

Versionshinweise zu VMware Cloud Director 10.2.2

VMware Cloud Director 10.2.2 | 8. April 2021 | Build 17855679 (installierter Build 17855680)

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

Inhalt dieses Dokuments

- [Neuheiten](#)
- [Systemanforderungen und Installation](#)
- [Dokumentation](#)
- [Vorherige Versionen von VMware Cloud Director 10.2.x](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

Neuheiten

VMware Cloud Director Version 10.2.2 umfasst Folgendes:

- **VMware Tanzu Mission Control unterstützt in VMware Cloud Director bereitgestellte Tanzu Kubernetes-Cluster** – Sie können einen in VMware Cloud Director bereitgestellten Kubernetes-Cluster an Tanzu Mission Control anhängen. Folglich wird der Cluster in der Tanzu Mission Control-Konsole angezeigt. Informationen zum Anhängen eines vorhandenen Clusters an Ihre VMware Tanzu Mission Control-Organisation finden Sie unter [Anhängen eines vorhandenen Clusters](#) in der *VMware Tanzu Mission Control-Produktdokumentation*.
- **Mandantennetzwerkisolierung bei Tanzu Kubernetes-Clustern** – Tanzu Kubernetes-Cluster sind nur von Arbeitslasten innerhalb desselben Organisations-VDC aus erreichbar, in dem ein Cluster erstellt wird. Bei Bedarf können Sie den externen Zugriff auf bestimmte Dienste in einem Tanzu Kubernetes-Cluster manuell konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren des externen Zugriffs auf einen Dienst in einem Tanzu Kubernetes-Cluster](#) im *VMware Cloud Director-Mandantenportal-Handbuch*.
- **Auswahl von Tanzu Kubernetes-Cluster-Pod- und -Dienste-CIDR** – Während der Erstellung eines Tanzu Kubernetes-Clusters können Sie bestimmte Bereiche von IP-Adressen für Kubernetes-Dienste und -Pods angeben. Weitere Informationen finden Sie unter [Erstellen eines Tanzu Kubernetes-Clusters](#) im *Handbuch für das VMware Cloud Director-Mandantenportal*.
- **VMware Cloud Director verwendet sein Verwaltungsnetzwerk für die Kommunikation mit Tanzu Kubernetes-Clustern** – Das VMware Cloud Director-Verwaltungsnetzwerk ist ein privates Netzwerk, das der Cloud-Infrastruktur dient und Clientsystemen den Zugriff zum Ausführen von Verwaltungsaufgaben in VMware Cloud Director ermöglicht. Frühere Versionen nutzen das Kubernetes-Dienstnetzwerk.
- **SNMP-Agent für VMware Cloud Director-Appliance** – Sie können den Agent so konfigurieren, dass er Abrufanforderungen abhört. Wenn bereits ein Net-SNMP-Agent vorhanden ist, ersetzt die VMware Cloud Director-Appliance während des Upgrades die Net-SNMP-Installation durch VMware-SNMP. Während der Einrichtung von VMware-SNMP konfiguriert die VMware Cloud Director-Appliance die für den SNMP-Vorgang benötigten Firewallregeln dynamisch. Sie müssen vor dem Upgrade alle vorhandenen Firewallregeln entfernen, die mit Net-SNMP funktionieren. Weitere Informationen finden Sie unter [Konfigurieren des SNMP-Agent für die VMware Cloud Director-Appliance](#) im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.
- **Globale Platzierungsrichtlinie** – Dienstanbieter können Platzierungsrichtlinien definieren, die über alle vCenter Server-Instanzen und Cluster in einer VMware Cloud Director-Umgebung hinweg effektiv funktionieren. Eine einzelne Platzierungsrichtlinie kann auf Hosts verweisen, die mehrere Cluster in einer oder mehreren vCenter Server-Instanzen umfassen. Grenzen in der zugrunde liegenden Infrastruktur werden hinter dem globalen logischen Konstrukt einer Platzierungsrichtlinie abstrahiert, wodurch sich eine logischere Erfahrung für Dienstanbieter und Mandanten ergibt. Diese Änderung ermöglicht das Erfassen der Platzierungsrichtlinie, wenn eine vApp-Vorlage anhand einer VM erstellt wird. Die resultierende vApp-Vorlage erbt jede Platzierungsrichtlinie von der ursprünglichen VM, selbst wenn sich VM und vApp-Vorlage in unterschiedlichen Provider-VDCs befinden. Es wird empfohlen, eine eindeutige Benennungskonvention für die

Platzierungsrichtlinien zu verwenden. Weitere Informationen finden Sie unter [Eine globale VM-Platzierungsrichtlinie erstellen](#) im *Handbuch für das VMware Cloud Director Service Provider Admin Portal*.

