

Notes de mise à jour de VMware Cloud Director 10.2

VMware Cloud Director 10.2 | 15 octobre 2020 | Build 17029810 (build installé 17008054)

Recherchez les ajouts et les mises à jour de ces notes.

Contenu de ce document

- [Nouveautés de cette version](#)
- [Sécurité](#)
- [Remarques relatives à la prise en charge du produit](#)
- [Mise à niveau à partir des versions précédentes](#)
- [Configuration système requise et installation](#)
- [Problèmes résolus](#)
- [Problèmes connus](#)

Nouveautés de cette version

VMware Cloud Director version 10.2 inclut les éléments suivants :

- **Parité fonctionnelle avancée NSX-T** : NSX Advanced Load Balancer (Avi), pare-feu distribué, VRF-Lite, mise en réseau inter-VDC, IPv6, double pile (IPv4/IPv6) sur le même réseau, SLAAC, DHCPv6, CVDS (vSphere 7.0/NSX-T 3.0), L2VPN – API uniquement
- **Prise en charge des applications modernes dans VMware Cloud Director avec vSphere with Kubernetes dans un environnement d'exécution Tanzu** : interface utilisateur du fournisseur et du locataire pour la gestion et l'utilisation des clusters Kubernetes
- **Améliorations apportées au dispositif virtuel VMware Cloud Director** : validation des entrées utilisateur lors du déploiement initial ; restauration de cellules simplifiée avec création de cellules en veille rationalisée
- **Améliorations du stockage** : contrôle d'IOPS au niveau du disque pour les fournisseurs et les locataires ; disques partagés
- **Améliorations de la sécurité** : reportez-vous à la section [Sécurité](#)
- **Améliorations de l'interface utilisateur** : recherche rapide, avis, gestion des certificats
- **Améliorations de l'extensibilité de la plate-forme**
- **Améliorations de l'échelle** : reportez-vous à la section [Valeurs maximales de configuration VMware](#)

Pour plus d'informations sur les fonctionnalités nouvelles et mises à jour de cette version, reportez-vous à la section [Nouveautés de VMware Cloud Director 10.2](#).

Pour les dernières notes de mise à jour des solutions de modules complémentaires VMware Cloud Director, reportez-vous aux liens suivants :

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

Sécurité

Le dispositif virtuel VMware Cloud Director 10.2 est fourni avec Photon OS mis à jour à la version décrite dans la page [Photon Security Advisory](#).

VMware Cloud Director 10.2 prend en charge les keystores PKCS12. Vous pouvez utiliser un keystore formaté au format PKCS12 lorsque vous configurez les connexions au réseau et à la base de données de VMware Cloud Director, ou lorsque vous utilisez l'outil de gestion des cellules pour générer ou remplacer des certificats. Pour plus d'informations, reportez-vous au *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*.

Remarques relatives à la prise en charge du produit

Les nœuds de cluster TKG sont isolés. Cependant, les services exposés par un cluster TKG sont accessibles aux utilisateurs disposant d'un accès réseau à l'adresse IP virtuelle ou au point de terminaison du service, et sont protégés par leurs propres mécanismes d'authentification et d'autorisation. Étant donné que l'authentification est la seule protection pour sécuriser l'accès aux charges de travail, il est vivement recommandé d'autoriser uniquement le trafic chiffré, tel que TLS, sur les services d'entrée.

