Erstellung des Tanzu Kubernetes-Clusters unter Verwendung des Kubernetes-Container-Cluster-Plug-Ins schlägt fehl**

Wenn Sie einen Tanzu Kubernetes-Cluster mithilfe des Kubernetes-Container-Cluster-Plug-Ins erstellen, müssen Sie eine Kubernetes-Version auswählen. Einige der Versionen im Dropdown-Menü sind nicht mit der unterstützten vSphere-Infrastruktur kompatibel. Wenn Sie eine nicht kompatible Version auswählen, schlägt die Clustererstellung fehl.

Problemumgehung: Löschen Sie den fehlgeschlagenen Clusterdatensatz und versuchen Sie es mit einer kompatiblen Tanzu Kubernetes-Version. Informationen zu den Inkompatibilitäten zwischen Tanzu Kubernetes und vSphere finden Sie unter [Aktualisieren der vSphere with Tanzu-Umgebung](#).

- **Neu Wenn ein Speicher-Pod oder Cluster eine Speicherrichtlinie unterstützt, können Sie die VMware Cloud Director-IOPS-Begrenzung für diese Speicherrichtlinie nicht aktivieren**

Wenn im Dienstleister-Adminportal ein oder mehrere Speicher-Pods oder Cluster eine Speicherrichtlinie unterstützen, können Sie die VMware Cloud Director-IOPS-Begrenzung für diese Speicherrichtlinie nicht aktivieren, selbst wenn Sie das Flag **Auswirkung auf Platzierung** deaktivieren.

Problemumgehung: Sie müssen über Zugriff auf Administratorebene verfügen, um dieses Problem zu umgehen.

1. Entfernen Sie in vCenter Server das Tag der Speicherrichtlinie aus allen Speicher-Pods, für die Sie IOPS aktivieren möchten, und aktualisieren Sie die Speicherrichtlinien.
2. Aktivieren Sie in VMware Cloud Director die IOPS-Beschränkung von VMware Cloud Director für die Speicherrichtlinie, indem Sie das Flag **Auswirkungen auf die Platzierung** deaktivieren.
3. Verbinden Sie in vCenter Server das Tag erneut mit den Speicher-Pods und aktualisieren Sie die Speicherrichtlinien.

- **Neu Wenn Sie die Liste der virtuellen Maschinen in einer vApp öffnen und die Option „Mehrfachauswahl“ aktivieren, steht das Menü „Aktionen“ nicht mehr zur Verfügung**

Wenn Sie die Liste der virtuellen Maschinen in einer vApp öffnen und die Option „Mehrfachauswahl“ aktivieren, steht das Menü „Aktionen“ nicht mehr zur Verfügung. Sie können mehrere virtuelle Maschinen auswählen, aber Sie können keine Aktionen gleichzeitig ausführen.

Umgehung: Nein

- **Neu Sie können die Einstellungen für die Netzwerkkarte einer eigenständigen virtuellen Maschine nicht bearbeiten**

Sie können die Einstellungen für die Netzwerkkarte einer eigenständigen virtuellen Maschine nicht aktualisieren. Wenn Sie auf „Bearbeiten“ klicken, um die Netzwerkkarteneinstellungen der virtuellen Maschine zu öffnen, wird die Seite „Einstellungen“ geöffnet, reagiert jedoch nicht mehr.

Problemumgehung:

1. Konvertieren Sie die eigenständige virtuelle Maschine in eine vApp.

2. Bearbeiten Sie die Einstellungen für die Netzwerkkarte der vApp.
3. Konvertieren Sie die vApp wieder in eine eigenständige virtuelle Maschine.

- **Neu Nachdem Sie die Veröffentlichungseinstellungen eines abonnierten Katalogs über die Benutzeroberfläche des Mandantenportals aktualisiert haben, schlägt die Synchronisierung dieses Katalogs mit dem Fehler „401 Nicht autorisiert“ fehl**

Nachdem Sie die **Veröffentlichungseinstellungen** eines abonnierten Katalogs über die Benutzeroberfläche des Mandantenportals aktualisiert haben, schlägt die Synchronisierung dieses Katalogs mit dem Fehler 401 Nicht autorisiert fehl. Dies ist der Fall, weil beim Aktualisieren der Katalogeinstellungen das vorhandene Kennwort gelöscht und auf null gesetzt wird.

Problemumgehung: Aktualisieren Sie die **Veröffentlichungseinstellungen** des Katalogs und setzen Sie das Kennwort erneut über die Benutzeroberfläche des Mandantenportals fest.

- **Neu Beim Upgrade von VMware Cloud Director von Version 10.1.2 auf Version 10.2 wird fälschlicherweise ein Fehler gemeldet**

Während des Upgrades von VMware Cloud Director auf Version 10.2 von Version 10.1.2 wird die folgende ungenaue Fehlermeldung angezeigt:

FEHLER: RPM ist für eine andere Version von VMware Cloud Director bereits installiert, aber diese Version wird nicht erkannt und ein Upgrade von dieser Version wird nicht unterstützt. Es wird nicht erwartet, dass dieses Upgrade erfolgreich ist, aber Sie können trotzdem auf eigenes Risiko fortfahren.

