

Notas da versão do VMware Cloud Director 10.2

VMware Cloud Director 10.2 | 15 OUT 2020 | Compilação 17029810 (compilação instalada 17008054)

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

O VMware Cloud Director versão 10.2 inclui o seguinte:

- **Paridade Funcional Avançada do NSX-T:** NSX Advanced Load Balancer (Avi), Firewall Distribuído, VRF-lite, Rede entre VDCs, IPv6, Pilha dupla (IPv4/IPv6) na mesma rede, SLAAC, DHCPv6, CVDS (vSphere 7.0/NSX-T 3.0), L2VPN – somente API
- **Suporte para aplicativos modernos no VMware Cloud Director com o Tanzu Runtime vSphere with Kubernetes:** UI de provedor e tenant para gerenciar e consumir clusters Kubernetes
- **Aprimoramentos de dispositivos virtuais do VMware Cloud Director:** validação da entrada do usuário durante a implantação inicial; restauração simplificada de células com a criação simplificada de células em espera
- **Aprimoramentos de armazenamento:** controle de IOPS em nível de disco para provedores e tenants; discos compartilhados
- **Aprimoramentos de segurança:** consulte a seção [Segurança](#)
- **Aprimoramentos de UI:** pesquisa rápida; comunicados; gerenciamento de certificados
- **Aprimoramentos na extensibilidade da plataforma**
- **Aprimoramentos de dimensionamento:** consulte [Máximos de configuração da VMware](#)

Para obter informações sobre os recursos novos e atualizados desta versão, consulte [Novidades no VMware Cloud Director 10.2](#).

Para acessar as notas de versão mais recentes das soluções de complementos do VMware Cloud Director, consulte os seguintes links:

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

Segurança

O dispositivo virtual do VMware Cloud Director 10.2 é fornecido com o Photon OS atualizado até este [Comunicado de segurança Photon](#).

O VMware Cloud Director 10.2 oferece suporte ao armazenamento de chaves PKCS12. Você pode usar um armazenamento de chaves formatado para PKCS12 ao configurar as conexões de rede e banco de dados do VMware Cloud Director ou ao usar a ferramenta de gerenciamento de células para gerar ou substituir certificados. Para obter mais informações, consulte o *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Notas de suporte do produto

Nós do cluster do TKG estão isolados. Entretanto, os serviços que um cluster TKG expõe são acessíveis a qualquer pessoa com acesso à rede ao serviço IP virtual ou endpoint e são protegidos pelos próprios mecanismos de autenticação e autorização dos serviços. Como a autenticação é a única proteção para o acesso seguro às cargas de trabalho, é altamente recomendável permitir apenas o tráfego criptografado, como o TLS, nos serviços de entrada.

Avisos de descontinuação e fim de suporte

- Não há suporte para a API versão 29 e anteriores do VMware Cloud Director.
- As versões 30 e 31 da API do VMware Cloud Director estão obsoletas.
- A versão 30 da API do VMware Cloud Director se tornará indisponível no próximo lançamento.
- O endpoint de login da API `/api/sessions` está obsoleto desde a API versão 33.0 do VMware Cloud Director/VMware Cloud Director 10.0 e deixará de ter suporte em um lançamento futuro 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` está obsoleta para os protocolos HTTP e HTTPS. A remoção de `/cloud/server_status` está planejada para um lançamento futuro do VMware Cloud Director. Você deve usar a `/api/server_status` para protocolos HTTP e HTTPS.
- As ações de redefinição `/amqp/action/resetAmqpCertificate` e `/amqp/action/resetAmqpKeyStore` foram removidas da API do VMware Cloud Director versão 35.0 devido à maneira como o VMware Cloud Director armazena e manipula certificados SSL. Você deve usar o endpoint `/cloudapi/1.0.0/ssl/trustedCertificates` para remover o relacionamento de confiança dos certificados.
- As ações de atualização `/amqp/action/updateAmqpCertificate` e `/amqp/action/updateLdapKeyStore` estão obsoletas. A remoção das ações está planejada para um lançamento futuro do VMware Cloud Director. Você pode usar o novo endpoint para confiar em certificados AMQP `/cloudapi/1.0.0/ssl/trustedCertificates`.
- As ações de redefinição `/ldap/action/resetLdapCertificate` e `/ldap/action/resetLdapKeyStore` foram removidas da API do VMware Cloud Director 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` estão preteridas e devem se perder o suporte em um lançamento futuro. 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 deste IDP deixará de ter suporte nas próximas versões 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.

