

# Versionshinweise zu VMware Cloud Director 10.2.2.3

VMware Cloud Director 10.2.2.3

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

<https://docs.vmware.com/de/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware Global, Inc.**  
Zweigniederlassung Deutschland  
Willy-Brandt-Platz 2  
81829 München  
Germany  
Tel.: +49 (0) 89 3706 17 000  
Fax: +49 (0) 89 3706 17 333  
[www.vmware.com/de](http://www.vmware.com/de)

Copyright © 2023 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

# Inhalt

- 1** Einführung 4
- 2** Neuheiten 5
- 3** Systemanforderungen und Installation 6
- 4** Dokumentation 7
- 5** Vorherige Versionen von VMware Cloud Director 10.2.x 8
- 6** Bekannte Probleme 9

# Einführung

# 1

VMware Cloud Director 10.2.2.3 | 14. April 2022 | Build 19585218 (installierter Build 19580548)

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

# Neuheiten

# 2

In der Patch-Version VMware Cloud Director 10.2.2.3 wurde CVE-2022-22966 behoben. Weitere Informationen finden Sie unter <https://www.vmware.com/security/advisories>.

# Systemanforderungen und Installation

# 3

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

# Dokumentation

# 4

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

# Vorherige Versionen von VMware Cloud Director 10.2.x

# 5

[Versionshinweise zu VMware Cloud Director 10.2.2.2](#)

[Versionshinweise zu VMware Cloud Director 10.2.2.1a](#)

[Versionshinweise zu VMware Cloud Director 10.2.2.1](#)

[Versionshinweise zu VMware Cloud Director 10.2.2](#)

[Versionshinweise zu VMware Cloud Director 10.2.1](#)

[Versionshinweise zu VMware Cloud Director 10.2](#)



# Bekannte Probleme

# 6

- **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.

- **Wenn Sie die LDAP-Seite in Ihrem Browser aktualisieren, gelangen Sie nicht zurück zur selben Seite**

Wenn Sie im Administratorportal des Dienstanbieters die Seite **LDAP** in Ihrem Browser aktualisieren, gelangen Sie zur Anbieterseite statt zurück zur Seite „LDAP“.

Umgehung: Nein

- **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:

- a Ein Systemadministrator muss eine VM-Größenrichtlinie mit der korrekten Konfiguration erstellen.
- b Ein Systemadministrator muss die neue VM-Größenrichtlinie im konvertierten Flex-Organisations-VDC veröffentlichen.

- c 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.

- **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 `Invalid VRO request params` 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.ja
va:238) at com.vmware.vim.install.impl.RegistrationProviderImpl.
(RegistrationProviderImpl.java:56) at
com.vmware.vim.install.RegistrationProviderFactory.getRegistrationProvider(Registra
tionProviderFactory.java:143) at
com.vmware.vcloud.vro.client.connection.STSClient.getRegistrationProvider(STSClient
.java:126) ... 136 more
```

Umgehung: Nein

- **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

- **Bei Verwendung des FIPS-Modus schlägt der Versuch, OpenSSL-generierte PKCS8-Dateien hochzuladen, mit einer Fehlermeldung fehl**

OpenSSL kann keine FIPS-konformen privaten Schlüssel generieren. Wenn sich VMware Cloud Director im FIPS-Modus befindet und Sie versuchen, mit OpenSSL generierte PKCS8-Dateien hochzuladen, schlägt der Upload mit einem Fehler des Typs `Bad`

```
request: org.bouncycastle.pkcs.PKCSException: unable to read encrypted data: ...
not available: No such algorithm: ... oder salt must be at least 128 bits 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 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 10.2.2 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 dazu, wie Sie ein Plug-In deaktivieren, 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.

```
Name must start with a letter and only contain alphanumeric or hyphen (-)
characters. (Max 128 characters).
```

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 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. 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 Sortierreihenfolge 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, 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 VMware Cloud Director 10.2.x-Site angemeldet sind oder versuchen, eine vCenter Server-Instanz bei einer VMware Cloud Director 10.2.x-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**.
- **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 `Named disk encryption is not supported in this version of vCenter Server` 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.

- **Nach dem Upgrade auf VMware Cloud Director 10.2.x schlägt der Import eines SSL-Zertifikats aus Cassandra mit einer Fehlermeldung im Zellenverwaltungstool fehl**

Wenn Sie das Zellenverwaltungstool zum SSL-Import aus Cassandra verwenden, schlägt der Vorgang mit einer Fehlermeldung fehl.

```
Unable to load VCD's SSL context.
```

Problemumgehung: Verwenden Sie das VMware Cloud Director Service Provider Admin Portal, um SSL aus Cassandra zu importieren. Weitere Informationen finden Sie unter [Importieren vertrauenswürdiger Zertifikate](#).

- **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