- **Gastanpassung für verschlüsselte VMs** – VMware Cloud Director 10.2.2 unterstützt die Gastanpassung von VMs, die auf verschlüsseltem Speicher ausgeführt werden.
- **Vorlagen für Organisations-VDCs** – Sie können VDC-Vorlagen erstellen und für Mandantenorganisationen freigeben, sodass Organisationsadministratoren die Vorlagen zum Erstellen von VDCs nutzen können. VMware Cloud Director 10.2.2 unterstützt die Nutzung eines NSX-T-basierten Netzwerks mit den Organisations-VDC-Vorlagen.
- **Aktualisierung von Speicherrichtlinien** – Dienstleister können mithilfe von Speicherrichtlinien in VMware Cloud Director ein mehrstufiges Speicherangebot erstellen, z. B. Gold, Silver und Bronze, oder Mandanten sogar dedizierten Speicher anbieten. Durch die Erweiterung von Speicherrichtlinien um die Unterstützung von VMware Cloud Director-Entitäten haben Sie die Flexibilität zu steuern, wie Sie die Speicherrichtlinien verwenden. Sie können nicht nur über mehrstufigen Speicher verfügen, sondern auch über isolierten Speicher für die Ausführung von VMs, Containern, Edge-Gateways usw.

Der Bedarf an gemeinsam genutztem Speicher über Cluster hinweg oder an einem preisgünstigeren Speicher für nicht ausgeführte Arbeitslasten ist ein gängiger Anwendungsfall, der mit diesem Update befriedigt wird. Anstatt eine Speicherrichtlinie mit allen VMware Cloud Director-Entitäten zu verwenden, können Sie ihre Speicherrichtlinie beispielsweise in eine *Arbeitslastspeicherrichtlinie* für alle ausgeführten VMs und Container und eine *Katalogspeicherrichtlinie* für längerfristige Speicherung aufteilen. Eine langsamere oder kostengünstige NFS-Option kann die *Katalogspeicherrichtlinie* sichern, während die *Arbeitslastspeicherrichtlinie* unter vSAN ausgeführt werden kann.

- **FIPS-** Diese VMware Cloud Director-Version umfasst die Unterstützung von Federal Information Processing Standards. Sowohl die VMware Cloud Director-Appliance als auch die Linux-Binärdatei können im FIPS-kompatiblen Modus ausgeführt werden. Der FIPS-Modus ist standardmäßig deaktiviert. Die Aktivierung des FIPS-Modus kann sich auf die Leistung von VMware Cloud Director auswirken. Wenn die Metrikerfassung konfiguriert ist, überprüfen Sie die Konfiguration der Server- und Clientkommunikation mit Cassandra über SSL. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren des FIPS-Modus in der VMware Cloud Director-Appliance](#) im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*. Alternativ finden Sie weitere Informationen zum Aktivieren von VMware Cloud Director unter Linux unter [FIPS-Modus für die Zellen in der Servergruppe aktivieren](#) im *Handbuch für das VMware Cloud Director Service Provider Admin Portal*.
- **Direkte Unterstützung von VDC-Netzwerken in Organisations-VDCs, die durch NSX-T Data Center gesichert sind** – Dienstleister können direkte VDC-Organisationsnetzwerke in VDCs erstellen, die durch NSX-T Data Center gesichert sind.
- **Automatische Skalierung** – Skalierungsgruppen sind ein neues Objekt auf oberster Ebene, das Mandanten dazu nutzen können, um automatisierte horizontale Verkleinerungs (Scale-in)- und Vergrößerungs (Scale-out)-Ereignisse in eine Arbeitslastengruppe zu implementieren. Sie können Auto-Skalierungsgruppen mit einer vApp-Quellvorlage, einem Lastausgleichsdiens-Netzwerk und einem Regelsatz für das Vergrößern oder Verkleinern der Gruppe basierend auf der CPU- und Arbeitsspeichernutzung konfigurieren. VMware Cloud Director fährt VMs in einer Skalierungsgruppe automatisch hoch oder herunter. Weitere Informationen finden Sie unter [Auto-Skalierung von Gruppen](#) im *Handbuch für das VMware Cloud Director-Mandantenportal*.
- **Update zu geführten Touren** – Dienstleister können benutzerdefinierte geführte Touren veröffentlichen und die Tour für Systemadministratoren oder Mandanten analysieren. Ab VMware Cloud Director 10.2.2 können Sie geführte Touren aus einem VMware Github-Repository oder einem benutzerdefinierten Github-Repository herunterladen.
- **Statische T-Shirt-Größe entfernen** – VMware Cloud Director 10.2.2 unterstützt nicht mehr die Verwendung der vordefinierten virtuellen Maschinengrößen, die seit vCloud Director for Service Providers 9.0 verfügbar sind. Sie können die VM-Größenrichtlinienfunktion verwenden, um eine vordefinierte VM-Größenrichtlinie bereitzustellen.

