

Notas da versão do VMware Cloud Director 10.1

VMware Cloud Director 10.1 | 9 ABR 2020 | Compilação 15967253 (compilação instalada 15967236)

Verifique se há adições e atualizações para estas notas da versão.

Conteúdo deste documento

- [O que há de novo nesta versão](#)
- [Segurança](#)
- [Notas de suporte do produto](#)
- [Atualização das versões anteriores](#)
- [Requisitos do sistema e instalação](#)
- [Problemas resolvidos](#)
- [Problemas conhecidos](#)

O que há de novo nesta versão

- Para obter informações sobre os recursos novos e atualizados nesta versão, consulte o informe técnico da VMware [O que há de novo no VMware vCloud Director 10.1](#).
- Comportamento alterado na interface de usuário do HTML5:
Nas versões anteriores do VMware Cloud Director, você pode usar o menu de ação do vApp na interface de usuário do HTML para parar ou desligar um vApp. Ambas as operações de energia desimplantam o vApp, mas afetam o vApp de maneira diferente. A operação de Desligar não segue as configurações de Ordem para Iniciar e Parar para as máquinas virtuais no vApp. A operação de Desligar também desimplanta quaisquer redes vApp desconectando todos os NICs da VM das redes de VDC da organização e removendo todos os edge gateways implantados para o vApp.

No VMware Cloud Director 10.1, realizar a operação de Desligar em um vApp em execução resulta no desligamento de todas as máquinas virtuais no vApp sem desimplantar o vApp e as máquinas virtuais nela. Os NICs das máquinas virtuais permanecem conectados às respectivas redes, e todos os edge gateways do vApp permanecem implantados. O vApp e as máquinas virtuais no vApp permanecem implantados. A ação de Desligar para cada uma das máquinas virtuais individuais no vApp permanece ativa e você pode usá-la para desligar uma máquina virtual. Essa ação resulta na desimplantação desta máquina virtual.

Quando você desliga um vApp, a operação de Desligar segue a ordem de início que você definiu nas configurações de Ordem para Iniciar e Parar. Como resultado, as máquinas virtuais são desligadas na ordem inversa de como você as configurou para inicialização. A configuração de Parar Espera não é aplicada durante a operação de Desligar. Quando você desliga um vApp, o estado de energia do vApp, que é derivado dos estados de energia das máquinas virtuais nele, é exibido como Desligado.

- O esquema da API do VMware Cloud Director 34.0 inclui a definição dos atributos `numberOfCpus` e `MemoryAllocationMB`.

Segurança

- **AVISO:** Após o upgrade para a versão 10.1, o VMware Cloud Director sempre verificará certificados para todos os endpoints de infraestrutura conectados a ele. Isso ocorre devido a uma alteração na maneira como o VMware Cloud Director gerencia certificados SSL. Se você não importar seus certificados para o VMware Cloud Director antes do upgrade, as conexões do vCenter Server e do NSX poderão apresentar erros de conexão devido a problemas de verificação de SSL. Nesse caso, após o upgrade, você tem duas opções:
 1. Execute o comando `trust-infra-certs` da ferramenta de gerenciamento de célula para se conectar automaticamente e recuperar certificados de todos os endpoints de infraestrutura para instâncias do vCenter Server e NSX Manager no armazenamento centralizado de certificados. Consulte [importar os certificados de Endpoints dos recursos do vSphere](#).
 2. Na interface do usuário do portal de administração do provedor de serviços, selecione cada instância do vCenter Server e do NSX e insira novamente as credenciais ao aceitar o certificado.
- A partir da versão 10.1, os provedores de serviços e tenants podem usar o VMware Cloud Director API para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger as conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos inacessíveis aos tenants que estão usando o VMware Cloud Director API para teste de conexão. Configure a lista de negação após uma instalação ou upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação de conexões de teste](#).
- O VMware Cloud Director 10.1 torna obsoleta a opção de confiar em todos os certificados SSL. Nessa versão, as conexões do vCenter Server e NSX não oferecem suporte a essa opção. Para todas as outras conexões, confiar em todos os certificados também está obsoleto e não será permitido após o VMware Cloud Director 10.1. Os administradores do sistema devem se preparar para essa transição.
 - Se você usar o LDAP para a organização do sistema do VMware Cloud Director, poderá usar a caixa de diálogo de confiança na primeira utilização na interface do usuário ou carregar certificados usando a API.
 - Faça a auditoria de todos os usos dessa opção e forneça os certificados apropriados usando a interface do usuário ou a API.
 - Comunique as alterações aos tenants. Todos os tenants que estão usando LDAP personalizado com a opção **Aceitar todos os certificados** habilitada devem fazer a transição dessa configuração. Os tenants podem usar a caixa de diálogo Confiar no primeiro uso na interface do usuário ou carregar certificados por meio da API.

