

Notas de la versión de VMware Cloud Director 10.2

VMware Cloud Director 10.2 | 15 de octubre de 2020 | Compilación 17029810 (compilación instalada 17008054)

Compruebe las adiciones y las actualizaciones de estas notas de la versión.

Contenido de este documento

- [Novedades de esta versión](#)
- [Seguridad](#)
- [Avisos de compatibilidad con el producto](#)
- [Actualización de versiones anteriores](#)
- [Requisitos del sistema e instalación](#)
- [Problemas resueltos](#)
- [Problemas conocidos](#)

Novedades de esta versión

La versión 10.2 de VMware Cloud Director incluye lo siguiente:

- **Paridad funcional avanzada de NSX-T:** NSX Advanced Load Balancer (Avi), firewall distribuido, VRF-Lite, Cross VDC Networking, IPv6, pila dual (IPv4/IPv6) en la misma red, SLAAC, DHCPv6, CVDS (vSphere 7.0/NSX-T 3.0), VPN de 2 capas (solo API).
- **Compatibilidad con aplicaciones modernas en VMware Cloud Director con vSphere with Kubernetes en tiempo de ejecución de Tanzu:** interfaz de usuario de proveedores y tenants para administrar y consumir clústeres de Kubernetes.
- **Mejoras del dispositivo virtual de VMware Cloud Director:** validación de la entrada del usuario durante la implementación inicial; restauración de celdas simplificada con creación de celdas en espera optimizada.
- **Mejoras de almacenamiento:** control de IOPS a nivel de disco para proveedores y tenants; discos compartidos.
- **Mejoras de seguridad:** consulte la sección [Seguridad](#).
- **Mejoras de la interfaz de usuario:** búsqueda rápida, avisos, administración de certificados.
- **Mejoras de la extensibilidad de la plataforma.**
- **Mejoras de escala:** consulte [Valores máximos de configuración de VMware](#).

Para obtener información sobre las funciones nuevas y actualizadas de esta versión, consulte [Novedades de VMware Cloud Director 10.2](#).

Para obtener las notas de la versión más recientes de las soluciones del complemento de VMware Cloud Director, consulte los siguientes vínculos:

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

Seguridad

El dispositivo virtual de VMware Cloud Director 10.2 incluye una instancia de Photon OS actualizada a este [aviso de seguridad de Photon](#).

VMware Cloud Director 10.2 admite los almacenes de claves PKCS12. Puede utilizar un almacén de claves con formato PKCS12 cuando configure las conexiones de red y de bases de datos de VMware Cloud Director, o bien cuando utilice la herramienta de

administración de celdas para generar o reemplazar certificados. Para obtener más información, consulte la *Guía de instalación, configuración y actualización de VMware Cloud Director*.

Avisos de compatibilidad con el producto

Los nodos del clúster de TKG están aislados. Sin embargo, cualquier persona con acceso de red al endpoint o la dirección IP virtual del servicio puede acceder a los servicios expuestos por un clúster de TKG, y dichos servicios están protegidos por sus propios mecanismos de autenticación y autorización. Dado que la autenticación es la única protección que se utiliza para proteger el acceso a las cargas de trabajo, se recomienda encarecidamente que solo permita el tráfico cifrado (como TLS) en los servicios de entrada.