Avertissements relatifs à la fin de vie et à la fin de prise en charge

- Les versions 29 et antérieures de VMware Cloud Director API ne sont pas prises en charge.
- Les versions 30 et 31 de VMware Cloud Director API sont déconseillées.
- VMware Cloud Director API version 30 deviendra indisponible dans les versions ultérieures.
- Le point de terminaison de connexion de l'API `/api/sessions` est déconseillé depuis VMware Cloud Director API version 33.0/VMware Cloud Director 10.0 et ne sera plus pris en charge dans une future version de VMware Cloud Director. Vous pouvez utiliser les points de terminaison de connexion VMware Cloud Director OpenAPI distincts pour l'accès du fournisseur de services et du locataire à VMware Cloud Director.
- L'API `/cloud/server_status` est déconseillée pour les protocoles HTTP et HTTPS. La suppression de `/cloud/server_status` interviendra dans une future version de VMware Cloud Director. Vous devez utiliser `/api/server_status` pour les protocoles HTTP et HTTPS.
- Les actions de réinitialisation `/amqp/action/resetAmqpCertificate` et `/amqp/action/resetAmqpKeyStore` ont été supprimées de VMware Cloud Director API version 35.0 en raison de la manière dont VMware Cloud Director stocke et gère les certificats SSL. Vous devez utiliser le point de terminaison `/cloudapi/1.0.0/ssl/trustedCertificates` pour désapprouver les certificats.
- Les actions de mise à jour `/amqp/action/updateAmqpCertificate` et `/amqp/action/updateLdapKeyStore` sont déconseillées. La suppression des actions est prévue dans une future version de VMware Cloud Director. Vous pouvez utiliser le nouveau point de terminaison pour l'approbation des certificats AMQP `/cloudapi/1.0.0/ssl/trustedCertificates`.
- Les actions de réinitialisation `/ldap/action/resetLdapCertificate` et `/ldap/action/resetLdapKeyStore` ont été supprimées depuis VMware Cloud Director API version 34.0 en raison de la manière dont VMware Cloud Director 10.1 stocke et gère les certificats SSL. Vous devez utiliser le point de terminaison `/cloudapi/1.0.0/ssl/trustedCertificates` pour désapprouver les certificats.
- Les actions de mise à jour `/ldap/action/updateLdapCertificate` et `/ldap/action/updateLdapKeyStore` sont déconseillées et ne seront plus prises en charge dans une future version. VMware Cloud Director introduit un nouveau point de terminaison pour l'approbation des certificats LDAP `/cloudapi/1.0.0/ssl/trustedCertificates`.
- vSphere déconseille vSphere SSO en tant que fournisseur d'identité SAML. Tous les déploiements VMware Cloud Director configurés pour utiliser vSphere SSO en tant que fournisseur d'identité SAML doivent migrer vers un autre fournisseur d'identité SAML externe. L'utilisation de ce fournisseur d'identité (IDP) ne sera plus prise en charge dans les futures versions de vSphere et de VMware Cloud Director.
- Les certificats DSA et DSS ne sont plus pris en charge, car ils ne disposent d'aucune suite de chiffrement recommandée.

Mise à niveau à partir des versions précédentes

Pour plus d'informations sur la mise à niveau vers VMware Cloud Director 10.2, les chemins et les workflows de mise à niveau et de migration, reportez-vous à [Mise à niveau et migration du dispositif VMware Cloud Director](#) ou [Mise à niveau de vCloud Director sur Linux](#).

Configuration requise et installation

Ports et protocoles

Pour plus d'informations sur les ports et protocoles réseau utilisés par VMware Cloud Director 10.2, consultez la page [VMware Ports and Protocols](#).

Matrice de compatibilité

Consultez les [Matrices d'interopérabilité des produits VMware](#) pour obtenir les informations les plus récentes :

- Interopérabilité de VMware Cloud Director avec d'autres plates-formes VMware.
- Bases de données VMware Cloud Director prises en charge
- NSX Advanced Load Balancer (Avi) : cette version de Cloud Director ne prend actuellement en charge que NSX Advanced Load Balancer (Avi) version 20.1.1

Systèmes d'exploitation des serveurs VMware Cloud Director pris en charge

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

Déploiement du dispositif VMware Cloud Director

Lorsque vous déployez le dispositif VMware Cloud Director 10.2 en tant que modèle OVF à l'aide de l'outil VMware OVF Tool, vous devez inclure le paramètre suivant, qui est nouveau pour la version 10.2 : `--x:enableHiddenProperties`. Si vous n'incluez pas ce paramètre, l'outil VMware OVF Tool échoue avec l'erreur La propriété `vcloudapp.nfs_mount.VMware_vCloud_Director` ne peut pas être configurée par l'utilisateur.

Consultez [Déploiement du dispositif VMware Cloud Director à l'aide de l'outil VMware OVF Tool](#).

Serveurs AMQP pris en charge

VMware Cloud Director utilise AMQP pour fournir le bus de message utilisé par les services d'extension, les extensions d'objet et les notifications. Cette version de VMware Cloud Director nécessite RabbitMQ version 3.8.x.

Pour plus d'informations, consultez le *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*.

Bases de données prises en charge pour le stockage des données des mesures historiques

VMware Cloud Director prend en charge Apache Cassandra versions 3.11.x.