Systemanforderungen und Installation

Informationen zu den Systemanforderungen und Installationsanweisungen finden Sie in den [Versionshinweisen zu VMware Cloud Director 10.2](#).

Informationen zur Konfiguration und Größenanpassung der Appliance finden Sie in den Richtlinien unter [VMware Cloud Provider Pod Designer - VMware Validated Designs for Cloud Providers](#).

Standardmäßig aktivierte Verschlüsselungs-Suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

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*.

Bereitstellen der VMware Cloud Director-Appliance

In bestimmten Fällen wird die Datei `vami_firstboot` nach der Bereitstellung der VMware Cloud Director-Appliance nicht automatisch gelöscht. Deshalb wird die Appliance beim nächsten Ein-/Ausschalten oder Neustarten der Appliance neu initialisiert. Führen Sie zur Vermeidung dieses Problems nach der Bereitstellung die folgenden Schritte auf jeder Appliance in der Servergruppe aus.

1. Stellen Sie fest, ob die Datei `/opt/vmware/etc/vami/flags/vami_firstboot` auf der VMware Cloud Director-Appliance vorhanden ist.
2. Wenn die Datei vorhanden ist, führen Sie zum Löschen der Datei folgenden Befehl aus.
`rm /opt/vmware/etc/vami/flags/vami_firstboot`

Dokumentation

Die vollständige Produktdokumentation finden Sie unter [Dokumentation zu VMware Cloud Director](#).

Vorherige Versionen von VMware Cloud Director 10.2.x

[Versionshinweise zu VMware Cloud Director 10.2.1](#)

[Versionshinweise zu VMware Cloud Director 10.2](#)

Behobene Probleme

- **Nach dem Upgrade auf VMware Cloud Director 10.2.x schlägt die Ausführung eines CMT-Befehls auf Cassandra mit SSL mit einer Fehlermeldung fehl**
Wenn Sie das Zellenverwaltungstool zum Konfigurieren oder erneuten Konfigurieren von Cassandra mit SSL verwenden, schlägt der Vorgang mit einer Fehlermeldung fehl.
Der VCD-SSL-Kontext kann nicht geladen werden.
- **Neu Nach dem Deaktivieren des Beitritts einer VM zu einer Domäne schlägt die Aktualisierung der VM-Hardwareeigenschaften mit einer Fehlermeldung fehl**
Wenn Sie den Beitritt einer VM zu einer Domäne deaktivieren, schlägt die Aktualisierung der Hardwareeigenschaften derselben VM mit einer Fehlermeldung fehl.
Fehler: <Domain name> sollte bei deaktiviertem Domänenbeitritt nicht angegeben werden.
- **Neu Nach dem Aktivieren des Beitritts einer VM zu einer Domäne schlägt die Aktualisierung der VM-Hardwareeigenschaften mit einer Fehlermeldung fehl**
Wenn Sie die Option „Diese VM aktivieren“ konfigurieren, um der Gastanpassung der Domäne beizutreten, schlägt die Aktualisierung der Hardwareeigenschaften derselben VM mit einer Fehlermeldung fehl.
Fehler: <UUID> Domänenname, Benutzername und Kennwort müssen angegeben werden, wenn „Domäne beitreten“ ausgewählt wurde
- **Wenn Sie eine vApp in einem Organisations-VDC mit einem Reservierungspool-Zuweisungsmodell von einer Vorlage instanziierten, weisen die bereitgestellten VMs falsche Konfigurationen auf.**
Dieses Problem tritt auf, wenn ein VDC mit dem Zuweisungsmodell ohne Reservierungspool einen Katalog unterstützt. Durch das Speichern einer vApp-Vorlage in diesem Katalog und das Instanziiieren einer vApp daraus in einem Organisations-VDC mit dem Reservierungspool-Zuweisungsmodell kommt es zu VMs mit falschen Konfigurationen für die Arbeitsspeicherreservierung und den Arbeitsspeichergrenzwert.