Advertencias sobre la finalización de la vida útil y del soporte

- No se admiten las versiones 29 y anteriores de la API de VMware Cloud Director.
- Las versiones 30 y 31 de la API de VMware Cloud Director han quedado obsoletas.
- La versión 30 de la API de VMware Cloud Director dejará de estar disponible en la próxima versión.
- El endpoint de inicio de sesión de la API `/api/sessions` ha quedado obsoleto a partir de la versión 33.0 de la API de VMware Cloud Director y de VMware Cloud Director 10.0, y no se admitirá en versiones futuras de VMware Cloud Director. Puede utilizar los endpoints de inicio de sesión independientes de OpenAPI para VMware Cloud Director a fin de que los tenants y los proveedores de servicios puedan acceder a VMware Cloud Director.
- La API `/cloud/server_status` ha quedado obsoleta para los protocolos HTTP y HTTPS. `/cloud/server_status` se eliminará en una versión futura de VMware Cloud Director. Debe utilizar `/api/server_status` para los protocolos HTTP y HTTPS.
- Las acciones de restablecimiento `/amqp/action/resetAmqpCertificate` y `/amqp/action/resetAmqpKeyStore` se han eliminado de la versión 35.0 de la API de VMware Cloud Director debido a la forma en la que VMware Cloud Director almacena y procesa los certificados SSL. Debe utilizar el endpoint `/cloudapi/1.0.0/ssl/trustedCertificates` para desconfiar de los certificados.
- Las acciones de actualización `/amqp/action/updateAmqpCertificate` y `/amqp/action/updateLdapKeyStore` han quedado obsoletas. Las acciones se eliminarán en una versión futura de VMware Cloud Director. Puede usar el nuevo endpoint para confiar en los certificados AMQP `/cloudapi/1.0.0/ssl/trustedCertificates`.
- Las acciones de restablecimiento `/ldap/action/resetLdapCertificate` y `/ldap/action/resetLdapKeyStore` se han eliminado de la versión 34.0 de la API de VMware Cloud Director en adelante debido a la forma en la que VMware Cloud Director 10.1 almacena y procesa los certificados SSL. Debe utilizar el endpoint `/cloudapi/1.0.0/ssl/trustedCertificates` para desconfiar de los certificados.
- Las acciones de actualización `/ldap/action/updateLdapCertificate` y `/ldap/action/updateLdapKeyStore` han quedado obsoletas y no se admitirán en versiones futuras. VMware Cloud Director introduce un nuevo endpoint para confiar en certificados LDAP: `/cloudapi/1.0.0/ssl/trustedCertificates`.
- vSphere deja de emplear SSO de vSphere como un IDP de SAML. Todas las implementaciones de VMware Cloud Director configuradas para usar SSO de vSphere como su IDP de SAML deben migrar a un IDP de SAML externo diferente. El uso de este IDP no se admitirá en las próximas versiones de vSphere y VMware Cloud Director.
- Ya no se admiten los certificados DSA y DSS, ya que no hay disponibles conjuntos de claves de cifrado recomendados para ellos.

Actualización de versiones anteriores

Para obtener más información sobre la actualización a VMware Cloud Director 10.2, los flujos de trabajo, y las rutas de actualización y migración, consulte [Actualizar y migrar el dispositivo de VMware Cloud Director](#) o [Actualizar vCloud Director en Linux](#).

Requisitos del sistema e instalación

Puertos y protocolos

Para obtener información sobre los protocolos y los puertos de red que VMware Cloud Director 10.2 utiliza, consulte [VMware Ports and Protocols](#).

Matriz de compatibilidad

Consulte las [Matrices de interoperabilidad de productos de VMware](#) para obtener información actualizada sobre:

- Interoperabilidad de VMware Cloud Director con otras plataformas de VMware
- Bases de datos de VMware Cloud Director compatibles
- NSX Advanced Load Balancer (Avi): esta versión de Cloud Director actualmente solo admite NSX Advanced Load Balancer (Avi) versión 20.1.1

Sistemas operativos de VMware Cloud Director Server compatibles

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

Implementar el dispositivo de VMware Cloud Director

Cuando se implementa el dispositivo de VMware Cloud Director 10.2 como una plantilla de OVF mediante VMware OVF Tool, se debe incluir el siguiente parámetro, el cual es nuevo para la versión 10.2: `--X:enableHiddenProperties`. Si no se incluye este parámetro, en VMware OVF Tool se produce el error La propiedad `vcloudapp.nfs_mount.VMware_vCloud_Director` no es configurable por el usuario..

Consulte [Implementar el dispositivo de VMware Cloud Director mediante VMware OVF Tool](#).

Servidores AMQP compatibles

VMware Cloud Director utiliza AMQP para proporcionar el bus de mensajes que emplean los servicios de extensión, las extensiones de objeto y las notificaciones. Esta versión de VMware Cloud Director requiere la versión 3.8.x de RabbitMQ.

Para obtener más información, consulte la *Guía de instalación, configuración y actualización de VMware Cloud Director*.

Bases de datos admitidas para almacenar datos de métricas históricas

VMware Cloud Director es compatible con las versiones 3.11.x de Apache Cassandra.

