

# Note di rilascio di VMware Cloud Director 10.1

VMware Cloud Director 10.1 | 9 APR 2020 | Build 15967253 (build installata 15967236)

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

- Per informazioni sulle funzionalità nuove e aggiornate di questa versione, vedere il white paper tecnico di VMware relativo alle [novità di VMware vCloud Director 10.1](#).
- Comportamento modificato nell'interfaccia utente HTML5:  
Nelle versioni precedenti di VMware Cloud Director, è possibile utilizzare il menu Azione della vApp nell'interfaccia utente HTML per arrestare o disattivare una vApp. Entrambe le operazioni di attivazione annullano la distribuzione della vApp, ma influiscono sulla vApp in modo diverso. L'operazione Disattiva non segue le impostazioni di Ordine di avvio e arresto per le macchine virtuali nella vApp. L'operazione Disattiva annulla anche la distribuzione di tutte le reti di vApp disconnettendo tutte le NIC delle macchine virtuali dalle reti VDC dell'organizzazione e rimuovendo tutti i gateway edge distribuiti per la vApp.

In VMware Cloud Director 10.1, l'esecuzione dell'operazione Disattiva in una vApp in esecuzione comporta la disattivazione di tutte le macchine virtuali nella vApp senza annullare la distribuzione della vApp e delle relative macchine virtuali. Le schede NIC delle macchine virtuali restano connesse alle rispettive reti e tutti i gateway edge della vApp rimangono distribuiti. La vApp e le macchine virtuali nella vApp rimangono distribuite. L'azione Disattiva per ciascuna delle singole macchine virtuali nella vApp rimane attiva ed è possibile utilizzarla per disattivare una macchina virtuale. Questa azione comporta l'annullamento della distribuzione di questa macchina virtuale.

Quando si disattiva una vApp, l'operazione Disattiva segue l'ordine di avvio definito nelle impostazioni di Ordine di avvio e arresto. Di conseguenza, le macchine virtuali vengono disattivate in ordine inverso rispetto a come sono state configurate per l'avvio. L'impostazione Attesa arresto non viene applicata durante l'operazione Disattiva. Quando si disattiva una vApp, lo stato di attivazione della vApp, derivato dagli stati di attivazione delle relative macchine virtuali, viene visualizzato come Disattivato.

- Lo schema dell'API 34.0 di VMware Cloud Director include la definizione per gli attributi numberOfCpus e MemoryAllocationMB.

## Sicurezza

- **ATTENZIONE:** dopo l'aggiornamento alla versione 10.1, VMware Cloud Director verificherà sempre i certificati per tutti gli endpoint dell'infrastruttura a cui è connesso. Ciò è dovuto a una modifica della modalità con cui VMware Cloud Director gestisce i certificati SSL. Se non si importano i certificati in VMware Cloud Director prima dell'aggiornamento, per le connessioni di vCenter Server e NSX potrebbero verificarsi errori di connessione non riuscita a causa di problemi della verifica di SSL. In questo caso, dopo l'aggiornamento, sono disponibili due opzioni:
  1. Eseguire il comando `trust-infra-certs` dello strumento di gestione delle celle per connettersi e recuperare automaticamente i certificati di tutti gli endpoint dell'infrastruttura per le istanze di vCenter Server e NSX Manager nell'archivio dei certificati centralizzato. Vedere [Importazione dei certificati di endpoint dalle risorse di vSphere](#).
  2. Nell'interfaccia utente del portale di amministrazione del provider di servizi, selezionare ciascuna istanza di vCenter Server e NSX e immettere di nuovo le credenziali mentre si accetta il certificato.
- A partire dalla versione 10.1, i provider di servizi e i tenant possono utilizzare l'API di VMware Cloud Director per testare le connessioni ai server remoti e per verificare l'identità dei server come parte di un handshake SSL. Per proteggere le connessioni di rete di VMware Cloud Director, configurare un elenco di host interni non consentiti che sono irraggiungibili per i tenant che utilizzano l'API di VMware Cloud Director per il test della connessione. Configurare l'elenco degli host interni dopo l'installazione o l'aggiornamento di VMware Cloud Director e prima di consentire ai tenant di accedere a VMware Cloud Director. Vedere [Configurazione di un elenco di elementi non consentiti per una connessione di prova](#).
- In VMware Cloud Director 10.1, il comportamento che considera attendibili tutti i certificati SSL è deprecato. In questa versione, le connessioni di vCenter Server e NSX non supportano questa opzione. Il comportamento che considera attendibili tutti i certificati è deprecato anche per tutte le altre connessioni e non sarà più supportato dopo VMware Cloud Director 10.1. Gli amministratori di sistema devono prepararsi a questa transizione.
  - Se si utilizza il protocollo LDAP per l'organizzazione del sistema VMware Cloud Director, è possibile utilizzare la finestra di dialogo `trust-on-first-use` nell'interfaccia utente o caricare i certificati mediante l'API.
  - Controllare tutti gli usi di questa opzione e fornire i certificati appropriati mediante l'interfaccia utente o l'API.
  - Comunicare le modifiche ai tenant. Questa configurazione deve essere modificata in tutti i tenant che utilizzano il protocollo LDAP personalizzato con l'opzione **Accetta tutti i certificati** abilitata. I tenant possono utilizzare la finestra di dialogo `trust-on-first-use` nell'interfaccia utente o caricare i certificati tramite l'API.

