vmware®

VMware Cloud Director 10.2.2.1 Release Notes

VMware Cloud Director 10.2.2.1 | 16 SEP 2021 | Build 18634229 (installed build 18634228)

Check for additions and updates to these release notes.

What's in this Document

- What's New
- System Requirements and Installation
- Documentation
- Previous Releases of VMware Cloud Director 10.2.x
- Resolved Issues
- Known Issues

What's New

The VMware Cloud Director 10.2.2.1 patch release provides bug fixes, updates the VMware Cloud Director appliance base OS and the VMware Cloud Director open-source components.

System Requirements and Installation

For information about system requirements and installation instructions, seeVMware Cloud Director 10.2 Release Notes.

Documentation

To access the full set of product documentation, go toVMware Cloud Director Documentation.

Previous Releases of VMware Cloud Director 10.2.x

VMware Cloud Director 10.2.2 Release Notes

VMware Cloud Director 10.2.1 Release Notes

VMware Cloud Director 10.2 Release Notes

Resolved Issues

- **New** VMware Cloud Director cannot load the login page

-
  If the jms.user.system.password value is missing from the VMware Cloud Director database, the cell fails to start and the VMware Cloud Director UI becomes unresponsive.
  The appliance log file displays the following error message.

  could not apply d0f0b0ec590... vten-4895: Ignore cache refresh if the property contains jms properties

- **New Importing a Bitnami application catalog from VMware Marketplace in VMware Cloud Director App Launchpad fails to complete and times out in an hour**
  As a service provider, when you subscribe an organization to a Bitnami application catalog from VMware Marketplace in VMware Cloud Director App Launchpad, the import process fails to complete and times out in an hour. The applications in the catalog are still available to tenants but launching an application from the catalog fails.

- **New Reauthentication to VMware Cloud Director by using a SAML user fails with a Single sign-on failed for this organization error message**
  If you log to VMware Cloud Director by using a SAML user configured to time out after more than 2 hours, when the VMware Cloud Director session expires and you try to reauthenticate by using the same SAML session, the operation fails with an error message.

  VMware Cloud Director SSO Failure. Single sign-on failed for this organization.

- **If you do not delete certain certificate and truststore files before upgrading a cell to VMware Cloud Director 10.2.2, the cell becomes inoperable**
  If any of the certificates.bak, proxycertificates.bak, and truststore.bak files exist in the /opt/vmware/vcloud-director/etc/ folder of the cell, after upgrading to version 10.2.2, the cell becomes inoperable. The logs show the following error.

  cp: cannot stat '/opt/vmware/vcloud-director/etc/proxycertificates.pem': No such file or directory

  cp: cannot stat '/opt/vmware/vcloud-director/etc/proxycertificates.key': No such file or directory

- **Powering on a vApp fails with Unable to deploy network error message**
  If a vApp consists of VMs in different power state, powering on the vApp fails with an error message.
  Unable to deploy network *network-name*. Failed to create distributed virtual port group because a distributed virtual port group of that name already exists.
  A subsequent power on of the vApp completes successfully.

- **In an NSX Data Center for vSphere edge gateway, adding a new static IP address to the list of suballocated IP pools fails with an error message**
  In an NSX Data Center for vSphere edge gateway with enabled IPsec VPN service, if the next hop IP address exists outside the subnet of the associated external network, adding a new static IP address to the list of suballocated IP pools fails with an error message.
  Static route next ho IP is not valid on selected interface.

- **The grid list view of IP allocation on an NSX Data Center for vSphere edge gateway appears empty**
  When you log in as an organization administrator to the tenant portal, the grid list view of IP allocation on an NSX Data Center for vSphere edge gateway appears empty.

- **Deploying a vApp from an OVF package fails with an error message**
  In VMware Cloud Director, if you generate an OVA file for a vApp configured with at least one

  disk larger than 8 GB, and you attempt to create a new vApp using this OVA file, the create
  operation fails with an error message.

operation fails with an error message.

The selected OVF is referencing more files that you are uploading.

This happens because the OVA file that you generate for the vApp is corrupted and is not usable.

- **While viewing the available VM consoles in a vApp, clicking on VM Consoles for a second time displays an empty list of available VM consoles**
  In the VMware Cloud Director tenant portal, if you view the vApps in a grid view, clicking **VM Consoles** for a second time results in an empty list of available VM consoles for the selected vApp.

- **The VMware Cloud Director HTML5 UI displays the old name for a renamed virtual machine**
  After renaming a VM, the **Name in vSphere** field on the VM general tab displays the old name instead of the new one.