Requisitos de espacio de disco

Cada servidor de VMware Cloud Director requiere aproximadamente 2.100 MB de espacio libre para los archivos de instalación y de registro.

Requisitos de memoria

Consulte la *Guía de instalación, configuración y actualización de VMware Cloud Director* para conocer los requisitos de memoria.

Requisitos de CPU

VMware Cloud Director es una aplicación enlazada a la CPU. Se deben seguir las directrices de sobreconfirmación de CPU para la versión de vSphere que corresponda. En entornos virtualizados, debe haber una proporción razonable entre CPU físicas y vCPU, independientemente del número de núcleos disponibles para VMware Cloud Director, de modo que no se produzca una extrema sobreconfirmación.

Paquetes de software de Linux necesarios

Cada servidor de VMware Cloud Director debe incluir instalaciones de varios paquetes comunes de software de Linux. Por lo general, los paquetes se instalan de forma predeterminada con el software del sistema operativo. Si falta algún paquete, se produce un error en el instalador y se muestra un mensaje de diagnóstico.

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
		which

krb5-libs libXt
libgcc libXtst

Además de los paquetes requeridos por el instalador, hay varios procedimientos para configurar conexiones de red y crear certificados SSL que requieren el uso del comando `nslookup` de Linux, el cual está disponible en el paquete `bind-utils` de Linux.

Servidores LDAP compatibles

Puede importar usuarios y grupos en VMware Cloud Director a partir de los siguientes servicios LDAP.

Plataforma	Servicio LDAP	Métodos de autenticación
Windows Server 2012	Active Directory	Simple, Simple SSL
Windows Server 2016	Active Directory	Simple, Simple SSL
Linux	OpenLDAP	Simple, Simple SSL

Protocolos de seguridad y conjuntos de cifrado admitidos

VMware Cloud Director requiere conexiones de cliente para garantizar la seguridad. TLS versión 1.0 y versión 1.1, así como SSL versión 3, han demostrado tener graves vulnerabilidades de seguridad, por lo que ya no se incluyen en el conjunto predeterminado de protocolos que el servidor ofrece al realizar una conexión del cliente. Los administradores del sistema pueden habilitar más protocolos y conjuntos de claves de cifrado. Consulte la sección sobre la herramienta de administración de celdas en la *Guía de instalación, configuración y actualización de VMware Cloud Director*. Se admiten los siguientes protocolos de seguridad:

- TLS versión 1.2
- TLS versión 1.1 (desactivado de forma predeterminada)
- TLS versión 1.0 (desactivado de forma predeterminada)

Conjuntos de claves de cifrado admitidos que están habilitados de forma predeterminada:

- 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

Los administradores del sistema pueden utilizar la herramienta de administración de celdas para habilitar de forma explícita otros conjuntos de claves de cifrado admitidos que están desactivados de forma predeterminada.

Nota: Para garantizar la interoperabilidad con versiones de vCenter Server anteriores a la 5.5-update-3e y versiones de `ovftool` anteriores a la 4.2, es necesario que VMware Cloud Director admita TLS 1.0. Puede usar la herramienta de administración de celdas para volver a configurar el conjunto de protocolos o cifrados SSL compatibles. Consulte la sección sobre la herramienta de administración de celdas en la *Guía de instalación, configuración y actualización de VMware Cloud Director*.

Exploradores compatibles

VMware Cloud Director es compatible con la versión principal actual y la versión principal anterior de los siguientes navegadores:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Nota: Internet Explorer 11 no es compatible con VMware Cloud Director 10.2 y versiones posteriores. Puede usar Microsoft Edge u otro navegador compatible. Si tiene que utilizar Internet Explorer 11, considere la posibilidad de seguir empleando la versión 10.0.x o 10.1.x de VMware Cloud Director hasta que pueda usar otro navegador.

Sistemas operativos invitados y versiones de hardware virtual compatibles

VMware Cloud Director admite todos los sistemas operativos invitados y todas las versiones de hardware virtual compatibles con los hosts ESXi que respaldan cada grupo de recursos.

