

Notas de la versión de VMware Cloud Director 10.1

VMware Cloud Director 10.1 | 9 de abril de 2020 | Compilación 15967253 (compilación instalada 15967236)

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

- Para obtener información sobre las funciones nuevas y actualizadas de esta versión, consulte el documento técnico de VMware [Novedades de VMware vCloud Director 10.1](#).
- Se ha modificado el comportamiento en la interfaz de usuario HTML5:

En versiones anteriores de VMware Cloud Director, el menú de acciones de la vApp en la interfaz de usuario HTML se puede utilizar para detener o apagar una vApp. Ambas operaciones de energía anulan la implementación de la vApp, pero afectan a la vApp de manera diferente. En la operación de apagado no se sigue la configuración de Orden de inicio y detención de las máquinas virtuales de la vApp. La operación de apagado también anula la implementación de todas las redes de vApp al desconectar todas las NIC de máquina virtual de las redes de VDC de organización y eliminar las puertas de enlace Edge implementadas para la vApp.

En VMware Cloud Director 10.1, cuando se realiza la operación de apagado en una vApp en ejecución, se apagan todas las máquinas virtuales de la vApp sin anular la implementación de la vApp ni las máquinas virtuales que contiene. Las NIC de las máquinas virtuales siguen conectadas a las redes respectivas y las puertas de enlace Edge de la vApp se mantienen implementadas. La vApp y las máquinas virtuales de la vApp se mantendrán implementadas. La acción de apagado de cada una de las máquinas virtuales de la vApp permanecerá activa y se podrá utilizar para apagar una máquina virtual. Esta acción tiene como resultado la anulación de la implementación de esa máquina virtual.

Cuando se apaga una vApp, la operación de apagado sigue el orden de inicio que se definió en la configuración de Orden de inicio y detención. En consecuencia, las máquinas virtuales se apagarán en orden inverso a cómo se configuró su inicio. La opción Espera de detención no se aplica durante la operación de apagado. Cuando se apaga una vApp, el estado de energía de la vApp, que se deriva de los estados de energía de las máquinas virtuales que contiene, aparece como Apagado.

- El esquema de la API 34.0 de VMware Cloud Director incluye la definición de los atributos `numberOfCpus` y `MemoryAllocationMB`.

Seguridad

- **ADVERTENCIA:** Después de actualizar a la versión 10.1, el software VMware Cloud Director siempre comprobará los certificados de los endpoints de infraestructura que se conecten con él. Esto se debe a un cambio en la manera en la que VMware Cloud Director administra los certificados SSL. Si los certificados no se importan en VMware Cloud Director antes de la actualización, es posible que las conexiones de vCenter Server y NSX muestren errores de conexión causados por problemas de verificación de SSL. En ese caso, tiene dos opciones después de realizar la actualización:
 1. Ejecute el comando `trust-infra-certs` de la herramienta de administración de celdas para conectarse y recuperar de forma automática los certificados de todos los endpoints de infraestructura de las instancias de vCenter Server y NSX Manager en el almacén de certificados centralizado. Consulte [Importar certificados de endpoints a partir de recursos de vSphere](#).
 2. En la interfaz de usuario de Service Provider Admin Portal, seleccione cada instancia de vCenter Server y NSX y vuelva a introducir las credenciales cuando acepte el certificado.
- A partir de la versión 10.1, los tenants y los proveedores de servicios pueden utilizar la API de VMware Cloud Director para probar conexiones con servidores remotos y comprobar la identidad del servidor como parte de un protocolo de enlace SSL. Para proteger las conexiones de red de VMware Cloud Director, configure una lista de hosts internos no permitidos a los que no pueden acceder los tenants que utilizan la API de VMware Cloud Director para las pruebas de conexión. Configure la lista de no permitidos después de instalar o actualizar VMware Cloud Director, y antes de conceder a los tenants acceso a VMware Cloud Director. Consulte [Configurar una lista de no permitidos de conexión de prueba](#).
- VMware Cloud Director 10.1 deja de utilizar el comportamiento por el que se confía en todos los certificados SSL. En esta versión, las conexiones de vCenter Server y NSX no admiten esta opción. Para todas las demás conexiones, también ha quedado obsoleta la confianza en todos los certificados y dejará de admitirse después de VMware Cloud Director 10.1. Los administradores del sistema deben prepararse para esta transición.
 - Si se utiliza LDAP en la organización del sistema de VMware Cloud Director, podrá utilizar el cuadro de diálogo de confianza en el primer uso de la interfaz de usuario o podrá cargar certificados mediante la API.
 - Audite todos los usos de esta opción y proporcione los certificados adecuados mediante la interfaz de usuario o la API.
 - Informe a los tenants de los cambios. Todos los tenants que utilizan un LDAP personalizado en el que se haya habilitado la opción **Aceptar todos los certificados** deben abandonar esta configuración. Los tenants pueden utilizar el cuadro de diálogo de confianza en el primer uso de la interfaz de usuario o pueden cargar certificados a través de la API.