Espace disque requis

Chaque serveur VMware Cloud Director requiert environ 2 100 Mo d'espace disque libre destiné aux fichiers d'installation et aux journaux.

Mémoire requise

Pour en savoir plus sur les exigences de mémoire, consultez le *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*.

Configuration requise du CPU

VMware Cloud Director est une application dédiée au CPU. Les directives de surcharge du CPU doivent être respectées pour la version appropriée de vSphere. Dans les environnements virtualisés, quel que soit le nombre de cœurs disponibles pour VMware Cloud Director, vous devez disposer d'un rapport cohérent entre vCPU et CPU physique, qui ne produit pas de surcharge extrême.

Packages logiciels Linux requis

Chaque serveur VMware Cloud Director doit inclure des installations de plusieurs modules logiciels Linux communs. Ces packages sont généralement installés par défaut avec le logiciel du système d'exploitation. En cas de modules manquants, le programme d'installation échoue et affiche un message de diagnostic.

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	

En plus des modules requis par le programme d'installation, plusieurs procédures de configuration des connexions réseau et de création de certificats SSL nécessitent l'utilisation de la commande Linux `nslookup`, disponible dans le module Linux `bind-utils`.

Serveurs LDAP pris en charge

Vous pouvez importer des utilisateurs et des groupes vers VMware Cloud Director à partir des services LDAP suivants.

Plate-forme	Service LDAP	Méthodes d'authentification
Windows Server 2012	Active Directory	Simple, SSL simple
Windows Server 2016	Active Directory	Simple, SSL simple
Linux	OpenLDAP	Simple, SSL simple

Protocoles de sécurité et suites de chiffrement pris en charge

VMware Cloud Director nécessite des connexions clientes sécurisées. SSL version 3 et TLS version 1.0 et 1.1 présentent de graves failles de sécurité et ne sont plus inclus dans l'ensemble de protocoles par défaut que le serveur met à disposition lors d'une connexion client. Les administrateurs système peuvent activer un plus grand nombre de protocoles et de suites de chiffrement. Reportez-vous à la section sur les outils de gestion des cellules du *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*. Les protocoles de sécurité suivants sont pris en charge :

- TLS version 1.2
- TLS version 1.1 (désactivé par défaut)
- TLS version 1.0 (désactivé par défaut)

Suites de chiffrement prises en charge activées par défaut :

- 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

Les administrateurs système peuvent utiliser l'outil de gestion des cellules pour activer explicitement les autres suites de chiffrement prises en charge qui sont désactivées par défaut.

Remarque : l'interopérabilité entre les versions de vCenter Server antérieures à la version 5.5-update-3e et les versions d'ovftool antérieures à la version 4.2 impose que VMware Cloud Director prenne en charge la version 1.0 de TLS. Vous pouvez utiliser l'outil de gestion des cellules pour reconfigurer l'ensemble de protocoles SSL ou de chiffrements pris en charge. Reportez-vous à la section sur les outils de gestion des cellules du *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*.

Navigateurs pris en charge

VMware Cloud Director est compatible avec la version majeure actuelle et la version majeure précédente des navigateurs suivants :

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Remarque : Internet Explorer 11 n'est pas pris en charge dans VMware Cloud Director 10.2 et versions ultérieures. Vous pouvez utiliser Microsoft Edge ou un autre navigateur pris en charge. Si vous devez utiliser Internet Explorer 11, pensez à rester sur VMware

Cloud Director version 10.0.x ou 10.1.x jusqu'à ce que vous puissiez utiliser un autre navigateur.

Systèmes d'exploitation invités et versions de matériel virtuel pris en charge

VMware Cloud Director prend en charge tous les systèmes d'exploitation invités et versions de matériel virtuel pris en charge par les hôtes ESXi sur lesquels repose chaque pool de ressources.

VMware Cloud Director WebMKS 2.1.1

La console VMware Cloud Director WebMKS 2.1.1 ajoute la prise en charge de :

- la touche Impr écran dans Google Chrome et dans Mozilla Firefox pour Windows ;
- la touche Windows dans Windows et macOS. Pour simuler un appui sur la touche Windows, appuyez sur CTRL+Windows dans le système d'exploitation Windows ou sur CTRL+Commande dans macOS.
- Détection automatique de la disposition du clavier dans Google Chrome et Mozilla Firefox.

