Notes de mise à jour de VMware Cloud Director 10.1

VMware Cloud Director 10.1 | 9 avril 2020 | Build 15967253 (build installé 15967236)

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

Contenu de ce document

Nouveautés de cette version

- Pour plus d'informations sur les fonctionnalités nouvelles et mises à jour de cette version, reportez-vous au livre blanc technique de VMware Nouveautés de VMware vCloud Director 10.1.
- Comportement modifié dans l'interface utilisateur HTML5 :
  Dans les versions antérieures de VMware Cloud Director, vous pouvez utiliser le menu d'actions de vApp de l'interface utilisateur HTML pour arrêter ou mettre hors tension un vApp. Ces deux opérations annulent le déploiement du vApp, mais affectent différemment le vApp. L'opération Mettre hors tension ne suit pas les paramètres d'ordre de démarrage et d'arrêt des machines virtuelles dans le vApp. Elle annule également le déploiement des réseaux vApp en déconnectant toutes les cartes réseau de machines virtuelles des réseaux VDC d'organisation et en supprimant les passerelles Edge déployées pour le vApp.

  Dans VMware Cloud Director 10.1, effectuer l'opération Mettre hors tension sur un vApp en cours d'exécution entraîne la mise hors tension de toutes les machines virtuelles du vApp sans annuler le déploiement du vApp et des machines virtuelles qu'il contient. Les cartes réseau des machines virtuelles restent connectées aux réseaux respectifs et toutes les passerelles Edge du vApp restent déployées. Le vApp et ses machines virtuelles restent déployées. L'opération Mettre hors tension de chaque machine virtuelle dans le vApp reste active et vous pouvez l'utiliser pour mettre hors tension une machine virtuelle. Elle entraîne l'annulation du déploiement de cette machine virtuelle.

  Lorsque vous mettez hors tension un vApp, l'opération Mettre hors tension suit l'ordre de démarrage que vous avez défini dans les paramètres d'ordre de démarrage et d'arrêt. Par conséquent, les machines virtuelles sont mises hors tension dans l'ordre inverse que vous avez configuré pour le démarrage. Le paramètre Délai d'arrêt n'est pas appliqué au cours de l'opération de mise hors tension. Lorsque vous mettez hors tension un vApp, l'état d'alimentation du vApp, qui est dérivé des états d'alimentation des machines virtuelles qu'il contient, s'affiche comme étant Hors tension.

- Le schéma VMware Cloud Director API 34.0 inclut la définition des attributs `numberOfCpus` et `MemoryAllocationMB`.

Sécurité

- **AVERTISSEMENT :** après la mise à niveau vers la version 10.1, VMware Cloud Director vérifie toujours les certificats pour tous les points de terminaison d'infrastructure qui y sont connectés. Cela est dû à une modification de la manière dont VMware Cloud Director gère les certificats SSL. Si vous n'importez pas vos certificats dans VMware Cloud Director avant la mise à niveau, les connexions vCenter Server et NSX peuvent afficher des erreurs de connexion infructueuses en raison de problèmes de vérification SSL. Dans ce cas, après la mise à niveau, vous avez deux options :
  1. Exécutez la commande de l'outil de gestion des cellules `trust-infra-certs` pour connecter et récupérer automatiquement les certificats de tous les points de terminaison d'infrastructure pour les instances de vCenter Server et de NSX Manager dans le magasin de certificats centralisé. Reportez-vous à la section Importer des certificats de point de terminaison depuis les ressources vSphere.
  2. Dans l'interface utilisateur du portail d'administration du fournisseur de services, sélectionnez chaque instance de vCenter Server et de NSX, puis entrez à nouveau les informations d'identification tout en acceptant le certificat.