Pacotes de código aberto atualizados

- Jackson-DataBind atualizado para a versão 2.9.10.1.
- JRE atualizado para a versão 1.8.0u231.
- OpenSSL atualizado para a versão 1.0.2u.
- XStream atualizado para a versão 1.4.11.1.

Notas de suporte do produto

O VMware Cloud Director 10.1 não oferece suporte ao vSphere 7.0 e ao NSX-T Data Center 3.0. A certificação de interoperabilidade está em andamento e o vSphere 7.0 e o NSX-T Data Center 3.0 terão suporte em uma

versão de patch secundária do VMware Cloud Director 10.1.

Não há suporte para as redes externas que são apoiadas por gateways de camada 0 VRF-Lite no NSX-T Data Center.

Avisos de descontinuação e fim de suporte

- Não há mais suporte para o banco de dados do SQL Server. Há suporte somente para o banco de dados PostgreSQL.
- O Oracle Linux não é mais compatível com o sistema operacional do host para instalar o aplicativo VMware Cloud Director.
- Não há suporte para a API versão 20 e anteriores do VMware Cloud Director.
- As versões 27.0 a 29.0 do VMware Cloud Director API estão obsoletas e devem se tornar incompatíveis após o VMware Cloud Director 10.1
- O VMware Cloud Director API versão 30.0 está obsoleto.
- A IU baseada em Flex foi removida do produto e não tem mais suporte.
- O endpoint de login da API `/api/sessions` está obsoleto no VMware Cloud Director API versão 33.0/VMware Cloud Director 10.0 e não terá suporte em uma versão futura do VMware Cloud Director. Você pode usar os endpoints de login do VMware Cloud Director OpenAPI separados para o provedor de serviços e acesso de tenant ao VMware Cloud Director.
- A API `/cloud/server_status` foi substituída por protocolos HTTP e HTTPS e será removida em uma versão futura. Você deve usar a `/api/server_status` para protocolos HTTP e HTTPS.
- As ações de redefinição `/ldap/action/resetLdapCertificate` e `/ldap/action/resetLdapKeyStore` são removidas do VMware Cloud Director API versão 34.0 devido à maneira como o VMware Cloud Director 10.1 armazena e manipula certificados SSL. Você deve usar o endpoint `/cloudapi/1.0.0/ssl/trustedCertificates` para não confiar em certificados.
- As ações de atualização `/ldap/action/updateLdapCertificate` e `/ldap/action/updateLdapKeyStore` foram descontinuadas e não terão suporte em versões futuras. O VMware Cloud Director apresenta um novo endpoint para confiar nos certificados LDAP `/cloudapi/1.0.0/ssl/trustedCertificates`.
- O vSphere substitui o vSphere SSO como um IDP SAML. Todas as implantações do VMware Cloud Director configuradas para usar o vSphere SSO como seu IDP SAML devem migrar para um IDP SAML externo diferente. O uso desse IDP não será permitido nas versões futuras do vSphere e do VMware Cloud Director.
- Os certificados DSA e DSS não têm mais suporte porque não há pacotes de codificação recomendados disponíveis para eles.

Aviso de futuro fim de suporte

- O VMware Cloud Director API 34.0 (VMware Cloud Director 10.1) contém APIs que estão sob descontinuação acelerada e serão removidas em versões futuras. Consulte [Guia de programação do VMware Cloud Director API](#).

Atualização das versões anteriores

Para obter mais informações sobre o upgrade para o VMware Cloud Director 10.1, caminhos e fluxos de trabalho de atualização e migração, consulte [Fazendo upgrade e migrando o VMware Cloud Director Appliance](#) ou [Fazendo upgrade do vCloud Director no Linux](#).