VMware Cloud Director WebMKS 2.1.1

La consola de VMware Cloud Director WebMKS 2.1.1 ahora admite lo siguiente:

- La tecla Imprimir pantalla en Google Chrome y en Mozilla Firefox para Windows.
- La tecla Windows en Windows y macOS. Para simular la pulsación de la tecla Windows, presione Ctrl + Windows en el sistema operativo Windows o Ctrl + Comando en macOS.
- Detección automática de la distribución del teclado en Google Chrome y Mozilla Firefox.

Problemas resueltos

- **Se produce un error al intentar agregar una regla NAT a una puerta de enlace NSX-T Edge**
Al intentar agregar una regla NAT a una puerta de enlace NSX-T Edge se produce el siguiente error: Los valores nuevos y obsoletos se han actualizado juntos para la redistribución, código de error 503266.
- **Se produce un error al mover una máquina virtual entre clústeres si el contenedor de almacenamiento de destino es un clúster de almacenes de datos**
Se produce un error al mover una máquina virtual entre clústeres si el contenedor de almacenamiento de destino es un clúster de almacenes de datos. Los registros muestran el siguiente error.

```
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 }
```

- **No se puede implementar el dispositivo si la opción "Caducar la contraseña raíz tras el primer inicio de sesión" está habilitada**
Cuando se intenta implementar un dispositivo, se produce un error en la implementación y se muestra el siguiente error en el registro /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.
- **En el portal para tenants de VMware Cloud Director, no funciona el filtrado avanzado de máquinas virtuales en función de la ubicación del VDC**
En la interfaz de usuario del portal para tenants de VMware Cloud Director, si intenta utilizar un filtro avanzado basado en la ubicación del VDC para filtrar las máquinas virtuales, se produce un error en la búsqueda.

Problemas conocidos

- **Nuevo Las máquinas virtuales dejan de ser conformes después de convertir un VDC de grupo de reserva en un VDC de organización flexible**
En un VDC de organización con un modelo de asignación de grupo de reserva, si algunas de las máquinas virtuales tienen una reserva distinta de cero para la CPU y la memoria, una configuración no ilimitada para la CPU y la memoria, o ambas, después de convertirse en un VDC de organización flexible, esas máquinas virtuales dejan de ser conformes. Si intenta hacer que las máquinas virtuales sean conformes de nuevo, el sistema aplica una directiva incorrecta para la reserva y el límite, y establece las reservas de CPU y memoria en cero y los límites en **Sin límite**.

Solución alternativa:

1. Un administrador del sistema debe crear una directiva de tamaño de máquinas virtuales con la configuración correcta.

2. Un administrador del sistema debe publicar la nueva directiva de tamaño de máquinas virtuales en el VDC de organización flexible convertido.
3. Los tenants pueden utilizar la API de VMware Cloud Director o el portal para tenants de VMware Cloud Director para asignar la directiva de tamaño de máquinas virtuales a las máquinas virtuales existentes en el VDC de organización flexible.

- **Nuevo El estado del Programa de mejora de la experiencia de cliente (CEIP) es **Enabled** incluso después de desactivarlo durante la instalación de VMware Cloud Director**

Durante la instalación de VMware Cloud Director, si desactiva la opción de unirse al CEIP, una vez finalizada la instalación, el estado del CEIP es Activo.

Solución alternativa: Desactive el CEIP siguiendo los pasos del procedimiento [Unirse o abandonar el Programa de mejora de la experiencia del cliente de VMware](#).

- **Nuevo En la interfaz de usuario del portal para tenants, al crear una regla de afinidad o antiafinidad, la anulación de la selección de la casilla Obligatoria no afecta a la configuración de la regla**

En la interfaz de usuario del portal para tenants, al crear una regla de afinidad o antiafinidad, la anulación de la selección de la casilla Obligatoria no afecta a la configuración de la regla. Las reglas de afinidad y antiafinidad siempre son obligatorias, lo que significa que, si no se puede cumplir una regla, las máquinas virtuales que se agregan a la regla no se encienden.

Solución alternativa: Ninguna.

- **Nuevo Después de actualizar a vCenter Server 7.0 Update 2a o Update 2b, no se pueden crear clústeres de Tanzu Kubernetes Grid**

Si la versión de vCenter Server subyacente es 7.0 Update 2a o Update 2b, cuando se intenta crear un clúster de Tanzu Kubernetes Grid mediante el complemento Kubernetes Container Clusters, se produce un error en la tarea.