Atualização das versões anteriores

Para obter mais informações sobre o upgrade para o VMware Cloud Director 10.2, 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 10.2, 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
- NSX Advanced Load Balancer (Avi) - Esta versão do Cloud Director atualmente é compatível apenas com o NSX Advanced Load Balancer (Avi) versão 20.1.1

Sistemas operacionais compatíveis com o VMware Cloud Director Server

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

Implantando o dispositivo VMware Cloud Director

Quando você implementa o dispositivo VMware Cloud Director 10.2 como um modelo OVF usando a VMware OVF Tool, deve incluir o seguinte parâmetro, que é novo para a versão 10.2: `--x:enableHiddenProperties`. Se esse parâmetro não for incluído, a VMware OVF Tool falhará com um erro `Property vcloudapp.nfs_mount.VMware_vCloud_Director is not user configurable..`. Consulte [Implantando o dispositivo VMware Cloud Director com o uso da VMware OVF Tool](#).

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 3.8.x.

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

O VMware Cloud Director é compatível com as versões 3.11.x do *Cassandra*.

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 (desativado por padrão)
- TLS versão 1.0 (desativado 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

Observação: Não há suporte para o Internet Explorer 11 no VMware Cloud Director 10.2 e versões posteriores. Você pode usar o Microsoft Edge ou outro navegador compatível. Se precisar usar o Internet Explorer 11, considere permanecer na versão do VMware Cloud Director 10.0.x ou 10.1.x até poder usar outro navegador.

Versões de sistemas operacionais convidados e de hardware virtual compatíveis

O VMware Cloud Director oferece suporte a todas as 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

- **Falha na tentativa de adicionar uma regra de NAT a um edge gateway do NSX-T**
Falha na tentativa de adicionar uma regra de NAT a um edge gateway do NSX-T com o erro: Valores novos e obsoletos foram atualizados juntos para redistribuição. Código de erro 503266.
- **A movimentação de uma VM entre clusters falhará se o contêiner de armazenamento de destino for um cluster de repositório de dados**
A movimentação de uma VM entre clusters falhará se o contêiner de armazenamento de destino for um cluster de repositório de dados. Os logs mostram o erro a seguir.


```
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 }
```
- **Não será possível implantar o dispositivo se a configuração “Expirar Senha Raiz Após o Primeiro Login” estiver ativada**
Ao tentar implantar um dispositivo, a implantação falha e o seguinte erro é encontrado no log /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.
- **No Portal de Tenant do VMware Cloud Director, a filtragem avançada de VMs com base no local do VDC não funciona**
Na interface de usuário do Portal do Tenant do VMware Cloud Director, se você tentar usar a filtragem avançada com base na
localização do VDC para filtrar as VMs, a pesquisa falhará com um erro.

Problemas conhecidos

- **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** O status do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) é **Ativado**, mesmo depois de desativá-lo durante a instalação do VMware Cloud Director

Durante a instalação do VMware Cloud Director, se você desativar a opção de ingressar no CEIP, após a conclusão da instalação, o status do CEIP ficará ativo.

Solução alternativa: Desative o CEIP seguindo as etapas no procedimento [Entrar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente da VMware](#).

- **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 Após o upgrade para o vCenter Server 7.0 Update 2a ou Update 2b, não é possível criar clusters Tanzu Kubernetes Grid**

Se a versão do vCenter Server subjacente for 7.0 Update 2a ou Update 2b, quando você tentar criar um cluster Tanzu Kubernetes Grid usando o plug-in Kubernetes Container Clusters, a tarefa falhará.

Solução alternativa: Nenhuma.

- **Novo Há uma falha na criação do cluster Tanzu Kubernetes usando o plug-in Kubernetes Container Clusters**

Quando você cria um cluster Tanzu Kubernetes usando o plug-in Kubernetes Container Clusters, é necessário selecionar uma versão do Kubernetes. Algumas das versões no menu suspenso não são compatíveis com a infraestrutura de suporte do vSphere. Quando você seleciona uma versão incompatível, a criação do cluster falha.

Solução alternativa: Exclua o registro de cluster com falha e tente novamente com uma versão compatível do Tanzu Kubernetes. Para obter informações sobre as incompatibilidades entre o Tanzu Kubernetes e o vSphere, consulte [Atualização do ambiente do vSphere with Tanzu](#).

- **Novo Se um pod de armazenamento ou cluster oferecer suporte a uma política de armazenamento, você não poderá ativar a limitação de IOPS do VMware Cloud Director nessa política de armazenamento**

No Portal de Administração do Provedor de Serviços, quando um ou mais pods de armazenamento ou clusters apoiam uma política de armazenamento, mesmo se você desativar o sinalizador **Afetar posicionamento**, não poderá ativar um IOPS do VMware Cloud Director limitando-se a essa política de armazenamento.

Solução alternativa: Você deve ter acesso em nível de administrador para solucionar esse problema.