## Pacchetti open source aggiornati

- jackson-databind aggiornato alla versione 2.9.10.1.
- jre aggiornato alla versione 1.8.0u231.
- openssl aggiornato alla versione 1.0.2u.
- xstream aggiornato alla versione 1.4.11.1.

## Avvisi relativi al supporto del prodotto

VMware Cloud Director 10.1 non supporta vSphere 7.0 e NSX-T Data Center 3.0. La certificazione di interoperabilità è in corso e vSphere 7.0 e NSX-T Data Center 3.0 saranno supportati in una versione di patch secondaria di VMware Cloud Director 10.1.

Le reti esterne supportate dai gateway di livello 0 di VRF-lite in NSX-T Data Center non sono supportate.

## Avvisi di fine ciclo di vita e fine supporto

- Il database di SQL Server non è più supportato. È supportato solo il database PostgreSQL.
- Oracle Linux non è più supportato come sistema operativo host per installare l'applicazione VMware Cloud Director.
- Le versioni 20 e precedenti dell'API di VMware Cloud Director non sono supportate.
- Le versioni dell'API di VMware Cloud Director dalla 27.0 alla 29.0 sono obsolete e non saranno più supportate dopo VMware Cloud Director 10.1.
- La versione 30.0 dell'API di VMware Cloud Director è obsoleta.
- L'interfaccia utente basata su Flex è stata rimossa dal prodotto e non è più supportata.
- L'endpoint di accesso dell'API `/api/sessions` è stato deprecato nell'API di VMware Cloud Director versione 33.0/VMware Cloud Director 10.0 e non sarà 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 deprecata per i protocolli HTTP e HTTPS e verrà rimossa in una versione futura. È necessario utilizzare `/api/server_status` per entrambi i protocolli HTTP e HTTPS.
- 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 supportate nelle versioni future. 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 versioni future 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.

## Prossimi avvisi di fine supporto

- La versione 34.0 dell'API di VMware Cloud Director (VMware Cloud Director 10.1) contiene API che verranno deprecate a breve e rimosse nelle versioni future. Vedere la [Guida alla programmazione dell'API di VMware Cloud Director](#).

## Aggiornamento da versioni precedenti

Per ulteriori informazioni sull'aggiornamento a VMware Cloud Director 10.1, 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 10.1, vedere [Porte e protocolli di VMware](#).

