

# Note di rilascio di VMware Cloud Director 10.2

VMware Cloud Director 10.2 | 15 OTT 2020 | Build 17029810 (build installata 17008054)

Controllare se sono presenti aggiunte o aggiornamenti a queste note di rilascio.

## Contenuto di questo documento

- [Novità di questa versione](#)
- [Sicurezza](#)
- [Avvisi relativi al supporto del prodotto](#)
- [Aggiornamento da versioni precedenti](#)
- [Requisiti di sistema e installazione](#)
- [Problemi risolti](#)
- [Problemi noti](#)

## Novità di questa versione

VMware Cloud Director versione 10.2 include quanto segue:

- **Parità funzionale avanzata di NSX-T:** NSX Advanced Load Balancer (Avi), firewall distribuito, VRF-Lite, reti inter-VDC, IPv6, dual stack (IPv4/IPv6) nella stessa rete, SLAAC, DHCPv6, CVDS (vSphere 7.0/NSX-T 3.0), VPN L2 - solo API
- **Supporto delle applicazioni moderne in VMware Cloud Director con Tanzu Runtime vSphere with Kubernetes:** interfaccia utente del provider e del tenant per la gestione e l'utilizzo dei cluster Kubernetes
- **Miglioramenti dell'appliance virtuale di VMware Cloud Director:** convalida dell'input utente durante la distribuzione iniziale; ripristino delle celle semplificato con la creazione ottimizzata delle celle di standby
- **Miglioramenti dello storage:** controllo IOPS a livello di disco per provider e tenant; dischi condivisi
- **Miglioramenti della sicurezza:** vedere la sezione [Sicurezza](#)
- **Miglioramenti dell'interfaccia utente:** Ricerca rapida; Avvisi; Gestione certificato
- **Miglioramenti dell'estendibilità della piattaforma**
- **Miglioramenti della scalabilità:** vedere [Valori massimi consentiti per la configurazione di VMware](#)

Per informazioni sulle funzionalità nuove e aggiornate di questa versione, vedere [Novità di VMware Cloud Director 10.2](#).

Per le note di rilascio più recenti relative ai componenti aggiuntivi di VMware Cloud Director, vedere i collegamenti seguenti:

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

## Sicurezza

L'appliance virtuale di VMware Cloud Director 10.2 viene fornita con Photon OS aggiornato fino a questo [avviso di sicurezza di Photon](#).

VMware Cloud Director 10.2 supporta gli archivi chiavi PKCS12. È possibile utilizzare un archivio chiavi con formattazione PKCS12 quando si configurano le connessioni di rete e database di VMware Cloud Director o quando si utilizza lo strumento di gestione delle celle per generare o sostituire i certificati. Per ulteriori informazioni, vedere *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

## Avvisi relativi al supporto del prodotto

I nodi del cluster TKG sono isolati. Tuttavia, i servizi esposti da un cluster TKG sono accessibili a tutti gli utenti con accesso di rete all'endpoint o all'IP virtuale del servizio e sono protetti dai meccanismi di autenticazione e autorizzazione dei servizi. Poiché l'autenticazione è l'unica protezione per l'accesso ai carichi di lavoro, è consigliabile consentire solo il traffico crittografato, ad esempio TLS, nei servizi in entrata.