1. No vCenter Server, remova a tag de política de armazenamento de todos os pods de armazenamento para os quais você deseja ativar o IOPS e atualize as políticas de armazenamento.
2. No VMware Cloud Director, ative a IOPS do VMware Cloud Director na política de armazenamento desativando o sinalizador **Afetar Posicionamento**.
3. No vCenter Server, reanexe a tag aos pods de armazenamento e atualize as políticas de armazenamento.

- **Novo Quando você abre a lista de Máquinas Virtuais em um vApp e ativa a opção Seleção múltipla, o menu de Ações fica indisponível**

Quando você abre a lista de Máquinas Virtuais em um vApp e ativa a opção Seleção múltipla, o menu de Ações fica indisponível. Você pode selecionar várias máquinas virtuais, mas não pode realizar qualquer ação nelas simultaneamente.

Solução alternativa: Nenhuma.

- **Novo Não é possível editar as configurações de NIC de uma máquina virtual independente**

Não é possível atualizar as configurações de NIC de uma máquina virtual autônoma. Quando você clica em Editar para abrir as configurações de NIC da máquina virtual, a página Configurações é aberta, mas fica sem resposta.

Solução alternativa:

1. Converta a máquina virtual autônoma em um vApp
2. Edite as configurações de NIC do vApp.
3. Converta o vApp novamente em uma máquina virtual autônoma.

- **Novo Depois de atualizar as Configurações de Publicação de um catálogo inscrito na UI do Portal de tenants, a sincronização desse catálogo falha com um erro de 401 Não Autorizado**

Depois de atualizar as **Configurações de Publicação** de um catálogo inscrito na UI do Portal de Tenants, a sincronização desse catálogo falha com um erro de 401 Não Autorizado. Isso acontece porque atualizar as configurações do catálogo faz com que a senha existente seja excluída e definida como nula.

Solução alternativa: Atualize as **Configurações de Publicação** do catálogo e defina a senha novamente na UI do Portal de Tenants.

- **Novo O upgrade do VMware Cloud Director para a versão 10.2 a partir da versão 10.1.2 relata incorretamente um erro**
Durante a atualização do VMware Cloud Director para a versão 10.2 a partir da versão 10.1.2, a seguinte mensagem de erro incorreta é exibida:

ERRO: O RPM para outra versão do VMware Cloud Director já está instalado, mas essa versão não é reconhecida, e não há suporte para a atualização dessa versão. Esse upgrade não é esperado com sucesso, mas você pode prosseguir mesmo assim por sua conta e risco.

O upgrade do VMware Cloud Director para a versão 10.2 a partir da versão 10.1.2 tem suporte, e você deve ignorar a mensagem de erro.

Solução alternativa: Ignore o erro.

- **Ao reinicializar o dispositivo do VMware Cloud Director, a API de serviços ou a UI de gerenciamento do dispositivo pode relatar que o serviço vmware-vcd está em estado de falha**

Ao reinicializar o dispositivo do VMware Cloud Director, a API de serviços ou a UI de gerenciamento do dispositivo pode relatar incorretamente que o serviço vmware-vcd está em estado de falha. Isso acontece quando o serviço vmware-vcd tenta ser iniciado antes que a pilha de rede do sistema operacional fique disponível. Como resultado, o serviço entra em estado de falha e você vê uma mensagem de erro indicando que o serviço não pôde se associar a uma ou mais portas. Posteriormente, vcd-watchdog iniciará o serviço vmware-vcd com êxito, mas o status do serviço systemd não refletirá isso.

Solução alternativa:

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

- **Se tiver quaisquer catálogos inscritos na sua organização, ao atualizar o VMware Cloud Director, a sincronização dos catálogos falhará**

Após a atualização, se você tiver assinado catálogos na sua organização, o VMware Cloud Director não confiará nos certificados de endpoint publicados automaticamente. Sem confiar nos certificados, a biblioteca de conteúdo não é sincronizada.

Solução alternativa: Confie manualmente nos certificados para cada assinatura de catálogo. Quando você edita as configurações de assinatura de catálogo, uma caixa de diálogo confiança na primeira utilização (TOFU) solicita que você confie no certificado de catálogo remoto.

Se você não tiver os direitos necessários para confiar no certificado, entre em contato com o administrador da organização.

- **Após o upgrade do VMware Cloud Director e a ativação da criação de clusters Tanzu Kubernetes, nenhuma política gerada automaticamente está disponível, e você não pode criar ou publicar uma política**

Quando você faz upgrade do VMware Cloud Director para a versão 10.2 e do vCenter Server para a versão 7.0.0d e cria um VDC de provedor com o suporte de um Cluster Supervisor, o VMware Cloud Director exibe um ícone do Kubernetes ao lado do VDC. No entanto, não há uma política do Kubernetes gerada automaticamente no novo VDC de provedor. Quando você tenta criar ou publicar uma política do Kubernetes em um VDC de organização, nenhuma classe de máquina está disponível.