Requisitos do sistema e instalação

Portas e protocolos

Para obter informações sobre as portas de rede e os protocolos usados pelo VMware Cloud Director 10.1, consulte [VMware Ports and Protocols](#).

Matriz de compatibilidade

Consulte as [Matrizes de interoperabilidade dos produtos VMware](#) para obter informações atualizadas sobre:

- Interoperabilidade do VMware Cloud Director com outras plataformas VMware
- Bancos de dados compatíveis com o VMware Cloud Director com suporte

Sistemas operacionais compatíveis com o VMware Cloud Director Server

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

Servidores AMQP compatíveis

O VMware Cloud Director usa o AMQP para fornecer o barramento de mensagem usado por serviços de extensão, extensões de objeto e notificações. Esta versão do VMware Cloud Director requer o RabbitMQ versão 3.7.9 ou 3.8.2

Para obter mais informações, consulte o *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Bancos de dados compatíveis para o armazenamento de dados históricos de métricas

Você pode configurar sua instalação do VMware Cloud Director para armazenar as métricas que o VMware Cloud Director coleta sobre o consumo de recursos e o desempenho da máquina virtual. Dados para métricas de históricos são armazenados em um banco de dados do Cassandra. O VMware Cloud Director é compatível com as versões 3.x do *Cassandra*.

Para obter mais informações, consulte o *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Requisitos de espaço em disco

Cada servidor do VMware Cloud Director requer aproximadamente 2100 MB de espaço livre para a instalação e os arquivos de log.

Requisitos de memória

Consulte o guia de instalação, configuração e upgrade do *VMware Cloud Director* para requisitos de memória

Requisitos de CPU

O VMware Cloud Director é um aplicativo associado à CPU. Siga as diretrizes de comprometimento excessivo da CPU para a versão apropriada do vSphere. Em ambientes virtualizados, independentemente do número de núcleos disponíveis para o VMware Cloud Director, deve haver uma proporção sensível de vCPU para CPU física, que não resulte em comprometimento excessivo.

Pacotes de software Linux necessários

Cada servidor do VMware Cloud Director deve incluir instalações de vários pacotes de software Linux comuns. Normalmente, esses pacotes são instalados por padrão com o software do sistema operacional. Se estiver faltando algum pacote, ocorrerá falha na instalação e será exibida uma mensagem 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	

Além dos pacotes necessários para o instalador, vários procedimentos de configuração de conexões de rede e criação de certificados SSL requerem o uso do comando `nslookup` do Linux, que está disponível no pacote `bind-utils` do Linux.

Servidores LDAP compatíveis

Você pode importar usuários e grupos para o VMware Cloud Director a partir dos serviços LDAP a seguir.

Plataforma	Serviço LDAP	Métodos de autenticação
Windows Server 2012	Active Directory	Simple, Simple SSL
Windows Server 2016	Active Directory	Simple, Simple SSL
Linux	OpenLDAP	Simple, Simple SSL

Protocolos de segurança e pacotes de codificação compatíveis

O VMware Cloud Director requer conexões de cliente para ser seguro. O SSL versão 3 e o TLS versão 1.0 e 1.1 apresentaram vulnerabilidades graves de segurança, por isso não fazem mais parte do conjunto de protocolos padrão oferecido pelo servidor ao fazer uma conexão de cliente. Os administradores do sistema podem habilitar mais protocolos e conjuntos de codificação. Consulte a seção Ferramenta de gerenciamento de células no *Guia de instalação, configuração e upgrade do VMware Cloud Director*. Os seguintes protocolos de segurança são compatíveis:

- TLS versão 1.2
- TLS versão 1.1 (desabilitado por padrão)
- TLS versão 1.0 (desabilitado por padrão)

Pacotes de codificação com suporte habilitados por padrão:

- 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

Os administradores do sistema podem usar a ferramenta de gerenciamento de célula para habilitar explicitamente outros pacotes de codificação com suporte que estejam desativados por padrão.