Das Upgrade von VMware Cloud Director von Version 10.1.2 auf Version 10.2 wird unterstützt, und Sie müssen die Fehlermeldung ignorieren.

Problemumgehung: Ignorieren Sie den Fehler.

- **Wenn Sie die VMware Cloud Director-Appliance, die Dienste-API oder die Benutzeroberfläche für die Appliance-Verwaltung neu starten, wird unter Umständen eine Meldung ausgegeben, dass sich der Dienst „vmware-vcd“ in einem fehlgeschlagenen Zustand befindet**

Wenn Sie die VMware Cloud Director-Appliance, die Dienste-API oder die Benutzeroberfläche für die Appliance-Verwaltung neu starten, wird unter Umständen fälschlicherweise eine Meldung ausgegeben, dass sich der Dienst vmware-vcd in einem fehlgeschlagenen Zustand befindet. Dies tritt auf, wenn versucht wird, den Dienst vmware-vcd zu starten, bevor der OS-Netzwerkstapel verfügbar wird. Dies führt dazu, dass der Dienst in einen fehlgeschlagenen Zustand versetzt wird und eine Fehlermeldung anzeigt, dass die Bindung des Diensts an einen oder mehrere Ports fehlgeschlagen ist. In der Folge startet vcd-watchdog den Dienst vmware-vcd erfolgreich, aber der Systemstatus systemd spiegelt dies nicht wider.

Problemumgehung:

1. Führen Sie `systemctl reset-failed vmware-vcd.service` aus.
2. Führen Sie `systemctl start vmware-vcd.service` aus.

- **Wenn Sie in Ihrer Organisation über abonnierte Kataloge verfügen und ein Upgrade von VMware Cloud Director durchführen, schlägt die Katalogsynchronisierung fehl**

Wenn Sie in Ihrer Organisation über abonnierte Kataloge verfügen, vertraut VMware Cloud Director nach dem Upgrade den veröffentlichten Endpoint-Zertifikaten nicht automatisch. Die Inhaltsbibliothek kann nicht synchronisiert werden, wenn die Zertifikate nicht als vertrauenswürdig eingestuft sind.

Problemumgehung: Stufen Sie die Zertifikate für jedes Katalogabonnement manuell als vertrauenswürdig ein. Wenn Sie die Einstellungen des Katalogabonnements bearbeiten, werden Sie in einem „Trust on First Use“-Dialogfeld (TOFU) dazu aufgefordert, dem Remote-Katalogzertifikat zu vertrauen.

Wenn Sie nicht über die erforderlichen Rechte zum Einstufen des Zertifikats als vertrauenswürdig verfügen, wenden Sie sich an den Administrator Ihrer Organisation.

- **Nach dem Upgrade von VMware Cloud Director und dem Aktivieren der Tanzu Kubernetes-Clustererstellung ist keine automatisch generierte Richtlinie verfügbar, und Sie können keine Richtlinie erstellen oder veröffentlichen**

Wenn Sie ein Upgrade von VMware Cloud Director auf Version 10.2 und von vCenter Server auf Version 7.0.0d durchführen und ein von einem Supervisor-Cluster gestütztes Provider-VDC erstellen, wird in VMware Cloud Director neben dem VDC ein Kubernetes-Symbol angezeigt. Es ist jedoch keine automatisch generierte Kubernetes-Richtlinie im neuen Provider-VDC vorhanden. Wenn Sie versuchen, eine Kubernetes-Richtlinie für ein Organisations-VDC zu erstellen oder zu veröffentlichen, sind keine Maschinenklassen verfügbar.

Problemumgehung: Stufen Sie das Kubernetes-Endpoint-Zertifikat manuell als vertrauenswürdig ein. Detaillierte Schritte finden Sie unter <https://kb.vmware.com/s/article/80996>.

- **Das Plug-In zum Einrichten von DRaaS und Migration wird in der oberen Navigationsleiste auf der VMware Cloud Director-Benutzeroberfläche zweimal angezeigt**

Dieses Problem tritt aufgrund des Rebranding von vCloud Availability 4.0.0 zu VMware Cloud Director Availability 4.0.0 auf. Seitdem gibt es zwei Plug-Ins. VMware Cloud Director deaktiviert das vCloud Availability 4.0.0-Plug-In nicht automatisch. Die alte und die neue Version werden in der oberen Navigationsleiste unter **Mehr** als das Plug-In zum Einrichten von DRaaS und Migration angezeigt.

Problemumgehung: Deaktivieren Sie das vCloud Availability 4.0.0-Plug-In manuell.

- **Eine Provider-VDC-Kubernetes-Richtlinie kann nicht für ein VDC veröffentlicht werden, wenn der Supervisor-Cluster, auf den sie verweist, nicht der primäre Cluster im Provider-VDC ist**

Wenn Sie über ein Provider-VDC mit mehreren Supervisor-Clustern verfügen, schlägt das Veröffentlichen einer Provider-VDC-Kubernetes-Richtlinie, die auf einen nicht primären Supervisor-Cluster verweist, mit einem `LMException`-Fehler fehl.