Problèmes résolus

- **Toute tentative d'ajout d'une règle NAT à une passerelle Edge NSX-T échoue**
Toute tentative d'ajout d'une règle NAT à une passerelle Edge NSX-T échoue avec l'erreur : Les valeurs nouvelles et désapprouvées ont été mises à jour pour la redistribution. Code d'erreur 503266.
- **Le déplacement d'une machine virtuelle entre des clusters échoue si le conteneur de stockage cible est un cluster de banques de données**
Le déplacement d'une machine virtuelle entre des clusters échoue si le conteneur de stockage cible est un cluster de banques de données. Les journaux affichent l'erreur suivante.

```
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 }
```

- **Impossible de déployer le dispositif si le paramètre « Expiration du mot de passe racine lors de la première connexion » est activé**
Lors d'une tentative de déploiement d'un dispositif, le déploiement échoue et le journal /opt/vmware/var/log/firstboot contient l'erreur suivante :
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.
- **Dans le portail de locataires VMware Cloud Director, le filtrage avancé des machines virtuelles en fonction de l'emplacement du VDC ne fonctionne pas**
Dans l'interface utilisateur du portail de locataires de VMware Cloud Director, si vous tentez d'utiliser un filtrage avancé basé sur l'emplacement du VDC pour filtrer les machines virtuelles, la recherche échoue avec une erreur.

Problèmes connus

- **Nouveau** Les machines virtuelles deviennent non conformes après la conversion d'un VDC de pool de réservation en VDC d'organisation Flex.
Dans un VDC d'organisation avec un modèle d'allocation de pool de réservation, si certaines machines virtuelles ont une réservation non nulle pour le CPU et la mémoire, une configuration non illimitée pour le CPU et la mémoire, ou les deux, après la conversion en VDC d'organisation Flex, ces machines virtuelles deviennent non conformes. Si vous tentez de rendre les machines virtuelles à nouveau conformes, le système applique une stratégie incorrecte pour la réservation et la limite, puis définit les réservations de CPU et de mémoire sur zéro et les limites sur **Illimité**.

Solution :

1. Un administrateur système doit créer une stratégie de dimensionnement de machine virtuelle avec la configuration appropriée.
2. Un administrateur système doit publier la nouvelle stratégie de dimensionnement de machine virtuelle dans le VDC d'organisation Flex converti.
3. Les locataires peuvent utiliser VMware Cloud Director API ou le portail de locataires de VMware Cloud Director pour attribuer la stratégie de dimensionnement de machine virtuelle aux machines virtuelles existantes dans le VDC d'organisation Flex.

- **Nouveau** L'état du programme d'amélioration du produit (CEIP) est **Activé** même après sa désactivation lors de l'installation de VMware Cloud Director

Pendant l'installation de VMware Cloud Director, si vous désactivez l'option visant à rejoindre le CEIP, une fois l'installation terminée, l'état du CEIP est actif.

Solution : désactivez le CEIP en suivant les étapes de la procédure [Rejoindre ou quitter le programme d'amélioration du produit VMware](#).

- **Nouveau** Dans l'interface utilisateur du portail de locataires, lorsque vous créez une règle d'affinité ou d'anti-affinité, décocher la case **Requis n'affecte pas la configuration de la règle**

Dans l'interface utilisateur du portail de locataires, lorsque vous créez une règle d'affinité ou d'anti-affinité, la désélection de la case Requis n'affecte pas la configuration de la règle. Les règles d'affinité et d'anti-affinité sont toujours requises, ce qui signifie que si les conditions d'une règle ne peuvent pas être satisfaites, les machines virtuelles ajoutées à la règle ne sont pas mises sous tension.

Solution : aucune.

- **Nouveau** Après la mise à niveau vers vCenter Server 7.0 Update 2a ou Update 2b, vous ne pouvez pas créer de clusters Tanzu Kubernetes Grid.

Si la version de vCenter Server sous-jacente est la version 7.0 Update 2a ou Update 2b, lorsque vous tentez de créer un cluster Tanzu Kubernetes Grid à l'aide du plug-in Clusters de conteneurs Kubernetes, la tâche échoue.

Solution : aucune.

- **Nouveau** Échec de la création d'un cluster Tanzu Kubernetes à l'aide du plug-in Clusters de conteneurs Kubernetes
Lorsque vous créez un cluster Tanzu Kubernetes à l'aide du plug-in Clusters de conteneurs Kubernetes, vous devez sélectionner une version de Kubernetes. Certaines versions du menu déroulant ne sont pas compatibles avec l'infrastructure vSphere de soutien. Lorsque vous sélectionnez une version non compatible, la création du cluster échoue.