Solución alternativa: Ninguna.

- **Nuevo Se produce un error al crear un clúster de Tanzu Kubernetes con el complemento de clústeres de contenedores de Kubernetes**

Al crear un clúster de Tanzu Kubernetes con el complemento de clústeres de contenedores de Kubernetes, hay que seleccionar una versión de Kubernetes. Algunas de las versiones del menú desplegable no son compatibles con la infraestructura de respaldo de vSphere. Cuando se selecciona una versión no compatible, se produce un error en la creación del clúster.

Solución alternativa: Elimine el registro del clúster con errores y vuelva a intentarlo con una versión de Tanzu Kubernetes compatible. Para obtener información sobre las incompatibilidades entre Tanzu Kubernetes y vSphere, consulte [Actualizar el entorno de vSphere with Tanzu](#).

- **Nuevo Si un pod de almacenamiento o un clúster respalda una política de almacenamiento, no se puede habilitar la limitación de IOPS de VMware Cloud Director en esa política de almacenamiento**

En el portal para administradores de proveedores de servicios, cuando uno o varios pods o clústeres de almacenamiento respaldan una política de almacenamiento, incluso si desactiva la marca **Impacto en la colocación**, no se puede habilitar la limitación de IOPS de VMware Cloud Director en esa política de almacenamiento.

Solución alternativa: Debe tener acceso de nivel de administrador para solucionar este problema.

1. En vCenter Server, elimine la etiqueta de política de almacenamiento de todos los pods de almacenamiento para los que desea habilitar IOPS y actualice las políticas de almacenamiento.
2. En VMware Cloud Director, desactive **Impacto en la colocación** para habilitar IOPS de VMware Cloud Director en la política de almacenamiento.
3. En vCenter Server, vuelva a asociar la etiqueta a los pods de almacenamiento y actualice las políticas de almacenamiento.

- **Nuevo Al abrir la lista de máquinas virtuales en una vApp y habilitar la opción Selección múltiple, el menú Acciones deja de estar disponible**

Al abrir la lista de máquinas virtuales en una vApp y habilitar la opción Selección múltiple, el menú Acciones deja de estar disponible. Puede seleccionar varias máquinas virtuales, pero no puede realizar ninguna acción en ellas de forma simultánea.

Solución alternativa: Ninguna.

- **Nuevo No se puede editar la configuración de NIC de una máquina virtual independiente**

No se puede actualizar la configuración de NIC de una máquina virtual independiente. Al hacer clic en Editar para abrir la configuración de NIC de la máquina virtual, la página Configuración se abre, pero deja de responder.

Solución alternativa:

1. Convierta la máquina virtual independiente en una vApp.

2. Edite la configuración de NIC de la vApp.
3. Vuelva a convertir la vApp en una máquina virtual independiente.

- **Nuevo Después de actualizar Configuración de publicación de un catálogo suscrito desde la interfaz de usuario del portal para tenants, la sincronización de este catálogo genera un error 401 No autorizado**

Después de actualizar **Configuración de publicación** de un catálogo suscrito desde la interfaz de usuario del portal para tenants, la sincronización de este catálogo genera un error 401 No autorizado. Esto ocurre porque la actualización de la configuración del catálogo hace que la contraseña existente se elimine y se establezca como nula.

Solución alternativa: Actualice **Configuración de publicación** del catálogo y vuelva a establecer la contraseña desde la interfaz de usuario del portal para tenants.

- **Nuevo La actualización de VMware Cloud Director a la versión 10.2 desde la versión 10.1.2 muestra un error incorrecto**
Durante la actualización de VMware Cloud Director a la versión 10.2 desde la versión 10.1.2, se muestra incorrectamente el siguiente mensaje de error:

ERROR: El RPM de otra versión de VMware Cloud Director ya está instalado, pero esa versión no se reconoce y no se admite la actualización desde ella. No se espera que esta actualización se realice correctamente, pero puede continuar de todos modos bajo su propio riesgo.

La actualización de VMware Cloud Director a la versión 10.2 desde la versión 10.1.2 sí se admite y se debe ignorar el mensaje de error.