Observação: A interoperação com versões do vCenter Server anteriores à 5.5-update-3e e com versões do ovftool anteriores à 4.2 requer que o VMware Cloud Director seja compatível com o TLS versão 1.0. Você pode usar a ferramenta de gerenciamento de células para reconfigurar o conjunto de protocolos SSL ou codificações compatíveis. Consulte a seção Ferramenta de gerenciamento de células no *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Navegadores compatíveis

O VMware Cloud Director é compatível com a versão principal anterior e a versão principal atual dos seguintes navegadores:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11

Versões de sistemas operacionais convidados e de hardware virtual compatíveis

O VMware Cloud Director oferece suporte a todas versões de sistemas operacionais convidados e de hardware virtual compatíveis com os hosts ESXi que suportam cada pool de recursos.

VMware Cloud Director WebMKS 2.1.1

O console do VMware Cloud Director WebMKS 2.1.1 adiciona suporte para:

- a tecla PrintScreen no Google Chrome e no Mozilla Firefox para Windows.
- a tecla Windows no Windows e no macOS. Para simular o pressionamento da tecla Windows, pressione Ctrl+Windows no SO Windows ou Ctrl+Command no macOS.
- Detecção automática de layout de teclado no Google Chrome e no Mozilla Firefox.

Problemas resolvidos

- **Ao associar dois sites do dispositivo do VMware Cloud Director, os objetos não estão visíveis entre esses sites**
Se você fizer uma associação de site e seus sites tiverem objetos, como organizações, VDCs de organização, vApps ou VMs, não será possível ver esses objetos do site atual. A IU do HTML 5 exibe

somente os objetos do outro site associado. O problema ocorre durante a comunicação de fan-out entre vários sites porque o arquivo /etc/hosts do dispositivo do VMware Cloud Director não tem o conteúdo correto.

- **Falha ao atualizar uma política de dimensionamento de VM com um erro de alocação de memória**
Se você converter um VDC de pool de alocações em um VDC de organização flexível, o vCloud Director manterá as informações de política máxima do VDC de pool de alocações antes da conversão. Falha das garantias de reserva de memória ou CPU superiores às reservas definidas no VDC do pool de alocação com um erro A reserva de máquina virtual ou as configurações de limite ou compartilhamentos são inválidas.
- **Desativar ou pausar a célula primária em um ambiente de várias células não reinicia as tarefas periódicas na célula secundária**
Em um ambiente de várias células, quando você desativa ou pausa a célula primária, as tarefas periódicas em execução no plano de fundo da célula principal não são iniciadas a partir da célula secundária.
- **A clonagem de uma VM em uma política de armazenamento baseada em host com serviços de dados habilitados para uma VM com uma política de armazenamento baseada em host diferente falha com um erro**
Se você criar uma VM que esteja em uma política de armazenamento que tenha regras baseadas em host, como IOPS ou VM habilitada para criptografia, as tentativas de clonagem da VM e alteração da política de armazenamento de VM de destino falharão com um erro A alteração ou aplicação de políticas de armazenamento de VM com recursos de serviço de dados durante operações de clonagem não é permitida. As políticas de armazenamento de VM com recursos de serviço de dados podem ser atribuídas à VM provisionada após a operação de clonagem ter sido concluída e antes da VM ser ligada.
- **A função de tenant global do vApp Author pode fazer upload e criar modelos e mídia sem ter o direito necessário para essas operações**
A função de tenant global do vApp Author, por padrão, tem o direito Adicionar um vApp da Minha Nuvem. Porque esse direito e o Modelo/Mídia: O direito Criar/Fazer Upload compartilha uma única operação, o VMware Cloud Director concede incorretamente também o Modelo/Mídia: O direito Criar/Carregar para a função do vApp Author.

O problema foi corrigido. Se você deseja que a função do vApp Author continue a ter o Modelo/Mídia: Direito Criar/Fazer Upload, um provedor de serviços pode adicionar o direito à função global do vApp Author e publicá-lo em uma organização.
- **As máquinas virtuais recém-criadas são implantadas na política de armazenamento padrão do VDC de organização**
No portal de tenant do vCloud Director, quando você cria uma nova máquina virtual independente, a opção para especificar a política de armazenamento está ausente. Como resultado, a máquina virtual criada é implantada com a política de armazenamento padrão do VDC de organização.

Problemas conhecidos

- **Novo Não é possível abrir um console web de VM ao usar o Microsoft Internet Explorer 11**
O uso do Microsoft Internet Explorer 11 para se conectar ao console de uma VM abre uma janela em branco, e você não pode acessar o console da VM.