## Avvisi di fine ciclo di vita e fine supporto

- L'API di VMware Cloud Director versione 29 e precedenti non sono supportate.
- L'API di VMware Cloud Director versioni 30 e 31 sono obsolete.
- L'API di VMware Cloud Director versione 30 non sarà più disponibile alla prossima release.
- L'endpoint di accesso dell'API `/api/sessions` è obsoleto a partire dall'API di VMware Cloud Director versione 33.0/VMware Cloud Director 10.0 ed è destinato a non essere supportato in una versione futura di VMware Cloud Director. È possibile utilizzare gli endpoint di accesso OpenAPI di VMware Cloud Director separati per il provider di servizi e l'accesso dei tenant a VMware Cloud Director.
- L'API `/cloud/server_status` è obsoleta per entrambi i protocolli HTTP e HTTPS. La rimozione di `/cloud/server_status` sarà effettuata in una versione futura di VMware Cloud Director. È necessario utilizzare `/api/server_status` per entrambi i protocolli HTTP e HTTPS.
- Le azioni di reimpostazione `/amqp/action/resetAmqpCertificate` e `/amqp/action/resetAmqpKeyStore` sono state rimosse dall'API di VMware Cloud Director versione 35.0 a causa del modo in cui VMware Cloud Director archivia e gestisce i certificati SSL. Per non considerare attendibili i certificati, è necessario utilizzare l'endpoint `/cloudapi/1.0.0/ssl/trustedCertificates`.
- Le azioni di aggiornamento `/amqp/action/updateAmqpCertificate` e `/amqp/action/updateLdapKeyStore` sono obsolete. La rimozione delle azioni sarà effettuata in una versione futura di VMware Cloud Director. È possibile utilizzare il nuovo endpoint per considerare attendibili i certificati AMQP `/cloudapi/1.0.0/ssl/trustedCertificates`.
- Le azioni di reimpostazione `/ldap/action/resetLdapCertificate` e `/ldap/action/resetLdapKeyStore` sono state rimosse dall'API di VMware Cloud Director API versione 34.0 a causa del modo in cui VMware Cloud Director 10.1 archivia e gestisce i certificati SSL. Per non considerare attendibili i certificati, è necessario utilizzare l'endpoint `/cloudapi/1.0.0/ssl/trustedCertificates`.
- Le azioni di aggiornamento `/ldap/action/updateLdapCertificate` e `/ldap/action/updateLdapKeyStore` sono obsolete e non saranno più supportate in una versione futura. VMware Cloud Director include un nuovo endpoint per considerare attendibili i certificati LDAP `/cloudapi/1.0.0/ssl/trustedCertificates`.
- In vSphere, SSO vSphere è deprecato come provider di identità SAML. Tutte le distribuzioni di VMware Cloud Director configurate per l'utilizzo di vSphere SSO come provider di identità SAML devono passare a un provider di identità SAML esterno diverso. L'uso di questo provider di identità non sarà supportato nelle prossime versioni di vSphere e VMware Cloud Director.
- I certificati DSA e DSS non sono più supportati perché non sono disponibili suite di crittografia consigliate per tali certificati.

## Aggiornamento da versioni precedenti

Per ulteriori informazioni sull'aggiornamento a VMware Cloud Director 10.2, sui flussi di lavoro e sui percorsi di aggiornamento e migrazione, vedere [Aggiornamento e migrazione dell'appliance di VMware Cloud Director](#) o [Aggiornamento di vCloud Director in Linux](#).

## Requisiti di sistema e installazione

### Porte e protocolli

Per informazioni sulle porte di rete e sui protocolli utilizzati da VMware Cloud Director 10.2, vedere [VMware Ports and Protocols](#).

### Matrice di compatibilità

Vedere le [matrici di interoperabilità dei prodotti VMware](#) per informazioni aggiornate su:

- Interoperabilità di VMware Cloud Director con le altre piattaforme VMware
- Database di VMware Cloud Director supportati

- NSX Advanced Load Balancer (Avi): questa versione di Cloud Director al momento supporta solo NSX Advanced Load Balancer (Avi) versione 20.1.1

## Sistemi operativi dei server VMware Cloud Director supportati

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

## Distribuzione dell'appliance VMware Cloud Director

Quando si distribuisce l'appliance di VMware Cloud Director 10.2 come modello OVF utilizzando VMware OVF Tool, è necessario includere il parametro seguente (appena introdotto nella versione 10.2): `--x:enableHiddenProperties`. Se non si include questo parametro, VMware OVF Tool terminerà con esito negativo mostrando un errore in cui viene indicato che la proprietà `vcloudapp.nfs_mount.VMware_vCloud_Director` non è configurabile dall'utente..

Vedere [Distribuzione dell'appliance VMware Cloud Director tramite VMware OVF Tool](#).

## Server AMQP supportati

VMware Cloud Director utilizza AMQP per fornire il bus di messaggi utilizzato dai servizi di estensione, dalle estensioni degli oggetti e dalle notifiche. Questa versione di VMware Cloud Director richiede la versione 3.8.x di RabbitMQ.

Per ulteriori informazioni, vedere *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

## Database supportati per l'archiviazione dei valori della cronologia

VMware Cloud Director supporta le versioni 3.11.x di Apache Cassandra.

## Requisiti di spazio su disco

Ogni server VMware Cloud Director richiede circa 2100 MB di spazio libero per i file di installazione e di registro.