- **In a multi-cell VMware Cloud Director installation, the synchronization of a subscribed catalog times out**
  If you disable the automatic download of content from an external catalog to a subscribed catalog, synchronizing the catalogs freezes at one percent and times out.

- **The Enable Logging toggle is active for an organization administrator role without the required set of rights**
  The **Enable Logging** toggle is active for a user assigned the organization administrator role even if the role does not have the **Configure System Logging** rights.

- **After reconnecting a vCenter Server instance, different vApp operations fail**
  After reconnecting a vCenter Server instance, different vApp operations, like deploying a new VM or a vApp, fail with an error message.

- **Creating a distributed firewall rule configured with a stretched network as the source fails with an error message**
  When attempting to create a distributed firewall rule, if you configure a stretched organization VDC network as the source, the create operation fails with an error message.
  Distributed Firewall rule <Firewall-name> has an invalid specification.

- **After reverting a VM to a snapshot, the VM network appears as disconnected**
  If you shutdown the guest operating system of a virtual machine by using the VM console and then you take a snapshot of a virtual machine, after reverting to the snapshot and powering on the VM, the VM network appears is disconnected.

- **Cluster updates in vCenter Server are increasing the CPU and memory consumption in VMware Cloud Director**
  Triggering different cluster updates in vCenter Server results in increased size of the VMware Cloud Director database, which can lead to high CPU and memory usage.

- **Some VM and vApp operations fail with a <DomainName> should not be provided when using Org settings error message**
  Editing a VM and deploying a VM or a vApp by using a template operations fail with an error message.
  <DomainName> should not be provided when using Org settings

- **Auto scale rule stops working**
  24 hours after you configure an auto scaling rule, the auto scaling service looses connection to VMware Cloud Director and the rule that triggers the growing or shrinking of scale groups stops working.

- **Powering on a VM fails with a No compatible host has sufficient resources to satisfy the reservation error message**
  In a provider virtual data center that has more than one resource pools, when you attempt to power on a VM, the operation fails with an error message.
  No compatible host has sufficient resources to satisfy the reservation.

Known Issues

- **New The Customer Experience Improvement Program (CEIP) status isEnabled even after deactivating it during the installation of VMware Cloud Director**
  During the installation of VMware Cloud Director, if you deactivate the option to join the CEIP, after the installation completes, the CEIP status is active.

  Workaround: Deactivate the CEIP by following the steps in theJoin or Leave the VMware Customer Experience Improvement Program procedure.

- **New Refreshing the LDAP page in your browser does not take you back to the same page**
  In the Service Provider Admin Portal, refreshing the **LDAP** page in your browser takes you to the provider page instead of back to the LDAP page.

  Workaround: None.

- **New VMs become non-compliant after converting a reservation pool VDC into a flex organization VDC**
  In an organization VDC with a reservation pool allocation model, if some of the VMs have nonzero reservation for CPU and Memory, non-unlimited configuration for CPU and Memory, or both, after converting into a flex organization VDC, these VMs become non-compliant. If you attempt to make the VMs compliant again, the system applies an incorrect policy for the reservation and limit and sets the CPU and Memory reservations to zero and the limits to **Unlimited**.

  Workaround:

  1. A system administrator must create a VM sizing policy with the correct configuration.
  2. A system administrator must publish the new VM sizing policy to the converted flex organization VDC.
  3. The tenants can use the VMware Cloud Director API or the VMware Cloud Director Tenant Portal to assign the VM sizing policy to the existing virtual machines in the flex organization VDC.

- **New When you enable FIPS mode, the vRealize Orchestrator integration fails with an error related to invalid parameters.**

  When you enable FIPS mode, the integration between VMware Cloud Director and vRealize Orchestrator does not work. The VMware Cloud Director UI returns an Invalid VRO request params error. The API calls return the following error:

Caused by: java.lang.IllegalArgumentException: 'param' arg cannot be null at
org.bouncycastle.jcajce.provider.ProvJKS$JKSKeyStoreSpi.engineLoad(Unknown Source) at
java.base/java.security.KeyStore.load(KeyStore.java:1513) at
com.vmware.vim.install.impl.CertificateGetter.createKeyStore(CertificateGetter.java:128) at
com.vmware.vim.install.impl.AdminServiceAccess.(AdminServiceAccess.java:157) at
com.vmware.vim.install.impl.AdminServiceAccess.createDiscover(AdminServiceAccess.java:238) at
com.vmware.vim.install.impl.RegistrationProviderImpl.(RegistrationProviderImpl.java:56) at
com.vmware.vim.install.RegistrationProviderFactory.getRegistrationProvider(RegistrationProviderFactory.java:143)
at com.vmware.vcloud.vro.client.connection.STSClient.getRegistrationProvider(STSClient.java:126) ... 136 more

Workaround: None.