## 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

## Sistemi operativi dei server VMware Cloud Director supportati

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

## 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 RabbitMQ versione 3.7.9 o 3.8.2

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

È possibile configurare l'installazione di VMware Cloud Director per archiviare le metriche raccolte da VMware Cloud Director sulle prestazioni delle macchine virtuali e l'utilizzo delle risorse. I dati relativi alle metriche cronologiche vengono archiviati in un database Cassandra. VMware Cloud Director supporta le versioni 3.x di Cassandra.

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

## 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 (disabilitato per impostazione predefinita)
- TLS versione 1.0 (disabilitato 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 altri pacchetti di crittografia supportati che sono disabilitati 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
- Microsoft Internet Explorer 11

## 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

- **Quando si associano due siti dell'appliance di VMware Cloud Director, gli oggetti non sono visibili nei siti**  
Se si crea un'associazione di siti e i siti includono oggetti come organizzazioni, VDC dell'organizzazione, vApp e macchine virtuali, non è possibile visualizzare gli oggetti del sito corrente. L'interfaccia utente HTML 5 mostra solo gli oggetti dell'altro sito associato. Il problema si verifica durante la comunicazione

multisito fan-out perché il file etc/hosts dell'appliance di VMware Cloud Director non include contenuti corretti.

- **L'aggiornamento di un criterio di ridimensionamento delle macchine virtuali non riesce e viene restituito un errore di allocazione della memoria**  
Se si converte il VDC di un pool di allocazioni in un VDC dell'organizzazione Flex, vCloud Director mantiene le informazioni del criterio massimo dal VDC del pool di allocazioni prima della conversione. La prenotazione della CPU o della memoria offre un valore superiore rispetto alle prenotazioni definite nel VDC del pool di allocazioni e viene visualizzato il messaggio di errore Le impostazioni di prenotazione, limite o condivisioni della macchina virtuale non sono valide
- **La disattivazione o la sospensione della cella primaria in un ambiente con più celle non consente di riavviare le attività periodiche nella cella secondaria**  
In un ambiente con più celle, quando si disattiva o si sospende la cella primaria, le attività periodiche in esecuzione in background nella cella primaria non vengono avviate dalla cella secondaria.
- **La clonazione di una macchina virtuale in un criterio di storage basato su host con i servizi dati abilitati, in una macchina virtuale con un criterio di storage basato su host diverso non riesce e viene visualizzato un messaggio di errore**  
Se si crea una macchina virtuale in un criterio di storage con regole basate su host come IOPS o la crittografia della macchina virtuale abilitata, il tentativo di clonazione della macchina virtuale e di modifica del criterio di storage della macchina virtuale di destinazione non riesce e viene visualizzato un messaggio di errore simile a La modifica o l'applicazione dei criteri di storage della macchina virtuale con funzionalità di servizi dati durante le operazioni di clonazione non è consentita. I criteri di storage della macchina virtuali con funzionalità di servizi dati possono essere assegnati alla macchina virtuale con provisioning dopo aver completato l'operazione di clonazione e prima di attivare la macchina virtuale.
- **Il ruolo del tenant globale Autore vApp può caricare e creare modelli e multimedia senza disporre del diritto necessario per queste operazioni**  
Per impostazione predefinita, il ruolo del tenant globale Autore vApp dispone del diritto Aggiungi una vApp da Cloud personale. Poiché questo diritto e il diritto Modello/Multimedia: Crea/Carica condividono una singola operazione, VMware Cloud Director concede erroneamente anche il diritto Modello/Multimedia: Crea/Carica al ruolo Autore vApp.  
  
Il problema è stato risolto. Se si desidera che il ruolo Autore vApp continui a disporre del diritto Modello/Multimedia: Crea/Carica, un provider di servizi può aggiungere il diritto al ruolo globale Autore vApp e pubblicarlo in un'organizzazione.
- **Le macchine virtuali appena create vengono distribuite nel criterio di storage predefinito del VDC dell'organizzazione**  
Nel portale tenant di vCloud Director, quando si crea una nuova macchina virtuale standalone, l'opzione per specificare il criterio di storage non è disponibile. Di conseguenza, la macchina virtuale creata viene distribuita con il criterio di storage predefinito del VDC dell'organizzazione.