Solution : supprimez l'enregistrement de cluster ayant échoué et réessayez avec une version compatible de Tanzu Kubernetes. Pour plus d'informations sur les incompatibilités entre Tanzu Kubernetes et vSphere, reportez-vous à la section [Mise jour de l'environnement vSphere with Tanzu](#).

- **Nouveau** Si une stratégie de stockage repose sur un espace de stockage ou un cluster, vous ne pouvez pas activer la limitation des IOPS de VMware Cloud Director sur celle-ci

Dans le portail d'administration des fournisseurs de services, lorsqu'une stratégie de stockage dépend d'un ou plusieurs espaces de stockage ou clusters, même si vous désactivez l'indicateur **Affecter le positionnement**, vous ne pouvez pas activer la limite des IOPS de VMware Cloud Director sur cette stratégie de stockage.

Solution : vous devez disposer d'un accès de niveau administrateur pour résoudre ce problème.

1. Dans vCenter Server, supprimez la balise de stratégie de stockage de tous les espaces de stockage pour lesquels vous souhaitez activer les IOPS et actualisez les stratégies de stockage.
2. Dans VMware Cloud Director, activez les IOPS de VMware Cloud Director dans la stratégie de stockage en désactivant l'indicateur **Affecter le positionnement**.
3. Dans vCenter Server, rattachez la balise aux espaces de stockage et actualisez les stratégies de stockage.

- **Nouveau** Lorsque vous ouvrez la liste des machines virtuelles dans un vApp et que vous activez l'option **Sélections multiples**, le menu **Actions** devient indisponible

Lorsque vous ouvrez la liste des machines virtuelles dans un vApp et que vous activez l'option **Sélections multiples**, le menu **Actions** devient indisponible. Vous pouvez sélectionner plusieurs machines virtuelles, mais vous ne pouvez effectuer aucune action simultanément sur celles-ci.

Solution : aucune.

- **Nouveau** Vous ne pouvez pas modifier les paramètres de carte réseau d'une machine virtuelle autonome

Vous ne pouvez pas mettre à jour les paramètres de carte réseau d'une machine virtuelle autonome. Lorsque vous cliquez sur Modifier pour ouvrir les paramètres de carte réseau de la machine virtuelle, la page Paramètres s'ouvre, mais cesse de répondre.

Solution :

1. Convertissez la machine virtuelle autonome en vApp.
 2. Modifiez les propriétés de carte réseau du vApp.
 3. Convertissez de nouveau le vApp en une machine virtuelle autonome.
- **Nouveau** Après la mise à jour des paramètres de publication d'un catalogue abonné à partir de l'interface utilisateur du portail de locataires, la synchronisation de ce catalogue échoue avec une erreur 401 Non autorisé

Après la mise à jour des Paramètres de publication d'un catalogue abonné à partir de l'interface utilisateur du portail de locataires, la synchronisation de ce catalogue échoue avec une erreur 401 Non autorisé. Cette erreur se produit, car la mise à jour des paramètres du catalogue entraîne la suppression du mot de passe existant et sa définition sur NULL.

Solution : mettez à jour les Paramètres de publication du catalogue et redéfinissez le mot de passe dans l'interface utilisateur du portail de locataires.

- **Nouveau** La mise à niveau de VMware Cloud Director vers la version 10.2 depuis la version 10.1.2 signale de manière incorrecte une erreur
Lors de la mise à niveau de VMware Cloud Director vers la version 10.2 depuis la version 10.1.2, le message d'erreur incorrect suivant s'affiche :

ERREUR : le RPM d'une autre version de VMware Cloud Director est déjà installé, mais cette version n'est pas reconnue et la mise à niveau à partir de cette version n'est pas prise en charge. Cette mise à niveau n'est pas censée réussir, mais vous pouvez continuer malgré tout à vos propres risques.

La mise à niveau de VMware Cloud Director vers la version 10.2 depuis la version 10.1.2 est prise en charge et vous devez ignorer le message d'erreur.

Solution : ignorez l'erreur.