- **New** **After upgrading to VMware Cloud Director 10.2.2.1, the Save button in the Edit Hard Disks wizard is greyed out**
  After upgrading to VMware Cloud Director 10.2.2.1, when you attempt to add a new hard disk to a VM, the **Save** button in the **Edit Hard Disks** wizard is greyed out and you cannot update the VM hard disk properties.

  Workaround: This issue is fixed in VMware Cloud Director 10.2.2.1a.

- **After upgrading to vCenter Server 7.0 Update 2a or Update 2b, you cannot create Tanzu Kubernetes Grid clusters**
  If the underlying vCenter Server version is 7.0 Update 2a or Update 2b, when you try to create a Tanzu Kubernetes Grid cluster by using the Kubernetes Container Clusters plug-in, the task fails.

  Workaround: None.

- **When using FIPS mode, trying to upload OpenSSL-generated PKCS8 files fails with an error**
  OpenSSL cannot generate FIPS-complaint private keys. When VMware Cloud Director is in FIPS mode and you try to upload PKCS8 files generated using OpenSSL, the upload fails with a Bad request: org.bouncycastle.pkcs.PKCSException: unable to read encrypted data: ... not available: No such algorithm: ... error or salt must be at least 128 bits error.

  Workaround: Disable FIPS mode to upload the PKCS8 files.

- **After upgrade, the System Configuration page of the VMware Cloud Director appliance management UI does not appear**
  After upgrading VMware Cloud Director appliance to version 10.2.2, the new System Configuration page of the appliance management UI does not appear.

  Workaround: To work around the issue and prevent it from recurring, clear the browser cache.

- **Creation of Tanzu Kubernetes cluster by using the Kubernetes Container Clusters plug-in fails**

  When you create a Tanzu Kubernetes cluster by using the Kubernetes Container Clusters plug-in, you must select a Kubernetes version. Some of the versions in the drop-down menu are not compatible with the backing vSphere infrastructure. When you select an incompatible version, the cluster creation fails.

Workaround: Delete the failed cluster record and retry with a compatible Tanzu Kubernetes version. For information on the incompatibilities between Tanzu Kubernetes and vSphere, see [Updating the vSphere with Tanzu Environment](#)

- **If you have any subscribed catalogs in your organization, when you upgrade VMware Cloud Director, the catalog synchronization fails**
  After upgrade, if you have subscribed catalogs in your organization, VMware Cloud Director does not trust the published endpoint certificates automatically. Without trusting the certificates, the content library fails to synchronize.

  Workaround: Manually trust the certificates for each catalog subscription. When you edit the catalog subscription settings, a trust on first use (TOFU) dialog prompts you to trust the remote catalog certificate.
  If you do not have the necessary rights to trust the certificate, contact your organization administrator.

- **After upgrading VMware Cloud Director and enabling the Tanzu Kubernetes cluster creation, no automatically generated policy is available and you cannot create or publish a policy**
  When you upgrade VMware Cloud Director to version 10.2.2 and vCenter Server to version 7.0.0d or later, and you create a provider VDC backed by a Supervisor Cluster, VMware Cloud Director displays a Kubernetes icon next to the VDC. However, there is no automatically generated Kubernetes policy in the new provider VDC. When you try to create or publish a Kubernetes policy to an organization VDC, no machine classes are available.

  Workaround: Manually trust the corresponding Kubernetes endpoint certificates.
  See VMware knowledge base article [83583](#).

- **The Setup DRaaS and Migration plug-in appears twice in the VMware Cloud Director UI top navigation bar**
  The issue occurs because of the rebranding of vCloud Availability 4.0.0 to VMware Cloud Director Availability 4.0.0 after which two plug-ins exist. VMware Cloud Director does not disable the vCloud Availability 4.0.0 plug-in automatically. The old and new versions appear as the Setup DRaaS and Migration plug-in in the top navigation bar under **More**.

  Workaround: Disable the vCloud Availability 4.0.0 plug-in. For information on how to disable a plug-in, see [Enable or Disable a Plug-in](#)

- **Entering a Kubernetes cluster name with non-Latin characters disables the Next button in the Create New Cluster wizard**
  The Kubernetes Container Clusters plug-in supports only Latin characters. If you enter non-Latin characters, the following error appears. Name must start with a letter and only contain alphanumeric or hyphen (-) characters. (Max 128 characters).