## Problemi noti

- **Novità Non è possibile aprire la console Web di una macchina virtuale quando si utilizza Microsoft Internet Explorer 11**  
Se si utilizza Microsoft Internet Explorer 11 per connettersi alla console di una macchina virtuale, viene aperta una finestra vuota e non è possibile accedere alla console della macchina virtuale.

Soluzione: nessuna.

- **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 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 Se si utilizza l'API di VMware Cloud Director per eseguire query in una vApp, vengono restituiti campi vuoti per gli attributi numberOfCpus e MemoryAllocationMB**  
Quando si utilizza l'API 33.0 di VMware Cloud Director o una versione precedente per eseguire una query REST API di una vApp, il corpo della risposta della REST API restituisce campi vuoti per gli attributi numberOfCpus e MemoryAllocationMB. Questo problema può verificarsi perché lo schema dell'API non include la definizione per gli attributi numberOfCpus MemoryAllocationMB.

Soluzione: Utilizzare l'API 34.0 di VMware Cloud Director per eseguire una query in una vApp.

- **Nuovo 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 "I valori nuovi e obsoleti sono stati aggiornati per la redistribuzione, codice di errore 503266".

Soluzione: Utilizzare l'API del criterio di NSX-T Data Center per aggiornare la configurazione della redistribuzione della rete esterna a cui è connesso il gateway edge NSX-T.

1. Prendere nota dell'ID del router di livello 0 che esegue il backup della rete esterna a cui è connesso il gateway edge NSX-T.
  - Eseguire una richiesta GET per ottenere un elenco dei router di livello 0 nell'ambiente in uso.  
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s
  - Esaminare l'elenco per identificare il livello 0 in base al nome visualizzato, che corrisponde al nome del router di livello 0 nella scheda Informazioni generali per la rete esterna nell'interfaccia utente di VMware Cloud Director.
2. Aggiornare manualmente la rete esterna (gateway di livello 0).
  - Eseguire una richiesta GET per ottenere l'elenco di localeServices nel router.  
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services



La risposta restituisce un servizio locale.

- Copiare localeService ID ed eseguire una richiesta GET per esaminarlo.

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

La risposta restituisce un elenco delle proprietà del servizio locale.

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

- Modificare la risposta nel modo seguente.

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

- Eseguire una richiesta PUT con le proprietà modificate per aggiornare il localeService del router di livello 0.

- **Nuovo La riassegnazione di una macchina virtuale a un cluster diverso non riesce se il contenitore di storage di destinazione è un cluster di datastore**

Quando si esegue un'operazione che genera un tentativo di riassegnazione di una macchina virtuale a un cluster diverso e il contenitore di storage di destinazione è un cluster di datastore, la migrazione non riesce e viene visualizzato un errore NO\_FEASIBLE\_PLACEMENT\_SOLUTION. Nei registri di VMware Cloud Director, viene visualizzato un errore di chiamata di Storage DRS con invalidProperty = spec.host.

Soluzione:

1. Utilizzare vSphere Client per disabilitare Storage DRS nel cluster di datastore di destinazione oppure utilizzare l'API di VMware Cloud Director per modificare lo storage di destinazione per la riassegnazione a un datastore.

2. Tentare di nuovo l'operazione non riuscita.

- **Nuovo La distribuzione dell'appliance VMware Cloud Director non riesce quando si abilita l'impostazione per la scadenza della password root al primo accesso**

Se si tenta di distribuire un'appliance con l'impostazione per la **scadenza della password root al primo accesso** abilitata, la distribuzione non riesce e il file di registro /opt/vmware/var/log/firstboot mostra un errore:

[ERROR] postgresauth script failed to execute.

Soluzione: disabilitare l'impostazione per la **scadenza della password root al primo accesso** e specificare una password root iniziale che contenga almeno otto caratteri, un carattere maiuscolo, un carattere minuscolo, una cifra numerica e un carattere speciale.