- À partir de la version 10.1, les fournisseurs de services et les locataires peuvent utiliser VMware Cloud Director API pour tester les connexions à des serveurs distants et pour vérifier l'identité du serveur dans le cadre d'une négociation SSL. Pour protéger les connexions réseau de VMware Cloud Director, configurez une liste d'exclusion d'hôtes internes qui ne sont pas accessibles aux locataires qui utilisent VMware Cloud Director API pour les tests de connexion. Configurez la liste d'exclusion après l'installation ou la mise à niveau de VMware Cloud Director et avant d'accorder aux locataires l'accès à VMware Cloud Director. Reportez-vous à la section Configurer une liste d'exclusion pour les tests de connexion.
- VMware Cloud Director 10.1 déconseille l'approbation de tous les certificats SSL. Dans cette version, les connexions vCenter Server et NSX ne prennent pas en charge cette option. Pour toutes les autres connexions, l'approbation de tous les certificats est également déconseillée et ne sera plus prise en charge après VMware Cloud Director 10.1. Les administrateurs système doivent se préparer à cette transition.
  - Si vous utilisez le protocole LDAP pour votre organisation du système VMware Cloud Director, vous pouvez utiliser la boîte de dialogue TOFU (trust-on-first-use) dans l'interface utilisateur ou télécharger des certificats à l'aide de l'API.
  - Auditez toutes les utilisations de cette option et fournissez les certificats appropriés à l'aide de l'interface utilisateur ou de l'API.
  - Communiquez les modifications apportées aux locataires. Tous les locataires qui utilisent le protocole LDAP personnalisé lorsque l'option **Accepter tous les certificats** est activée doivent exclure cette configuration. Les locataires peuvent utiliser la boîte de dialogue TOFU (trust-on-first-use) dans l'interface utilisateur ou télécharger des certificats à l'aide de l'API.

Modules Open Source mis à jour

- `jackson-databind` mis à jour vers la version 2.9.10.1.
- `jre` mis à jour vers la version 1.8.0u231.
- `openssl` mis à jour vers la version 1.0.2u.
- `xstream` mis à jour vers la version 1.4.11.1.

Remarques relatives à la prise en charge du produit

VMware Cloud Director 10.1 ne prend pas en charge vSphere 7.0 et NSX-T Data Center 3.0. La certification d'interopérabilité est en cours, et vSphere 7.0 et NSX-T Data Center 3.0 seront pris en charge dans une version de correctif mineure de VMware Cloud Director 10.1.

Les réseaux externes reposant sur des passerelles de niveau 0 VRF-lite dans NSX-T Data Center ne sont pas pris en charge.

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

- La base de données SQL Server n'est plus prise en charge. Seule la base de données PostgreSQL est prise en charge.
- Oracle Linux n'est plus pris en charge en tant que système d'exploitation hôte pour installer l'application VMware Cloud Director.
- Les versions 20 et antérieures de VMware Cloud Director API ne sont pas prises en charge.
- Les versions 27.0 à 29.0 de VMware Cloud Director API sont déconseillées et ne seront plus prises en charge après VMware Cloud Director 10.1
- VMware Cloud Director API version 30.0 est déconseillé.
- L'interface utilisateur basée sur Flex a été supprimée du produit et n'est plus prise en charge.
- Le point de terminaison de connexion de l'API `/api/sessions` est déconseillé dans 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, et sera supprimée dans une version ultérieure. Vous devez utiliser `/api/server_status` pour les protocoles HTTP et HTTPS.
- Les actions de réinitialisation `/ldap/action/resetLdapCertificate` et `/ldap/action/resetLdapKeyStore` ont été supprimées de 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 les versions ultérieures. 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 ne sera pas 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.

Remarque concernant la fin prochaine de la prise en charge

- VMware Cloud Director API 34.0 (VMware Cloud Director 10.1) contient des API en phase de désapprobation accélérée et qui seront supprimées des versions ultérieures. Reportez-vous au Guide de programmation de VMware Cloud Director API.

Mise à niveau à partir des versions précédentes

Pour plus d'informations sur la mise à niveau vers VMware Cloud Director 10.1, 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 réseau et protocoles utilisés par VMware Cloud Director 10.1, consultez Ports et protocoles VMware.

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

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

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

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 requiert RabbitMQ version 3.7.9 ou 3.8.2.