Solución alternativa: Ignore el error.

- **Cuando se reinicia el dispositivo de VMware Cloud Director, es posible que la API de servicios o la interfaz de usuario de administración de dispositivos informen de que el servicio vmware-vcd se encuentra en un estado erróneo.**
Cuando se reinicia el dispositivo de VMware Cloud Director, es posible que la API de servicios o la interfaz de usuario de administración de dispositivos informen por error de que el servicio vmware-vcd se encuentra en un estado erróneo. Esto sucede cuando el servicio vmware-vcd intenta iniciarse antes de que la pila de redes del sistema operativo esté disponible. Debido a ello, el servicio entra en un estado erróneo y aparece un mensaje de error que indica que el servicio no se pudo enlazar con uno o varios puertos. Por tanto, vcd-watchdog inicia correctamente el servicio vmware-vcd, pero el estado del servicio systemd no refleja este hecho.

Solución alternativa:

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

- **Si hay catálogos suscritos en su organización, cuando VMware Cloud Director se actualice, se producirá un error en la sincronización de catálogos**

Después de la actualización, si tiene catálogos suscritos en su organización, VMware Cloud Director no confía automáticamente en los certificados de endpoints publicados. Si no se confía en los certificados, se producirá un error en la sincronización de la biblioteca de contenido.

Solución alternativa: Confíe manualmente en los certificados de cada suscripción del catálogo. Cuando edite la configuración de suscripción del catálogo, se le pedirá en un cuadro de diálogo de confianza en el primer uso (Trust On First Use, TOFU) que confíe en el certificado del catálogo remoto.

Si no tiene los derechos necesarios para confiar en el certificado, póngase en contacto con el administrador de su organización.

- **Tras actualizar VMware Cloud Director y habilitar la creación del clúster de Tanzu Kubernetes, no hay disponible ninguna directiva generada automáticamente y no se puede crear ni publicar ninguna directiva**

Cuando VMware Cloud Director se actualiza a la versión 10.2 y vCenter Server a la versión 7.0.0d, y se crea un VDC de proveedor respaldado por un clúster supervisor, VMware Cloud Director muestra un icono de Kubernetes junto al VDC. Sin embargo, no hay ninguna directiva de Kubernetes generada automáticamente en el nuevo VDC de proveedor. Cuando se intenta crear o publicar una directiva de Kubernetes en un VDC de organización, no hay clases de máquinas disponibles.

Solución alternativa: Confíe manualmente en el certificado del endpoint de Kubernetes. Para obtener pasos detallados, consulte <https://kb.vmware.com/s/article/80996>.

- **El complemento de configuración de DRaaS y migración aparece dos veces en la barra de navegación superior de la interfaz de usuario de VMware Cloud Director**

El problema se produce debido al cambio de marca de vCloud Availability 4.0.0 a VMware Cloud Director Availability 4.0.0, tras lo cual existen dos complementos. VMware Cloud Director no desactiva el complemento de vCloud Availability 4.0.0 de forma automática. Las versiones anteriores y las nuevas aparecen como el complemento de configuración de DRaaS y migración en la barra de navegación superior, bajo **Más**.

Solución alternativa: Desactive manualmente el complemento de vCloud Availability 4.0.0.

- **No puede publicar una política de Kubernetes de VDC de proveedor en un VDC si el clúster supervisor al que apunta no es el clúster principal en el VDC de proveedor**

Si tiene un VDC de proveedor con varios clústeres supervisores, la publicación de una política de Kubernetes de VDC que apunta a un clúster supervisor no principal no se realiza correctamente y se produce un error `LMException`.

Solución alternativa: Asegúrese de que el VDC de proveedor solo está respaldado por un único clúster supervisor, y que dicho clúster es el principal. Un VDC de proveedor puede estar respaldado por clústeres de hosts y un clúster supervisor, pero el clúster supervisor debe ser el principal.

- **Al introducir un nombre de clúster de Kubernetes con caracteres no latinos, se desactiva el botón Siguiente del asistente de creación de nuevos clústeres**

El complemento de clústeres de contenedores de Kubernetes solo admite caracteres latinos. Si introduce caracteres que no son latinos, se muestra el siguiente error. El nombre debe comenzar por una letra, y solo debe contener caracteres alfanuméricos o guiones (-). (Máximo 128 caracteres).