## Requisiti di memoria

Per i requisiti di memoria, consultare *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

## Requisiti della CPU

VMware Cloud Director è un'applicazione basata sulla CPU. Seguire le linee guida sull'overcommit della CPU relative alla versione di vSphere appropriata. Negli ambienti virtualizzati, indipendentemente dal numero di core disponibili per VMware Cloud Director, deve esserci un rapporto ragionevole tra CPU virtuali e CPU fisiche, che non comporti l'overcommit estremo.

## Pacchetti software Linux richiesti

Ciascun server VMware Cloud Director deve includere le installazioni dei pacchetti software Linux più comuni. Per impostazione predefinita, i pacchetti vengono generalmente installati con il software del sistema operativo. Se mancano uno o più pacchetti, l'esecuzione del programma di installazione non riesce e viene visualizzato un messaggio diagnostico.

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	

In aggiunta ai pacchetti richiesti dal programma di installazione, diverse procedure per la configurazione delle connessioni di rete e la creazione dei certificati SSL richiedono l'uso del comando `nslookup` di Linux, disponibile nel pacchetto `bind-utils` di Linux.

## Server LDAP supportati

È possibile importare utenti e gruppi in VMware Cloud Director dai servizi LDAP seguenti.

Piattaforma	Servizio LDAP	Metodi di autenticazione
Windows Server 2012	Active Directory	Semplice, SSL semplice
Windows Server 2016	Active Directory	Semplice, SSL semplice
Linux	OpenLDAP	Semplice, SSL semplice

## Protocolli di protezione e pacchetti di crittografia supportati

È necessario che le connessioni client di VMware Cloud Director siano protette. Poiché nei protocolli SSL versione 3 e TLS versioni 1.0 e 1.1 sono state individuate gravi vulnerabilità della sicurezza, tali protocolli non sono più inclusi nel set di protocolli predefinito che il server consente di utilizzare durante la creazione di una connessione client. Gli amministratori di sistema possono abilitare più protocolli e pacchetti di crittografia. Vedere la sezione relativa allo strumento di gestione delle celle nella *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*. Sono supportati i seguenti protocolli di protezione:

- TLS versione 1.2
- TLS versione 1.1 (disattivato per impostazione predefinita)
- TLS versione 1.0 (disattivato per impostazione predefinita)

Suite di crittografia supportate abilitate per impostazione predefinita:

- 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

Gli amministratori di sistema possono utilizzare lo strumento di gestione delle celle per abilitare in modo esplicito le altre suite di crittografia supportate che sono disattivate per impostazione predefinita.

**Nota:** l'interoperabilità con le versioni di vCenter Server precedenti alla 5.5-update-3e e con le versioni di `ovftool` precedenti alla 4.2 richiede che VMware Cloud Director supporti TLS versione 1.0. È possibile utilizzare lo strumento di gestione delle celle per riconfigurare il set di protocolli o di pacchetti di crittografia SSL supportati. Vedere la sezione relativa allo strumento di gestione delle celle nella *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

## Browser supportati

VMware Cloud Director è compatibile con la versione principale corrente e precedente dei browser seguenti:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

**Nota:** Internet Explorer 11 non è supportato in VMware Cloud Director 10.2 e versioni successive. È possibile utilizzare Microsoft Edge o un altro browser supportato. Se è necessario utilizzare Internet Explorer 11, è consigliabile rimanere in VMware Cloud Director versione 10.0.x o 10.1.x fino a quando non è possibile utilizzare un altro browser.

## Versioni dei sistemi operativi guest e dell'hardware virtuale supportate

VMware Cloud Director supporta tutte le versioni dei sistemi operativi guest e dell'hardware virtuale supportate dagli host ESXi che supportano ogni pool di risorse.

## VMware Cloud Director WebMKS 2.1.1

La console di VMware Cloud Director WebMKS 2.1.1 aggiunge il supporto per:

- La chiave PrintScreen in Google Chrome e in Mozilla Firefox per Windows.
- La chiave Windows in Windows e macOS. Per simulare la pressione del tasto Windows, premere Ctrl+Windows nel sistema operativo Windows o Ctrl+Cmd in macOS.
- Rilevamento automatico del layout della tastiera in Google Chrome e Mozilla Firefox.