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

Vous pouvez configurer votre installation de VMware Cloud Director de façon à stocker les mesures que VMware Cloud Director collecte sur les performances et la consommation de ressources de la machine virtuelle. Les données des mesures historiques sont stockées dans une base de données Cassandra. VMware Cloud Director prend en charge Cassandra versions 3.*x*.

Pour plus d'informations, reportez-vous au *Guide d'installation, de configuration et de mise à niveau de VMware Cloud Director*.

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
bash
chkconfig
coreutils
findutils
glibc
grep
initscripts
krb5-libs
libgcc
libICE
libSM
libstdc++
libX11
libXau
libXdmcp
libXext
libXi
libXt
libXtst
module-init-tools
net-tools
pciutils
procps
redhat-lsb
sed
tar
wget
which
```

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 d'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
- Microsoft Internet Explorer 11

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

- **Lorsque vous associez deux sites de dispositifs VMware Cloud Director, les objets ne sont pas visibles sur les sites**
  Si vous créez une association de sites et que vos sites disposent d'objets tels que des organisations, des VDC d'organisation, des vApp ou des machines virtuelles, vous ne pouvez pas voir les objets du site actuel. L'interface utilisateur HTML 5 affiche uniquement les objets de l'autre site associé. Ce problème se produit lors d'une communication multisite ramifiée, car le fichier `/etc/hosts` du dispositif VMware Cloud Director ne dispose pas du contenu approprié.

- **La mise à jour d'une stratégie de dimensionnement de machine virtuelle échoue avec une erreur d'allocation de mémoire**
  Si vous convertissez un VDC de pool d'allocation en un VDC d'organisation Flex, vCloud Director conserve les informations de stratégie maximales du VDC de pool d'allocation avant la conversion. Les garanties de réservation de CPU ou de mémoire supérieures aux réservations définies dans le VDC de pool d'allocation échouent avec l'erreur `La réservation de machine virtuelle ou les paramètres de limite ou de parts ne sont pas valides.`

- **La mise au repos ou en pause d'une cellule principale dans un environnement à cellules multiples ne fait pas redémarrer les tâches sur la cellule secondaire**
  Dans un environnement à cellules multiples, lorsque vous mettez la cellule principale en veille ou en pause, les tâches périodiques qui s'exécutent en arrière-plan de la cellule principale ne sont pas démarrées à partir de la cellule secondaire.

- **Le clonage d'une machine virtuelle observant une stratégie de stockage basée sur l'hôte pour laquelle des services de données sont activés sur une machine virtuelle observant une autre stratégie de stockage basée sur l'hôte échoue avec une erreur**
  Si vous créez une machine virtuelle observant une stratégie de stockage incluant des règles basées sur l'hôte, telles que l'IOPS ou le chiffrement de VM activé, la tentative de clonage de la machine virtuelle et de modification de la stratégie de stockage de la machine virtuelle cible échoue avec l'erreur `La modification ou l'application de stratégies de stockage de VM incluant une capacité de service de données pendant des opérations de clonage est interdite. Les stratégies de stockage de machine virtuelle incluant des capacités de service de données peuvent être attribuées à la machine virtuelle provisionnée après l'opération de clonage et avant la mise sous tension de la machine virtuelle.`

- **Le rôle de locataire global Auteur de vApp peut télécharger et créer des modèles et des supports sans disposer des droits nécessaires pour ces opérations**
  Par défaut, le rôle de locataire global Auteur de vApp dispose du droit `Ajouter un vApp à partir de Mon Cloud`. Comme ce droit et le droit `Modèle/support : Créer/Télécharger` partagent une seule opération, VMware Cloud Director accorde également de manière incorrecte le droit `Modèle/Support : Créer/Télécharger` au rôle Auteur de vApp.

  Le problème est résolu. Si vous souhaitez que le rôle Auteur de vApp continue de disposer du droit `Modèle/Support : Créer/Télécharger`, un fournisseur de services peut ajouter le droit au rôle global Auteur de vApp et le publier dans une organisation.