Solución alternativa: Ninguna.

- **En el complemento de clústeres de contenedores de Kubernetes, las cuadrículas de datos pueden aparecer vacías mientras se cargan**

En el complemento de clústeres de contenedores de Kubernetes, algunas cuadrículas de datos aparecen vacías mientras se cargan debido a que no aparece el indicador giratorio de carga.

Solución alternativa: Ninguna.

- **Después de cambiar el tamaño de un clúster de TKGI, algunos valores de la cuadrícula de datos aparecen en blanco o no son aplicables**

Cuando se cambia el tamaño de un clúster de VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), los valores de clúster de la organización y el VDC en la vista de cuadrícula de datos parecen estar en blanco o no disponibles.

Solución alternativa: Ninguna.

- **Al filtrar una cuadrícula de selección múltiple, los elementos filtrados desaparecen si se desplaza a otra página**

En las cuadrículas de selección múltiple, si filtra los resultados y hay más de una página disponible, las siguientes páginas de resultados filtrados se mostrarán vacías. Este problema se produce en cuadros de diálogo en los que puede seleccionar y filtrar varios elementos de una lista (por ejemplo, añadir políticas de almacenamiento a un VDC de organización, o compartir una vApp o una máquina virtual con usuarios o grupos).

Solución alternativa: Cambie el tamaño de cualquiera de las columnas de la cuadrícula.

- **Al filtrar avisos por prioridad, se produce un error de servidor interno**

Cuando se utiliza la API de VMware Cloud Director, se produce un error al aplicar un filtro de prioridad a un aviso.

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

Solución alternativa: Obtenga todos los avisos y filtrelos manualmente.

- **La documentación de la API proporciona una descripción incorrecta del criterio de ordenación de prioridad de Aviso**

El objeto de modelo Aviso contiene un campo de prioridad para especificar la urgencia de cada aviso que se cree. La documentación de la API de Aviso indica de forma incorrecta que las prioridades se enumeran según un criterio de ordenación descendente. La documentación de la API de VMware Cloud Director enumera las prioridades de un aviso según un criterio de ordenación ascendente.

Solución alternativa: Ninguna.

- **Cuando un usuario con la función Usuario de vApp intenta crear una vApp a partir de una plantilla, puede aparecer el mensaje "Se deniega esta operación"**

Si la función de usuario que tiene asignada es Usuario de vApp, cuando intenta crear una vApp a partir de una plantilla y personaliza las políticas de tamaño de máquinas virtuales de las máquinas virtuales en la vApp, aparece el mensaje "Se deniega esta operación". Esto se produce porque la función Usuario de vApp permite crear instancias de vApp a partir de plantillas, pero no incluye derechos que permitan personalizar la memoria, la CPU o el disco duro de una máquina virtual. Al cambiar la política de tamaño, podría modificar también la memoria o la CPU de la máquina virtual.

Solución alternativa: Ninguna.

- **El tiempo de inactividad de NFS puede provocar un funcionamiento incorrecto de las funcionalidades del clúster del dispositivo de VMware Cloud Director**

Si NFS no está disponible debido a que, por ejemplo, el recurso compartido de NFS está lleno o a que se vuelve de solo lectura, puede provocar un funcionamiento incorrecto de las funcionalidades del clúster del dispositivo. La interfaz de usuario HTML5 no responde mientras la instancia de NFS esté inactiva o no se pueda acceder a ella. También pueden resultar afectadas otras funcionalidades, como las barreras de las celdas principales con errores, los intercambios de celdas, la promoción de celdas en espera, etc. Para obtener más información sobre la configuración correcta del almacenamiento compartido de NFS, consulte [Preparar el almacenamiento del servidor de transferencia para el dispositivo de VMware Cloud Director](#).

Solución alternativa:

- Corrija el estado de NFS para que no sea de solo lectura.
- Si está lleno, limpie el recurso compartido de NFS.
- **Al confiar en un endpoint cuando se agregan recursos de vCenter Server y NSX en un entorno multisitio, el endpoint no se agrega al área de almacenamiento de certificados centralizada**

En un entorno multisitio, al utilizar la interfaz de usuario HTML5, si se inició sesión en un sitio de vCloud Director 10.0 o si se intenta registrar una instancia de vCenter Server en un sitio de vCloud Director 10.0, VMware Cloud Director no agregará el endpoint al área de almacenamiento de certificados centralizada.