## Problemi risolti

- **Il tentativo di aggiunta di una regola NAT a un gateway edge NSX-T non riesce**

Il tentativo di aggiunta di una regola NAT a un gateway edge NSX-T non riesce con l'errore: New and deprecated values have been updated together for redistribution., error code 503266.

- **Lo spostamento di una macchina virtuale tra cluster non riesce se il contenitore di storage di destinazione è un cluster di datastore**

Lo spostamento di una macchina virtuale tra cluster non riesce se il contenitore di storage di destinazione è un cluster di datastore. I registri includono il seguente messaggio di errore.

```
2020-05-18 15:51:12,083 | ERROR | task-service-activity-pool-23 | SdrsPlacementManagerImpl | SDRS invocation error
| requestId=eaa593e5-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 }
```

- **Non è possibile distribuire l'appliance se l'impostazione "Scadenza password root al primo accesso" è abilitata**

Quando si tenta di distribuire un'appliance, la distribuzione non riesce e nel registro viene visualizzato il seguente messaggio errore /opt/vmware/var/log/firstboot:

```
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.
```

- **Nel portale tenant di VMware Cloud Director, il filtro avanzato delle macchine virtuali in base alla posizione del VDC non funziona**

Nell'interfaccia utente del portale tenant di VMware Cloud Director, se si tenta di utilizzare il filtro avanzato in base alla posizione del VDC per filtrare le macchine virtuali, la ricerca non riesce e viene visualizzato un messaggio errore.

## Problemi noti

- **Nuovo Le macchine virtuali diventano non conformi dopo la conversione di un VDC del pool di prenotazioni in un VDC dell'organizzazione Flex**

In un VDC dell'organizzazione con un modello di allocazione del pool di prenotazioni, se alcune macchine virtuali hanno una prenotazione diversa da zero per CPU e memoria, una configurazione non illimitata per CPU e memoria o entrambe, dopo la conversione in un VDC dell'organizzazione Flex, queste macchine virtuali diventano non conformi. Se si tenta di rendere le macchine virtuali di nuovo conformi, il sistema applica un criterio non corretto per la prenotazione e il limite e imposta le prenotazioni di CPU e memoria su zero e il limite su **Illimitato**.

Soluzione:

1. Un amministratore di sistema deve creare un criterio di dimensionamento della macchina virtuale con la configurazione corretta.
2. Un amministratore di sistema deve pubblicare il nuovo criterio di dimensionamento della macchina virtuale nel VDC dell'organizzazione Flex convertito.
3. I tenant possono utilizzare l'API di VMware Cloud Director o il portale tenant di VMware Cloud Director per assegnare il criterio di dimensionamento della macchina virtuale alle macchine virtuali esistenti nel VDC dell'organizzazione Flex.

- **Nuovo** Lo stato del programma Analisi utilizzo software è **Enabled** anche dopo la disattivazione durante l'installazione di VMware Cloud Director

Durante l'installazione di VMware Cloud Director, se si disattiva l'opzione per partecipare al programma Analisi utilizzo software, al termine dell'installazione lo stato del programma Analisi utilizzo software è attivo.

Soluzione: Disattivare il programma CEIP seguendo i passaggi della procedura [Attivazione o disattivazione della partecipazione al programma CEIP VMware](#).

- **Nuovo** Nell'interfaccia utente del portale tenant, quando si crea una regola di affinità o anti-affinità, la deselection della casella di controllo **Obbligatorio** non influisce sulla configurazione della regola

Nell'interfaccia utente del portale tenant, quando si crea una regola di affinità o anti-affinità, la deselection della casella di controllo Obbligatorio non influisce sulla configurazione della regola. Le regole di affinità e anti-affinità sono sempre obbligatorie. Ciò significa che se non è possibile soddisfare una regola, le macchine virtuali aggiunte alla regola non vengono accese.

Soluzione: nessuna.

- **Nuovo** Dopo l'aggiornamento a vCenter Server 7.0 Update 2a o Update 2b, non è possibile creare cluster di Tanzu Kubernetes Grid

Se la versione dell'istanza di vCenter Server sottostante è 7.0 Update 2a o Update 2b, quando si tenta di creare un cluster di Tanzu Kubernetes Grid utilizzando il plug-in Kubernetes Container Clusters, l'attività non riesce.