Paquetes de código abierto actualizados

- `jackson-databind` se actualizó a la versión 2.9.10.1.
- `jre` se actualizó a la versión 1.8.0u231.
- `openssl` se actualizó a la versión 1.0.2u.
- `xstream` se actualizó a la versión 1.4.11.1.

Avisos de compatibilidad con el producto

VMware Cloud Director 10.1 no es compatible con vSphere 7.0 ni NSX-T Data Center 3.0. La certificación de interoperabilidad está en curso, y vSphere 7.0 y NSX-T Data Center 3.0 se admitirán en una versión de revisión secundaria de VMware Cloud Director 10.1.

No se admiten las redes externas que están respaldadas mediante puertas de enlace de nivel 0 de VRF-lite en NSX-T Data Center.

Advertencias sobre la finalización de la vida útil y del soporte

- Ya no se admite la base de datos de SQL Server. Solo se admite la base de datos de PostgreSQL.
- Ya no se admite Oracle Linux como sistema operativo del host para instalar la aplicación VMware Cloud Director.
- No se admiten las versiones 20 y anteriores de la API de VMware Cloud Director.
- Las versiones 27.0-29.0 de la API de VMware Cloud Director han quedado obsoletas y no se admitirán después de VMware Cloud Director 10.1
- La versión 30.0 de la API de VMware Cloud Director ha quedado obsoleta.
- La interfaz de usuario basada en Flex se eliminó del producto y ya no se admite.
- El endpoint de inicio de sesión de la API `/api/sessions` ha quedado obsoleto en la versión 33.0 de la API de VMware Cloud Director y en VMware Cloud Director 10.0, y no se admitirá en una versión futura 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, y se eliminará en una versión futura. Debe utilizar `/api/server_status` para los protocolos HTTP y HTTPS.
- 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 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 futuras versiones. 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 futuras 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.

Aviso de próxima finalización del soporte

- La versión 34.0 de la API de VMware Cloud Director (VMware Cloud Director 10.1) contiene algunas API que pronto quedarán obsoletas y que se eliminarán en futuras versiones. Consulte la [Guía de programación de la API de VMware Cloud Director](#).

Actualización de versiones anteriores

Para obtener más información sobre la actualización a VMware Cloud Director 10.1, 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 utiliza VMware Cloud Director 10.1, consulte [Puertos y protocolos de VMware](#).

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

Sistemas operativos de VMware Cloud Director Server compatibles

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

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 RabbitMQ 3.7.9 o 3.8.2.

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

Puede configurar la instalación de VMware Cloud Director para almacenar las métricas que recopila VMware Cloud Director sobre el rendimiento y el uso de recursos de las máquinas virtuales. Los datos de las métricas históricas se almacenan en una base de datos Cassandra. VMware Cloud Director es compatible con las versiones 3.x de Cassandra.

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

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
krb5-libs	libXt	which
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 (deshabilitado de forma predeterminada)
- TLS versión 1.0 (deshabilitado 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 deshabilitados 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
- Microsoft Internet Explorer 11

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

- Al asociar dos sitios de dispositivo de VMware Cloud Director, los objetos no pueden verse en los sitios

Si se establece una asociación de sitios y los sitios cuentan con objetos como organizaciones, VDC de organización, vApps o máquinas virtuales, estos objetos no se pueden ver desde el sitio actual. La interfaz de usuario HTML5 solo muestra los objetos del otro sitio asociado. Este problema se produce durante la comunicación de distribución multisitio porque el archivo `/etc/hosts` del dispositivo de VMware Cloud Director no tiene el contenido correcto.

- **Se produce un error de asignación de memoria al actualizar una política de tamaño de máquinas virtuales**

Si convierte un VDC de grupo de asignación a un VDC de organización de Flex, vCloud Director conserva la información de la política máxima del VDC de grupo de asignación antes de la conversión. Las garantías de reserva de CPU o memoria superiores a las reservas que se definen en el VDC de grupo de asignación generan el error La configuración de la reserva, el límite o los recursos compartidos de la máquina virtual no es válida.