- **Wenn Sie versuchen, eine VM aus einer vApp zu löschen, schlägt diese VM unmittelbar nach dem Aufheben der Bereitstellung mit einer Fehlermeldung fehl**
Wenn Sie eine VM mithilfe der VMware Cloud Director-API aus einer vApp löschen, schlägt der Vorgang unmittelbar nach dem Aufheben der Bereitstellung mit einer Fehlermeldung fehl.
Objekt konnte nicht gelöscht werden.
- **Importierte LDAP-Benutzer verfügen nicht über die Rechte zum Ändern des Benutzerkennworts, sehen aber die Option „Kennwort ändern“ auf der Benutzeroberfläche des Mandantenportals.**
Wenn ein importierter LDAP-Benutzer im VMware Cloud Director-Mandantenportal zur oberen Navigationsleiste navigiert und auf seinen Benutzernamen klickt, zeigt das Dropdown-Menü fälschlicherweise die Option „Kennwort ändern“ an, obwohl der Benutzer nicht über die Rechte zum Ändern des Benutzerkennworts verfügt.
- **In einer vApp, die mit einem direkten VDC-Organisationsnetzwerk verbunden ist, können Sie den IP-Modus für die Netzwerkkarte einer virtuellen Maschine nicht auf „Statisch – IP-Pool“ festlegen**
In einer vApp, die mit einem direkten VDC-Organisationsnetzwerk verbunden ist, können Sie den IP-Modus für die Netzwerkkarte einer virtuellen Maschine nicht auf „Statisch – IP-Pool“ festlegen. Dies ist der Fall, wenn das direkte Netzwerk von einem externen Netzwerk mit mehreren Subnetzen unterstützt wird und der IP-Pool des ersten Subnetzes vollständig ausgelastet ist. Wenn Sie der VM eine andere Netzwerkkarte oder der vApp eine andere VM hinzufügen und den IP-Modus auf Statisch – IP-Pool festlegen, wendet VMware Cloud Director die Einstellungen nicht an und ändert den IP-Modus in DHCP.
- **Beim Versuch, VMware Cloud Director 10.1.2 auf Version 10.2.x zu aktualisieren, wird fälschlicherweise ein Fehler gemeldet**
Beim Upgrade von VMware Cloud Director 10.1.2 auf die Version 10.2.x wird fälschlicherweise die folgende Fehlermeldung eingeblendet:

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.

VMware Cloud Director unterstützt Upgrades von Version 10.1.2 auf Version 10.2.x, und Sie können die Fehlermeldung ignorieren.
- **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 und eine Fehlermeldung mit dem Hinweis angezeigt wird, 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.
- **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 LException-Fehler fehl.
- **Wenn ein Speicher-Pod oder Cluster eine Speicherrichtlinie sichert, können Sie die VMware Cloud Director-IOPS-Begrenzung für diese Speicherrichtlinie nicht aktivieren**
Wenn im Dienstanbieter-Administratorportal 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.
- **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 das vorhandene Kennwort beim Aktualisieren der Katalogeinstellungen gelöscht und auf null gesetzt wird.