- **Les machines virtuelles récemment créées sont déployées sur la stratégie de stockage par défaut du VDC d'organisation**
  Dans le portail de locataires vCloud Director, lorsque vous créez une machine virtuelle autonome, l'option pour spécifier la stratégie de stockage est manquante. Par conséquent, la machine virtuelle créée est déployée avec la stratégie de stockage par défaut du VDC d'organisation.

Problèmes connus

- **Nouveau Impossible d'ouvrir une console Web de machine virtuelle avec Microsoft Internet Explorer 11**
  L'utilisation de Microsoft Internet Explorer 11 pour vous connecter à la console d'une machine virtuelle ouvre une fenêtre vide blanche et vous ne pouvez pas accéder à la console de machine virtuelle.

  Solution : aucune.

- **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 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 L'utilisation de VMware Cloud Director API pour interroger un vApp renvoie des champs vides pour les attributs numberOfCpus et MemoryAllocationMB**
  Lorsque vous utilisez VMware Cloud Director API 33.0 ou une version antérieure pour exécuter une requête de vApp REST API, le corps de la réponse REST API renvoie des champs vides pour les attributs `numberOfCpus` et `MemoryAllocationMB`. Cela peut se produire, car le schéma d'API n'inclut pas la définition des attributs `numberOfCpus` et `MemoryAllocationMB`.

  Solution : utilisez VMware Cloud Director API 34.0 pour interroger un vApp.

- **Nouveau 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 ensemble pour la redistribution, code d'erreur 503266 ».

  Solution : utilisez l'API de stratégie de NSX-T Data Center pour mettre à jour la configuration de la redistribution du réseau externe auquel la passerelle Edge NSX-T est connectée.

  1. Notez l'ID du routeur de niveau 0 dont dépend le réseau externe auquel votre passerelle Edge NSX-T est connectée.
     - Effectuez une demande GET pour obtenir une liste des routeurs de niveau 0 dans votre environnement.
       `GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s`

- Examinez la liste pour identifier le niveau 0 par son nom d'affichage, qui correspond au nom du routeur de niveau 0 dans l'onglet Informations générales pour le réseau externe dans l'interface utilisateur de VMware Cloud Director.

2. Mettez à jour le réseau externe (passerelle de niveau 0) manuellement.

   - Effectuez une demande GET pour obtenir la liste des `localeServices` sur le routeur.
     `GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services`
     La réponse renvoie un service de paramètres régionaux.
   - Copiez l'`ID localeService` et effectuez une demande GET pour l'examiner.

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

     La réponse renvoie la liste des propriétés du service de paramètres régionaux.

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

   - Modifiez la réponse de la manière suivante.

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

   - Effectuez une demande PUT avec les propriétés modifiées pour mettre à jour le `LocaleService` du routeur de niveau 0.

- Nouveau **Échec du déplacement d'une machine virtuelle vers un autre cluster si le conteneur de stockage cible est un cluster de banque de données**
  Lorsque vous effectuez une opération qui entraîne une tentative de déplacement d'une machine virtuelle vers un autre cluster et que le conteneur de stockage cible est un cluster de banque de données, la migration échoue avec une erreur `NO_FEASIBLE_PLACEMENT_SOLUTION`. Dans les journaux de VMware Cloud Director, vous voyez une erreur d'invocation de Storage DRS avec `invalidProperty = spec.host`.

  Solution :

  1. Utilisez vSphere Client pour désactiver Storage DRS sur le cluster de banque de données cible ou utilisez VMware Cloud Director API pour modifier le stockage cible pour le déplacement vers une banque de données.

2. Retentez l'opération qui a échoué.

- Nouveau **Échec du déploiement du dispositif VMware Cloud Director lorsque vous activez le paramètre d'expiration du mot de passe racine lors de la première connexion**
  Si vous tentez de déployer un dispositif avec le paramètre **Expiration du mot de passe racine lors de la première connexion** activé, le déploiement échoue et le fichier journal `/opt/vmware/var/log/firstboot` affiche une erreur :