Solução alternativa: Nenhuma.

- **Novo As VMs se tornarão incompatíveis após converter um VDC de pool de reservas em um VDC de organização flexível**

Em um VDC de organização com um modelo de alocação de pool de reservas, se algumas das VMs tiverem reserva diferente de zero para CPU e Memória, configuração não ilimitada para CPU e Memória, ou ambas, após a conversão em um VDC de organização flexível, essas VMs se tornarão incompatíveis. Se você tentar tornar as VMs compatíveis novamente, o sistema aplicará uma política incorreta para a reserva e o limite e definirá as reservas de CPU e Memória como zero e os limites como **ilimitados**.

Solução alternativa:

1. Um administrador do sistema deve criar uma política de dimensionamento de VM com a configuração correta.
 2. Um administrador do sistema deve publicar a nova política de dimensionamento de VM no VDC de organização flexível convertido.
 3. Os tenants podem usar a API do VMware Cloud Director ou o Portal de Tenant do VMware Cloud Director para atribuir a política de dimensionamento de VM às máquinas virtuais existentes no VDC de organização flexível.
- **Novo Na interface de usuário do Portal de Tenant, quando você cria uma regra de afinidade ou antiafinidade, desmarcar a caixa de seleção Obrigatório não afeta a configuração da regra**
Na interface de usuário do Portal de Tenant, quando você cria uma regra de afinidade ou antiafinidade, desmarcar a caixa de seleção Obrigatório não afeta a configuração da regra. As regras de afinidade e antiafinidade são sempre Obrigatórias, o que significa que, se uma regra não puder ser atendida, as VMs adicionadas à regra não serão ligadas.

Solução alternativa: Nenhuma.

- **NOVO Usar a API do VMware Cloud Director para consultar um vApp retorna campos vazios para os atributos numberOfCpus e MemoryAllocationMB**
Quando você usa a API do VMware Cloud Director 33.0 ou uma versão anterior para executar uma consulta de REST API do vApp, o corpo da resposta do REST API retorna campos vazios para os atributos numberOfCpus e MemoryAllocationMB. Isso pode acontecer porque o esquema de API não inclui a definição dos atributos numberOfCpus e MemoryAllocationMB.

Solução alternativa: Use a API do VMware Cloud Director 34.0 para consultar um vApp.

- **Novo Falha na tentativa de adicionar uma regra de NAT a um gateway do NSX-T Edge**
A tentativa de adicionar uma regra de NAT a um gateway do NSX-T Edge falha com o erro "Valores novos e obsoletos foram atualizados juntos para redistribuição, código de erro 503266".

Solução alternativa: Use a API de política do NSX-T Data Center para atualizar a configuração de redistribuição da rede externa à qual o gateway do NSX-T Edge está conectado.

1. Observe o ID do roteador de Camada 0 que serve de suporte para a rede externa à qual seu gateway do NSX-T Edge está conectado.
 - Realize uma solicitação GET para obter uma lista dos roteadores de camada 0 no seu ambiente.
`GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s`
 - Examine a lista para identificar a camada 0 por seu nome para exibição, que corresponde ao nome do roteador de camada 0 na guia Informações gerais da rede externa na UI do VMware Cloud Director.
2. Atualize a rede externa manualmente (gateway de Camada 0).
 - Realize uma solicitação GET para obter a lista de localeServices no roteador.
`GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services`
A resposta retorna um serviço de localidade.

- Copie o ID de localeService e realize uma solicitação GET para examiná-lo.