- 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.
- 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.
- Wenn ein vApp-Benutzer versucht, eine vApp anhand einer Vorlage zu erstellen, wird für den Vorgang die Meldung „Dieser Vorgang wird verweigert“ angezeigt**
 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 ändern Sie den Arbeitsspeicher oder die CPU der virtuellen Maschine.
- 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.
- Bei Verwendung der VMware Cloud Director-API zum Abrufen eines Hosts wird ein falscher Wert für den Parameter „numOfCpusLogical“ zurückgegeben**
 Wenn Sie den API-Aufruf `GET /admin/extension/host/{id}` ausführen, um einen Host abzurufen, zeigt das Feld `NumOfCpusLogical` anstelle der logischen CPUs die Anzahl der physischen CPUs an.
 Das Problem wurde in der folgenden Version behoben, indem das Feld `NumOfCpusLogical` als veraltet abgewertet wurde und dem Textkörper der Ausgabe zwei neue Felder hinzugefügt wurden:
`NumOfCpuCoresPhysical`
`NumOfCpuCoresLogical`
- VMware Cloud Director-Spitzen im CPU-Verbrauch führen zu einer Verlangsamung des Systems**
 Bestimmte VMware Cloud Director-Zellen weisen einen hohen CPU-Verbrauch durch den Dienst `vccloud` auf. Durch den hohen CPU-Verbrauch wird die Zellenleistung beeinträchtigt, und bestimmte Aufgaben schlagen fehl.
- Sie können keine Gastanpassung auf einer verschlüsselten virtuellen Maschine vornehmen**
 Wenn Sie eine VM mit einer Speicherrichtlinie verknüpfen, die über die VM-Verschlüsselungsfunktion verfügt, werden die Gastanpassungskonfigurationen beim Aktivieren der Gastanpassung auf der VM nicht angewendet.
- Das Deaktivieren eines auf NSX-T-Richtlinien basierenden IPsec-VPN schlägt mit einer Fehlermeldung fehl**
 Wenn Sie die HTML5-Benutzeroberfläche oder die VMware Cloud Director-API verwenden, um ein auf NSX-T-Richtlinien basierendes IPsec-VPN zu deaktivieren, schlägt der Vorgang mit der Fehlermeldung `Fehlercode 500090` fehl.
- Beim Instanzieren einer VM von einer Vorlage wird die VM nicht mit der richtigen Konfiguration für den Netzwerkadaptertyp bereitgestellt**
 Wenn Sie eine VM aus einer Vorlage instanzieren, behält die bereitgestellte VM die richtige Konfiguration für den Netzwerkadaptertyp nicht bei.
- Bei einer Installation mit VMware Cloud Director mit mehreren Zellen kommt es bei der Synchronisierung eines abonnierten Katalogs zu einer Zeitüberschreitung (Timeout)**
 Wenn Sie das automatische Herunterladen von Inhalten aus einem externen Katalog in einen abonnierten Katalog deaktivieren, friert die Synchronisierung der Kataloge bei einem Prozent ein und es kommt zu einem Timeout.
- Der Versuch, sich bei VMware Cloud Director anzumelden, wenn ein LDAP-Benutzer mit einer geerbten Gruppenrolle verwendet wird, schlägt fehl**
 Wenn Sie sich als ein LDAP-Benutzer anmelden, der seine Rolle von einer LDAP-Gruppe erbt, schlägt der Anmeldevorgang fehl und es wird eine Authentifizierungsfehler Fehlermeldung ausgegeben.
- VMware Cloud Director meldet Sie bei allen geöffneten Browsersitzungen ab**

Wenn Sie die HTML5-Benutzeroberfläche in mehreren Browserfenstern oder Registerkarten öffnen und Sie in allen nicht länger als die in der Konfiguration „**Zeitlimit für Leerlaufsitzung**“ angegebene Dauer aktiv sind, meldet Sie VMware Cloud Director bei allen geöffneten Sitzungen ab.

- **Wenn Sie den Chrome-Browser verwenden und auf einen Datenspeichernamen in der Liste aller Datenspeicher klicken, wird die Detailseite des Datenspeichers nicht geöffnet**

Wenn Sie das VMware Cloud Director Service Provider-Portal in Chrome öffnen und auf einen Datenspeichernamen in der Liste aller Datenspeicher klicken, wird die Detailseite des Datenspeichers nicht geöffnet.

- **Durch das Aktualisieren des Namens und der Beschreibung einer Sicherheitsgruppe werden die vorhandenen Mitglieder aus der Gruppe entfernt**

Wenn Sie den Namen oder die Beschreibung einer Sicherheitsgruppe aktualisieren, werden die vorhandenen Mitglieder aus der Gruppe entfernt.

- **Der Assistent zum Erstellen einer vApp aus einer OVF-Datei zeigt die Produkt- und Anbieternamen als Links an, die auf das VMware Cloud Director-Mandantenportal zurückverlinken**

Wenn Sie eine vApp aus einem OVF-Paket erstellen, werden die Namen für **Produkt** und **Anbieter** auf der Seite **Details überprüfen** des Assistenten als Links angezeigt, die zum VMware Cloud Director-Mandantenportal zurückführen.

- **Das Erstellen einer vApp aus einer OVA schlägt mit einem Fehler wegen Zeitüberschreitung fehl**

Wenn eine OVA-Datei größer als 8 GB ist, schlägt das Erstellen einer vApp aus dieser OVA-Datei mit einer Fehlermeldung des Typs Zeitüberschreitung fehl.

- **Der Assistent „Gruppe bearbeiten“ zeigt nicht alle verfügbaren Mandantenrollen an**

Wenn Ihre Organisation aus mehr als 15 Mandantenrollen besteht, zeigt das Dropdown-Menü **Rolle** im Assistenten **Gruppe bearbeiten** nur 15 Rollen an.