- **Poner la celda principal en modo inactivo o en pausa en un entorno de varias celdas no reinicia las tareas periódicas en la celda secundaria**

En un entorno de varias celdas, al poner la celda principal en modo inactivo o en pausa, las tareas periódicas que se ejecutan en el segundo plano de la celda principal no se inician desde la celda secundaria.

- **Se produce un error en la clonación de una máquina virtual en una política de almacenamiento basada en host con servicios de datos habilitados en una máquina virtual con otra política de almacenamiento basada en host**

Si se crea una máquina virtual que se encuentra en una política de almacenamiento con reglas basadas en host habilitadas (como cifrado de máquinas virtuales o IOPS), se produce un error al intentar clonar la máquina virtual y cambiar la política de almacenamiento de la máquina virtual de destino, y se muestra el mensaje No se permite el cambio ni la aplicación de políticas de almacenamiento de máquina virtual con capacidades de servicio de datos durante las operaciones de clonación. Las políticas de almacenamiento de máquina virtual con capacidades de servicio de datos se pueden asignar a la máquina virtual aprovisionada después de que se complete la operación de clonación y antes de que se encienda la máquina virtual.

- **La función de tenant global Autor de vApp puede cargar y crear plantillas y medios sin tener los derechos necesarios para estas operaciones**

De forma predeterminada, la función de tenant global Autor de vApp cuenta con el derecho Agregar una vApp desde mi nube. Debido a que este derecho y el derecho Plantilla/Medio: Crear/Cargar comparten una sola operación, VMware Cloud Director también concede el derecho Plantilla/Medio: Crear/Cargar a la función Autor de vApp por error.

El problema se solucionó. Si desea que la función Autor de vApp siga teniendo el derecho Plantilla/Medio: Crear/Cargar, un proveedor de servicios puede agregar el derecho a la función global Autor de vApp y publicarla en una organización.

- **Las máquinas virtuales recién creadas se implementan en la política de almacenamiento predeterminada del VDC de organización**

En el portal para tenants de vCloud Director, al crear una nueva máquina virtual independiente, falta la opción para especificar la política de almacenamiento. Como resultado, la máquina virtual creada se implementa con la política de almacenamiento predeterminada del VDC de organización.

Problemas conocidos

- **Nuevo** No se puede abrir una consola web de máquina virtual cuando se utiliza Microsoft Internet Explorer 11

Al usar Microsoft Internet Explorer 11 para conectarse a la consola de una máquina virtual, se abre una ventana vacía en blanco y no se puede acceder a la consola de máquina virtual.

Solución alternativa: Ninguna.

- **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 política 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 política de tamaño de máquinas virtuales con la configuración correcta.
2. Un administrador del sistema debe publicar la nueva política 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 política de tamaño de máquinas virtuales a las máquinas virtuales existentes en el VDC de organización flexible.

- **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 El uso de la API de VMware Cloud Director para consultar una vApp devuelve campos vacíos para los atributos numberOfCpus y MemoryAllocationMB**

Cuando se utiliza la API 33.0 de VMware Cloud Director o una versión anterior para ejecutar una consulta de REST API de vApp, el cuerpo de respuesta de REST API devuelve campos vacíos para los atributos numberOfCpus y MemoryAllocationMB. Esto puede ocurrir porque el esquema de API no incluye la definición de los atributos numberOfCpus y MemoryAllocationMB.

Solución alternativa: Utilice la API 34.0 de VMware Cloud Director para consultar una vApp.

- **Nuevo 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".

Solución alternativa: Utilice la API de la directiva de NSX-T Data Center para actualizar la configuración de redistribución de la red externa a la que está conectada la puerta de enlace NSX-T Edge.

1. Tenga en cuenta el identificador del enrutador de nivel 0 que respalda la red externa a la que está conectada la puerta de enlace NSX-T Edge.
 - Realice una solicitud GET para obtener una lista de los enrutadores de nivel 0 de su entorno.
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s
 - Examine la lista para identificar el nivel 0 por su nombre para mostrar, el cual coincide con el nombre del enrutador de nivel 0 en la pestaña Información general de la red externa en la

interfaz de usuario de VMware Cloud Director.

2. Actualice manualmente la red externa (puerta de enlace de nivel 0).

- Realice una solicitud GET para obtener la lista de localeServices en el enrutador.
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services
La respuesta devuelve un servicio de configuración regional.
- Copie el ID de localeService y realice una solicitud GET para examinarlo.

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

La respuesta devuelve una lista de las propiedades del servicio de configuración regional.

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

- Modifique la respuesta de la siguiente manera.