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

A resposta retorna uma lista das propriedades para o serviço de localidade.

```
{
  "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 a resposta da seguinte maneira.

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

- Realize uma solicitação PUT com as propriedades modificadas para atualizar o localeService do roteador de Camada 0.

- **Novo** A realocação de uma máquina virtual a um cluster diferente falhará se o contêiner de armazenamento de destino for um cluster de armazenamento de dados

Quando você executa uma operação que resulta em uma tentativa de realocar uma máquina virtual a um cluster diferente e o contêiner de armazenamento de destino é um cluster de armazenamento de dados, a migração falha com um erro NO_FEASIBLE_PLACEMENT_SOLUTION. Nos logs do VMware Cloud Director, você vê um erro de invocação do DRS de Armazenamento com invalidProperty = spec.host.

Solução alternativa:

1. Use o vSphere Client para desativar o DRS de Armazenamento no cluster de datastore de destino ou use a API do VMware Cloud Director para alterar o armazenamento de destino para a realocação a um datastore.

2. Tente novamente a operação com falha.

- **Novo** A implantação do dispositivo do VMware Cloud Director falha quando você ativa a configuração para expirar a senha raiz no primeiro login

Se você tentar implantar um dispositivo com a configuração **Expirar Senha Raiz no Primeiro Login** ativada, a implantação falhará e o arquivo de log /opt/vmware/var/log/firstboot exibirá um erro:

[ERRO] falha ao executar o script postgresauth.

Solução alternativa: Desative a configuração **Expirar Senha Raiz no Primeiro Login** e especifique uma senha raiz inicial que contenha pelo menos oito caracteres, um caractere maiúsculo, um caractere minúsculo, um dígito numérico e um caractere especial.

- **Novo Quando um Usuário do vApp tenta criar um vApp a partir de um modelo, isso pode resultar na mensagem "Operação negada"**

Se a função de usuário atribuída for Usuário do vApp, quando você tentar criar um vApp a partir de um modelo e personaliza as políticas de dimensionamento da VM para as máquinas virtuais no vApp, isso resultará na mensagem "Operação negada". Isso acontece porque a função de usuário do vApp permite instanciar vApps a partir de modelos, mas não inclui direitos que permitem personalizar a memória, a CPU ou o disco rígido de uma máquina virtual. Ao alterar a política de dimensionamento, você pode estar alterando a memória ou a CPU da máquina virtual.

Solução alternativa: Nenhuma.

- **Novo O tempo de inatividade do NFS pode causar mau funcionamento das funcionalidades do cluster do dispositivo do VMware Cloud Director**

Se o NFS não estiver disponível devido ao compartilhamento completo do NFS, tornar-se somente leitura e assim por diante, poderá causar um mau funcionamento das funcionalidades do cluster do dispositivo. A IU do HTML5 não responde enquanto o NFS está inativo ou não pode ser acessado. Outras funcionalidades que podem ser afetadas são a exclusão de uma célula primária com falha, a alternância, a promoção de uma célula em espera e assim por diante. Para obter mais informações sobre como configurar corretamente o armazenamento compartilhado do NFS, consulte [Preparando o armazenamento do servidor de transferência para o VMware Cloud Director Appliance](#).

Solução alternativa:

- Corrija o estado do NFS para que ele não seja somente leitura.
- Limpe o compartilhamento do NFS se ele estiver cheio.

- **Novo Confiar em um endpoint ao adicionar o vCenter Server e recursos do NSX em um ambiente de vários sites não adiciona o endpoint à área de armazenamento centralizado de certificados**

Ao usar a interface de usuário do HTML5 em um ambiente de vários sites, se você estiver conectado a um site do vCloud Director 10.0 ou tentando registrar uma instância do vCenter Server em um site do vCloud Director 10.0, o VMware Cloud Director não adicionará o endpoint à área de armazenamento centralizado de certificados.

Solução alternativa:

- Importe o certificado para o site do VMware Cloud Director 10.1 usando a API.
- Para acionar a funcionalidade de gerenciamento de certificados, navegue até o portal de administração do SP do site do VMware Cloud Director 10.1, vá para a caixa de diálogo **Editar** do serviço e clique em **Salvar**.

- **Novo A tentativa de criptografar os discos nomeados no vCenter Server versão 6.5 ou anterior falha com um erro**

Para instâncias do vCenter Server versão 6.5 ou anterior, se você tentar associar discos nomeados novos ou existentes a uma política habilitada para criptografia, a operação falhará com um erro A criptografia de disco nomeada não tem suporte nesta versão do vCenter Server.