- **Nach dem Löschen eines VDC-Organisationsnetzwerks schlägt die Aktualisierung einer Firewallregel für ein Edge-Gateway mit einer Fehlermeldung fehl**

Wenn Sie ein VDC-Organisationsnetzwerk löschen, das in einer Firewallregel für ein Edge-Gateway verwendet wird, schlägt jede nachfolgende Aktualisierung einer anderen Firewallregel für dasselbe Edge-Gateway mit einer Fehlermeldung fehl.

Der Quell-/Zieltyp der Edge-Firewall mit dem Wert `??virtualwire-xx??` wird von VMware Cloud Director nicht erkannt und nicht unterstützt.

- **Die Schaltfläche „Speichern“ im Assistenten „Regeln bearbeiten“ ist ausgegraut, und Sie können die Firewallregeln nicht aktualisieren**

Wenn eine NSX-T Data Center-Firewallregel für die Verwendung einer **Reject**-Aktion konfiguriert ist und Sie die Firewallregel in der HTML5-Benutzeroberfläche aktualisieren, ist die Schaltfläche **Speichern** im Assistenten **Firewall bearbeiten** ausgegraut.

- **Das Aktivieren einer vApp schlägt mit der Fehlermeldung „Zustand ungültig“ fehl**

Wenn das Einschalten einer vApp länger als 3 Minuten dauert, schlägt der Vorgang mit der Fehlermeldung **Zustand ungültig** fehl.

- **Die interne Schnittstelle des NSX Edge Gateways wird für ein VDC, das mithilfe einer VDC-Vorlage bereitgestellt wurde, getrennt**

Wenn Sie die VMware Cloud Director-API verwenden, um ein neues VDC von einer VDC-Vorlage zu erstellen, die Konfigurationen für ein geroutetes Netzwerk enthält, wird die interne Schnittstelle des bereitgestellten NSX Edge getrennt.

- **Der Assistent zum Erstellen von Edge-Gateways kann nicht mehr als 15 für ein Organisations-VDC verfügbare Edge-Cluster anzeigen**

Wenn Sie in einem Organisations-VDC, das mit mehr als 15 Edge-Clustern konfiguriert ist, ein neues Edge-Gateway bereitstellen, werden auf der Seite **Edge-Cluster** des Assistenten **Edge-Gateway erstellen** nur 15 Edge-Cluster angezeigt.

- **Das Datenraster in „Edge-Cluster-Zuweisung bearbeiten“ wird leer angezeigt**

Wenn Sie einer Datencentergruppe ein Edge-Gateway hinzufügen, scheint das Datenraster im Assistenten **Edge-Cluster-Zuweisung bearbeiten** leer zu sein.

- **Der Ausführungsassistent für einen vRealize Orchestrator-Workflow zeigt anstelle des VDC-Namens die VDC-URL an**

Wenn Sie in VMware Cloud Director einen vRealize Orchestrator-Workflow initiieren, zeigt der Assistent **Dienst ausführen** anstelle des VDC-Namens die URL an.

- **Nach dem Upgrade auf VMware Cloud Director 10.2 meldet die Dienstüberwachung, dass der Konsolen-Proxy-Endpoint nicht verfügbar ist**
Nach dem Upgrade von vCloud Director 9.7 auf VMware Cloud Director 10.2 meldet die Lastausgleichsdienst-Dienstüberwachung, dass der Konsolen-Proxy-Endpoint **Nicht verfügbar** ist, und ein Zugriffsversuch auf die Zelle schlägt mit der Fehlermeldung ERR_CONNECTION_REFUSED fehl.
- **Nach dem Deaktivieren einer VM für den Beitritt zu einer Domäne schlagen einige Vorgänge auf der VM mit der Fehlermeldung „DomainName sollte bei deaktiviertem Domänenbeitritt nicht angegeben werden“ fehl**
Wenn Sie die Gastanpassung **Aktivierung dieser VM, um der Domäne beizutreten** für eine VM aktivieren und sie später deaktivieren, schlägt das Umbenennen der VM oder das Hinzufügen der VM zu einer vApp mit einer Fehlermeldung fehl.
DomainName sollte bei deaktiviertem Domänenbeitritt nicht angegeben werden

Bekannte Probleme

- **Neu Das Mounten eines NFS-Datenspeichers aus einem NetApp-Speicher-Array schlägt während der anfänglichen Konfiguration der VMware Cloud Director-Appliance mit einer Fehlermeldung fehl**
Wenn Sie während der anfänglichen Konfiguration der VMware Cloud Director-Appliance einen NFS-Datenspeicher aus dem NetApp-Speicher-Array konfigurieren, schlägt der Vorgang mit einer Fehlermeldung fehl.
Backend-Validierung von NFS fehlgeschlagen mit: gehört einem unbekannten Benutzer.