- **Nuovo** 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.

- **Nuovo** 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.

- **Nuovo** 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**.

- **Nuovo** 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.

- **Nuovo** In un ambiente misto multisito con VMware Cloud Director versioni 10.0 e 10.1, è possibile considerare attendibili i certificati per le connessioni di vCenter Server e NSX solo per gli oggetti del

### sito locale

Se si dispone di un ambiente multisito con VMware Cloud Director versioni 10.0 e 10.1 associati tra loro, quando si accede a uno dei siti, non è possibile registrare le istanze di vCenter Server o NSX Manager nell'altro sito.

Soluzione: accedere al sito in cui si desidera registrare l'istanza di vCenter Server o NSX Manager e avviare il processo di registrazione.

- **Nuovo Nel portale tenant di VMware Cloud Director, non è possibile filtrare le macchine virtuali in base al data center nell'opzione di filtraggio avanzato per le macchine virtuali nella scheda Applicazioni**

Nel portale tenant di VMware Cloud Director, quando si accede alle macchine virtuali nella scheda Applicazioni nella barra di spostamento superiore, il filtraggio delle macchine virtuali in base al data center dall'opzione di filtraggio avanzato genera un errore Richiesta non valida: Nome di proprietà vdcName sconosciuto.

Soluzione: dalla barra di spostamento superiore, selezionare **Data center**, quindi selezionare un data center per visualizzare le relative macchine virtuali.

- **Nuovo I servizi di estensione non possono elaborare i messaggi RabbitMQ da VMware Cloud Director**

I servizi di estensione che si basano su RabbitMQ non possono ottenere l'intestazione `notification.type` da un messaggio perché l'intestazione ha un nuovo nome temporaneo. Il nome dell'intestazione per VMware Cloud Director 10.1.0 è `notification.operationType`.

Soluzione: se i servizi di estensione elaborano i messaggi RabbitMQ da VMware Cloud Director e utilizzano l'intestazione del messaggio `notification.type`, è necessario modificarli. Se l'intestazione `notification.type` header non è disponibile, i servizi di estensione devono ottenere il valore dall'intestazione `notification.operationType`. Questa modifica è necessaria solo per la versione 10.1.0.

- **Nel portale di amministrazione del provider di servizi di VMware Cloud Director, l'eliminazione di un virtual data center dell'organizzazione non riesce e viene visualizzato un errore**

Nel portale di amministrazione del provider di servizi di VMware Cloud Director, se si aggiunge un gateway edge al VDC dell'organizzazione e si abilita il gateway per fornire il routing distribuito di VMware Cloud Director, il tentativo di eliminazione del VDC dell'organizzazione in modo ricorsivo non riesce con un messaggio di errore Impossibile eliminare la rete VDC dell'organizzazione.

Soluzione:

1. utilizzando l'API, eliminare le reti VDC dell'organizzazione e i gateway edge associati al VDC dell'organizzazione.
2. Utilizzando l'API, eliminare il VDC dell'organizzazione.

- **Se si disabilita l'accesso del provider all'endpoint di accesso dell'API legacy, tutte le integrazioni dell'API che si basano sull'accesso dell'amministratore di sistema smettono di funzionare, inclusi vCloud Usage Meter e vCloud Availability for VMware Cloud Director**

A partire da vCloud Director 10.0, è possibile utilizzare endpoint di accesso VMware Cloud Director OpenAPI separati per l'accesso del provider di servizi e del tenant a VMware Cloud Director. Se l'accesso del provider di servizi all'endpoint legacy `/api/sessions` è disabilitato, i prodotti che si integrano con VMware Cloud Director, come vCloud Usage Meter e vCloud Availability for VMware Cloud Director, smettono di funzionare. Questi prodotti richiederanno una patch per continuare a funzionare.

Il problema riguarda solo gli amministratori di sistema e non l'accesso del tenant.

Soluzione: riabilitare l'accesso del provider di servizi all'endpoint `/api/sessions` legacy utilizzando lo strumento di gestione delle celle.