Solução alternativa: Nenhuma.

- **Novo Em um ambiente misto multisite com versões as 10.0 e 10.1 do VMware Cloud Director, a confiança dos certificados para conexões do vCenter Server e NSX funciona apenas para os objetos do site local**

Se você tiver um ambiente multisite com as versões 10.0 e 10.1 do VMware Cloud Director associadas entre si, quando fizer login em um dos sites, não será possível registrar as instâncias do vCenter Server ou

NSX Manager no outro site.

Solução alternativa: Faça login no site no qual você deseja registrar a instância do vCenter Server ou NSX Manager e inicie o processo de registro.

- **Novo No Portal de Tenant do VMware Cloud Director, não é possível filtrar VMs por centro de dados da opção de filtragem avançada para máquinas virtuais na guia Aplicativos**

No Portal de Tenant do VMware Cloud Director, quando você navegar para Máquinas Virtuais na guia Aplicativos da barra de navegação superior, filtrar as máquinas virtuais por centro de dados a partir da opção de filtragem avançada resultará em um erro Solicitação Incorreta: Nome de propriedade vdcName desconhecido.

Solução alternativa: Na barra de navegação superior, selecione **Centros de Dados** e selecione um centro de dados para exibir as máquinas virtuais nele.

- **Novo Os serviços de extensão não podem processar mensagens do RabbitMQ do VMware Cloud Director**

Os serviços de extensão que dependem do RabbitMQ não podem obter o cabeçalho `notification.type` de uma mensagem, pois o cabeçalho tem um novo nome temporário. O nome do cabeçalho para o VMware Cloud Director 10.1.0 é `notification.operationType`.

Solução alternativa: Se os serviços de extensão processarem mensagens do RabbitMQ do VMware Cloud Director e usarem o cabeçalho de mensagem `notification.type`, você deverá alterá-los. Se o cabeçalho `notification.type` não estiver disponível, os serviços de extensão deverão obter o valor do cabeçalho `notification.operationType`. Essa alteração só é necessária para a versão 10.1.0.

- **No Portal de Administração do VMware Cloud Director Service Provider, a exclusão de um centro de dados virtual da organização falha com um erro**

No Portal de Administração do VMware Cloud Director Service Provider, se você adicionar um edge gateway ao VDC de organização e ativar o gateway para fornecer o Roteamento Distribuído do VMware Cloud Director, tentar excluir o VDC de organização falhará recursivamente com uma mensagem de erro Não é possível excluir a rede do VDC de Organização.

Solução alternativa:

1. Usando a API, exclua as redes de VDC de organização e os edge gateways associados ao VDC de organização.
 2. Usando a API, exclua o VDC de organização.
- **Se você desativar o acesso do provedor ao endpoint de login da API herdada, todas as integrações da API que dependem do login do administrador do sistema deixarão de funcionar, incluindo o vCloud Usage Meter e o vCloud Availability for VMware Cloud Director**
A partir do vCloud Director 10.0, você pode usar endpoints separados de login de OpenAPI do VMware Cloud Director para o provedor de serviços e o tenant acessarem o VMware Cloud Director. Se o acesso pelo provedor de serviços ao endpoint `/api/sessions` herdado estiver desativado, isso fará com que os produtos que se integram ao VMware Cloud Director, como o vCloud Usage Meter e o vCloud Availability for VMware Cloud Director, parem de funcionar. Esses produtos precisarão de um patch para continuar funcionando.

O problema afeta apenas os administradores do sistema. O login do tenant não é afetado.

Solução alternativa: reative o acesso do provedor de serviços ao endpoint `/api/sessions` herdado usando a ferramenta de gerenciamento de célula.

- **Quando você altera os valores de garantia de reserva de um VDC, as VMs existentes não são atualizadas adequadamente, mesmo após uma reinicialização**

Se você tiver um VDC de organização flexível com a política padrão do sistema e as máquinas virtuais ligadas nesse VDC estiverem com a política de dimensionamento padrão, quando você aumentar o valor da garantia de recurso do VDC, a reserva de recursos para as VMs existentes não será atualizada e elas também não serão marcadas como fora de conformidade. O problema também ocorre quando você converte um modelo de alocação de VDC herdado em um modelo de alocação flexível e as VMs existentes se tornam fora de conformidade com a nova política padrão do VDC de organização flexível após a conversão.

Solução alternativa:

1. Para encontrar o identificador da VM, no Portal de Tenant do VMware Cloud Director, navegue até a página Detalhes da VM. O URL mostra o identificador