Problemumgehung: Konfigurieren Sie die VMware Cloud Director-Appliance mithilfe der API der VMware Cloud Director-Appliance.
- **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 die LDAP-Seite in Ihrem Browser aktualisieren, gelangen Sie nicht zurück zur selben Seite**
Wenn Sie im Administratorportal des Dienstansbieters die Seite **LDAP** in Ihrem Browser aktualisieren, gelangen Sie zur Anbieterseite statt zurück zur Seite „LDAP“.

Umgehung: Nein
- **Neu Sie können die LDAP-Synchronisierungseinstellungen für Ihre Organisation nicht bearbeiten**
Wenn Sie auf der Registerkarte **LDAP-Synchronisierungseinstellungen** im VMware Cloud Director Service Provider Admin Portal auf **Bearbeiten** klicken, passiert nichts und Sie können die LDAP-Einstellungen für Ihre Organisation nicht bearbeiten.

Umgehung: Nein
- **Neu VMware Cloud Director zeigt einen falschen Wert für die Startzeit der LDAP-Synchronisierung an**
Im VMware Cloud Director Service Provider Admin Portal zeigt die LDAP-Synchronisierungsseite das Datum und die Uhrzeit des Öffnens der Seite als **Startzeit der Synchronisierung** anstelle von Datum und Uhrzeit an, die Sie konfigurieren.

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 den FIPS-Modus aktivieren, schlägt die vRealize Orchestrator-Integration mit einem Fehler im Zusammenhang mit ungültigen Parametern fehl.**

Wenn Sie den FIPS-Modus aktivieren, funktioniert die Integration zwischen VMware Cloud Director und vRealize Orchestrator nicht. Die VMware Cloud Director-Benutzeroberfläche gibt einen Fehler des Typs Ungültige VRO-Anforderungsparameter zurück. Die API-Aufrufe geben einen Fehler ähnlich dem folgenden zurück:

```
Caused by: java.lang.IllegalArgumentException: 'param' arg cannot be null at
org.bouncycastle.jcajce.provider.ProvJKS$JKSKeyStoreSpi.engineLoad(Unknown Source) at
java.base/java.security.KeyStore.load(KeyStore.java:1513) at
com.vmware.vim.install.impl.CertificateGetter.createKeyStore(CertificateGetter.java:128) at
com.vmware.vim.install.impl.AdminServiceAccess.(AdminServiceAccess.java:157) at
com.vmware.vim.install.impl.AdminServiceAccess.createDiscover(AdminServiceAccess.java:238) at
com.vmware.vim.install.impl.RegistrationProviderImpl.(RegistrationProviderImpl.java:56) at
com.vmware.vim.install.RegistrationProviderFactory.getRegistrationProvider(RegistrationProviderFactory.java:143)
at com.vmware.vcloud.vro.client.connection.STSClient.getRegistrationProvider(STSClient.java:126) ... 136 more
```

Umgehung: Nein

- **Neu VMware Cloud Director-API-Aufrufe zum Abrufen vCenter Server-Informationen geben eine URL anstelle einer UUID zurück**

Dieses Problem tritt bei vCenter Server-Instanzen auf, bei denen die anfängliche Registrierung bei VMware Cloud Director Version 10.2.1 und früher fehlgeschlagen ist. Wenn Sie für diese vCenter Server-Instanzen API-Aufrufe zum Abrufen der vCenter Server-Informationen ausführen, gibt die VMware Cloud Director-API fälschlicherweise eine URL anstelle der erwarteten UUID zurück.

Problemumgehung: Verbinden Sie die vCenter Server-Instanz erneut mit VMware Cloud Director.

- **Neu VMware Cloud Director benötigt mehr Zeit, um Sie von der HTML5-Benutzeroberfläche abzumelden, als in der Konfiguration „Zeitlimit für Leerlaufsitzung“ angegeben wird.**

VMware Cloud Director benötigt doppelt so lange wie in der Konfiguration **Zeitlimit für Leerlaufsitzung** angegeben wird, um Sie von der HTML5-Benutzeroberfläche abzumelden.

Problemumgehung: Sie müssen das Fenster minimieren oder im selben Fenster zu einer anderen Registerkarte wechseln.