Soluzione: nessuna.

- **Nuovo** La creazione del cluster Tanzu Kubernetes utilizzando il plug-in Kubernetes Container Cluster non riesce

Quando si crea un cluster Tanzu Kubernetes utilizzando il plug-in Kubernetes Container Cluster, è necessario selezionare una versione di Kubernetes. Alcune delle versioni nel menu a discesa non sono compatibili con l'infrastruttura di vSphere di supporto. Quando si seleziona una versione non compatibile, la creazione del cluster non riesce.

Soluzione: eliminare il record del cluster non riuscito e riprovare con una versione di Tanzu Kubernetes compatibile. Per informazioni sulle incompatibilità tra Tanzu Kubernetes e vSphere, vedere [Aggiornamento dell'ambiente vSphere with Tanzu](#).

- **Nuovo** Se un pod di storage o un cluster supporta un criterio di storage, non è possibile abilitare la limitazione di IOPS di VMware Cloud Director in tale criterio di storage

Nel portale di amministrazione del provider di servizi, quando uno o più cluster o pod di storage supportano un criterio di storage, anche se si disattiva il contrassegno **Impatto sul posizionamento**, non è possibile abilitare la limitazione di IOPS di VMware Cloud Director in tale criterio di storage.

Soluzione: per risolvere questo problema, è necessario disporre di accesso a livello di amministratore.

1. In vCenter Server, rimuovere il tag dei criteri di storage da tutti i pod di storage per i quali si desidera abilitare IOPS e aggiornare i criteri di storage.
2. In VMware Cloud Director, abilitare VMware Cloud Director IOPS nel criterio di storage disattivando **Impatto sul posizionamento**.
3. In vCenter Server, ricollegare il tag ai pod di storage e aggiornare i criteri di storage.

- **Nuovo** Quando si apre l'elenco delle macchine virtuali in una vApp e si abilita l'opzione **Selezione multipla**, il menu **Azioni** diventa non disponibile

Quando si apre l'elenco delle macchine virtuali in una vApp e si abilita l'opzione Selezione multipla, il menu Azioni diventa non disponibile. È possibile selezionare più macchine virtuali, ma non è possibile eseguire alcuna azione su di esse simultaneamente.

Soluzione: nessuna.

- **Nuovo** Non è possibile modificare le impostazioni della NIC di una macchina virtuale indipendente

Non è possibile aggiornare le impostazioni della NIC di una macchina virtuale indipendente. Quando si fa clic su Modifica per aprire le impostazioni della NIC della macchina virtuale, la pagina Impostazioni viene aperta ma non risponde.

Soluzione:

1. Convertire la macchina virtuale indipendente in una vApp
2. Modificare le impostazioni della NIC della vApp.
3. Riconvertire la vApp in una macchina virtuale indipendente.

- **Nuovo** Dopo aver aggiornato le impostazioni di pubblicazione di un catalogo sottoscritto dall'interfaccia utente del portale tenant, la sincronizzazione del catalogo non riesce e viene visualizzato il messaggio di errore "401 Non autorizzato"

Dopo aver aggiornato le **impostazioni di pubblicazione** di un catalogo sottoscritto dall'interfaccia utente del portale tenant, la sincronizzazione del catalogo non riesce e si verifica un errore 401 Non autorizzato. Ciò accade perché l'aggiornamento delle impostazioni del catalogo causa l'eliminazione della password esistente e l'impostazione su null.

Soluzione: aggiornare le **impostazioni di pubblicazione** del catalogo e impostare nuovamente la password dall'interfaccia utente del portale tenant.

- **Nuovo L'aggiornamento di VMware Cloud Director alla versione 10.2 dalla versione 10.1.2 segnala erroneamente un errore**

Durante l'aggiornamento di VMware Cloud Director alla versione 10.2 dalla versione 10.1.2, viene visualizzato il seguente messaggio di errore inesatto:

ERRORE: l'RPM per un'altra versione di VMware Cloud Director è già installato, ma tale versione non è riconosciuta e l'aggiornamento da tale versione non è supportato. Questo aggiornamento non dovrebbe riuscire, ma è comunque possibile procedere a proprio rischio.

È supportato l'aggiornamento di VMware Cloud Director alla versione 10.2 dalla versione 10.1.2 ed è necessario ignorare il messaggio di errore.