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

- Realice una solicitud PUT con las propiedades modificadas para actualizar el localeService del enrutador de nivel 0.
- **Nuevo Se produce un error al reubicar una máquina virtual en un clúster diferente si el contenedor de almacenamiento de destino es un clúster de almacenes de datos**

Cuando se realiza una operación que provoca un intento de reubicar una máquina virtual en un clúster diferente y el contenedor de almacenamiento de destino es un clúster de almacenes de datos, se produce un error del tipo NO_FEASIBLE_PLACEMENT_SOLUTION en la migración. En los registros de VMware Cloud Director, aparece un error de invocación de Storage DRS con invalidProperty = spec.host.

Solución alternativa:

1. Use la instancia de vSphere Client para deshabilitar Storage DRS en el clúster de almacenes de datos de destino o utilice la API de VMware Cloud Director para cambiar el almacenamiento de destino para reubicarlo en un almacén de datos.

2. Vuelva a intentar la operación en la que se generó un error.

- **Nuevo** Se produce un error en la implementación del dispositivo de VMware Cloud Director cuando se habilita la opción para que la contraseña raíz caduque después del primer inicio de sesión. Si intenta implementar un dispositivo en el que se habilitó la opción **Caducar la contraseña raíz tras el primer inicio de sesión**, se produce un error en la implementación y el archivo de registro `/opt/vmware/var/log/firstboot` muestra el siguiente error:

[ERROR] postgresauth script failed to execute.

Solución alternativa: Deshabilite la opción **Caducar la contraseña raíz tras el primer inicio de sesión** y especifique una contraseña raíz inicial que contenga al menos ocho caracteres, un carácter en mayúscula, un carácter en minúscula, un número y un carácter especial.

- **Nuevo** Cuando un 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.

- **Nuevo** 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.
- **Nuevo** 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**.
- **Nuevo** 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.

- **Nuevo** En un entorno multisitio mezclado con versiones 10.0 y 10.1 de VMware Cloud Director, la confianza en los certificados para las conexiones de vCenter Server y NSX solo funciona para los objetos del sitio local

Si tiene un entorno multisitio con las versiones 10.0 y 10.1 de VMware Cloud Director asociadas entre sí, cuando inicie sesión en uno de los sitios, no podrá registrar instancias de vCenter Server o NSX Manager en el otro sitio.

Solución alternativa: Inicie sesión en el sitio en el que desea registrar la instancia de vCenter Server o NSX Manager, e inicie el proceso de registro.

- **Nuevo** En el portal para tenants de VMware Cloud Director, no se pueden filtrar las máquinas virtuales por centro de datos desde la opción Filtrado avanzado para máquinas virtuales en la pestaña Aplicaciones

En el portal para tenants de VMware Cloud Director, si se desplaza hasta Máquinas virtuales en la pestaña Aplicaciones de la barra de navegación superior, al filtrar las máquinas virtuales por centro de datos con la opción de filtro avanzado, se produce el error Solicitud incorrecta: Nombre de propiedad desconocida vdcName.

Solución alternativa: En la barra de navegación superior, seleccione **Centros de datos** y elija un centro de datos para ver las máquinas virtuales que contiene.

- **Nuevo** Los servicios de extensión no pueden procesar los mensajes de RabbitMQ provenientes de VMware Cloud Director

Los servicios de extensión que dependen de RabbitMQ no pueden obtener el encabezado `notification.type` de un mensaje debido a que el encabezado tiene un nuevo nombre temporal. El nombre del encabezado para VMware Cloud Director 10.1.0 es `notification.operationType`.

Solución alternativa: Si los servicios de extensión procesan mensajes de RabbitMQ provenientes de VMware Cloud Director y utilizan el encabezado de mensaje `notification.type`, debe cambiarlos. Si el encabezado `notification.type` no está disponible, los servicios de extensión deben obtener el valor del encabezado `notification.operationType`. Este cambio solo es necesario en la versión 10.1.0.

- **En VMware Cloud Director Service Provider Admin Portal, se produce un error al eliminar un centro de datos virtual de organización**

En VMware Cloud Director Service Provider Admin Portal, si agrega una puerta de enlace Edge al VDC de organización y habilita la puerta de enlace para proporcionar enrutamiento distribuido de VMware Cloud Director, se genera un error de forma recursiva al intentar eliminar el VDC de organización y se muestra el mensaje de error No se puede eliminar la red de VDC de organización.