- **Lorsque vous redémarrez le dispositif VMware Cloud Director, l'API de services ou l'interface utilisateur de gestion du dispositif peut signaler que le service vmware-vcd est dans un état d'échec.**
Lorsque vous redémarrez le dispositif VMware Cloud Director, l'API de services ou l'interface utilisateur de gestion du dispositif peut signaler par erreur que le service vmware-vcd est dans un état d'échec. Cela se produit lorsque le service vmware-vcd tente de démarrer avant que la pile de mise en réseau du SE ne soit disponible. Par conséquent, le service entre en état d'échec et un message d'erreur s'affiche indiquant que le service n'a pas pu se lier à un ou plusieurs ports. Par la suite, vcd-watchdog démarre le service vmware-vcd, mais l'état de service systemd ne reflète pas cette erreur.

Solution :

1. Exécutez `systemctl reset-failed vmware-vcd.service`.
 2. Exécutez `systemctl start vmware-vcd.service`.
- **Si vous disposez de catalogues abonnés dans votre organisation, lorsque vous mettez à niveau VMware Cloud Director, la synchronisation des catalogues échoue**
Après la mise à niveau, si vous disposez de catalogues abonnés dans votre organisation, VMware Cloud Director n'approuve pas les certificats de point de terminaison publiés automatiquement. Sans l'approbation des certificats, la bibliothèque de contenu ne parvient pas à se synchroniser.

Solution : approuvez manuellement les certificats pour chaque abonnement au catalogue. Lorsque vous modifiez les paramètres d'abonnement au catalogue, une boîte de dialogue TOFU (Trust On First Use, approuver lors de la première utilisation) vous invite à approuver le certificat du catalogue distant.

Si vous ne disposez pas des droits nécessaires pour approuver le certificat, contactez l'administrateur de votre organisation.

- **Après la mise à niveau de VMware Cloud Director et l'activation de la création de clusters Tanzu Kubernetes, aucune stratégie automatiquement générée n'est disponible et vous ne pouvez ni créer ni publier une stratégie**
Lorsque vous mettez à niveau VMware Cloud Director vers la version 10.2 et vCenter Server vers la version 7.0.0d, et que vous créez un VDC fournisseur reposant sur un cluster superviseur, VMware Cloud Director affiche une icône Kubernetes en regard du VDC. Cependant, aucune stratégie Kubernetes n'est automatiquement générée dans le nouveau VDC fournisseur. Lorsque vous tentez de créer ou de publier une stratégie Kubernetes dans un VDC d'organisation, aucune classe de machine n'est disponible.

Solution : approuvez manuellement le certificat de point de terminaison Kubernetes. Pour voir les étapes détaillées, consultez <https://kb.vmware.com/s/article/80996>.

- **Le plug-in Configuration de DRaaS et migration s'affiche deux fois dans la barre de navigation supérieure de l'interface utilisateur de VMware Cloud Director**

Ce problème se produit en raison du changement de nom de vCloud Availability 4.0.0 en VMware Cloud Director Availability 4.0.0 après lequel deux plug-ins existent. VMware Cloud Director ne désactive pas le plug-in vCloud Availability 4.0.0 automatiquement. L'ancienne et la nouvelle versions s'affichent en tant que plug-in Configuration de DRaaS et migration dans la barre de navigation supérieure sous **Plus**.

Solution : désactivez manuellement le plug-in vCloud Availability 4.0.0.

- **Impossible de publier une stratégie Kubernetes de VDC fournisseur sur un VDC si le cluster superviseur vers lequel il pointe n'est pas le cluster principal dans le VDC fournisseur**

Si vous disposez d'un VDC fournisseur comportant plusieurs clusters superviseurs, la publication d'une stratégie Kubernetes de VDC fournisseur qui pointe vers un cluster superviseur non principal échoue avec une erreur `LMException`.

Solution : assurez-vous que le VDC fournisseur repose sur un seul cluster superviseur et que ce cluster est le cluster principal. Un VDC fournisseur peut reposer sur des clusters d'hôtes et un cluster superviseur, mais le cluster superviseur doit être le cluster principal.

- **La saisie d'un nom de cluster Kubernetes avec des caractères non latins désactive le bouton Suivant dans l'assistant Créer un cluster**

Le plug-in Clusters de conteneurs Kubernetes prend en charge uniquement des caractères latins. Si vous entrez des caractères non latins, l'erreur suivante s'affiche. Le nom doit commencer par une lettre et ne contenir que des caractères alphanumériques ou des traits d'union (-). (128 caractères au maximum).