  ```
  [ERROR] postgresauth script failed to execute.
  ```

  Solution : désactivez le paramètre **Expiration du mot de passe racine lors de la première connexion** et spécifiez un mot de passe racine initial contenant au moins huit caractères, une majuscule, une minuscule, un chiffre et un caractère spécial.

- Nouveau **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.

- Nouveau **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.
- Nouveau **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**.

- **Nouveau Une tentative de chiffrement des disques nommés dans vCenter Server version 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.

- **Nouveau Dans un environnement multisite mixte avec VMware Cloud Director 10.0 et 10.1, l'approbation des certificats pour les connexions vCenter Server et NSX fonctionne uniquement pour les objets du site local**
  Si vous disposez d'un environnement multisite avec les versions 10.0 et 10.1 de VMware Cloud Director associées l'une à l'autre, lorsque vous vous connectez à l'un des sites, vous ne pouvez pas enregistrer des instances de vCenter Server ou de NSX Manager sur l'autre site.

  Solution : connectez-vous au site dans lequel vous souhaitez enregistrer l'instance de vCenter Server ou de NSX Manager, puis démarrez le processus d'enregistrement.

- **Nouveau Dans le portail de locataires de VMware Cloud Director, vous ne pouvez pas filtrer les machines virtuelles par centre de données à partir de l'option de filtrage avancé pour les machines virtuelles sous l'onglet Applications**
  Dans le portail de locataires de VMware Cloud Director, lorsque vous accédez à l'option Machines virtuelles sous l'onglet Applications dans la barre de navigation supérieure, le filtrage des machines virtuelles par centre de données à partir de l'option de filtrage avancé génère une erreur `Demande incorrecte : Nom de propriété inconnu vdcName`.

  Solution : dans la barre de navigation supérieure, sélectionnez **Centres de données** et sélectionnez un centre de données pour afficher les machines virtuelles qu'il contient.

- **Nouveau Les services d'extension ne peuvent pas traiter les messages RabbitMQ de VMware Cloud Director**
  Les services d'extension qui reposent sur RabbitMQ ne peuvent pas obtenir l'en-tête `notification.type` d'un message, car l'en-tête a un nouveau nom temporaire. Le nom d'en-tête pour VMware Cloud Director 10.1.0 est `notification.operationType`.

  Solution : si vos services d'extension traitent des messages RabbitMQ de VMware Cloud Director et que vous utilisez l'en-tête de message `notification.type`, vous devez les modifier. Si l'en-tête notification.type n'est pas disponible, les services d'extension doivent obtenir la valeur de l'en-tête `notification.operationType`. Cette modification est nécessaire uniquement pour la version 10.1.0.

- **Dans le portail d'administration du fournisseur de services VMware Cloud Director, la suppression d'un centre de données virtuel d'organisation échoue avec une erreur**
  Dans le portail d'administration du fournisseur de services VMware Cloud Director, si vous ajoutez une passerelle Edge à votre VDC d'organisation et que vous activez la passerelle pour fournir le routage distribué VMware Cloud Director, la tentative de suppression récursive du VDC d'organisation échoue avec un message d'erreur `Impossible de supprimer le réseau VDC d'organisation`.

  Solution :

  1. à l'aide de l'API, supprimez les réseaux VDC d'organisation et les passerelles Edge associées au VDC d'organisation.
  2. À l'aide de l'API, supprimez le VDC d'organisation.
- **Si vous désactivez l'accès du fournisseur au point de terminaison de la connexion à l'API héritée, toutes les intégrations d'API qui reposent sur la connexion de l'administrateur système cessent de**

fonctionner, y compris vCloud Usage Meter et vCloud Availability for VMware Cloud Director
À partir de vCloud Director 10.0, vous pouvez utiliser des points de terminaison de connexion VMware Cloud Director OpenAPI distincts pour l'accès du fournisseur de services et des locataires à VMware Cloud Director. Si l'accès du fournisseur de services au point de terminaison `/api/sessions` hérité est désactivé, les produits qui s'intègrent à VMware Cloud Director, comme vCloud Usage Meter et vCloud Availability for VMware Cloud Director, cessent de fonctionner. Ces produits nécessitent un correctif pour continuer à fonctionner.