- **Quando si modificano i valori di garanzia della prenotazione di un VDC, le macchine virtuali esistenti non vengono aggiornate di conseguenza anche dopo un riavvio**

Se si dispone di un VDC dell'organizzazione Flex con il criterio predefinito di sistema e nelle macchine virtuali attivate su tale VDC viene applicato il criterio di ridimensionamento predefinito, quando si aumenta il valore di garanzia della risorsa del VDC, la prenotazione della risorsa per le macchine virtuali esistenti non viene aggiornata e le macchine virtuali non vengono inoltre contrassegnate come non conformi. Il problema si verifica anche quando si converte un modello di allocazione del VDC legacy in un modello di allocazione Flex e le macchine virtuali esistenti diventano non conformi al nuovo criterio predefinito del VDC dell'organizzazione Flex dopo la conversione.

Soluzione:

1. Per trovare l'identificatore della macchina virtuale, nel portale tenant di VMware Cloud Director, passare alla pagina Dettagli della macchina virtuale. L'URL mostra l'identificatore  
`https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifier/general`
2. Per visualizzare le macchine virtuali non conformi nell'interfaccia utente di VMware Cloud Director, eseguire un controllo di conformità esplicito rispetto alle macchine virtuali utilizzando l'API di VMware Cloud Director.  
POST: `https://VCD_IP_Address/api/vApp/vm-Identifier/action/checkComputePolicyCompliance`
3. Per riapplicare il criterio e riconfigurare le prenotazioni delle risorse, nel portale tenant di VMware Cloud Director fare clic su **Rendi macchina virtuale conforme** per una macchina virtuale non conforme.

- **In VMware Cloud Director vengono visualizzate informazioni non corrette sulle macchine virtuali in esecuzione, sulle macchine virtuali totali e sulle statistiche della CPU e della memoria in istanze di vCenter Server dedicate**

Se la versione di un'istanza di vCenter Server dedicata è 6.0 Update 3i o precedente, 6.5 Update 2 o precedente oppure 6.7 Update 1 o precedente, in VMware Cloud Director vengono visualizzate informazioni non corrette sulle macchine virtuali in esecuzione, sulle macchine virtuali totali e sui dati statistici relativi a CPU e memoria nell'istanza di vCenter Server. Nel riquadro di vCenter Server dedicato nel portale tenant e nelle informazioni di vCenter Server dedicate nel portale di amministrazione del provider di servizi viene visualizzato zero per le macchine virtuali in esecuzione e le macchine virtuali totali, anche quando sono presenti macchine virtuali nell'ambiente vSphere.

Soluzione: Aggiornare l'istanza di vCenter Server alla versione 6.0 Update 3j, 6.5 Update 3, 6.7 Update 2 o successiva.

- **La modifica del criterio di calcolo di una macchina virtuale accesa potrebbe non riuscire**

Quando si tenta di modificare il criterio di calcolo di una macchina virtuale accesa, se il nuovo criterio di calcolo è associato a un criterio di calcolo del VDC del provider che dispone di gruppi di macchine virtuali o di gruppi di macchine virtuali logiche, si verifica un errore. Il messaggio di errore contiene:  
Underlying system error: com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation.

Soluzione: spegnere la macchina virtuale e riprovare l'operazione.

- **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.

- **VMware Cloud Director 10.1 supporta solo un elenco di parametri di input dei flussi di lavoro di vRealize Orchestrator**

VMware Cloud Director 10.1 supporta i seguenti parametri di input dei flussi di lavoro di vRealize Orchestrator:

- booleano
- sdkObject
- SecureString
- numero
- mimeAttachment
- proprietà
- data
- composito
- Regex
- encryptedString
- array

Soluzione: Nessuna

- **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 (VVOs)**

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 VVOs. 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 VVOs. Per consolidare una macchina virtuale con uno snapshot in un archivio dati VAAI o VVOI, trasferire la macchina virtuale in un contenitore di storage diverso.

- **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.