Solução alternativa: Confie manualmente no certificado do endpoint do Kubernetes. Para conhecer as etapas detalhadas, consulte <https://kb.vmware.com/s/article/80996>.

- **O plug-in Setup DRaaS and Migration aparece duas vezes na barra de navegação superior da UI do VMware Cloud Director**

O problema ocorre devido à redefinição da marca do vCloud Availability 4.0.0 para o VMware Cloud Director Availability 4.0.0, após a qual existem dois plug-ins. O VMware Cloud Director não desativa o plug-in do vCloud Availability 4.0.0 automaticamente. A versão antiga e a nova aparecem como o plug-in Setup DRaaS and Migration na barra de navegação superior, em **Mais**.

Solução alternativa: Desative manualmente o plug-in do vCloud Availability 4.0.0.

- **Não será possível publicar uma política do Kubernetes do VDC de provedor em um VDC se o cluster do supervisor ao qual ela aponta não for o cluster primário no VDC de provedor**

Se você tiver um VDC de provedor com vários clusters de supervisor, a publicação de uma política do Kubernetes de VDC de provedor que aponta para um cluster de supervisor não primário falhará com um erro de `LMException`.

Solução alternativa: Certifique-se de que o VDC de provedor tenha o apoio de apenas um cluster de supervisor e que o cluster seja o cluster primário. Um VDC de provedor pode ser compatível com clusters de host e um cluster de supervisor, mas o cluster de supervisor deve ser o principal.

- **Inserir um nome de cluster Kubernetes com caracteres não latinos desativa o botão Avançar no assistente para Criar Novo Cluster**

O plug-in Kubernetes Container Clusters é compatível apenas com caracteres latinos. Se você inserir caracteres não latinos, o seguinte erro será exibido. O nome deve começar com uma letra e conter apenas caracteres alfanuméricos ou hífen (-). (No máximo 128 caracteres).

Solução alternativa: Nenhuma.

- **No plug-in Kubernetes Container Clusters, grades de dados podem aparecer vazias durante o carregamento**

No plug-in Kubernetes Container Clusters, algumas grades de dados aparecem vazias durante o carregamento porque o controle giratório de carga não é exibido.

Solução alternativa: Nenhuma.

- **Após o redimensionamento de um cluster TKGI, alguns valores na grade de dados aparecem como em branco ou não aplicáveis**

Quando você redimensiona um cluster VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), os valores de cluster para a organização e o VDC na exibição da grade de dados parecem estar em branco ou não aplicáveis.

Solução alternativa: Nenhuma.

- **Ao filtrar uma grade de várias seleções, navegar para outra página faz com que os itens filtrados desapareçam**

Em grades de várias seleções, se você filtrar os resultados e mais de uma página estiver disponível, as páginas seguintes dos resultados filtrados aparecerão vazias. O problema ocorre nas caixas de diálogo em que você pode selecionar vários itens de uma lista e filtrá-los, por exemplo, adicionando políticas de armazenamento a um VDC de organização ou compartilhando um vApp ou uma VM com usuários ou grupos.

Solução alternativa: Redimensione qualquer uma das colunas da grade.

- **A filtragem de comunicados por prioridade resulta em um erro interno do servidor**

Quando você usa a API do VMware Cloud Director, a aplicação de um filtro de prioridade a um comunicado falha com um erro.

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

Solução alternativa: Obter todos os comunicados e filtre-os manualmente.

- **A documentação da API fornece uma descrição incorreta da ordem de classificação de prioridades do comunicado**

O objeto de modelo de Comunicado contém um campo de prioridade para especificar a urgência de cada comunicado que você cria. A documentação da API de Comunicado informa incorretamente que as prioridades estão listadas em ordem de classificação decrescente. A documentação da API do VMware Cloud Director lista as prioridades para um comunicado em ordem de classificação crescente.

Solução alternativa: Nenhuma.

- **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 personalizar 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.

- **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.
- **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**.
- **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.

- **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.

- **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.

- **Após o upgrade do vCloud Director 10.0, uma VM recém-implantada de um modelo Linux com personalização de SO convidado e conectividade IPv6 ativada passa por problemas de conectividade de rede**

Após o upgrade do vCloud Director 10.0, se você implantar uma nova VM usando um modelo de VM Linux criado na versão 10.0 com personalização de SO convidado e conectividade IPv6 ativadas, a VM implantada apresentará problemas de conectividade de rede. Isso pode acontecer porque o processo de implantação cria entradas duplicadas para os parâmetros VM_DOMAIN_NAME e VM_HOST_NAME no arquivo /etc/hosts da VM.

Solução alternativa: Remova as entradas duplicadas de VM_DOMAIN_NAME e VM_HOST_NAME do arquivo /etc/hosts da VM.

- **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.