Problemumgehung: Stellen Sie sicher, dass das Provider-VDC von nur einem Supervisor-Cluster gestützt wird und dass der Cluster der primäre Cluster ist. Ein Provider-VDC kann von Host-Clustern und von einem Supervisor-Cluster gestützt werden, aber der Supervisor-Cluster muss der primäre Cluster sein.

- **Wenn Sie einen Kubernetes-Clusternamen mit nicht lateinischen Zeichen eingeben, wird die Schaltfläche „Weiter“ im Assistenten zum Erstellen eines neuen Clusters deaktiviert**

Das Kubernetes-Container-Cluster-Plug-In unterstützt ausschließlich lateinische Zeichen. Wenn Sie nicht lateinische Zeichen eingeben, wird sinngemäß der folgende Fehler angezeigt. Der Name muss mit einem Buchstaben beginnen und darf nur alphanumerische Zeichen und Bindestrich (-) enthalten. (Maximum: 128 Zeichen)

Umgehung: Nein

- **Im Kubernetes-Container-Cluster-Plug-In werden Datenraster während des Ladens möglicherweise leer angezeigt**
Im Kubernetes-Container-Cluster-Plug-In werden manche Datenraster während des Ladens leer angezeigt, weil der Wartekreislauf für den Ladevorgang nicht angezeigt wird.

Umgehung: Nein

- **Nach dem Ändern der Größe eines TKGI-Clusters werden manche Werte im Datenraster leer oder als nicht anwendbar angezeigt**

Wenn Sie die Größe eines TKGI-Clusters (VMware Tanzu Kubernetes Grid Integrated Edition) ändern, werden die Clusterwerte für die Organisation und das VDC in der Datenrasteransicht leer oder als nicht anwendbar angezeigt.

Umgehung: Nein

- **Wenn Sie ein Raster mit mehreren Auswahlmöglichkeiten filtern, werden die gefilterten Elemente nicht mehr angezeigt, wenn Sie zu einer anderen Seite navigieren**

Wenn Sie in Rastern mit mehreren Auswahlmöglichkeiten die Ergebnisse filtern und mehr als eine Seite verfügbar ist, werden die nächsten Seiten der gefilterten Ergebnisse leer angezeigt. Dieses Problem tritt in Dialogfeldern auf, in denen Sie mehrere Elemente aus einer Liste auswählen und filtern können, z. B. beim Hinzufügen von Speicherrichtlinien zu einem Organisations-VDC oder bei der Freigabe einer vApp oder einer VM für Benutzer oder Gruppen.

Problemumgehung: Ändern Sie die Größe der jeweiligen Spalten.

- **Das Filtern von Empfehlungen nach Prioritätsergebnissen führt zu einem internen Serverfehler**

Wenn Sie die VMware Cloud Director-API verwenden, schlägt das Anwenden eines Prioritätsfilters auf eine Empfehlung mit einem Fehler fehl.

```
"minorErrorCode": "INTERNAL_SERVER_ERROR" "message": "[ d0ec01b3-019f-4ed2-a012-1f7f5e33cb7f ] java.lang.String cannot be cast to java.lang.Integer"
```

Problemumgehung: Rufen Sie alle Empfehlungen ab und filtern Sie sie manuell.

- **Die API-Dokumentation enthält eine unzutreffende Beschreibung der Sortierreihenfolge für die Priorität von Empfehlungen**

Das Empfehlungs-Modellobjekt enthält ein Prioritätsfeld zum Angeben der Dringlichkeit für jede von Ihnen erstellte Empfehlung. In der Dokumentation zur Empfehlungs-API wird fälschlicherweise angegeben, dass die Prioritäten in absteigender Sortierreihenfolge aufgelistet werden. Die Dokumentation zur VMware Cloud Director-API listet die Prioritäten für eine Empfehlung in aufsteigender Reihenfolge auf.

Umgehung: Nein

- **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

- **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.
- **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 Dienstanbieters auf der VMware Cloud Director 10.1-Site, wechseln zum Dialogfeld **Bearbeiten** des Diensts und klicken auf **Speichern**.
- **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

- **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.

- **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.

- **Nach dem Upgrade von vCloud Director 10.0 treten bei einer VM, die anhand einer Linux-Vorlage mit aktivierter Anpassung des Gastbetriebssystems und IPv6-Konnektivität neu bereitgestellt wurde, Probleme mit der Netzwerkonnektivität auf**

Wenn Sie nach dem Upgrade von vCloud Director 10.0 eine neue VM mithilfe einer in Version 10.0 erstellten Linux-VM-Vorlage mit aktivierter Anpassung des Gastbetriebssystems und IPv6-Konnektivität bereitstellen, treten bei der bereitgestellten VM Probleme mit der Netzwerkkonnektivität auf. Ursache: Während der Bereitstellung werden doppelte Einträge für die Parameter VM_DOMAIN_NAME und VM_HOST_NAME in der Datei /etc/hosts der VM erstellt.

Problemumgehung: Entfernen Sie die doppelten Einträge für die Parameter VM_DOMAIN_NAME und VM_HOST_NAME aus der Datei /etc/hosts der VM.

- **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