Solution : aucune.

- **Dans le plug-in Clusters de conteneurs Kubernetes, les grilles de données peuvent apparaître vides lors du chargement**
Dans le plug-in Clusters de conteneurs Kubernetes, certaines grilles de données apparaissent vides lors du chargement, car l'indicateur de chargement ne s'affiche pas.

Solution : aucune.

- **Après le redimensionnement d'un cluster TKGI, certaines valeurs de la grille de données s'affichent comme vides ou ne sont pas applicables**

Lorsque vous redimensionnez un cluster VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), les valeurs de cluster de l'organisation et du VDC dans la vue de la grille de données semblent être vides ou sans objet.

Solution : aucune.

- **Lors du filtrage d'une grille à sélections multiples, l'accès à une autre page entraîne la disparition des éléments filtrés**
Dans les grilles à sélections multiples, si vous filtrez les résultats et que plusieurs pages sont disponibles, les pages suivantes des résultats filtrés semblent vides. Ce problème se produit dans les boîtes de dialogue dans lesquelles vous pouvez sélectionner plusieurs éléments dans une liste et les filtrer, par exemple lors de l'ajout de stratégies de stockage à un VDC d'organisation ou le partage d'un vApp ou d'une machine virtuelle avec des utilisateurs ou des groupes.

Solution : redimensionnez les colonnes de la grille.

- **Le filtrage des conseils par priorité entraîne une erreur de serveur interne**

Lorsque vous utilisez VMware Cloud Director API, l'application d'un filtre de priorité à un conseil échoue avec une erreur.

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

Solution : obtenez tous les conseils et filtrez-les manuellement.

- **La documentation de l'API fournit une description incorrecte de l'ordre de tri de la priorité des conseils**

L'objet de modèle de conseil contient un champ de priorité pour spécifier l'urgence de chaque conseil que vous créez. La documentation d'Advisory API indique de manière erronée que les priorités sont répertoriées par ordre de tri décroissant. La documentation de VMware Cloud Director API répertorie les priorités d'un conseil par ordre de tri croissant.

Solution : aucune.

- **Lorsqu'un utilisateur de vApp tente de créer un vApp à partir d'un modèle, cela peut entraîner la génération du message « L'opération est refusée »**

Si votre rôle d'utilisateur attribué est Utilisateur de vApp, lorsque vous tentez de créer un vApp à partir d'un modèle et que vous personnalisez les stratégies de dimensionnement de machine virtuelle pour les machines virtuelles du vApp, le message « L'opération est refusée » est renvoyé. Cela se produit, car le rôle Utilisateur de vApp vous permet d'instancier des vApp à partir de modèles, mais il n'inclut pas les droits qui vous permettent de personnaliser la mémoire, le CPU ou le disque dur d'une machine virtuelle. En modifiant la stratégie de dimensionnement, vous pouvez modifier la mémoire ou le CPU de la machine virtuelle.

Solution : aucune.

- **L'indisponibilité de NFS peut entraîner un dysfonctionnement des fonctionnalités d'un cluster de dispositifs VMware Cloud Director**

Si NFS n'est pas disponible en raison de la saturation du partage NFS, de sa conversion en lecture seule, etc., les fonctionnalités du cluster de dispositifs risquent de présenter des dysfonctionnements. L'interface utilisateur HTML5 ne répond pas lorsque NFS est arrêté ou est inaccessible. Les autres fonctionnalités susceptibles d'être affectées sont la clôture d'une cellule principale ayant échoué, le basculement, la promotion d'une cellule en veille, etc. Pour plus d'informations sur la configuration appropriée du stockage partagé NFS, reportez-vous à la section [Préparation du stockage du serveur de transfert pour le dispositif VMware Cloud Director](#).

Solution :

- corrigez l'état de NFS de sorte qu'il ne soit pas Lecture seule.
- Nettoyez le partage NFS s'il est saturé.

- **L'approbation d'un point de terminaison lors de l'ajout de ressources vCenter Server et NSX dans un environnement multisite n'ajoute pas le point de terminaison à la zone de stockage de certificats centralisée**

Dans un environnement multisite, lors de l'utilisation de l'interface utilisateur HTML5, si vous êtes connecté à un site vCloud Director 10.0 ou que vous tentez d'enregistrer une instance de vCenter Server sur un site vCloud Director 10.0, VMware Cloud Director n'ajoutera pas le point de terminaison à la zone de stockage de certificats centralisée.