  Workaround: None.

- **After resizing a TKGI cluster, some values in the data grid appear as blank or not applicable**
  When you resize a VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) cluster, the cluster values for the organization and VDC in the data grid view appear to be blank or N/A.

Workaround: None.

- **Filtering of advisories by priority results in an internal server error**
  When you use the VMware Cloud Director API, applying a priority filter to an advisory fails with an error.

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

  Workaround: Obtain all advisories and filter them manually. For information, see the VMware Cloud Director OpenAPI documentation.

- **The API documentation provides an incorrect description of the Advisory priority sort order**
  The Advisory model object contains a priority field to specify the urgency of each advisory that you create. The Advisory API documentation incorrectly states that the priorities are listed in descending sort order. The VMware Cloud Director API documentation lists the priorities for an advisory in ascending sort order.

  Workaround: None.

- **NFS downtime can cause VMware Cloud Director appliance cluster functionalities to malfunction**
  If the NFS is unavailable due to the NFS share being full, becoming read only, and so on, can cause appliance cluster functionalities to malfunction. HTML5 UI is unresponsive while the NFS is down or cannot be reached. Other functionalities that might be affected are the fencing out of a failed primary cell, switchover, promoting a standby cell, and so on. For more information about setting up correctly the NFS shared storage, see Preparing the Transfer Server Storage for the VMware Cloud Director Appliance.

  Workaround:

  - Fix the NFS state so that it is not read-only.
  - Clean up the NFS share if it is full.

- **Trusting an endpoint while adding vCenter Server and NSX Resources in a multisite environment does not add the endpoint to the centralized certificate storage area**
  In a multisite environment, while using the HTML5 UI, if you are logged in to a vCloud Director 10.0 site or trying to register a vCenter Server instance to a vCloud Director 10.0 site, VMware Cloud Director will not add the endpoint to the centralized certificate storage area.

  Workaround:

  - Import the certificate into the VMware Cloud Director 10.1 site by using the API.
  - To trigger the certificate management functionality, navigate to the SP Admin Portal of the VMware Cloud Director 10.1 site, go to the **Edit** dialog of the service, and click **Save**.

- **Trying to encrypt named disks in vCenter Server version 6.5 or earlier fails with an error**
  For vCenter Server instances version 6.5 or earlier, if you try to associate new or existing named disks with an encryption enabled policy, the operation fails with a Named disk encryption

is not supported in this version of vCenter Server. error.

Workaround: None.

- **When using the VMware Cloud Director Service Provider Admin Portal with Firefox, you cannot load the tenant networking screens**
  If you are using the VMware Cloud Director Service Provider Admin Portal with Firefox, the tenant networking screens, for example, the **Manage Firewall** screen for an organization virtual data center, might fail to load. This issue happens if your Firefox browser is configured to block Third-Party cookies.

  Workaround: Configure your Firefox browser to allow third-party cookies. For information, go to https://support.mozilla.org/en-US/ and see the **Websites say cookies are blocked - Unblock them** KB.

- **A fast-provisioned virtual machine created on a VMware vSphere Storage APIs Array Integration (VAAI) enabled NFS array, or vSphere Virtual Volumes (VVols) cannot be consolidated**
  In-place consolidation of a fast provisioned virtual machine is not supported when a native snapshot is used. Native snapshots are always used by VAAI-enabled datastores, as well as by VVols. When a fast-provisioned virtual machine is deployed to one of these storage containers, that virtual machine cannot be consolidated .

  Workaround: Do not enable fast provisioning for an organization VDC that uses VAAI-enabled NFS or VVols. To consolidate a virtual machine with a snapshot on a VAAI or a VVol datastore, relocate the virtual machine to a different storage container.

- **After upgrade to VMware Cloud Director 10.2.x, importing an SSL certificate from Cassandra fails with an error message in the cell-management-tool**
  When you use the cell-management-tool to import SSL from Cassandra, the operation fails with an error message.
  Unable to load VCD's SSL context.

  Workaround: Use the VMware Cloud Director Service Provider Admin Portal to import the SSL from Cassandra. For information, seeImport Trusted Certificates.

- **When you use the VMware Cloud Director API to create a VM from a template and you don't specify a default storage policy, if there is no default storage policy set for the template, the newly created VM attempts to use the storage policy of the source template itself**
  When you use the VMware Cloud Director API to create a VM from a template and you don't specify a default storage policy, if there is no default storage policy set for the template, the newly created VM attempts to use the storage policy of the source template itself instead of using the storage policy of the organization VDC in which you are deploying it.

  Workaround: None.