Soluzione: ignorare l'errore.

- **Quando si riavvia l'appliance VMware Cloud Director, l'API dei servizi o l'interfaccia utente di gestione dell'appliance possono segnalare che il servizio vmware-vcd si trova in uno stato di errore**

Quando si riavvia l'appliance VMware Cloud Director, l'API dei servizi o l'interfaccia utente di gestione dell'appliance possono erroneamente segnalare che il servizio vmware-vcd si trova in uno stato di errore. Questo si verifica quando il servizio vmware-vcd effettua un tentativo di avvio prima che lo stack di rete del sistema operativo sia disponibile. Di conseguenza il servizio entra in uno stato di errore, visualizzando un messaggio di errore che indica che il binding di una o più porte non è riuscito. Successivamente, vcd-watchdog avvia correttamente il servizio vmware-vcd, ma lo stato del servizio systemd non riflette l'esito dell'operazione riuscita.

Soluzione:

1. eseguire `systemctl reset-failed vmware-vcd.service`.
2. Eseguire `systemctl start vmware-vcd.service`.

- **Se nell'organizzazione sono presenti cataloghi sottoscritti, quando si esegue l'aggiornamento di VMware Cloud Director, la sincronizzazione del catalogo non riesce**

Dopo l'aggiornamento, se sono presenti cataloghi sottoscritti nell'organizzazione, VMware Cloud Director non considera attendibili automaticamente i certificati degli endpoint pubblicati. Se i certificati non vengono considerati attendibili, la sincronizzazione della libreria dei contenuti non riesce.

Soluzione: tramite un'operazione manuale, considerare attendibili i certificati per ogni sottoscrizione di catalogo. Quando si modificano le impostazioni della sottoscrizione del catalogo, viene visualizzata una finestra di dialogo Trust On First Use (TOFU) che richiede di considerare attendibile il certificato del catalogo remoto.

Se non si dispone dei diritti necessari per considerare attendibile il certificato, contattare l'amministratore dell'organizzazione.

- **Dopo l'aggiornamento di VMware Cloud Director e l'abilitazione della creazione cluster di Tanzu Kubernetes, non è disponibile alcun criterio generato automaticamente e non è possibile creare o pubblicare un criterio**

Quando si esegue l'aggiornamento di VMware Cloud Director alla versione 10.2 e di vCenter Server alla versione 7.0.0d e si crea un VDC del provider supportato da un cluster supervisore, in VMware Cloud Director viene visualizzata un'icona di Kubernetes accanto al VDC. Tuttavia, nel nuovo VDC del provider non è presente alcun criterio Kubernetes generato automaticamente. Quando si tenta di creare o pubblicare un criterio Kubernetes in un VDC dell'organizzazione, non sono disponibili classi di macchine.

Soluzione: tramite un'operazione manuale, considerare attendibile il certificato dell'endpoint Kubernetes. Per la procedura dettagliata, vedere <https://kb.vmware.com/s/article/80996>.

- **Il plug-in Setup DRaaS and Migration viene visualizzato due volte nella barra di navigazione superiore dell'interfaccia utente di VMware Cloud Director**

Il problema si verifica perché vCloud Availability 4.0.0 è stato ridenominato VMware Cloud Director Availability 4.0.0 e sono ora presenti due plug-in. VMware Cloud Director non disattiva automaticamente il plug-in vCloud Availability 4.0.0. Le versioni precedente e nuova vengono visualizzate come plug-in Setup DRaaS and Migration nella barra di navigazione superiore in **Altro**.

Soluzione: disattivare manualmente il plug-in vCloud Availability 4.0.0.



- **Non è possibile pubblicare un criterio Kubernetes in un VDC se il cluster supervisore a cui punta non è il cluster primario nel VDC del provider**

Se si dispone di un VDC del provider con più cluster supervisore, la pubblicazione di un criterio Kubernetes del VDC del provider che punta a un cluster supervisore non primario non riesce e viene visualizzato il messaggio di errore `LMException`.

Soluzione: assicurarsi che il VDC del provider sia supportato da un solo cluster supervisore e che il cluster sia il cluster primario. Un VDC del provider può essere supportato da cluster host e da un cluster supervisore, ma il cluster supervisore deve essere quello primario.