Solution :

- importez le certificat sur le site VMware Cloud Director 10.1 à l'aide de l'API.
- Pour déclencher la fonctionnalité de gestion des certificats, accédez au portail d'administration du fournisseur de services du site VMware Cloud Director 10.1, accédez à la boîte de dialogue **Modifier** du service, puis cliquez sur **Enregistrer**.
- **Une tentative de chiffrement des disques nommés dans vCenter Server 6.5 ou version antérieure échoue avec une erreur**
Pour les instances de vCenter Server version 6.5 ou version antérieure, si vous tentez d'associer des disques nommés nouveaux ou existants à une stratégie de chiffrement activé, l'opération échoue avec une erreur Le chiffrement du disque nommé n'est pas pris en charge dans cette version de vCenter Server.

Solution : aucune.

- **Lorsque vous utilisez le portail d'administration du fournisseur de services VMware Cloud Director avec Firefox, vous ne pouvez pas charger les écrans de mise en réseau du locataire**

Si vous utilisez le portail d'administration du fournisseur de services VMware Cloud Director avec Firefox, les écrans de mise en réseau du locataire, par exemple, l'écran **Gérer le pare-feu** pour un centre de données virtuel d'organisation, peuvent ne pas se charger. Ce problème se produit si votre navigateur Firefox est configuré pour bloquer les cookies tiers.

Solution : configurez votre navigateur Firefox afin d'autoriser les cookies tiers.

- **Une machine virtuelle à provisionnement rapide qui est créée sur une baie NFS où l'intégration VAAI (VMware vSphere Storage APIs Array Integration) est activée ou sur des VVol (vSphere Virtual Volumes) ne peut pas être consolidée.**

La consolidation sur place d'une machine virtuelle à provisionnement rapide n'est pas prise en charge lors de l'utilisation d'un snapshot natif. Les snapshots natifs sont toujours utilisés par les banques de données VAAI, ainsi que par les VVol. Lorsqu'une machine virtuelle à provisionnement rapide est déployée sur l'un de ces conteneurs de stockage, cette machine virtuelle ne peut pas être consolidée.

Solution : n'activez pas le provisionnement rapide pour un VDC d'organisation qui utilise des NFS VAAI ou des VVol. Pour consolider une machine virtuelle avec un snapshot sur un VAAI ou une banque de données VVol, déplacez la machine virtuelle vers un conteneur de stockage différent.

- **Après une mise à niveau de vCloud Director 10.0, une machine virtuelle, récemment déployée à partir d'un modèle Linux dans lequel la personnalisation de système d'exploitation invité et la connectivité IPv6 sont activées, rencontre des problèmes de connectivité réseau**

Après la mise à niveau de vCloud Director 10.0, si vous déployez une nouvelle machine virtuelle à l'aide d'un modèle de machine virtuelle Linux créé dans la version 10.0 dans lequel la personnalisation du système d'exploitation invité et la connectivité IPv6 sont activées, la machine virtuelle déployée rencontre des problèmes de connectivité réseau. Cela peut se

produire, car le processus de déploiement crée des entrées en double pour les paramètres VM_DOMAIN_NAME et VM_HOST_NAME du fichier /etc/hosts de la machine virtuelle.

Solution : supprimez les entrées en double VM_DOMAIN_NAME et VM_HOST_NAME du fichier /etc/hosts de la machine virtuelle.

- **Lorsque vous utilisez VMware Cloud Director API pour créer une machine virtuelle à partir d'un modèle et que vous ne spécifiez pas de stratégie de stockage par défaut, s'il n'y a pas paramètre de stratégie de stockage par défaut défini pour le modèle, la machine virtuelle récemment créée tente d'utiliser la stratégie de stockage du modèle source**

Lorsque vous utilisez VMware Cloud Director API pour créer une machine virtuelle à partir d'un modèle et que vous ne spécifiez pas de stratégie de stockage par défaut, si aucune stratégie de stockage par défaut n'est définie pour le modèle, la machine virtuelle récemment créée tente d'utiliser la stratégie de stockage du modèle source au lieu d'utiliser la stratégie de stockage du VDC d'organisation dans lequel vous la déployez.

Solution : aucune.