- **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 Wenn Sie bestimmte Zertifikats- und Truststore-Dateien vor dem Upgrade einer Zelle auf VMware Cloud Director 10.2.2 nicht löschen, ist die Zelle nicht mehr funktionsfähig**

Wenn eine der Dateien `certificates.bak`, `proxycertificates.bak` und `truststore.bak` im Ordner `/opt/vmware/vcloud-director/etc/` der Zelle vorhanden ist, funktioniert die Zelle nach dem Upgrade auf Version 10.2.2 nicht mehr. In den Protokollen wird der folgende Fehler aufgeführt.

```
cp: cannot stat '/opt/vmware/vcloud-director/etc/proxycertificates.pem': No such file or directory
cp: cannot stat '/opt/vmware/vcloud-director/etc/proxycertificates.key': No such file or directory
```

Problemumgehung: Führen Sie `/opt/vmware/vcloud-director/bin/configure` aus.

- **Neu Der Versuch, von OpenSSL erzeugte PKCS8-Dateien auf eine VMware Cloud Director-Appliance im FIPS-Modus hochzuladen, schlägt mit einem Fehler fehl**

OpenSSL kann keine FIPS-konformen privaten Schlüssel generieren. Wenn sich VMware Cloud Director im FIPS-Modus befindet und Sie versuchen, mithilfe von OpenSSL generierte PKCS8-Dateien hochzuladen, schlägt das Hochladen mit einem Fehler des Typs Fehlerhafte Anforderung: `org.bouncycastle.pkcs.PKCSException: verschlüsselte Daten können nicht gelesen werden: ... nicht verfügbar: Algorithmus nicht vorhanden: ...` oder mit einem Fehler des Typs Salt muss mindestens 128 Bit aufweisen fehl.

Problemumgehung: Deaktivieren Sie den FIPS-Modus, um die PKCS8-Dateien hochzuladen.

- **Nach dem Upgrade wird die Seite „Systemkonfiguration“ der Verwaltungsoberfläche der VMware Cloud Director-Appliance nicht angezeigt**

Nach dem Upgrade der VMware Cloud Director-Appliance auf Version 10.2.2 wird die neue Seite „Systemkonfiguration“ der Verwaltungsoberfläche der Appliance nicht angezeigt.

Problemumgehung: Um dieses Problem zu vermeiden und eine Wiederholung zu verhindern, löschen Sie den Browser-Cache.

- **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](#).

- **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 notwendigen Berechtigungen 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 10.2.2 und von vCenter Server auf Version 7.0.0d oder höher 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 die entsprechenden Kubernetes-Endpoint-Zertifikate manuell als vertrauenswürdig ein. Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel [83583](#).

- **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. Weitere Informationen zum Deaktivieren eines Plug-Ins finden Sie unter [Aktivieren oder Deaktivieren eines Plug-Ins](#).

- **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

- **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

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

Wenn Sie die VMware Cloud Director-API zum Anwenden eines Prioritätsfilters auf eine Empfehlung verwenden, schlägt der Vorgang mit einer Fehlermeldung 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. Weitere Informationen finden Sie in der Dokumentation zur [VMware Cloud Director OpenAPI](#).

- **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 Reihenfolge aufgelistet werden. Die Dokumentation zur VMware Cloud Director-API listet die Prioritäten für eine Empfehlung in aufsteigender Reihenfolge auf.

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, weil es voll ist, unter Schreibschutz gestellt wird usw., funktionieren die Clusterfunktionen der Appliance nicht mehr ordnungsgemäß. 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 sich in einer Umgebung mit mehreren Sites unter Verwendung der HTML5-Benutzeroberfläche bei einer vCloud Director 10.0-Site anmelden oder eine vCenter Server-Instanz bei einer vCloud Director 10.0-Site 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. Informationen hierzu finden Sie unter <https://support.mozilla.org/de-DE/> im KB-Artikel **Websites say cookies are blocked - Unblock them** (Websites melden, dass Cookies blockiert werden – so beheben Sie das Problem).

- **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.

- **Die Umschaltoption „Protokollierung aktivieren“ ist für eine Organisationsadministratorrolle ohne die erforderlichen Rechte aktiv**

Die Umschaltoption **Protokollierung aktivieren** ist für einen Benutzer aktiv, dem die Organisationsadministratorrolle zugewiesen wurde, auch wenn die Rolle nicht über die Rechte **Systemprotokollierung konfigurieren** verfügt.

Problemumgehung: Dieses Problem wurde in der Patch-Version VMware Cloud Director 10.2.2.1 behoben.

- **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