- **L'inserimento del nome di un cluster con caratteri non latini disattiva il pulsante Avanti nella procedura guidata Crea nuovo cluster.**

Il plug-in Kubernetes Container Clusters supporta solo caratteri latini. Se si immettono caratteri non latini, viene visualizzato il seguente messaggio di errore. Il nome deve iniziare con una lettera e può contenere solo caratteri alfanumerici o trattino (-). (Massimo 128 caratteri).

Soluzione: nessuna.

- **Nel plug-in Kubernetes Container Clusters, è possibile che le griglie dei dati vengano visualizzate vuote durante il caricamento**

Nel plug-in Kubernetes Container Clusters, alcune griglie di dati vengono visualizzate vuote durante il caricamento perché il selettore di caricamento non è disponibile.

Soluzione: nessuna.

- **Dopo il ridimensionamento di un cluster TKGI, alcuni valori nella griglia dati vengono visualizzati come vuoti o non applicabili**

Quando si ridimensiona un cluster VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), i valori del cluster per l'organizzazione e il VDC nella vista della griglia dei dati sembrano vuoti o non disponibili.

Soluzione: nessuna.

- **Quando si filtra una griglia di selezione multipla, se si naviga verso un'altra pagina gli elementi filtrati scompaiono**

Nelle griglie di selezione multipla, se si filtrano i risultati e ne derivano più pagine, le pagine dei risultati filtrati successive alla prima appaiono vuote. Il problema si verifica nelle finestre di dialogo in cui è possibile selezionare più elementi da un elenco e filtrarli, ad esempio aggiungendo criteri di storage a un VDC dell'organizzazione o condividendo una vApp o una macchina virtuale con utenti o gruppi.

Soluzione: ridimensionare una delle colonne della griglia.

- **Quando si filtrano avvisi per priorità viene generato un errore interno del server**

Quando si utilizza l'API di VMware Cloud Director, l'applicazione di un filtro di priorità a un avviso non riesce e viene visualizzato un errore.

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

Soluzione: ottenere tutti gli avvisi e filtrarli manualmente.

- **La documentazione dell'API fornisce una descrizione errata dell'ordinamento delle priorità di Advisory**

L'oggetto modello Advisory contiene un campo di priorità per specificare l'urgenza di ogni avviso creato. La documentazione dell'API di Advisory indica erroneamente che le priorità sono elencate in ordine decrescente. La documentazione dell'API di VMware Cloud Director elenca le priorità per un avviso in ordine crescente.

Soluzione: nessuna.

- **Quando un utente di vApp tenta di creare una vApp da un modello, è possibile che venga visualizzato il messaggio "Questa operazione non è consentita"**

Se si dispone del ruolo Utente vApp, quando si tenta di creare una vApp da un modello e si personalizzano i criteri di dimensionamento delle macchine virtuali per le macchine virtuali nella vApp, viene visualizzato il messaggio "Questa operazione non è consentita". Questo problema si verifica perché il ruolo Utente vApp consente di creare istanze di vApp da modelli, ma non include diritti che consentono di personalizzare la memoria, la CPU o il disco rigido di una macchina virtuale. Modificando il criterio di dimensionamento, è possibile modificare la memoria o la CPU della macchina virtuale.

Soluzione: nessuna.



- **L'inattività di NFS può causare il malfunzionamento delle funzionalità del cluster dell'appliance di VMware Cloud Director**

Se NFS non è disponibile perché la condivisione NFS è piena, diventando di sola lettura e così via, è possibile che si verifichi un malfunzionamento delle funzionalità del cluster dell'appliance. L'interfaccia utente HTML5 non risponde se NFS è inattivo o non può essere raggiunto. Altre funzionalità che potrebbero essere interessate sono la rimozione della priorità applicata a una cella primaria non riuscita, il cambio, la promozione di una cella di standby e così via. Per ulteriori informazioni sulla configurazione corretta dello storage condiviso NFS, vedere [Preparazione dello storage del server di trasferimento per l'appliance VMware Cloud Director](#).

Soluzione:

- Correggere lo stato NFS in modo che non sia di sola lettura.
- Pulire la condivisione NFS se è piena.
- **Se si considera attendibile un endpoint durante l'aggiunta delle risorse di vCenter Server e NSX in un ambiente multisito, l'endpoint non viene aggiunto all'area di storage dei certificati centralizzata**  
In un ambiente multisito, durante l'utilizzo dell'interfaccia utente HTML5, se si è connessi a un sito di vCloud Director 10.0 o si tenta di registrare un'istanza di vCenter Server in un sito di vCloud Director 10.0, VMware Cloud Director non aggiunge l'endpoint all'area di storage dei certificati centralizzata.