Solución alternativa:

1. A través de la API, elimine las redes de VDC de organización y las puertas de enlace Edge asociadas al VDC de organización.
 2. A través de la API, elimine el VDC de organización.
- **Si deshabilita el acceso de proveedores al endpoint de inicio de sesión de API heredado, todas las integraciones de la API que dependen del inicio de sesión del administrador del sistema dejan de funcionar, lo que incluye vCloud Usage Meter y vCloud Availability for VMware Cloud Director**
A partir de vCloud Director 10.0, puede usar endpoints independientes de inicio de sesión de OpenAPI para VMware Cloud Director a fin de que los tenants y los proveedores de servicios puedan acceder a VMware Cloud Director. Si está deshabilitado el acceso de proveedores de servicios al endpoint `/api/sessions` heredado, los productos que se integran con VMware Cloud Director (como vCloud Usage Meter y vCloud Availability for VMware Cloud Director) dejan de funcionar. Estos productos necesitarán una revisión para seguir funcionando.

Este problema solo afecta a los administradores del sistema. El inicio de sesión de tenants no se ve afectado.

Solución alternativa: Vuelva a habilitar el acceso de proveedores de servicios al endpoint `/api/sessions` heredado mediante la herramienta de administración de celdas.

- **Cuando se cambian los valores de garantía de reserva de un VDC, las máquinas virtuales existentes no se actualizan en consecuencia, incluso después de un reinicio**

Si tiene un VDC de organización de Flex con la política predeterminada del sistema y las máquinas virtuales encendidas en ese VDC tienen la política de tamaño predeterminada, cuando aumente el valor de garantía de recursos del VDC, la reserva de recursos de las máquinas virtuales existentes no se actualizará y estas no se marcarán como no conformes. Ese mismo problema también se produce cuando se convierte un modelo de asignación de VDC heredado en un modelo de asignación de Flex y las máquinas virtuales existentes pasan a ser no conformes con la nueva política predeterminada del VDC de organización de Flex después de la conversión.

Solución alternativa:

1. Para buscar el identificador de máquina virtual, en el portal para tenants de VMware Cloud Director, desplácese hasta la página Detalles de la máquina virtual. La URL muestra el identificador `https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Idenfier/general`
2. Para mostrar las máquinas virtuales no conformes en la interfaz de usuario de VMware Cloud Director, realice una comprobación de conformidad explícita en las máquinas virtuales mediante la API de VMware Cloud Director.
POST: `https://VCD_IP_Address/api/vApp/vm-Idenfier/action/checkComputePolicyCompliance`
3. Para volver a aplicar la política y reconfigurar las reservas de recursos, en el portal para tenants de VMware Cloud Director, haga clic en **Hacer que la máquina virtual sea compatible** para una máquina virtual no conforme.

- **VMware Cloud Director muestra información incorrecta sobre las máquinas virtuales en ejecución, las máquinas virtuales totales, y las estadísticas de memoria y CPU en instancias de vCenter Server dedicadas**

Si la versión de una instancia dedicada de vCenter Server es 6.0 Update 3i o anterior, 6.5 Update 2 o anterior, o 6.7 Update 1 o anterior, VMware Cloud Director muestra información incorrecta sobre las máquinas virtuales en ejecución, las máquinas virtuales totales, y las estadísticas de memoria y CPU en la instancia de vCenter Server. El mosaico de la instancia de vCenter Server dedicada en el portal para tenants y la información de la instancia de vCenter Server dedicada en Service Provider Admin Portal muestran que existen cero máquinas virtuales en ejecución y cero máquinas virtuales totales, incluso cuando hay máquinas virtuales en el entorno de vSphere.

Solución alternativa: Actualice la instancia de vCenter Server a la versión 6.0 Update 3j, 6.5 Update 3, 6.7 Update 2 o posterior.

- **Es posible que se produzca un error al cambiar la política de recursos informáticos de una máquina virtual encendida**

Cuando se intenta cambiar la política de recursos informáticos de una máquina virtual encendida, si la nueva política de recursos informáticos está asociada a una política de recursos informáticos de VDC de proveedor que tiene grupos de máquinas virtuales o grupos de máquinas virtuales lógicas, se produce un error. El mensaje de error contiene: Error de sistema subyacente:

`com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation.`

Solución alternativa: Apague la máquina virtual y vuelva a intentar la operación.

- **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.

- **VMware Cloud Director 10.1 solo admite una lista de parámetros de entrada de flujos de trabajo de vRealize Orchestrator**

VMware Cloud Director 10.1 admite los siguientes parámetros de entrada de flujos de trabajo de vRealize Orchestrator:

- boolean
- sdkObject
- secureString
- number
- mimeAttachment
- properties
- date
- composite
- regex
- encryptedString
- array

Solución alternativa: Ninguna

- **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.

- **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.