`https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifier/general`
2. Para exibir as VMs não compatíveis na interface de usuário do VMware Cloud Director, realize uma verificação de compatibilidade explícita nas VMs usando a API do VMware Cloud Director.
POST: `https://VCD_IP_Address/api/vApp/vm-Identifier/action/checkComputePolicyCompliance`
3. Para reaplicar a política e reconfigurar as reservas de recursos, no Portal do Tenant do VMware Cloud Director, clique em **Tornar a VM Compatível** para uma VM não compatível.

- **O VMware Cloud Director exibe informações incorretas sobre as VMs em execução, VMs totais e estatísticas de memória nas instâncias dedicadas do vCenter Server**

Se uma instância dedicada do vCenter Server tiver a versão 6.0 Update 3i ou anterior, 6.5 Update 2 ou anterior, ou 6.7 Update 1 ou anterior, o VMware Cloud Director exibirá informações incorretas sobre execução de VMs, total de VMs e informações estatísticas de CPU e memória na instância do vCenter Server. O bloco do vCenter Server dedicado no Portal do Tenant e as informações do vCenter Server dedicado no Portal de Administração do Provedor de Serviços exibem zero para as VMs em execução e VMs totais, mesmo quando há máquinas virtuais no ambiente vSphere.

Solução alternativa: Atualize a instância do vCenter Server para a versão 6.0 Update 3J, 6.5 Update 3, 6.7 Update 2 ou posterior.

- **A alteração da política de processamento de uma VM ligada pode falhar**

Ao tentar alterar a política de processamento de uma VM ligada, se a nova política de processamento estiver associada a uma política de processamento de VDC de provedor com Grupos de VM ou Grupos de VMs Lógicas, ocorrerá um erro. A mensagem de erro contém: Erro do sistema subjacente:
`com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation.`

Solução alternativa: Desligue a VM e tente realizar a operação novamente.

- **Ao usar o Portal do Administrador do VMware Cloud Director Service Provider com o Firefox, não é possível carregar as telas do sistema de rede de tenant**

Se você estiver usando o Portal do Administrador do VMware Cloud Director Service Provider com o Firefox, poderá ocorrer falha no carregamento de telas do sistema de rede de tenant, como a tela de **gerenciamento de firewall** para o centro de dados virtuais de uma organização. Esse problema ocorrerá se o navegador Firefox estiver configurado para bloquear cookies de terceiros.

Solução alternativa: Configure o navegador Firefox para permitir cookies de terceiros.

- **O VMware Cloud Director 10.1 oferece suporte a apenas uma lista de parâmetros de entrada de fluxos de trabalho do vRealize Orchestrator**

O VMware Cloud Director 10.1 oferece suporte aos seguintes parâmetros de entrada de fluxos de trabalho do vRealize Orchestrator:

- `boolean`
- `sdkObject`
- `secureString`

- o number
- o mimeTypeAttachment
- o properties
- o date
- o composite
- o regex
- o encryptedString
- o array

Solução alternativa: Nenhuma

- **Não é possível consolidar uma máquina virtual de provisionamento rápido criada em uma matriz NFS ativada pelo VMware vSphere Storage APIs Array Integration (VAAI) ou em vSphere Virtual Volumes (VVols)**

Não há suporte para a consolidação no local de uma máquina virtual de provisionamento rápido quando um snapshot nativo é usado. Snapshots nativos sempre são usados por repositórios de dados ativados via VAAI, bem como por VVols. Quando uma máquina virtual de provisionamento rápido é implantada em um desses contêineres de armazenamento, não é possível consolidar essa máquina virtual.

Solução alternativa: Não ative o provisionamento rápido para o VDC de uma organização que use NFS ativado via VAAI ou VVols. Para consolidar uma máquina virtual com um snapshot em um repositório de dados VAAI ou VVol, realoque a máquina virtual a outro contêiner de armazenamento.

- **Quando você usa a API do VMware Cloud Director para criar uma VM a partir de um modelo e não especifica uma política de armazenamento padrão, se não houver uma política de armazenamento padrão definida para o modelo, a VM recém-criada tentará usar a política de armazenamento do próprio modelo de origem**

Quando você usa a API do VMware Cloud Director para criar uma VM a partir de um modelo e não especifica uma política de armazenamento padrão, se não houver uma política de armazenamento padrão definida para o modelo, a VM recém-criada tentará usar a política de armazenamento do próprio modelo de origem em vez de usar a política de armazenamento do VDC de organização no qual você está implantando.

Solução alternativa: Nenhuma.