Soluzione:

- Importare il certificato nel sito di VMware Cloud Director 10.1 utilizzando l'API.
- Per attivare la funzionalità di gestione dei certificati, passare al portale di amministrazione SP del sito di VMware Cloud Director 10.1, visualizzare la finestra di dialogo **Modifica** del servizio e fare clic su **Salva**.
- **Il tentativo di crittografare dischi denominati in vCenter Server versione 6.5 o precedente non riesce e viene visualizzato un errore**  
Per le istanze di vCenter Server versione 6.5 o precedenti, se si tenta di associare dischi denominati nuovi o esistenti a un criterio abilitato per la crittografia, l'operazione non riesce e viene visualizzato il messaggio di errore La crittografia del disco denominato non è supportata in questa versione di vCenter Server.

Soluzione: nessuna.

- **Quando si utilizza il portale di amministrazione del provider di servizi di VMware Cloud Director con Firefox, non è possibile caricare le schermate di creazione della rete del tenant**  
Se si utilizza il portale di amministrazione del provider di servizi di VMware Cloud Director in Firefox, è possibile che non riesca il caricamento delle schermate di creazione della rete del tenant, ad esempio **Gestisci firewall** per un virtual data center dell'organizzazione. Questo problema si verifica se il browser Firefox è configurato per il blocco dei cookie di terze parti.

Soluzione: configurare il browser Firefox in modo da consentire i cookie di terze parti.

- **Non è possibile consolidare una macchina virtuale con provisioning rapido creata in un array NFS abilitato per VMware vSphere Storage APIs Array Integration (VAAI) o in vSphere Virtual Volumes (VVols)**  
Il consolidamento sul posto di una macchina virtuale con provisioning rapido non è supportato quando viene utilizzato uno snapshot nativo. Gli snapshot nativi vengono sempre utilizzati dagli archivi dati abilitati per VAAI, nonché da VVols. Quando una macchina virtuale con provisioning rapido viene distribuita in uno di questi contenitori di storage, tale macchina virtuale non può essere consolidata.

Soluzione: non abilitare il provisioning rapido per un VDC dell'organizzazione che utilizzi NFS abilitato per VAAI o VVols. Per consolidare una macchina virtuale con uno snapshot in un archivio dati VAAI o VVol, trasferire la macchina virtuale in un contenitore di storage diverso.

- **Dopo l'aggiornamento da vCloud Director 10.0, si verificano problemi di connettività di rete in una macchina virtuale appena distribuita da un modello Linux con personalizzazione del sistema operativo guest e connettività IPv6 abilitate.**  
Dopo l'aggiornamento da vCloud Director 10.0, se si distribuisce una nuova macchina virtuale utilizzando un modello di macchina virtuale Linux creato nella versione 10.0 con la personalizzazione del sistema operativo guest e la connettività IPv6 abilitate, nella macchina virtuale distribuita si verificano problemi di connettività di rete. Questo problema può verificarsi perché il processo di distribuzione crea voci duplicate per i parametri VM\_DOMAIN\_NAME e VM\_HOST\_NAME nel file /etc/hosts della macchina virtuale.

Soluzione: Rimuovere le voci duplicate di VM\_DOMAIN\_NAME e VM\_HOST\_NAME dal file /etc/hosts della macchina virtuale.

- **Quando si utilizza l'API di VMware Cloud Director per creare una macchina virtuale da un modello e non si specifica un criterio di storage predefinito, in assenza di un criterio di storage predefinito impostato per il modello, la macchina virtuale appena creata tenta di utilizzare il criterio di storage del modello di origine stesso**

Quando si utilizza l'API di VMware Cloud Director per creare una macchina virtuale da un modello e non si specifica un criterio di storage predefinito, in assenza di un criterio di storage predefinito impostato per il modello, la macchina virtuale appena creata tenta di utilizzare il criterio di storage del modello di origine stesso anziché utilizzare il criterio di storage del VDC dell'organizzazione in cui lo si sta distribuendo.

Soluzione: nessuna.