Solución alternativa:

- Importe el certificado en el sitio de VMware Cloud Director 10.1 mediante la API.
 - Para activar la funcionalidad de administración de certificados, desplácese hasta Service Provider Admin Portal del sitio de VMware Cloud Director 10.1, vaya al cuadro de diálogo **Editar** del servicio y haga clic en **Guardar**.
 - **Se produce un error al intentar cifrar discos con nombre en vCenter Server 6.5 o una versión anterior**
- En el caso de las instancias de vCenter Server 6.5 o una versión anterior, si intenta asociar discos con nombre nuevos o existentes a una política habilitada para el cifrado, la operación genera el error En esta versión de vCenter Server no se admite el cifrado de discos con nombre.

Solución alternativa: Ninguna.

- **Al utilizar VMware Cloud Director Service Provider Admin Portal con Firefox, no se pueden cargar las pantallas de redes de tenant**

Si utiliza VMware Cloud Director Service Provider Admin Portal con Firefox, es posible que no se carguen las pantallas de redes de tenant (por ejemplo, la pantalla **Administrar firewall** de un centro de datos virtual de organización). Este problema ocurre si el navegador Firefox está configurado para bloquear las cookies de terceros.

Solución alternativa: Configure el navegador Firefox para permitir las cookies de terceros.

- **No se puede consolidar una máquina virtual con aprovisionamiento rápido creada en una matriz de NFS habilitada para VMware vSphere Storage APIs Array Integration (VAAI) o en vSphere Virtual Volumes (VVols)**

No se admite la consolidación local de una máquina virtual con aprovisionamiento rápido cuando se utiliza una snapshot nativa. Tanto los almacenes de datos habilitados para VAAI como las instancias de VVols utilizan siempre snapshots nativos. Cuando se implementa una máquina virtual con aprovisionamiento rápido en uno de estos contenedores de almacenamiento, dicha máquina virtual no puede consolidarse.

Solución alternativa: No habilite el aprovisionamiento rápido de un VDC de organización que utilice una instancia de NFS habilitada para VAAI o VVols. Para consolidar una máquina virtual con una snapshot en un almacén de datos de VVol o VAAI, coloque la máquina virtual en un contenedor de almacenamiento diferente.

- **Después de actualizar desde vCloud Director 10.0, una máquina virtual recién implementada desde una plantilla de Linux con la personalización del sistema operativo invitado habilitada y la conectividad IPv6 experimenta problemas de conectividad de red**

Después de actualizar desde vCloud Director 10.0, si se implementa una nueva máquina virtual mediante una plantilla de máquina virtual de Linux creada en la versión 10.0 con personalización del sistema operativo invitado habilitada y conectividad IPv6, la máquina virtual implementada experimenta problemas de conectividad de red. Esto puede ocurrir porque el proceso de implementación crea entradas duplicadas para los parámetros VM_DOMAIN_NAME y VM_HOST_NAME en el archivo /etc/hosts de la máquina virtual.

Solución alternativa: Elimine las entradas duplicadas VM_DOMAIN_NAME y VM_HOST_NAME del archivo /etc/hosts de la máquina virtual.

- **Cuando se utiliza la API de VMware Cloud Director para crear una máquina virtual a partir de una plantilla y no se especifica una política de almacenamiento predeterminada, si no se ha establecido una configuración de política de**

almacenamiento predeterminada para la plantilla, la máquina virtual recién creada intenta utilizar la política de almacenamiento de la propia plantilla de origen

Cuando se utiliza la API de VMware Cloud Director para crear una máquina virtual a partir de una plantilla y no se especifica una política de almacenamiento predeterminada, si no hay ninguna política de almacenamiento predeterminada establecida para la plantilla, la máquina virtual recién creada intenta utilizar la propia política de almacenamiento de plantilla de origen en lugar de utilizar la política de almacenamiento del VDC de organización en el cual se está implementando.

Solución alternativa: Ninguna.