Le problème concerne uniquement les administrateurs système. La connexion du locataire n'est pas affectée.

Solution : réactivez l'accès du fournisseur de services au point de terminaison `/api/sessions` hérité à l'aide de l'outil de gestion des cellules.

- **Lorsque vous modifiez les valeurs de garantie de réservation d'un VDC, les machines virtuelles existantes ne sont pas mises à jour en conséquence même après un redémarrage**
  Si vous disposez d'un VDC d'organisation Flex avec la stratégie système par défaut et que des machines virtuelles sous tension sur ce VDC sont associées à la stratégie de dimensionnement par défaut, lorsque vous augmentez la valeur de garantie des ressources du VDC, la réservation de ressources pour les machines virtuelles existantes n'est pas mise à jour et elles ne sont pas non plus marquées comme non conformes. Ce problème se produit également lorsque vous convertissez un modèle d'allocation de VDC hérité en modèle d'allocation Flex et que les machines virtuelles existantes deviennent non conformes avec la nouvelle stratégie par défaut du VDC d'organisation Flex après la conversion.

  Solution :

  1. Pour trouver l'identifiant de la machine virtuelle, dans le portail des locataires de VMware Cloud Director, accédez à la page Détails de la machine virtuelle. L'URL affiche l'identifiant `https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifier/general`
  2. Pour afficher les machines virtuelles non conformes dans l'interface utilisateur de VMware Cloud Director, effectuez une vérification de conformité explicite par rapport aux machines virtuelles à l'aide de VMware Cloud Director API.
     `POST: https://VCD_IP_Address/api/vApp/vm-Identifier/action/checkComputePolicyCompliance`
  3. Pour réappliquer la stratégie et reconfigurer les réservations de ressources, dans le portail de locataires de VMware Cloud Director, cliquez sur **Rendre la VM conforme** pour une machine virtuelle non conforme.
- **VMware Cloud Director affiche des informations incorrectes sur les machines en cours d'exécution, l'ensemble des machines virtuelles, ainsi que des statistiques de CPU et de mémoire erronées dans des instances dédiées de vCenter Server**
  Si une instance dédiée de vCenter Server est de version 6.0 Update 3i ou antérieure, 6.5 Update 2 ou antérieure, ou 6.7 Update 1 ou antérieure, VMware Cloud Director affiche des informations incorrectes sur les machines virtuelles en cours d'exécution et sur l'ensemble des machines virtuelles, ainsi que des informations statistiques erronées sur le CPU et la mémoire dans l'instance de vCenter Server. La vignette de l'instance dédiée de vCenter Server dans le portail de locataires et les informations sur cette instance dans le portail d'administration du fournisseur de services affichent zéro pour le nombre de machines virtuelles en cours d'exécution et le nombre total de machines virtuelles, en dépit de la présence de machines virtuelles dans l'environnement vSphere.

  Solution : mettez à niveau l'instance de vCenter Server vers la version 6.0 Update 3j, 6.5 Update 3, 6.7 Update 2 ou version ultérieure.

- **La modification de la stratégie de calcul d'une machine virtuelle sous tension peut échouer**
  Lors d'une tentative de modification de la stratégie de calcul d'une machine virtuelle sous tension, si la nouvelle stratégie de calcul est associée à une stratégie de calcul de VDC fournisseur comportant des groupes de machines virtuelles ou des groupes de machines virtuelles logiques, une erreur se produit. Le

message d'erreur contient : `Erreur système sous-jacente : com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation`.

Solution : mettez la machine virtuelle hors tension et recommencez l'opération.

- **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.

- **VMware Cloud Director 10.1 prend en charge uniquement une liste de paramètres d'entrée des workflows vRealize Orchestrator**
  VMware Cloud Director 10.1 prend en charge les paramètres d'entrée des workflows vRealize Orchestrator suivants :

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

  Solution : aucune

- **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.

- **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.